Data Encryption Workshop

User Guide

Issue	33
Date	2023-06-30

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

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

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

Contents

1 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	AES_256	AES symmetric key	Encrypts and decrypts a small amount of data or data keys.
Symmetric key	AES	● HMAC_256 ● HMAC_384 ● HMAC_512	HMAC symmetric key	Generates and verifies a message authentication code

Key Type	Algorithm Type	Key Specifications	Description	Usage
Symmetric key	SM3	HMAC_SM3	SM3 symmetric key	Generates and verifies a message authentication code
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

1.2 Creating a Key

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

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

Prerequisites

The account has KMS CMKFullAccess or higher permissions.

Constraints

- You can create up to 20 custom keys, excluding default keys.
- Symmetric keys are created using the AES key. The AES-256 key can be used to encrypt and decrypt a small amount of data or data keys. The HMAC key is used to generate and verify message authentication codes.
- Asymmetric keys are created using RSA or ECC algorithms. RSA keys can be used for encryption, decryption, digital signature, and signature verification. ECC keys can be used only for digital signature and signature verification.
- Aliases of default keys end with **/default**. When choosing aliases for your custom keys, do not use aliases ending with **/default**.
- DEW keys can be called through APIs for 20,000 times free of charge.

Scenarios

- **Encrypt data in OBS**
- **Encrypt data in EVS**
- **Encrypt data in IMS**

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

Creating a Key

Step 1 Log in to the management console.

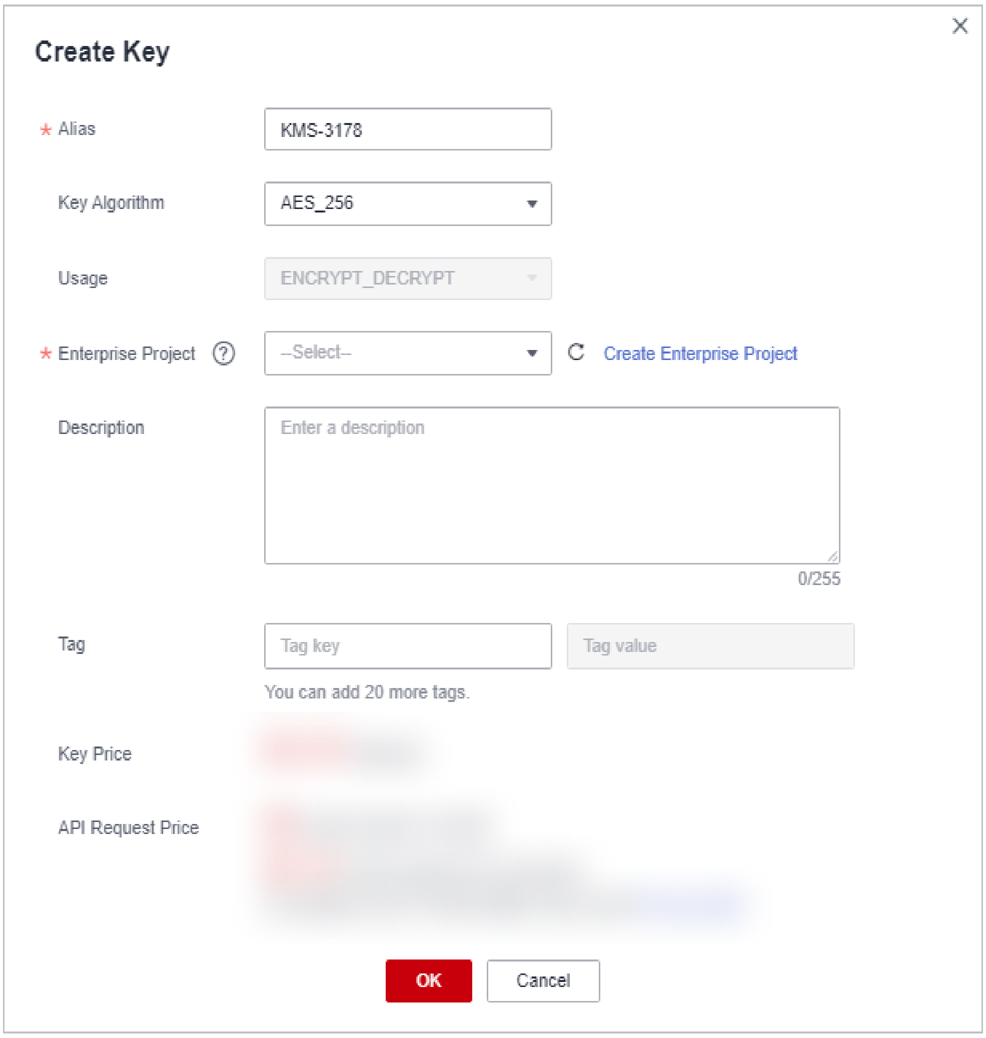
Step 2 Click 📍 in the upper left corner of the management console and select a region or project.

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

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

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

Figure 1-1 Creating a key



Create Key

* Alias: KMS-3178

Key Algorithm: AES_256

Usage: ENCRYPT_DECRYPT

* Enterprise Project: --Select--

Description: Enter a description

0/255

Tag: Tag key | Tag value

You can add 20 more tags.

Key Price

API Request Price

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

  NOTE

  – You can enter digits, letters, underscores (_), hyphens (-), colons (:), and slashes (/).

  – You can enter up to 255 characters.

- **Key Algorithm**: Select a key algorithm. For more information, see **Table 1-2**.

Table 1-2 Key algorithms supported by KMS

Key Type	Algorithm Type	Key Specifications	Description	Usage
Symmetric key	AES	AES_256	AES symmetric key	Encrypts and decrypts a small amount of data or data keys.
Symmetric key	AES	– HMAC_256 – HMAC_384 – HMAC_512	HMAC symmetric key	Generates and verifies a message authentication code
Symmetric key	SM3	HMAC_SM3	SM3 symmetric key	Generates and verifies a message authentication code
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

- **Usage**: Select **SIGN_VERIFY**, **ENCRYPT_DECRYPT**, or **GENERATE_VERIFY_MAC**.
  - For an AES_256 symmetric key, the default value is **ENCRYPT_DECRYPT**.
  - For an HMAC symmetric key, the default value is **GENERATE_VERIFY_MAC**.

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

  NOTE

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

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

  If you are an enterprise user and have created an enterprise project, select the required enterprise project from the drop-down list. The default project is **default**.

  If there are no **Enterprise Management** options displayed, you do not need to configure it.

  NOTE

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

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

NOTE

- After creating a CMK, you can click the alias of the CMK to go to the CMK details page and add a tag to the CMK.
- The same tag (including tag key and tag value) can be used for different custom keys. However, under the same custom key, one tag key can have only one tag value.
- A maximum of 20 tags can be added for one custom key.
- If you want to delete a tag from the tag list when adding multiple tags, you can click **Delete** in the row where the tag to be added is located to delete the tag.

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

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

----End

Related Operations

- For details about how to upload objects with server-side encryption, see section "Uploading a File with Server-Side Encryption" in the *Object Storage Service Console Operation Guide*.
- For details about how to encrypt data on EVS disks, see section **Purchasing an EVS Disk** in the *Elastic Volume Service User Guide*.
- For details about how to encrypt private images, see section "Encrypting an Image" in the *Image Management Service User Guide*.
- For details about how to encrypt disks for a database instance in RDS, see section "Purchasing an Instance" in the *Relational Database Service User Guide*.

- For details about how to create a DEK and a plaintext-free DEK, see sections "Creating a DEK" and "Creating a Plaintext-Free DEK" in the *Data Encryption Workshop API Reference*.
- For details about how to encrypt and decrypt a DEK for a user application, see sections "Encrypting a DEK" and "Decrypting a DEK" in the *Data Encryption Workshop API Conference*.

1.3 Creating CMKs Using Imported Key Materials

1.3.1 Overview

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

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

Important Notes

- Security

  You need to ensure that random sources meet your security requirements when using them to generate key materials. When using the import key function, you need to be responsible for the security of your key materials. Save the original backup of the key material so that the backup key material can be imported to the KMS in time when the key material is deleted accidentally.

- Availability and Durability

  Before importing the key material into KMS, you need to ensure the availability and durability of the key material.

  Differences between the imported key material and the key material generated by KMS are shown in **Table 1-3**.

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

Key Material Source	Difference
Imported keys	- 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. **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.
Keys created in KMS	- 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.

Procedure

Step 1 **Log in to the management console**.

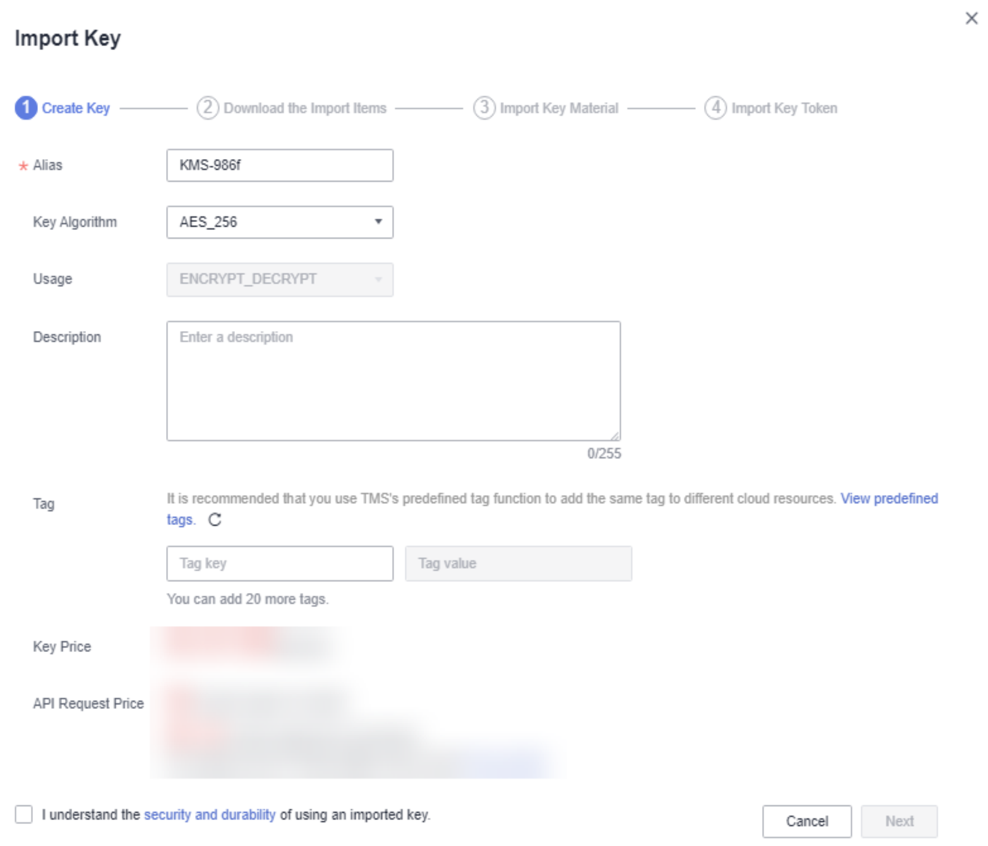
Step 2 Click in the upper left corner of the management console and select a region or project.

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

Step 4 Click **Import Key**. The **Import Key** dialog box is displayed.

Step 5 Configure key parameters.

Figure 1-2 Creating an empty key



Import Key

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

* Alias: KMS-986f

Key Algorithm: AES_256

Usage: ENCRYPT_DECRYPT

Description: Enter a description

0/255

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.

Key Price

API Request Price

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

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

  NOTE

  - You can enter digits, letters, underscores (_), hyphens (-), colons (:), and slashes (/).
  - You can enter up to 255 characters.

- **Key Algorithm**: Select a key algorithm. For more information, see **Table 1-4**.

Table 1-4 Key algorithms supported by KMS

Key Type	Algorithm Type	Key Specifications	Description	Usage
Symmetric key	AES	AES_256	AES symmetric key	Encrypts and decrypts a small amount of data or data keys.
Symmetric key	AES	– HMAC_256 – HMAC_384 – HMAC_512	HMAC symmetric key	Generates and verifies a message authentication code
Symmetric key	SM3	HMAC_SM3	SM3 symmetric key	Generates and verifies a message authentication code
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

- **Usage**: Select **SIGN_VERIFY**, **ENCRYPT_DECRYPT**, or **GENERATE_VERIFY_MAC**.
  - For an AES_256 symmetric key, the default value is **ENCRYPT_DECRYPT**.
  - For an HMAC symmetric key, the default value is **GENERATE_VERIFY_MAC**.
  - For RSA asymmetric keys, select **ENCRYPT_DECRYPT** or **SIGN_VERIFY**. The default value is **SIGN_VERIFY**.
  - For an ECC asymmetric key, the default value is **SIGN_VERIFY**.

NOTE

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

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

  If you are an enterprise user and have created an enterprise project, select the required enterprise project from the drop-down list. The default project is **default**.

  If there are no **Enterprise Management** options displayed, you do not need to configure it.

  NOTE

  – You can use enterprise projects to manage cloud resources and project members. For more information about enterprise projects, see **What Is Enterprise Project Management Service?**

  – For details about how to enable the enterprise project function, see **Enabling the Enterprise Center**.

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

NOTE

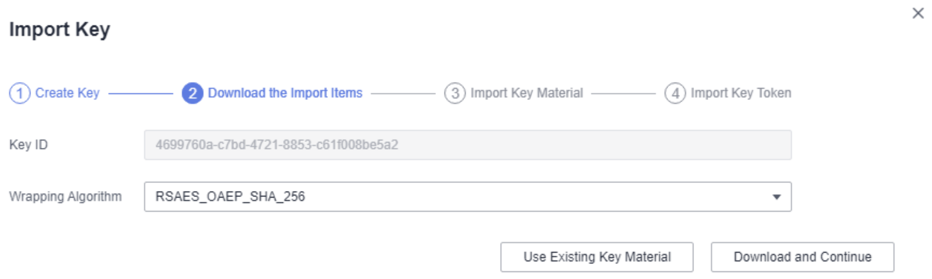
- If a custom key has been created without any tag, you can add a tag to the custom key later as necessary. Click the alias of the custom key, click the **Tags** tab, and click **Add Tag**.
- The same tag (including tag key and tag value) can be used for different custom keys. However, under the same custom key, one tag key can have only one tag value.
- A maximum of 20 tags can be added for one custom key.
- If you want to delete a tag from the tag list when adding multiple tags, you can click **Delete** in the row where the tag to be added is located to delete the tag.

Step 7 Click **security and durability** to understand the security and durability of the imported key.

Step 8 Select **I understand the security and durability of using an imported key**, and create a custom key whose key material is empty.

Step 9 Click **Next** to go to the **Download the Import Items** step. Select a key wrapping algorithm based on **Table 1-5**.

Figure 1-3 Obtaining the wrapping key and import token



Key ID: 4699760a-c7bd-4721-8853-c61f008be5a2

Wrapping Algorithm: RSAES_OAEP_SHA_256

Table 1-5 Key wrapping algorithms

Algorithm	Description	Configuration
RSAES_OAEP_SHA_256	RSA algorithm that uses OAEP and has the **SHA-256** hash function	Select an algorithm based on your HSM functions. 1. If the HSMs support the **RSAES_OAEP_SHA_256** algorithm, use **RSAES_OAEP_SHA_256** to encrypt key materials. 2. If the HSMs do not support **OAEP**, use **RSAES_PKCS1_V1_5** to encrypt key materials. **NOTICE** The **RSAES_OAEP_SHA_1** algorithm is no longer secure. Exercise caution when performing this operation.
RSAES_OAEP_SHA_1	RSA algorithm that uses Optimal Asymmetric Encryption Padding (OAEP) and has the **SHA-1** hash function	

NOTE

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

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

1. Obtain the wrapping key and import token.
   - Method 1: Click **Download and Continue**. The downloaded file is the wrapping key.

     Figure 1-4 Downloaded file

     wrappingKey_ffe[redacted]a7-a29927851940.bin

     ▪ **wrappingKey_***KeyID* is the wrapping key. It is encoded in binary format and used to encrypt the wrapping key of the key material.

     ▪ Import token: You do not need to download it. The import wizard automatically transfers the import token. If you close the wizard before completing the import, the token will automatically become invalid.

NOTICE

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

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

– Method 2: Obtain the wrapping key and import token by calling APIs.

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

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

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

  The following example describes how to obtain the wrapping key and import token of a CMK (ID: **43f1ffd7-18fb-4568-9575-602e009b7ee8**; algorithm: **RSAES_OAEP_SHA_256**).

  ○ Example request

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

  ○ Example response

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

ii. Save the wrapping key and convert its format. Only the key material encrypted using the converted wrapping key can be imported to the management console.

  1) Copy the content of the wrapping key **public_key**, paste it to a .txt file, and save the file as **PublicKey.b64**.

  2) Use OpenSSL to run the following command to perform Base-64 coding on the content of the **PublicKey.b64** file to generate binary data, and save the converted file as **PublicKey.bin**:

  openssl enc -d -base64 -A -in PublicKey.b64 -out PublicKey.bin

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

2. Use the wrapping key to encrypt the key material.

NOTE

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

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

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

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

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

NOTE

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

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

- If the AES256 symmetric key algorithm is used, run the following command on the client where the OpenSSL tool has been installed:

  openssl rand -out *PlaintextKeyMaterial.bin* 32

- If the RSA and ECC asymmetric key algorithms are used, run the following command on the client where the OpenSSL tool has been installed:

  1) Generate a hexadecimal AES256 key.

     openssl rand -out 0xPlaintextKeyMaterial.bin -hex 32

  2) Convert the hexadecimal AES256 key to the binary format.

     cat 0xPlaintextKeyMaterial.bin | xxd -r -ps > PlaintextKeyMaterial.bin

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

If the wrapping key was downloaded from the console, replace ***PublicKey.bin*** in the following command with the wrapping key name *wrappingKey_keyID*.

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

Wrapping Key Algorithm	Key Material Encryption
RSAES_OAEP_SHA_256	**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**

Wrapping Key Algorithm	Key Material Encryption
RSAES_OAEP_SHA_1	**openssl pkeyutl** **-in** ***PlaintextKeyMaterial.bin*** **-inkey** ***PublicKey.bin*** **-out** ***EncryptedKeyMaterial.bin*** **-keyform der** **-pubin -encrypt** **-pkeyopt rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha1**

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

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

  1) Generate a private key.

     openssl genrsa -out pkcs1_rsa_private_key.pem 4096

  2) Convert the format to PKCS8.

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

  3) Convert the PKCS8 format to the DER format.

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

  4) Use a temporary key material to encrypt the private key.

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

     NOTE

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

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

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

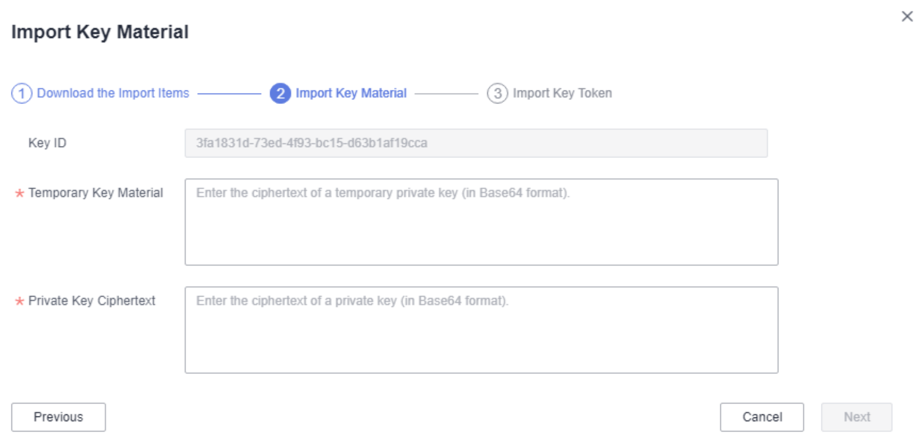
Parameter	Description
Key ID	Random ID of a CMK generated during the CMK creation

Parameter	Description
Key material	Import a key material. For example, use the **EncryptedKeyMaterial.bin** file in **Step 10.2.b**.

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

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

Figure 1-5 Importing key materials



Key ID: 3fa1831d-73ed-4f93-bc15-d63b1af19cca

* Temporary Key Material: Enter the ciphertext of a temporary private key (in Base64 format).

* Private Key Ciphertext: Enter the ciphertext of a private key (in Base64 format).

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

Table 1-9 Parameters for importing a key token

Parameter	Description
Key ID	Random ID of a CMK generated during the CMK creation
Key import token	Select the import token obtained via API in **12.b**.

Parameter	Description
Key material expiration mode	● **Key material will never expire**: You use this option to specify that key materials will not expire after import. ● **Key material will expire**: You use this option to specify the expiration time of the key materials. By default, key materials expire in 24 hours after import. After the key material expires, the system automatically deletes the key material within 24 hours. Once the key material is deleted, the key cannot be used and its status changes to **Pending import**.

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

NOTICE

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

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

----End

1.3.3 Deleting Key Materials

When importing key materials, you can specify their expiration time. After the key material expires, KMS deletes it, and the status of 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.

Prerequisites

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

Constraints

- To re-import a deleted key material, ensure the imported material is the same as the deleted one.
- Data encrypted using a CMK cannot be decrypted if the key material of the custom key was deleted. To decrypt the data, re-import the key material.
- After the deletion, the CMK will become unavailable and its status will change to **Pending import**.

- The key materials of asymmetric keys cannot be directly deleted. To delete them, perform the instructions in **Deleting One or More CMKs**.

Procedure

Step 1 **Log in to the management console**.

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

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

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

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

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

----End

1.4 Managing CMKs

1.4.1 Viewing a CMK

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

Procedure

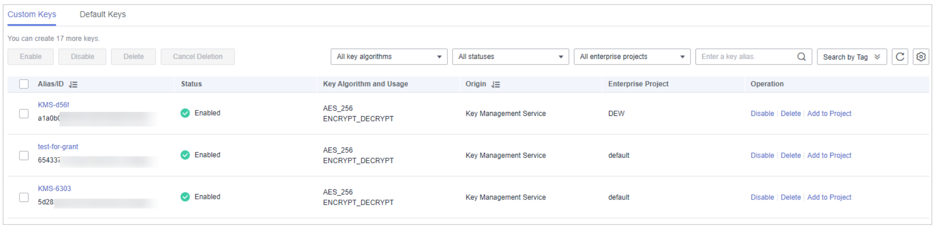
Step 1 **Log in to the management console**.

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

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

Step 4 Check the key list. **Table 1-10** describes the parameters.

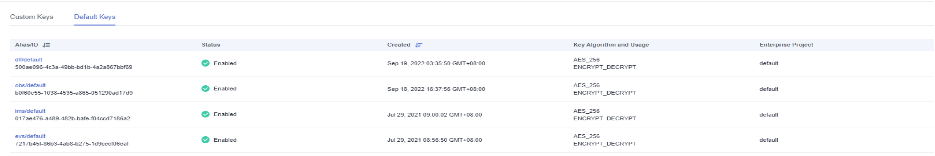
Figure 1-6 Custom keys



You can create 17 more keys.

	Alias/ID	Status	Key Algorithm and Usage	Origin	Enterprise Project	Operation
□	KMS-d56f a1a0b[redacted]	Enabled	AES_256 ENCRYPT_DECRYPT	Key Management Service	DEW	Disable | Delete | Add to Project
□	test-for-grant 654337[redacted]	Enabled	AES_256 ENCRYPT_DECRYPT	Key Management Service	default	Disable | Delete | Add to Project
□	KMS-6303 5d28[redacted]	Enabled	AES_256 ENCRYPT_DECRYPT	Key Management Service	default	Disable | Delete | Add to Project

Figure 1-7 Default keys



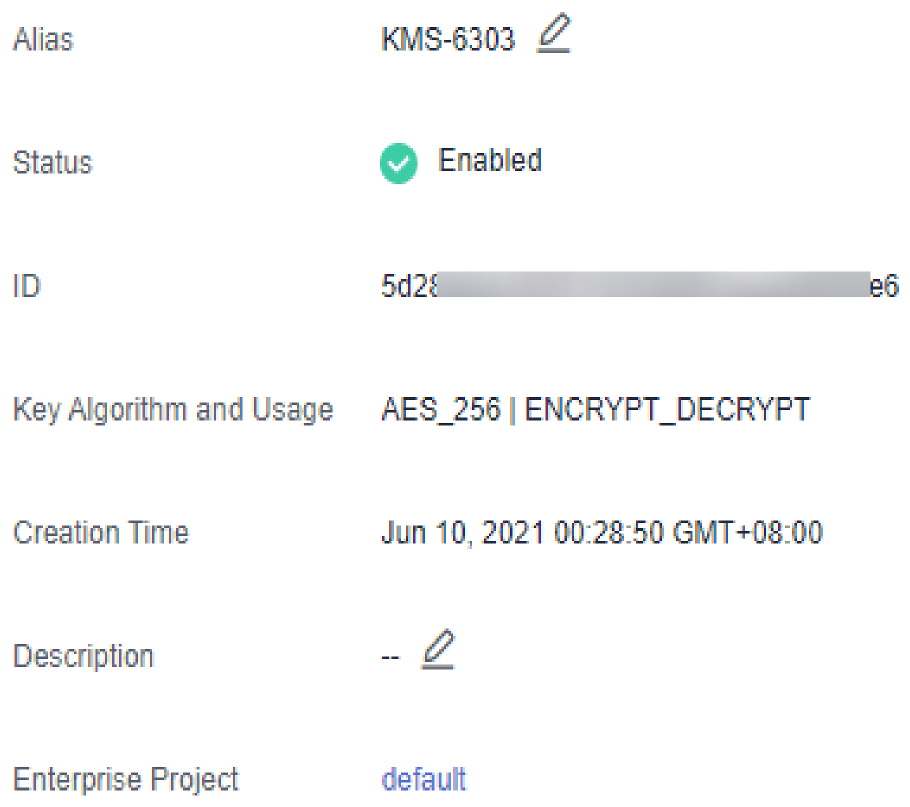
Alias/ID	Status	Created	Key Algorithm and Usage	Enterprise Project
dlf/default 500ae096-4c3a-49bb-bd1b-4a2a867bbf69	Enabled	Sep 19, 2022 03:35:50 GMT+08:00	AES_256 ENCRYPT_DECRYPT	default
obs/default b0f60e55-1038-4535-a865-051290ad17d9	Enabled	Sep 18, 2022 16:37:56 GMT+08:00	AES_256 ENCRYPT_DECRYPT	default
ims/default 017ae476-a489-482b-bafe-f04ccd7186a2	Enabled	Jul 29, 2021 09:00:02 GMT+08:00	AES_256 ENCRYPT_DECRYPT	default
evs/default 7217b45f-86b3-4ab8-b275-1d9cecf06eaf	Enabled	Jul 29, 2021 08:56:50 GMT+08:00	AES_256 ENCRYPT_DECRYPT	default

Table 1-10 Key list parameters

Parameter	Description
Alias/ID	Alias 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: ● **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**.
Creation Time	Creation time of the CMK
Key Algorithm and Usage	Key algorithm selected during key creation and its usage
Enterprise Project	Enterprise project the CMK is used for

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

Figure 1-8 CMK details



Alias	KMS-6303 ✎
Status	✓ Enabled
ID	5d2[redacted]e6
Key Algorithm and Usage	AES_256 | ENCRYPT_DECRYPT
Creation Time	Jun 10, 2021 00:28:50 GMT+08:00
Description	-- ✎
Enterprise Project	default

NOTE

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

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

----End

1.4.2 Enabling One or More CMKs

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

Prerequisites

The custom key you want to enable is in **Disabled** status.

Procedure

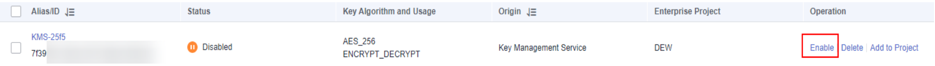
Step 1 Log in to the management console.

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

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

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

Figure 1-9 Enabling a key



□ Alias/ID	Status	Key Algorithm and Usage	Origin	Enterprise Project	Operation
□ KMS-25f5 7f39[redacted]	Disabled	AES_256 ENCRYPT_DECRYPT	Key Management Service	DEW	Enable Delete | Add to Project

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

NOTE

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

----End

1.4.3 Disabling One or More CMKs

This section describes how to use the KMS console to disable one or more custom keys, thereby protecting data in urgent cases.

After being disabled, a custom key cannot be used to encrypt or decrypt any data. Before using a disabled CMK to encrypt or decrypt data, you must enable it by following instructions in **Enabling One or More CMKs**.

Prerequisites

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

Constraints

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

Procedure

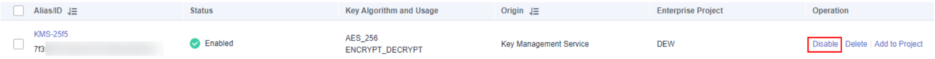
Step 1 **Log in to the management console**.

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

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

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

Figure 1-10 Disabling one CMK



□ Alias/ID	Status	Key Algorithm and Usage	Origin	Enterprise Project	Operation
□ KMS-25f5 7f3[redacted]	Enabled	AES_256 ENCRYPT_DECRYPT	Key Management Service	DEW	Disable Delete | Add to Project

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

NOTE

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

----End

1.4.4 Deleting One or More CMKs

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

Prerequisites

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

Constraints

- A key will not be deleted until its scheduled deletion period expires. You can set the period to a value within the range 7 to 1096 days.

  Before the specified deletion date, you can cancel the deletion if you want to use the CMK. Once the scheduled deletion has taken effect, the CMK will be deleted permanently and you will not be able to decrypt data encrypted by the CMK. Exercise caution when performing this operation.
- For details about the billing information about a CMK scheduled to be deleted, see **Will a CMK Be Charged After It Is Scheduled to Delete?**
- Default keys created by KMS cannot be scheduled for deletion.

