Data Encryption Workshop

# User Guide

| | |
|---|---|
| **Issue** | 06 |
| **Date** | 2025-12-16 |

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

## Trademarks and Permissions

HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

## Notice

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

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

## Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

# Contents

**1 Creating a User and Authorizing the User the Permission to Access DEW.............. 1**

**2 Key Management Service.......................................................................................... 8**

2.1 Overview.................................................................................................................................... 8

2.2 Creating a Key......................................................................................................................... 14

2.2.1 Creating a Custom Key......................................................................................................... 14

2.2.2 Importing a Key.................................................................................................................... 19

2.3 Using a Key.............................................................................................................................. 29

2.3.1 Using KMS for Encryption.................................................................................................... 29

2.3.2 Encrypting and Decrypting Small-size Data Online Using a Custom Key..................................... 33

2.4 Managing Keys......................................................................................................................... 35

2.4.1 Viewing Key Details.............................................................................................................. 35

2.4.2 Creating an Alias for a Custom Key....................................................................................... 37

2.4.3 Adding a Tag to a Custom Key.............................................................................................. 38

2.4.4 Creating a Grant for a Custom Key........................................................................................ 40

2.4.5 Adding a Custom Key to an Enterprise Project........................................................................ 47

2.4.6 Viewing the Number of Key Accounting Requests................................................................... 48

2.4.7 Enabling Key Rotation.......................................................................................................... 50

**3 Key Pair Service.......................................................................................................55**

3.1 Overview.................................................................................................................................. 55

3.2 Creating a Key Pair.................................................................................................................. 56

3.3 Using a Key Pair....................................................................................................................... 65

3.3.1 Binding a Key Pair to an ECS................................................................................................. 65

3.3.2 Using a Private Key to Log In to the Linux ECS....................................................................... 78

3.3.3 Using a Private Key to Obtain the Login Password of Windows ECS ........................................ 80

3.4 Managing Key Pairs.................................................................................................................. 81

3.4.1 Upgrading a Private Key Pair to an Account Key Pair............................................................... 81

3.4.2 Managing Public and Private Keys.......................................................................................... 82

**4 Cloud Secret Management Service.......................................................................... 87**

4.1 Overview.................................................................................................................................. 87

4.2 Creating a Secret...................................................................................................................... 88

4.3 Managing Secrets..................................................................................................................... 95

4.3.1 Adding a Tag to a Secret........................................................................................................ 95

4.3.2 Associating a Secret with an Event 97
4.3.3 Managing Secret Versions 100
5 Dedicated HSM 104
5.1 Overview 104
5.2 Purchasing a Dedicated HSM Instance 109
5.2.1 Creating a Dedicated HSM Instance 109
5.3 Activating and Using a Dedicated HSM Instance 112
5.3.1 Activating a Dedicated HSM Instance 112
5.3.2 Using Dedicated HSM Instances 116
5.4 Managing Dedicated HSM Instances 118
5.4.1 Viewing Dedicated HSM Instances 118
5.4.2 Adding a Tag to a Dedicated HSM Instance 121
6 Tags and Quotas 125
6.1 Tag Management 125
6.1.1 Overview 125
6.1.2 Creating a Tag Policy 126
6.1.3 Creating a Tag 128
6.1.4 Searching for a Custom Key by Tag 130
6.1.5 Modifying a Tag Value 130
6.1.6 Deleting a Tag 131
6.2 Quota Adjustment 132
7 Monitoring and Auditing 134
7.1 Using Cloud Eye to Monitor DEW 134
7.1.1 Metrics Supported by DEW 134
7.1.2 Events Supported by DEW 136
7.1.3 Creating an Alarm Rule for Metrics and Events 138
7.1.4 Viewing Metric and Event Monitoring Data 145
7.2 Using CTS to Audit DEW 146
7.2.1 Operations supported by CTS 146
7.2.2 Viewing CTS Traces in the Trace List 149
8 Permissions Management 155
8.1 Creating a Custom DEW Policy 155
8.2 Critical Operation Protection 157

# 1 Creating a User and Authorizing the User the Permission to Access DEW

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

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

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

This section describes the procedure for granting permissions (see **Figure 1-1**).

## Prerequisites

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

For the system policies of other services, see **System Permissions**.

**Table 1-1** KMS system policies

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

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

**Table 1-2** KPS system policies

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

**Table 1-3** CSMS system policies

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

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

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

| Operation | KMS Administrator | KMS CMKFullAccess | DEW KeypairFullAccess | DEW KeypairReadOnlyAccess |
|---|---|---|---|---|
| Creating a key | √ | √ | x | x |
| Enable a key | √ | √ | x | x |

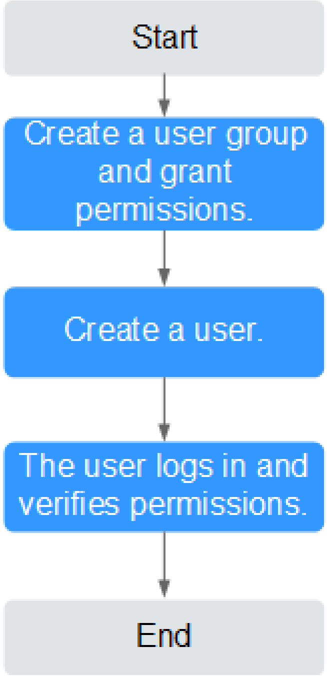
| Operation | KMS Administrator | KMS CMKFullAccess | DEW KeypairFullAccess | DEW KeypairReadOnlyAccess |
|---|---|---|---|---|
| Disable a key | √ | √ | x | x |
| Schedule key deletion | √ | √ | x | x |
| Cancel scheduled key deletion | √ | √ | x | x |
| Modify a key alias | √ | √ | x | x |
| Modify key description | √ | √ | x | x |
| Generate a random number | √ | √ | x | x |
| Create a DEK | √ | √ | x | x |
| Create a plaintext-free DEK | √ | √ | x | x |
| Encrypt a DEK | √ | √ | x | x |
| Decrypt a DEK | √ | √ | x | x |
| Obtain parameters for importing a key | √ | √ | x | x |
| Import key materials | √ | √ | x | x |
| Delete key materials | √ | √ | x | x |
| Create a grant | √ | √ | x | x |
| Revoke a grant | √ | √ | x | x |
| Retire a grant | √ | √ | x | x |
| Query the grant list | √ | √ | x | x |

| Operation | KMS Administrator | KMS CMKFullAccess | DEW KeypairFullAccess | DEW KeypairReadOnlyAccess |
|---|---|---|---|---|
| Query retirable grants | √ | √ | x | x |
| Encrypt data | √ | √ | x | x |
| Decrypt data | √ | √ | x | x |
| Send signature messages | √ | √ | x | x |
| Authenticate signature | √ | √ | x | x |
| Enabling key rotation | √ | √ | x | x |
| Modify key rotation interval | √ | √ | x | x |
| Disabling key rotation | √ | √ | x | x |
| Query key rotation status | √ | √ | x | x |
| Query CMK instances | √ | √ | x | x |
| Query key tags | √ | √ | x | x |
| Query project tags | √ | √ | x | x |
| Batch add or delete key tags | √ | √ | x | x |
| Add tags to a key | √ | √ | x | x |
| Delete key tags | √ | √ | x | x |
| Query the key list | √ | √ | x | x |
| Query key details | √ | √ | x | x |

| Operation | KMS Administrator | KMS CMKFullAccess | DEW KeypairFullAccess | DEW KeypairReadOnlyAccess |
|---|---|---|---|---|
| Query public key | √ | √ | x | x |
| Query instance quantity | √ | √ | x | x |
| Query quotas | √ | √ | x | x |
| Query the key pair list | x | x | √ | √ |
| Create or import a key pair | x | x | √ | x |
| Query key pairs | x | x | √ | √ |
| Delete a key pair | x | x | √ | x |
| Update key pair description | x | x | √ | x |
| Bind a key pair | x | x | √ | x |
| Unbind a key pair | x | x | √ | x |
| Query a binding task | x | x | √ | √ |
| Query failed tasks | x | x | √ | √ |
| Delete all failed tasks | x | x | √ | x |
| Delete a failed task | x | x | √ | x |
| Query running tasks | x | x | √ | √ |

## Authorization Process

**Figure 1-1** 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 to the management console as the created user** and verify the permissions.

   Log in to the console as newly created user, and verify that the user only has the assigned permissions.

   – Choose **Service List** > **Data Encryption Workshop**. In the navigation pane, choose **Key Pair Service**. If a message appears indicating lack of permissions, the **KMS CMKFullAccess** policy has taken effect.

   – Click **Service List** and select a service other than DEW. If a message is displayed indicating that you do not have permission to access the service, the **KMS CMKFullAccess** policy has taken effect.

## Tenant Guest Roles

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

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

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

If you want to configure the Tenant Guest role for an IAM user but do not want to have the preceding permissions, you need to configure a custom deny policy for the IAM user. For details about how to configure a custom policy, see **8.1 Creating a Custom DEW Policy**.

# 2 Key Management Service

## 2.1 Overview

KMS allows you to manage the lifecycle of keys and encrypt and decrypt data.

The core key components in KMS include **customer master keys (CMKs)** and **data encryption keys (DEKs)**. CMK, the top-level key of the user, is used to encrypt and decrypt sensitive data and generate DEKs. DEK, the second-level key in the envelope encryption process, is used to encrypt service and is protected by CMKs.

### Key Types

KMS provides default keys, custom keys, and external keys to meet security and compliance requirements in different service scenarios. The following table lists the details.

**Table 2-1** Key types

| Key Type | Scenario | Function | Algorithm Type | Key Specifications | Description |
|---|---|---|---|---|---|
| **Default key** | Used by cloud services for server-side encryption.<br>For details, see **Cloud Services Integrated with KMS**. | Only data encryption and decryption are supported. | AES | AES_256 (AES-256-GCM authentication encryption) | Default keys are created and managed by KMS. The alias of a default key ends with **/default**. |

| Key Type | Scenario | Function | Algorithm Type | Key Specifications | Description |
|---|---|---|---|---|---|
| **Custom key** | ● Created by users to build application-layer cryptographic solutions. For example, you can create a master key using the AES algorithm for custom data encryption and decryption, and create a master key using the RSA or ECC algorithm for digital signature calculation and verification.<br>● Used by cloud services for server-side encryption. | Data encryption, decryption, and digital signature are supported. | AES<br>SHA<br>RSA<br>ECC | ● Symmetric keys: AES_256 (AES-256-GCM authentication encryption mode)<br>● Summary keys: HMAC_256, HMAC_384, and HMAC_512<br>● Asymmetric keys: RSA_2048, RSA_3072, RSA_4096, EC_P256, and EC_P384<br>For details, see **Key Algorithms and Specifications Supported by KMS**. | You can create a key and manage its lifecycle on KMS, which generates **key materials**. |

| Key Type | Scenario | Function | Algorithm Type | Key Specifications | Description |
|---|---|---|---|---|---|
| | For details, see **Cloud Services Integrated with KMS**. | | | | |

| Key Type | Scenario | Function | Algorithm Type | Key Specifications | Description |
|---|---|---|---|---|---|
| **External key** | • Created by users to build application-layer cryptographic solutions. For example, you can create a master key using the AES algorithm for custom data encryption and decryption.<br>• Used by cloud services for server-side encryption. For details, see **Cloud Services Integrated with KMS**. | Data encryption, decryption, and digital signature are supported. | AES<br>RSA<br>ECC | • Symmetric keys: AES_256 (AES-256-GCM authentication encryption mode)<br>• Asymmetric keys: RSA_2048, RSA_3072, RSA_4096, EC_P256, and EC_P384<br>For details, see **Key Algorithms and Specifications Supported by KMS**. | You can create a key and manage its lifecycle on KMS. You need to import the **key materials**. |

### Key Algorithms and Specifications Supported by KMS

**Table 2-2** Key algorithms supported by KMS

| Key Type | Algorithm Type | Key Specifications | Description | Scenario |
|---|---|---|---|---|
| Symmetric key | AES | AES_256 (AES-256-GCM authentication encryption) | AES symmetric key | - Data encryption and decryption<br>- DEK encryption and decryption<br>**NOTE**<br>You can encrypt and decrypt a small amount of data using the online tool on the console.<br>You need to call APIs to encrypt and decrypt a large amount of data. |
| Digest key | SHA | - HMAC_256<br>- HMAC_384<br>- HMAC_512 | Digest key | - Data tampering prevention<br>- Data integrity verification |
| Asymmetric key | RSA | - RSA_2048<br>- RSA_3072<br>- RSA_4096 | RSA asymmetric key | - Digital signature and signature verification<br>- Data encryption and decryption<br>**NOTE**<br>Asymmetric keys are applicable to signature and signature verification scenarios. Asymmetric keys are not efficient enough for data encryption. Symmetric keys are suitable for encrypting and decrypting data. |
| Asymmetric key | ECC | - EC_P256<br>- EC_P384 | Elliptic curve recommended by NIST | Digital signature and signature verification |

**Table 2-3** describes the encryption and decryption algorithms supported for user-imported keys.

**Table 2-3** 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.<br>If the HSMs support the **RSAES_OAEP_SHA_256** algorithm, use **RSAES_OAEP_SHA_256** to encrypt key materials.<br>**NOTICE**<br>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 | |

## KMS-Created and Imported Key Materials

A key contains key metadata (key ID, key name, description, key status, and creation date) and **key materials** used for data encryption and decryption.

- When you create a custom key on the KMS console, KMS automatically generates a key material for the key.
- If you want to use your own key material, set **Source** to **External** when you create a key on KMS, and import the key material.

**Table 2-4** Differences between imported key materials and key materials generated by KMS

| Key Material Source | Difference |
|---|---|
| KMS | ● The key material cannot be manually deleted.<br>● Only symmetric keys can be rotated.<br>● You cannot set the expiration time for the key material. |

| Key Material Source | Difference |
|---|---|
| User import | ● You can delete the key material, but cannot delete the custom key or its metadata.<br>● Key rotation is not supported.<br>● When importing the key material, you can set the expiration time of the key material. After the key material expires, KMS automatically deletes the key material within 24 hours, but does not delete the custom key or its metadata.<br>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.<br>**NOTE**<br>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. |

# 2.2 Creating a Key

## 2.2.1 Creating a Custom Key

This section describes how to create a custom key on the KMS console, which includes symmetric keys and asymmetric keys. You can also perform the following operations:

- **Creating a Custom Key**
- **Enabling a Custom Key**
- **Disabling a Custom Key**
- **Scheduling the Deletion of a Key**
- **Canceling the Scheduled Deletion of a Key**

### Prerequisites

When you create a key as an IAM user, you have granted the KMS CMKFullAccess or higher permissions to the IAM user. For details, see **1 Creating a User and Authorizing the User the Permission to Access DEW**.

### Constraints

- You can create up to 100 custom keys, excluding default keys.
- Symmetric keys are created using the AES key. The AES-256 key can be used to encrypt and decrypt a small amount of data or data keys. The HMAC key is used to verify data integrity.

- Asymmetric keys are created using RSA or ECC algorithms. RSA keys can be used for encryption, decryption, digital signature, and signature verification. ECC keys can be used only for digital signature and signature verification.
- Aliases of default keys end with **/default**. When choosing aliases for your custom keys, do not use aliases ending with **/default**.
- KMS keys can be called through APIs for 20,000 times free of charge per month.

## Scenarios

- **2.3.1 Using KMS for Encryption**
- **2.3.2 Encrypting and Decrypting Small-size Data Online Using a Custom Key**
- 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 Custom Key

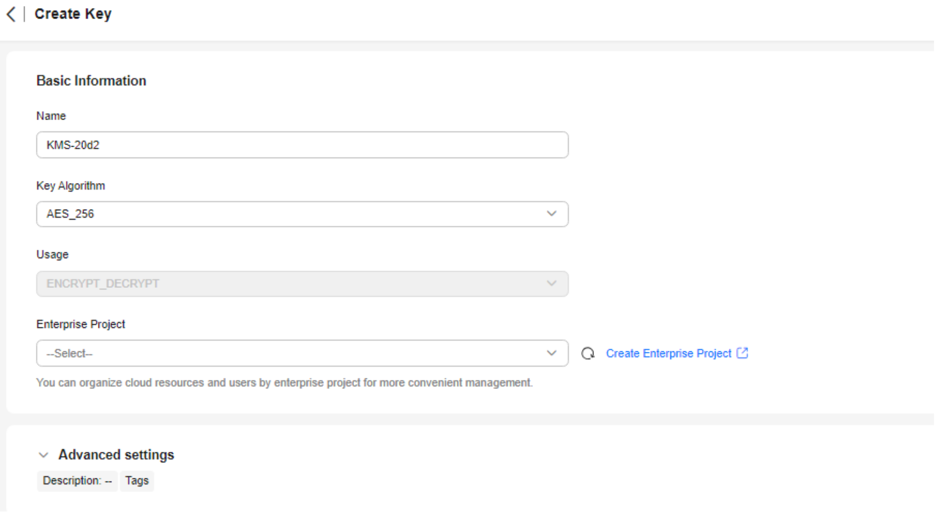
**Step 1** Log in to the **DEW console**.

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

**Step 3** Click **Create Key** in the upper right corner.

**Step 4** Configure the parameters as follows:

**Figure 2-1** Creating a key



Create Key

Basic Information

Name: KMS-20d2

Key Algorithm: AES_256

Usage: ENCRYPT_DECRYPT

Enterprise Project: --Select--

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

Advanced settings

Description: --

**Table 2-5** Key parameter configurations

| Parameter | Description |
|---|---|
| Name | Name of the key you are creating.<br>**NOTE**<br>- You can enter digits, letters, underscores (_), hyphens (-), colons (:), and slashes (/).<br>- You can enter up to 255 characters. |
| Key Algorithm | Select a key algorithm. For details about the key algorithms supported by KMS, see **Table 2-2**. |
| Usage | Key usage. The value cannot be changed after the key is created. The value can be **SIGN_VERIFY**, **ENCRYPT_DECRYPT**, or **GENERATE_VERIFY_MAC**.<br>- For AES_256 symmetric keys, the default value is **ENCRYPT_DECRYPT**.<br>- For HMAC symmetric keys, the default value is **GENERATE_VERIFY_MAC**.<br>- For RSA asymmetric keys, select **ENCRYPT_DECRYPT** or **SIGN_VERIFY**. The default value is **SIGN_VERIFY**.<br>- For ECC asymmetric keys, the default value is **SIGN_VERIFY**. You can also select **KEY_AGREEMENT**. |
| Enterprise Project | This parameter is provided for enterprise users.<br>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**.<br>If there are no **Enterprise Management** options displayed, you do not need to configure it.<br>**NOTE**<br>- 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?**<br>- For details about how to enable the enterprise project function, see **Enabling the Enterprise Center**. |
| Key Material Source | - Key management<br>- External |
| Advanced settings | - Description<br>Description of the key.<br>- Tag<br>You can add tags to a secret as you need.<br>**NOTE**<br>A maximum of 20 tags can be added for one custom key. |

**Step 5** Click **OK**.

**----End**

## Enabling a Custom Key

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

**Step 1** Locate the target key in the list and click **Enable** in the **Operation** column.

**Step 2** In the displayed dialog box, click **OK**.

NOTE

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

**----End**

## Disabling a Custom Key

This section describes how to disable a certain custom key to protect data. After a custom key is disabled, you cannot use it to encrypt or decrypt any data.

- Default keys cannot be disabled.
- A disabled key is still billable. Only deleted keys are not charged.

**Step 1** Locate the target key in the list and click **Disable** in the **Operation** column.

**Step 2** In the displayed dialog box, select **I understand the impact of disabling keys**, and click **OK**.

NOTE

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

**----End**

## Scheduling the Deletion of a Key

You cannot directly delete a key on KMS. Instead, you can set a scheduled deletion date for the key, which ranges from 7 to 1,096 days.

Only custom keys in the **Enabled**, **Disabled**, or **Pending import** state can be deleted. Default keys cannot be deleted.

NOTE

- The system will delete the key once the deletion period expires. The content encrypted using the key and the generated data key cannot be decrypted. Before deleting a key, ensure that it is no longer in use. Otherwise, your service will be unavailable. You can check the key usage in either of the following ways:
  - Check the CMK permission to determine its possible usage scope. For details, see **Querying a Grant**.
  - Check audit logs to determine the actual usage. For details, see **7.2.2 Viewing CTS Traces in the Trace List**.
- To delete a master key with replica key created, delete the replica key first.

To schedule the deletion of multiple keys at a time, select them and click **Delete** in the upper left corner of the list. The following describes how to delete a single key.

**Step 1** Locate the target key in the list and click **Delete** in the **Operation** column.

**Step 2** On the displayed page, configure **Waiting Period**.

Select **Verification Method** and complete the verification as prompted.

**Step 3** Enter **DELETE** in the confirmation dialog box if deletion verification is disabled and click **OK**.

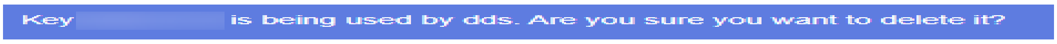
If you have enabled deletion verification, select a verification mode, click **Get Code**, enter the code, and click **OK**.

NOTE

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

**Step 4** If a key is used to encrypt DDS, RDS, or NoSQL, after you click **OK**, a message "Key *XXX* is being used by *XXX*. Are you sure you want to delete it?" is displayed, as shown in **Figure 2-2**. Click **Yes** to delete the key.

**Figure 2-2** Confirming the deletion



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

**----End**

## Canceling the Scheduled Deletion of a Key

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.

To cancel the deletion of multiple keys at a time, select them and click **Cancel Deletion** in the upper left corner of the list. The following describes how to cancel the scheduled deletion of a key.

**Step 1** Locate the target key in the list and click **Cancel Deletion** in the **Operation** column.

**Step 2** In the displayed dialog box, click **OK**.

After the cancelation, the key's status becomes **Disabled**. To enable the key, follow the instructions provided in **Enabling a Custom Key**.

**----End**

## Related Operations

- For details about how cloud services use KMS for encryption, see **Cloud Services with KMS Integrated**.
- For details about how to create a DEK and a plaintext-free DEK, see sections "Creating a DEK" and "Creating a Plaintext-Free DEK" in *Data Encryption Workshop API Reference*.
- For details about how to encrypt and decrypt a DEK for a user application, see sections "Encrypting a DEK" and "Decrypting a DEK" in *Data Encryption Workshop API Conference*.

# 2.2.2 Importing a Key

If you want to use your own key materials instead of the KMS-generated materials, you can import your key materials to KMS on the console. Keys 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

Key materials cannot be imported for HMAC digest keys and cannot be deleted for asymmetric keys.

## Important Notes

Pay attention to the following when you import key materials:

- Security

  You need to ensure that random sources meet your security requirements when using them to generate key materials. When using the import key materials 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.
- 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, as the metadata and key material of the custom key must be consistent.

## Operation Process

| Scenario | Procedure |
|---|---|
| Using existing key materials | 1. **Creating a key whose material source is external**: Create an empty key whose material source is external.<br>2. **Importing key material (existing key material)**: Import key material and token to the created empty key. |
| Downloading key materials by calling APIs | 1. **Creating a key whose material source is external**: Create an empty key whose material source is external.<br>2. **Downloading wrapping key and importing a token (by calling the API)**: Download the wrapping key and import the token by calling the API.<br>3. **Using wrapping key to encrypt key material**: Use HSM or OpenSSL to encrypt the wrapping key into key material.<br>4. **Importing key material (existing key material)**: Import key material and token to the created empty key. |
| Downloading key materials on the KMS console | 1. **Creating a key whose material source is external**: Create an empty key whose material source is external.<br>2. **Downloading wrapping key and importing the token (from the KMS console)**: Download wrapping key from the KMS console. The import token is automatically guided by the console.<br>NOTICE<br>After downloading wrapping key, do not close or exit the **Import Key Material** dialog box. After the key material is encrypted, you need to perform the **Import Key Material (Continue to Import Key Material)** in this dialog box.<br>3. **Using wrapping key to encrypt key material**: Use HSM or OpenSSL to encrypt wrapping key into key material.<br>4. **Importing Key Material (Continue Importing Key Material)**: Import the key material to the created empty key. |

## Step 1: Creating a Key Using External Materials

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

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

**Step 3** Click **Create Key** in the upper right corner of the page to create an empty key whose **Source** is **External**. For details about more parameters, see **Step 4**.

**----End**

## Step 2: Downloading the Wrapping Key and Importing Token

The key management function provides two download modes:

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

## Downloading the Wrapping Key By Calling APIs

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

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

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

- Example request

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

- Example response

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

**Step 2** Save the wrapping key and convert its format. Only the key material encrypted using the converted wrapping key can be imported to the management console.

1. Copy the content of the wrapping key **public_key**, paste it to a .txt file, and save the file as **PublicKey.b64**.
2. Use OpenSSL to run the following command to perform Base-64 coding on the content of the **PublicKey.b64** file to generate binary data, and save the converted file as **PublicKey.bin**:

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

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

**----End**

## Downloading the Wrapping Key on the KMS Console

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

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

**Step 3** In the **Custom Keys** tab, locate the key created by **Step 1: Creating a Key Using External Materials** and click **Import Key Material** in the **Operation** column.

**Step 4** In the **Download the Import Items** area, select a key wrapping algorithm based on **Key wrapping algorithm**.

**Table 2-6** 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.<br>If the HSMs support the **RSAES_OAEP_SHA_256** algorithm, use **RSAES_OAEP_SHA_256** to encrypt key materials. |

**Step 5** Click **Download Key Material** to download the wrapping key file, as shown in **Figure 2-3**.

**Figure 2-3** Downloading a 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 console automatically passes the import token. Therefore, do not close or exit the **Import Key Material** dialog box after the key material is downloaded. Otherwise, the imported token will automatically become invalid.

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

**----End**

## Step 3: Using Wrapping Key to Encrypt Key Materials

Symmetric and asymmetric key encryption modes generate different key materials.

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

## Symmetric Keys

- 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. To generate a key material for a 256-bit symmetric key, on the agent where OpenSSL has been installed, run the following command to generate the key material and save it as **PlaintextKeyMaterial.bin**:

  - AES256 symmetric key

    **openssl rand -out** ***PlaintextKeyMaterial.bin*** **32**

  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 2-7** 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** |

## Asymmetric Keys

- 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. To generate a key material for a 256-bit symmetric key, on the agent where OpenSSL has been installed, run the following command to generate the key material and save it as **PlaintextKeyMaterial.bin**:

- RSA and ECC asymmetric keys

  1) Generate a hexadecimal AES256 key.

     **openssl rand -out 0xPlaintextKeyMaterial.bin -hex 32**

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

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

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

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

**Table 2-8** 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** |

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

- Take the **RSA4096 algorithm** as an example.

  1) Generate a private key.

     **openssl genrsa -out pkcs1_rsa_private_key.pem 4096**

  2) Convert the format to PKCS8.

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

  3) Convert the PKCS8 format to the DER format.

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

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

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

NOTE

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

## Step 4: Importing Key Materials

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

- If the key material is downloaded by calling the API or the key material already exists, run the **Importing Existing Key Materials**.
- To download the key material using the KMS console, run the **Importing Key Materials**.

## Importing Existing Key Materials

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

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

**Step 3** In the **Custom Keys** tab, locate the key created by **Step 1: Creating a Key Using External Materials** and click **Import Key Material** in the **Operation** column.

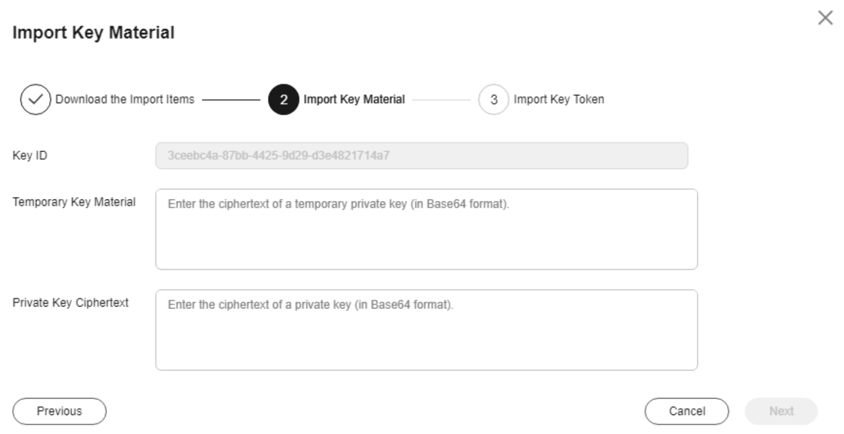
**Step 4** In the **Download the Import Items** area, select a key wrapping algorithm based on **Key wrapping algorithm**.

