

Data Encryption Workshop

User Guide

Issue 35
Date 2025-01-23



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2025. All rights reserved.

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

Trademarks and Permissions



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

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

Notice

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

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

Contents

1 Key Management Service.....	1
1.1 Key Types.....	1
1.2 Creating a Key.....	2
1.3 Creating CMKs Using Imported Key Materials.....	6
1.3.1 Overview.....	6
1.3.2 Importing Key Materials.....	7
1.3.3 Deleting Key Materials.....	17
1.4 Managing CMKs.....	18
1.4.1 Viewing a Key.....	18
1.4.2 Enabling a Key.....	20
1.4.3 Disabling a Key.....	21
1.4.4 Deleting a Key.....	22
1.4.5 Canceling the Scheduled Deletion of One or More CMKs.....	23
1.4.6 Adding a Key to a Project.....	24
1.4.7 Viewing the Number of Key Accounting Requests.....	25
1.5 Searching for a Key.....	27
1.6 Using the Online Tool to Encrypt and Decrypt Small-Size Data.....	27
1.7 Key Alias.....	29
1.8 Managing Tags.....	30
1.8.1 Adding a Tag.....	30
1.8.2 Modifying Tag Values.....	32
1.8.3 Deleting Tags.....	33
1.9 Rotating CMKs.....	34
1.9.1 About Key Rotation.....	34
1.9.2 Enabling Key Rotation.....	36
1.9.3 Disabling Key Rotation.....	39
1.10 Managing a Grant.....	40
1.10.1 Creating a Grant.....	40
1.10.2 Querying a Grant.....	43
1.10.3 Revoking a Grant.....	45
1.10.4 Editing a Grant.....	46
2 Cloud Secret Management Service.....	48
2.1 Secret Overview.....	48

2.2 Rotation Policy.....	49
2.3 Creating a Secret.....	50
2.3.1 Creating a Shared Secret.....	50
2.3.2 Creating a Rotation Secret.....	52
2.4 Managing Secrets.....	57
2.4.1 Viewing a Secret.....	57
2.4.2 Searching for Secrets by Event.....	58
2.4.3 Deleting a Secret.....	59
2.4.4 Restoring a Secret from a Backup.....	60
2.5 Managing Secret Versions.....	61
2.5.1 Saving and Viewing Secret Values.....	61
2.5.2 Critical Operation Protection.....	62
2.5.3 Managing Secret Version Statuses.....	64
2.5.4 Setting the Version Expiration Time.....	66
2.5.5 Rotation Secret Version.....	67
2.6 Managing Tags.....	70
2.6.1 Adding a Tag.....	70
2.6.2 Searching for a Secret by Tag.....	71
2.6.3 Modifying a Tag Value.....	72
2.6.4 Deleting a Tag.....	73
2.7 Creating an Event.....	74
2.8 Managing Events.....	75
2.8.1 Viewing Events.....	75
2.8.2 Editing an Event.....	77
2.8.3 Enabling an Event.....	77
2.8.4 Disabling an Event.....	78
2.8.5 Deleting an Event.....	79
2.9 Viewing Notifications.....	79
3 Key Pair Service.....	81
3.1 Creating a Key Pair.....	81
3.2 Importing a Key Pair.....	86
3.3 Upgrading a Key Pair.....	89
3.4 Deleting a Key Pair.....	90
3.5 Using Key Pairs.....	91
3.5.1 Binding a Key Pair.....	91
3.5.2 Binding Key Pairs in Batches.....	94
3.5.3 Viewing a Key Pair.....	96
3.5.4 Resetting a Key Pair.....	98
3.5.5 Replacing a Key Pair.....	99
3.5.6 Unbinding a Key Pair.....	102
3.6 Downloading a Public Key.....	104
3.7 Managing Private Keys.....	104

3.7.1 Importing a Private Key.....	104
3.7.2 Exporting a Private Key.....	107
3.7.3 Clearing a Private Key.....	108
3.8 Using a Private Key to Log In to the Linux ECS.....	109
3.9 Using a Private Key to Obtain the Login Password of Windows ECS	111
4 Dedicated HSM.....	113
4.1 Operation Guide.....	113
4.2 Purchasing a Dedicated HSM Instance.....	115
4.2.1 Creating a Dedicated HSM Instance.....	115
4.2.2 Activating a Dedicated HSM Instance.....	119
4.3 Viewing Dedicated HSM Instances.....	122
4.4 Using Dedicated HSM Instances.....	125
4.5 Managing Tags.....	127
4.5.1 Adding a Tag.....	127
4.5.2 Searching for a Dedicated HSM Instance by Tag.....	129
4.5.3 Modifying a Tag Value.....	130
4.5.4 Deleting a Tag.....	131
5 Tag Management.....	133
5.1 Overview.....	133
5.2 Creating a Tag Policy.....	135
5.3 Creating a Tag.....	136
5.4 Searching for a Custom Key by Tag.....	138
5.5 Modifying a Tag Value.....	139
5.6 Deleting a Tag.....	140
6 Auditing Logs.....	142
6.1 Operations supported by CTS.....	142
6.2 Viewing CTS Traces in the Trace List.....	145
7 Sharing.....	149
7.1 Overview.....	149
7.2 Shared KMS.....	151
7.3 Activating a Dedicated HSM Instance Using a Shared VPC.....	153
7.4 Updating a Resource Share.....	155
7.5 Leaving a Resource Share.....	156
8 Permission Control.....	157
8.1 Creating a User and Authorizing the User the Permission to Access DEW.....	157
8.2 Creating a Custom DEW Policy.....	163

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">AES_256	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">• HMAC_256• HMAC_384• HMAC_512	SHA digest key	<ul style="list-style-type: none">• Data tampering prevention• Data integrity verification
Digest key	SM3	<ul style="list-style-type: none">• HMAC_SM3	SM3 digest key	<ul style="list-style-type: none">• Data tampering prevention• Data integrity verification
Asymmetric key	RSA	<ul style="list-style-type: none">• RSA_2048• RSA_3072• RSA_4096	RSA asymmetric password	Encrypts and decrypts a small amount of data or creates digital signatures.
	ECC	<ul style="list-style-type: none">• EC_P256• EC_P384	Elliptic curve recommended by NIST	Digital signature

1.2 Creating a 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 100 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**.


- KMS 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](#).

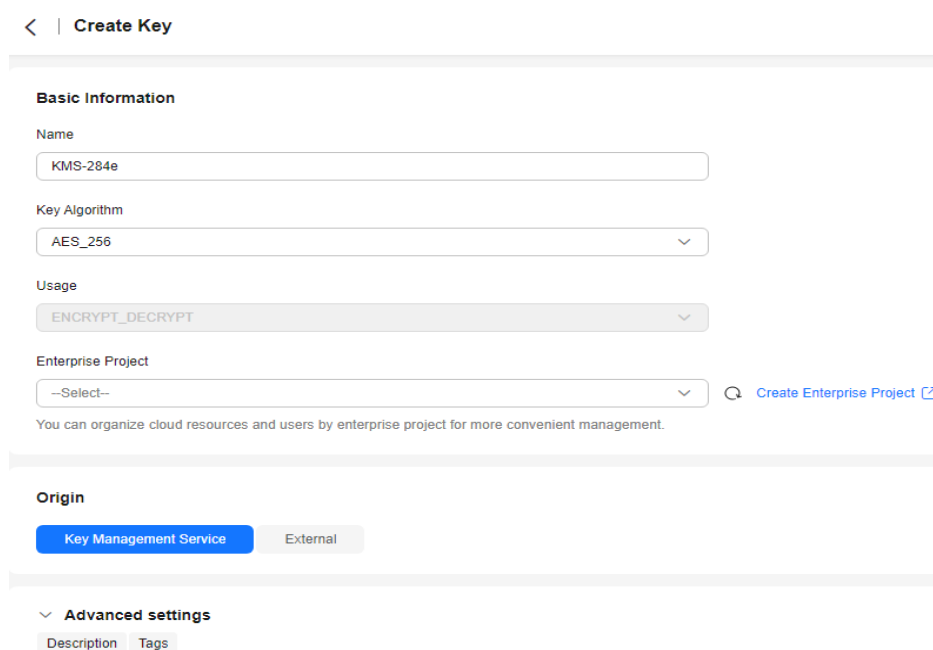
Step 2 Click  in the upper left corner of the management console and select a region or project.

Step 3 In the navigation on the left, choose  > **Security & Compliance** > **Data Encryption Workshop**.

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

Step 5 Go to the **Create Secret** page. Set the parameters.

Figure 1-1 Creating a key



< | Create Key

Basic Information

Name
KMS-284e

Key Algorithm
AES_256

Usage
ENCRYPT_DECRYPT

Enterprise Project
--Select-- [Create Enterprise Project](#)

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

Origin

Key Management Service External

Advanced settings
Description Tags

Table 1-2 Key parameter configuration

Parameter	Description
Name	<p>Name of the key you are creating.</p> <p>NOTE</p> <ul style="list-style-type: none"> You can enter digits, letters, underscores (_), hyphens (-), colons (:), and slashes (/). You can enter up to 255 characters.
Key Algorithm	<p>Select a key algorithm. For details about the key algorithms supported by KMS, see Table 1-3.</p>
Usage	<p>Key usage. The value cannot be changed after the key is created. The value can be SIGN_VERIFY, ENCRYPT_DECRYPT, or GENERATE_VERIFY_MAC.</p> <ul style="list-style-type: none"> 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.
Enterprise Project	<p>This parameter is provided for enterprise users.</p> <p>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.</p> <p>If there are no Enterprise Management options displayed, you do not need to configure it.</p> <p>NOTE</p> <ul style="list-style-type: none"> 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.
Key Material Source	<ul style="list-style-type: none"> Key management External
Advanced settings	<ul style="list-style-type: none"> Description Description of the key. Tag You can add tags to a secret as you need. For details about operations on tags, see Tag Management. <p>NOTE You can add at most 20 tags to a secret.</p>

- **Key Algorithm:** Select a key algorithm. For more information, see [Table 1-3](#).

Table 1-3 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.
Digest key	SHA	- HMAC_256 - HMAC_384 - HMAC_512	SHA digest key	- Data tampering prevention - Data integrity verification
Digest key	SM3	- HMAC_SM3	SM3 digest key	- Data tampering prevention - Data integrity verification
Asymmetric key	RSA	- RSA_2048 - RSA_3072 - RSA_4096	RSA asymmetric password	Encrypts and decrypts a small amount of data or creates digital signatures.
	ECC	- EC_P256 - EC_P384	Elliptic curve recommended by NIST	Digital signature

Step 6 Click **OK**. In the CMK list, you can view created CMKs. The default status of a CMK is **Enabled**. The default status is **Pending import** whose material source is **External**.

----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 KMS console to create a custom key whose key material source is external, 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 1-4](#).

Table 1-4 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">You can delete the key material, but cannot delete the custom key and its metadata.Such keys cannot be rotated.When importing the key material, you can set the expiration time of the key material. After the key material expires, the KMS automatically deletes the key material within 24 hours, but does not delete the 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. <p>NOTE Keys using RSA_2048, RSA_3072, RSA_4096, EC_P256, and EC_P384 algorithms are permanently valid. Their key materials cannot be manually deleted, and their expiration time cannot be configured.</p>
Keys created in KMS	<ul style="list-style-type: none">The key material cannot be manually deleted.Symmetric keys can be rotated.You cannot set the expiration time for key material.

- Association

When a key material is imported to a 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.


Operation Process

Scenario	Procedure
Using existing key materials	<ol style="list-style-type: none"> Creating a key whose material source is external: Create an empty key whose material source is external. Importing key material (existing key material): Import key material and token to the created empty key.
Downloading key materials by calling APIs	<ol style="list-style-type: none"> Creating a key whose material source is external: Create an empty key whose material source is external. Downloading wrapping key and importing a token (by calling the API): Download the wrapping key and import the token by calling the API. Using wrapping key to encrypt key material: Use HSM or OpenSSL to encrypt wrapping key into key material. Importing key material (existing key material): Import key material and token to the created empty key.
Downloading key materials on the KMS console	<ol style="list-style-type: none"> Creating a key whose material source is external: Create an empty key whose material source is external. Downloading wrapping key and importing the token (from the KMS console): Download wrapping key from the KMS console. The import token is automatically guided by the console. NOTICE After downloading wrapping key, do not close or exit the Import Key Material dialog box. After the key material is encrypted, you need to perform the Import Key Material (Continue to Import Key Material) in this dialog box. Using wrapping key to encrypt key material: Use HSM or OpenSSL to encrypt wrapping key into key material. Importing Key Material (Continue Importing Key Material): Import the key material to the created empty key.

Step 1: Creating a Key Whose Material Source Is External

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 In the navigation on the left, choose  > **Security & Compliance** > **Data Encryption Workshop**.

Step 4 Click **Create Key** in the upper right corner of the page to create an empty key whose **Source** is **External**. For details about more parameters, see [Step 5](#).

----End

Step 2: Downloading Wrapping Key and Importing Token

The key management function provides two download modes:

- Download the wrapping key and import token by calling the API.
- Download the wrapping key from the KMS console. The import token is automatically passed by the console. Therefore, do not close or exit the **Import Key Material** dialog box after the key material is downloaded. Otherwise, the imported token will automatically become invalid.

Downloading the Wrapping Key By Calling APIs

Step 1 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
}
```

Step 2 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
```

Step 3 Save the import token, copy the content of the **import_token** token, paste it to a .txt file, and save the file as **ImportToken.b64**.

----End

Downloading the Wrapping Key on the KMS 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** In the navigation on the left, choose  > **Security & Compliance** > **Data Encryption Workshop**.
- Step 4** On the **Custom Keys** tab page, locate the key created by [Step 1: Creating a Key Whose Material Source Is External](#) and click **Import Key Material** in the **Operation** column.
- Step 5** In the **Download the Import Items** area, select a key wrapping algorithm based on [Key wrapping algorithm](#).

Figure 1-2 Obtaining the wrapping key and import token

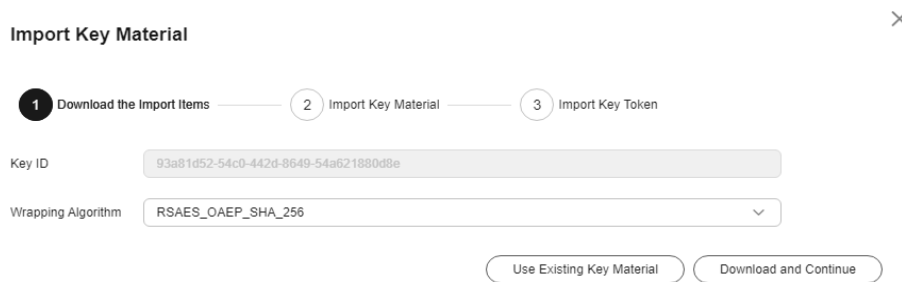
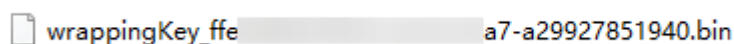


Table 1-5 Key wrapping algorithms

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

- Step 6** Click **Download and Continue** to download the wrapping key file, as shown in [Figure 1-3](#).

Figure 1-3 Downloading a file



- **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 console automatically passes the import token. Therefore, do not close or exit the **Import Key Material** dialog box after the key material is downloaded. Otherwise, the imported token will automatically become invalid.

After downloading wrapping key, [use it to encrypt the key material](#). Then, import the key material in the **Import Key Material** dialog box. For details, see [Importing Key Material](#).

----End

Step 3: Using wrapping key to Encrypt Key Materials

Symmetric and asymmetric key encryption modes generate different key materials.

- Symmetric key: The key material is **EncryptedKeyMaterial.bin**.
- Asymmetric key: **EncryptedKeyMaterial.bin** (temporary key material) and **out_rsa_private_key.der** (private key ciphertext)

Symmetric Key

- 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.

- To generate a key material for a 256-bit symmetric key, on the agent where OpenSSL has been installed, run the following command to generate the key material and save it as **PlaintextKeyMaterial.bin**:
 - AES256 symmetric key
openssl rand -out PlaintextKeyMaterial.bin 32
- Use the downloaded wrapping key to encrypt the key material and save the encrypted key material as **EncryptedKeyMaterial.bin**.

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	<code>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</code>

Asymmetric Key

- 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.

- To generate a key material for a 256-bit symmetric key, on the agent where OpenSSL has been installed, run the following command to generate the key material and save it as **PlaintextKeyMaterial.bin**:
 - RSA and ECC asymmetric keys
 - 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 1-7 Encrypting the generated key material using the downloaded wrapping key

Wrapping Key Algorithm	Key Material Encryption
RSAES_OAEP_SHA_256	<code>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</code>

- c. 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.
 - 1) Generate a private key.

```
openssl ecparam -genkey -name SM2 -out pkcs1_sm2_private_key.pem
```
 - 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 4: Importing Key Materials


The import method varies depending on the key material download method.

- If the key material is downloaded by calling the API or the key material already exists, run the [Importing Existing Key Materials](#).
- To download the key material using the KMS console, run the [Importing Key Material](#).

Importing Existing Key Materials

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 In the navigation on the left, choose  > **Security & Compliance** > **Data Encryption Workshop**.

Step 4 On the **Custom Keys** tab page, locate the key created by [Step 1: Creating a Key Whose Material Source Is External](#) and click **Import Key Material** in the **Operation** column.

Step 5 In the **Download the Import Items** area, select a key wrapping algorithm based on [Key wrapping algorithm](#).

Figure 1-4 Obtaining the wrapping key and import token

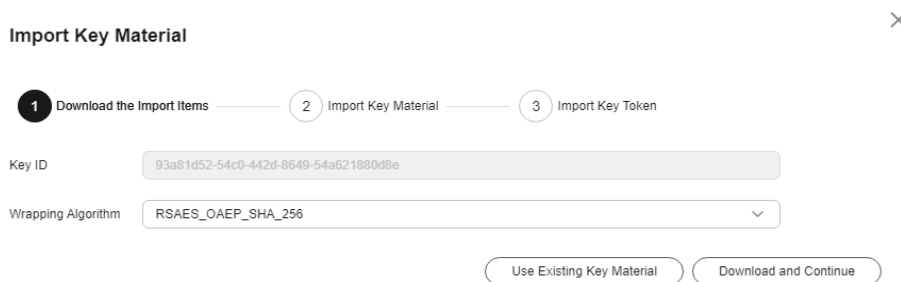


Table 1-8 Key wrapping algorithms

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

Step 6 Click **Use Existing Key Material**. In the **Import Key Material** area, enter **Key Material**.

Figure 1-5 Import key materials

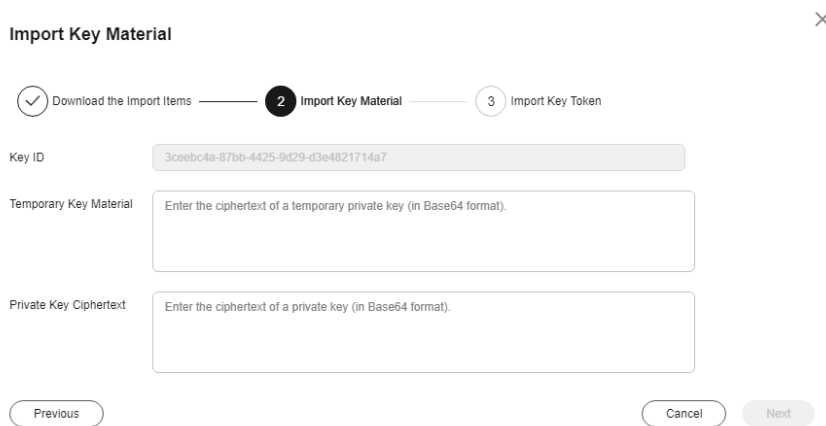


Table 1-9 Key material description

Scenario	Description
Symmetric key	Use the key material encrypted by wrapping key. For example, the EncryptedKeyMaterial.bin file in Step 3: Using wrapping key to Encrypt Key Materials .

Scenario	Description
Asymmetric key	Use the temporary key material and private key ciphertext encrypted by wrapping key. For example, the temporary key material EncryptedKeyMaterial.bin and private key ciphertext out_rsa_private_key.der in Step 3: Using wrapping key to Encrypt Key Materials .

Step 7 Click **Next**. In the **Import Key Token** area, set parameters based on [Table 1-10](#).

Figure 1-6 Importing a key token

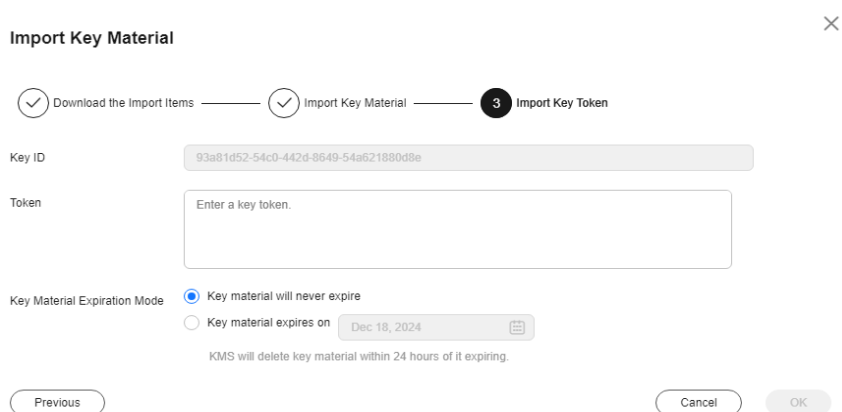


Table 1-10 Parameters for importing a key token

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

Step 8 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

Importing Key Material

Step 1 In the **Import Key Material** dialog box (**Step 6**) on the management console, add the **Key Material** file in the **Import Key Material** configuration item.

Figure 1-7 Import key materials

Table 1-11 Key material description

Scenario	Description
Symmetric key	Use the key material encrypted by wrapping key. For example, the EncryptedKeyMaterial.bin file in Step 3: Using wrapping key to Encrypt Key Materials .
Asymmetric key	Use the temporary key material and private key ciphertext encrypted by wrapping key. For example, the temporary key material EncryptedKeyMaterial.bin and private key ciphertext out_rsa_private_key.der in Step 3: Using wrapping key to Encrypt Key Materials .

Step 2 Click **Next** to go to the **Import Key Token** step. Configure the parameters as described in **Table 1-12**.

Figure 1-8 Importing a key token

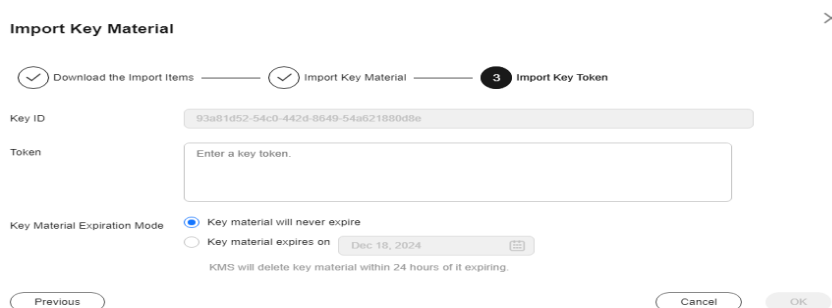


Table 1-12 Parameters for importing a key token

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

Step 3 Click **OK**. When the **Key imported successfully** message is displayed in the upper right corner, the materials are imported.

NOTICE

Key material can be successfully imported when it matches the corresponding key ID.

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 a 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 In the navigation on the left, choose  > **Security & Compliance** > **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 Key

This section describes how to view the information about the custom key on the KMS console, including the key alias/ID 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** In the navigation on the left, choose  > **Security & Compliance** > **Data Encryption Workshop.**
- Step 4** Check the key list. [Table 1-13](#) describes the parameters.

Figure 1-9 Custom keys

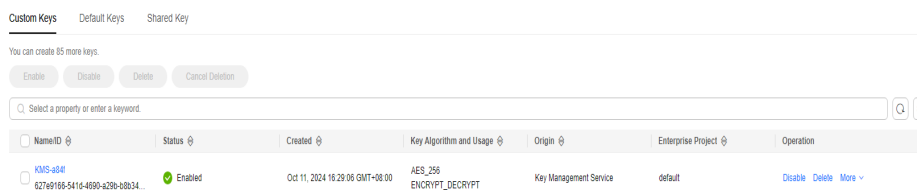


Figure 1-10 Default keys

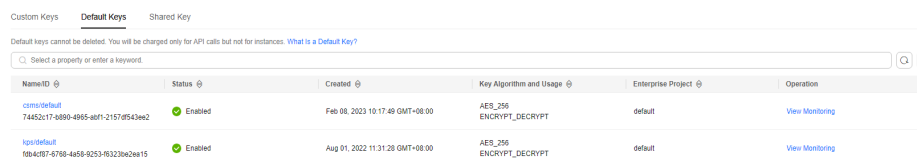


Table 1-13 Key list parameters





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

Parameter	Description
Origin	Source of key material, which can be one of the following: <ul style="list-style-type: none"> • External The key is imported to the KMS from an external system. • Key Management Service The key is a default key or created in KMS.
Enterprise Project	Enterprise project the CMK is used for

Step 5 You can click the key name to view its details, as shown in [Figure 1-11](#).