Procedure

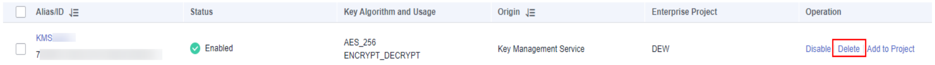
Step 1 **Log in to the management console**.

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

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

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

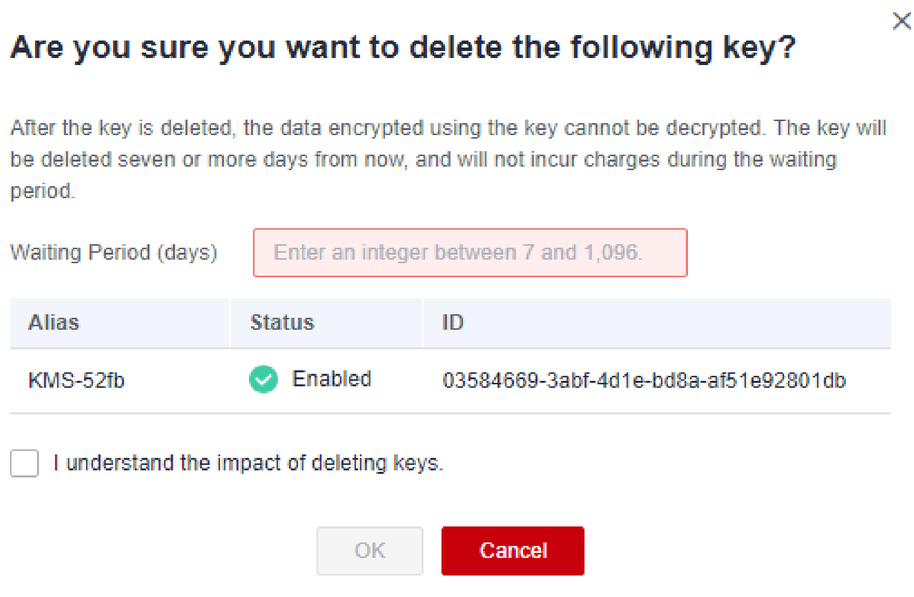
Figure 1-11 Scheduling the deletion of one CMK



□ Alias/ID	Status	Key Algorithm and Usage	Origin	Enterprise Project	Operation
□ KMS[redacted] 7[redacted]	✓ Enabled	AES_256 ENCRYPT_DECRYPT	Key Management Service	DEW	Disable Delete Add to Project

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



Are you sure you want to delete the following key?

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

Waiting Period (days) Enter an integer between 7 and 1,096.

Alias	Status	ID
KMS-52fb	✓ Enabled	03584669-3abf-4d1e-bd8a-af51e92801db

□ I understand the impact of deleting keys.

NOTE

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

Step 6 In the confirmation dialog box, enter **DELETE** and click **OK**. A message is displayed, indicating that the key deletion task is delivered successfully.

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. You need to click **Yes**.

NOTE

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

----End

1.4.5 Canceling the Scheduled Deletion of One or More CMKs

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

Prerequisites

The CMK for which you want to cancel the scheduled deletion is in **Pending deletion** status.

Procedure

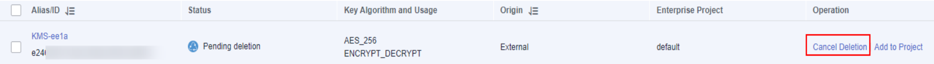
Step 1 Log in to the management console.

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

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

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

Figure 1-13 Canceling the scheduled deletion of one CMK



□	Alias/ID	Status	Key Algorithm and Usage	Origin	Enterprise Project	Operation
□	KMS-ee1a e24[redacted]	Pending deletion	AES_256 ENCRYPT_DECRYPT	External	default	Cancel Deletion Add to Project

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

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

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

----End

1.4.6 Adding a Key to a Project

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

> NOTE
>
> The enterprise project of default keys cannot be changed.

Procedure

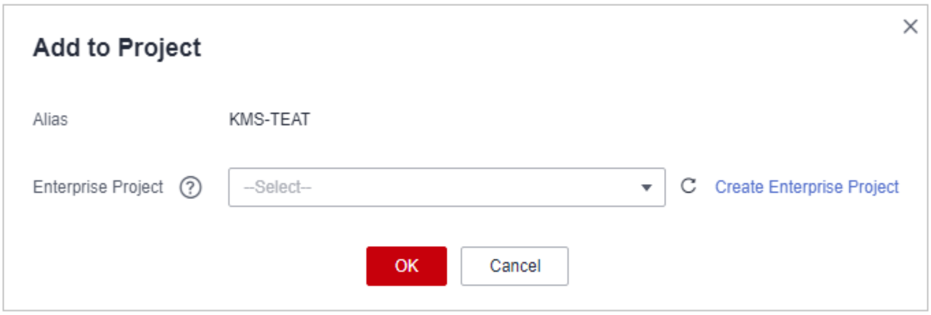
Step 1 Log in to the management console.

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

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

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

Figure 1-14 Adding a key to a project



Add to Project

Alias: KMS-TEAT

Enterprise Project: --Select--

Step 5 Select a project.

Step 6 Click **OK**.

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

Step 4 Click the search bar and select the criteria for filtering keys, as shown in **Figure 1-15**. Search for a key by specifying attributes.

Figure 1-15 Search bar

NOTE

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.

Constraints

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

Encrypting Data

Step 1 Log in to the management console.

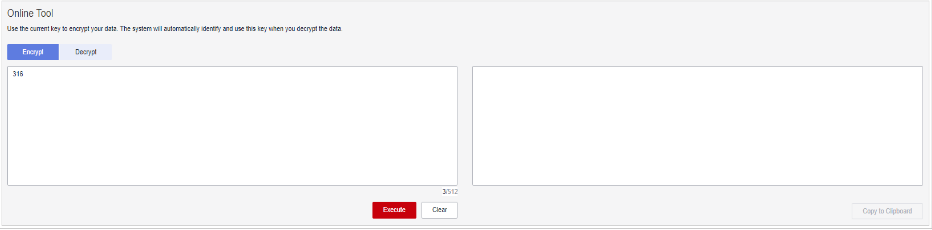
Step 2 Click in the upper left corner of the management console and select a region or project.

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

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

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

Figure 1-16 Encrypting data



Online Tool

Use the current key to encrypt your data. The system will automatically identify and use this key when you decrypt the data.

316

3/512

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

NOTE

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

----End

Decrypting Data

Step 1 Log in to the management console.

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

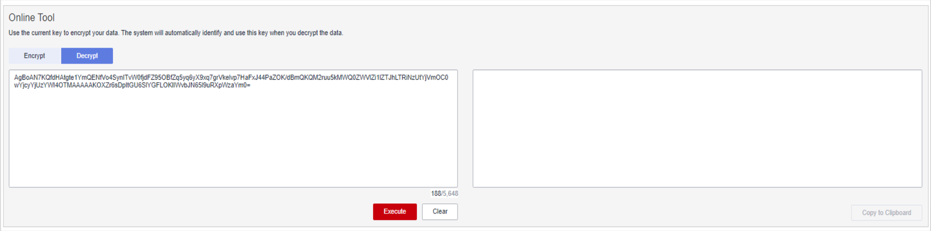
Step 3 You can click any non-default key in **Enabled** status to go to the encryption and decryption page of the online tool.

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

NOTE

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

Figure 1-17 Decrypting data



Use the current key to encrypt your data. The system will automatically identify and use this key when you decrypt the data.

```
AgBoAN7KQfdHAtgte1YmQENfVo4SynITvW0fjdFZ95OBfZq5yq6yX9xq7grVkelvp7HaFxJ44PaZOK/dBmQKQM2ruu5kMWQ0ZWVlZi1lZTJhLTRiNzUtYjVmOC0
wYjcyYjUzYWI4OTMAAAAAKOXZr6sDpltGU6SlYGFLOKllWvbJN65l9uRXpWzaYm0=
```

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

NOTE

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

----End

1.7 Managing Tags

1.7.1 Adding a Tag

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

Constraints

Tags cannot be added to default keys.

Procedure

Step 1 **Log in to the management console**.

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

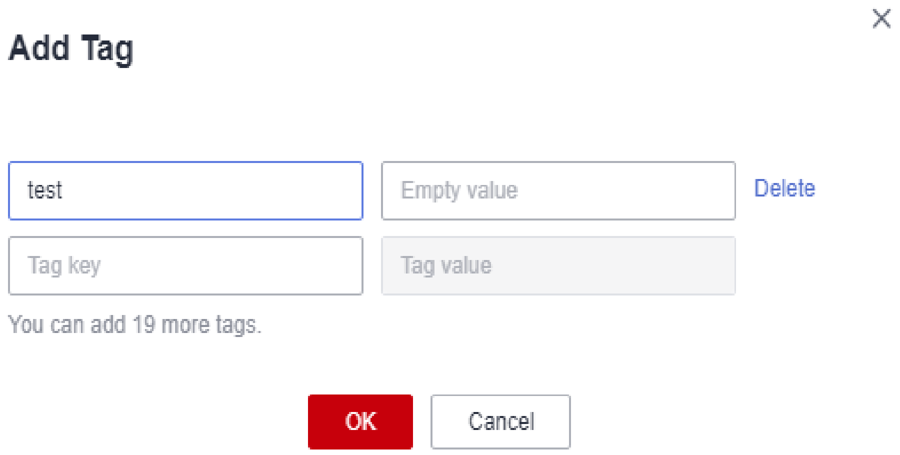
Step 3 Click ☰. Choose **Security & Compliance** > **Data Encryption Workshop**.

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

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

Step 6 Click **Add Tag**. In the **Add Tag** dialog box, enter the tag key and tag value. **Table 1-11** describes the parameters.

Figure 1-18 Adding a tag


Add Tag

test | Empty value | Delete

Tag key | Tag value

You can add 19 more tags.

NOTE

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

Table 1-11 Tag parameters

Parameter	Description	Value	Example Value
Tag key	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.	• 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: – Chinese – English – Numbers – Space – Special characters: _.:/=+-@	cost

Parameter	Description	Value	Example Value
Tag value	Value of the tag	● This parameter can be empty. ● 255 characters limit. ● The following character types are allowed: – Chinese – English – Numbers – Space – Special characters: _.:/=+-@	100

Step 7 Click **OK** to complete.

----End

1.7.2 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

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

Procedure

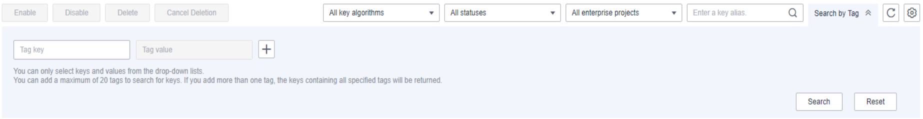
Step 1 Log in to the management console.

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

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

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

Figure 1-19 Searching for tags

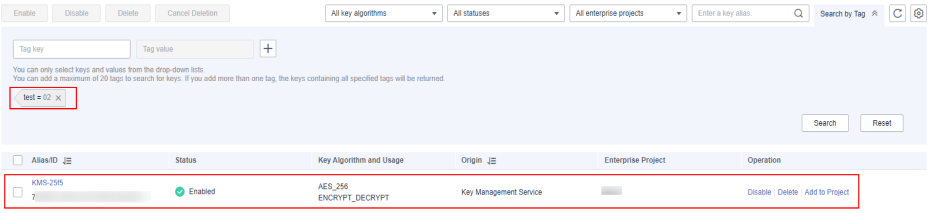


You can only select keys and values from the drop-down lists.
You can add a maximum of 20 tags to search for keys. If you add more than one tag, the keys containing all specified tags will be returned.

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

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

Figure 1-20 Search results



You can only select keys and values from the drop-down lists.
You can add a maximum of 20 tags to search for keys. If you add more than one tag, the keys containing all specified tags will be returned.

Alias/ID	Status	Key Algorithm and Usage	Origin	Enterprise Project	Operation
KMS-25f5 7[redacted]	Enabled	AES_256 ENCRYPT_DECRYPT	Key Management Service	[redacted]	Disable | Delete | Add to Project

NOTE

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

----End

1.7.3 Modifying Tag Values

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

Procedure

Step 1 **Log in to the management console**.

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

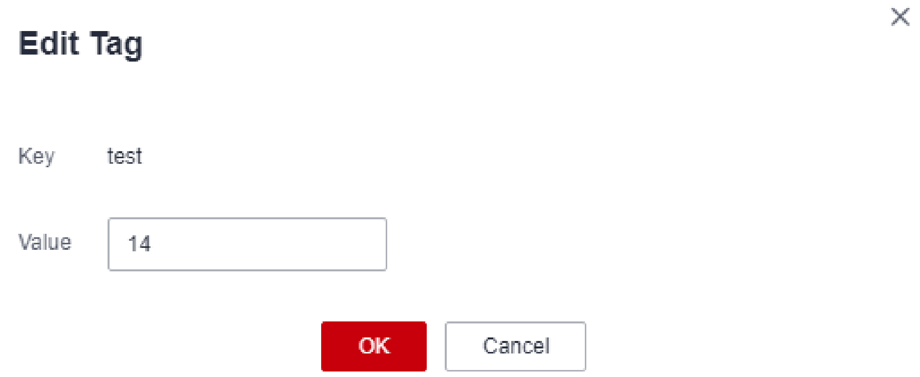
Step 3 Click ☰. Choose **Security & Compliance** > **Data Encryption Workshop**.

Step 4 Click the alias of the desired 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



Edit Tag

Key test

Value 14

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

----End

1.7.4 Deleting Tags

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

Procedure

Step 1 **Log in to the management console**.

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

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

Step 4 Click the alias of the desired 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

1.8 Rotating CMKs

1.8.1 About Key Rotation

Purpose of Key Rotation

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

The purposes of key rotation are:

- To reduce the amount of data encrypted by each key.

  A key will be insecure if it is used to encrypt a huge number of data. The amount of data encrypted a key refers to the total number of bytes or messages encrypted using the key.

- To enhance the capability of responding to security events.

  In your initial system security design, you shall design the key rotation function and use it for routine O&M, so that it will be at hand when an emergency occurs.

- To enhance the data isolation capability.

  The ciphertext data generated before and after key rotation will be isolated. You can identify the impact scope of a security event based on the key involved and take actions accordingly.

Key Rotation Methods

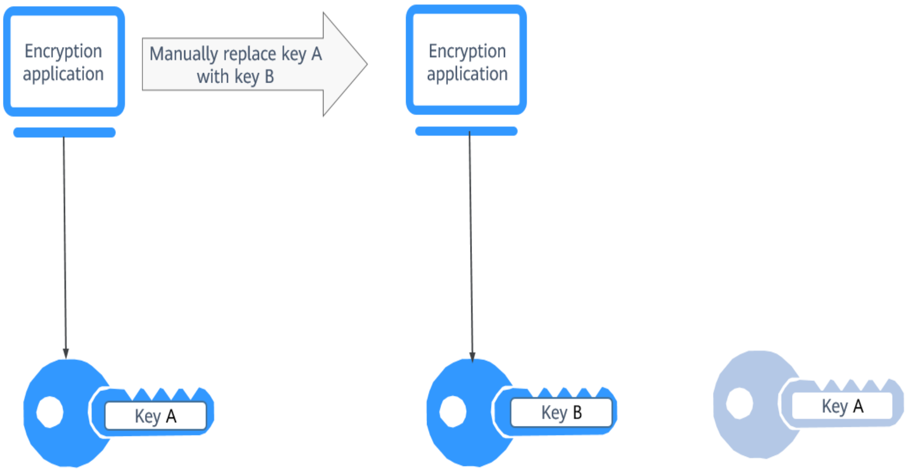
You can use either of the following key rotation methods:

- Manual key rotation

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

  Take OBS as an example. To manually rotate a key, create a new 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

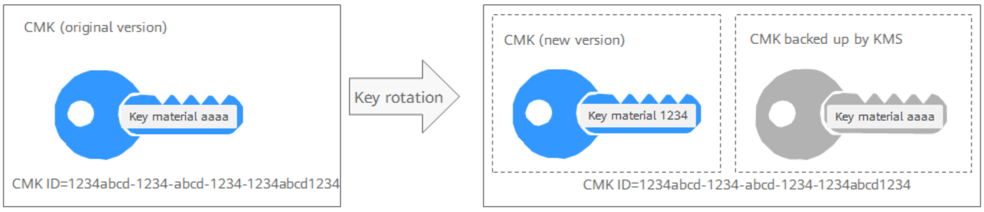
  KMS automatically rotates keys based on the configured rotation period (365 days by default). The system automatically generates a new key to replace the key in use. Automatic key rotation only changes the key material of a CMK. The logical attributes of the key will not change, including its key ID,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

  Automatic key rotation has the following characteristics:

a. Enable rotation for an existing custom key. KMS will automatically generate new key materials for the custom key.

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

Figure 1-23 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 1-12 Key rotation modes

Key Type	Rotation Mode
Default key	Cannot be rotated.
Custom key	Can only be manually rotated. For more information about custom keys, see **Overview**.
Symmetric key	Can be automatically or manually rotated.
Asymmetric key	Can only be manually rotated.
Disabled CMK	Disabled CMKs are not rotated. KMS keeps their rotation status unchanged. After a 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**.

Key Type	Rotation Mode
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**.

1.8.2 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**.

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.

Procedure

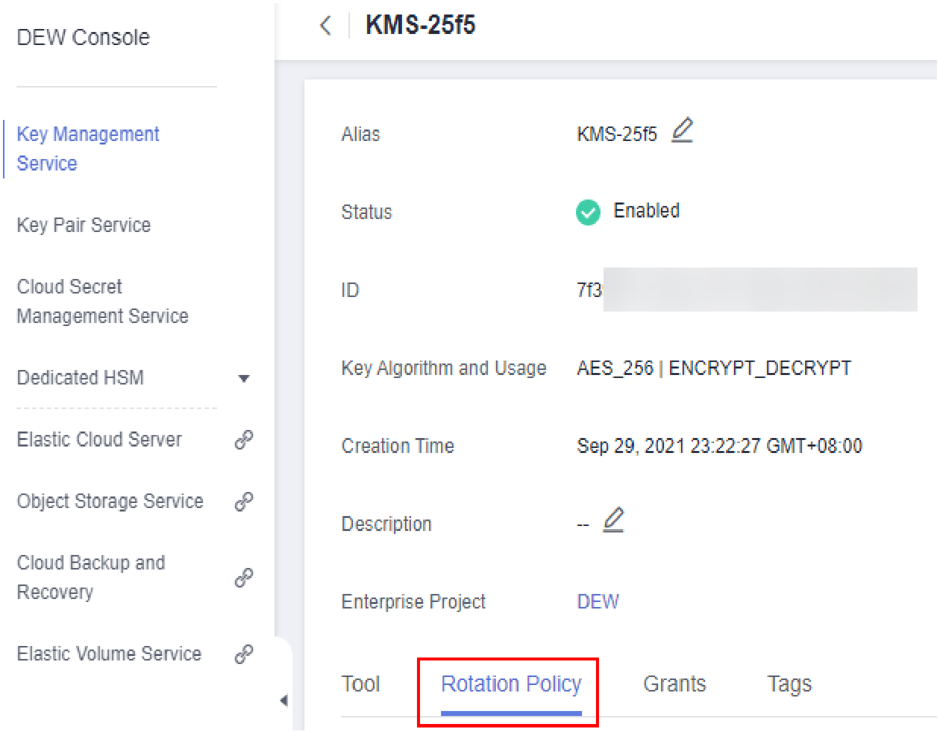
Step 1 **Log in to the management console**.

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

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

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

Figure 1-24 Key details



Alias KMS-25f5

Status Enabled

ID 7f3[redacted]

Key Algorithm and Usage AES_256 | ENCRYPT_DECRYPT

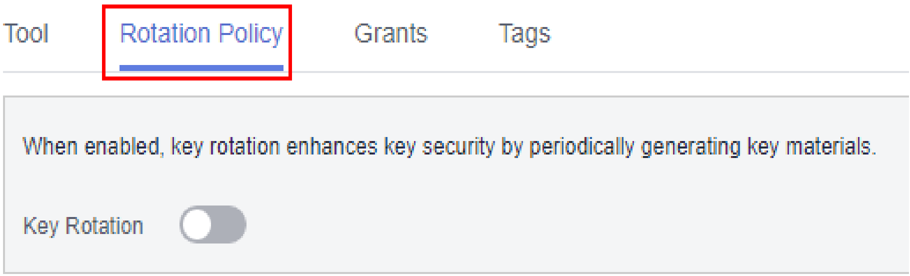
Creation Time Sep 29, 2021 23:22:27 GMT+08:00

Description --

Enterprise Project DEW

Step 5 Click the **Rotation Policy** tab. The rotation switch is displayed, as shown in **Figure 1-25**.

Figure 1-25 Key rotation



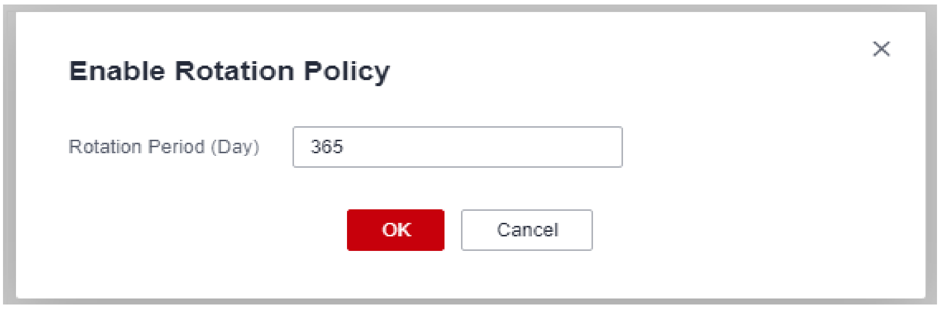
When enabled, key rotation enhances key security by periodically generating key materials.

Key Rotation

Step 6 Click ○ to enable key rotation.

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

Figure 1-26 Enabling key rotation



Enable Rotation Policy

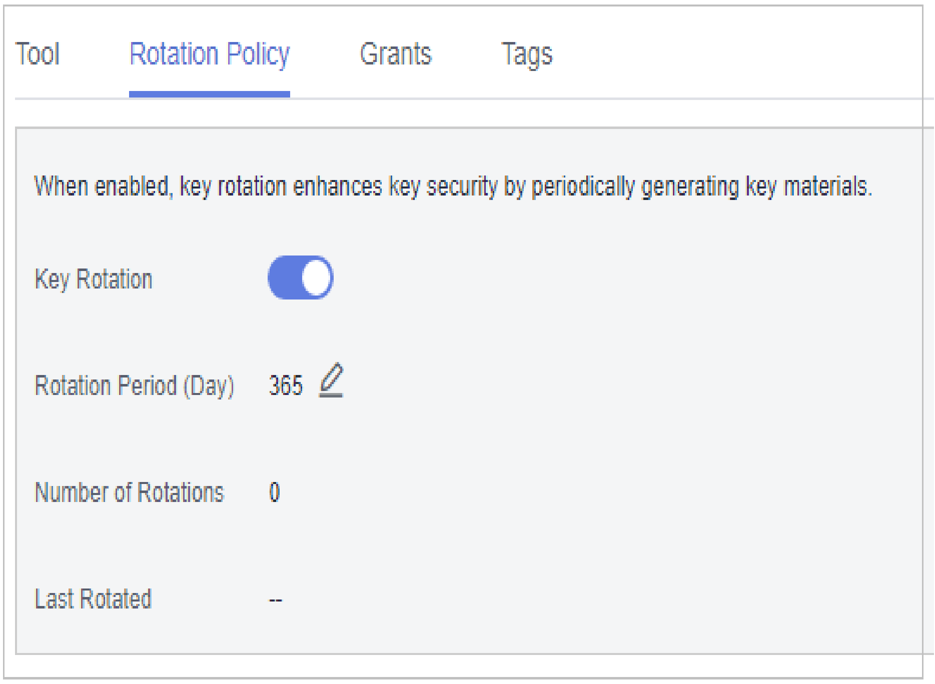
Rotation Period (Day) 365

Table 1-13 Key rotation parameters

Parameter	Description
Key rotation	Rotation switch. The default status is ○. ○: disabled ●: enabled After rotation is enabled, the key will be rotated based on your set period. **NOTE** 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.
Rotation Period (day)	Rotation period (day). The value is an integer ranging from 30 to 365. The default value is **365**. Configure the period based on how often a custom key is used. If it is frequently used, configure a short period; otherwise, set a long one.

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

Figure 1-27 Key rotation details



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

1.8.3 Disabling Key Rotation

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

Prerequisites

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

Procedure

Step 1 Log in to the management console.

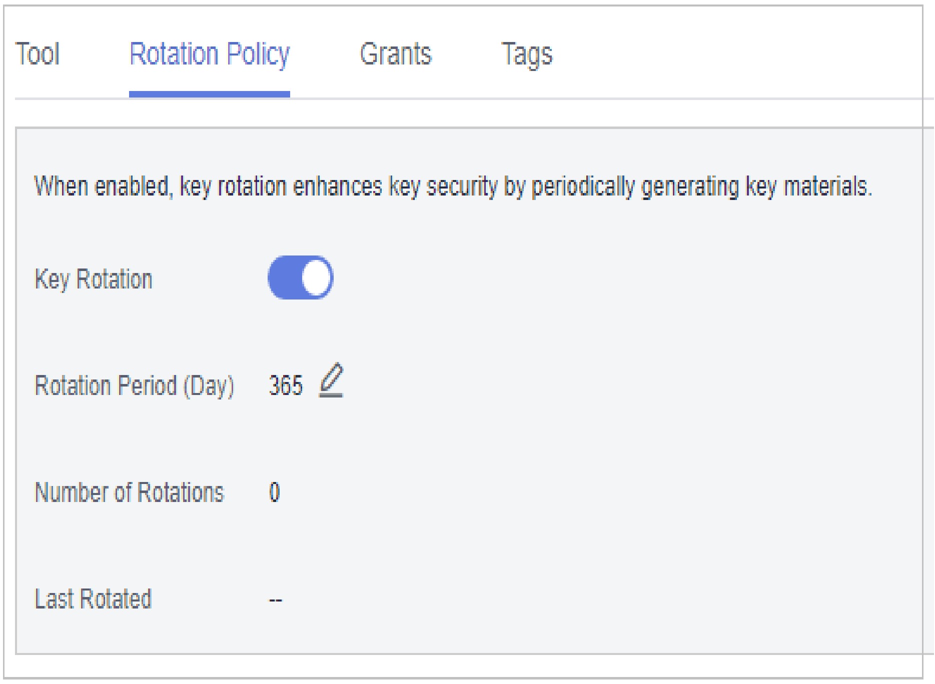
Step 2 Click in the upper left corner of the management console and select a region or project.

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

Step 4 Click the alias of a symmetric key.

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

Figure 1-28 Key rotation details



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

Key Rotation ●

Rotation Period (Day) 365

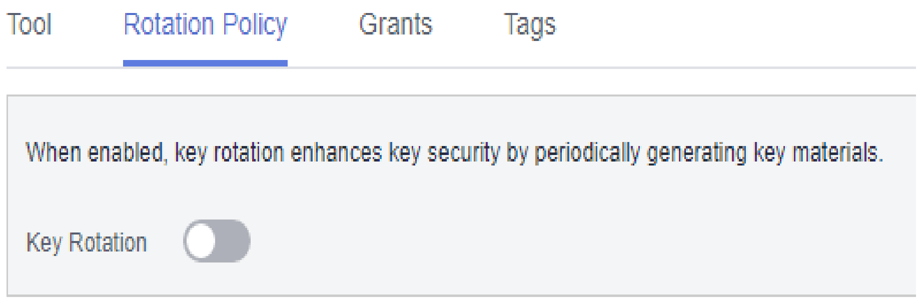
Number of Rotations 0

Last Rotated --

Step 6 Click ● to disable key rotation.

Step 7 Check the rotation status, as shown in **Figure 1-29**.

Figure 1-29 Disabling key rotation



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

Key Rotation ○

----End

1.9 Managing a Grant

1.9.1 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 desired custom key is in **Enabled** status.

Constraints

- The owner of a custom key can create a grant for the custom key on the KMS console or by calling APIs. The IAM users or accounts who have the grant creation permission assigned by the owner of the custom key can create grants for the custom key only by calling APIs.
- A maximum of 100 grants can be created for a custom key.

Procedure

Step 1 Log in to the management console.

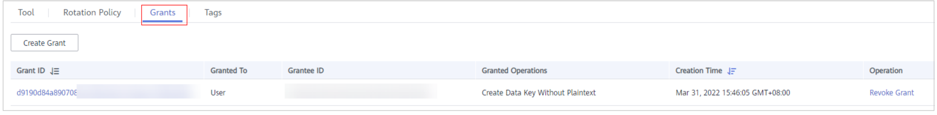
Step 2 Click in the upper left corner of the management console and select a region or project.

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

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

Step 5 Click the **Grants** tab.