**Table 2-9** 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.<br>If the HSMs support the **RSAES_OAEP_SHA_256** algorithm, use **RSAES_OAEP_SHA_256** to encrypt key materials. |

**Step 5** Click **Use Existing Key Material**. In the **Import Key Material** area, enter **Key Material**.

**Figure 2-4** Importing key materials



Key ID: 3ceebc4a-87bb-4425-9d29-d3e4821714a7

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).

**Table 2-10** Key materials

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

**Step 6** Click **Next**. In the **Import Key Token** area, set parameters based on **Table 2-11**.

**Table 2-11** Parameters for importing a key token

| Parameter | Description |
|---|---|
| Key ID | Random ID of a CMK generated during the CMK creation |
| Key import token | Enter the import token obtained in **Downloading the Wrapping Key By Calling APIs**. |
| Key material expiration mode | ● **Key material will never expire**: You use this option to specify that key materials will not expire after import.<br>● **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.<br>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 7** Click **OK**. When message "Key imported successfully" is displayed in the upper right corner, the materials are imported.

NOTICE

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

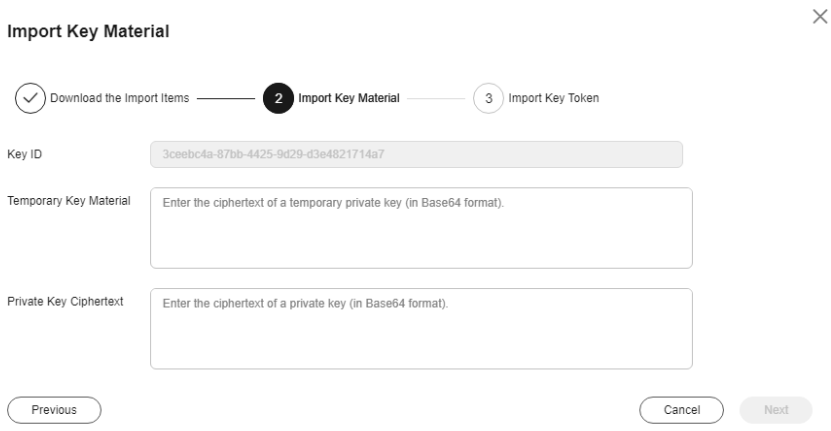
Your imported materials are displayed in the key list. The default status of an imported key is **Enabled**.

**----End**

## Importing Key Materials

**Step 1** In the **Import Key Material** dialog box (**Step 5**) on the management console, add the **Key Material** file in the **Import Key Material** configuration item.

**Figure 2-5** Importing key materials



Import Key Material

Key ID: 3ceebc4a-87bb-4425-9d29-d3e4821714a7

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).

**Table 2-12** Key materials

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

**Step 2** Click **Next** to go to the **Import Key Token** step. Configure the parameters as described in **Table 2-13**.

**Table 2-13** Parameters for importing a key token

| Parameter | Description |
|---|---|
| Key ID | Random ID of a CMK generated during the CMK creation |
| Key material expiration mode | ● **Key material will never expire**: You use this option to specify that key materials will not expire after import.<br>● **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.<br>After the key material expires, the system automatically deletes the key material within 24 hours. Once the key material is deleted, the key cannot be used and its status changes to **Pending import**. |

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

NOTICE

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

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

**----End**

## Deleting Key Materials

After the imported key materials are expired or deleted, the key using the materials becomes unavailable and its status changes to **Pending import**. In this case, you need to **import the same key materials again**. Only by then can the custom key decrypts all data encrypted before the key material is deleted.

NOTE

Key materials cannot be deleted for asymmetric keys.

To delete key materials, use either of the following methods:

- **Method 1**: KMS deletes expired key materials.

  When you import key materials, specify the expiration time. KMS will delete the key materials after they expire.

- **Method 2**: Delete key materials on the console.

  a. Locate the target key material and choose **More** > **Delete Key Material**.

  b. In the displayed dialog box, enter **DELETE**, and click **OK**. When **Key material deleted successfully** is displayed in the upper right corner, the key materials are deleted.

### Importing the Same Key Materials Again

When key materials are expired or deleted, you need to import the same materials again to continue using the key.

1. Download the wrapping public key and import token again. For details, see **Step 2: Downloading the Wrapping Key and Importing Token**.

   📖 NOTE

   Key wrapping will not affect key materials. Therefore, you can use different wrapping public keys and algorithms to import the same key materials.

2. Use the wrapping public key to encrypt the key materials. For details, see **Step 3: Using Wrapping Key to Encrypt Key Materials**.

   📖 NOTE

   The key materials must be those used before expiration.

3. Use the import token to import the encrypted key materials. For details, see **Step 4: Importing Key Materials**.

# 2.3 Using a Key

## 2.3.1 Using KMS for Encryption

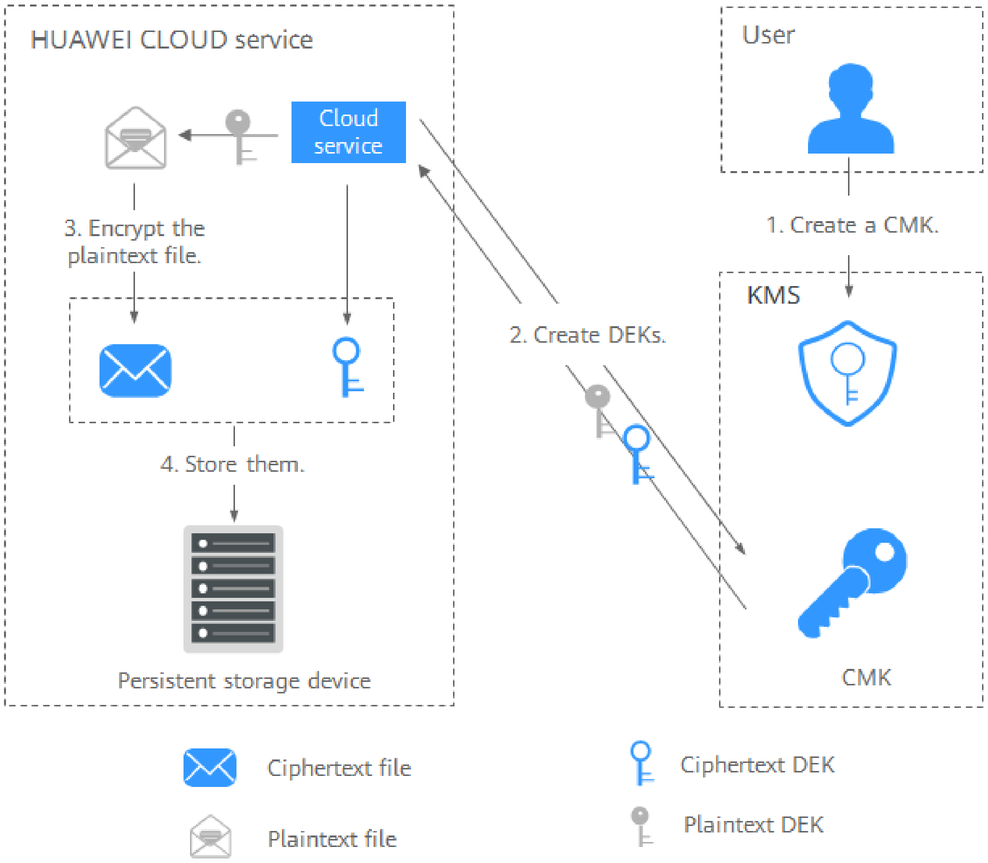
### Prerequisites

All the custom keys mentioned in this section are symmetric keys. For details about symmetric keys and asymmetric keys, see **Key Types**.

### Interacting with Huawei Cloud Services

Huawei Cloud services use the envelope encryption technology and call KMS APIs to encrypt service resources. Your CMKs are under your own management. With your grant, Huawei Cloud services use a specific custom key of yours to encrypt data. For details about cloud services using KMS for encryption, see **Cloud Services with KMS Integrated**.

**Figure 2-6** How Huawei Cloud uses KMS for encryption



The encryption process is as follows:

1. Create a custom key on KMS.
2. Huawei Cloud services call the **create-datakey** API of the KMS to create a DEK. Then you get a plaintext DEK and a ciphertext DEK.

   NOTE

   Ciphertext DEKs are generated when you use a CMK to encrypt the plaintext DEKs.
3. Huawei Cloud services use the plaintext DEK to encrypt a plaintext file, generating a ciphertext file.
4. Huawei Cloud services store the ciphertext DEK and ciphertext file in a persistent storage device or a storage service.

NOTE

When users download the data from a Huawei Cloud service, the service uses the custom key specified by KMS to decrypt the ciphertext DEK, uses the decrypted DEK to decrypt data, and then provides the decrypted data for users to download.

## Working with User Applications

To encrypt plaintext data, a user application can call the necessary KMS API to create a DEK. The DEK can then be used to encrypt the plaintext data. Then the application can store the encrypted data. In addition, the user application can call the KMS API to create CMKs. DEKs can be stored in ciphertext after being encrypted with the CMKs.

Envelope encryption is implemented, with CMKs stored in KMS and ciphertext DEKs in user applications. KMS is called to decrypt a ciphertext DEK only when necessary.

The encryption process is as follows:

1. The application calls the **create-key** API of KMS to create a custom key.
2. The application calls the **create-datakey** API of KMS to create a DEK. Then you get a plaintext DEK and a ciphertext DEK.

   NOTE

   Ciphertext DEKs are generated when you use a CMK to encrypt the plaintext DEKs in **1**.
3. The application uses the plaintext DEK to encrypt a plaintext file. A ciphertext file is generated.
4. The application saves the ciphertext DEK and the ciphertext file together in a persistent storage device or a storage service.

## Cloud Services with KMS Integrated

KMS provides CMK management and encryption capabilities for cloud services.

**Table 2-14** Cloud services supported by KMS

| Service Name | How to Use | Reference |
|---|---|---|
| Object Storage Service (OBS) | You can upload objects to and download them from OBS in common mode or server-side encryption mode. When you upload objects in encryption mode, data is encrypted at the server side and then securely stored on OBS in ciphertext. When you download encrypted objects, the data in ciphertext is decrypted at the server side and then provided to you in plaintext. OBS supports the server-side encryption with KMS-managed keys (SSE-KMS). In this mode, OBS uses the keys provided by KMS for server-side encryption. | **Encrypting Data in OBS** |
| Elastic Volume Service (EVS) | If you enable the encryption function when creating an EVS disk, the disk will be encrypted with the DEK generated by using your CMK. Data stored in the EVS disk will be automatically encrypted. | **Encrypting Data in EVS** |

| Service Name | How to Use | Reference |
|---|---|---|
| Image Management Service (IMS) | When creating a private image using an external image file, you can enable the private image encryption function and select a CMK provided by KMS to encrypt the image. | **Encrypting Data in IMS** |
| Relational Database Service (RDS) | When purchasing a database instance, you can enable the disk encryption function of the database instance and select a CMK created on KMS to encrypt the disk of the database instance. Enabling the disk encryption function will enhance data security. | **Encrypting an RDS DB Instance** |
| Document Database Service (DDS) | When purchasing a DDS instance, you can enable the disk encryption function of the instance and select a CMK created on KMS to encrypt the disk of the instance. Enabling the disk encryption function will enhance data security. | **Encrypting a DDS DB Instance** |
| Elastic Cloud Server (ECS) | ECS uses image encryption or data disk encryption to encrypt ECS resources.<br>● When creating an ECS, if you select an encrypted image, the system disk of the created ECS automatically has encryption enabled, with its encryption mode same as the image encryption mode. For details about image encryption, see **Encrypting Data in IMS**.<br>● When creating an ECS, you can encrypt added data disks.<br>For details about data disk encryption, see **Encrypting Data in IMS**. | **Encrypting Data in ECS** |
| Scalable File Service Turbo (SFS Turbo) | When creating an SFS Turbo file system, use the key provided by KMS to encrypt the file system for core data security. | **Creating an SFS Turbo File System** |
| FunctionGraph | To decrypt sensitive data, such as database passwords and API keys, during function runtime, you can use the KMS SDK to dynamically operate keys. You can host encryption and decryption keys in KMS and create an agency in IAM for FunctionGraph to access KMS. | **Asset Identification and Management** |
| Cloud Operations Center (COC) | COC uses KMS to encrypt your host accounts for better security. Before using KMS, create a key first. | **Key Management** |

| Service Name | How to Use | Reference |
|---|---|---|
| Cloud Data Migration (CDM) | When migrating files to a file system, CDM can encrypt and decrypt the files using the keys provided by KMS. | **Encryption and Decryption During File Migration** |
| Data Security Center (DSC) | You can use the encryption algorithms and encryption master keys to generate an encryption configuration for data masking. | **Configuring a Data Masking Rule** |
| Workspace | You can use the key provided by KMS to encrypt disks when purchasing a workspace. | **Purchasing Yearly/Monthly-billed Desktops** |
| GeminiDB | You can use the key provided by KMS to encrypt static data in the database when purchasing a GeminiDB instance. | **Buying and Connecting to a Cluster Instance** |

## 2.3.2 Encrypting and Decrypting Small-size Data Online Using a Custom Key

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

### Prerequisites

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

### Constraints

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

### Encrypting Data

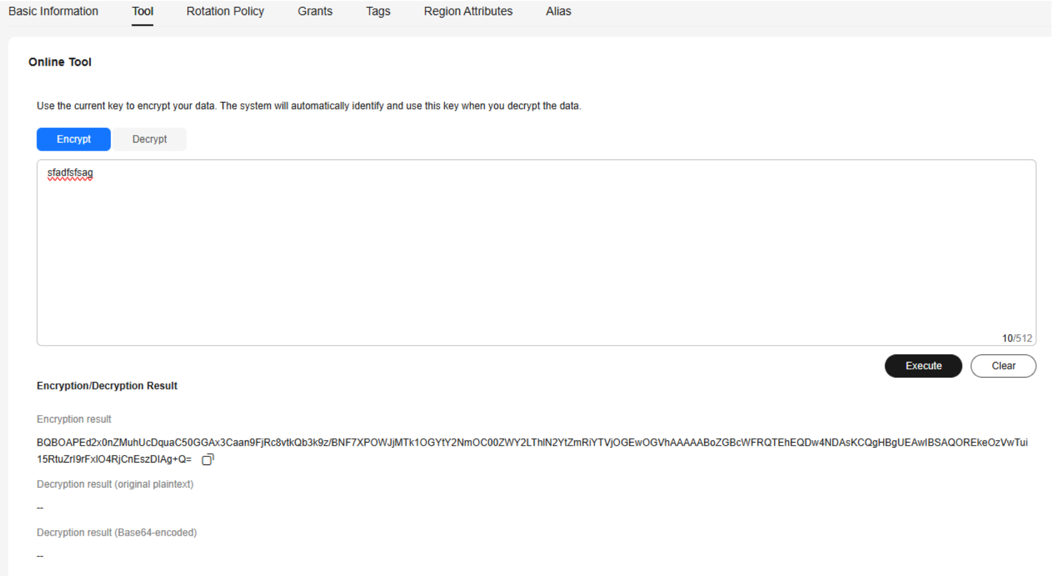
**Step 1** Log in to the **DEW console**.

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

**Step 3** Click the name of the target custom key to access the key details page. Click the **Tool** tab.

**Step 4** Click **Encrypt**. In the text box on the left, enter the data to be encrypted, as shown in **Figure 2-7**.

**Figure 2-7** 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.

sfadfsfsag

10/512

Encryption/Decryption Result

Encryption result

BQBOAPEd2x0nZMuhUcDquaC50GGAx3Caan9FjRc8vtkQb3k9z/BNF7XPOWJjMTk1OGYtY2NmOC00ZWY2LThlN2YtZmRiYTVjOGEwOGVhAAAAABoZGBcWFRQTEhEQDw4NDAsKCQgHBgUEAwIBSAQOREkeOzVwTui15RtuZrI9rFxlO4RjCnEszDIAg+Q=

Decryption result (original plaintext)

--

Decryption result (Base64-encoded)

--

**Step 5** Click **Execute**. The encrypted data is displayed in the **Encryption/Decryption Result** area.

NOTE

- Use the current CMK to encrypt the data.
- To clear your input, click **Clear**.
- In the **Encryption result** area, click to copy the encrypted data and save it to a local file.

**----End**

## Decrypting Data

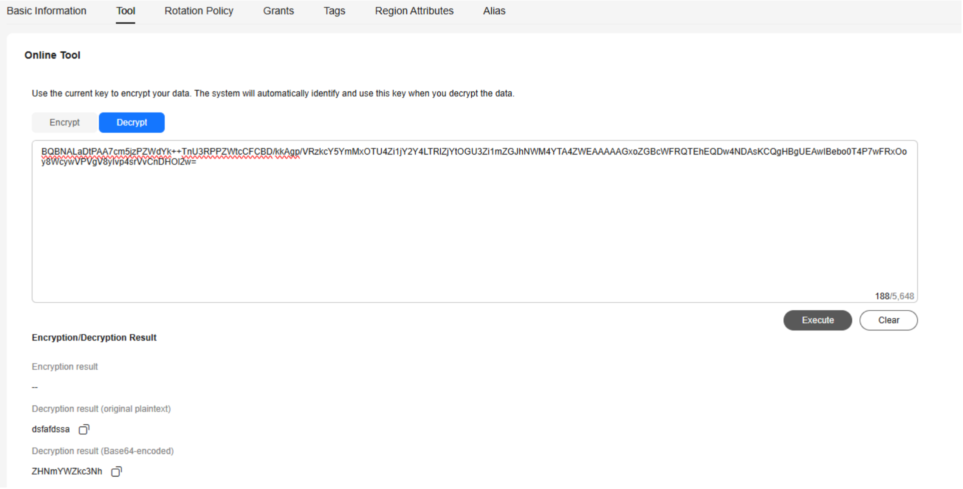
**Step 1** Click a non-default key in the **Enabled** state and go to the **Tool** tab.

**Step 2** Click **Decrypt** and enter the data to be decrypted in the text box, as shown in **Figure 2-8**.

NOTE

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

**Figure 2-8** Decrypting 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.

```
BQBNALaDtPAA7cm5jzPZWdYk++TnU3RPPZWtcCFCBD/kkAgp/VRzkcY5YmMxOTU4Zi1jY2Y4LTRlZjYtOGU3Zi1mZGJhNWM4YTA4ZWEAAAAAGxoZGBcWFRQTEhEQDw4NDAsKCQgHBgUEAwIBebo0T4P7wFRxOo
y8WcywVPVgV8ylvp4srVvCnDHOl2w=
```

Encryption/Decryption Result

Encryption result

--

Decryption result (original plaintext)

dsfafdssa ⧉

Decryption result (Base64-encoded)

ZHNmYWZkc3Nh ⧉

**Step 3** Click **Execute**. The decrypted data is displayed in the **Encryption/Decryption Result** area.

NOTE

- In the **Decryption result** area, click ⧉ to copy the decrypted data and save it to a local file.
- The information to be encrypted using commands or APIs cannot contain special characters. Otherwise, the decryption result may fail to be displayed on the console.
- Enter the plaintext on the console, the text will be encoded to Base64 format before encryption.

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

**----End**

# 2.4 Managing Keys

## 2.4.1 Viewing Key Details

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

### Procedure

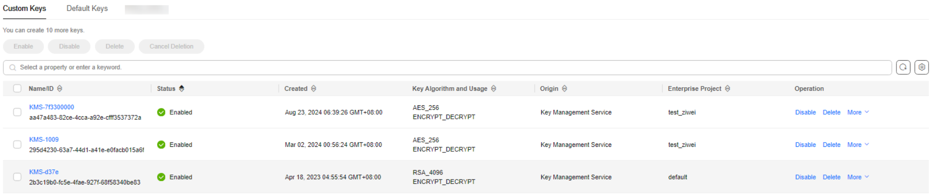
**Step 1** Log in to the **DEW console**.

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

**Step 3** Check the key list. **Table 2-15** describes the parameters.

Click the search bar and select the criteria for filtering keys. Search for a key by specifying attributes.

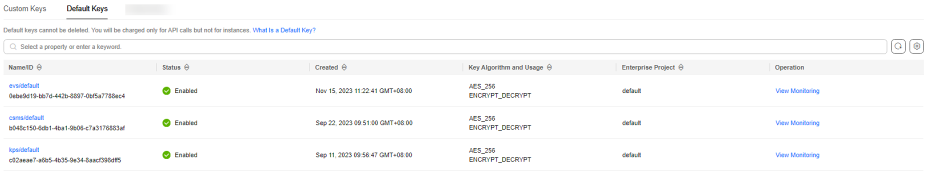
**Figure 2-9** Custom keys



You can create 10 more keys.

| | Name/ID | Status | Created | Key Algorithm and Usage | Origin | Enterprise Project | Operation |
|---|---|---|---|---|---|---|---|
| □ | KMS-7f3300000<br>aa47a483-82ce-4cca-a92e-cfff3537372a | Enabled | Aug 23, 2024 06:39:26 GMT+08:00 | AES_256<br>ENCRYPT_DECRYPT | Key Management Service | test_ziwei | Disable Delete More |
| □ | KMS-1009<br>295d4230-63a7-44d1-a41e-e0facb015a6f | Enabled | Mar 02, 2024 00:56:24 GMT+08:00 | AES_256<br>ENCRYPT_DECRYPT | Key Management Service | test_ziwei | Disable Delete More |
| □ | KMS-d37e<br>2b3c19b0-fc5e-4fae-927f-68f58340be83 | Enabled | Apr 18, 2023 04:55:54 GMT+08:00 | RSA_4096<br>ENCRYPT_DECRYPT | Key Management Service | default | Disable Delete More |

**Figure 2-10** Default keys



Default keys cannot be deleted. You will be charged only for API calls but not for instances. What Is a Default Key?

| Name/ID | Status | Created | Key Algorithm and Usage | Enterprise Project | Operation |
|---|---|---|---|---|---|
| evs/default<br>0ebe9d19-bb7d-442b-8897-0bf5a7788ec4 | Enabled | Nov 15, 2023 11:22:41 GMT+08:00 | AES_256<br>ENCRYPT_DECRYPT | default | View Monitoring |
| csms/default<br>b048c150-6db1-4ba1-9b06-c7a3176883af | Enabled | Sep 22, 2023 09:51:00 GMT+08:00 | AES_256<br>ENCRYPT_DECRYPT | default | View Monitoring |
| kps/default<br>c02aeae7-a6b5-4b35-9e34-8aacf398dff5 | Enabled | Sep 11, 2023 09:56:47 GMT+08:00 | AES_256<br>ENCRYPT_DECRYPT | default | View Monitoring |

**Table 2-15** Key list parameters

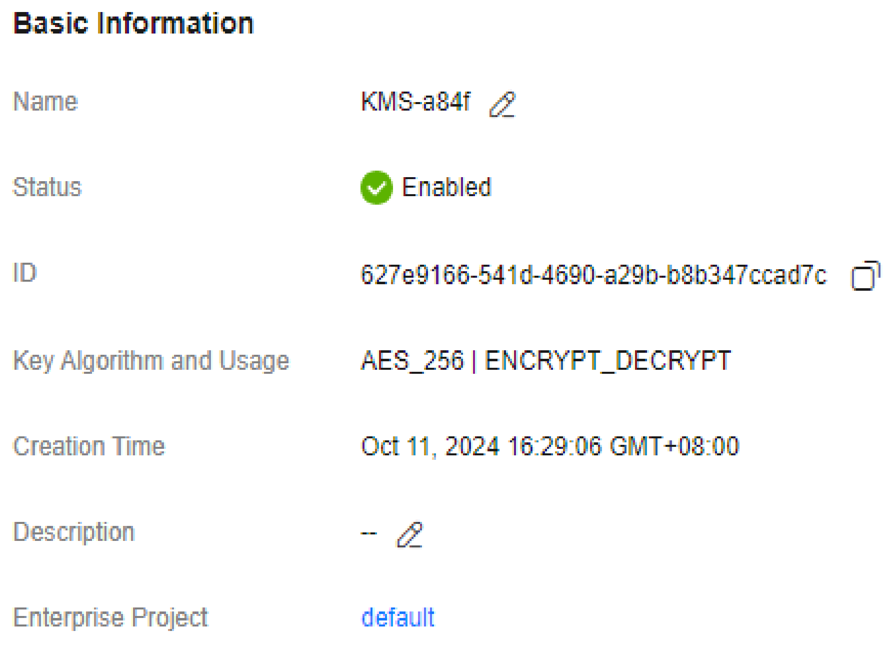
| Parameter | Description |
|---|---|
| Name/ID | Name of a key and the random ID of a key generated during its creation.<br>**NOTE**<br>Use this ID as the value of **Path** if you are creating a custom policy in IAM and have selected **Specify resource path** for **KeyId**. |
| Status | Status of a CMK, which can be one of the following:<br>● **Enabled**<br>The CMK is enabled.<br>● **Disabled**<br>The CMK is disabled.<br>● **Pending deletion**<br>The CMK is scheduled for deletion.<br>● **Pending import**<br>If your CMK does not have materials, its status is **Pending import**. |
| Created | Creation time of the CMK |
| Key Algorithm and Usage | Key algorithm selected during key creation and its usage |
| Origin | Source of key material, which can be one of the following:<br>● **External**<br>The key is imported to the KMS from an external system.<br>● **Key Management Service**<br>The key is a default key or created in KMS. |
| Enterprise Project | Enterprise project the CMK is used for |

**Step 4** You can click the key name to view its details, as shown in **Figure 2-11**.

Hover the cursor over the target key and click ✎ to modify the name or description.

- A default key, whose alias suffix is **/default**, does not allow name or description changes.
- A key in the **Pending deletion** state does not allow name or description changes.

**Figure 2-11** Key details



**Basic Information**

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

**----End**

## 2.4.2 Creating an Alias for a Custom Key

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

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

### Constraints

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

### Creating an Alias for a Custom Key

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

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

**Step 3** Click the target key name. On the key details page, click the **Alias** tab.

**Step 4** Click **Create Alias**. Enter the alias in the displayed dialog box and click **OK**.

NOTE

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

**----End**

## Deleting an Alias

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

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

**Step 3** Click the target key name. On the key details page, click the **Alias** tab.

**Step 4** Locate the target alias and click **Delete** in the **Operation** column.

**Step 5** In the displayed dialog box, select **Verification Method**, perform operations as prompted, and click **OK**.

**----End**

# 2.4.3 Adding a Tag to a Custom Key

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.

## Adding a Tag to a Custom Key

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

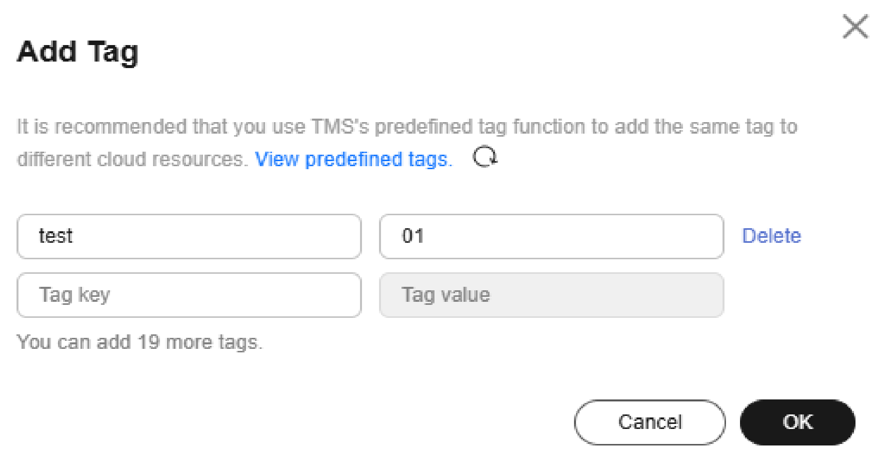
**Step 2** Click 📍 in the upper left corner and select a region or project.

**Step 3** Click the custom key name to access its details page.

**Step 4** Click **Tags** to go to the tag management tab.

**Step 5** Click **Add Tag**, as shown in **Figure 2-12**. In the **Add Tag** dialog box, enter the tag key and tag value. **Table 2-16** describes the parameters.