Figure 1-11 CMK details

Basic Information

Name	KMS-a84f 
Status	 Enabled
ID	627e9166-541d-4690-a29b-b8b347ccad7c 
Key Algorithm and Usage	AES_256 ENCRYPT_DECRYPT
Creation Time	Oct 11, 2024 16:29:06 GMT+08:00
Description	-- 
Enterprise Project	default

 **NOTE**

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

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

----End

1.4.2 Enabling a Key


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 In the navigation on the left, choose  > **Security & Compliance** > **Data Encryption Workshop**.

Step 4 Locate the target key in the list and click **Enable** in the **Operation** column.

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

NOTE

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

----End

1.4.3 Disabling a Key

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 key to encrypt or decrypt data, you must enable it by following instructions in [Enabling a Key](#).

Prerequisites


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


Constraints

- Default keys created by KMS cannot be disabled.
- A disabled key 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 In the navigation on the left, choose  > **Security & Compliance** > **Data Encryption Workshop**.

Step 4 Locate the target key in the list and click **Disable** in the **Operation** column.

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

 **NOTE**

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

----End

1.4.4 Deleting a Key

Before deleting the key, 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 [Viewing CTS Traces in the Trace List](#).

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.
- Before deleting a multi-region CMK, delete all replica keys.

Procedure

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

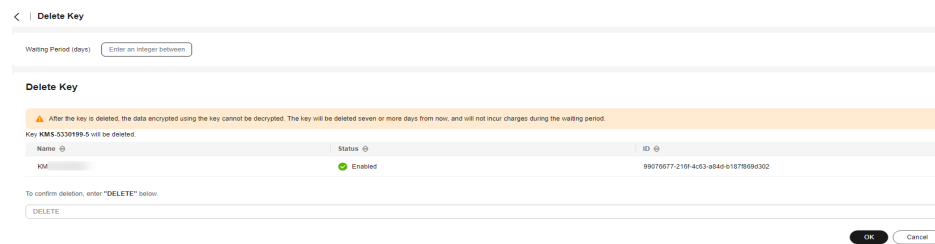
Step 2 Click  in the upper left corner of the management console and select a region or project.

Step 3 In the navigation on the left, choose  > **Security & Compliance** > **Data Encryption Workshop**.

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

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

Figure 1-12 Entering the period after which you want the deletion to take effect



NOTE

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

Step 6 Enter **DELETE** in the confirmation dialog box if deletion verification is disabled and click **OK**.

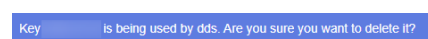
If you have enabled deletion verification, select a verification mode, click **Get Code**, enter the code, and click **OK**.

NOTE

To disable operation protection, go to the **Security Settings** page, click **Disable** next to **Operation Protection** in the **Critical Operations** tab, or click **Disable Operation Protection** on the deletion page.

Step 7 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 1-13](#). Click **Yes**.

Figure 1-13 Confirming the deletion



----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 In the navigation on the left, choose  > **Security & Compliance** > **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 a Key](#).
- If the CMK is created using imported materials, its status becomes **Disabled** after the cancellation. To enable the CMK, see [Enabling a Key](#).
- 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 the enterprise project function, see [Enabling the Enterprise Center](#).
- The enterprise project of default keys cannot be changed.

Procedure

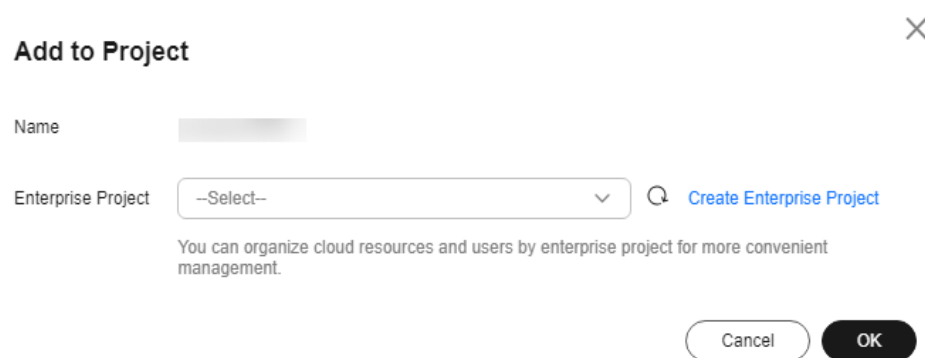
Step 1 [Log in to the management console.](#)

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

Step 3 In the navigation on the left, choose  > **Security & Compliance** > **Data Encryption Workshop**.

Step 4 Locate the target key and choose **More** > **Add to Project** in the **Operation** column.

Figure 1-14 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 5 Select a project. Click **OK**.

----End

1.4.7 Viewing the Number of Key Accounting Requests


Cloud Eye (CES) monitors all keys of the current user and allows you to query the number of typical calling requests, including key billing requests and key detail requests. This section describes how to query the key billing requests using the monitoring function.

Constraints

- This function is available only for the enabled or disabled keys.
- This function is available for the default keys.

Viewing Monitoring Details of 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** In the navigation on the left, choose  > **Security & Compliance** > **Data Encryption Workshop**.
- Step 4** Locate the target key and choose **More** > **View Monitoring** in the **Operation** column.
- Step 5** On the key details page, key calling details are displayed, as shown in **Figure 1-15**.

Figure 1-15 Monitoring details of a key



 **NOTE**

All metric types are displayed by default. You can set the metric and time range.

----End

Viewing Monitoring Details of Multiple Keys



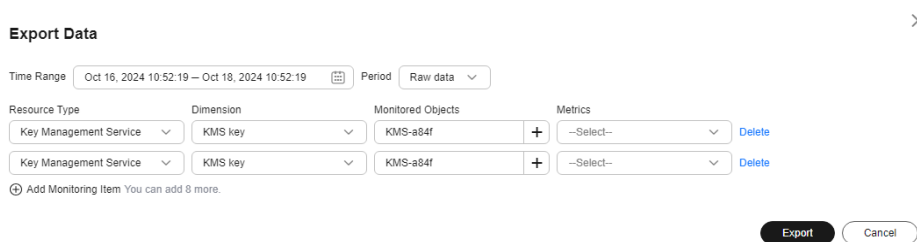
- Step 1** [Log in to the management console](#).
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click  in the upper left corner and choose **Management & Governance** > **Cloud Eye**. The **Overview** page is displayed.
- Step 4** In the navigation pane on the left, choose **Cloud Service Monitoring** > **Key Management Service**.
- Step 5** Select multiple target keys, click **Export Data** in the upper left corner of the page, set parameters, and click **Export**.

Figure 1-16 Exporting monitoring data



Step 6 After the data is exported, go to the Cloud Eye console. In the navigation pane on the left, choose **Task Center**. The **Monitoring Data Export Tasks** tab is displayed by default.

Step 7 Locate the target task and click **Download** in the **Operation** column.


----End


1.5 Searching for a Key

This section describes how to search for a custom key by specifying attributes on the KMS page.

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 In the navigation on the left, choose  > **Security & Compliance** > **Data Encryption Workshop**.

Step 4 Click the search bar and select the criteria for filtering keys, as shown in [Figure 1-17](#). Search for a key by specifying attributes.

Figure 1-17 Search bar



NOTE

- You can search for keys by name, ID, status, creation time, algorithm, usage, material expiration time, material source, and enterprise project.
- You can search for keys by attribute combination. For example, if **Status** is set to **Enabled** and **Key Algorithm** is set to **AES_256**, all custom keys that meet the criteria are displayed.

----End

1.6 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.
- After an API is called to encrypt data, the online tool cannot be used to decrypt the data.

Encrypting Data

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

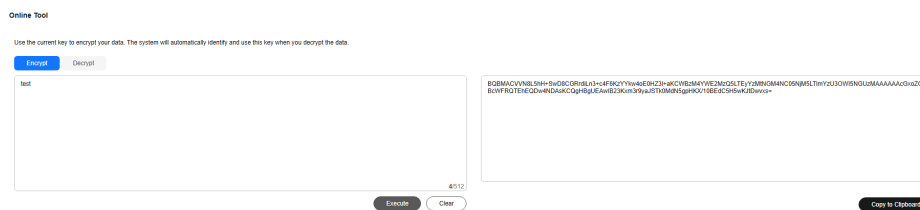
Step 2 Click  in the upper left corner of the management console and select a region or project.

Step 3 In the navigation on the left, choose  > **Security & Compliance** > **Data Encryption Workshop**.

Step 4 Click the name of the target custom key to access the key details page. Click the **Tool** tab.

Step 5 Click **Encrypt**. In the text box on the left, enter the data to be encrypted, as shown in [Figure 1-18](#).

Figure 1-18 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

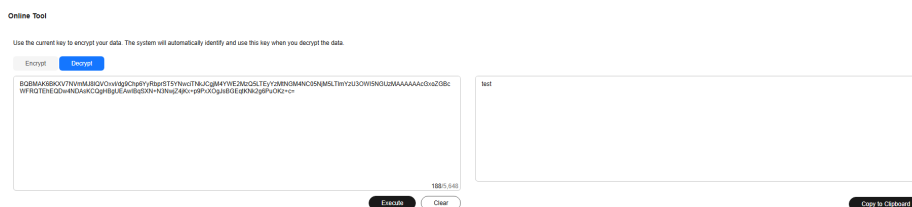
Step 1 [Log in to the management console](#).

- Step 2** In the navigation on the left, choose  > **Security & Compliance** > **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 1-19](#).

 **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 1-19 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

1.7 Key Alias

An alias is an identifier of a key. You can use the alias as the key ID during API calling. The original key alias is not used as the key name.


This section describes how to add and delete an alias for a key.


Constraints

- An alias can be used for only one key. A key can have multiple aliases.
- The aliases are unique in a region but can be the same in different regions.
- The aliases cannot be modified once being created.
- A maximum of 50 aliases can be created for a key.

Creating an Alias

- 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 In the navigation on the left, choose  > **Security & Compliance** > **Data Encryption Workshop**.

Step 4 Click the target key name. On the key details page, click the **Alias** tab.

Step 5 Click **Create Alias**. Enter the alias in the displayed dialog box and click **OK**.


 **NOTE**


Only digits, letters, underscores (_), hyphens (-), colons (:), and slashes (/) are allowed.

----End

Deleting an Alias

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 In the navigation on the left, choose  > **Security & Compliance** > **Data Encryption Workshop**.

Step 4 Click the target key name. On the key details page, click the **Alias** tab.

Step 5 Enter **DELETE** in the confirmation dialog box if deletion verification is disabled and click **OK**.

If you have enabled deletion verification, select a verification mode, click **Get Code**, enter the code, and click **OK**.

 **NOTE**

To disable operation protection, go to the **Security Settings** page, click **Disable** next to **Operation Protection** in the **Critical Operations** tab, or click **Disable Operation Protection** on the deletion page.

----End

1.8 Managing Tags

1.8.1 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.

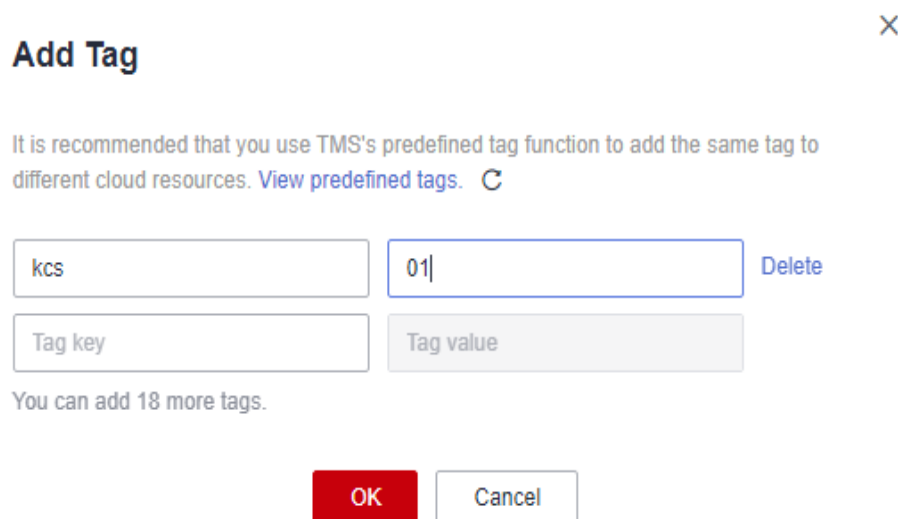
Step 3 In the navigation on the left, choose  > **Security & Compliance** > **Data Encryption Workshop**.

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**, as shown in [Figure 1-20](#). In the **Add Tag** dialog box, enter the tag key and tag value. [Table 1-14](#) describes the parameters.

Figure 1-20 Adding a tag



Add Tag ×

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

kcs	01	Delete
Tag key	Tag value	

You can add 18 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*.
- 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 1-14 Tag parameters

Parameter	Description	Value	Example Value
Tag key	Name of a tag. The same tag (including tag key and tag value) can be used for different 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.	<ul style="list-style-type: none">• Mandatory.• The tag key must be unique for the same custom key.• 128 characters limit.• The value cannot start or end with a space.• Cannot start with _sys_.• The following character types are allowed:<ul style="list-style-type: none">- Chinese- English- Numbers- Space- Special characters: <code>._:/=+-@</code>	cost
Tag value	Value of the tag	<ul style="list-style-type: none">• This parameter can be empty.• 255 characters limit.• The following character types are allowed:<ul style="list-style-type: none">- Chinese- English- Numbers- Space- Special characters: <code>._:/=+-@</code>	100

Step 7 Click **OK** to complete.

----End

1.8.2 Modifying Tag Values

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

Procedure



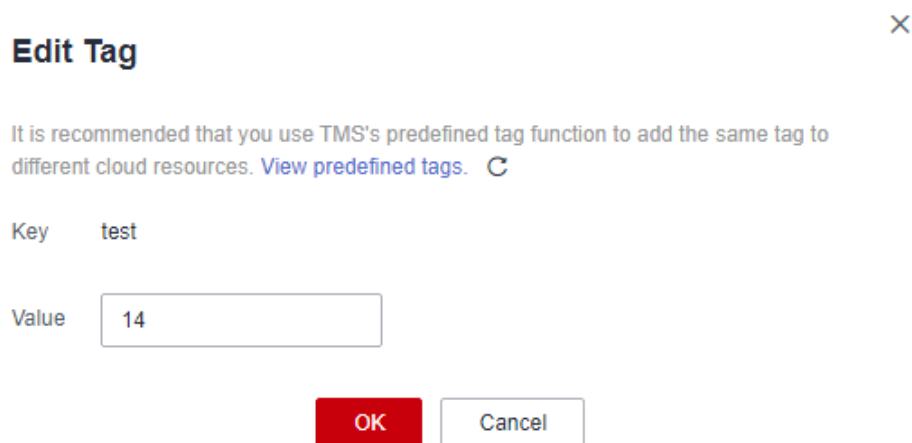
- Step 1** [Log in to the management console.](#)
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** In the navigation on the left, choose  > **Security & Compliance** > **Data Encryption Workshop.**
- Step 4** Click the alias of the target 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 1-21 Editing a tag





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

1.8.3 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** In the navigation on the left, choose  > **Security & Compliance** > **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

1.9 Rotating CMKs

1.9.1 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:

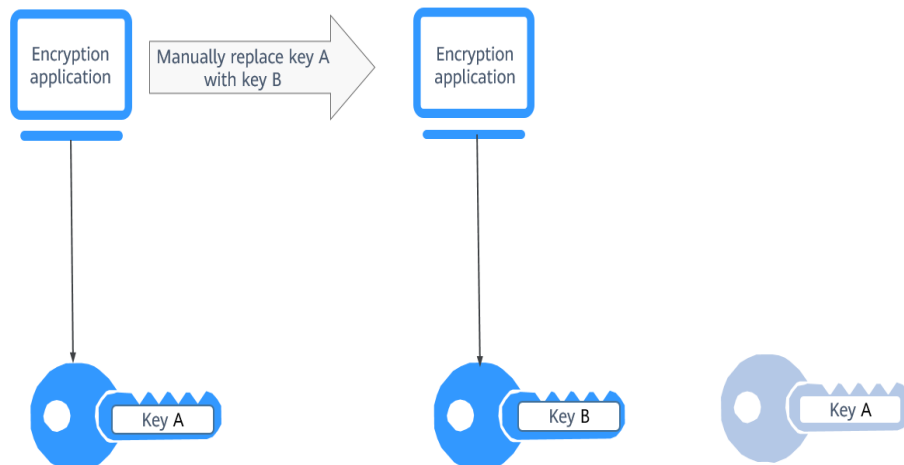
- To reduce the amount of data encrypted by each key.
A key will be insecure if it is used to encrypt a huge number of data. The amount of data encrypted a key refers to the total number of bytes or messages encrypted using the key.
- To enhance the capability of responding to security events.
In your 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.
Example:
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 1-22 Manual key rotation



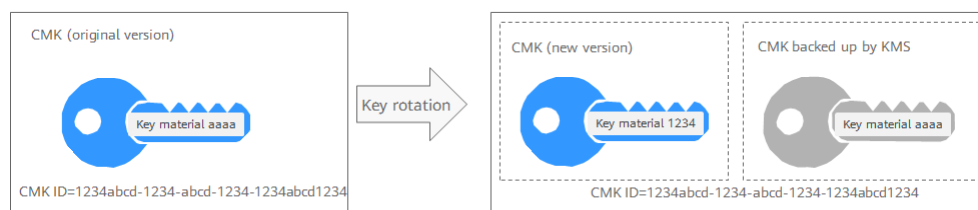
- Automatic key rotation

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

Automatic key rotation has the following characteristics:

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

Figure 1-23 Key rotation



NOTE

KMS retains all versions of a 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 1-15 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">• Symmetric key: Can be automatically or manually rotated.• Asymmetric key: Can only be manually rotated.
Disabled CMK	Disabled CMKs are not rotated. KMS keeps their rotation status unchanged. After a 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 Disabling One or More CMKs .
CMKs in pending deletion state	KMS does not rotate CMKs in pending deletion status. After you cancel the deletion of a CMK, the previous key rotation status will be restored. If the 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 Scheduling the Deletion of One or More Keys .

 **NOTE**

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

Pricing for Key Rotation

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

1.9.2 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 In the navigation on the left, choose  > **Security & Compliance** > **Data Encryption Workshop**.

Step 4 Click the name of the custom key to view its details.

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




Step 6 Click  to enable key rotation.

Step 7 Configure the rotation period and click **OK**, as shown in [Figure 1-24](#). For more information, see [Table 1-16](#).

Figure 1-24 Enabling key rotation



Table 1-16 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>NOTE 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 365.</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>

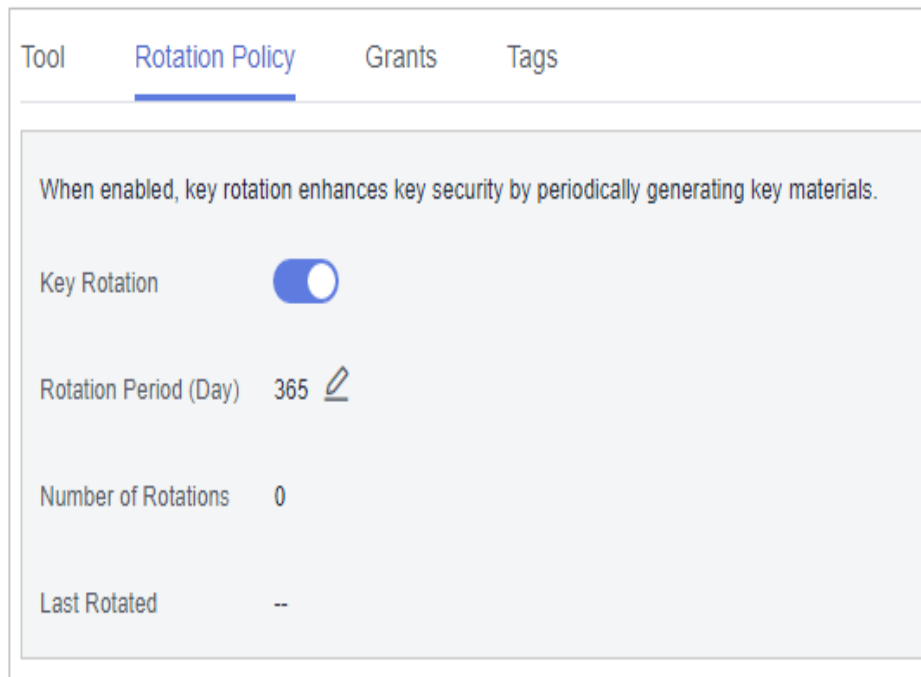
Step 8 Check rotation details, as shown in the following figure.

Figure 1-25 Key rotation details


Rotation Policy

When enabled, key rotation enhances key security by periodically generating key materials.

Key Rotation	
Rotation Period (Day)	365 
Number of Rotations	0
Last Rotated	--



 **NOTE**

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

----End

1.9.3 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 In the navigation on the left, choose  > **Security & Compliance** > **Data Encryption Workshop**.

Step 4 Click the name of the symmetric key to view its details.

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**.

----End

1.10 Managing a Grant

1.10.1 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 In the navigation on the left, choose  > **Security & Compliance** > **Data Encryption Workshop**.

Step 4 Click the name 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 1-26 Creating a grant (for a user)

Create Grant ×

User or Account: Account User

Enter the user ID of the grantee.

The IAM identity policy is used. Use account authorization. Obtain the user ID on the My Credentials page.

Name: Enter a username.

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"/> Create Data Key Pair
<input type="checkbox"/> Encrypt Data Key	<input type="checkbox"/> Retire Grant
<input type="checkbox"/> Decrypt Data Key	<input type="checkbox"/> Decrypt Data
<input type="checkbox"/> Encrypt Data	

Cancel OK

Figure 1-27 Creating a grant (for an account)

Create Grant ×

User or Account: Account User

Enter an account ID.

The IAM identity policy is used. Use account authorization. Obtain the account ID on the My Credentials page.

Name: Enter an account name.

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"/> Create Data Key Pair
<input type="checkbox"/> Encrypt Data Key	<input type="checkbox"/> Retire Grant
<input type="checkbox"/> Decrypt Data Key	<input type="checkbox"/> Decrypt Data
<input type="checkbox"/> Encrypt Data	

Cancel OK

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 1-17](#).

NOTICE

A grantee can perform the authorized operations only by calling the necessary APIs. For details, see the *Key Management Service API Reference*.

Table 1-17 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"> • User User ID: Enter the IAM user ID. To obtain the ID, click the username in the upper right corner of the page, choose My Credentials. Choose API Credentials from the navigation pane, and copy the value of IAM User ID. After the authorization is complete, the IAM user can use the specified keys. • Account Account ID: Enter the IAM user ID. To obtain the ID, click the username in the upper right corner of the page, choose My Credentials. Choose API Credentials from the navigation pane and copy the value of Account ID. After the authorization is complete, all IAM users under the account can use the specified keys. 	d9a6b2bdaedd 4ba586cabe63 72d1b312
Grant Name	<p>You can name the grant.</p> <p>NOTE</p> <ul style="list-style-type: none"> • You can enter digits, letters, underscores (_), hyphens (-), colons (:), and slashes (/). 	test
Operations	<p>You can authorize multiple permissions. The following permissions can be authorized:</p> <ul style="list-style-type: none"> • Query Key Details • Create Grant • Retire Grant <p>For details about how to authorize a key algorithm, see Table 1-18.</p>	-

Table 1-18 Granting operations

Key Algorithm	Key Type	Usage	Granted Operations
<ul style="list-style-type: none"> • AES_256 	Symmetric key	ENCRYPT_DECRYPT	<ul style="list-style-type: none"> • Create Data Key Without Plaintext • Create Data Key • Encrypt Data Key • Decrypt Data Key • Encrypt Data • Decrypt Data
<ul style="list-style-type: none"> • RSA_2048 • RSA_3072 • RSA_4096 • EC_P256 • EC_P384 	Asymmetric key	SIGN_VERIFY	<ul style="list-style-type: none"> • Query a public key • Signature • Signature verification
<ul style="list-style-type: none"> • RSA_2048 • RSA_3072 • RSA_4096 	Asymmetric key	ENCRYPT_DECRYPT	<ul style="list-style-type: none"> • Query a public key • Encrypt Data • Decrypt Data
<ul style="list-style-type: none"> • HMAC_256 • HMAC_384 • HMAC_512 	Digest key	GENERATE_VERIFY_MAC	<ul style="list-style-type: none"> • Generate HMAC • Verify HMAC

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

1.10.2 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** In the navigation on the left, choose  > **Security & Compliance** > **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 1-19](#) describes the parameters.

Table 1-19 Parameter description

Parameter	Description
Grant Name	Name of the grant when created
Grantee ID	ID of the authorized user or account.
Granted To	Whether permissions are granted to a user or account.
Granted Operations	Authorized operations (such as Create Data Key) on the custom key
Created	Time when the grant is created
Operation	Operations that can be performed on a grant. For example, you can revoke a grant.