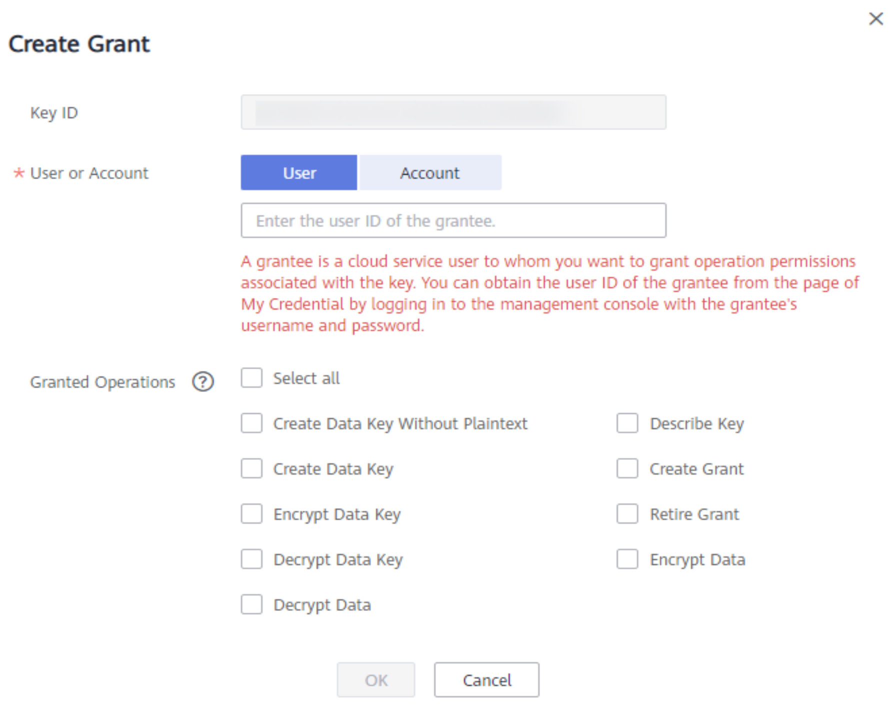
Figure 1-30 Grant tab page



Grant ID	Granted To	Grantee ID	Granted Operations	Creation Time	Operation
d9190d84a89070E[redacted]	User	[redacted]	Create Data Key Without Plaintext	Mar 31, 2022 15:46:05 GMT+08:00	Revoke Grant

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

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



Create Grant

Key ID

* User or Account — User | Account

Enter the user ID of the grantee.

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

Granted Operations

□ Select all

□ Create Data Key Without Plaintext　□ Describe Key

□ Create Data Key　□ Create Grant

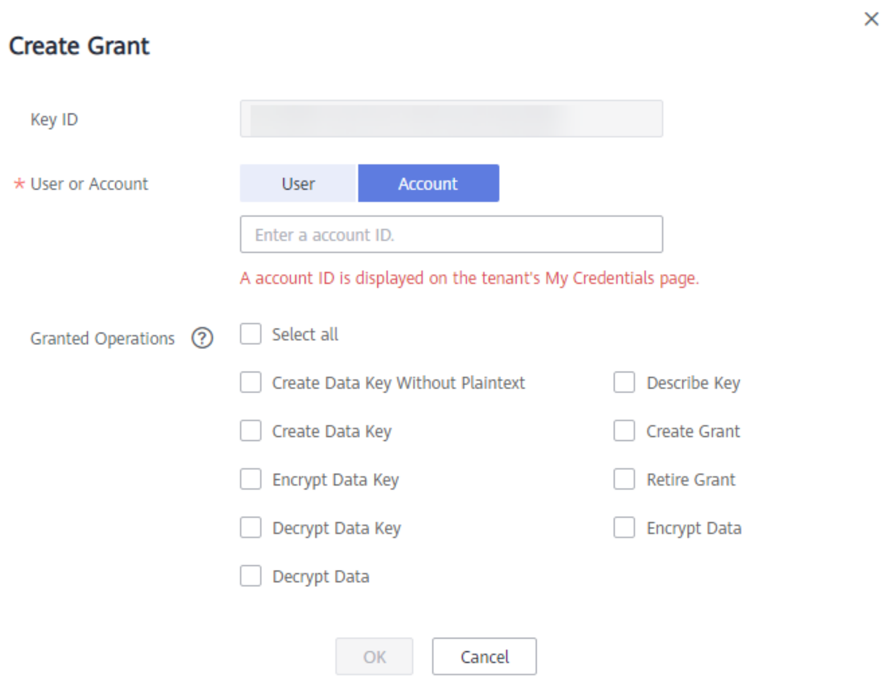
□ Encrypt Data Key　□ Retire Grant

□ Decrypt Data Key　□ Encrypt Data

□ Decrypt Data

OK　Cancel

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



Create Grant

Key ID

* User or Account — User | Account

Enter a account ID.

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

Granted Operations

□ Select all

□ Create Data Key Without Plaintext　□ Describe Key

□ Create Data Key　□ Create Grant

□ Encrypt Data Key　□ Retire Grant

□ Decrypt Data Key　□ Encrypt Data

□ Decrypt Data

OK　Cancel

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

NOTICE

A grantee can perform the authorized operations only by calling the necessary APIs. For details, see the *Data Encryption Workshop API Reference*.

Table 1-14 Parameter description

Parameter	Description	Example Value
Key ID	ID of a custom key (automatically read by the system)	-
User or Tenant	Whether a user or an account is authorized. ● User User ID: Enter the IAM user ID. To obtain the ID, click the username in the upper right corner of the page, choose **My Credentials**. Choose **API Credentials** from the navigation pane, and copy the value of **IAM User ID**. After the authorization is complete, the IAM user can use the specified keys. ● Account Account ID: Enter the IAM user ID. To obtain the ID, click the username in the upper right corner of the page, choose **My Credentials**. Choose **API Credentials** from the navigation pane, and copy the value of **Account ID**. After the authorization is complete, all IAM users under the account can use specified keys.	d9a6b2bdaedd4ba586cabe6372d1b312

Parameter	Description	Example Value
Operations	The following permissions can be authorized: **NOTE** - You can create multiple grants on a custom key to provide different permissions to the same user. The user's permissions on the custom key are the combination of all the grants. - This parameter cannot be left blank. - Selecting only **Create Grant** is not allowed. - **Create Data Key Without Plaintext** - **Create Data Key** - **Encrypt Data Key** - **Decrypt Data Key** - **Query Key Information** - **Create Grant** - **Retire Grant** – A grantee can retire a grant if the grantee does not need that permission. – If, before retiring a grant, the grantee has granted the permission to another user, that user's permission will not be affected by the grant retirement. - **Encrypt Data** - **Decrypt Data**	-

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

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

----End

1.9.2 Querying a Grant

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

Prerequisites

You have created a grant.

Procedure

Step 1 **Log in to the management console**.

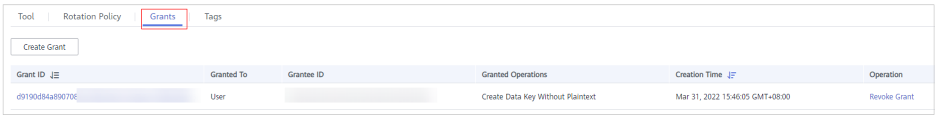
Step 2 Click in the upper left corner of the management console and select a region or project.

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

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

Step 5 Click the **Grants** tab. Information about the custom key and grants created on it are displayed. See **Figure 1-33**.

Figure 1-33 Grant tab page



Grant ID	Granted To	Grantee ID	Granted Operations	Creation Time	Operation
d9190d84a89070E[redacted]	User	[redacted]	Create Data Key Without Plaintext	Mar 31, 2022 15:46:05 GMT+08:00	Revoke Grant

Table 1-15 describes the parameters.

Table 1-15 Parameter description

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

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

----End

1.9.3 Revoking a Grant

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

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

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

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

Prerequisites

You have created a grant.

Procedure

Step 1 **Log in to the management console**.

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

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

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

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

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

----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.

RDS Secrets

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

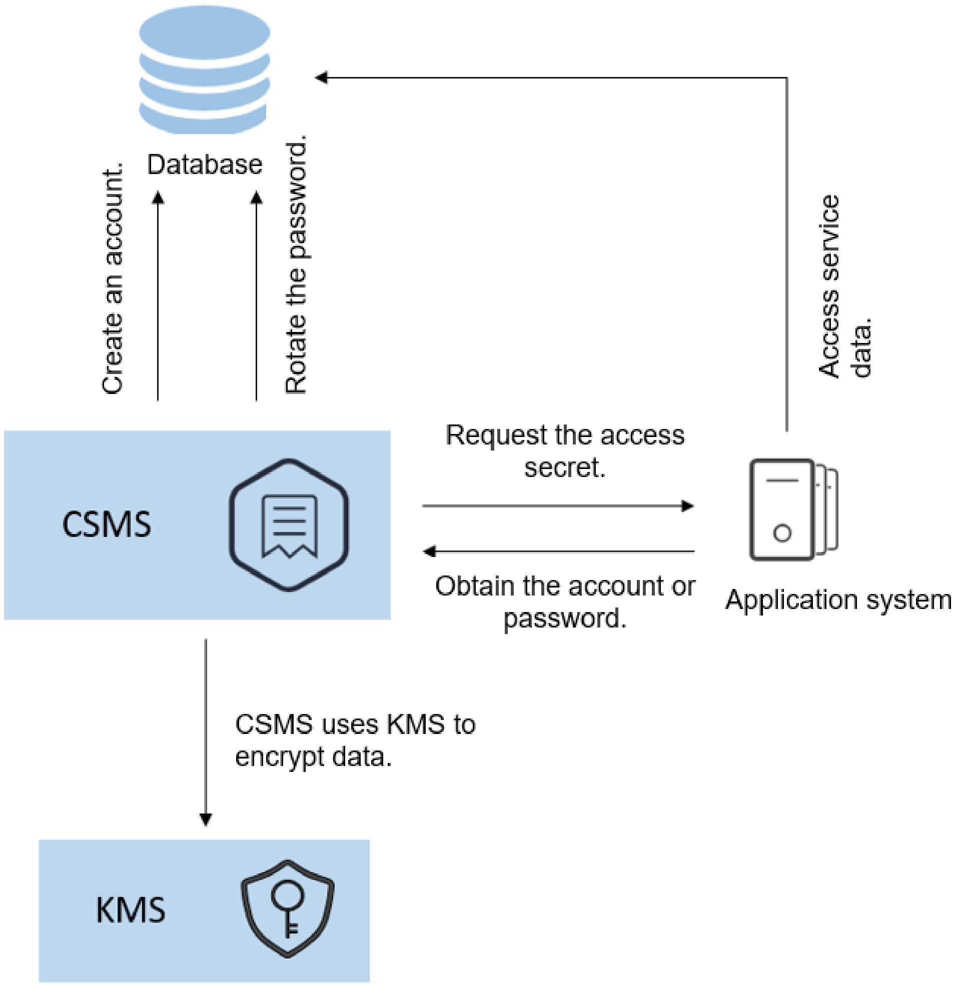
Differences Between Shared Secrets and RDS Secrets

Table 2-1 Credential difference

	Shared Secret	RDS Secret
Application Scenario	Supports full lifecycle management of customized secrets in different scenarios.	Automatically hosts Huawei Cloud RDS database secrets.
Automatic Rotation	Not supported. Users need to trigger the rotation.	Supported. Single-user and dual-user rotation models are supported.

Getting Started

Figure 2-1 Architecture



Process description:

1. Create an RDS 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 use 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 Common Secret

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

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

Constraints

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

Creating a Secret

Step 1 Log in to the management console.

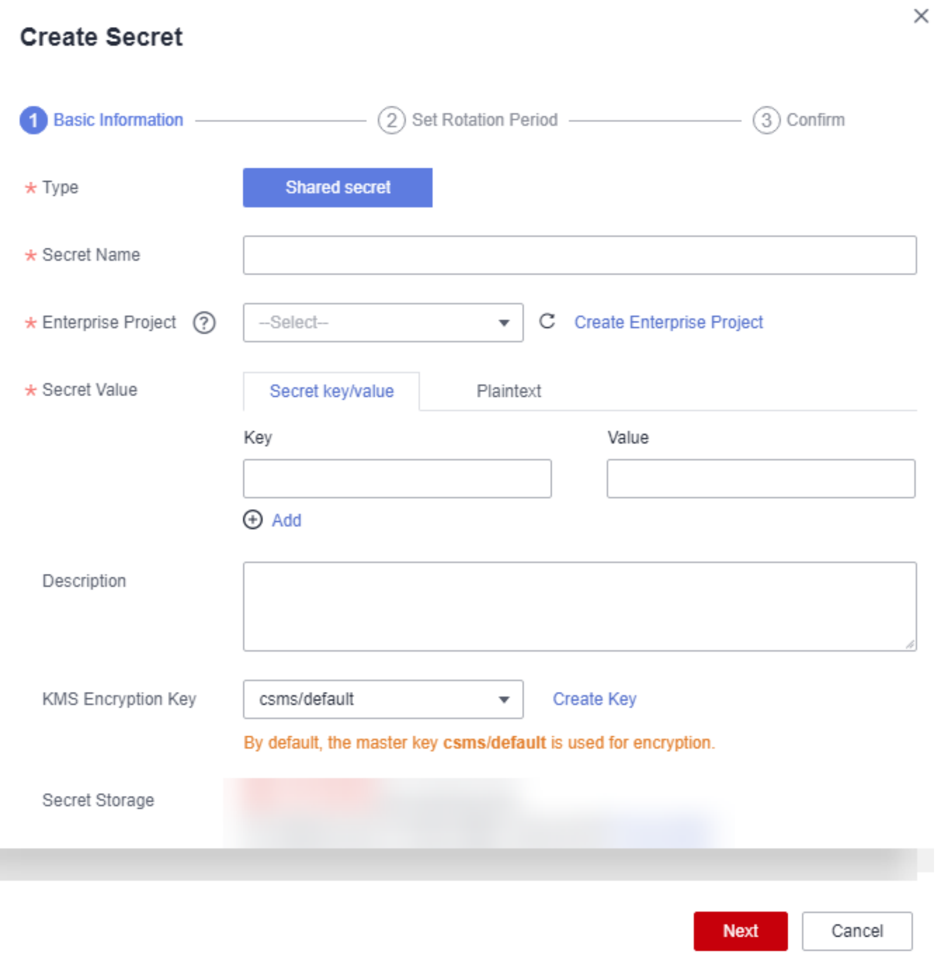
Step 2 Click 📍 in the upper left corner of the management console and select a region or project.

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

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

Step 5 Click **Create Secret**. Configure parameters in the **Create Secret** dialog box, as shown in **Figure 2-2**. For more information, see **Table 2-2**.

Figure 2-2 Creating a secret



Create Secret

1 Basic Information — 2 Set Rotation Period — 3 Confirm

* Type: Shared secret

* Secret Name:

* Enterprise Project ⓘ: --Select-- Create Enterprise Project

* Secret Value: Secret key/value | Plaintext

Key: Value:

⊕ Add

Description:

KMS Encryption Key: csms/default Create Key

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

Secret Storage

Next Cancel

Table 2-2 Secret parameters

Parameter	Description
Type	Secret type. The default value is **Shared secret**.
Secret Name	Secret name
Enterprise Project	Enterprise project that the secret is to be bound to
Secret Value	Secret key/value pair and the plaintext secret to be encrypted
Description	Description of a secret
KMS Encryption Key	Select the default key **csms/default** or a custom key created on KMS. **NOTE** By default, the default key **csms/default** created by CSMS is used as the encryption master key of the current secret. You can also create a key or use a custom key on the KMS console. For details, see **Creating a Key**.
Associated Event	When creating a secret, you can associate it with a secret event. You can add, delete, modify, and query secret versions on the event notification page.

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

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

Step 8 Click **OK**.

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

----End

2.3.2 Creating an RDS Secret

This section describes how to create an RDS secret on the secret management page.

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.
- RDS secrets support the following DB engines: MySQL and PostgreSQL. Currently, the SQL Server database is not supported.

Creating a Common Secret

Step 1 Log in to the management console.

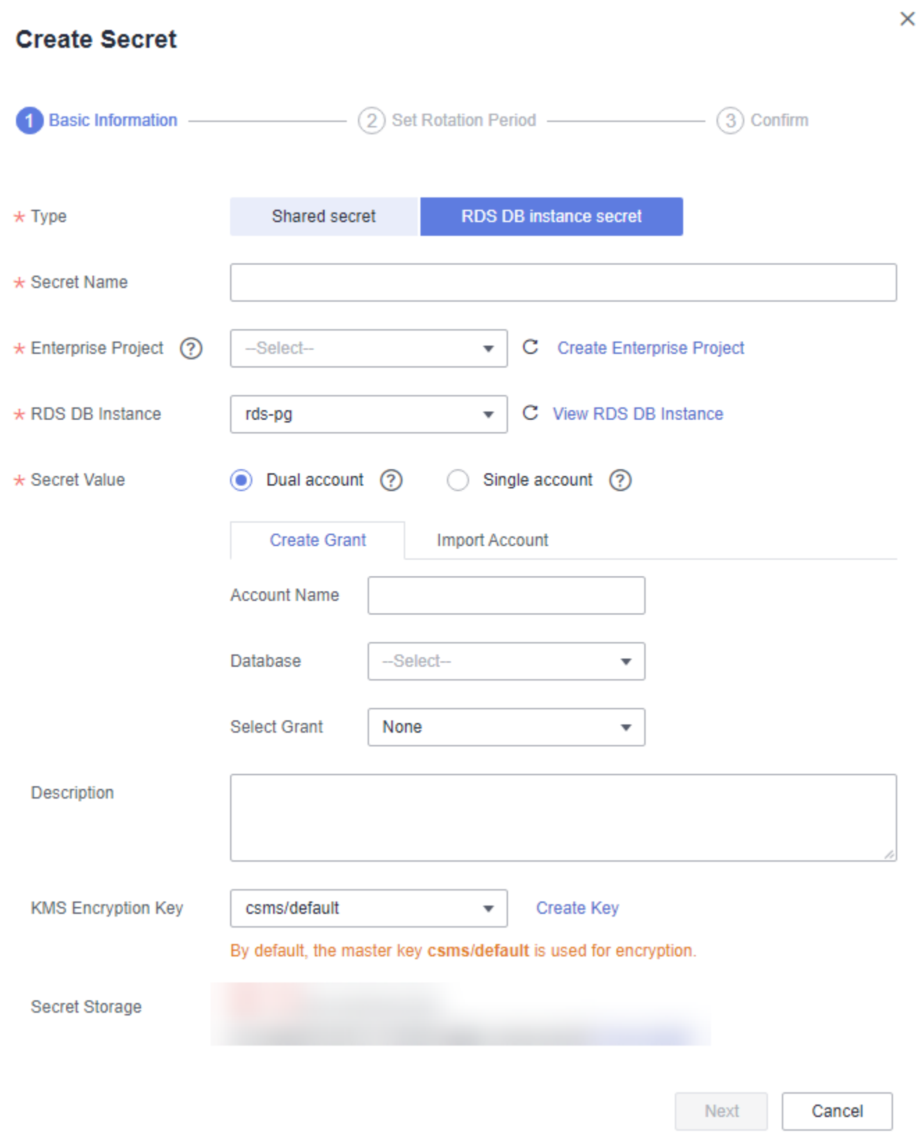
Step 2 Click 📍 in the upper left corner of the management console and select a region or project.

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

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

Step 5 Click **Create Secret** and select the **RDS DB instance secret**, as shown in Figure 2-3.

Figure 2-3 RDS DB instance secret



Create Secret

① Basic Information ② Set Rotation Period ③ Confirm

* Type	Shared secret / **RDS DB instance secret**
* Secret Name	
* Enterprise Project	--Select--
* RDS DB Instance	rds-pg
* Secret Value	● Dual account ○ Single account
Account Name	
Database	--Select--
Select Grant	None
Description	
KMS Encryption Key	csms/default
Secret Storage	

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

Step 6 In the **Create Secret** dialog box, set the parameters. For details about the parameters, see Table 2-3.

Table 2-3 RDS secret parameters

Parameter	Description
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**. If there are no **Enterprise Management** options displayed, you do not need to configure it.
RDS DB Instance Secret	Select the name of the instance you created on the RDS console (applicable only to MySQL databases).
Secret Value	Secret key/value pair and the plaintext secret to be encrypted ● If you select **Single account**, you need to enter an available database account. ● If you select **Dual account**, you need to enter two available database accounts. For details about the differences, see **Rotation Policy**.
Description	Description of a secret
KMS Encryption Key	Select the default master key **csms/default** or a user key that has been created on KMS. **NOTE** 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 key and use a user-defined encryption key on the KMS console. For details, see **Creating a Key**.

Step 7 Click **Next** and set the rotation period.

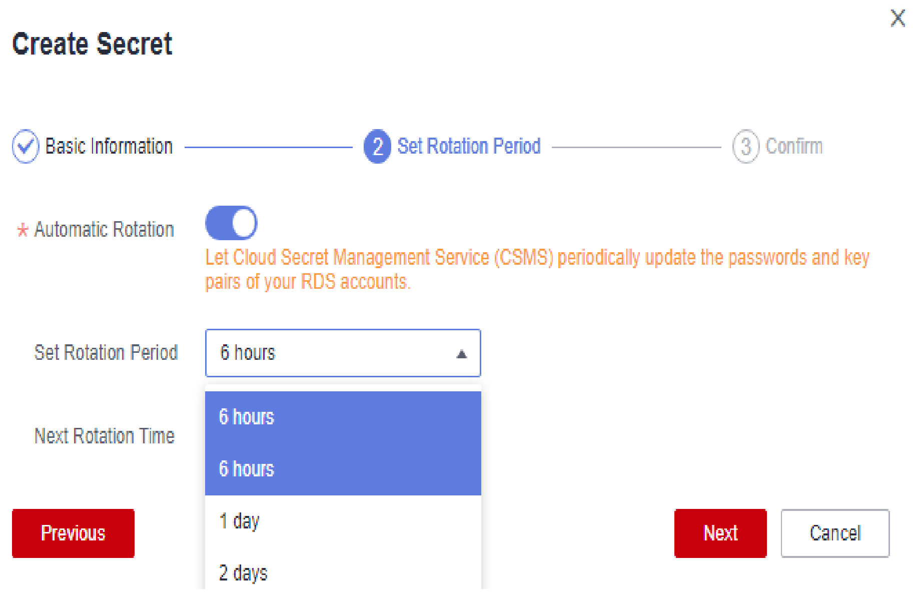
NOTICE

If the automatic rotation function is disabled, you need to manually rotate the secrets. To enable automatic rotation, click **Set Rotation Policy** on the secret details page, enable automatic rotation, and set the rotation period.

Step 8 Toggle on the automatic rotation switch and select a rotation period. You can select a preset rotation period or customize a rotation period.

The value ranges from 6 hours to 8,760 hours. The default value is 6 hours.

Figure 2-4 Selecting a rotation period



* Automatic Rotation
Let Cloud Secret Management Service (CSMS) periodically update the passwords and key pairs of your RDS accounts.

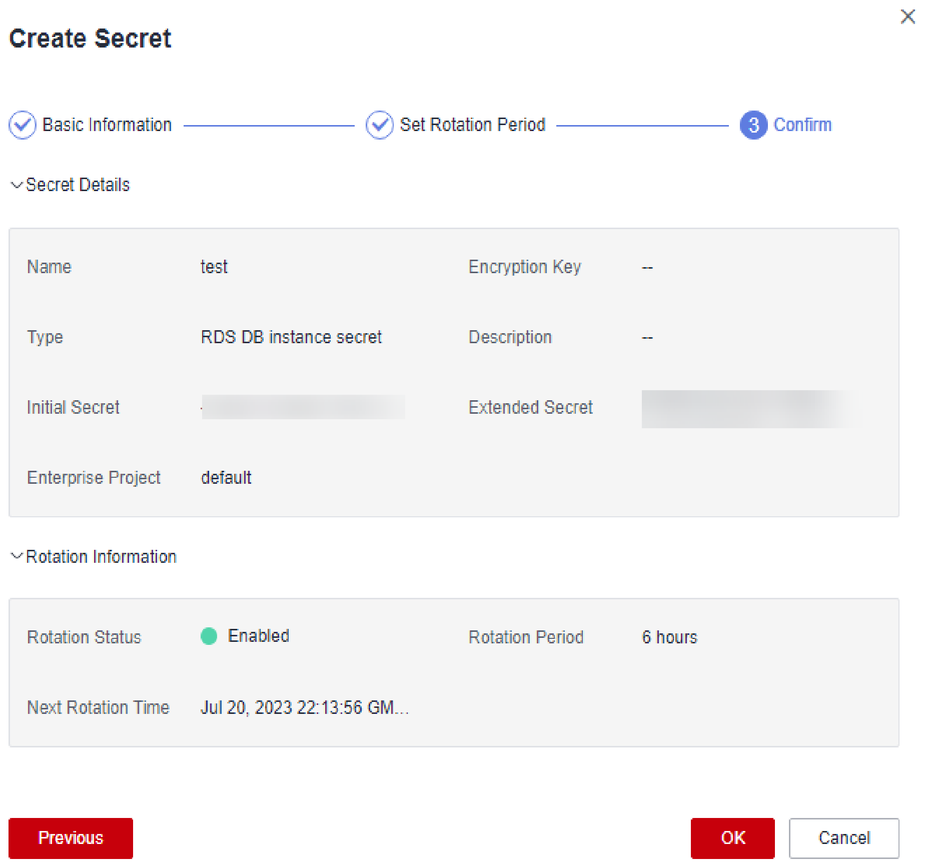
Set Rotation Period: 6 hours

Next Rotation Time

- 6 hours
- 6 hours
- 1 day
- 2 days

Step 9 Click **Next** and confirm the creation information.

Figure 2-5 Secret information



Secret Details

Name	test	Encryption Key	--
Type	RDS DB instance secret	Description	--
Initial Secret		Extended Secret	
Enterprise Project	default		

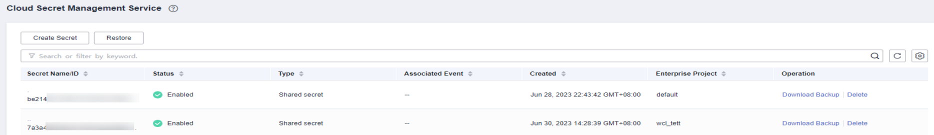
Rotation Information

Rotation Status	● Enabled	Rotation Period	6 hours
Next Rotation Time	Jul 20, 2023 22:13:56 GM...		

Step 10 Click **OK**. A message is displayed in the upper right corner of the page, indicating that the secret is created successfully.

Step 11 You can view the created secrets in the secret list, as shown in **Figure 2-6**. The default status of a secret is **Enabled**.

Figure 2-6 Secret list



Cloud Secret Management Service

Secret Name/ID	Status	Type	Associated Event	Created	Enterprise Project	Operation
be214[redacted]	Enabled	Shared secret	--	Jun 28, 2023 22:43:42 GMT+08:00	default	Download Backup | Delete
7a3a[redacted]	Enabled	Shared secret	--	Jun 30, 2023 14:28:39 GMT+08:00	wcl_tett	Download Backup | Delete

----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**.

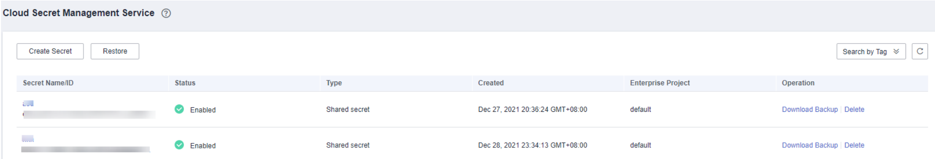
Step 2 Click in the upper left corner of the management console and select a region or project.

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

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

Step 5 Check the secret list. For more information, see **Table 2-4**.

Figure 2-7 Secret list



Cloud Secret Management Service

Secret Name/ID	Status	Type	Created	Enterprise Project	Operation
[redacted]	Enabled	Shared secret	Dec 27, 2021 20:36:24 GMT+08:00	default	Download Backup | Delete
[redacted]	Enabled	Shared secret	Dec 28, 2021 23:34:13 GMT+08:00	default	Download Backup | Delete

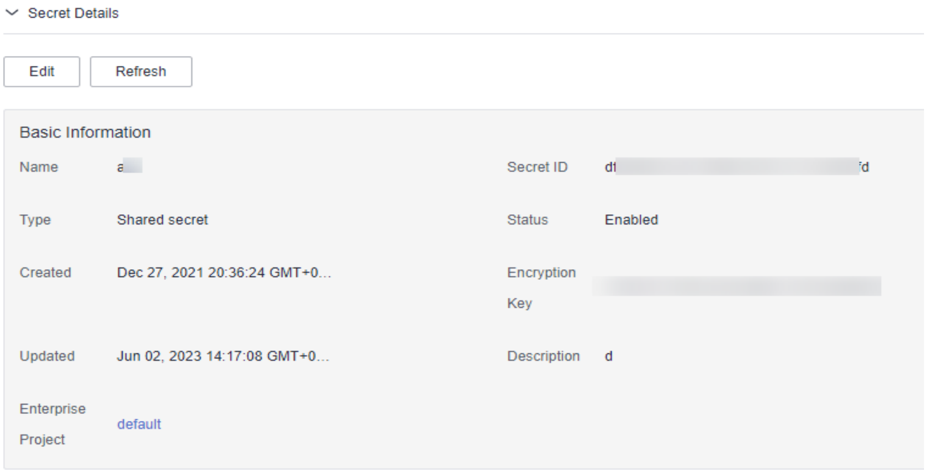
Table 2-4 Secret list parameters

Parameter	Description
Secret Name/ID	Secret name
Status	Status of a secret. The value can be **Enabled** or **Pending deletion**.
Type	Secret type, including shared secrets and RDS DB instance secrets.
Created	Time when a secret is created

Parameter	Description
Enterprise Project	Enterprise project that the secret is to be bound to
Operation	You can manage secrets in the **Operation** column, for example, download secret backup, delete secrets, and cancel secret deletion.

Step 6 Click a secret to view its details. See **Figure 2-8**.

Figure 2-8 Secret details



Basic Information

Name: a[redacted]

Secret ID: d[redacted]d

Type: Shared secret

Status: Enabled

Created: Dec 27, 2021 20:36:24 GMT+0...

Encryption Key: [redacted]

Updated: Jun 02, 2023 14:17:08 GMT+0...