**Figure 2-12** 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 |
|---|---|
| test | 01 |

You can add 19 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*.
- If you want to delete a tag from the tag list when adding multiple tags, locate the target tag and click **Delete** on the right.

**Table 2-16** Tag parameters

| Parameter | Description | Value | Example Value |
|---|---|---|---|
| Tag key | Name of a tag.<br>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.<br>A maximum of 20 tags can be added for one custom key. | • Mandatory.<br>• The tag key must be unique for the same custom key.<br>• 128 characters limit.<br>• The value cannot start or end with a space.<br>• Cannot start with **_sys_**.<br>• The following character types are allowed:<br>– Chinese<br>– English<br>– Numbers<br>– Space<br>– Special characters: _.:/=+-@ | cost |

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

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

**----End**

## Modifying a Tag Value

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

**Step 1** Click the target custom key alias to access its details page.

**Step 2** Click the **Tags** tab.

**Step 3** Locate the target tag in the list and click **Edit** in the **Operation** column.

**Step 4** In the displayed **Edit Tag** dialog box, enter a tag value, and click **OK**.

**----End**

## Deleting a Tag

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

**Step 1** Click the target custom key alias to access its details page.

**Step 2** Click the **Tags** tab.

**Step 3** Locate the target tag in the list and click **Delete** in the **Operation** column.

**Step 4** In the displayed **Delete Tag** dialog box, click **Yes**.

**----End**

# 2.4.4 Creating a Grant for a Custom Key

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 IAM user or account to be authorized.
  - User ID: To obtain the user ID, hover the cursor over the username in the upper right corner, and choose **My Credentials**. On the displayed **API Credentials** page, obtain the IAM user ID.
  - Account ID: To obtain the account ID, hover the cursor over the username in the upper right corner, and choose **My Credentials**. On the displayed **API Credentials** page, obtain the account ID.
- The custom key is in the **Enabled** state.

## 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.

## Creating a Grant for a Custom Key

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

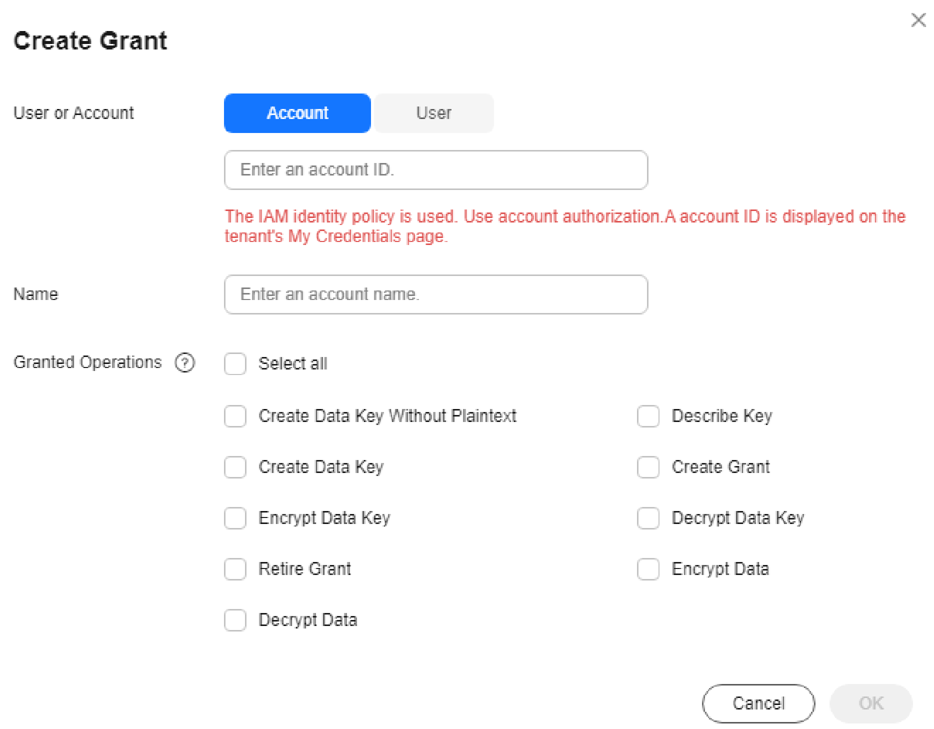
**Step 2** Click 📍 in the upper left corner and select a region or project.

**Step 3** Click the name of the target custom key to go to its details page and create a grant on it.

**Step 4** Click the **Grants** tab.

**Step 5** Click **Create Grant**. The **Create Grant** dialog box is displayed.

**Figure 2-13** Creating a grant (for an account)



Create Grant

User or Account: Account

Enter an account ID.

The IAM identity policy is used. Use account authorization.A account ID is displayed on the tenant's My Credentials page.

Name: Enter an account name.

Granted Operations

□ Select all

□ Create Data Key Without Plaintext
□ Describe Key
□ Create Data Key
□ Create Grant
□ Encrypt Data Key
□ Decrypt Data Key
□ Retire Grant
□ Encrypt Data
□ Decrypt Data

**Step 6** In the displayed dialog box, set the parameters by referring to **Table 2-17**.

NOTICE

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

**Table 2-17** Parameters for creating a grant

| Parameter | Description | Example Value |
|---|---|---|
| User or Account | Whether a user or an account is granted.<br>● **User**<br>User ID: To obtain the user ID, hover the cursor over the username in the upper right corner, and choose **My Credentials**. On the displayed **API Credentials** page, obtain the IAM user ID.<br>After the grant is created, the IAM user can use the specified keys.<br>● **Account**<br>Account ID: To obtain the account ID, hover the cursor over the username in the upper right corner, and choose **My Credentials**. On the displayed **API Credentials** page, obtain the account ID.<br>After the grant is created, all IAM users under the account can use the specified keys. | d9a6b2bdaedd4ba586cabe6372d1b312 |
| Name | You can name the grant.<br>**NOTE**<br>● You can enter digits, letters, underscores (_), hyphens (-), colons (:), and slashes (/). | test |

| Parameter | Description | Example Value |
|---|---|---|
| Granted Operations | The allowed grants are shown below.<br>**NOTE**<br>● 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.<br>● This parameter cannot be left blank.<br>● Selecting only **Create Grant** is not allowed.<br>● **Create Data Key Without Plaintext**<br>● **Create Data Key**<br>● **Encrypt Data Key**<br>● **Decrypt Data Key**<br>● **Query Key Details**<br>● **Create Grant**<br>● **Retire Grant**<br>– A grantee can retire a grant if the grantee does not need that permission.<br>– 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.<br>● **Encrypt Data**<br>● **Decrypt Data**<br>You can select multiple grants. The following grants can be created for all keys:<br>● **Query Key Details**<br>● **Create Grant**<br>● **Retire Grant**<br>For details about how to authorize a key algorithm, see **Table 2-18**. | - |

**Table 2-18** Granting operations

| Key Algorithm | Key Type | Usage | Granted Operations |
|---|---|---|---|
| • AES_256 | Symmetric key | ENCRYPT_DECRYPT | • Create Data Key Without Plaintext<br>• Create Data Key<br>• Encrypt Data Key<br>• Decrypt Data Key<br>• Encrypt Data<br>• Decrypt Data<br>• Create Data Key Pair<br>• Query Key Details<br>• Create Grant<br>• Retire Grant |
| • RSA_2048<br>• RSA_3072<br>• RSA_4096<br>• EC_P256<br>• EC_P384 | Asymmetric key | SIGN_VERIFY | • Query Key Details<br>• Query Public Key Information<br>• Create Grant<br>• Retire Grant<br>• Signature<br>• Signature Verification |
| • RSA_2048<br>• RSA_3072<br>• RSA_4096 | Asymmetric key | ENCRYPT_DECRYPT | • Query Key Details<br>• Create Grant<br>• Retire Grant<br>• Query Public Key Information<br>• Encrypt Data<br>• Decrypt Data |
| • HMAC_256<br>• HMAC_384<br>• HMAC_512 | Digest key | GENERATE_VERIFY_MAC | • Generate HMAC<br>• Verify HMAC |

**Step 7** Click **OK**. When message **Grant created successfully** is displayed in the upper right corner, the grant has been created.

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

**----End**

## Querying a Grant

You can view the details about a custom key grant on the KMS console, such as the grant ID, grantee user ID, granted operation, and creation time.

**Step 1** Click the target custom key alias to access its details page.

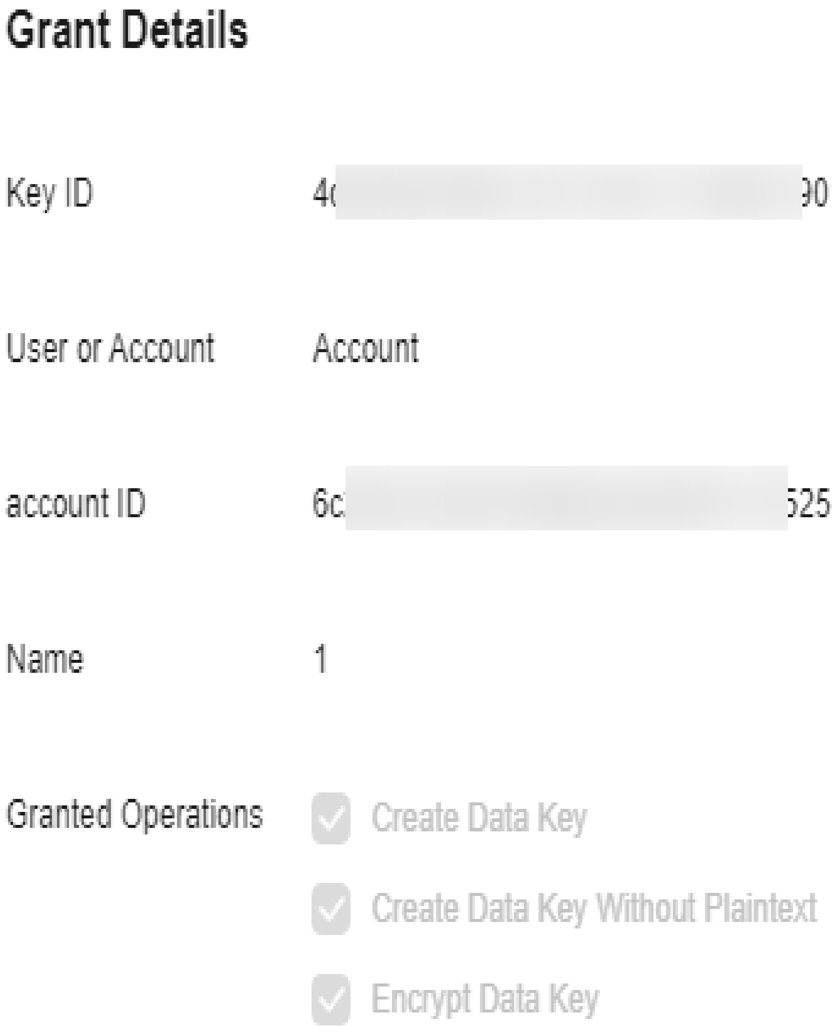
**Step 2** Click the **Grants** tab to view the grants created for the custom key. **Table 2-19** describes the parameters.

**Table 2-19** Parameters

| Parameter | Description |
|---|---|
| Grant Name | Name of the grant when created |
| Granted To | Whether permissions are granted to a user or account. |
| Operations | Authorized operations (such as **Create Data Key**) on the custom key |
| Creation Time | Time when the grant is created |

**Step 3** Click the target grant, the grant details are displayed on the right, as shown in **Figure 2-14**.

**Figure 2-14** Viewing grant details



## Grant Details

| | |
|---|---|
| Key ID | [redacted] |
| User or Account | Account |
| account ID | [redacted] |
| Name | 1 |
| Granted Operations | ☑ Create Data Key<br>☑ Create Data Key Without Plaintext<br>☑ Encrypt Data Key |

**----End**

## 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.

**Step 1** Click the target custom key alias to access its details page.

**Step 2** In the **Grants** tab, locate the target grant and click **Revoke Grant** in the **Operation** column.

**Step 3** Enter **DELETE** in the confirmation dialog box and click **OK** if verification is not enabled.

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

NOTE

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

**----End**

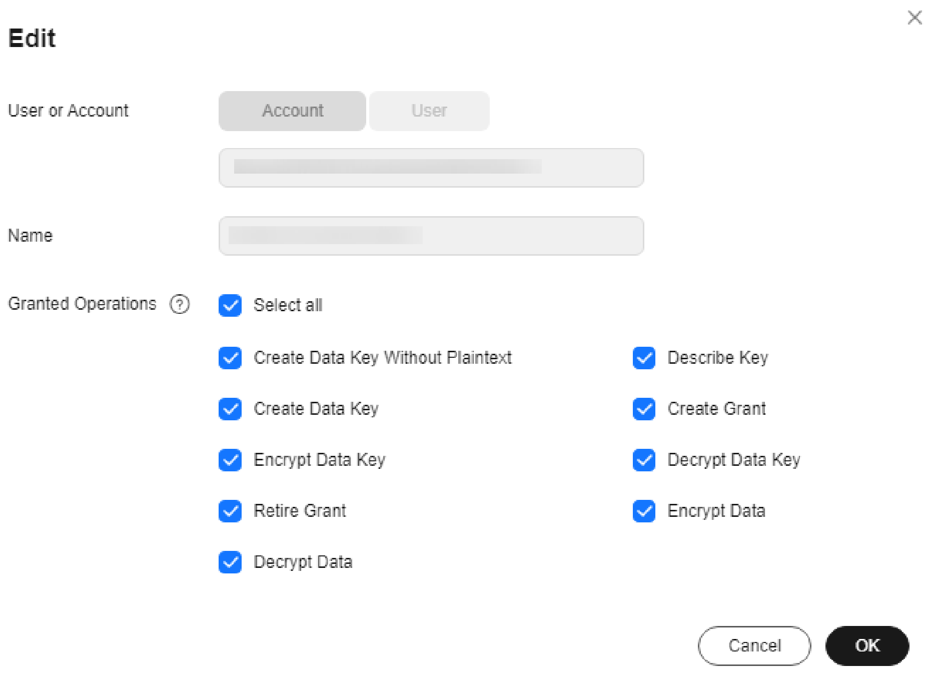
## Editing a Grant

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

**Step 1** Click the target custom key alias to access its details page.

**Step 2** In the **Grants** tab, locate the target grant, click **Edit** in the **Operation** column, and select the granted operations to be edited, as shown in **Figure 2-15**.

**Figure 2-15** Editing a grant



Edit

User or Account: Account | User

Name

Granted Operations:

☑ Select all

☑ Create Data Key Without Plaintext
☑ Describe Key
☑ Create Data Key
☑ Create Grant
☑ Encrypt Data Key
☑ Decrypt Data Key
☑ Retire Grant
☑ Encrypt Data
☑ Decrypt Data

Cancel | OK

**Step 3** Click **OK**.

**----End**

## 2.4.5 Adding a Custom Key to an Enterprise Project

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

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

## Constraints

- The enterprise project management function has been enabled.

  If you did not enable the enterprise project management function, the **Enterprise Project** option is not displayed on the console by default, and you cannot add keys to a project. For details about how to enable an enterprise project, see **Enabling Enterprise Center**.
- The enterprise project of default keys cannot be changed.

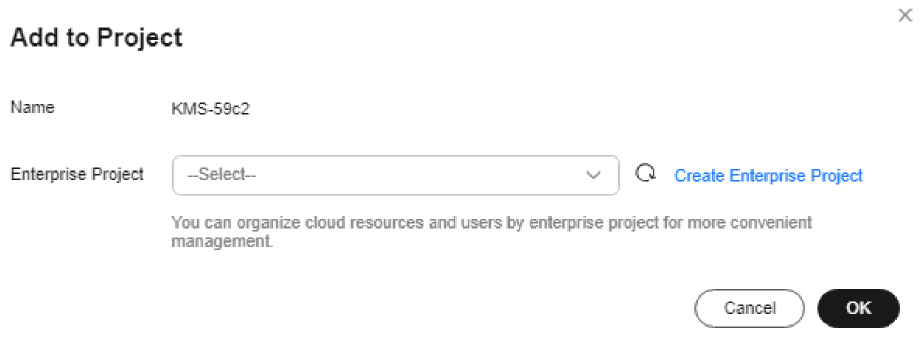
## Procedure

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

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

**Step 3** Locate the target key and choose **More** > **Add to Project** in the **Operation** column.

**Figure 2-16** Adding a key to a project



Add to Project

Name KMS-59c2

Enterprise Project --Select--

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

NOTE

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

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

**Step 4** Select a project. Click **OK**.

**----End**

## 2.4.6 Viewing the Number of Key Accounting Requests

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

## Constraints

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

## Viewing Monitoring Details of a Key

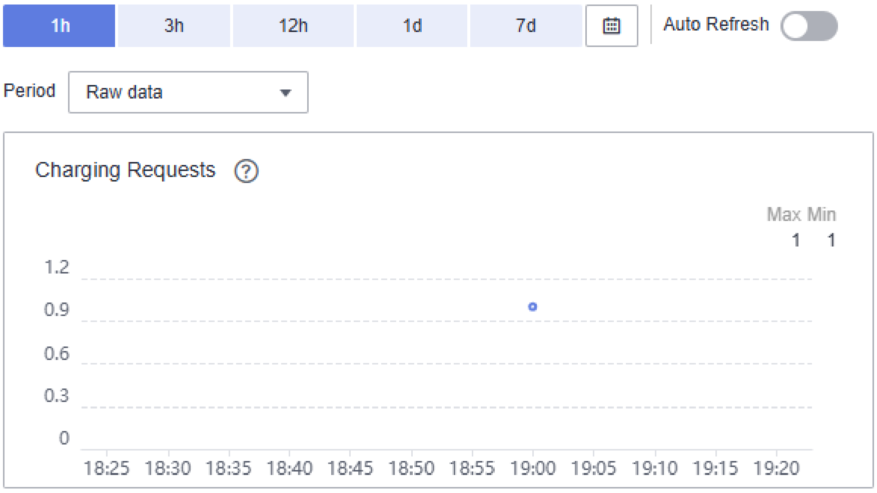
**Step 1** Log in to the **DEW console**.

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

**Step 3** Locate the target key and choose **More** > **View Monitoring** in the **Operation** column.

**Step 4** On the key details page, key calling details are displayed, as shown in **Figure 2-17**.

**Figure 2-17** Monitoring details of a key



NOTE

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

**----End**

## Viewing Monitoring Details of Multiple Keys

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

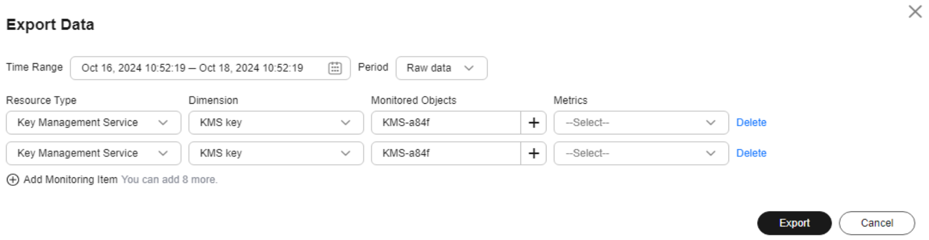
**Step 2** Click in the upper left corner and select a region or project.

**Step 3** Click ☰ in the upper left corner and choose **Management & Governance** > **Cloud Eye**. The **Overview** page is displayed.

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

**Step 5** Select multiple target keys, click **Export Data** in the upper left corner of the page, set parameters, and click **Export**.

**Figure 2-18** Exporting monitoring data



Export Data

Time Range: Oct 16, 2024 10:52:19 — Oct 18, 2024 10:52:19
Period: Raw data

| Resource Type | Dimension | Monitored Objects | Metrics |
|---|---|---|---|
| Key Management Service | KMS key | KMS-a84f | --Select-- |
| Key Management Service | KMS key | KMS-a84f | --Select-- |

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

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

**----End**

## 2.4.7 Enabling Key Rotation

KMS allows you to periodically rotate keys to enhance security for keys and service data. This section describes how keys are rotated in KMS and how to configure key rotation.

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.

### 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 amount of data. The amount of data encrypted a key refers to the total number of bytes or messages encrypted using the key.

- To enhance the capability of responding to security events.

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

- To enhance the data isolation capability.

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

### Key Rotation Methods

You can use either of the following key rotation methods:

- Manual key rotation

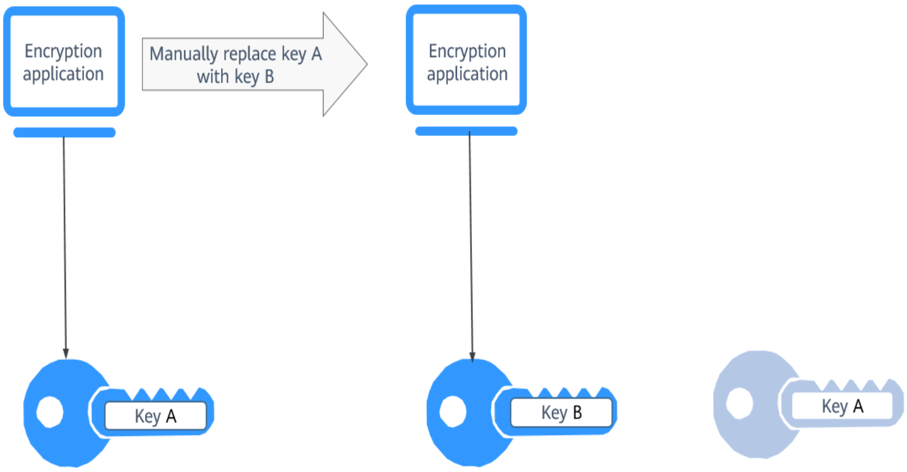
Method 1: Create a key B to replace the currently used key A.

Method 2: Modify the key A and use it.

An example command is provided as follows:

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

**Figure 2-19** Manual key rotation



- Automatic key rotation

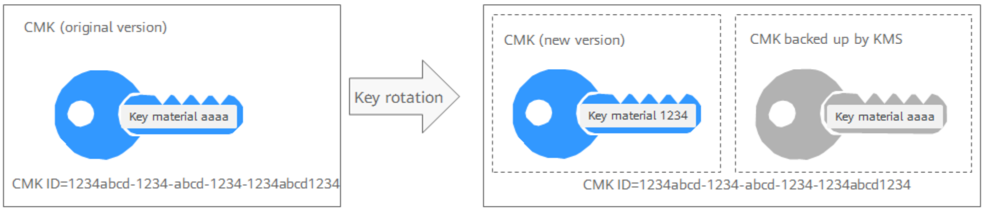
  KMS automatically rotates keys based on the configured rotation period (365 days by default). The system automatically generates a new key to replace the key in use. Automatic key rotation only changes the key material of a CMK. The logical attributes of the key will not change, including its key ID, 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 2-20** 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 2-20** Key rotation modes

| Key Type | Rotation Mode |
|---|---|
| Default key | Cannot be rotated. |
| Custom key | Keys can be rotated automatically or manually, depending on the key algorithm type.<br>● Symmetric key: Can be automatically or manually rotated.<br>● 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. |
| 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. |

NOTE

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

## Constraints

- A disabled custom key is never rotated, even if rotation is enabled for it.

  KMS resumes rotation when this custom key is enabled. If you enable this custom key after one rotation period has passed, KMS will rotate it within 24 hours.
- Only CMKs can be rotated.
- Only symmetric keys can be rotated.

- Key rotation is supported only for enabled keys with KMS-generated key materials.
- Enabling key rotation may incur additional fees. For details, see **Billing Description**.

## Enabling Key Rotation

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

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

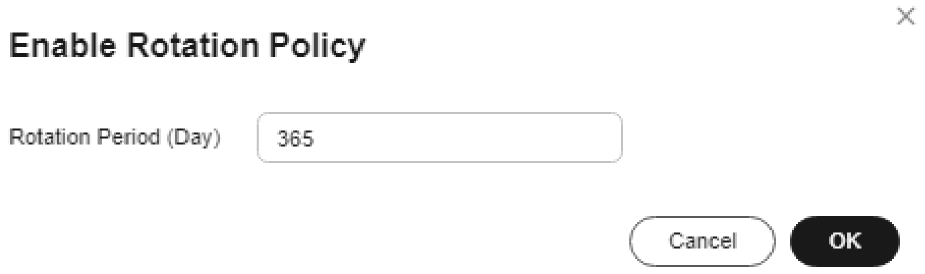
**Step 3** Click the custom key name to access its details page.

**Step 4** Click the **Rotation Policy** tab. The rotation switch is displayed.

**Step 5** Click ○ to enable key rotation.

**Step 6** Configure the rotation period and click **OK**, as shown in **Figure 2-21**. For more information, see **Table 2-21**.

**Figure 2-21** Enabling key rotation



Enable Rotation Policy

Rotation Period (Day) 365

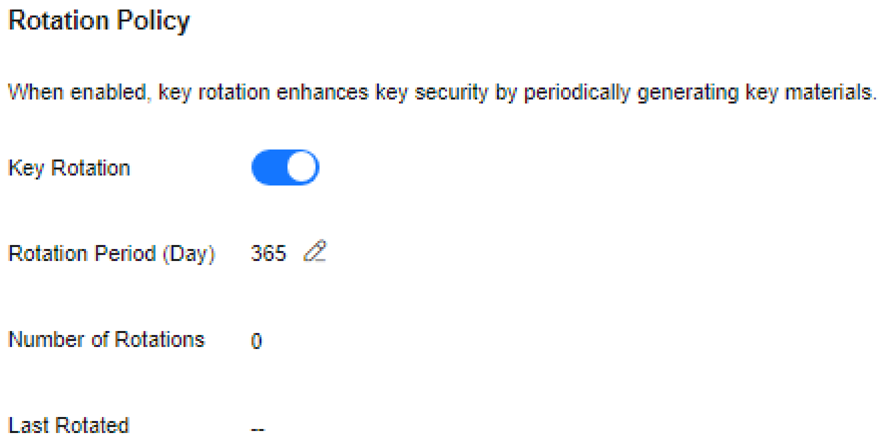
**Table 2-21** Key rotation parameters

| Parameter | Description |
|---|---|
| Key rotation | Rotation switch. The default status is ○.<br>○: disabled<br>●: enabled<br>After rotation is enabled, the key will be rotated based on your set period.<br>**NOTE**<br>A disabled custom key is never rotated, even if rotation is enabled for it.<br>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. |

| Parameter | Description |
|---|---|
| Rotation Period (day) | Rotation period (day). The value is an integer ranging from 30 to 365. The default value is **365**.<br>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 7** Check rotation details, as shown in the following figure.

**Figure 2-22** Key rotation details



Rotation Policy

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

Key Rotation ●

Rotation Period (Day) 365 ✎

Number of Rotations 0

Last Rotated --

NOTE

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

**----End**

## Disabling Key Rotation

**Step 1** Click the custom key name to access its details page.

**Step 2** Click the **Rotation Policy** tab.

**Step 3** Click ● to disable key rotation.

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

**----End**

# 3 Key Pair Service

## 3.1 Overview

A key pair, including a public key and a private key, is usually used in asymmetric encryption scenarios, also called public key encryption. A **public key** can be publicly allocated to any user to encrypt data or verify signatures, while a **private key** must be kept securely and available only for the owner to decrypt data or generate signatures.

### Working Principles

- **Encryption and decryption**
  - When you use a public key to encrypt data, only the corresponding private key can be used to decrypt the data. For example, user A hopes to send messages to user B securely. In this case, A can use B's public key to encrypt the messages, and B can use its private key to decrypt the messages.
  - If you use a private key to encrypt data, the public key can be used to decrypt data. This method is mainly used for digital signature to verify the information source and integrity.
- **Digital signature**
  - A uses its private key to generate a signature for data, and then sends the data and signature to B.
  - B uses A's public key to verify the signature. If the verification is successful, the data is not tampered with and is from A.

### Cryptographic Algorithms Supported by KPS

- The SSH key pairs created on the management console support the following cryptographic algorithms:
  - SSH-ED25519
  - ECDSA-SHA2-NISTP256
  - ECDSA-SHA2-NISTP384
  - ECDSA-SHA2-NISTP521

  - SSH_RSA: The length can be 2,048, 3,072, or 4,096 bits.
- The SSH keys imported to the KPS console support the following cryptographic algorithms:
  - SSH-DSS (not recommended)
  - SSH-ED25519
  - ECDSA-SHA2-NISTP256
  - ECDSA-SHA2-NISTP384
  - ECDSA-SHA2-NISTP521
  - SSH_RSA: The length can be 2,048, 3,072, or 4,096 bits.