- Step 6** Click the target grant, the grant details are displayed on the right, as shown in [Figure 1-28](#).

Figure 1-28 Viewing grant details

Grant Details

Key ID	4c [redacted] 301f
User or Account	Account
account ID	6c [redacted] 525
Name	1
Granted Operations	<input checked="" type="checkbox"/> Create Data Key <input checked="" type="checkbox"/> Create Data Key Without Plaintext <input checked="" type="checkbox"/> Encrypt Data Key

----End

1.10.3 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 In the navigation on the left, choose  > **Security & Compliance** > **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 If verification is not enabled, enter **DELETE** in the confirmation dialog box, and click **OK**.

If you have enabled deletion verification, select a verification mode, click **Get Code**, enter the code, and click **OK**.

NOTE

To disable operation protection, go to the **Security Settings** page, click **Disable** next to **Operation Protection** in the **Critical Operations** tab, or click **Disable Operation Protection** on the deletion page.

----End

1.10.4 Editing a Grant


After you create a grant for an account or IAM user, you can edit the grant to change their operation permissions.


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 In the navigation on the left, choose  > **Security & Compliance** > **Data Encryption Workshop**.

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

Step 5 Locate the target grant, click **Edit** in the **Operation** column, and select the granted operations to be edited, as shown in [Figure 1-29](#).

Figure 1-29 Editing a grant

Edit ×

User or Account **Account** User

72c 62e

Name

Granted Operations ⓘ

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

Cancel OK

Step 6 Click **OK**.

----End

2 Cloud Secret Management Service

2.1 Secret Overview

Shared Secrets

Full lifecycle management is supported for customized secrets in different scenarios. You can use CSMS to centrally manage, retrieve, and securely store various types of secrets, such as database account passwords, server passwords, SSH keys, and access keys. Multiple versions can be managed, so you can rotate secrets.

Secret Rotation

Database secret leakage is the main cause of data leakage. CSMS supports RDS and TaurusDB secrets hosting, as well as automatic and manual rotation, meeting various database secret management scenarios and reducing security risks faced by service data.

Differences Between Shared Secrets and RDS Secrets

Table 2-1 Secret types

Type	Shared secret	Rotated secret
Application Scenario	Supports full lifecycle management of customized secrets in different scenarios.	<ul style="list-style-type: none">• RDS secrets: Automatically hosts Huawei Cloud RDS database secrets.• TaurusDB secrets: Automatically Host Huawei Cloud TaurusDB secrets.
Automatic Rotation	Not supported. Users need to trigger the rotation.	Supported. Single-user and dual-user rotation models are supported.

Using Rotated Secrets

Process description:

1. Create a rotated secret.
 - Set the secret name and tag.
 - Configure an automatic rotation policy.
2. An application system can request an access secret from CSMS and obtain the secret value to access the corresponding database. For details about how to call APIs, see [Querying the Secret Version and Value](#).
3. The application system uses the returned secret value to parse the plaintext data. After obtaining the account and password, the application system can access the target database corresponding to the user.

CAUTION

- After automatic rotation is enabled, the passwords hosted by the database instance will be updated periodically. Ensure that the application that uses the database instance has completed code adaptation so that the latest secrets can be dynamically obtained when the database connection is established.
 - Do not cache any information in secrets. Otherwise, the account and password may become invalid after rotation, causing database connection failures.
-

2.2 Rotation Policy

Single-User Rotation

The single-user rotation policy applies to single-user scenarios. It is mainly used for accounts with low-frequency rotation and low reliability requirements. This is a simple rotation policy suitable for most cases. The current secret may be temporarily unavailable at the moment when the password is reset.

You can use single-user rotation to:

- Select or create a database account as the secret value when creating a database account.
- For database access, a database connection is not deleted during secret rotation. After the rotation, new connections use the new secrets.

Dual-User Rotation

Dual-user rotation is mainly used for accounts with high rotation frequency and high rotation reliability requirements. Two accounts with the same permission are hosted. The secret of the **SYSPREVIOUS** status is rotated each time. Program access will not be interrupted when a password is reset and switched. During the rotation, the status of the new secret is changed to **SYSPENDING**, and the RDS API is called to reset the password. After the password is reset, the status of the

new secret is changed from **SYSPENDING** to **SYSCURRENT**, and the status of the secret in the **SYSCURRENT** state is changed to **SYSPREVIOUS**.

- You need to select or create two database accounts as secret values.
- The two secret values are rotated alternately. You need to obtain the secret value of **SYSCURRENT** each time.

2.3 Creating a Secret

2.3.1 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 In the navigation on the left, choose  > **Security & Compliance** > **Data Encryption Workshop**.

Step 4 In the navigation pane on the left, choose **Cloud Secret Management Service** > **Secrets**.

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

Figure 2-1 Creating a secret

Basic Information

Type

Shared secret
 Rotated secret

Secret Name

Enterprise Project

[Create Enterprise Project](#)

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

Secret Value

Secret key/value
 Plaintext

[+ Add](#)

KMS Encryption Key

Select from List
 Enter

Use this if the current account key is used or a key is shared.

[Create Key](#)

By default, the master key csms/default is used for encryption.

⚠ If KMS encryption is used, what you use beyond the free API request quota given by KMS will be billed. [Pricing details](#)

▼ **Advanced settings**

Table 2-2 Secret parameters

Parameter	Description
Type	Secret type. The default value is Shared secret .
Secret Name	Secret name NOTE Only letters, digits, hyphens (-), and underscores (_) are supported.
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 default . NOTE If you have not enabled enterprise management, this parameter will not be displayed.

Parameter	Description
Secret Value	Secret key/value pair and the plaintext secret to be encrypted
KMS Encryption Key	Select the default key csms/default or a custom key created on KMS. NOTE <ul style="list-style-type: none">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 csms/default for you to use.For details about the custom keys created on KMS, see Creating a Key.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 .
Advanced settings	<ul style="list-style-type: none">Associated Event Select an associated event for the secret. You can check information such as secret rotation and version expiration.Description Description of a secretTag You can add tags to a secret as you need. NOTE You can add at most 20 tags to a secret.

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

2.3.2 Creating a Rotation Secret

This section describes how to create a rotation secret on the secret management page.

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

Constraints

- You 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.
- RDS secrets support the following DB engines: MySQL.

- TaurusDB is supported for TaurusDB secrets.
- When the rotation function is enabled for the first time, CSMS automatically creates an agency for the user in the current project of the region after the user confirms the authorization. Therefore, users need to ensure that the account has the following IAM permissions:
iam:permissions:grantRoleToAgencyOnProject, iam:agencies:listAgencies, iam:roles:listRoles, iam:agencies:createAgency, iam:permissions:checkRoleForAgencyOnProject and iam:roles:createRole.
The agency to be created varies depending on the type of the secret to be rotated.
 - **RDS secret**
 - Create an agency named **CSMSAccessFunctionGraph** with account named **op_svc_kms** and permission named **CSMSAccessFunctionGraph**. The agency uses a project-level service policy, which includes the **functiongraph:function:invoke** permission for **FunctionGraph**.
 - Create an agency named **FunctionGraphAgencyForRotateRDSByCSMSV3**. The cloud service is **FunctionGraph**, and the permission name is **FunctionGraphAgencyForRotateRDSByCSMSV3**. The project-level service policy is used, including:
 - **CSMS** permissions: csms:secret:getVersion, csms:secret:listVersion, csms:secret:createVersion, csms:secret:getStage, csms:secret:get and csms:secret:updateStage.
 - **VPC** permissions: vpc:ports:create, vpc:vpcs:get, vpc:ports:get, vpc:ports:delete and vpc:subnets:get.
 - **KMS** permissions: kms:cmk:createDataKey and kms:cmk:decryptDataKey.
 - **RDS** permission: rds:password:update
 - **TaurusDB secret**
 - Create an agency named **CSMSAccessFunctionGraph** with account **op_svc_kms** and permission **CSMSAccessFunctionGraph**. The agency uses a project-level service policy, including the **functiongraph:function:invoke** permission for **FunctionGraph** to synchronously execute functions.
 - Create an agency named **FunctionGraphAgencyForRotateGaussDBByCSMSV3**. The cloud service is **FunctionGraph**, and the permission name is **FunctionGraphAgencyForRotateGaussDBByCSMSV3**. The project-level service policy is used, including:
 - **CSMS** permissions: csms:secretVersion:get, csms:secretVersion:list, csms:secretVersion:create, csms:secretStage:get, csms:secret:get and csms:secretStage:update.
 - **VPC** permissions: vpc:ports:create, vpc:vpcs:get, vpc:ports:get, vpc:ports:delete and vpc:subnets:get.

- **KMS** permissions: kms:dek:create and kms:dek:decrypt.
- **TaurusDB** permission: gaussdb:user:modify

Creating a Rotation Secret

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

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

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

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

Step 5 Click **Create Secret** and set **Type** to **Rotated secret.**

Figure 2-2 Creating a rotated secret

Basic Information

Type

Shared secret **Rotated secret**

RDS secret

Secret Name

Enterprise Project

--Select-- [Create Enterprise Project](#)

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

RDS DB Instance

rds-fc3 [View RDS DB Instance](#)

Secret Value

Dual account Single account

Account Name

--Select--

Password

Creating a cloned account

⚠ This will create an account with the same permissions as your current account. Ensure that you have the permissions to create an account.

I understand the risks.

KMS Encryption Key

Select from List Enter

Use this if the current account key is used or a key is shared.

csms/default [Create Key](#)

By default, the master key csms/default is used for encryption.

⚠ If KMS encryption is used, what you use beyond the free API request quota given by KMS will be billed. [Pricing details](#)

Advanced settings

Associated Event Description Tags

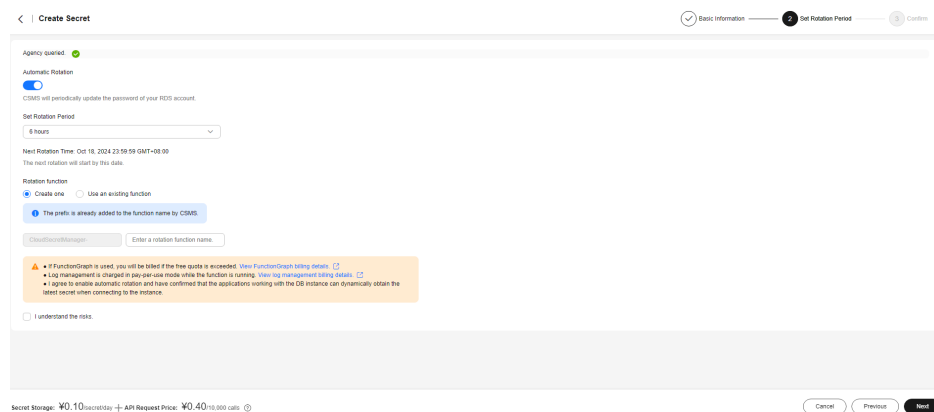
Step 6 In the displayed **Create Secret** dialog box, set the parameters. For details about the parameters, see [Table 2-3](#).

Table 2-3 Parameters for rotated secrets

Parameter	Description
Type	Type of the created rotation secret. Choose an RDS secret. The following types are available: <ul style="list-style-type: none">• RDS secret• TaurusDB secret
Secret Name	Secret name
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 default . NOTE If you have not enabled enterprise management, this parameter will not be displayed.
Instance	Select the service instance corresponding to the target secret type. NOTE <ul style="list-style-type: none">• RDS secrets support the following DB engines: MySQL.• TaurusDB is supported for TaurusDB secrets.
Secret Value	Account name and password to be encrypted. <ul style="list-style-type: none">• If Single account is selected, you need to enter an available database account.• If Dual account is selected, after you enter an available database account, a cloned account with the same permissions is created. For details, see Rotation Policy .
KMS Encryption Key	The following keys can be selected:

Step 7 Enable **Automatic Rotation**, set the rotation period and function, select **I understand the risks.**, and click **Next**. You can select an existing period or set a custom one.

Figure 2-3 Enabling automatic rotation



Step 8 Click **Next**, confirm the information, and click **OK**.

----End


2.4 Managing Secrets


2.4.1 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 In the navigation on the left, choose  > **Security & Compliance** > **Data Encryption Workshop**.

Step 4 In the navigation pane on the left, choose **Cloud Secret Management Service** > **Secrets**.

Step 5 Check the secret list. For more information, see [Table 2-4](#).

Figure 2-4 Secret list

Secret NameID	Status	Type	Associated Event	Created	Enterprise Project	Operation
b169c0c5-14a8-488e-8289-e670e...	Enabled	RDS secret	--	Oct 26, 2024 09:20:57 GMT+08:00	default	Download Backup Delete
9db0ba90-828f-4469-b1a3-48a2d...	Enabled	RDS secret	--	Aug 22, 2024 10:47:58 GMT+08:00	default	Download Backup Delete
50c58c7510b-424a-a994-f315-889...	Enabled	Shared secret		Aug 30, 2024 10:18:05 GMT+08:00	default	Download Backup Delete

Table 2-4 Secret list parameters

Parameter	Description
Secret Name/ID	Secret name
Status	Status of a secret. The value can be Enabled or Pending deletion .
Type	Secret type. The value can be Shared secret .
Associated events	Bound event notification when the secret was created.
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 Operation column, for example, download secret backup and delete a secret.

Step 6 Click a secret to view its details, as shown in [Figure 2-5](#).

Figure 2-5 Secret details

Basic Information		Secret ID	
Name	00:00:00:00:00:00	fd556c7-510b-424a-a694-f315d80146d5	fd556c7-510b-424a-a694-f315d80146d5
Type	Shared secret	Status	Enabled
Created	Aug 30, 2024 19:15:05 GMT+08:00	Encryption Key	6452d410-dbb7-4700-9c10-9ff1d470e132
Updated	Aug 30, 2024 19:15:05 GMT+08:00	Description	—
Enterprise Project	default	Associated Event	View

NOTE

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

----End

2.4.2 Searching for Secrets by Event


Search for secrets by associated event on the secret management page.


Prerequisites

The secret you want to search for has been associated with an event.

Procedure

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

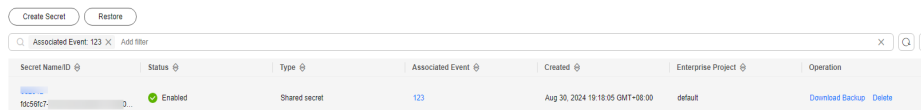
Step 2 Click  in the upper left corner of the management console and select a region or project.

Step 3 In the navigation on the left, choose  > **Security & Compliance** > **Data Encryption Workshop**.

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

Step 5 Click the search bar and select the **Associated Event** as the secret filtering condition, as shown in [Figure 2-6](#). Search for a secret by specifying the associated event.

Figure 2-6 Searching for a secret



----End

2.4.3 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.

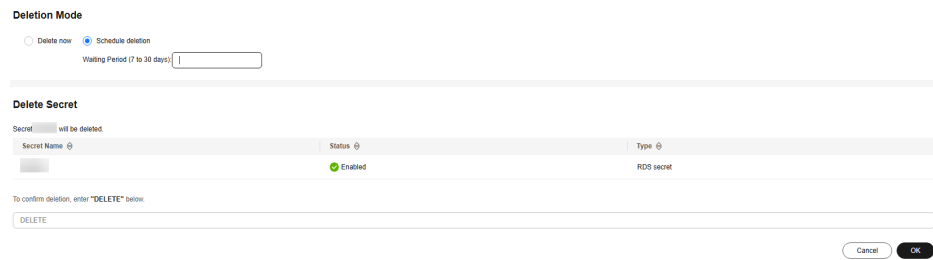
Step 3 In the navigation on the left, choose  > **Security & Compliance** > **Data Encryption Workshop**.

Step 4 In the navigation pane on the left, choose **Cloud Secret Management Service** > **Secrets**.

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 2-7 Setting schedule deletion



----End

2.4.4 Restoring a Secret from a Backup

DEW allows you to restore a secret from backup.

Prerequisites

- The secret backup is downloaded during secret creation.
- After a secret is restored from backup, the secret ID will be changed.

Procedure



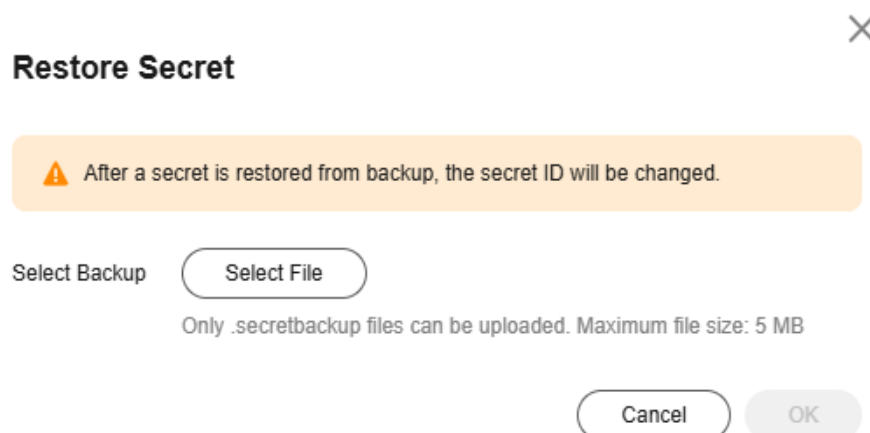
- Step 1** [Log in to the management console.](#)
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** In the navigation on the left, choose  > **Security & Compliance** > **Data Encryption Workshop.**
- Step 4** In the navigation pane on the left, choose **Cloud Secret Management Service** > **Secrets.**
- Step 5** Click **Restore Secret**, select a backup file, and click **OK.**

Figure 2-8 Restoring a secret backup



----End

2.5 Managing Secret Versions

2.5.1 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.
- For RDS and TaurusDB secrets, do not manually input the secret values.

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.

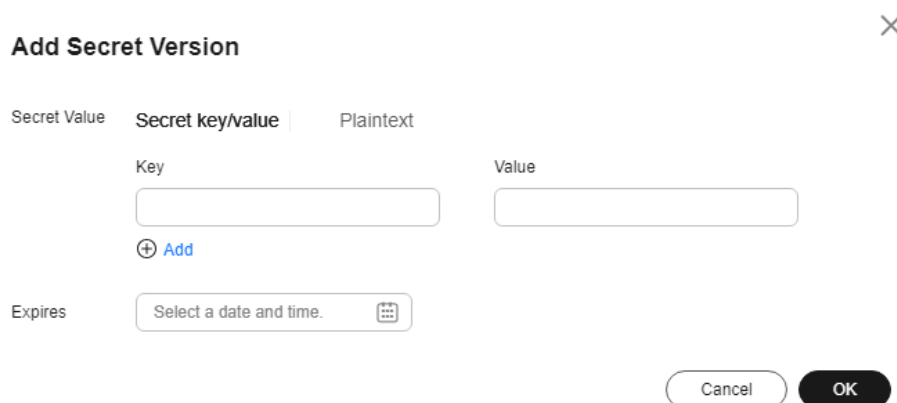
Step 3 In the navigation on the left, choose  > **Security & Compliance > Data Encryption Workshop.**

Step 4 In the navigation pane on the left, choose **Cloud Secret Management Service > Secrets.**

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

Step 6 In the area, click **Add Secret Version**, as shown in [Figure 2-9](#). Configure **Secret key/value** or **Plaintext**.

Figure 2-9 Adding a secret value




Add Secret Version ✕

Secret Value **Secret key/value** | Plaintext

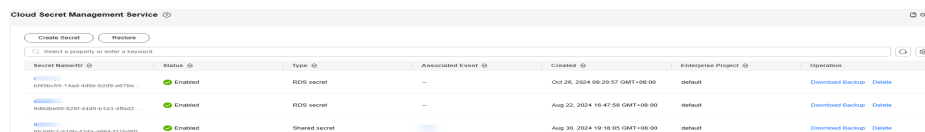
Key Value

+ Add

Expires 

- 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 2-10](#).

Figure 2-10 Secret version list



Secret Name	Status	Type	Associated Event	Created	Enterprise Project	Operation
SECRET-1-1234-5678-9012-3456	Enabled	RDS secret	--	Oct 26, 2024 09:20:57 GMT+08:00	default	Download Backup Delete
SECRET-2-1234-5678-9012-3456	Enabled	RDS secret	--	Aug 22, 2024 10:47:58 GMT+08:00	default	Download Backup Delete
SECRET-3-1234-5678-9012-3456	Enabled	Shared secret	--	Aug 20, 2024 18:18:05 GMT+08:00	default	Download Backup Delete

- Step 10** If critical operation protection is enabled, after you click **View Secret**, you need to pass the operation verification before viewing the secret value.

If critical operation protection is not enabled, after you click **View Secret**, click **OK** to view the secret value.

 **NOTE**

For details about enabling critical operation protection, see [Critical Operation Protection](#). Generally, secret values are obtained by applications through API calls. If you need to check the secret value on the service console, enable this function for data security. Confirm again and click **OK**.

- Step 11** View the secret value and click **OK**.

----End

2.5.2 Critical Operation Protection

Operation protection is supported in secret management. If you want to perform critical operations on the console, an identify verification method is required. Enable this function for your account security. It will take effect for both the account and users under the account.

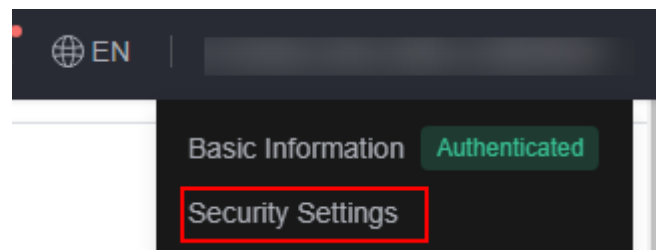
Constraints

Only operations that are performed on the console are protected by this function.

Enabling operation protection

- Step 1** [Log in to the management console](#).
- Step 2** On the console, locate the user name in the upper right corner, and select **Security Settings** from the drop-down list.

Figure 2-11 Security settings



Step 3 Go to the security settings page and click **Critical Operations**. Locate **Operation Protection** and click **Enable**.

Step 4 On the **Operation Protection** page, choose **Enable**, and click **OK** to enable operation protection.

In this case, if you or the IAM users under your account perform critical operations such as viewing secret value or deleting a key, you are required to enter a verification code, avoiding risks and loss for your service.

 **NOTE**

- When performing a critical operation, you will be asked to choose a verification method from email, SMS, and virtual MFA device.
 - If you only bind a phone number, only SMS verification is available for verification.
 - If you only bind an email address, only email is available for verification.
 - If you have not bound any method, bind one to perform critical operations.
- To modify the verification phone number, email address, or the virtual MFA device, see [Basic Information](#).

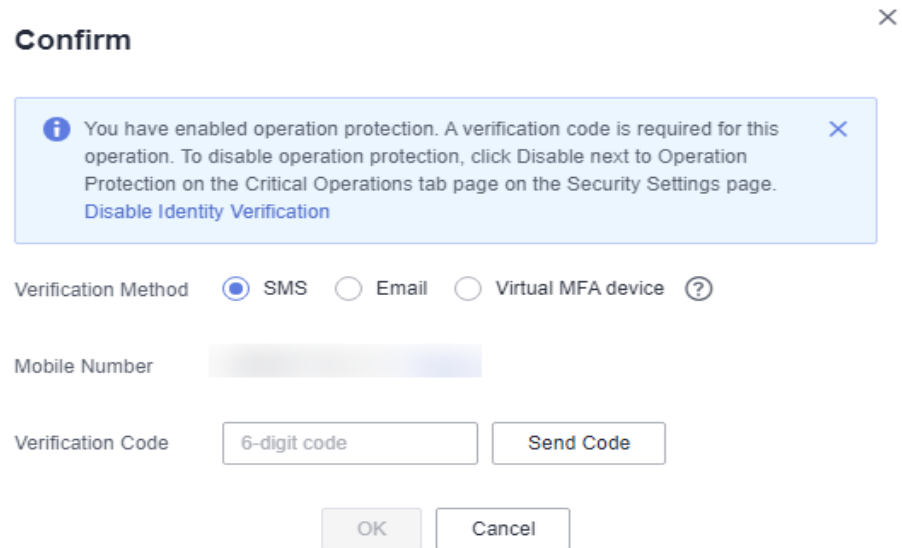
----End

Verifying the Operation Protection

If you have enabled operation protection, there will be a verification when you perform critical operations such as viewing the secret value. Select a verification mode based on your bound information, as shown in [Figure 2-12](#).

- If you have bound an email address, enter the email verification code.
- If you have bound a mobile number, enter the SMS verification code.
- If you have bound a virtual MFA device, enter the 6-digit dynamic verification code on the MFA device.