Description: d

Enterprise Project: default

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**.

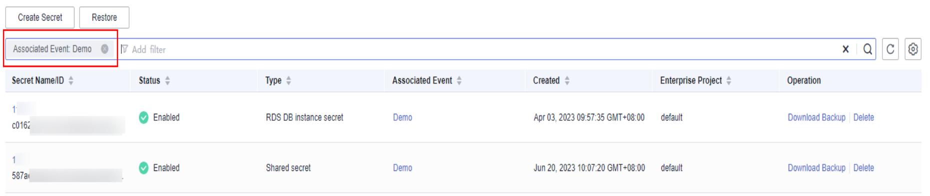
Step 2 Click 📍 in the upper left corner of the management console and select a region or project.

Step 3 Click ☰. 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 2-9**. Search for a secret by specifying the associated event.

Figure 2-9 Searching for a secret



Secret Name/ID	Status	Type	Associated Event	Created	Enterprise Project	Operation
1 [redacted] c0162 [redacted]	Enabled	RDS DB instance secret	Demo	Apr 03, 2023 09:57:35 GMT+08:00	default	Download Backup | Delete
1 [redacted] 587a [redacted]	Enabled	Shared secret	Demo	Jun 20, 2023 10:07:20 GMT+08:00	default	Download Backup | Delete

----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.

Procedure

Step 1 **Log in to the management console**.

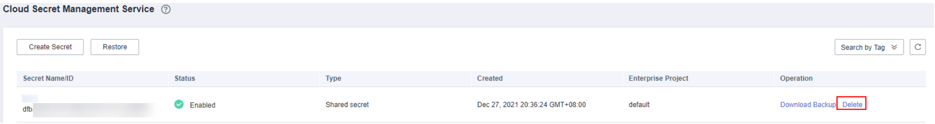
Step 2 Click in the upper left corner of the management console and select a region or project.

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

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

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

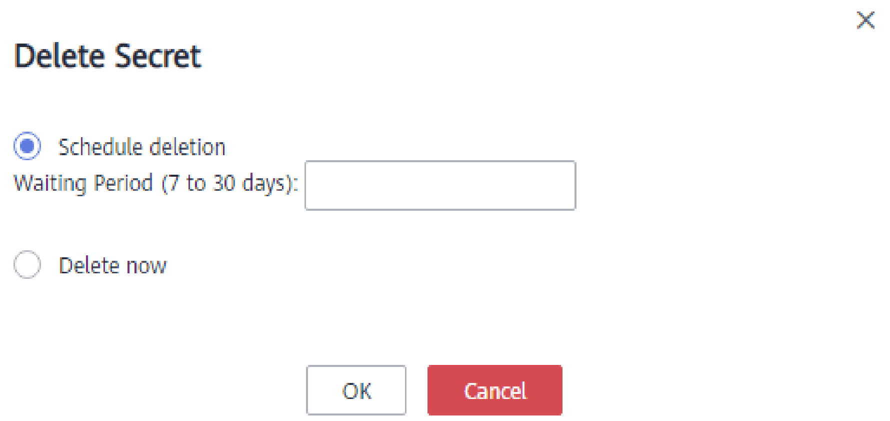
Figure 2-10 Deleting a secret



Secret Name/ID	Status	Type	Created	Enterprise Project	Operation
[redacted] dfb [redacted]	Enabled	Shared secret	Dec 27, 2021 20:36:24 GMT+08:00	default	Download Backup Delete

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

Figure 2-11 Deleting a secret



Delete Secret

● Schedule deletion

Waiting Period (7 to 30 days):

○ Delete now

Step 7 Click **OK**.

NOTE

- A secret will not be deleted until its scheduled deletion period expires. You can set the period to a value within the range 7 to 30 days. Before the specified deletion date, you can cancel the deletion if you want to use the secret. If the scheduled deletion period of a secret expires, the secret will be deleted and cannot be restored.
- For details about the billing information about a secret to be deleted, see **Are Credentials Scheduled to Be Deleted Billed?**
- If you delete a secret immediately, you can restore it using the secret backup that you have downloaded in advance. Exercise caution when performing this operation.

----End

2.5 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.
- RDS secrets do not support storing 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.

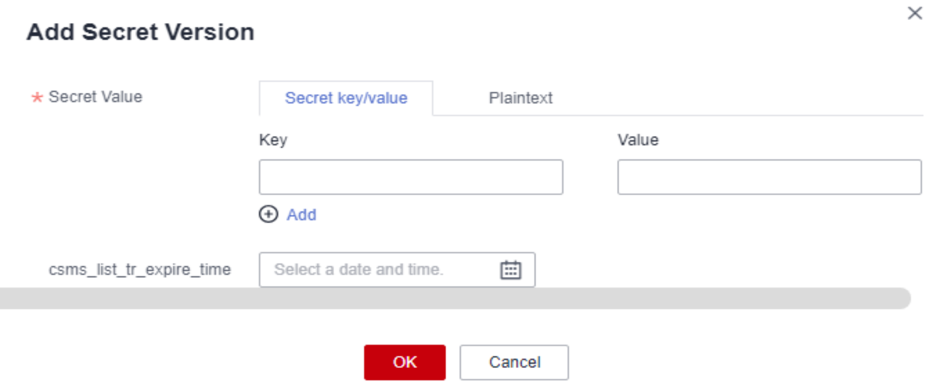
Step 3 Click ☰. Choose **Security & Compliance** > **Data Encryption Workshop**.

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

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

Step 6 In the **Version List** area, click **Add Secret Version**. Configure the secret key and value in the dialog box that is displayed.

Figure 2-12 Adding a secret value



Add Secret Version

* Secret Value: Secret key/value | Plaintext

Key:

Value:

csms_list_tr_expire_time: Select a date and time.

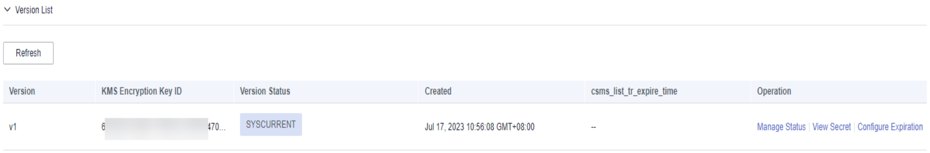
Step 7 You can select an expiration time for the stored secret value. The time can be specific to seconds. After the setting is complete, you can view the expiration time in the secret version list. For example, Jun 30, 2023 19:52:59.

Step 8 Click **OK**. A message is displayed in the upper right corner of the page, indicating that the value is added successfully.

View the latest secret value in the secret version list.

Step 9 In the **Version List** area, click **View Secret** in the **Operation** column of a secret.

Figure 2-13 Secret version list



Version List

Refresh

Version	KMS Encryption Key ID	Version Status	Created	csms_list_tr_expire_time	Operation
v1	6[redacted]470...	SYSCURRENT	Jul 17, 2023 10:56:08 GMT+08:00	--	Manage Status | View Secret | Configure Expiration

Step 10 In the **View Secret** dialog box, click **Yes**.

> NOTE
>
> Secret values are generally obtained via APIs. Checking the values on the console incurs security risks. If you are sure you want to check them on the console, click **Yes**.

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

----End

2.5.2 Managing Secret Version Statuses

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

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

Constraints

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

Procedure

Step 1 Log in to the management console.

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

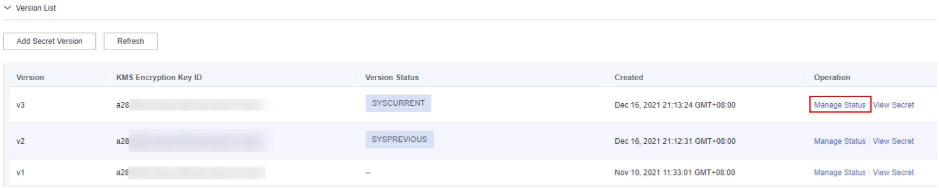
Step 3 Click ☰. Choose **Security & Compliance** > **Data Encryption Workshop**.

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

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

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

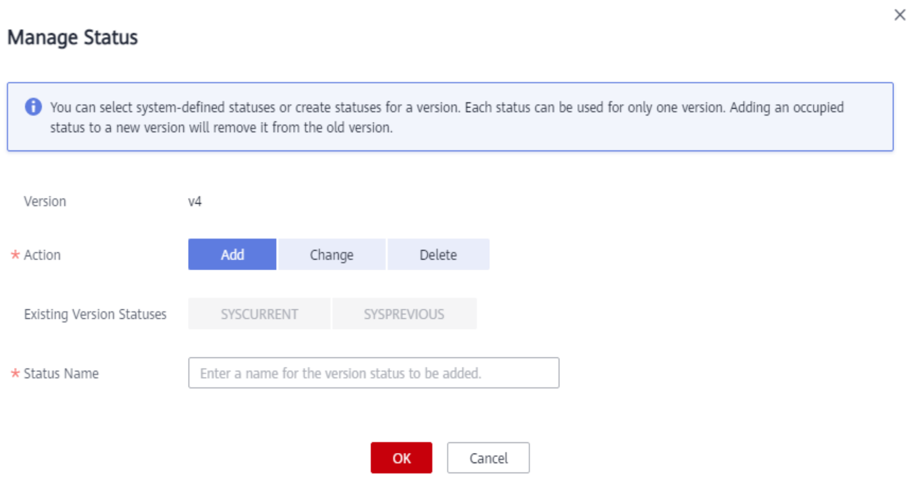
Figure 2-14 Secret version list



Version	KMS Encryption Key ID	Version Status	Created	Operation
v3	a28[redacted]	SYSCURRENT	Dec 16, 2021 21:13:24 GMT+08:00	Manage Status | View Secret
v2	a28[redacted]	SYSPREVIOUS	Dec 16, 2021 21:12:31 GMT+08:00	Manage Status | View Secret
v1	a28[redacted]	--	Nov 10, 2021 11:33:01 GMT+08:00	Manage Status | View Secret

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

Figure 2-15 Managing statuses



Manage Status

You can select system-defined statuses or create statuses for a version. Each status can be used for only one version. Adding an occupied status to a new version will remove it from the old version.

Version: v4

* Action: Add | Change | Delete

Existing Version Statuses: SYSCURRENT | SYSPREVIOUS

* Status Name: Enter a name for the version status to be added.

- Adding a version status

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

  NOTE

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

- Updating the version status of a secret

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

- Deleting the version status of a secret

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

  NOTE

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

----End

2.5.3 Rotation Secret Version

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

Constraints

- The secret type is RDS DB instance secret.
- You need to use an IAM agency to authorize the **op_svc_kms** account, **KMS CMKFullAccess**, and **RDS FullAccess** permissions (required only when automatic rotation is enabled).
- The secret account must be an existing RDS database account.

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.

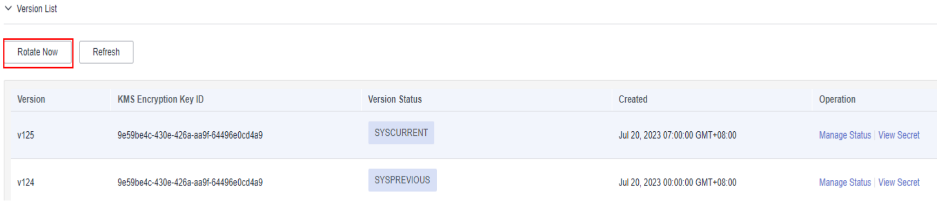
Step 3 Click . Choose **Security & Compliance** > **Data Encryption Workshop**.

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

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

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

Figure 2-16 Version list



Version	KMS Encryption Key ID	Version Status	Created	Operation
v125	9e59be4c-430e-426a-aa9f-64496e0cd4a9	SYSCURRENT	Jul 20, 2023 07:00:00 GMT+08:00	Manage Status | View Secret
v124	9e59be4c-430e-426a-aa9f-64496e0cd4a9	SYSPREVIOUS	Jul 20, 2023 00:00:00 GMT+08:00	Manage Status | View Secret

Step 7 On the **Rotate Now** page, click **OK**. If a message indicating rotation success is displayed in the upper right corner, the version switchover is complete.

Step 8 After the version rotation is complete, the version whose status is **SYSCURRENT** is the latest secret version.

----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.

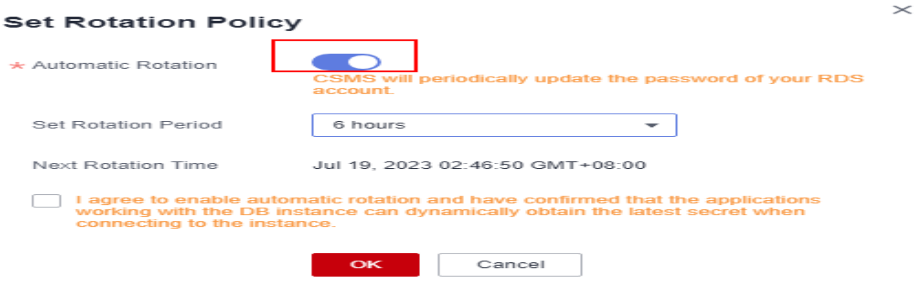
Step 3 Click . Choose **Security & Compliance** > **Data Encryption Workshop**.

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

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

Step 6 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 2-17**.

Figure 2-17 Automatic rotation



Set Rotation Policy

* Automatic Rotation

CSMS will periodically update the password of your RDS account.

Set Rotation Period: 6 hours

Next Rotation Time: Jul 19, 2023 02:46:50 GMT+08:00

□ I agree to enable automatic rotation and have confirmed that the applications working with the DB instance can dynamically obtain the latest secret when connecting to the instance.

Step 7 Set the rotation period and click **OK**. A message indicating the rotation policy is set successfully is displayed in the upper right corner.

----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.

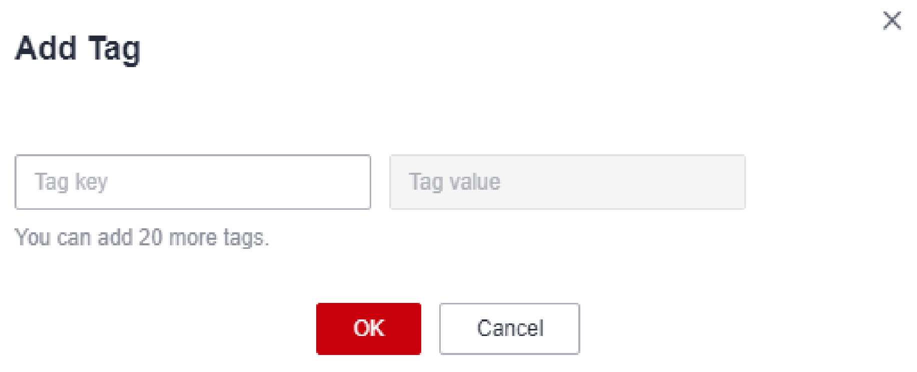
Step 3 Click ☰. Choose **Security & Compliance** > **Data Encryption Workshop**.

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

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

Step 6 In the **Tags** area, click **Add Tag**. In the **Add Tag** dialog box, enter the tag key and tag value. **Table 2-5** describes the parameters.

Figure 2-18 Add a tag



You can add 20 more tags.

NOTE

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

Table 2-5 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.	● 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: – Chinese – English – Numbers – Space – Special characters: _.:/=+-@
Tag value	Value of the tag	● Optional ● 255 characters limit. ● The following character types are allowed: – Chinese – English – Numbers – Space – Special characters: _.:/=+-@

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.

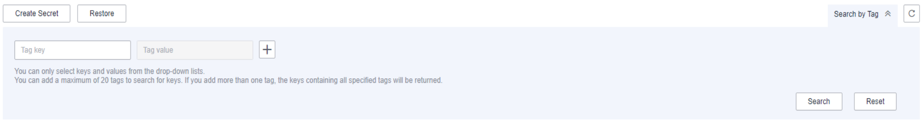
Step 2 Click in the upper left corner of the management console and select a region or project.

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

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

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

Figure 2-19 Search box

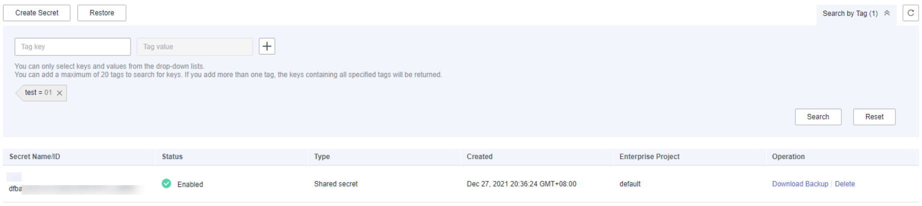


You can only select keys and values from the drop-down lists.
You can add a maximum of 20 tags to search for keys. If you add more than one tag, the keys containing all specified tags will be returned.

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 2-20.

Figure 2-20 Search result



You can only select keys and values from the drop-down lists.
You can add a maximum of 20 tags to search for keys. If you add more than one tag, the keys containing all specified tags will be returned.

Secret Name/ID	Status	Type	Created	Enterprise Project	Operation
dfba[redacted]	Enabled	Shared secret	Dec 27, 2021 20:36:24 GMT+08:00	default	Download Backup | Delete

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.

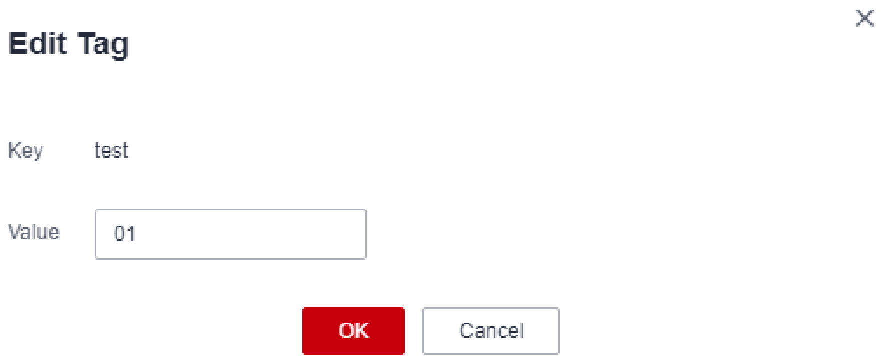
Step 3 Click ☰. Choose **Security & Compliance** > **Data Encryption Workshop**.

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

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

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

Figure 2-21 Editing a tag



Edit Tag

Key test

Value 01

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.

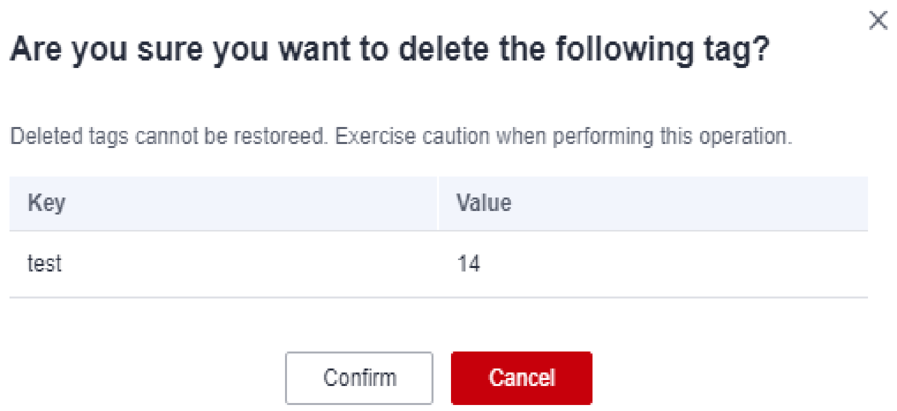
Step 3 Click ☰. Choose **Security & Compliance** > **Data Encryption Workshop**.

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

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

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

Figure 2-22 Deleting a tag



Are you sure you want to delete the following tag?

Deleted tags cannot be restoreed. Exercise caution when performing this operation.

Key	Value
test	14

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

----End

2.7 Creating an Event

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**.

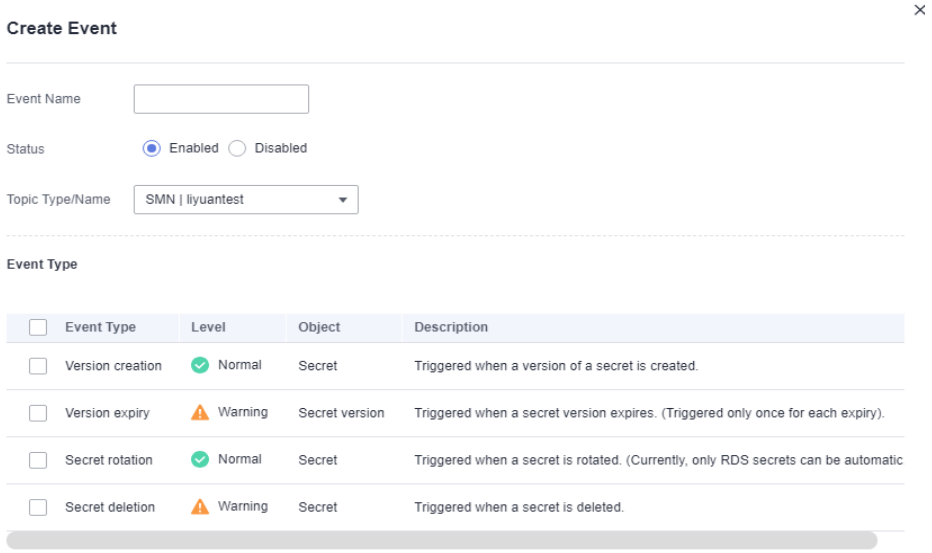
Step 2 Click 📍 in the upper left corner of the management console and select a region or project.

Step 3 Click ☰. 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. The page for creating an event is displayed, as shown in **Creating an event**.

Figure 2-23 Creating an event



Create Event

Event Name

Status ● Enabled ○ Disabled

Topic Type/Name SMN | liyuantest

Event Type

□	Event Type	Level	Object	Description
□	Version creation	✓ Normal	Secret	Triggered when a version of a secret is created.
□	Version expiry	⚠ Warning	Secret version	Triggered when a secret version expires. (Triggered only once for each expiry).
□	Secret rotation	✓ Normal	Secret	Triggered when a secret is rotated. (Currently, only RDS secrets can be automatic
□	Secret deletion	⚠ Warning	Secret	Triggered when a secret is deleted.

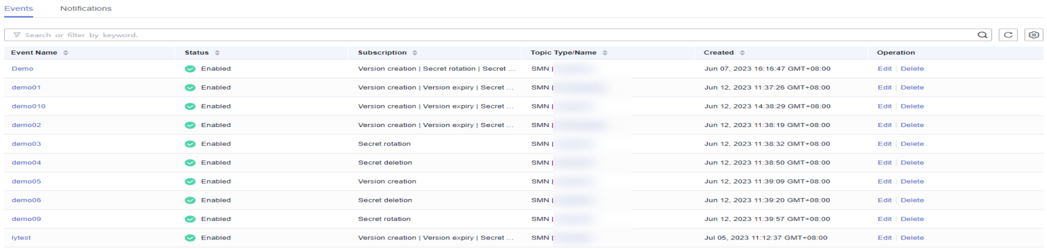
Table 2-6 Parameters for creating an event

Parameter	Description
Event Name	Name of the event to be created.
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**, **Secret rotation**, and **Secret deletion**.

Step 6 Click **OK**.

Step 7 View the created event in the event list, as shown in **Figure 2-24**. The default event status is **Enabled**.

Figure 2-24 Event list



Events | Notifications

Search or filter by keyword.

Event Name	Status	Subscription	Topic Type/Name	Created	Operation
Demo	Enabled	Version creation | Secret rotation | Secret ...	SMN | [redacted]	Jun 07, 2023 16:16:47 GMT+08:00	Edit | Delete
demo01	Enabled	Version creation | Version expiry | Secret ...	SMN | [redacted]	Jun 12, 2023 11:37:26 GMT+08:00	Edit | Delete
demo010	Enabled	Version creation | Version expiry | Secret ...	SMN | [redacted]	Jun 12, 2023 14:38:29 GMT+08:00	Edit | Delete
demo02	Enabled	Version creation | Version expiry | Secret ...	SMN | [redacted]	Jun 12, 2023 11:38:19 GMT+08:00	Edit | Delete
demo03	Enabled	Secret rotation	SMN | [redacted]	Jun 12, 2023 11:38:32 GMT+08:00	Edit | Delete
demo04	Enabled	Secret deletion	SMN | [redacted]	Jun 12, 2023 11:38:50 GMT+08:00	Edit | Delete
demo05	Enabled	Version creation	SMN | [redacted]	Jun 12, 2023 11:39:09 GMT+08:00	Edit | Delete
demo06	Enabled	Secret deletion	SMN | [redacted]	Jun 12, 2023 11:39:20 GMT+08:00	Edit | Delete
demo09	Enabled	Secret rotation	SMN | [redacted]	Jun 12, 2023 11:39:57 GMT+08:00	Edit | Delete
lytest	Enabled	Version creation | Version expiry | Secret ...	SMN | [redacted]	Jul 05, 2023 11:12:37 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.

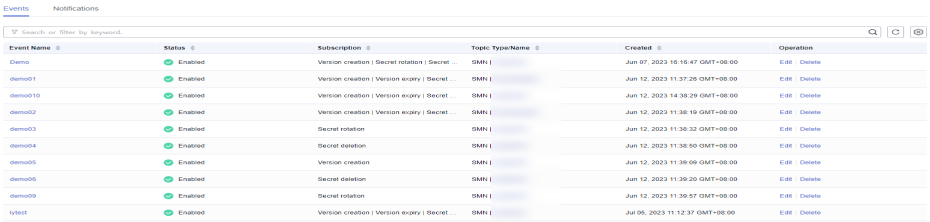
Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 Click ☰. 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 2-25 Event list



Events | Notifications

Search or filter by keyword.

Event Name	Status	Subscription	Topic Type/Name	Created	Operation
Demo	Enabled	Version creation | Secret rotation | Secret ...	SMN | [redacted]	Jun 07, 2023 16:16:47 GMT+08:00	Edit | Delete
demo01	Enabled	Version creation | Version expiry | Secret ...	SMN | [redacted]	Jun 12, 2023 11:37:26 GMT+08:00	Edit | Delete
demo010	Enabled	Version creation | Version expiry | Secret ...	SMN | [redacted]	Jun 12, 2023 14:38:29 GMT+08:00	Edit | Delete
demo02	Enabled	Version creation | Version expiry | Secret ...	SMN | [redacted]	Jun 12, 2023 11:38:19 GMT+08:00	Edit | Delete
demo03	Enabled	Secret rotation	SMN | [redacted]	Jun 12, 2023 11:38:32 GMT+08:00	Edit | Delete
demo04	Enabled	Secret deletion	SMN | [redacted]	Jun 12, 2023 11:38:50 GMT+08:00	Edit | Delete
demo05	Enabled	Version creation	SMN | [redacted]	Jun 12, 2023 11:39:09 GMT+08:00	Edit | Delete
demo06	Enabled	Secret deletion	SMN | [redacted]	Jun 12, 2023 11:39:20 GMT+08:00	Edit | Delete
demo09	Enabled	Secret rotation	SMN | [redacted]	Jun 12, 2023 11:39:57 GMT+08:00	Edit | Delete
lytest	Enabled	Version creation | Version expiry | Secret ...	SMN | [redacted]	Jul 05, 2023 11:12:37 GMT+08:00	Edit | Delete

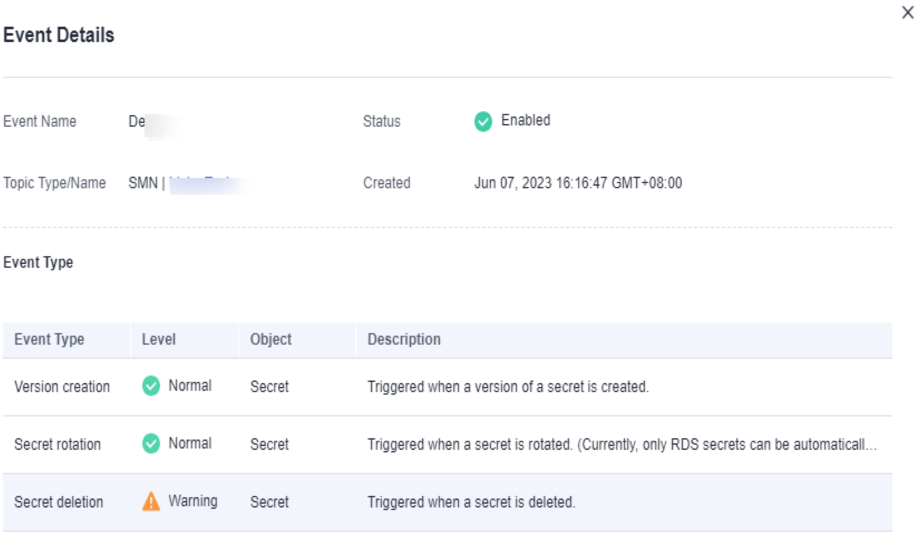
Table 2-7 Parameters in the event list

Parameter	Description
Event Name	Name of an event

Parameter	Description
Status	Event status, including: - **Enabled** The event is enabled. - **Disabled** The event is disabled.
Subscription	Event type selected during event creation. The options are as follows: - **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 name of an event name to view the event details, as shown in **Figure 2-26**.

Figure 2-26 Event details



Event Details

Event Name De[redacted]

Status ✓ Enabled

Topic Type/Name SMN | [redacted]

Created Jun 07, 2023 16:16:47 GMT+08:00

Event Type

Event Type	Level	Object	Description
Version creation	✓ Normal	Secret	Triggered when a version of a secret is created.
Secret rotation	✓ Normal	Secret	Triggered when a secret is rotated. (Currently, only RDS secrets can be automaticall...
Secret deletion	⚠ Warning	Secret	Triggered when a secret is deleted.

----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.