### Usage Process

| Operation | Description |
|---|---|
| **3.2 Creating a Key Pair** | Describes how to create and delete a key pair. |
| **3.3 Using a Key Pair** | Describes how to bind a key pair to an ECS, use a private key to log in to Linux ECS, and use a private key to obtain the password for logging in to Windows ECS. |
| **3.4 Managing Key Pairs** | Describes how to:<br>● **Upgrade a private a key pair to an account key pair**.<br>● **Download a public key**.<br>● **Import a private key**.<br>● **Export a private key**.<br>● **Clear a private key**. |

## 3.2 Creating a Key Pair

For system security purposes, you should use the key pair authentication mode to authenticate the user who attempts to log in to an ECS. You can create a key pair and use it for authentication when logging in to your ECS.

NOTE

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

### Methods of Creating a Key Pair

**Table 3-1** describes the methods of creating a key pair.

**Table 3-1** Key pair creation methods

| Creation Method | Difference |
|---|---|
| **Creating a Key Pair on the Management Console**<br>**NOTE**<br>- **Account key pair**:<br>  - Only users with the Tenant Administrator system role can create an account key pair upon first creation.<br>  - An account key pair can be used by multiple IAM users under the account.<br>- **Private key pair**: Only the IAM user who creates the private key pair on the console can use it. If multiple IAM users need to use the same key pair, upgrade it to an account key pair. For details, see **3.4.1 Upgrading a Private Key Pair to an Account Key Pair**. | - Public keys are stored in Huawei Cloud, while private keys can either be downloaded and stored locally by the user or managed in Huawei Cloud. Huawei Cloud uses encryption keys provided by KMS to encrypt private keys, ensuring secure storage and access.<br>- Key pairs created on the console support the following cryptographic algorithms:<br>  – SSH-ED25519<br>  – ECDSA-SHA2-NISTP256<br>  – ECDSA-SHA2-NISTP384<br>  – ECDSA-SHA2-NISTP521<br>  – SSH_RSA: The length can be 2,048, 3,072, or 4,096 bits. |
| **Creating a Key Pair Using PuTTYgen**<br>**NOTE**<br>PuTTYgen is a tool for generating public and private keys. You can obtain the tool from **https://www.putty.org/**. | Both public and private keys are stored locally. |
| **Importing a Key Pair**<br>**NOTE**<br>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 IAM user separately. | - The SSH keys imported to the KPS console support the following cryptographic algorithms:<br>  – SSH-DSS (not recommended)<br>  – SSH-ED25519<br>  – ECDSA-SHA2-NISTP256<br>  – ECDSA-SHA2-NISTP384<br>  – ECDSA-SHA2-NISTP521<br>  – SSH_RSA: The length can be 2,048, 3,072, or 4,096 bits.<br>- PKCS8 is supported for imported private keys. Convert the format if PKCS1 is used. |

## Creating a Key Pair

There are three ways to create a key pair on KPS.

## Creating a Key Pair on the Management Console

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

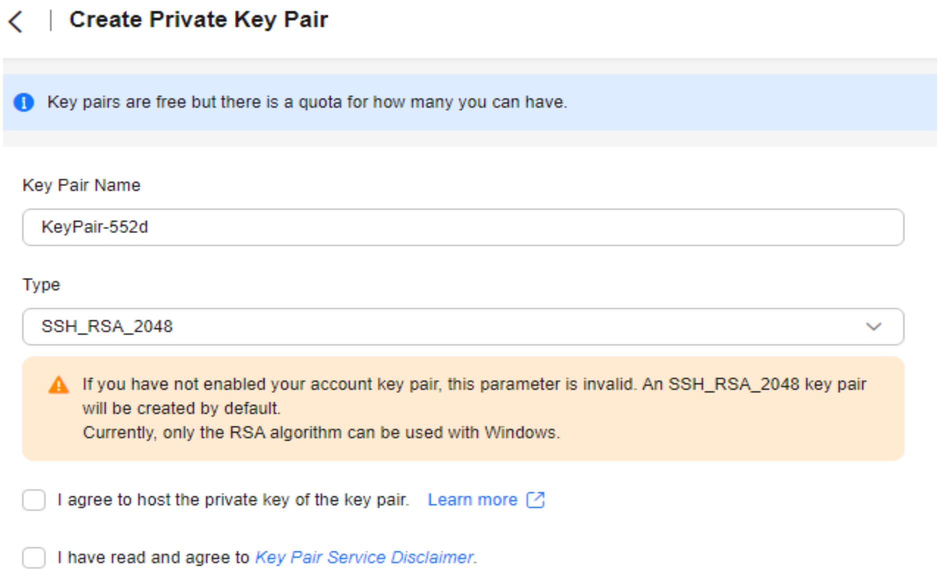
**Step 2** Click in the upper left corner of the console and select a region or project.

**Step 3** In the navigation pane on the left, click **Key Pair Service**.

**Step 4** On the displayed page, create a private key pair or account key pair as required.

**Step 5** Click **Create Key Pair**. On the displayed page, enter the key pair name, as shown in **Figure 3-1**.

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



< | Create Private Key Pair

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

Key Pair Name: KeyPair-552d

Type: SSH_RSA_2048

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

□ I agree to host the private key of the key pair. Learn more

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

**Step 6** (Optional) Select a key pair type.

NOTE

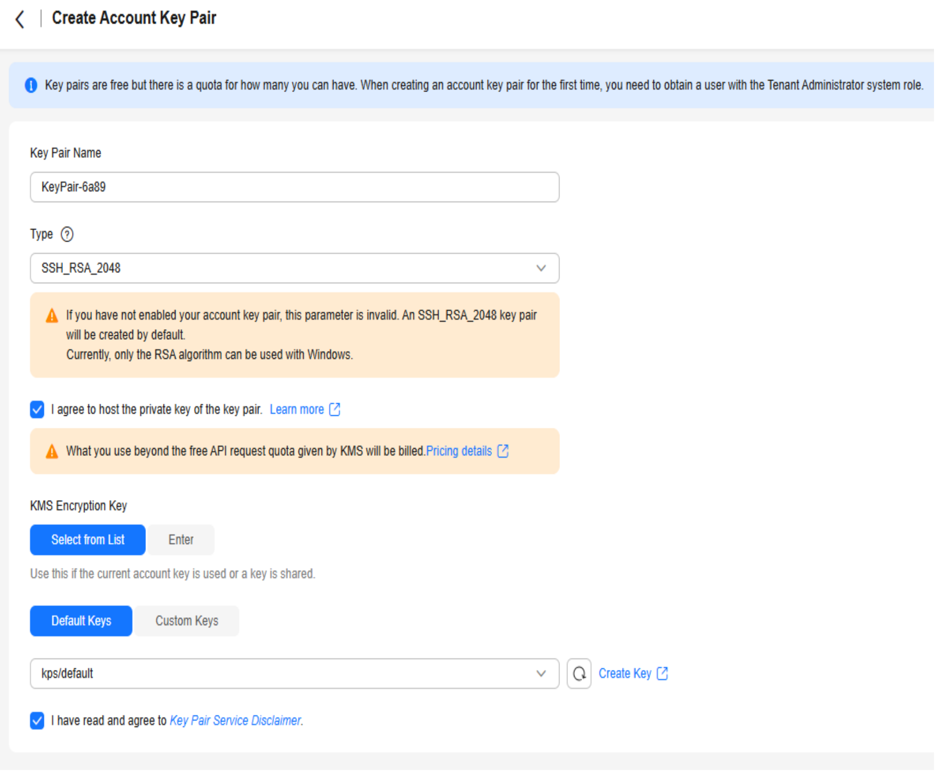
- When you create a private key pair, this parameter is available only when there is an account key pair under the account. The account key pair can be either created or upgraded from a private key pair. Otherwise, only the default SSH_RSA_2048 key pair is created.
- Currently, only the RSA algorithm can be used with Windows.

**Step 7** Read and select **I agree to host the private key of the key pair** if needed. Set **KMS Encryption Key** and select an encryption key. Skip this step if not needed.

- **Select from list**: Select this if you want to use the key used or shared by the current account.
  - **Default Keys**: KPS uses the default encryption key **kps/default** provided by KMS to encrypt private keys.
  - **Custom Keys**: Select a custom key created on KMS to encrypt the private key. For details, see **Creating a Key**. To use a shared key created using RAM, accept the shared key, and select it from the bottom of the drop-down list, **Shared** is displayed next to the key name.

- **Enter**: Select this when you need to use an authorized key. Only the ID of a symmetric key is supported. After a grant is created, you can select this mode, and enter the key ID to use the authorized key for encryption. For details, see **Creating a Grant**.

**Figure 3-2** Managing private keys



Create Account Key Pair

Key pairs are free but there is a quota for how many you can have. When creating an account key pair for the first time, you need to obtain a user with the Tenant Administrator system role.

Key Pair Name

KeyPair-6a89

Type

SSH_RSA_2048

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

☑ I agree to host the private key of the key pair. Learn more

What you use beyond the free API request quota given by KMS will be billed.Pricing details

KMS Encryption Key

Select from List | Enter

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

Default Keys | Custom Keys

kps/default

Create Key

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

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

**Step 9** Click **OK**. The browser automatically downloads the private key file to the local PC.

NOTICE

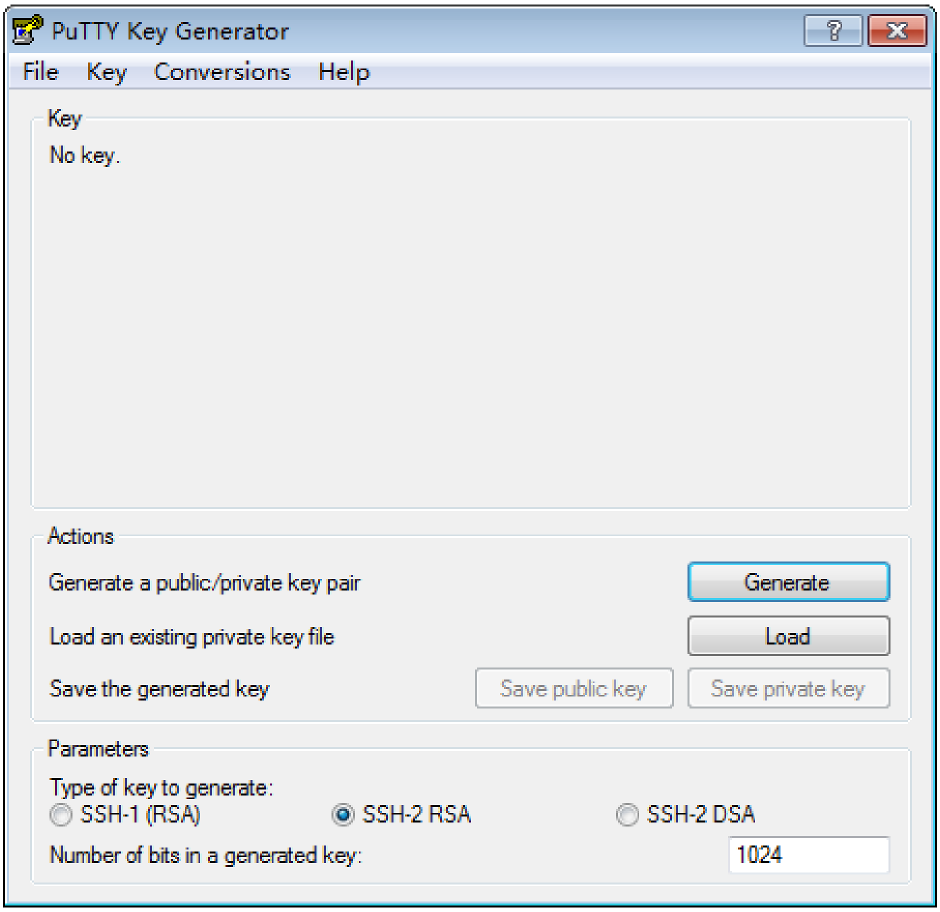
- If the private key is not managed, it can be downloaded only once. Keep it properly. If the private key is lost, you can bind a key pair to the ECS again by resetting the password or key pair. For details, see **How Do I Handle the Failure in Logging In to ECS After Unbinding the Key Pair?**
- If you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

**----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.

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 3-2**.

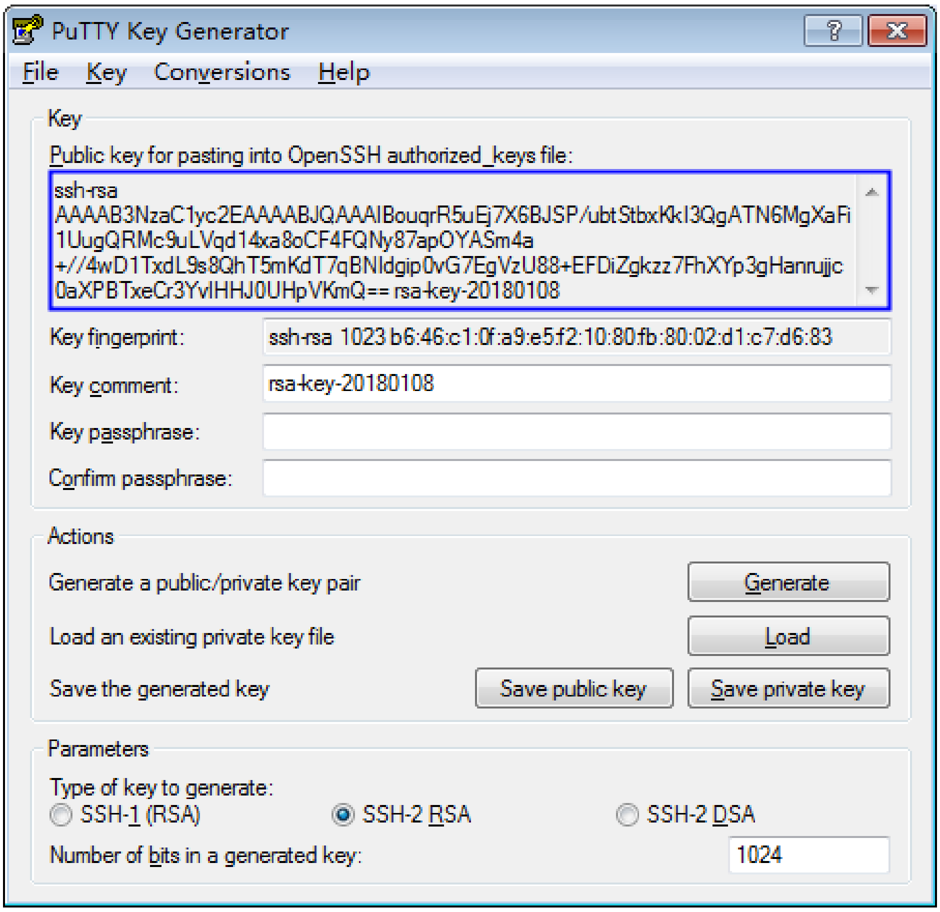
**Table 3-2** Parameter description

| Parameter | Description |
|---|---|
| Type of key to generate | - The SSH keys imported to the KPS console support the following cryptographic algorithms:<br>– SSH-DSS (not recommended)<br>– SSH-ED25519<br>– ECDSA-SHA2-NISTP256<br>– ECDSA-SHA2-NISTP384<br>– ECDSA-SHA2-NISTP521<br>– SSH_RSA: The length can be 2,048, 3,072, or 4,096 bits.<br>- PKCS8 is supported for imported private keys. Convert the format if PKCS1 is used. |
| Number of bits in a generated key | |

**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
AAAAB3NzaC1yc2EAAAABJQAAAIBougrR5uEj7X6BJSP/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

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

NOTICE

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

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

NOTICE

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

**Table 3-3** 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.<br>● Manage the private key on the management console. | 1. Choose **Conversions** > **Export OpenSSH key**.<br>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**.<br>**NOTE**<br>Do not enter the **Key passphrase** information. Otherwise, the password fails to be obtained.<br>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**.<br>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**

## Importing a Key Pair

Ensure that there is no private key pair with the same name under the IAM user. If a private key with the same name already exists, a message will be displayed when you import an account key pair, indicating that the key pair name already exists. PKCS8 is supported for imported private keys. Convert the format if PKCS1 is used.

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

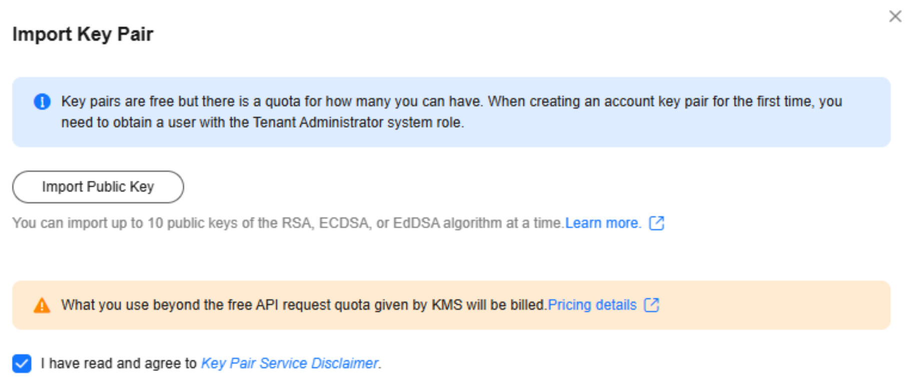
**Step 2** Click 📍 in the upper left corner of the management console and select a region or project.

**Step 3** In the navigation pane on the left, click **Key Pair Service**.

**Step 4** In the displayed **Account Key Pairs** tab, create or import a key pair as needed.

**Step 5** Click **Import Key Pair**. In the displayed dialog box, click **Import Public Key**, as shown in **Figure 3-5**.

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


Import Key Pair

Key pairs are free but there is a quota for how many you can have. When creating an account key pair for the first time, you need to obtain a user with the Tenant Administrator system role.

Import Public Key

You can import up to 10 public keys of the RSA, ECDSA, or EdDSA algorithm at a time.Learn more.

What you use beyond the free API request quota given by KMS will be billed.Pricing details

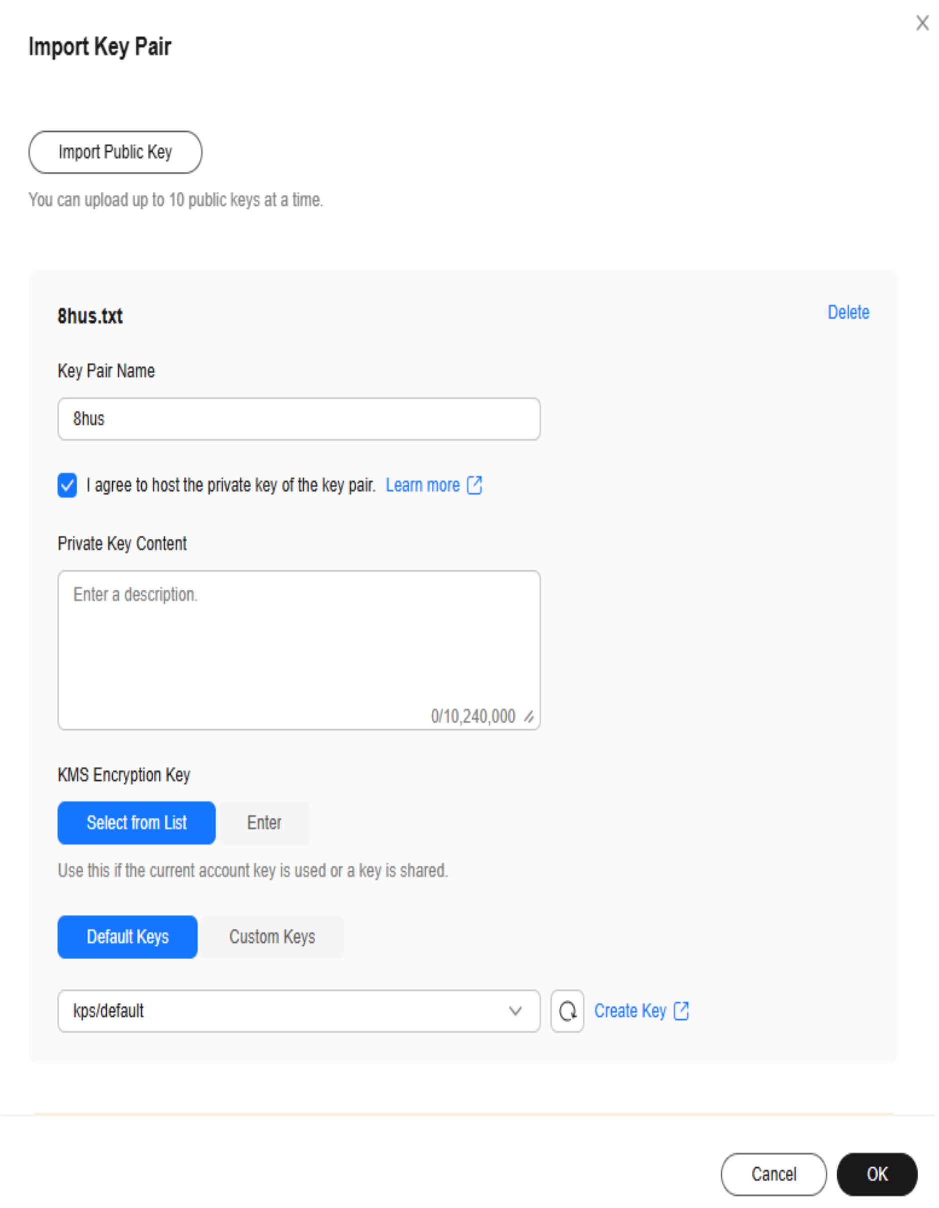
☑ I have read and agree to *Key Pair Service Disclaimer*.

NOTE

- Currently, a maximum of 10 public keys can be imported at a time.
- You can customize the name of an imported key pair.
- If a message is displayed, indicating that the name already exists, change the key pair name.

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

**Figure 3-6** Managing private keys



Import Key Pair

You can upload up to 10 public keys at a time.

8hus.txt

Key Pair Name: 8hus

☑ I agree to host the private key of the key pair. Learn more

Private Key Content: Enter a description. 0/10,240,000

KMS Encryption Key: Select from List

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

Default Keys

kps/default

1. Copy and paste the private key content to the **Private Key Content** text box.
2. Select an encryption key from the **KMS encryption** drop-down list box.
   - **Select from list**: Select this if you want to use the key used or shared by the current account.
     - **Default Keys**: KPS uses the default encryption key **kps/default** provided by KMS to encrypt private keys.
     - **Custom Keys**: Select a custom key created on KMS to encrypt the private key. For details, see **Creating a Key**. To use a shared key created using RAM, accept the shared key, and select it from the bottom of the drop-down list, **Shared** is displayed next to the key name.

- **Enter**: Select this when you need to use an authorized key. Only the ID of a symmetric key is supported. After a grant is created, you can select this mode, and enter the key ID to use the authorized key for encryption. For details, see **Creating a Grant**.

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

**Step 8** Click **OK** to import the key pair.

**----End**

## Deleting a Key Pair

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

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

**Step 1** In the navigation pane on the left, click **Key Pair Service**.

**Step 2** Locate the target key pair and click **Delete**.

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

**Step 3** Enter **DELETE** in the confirmation dialog box if deletion verification is disabled and click **OK**.

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

NOTE

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

**----End**

# 3.3 Using a Key Pair

## 3.3.1 Binding a Key Pair to an ECS

If you set the login mode to **Password** when purchasing an ECS running Linux, and you need to change the login mode to **Key Pair**, you can bind the key pair to the ECS on the KPS console, KPS will configure the key pair. After the key pair is bound, you can use the private key to log in to the ECS.

## Operation

**Table 3-4** describes the operation guide.

**Table 3-4** Operation

| Operation | Application Scenario | Prerequisites | Constraints |
|---|---|---|---|
| Binding a key pair<br>● **Binding a Key Pair**<br>● **Binding Key Pairs in Batches** | Log in to the ECS using a key pair. | ● The ECS must be in the **Running** or **Shut down** state.<br>● The ECS whose key pair is to be reset must use the public image provided by Huawei Cloud.<br>● 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 the key pair. Otherwise, the key pair fails to be bound.<br>● The SSH port (**22** by default) of the ECS security group must allow traffic from the **100.125.0.0/16** CIDR block in advance. | ● On the management console, key pairs cannot be bound to ECSs that run Windows.<br>● Key pairs cannot be bound to public images running CoreOS, openEuler, FreeBSD (Other), Kylin V10 64-bit, UnionTech OS Server 20, Euler 64-bit, or CentOS Stream 8 64-bit.<br>● You can bind key pairs to a maximum of 10 ECSs at a time. |
| **Viewing a Key Pair** | You can view the key pair information on the KPS console, including the name, fingerprint, and private key. | - | - |

| Operation | Application Scenario | Prerequisites | Constraints |
|---|---|---|---|
| **Resetting a Key Pair** | If the private key is lost, use a new key pair to bind to the ECS. | ● The ECS whose key pair is to be reset must use the public image provided by Huawei Cloud.<br>● 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.<br>● The ECS must be in the **Shut down** state. | - |
| **Replacing a Key Pair** | If your private key is leaked, you must replace the public key of the ECS with a new key pair. After the replacement, only the new private key can be used for authentication — the original private key will no longer grant access. | ● The ECS whose key pair is to be replaced uses the public image provided by Huawei Cloud.<br>● 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.<br>● The ECS must be in the **Running** state. | - |

| Operation | Application Scenario | Prerequisites | Constraints |
|---|---|---|---|
| **Unbinding a Key Pair** | If you no longer want to use a key pair to log in to an ECS, change the login mode to password. | - The ECS must be in the **Running** or **Shut down** state.<br>- The ECS whose key pair is to be unbound uses the public image provided by Huawei Cloud.<br>- 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. | - If you have not set a password for logging in to the ECS, or you have forgotten your password, reset the login password on the ECS management console. For details, see *Elastic Cloud Server User Guide*.<br>- If you set login mode to **Key Pair** when you create the ECS, after the key pair is unbound, shut down the ECS first to bind a key pair again.<br>- To log in to the ECS, after you unbind the key pair, reset the password in time on the ECS console. For details, see *Elastic Search Server User Guide*.<br>- You can unbind an ECS on the KPS console for the following OSs: EulerOS, CentOS, RedHat, SUSE, Debian, openSUSE, Oracle Linux, Fedora, Ubuntu, Huawei Cloud EulerOS, AlmaLinux, Rocky Linux, CentOS Stream, and openEuler. |

## Binding a Key Pair

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

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

**Step 3** In the navigation pane on the left, click **Key Pair Service**.

**Step 4** Click **ECS List** to view ECSs.

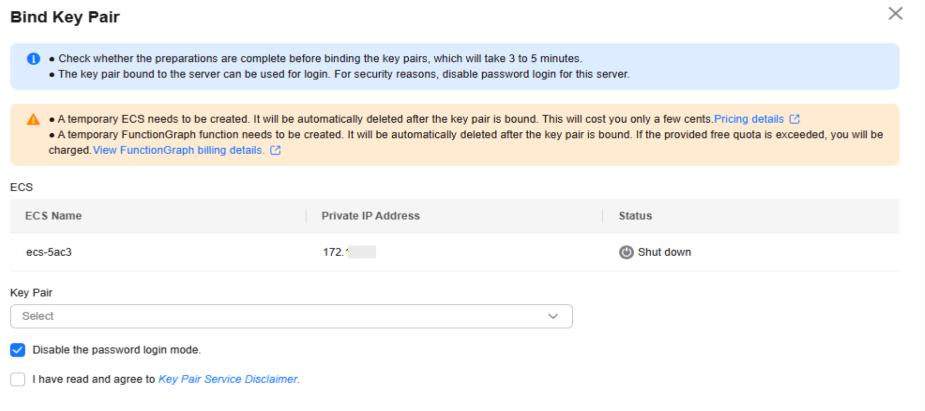
**Step 5** Locate the target ECS and click **Bind** in the **Operation**. The **Bind Key Pair** dialog box is displayed.

- If the ECS is shut down, a dialog box will be displayed, as shown in **Figure 3-7**.

  NOTE

  You need to create a temporary ECS with no more than 4 vCPUs and 8 GB memory. The ECS will be automatically deleted after being used.