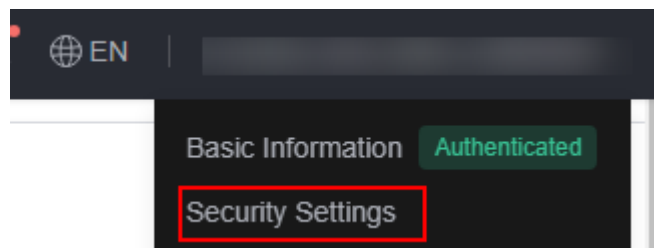
Figure 2-12 Operation protection verification



Disabling Operation Protection

- Step 1** [Log in to the management console.](#)
- Step 2** On the console, locate the user name in the upper right corner, and select **Security Settings** from the drop-down list.

Figure 2-13 Security settings



- Step 3** Go to the security settings page and click **Critical Operations**. Locate **Operation Protection** and click **Modify**.
- Step 4** On the **Operation Protection** page, choose **Disable**, click **OK**, and pass the verification.

----End

Related Links

- [How Do I Bind a Virtual MFA Device?](#)
- [How Do I Obtain a Virtual MFA Verification Code?](#)

2.5.3 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 In the navigation on the left, choose  > **Security & Compliance** > **Data Encryption Workshop**.

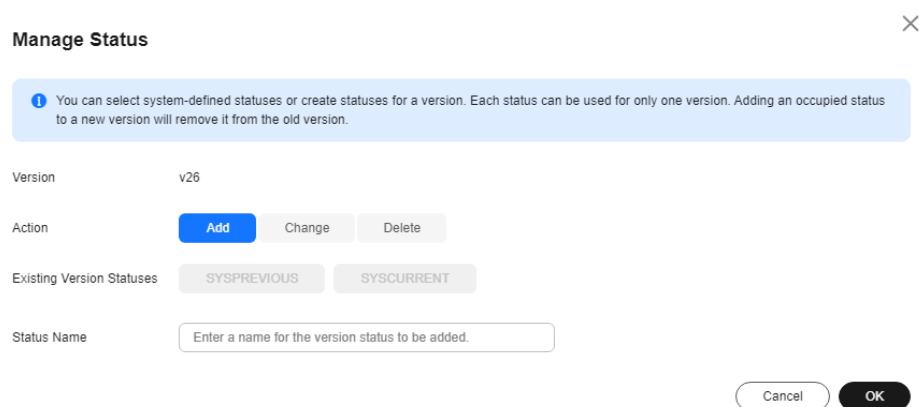
Step 4 In the navigation pane on the left, choose **Cloud Secret Management Service** > **Secrets**.

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 2-14 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

2.5.4 Setting the Version Expiration Time

This section describes how to set the version expiration time on the secret details page.

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** In the navigation on the left, choose  > **Security & Compliance** > **Data Encryption Workshop**.
- Step 4** In the navigation pane on the left, choose **Cloud Secret Management Service** > **Secrets**.
- Step 5** Click a secret name to go to the details page.
- Step 6** In the **Version** area, click **Configure Expiration** of the target secret.
- Step 7** On the displayed page, set an expiration time, and click **OK**.

 **NOTE**

The expiration time can be set to a date or a number of days. After the expiration date is set, the expiration date is displayed.

Figure 2-15 Setting an expiration time

Configure Expiration

Version v2

KMS Encryption Key ID 5645036c-2d2e-4a5f-92d5-6d758072084d

Version Status SYSCURRENT

Created Oct 28, 2024 22:17:00 GMT+08:00

Expiration Time **Date** Days

Select a date and time.

Cancel OK

----End

2.5.5 Rotation Secret Version

This section describes how to rotate secret versions on the secret details page.

Constraints


- The secret type is rotation secret.
- The secret account must be an existing database account.
- When the rotation function is enabled for the first time, CSMS automatically creates an agency for the user in the current project of the region after the user confirms the authorization. Therefore, users need to ensure that the account has the following IAM permissions:
iam:permissions:grantRoleToAgencyOnProject, iam:agencies:listAgencies, iam:roles:listRoles, iam:agencies:createAgency, iam:permissions:checkRoleForAgencyOnProject and iam:roles:createRole.
The agency to be created varies depending on the type of the secret to be rotated.
 - **RDS secret**
 - Create an agency named **CSMSAccessFunctionGraph** with account named **op_svc_kms** and permission named **CSMSAccessFunctionGraph**. The agency uses a project-level service policy, which includes the **functiongraph:function:invoke** permission for **FunctionGraph**.
 - Create an agency named **FunctionGraphAgencyForRotateRDSByCSMSV3**. The cloud service


is **FunctionGraph**, and the permission name is **FunctionGraphAgencyForRotateRDSByCSMSV3**. The project-level service policy is used, including:

- **CSMS** permissions: csms:secret:getVersion, csms:secret:listVersion, csms:secret:createVersion, csms:secret:getStage, csms:secret:get and csms:secret:updateStage.
 - **VPC** permissions: vpc:ports:create, vpc:vpcs:get, vpc:ports:get, vpc:ports:delete and vpc:subnets:get.
 - **KMS** permissions: kms:cmk:createDataKey and kms:cmk:decryptDataKey.
 - **RDS** permission: rds:password:update
- **TaurusDB secret**
- Create an agency named **CSMSAccessFunctionGraph** with account **op_svc_kms** and permission **CSMSAccessFunctionGraph**. The agency uses a project-level service policy, including the functiongraph:function:invoke permission for **FunctionGraph** to synchronously execute functions.
 - Create an agency named **FunctionGraphAgencyForRotateGaussDBByCSMSV3**. The cloud service is **FunctionGraph**, and the permission name is **FunctionGraphAgencyForRotateGaussDBByCSMSV3**. The project-level service policy is used, including:
 - **CSMS** permissions: csms:secretVersion:get, csms:secretVersion:list, csms:secretVersion:create, csms:secretStage:get, csms:secret:get and csms:secretStage:update.
 - **VPC** permissions: vpc:ports:create, vpc:vpcs:get, vpc:ports:get, vpc:ports:delete and vpc:subnets:get.
 - **KMS** permissions: kms:dek:create and kms:dek:decrypt.
 - **TaurusDB** permission: gaussdb:user:modify

Manual Rotation

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 In the navigation on the left, choose  > **Security & Compliance** > **Data Encryption Workshop**.

Step 4 In the navigation pane on the left, choose **Cloud Secret Management Service** > **Secrets**.

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

Step 6 In the **Version** area, click **Rotate Now**.

Step 7 On the displayed page, enter **ROTATE**, and click **OK**.


Step 8 Wait until a message is displayed in the upper right corner, indicating the rotation starts now.


Step 9 After the version is rotated, the latest secret version is in **SYSCURRENT** state.

----End

Automatic Rotation

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.

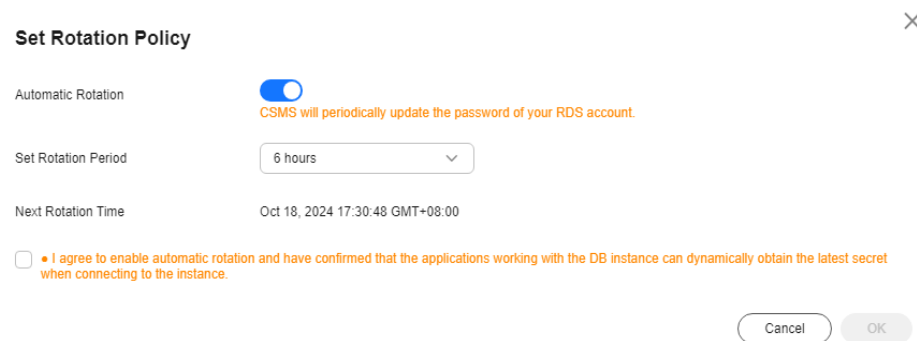
Step 3 In the navigation on the left, choose  > **Security & Compliance** > **Data Encryption Workshop**.

Step 4 In the navigation pane on the left, choose **Cloud Secret Management Service** > **Secrets**.

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

Step 6 Click **Set Rotation Policy** in the upper right corner. On the **Set Rotation Policy** page, toggle on the **Automatic Rotation** switch, as shown in [Figure 2-16](#).

Figure 2-16 Automatic rotation



Step 7 Set an automatic rotation period, select the risk warning, and click **OK**. A message indicating the rotation policy is set successfully is displayed in the upper right corner.

Step 8 After automatic rotation is enabled, if the secret version fails to be rotated, you can view the number of rotation failures in the current version area. You can click the number of rotation failures to view the rotation failure records.

NOTE

- If the rotation fails for three consecutive times, the automatic rotation button of the secret is disabled.
- Rotation failure records cannot be manually deleted. They are stored for one month and will be automatically deleted after one month.

----End

2.6 Managing Tags

2.6.1 Adding a Tag

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

Procedure



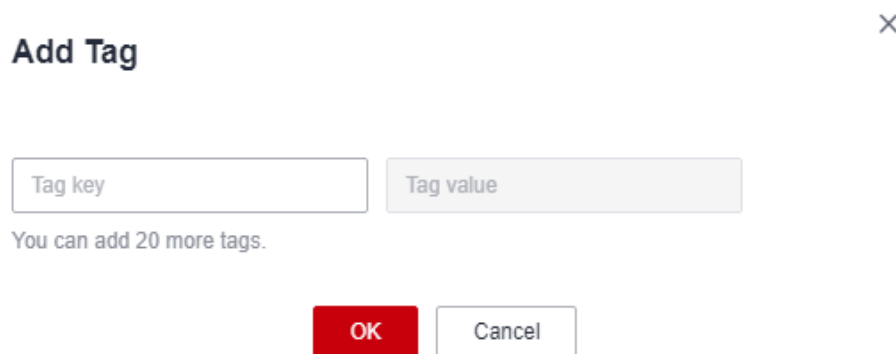
- Step 1** [Log in to the management console.](#)
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** In the navigation on the left, choose  > **Security & Compliance** > **Data Encryption Workshop**.
- Step 4** In the navigation pane on the left, choose **Cloud Secret Management Service** > **Secrets**.
- 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 2-17](#). In the **Add Tag** dialog box, enter the tag key and tag value. [Table 2-5](#) describes the parameters.

Figure 2-17 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 2-5 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">• Mandatory.• The tag key must be unique for the same custom key.• 128 characters limit.• The value cannot start or end with a space.• Cannot start with _sys_.• The following character types are allowed:<ul style="list-style-type: none">- Chinese- English- Numbers- Space- Special characters: <code>._:/=+-@</code>
Tag value	Value of the tag	<ul style="list-style-type: none">• Optional• 255 characters limit.• The following character types are allowed:<ul style="list-style-type: none">- Chinese- English- Numbers- Space- Special characters: <code>._:/=+-@</code>

Step 7 Click **OK**.

----End

2.6.2 Searching for a Secret by Tag

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

Prerequisites

Tags have been added.

Procedure



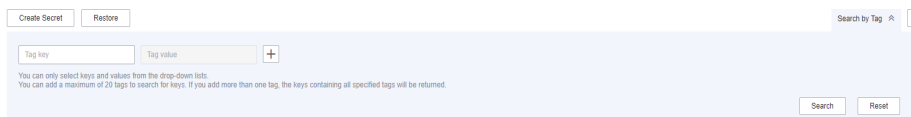
- Step 1** [Log in to the management console.](#)
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** In the navigation on the left, choose  > **Security & Compliance** > **Data Encryption Workshop.**
- Step 4** In the navigation pane on the left, choose **Cloud Secret Management Service** > **Secrets.**
- Step 5** Click **Search by Tag** to show the search box, as shown in [Figure 2-18.](#)

Figure 2-18 Search box




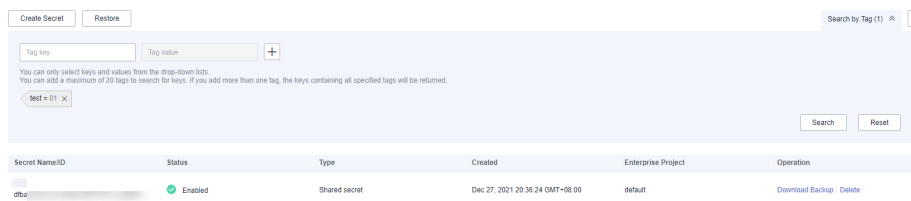

- Step 6** In the search box, enter or select a tag key and a tag value.
- Step 7** Click  to add the input to the search criteria, and click **Search**, as shown in [Figure 2-19.](#)

Figure 2-19 Search result



NOTE

- Multiple tags can be added for one search. A maximum of 20 tags can be added for one search. Each search result meets all the search criteria.
- To delete a tag from the search criteria, click  next to the tag.
- You can click **Reset** to reset the search criteria.

----End

2.6.3 Modifying a Tag Value

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

Procedure

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



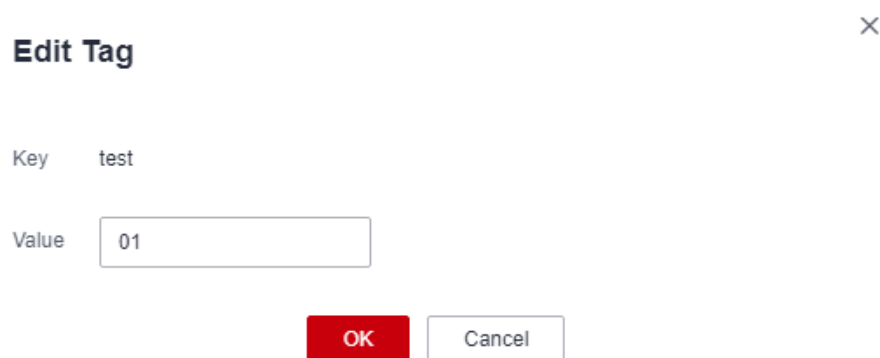
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** In the navigation on the left, choose  > **Security & Compliance > Data Encryption Workshop.**
- Step 4** In the navigation pane on the left, choose **Cloud Secret Management Service > Secrets.**
- Step 5** Click a secret name to go to the details page.
- Step 6** In the **Tags** area, click **Edit.**

Figure 2-20 Editing a tag





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

2.6.4 Deleting a Tag

This section describes how to delete tags on the CSMS console.

Procedure

- Step 1** [Log in to the management console.](#)
 - Step 2** Click  in the upper left corner of the management console and select a region or project.
 - Step 3** In the navigation on the left, choose  > **Security & Compliance > Data Encryption Workshop.**
 - Step 4** In the navigation pane on the left, choose **Cloud Secret Management Service > Secrets.**
 - 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

2.7 Creating an Event

With event notification, you can understand the secret version changes. The notifications are in JSON format, which is applicable to automatic parsing in machine-machine scenarios. This section describes how to create an event on the **Events** page.

When creating an event, you can set the event type to new **Version creation**, **Version expiry**, **Secret rotation**, and **Secret deletion**.

Constraints

You can create a maximum of 30 events.

Procedure



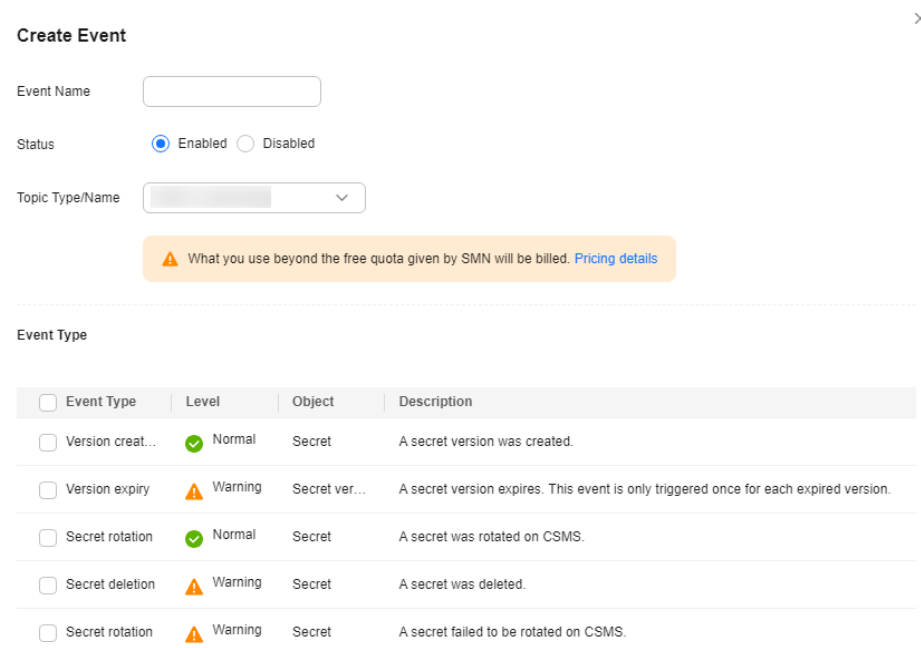
- Step 1** [Log in to the management console](#).
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** In the navigation on the left, choose  > **Security & Compliance** > **Data Encryption Workshop**.
- Step 4** In the navigation pane on the left, choose **Cloud Secret Management Service** > **Events**. The **Events** page is displayed.
- Step 5** Click **Create Event** in the upper right corner.

Figure 2-21 Creating an event



Event Type	Level	Object	Description
<input type="checkbox"/> Version creat...	Normal	Secret	A secret version was created.
<input type="checkbox"/> Version expiry	Warning	Secret ver...	A secret version expires. This event is only triggered once for each expired version.
<input type="checkbox"/> Secret rotation	Normal	Secret	A secret was rotated on CSMS.
<input type="checkbox"/> Secret deletion	Warning	Secret	A secret was deleted.
<input type="checkbox"/> Secret rotation	Warning	Secret	A secret failed to be rotated on CSMS.

Table 2-6 Parameters for creating an event

Parameter	Description
Event Name	Name of the event to be created. NOTE Only letters, digits, hyphens (-), and underscores (_) are supported.
Status	The options are Enabled and Disabled . By default, Enabled is selected.
Topic Type/Name	Topic type: SMN is selected by default. Topic name: name of the topic created in SMN. NOTE For details about how to create a custom topic type or name, see Creating a Topic .
Event Type	Supported event types, including Version creation , Version expiry , and Secret deletion .

Step 6 Click **OK**.

Step 7 View the created event in the event list. The default event status is **Enabled**.

Figure 2-22 Event list

Event Name	Status	Subscription	Topic Type/Name	Created	Operation
123	Enabled	Version creation Version expiry Secret...	SMN	Jun 28, 2024 10:31:24 GMT+08:00	Edit Delete

----End


2.8 Managing Events


2.8.1 Viewing Events

This section describes how to view the information about the created events on the **Events** page, including the event name, status, subscription event type, topic type/name, and 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 In the navigation on the left, choose  > **Security & Compliance** > **Data Encryption Workshop**.

Step 4 In the navigation pane on the left, choose **Cloud Secret Management Service** > **Events**. The **Events** page is displayed.

Step 5 In the event list, view the event information. [Table 2-7](#) describes the parameters in the event list.

Figure 2-23 Event list

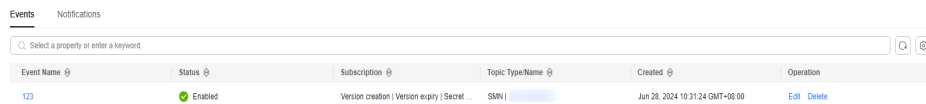
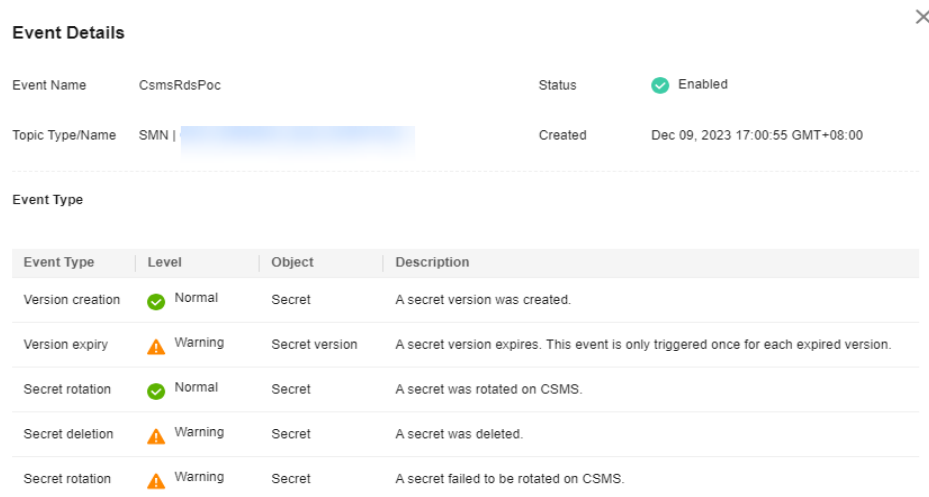


Table 2-7 Parameters in the event list

Parameter	Description
Event Name	Name of an event
Status	Event status, including: <ul style="list-style-type: none"> • Enabled • Disabled
Subscription	Event type selected during event creation. The options are as follows: <ul style="list-style-type: none"> • Version creation • Version expiry • Secret rotation • Secret deletion
Topic Type/Name	Topic type: SMN is selected by default. Topic name: name of the topic created in SMN.
Created	Time when the event is created
Operation	You can edit or delete an event in the Operation column.

Step 6 Click the event name to view its details.

Figure 2-24 Event details



Event Details ✕

Event Name: CsmsRdsPoc Status: ✔ Enabled

Topic Type/Name: SMN | Created: Dec 09, 2023 17:00:55 GMT+08:00

Event Type



Event Type	Level	Object	Description
Version creation	✔ Normal	Secret	A secret version was created.
Version expiry	⚠ Warning	Secret version	A secret version expires. This event is only triggered once for each expired version.
Secret rotation	✔ Normal	Secret	A secret was rotated on CSMS.
Secret deletion	⚠ Warning	Secret	A secret was deleted.
Secret rotation	⚠ Warning	Secret	A secret failed to be rotated on CSMS.

----End

2.8.2 Editing an Event

This section describes how to modify an event type on the **Events** page.

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** In the navigation on the left, choose  > **Security & Compliance** > **Data Encryption Workshop**.
- Step 4** In the navigation pane on the left, choose **Cloud Secret Management Service** > **Events**. The **Events** page is displayed.
- Step 5** Locate the target event and click **Edit** in the **Operation** column.
- Step 6** Select the target event type.
- Step 7** Click **OK**.

----End

2.8.3 Enabling an Event

This section describes how to enable a disabled event on the **Events** page.

Prerequisites

The event to be enabled must be in the **Disabled** state.

Procedure



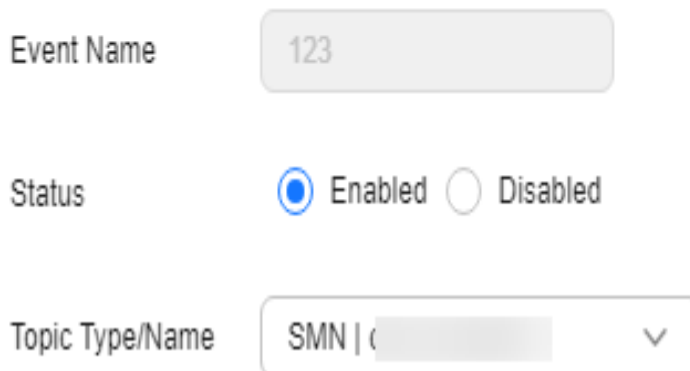
- Step 1** [Log in to the management console.](#)
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** In the navigation on the left, choose  > **Security & Compliance** > **Data Encryption Workshop.**
- Step 4** In the navigation pane on the left, choose **Cloud Secret Management Service** > **Events.** The **Events** page is displayed.
- Step 5** Locate the target event to be enabled, click **Edit** in the **Operation** column.
- Step 6** Select **Enabled** for **Status.**

Figure 2-25 Enabling an event

Edit Event



Event Name

Status Enabled Disabled

Topic Type/Name ▼

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

----End

2.8.4 Disabling an Event



This section describes how to disable an enabled event on the **Events** page.

Prerequisites

The event to be disabled must be in the **Enabled** 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** In the navigation on the left, choose  > **Security & Compliance** > **Data Encryption Workshop**.
- Step 4** In the navigation pane on the left, choose **Cloud Secret Management Service** > **Events**. The **Events** page is displayed.
- Step 5** Locate the target event to be disabled, click **Edit** in the **Operation** column.
- Step 6** Select **Disabled** for **Status**.
- Step 7** Click **OK**. A message is displayed in the upper right corner of the page, indicating that the event is disabled successfully.
- End



2.8.5 Deleting an Event

This section describes how to delete a created event on the **Events** page. Before deleting an event, ensure that the event is no longer used.

Constraints

Event notifications can be deleted only after all associated secrets have been canceled. If the associated secret is not canceled, the deletion 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** In the navigation on the left, choose  > **Security & Compliance** > **Data Encryption Workshop**.
- Step 4** In the navigation pane on the left, choose **Cloud Secret Management Service** > **Events**. The **Events** page is displayed.
- Step 5** Click **Delete** in the **Operation** column of the target event. The **Delete Event** dialog box is displayed.
- End


2.9 Viewing Notifications

This section describes how to view the event notifications.