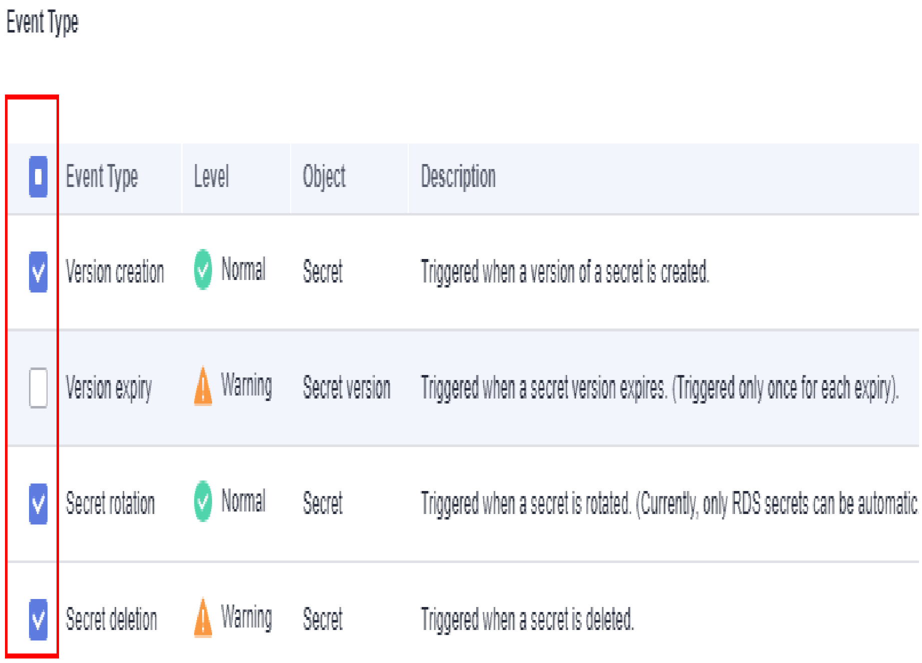
Step 3 Click ☰. Choose **Security & Compliance** > **Data Encryption Workshop**.

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

Step 5 Click **Edit** in the **Operation** column of the target event. The **Edit Event** page is displayed.

Step 6 Select the target event type, as shown in **Figure 2-27**.

Figure 2-27 Editing an event



Event Type

■	Event Type	Level	Object	Description
☑	Version creation	✓ Normal	Secret	Triggered when a version of a secret is created.
☐	Version expiry	⚠ Warning	Secret version	Triggered when a secret version expires. (Triggered only once for each expiry).
☑	Secret rotation	✓ Normal	Secret	Triggered when a secret is rotated. (Currently, only RDS secrets can be automatic
☑	Secret deletion	⚠ Warning	Secret	Triggered when a secret is deleted.

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.

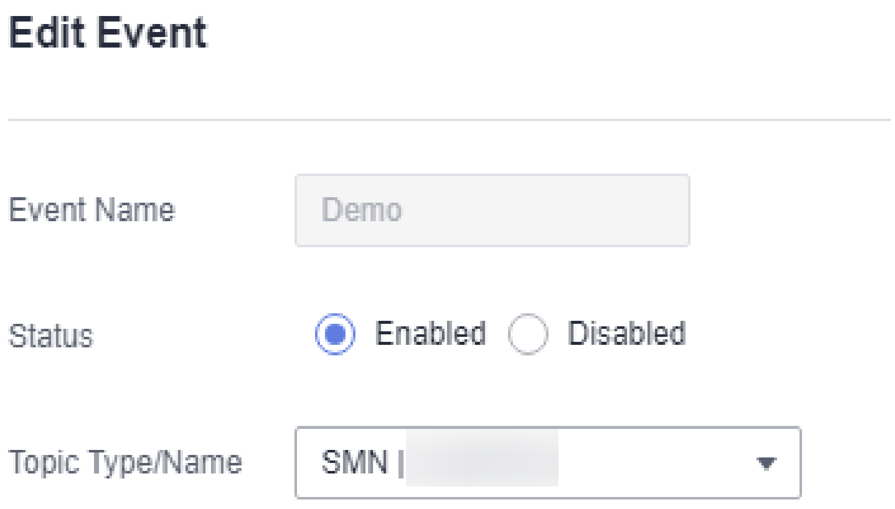
Step 3 Click ☰. Choose **Security & Compliance** > **Data Encryption Workshop**.

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

Step 5 Click **Edit** in the **Operation** column of the target event. The **Edit Event** page is displayed.

Step 6 Select **Enabled** for **Status**.

Figure 2-28 Enabling an event



Edit Event

Event Name: Demo

Status: ● Enabled ○ Disabled

Topic Type/Name: SMN | [redacted]

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.

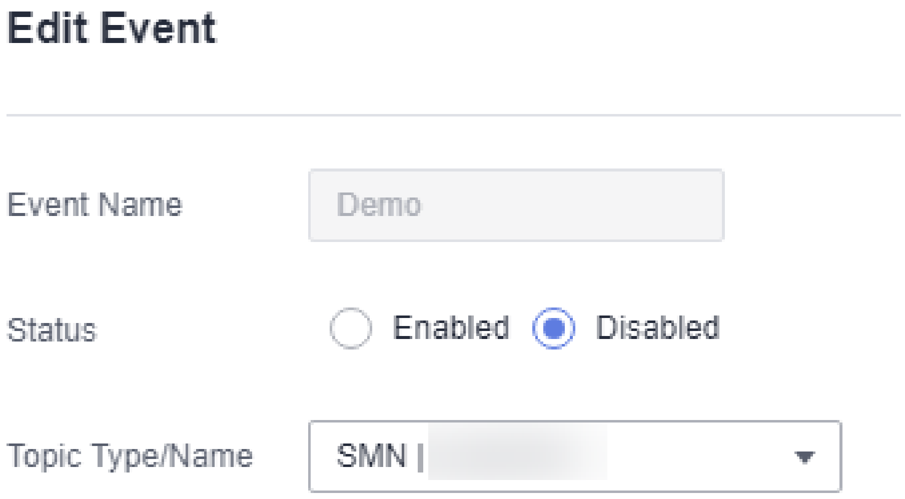
Step 3 Click ☰. Choose **Security & Compliance** > **Data Encryption Workshop**.

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

Step 5 Click **Edit** in the **Operation** column of the target event. The **Edit Event** page is displayed.

Step 6 Select **Disabled** for **Status**.

Figure 2-29 Disabling an event



Edit Event

Event Name: Demo

Status: ○ Enabled ● Disabled

Topic Type/Name: SMN | [redacted]

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.

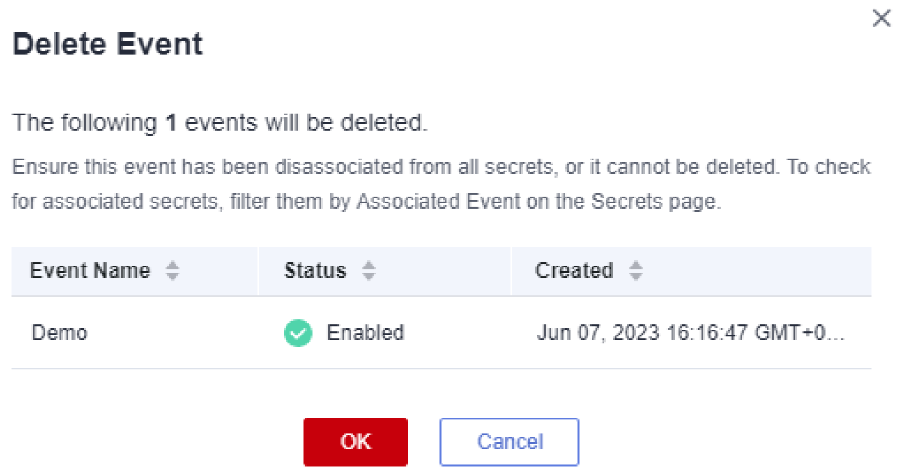
Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 Click ☰. 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.

Figure 2-30 Deleting an event



Delete Event

The following 1 events will be deleted.

Ensure this event has been disassociated from all secrets, or it cannot be deleted. To check for associated secrets, filter them by Associated Event on the Secrets page.

Event Name	Status	Created
Demo	✓ Enabled	Jun 07, 2023 16:16:47 GMT+0...

Step 6 Click **OK**.

----End

2.9 Viewing Notifications

This section describes how to view the event notifications.

Procedure

Step 1 **Log in to the management console**.

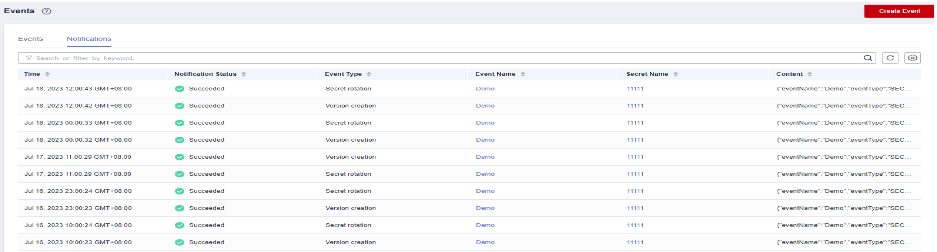
Step 2 Click 📍 in the upper left corner of the management console and select a region or project.

Step 3 Click ☰. 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 the **Notifications** tab. The page for viewing notifications is displayed, as shown in **Figure 2-31**.

Figure 2-31 Viewing notifications



Time	Notification Status	Event Type	Event Name	Secret Name	Content
Jul 18, 2023 12:00:43 GMT+08:00	Succeeded	Secret rotation	Demo	11111	{"eventName":"Demo","eventType":"SEC...
Jul 18, 2023 12:00:42 GMT+08:00	Succeeded	Version creation	Demo	11111	{"eventName":"Demo","eventType":"SEC...
Jul 18, 2023 00:00:33 GMT+08:00	Succeeded	Secret rotation	Demo	11111	{"eventName":"Demo","eventType":"SEC...
Jul 18, 2023 00:00:32 GMT+08:00	Succeeded	Version creation	Demo	11111	{"eventName":"Demo","eventType":"SEC...
Jul 17, 2023 11:00:29 GMT+08:00	Succeeded	Version creation	Demo	11111	{"eventName":"Demo","eventType":"SEC...
Jul 17, 2023 11:00:29 GMT+08:00	Succeeded	Secret rotation	Demo	11111	{"eventName":"Demo","eventType":"SEC...
Jul 16, 2023 23:00:24 GMT+08:00	Succeeded	Secret rotation	Demo	11111	{"eventName":"Demo","eventType":"SEC...
Jul 16, 2023 23:00:23 GMT+08:00	Succeeded	Version creation	Demo	11111	{"eventName":"Demo","eventType":"SEC...
Jul 16, 2023 10:00:24 GMT+08:00	Succeeded	Secret rotation	Demo	11111	{"eventName":"Demo","eventType":"SEC...
Jul 16, 2023 10:00:23 GMT+08:00	Succeeded	Version creation	Demo	11111	{"eventName":"Demo","eventType":"SEC...

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

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

NOTE

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

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

- Creating a key pair on the management console

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

  NOTE

  - The key pair created on the management console uses the **SSH-2 (RSA, 2048)** encryption and decryption algorithm.
  - Key pairs created by an IAM user on the management console can be used only by the user. If multiple IAM users need to use the same key pair, you can create an account key pair.

- Creating a key pair using the PuTTYgen tool

  Both the public key and private key can be stored on the local host. For details, see **Creating a Key Pair Using PuTTYgen**.

  NOTE

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

Prerequisites

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

Creating a Key Pair Using the Management Console

Step 1 Log in to the management console.

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

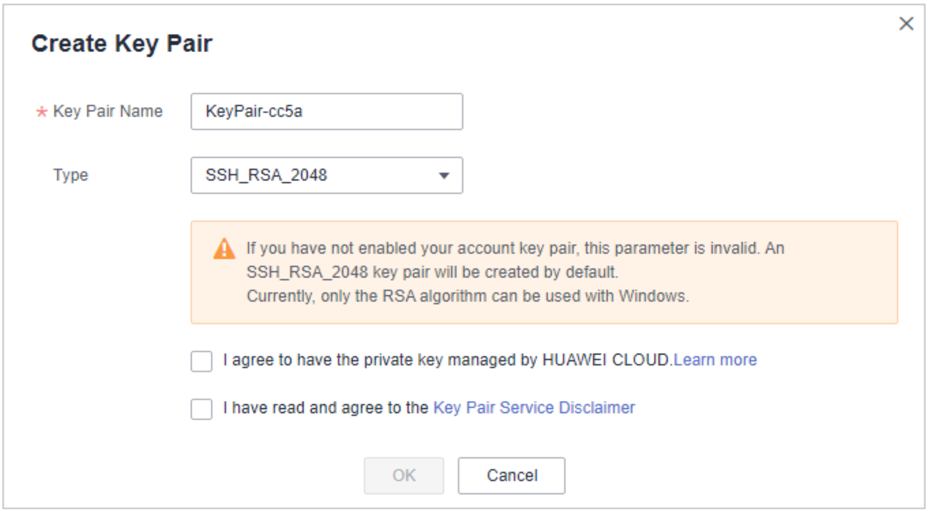
Step 3 Click ☰. Choose **Security & Compliance** > **Data Encryption Workshop**.

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

Step 5 Click **Create Key Pair**.

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

Figure 3-1 Creating a key pair



Create Key Pair

* Key Pair Name: KeyPair-cc5a

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 have the private key managed by HUAWEI CLOUD.Learn more

□ I have read and agree to the 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

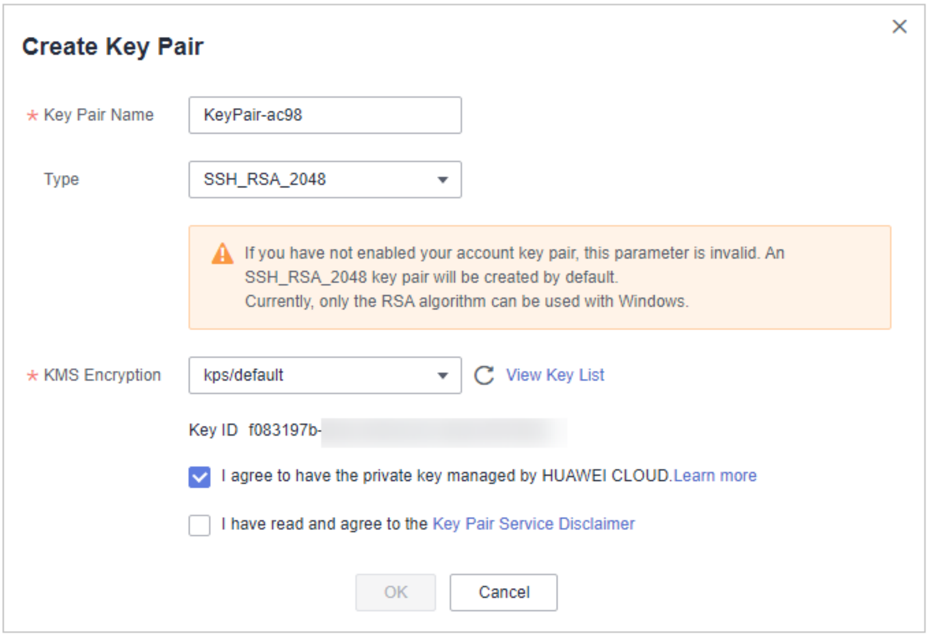
Currently, only the RSA algorithm can be used with Windows.

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

NOTE

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

Figure 3-2 Managing private keys



Create Key Pair

* Key Pair Name: KeyPair-ac98

Type: SSH_RSA_2048

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

* KMS Encryption: kps/default

Key ID f083197b-[redacted]

☑ I agree to have the private key managed by HUAWEI CLOUD.Learn more

□ I have read and agree to the Key Pair Service Disclaimer

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

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

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

NOTICE

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

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

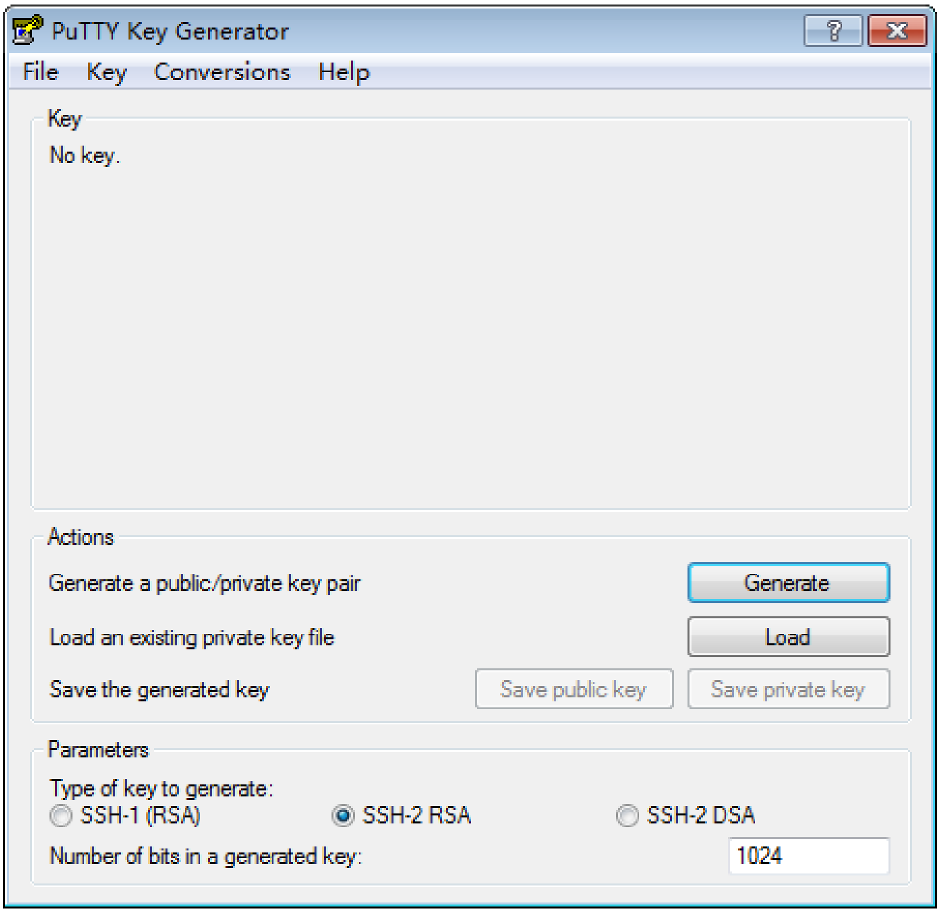
After the key pair is created, you can view it in the list of key pairs. The list displays information such as key pair name, fingerprint, private key, and quantity.

----End

Creating a Key Pair Using PuTTYgen

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

Figure 3-3 PuTTY Key Generator



No key.

Generate a public/private key pair

Load an existing private key file

Save the generated key

Type of key to generate:
○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 1024

Step 2 Configure the parameters as described in **Table 3-1**.