  **Figure 3-7** Binding a key pair (1)

  **Bind Key Pair**

  - Check whether the preparations are complete before binding the key pairs, which will take 3 to 5 minutes.
  - The key pair bound to the server can be used for login. For security reasons, disable password login for this server.

  - A temporary ECS needs to be created. It will be automatically deleted after the key pair is bound. This will cost you only a few cents. Pricing details
  - A temporary FunctionGraph function needs to be created. It will be automatically deleted after the key pair is bound. If the provided free quota is exceeded, you will be charged. View FunctionGraph billing details.

  ECS

  | ECS Name | Private IP Address | Status |
  |---|---|---|
  | ecs-5ac3 | 172.[redacted] | Shut down |

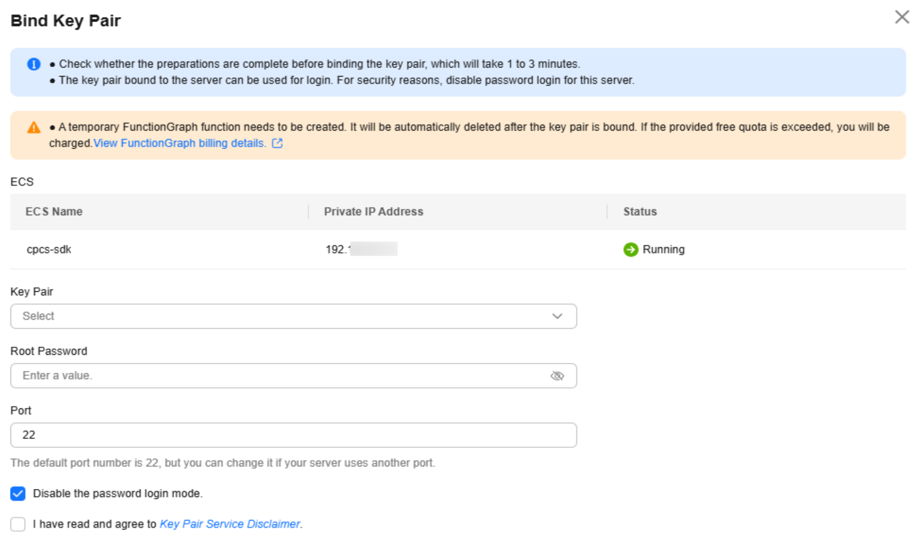
  Key Pair: Select

  ☑ Disable the password login mode.

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

- If the ECS is running, you need to provide the root password, as shown in **Figure 3-8**.

  **Figure 3-8** Binding a key pair (2)

  **Bind Key Pair**

  - Check whether the preparations are complete before binding the key pair, which will take 1 to 3 minutes.
  - The key pair bound to the server can be used for login. For security reasons, disable password login for this server.

  - A temporary FunctionGraph function needs to be created. It will be automatically deleted after the key pair is bound. If the provided free quota is exceeded, you will be charged. View FunctionGraph billing details.

  ECS

  | ECS Name | Private IP Address | Status |
  |---|---|---|
  | cpcs-sdk | 192.[redacted] | Running |

  Key Pair: Select

  Root Password: Enter a value.

  Port: 22

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

  ☑ Disable the password login mode.

  □ I have read and agree to *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 it down, and bind the key pair when the ECS is in **Shut down** state.

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

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

NOTE

Before using user-defined port, ensure that:

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

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

NOTE

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

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

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

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

**----End**

## Binding Key Pairs in Batches

Binding key pairs in batches is supported when multiple ECSs need to be bound to the same key pair and the ECSs are in the **Running** state.

- Scenario 1: If the ECSs to be bound to a key pair share the same password, you can use one-click binding, that is, select the key pair to be bound to and enter the root password of the ECSs.
- Scenario 2: If the ECSs to be bound to a key pair use different root passwords, you need to use separate binding, that is, select the key pair to be bound to and enter the root password of each ECS.

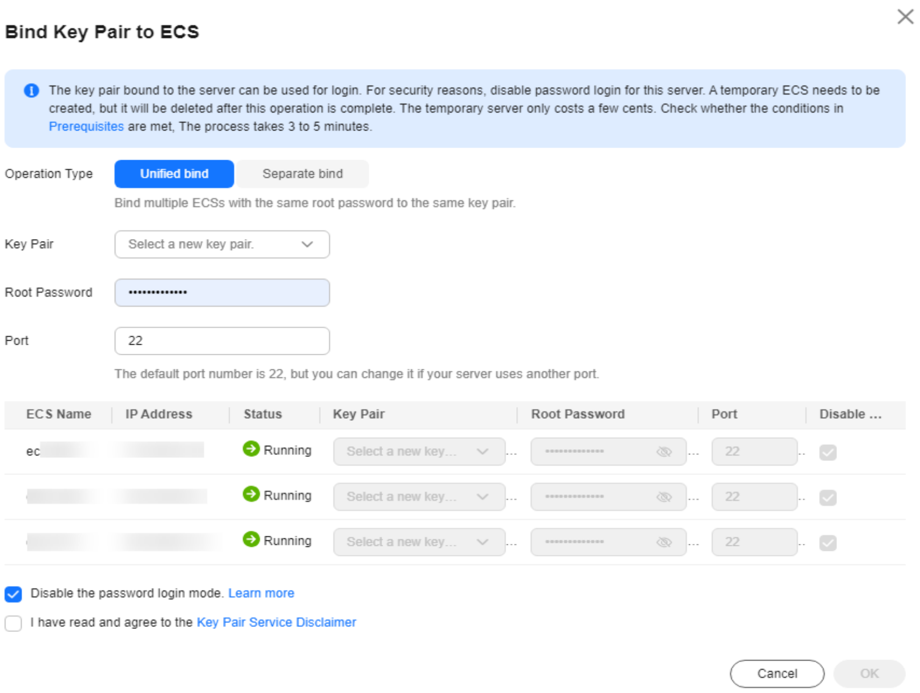
**Step 1** In the navigation pane on the left, click **Key Pair Service**.

**Step 2** Click **ECS List** to view ECSs.

**Step 3** Select the servers to be bound in batches and click **Bind** above the search box.

- If the passwords of the ECSs to be bound are the same, you can select a key pair by one click and enter the password to bind the key pair, as shown in **Figure 3-9**.

**Figure 3-9** Unified bind



Bind Key Pair to ECS

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

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

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

Key Pair: Select a new key pair.

Root Password: •••••••••••••

Port: 22

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

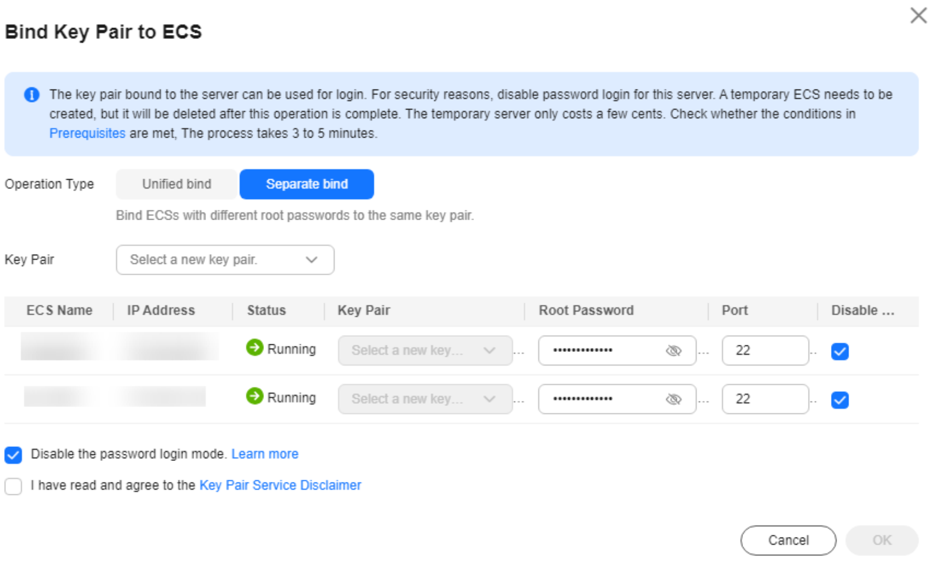
| ECS Name | IP Address | Status | Key Pair | Root Password | Port | Disable ... |
|---|---|---|---|---|---|---|
| ec[redacted] | [redacted] | Running | Select a new key... | ••••••••••••• | 22 | ☑ |
| [redacted] | [redacted] | Running | Select a new key... | ••••••••••••• | 22 | ☑ |
| [redacted] | [redacted] | 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 3-10**.

**Figure 3-10** Separate bind



Bind Key Pair to ECS

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

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

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

Key Pair: Select a new key pair.

| ECS Name | IP Address | Status | Key Pair | Root Password | Port | Disable ... |
|---|---|---|---|---|---|---|
| [redacted] | [redacted] | Running | Select a new key... | ••••••••••••• | 22 | ☑ |
| [redacted] | [redacted] | 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.

**----End**

## Viewing a Key Pair

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

**Step 1** In the navigation pane on the left, click **Key Pair Service**.

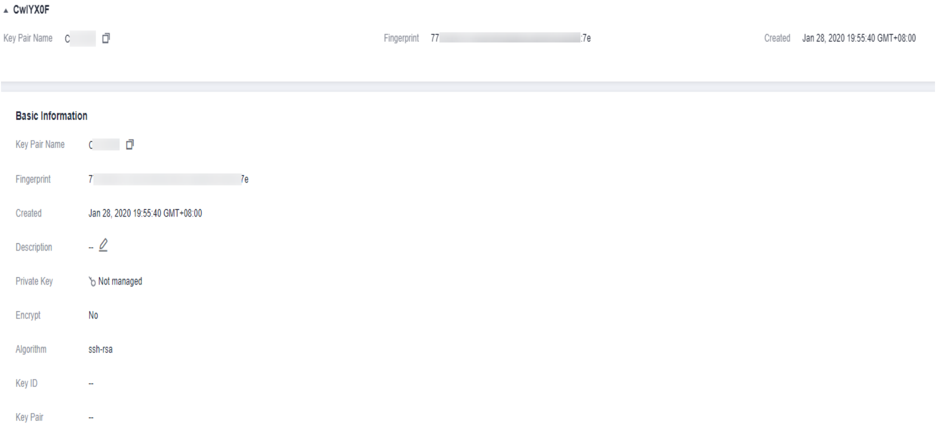
**Step 2** Click the **Private Key Pairs** tab and view information about the key pair in the key pair list.

NOTE

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

**Step 3** Click the name of the target key pair. The detailed information about the key pair and the list of ECSs using the key pair are displayed, as shown in **Figure 3-11**.

**Figure 3-11** Key pair details



▲ CwIYX0F

Key Pair Name C[redacted]
Fingerprint 77[redacted]:7e
Created Jan 28, 2020 19:55:40 GMT+08:00

Basic Information

Key Pair Name C[redacted]
Fingerprint 7[redacted]7e
Created Jan 28, 2020 19:55:40 GMT+08:00
Description --
Private Key Not managed
Encrypt No
Algorithm ssh-rsa
Key ID --
Key Pair --

NOTE

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

**Table 3-5** lists the parameters of the ECS to which the key pair is bound.

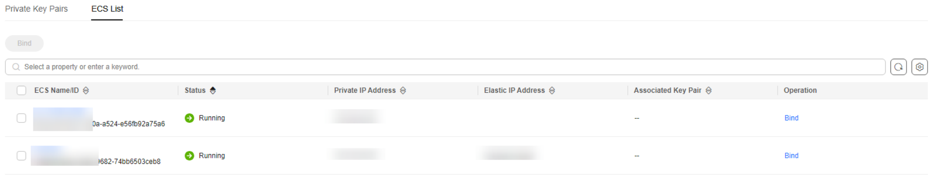
**Table 3-5** Parameters of an ECS

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

| Parameter | Description |
|---|---|
| Status | Status of an ECS. The possible values are as follows:<br>● **Running**<br>● **Creating**<br>● **Faulty**<br>● **Shut down** |
| Private IP Address | Private IP address |
| Elastic IP Address | Elastic IP address |
| Bind Key Pair | Key pair bound to the ECS |

**Step 4** Click **ECS List** to view ECSs.

**Figure 3-12** ECS list



| | ECS Name/ID | Status | Private IP Address | Elastic IP Address | Associated Key Pair | Operation |
|---|---|---|---|---|---|---|
| □ | [redacted]0a-a524-e56fb92a75a6 | Running | [redacted] | | -- | Bind |
| □ | [redacted]682-74bb6503ceb8 | Running | [redacted] | [redacted] | -- | Bind |

**Step 5** Click the number next to in the **Status** column to view the failed tasks, as shown in **Figure 3-13**.

Status of resetting or replacing the key pair:

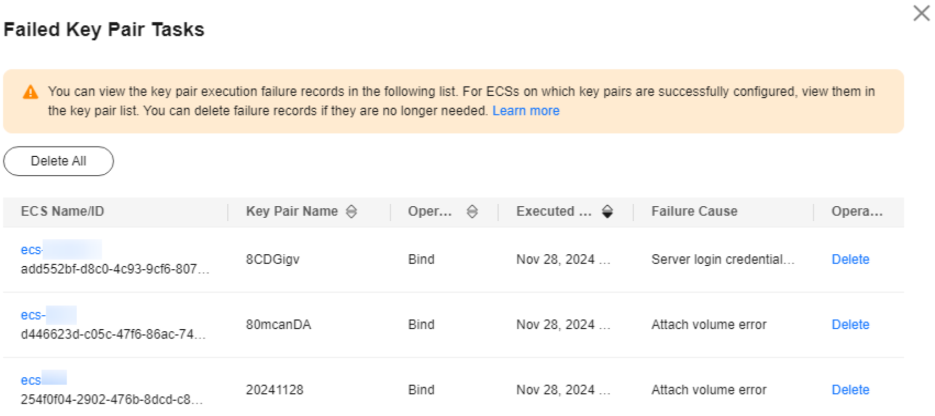
: Executing

: Execution failed

NOTE

- Locate the target failed key pair task and click **Delete** in **Operation** column. You can also click **Delete All** on top of the list to delete all failed tasks.
- Click **Learn more** to view related documents.

**Figure 3-13** Failed key pair tasks



Failed Key Pair Tasks

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

| ECS Name/ID | Key Pair Name | Oper... | Executed ... | Failure Cause | Opera... |
|---|---|---|---|---|---|
| ecs-[redacted]<br>add552bf-d8c0-4c93-9cf6-807... | 8CDGigv | Bind | Nov 28, 2024 ... | Server login credential... | Delete |
| ecs-[redacted]<br>d446623d-c05c-47f6-86ac-74... | 80mcanDA | Bind | Nov 28, 2024 ... | Attach volume error | Delete |
| ecs[redacted]<br>254f0f04-2902-476b-8dcd-c8... | 20241128 | Bind | Nov 28, 2024 ... | Attach volume error | Delete |

**----End**

## Resetting a Key Pair

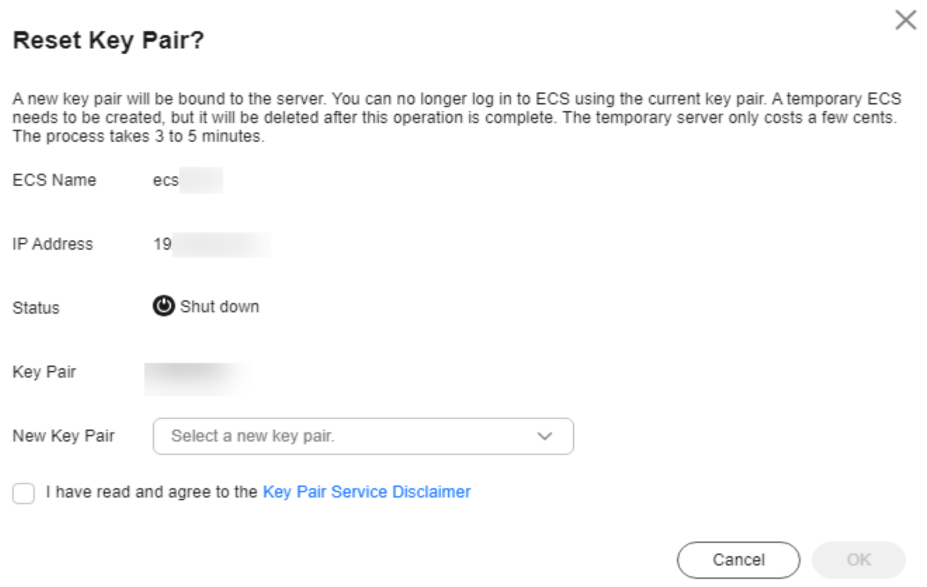
If your private key is lost, you can use a new key pair to reconfigure the ECS through the management console. After resetting the key pair, you need to use the private key of the new key pair to log in to the ECS, and the original private key cannot be used to log in to the ECS.

- The ECS whose key pair is to be reset must use 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.

**Step 1** In the navigation pane on the left, click **Key Pair Service**.

**Step 2** Click the **ECS List** tab, locate the target ECS in the list and click **Reset** in the **Operation** column. The key pair reset dialog box is displayed, as shown in **Figure 3-14**.

**Figure 3-14** Resetting a key pair



Reset Key Pair?

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

ECS Name ecs[redacted]

IP Address 19[redacted]

Status Shut down

Key Pair [redacted]

New Key Pair Select a new key pair.

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

**Step 3** Select a new key pair from the drop-down list box of **New Key Pair**.

**Step 4** Click **OK**. The ECS key pair will be reset in about 10 minutes.

**----End**

## Replacing a Key Pair

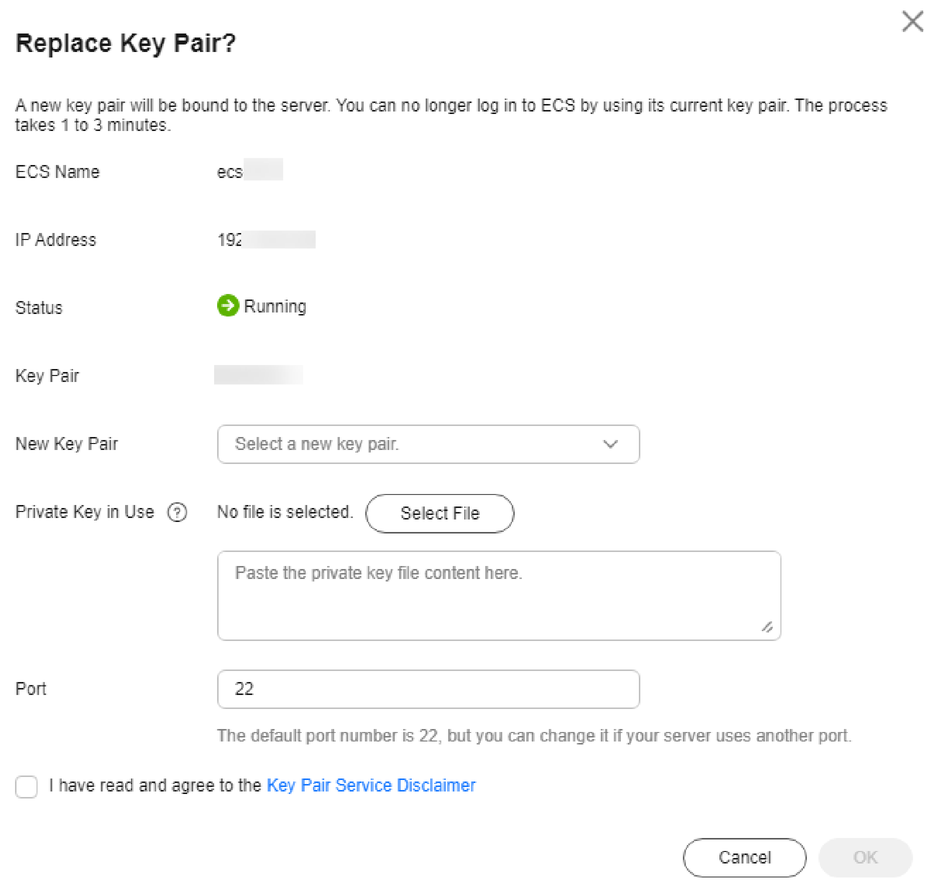
If your private key is leaked, you can use a new key pair to replace the public key of the ECS through the management console. After replacing the key pair, you need to use the private key of the new key pair to log in to the ECS, and the original private key cannot be used to log in to the ECS.

- 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.

**Step 1** In the navigation pane on the left, click **Key Pair Service**.

**Step 2** Click the **ECS List** tab, locate the target ECS in the list and click **Replace** in the **Operation** column. The key pair replacement dialog box is displayed, as shown in Figure 3-15.

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



Replace Key Pair?

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

| | |
|---|---|
| ECS Name | ecs[redacted] |
| IP Address | 192[redacted] |
| Status | Running |
| Key Pair | [redacted] |
| New Key Pair | Select a new key pair. |
| Private Key in Use | No file is selected. Select File<br>Paste the private key file content here. |
| Port | 22<br>The default port number is 22, but you can change it if your server uses another port. |

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

**Step 3** Select a new key pair from the drop-down list box of **New Key Pair**.

**Step 4** 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 5** Click **OK**. The key pair will be replaced in about one minute.

**----End**

## Unbinding a Key Pair

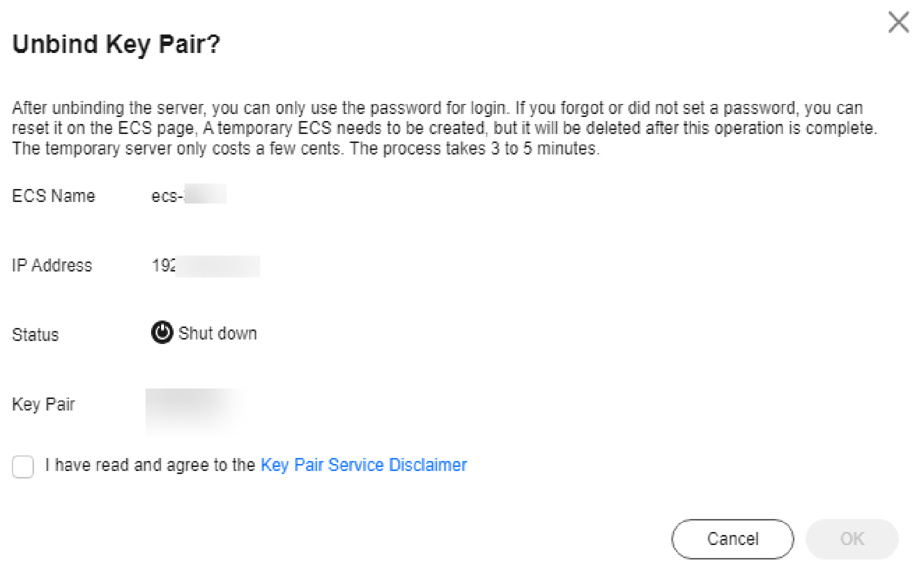
If you want to change the login mode from **Key Pair** to **Password**, unbind the key pair on the KPS console.

**Step 1** In the navigation pane on the left, click **Key Pair Service**.

**Step 2** Click the **ECS List** tab, locate the target ECS in the list, and click **Unbind** in the **Operation** column.

- If the ECS is shut down, a dialog box will be displayed, as shown in **Figure 3-16**.

**Figure 3-16** Unbinding a key pair (1)



**Unbind Key Pair?**

After unbinding the server, you can only use the password for login. If you forgot or did not set a password, you can reset it on the ECS page, A temporary ECS needs to be created, but it will be deleted after this operation is complete. The temporary server only costs a few cents. The process takes 3 to 5 minutes.

ECS Name ecs-[redacted]

IP Address 192[redacted]

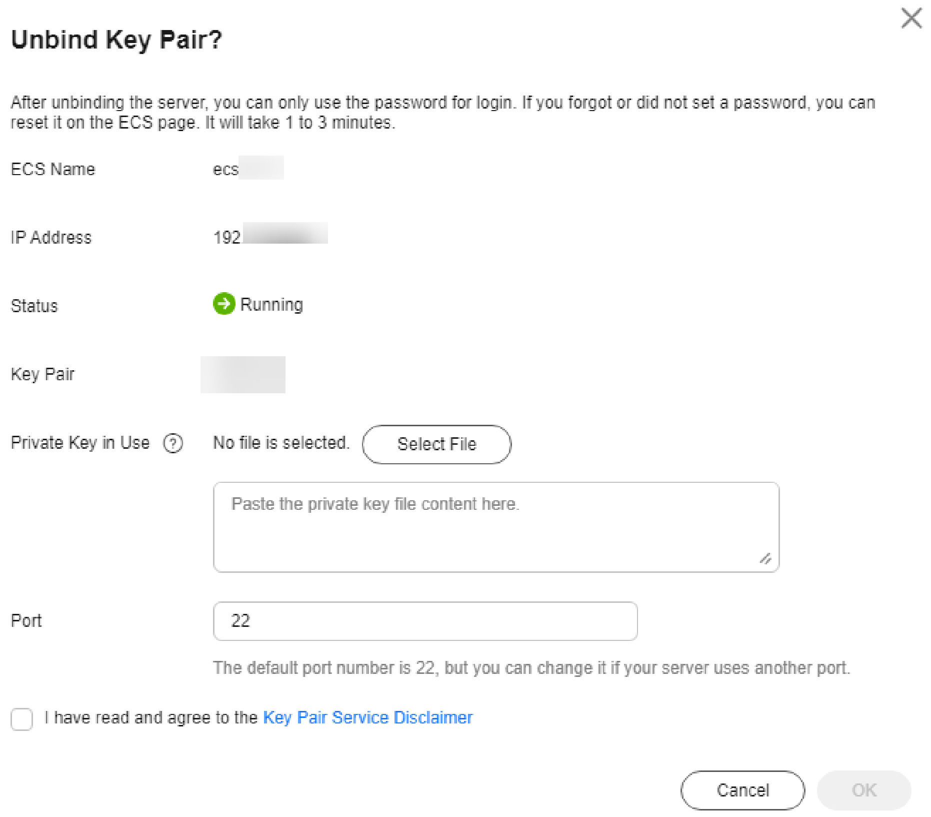
Status Shut down

Key Pair [redacted]

□ 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 3-17**.

**Figure 3-17** Unbinding a key pair (2)



**Unbind Key Pair?**

After unbinding the server, you can only use the password for login. If you forgot or did not set a password, you can reset it on the ECS page. It will take 1 to 3 minutes.

ECS Name ecs[redacted]

IP Address 192[redacted]

Status Running

Key Pair [redacted]

Private Key in Use ? No file is selected. Select File

Paste the private key file content here.

Port 22

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

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

**Step 3** 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 4** Click **OK**. The key pair will be unbound from the ECS in about one minute.

NOTE

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

**----End**

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

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

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

### Prerequisites

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

### Constraints

The private key files of the ECS must meet the requirements list in the following table.

**Table 3-6** 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**.

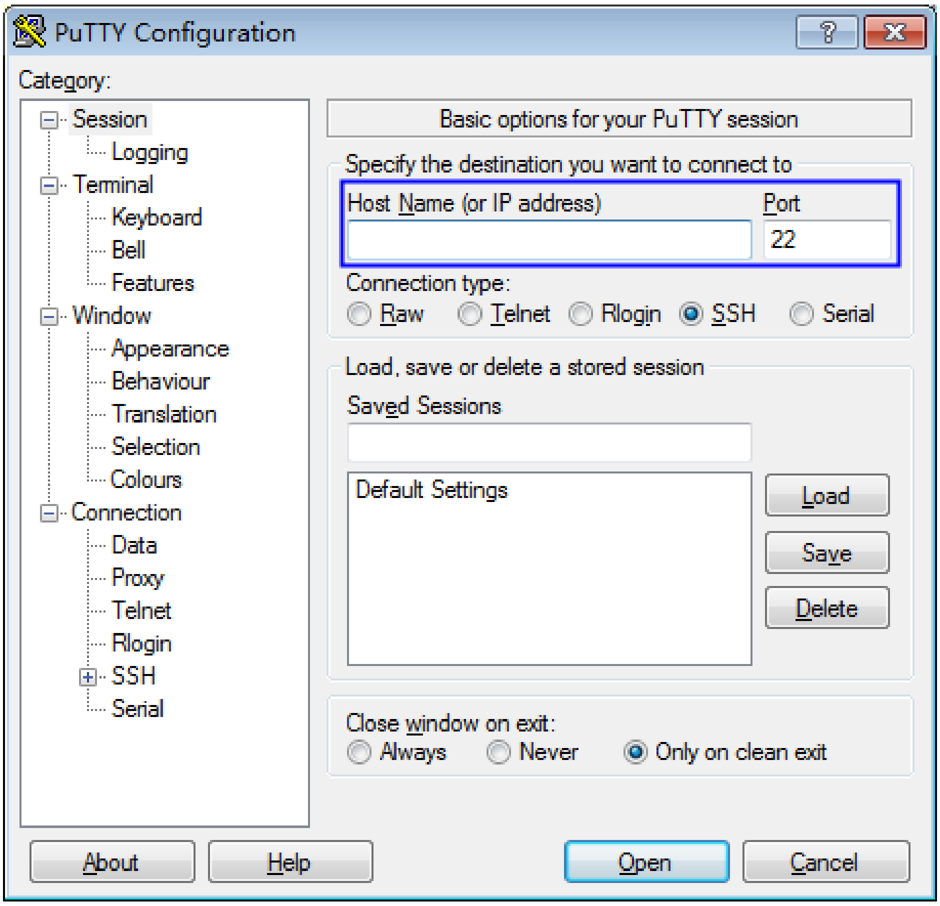
NOTE

- 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 3-18** 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**.