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 In the navigation on the left, choose  > **Security & Compliance** > **Data Encryption Workshop**.

Step 4 In the navigation pane on the left, choose **Cloud Secret Management Service** > **Events**.

Step 5 Click the **Notifications** tab. The page for viewing notifications is displayed,

Step 6 On the **Notifications** tab page, you can view the changes made to the secrets of the associated events.

----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.

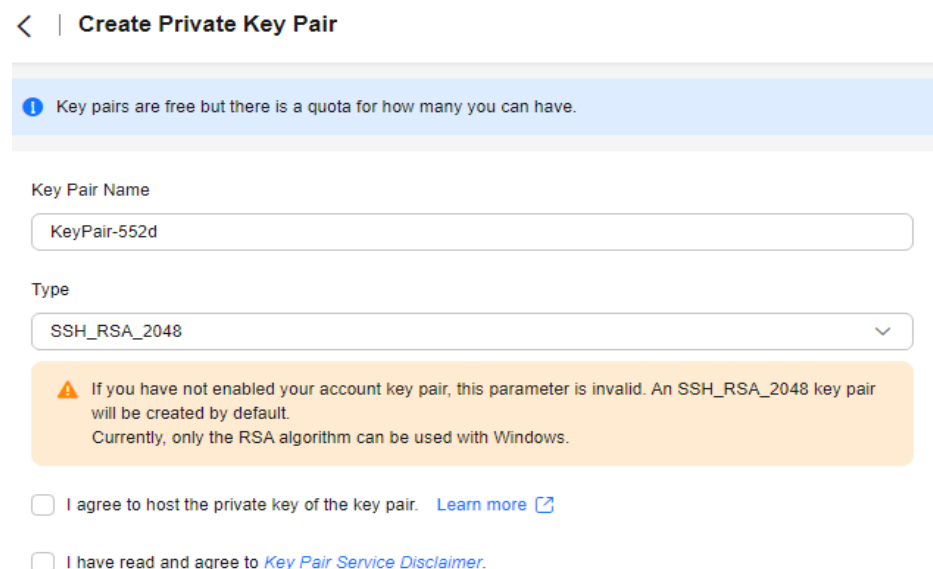
Step 3 Click  in the upper left corner and choose **Security & Compliance > Data Encryption Workshop**.

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

Step 5 In the displayed **Private Key Pairs** tab, create a private key pair or an account key pair as required.

Step 6 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



< | **Create Private Key Pair**

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

Key Pair Name
KeyPair-552d

Type
SSH_RSA_2048

⚠ 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.

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

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

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

NOTE

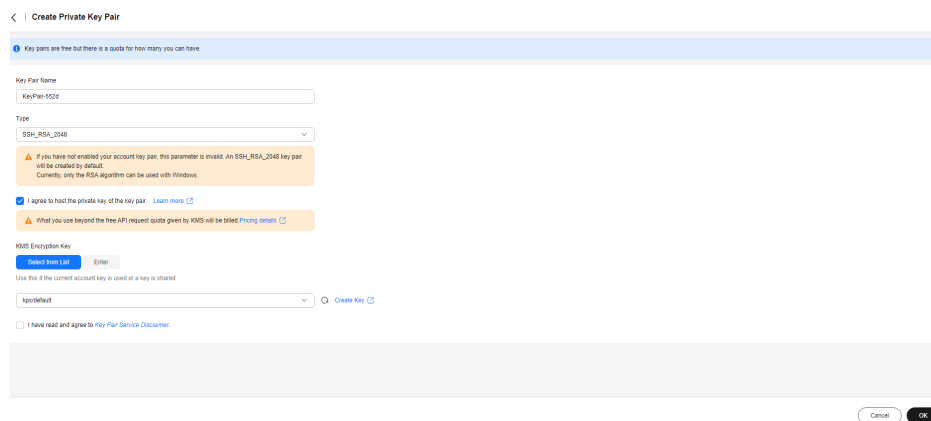
Currently, only the RSA algorithm can be used with Windows.

Step 8 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



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

Step 10 Click **OK**. The browser automatically downloads the private key. When the private key is downloaded, a dialog box is displayed.

Step 11 Save the private key as prompted by the dialog box.

NOTICE

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

Step 12 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**

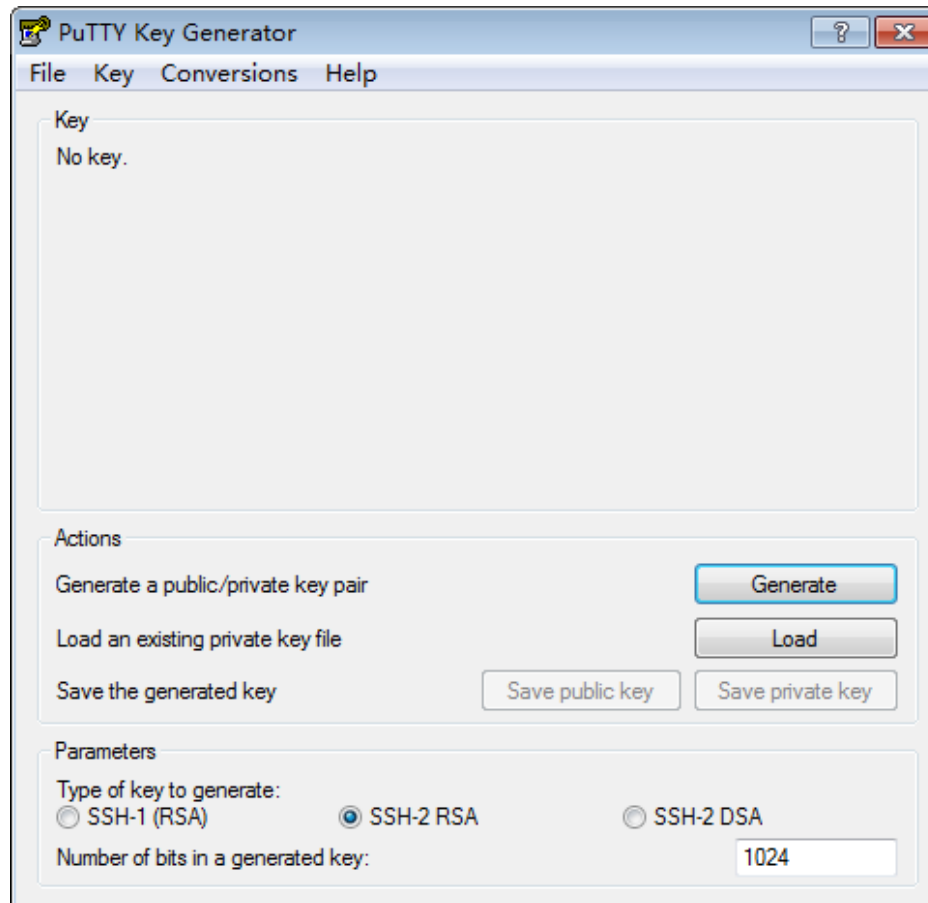
After the key pair is created, download the private key to your local host and keep it securely.

----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



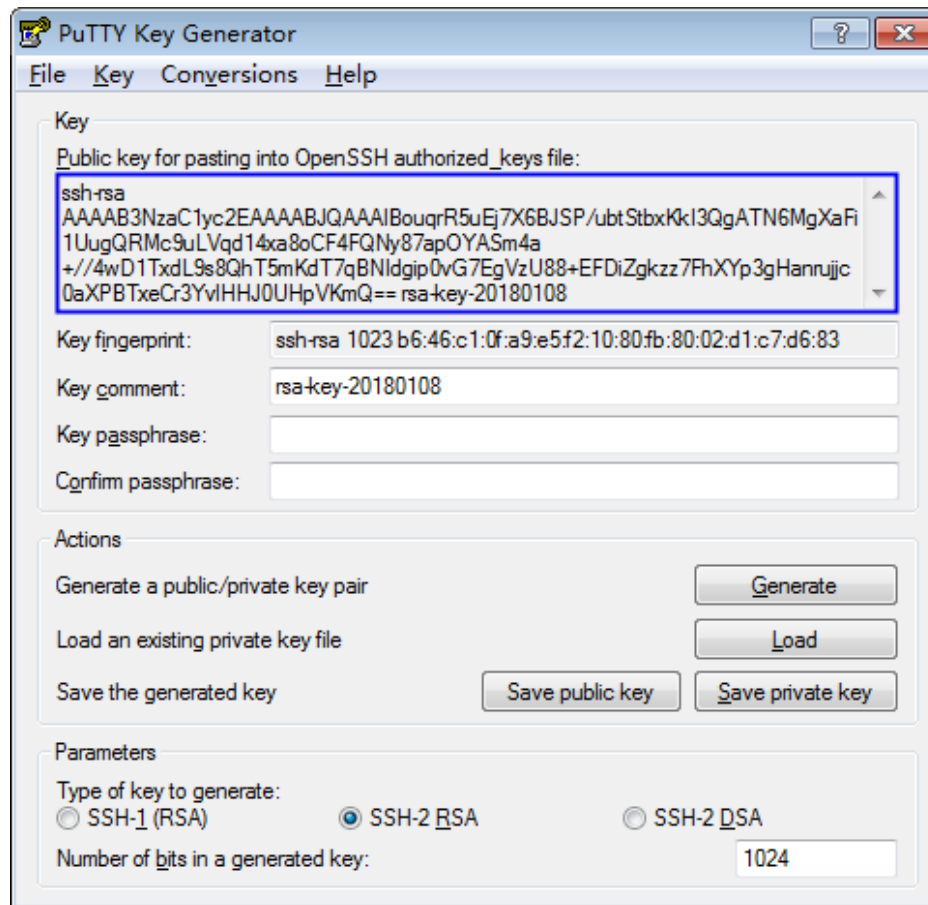
- Step 2** Configure the parameters as described in [Table 3-1](#).

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 SSH-2 RSA is supported.
Number of bits in a generated key	Length of a key pair to be imported to the management console. Currently, the following length values are supported: 1024, 2048, and 4096 .

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

Figure 3-4 Obtaining the public and private keys



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

NOTICE

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

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

----End

3.2 Importing a Key Pair

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

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 (not recommended)
 - 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.

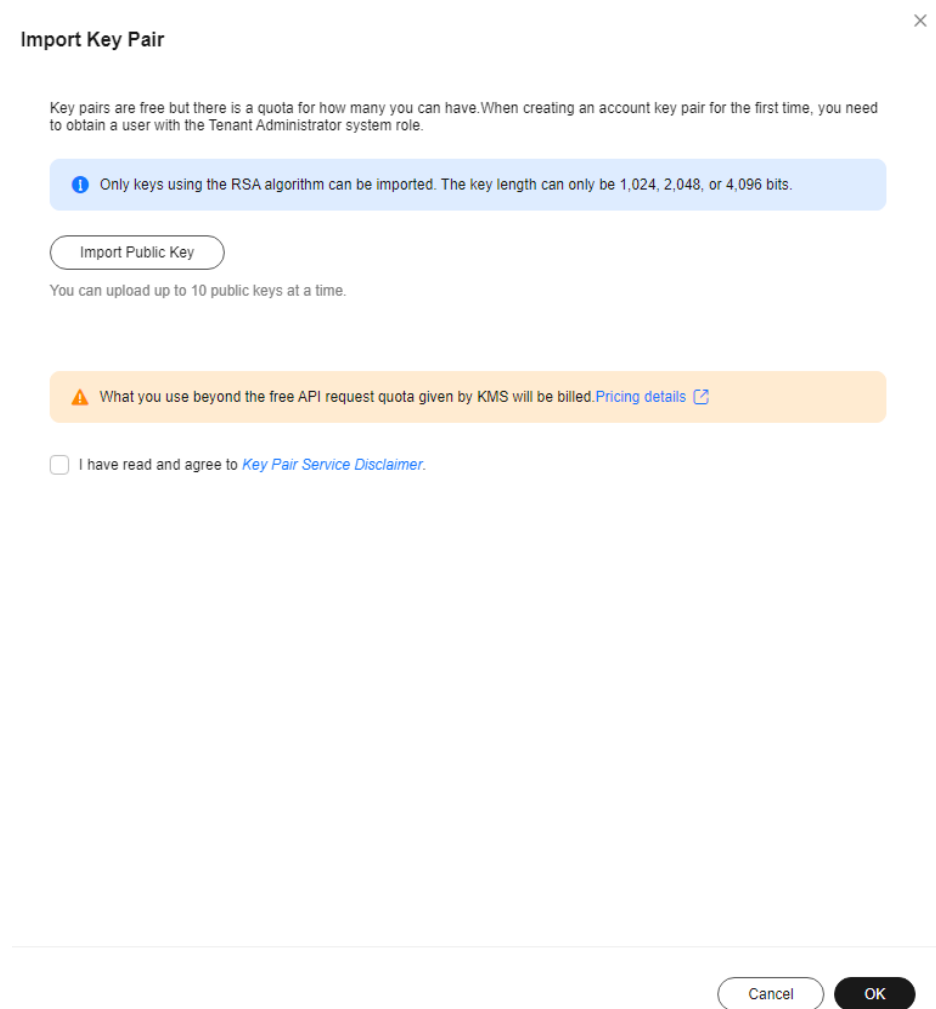
Step 3 Click  in the upper left corner and choose **Security & Compliance > Data Encryption Workshop.**

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

Step 5 In the displayed **Account Key Pairs** tab, create or import a key pair as needed.

Step 6 Click **Import Key Pair.** In the displayed dialog box, click , as shown in [Figure 3-5.](#)

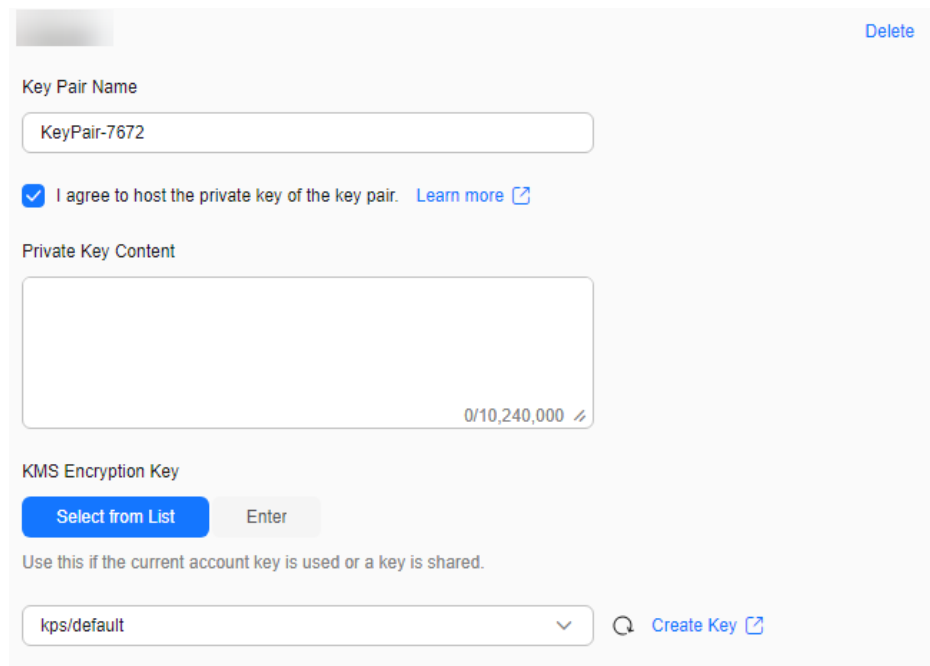
Figure 3-5 Importing a key pair



NOTE

- Currently, a maximum of 10 public keys can be imported at a time.
- 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 7 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

The screenshot shows a web interface for managing private keys. At the top right is a 'Delete' button. Below it is a 'Key Pair Name' field containing 'KeyPair-7672'. A checkbox is checked with the text 'I agree to host the private key of the key pair.' and a 'Learn more' link. Below that is a 'Private Key Content' text area with a character count of '0/10,240,000'. Underneath is a 'KMS Encryption Key' section with a 'Select from List' button and an 'Enter' button. Below this is a note: 'Use this if the current account key is used or a key is shared.' At the bottom is a dropdown menu showing 'kps/default' and a 'Create Key' button.

1. 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 8 Read the *Key Pair Service Disclaimer* and select **I have read and agree to the Key Pair Service Disclaimer**.

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

----End

3.3 Upgrading a Key Pair

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

Prerequisites


- A key pair has been created or imported.
- 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.

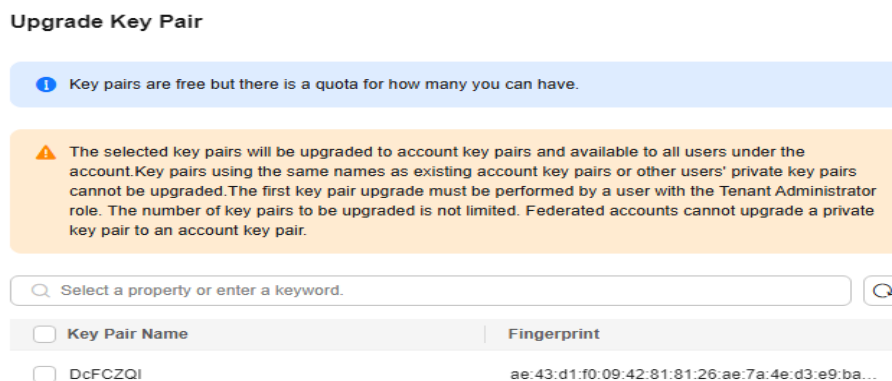
Step 3 Click  in the upper left corner and choose **Security & Compliance > Data Encryption Workshop**.

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  in the upper left corner and choose **Security & Compliance > Data Encryption Workshop**.

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

Step 5 In the row containing the 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  in the upper left corner and choose **Security & Compliance > Data Encryption Workshop**.

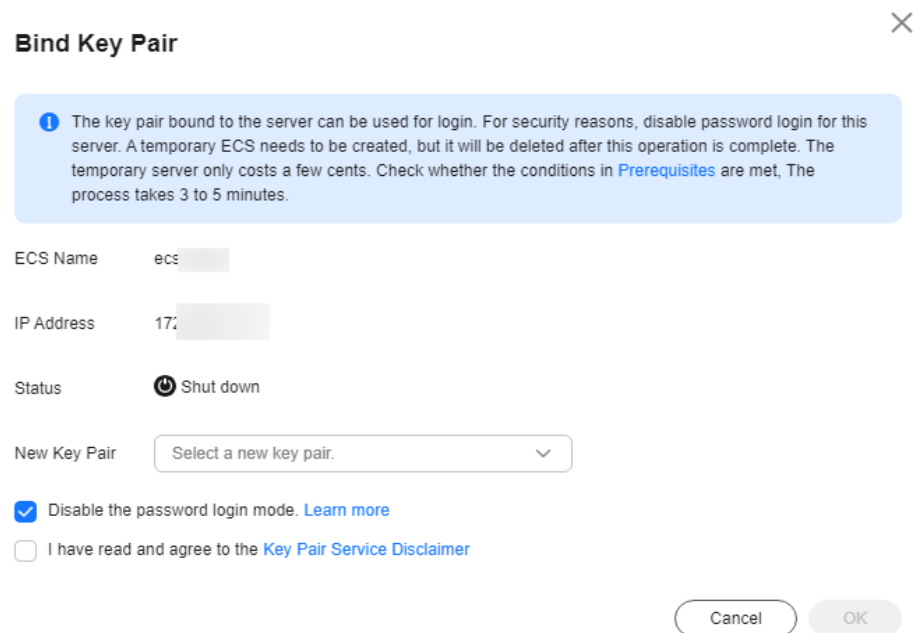
Step 4 In the navigation pane on the left, click **Key Pair Service**.

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.

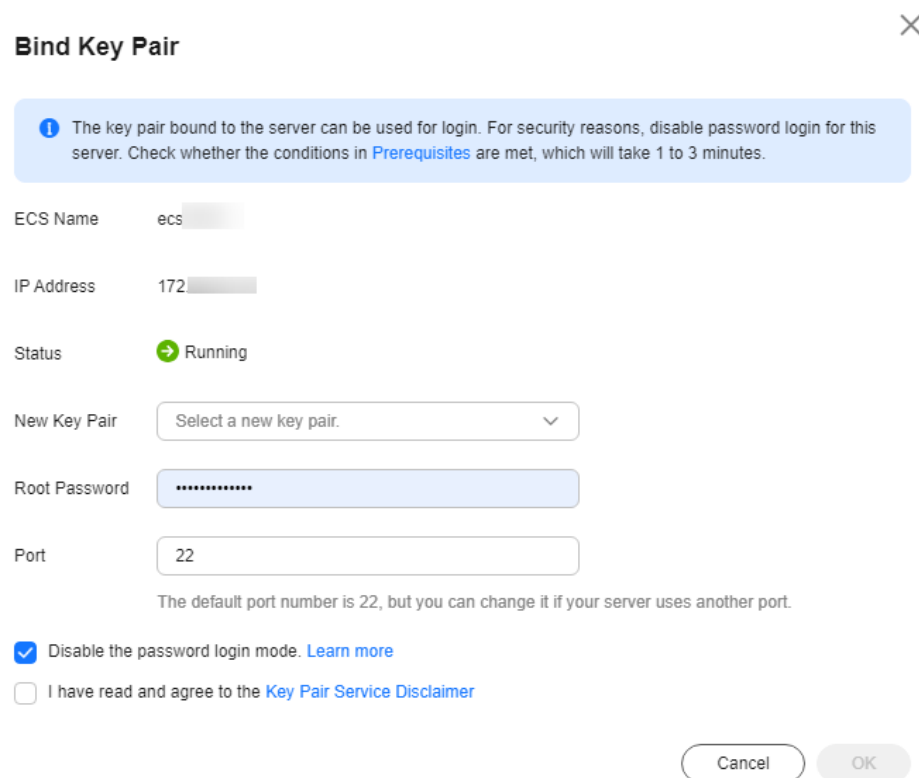
- If the ECS is shut down, a dialog box will be displayed, as shown in [Figure 3-8](#).

Figure 3-8 Binding a key pair (1)



- 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 ✕

1 The key pair bound to the server can be used for login. For security reasons, disable password login for this server. Check whether the conditions in [Prerequisites](#) are met, which will take 1 to 3 minutes.

ECS Name ecs

IP Address 172

Status ➔ Running

New Key Pair Select a new key pair. ▾

Root Password

Port 22

The default port number is 22, but you can change it if your server uses another port.

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

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

Cancel OK

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

Before using user-defined port, ensure that:

- The key pair can be connected to the ECS using the port. For details about how to modify the security group configuration of an ECS, see [Configuring Security Group Rules](#).
- Modify the default port of the ECS and ensure that the port is enabled. For details, see [Enhancing Security for SSH Logins to Linux ECSs](#).

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  in the upper left corner and choose **Security & Compliance > 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 ✕

1 The key pair bound to the server can be used for login. For security reasons, disable password login for this server. A temporary ECS needs to be created, but it will be deleted after this operation is complete. The temporary server only costs a few cents. Check whether the conditions in [Prerequisites](#) are met. The process takes 3 to 5 minutes.

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

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

Key Pair:

Root Password:

Port:

The default port number is 22, but you can change it if your server uses another port.

ECS Name	IP Address	Status	Key Pair	Root Password	Port	Disable ...
ec-...	...	Running	Select a new key... v	*****	22	<input checked="" type="checkbox"/>
...	...	Running	Select a new key... v	*****	22	<input checked="" type="checkbox"/>
...	...	Running	Select a new key... v	*****	22	<input checked="" type="checkbox"/>

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

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

- 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 ✕

1 The key pair bound to the server can be used for login. For security reasons, disable password login for this server. A temporary ECS needs to be created, but it will be deleted after this operation is complete. The temporary server only costs a few cents. Check whether the conditions in [Prerequisites](#) are met. The process takes 3 to 5 minutes.

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

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

Key Pair:

ECS Name	IP Address	Status	Key Pair	Root Password	Port	Disable ...
...	...	Running	Select a new key... v	*****	22	<input checked="" type="checkbox"/>
...	...	Running	Select a new key... v	*****	22	<input checked="" type="checkbox"/>

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

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

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

Before using user-defined port, ensure that:

- The key pair can be connected to the ECS using the port. For details about how to modify the security group configuration of an ECS, see [Configuring Security Group Rules](#).
- Modify the default port of the ECS and ensure that the port is enabled. For details, see [Enhancing Security for SSH Logins to Linux ECSs](#).

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, and private 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  in the upper left corner and choose **Security & Compliance > Data Encryption Workshop**.