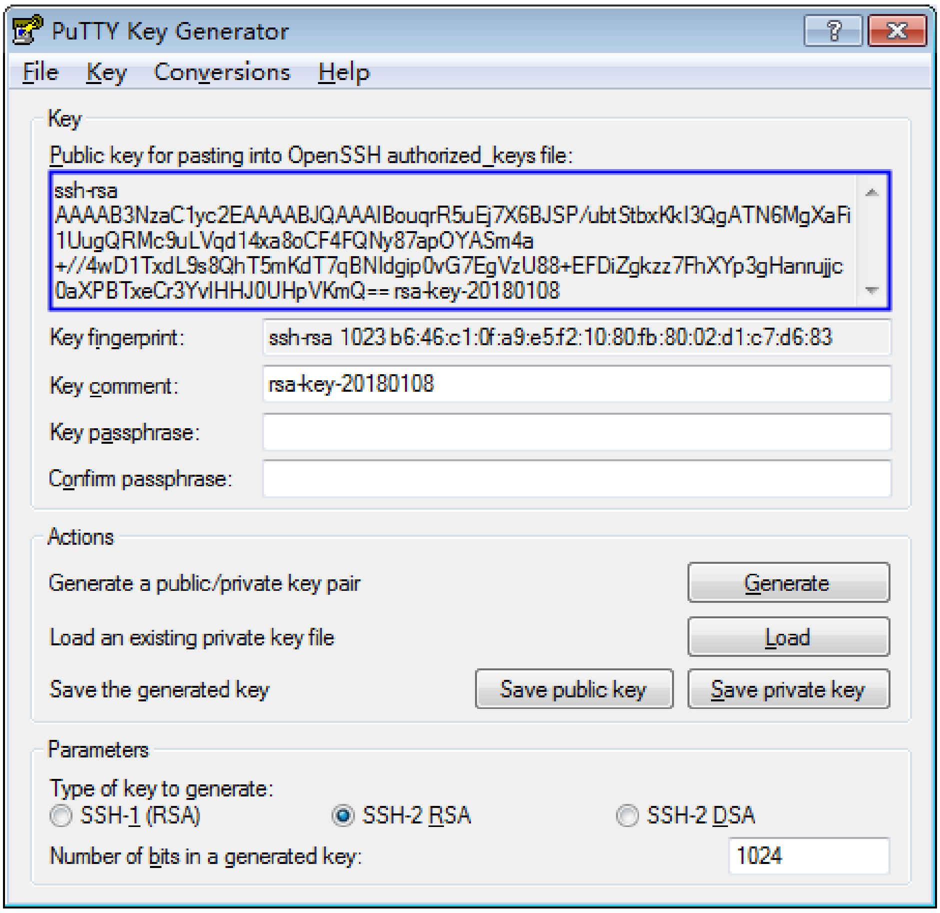
Table 3-1 Parameter description

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



Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAIBouqrR5uEj7X6BJSP/ubtStbxKkI3QgATN6MgXaFi
1UugQRMc9uLVqd14xa8oCF4FQNy87apOYASm4a
+//4wD1TxdL9s8QhT5mKdT7qBNIdgip0vG7EgVzU88+EFDiZgkzz7FhXYp3gHanrujjc
0aXPBTxeCr3YvIHHJ0UHpVKmQ== rsa-key-20180108
```

Key fingerprint: ssh-rsa 1023 b6:46:c1:0f:a9:e5:f2:10:80:fb:80:02:d1:c7:d6:83

Key comment: rsa-key-20180108

Key passphrase:

Confirm passphrase:

Generate a public/private key pair — Generate

Load an existing private key file — Load

Save the generated key — Save public key — Save private key

Type of key to generate:
○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 1024

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

NOTICE

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

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

NOTICE

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

Table 3-2 Format of a private key file

Private Key File Format	Private Key Usage Scenario	Saving Method
PEM	● Use the Xshell tool to log in to the cloud server running the Linux operating system. ● Manage the private key on the management console.	1. Choose **Conversions** > **Export OpenSSH key**. 2. 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.	1. Choose **Conversions** > **Export OpenSSH key**. NOTE Do not enter the **Key passphrase** information. Otherwise, the password fails to be obtained. 2. 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.	1. On the **PuTTY Key Generator** page, choose **File** > **Save private key**. 2. Save the private key, for example, **kp-123.ppk**, to a local directory.

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

----End

3.2 Importing a Key Pair

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

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

Prerequisites

- The public and private key files of the key pair to be imported are ready.
- The imported key pair is an account key pair. If a private key pair with the same name has been created, the system displays a message indicating that the key pair name already exists when you import the account key pair.

- Each IAM user does not have a private key pair with the same name.

Constraints

- The SSH keys imported to the KPS console support the following cryptographic algorithms:
  - SSH-DSS
  - SSH-ED25519
  - ECDSA-SHA2-NISTP256
  - ECDSA-SHA2-NISTP384
  - ECDSA-SHA2-NISTP521
  - SSH_RSA: The length can be 2048, 3072, 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?**

Procedure

Step 1 **Log in to the management console**.

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

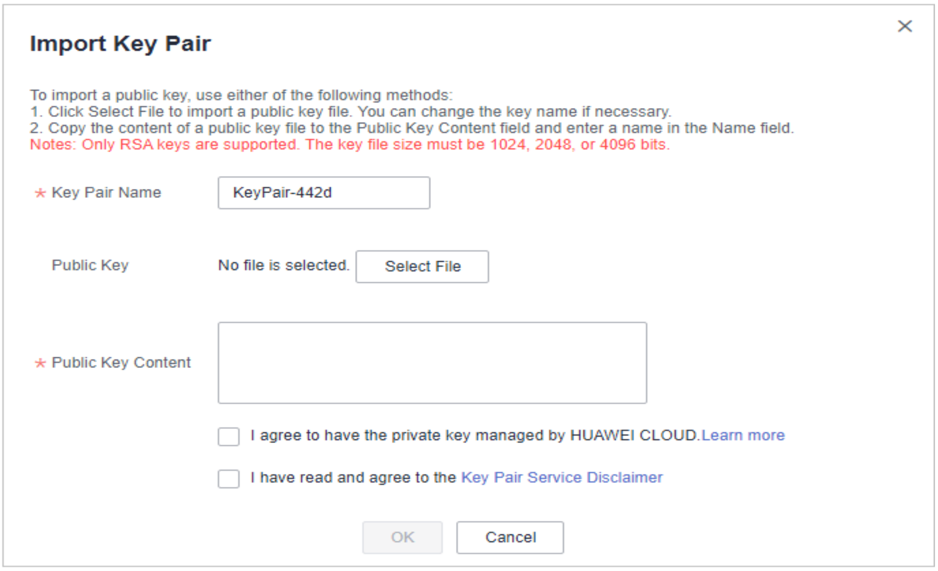
Step 3 Click ☰. Choose **Security & Compliance** > **Data Encryption Workshop**.

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

Step 5 Click **Import Key Pair**.

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

Figure 3-5 Importing a key pair



Import Key Pair

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

* Key Pair Name: KeyPair-442d

Public Key: No file is selected.

* Public Key Content:

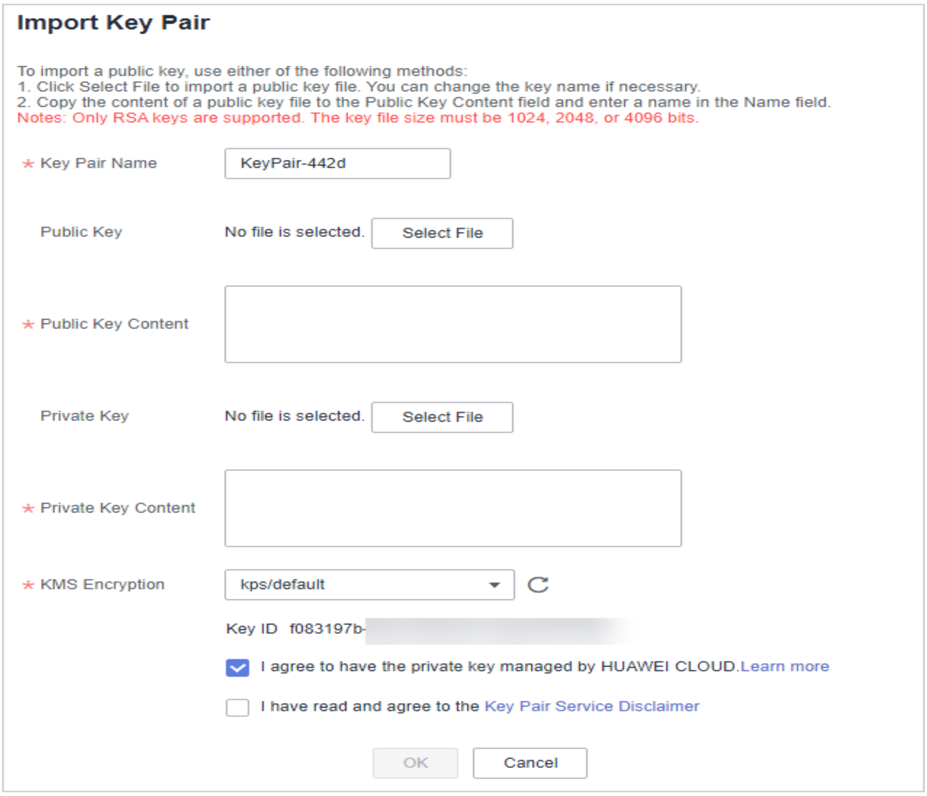
×
Select File
□ I agree to have the private key managed by HUAWEI CLOUD.Learn more
□ I have read and agree to the Key Pair Service Disclaimer
OK
Cancel

NOTE

- You can customize the name of an imported key pair.
- If the system displays a message indicating that the name already exists, you need to change the key pair name because the name has been created by another IAM user.

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

Figure 3-6 Managing private keys



Import Key Pair

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

* Key Pair Name	KeyPair-442d
Public Key	No file is selected. Select File
* Public Key Content	
Private Key	No file is selected. Select File
* Private Key Content	
* KMS Encryption	kps/default
	Key ID f083197b-[redacted]

☑ I agree to have the private key managed by HUAWEI CLOUD.Learn more

□ I have read and agree to the Key Pair Service Disclaimer

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

   NOTE

   – KPS uses the encryption key provided by KMS to encrypt private keys. When the user uses the KMS encryption function of the key pair, KMS automatically creates a default master key **kps/default** for encryption of the key pair.

   – You can select an existing encryption key or click **View Key List** to create one.

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

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

----End

3.3 Upgrading a Key Pair

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

Prerequisites

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

Procedure

Step 1 Log in to the management console.

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

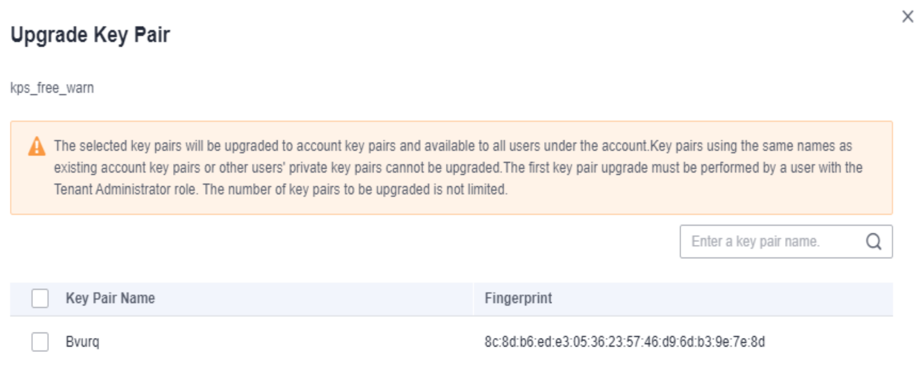
Step 3 Click ☰. Choose **Security & Compliance** > **Data Encryption Workshop**.

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

Step 5 Click **Upgrade Key Pair**.

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

Figure 3-7 Upgrading a key pair



Upgrade Key Pair ×

kps_free_warn

⚠ The selected key pairs will be upgraded to account key pairs and available to all users under the account.Key pairs using the same names as existing account key pairs or other users' private key pairs cannot be upgraded.The first key pair upgrade must be performed by a user with the Tenant Administrator role. The number of key pairs to be upgraded is not limited.

Enter a key pair name.

□ Key Pair Name	Fingerprint
□ Bvurq	8c:8d:b6:ed:e3:05:36:23:57:46:d9:6d:b3:9e:7e:8d

NOTE

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

----End

3.4 Managing Key Pairs

3.4.1 Binding a Key Pair

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

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

Prerequisites

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

Constraints

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

Binding a Key Pair

Step 1 Log in to the management console.

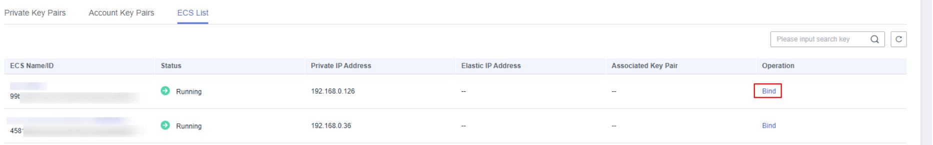
Step 2 Click 📍 in the upper left corner of the management console and select a region or project.

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

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

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

Figure 3-8 Binding

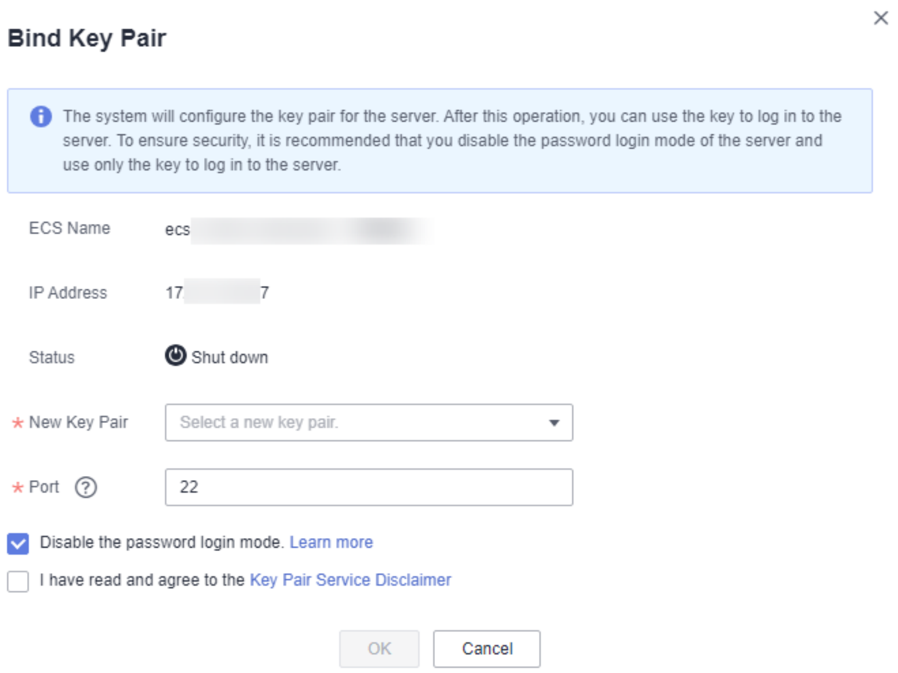


ECS Name/ID	Status	Private IP Address	Elastic IP Address	Associated Key Pair	Operation
99[redacted]	Running	192.168.0.126	--	--	Bind
458[redacted]	Running	192.168.0.36	--	--	Bind

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

- If the ECS is shut down, a dialog box will be displayed, as shown in **Figure 3-9**.

Figure 3-9 Binding a key pair (1)



Bind Key Pair

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

ECS Name ecs[redacted]

IP Address 17[redacted]7

Status Shut down

* New Key Pair: Select a new key pair.

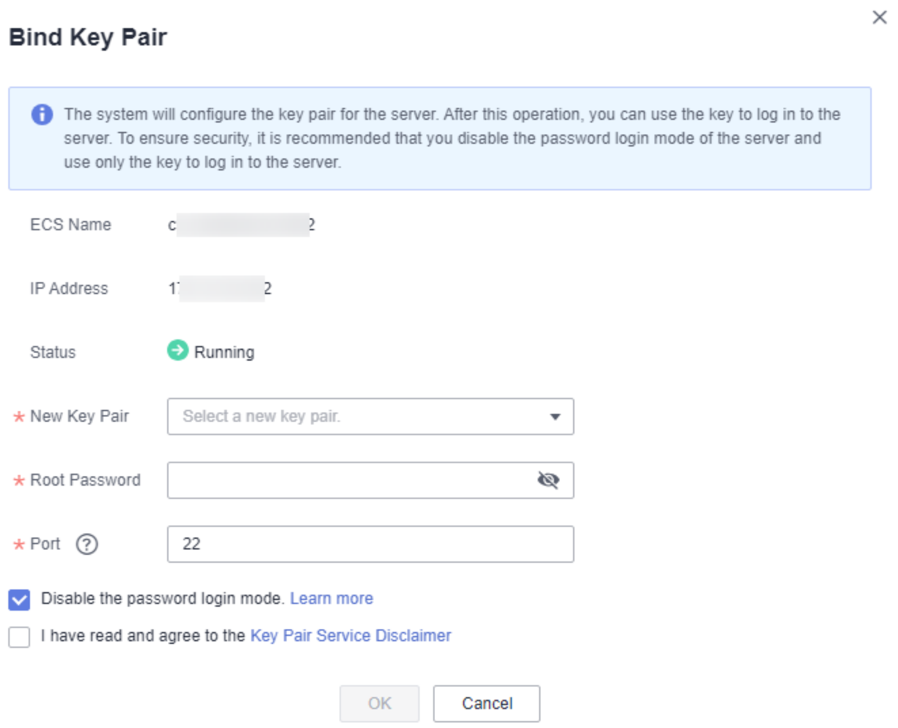
* Port: 22

☑ Disable the password login mode. Learn more

□ I have read and agree to the Key Pair Service Disclaimer

- If the ECS is running, you need to provide the root password. See **Figure 3-10**.

Figure 3-10 Binding a key pair (2)



Bind Key Pair

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

ECS Name c[redacted]2

IP Address 1[redacted]2

Status Running

* New Key Pair: Select a new key pair.

* Root Password:

* Port: 22

☑ Disable the password login mode. Learn more

□ I have read and agree to the Key Pair Service Disclaimer

NOTE

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

3.4.2 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 different key pairs.

Prerequisites

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

Constraints

- On the management console, key pairs cannot be bound to ECSs that run Windows.
- Key pairs cannot be bound to public images running CoreOS, OpenEuler, FreeBSD (Other), Kylin V10 64-bit, or UnionTech OS Server 20 Euler 64-bit.
- You can bind key pairs to a maximum of 10 ECSs at a time.

Procedure

Step 1 Log in to the management console.

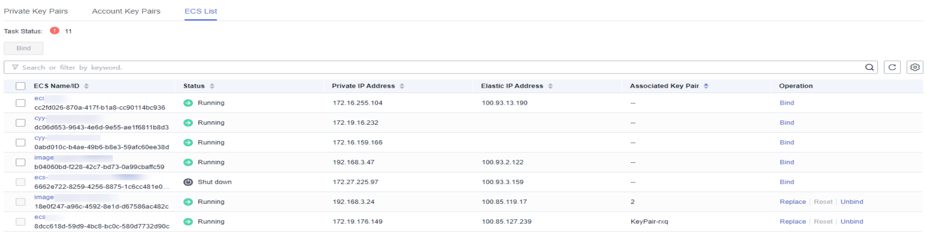
Step 2 Click in the upper left corner of the management console and select a region or project.

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

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

Step 5 Click **ECS List**. The ECS list page is displayed, as shown in **Figure 3-11**.

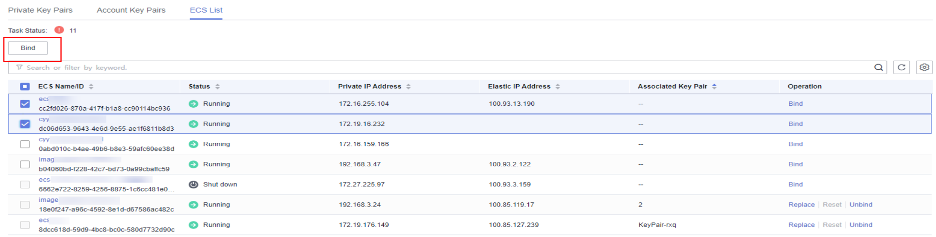
Figure 3-11 ECS list



□	ECS Name/ID	Status	Private IP Address	Elastic IP Address	Associated Key Pair	Operation
□	ecs [redacted] cc2fd026-870a-417f-b1a8-cc90114bc936	Running	172.16.255.104	100.93.13.190	--	Bind
□	cyy-[redacted] dc06d653-9643-4e6d-9e55-ae1f6811b8d3	Running	172.19.16.232		--	Bind
□	cyy-[redacted] 0abd010c-b4ae-49b6-b8e3-59afc60ee38d	Running	172.16.159.166		--	Bind
□	image[redacted] b04060bd-f228-42c7-bd73-0a99cbaffc59	Running	192.168.3.47	100.93.2.122	--	Bind
□	ecs-[redacted] 6662e722-8259-4256-8875-1c6cc481e0...	Shut down	172.27.225.97	100.93.3.159	--	Bind
□	image[redacted] 18e0f247-a96c-4592-8e1d-d67586ac482c	Running	192.168.3.24	100.85.119.17	2	Replace | Reset | Unbind
□	ecs[redacted] 8dcc618d-59d9-4bc8-bc0c-580d7732d90c	Running	172.19.176.149	100.85.127.239	KeyPair-rxq	Replace | Reset | Unbind

Step 6 Select the servers to be bound in batches and click **Bind** above the search box, as shown in **Binding key pairs in batches**.

Figure 3-12 Binding key pairs in batches

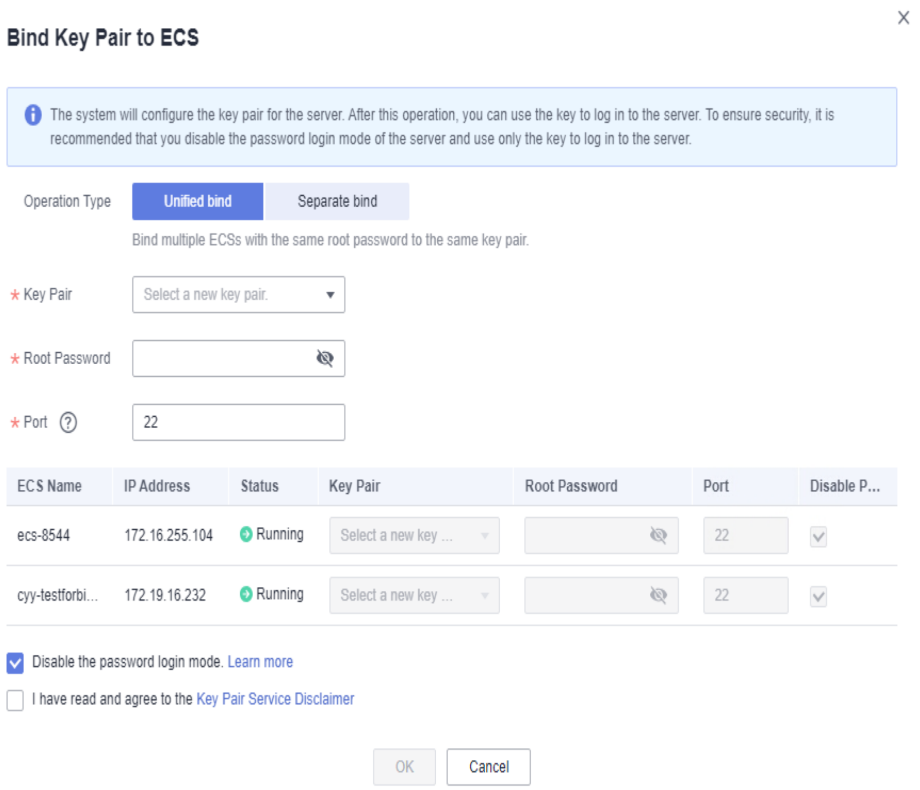


■	ECS Name/ID	Status	Private IP Address	Elastic IP Address	Associated Key Pair	Operation
☑	ecs[redacted] cc2fd026-870a-417f-b1a8-cc90114bc936	Running	172.16.255.104	100.93.13.190	--	Bind
☑	cyy[redacted] dc06d653-9643-4e6d-9e55-ae1f6811b8d3	Running	172.19.16.232		--	Bind
□	cyy[redacted] 0abd010c-b4ae-49b6-b8e3-59afc60ee38d	Running	172.16.159.166		--	Bind
□	imag[redacted] b04060bd-f228-42c7-bd73-0a99cbaffc59	Running	192.168.3.47	100.93.2.122	--	Bind
□	ecs-[redacted] 6662e722-8259-4256-8875-1c6cc481e0...	Shut down	172.27.225.97	100.93.3.159	--	Bind
□	image[redacted] 18e0f247-a96c-4592-8e1d-d67586ac482c	Running	192.168.3.24	100.85.119.17	2	Replace | Reset | Unbind
□	ecs[redacted] 8dcc618d-59d9-4bc8-bc0c-580d7732d90c	Running	172.19.176.149	100.85.127.239	KeyPair-rxq	Replace | Reset | Unbind

Step 7 Click **Bind**. The **Bind Key Pair to ECS** dialog box is displayed.

- 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, as shown in **Figure 3-13**.

Figure 3-13 Unified bind



Bind Key Pair to ECS

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

Operation Type: Unified bind | Separate bind

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

* Key Pair: Select a new key pair.

* Root Password:

* Port: 22

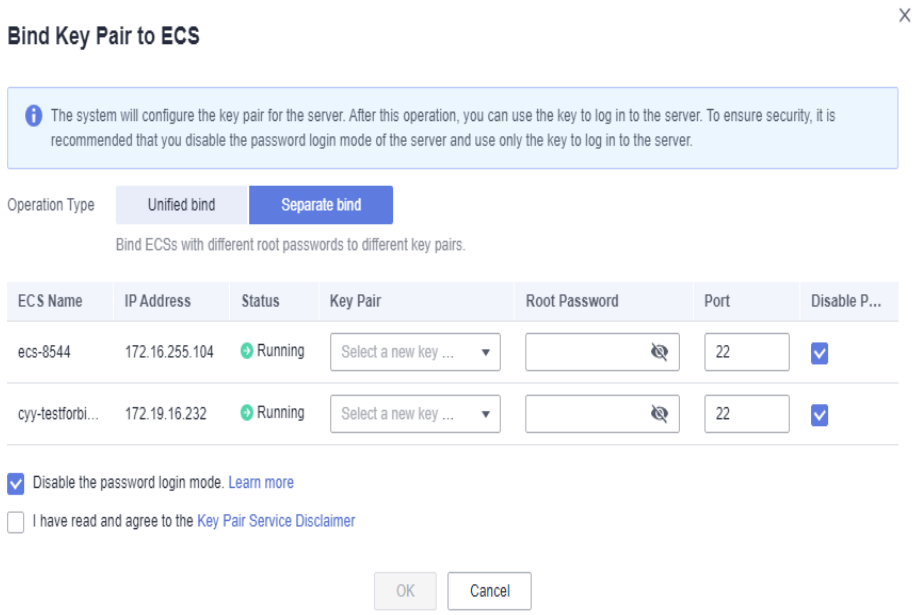
ECS Name	IP Address	Status	Key Pair	Root Password	Port	Disable P...
ecs-8544	172.16.255.104	Running	Select a new key ...		22	✓
cyy-testforbi...	172.19.16.232	Running	Select a new key ...		22	✓

☑ 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, as shown in **Figure 3-14**.

Figure 3-14 Separate bind



Bind Key Pair to ECS

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

Operation Type: Unified bind | Separate bind

Bind ECSs with different root passwords to different key pairs.

ECS Name	IP Address	Status	Key Pair	Root Password	Port	Disable P...
ecs-8544	172.16.255.104	Running	Select a new key ...		22	☑
cyy-testforbi...	172.19.16.232	Running	Select a new key ...		22	☑

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

Step 11 Click **OK**. The key pairs are bound in batches. The binding takes about 3 to 5 minutes.

----End

3.4.3 Viewing a Key Pair

This section describes how to view the key pair information, including the names, fingerprints, private keys, and used keys on the KPS page of the DEW console.

Procedure

Step 1 **Log in to the management console**.

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

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

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

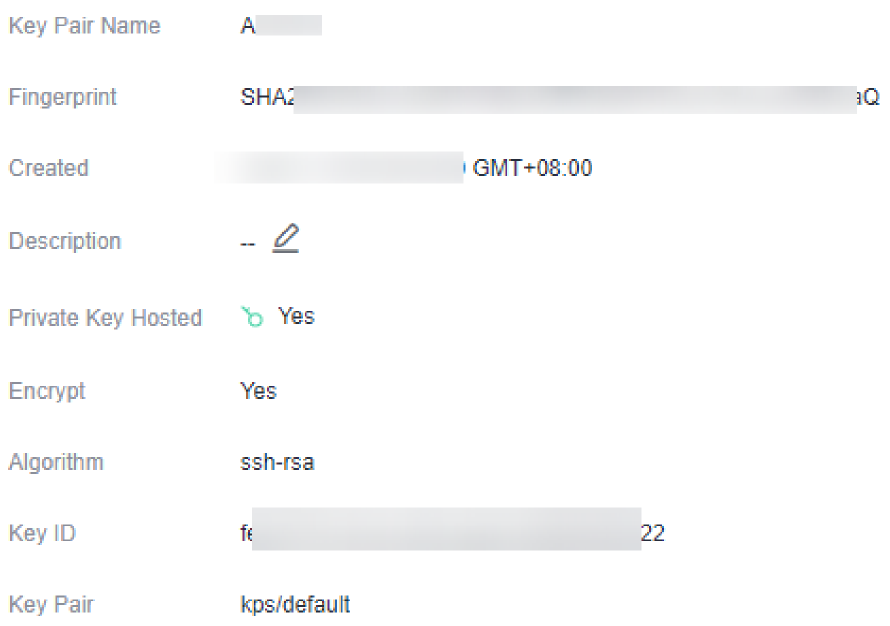
Step 5 Click the **Private Key Pairs** tab and view information about the key pair in the key pair list.

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.

Figure 3-15 Key pair details



Key Pair Name	A[redacted]
Fingerprint	SHA[redacted]Q
Created	[redacted] GMT+08:00
Description	--
Private Key Hosted	Yes
Encrypt	Yes
Algorithm	ssh-rsa
Key ID	f[redacted]22
Key Pair	kps/default

NOTE

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

Bind a key pair to ECSs. For details about parameters, see **Table 3-3**.

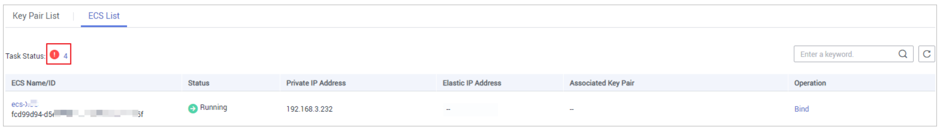
Table 3-3 Parameter description

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

Parameter	Description
Status	Statuses of an ECS are as follows: ● Running ● Creating ● Faulty ● Shut down ● DELETE ● HARD_REBOOT ● MIGRATING ● REBOOT ● RESIZE ● REVERT_RESIZE ● SHELVED ● SHELVED_OFF ● LOADED ● UNKNOWN ● VERIFY_RESIZE
Private IP address	Private IP Address
EIP	Elastic IP address
Bound key pair	Key pair that is bound to the ECS

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

Figure 3-16 ECS list



Task Status: ! 4

ECS Name/ID	Status	Private IP Address	Elastic IP Address	Associated Key Pair	Operation
ecs-[redacted] fcd99d94-d5[redacted]5f	Running	192.168.3.232	--	--	Bind

Step 8 Click the number next to the task status icon ! to view failed tasks, as shown in **Figure 3-17**.

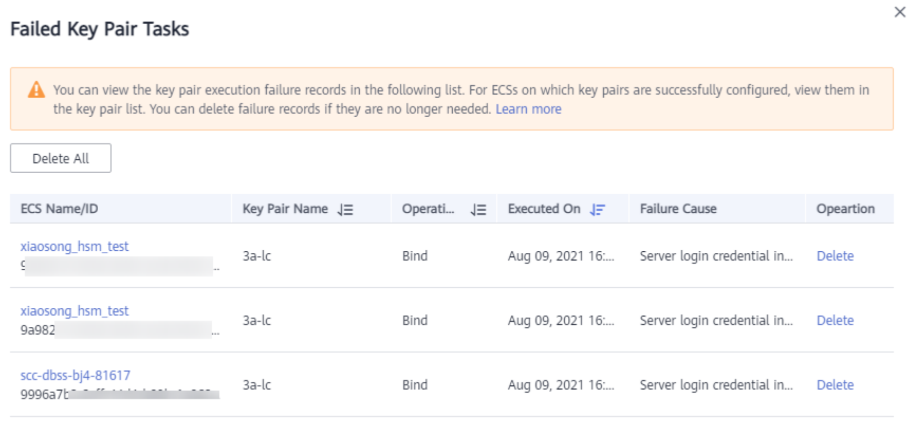
NOTE

Status of resetting or replacing the key pair:

: Executing

!: Execution failed

Figure 3-17 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

ECS Name/ID	Key Pair Name	Operati...	Executed On	Failure Cause	Opeartion
xiaosong_hsm_test 9[redacted]...	3a-lc	Bind	Aug 09, 2021 16:...	Server login credential in...	Delete
xiaosong_hsm_test 9a982[redacted]...	3a-lc	Bind	Aug 09, 2021 16:...	Server login credential in...	Delete
scc-dbss-bj4-81617 9996a7b[redacted]	3a-lc	Bind	Aug 09, 2021 16:...	Server login credential in...	Delete

NOTE

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

----End

3.4.4 Resetting a Key Pair

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

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

Prerequisites

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

Procedure

Step 1 Log in to the management console.

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

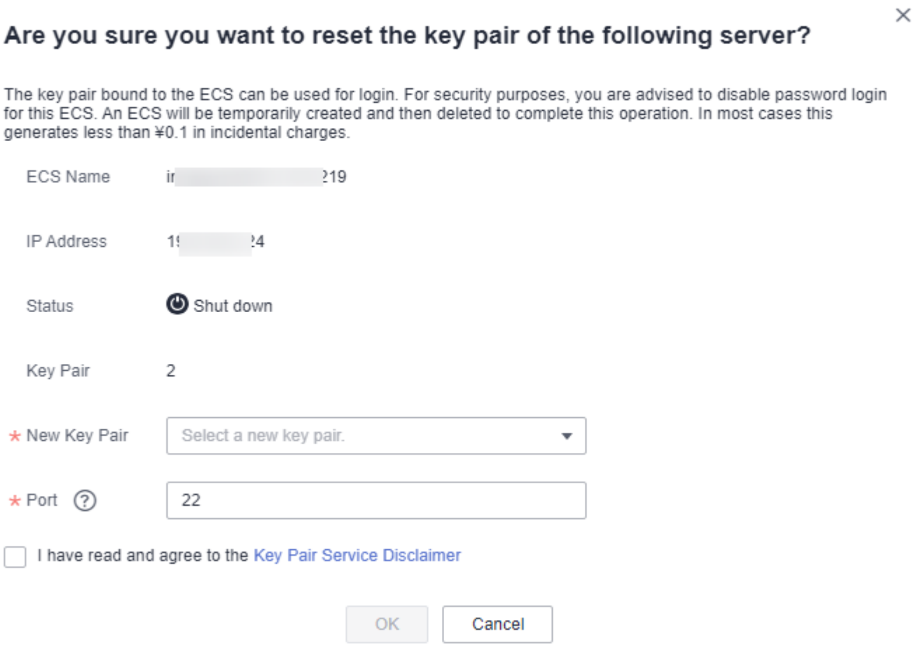
Step 3 Click ☰. Choose **Security & Compliance** > **Data Encryption Workshop**.

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

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

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

Figure 3-18 Resetting a key pair



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

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

ECS Name ir[redacted]219

IP Address 1[redacted]4

Status Shut down

Key Pair 2

* New Key Pair Select a new key pair.

* Port 22

□ I have read and agree to the Key Pair Service Disclaimer

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

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

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

----End

3.4.5 Replacing a Key Pair

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

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

Prerequisites

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

Procedure

Step 1 Log in to the management console.

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

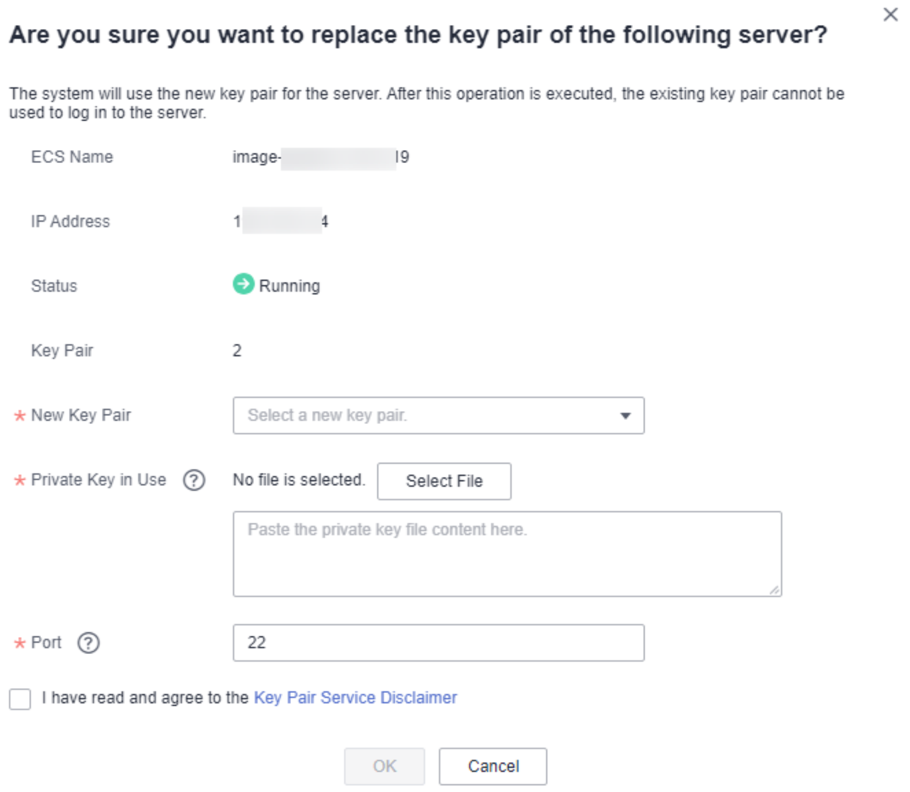
Step 3 Click ☰. Choose **Security & Compliance** > **Data Encryption Workshop**.

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

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

Step 6 Click **Replace** in the row of an ECS. Set parameters in the dialog box that is displayed.

Figure 3-19 Replacing a key pair



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

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

ECS Name	image-[redacted]l9
IP Address	1[redacted]4
Status	Running
Key Pair	2
* New Key Pair	Select a new key pair.
* Private Key in Use	No file is selected. Select File Paste the private key file content here.
* Port	22

□ I have read and agree to the Key Pair Service Disclaimer

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

Step 8 Click **Select File** to upload the private key (in .pem format) of the original key pair or copy the private key content to the text box.

NOTE

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

Step 9 The default port number is 22 and can be modified.

NOTE

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

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

----End

3.4.6 Unbinding a Key Pair

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

Prerequisites

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

Constraints

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

Procedure

Step 1 Log in to the management console.

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

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

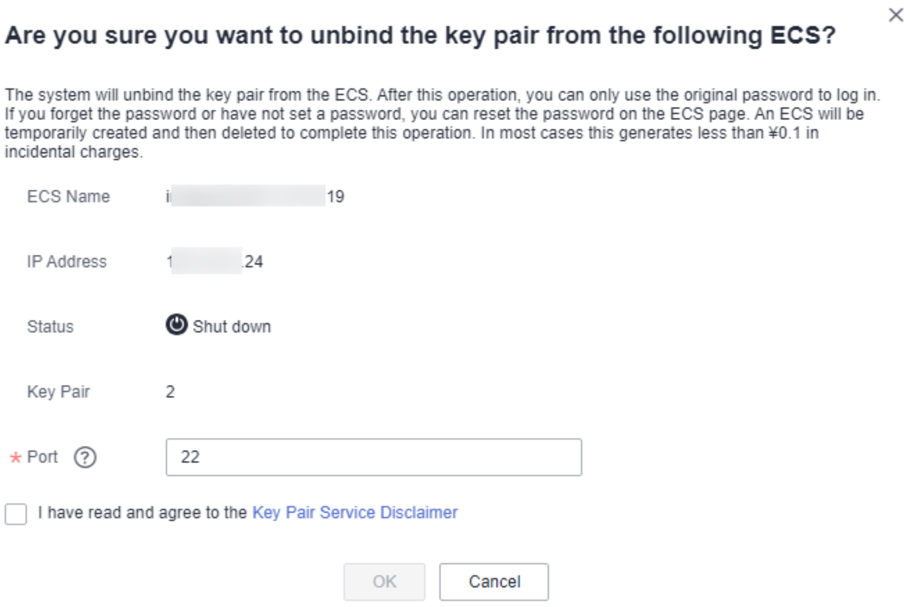
Step 4 In the navigation pane on the left, click **Key Pair Service**.

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

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

- If the ECS is shut down, a dialog box will be displayed, as shown in **Figure 3-20**.

Figure 3-20 Unbinding a key pair (1)



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

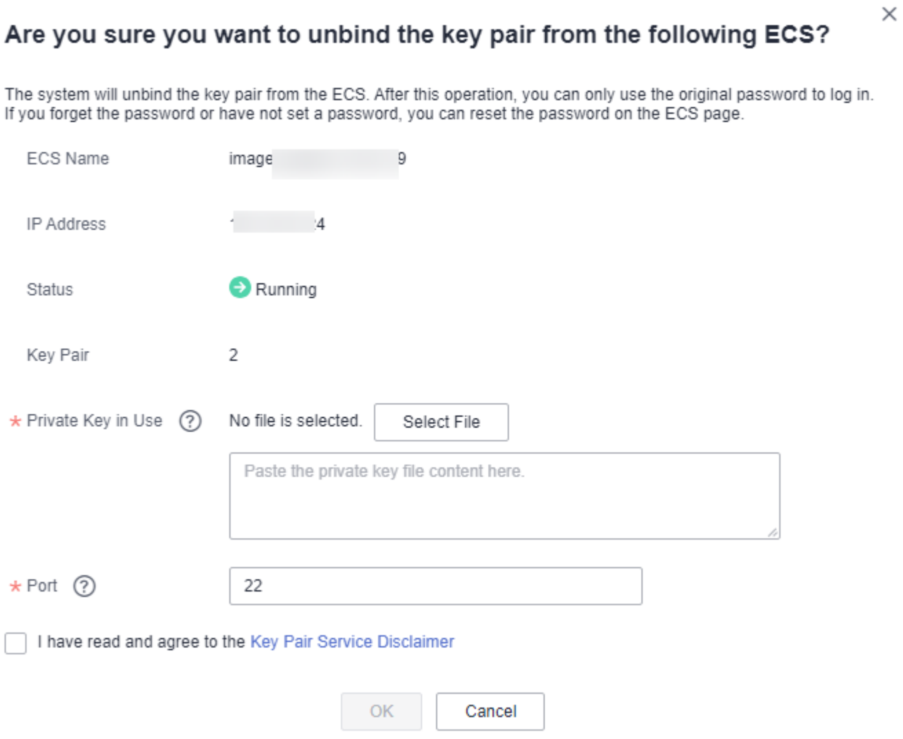
The system will unbind the key pair from the ECS. After this operation, you can only use the original password to log in. If you forget the password or have not set a password, you can reset the password on the ECS page. An ECS will be temporarily created and then deleted to complete this operation.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

ECS Name	i[redacted]19
IP Address	1[redacted].24
Status	Shut down
Key Pair	2
* Port	22

□ I have read and agree to the Key Pair Service Disclaimer

- If the ECS is running, a dialog box will be displayed, as shown in **Figure 3-21**.

Figure 3-21 Unbinding a key pair (2)



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

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

ECS Name: image[redacted]9

IP Address: [redacted]4

Status: Running

Key Pair: 2

* Private Key in Use: No file is selected. Select File

Paste the private key file content here.

* Port: 22

□ I have read and agree to the Key Pair Service Disclaimer

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

NOTE

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

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

NOTE

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

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

NOTE

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

----End

3.4.7 Deleting a Key Pair

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

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

Constraints

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

Procedure

Step 1 **Log in to the management console**.

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

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

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

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

NOTE

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

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

----End

3.5 Managing Private Keys

3.5.1 Importing a Private Key

To facilitate local private key management, you can import the private key to the KPS console for centralized management of your private keys. The managed private keys are encrypted by the keys provided by KMS, ensuring security for storage, import, and export of the private keys. You can download the private keys from the management console whenever you need. To ensure the security of the private keys, keep the downloaded private keys properly.

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

Prerequisites

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

Constraints

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

Procedure

Step 1 **Log in to the management console**.

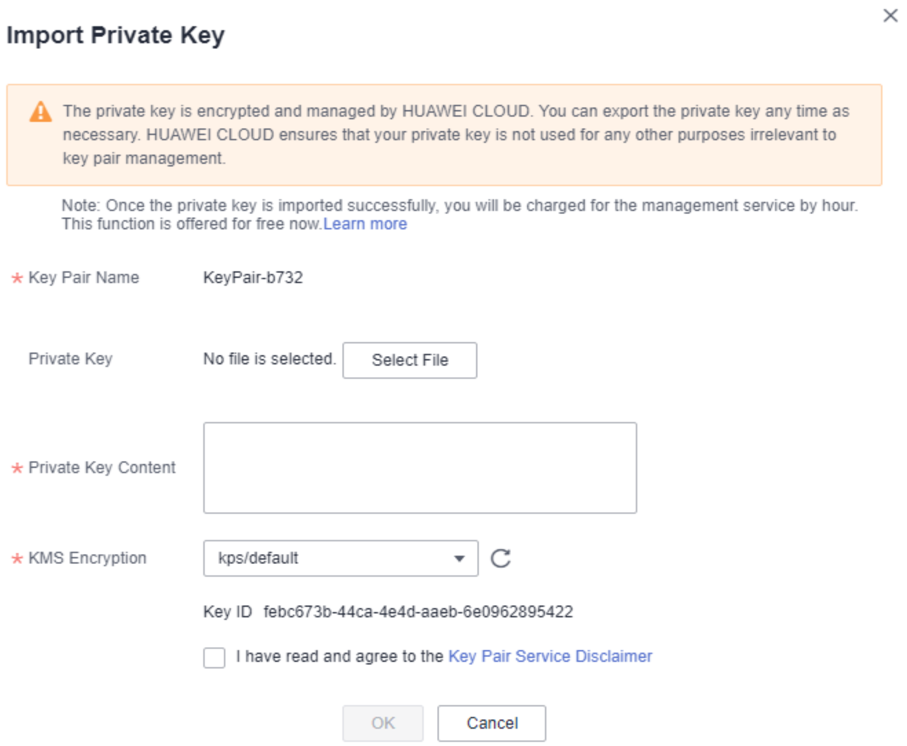
Step 2 Click 📍 in the upper left corner of the management console and select a region or project.

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

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

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

Figure 3-22 Importing a private key



Import Private Key

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

Note: 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: KeyPair-b732

Private Key: No file is selected. Select File

* Private Key Content:

* KMS Encryption: kps/default

Key ID febc673b-44ca-4e4d-aaeb-6e0962895422

□ I have read and agree to the Key Pair Service Disclaimer

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

NOTE

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

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

NOTE

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

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

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

----End

3.5.2 Exporting a Private Key

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

Prerequisites

The private key has been managed on the management console.

Constraints

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

Procedure

Step 1 Log in to the management console.

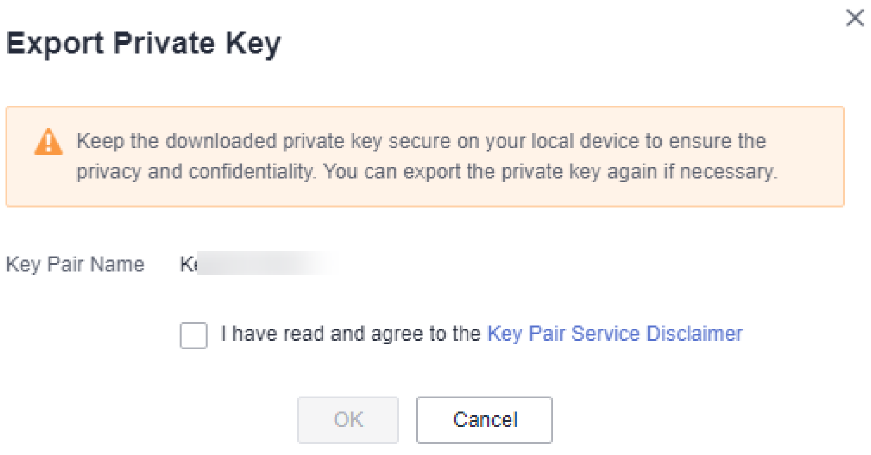
Step 2 Click 📍 in the upper left corner of the management console and select a region or project.

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

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

Step 5 Click **Export Private Key** in the row where the target key pair resides. The **Export Private Key** dialog box is displayed, as shown in Figure 3-23.

Figure 3-23 Exporting a private key



Export Private Key

Keep the downloaded private key secure on your local device to ensure the privacy and confidentiality. You can export the private key again if necessary.

Key Pair Name Ke[redacted]

□ I have read and agree to the Key Pair Service Disclaimer

Step 6 Select **I have read and agree to the Key Pair Service Disclaimer**.

Step 7 Click **OK**. The browser automatically downloads the private key.

NOTICE

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

----End

3.5.3 Clearing a Private Key

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

Prerequisites

The private key has been managed on the management console.

Constraints

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

Procedure

Step 1 Log in to the management console.

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

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

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

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

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

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

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

----End

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

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

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

Prerequisites

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

Constraints

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

Table 3-4 Private key file formats

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

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

Logging In from a Windows Computer

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

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

Step 1 Double-click **PuTTY.EXE**. The **PuTTY Configuration** page is displayed.

Step 2 Choose **Connection** > **Data**. Enter the image username in **Auto-login username**.

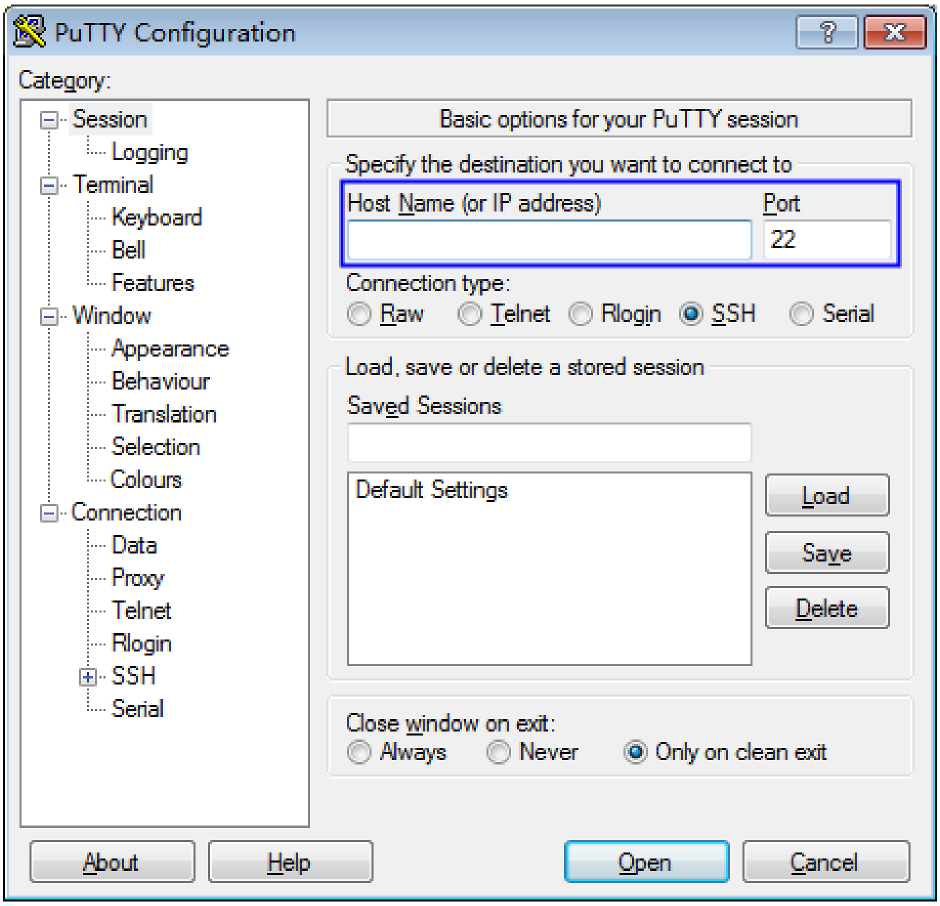
NOTE

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

Step 3 Choose **Connection** > **SSH** > **Auth**. In **Private key file for authentication**, click **Browse** and select a private key file (in the **.ppk** format).

Step 4 Click **Session** and enter the EIP of the ECS under **Host Name (or IP address)**.