**----End**

## Logging In from a Linux Computer

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

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

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

NOTE

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

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

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

NOTE

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

**----End**

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

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

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

## Prerequisites

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

## Constraints

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

Clearing the initial password information does not affect ECS operation or login. Once cleared, the password cannot be restored. Before deleting a password, record the password information. For details, see *Elastic Cloud Server User Guide*.

- You can also call the API to obtain the initial password of the Windows ECS. For details, see *Elastic Cloud Server API Reference*.
- The ECS private key file must be in .pem format.

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

## Procedure

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

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

**Step 3** Click ☰. Under **Computing**, click **Elastic Cloud Server**.

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

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

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

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

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

**----End**

# 3.4 Managing Key Pairs

## 3.4.1 Upgrading a Private Key Pair to an Account Key Pair

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

### Prerequisites

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

### Constraints

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

- Once a private key pair is upgraded to an account key pair, it cannot be changed back.

## Procedure

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

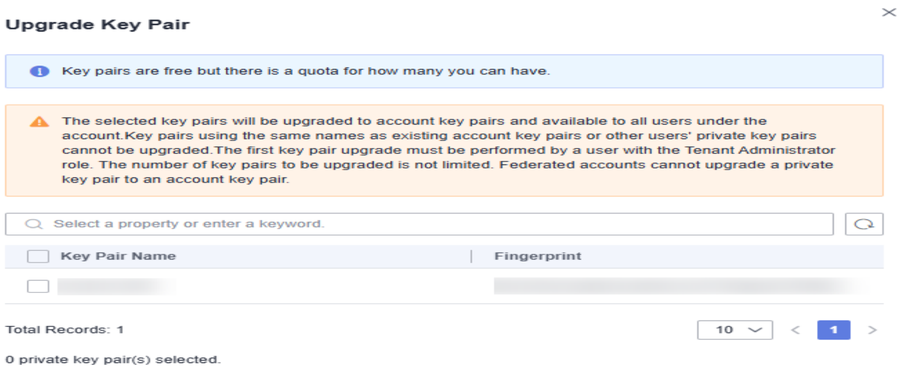
**Step 2** Click in the upper left corner of the console and select a region or project.

**Step 3** In the navigation pane on the left, click **Key Pair Service**.

**Step 4** Click the **Private Key Pairs** tab and then click **Upgrade Key Pair**.

**Step 5** In the displayed dialog box, select the key pair to be upgraded, and click **OK**, as shown in **Figure 3-19**.

**Figure 3-19** Upgrading a key pair



Upgrade Key Pair

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

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. Federated accounts cannot upgrade a private key pair to an account key pair.

Select a property or enter a keyword.

| □ Key Pair Name | Fingerprint |
|---|---|
| □ [redacted] | [redacted] |

Total Records: 1

0 private key pair(s) selected.

NOTE

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

**----End**

## 3.4.2 Managing Public and Private Keys

After a key pair is created on KPS, the public key is automatically stored in Huawei Cloud, while you need to download and store the private key. 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.

This section describes how to:

- **Downloading a Public Key**
- **Importing a Private Key**
- **Exporting a Private Key**
- **Clearing a Private Key**

## 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?**

## Downloading a Public Key

To download a public key to the local PC from KPS, perform the following steps:

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

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

**Step 3** In the navigation pane on the left, click **Key Pair Service**.

**Step 4** Locate the target key pair and click **Download Public Key** in the **Operation** column. The public key file in TXT format is obtained.

**----End**

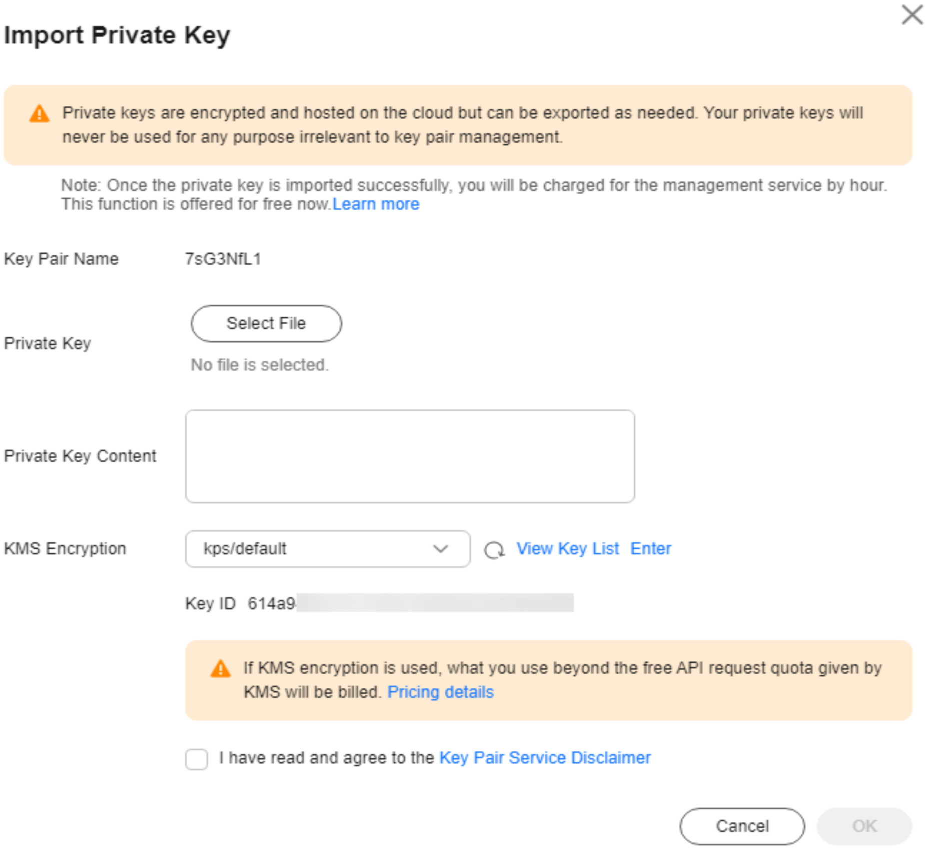
## Importing a Private Key

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.

**Step 1** In the navigation pane on the left, click **Key Pair Service**.

**Step 2** Locate the target public key and click **Import Private Key** in the **Operation** column. The **Import Private Key** page is displayed, as shown in **Figure 3-20**.

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



Import Private Key

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

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

Key Pair Name 7sG3NfL1

Private Key Select File
No file is selected.

Private Key Content

KMS Encryption kps/default View Key List Enter

Key ID 614a9

If KMS encryption is used, what you use beyond the free API request quota given by KMS will be billed. Pricing details

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

**Step 3** Click **Select File**, select a local .pem private key file. Alternatively, you can copy and paste the private key content to the **Private Key Content** text box.

NOTE

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

**Step 4** Select an encryption key from the **KMS encryption** drop-down list box.

NOTE

- KPS encrypts private keys using the encryption key provided by KMS. When you use the KMS encryption function of the key pair, KMS creates a default key **kps/default** for you to use.
- For details about how to create a custom key on KMS, see **Creating a Key**.
- After a grant is created, you can switch to the manual input mode, and enter the key ID to use the granted key for encryption. For details, see **Creating a Grant**.

**Step 5** Click **OK** to complete the import.

**----End**

## Exporting a Private Key

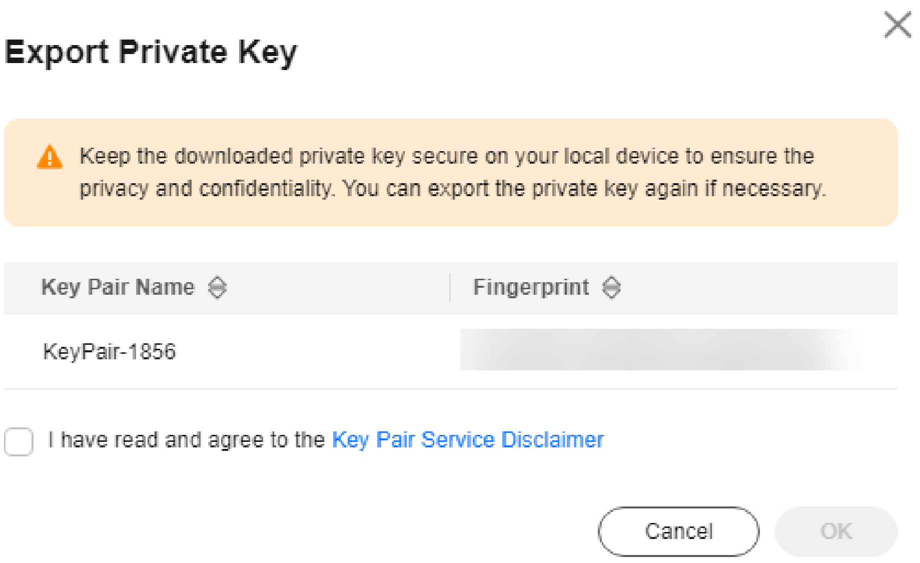
If you have the private keys managed by the management console, you can download the private keys whenever you need. To ensure the security of the private key, keep the downloaded private key properly.

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.

**Step 1** In the navigation pane on the left, click **Key Pair Service**.

**Step 2** Locate the target key pair and click **Export Private Key** in the **Operation** column. The **Export Private Key** dialog box is displayed, as shown in **Figure 3-21**.

**Figure 3-21** 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 | Fingerprint |
|---|---|
| KeyPair-1856 | [redacted] |

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

NOTE

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

**Step 3** Click **OK**. The browser automatically downloads the private key.

NOTICE

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.

**----End**

## 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.

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.

**Step 1** In the navigation pane on the left, click **Key Pair Service**.

**Step 2** Locate the target key pair and choose **More** > **Clear Private Key** in the **Operation** column.

**Step 3** 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**

# 4 Cloud Secret Management Service

## 4.1 Overview

A secret is used to verify identity and authorize access. In the information security and identity authentication fields, a secret is a key mechanism to ensure that only authorized users can access the system, resources, or services. Secrets include usernames and passwords, digital certificates, key pairs (public and private keys), tokens, biometric information, one-time passwords (OTPs), and smart cards.

### Shared Secrets

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

### Secret Rotation

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

**Table 4-1** Supported rotated secret types

| Type | Database Type/Instance |
|---|---|
| RDS secret | MySQL |
| TaurusDB secret | TaurusDB instance, formerly GaussDB(for MySQL) instance |

### Differences Between Shared Secrets and Rotated Secrets

**Table 4-2** Secret types

| **Type** | Shared secret | Rotated secret |
|---|---|---|
| **Application Scenario** | Supports full lifecycle management of customized secrets in different scenarios. | ● RDS secrets: Automatically hosts Huawei Cloud RDS database secrets.<br>● TaurusDB secrets: Automatically hosts Huawei Cloud TaurusDB secrets. |
| **Automatic Rotation** | Not supported. Users need to trigger the rotation. | Supported. Single-user and dual-user rotation models are supported. |

### Using Rotated Secrets

Process description:

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

⚠ CAUTION

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

## 4.2 Creating a Secret

When you create a secret on CSMS for secret hosting, the secret value will be stored in the original secret version, which is marked as **SYSCURRENT**.

Secret value, the detailed content of a secret, is used to verify user identity or authorization during authentication. It can be of various forms, depending on the used authentication mechanism. Typical secret values include:

- **Username and password**: A username is the identity of a user, and a password is the key secret value for user identity authentication.
- **Digital certificate**: The public key and identity, which are the secret values of a certificate, are used to verify the identity of a user or device.
- **Key pair**: The private key, which is the secret value, is used for signature and decryption.
- **Token**: A token is a temporary secret value used for identity authentication.
- **Biometric recognition information**: Biometric feature data, such as fingerprint, facial recognition, and iris recognition, is the secret value.
- **One-time password (OTP)**: An OTP generated via SMS, email, or a certain application is the secret value.

## Constraints

- At most 500 secrets can be created on CSMS.
- A secret can be no larger than 64 KB.
- 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 Shared Secret

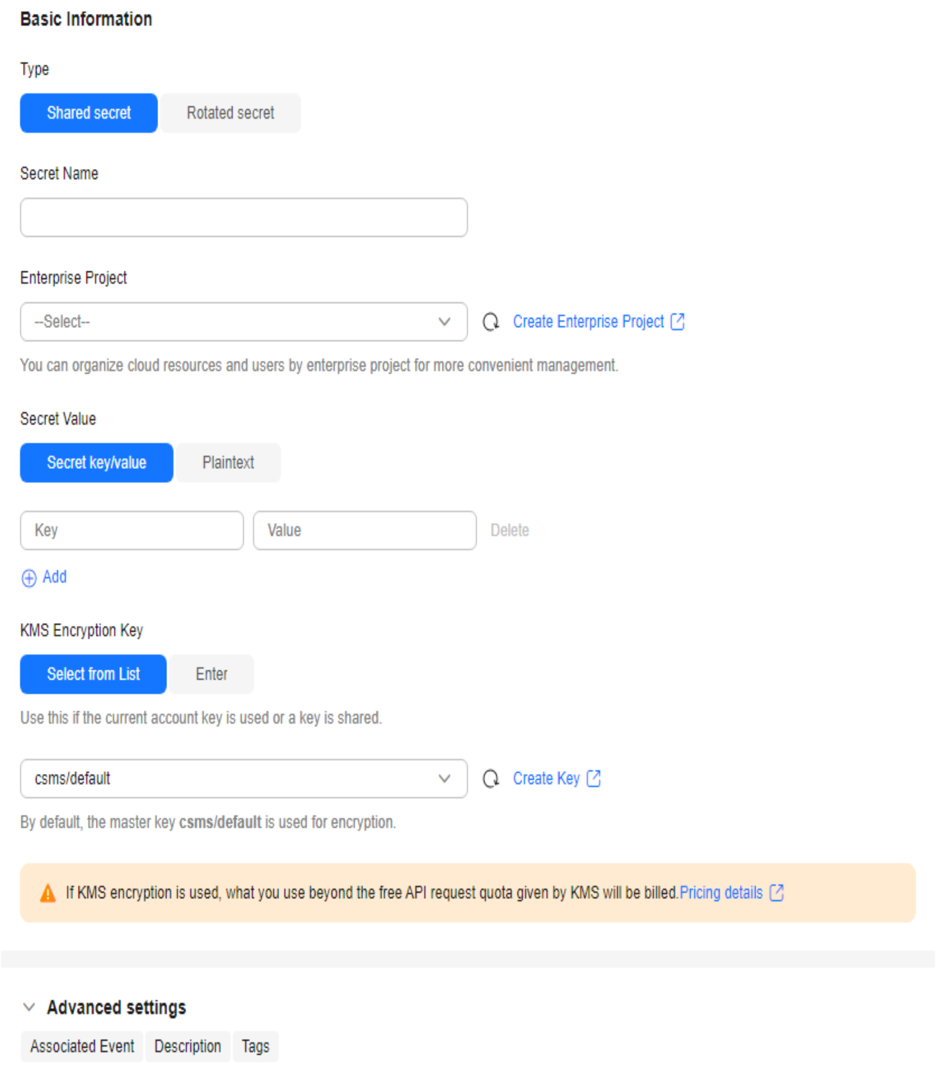
**Step 1** Log in to the **DEW console**.

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

**Step 3** In the navigation pane on the left, choose **Cloud Secret Management Service** > **Secrets**.

**Step 4** Click **Create Secret**. Configure parameters in the **Create Secret** dialog box, as shown in **Figure 4-1**. For details about the parameters, see **Table 4-3**.

**Figure 4-1** Creating a Secret



Basic Information

Type

Shared secret | Rotated secret

Secret Name

Enterprise Project

--Select-- Create Enterprise Project

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

Secret Value

Secret key/value | Plaintext

Key | Value | Delete

Add

KMS Encryption Key

Select from List | Enter

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

csms/default Create Key

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

If KMS encryption is used, what you use beyond the free API request quota given by KMS will be billed.Pricing details

Advanced settings

Associated Event | Description | Tags

**Table 4-3** Secret parameters

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

| Parameter | Description |
|---|---|
| Secret Value | Secret key/value pair or the plaintext secret to be encrypted<br>Secret value, the detailed content of a secret, is used to verify user identity or authorization during authentication. It can be of various forms, depending on the used authentication mechanism. Typical secret values include:<br>● **Username and password**: A username is the identity of a user, and a password is the key secret value for user identity authentication.<br>● **Digital certificate**: The public key and identity, which are the secret values of a certificate, are used to verify the identity of a user or device.<br>● **Key pair**: The private key, which is the secret value, is used for signature and decryption.<br>● **Token**: A token is a temporary secret value used for identity authentication.<br>● **Biometric recognition information**: Biometric feature data, such as fingerprint, facial recognition, and iris recognition, is the secret value.<br>● **One-time password (OTP)**: An OTP generated via SMS, email, or a certain application is the secret value. |
| KMS Encryption Key | The following modes are supported:<br>● **Select from list**: Select this if you want to use the key used or shared by the current account. Select the default key **csms/default** or a custom key created on KMS.<br>● **Enter**: Enter the ID of the authorized key. Enter an encryption key if an authorized key is used. Only symmetric algorithm key IDs are supported. Do not enter an asymmetric key ID.<br>**NOTE**<br>● CSMS encrypts secret values using the encryption key provided by KMS. When you use the KMS encryption function, KMS creates a default key **csms/default** for you to use.<br>● For details about how to create a custom key on KMS, see **Creating a Key**.<br>● After a grant is created, you can switch to the manual input mode, and enter the key ID to use the granted key for encryption. For details, see **Creating a Grant**. |

| Parameter | Description |
|---|---|
| Advanced settings | ● **Associated events**<br>Select an associated event for the secret. You can check information such as secret rotation and version expiration.<br>● **Description**<br>Description of a secret<br>● **Tag**<br>You can add tags to a secret as you need.<br>NOTE<br>You can add at most 20 tags to a secret. |

**Step 5** Click **Next**. You cannot select a rotation period for common secrets. Go to the next step.

**Step 6** Click **Next** and confirm the creation information.

**Step 7** Click **OK**. In the secret list, you can view the created secrets. The default status of a secret is **Enabled**.

**----End**

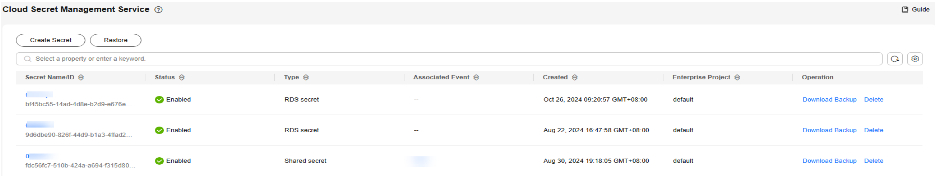
## Viewing Secret Details

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**.

**Step 1** In the navigation pane on the left, choose **Cloud Secret Management Service** > **Secrets**.

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

**Figure 4-2** Secret list



Cloud Secret Management Service
Guide
Create Secret
Restore
Select a property or enter a keyword.

| Secret Name/ID | Status | Type | Associated Event | Created | Enterprise Project | Operation |
|---|---|---|---|---|---|---|
| [redacted]<br>bf45bc55-14ad-4d8e-b2d9-e676e... | Enabled | RDS secret | -- | Oct 26, 2024 09:20:57 GMT+08:00 | default | Download Backup Delete |
| [redacted]<br>9d6dbe90-826f-44d9-b1a3-4ffad2... | Enabled | RDS secret | -- | Aug 22, 2024 16:47:58 GMT+08:00 | default | Download Backup Delete |
| [redacted]<br>fdc56fc7-510b-424a-a694-f315d80... | Enabled | Shared secret | [redacted] | Aug 30, 2024 19:18:05 GMT+08:00 | default | Download Backup Delete |

**Table 4-4** Secret list parameters

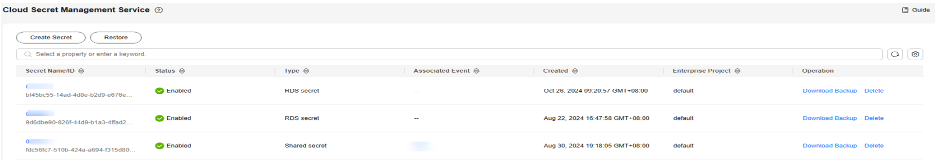
| Parameter | Description |
|---|---|
| Secret Name/ID | Secret name and ID |
| Status | Status of a secret. The value can be **Enabled** or **Pending deletion**. |
| Type | Secret type, including shared secret, RDS DB secret, and TaurusDB secret. |

| Parameter | Description |
|---|---|
| Associated events | Bound event notification when the secret was created. |
| Creation Time | Time when the secret is created |
| Enterprise Project | Enterprise project that the secret is to be bound to |

**Step 3** Click a secret to view its details, as shown in **Figure 4-3**.

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

**Figure 4-3** Secret details



Cloud Secret Management Service

| Secret Name/ID | Status | Type | Associated Event | Created | Enterprise Project | Operation |
|---|---|---|---|---|---|---|
| [redacted]<br>bf45bc55-14ad-4d8e-b2d9-e676e... | Enabled | RDS secret | -- | Oct 26, 2024 09:20:57 GMT+08:00 | default | Download Backup Delete |
| [redacted]<br>9d6dbe90-826f-44d9-b1a3-4ffad2... | Enabled | RDS secret | -- | Aug 22, 2024 16:47:58 GMT+08:00 | default | Download Backup Delete |
| [redacted]<br>fdc56fc7-510b-424a-a694-f315d80... | Enabled | Shared secret | [redacted] | Aug 30, 2024 19:18:05 GMT+08:00 | default | Download Backup Delete |

**----End**

## Downloading a Secret Backup

To download a secret to a local PC for backup, perform the following steps:

**Step 1** In the navigation pane on the left, choose **Cloud Secret Management Service** > **Secrets**.

**Step 2** Locate the target secret in the list and click **Download Backup** in the **Operation** column.

The secret file will be downloaded to the local host and is named *Secret name*.**secretbackup**.

**----End**

## Restoring a Secret from a Backup

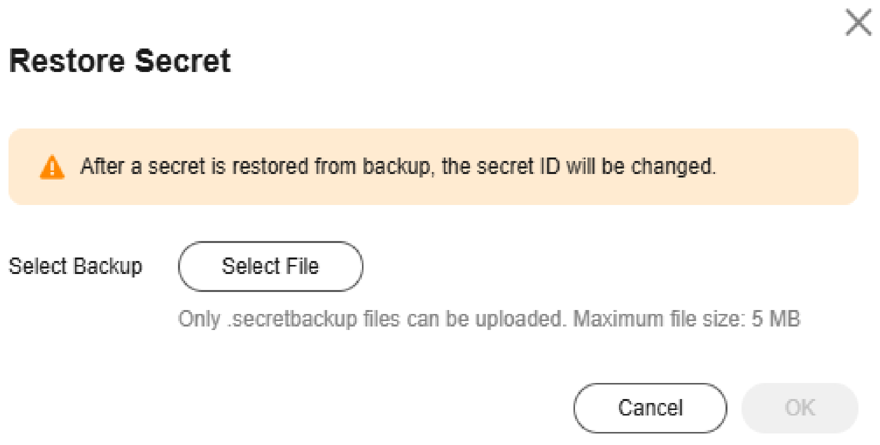
DEW allows you to restore a secret from backup. After a secret is restored from backup, the secret ID will be changed.

Only secret backup files smaller than 5 MB can be uploaded.

**Step 1** In the navigation pane on the left, choose **Cloud Secret Management Service** > **Secrets**.

**Step 2** Click **Restore Secret**, select a backup file, and click **OK**.

**Figure 4-4** Restoring a secret backup



Restore Secret

After a secret is restored from backup, the secret ID will be changed.

Select Backup Select File

Only .secretbackup files can be uploaded. Maximum file size: 5 MB

**----End**

## Deleting a Secret

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

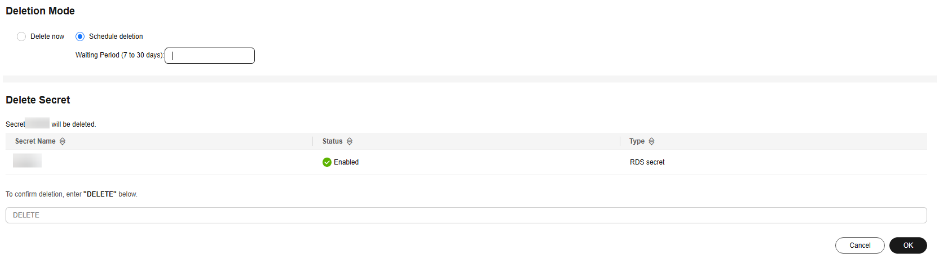
- A secret will not be deleted until its scheduled deletion period expires. You can set the period to a value within the range 7 to 30 days. Before the specified deletion date, you can cancel the deletion if you want to use the secret. If the scheduled deletion period of a secret expires, the secret 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.

**Step 1** In the navigation pane on the left, choose **Cloud Secret Management Service** > **Secrets**.

**Step 2** Locate the target secret and click **Delete**.

**Step 3** On the displayed page, select a deletion mode. If you want to delete the secret in a specific time, set **Schedule deletion**.

**Figure 4-5** Setting schedule deletion



Deletion Mode

○ Delete now ● Schedule deletion

Waiting Period (7 to 30 days):

Delete Secret

Secret [redacted] will be deleted.

| Secret Name | Status | Type |
|---|---|---|
| [redacted] | ✓ Enabled | RDS secret |

To confirm deletion, enter **"DELETE"** below.

DELETE

**Step 4** Enter **DELETE** in the confirmation dialog box if deletion verification is disabled and click **OK**.

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

NOTE

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

**----End**

# 4.3 Managing Secrets

## 4.3.1 Adding a Tag to a Secret

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

### Prerequisites

**A secret has been created**.

### Procedure

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

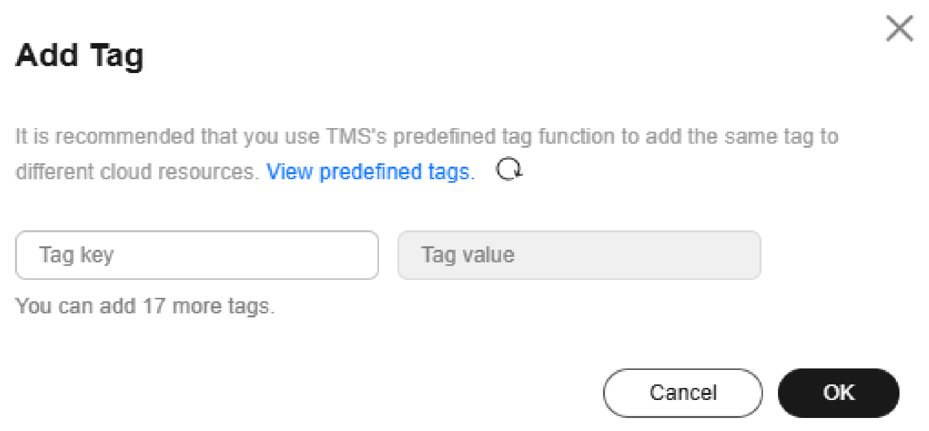
**Step 2** Click 📍 in the upper left corner and select a region or project.