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

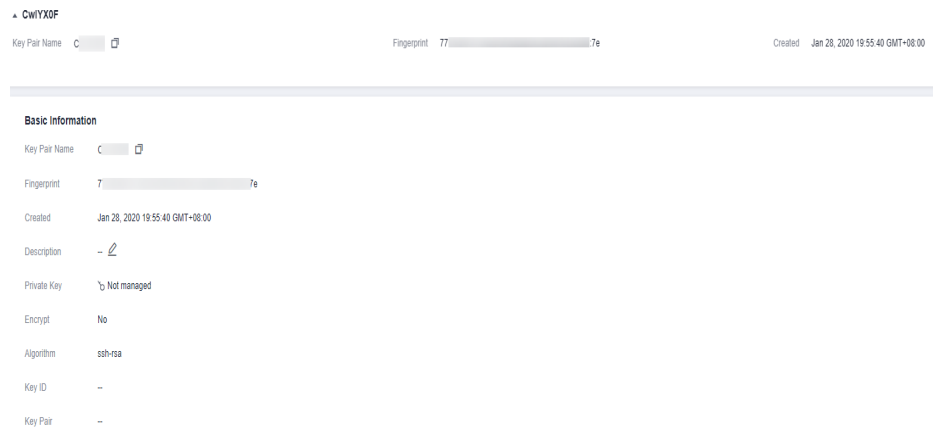
Step 5 Click the **Private Key Pairs** tab and view information about the key pair in the key pair list.

 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.

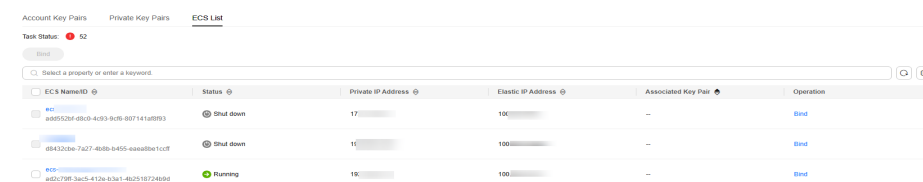
Table 3-3 lists the parameters of the ECS to which the key pair is bound.


Table 3-3 ECS parameters

Parameter	Description
ECS Name/ID	Name and ID of an ECS
Status	Status of an ECS. Possible values are as follows: <ul style="list-style-type: none"> Running Creating Faulty Shut down
Private IP address	Private IP Address
Elastic IP Address	Elastic IP address
Associated 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	Oper...	Executed ...	Failure Cause	Opera...
<small>ecs-</small> add552bf-d8c0-4c93-9cf6-907...	8CDGlgv	Bind	Nov 28, 2024 ...	Server login credential...	Delete
<small>ecs-</small> d446623d-c05c-47f6-86ac-74...	80mcanDA	Bind	Nov 28, 2024 ...	Attach volume error	Delete
<small>ecs-</small> 254f0f04-2902-476b-8dcd-c8...	20241128	Bind	Nov 28, 2024 ...	Attach volume error	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.](#)



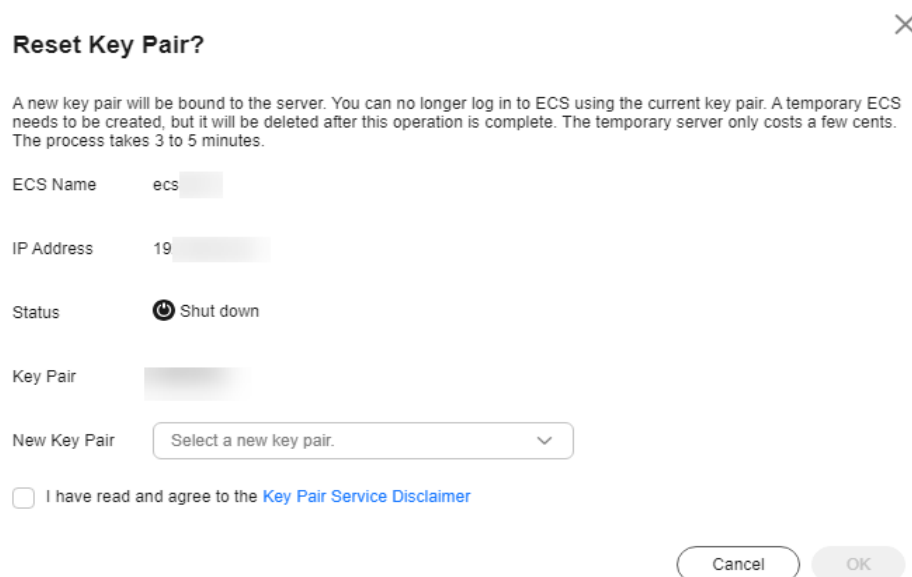
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click  in the upper left corner and choose **Security & Compliance > Data Encryption Workshop**.
- Step 4** In the navigation pane on the left, click **Key Pair Service**.
- Step 5** Click the **ECS List** tab, locate the target ECS in the list and click **Reset** in the **Operation** column. The key pair reset dialog box is displayed, as shown in [Figure 3-15](#).

Figure 3-15 Resetting a key pair




Reset Key Pair?

A new key pair will be bound to the server. You can no longer log in to ECS using the current key pair. A temporary ECS needs to be created, but it will be deleted after this operation is complete. The temporary server only costs a few cents. The process takes 3 to 5 minutes.

ECS Name ecs

IP Address 19

Status  Shut down

Key Pair

New Key Pair Select a new key pair.

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

Cancel OK

- Step 6** Select a new key pair from the drop-down list box of **New Key Pair**.
- Step 7** The default port number is 22 and can be modified.

 **NOTE**

Before using user-defined port, ensure that:

- The key pair can be connected to the ECS using the port. For details about how to modify the security group configuration of an ECS, see [Configuring Security Group Rules](#).
- Modify the default port of the ECS and ensure that the port is enabled. For details, see [Enhancing Security for SSH Logins to Linux ECSs](#).

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

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

----End

3.5.5 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  in the upper left corner and choose **Security & Compliance > Data Encryption Workshop**.

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

Step 5 Click the **ECS List** tab, locate the target ECS in the list and click **Replace** in the **Operation** column. The key pair replacement dialog box is displayed, as shown in [Figure 3-16](#).

Figure 3-16 Replacing a key pair

✕

Replace Key Pair?

A new key pair will be bound to the server. You can no longer log in to ECS by using its current key pair. The process takes 1 to 3 minutes.

ECS Name: ecs

IP Address: 192

Status: ➔ Running

Key Pair: [Redacted]

New Key Pair:

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

Paste the private key file content here.

Port:

The default port number is 22, but you can change it if your server uses another port.

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

Step 6 Select a new key pair from the drop-down list box of **New Key Pair**.

Step 7 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 8 The default port number is 22 and can be modified.

NOTE

Before using user-defined port, ensure that:

- The key pair can be connected to the ECS using the port. For details about how to modify the security group configuration of an ECS, see [Configuring Security Group Rules](#).
- Modify the default port of the ECS and ensure that the port is enabled. For details, see [Enhancing Security for SSH Logins to Linux ECSs](#).

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 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.

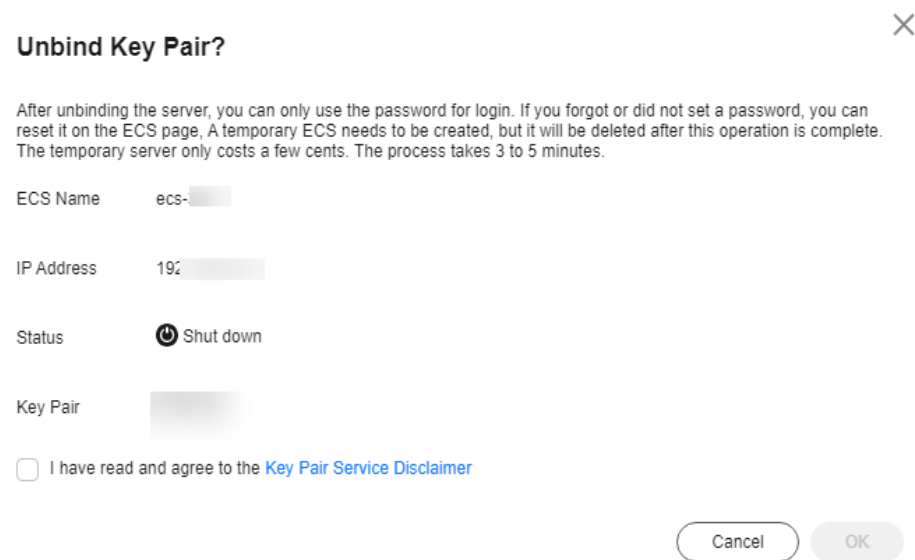
Step 3 Click  in the upper left corner and choose **Security & Compliance > Data Encryption Workshop**.

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

Step 5 Click the **ECS List** tab, locate the target ECS in the list and click **Unbind** in the **Operation** column.

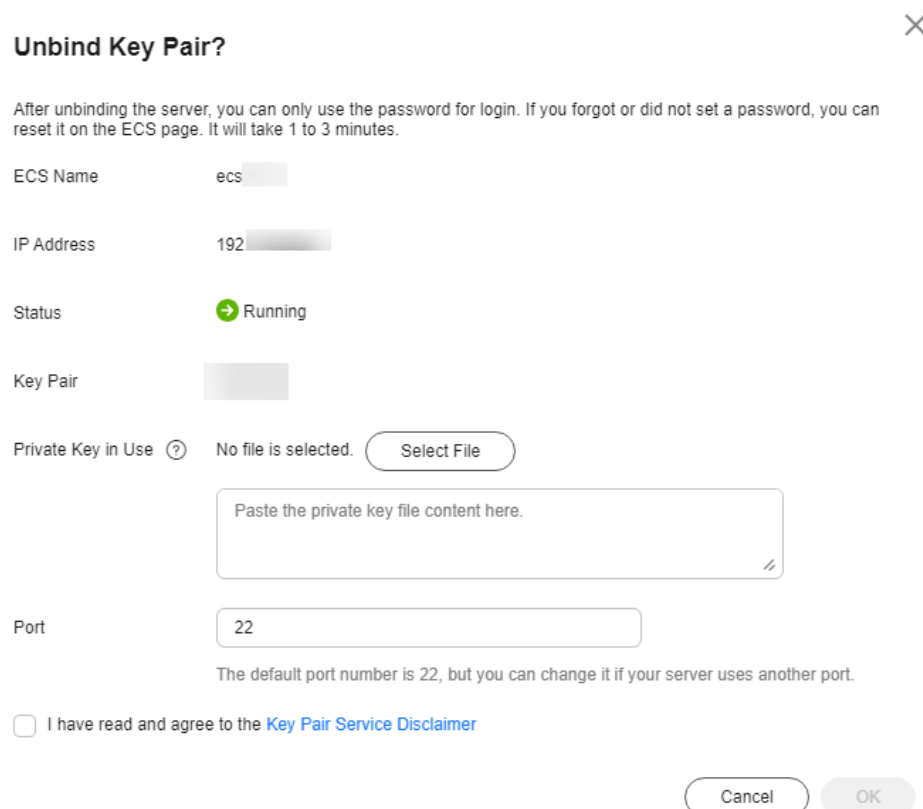
- If the ECS is shut down, a dialog box will be displayed, as shown in [Figure 3-17](#).

Figure 3-17 Unbinding a key pair (1)



- 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)



Step 6 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 7 The default port number is 22 and can be modified.

 NOTE

Before using user-defined port, ensure that:

- The key pair can be connected to the ECS using the port. For details about how to modify the security group configuration of an ECS, see [Configuring Security Group Rules](#).
- Modify the default port of the ECS and ensure that the port is enabled. For details, see [Enhancing Security for SSH Logins to Linux ECSs](#).

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

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

 NOTE

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 Downloading a Public Key

After the key pair is created, you can download the public key. This section describes how to download a public key on the KPS 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  in the upper left corner and choose **Security & Compliance > Data Encryption Workshop**.

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

Step 5 Locate the target key pair, click **Download Public Key** in the **Operation** column. The public key in .txt format is obtained.

----End

3.7 Managing Private Keys

3.7.1 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?](#).

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  in the upper left corner and choose **Security & Compliance > Data Encryption Workshop**.

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

Step 5 Click **Import Private Key** in the row where the target public key is located. Set parameters in the **Import Private Key** dialog box, as shown in [Figure 3-19](#).

Figure 3-19 Importing a private key

✕

Import Private Key

⚠ Private keys are encrypted and hosted on the cloud but can be exported as needed. Your private keys will never be used for any purpose irrelevant to key pair management.

Note: Once the private key is imported successfully, you will be charged for the management service by hour. This function is offered for free now. [Learn more](#)

Key Pair Name 7sG3NFL1

Private Key

No file is selected.

Private Key Content

KMS Encryption

Key ID 614a9

⚠ If KMS encryption is used, 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 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 **.ppk** 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

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

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

----End

3.7.2 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



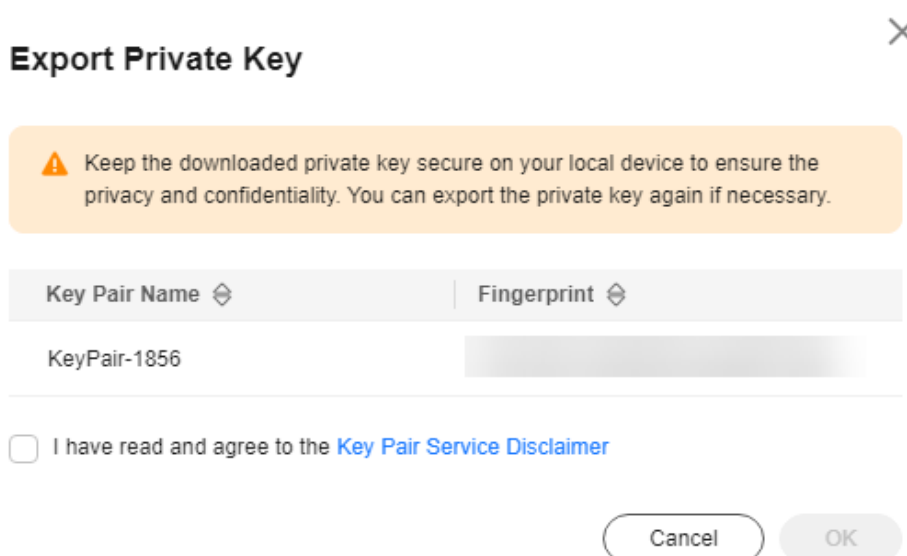
- Step 1** [Log in to the management console](#).
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click  in the upper left corner and choose **Security & Compliance > Data Encryption Workshop**.
- Step 4** In the navigation pane on the left, click **Key Pair Service**.
- Step 5** Click **Export Private Key** in the row where the target key pair resides. The **Export Private Key** dialog box is displayed, as shown in [Figure 3-20](#).

Figure 3-20 Exporting a private key



 **NOTE**

You can select multiple private keys and click **Export Private Key** to export them in batches.

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

3.7.3 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  in the upper left corner and choose **Security & Compliance > Data Encryption Workshop**.

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

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

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

3.8 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**.

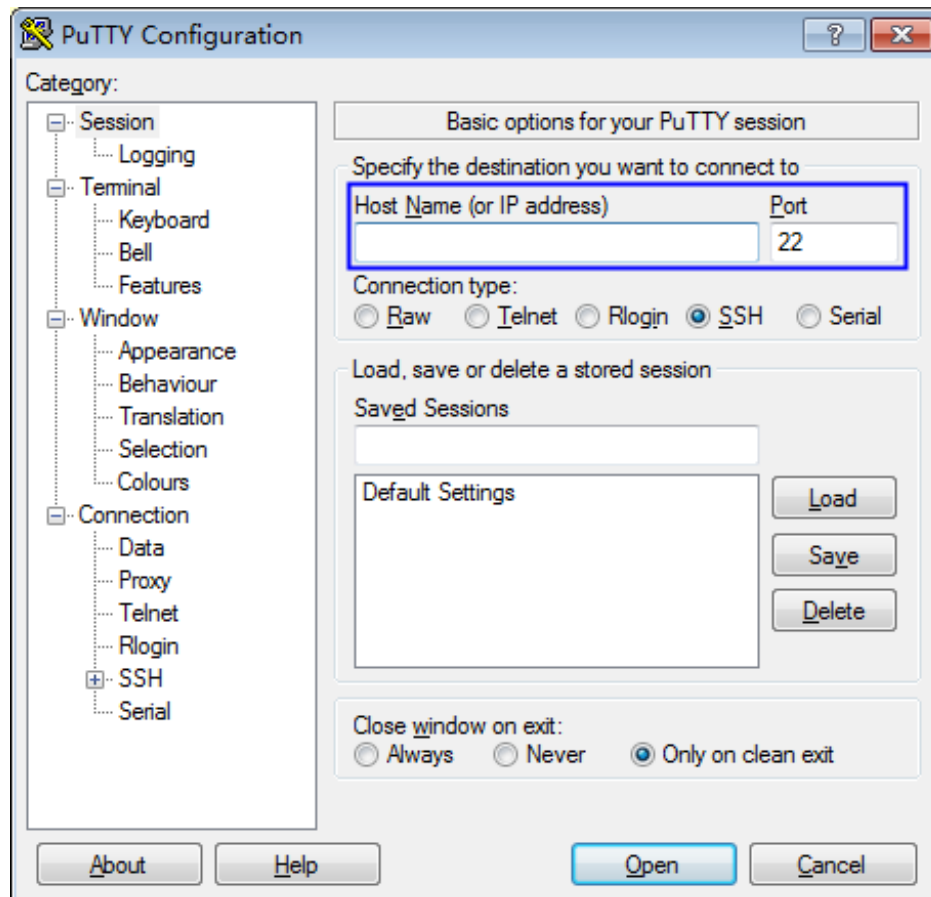
NOTE

- 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

3.9 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 *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 list, 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

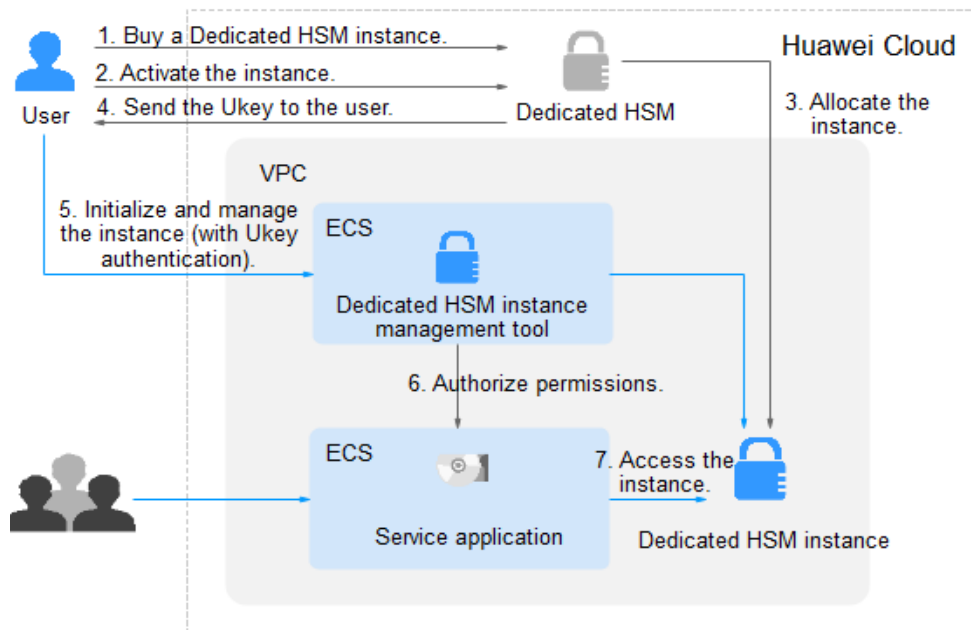


Table 4-1 describes the operation guide.

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 Activating a Dedicated HSM Instance .	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"> A security expert sends the Ukey to the email address you provided. A UKey is the only identifier of a Dedicated HSM user. Keep it properly. A security expert will provide you with the software and guide for initializing Dedicated HSM instances. If you have any questions, contact the expert. <p>NOTE You can submit a Service Ticket 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"> Install the tool for managing Dedicated HSM instances on the instance management node. Use the UKey and the management tool to initialize the Dedicated HSM instance, and register an administrator to manage the Dedicated HSM instance and the key. <p>For details, see Initializing a Dedicated HSM Instance.</p>	User
6	Install the security agent and granting access permissions.	<p>Install and initialize the security agent on service application nodes.</p> <p>For details, see Installing the Security Agent and Granting Access Permissions.</p>	User
7	Access the instance.	Service applications access the Dedicated HSM instances through APIs or SDK.	User

4.2 Purchasing a Dedicated HSM Instance

4.2.1 Creating a Dedicated HSM Instance

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

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

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

Prerequisites


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


Constraints

- 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 In the navigation on the left, choose  > **Security & Compliance** > **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



Step 7 Select a region and project.

Figure 4-3 Selecting a region



NOTE


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

Step 8 Select an instance edition. For details, see [Figure 4-4](#). [Table 4-2](#) lists related parameters.

Figure 4-4 Platinum edition

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

Encryption Algorithm
 Symmetric algorithm: AES and 3DES
 Asymmetric algorithm: RSA, ECDSA, and DSA
 Hash algorithm: SHA1 and SHA2
 Digest algorithm: SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, and SHA3-512

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

Performance
 Data Communication Protocol: TCP/IP with the maximum concurrent connection of 2,048
 RSA2048 signature computing performance: 1,500 TPS
 RSA2048 signature verification computing performance: 25,000 TPS
 ECDSA256 signature computing performance: 23,000 TPS
 ECDSA256 signature verification computing performance: 9,000 TPS
 DSA2048 signature computing performance: 2,800 TPS
 DSA2048 signature verification computing performance: 3,000 TPS

Certification FIPS 140-2 Level 3

Table 4-2 Edition parameters

Parameter	Description
Service Edition	Platinum edition
Encryption Algorithm	Algorithm supported by the HSM instance. <ul style="list-style-type: none"> • Symmetric algorithm: AES • Asymmetric algorithm: RSA, DSA, ECDSA, DE, and ECDH • Digest algorithm: SHA1, SHA256, SHA384
Specifications	Performance specifications supported by platinum edition, including: <ul style="list-style-type: none"> • Data communication protocol: TCP/IP (maximum number of concurrent connections: 2048) • RSA2048 signature computing performance: 1,500 TPS • RSA2048 signature verification computing performance: 25,000 TPS • ECDSA256 signature computing performance: 23,000 TPS • ECDSA256 signature verification computing performance: 9,000 TPS • DSA2048 signature computing performance: 2,800 TPS • DSA2048 signature verification computing performance: 3,000 TPS
Certification	FIPS 140-2 Level 3 certified

Step 9 Type the instance name.

Figure 4-5 Setting an instance name



The screenshot shows a text input field labeled 'Instance Name' containing the text 'DedicatedHSM-a766'. Below the field is a small note: 'When multiple instances are purchased, the system automatically adds a four-digit number to the end of each instance name for sequencing. For example, if the instance name is dhsm, the first instance will be displayed as dhsm-0001. If dhsm-0001 already exists, the first instance will be displayed as dhsm-0002.'

Step 10 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 11 Set the duration and number of Dedicated HSM instances to be purchased.

1. Set the required duration.

The required duration ranges from one month to one year.

2. Set the **Quantity**.

You can set the quantity as required.

To ensure high service reliability, you need to purchase at least two Dedicated HSM instances. You can purchase a maximum of 20 Dedicated HSM instances.

 **NOTE**

A single instance is only suitable for testing. If you want to purchase one for testing, contact our Huawei Cloud security experts.

Step 12 (Optional) Add tags to the dedicated HSM instance as needed, and enter the tag key and tag value.

 **NOTE**

- To add tags for an instance, locate the instance, and click **Tag** in the **Operation** column. For details about other operations, see [Tag Management](#).
- An instance can have up to 20 tags.

Step 13 Confirm the configuration and click **Next**. For any doubt about the pricing, click **Pricing details** to understand more.

Step 14 On the **Order Details** page, confirm the order details, read and select **I have read and agree to the Privacy Policy Statement**.

Step 15 Click **Pay Now**. On the displayed page, select a payment method and pay.

Step 16 After successful payment, you can view the information about the HSM instance on the HSM instance list page.

If the status of an HSM instance is **Installing**, it indicates that the instance is purchased successfully.