Figure 3-24 Configuring the EIP



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address) Port
22

Connection type:
○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions

Default Settings

Close window on exit:
○ Always ○ Never ● Only on clean exit

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

----End

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

Step 1 Start the Xshell tool.

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

ssh *Username*@*EIP*

An example command is provided as follows:

ssh *root@192.168.1.1*

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

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

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

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

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

----End

Logging In from a Linux Computer

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

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

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

NOTE

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

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

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

NOTE

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

----End

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

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

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

Prerequisites

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

Constraints

- After obtaining the initial password, you are advised to clear the password information recorded in the system to increase system security.

  Clearing the initial password information does not affect ECS operation or login. Once cleared, the password cannot be restored. Before deleting a password, you are advised to record it. For details, see *Elastic Cloud Server User Guide*.
- You can also call the API to obtain the initial password of the Windows ECS. For details, see *Elastic Cloud Server API Reference*.
- The ECS private key file must be in .pem format.

  If the file is in the .ppk format, convert it to a .pem file. For details, see **How Do I Convert the Format of a Private Key File?**

Procedure

Step 1 **Log in to the management console**.

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

Step 3 Click ☰ and choose **Compute** > **Elastic Cloud Server**.

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

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

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

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

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

----End

4 Dedicated HSM

4.1 Operation Guide

Restrictions

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

Operation Guide

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

Figure 4-1 Operation Guide

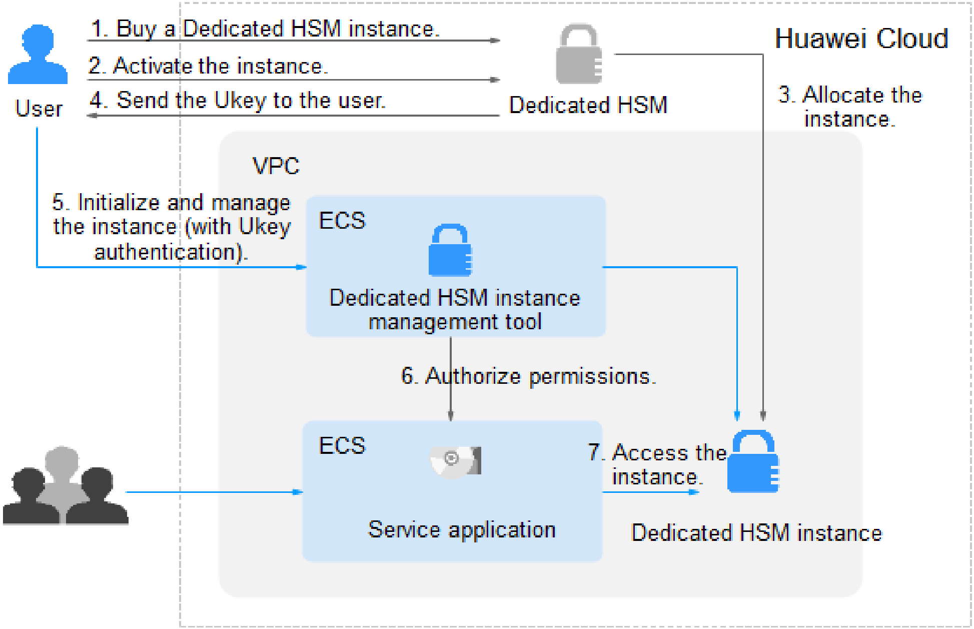

1. Buy a Dedicated HSM instance.
2. Activate the instance.
4. Send the Ukey to the user.
User
Dedicated HSM
Huawei Cloud
3. Allocate the instance.
VPC
5. Initialize and manage the instance (with Ukey authentication).
ECS
Dedicated HSM instance management tool
6. Authorize permissions.
ECS
Service application
7. Access the instance.
Dedicated HSM instance

Table 4-1 describes the operation guide.

Table 4-1 Operation guide descriptions

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

No.	Procedure	Description	Operated By
4	Provide the UKey, initialization guide, and software.	● A security expert sends the Ukey to the email address you provided. A UKey is the only identifier of a Dedicated HSM user. Keep it properly. ● A security expert will provide you with the software and guide for initializing Dedicated HSM instances. If you have any questions, contact the expert.	Dedicated HSM security expert
5	Initialize and manage instances (involving UKey authentication).	1. Install the tool for managing Dedicated HSM instances on the instance management node. 2. 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. For details, see **Initializing a Dedicated HSM Instance**.	User
6	Install the security agent and granting access permissions.	Install and initialize the security agent on service application nodes. For details, see **Installing the Security Agent and Granting Access Permissions**.	User
7	Access the instance.	Service applications access the Dedicated HSM instances through APIs or SDK.	User

4.2 Purchasing a Dedicated HSM Instance

4.2.1 Creating a Dedicated HSM Instance

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

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

- Initial installation fee, charged when you create a Dedicated HSM instance.
- Yearly/Monthly fee, charged when **Activating a Dedicated HSM Instance**.

Prerequisites

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

Constraints

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

  You need to activate the instance before using it.

Procedure

Step 1 **Log in to the management console**.

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

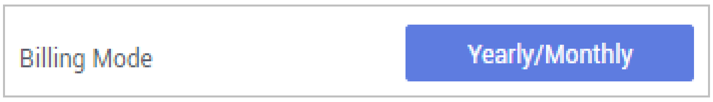
Step 3 Click ☰. Choose **Security & Compliance** > **Data Encryption Workshop**.

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

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

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

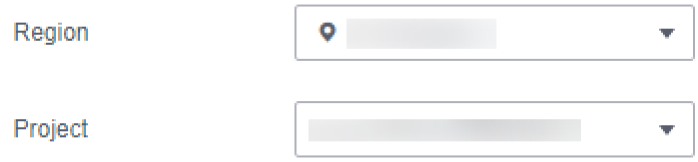
Figure 4-2 Billing Mode



Billing Mode: Yearly/Monthly

Step 7 Select a region and project.

Figure 4-3 Selecting a region



Region

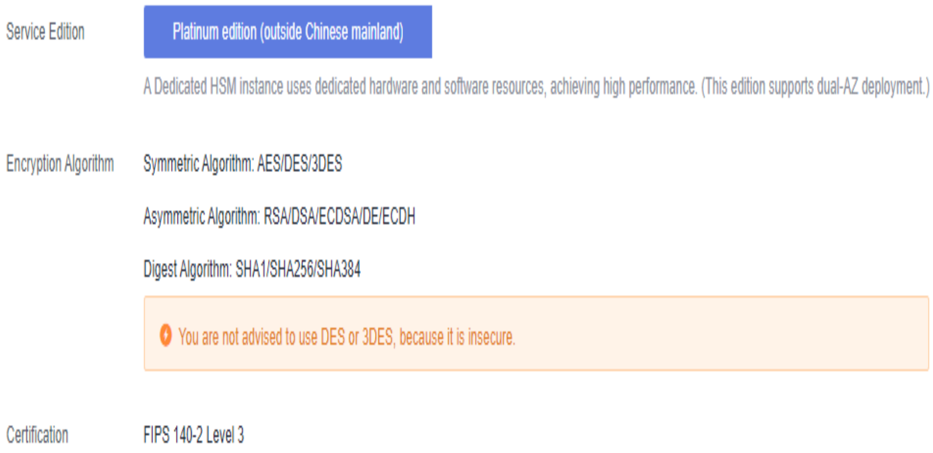
Project

NOTE

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

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

Figure 4-4 Platinum edition (outside Chinese mainland)



Service Edition: Platinum edition (outside Chinese mainland)

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

Encryption Algorithm: Symmetric Algorithm: AES/DES/3DES

Asymmetric Algorithm: RSA/DSA/ECDSA/DE/ECDH

Digest Algorithm: SHA1/SHA256/SHA384

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

Certification: FIPS 140-2 Level 3

Table 4-2 Edition parameters

Parameter	Description
Service Edition	Platinum edition (outside Chinese mainland)
Encryption Algorithm	Algorithm supported by the HSM instance. ● Symmetric algorithm: AES ● Asymmetric algorithm: RSA, DSA, ECDSA, DE, and ECDH ● Digest algorithm: SHA1, SHA256, SHA384
Certification	FIPS 140-2 Level 3 certified

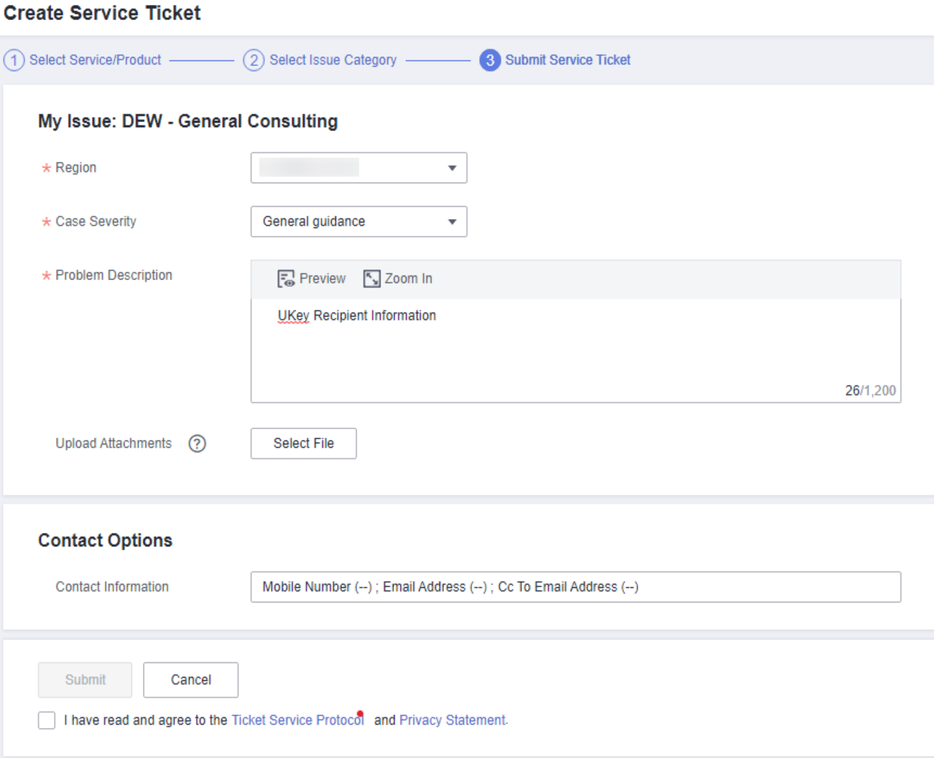
Step 9 Choose **Service Tickets** > **Create Service Ticket**. Our Huawei Cloud experts will contact you and provide a customized purchase plan and its quote.

- In the **Case Severity** drop-down list, select **General guidance**.
- In the **Problem Description** text box, enter **Dedicated HSM Contact Information**.
- **Contact Information**: Enter the phone number and email address to receive the progress information of the service ticket.

NOTICE

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

Figure 4-5 Creating a service ticket



Create Service Ticket

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

My Issue: DEW - General Consulting

* Region	[redacted]
* Case Severity	General guidance
* Problem Description	Preview Zoom In UKey Recipient Information 26/1,200
Upload Attachments ?	Select File

Contact Options

Contact Information	Mobile Number (--) ; Email Address (--) ; Cc To Email Address (--)

Submit Cancel

□ I have read and agree to the Ticket Service Protocol and Privacy Statement.

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

NOTE

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

----End

4.2.2 Activating a Dedicated HSM Instance

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

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

Prerequisites

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

Constraints

- The instance name can contain only letters, digits, underscores (_), and hyphens (-).
- Two nodes are created as the background resource pool for a Dedicated HSM instance. To ensure high availability of the nodes, a floating IP address is assigned to the instance.

- If the instance fails to be created, you can click **Delete** in the row where the instance is located to delete it. Then apply for a refund by submitting a service ticket.
- After a Dedicated HSM instance is successfully created, it can neither be changed to another type nor be refunded. To use a Dedicated HSM instance of another type, you need to buy another one.

Procedure

Step 1 Log in to the management console.

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

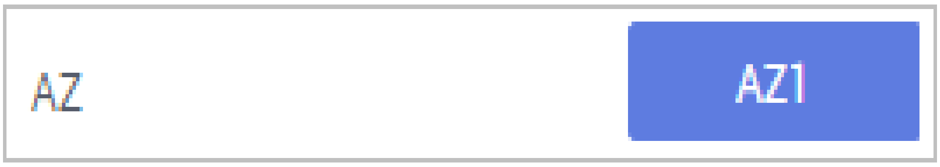
Step 3 Click ☰. Choose **Security & Compliance** > **Data Encryption Workshop**.

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

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

Step 6 Select an AZ.

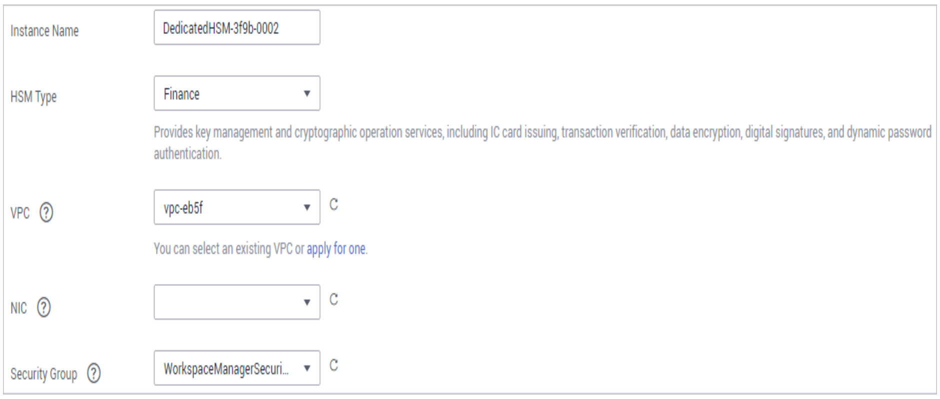
Figure 4-6 Selecting an AZ



AZ: AZ1

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



Instance Name: DedicatedHSM-3f9b-0002

HSM Type: Finance

Provides key management and cryptographic operation services, including IC card issuing, transaction verification, data encryption, digital signatures, and dynamic password authentication.

VPC: vpc-eb5f

You can select an existing VPC or apply for one.

NIC:

Security Group: WorkspaceManagerSecuri...

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**. ● **Finance**: Provides key management and encryption computing services, including IC card issuing, transaction verification, data encryption, digital signatures, and dynamic password authentication. ● **Server**: Provides secure, complete key management services and high-performance concurrent cryptographic operations, such as data signatures, signature verification, and data encryption/decryption. ● **Signature server**: Guarantees the integrity, confidentiality, anti-repudiation, and post-event traceability of user data by using digital signatures, digital envelopes, and digital digests.	**Finance**
VPC	You can select an existing Virtual Private Cloud (VPC), or click **Apply for VPC** to create one. For more information about VPC, see the *Virtual Private Cloud User Guide*.	vpc-test-dhsm
NIC	All available subnets are displayed on the page. The system automatically assigns three IP address to the instance. **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. For more information about subnets, see the *Virtual Private Cloud User Guide*.	**subnet-test-dhsm (192.168.0.0/24)**

Parameter	Description	Example Value
Security Group	The security group configured for the instance is displayed on the page. Once a security group is selected for an instance, the instance is protected by the security group access rules. For more information about security groups, see the *Virtual Private Cloud User Guide*.	WorkspaceUserSecurityGroup

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

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

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

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

1. Set the required duration.

   The required duration ranges from one month to one year.

   NOTE

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

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

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

3. On the **Order Details** page, confirm the order details, read and select **I have read and agree to the Privacy Policy Statement**.
4. Click **Pay Now** to pay for the yearly or monthly package.
5. On the **Pay** page, select a payment method to pay for your order.

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

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

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

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

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

     NOTE

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

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

NOTE

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

----End

4.3 Viewing Dedicated HSM Instances

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

Procedure

Step 1 Log in to the management console.

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

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

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

Table 4-4 describes the parameters in the HSM instance list.

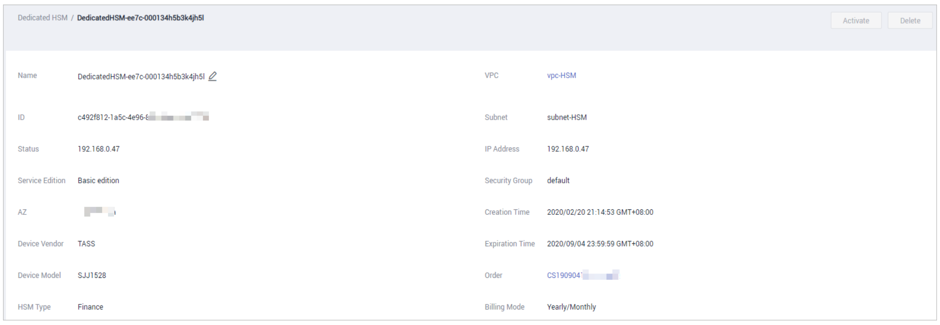
Table 4-4 Dedicated HSM instance parameters

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

Parameter	Description
Status	Status of a Dedicated HSM instance: ● 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 (outside Chinese mainland)** ● Platinum edition (outside Chinese mainland): You can exclusively use the HSM subrack, power supply, the network bandwidth, and API resources of the HSM. 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 click the name of a Dedicated HSM instance to view details about the instance, as shown in **Figure 4-8**.

Figure 4-8 Details about Dedicated HSM instances



Dedicated HSM / DedicatedHSM-ee7c-000134h5b3k4jh5l

Name	DedicatedHSM-ee7c-000134h5b3k4jh5l	VPC	vpc-HSM
ID	c492f812-1a5c-4e96-[redacted]	Subnet	subnet-HSM
Status	192.168.0.47	IP Address	192.168.0.47
Service Edition	Basic edition	Security Group	default
AZ	[redacted]	Creation Time	2020/02/20 21:14:53 GMT+08:00
Device Vendor	TASS	Expiration Time	2020/09/04 23:59:59 GMT+08:00
Device Model	SJJ1528	Order	CS190904[redacted]
HSM Type	Finance	Billing Mode	Yearly/Monthly

For more information, see **Table 4-5**.

Table 4-5 Parameter description

Parameter	Description
Name	Name of a Dedicated HSM instance
ID	ID of an instance
Status	Status of a Dedicated HSM instance: ● 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**.

Parameter	Description
VPC	VPC to which the instance belongs For more information about VPC, see *Virtual Private Cloud User Guide*.
Subnet	Subnet where the instance is located. For more information about subnets, see *Virtual Private Cloud User Guide*.
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 *Virtual Private Cloud User Guide*.
Creation Time	Time when the instance is purchased
Expiration Time	Time when the instance expires
Order	Order ID of the instance. You can click the order number to query the order details.
Billing Mode	Yearly/Monthly prepaid package

----End

4.4 Managing Tags

4.4.1 Adding a Tag

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

Procedure

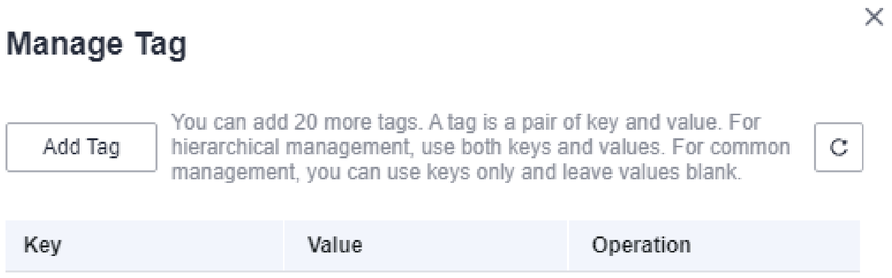
Step 1 Click 📍 in the upper left corner of the management console and select a region or project.

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

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

Step 4 In the **Operation** column of an instance, click **Manage Tag**. The **Manage Tag** page is displayed, as shown in **Figure 4-9**.

Figure 4-9 Manage Tag



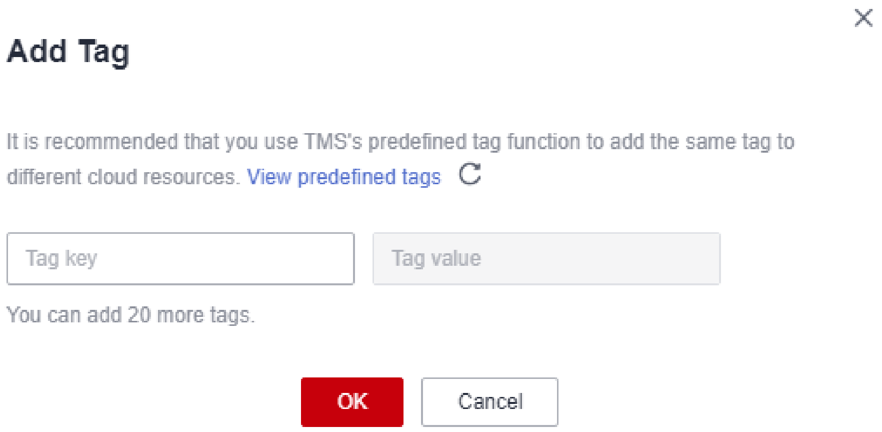
Manage Tag

You can add 20 more tags. A tag is a pair of key and value. For hierarchical management, use both keys and values. For common management, you can use keys only and leave values blank.

Key	Value	Operation

Step 5 Click **Add Tag**. In the dialog box that is displayed, enter the tag key and tag value. For details about the parameters, see **Table 4-6**.

Figure 4-10 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.

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 4-6 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.	● 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: – Chinese – English – Numbers – Space – Special characters: _.:/=+-@
Tag value	Value of the tag	● Optional ● 255 characters limit. ● The following character types are allowed: – Chinese – English – Numbers – Space – Special characters: _.:/=+-@

Step 6 Click **OK**.

----End

4.4.2 Searching for a Dedicated HSM Instance by Tag

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

Prerequisites

Tags have been added.

Procedure

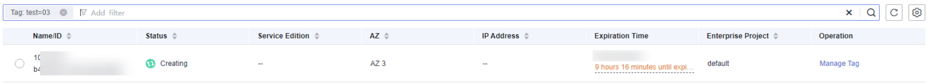
Step 1 Click in the upper left corner of the management console and select a region or project.

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

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

Step 4 Click the search box and select a tag as the filter attribute to search for Dedicated HSM instances, as shown in **Figure 4-11**.

Figure 4-11 Searching for a Dedicated HSM instance



Tag: test=03 | Add filter

	Name/ID	Status	Service Edition	AZ	IP Address	Expiration Time	Enterprise Project	Operation
○	10 [redacted] b4	Creating	--	AZ 3	--	[redacted] 9 hours 16 minutes until expi...	default	Manage Tag

----End

4.4.3 Modifying a Tag Value

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

Procedure

Step 1 Click in the upper left corner of the management console and select a region or project.

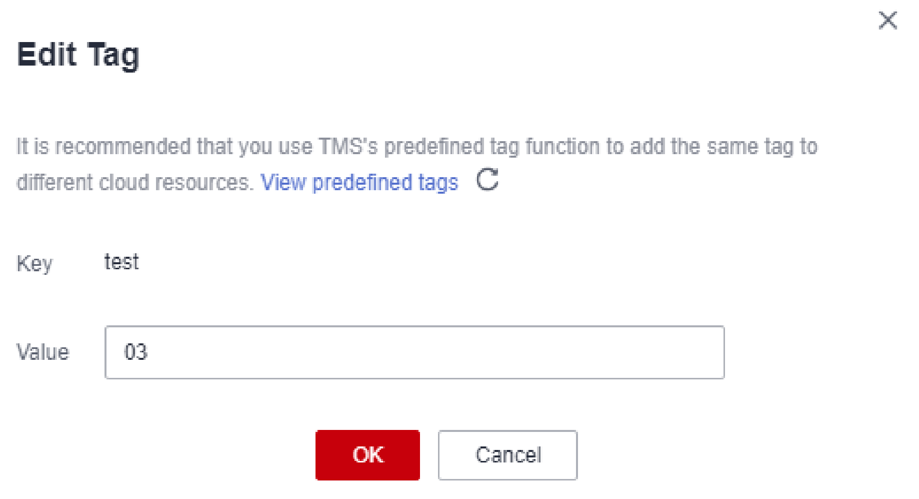
Step 2 Click ☰. Choose **Security & Compliance** > **Data Encryption Workshop**.

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

Step 4 Click **Manage Tag** in the row where the target instance is located. The **Manage Tag** dialog box is displayed.

Step 5 Click **Edit**. The **Edit Tag** dialog box is displayed. After changing the tag value, click **OK**.

Figure 4-12 Editing a tag



Edit Tag

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

Key test

Value 03

----End

4.4.4 Deleting a Tag

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

Procedure

Step 1 Click 📍 in the upper left corner of the management console and select a region or project.

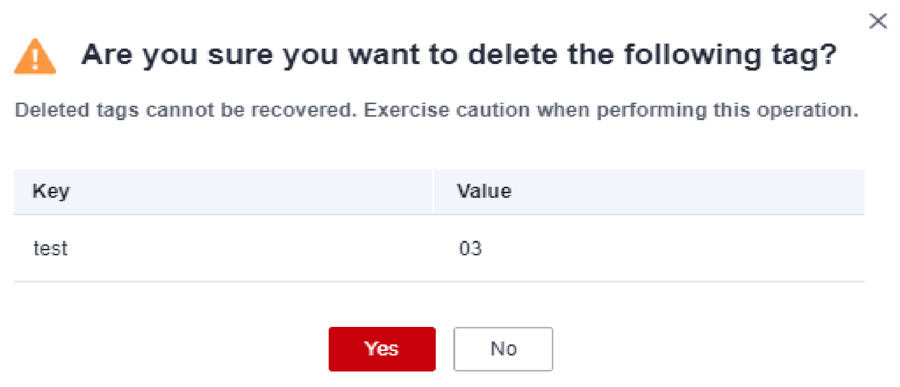
Step 2 Click ☰. Choose **Security & Compliance** > **Data Encryption Workshop**.

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

Step 4 Click **Manage Tag** in the row where the target instance is located. The **Manage Tag** dialog box is displayed.

Step 5 In the **Operation** column of a tag, click **Delete**.

Figure 4-13 Deleting a tag



Are you sure you want to delete the following tag?

Deleted tags cannot be recovered. Exercise caution when performing this operation.

Key	Value
test	03

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

----End

4.5 Using Dedicated HSM Instances

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

Prerequisites

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

Table 4-7 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	*Dedicated HSM Instance User Manual* and *Dedicated HSM Instance Installation Guide*	
Security agent software	Establishes a secure connection with the instance.	
SDK	Provides APIs for Dedicated HSM. You can use the SDK to establish secure connections with instances.	
Dedicated HSM instance management node (for example, an ECS)	Run the Dedicated HSM instance management tool, which is in the same VPC where the Dedicated HSM instance resides, and allocate elastic IP addresses for remote connections.	Purchase ECSs as needed. For details, see **Purchasing an ECS**.

Item	Description	How to Obtain
Service application nodes (for example, ECSs)	Run the security agent software and users' service applications, which must be in the VPC where the Dedicated HSM instance is deployed.	

Initializing a Dedicated HSM Instance

NOTE

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

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

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

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

     NOTE

     After the Dedicated HSM instance is initialized, you can unbind from the elastic IP address. The binding and unbinding operations can be performed whenever needed.
   - Set other parameters based on the site requirements.

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

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

NOTE

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

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

----End

Installing the Security Agent and Granting Access Permissions

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

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

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

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

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

NOTE

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

----End

5 Auditing Logs

5.1 Operations supported by CTS

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

Table 5-1 DEW operations supported by CTS

Operation	Resource Type	Trace Name
Creating a CMK	cmk	createKey
Creating a DEK	cmk	createDataKey
Creating a plaintext-free DEK	cmk	createDataKeyWithoutPlaintext
Enabling a CMK	cmk	enableKey
Disabling a CMK	cmk	disableKey
Encrypting a DEK	cmk	encryptDatakey
Decrypting a DEK	cmk	decryptDatakey
Scheduling the deletion of a CMK	cmk	scheduleKeyDeletion
Canceling the scheduled deletion of a CMK	cmk	cancelKeyDeletion
Generating random numbers	rng	genRandom
Changing the alias of a CMK	cmk	updateKeyAlias
Changing the description of a CMK	cmk	updateKeyDescription

Operation	Resource Type	Trace Name
Prompting risks about CMK deletion	cmk	deleteKeyRiskTips
Importing key material	cmk	importKeyMaterial
Deleting key material	cmk	deleteImportedKeyMaterial
Creating a grant	cmk	createGrant
Retiring a grant	cmk	retireGrant
Revoking a grant	cmk	revokeGrant
Encrypting data	cmk	encryptData
Decrypting data	cmk	decryptData
Adding a tag	cmk	createKeyTag
Deleting a tag	cmk	deleteKeyTag
Adding or deleting tags in batches	cmk	batchCreateKeyTags
Batch deleting tags	cmk	batchDeleteKeyTags
Enabling key rotation	cmk	enableKeyRotation
Modifying key rotation interval	cmk	updateKeyRotationInterval
Disabling key rotation	cmk	disableKeyRotation
Creating a secret	csms	createSecret
Updating a secret	csms	updateSecret
Deleting a secret	csms	forceDeleteSecret
Schedule the deletion of a secret	csms	scheduleDelSecret
Canceling the scheduled deletion of a secret	csms	restoreSecretFromDeletedStatus
Creating a secret status	csms	createSecretStage
Updating a secret status	csms	updateSecretStage
Deleting a secret status	csms	deleteSecretStage
Creating a secret version	csms	createSecretVersion
Downloading secret backup	csms	backupSecret
Restoring secret backup	csms	restoreSecretFromBackupBlob

Operation	Resource Type	Trace Name
Creating or importing an SSH key pair	keypair	createOrImportKeypair
Deleting an SSH key pair	keypair	deleteKeypair
Importing a private key	keypair	importPrivateKey
Exporting a private key	keypair	exportPrivateKey
Purchasing an HSM instance	hsm	purchaseHsm
Configuring an HSM instance	hsm	createHsm
Deleting an HSM instance	hsm	deleteHsm

5.2 Using CTS to Query DEW Operation Traces

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

Viewing Audit Logs of DEW

Step 1 Log in to the management console.

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

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

- **Trace Type**, **Trace Source**, **Resource Type**, and **Search By**

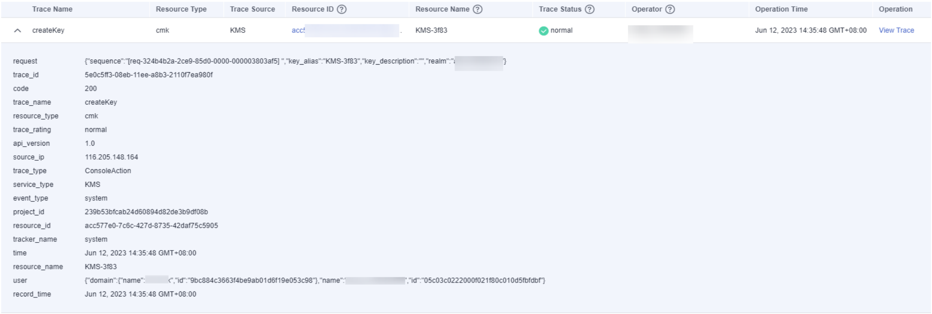
  Select the filter from the drop-down list.

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

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

Step 5 Click ⌄ on the left of a trace to see its details. See **Figure 5-1**.

Figure 5-1 Expanding trace details

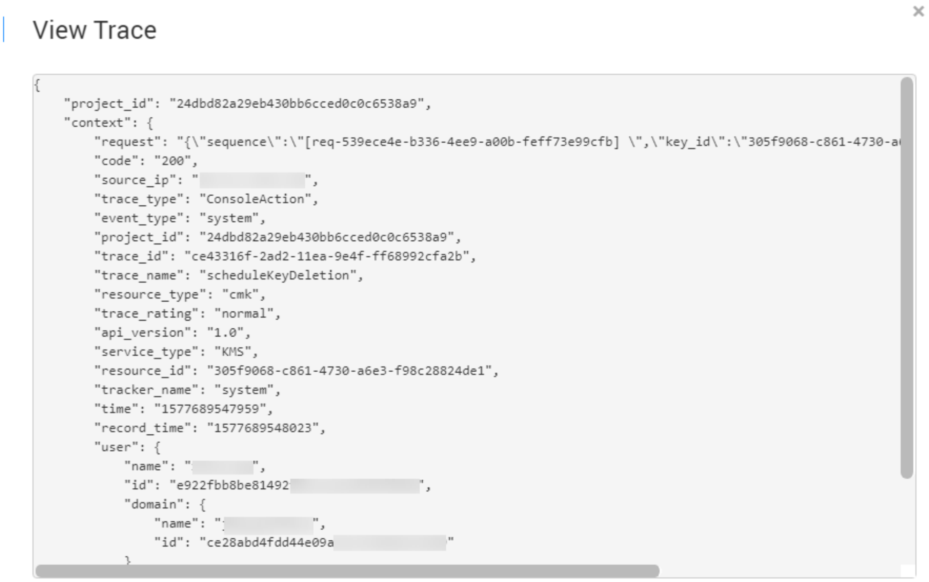


Trace Name	Resource Type	Trace Source	Resource ID ⓘ	Resource Name ⓘ	Trace Status ⓘ	Operator ⓘ	Operation Time	Operation
createKey	cmk	KMS	acc[redacted]	KMS-3f83	✓ normal	[redacted]	Jun 12, 2023 14:35:48 GMT+08:00	View Trace

request	{"sequence":"[req-324b4b2a-2ce9-85d0-0000-000003803af5] ","key_alias":"KMS-3f83","key_description":"","realm":"[redacted]"}
trace_id	5e0c5ff3-08eb-11ee-a8b3-2110f7ea980f
code	200
trace_name	createKey
resource_type	cmk
trace_rating	normal
api_version	1.0
source_ip	116.205.148.164
trace_type	ConsoleAction
service_type	KMS
event_type	system
project_id	239b53bfcab24d60894d82de3b9df08b
resource_id	acc577e0-7c6c-427d-8735-42daf75c5905
tracker_name	system
time	Jun 12, 2023 14:35:48 GMT+08:00
resource_name	KMS-3f83
user	{"domain":{"name":"[redacted]","id":"9bc884c3663f4be9ab01d6f19e053c98"},"name":"[redacted]","id":"05c03c0222000f021f80c010d5fbfdbf"}
record_time	Jun 12, 2023 14:35:48 GMT+08:00

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

Figure 5-2 Viewing traces



View Trace