**Step 3** In the navigation pane on the left, choose **Cloud Secret Management Service** > **Secrets**.

**Step 4** Click a secret name to access its details page.

**Step 5** In the **Tags** area, click **Add Tag**, as shown in **Figure 4-6**. In the **Add Tag** dialog box, enter the tag key and tag value. **Table 4-5** describes the parameters.

**Figure 4-6** 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.

You can add 17 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 4-5** Tag parameters

| Parameter | Description | Remarks |
|---|---|---|
| Tag key | Tag name.<br>The tag keys of a secret cannot have duplicate values. A tag key can be used for multiple secrets.<br>A secret can have up to 20 tags. | ● Mandatory.<br>● The tag key must be unique for the same custom key.<br>● 128 characters limit.<br>● The value cannot start or end with a space.<br>● Cannot start with **_sys_**.<br>● The following character types are allowed:<br>– Chinese<br>– English<br>– Numbers<br>– Space<br>– Special characters: _.:/=+-@ |
| Tag value | Value of the tag | ● Optional<br>● 255 characters limit.<br>● The following character types are allowed:<br>– Chinese<br>– English<br>– Numbers<br>– Space<br>– Special characters: _.:/=+-@ |

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

**----End**

## Related Operations

- **Modifying a tag value**:

   a. Click a secret name to access its details page.
   b. In the **Tags** area, locate the target tag and click **Edit** in the **Operation** column.
   c. In the **Edit Tag** dialog box, enter a tag value and click **OK**.

- **Deleting a tag**:
   a. Click a secret name to access its details page.
   b. In the **Tags** area, locate the target tag and click **Delete** in the **Operation** column.
   c. In the **Delete Tag** dialog box, click **Yes**.

## 4.3.2 Associating a Secret with an Event

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

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

### Constraints

- You can create up to 30 events.
- Simple Message Notification (SMN) is required when you create an SMN message type. SMN is billed based on the actual usage. For details, see **SMN Pricing Details**.

   NOTE

   Before setting alarm notifications, create a message topic in SMN.

### Associating a Secret with an Event

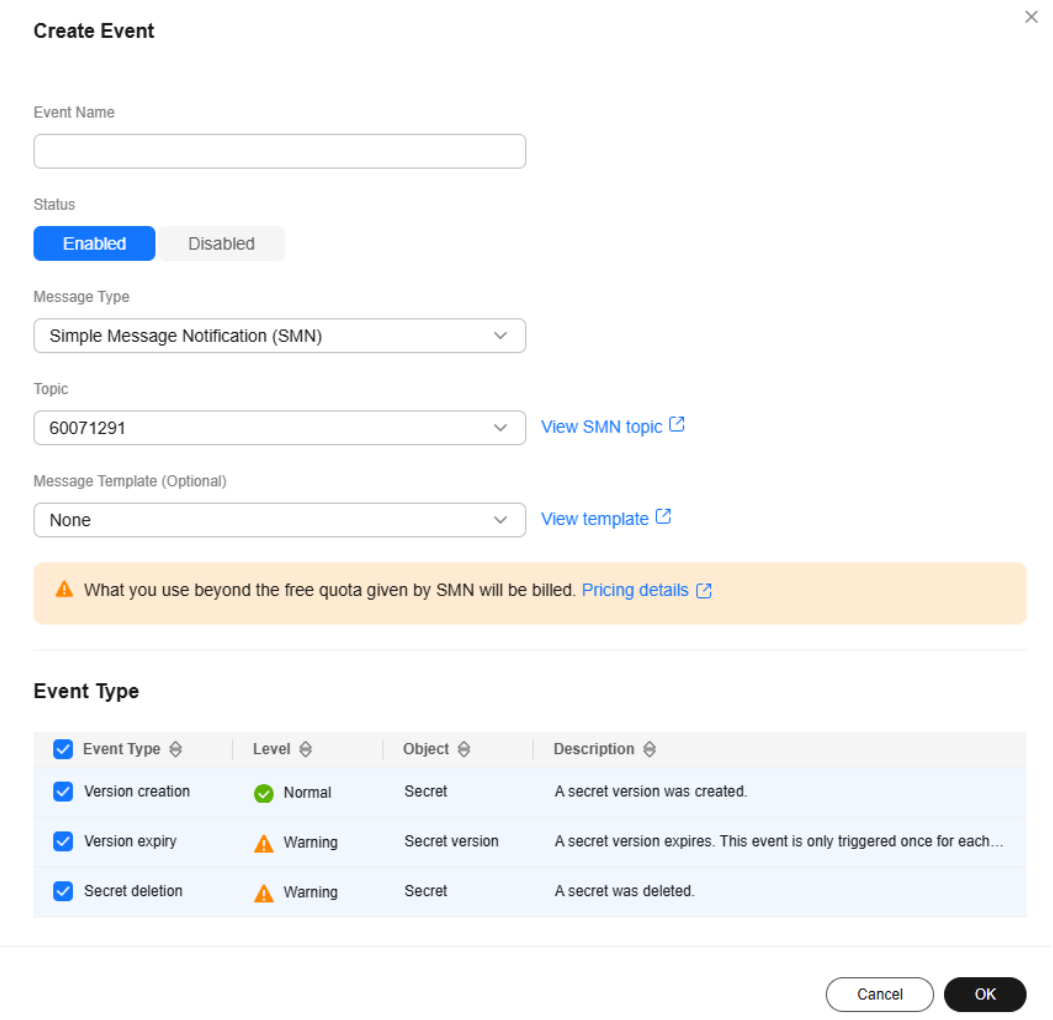
**Step 1** Log in to the **DEW console**.

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

**Step 3** In the navigation pane on the left, choose **Cloud Secret Management Service** > **Events**. The **Events** page is displayed.

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

**Figure 4-7** Creating an event



Create Event

Event Name

Status

Enabled Disabled

Message Type

Simple Message Notification (SMN)

Topic

60071291 View SMN topic

Message Template (Optional)

None View template

What you use beyond the free quota given by SMN will be billed. Pricing details

Event Type

| Event Type | Level | Object | Description |
|---|---|---|---|
| ☑ Version creation | Normal | Secret | A secret version was created. |
| ☑ Version expiry | Warning | Secret version | A secret version expires. This event is only triggered once for each... |
| ☑ Secret deletion | Warning | Secret | A secret was deleted. |

**Table 4-6** Parameters for creating an event

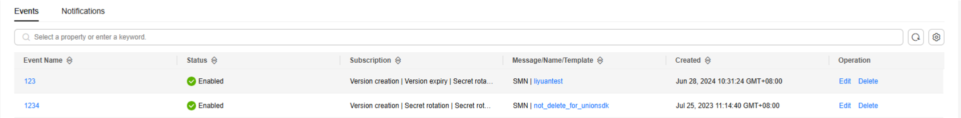
| Parameter | Description |
|---|---|
| Event Name | Name of the event to be created.<br>**NOTE**<br>Only letters, digits, hyphens (-), and underscores (_) are supported. |
| Status | The options are **Enabled** and **Disabled**. By default, **Enabled** is selected. |
| Message Type | **Simple Message Notification (SMN)**: When a selected event is triggered for the target secret, CSMS sends a notification through SMN. |

| Parameter | Description |
|---|---|
| Topic Name | Select a topic from the drop-down list or create a topic.<br>If there are no topics, click **View SMN topic** and perform the following steps to create a topic:<br>1. Create a topic. For details, see **Creating a Topic**.<br>2. Add one or more subscriptions to the topic. You will need to provide a phone number, email address, function, platform application endpoint, DMS endpoint, or HTTP/HTTPS endpoint for receiving alarm notifications. For details, see **Adding a Subscription**.<br>3. Confirm the subscription. Add and confirm the subscription.<br>For details about topics and subscriptions, see the *Simple Message Notification User Guide*. |
| Message Template | (Optional) Select a message template created in SMN or leave it as **None**. |
| Event Type | Supported event types, including **Version creation**, **Version expiry**, and **Secret deletion**. |

**Step 5** Click **OK**.

**Step 6** View the created event in the event list. The default event status is **Enabled**.

**Figure 4-8** Event list



Events | Notifications

Select a property or enter a keyword.

| Event Name | Status | Subscription | Message/Name/Template | Created | Operation |
|---|---|---|---|---|---|
| 123 | Enabled | Version creation \| Version expiry \| Secret rota... | SMN \| liyuantest | Jun 28, 2024 10:31:24 GMT+08:00 | Edit Delete |
| 1234 | Enabled | Version creation \| Secret rotation \| Secret rot... | SMN \| not_delete_for_unionsdk | Jul 25, 2023 11:14:40 GMT+08:00 | Edit Delete |

**----End**

## Viewing Event Notification Records

**Step 1** In the navigation pane on the left, choose **Cloud Secret Management Service** > **Events**. The **Events** page is displayed.

**Step 2** Click the **Notifications** tab.

**Step 3** In the **Notifications** tab, you can view the changes made to the secrets of the associated events.

**----End**

## Related Operations

- **Viewing event details**: Click the event name to view its details.
- **Editing an event**: Locate the target event and click **Edit** in the **Operation** column. On the displayed page, edit message type and event type as required.

- **Enabling an event**:
  a. Locate the target disabled event and click **Edit** in the **Operation** column.
  b. Set **Status** to **Enabled**.
  c. Click **OK**. A message is displayed in the upper right corner of the page, indicating that the event is enabled.
- **Disabling an event**:
  a. Locate the target enabled event and click **Edit** in the **Operation** column.
  b. Set **Status** to **Disabled**.
  c. Click **OK**. A message is displayed in the upper right corner of the page, indicating that the event is disabled.
- **Deleting an event**: Locate the target event and click **Delete** in the **Operation** column. In the displayed dialog box, enter **DELETE** and click **OK**.

  NOTE

  Event notifications can be deleted only after all associated secrets have been canceled. If the associated secret is not canceled, the deletion will fail.

## 4.3.3 Managing Secret Versions

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 is in the **SYSCURRENT** state. The previous version is in the **SYSPREVIOUS** state.

This section describes how to:

- Saving and Viewing Secret Values
- Managing Secret Version Statuses
- Setting the Version Expiration Time for a Secret

### Constraints

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

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

### Saving and Viewing Secret Values

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

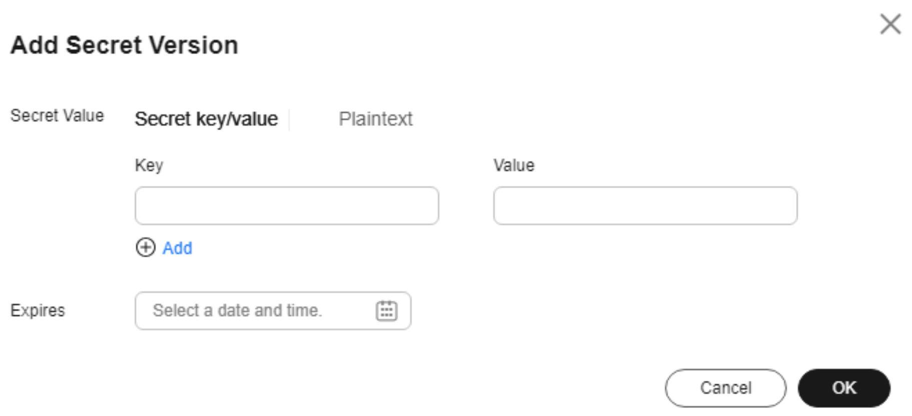
**Step 2** Click 📍 in the upper left corner and select a region or project.

**Step 3** In the navigation pane on the left, choose **Cloud Secret Management Service** > **Secrets**.

**Step 4** Click a secret name to access its details page.

**Step 5** In the **Version** area, click **Add Secret Version**, as shown in **Figure 4-9**. In the displayed dialog box, configure **Secret key/value** or **Plaintext**.

**Figure 4-9** Adding a secret value



Add Secret Version

Secret Value: Secret key/value | Plaintext

Key:

Value:

Add

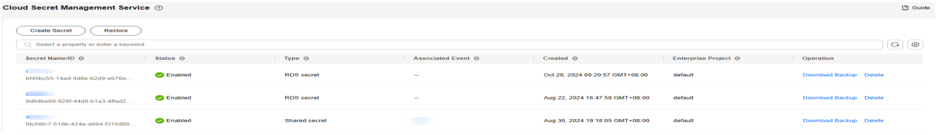
Expires: Select a date and time.

**Step 6** 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 7** Click **OK**. A message is displayed in the upper right corner of the page, indicating that the value is added successfully.

**Step 8** In the **Version List** area, locate the target secret version, click **View Secret** in the **Operation** column, as shown in **Figure 4-10**.

**Figure 4-10** Secret version list



Cloud Secret Management Service

| Secret Name/ID | Status | Type | Associated Event | Created | Enterprise Project | Operation |
|---|---|---|---|---|---|---|
| [redacted]<br>bf45bc55-14ad-4d8e-b2d9-e676e... | Enabled | RDS secret | -- | Oct 26, 2024 09:20:57 GMT+08:00 | default | Download Backup Delete |
| [redacted]<br>9d6dbe90-826f-44d9-b1a3-4ffad2... | Enabled | RDS secret | -- | Aug 22, 2024 16:47:58 GMT+08:00 | default | Download Backup Delete |
| [redacted]<br>fdc56fc7-510b-424a-a694-f315d80... | Enabled | Shared secret | [redacted] | Aug 30, 2024 19:18:05 GMT+08:00 | default | Download Backup Delete |

**Step 9** If critical operation protection is enabled, after you click **View Secret**, you need to pass the operation verification before viewing the secret value.

NOTE

For details about enabling critical operation protection, see **8.2 Critical Operation Protection**.

Generally, secret values are obtained by applications through API calls. If you need to check the secret value on the service console, enable this function for data security. Confirm again and click **OK**.

**Step 10** Click **OK**.

**----End**

## Managing Secret Version Statuses

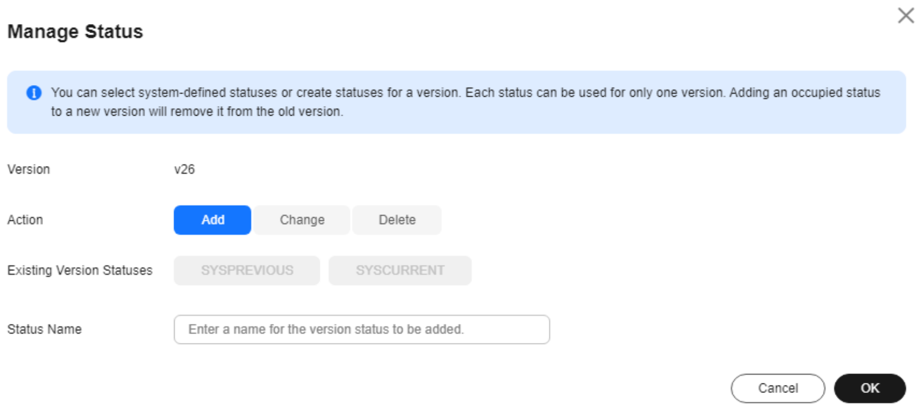
**Step 1** In the navigation pane on the left, choose **Cloud Secret Management Service** > **Secrets**.

**Step 2** Click a secret name to access its details page.

**Step 3** In the **Version List** area, click **Manage Status** in the **Operation** column.

**Step 4** In the **Manage Status** dialog box, add, change, or delete the status of a secret version.

**Figure 4-11** 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 v26

Action: Add

Existing Version Statuses: SYSPREVIOUS SYSCURRENT

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

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

- Deleting the version status

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

  NOTE

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

**----End**

## Setting the Version Expiration Time for a Secret

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

**Step 1** In the navigation pane on the left, choose **Cloud Secret Management Service** > **Secrets**.

**Step 2** Click a secret name to access its details page.

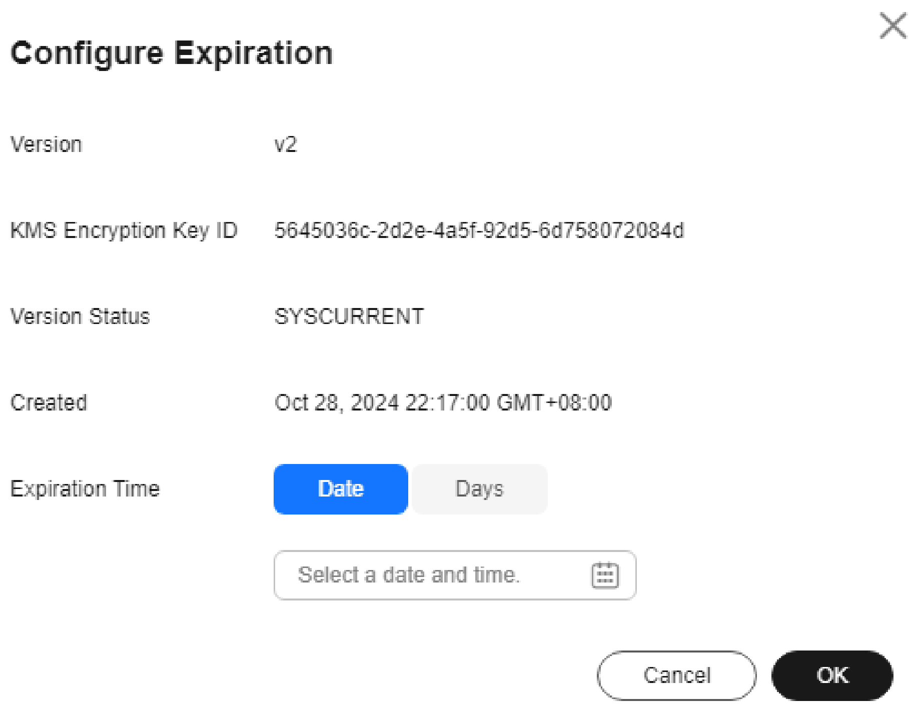
**Step 3** In the **Version** area, click **Configure Expiration** of the target secret.

**Step 4** On the displayed page, set an expiration time, and click **OK**.

NOTE

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

**Figure 4-12** Setting an expiration time



Configure Expiration

Version: v2

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

Version Status: SYSCURRENT

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

Expiration Time: Date | Days

Select a date and time.

**----End**

# 5 Dedicated HSM

## 5.1 Overview

Dedicated HSM is devoted to provide customers with **independent cryptographic resources** and **customized services** to meet specific service and security requirements. Generally, it includes:

- **Independent cryptographic resources**: You can use exclusive resources, such as HSMs and KMS, to ensure the independence and security of encryption operations.
- **Customized cryptographic policies**: You can customize cryptographic algorithms, key management policies, and access control policies as required.
- **Data isolation**: Ensure that your data is completely separated from the data of other users through physical or logical isolation to prevent data leakage.

### Restrictions

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

### Supported Cryptography Algorithms

You can use international common cryptographic algorithms to meet various user requirements.

**Table 5-1** Supported cryptography algorithms

| Category | Common Cryptographic Algorithm |
|---|---|
| Symmetric cryptographic algorithm | AES |

| Category | Common Cryptographic Algorithm |
|---|---|
| Asymmetric cryptographic algorithm | RSA, DSA, ECDSA, DH, and ECDH |
| Digest algorithm | SHA1, SHA256, and SHA384 |

## Supported HSMs

**Table 5-2** Supported HSMs

| HSM Type | Function | Scenario |
|---|---|---|
| Cloud HSM | ● Data encryption and decryption<br>● Data signature and verification<br>● Data digest<br>● Generation and verification of MAC addresses | Basic password calculations in applications of a wide range of industries, such as identity authentication, data protection, SSL keys, and computation offloading. |
| Financial HSM | ● Generation, encryption, conversion, and verification of personal identification number (PIN)<br>● Generation and verification of Media Access Control (MAC)<br>● Generation and verification of Card Verification Value (CVV)<br>● Generation and verification of Type Allocation Code (TAC)<br>● Typical Racal instruction set<br>● People's Bank of China (PBOC) 3.0 common instruction set | Cryptographic calculation in financial systems, such as card issuing systems and point of sale (POS) systems |
| Signature verification server | ● Signing and signature verification<br>● Encoding and decoding of digital envelopes<br>● Encoding and decoding of signed digital envelopes<br>● Certificate verification | Signature usage in Certificate Authority (CA) systems, certificate verification, encrypted transmission of a large amount of data, and identity authentication |

## Operation Guide

To use Dedicated HSM on the cloud, you can create Dedicated HSM instances through the management console. After a Dedicated HSM instance is created, you will receive the UKey sent by Dedicated HSM. You need to use the UKey to initialize and control the instance. You can use the management tool to authorize service applications the permission to access Dedicated HSM instances. **Figure 5-1** illustrates the operation flow.

**Figure 5-1** Operation Guide

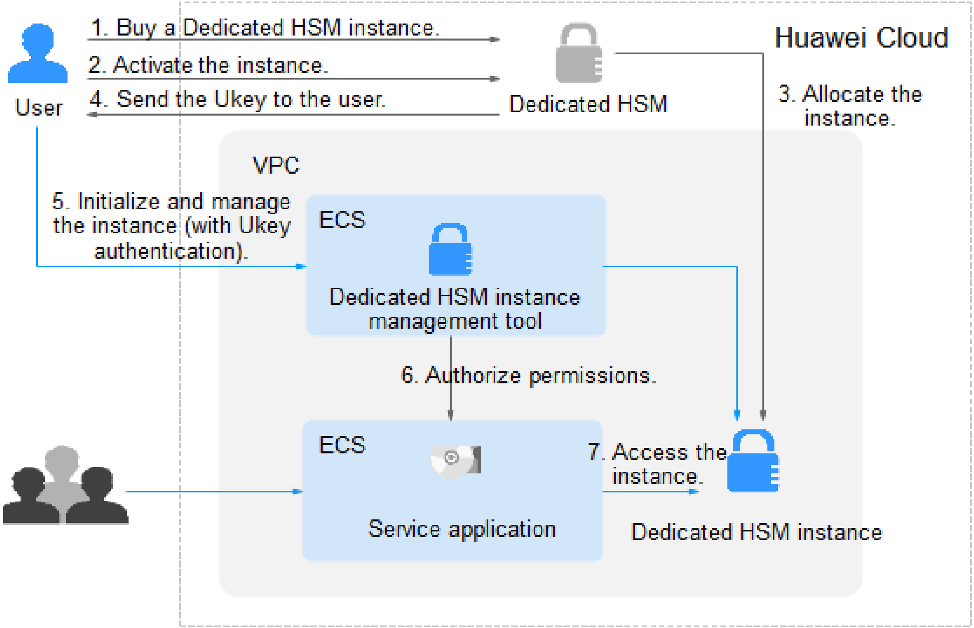

1. Buy a Dedicated HSM instance.
2. Activate the instance.
4. Send the Ukey to the user.
User
Dedicated HSM
Huawei Cloud
3. Allocate the instance.
VPC
5. Initialize and manage the instance (with Ukey authentication).
ECS
Dedicated HSM instance management tool
6. Authorize permissions.
ECS
Service application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

**Table 5-3** describes the operation guide.

**Table 5-3** 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 **5.3.1 Activating a Dedicated HSM Instance**. | User |

| No. | Procedure | Description | Operated By |
|---|---|---|---|
| 3 | Allocate a Dedicated HSM instance. | A security expert will contact you through the contact information you provided and determine whether the instance ordered meets your service requirements. The instance will be allocated after the expert reviews and confirms your order. | Dedicated HSM security expert |
| 4 | Obtain the UKey, initialization documents, 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.<br>● A security expert will provide you with the software and guide for initializing Dedicated HSM instances. If you have any questions, contact the expert.<br>**NOTE**<br>You can **submit a service ticket** to provide the Ukey recipient address and contact security experts for guidance. | 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.<br>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.<br>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.<br>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 |

## Dedicated HSM and CPCS

Dedicated HSM and CPCS are both used for encryption and security assurance. However, their functions, applications, and management methods differ. For details, see **Table 5-4**.

**Table 5-4** Differences and connections between Dedicated HSM and CPCS

| **Service** | Dedicated HSM | CPCS |
|---|---|---|
| **Function** | ● Dedicated HSMs are provided for users to enjoy exclusive resources.<br>● The main functions include encryption, decryption, signature, signature verification, key generation, and secure storage.<br>● Multiple algorithms certified by CSCA are supported.<br>● It can be used for scenarios that require high security and performance, such as financial payment and electronic signature. | ● A one-stop cryptographic service management platform is provided. Cluster deployment is supported.<br>● The main functions include not only encryption, decryption, signature, and signature verification, but also key management, timestamp, electronic seal, and database encryption. |
| **Application** | ● Used for scenarios that require high data security and performance, such as financial payment, electronic signature, and securities services.<br>● Applicable to enterprises and organizations that meet regulatory compliance requirements. | ● Applicable to enterprises and organizations that require multiple cryptographic services and need to pass the cryptography test quickly.<br>● Used for scenarios that require multiple cryptographic services, such as electronic contracts, electronic invoices, and electronic medical records. |

| | | |
|---|---|---|
| **Management method** | ● You can perform initialization and permission management by managing the client.<br>● Hardware resources of high security are provided. You have full control over the generation, storage, and access authorization of keys. | ● Central management on the console is provided. Automatic deployment and monitoring are supported.<br>● Cluster deployment is supported, and elastic scaling and application-level isolation are supported. |
| **Connection** | ● **Mutual goal**: Provide secure cryptographic services to protect data security and integrity.<br>● **Integration and complementarity**: These two services can be integrated in certain scenarios. For example, Dedicated HSM can be used as the underlying cryptographic resource of CPCS, providing high-performance encryption computing support. | |

# 5.2 Purchasing a Dedicated HSM Instance

## 5.2.1 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 **5.3.1 Activating a Dedicated HSM Instance**.

### Prerequisites

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

### Constraints

You need to activate the instance before using it.

## Procedure

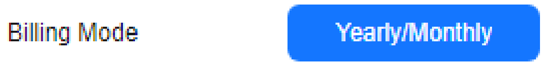
**Step 1** Log in to the **DEW console**.

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

**Step 3** Click **Create Dedicated HSM** in the upper right corner of the page.

**Step 4** **Billing Mode** can only be set to **Yearly/Monthly**.

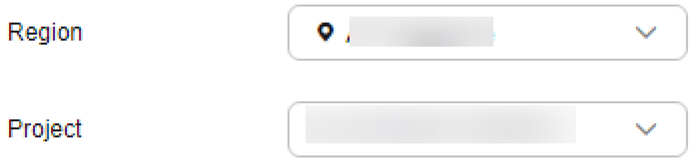
**Figure 5-2** Billing Mode



Billing Mode: Yearly/Monthly

**Step 5** Select a region and project.

**Figure 5-3** Selecting a region



Region: [redacted]

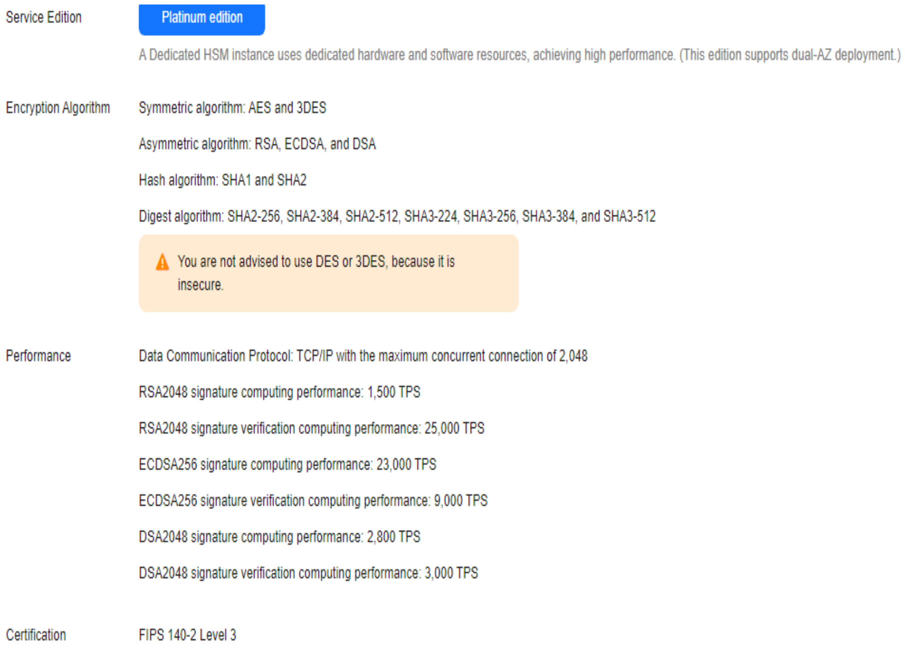
Project: [redacted]

**NOTE**

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

**Step 6** Select an instance edition. For details, see **Figure 5-4**. **Table 5-5** lists related parameters.

**Figure 5-4** Platinum edition



Service Edition: Platinum edition

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

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

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

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

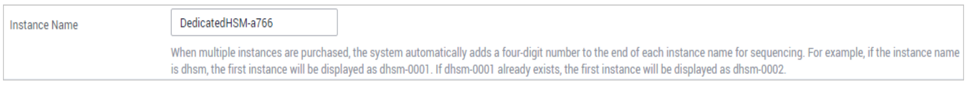
Certification: FIPS 140-2 Level 3

**Table 5-5** Edition parameters

| Parameter | Description |
|---|---|
| Service Edition | Platinum edition |
| Encryption Algorithm | Algorithm supported by the HSM instance.<br>● Symmetric algorithms: AES and DES<br>● Asymmetric algorithms: RSA, DSA, ECDSA, and ECDH<br>● Digest algorithms: SHA1, SHA256, and SHA384 |
| Specifications | Performance specifications supported by platinum edition, including:<br>● Data communication protocol: TCP/IP (maximum number of concurrent connections: 2,048)<br>● RSA2048 signature computing performance: 1,500 TPS<br>● RSA2048 signature verification computing performance: 25,000 TPS<br>● ECDSA256 signature computing performance: 23,000 TPS<br>● ECDSA256 signature verification computing performance: 9,000 TPS<br>● DSA2048 signature computing performance: 2,800 TPS<br>● DSA2048 signature verification computing performance: 3,000 TPS |
| Certification | FIPS 140-2 Level 3 certified |

**Step 7** Set the instance name.

**Figure 5-5** Setting an instance name



Instance Name: DedicatedHSM-a766

When multiple instances are purchased, the system automatically adds a four-digit number to the end of each instance name for sequencing. For example, if the instance name is dhsm, the first instance will be displayed as dhsm-0001. If dhsm-0001 already exists, the first instance will be displayed as dhsm-0002.