----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 In the navigation on the left, choose  > **Security & Compliance** > **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

AZ 

AZ1

AZ2

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

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

- Instance Name:** DedicatedHSM-60071291-0002
- Enterprise Project:** default (with a 'Create Enterprise Project' link)
- HSM Type:** Finance (with a description: 'Provides key management and cryptographic operation services, including IC card issuing, transaction verification, data encryption, digital signatures, and dynamic password authentication.')
 - **Finance:** Provides key management and encryption computing services, including IC card issuing, transaction verification, data encryption, digital signatures, and dynamic password authentication.
 - **Server:** Provides secure, complete key management services and high-performance concurrent cryptographic operations, such as data signatures, signature verification, and data encryption/decryption.
 - **Signature server:** Guarantees the integrity, confidentiality, anti-repudiation, and post-event traceability of user data by using digital signatures, digital envelopes, and digital digests.
- VPC:** vpc- (with a note: 'You can select an existing VPC or apply for one.')
 - **Assign IPv6 address to instance:**
 - **EIP Binding:**
- Subnet:** subnet- (with a note: 'You can select an existing VPC or apply for one.')
 - **Assign IPv6 address to instance:**
 - **EIP Binding:**
- Security Group:** kubernetes.io-default-sg-0

Table 4-3 Activation parameters

Parameter	Description	Example Value
Instance Name	Name of a Dedicated HSM instance NOTE The instance name can contain only letters, digits, underscores (_), and hyphens (-).	DedicatedHSM-3c98-0002
Enterprise Project	Enterprise project that the dedicated HSM is to be bound to	default
HSM Type	Available HSM types include Finance , Server , and Signature server . <ul style="list-style-type: none"> • Finance: Provides key management and encryption computing services, including IC card issuing, transaction verification, data encryption, digital signatures, and dynamic password authentication. • Server: Provides secure, complete key management services and high-performance concurrent cryptographic operations, such as data signatures, signature verification, and data encryption/decryption. • Signature server: Guarantees the integrity, confidentiality, anti-repudiation, and post-event traceability of user data by using digital signatures, digital envelopes, and digital digests. 	Finance

Parameter	Description	Example Value
VPC	You can select an existing Virtual Private Cloud (VPC), or click Apply for VPC to create one. For more information about VPC, see the <i>Virtual Private Cloud User Guide</i> .	vpc-test-dhsm
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> . NOTE Two nodes are created as the background resource pool for a Dedicated HSM instance. To ensure high availability of the nodes, a floating IP address is assigned to the instance.	subnet-test-dhsm (192.168.0.0 /24)
EIP Binding	After this parameter is enabled, you can bind an EIP to the Dedicated HSM instance to enable public access to the instance.	-
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  in the upper left corner and choose **Security & Compliance > Data Encryption Workshop**.


Step 3 In the navigation pane on the left, 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	Status of a Dedicated HSM instance: <ul style="list-style-type: none">• Installing After you pay the initial installation fee, the purchased instance will be installed. The status of the Dedicated HSM instance will be Installing.• To be activated The status of an instance that has been installed but not activated is To be activated.• Creating After you have activated an instance, the system will allocate the instance to you according to your configuration. The instance is in the status of Creating during this process.• Creation failed Due to insufficient resources or network faults, an instance may fail to be created. In this case, the instance will be in the status of Creation failed.• Running After an instance is configured and allocated, it will be in the status of Running.• Frozen If an instance is not renewed upon its expiration, its status changes to Frozen.
Service Edition	Platinum edition: You can exclusively use the HSM subrack, power supply, the network bandwidth, and API resources of the HSM.
AZ	AZ of a device
IP Address	Floating IP address of the Dedicated HSM instance
Expiration Time	Expiration time of the purchased HSM instance.

Step 5 You can select the name of a Dedicated HSM instance and click  to view details about the instance.

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

Parameter	Description
Status	Status of a Dedicated HSM instance: <ul style="list-style-type: none">• Installing After you pay the initial installation fee, the purchased instance will be installed. The status of the Dedicated HSM instance will be Installing.• To be activated The status of an instance that has been installed but not activated is To be activated.• Creating After you have activated an instance, the system will allocate the instance to you according to your configuration. The instance is in the status of Creating during this process.• Creation failed Due to insufficient resources or network faults, an instance may fail to be created. In this case, the instance will be in the status of Creation failed.• Running After an instance is configured and allocated, it will be in the status of Running.• Frozen If an instance is not renewed upon its expiration, its status changes to Frozen.
Service Edition	Platinum edition: You can exclusively use the HSM subrack, power supply, the network bandwidth, and API resources of the HSM.
HSM Type	HSM types of an instance, including Finance , Server , and Signature verification server .
VPC	VPC to which the instance belongs For more information about VPC, see <i>Virtual Private Cloud User Guide</i> .
Subnet	Subnet where the instance is located. For more information about subnets, see <i>Virtual Private Cloud User Guide</i> .
IP Address	Floating IP address of the Dedicated HSM instance
Security Group (SG)	Security group to which the instance belongs For more information about security groups, see <i>Virtual Private Cloud User Guide</i> .
Creation Time	Time when the instance is purchased
Expiration Time	Time when the instance expires

Parameter	Description
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, the Ukey used for initializing the Dedicated HSM instance will be sent to your email address. A Dedicated HSM service expert will also contact you and send related documents and software, including the tool used for managing Dedicated HSM instances, and the security agent and SDK used for service calls.

Prerequisites

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

Table 4-6 Required information

Item	Description	How to Obtain
Ukey	Stores the permission management information about the instance.	After the order is paid and the Dedicated HSM instance is configured, the Ukey will be sent to the recipient email address your provided.
Dedicated HSM instance management tool	Works with the UKey to remotely manage instances.	A service expert will also contact you and send related documents and software.
Dedicated HSM instance documents	<i>Dedicated HSM Instance User Manual</i> and <i>Dedicated HSM Instance Installation Guide</i>	
Security agent software	Establishes a secure connection with the instance.	
SDK	Provides APIs for Dedicated HSM. You can use the SDK to establish secure connections with instances.	

Item	Description	How to Obtain
Dedicated HSM instance management node (for example, an ECS)	Run the Dedicated HSM instance management tool, which is in the same VPC where the Dedicated HSM instance resides, and allocate elastic IP addresses for remote connections.	Purchase ECSs as needed. For details, see Purchasing an ECS .
Service application nodes (for example, ECSs)	Run the security agent software and users' service applications, which must be in the VPC where the Dedicated HSM instance is deployed.	


Initializing a Dedicated HSM Instance

NOTE

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

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

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

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

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



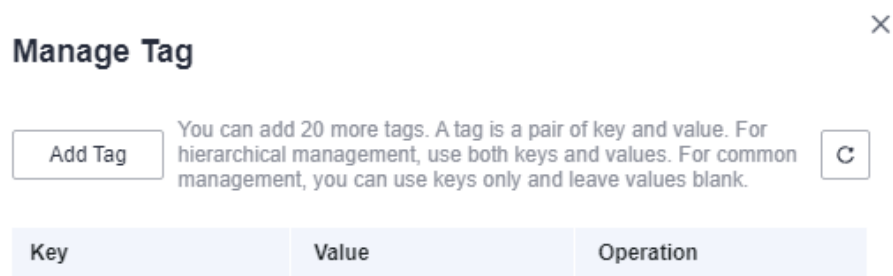
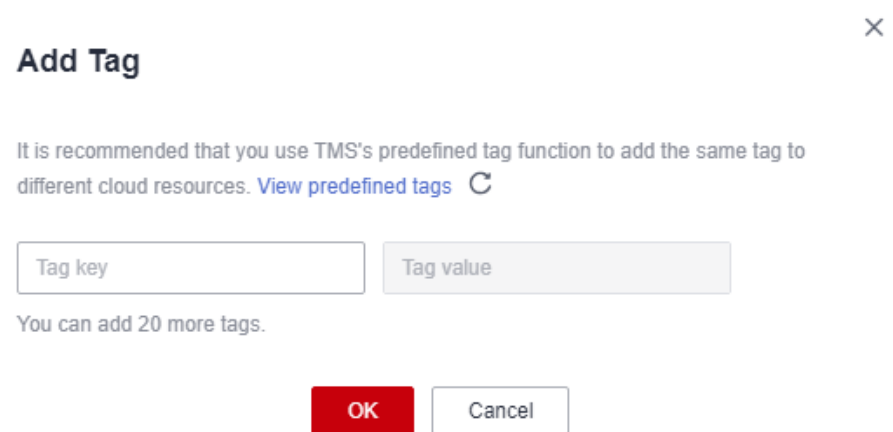
- Step 1** [Log in to the management console](#).
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click . Choose **Security & Compliance** > **Data Encryption Workshop**.
- Step 4** In the navigation pane on the left, choose **Dedicated HSM**.
- Step 5** In the **Operation** column of an instance, click **Manage Tag**. The **Manage Tag** page is displayed, as shown in [Figure 4-8](#).

Figure 4-8 Manage Tag



Step 6 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 4-9 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"> • Mandatory. • The tag key must be unique for the same custom key. • 128 characters limit. • The value cannot start or end with a space. • Cannot start with _sys_. • The following character types are allowed: <ul style="list-style-type: none"> - Chinese - English - Numbers - Space - Special characters: <code>._:/=+-@</code>
Tag value	Value of the tag	<ul style="list-style-type: none"> • Optional • 255 characters limit. • The following character types are allowed: <ul style="list-style-type: none"> - Chinese - English - Numbers - Space - Special characters: <code>._:/=+-@</code>

Step 7 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** [Log in to the management console.](#)
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click . Choose **Security & Compliance > Data Encryption Workshop.**
- Step 4** In the navigation pane on the left, choose **Dedicated HSM.**
- Step 5** Click the search box and select a tag as the filter attribute to search for Dedicated HSM instances, as shown in [Figure 4-10.](#)

Figure 4-10 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 exp.	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



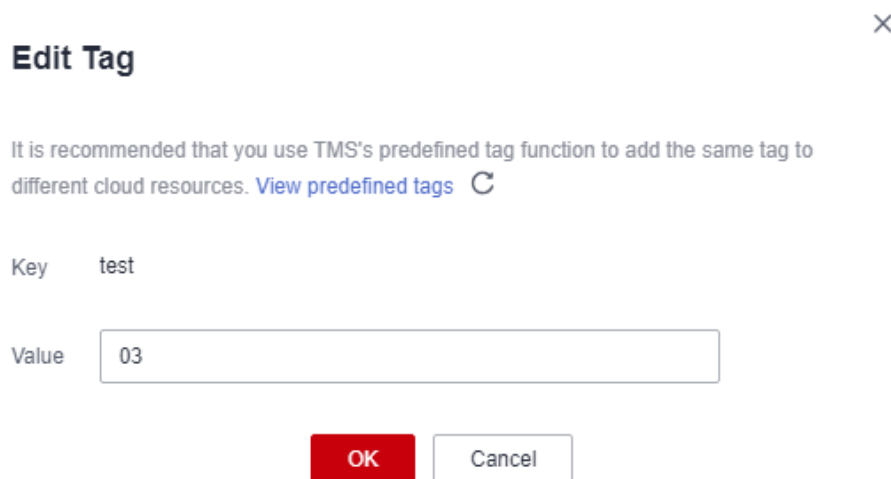
- Step 1** [Log in to the management console.](#)
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click . Choose **Security & Compliance > Data Encryption Workshop.**
- Step 4** In the navigation pane on the left, choose **Dedicated HSM.**
- Step 5** Click **Manage Tag** in the row where the target instance is located. The **Manage Tag** dialog box is displayed.
- Step 6** Click **Edit**. The **Edit Tag** dialog box is displayed. After changing the tag value, click **OK**.

Figure 4-11 Editing a tag



----End

4.5.4 Deleting a Tag

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

Procedure



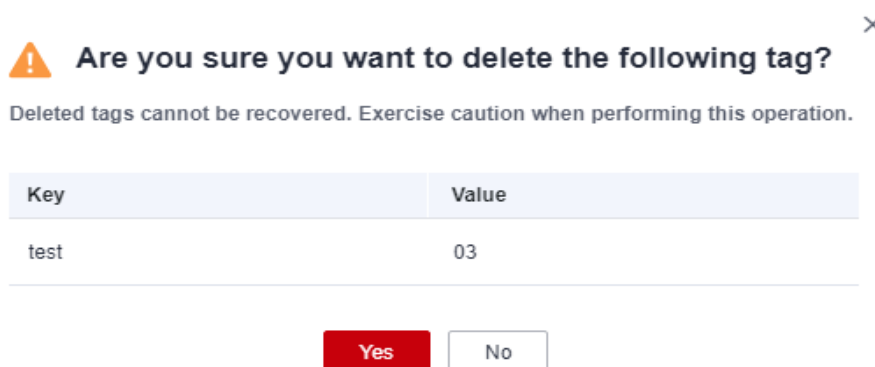
- Step 1** [Log in to the management console.](#)
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click . Choose **Security & Compliance > Data Encryption Workshop.**
- Step 4** In the navigation pane on the left, choose **Dedicated HSM.**
- Step 5** Click **Manage Tag** in the row where the target instance is located. The **Manage Tag** dialog box is displayed.
- Step 6** In the **Operation** column of a tag, click **Delete.**

Figure 4-12 Deleting a tag



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

----End

5 Tag Management

5.1 Overview

Scenario

Tags are the identifier of DEW. Adding tag allows you to easily recognize and manage your data encryption resources.

Tags can be added during or after resource creation.

Tag Naming Rules

- Each tag consists of a key-value pair.
- You can add at most 20 tags to a DEW resource.
- For each resource, a tag key must be unique and can have only one tag value.
- A tag consists of a tag key and a tag value. The naming rules are listed in [Table 5-1](#).
- Tags are key-value pairs, which are used to identify, classify, and search for vaults. Vault tags are used to filter and manage vaults only. A vault can have up to 10 tags.

NOTE

If you have configured tag policies for DEW, add tags for keys and secrets based on the policies. If the tag does not comply with the policies, keys and secrets may fail to be created. Contact the administrator to learn more about tag policies.

Table 5-1 Tag parameters

Parameter	Rules	Example
Tag key	<ul style="list-style-type: none"> ● This parameter is mandatory. ● The tag key must be unique for the same custom key. ● 128 characters limit. ● The value cannot start or end with a space. ● The value cannot start with _sys_. ● The following character types are allowed: <ul style="list-style-type: none"> - Chinese - English - Digits - Space - Special characters: _:=+@ 	cost
Tag value	<ul style="list-style-type: none"> ● This parameter can be left empty. ● 255 characters limit. ● The following character types are allowed: <ul style="list-style-type: none"> - Chinese - English - Digits - Space - Special characters: _:=+@ 	100

5.2 Creating a Tag Policy

Introduction

Tag policies are a type of policy that can help you standardize tags across resources in your organization's accounts. A tag policy is only applied to tagged resources and tags that are defined in that policy.

For example, a tag policy can specify that a tag attached to a resource must use the case treatment and tag values defined in the tag policy. If the case and value of the tag do not comply with the tag policy, the resource will be marked as non-compliant.

You can use tag policies as detective or preventive guardrails:

1. Detective guardrails: If a resource tag violates the tag policy, the resource will appear as noncompliant in the compliance result.
2. Preventive guardrails: If enforcement is enabled for a tag policy, non-compliant tagging operations will be prevented from being performed on specified resource types.

Constraints

Only organization administrators can create a tag policy.

NOTE

Before you create a tag policy and add it to the organization unit and account, a tag policy must be enabled by the administrator account. For details, see [Enabling or Disabling the Tag Policy Type](#).

Procedure


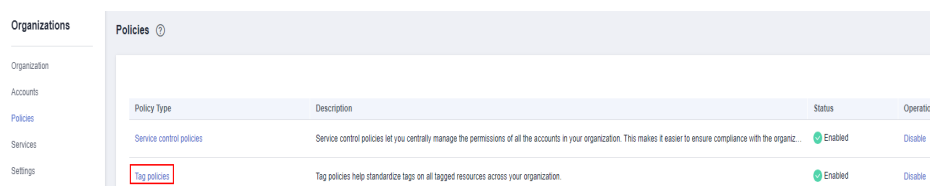
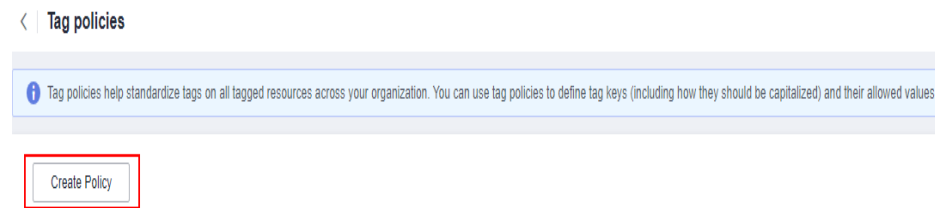
- Step 1** Log in to Huawei Cloud as the organization administrator or using the management account.
- Step 2** Click  on the left, choose **Management & Governance > Organizations**. The organization management page is displayed.
- Step 3** Click **Policies** on the left to go to the policy management page and click **Tag policies**.

Figure 5-1 Accessing the **Tag policies** page



- Step 4** Click **Create Policy**.

Figure 5-2 Creating a policy



- Step 5** Enter a policy name. Ensure that you are entering a unique policy name, different from any existing name.
- Step 6** Set a policy according to [Tag Policy Syntax](#). The system automatically verifies the syntax. If the syntax is incorrect, modify it as prompted.
- Step 7** (Optional) Add one or more tags to the policy. Enter a tag key and a tag value, and click **Add**.
- Step 8** Click **Save** in the lower right corner. If the tag policy is created successfully, it will be added to the list.

 **NOTE**

To update or delete a tag policy, see [Updating or Deleting a Tag Policy](#).

To attach or detach a tag policy, see [Attaching or Detaching a Tag Policy](#).

----End

5.3 Creating a Tag

This section describes how to add tags for existing keys, secrets, and Dedicated HSM instances.

Constraints

Tags cannot be added to default keys.

Key Management



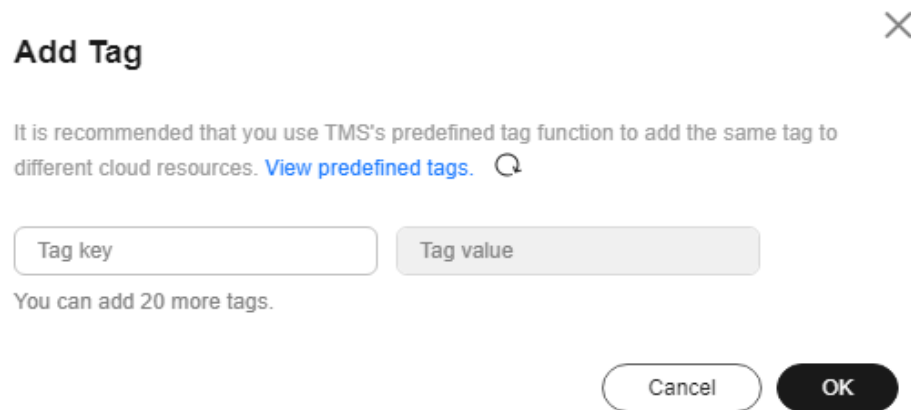
- Step 1** [Log in to the management console](#).
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** In the navigation on the left, choose  > **Security & Compliance** > **Data Encryption Workshop**.
- Step 4** Click the alias of the target custom key to view its details.
- Step 5** Click **Tags** to go to the tag management page.
- Step 6** Click **Add Tag**. In the displayed dialog box, set **Tag key** and **Tag value**, as shown in [Adding a tag](#).

Figure 5-3 Adding a tag



NOTE

To delete a tag, click **Delete** next to it.


- 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.


Step 7 Click **OK** to complete.

----End

CSMS

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.

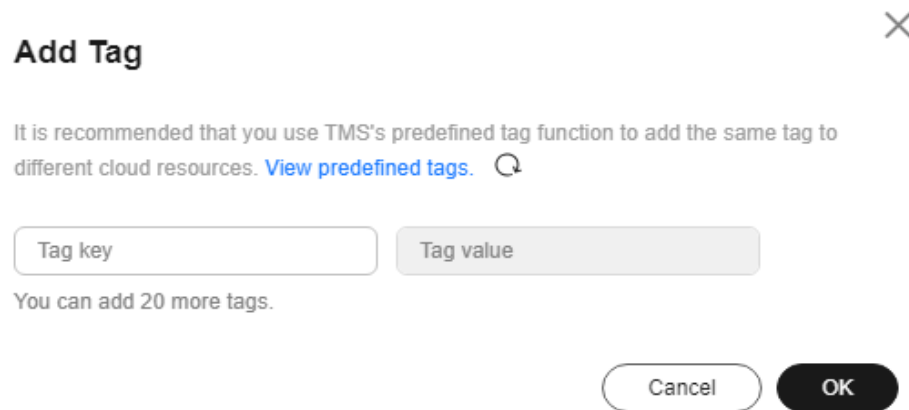
Step 3 In the navigation on the left, choose  > **Security & Compliance** > **Data Encryption Workshop**.

Step 4 In the navigation pane on the left, choose **Cloud Secret Management Service** > **Secrets**.

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

Step 6 In the **Tags** area, click **Add Tag**. In the displayed **Add Tag** dialog box, enter a **Tag key** and **Tag value**.

Figure 5-4 Adding a tag



Add Tag

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

Tag key Tag value

You can add 20 more tags.

Cancel OK


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.

Step 7 Click **OK**.

----End

Dedicated HSM

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 **Tag Management** in the **Operation** column.

Step 5 Click **Add Tag**. On the displayed dialog box, set **Tag key** and **Tag value**.

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.

Step 6 Click **OK**.

----End


5.4 Searching for a Custom Key by Tag

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

Prerequisites


Tags have been added.


Constraints

- At most 20 tags can be added for one search. If multiple tags are added, custom keys that meet all search criteria will be displayed.
- If you want to delete an added tag from the search criteria, click  next to the tag.

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 In the navigation on the left, choose  > **Security & Compliance** > **Data Encryption Workshop**.

Step 4 Click the search box and enter the tag key and tag value of the resource you want to search for. The custom keys that meet the search criteria are displayed.

NOTE

- At most 20 tags can be added for one search. If multiple tags are added, custom keys that meet all search criteria will be displayed.
- If you want to delete an added tag from the search criteria, click  next to the tag.


----End

5.5 Modifying a Tag Value

This section describes how to modify a created tag.

Procedure

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

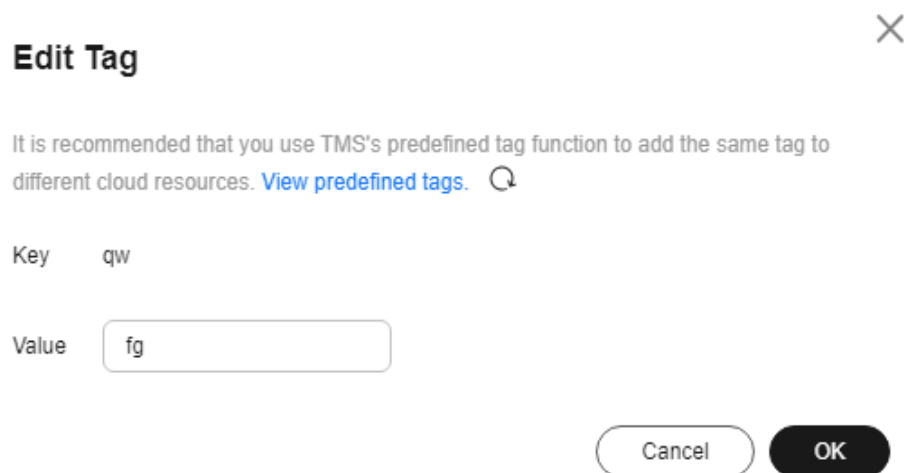
Step 2 Click  in the upper left corner of the management console and select a region or project.

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

Step 4 Choose the service from the left, click the instance whose tag need to be modified, and go to the details page.

Step 5 Select the corresponding tags, click **Edit**, and the **Edit Tag** box is displayed. After changing the tag value, click **OK**.

Figure 5-5 Editing a tag



-----End

5.6 Deleting a Tag

This section describes how to delete a created tag.

Procedure



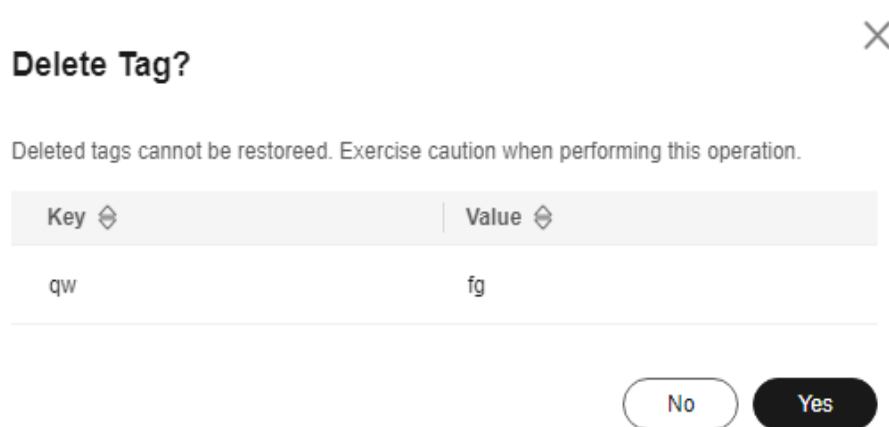
- Step 1** [Log in to the management console.](#)
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click . Choose **Security & Compliance > Data Encryption Workshop.**
- Step 4** Choose the service from the left, click the instance whose tag need to be deleted, and go to the details page.
- Step 5** In the **Operation** column of a tag, click **Delete.**

Figure 5-6 Delete a tag



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

----End

6 Auditing Logs

6.1 Operations supported by CTS

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

Table 6-1 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 6-2 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 6-3 KMS operations recorded by KPS

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

Table 6-4 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

6.2 Viewing CTS Traces in the Trace List

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 Object Storage Service (OBS) buckets. Cloud Trace Service (CTS) stores operation records (traces) generated in the last seven days.