```
{
    "project_id": "24dbd82a29eb430bb6cced0c0c6538a9",
    "context": {
        "request": "{\"sequence\":\"[req-539ece4e-b336-4ee9-a00b-feff73e99cfb] \",\"key_id\":\"305f9068-c861-4730-a
        "code": "200",
        "source_ip": "[redacted]",
        "trace_type": "ConsoleAction",
        "event_type": "system",
        "project_id": "24dbd82a29eb430bb6cced0c0c6538a9",
        "trace_id": "ce43316f-2ad2-11ea-9e4f-ff68992cfa2b",
        "trace_name": "scheduleKeyDeletion",
        "resource_type": "cmk",
        "trace_rating": "normal",
        "api_version": "1.0",
        "service_type": "KMS",
        "resource_id": "305f9068-c861-4730-a6e3-f98c28824de1",
        "tracker_name": "system",
        "time": "1577689547959",
        "record_time": "1577689548023",
        "user": {
            "name": "[redacted]",
            "id": "e922fbb8be81492[redacted]",
            "domain": {
                "name": "[redacted]",
                "id": "ce28abd4fdd44e09a[redacted]"
            }
```

----End

6 Permission Control

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

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

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

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

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

Prerequisites

Before authorizing permissions to a user group, you need to know which DEW permissions can be added to the user group. **Table 6-1** describes the DEW system policies.

For the system policies of other services, see **System Permissions**.

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

Role/Policy Name	Description	Type	Dependency
KMS Administrator	Key Management Service (KMS) administrator, who has all permissions of the service.	System role	None

Role/Policy Name	Description	Type	Dependency
KMS CMKFullAccess	All permissions for encryption keys in Key Management Service (KMS). Users with these permissions can perform all the operations allowed by policies.	System policy	None
DEW KeypairFullAccess	Full permissions for KPS. Users with these permissions can perform all the operations allowed by policies.	System policy	None
DEW KeypairReadOnlyAccess	Read-only permissions for Key Pair Service (KPS) in DEW. Users with this permission can only view KPS data.	System policy	None
CSMS FullAccess	All permissions for Cloud Secret Management Service (CSMS) in DEW. Users with these permissions can perform all the operations allowed by policies.	System policy	None
CSMS ReadOnlyAccess	Read-only permissions for Cloud Secret Management Service (CSMS) in DEW. Users with these permissions can perform all the operations allowed by policies.	System policy	None

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

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

Operation	KMS Administrator	KMS CMKFullAccess	DEW KeypairFullAccess	DEW KeypairReadOnlyAccess
Creating a key	√	√	x	x
Enable a key	√	√	x	x
Disable a key	√	√	x	x
Schedule key deletion	√	√	x	x

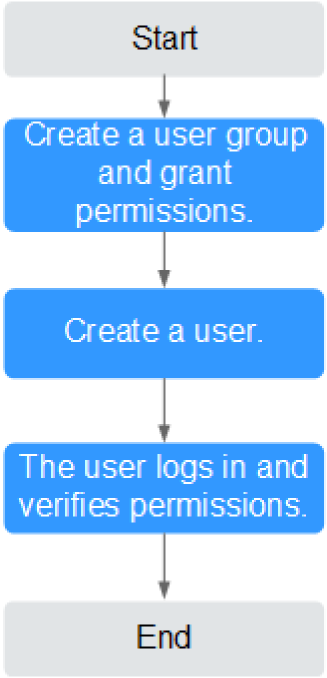
Operation	KMS Administrator	KMS CMKFullAccess	DEW KeypairFullAccess	DEW KeypairReadOnlyAccess
Cancel scheduled key deletion	√	√	x	x
Modify a key alias	√	√	x	x
Modify key description	√	√	x	x
Generate a random number	√	√	x	x
Create a DEK	√	√	x	x
Create a plaintext-free DEK	√	√	x	x
Encrypt a DEK	√	√	x	x
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
Retire a grant	√	√	x	x
Query the grant list	√	√	x	x
Query retirable grants	√	√	x	x
Encrypt data	√	√	x	x
Decrypt data	√	√	x	x

Operation	KMS Administrator	KMS CMKFullAccess	DEW KeypairFullAccess	DEW KeypairReadOnlyAccess
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
Query the key list	√	√	x	x
Query key details	√	√	x	x
Query public key	√	√	x	x
Query instance quantity	√	√	x	x

Operation	KMS Administrator	KMS CMKFullAccess	DEW KeypairFullAccess	DEW KeypairReadOnlyAccess
Query quotas	√	√	x	x
Query the key pair list	x	x	√	√
Create or import a key pair	x	x	√	x
Query key pairs	x	x	√	√
Delete a key pair	x	x	√	x
Update key pair description	x	x	√	x
Bind a key pair	x	x	√	x
Unbind a key pair	x	x	√	x
Query a binding task	x	x	√	√
Query failed tasks	x	x	√	√
Delete all failed tasks	x	x	√	x
Delete a failed task	x	x	√	x
Query running tasks	x	x	√	√

Authorization Process

Figure 6-1 Authorizing the DEW access permission to a user


Start
Create a user group and grant permissions.
Create a user.
The user logs in and verifies permissions.
End

1. **Create a user group and assign permissions.**

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

2. **Create a user and add it to a user group.**

   Create a user on the IAM console and add the user to the user group created in **1**.

3. **Log in** and verify permissions.

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

   - Choose **Service List** > **Data Encryption Workshop**. In the navigation pane, choose **Key Pair Service**. If a message appears indicating lack of permissions, the **KMS CMKFullAccess** policy has taken effect.
   - Click **Service List** and select a service other than DEW. If a message is displayed indicating that you do not have permission to access the service, the **KMS CMKFullAccess** policy has taken effect.

6.2 Creating a Custom DEW Policy

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

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

- Visual editor: You can select policy configurations without the need to know policy syntax.

Custom KMS policy parameters:

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

- JSON: Edit JSON policies from scratch or based on an existing policy. For details about how to create custom policies, see **Creating a Custom Policy**.

Example Custom Policies

- Example: authorizing users to create and import keys

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

- Example: denying deletion of key tags

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

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

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

- Example: authorizing users to use keys

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

- Example: multi-action policy

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

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

A Change History

Released On	Description
2023-06-30	This is the thirty-third official release. Added section **Searching for a Key** and updated the search method. Added section **Secret Overview** to describe shared secrets and RDS secrets. Added section **Rotation Policy** to describe single-user and dual-user rotation. Added section **Creating an RDS Secret** to describe the process of creating an RDS secret. Added section **Rotation Secret Version** to describe the automatic rotation of RDS secrets. Added section **Creating an Event** to describe the process of creating event notifications. Added section **Managing Events** to describe how to view, search for, enable, disable, and delete events. Added section **Viewing Notifications** to describe how does a notification is generated when an event is triggered. Added section **Binding Key Pairs in Batches** to describe how to bind key pairs in batches. Added section **Managing Tags** to describe how to add, delete, modify, and query tags for Dedicated HSM Instances. Added the description of HMAC-based key algorithms in section **Key Types**. Modified the description of HMAC keys constraints and usage in section **Creating a Key**. Added the description of port 22 in section **Managing Key Pairs**.

Released On	Description
2023-02-21	This is the thirty-second official release. Added secret management events in **Operations supported by CTS**.
2023-01-11	This is the thirty-first official release. Optimized the description about encrypting key materials in **Importing Key Materials**.
2022-11-22	This is the thirtieth official release. Moved "Dedicated HSM > Editions" from *User Guide* to *Service Overview*.
2022-11-15	This is the twenty-ninth official release. Added **Managing a Grant**.
2022-07-22	This is the twenty-eighth official release. Optimized **About Key Rotation**.
2021-12-17	This is the twenty-seventh official release. Modified the following sections: ● In **Creating CMKs Using Imported Key Materials**, asymmetric keys can be imported. ● In **Deleting Key Materials**, the key materials of asymmetric keys cannot be directly deleted.
2021-10-26	This is the twenty-sixth official release. Added **Cloud Secret Management Service**.
2021-09-30	This is the twenty-fifth official release. ● Added description about Chinese cryptographic algorithms in **Creating a Key**. ● Added description about Chinese cryptographic algorithms in **Creating CMKs Using Imported Key Materials**. ● Updated screenshots in **Managing Key Pairs**.
2021-08-30	This is the twenty-fourth official release. Changed the professional edition to the platinum edition.

Released On	Description
2021-07-20	This is the twenty-third official release. - Changed the entry of DEW from **Security** to **Security and Compliance**. - Modified the key creation procedure and screenshots in **Creating a Key**. - Optimized content and updated screenshots in **Managing CMKs**. - Optimized the description of key pairs in **Managing Key Pairs**. - Added description about key types in **Key Types**. - Optimized operations in **Managing Private Keys**. - Optimized operations in **Dedicated HSM**.
2021-06-30	This is the twenty-second official release. - Added **Adding a Key to a Project**. - Added constraints in **Binding a Key Pair**. - Updated screenshots in **Managing CMKs**.
2021-02-22	This is the twenty-first official release. Modified section "Creating a Dedicated HSM Instance."
2020-12-21	This is the twentieth official release. Optimized sections in this document.
2020-12-14	This is the nineteenth official release. Modified **Creating a Key**.
2020-09-25	This is the eighteenth official release. Modified section "Creating a Dedicated HSM Instance."
2020-08-24	This is the seventeenth official release. Added the description about how to obtain KeyId in **Creating a Custom DEW Policy**.

Released On	Description
2020-08-12	This is the sixteenth official release. - Added **Upgrading a Key Pair**. - Updated screenshots in **Creating a Key Pair**. - Updated screenshots in **Importing a Key Pair**. - Updated screenshots in **Viewing a Key Pair**. - Updated screenshots and added descriptions in **Deleting a Key Pair**. - Updated screenshots and added descriptions in **Importing a Private Key**. - Updated screenshots and added descriptions in **Exporting a Private Key**. - Updated screenshots and added descriptions in **Clearing a Private Key**.
2020-07-14	This is the fifteenth official release. - Added **Creating CMKs Using Imported Key Materials**. - Added the description about enterprise project functions in **Creating a Key**, **Creating CMKs Using Imported Key Materials**, and **Viewing a CMK**.
2020-04-07	This is the fourteenth official release. Updated the screenshots.
2020-02-10	This is the thirteen official release. Modified **Permission Control**.
2019-08-09	This is the twelfth official release. Modified section **Key Management Service**: updated screenshots.
2019-07-19	This is the eleventh official release. - Added **Activating a Dedicated HSM Instance**. - Added **Viewing Dedicated HSM Instances**.
2019-07-12	This is the tenth official release. Added **Purchasing a Dedicated HSM Instance**.

Released On	Description
2019-07-04	This is the ninth official release. - Added the method of viewing key usage records in **Deleting One or More CMKs**. - Modified section **Key Pair Service**: updated screenshots. - Added **Using Dedicated HSM Instances**. - Added the resource types and event names of purchasing, configuring, and deleting an HMS instance to the table "DEW operations supported by CTS".
2019-04-22	This is the eighth official release. Optimized the flowchart and architecture graphs.
2018-10-25	This is the seventh official release. Modified section **Viewing a Key Pair**: added the description about the page that displays details of key pairs.
2018-08-30	This is the sixth official release. - Added **Dedicated HSM**. - Added section "Encrypting Your Service System Using Dedicated HSM". - Added **Using Dedicated HSM Instances**.
2018-07-05	This is the fifth official release. - Modified section **Creating a Key**: added the procedure for adding a tag. - Updated screenshots.
2018-05-30	This is the fourth official release. - Added **Binding a Key Pair**. - Added **Unbinding a Key Pair**. - Added **Resetting a Key Pair**. - Added **Replacing a Key Pair**. - Added the description about deleting failure records in **Viewing a Key Pair**. - Modified section **Viewing a Key Pair**: added the description about the list of ECSs bound to key pairs.

Released On	Description
2018-04-30	This is the third official release. ● Added **Adding a Tag**. ● Added section "Searching for Tags". ● Added **Modifying Tag Values**. ● Added **Deleting Tags**. ● Updated screenshots.
2018-01-30	This is the second official release. ● Added section "SSH Key Pair". ● Added **Creating a Key Pair**. ● Added **Importing a Key Pair**. ● Added **Viewing a Key Pair**. ● Added **Deleting a Key Pair**.
2017-12-31	This is the first official release.