NOTE

These operation records are retained for seven days on the CTS console and are automatically deleted upon expiration. Manual deletion is not supported.


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




- [Viewing Real-Time Traces in the Trace List of the New Edition](#)
- [Viewing Real-Time Traces in the Trace List of the Old Edition](#)

Constraints


- Traces of a single account can be viewed on the CTS console. Multi-account traces can be viewed only on the **Trace List** page of each account, or in the OBS bucket or the **CTS/system** log stream configured for the management tracker with the organization function enabled.
- You can only query operation records of the last seven days on the CTS console. To store operation records for longer than seven days, you must configure transfer to OBS or Log Tank Service (LTS) so that you can view them in OBS buckets or LTS log groups.
- After performing operations on the cloud, you can query management traces on the CTS console one minute later and query data traces five minutes later.
- Data traces are not displayed in the trace list of the new version. To view them, you need to go to the old version.

Viewing Real-Time Traces in the Trace List of the New Edition

1. Log in to the management console.
2. Click  in the upper left corner and choose **Management & Governance** **Management & Deployment** > **Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.
4. On the **Trace List** page, use advanced search to query traces. You can combine one or more filters.
 - **Trace Name:** Enter a trace name.
 - **Trace ID:** Enter a trace ID.
 - **Resource Name:** Enter a resource name. If the cloud resource involved in the trace does not have a resource name or the corresponding API

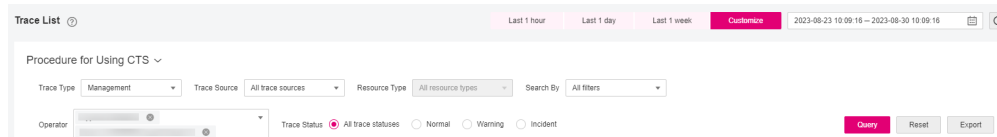
- operation does not involve the resource name parameter, leave this field empty.
- **Resource ID:** Enter a resource ID. Leave this field empty if the resource has no resource ID or if resource creation failed.
 - **Trace Source:** Select a cloud service name from the drop-down list.
 - **Resource Type:** Select a resource type from the drop-down list.
 - **Operator:** Select one or more operators from the drop-down list.
 - **Trace Status:** Select **normal**, **warning**, or **incident**.
 - **normal:** The operation succeeded.
 - **warning:** The operation failed.
 - **incident:** The operation caused a fault that is more serious than the operation failure, for example, causing other faults.
 - **Enterprise Project ID:** Enter an enterprise project ID.
 - **Access Key:** Enter a temporary or permanent access key ID.
 - **Time range:** Select **Last 1 hour**, **Last 1 day**, or **Last 1 week**, or specify a custom time range within the last seven days.
5. On the **Trace List** page, you can also export and refresh the trace list, and customize columns to display.
- Enter any keyword in the search box and press **Enter** to filter desired traces.
 - Click **Export** to export all traces in the query result as an .xlsx file. The file can contain up to 5,000 records.
 - Click  to view the latest information about traces.
 - Click  to customize the information to be displayed in the trace list. If **Auto wrapping** is enabled () , excess text will move down to the next line; otherwise, the text will be truncated. By default, this function is disabled.
6. For details about key fields in the trace structure, see [Trace Structure](#) section "Trace References" > "Trace Structure" and [Example Traces](#) section "Trace References" > "Example Traces".
7. (Optional) On the **Trace List** page of the new edition, click **Go to Old Edition** in the upper right corner to switch to the **Trace List** page of the old edition.

Viewing Real-Time Traces in the Trace List of the Old Edition

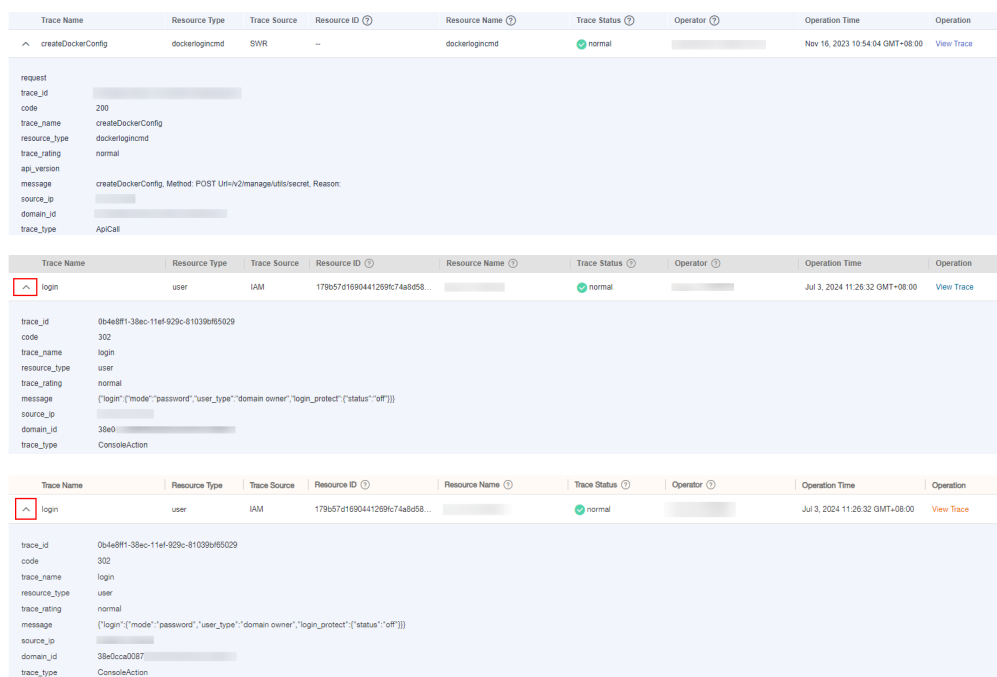
1. Log in to the management console.
2. Click  in the upper left corner and choose **Management & Governance** **Management & Deployment** > **Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.
4. Each time you log in to the CTS console, the new edition is displayed by default. Click **Go to Old Edition** in the upper right corner to switch to the trace list of the old edition.

- Set filters to search for your desired traces, as shown in **Figure 6-1**. The following filters are available.

Figure 6-1 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: Select **Last 1 hour, Last 1 day, or Last 1 week**, or specify a custom time range within the last seven days.
- Click **Query**.
 - 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 5,000 records.
 - Click to view the latest information about traces.
 - Click on the left of a trace to expand its details.



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

View Trace
×

```

{
  "request": "",
  "trace_id": " ",
  "code": "200",
  "trace_name": "createDockerConfig",
  "resource_type": "dockerlogincmd",
  "trace_rating": "normal",
  "api_version": "",
  "message": "createDockerConfig, Method: POST Url=/v2/manage/utis/secret, Reason:",
  "source_ip": " ",
  "domain_id": " ",
  "trace_type": "ApiCall",
  "service_type": "SWR",
  "event_type": "system",
  "project_id": " ",
  "response": "",
  "resource_id": "",
  "tracker_name": "system",
  "time": "Nov 16, 2023 10:54:04 GMT+08:00",
  "resource_name": "dockerlogincmd",
  "user": {
    "domain": {
      "name": " ",
      "id": " "
    }
  }
}

```

- For details about key fields in the trace structure, see [Trace Structure](#) section "Trace References" > "Trace Structure" and [Example Traces](#) section "Trace References" > "Example Traces" in the *CTS User Guide*.
- (Optional) On the **Trace List** page of the old edition, click **New Edition** in the upper right corner to switch to the **Trace List** page of the new edition.

7 Sharing

7.1 Overview

Based on Resource Access Manager (RAM), resource owners can configure the sharing permissions based on the least privilege principle and different usage requirements. Resource users can only access resources within their permissions, improving resource management security and user experience. For more information about RAM, see [What Is RAM?](#).

If your account is managed by Huawei Cloud organizations, you can enable this function to share resources more easily. If your account is in an organization, you can share resources with a specified account or all accounts in the organizations, needless to select all accounts one by one. For details, see [Enabling Sharing with Organizations](#).

Constraints

- You must own the KMS key resources. You cannot share the KMS key resources that have been shared with you.
- If you need to share KMS key resources with your organization, enable this function. For more information, see [Enabling Sharing with Organizations](#).

Key Owner and Recipient Permissions

Key owners can perform all operations on keys, while recipients can only perform certain operations. For details, see [Table 7-1](#).

Table 7-1 Operations supported for key recipients

Role	Allowed Operation	Description
Recipient	kms:cmk:get	Access through the console or API
	kms:cmk:createDataKey	Access through API only

Role	Allowed Operation	Description
	kms:cmk:createDataKeyWithoutPlaintext	Access through API only
	kms:cmk:encryptDataKey	Access through API only
	kms:cmk:decryptDataKey	Access through API only
	kms:cmk:encryptData	Access through the console or API
	kms:cmk:decryptData	Access through the console or API
	kms:cmk:sign	Access through API only
	kms:cmk:verify	Access through API only
	kms:cmk:generateMac	Access through API only
	kms:cmk:verifyMac	Access through API only
	kms:cmk:getPublicKey	Access through the console or API
	kms:cmk:getRotation	Access through the console or API
	kms:cmk:getTags	Access through the console or API

Supported Resource Types and Regions

The following table lists the resource types and regions can be shared in DEW.

Table 7-2 Supported resource types and regions in DEW

Cloud Service	Resource Type	Supported Region
KMS	CMK	CN North-Beijing1 CN North-Beijing4 CN East-Shanghai1 CN East-Shanghai2 CN South-Shenzhen CN Southwest-Guiyang1 CN South-Guangzhou

Billing

For details about KMS billing, see .

Owners of shared keys need to pay for the key instance and API calling fees, that is, only the resource owner will be charged for shared resources.

7.2 Shared KMS


Scenario

To share your KMS resources with other accounts, create a resource share first. During the creation, you need to specify resources to be shared, configure permissions, specify users to be shared with, and confirm the configuration.

You can use shared KMS to encrypt the secrets and key pairs in DEW, and create an encryption task for instances in Relational Database Service (RDS), Document Database Service (DDS), and Object Storage Service (OBS).

Creating Shared KMS Resources

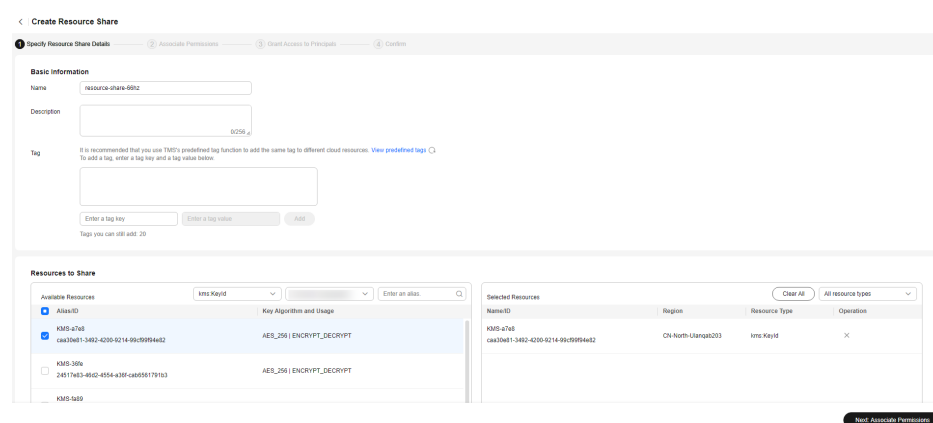
Step 1 [Log in to the management console.](#)

Step 2 Click  in the upper left corner and choose **Management & Governance Resource Access Manager** .

Step 3 In the navigation pane on the left, choose **Shared by Me > Resource Shares**.

Step 4 Click **Create Resource Share** in the upper right corner.

Figure 7-1 Specifying shared resources



Step 5 Set resource type to **kms:KeyId**, choose the corresponding region, and select keys to be shared. Click **Next: Associate Permissions**.

Step 6 Associate a RAM managed permission with each resource type on the displayed page. Then, click **Next: Specify Principals** in the lower right corner.

Step 7 Specify the target principals and click **Next: Confirm** in the lower right corner.

Table 7-3 Parameters

Parameter	Description
Principal Type	<ul style="list-style-type: none"> Organization For details about how to create an organization, see . <p>NOTE If you have not enabled resource sharing with organizations, this parameter cannot be set to Organization. For details, see .</p> <ul style="list-style-type: none"> Huawei Cloud account ID

Step 8 Check the configurations and click **Submit** in the lower right corner.


 **NOTE**


After a shared instance is created, the organization accepts the instance automatically, while Huawei cloud accounts need to perform certain operations. For details, see .

----End

Viewing Shared KMS Resources

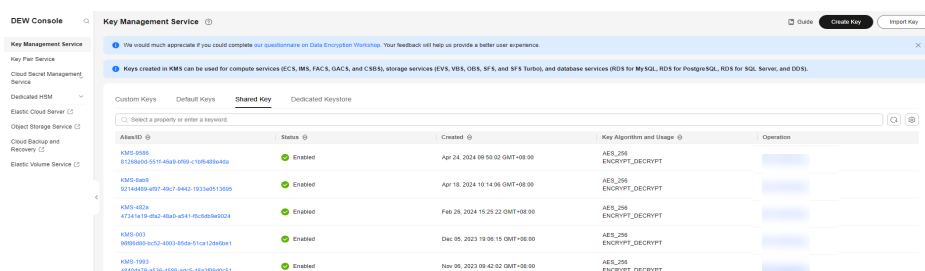
Step 1 [Log in to the management console.](#)

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

Step 3 In the navigation on the left, choose  > **Security & Compliance** > **Data Encryption Workshop**.

Step 4 Check the shared key resources in the **Shared Key** tab.

Figure 7-2 Shared keys




 **NOTE**


In the **Shared Key** tab, you can choose a scenario by entering the copied KMS encryption key ID.

----End

Using Shared KMS Resources

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

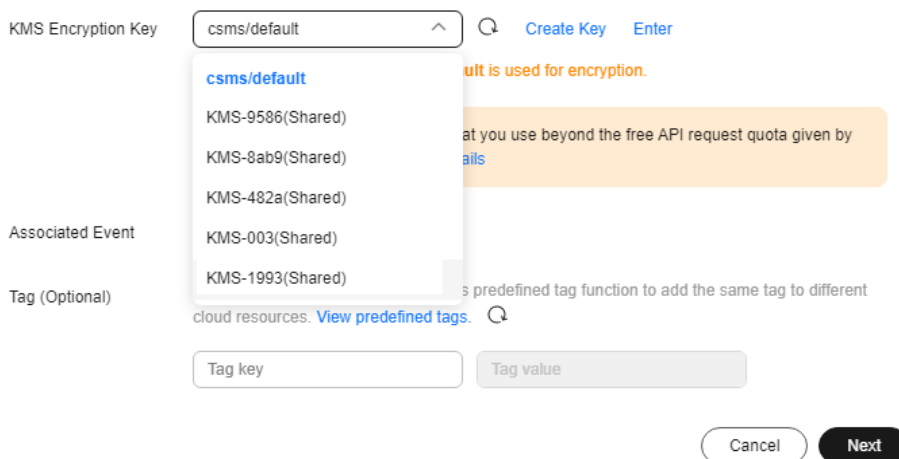
Step 2 Click  in the upper left corner of the management console and select a region or project.

Step 3 In the navigation on the left, choose  > **Security & Compliance** > **Data Encryption Workshop.**

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

Step 5 Click **Create Secret.** On the displayed page, select or enter a shared key for **KMS Encryption Key.**

Figure 7-3 Selecting a shared key



NOTE

- When creating a key pair, you can select shared KMS keys.
- When creating an RDS, DDS, or OBS instance, you can choose shared KMS keys. For details, see .

-----End

7.3 Activating a Dedicated HSM Instance Using a Shared VPC

Scenario

After a Dedicated HSM instance is created, you need to activate it before using it. To do so, you need to bind it to a VPC. You can apply for a VPC or use a shared VPC.

Creating Shared VPC Resources


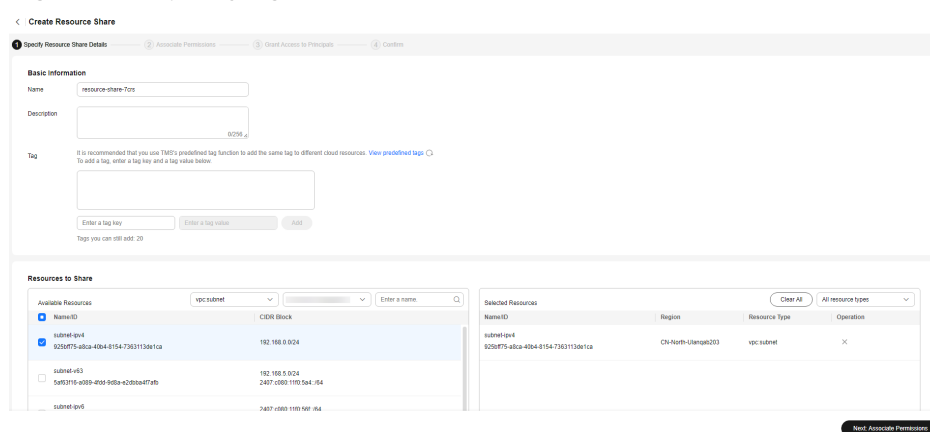
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner, choose **Management & Governance > Resource Access Manager**.
- Step 3** In the navigation pane on the left, choose **Shared by Me > Resource Shares**.
- Step 4** Click **Create Resource Share** in the upper right corner.

Figure 7-4 Specifying shared resources



- Step 5** Set resource type to **vpc:subnet**, choose the corresponding region, and select the VPC to be shared. Click **Next: Associate Permissions**.
- Step 6** Associate a RAM managed permission with each resource type on the displayed page. Then, click **Next: Specify Principals** in the lower right corner.
- Step 7** Specify the target principals and click **Next: Confirm** in the lower right corner.

Table 7-4 Parameters

Parameter	Description
Principal Type	<ul style="list-style-type: none"> ● Organization For details about how to create an organization, see . NOTE If you have not enabled resource sharing with organizations, this parameter cannot be set to Organization. For details, see . ● Huawei Cloud account ID

- Step 8** Check the configurations and click **Submit** in the lower right corner.

----End

Using Shared VPC Resources



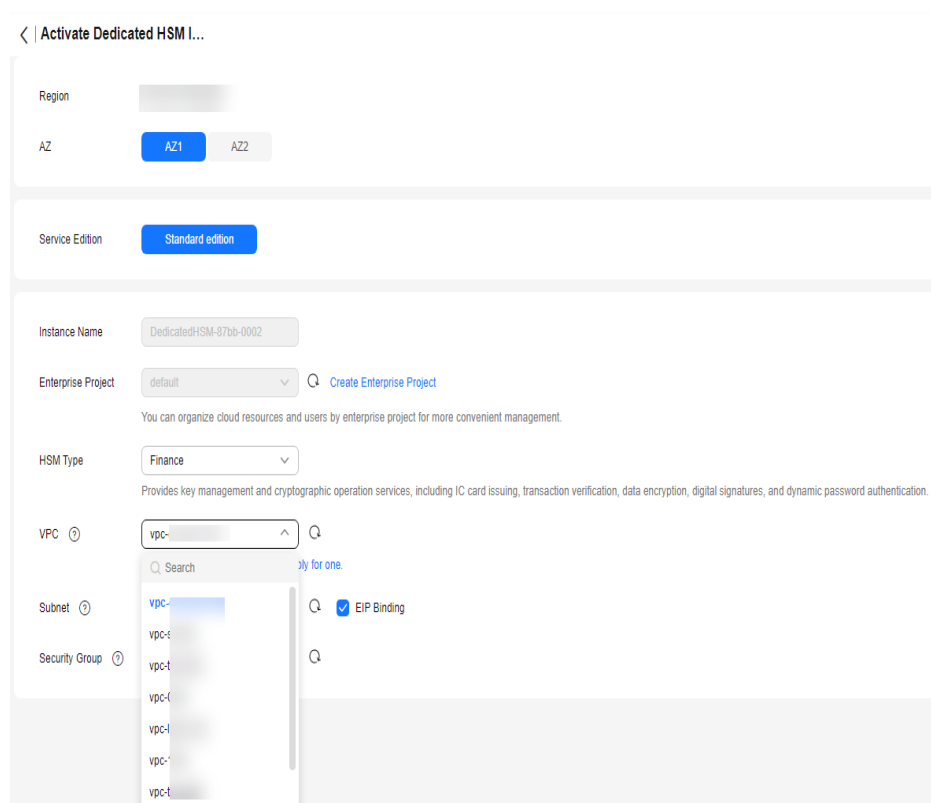
- Step 1** [Log in to the management console](#).
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** In the navigation on the left, choose  > **Security & Compliance** > **Data Encryption Workshop**.
- Step 4** In the navigation pane on the left, choose **Dedicated HSM** > **Instances**.
- Step 5** Locate the target Dedicated HSM, click **Activate** in the **Operation** column.
- Step 6** In the **VPC** drop-down list, choose a shared VPC instance, configure the parameters, and click **Activate**.

Figure 7-5 Selecting a shared VPC




----End

7.4 Updating a Resource Share

You can update a resource share at any time, including updating its name, description, tags, shared resources, RAM managed permissions, and principals.


Procedure

- Step 1** [Log in to the management console.](#)
 - Step 2** Click  in the upper left corner and choose **Management & Governance Resource Access Manager**.
 - Step 3** In the navigation pane on the left, choose **Shared by Me > Resource Shares**.
 - Step 4** Select the resource share to be updated and click **Edit** in the **Operation** column.
 - Step 5** Update the resource share on the displayed page. You can modify its name, description, tags, and add or delete shared resources.
 - Step 6** After the update is complete, click **Next: Associate Permissions** in the lower right corner.
 - Step 7** Add or delete the permissions supported by **kms:KeyId**. Wait until the update is complete, click **Next: Grant Access to Principals**.
 - Step 8** On the displayed page, add or delete principals based on your needs. Then, click **Next: Confirm** in the lower right corner.
 - Step 9** Confirm the configurations and click **OK** in the lower right corner.
- End

7.5 Leaving a Resource Share

If you no longer need to access shared key resources, you can leave at any time. After leaving the share, you cannot access the shared keys.

Procedure

- Step 1** [Log in to the management console.](#)
 - Step 2** Click  in the upper left corner and choose **Management & Governance Resource Access Manager**.
 - Step 3** In the navigation pane on the left, choose **Shared with Me > Resource Shares**.
 - Step 4** In the **Accepted Resource Shares** tab, locate the target instance, and click **Leave** in the **Operation** column.
 - Step 5** Click **Leave** in the displayed dialog box.
- End

8 Permission Control

8.1 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 8-1](#)).

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 8-1 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 8-2 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 8-3 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 8-4 describes the common operations supported by each system-defined permission of DEW. Select the permissions as needed.

Table 8-4 Common operations supported by each system-defined policy or role

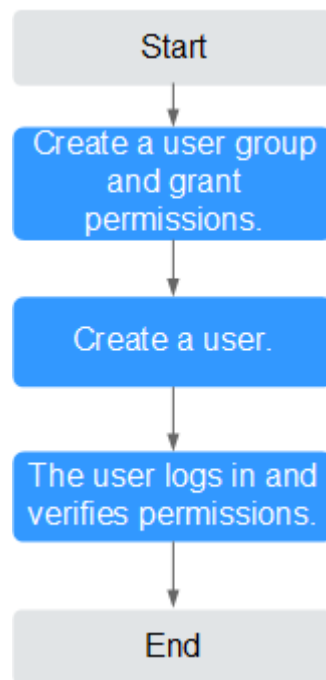
Operation	KMS Administrator	KMS CMKFullAccess	DEW KeypairFullAccess	DEW KeypairReadOnlyAccess
Creating a key	√	√	x	x
Enable a key	√	√	x	x
Disable a key	√	√	x	x
Schedule key deletion	√	√	x	x
Cancel scheduled key deletion	√	√	x	x
Modify a key alias	√	√	x	x
Modify key description	√	√	x	x
Generate a random 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 8-1 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.

Tenant Guest Roles

If you have configured **Tenant Guest** permissions for the IAM account, apart from the read-only permissions for all cloud services except Identity and Access Management (IAM), you also have the following KMS permissions:

- **kms:cmk:create**: Create a key.
- **kms:cmk:createDataKey**: Create a DEK.
- **kms:cmk:createDataKeyWithoutPlaintext**: Create a plaintext-free DEK.

- **kms:cmk:encryptDataKey**: Encrypt the DEK.
- **kms:cmk:decryptDataKey**: Decrypt a DEK.
- **kms:cmk:retireGrant**: Retire a grant.
- **kms:cmk:decryptData**: Decrypt data.
- **kms:cmk:encryptData**: Encrypt data.
- **kms::generateRandom**: Generate a random number.

If you want to configure the Tenant Guest role for an IAM user but do not want to have the preceding permissions, you need to configure a custom deny policy for the IAM user. For details about how to configure a custom policy, see [Creating a Custom DEW Policy](#).

8.2 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"
      ]
    }
  ]
}
```