**Step 8** 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 9** Set the duration and number of Dedicated HSM instances to be purchased.

1. Set the required duration.

   The required duration ranges from one month to one year.

2. Set the **Quantity**.

   You can set the quantity as required.

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

   NOTE

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

**Step 10** (Optional) Add tags to the dedicated HSM instance as needed, and enter the tag key and tag value.

NOTE

- To add tags for an instance, locate the instance, and click **Tag** in the **Operation** column. For details about other operations, see **6.1 Tag Management**.
- An instance can have up to 20 tags.

**Step 11** Confirm the configuration and click **Next**. For any doubt about the pricing, click **Pricing details** to understand more.

**Step 12** On the **Order Details** page, confirm the order details, read and select **I have read and agree to the Privacy Policy Statement**.

**Step 13** Click **Pay Now**. On the displayed page, select a payment method and pay.

**Step 14** After successful payment, you can view the information about the HSM instance on the HSM instance list page.

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

**----End**

# 5.3 Activating and Using a Dedicated HSM Instance

## 5.3.1 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 locate the target instance and click **Delete**. Then apply for a refund by submitting a service ticket.
- After a Dedicated HSM instance is successfully created, it cannot be changed to another type. To use a Dedicated HSM instance of another type, you need to buy another one.

## Procedure

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

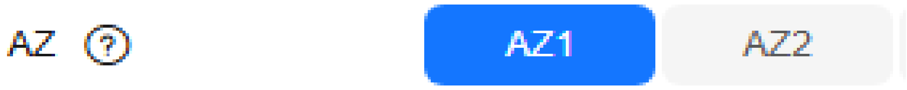
**Step 2** Click in the upper left corner and select a region or project.

**Step 3** In the navigation pane on the left, choose **Dedicated HSM** > **Instances**.

**Step 4** Locate the target instance and click **Activate** in the **Operation** column.

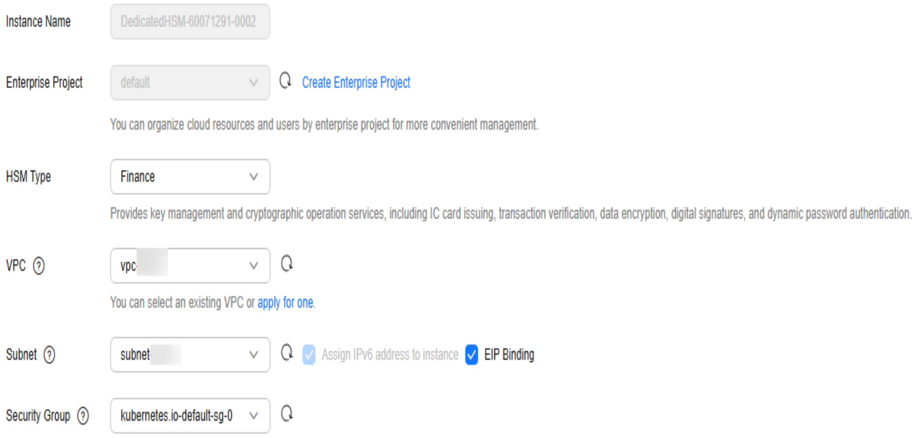
**Step 5** Select an AZ.

**Figure 5-6** Selecting an AZ



**Step 6** Enter activation information, as shown in **Figure 5-7**. **Table 5-6** describes the parameters.

**Figure 5-7** Configuring a Dedicated HSM instance



Instance Name: DedicatedHSM-60071291-0002

Enterprise Project: default Create Enterprise Project

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

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-[redacted]

You can select an existing VPC or apply for one.

Subnet ?: subnet-[redacted] ☑ Assign IPv6 address to instance ☑ EIP Binding

Security Group ?: kubernetes.io-default-sg-0

**Table 5-6** Parameter description

| Parameter | Description | Example Value |
|---|---|---|
| Instance Name | Name of a Dedicated HSM instance<br>**NOTE**<br>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**.<br>● **Finance**: Provides key management and encryption computing services, including IC card issuing, transaction verification, data encryption, digital signatures, and dynamic password authentication.<br>● **Server**: Provides secure, complete key management services and high-performance concurrent cryptographic operations, such as data signatures, signature verification, and data encryption/decryption.<br>● **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.<br>For more information about VPC, see the *Virtual Private Cloud User Guide*. | vpc-test-dhsm |
| Subnet | All available subnets are displayed on the page. The system automatically assigns three IP address to the instance. For more information about subnets, see the *Virtual Private Cloud User Guide*.<br>**NOTE**<br>Two nodes are created as the background resource pool for a Dedicated HSM instance. To ensure high availability of the nodes, a floating IP address is assigned to the instance. | **subnet-test-dhsm (192.168.0.0/24)** |
| EIP Binding | After this parameter is enabled, you can bind an EIP to the Dedicated HSM instance to enable public access to the instance. | - |

| 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.<br>For more information about security groups, see the *Virtual Private Cloud User Guide*. | WorkspaceUserSecurityGroup |

**Step 7** 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 8** If you have purchased a Dedicated HSM instance in platinum edition:

1. Set the required duration.

   The required duration ranges from one month to one year.

   NOTE

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

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

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

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

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

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

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

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

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

     NOTE

     If the instance fails to be created, you can locate the instance, and click **Delete**. Then apply for a refund by submitting a service ticket.

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

NOTE

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

**----End**

## 5.3.2 Using Dedicated HSM Instances

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

### Prerequisites

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

**Table 5-7** 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 you 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. | |

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

## Initializing a Dedicated HSM Instance

NOTE

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

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

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

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

# 5.4 Managing Dedicated HSM Instances

## 5.4.1 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 **DEW console**.

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

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

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

**Table 5-8** 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:<br>● Installing After you pay the initial installation fee, the purchased instance will be installed. The status of the Dedicated HSM instance will be **Installing**.<br>● To be activated The status of an instance that has been installed but not activated is **To be activated**.<br>● 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.<br>● 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**.<br>● Running After an instance is configured and allocated, it will be in the status of **Running**.<br>● Frozen If an instance is not renewed upon its expiration, its status changes to **Frozen**. |
| Service Edition | Platinum edition: You can exclusively use the HSM subrack, power supply, the network bandwidth, and API resources of the HSM. |
| AZ | AZ of a device |
| IP Address | Floating IP address of the Dedicated HSM instance |
| Expiration Time | Expiration time of the purchased HSM instance. |

**Step 5** Locate a Dedicated HSM instance and click ^ to view its details.

For more information, see **Table 5-9**.

**Table 5-9** Parameter description

| Parameter | Description |
|---|---|
| Name | Name of a Dedicated HSM instance |
| ID | ID of an instance |

| Parameter | Description |
|---|---|
| Status | Status of a Dedicated HSM instance:<br>● Installing<br>After you pay the initial installation fee, the purchased instance will be installed. The status of the Dedicated HSM instance will be **Installing**.<br>● To be activated<br>The status of an instance that has been installed but not activated is **To be activated**.<br>● Creating<br>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.<br>● Creation failed<br>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**.<br>● Running<br>After an instance is configured and allocated, it will be in the status of **Running**.<br>● Frozen<br>If an instance is not renewed upon its expiration, its status changes to **Frozen**. |
| Service Edition | Platinum edition: You can exclusively use the HSM subrack, power supply, the network bandwidth, and API resources of the HSM. |
| HSM Type | HSM types of an instance, including **Finance**, **Server**, and **Signature verification server**. |
| VPC | VPC to which the instance belongs<br>For more information about VPC, see *Virtual Private Cloud User Guide*. |
| Subnet | Subnet where the instance is located.<br>For more information about subnets, see *Virtual Private Cloud User Guide*. |
| IP Address | Floating IP address of the Dedicated HSM instance |
| Security Group | Security group to which the instance belongs<br>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 |

| Parameter | Description |
|---|---|
| Order | Order ID of the instance. You can click the order number to query the order details. |
| Billing Mode | Yearly/Monthly prepaid package |

**----End**

## 5.4.2 Adding a Tag to a Dedicated HSM Instance

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

### Adding a Tag to a Dedicated HSM Instance

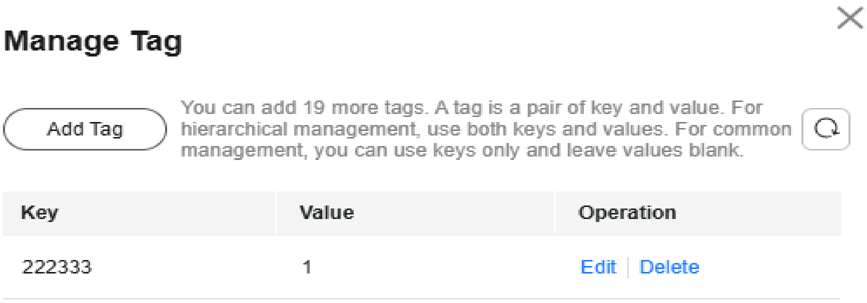
**Step 1** Log in to the **DEW console**.

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

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

**Step 4** Locate the target instance and click **Manage Tag** in the **Operation** column. The tag management dialog box is displayed, as shown in **Figure 5-8**.

**Figure 5-8** Managing tags



Manage Tag

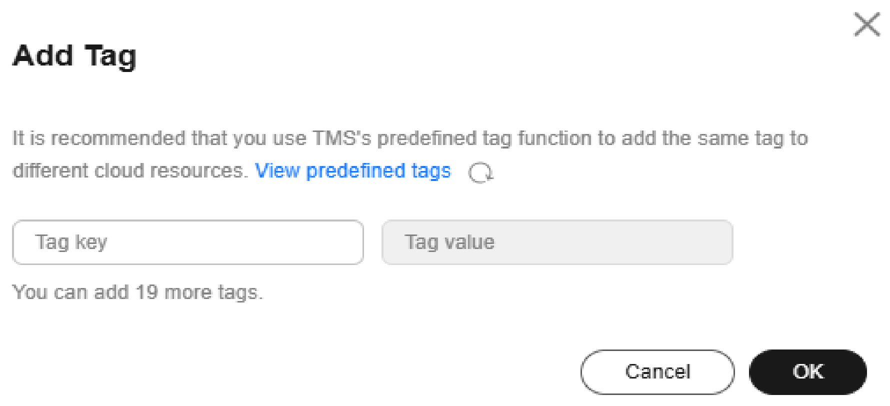
Add Tag

You can add 19 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 |
|---|---|---|
| 222333 | 1 | Edit \| Delete |

**Step 5** Click **Add Tag**. In the displayed dialog box, enter the tag key and tag value. For details about the parameters, see **Table 5-10**.

**Figure 5-9** 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 19 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 5-10** Tag parameters

| Parameter | Description | Remarks |
|---|---|---|
| Tag key | Tag name.<br>The tag keys of a secret cannot have duplicate values. A tag key can be used for multiple secrets.<br>A secret can have up to 20 tags. | ● Mandatory.<br>● The tag key must be unique for the same custom key.<br>● 128 characters limit.<br>● The value cannot start or end with a space.<br>● Cannot start with **_sys_**.<br>● The following character types are allowed:<br>– Chinese<br>– English<br>– Numbers<br>– Space<br>– Special characters: _.:/=+-@ |

| Parameter | Description | Remarks |
|---|---|---|
| Tag value | Value of the tag | ● Optional<br>● 255 characters limit.<br>● The following character types are allowed:<br>– Chinese<br>– English<br>– Numbers<br>– Space<br>– Special characters: _.:/=+-@ |

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

**----End**

## Modifying a Tag Value

**Step 1** In the navigation pane on the left, choose **Dedicated HSM**.

**Step 2** Locate the target instance and click **Manage Tag** in the **Operation** column. The **Manage Tag** dialog box is displayed.

**Step 3** Click **Edit**. The **Edit Tag** dialog box is displayed. After changing the tag value, click **OK**.

**----End**

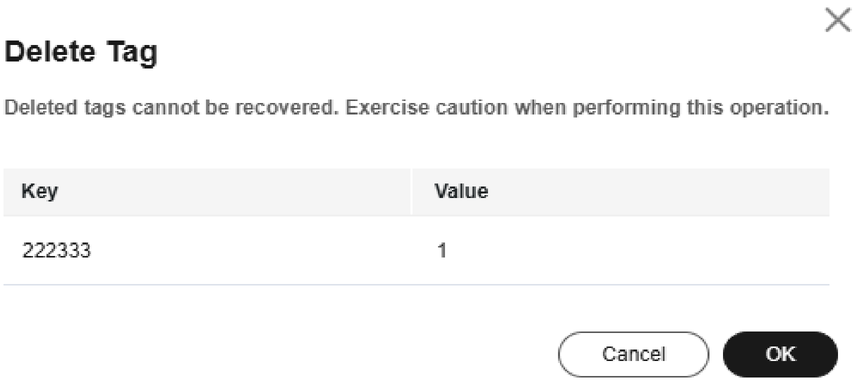
## Deleting a Tag

**Step 1** In the navigation pane on the left, choose **Dedicated HSM**.

**Step 2** Locate the target instance and click **Manage Tag** in the **Operation** column. The **Manage Tag** dialog box is displayed.

**Step 3** Locate the target tag and click **Delete** in the **Operation** column.

**Figure 5-10** Deleting a tag



Delete Tag

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

| Key | Value |
|---|---|
| 222333 | 1 |

**Step 4** In the **Delete Tag** dialog box, click **Yes**.

**----End**

# 6 Tags and Quotas

## 6.1 Tag Management

### 6.1.1 Overview

#### Scenario

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

Tags can be added during or after resource creation.

#### Tag Naming Rules

- Each tag consists of a key-value pair.
- A maximum of 20 tags can be added to a resource.
- For each resource, a tag key must be unique and can have only one tag value.
- A tag consists of a tag key and a tag value. The naming rules are listed in **Table 6-1**.
- Tags are key-value pairs, which are used to identify, classify, and search for vaults. Vault tags are used to filter and manage vaults only. A vault can have up to 10 tags.

  **NOTE**

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

**Table 6-1** Tag parameters

| Parameter | Rules | Example |
|---|---|---|
| Tag key | ● This parameter is mandatory.<br>● The tag key must be unique for the same custom key.<br>● 128 characters limit.<br>● The value cannot start or end with a space.<br>● The value cannot start with **_sys_**.<br>● The following character types are allowed:<br>– Chinese<br>– English<br>– Digits<br>– Space<br>– Special characters: _.:=+-@ | cost |
| Tag value | ● This parameter can be left empty.<br>● 255 characters limit.<br>● The following character types are allowed:<br>– Chinese<br>– English<br>– Digits<br>– Space<br>– Special characters: _.:=+-@ | 100 |

## 6.1.2 Creating a Tag Policy

### Introduction

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

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

You can use tag policies as detective or preventive guardrails:

1. Detective guardrails: If a resource tag violates the tag policy, the resource will appear as non-compliant in the compliance result.

2. Preventive guardrails: If enforcement is enabled for a tag policy, non-compliant tagging operations will be prevented from being performed on specified resource types.

## Constraints

Only organization administrators can create a tag policy.

NOTE

Before you create a tag policy and add it to the organization unit and account, a tag policy must be enabled by the administrator account. For details, see .

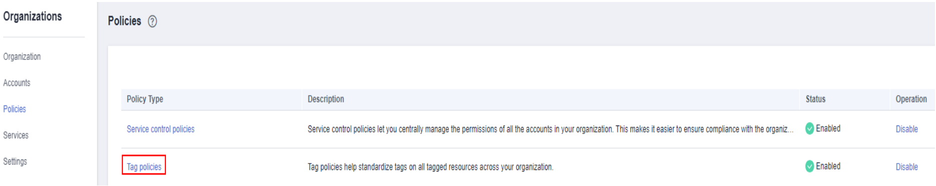
## Procedure

**Step 1** Log in to Huawei Cloud as the organization administrator or using the management account.

**Step 2** Click ☰ on the left, choose **Management & Governance** > **Organizations**. The organization management page is displayed.

**Step 3** Click **Policies** on the left to go to the policy management page and click **Tag policies**.

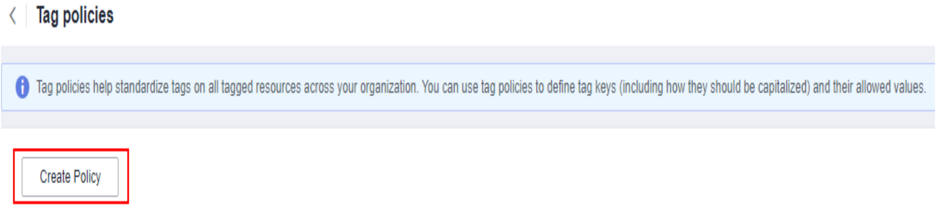
**Figure 6-1** Accessing the **Tag policies** page



| Policy Type | Description | Status | Operation |
|---|---|---|---|
| Service control policies | Service control policies let you centrally manage the permissions of all the accounts in your organization. This makes it easier to ensure compliance with the organiz... | Enabled | Disable |
| Tag policies | Tag policies help standardize tags on all tagged resources across your organization. | Enabled | Disable |

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

**Figure 6-2** Creating a policy



Tag policies help standardize tags on all tagged resources across your organization. You can use tag policies to define tag keys (including how they should be capitalized) and their allowed values.

**Step 5** Enter a policy name. Ensure that you are entering a unique policy name, different from any existing name.

**Step 6** Set a policy according to **Tag Policy Syntax**. The system automatically verifies the syntax. If the syntax is incorrect, modify it as prompted.

**Step 7** (Optional) Add one or more tags to the policy. Enter a tag key and a tag value, and click **Add**.

**Step 8** Click **Save** in the lower right corner. If the tag policy is created successfully, it will be added to the list.

NOTE

To update or delete a tag policy, see **Updating or Deleting a Tag Policy**.

To attach or detach a tag policy, see **Attaching or Detaching a Tag Policy**.

**----End**

## 6.1.3 Creating a Tag

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

### Constraints

Tags cannot be added to default keys.

### Key Management

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

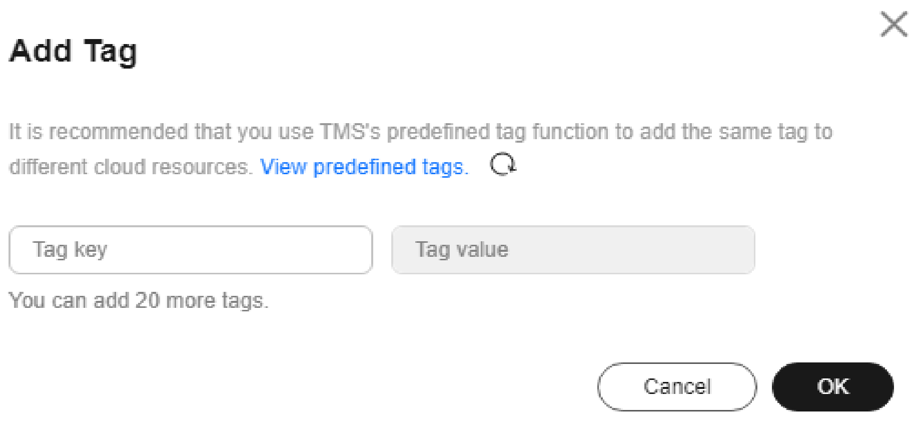
**Step 2** Click 📍 in the upper left corner and select a region or project.

**Step 3** Click the alias of the target custom key to view its details.

**Step 4** Click **Tags** to go to the tag management page.

**Step 5** Click **Add Tag**. In the displayed dialog box, set **Tag key** and **Tag value**, as shown in **Figure 6-3**.

**Figure 6-3** 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

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

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

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

**----End**

## CSMS

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

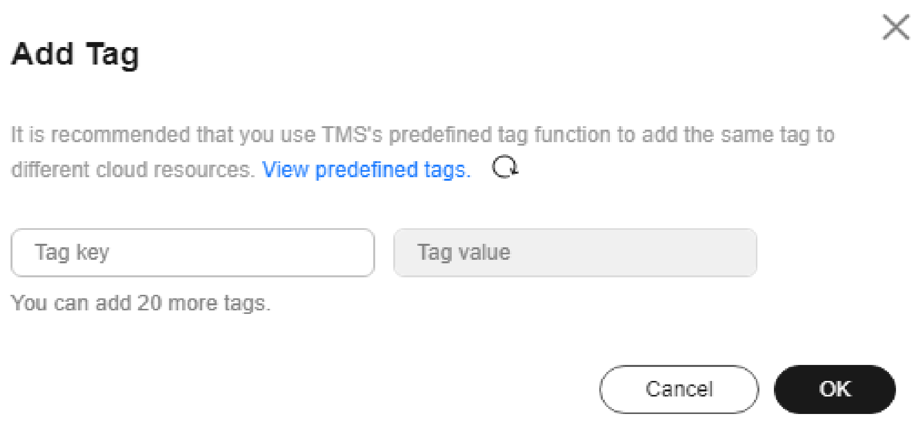
**Step 2** Click in the upper left corner and select a region or project.

**Step 3** In the navigation pane on the left, choose **Cloud Secret Management Service** > **Secrets**.

**Step 4** Click a secret name to access its details page.

**Step 5** In the **Tags** area, click **Add Tag**. In the displayed **Add Tag** dialog box, enter a **Tag key** and **Tag value**.

**Figure 6-4** Adding a tag



Add Tag

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

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.

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

**----End**

## Dedicated HSM

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

**Step 2** In the navigation pane on the left, choose **Dedicated HSM**.

**Step 3** Click **Tag Management** in the **Operation** column.

**Step 4** Click **Add Tag**. On the displayed dialog box, set **Tag key** and **Tag value**.

NOTE

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

**Step 5** Click **OK**.

**----End**

# 6.1.4 Searching for a Custom Key by Tag

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

## Prerequisites

Tags have been added.

## Constraints

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

## Procedure

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

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

**Step 3** Click the search box and enter the tag key and tag value of the resource you want to search for. The custom keys that meet the search criteria are displayed.

NOTE

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

**----End**

# 6.1.5 Modifying a Tag Value

This section describes how to modify a created tag.

## Procedure

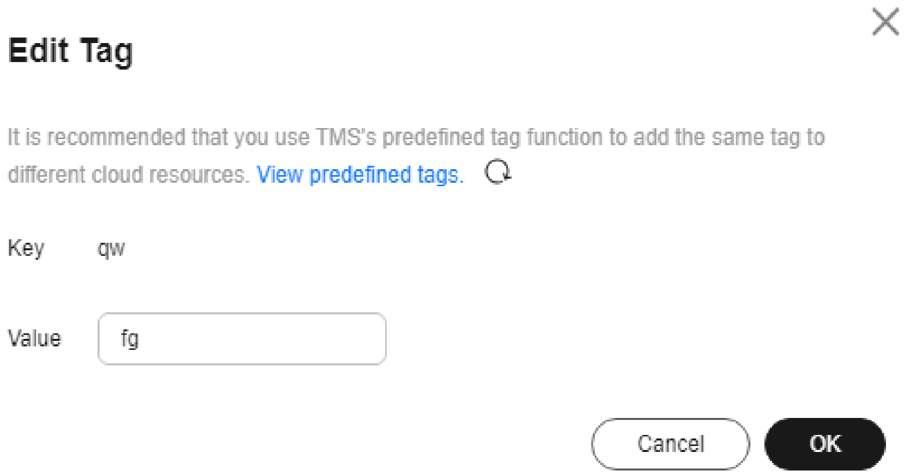
**Step 1** Log in to the **DEW console**.

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

**Step 3** Choose the service from the left, click the instance whose tag needs to be modified, and go to the details page.

**Step 4** Select the corresponding tags, click **Edit**, and the **Edit Tag** box is displayed. After changing the tag value, click **OK**.

**Figure 6-5** 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 qw

Value fg

**----End**

# 6.1.6 Deleting a Tag

This section describes how to delete a created tag.

## Procedure

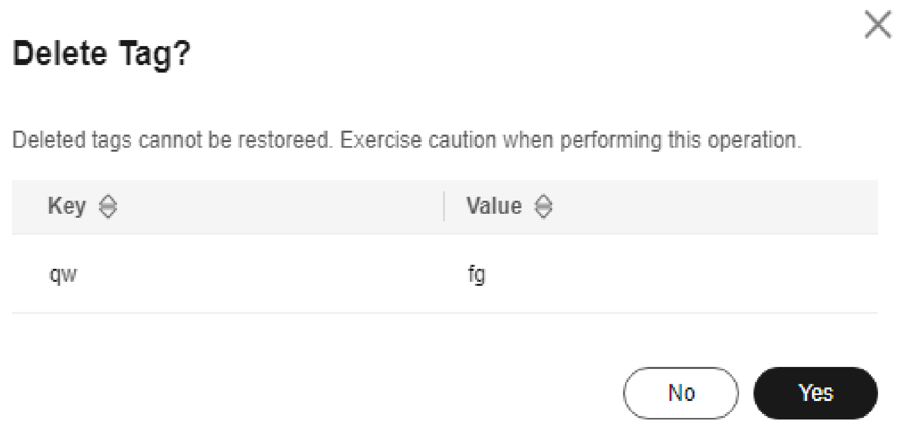
**Step 1** Log in to the **DEW console**.

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

**Step 3** Choose the service from the left, click the instance whose tag needs to be deleted, and go to the details page.

**Step 4** In the **Operation** column of a tag, click **Delete**.

**Figure 6-6** Deleting a tag



Delete Tag?

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

| Key | Value |
|---|---|
| qw | fg |

**Step 5** In the **Delete Tag** dialog box, click **Yes**.

**----End**

# 6.2 Quota Adjustment

## What Is a Quota?

Quotas put limits on the quantity and capacity of resources available to users to prevent resource abuse. For example, the maximum number of CMKs that you can create.

If the existing resource quota cannot meet your service requirements, you can apply for a higher quota.

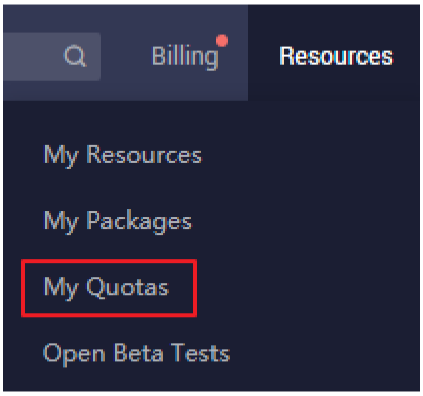
## Viewing Quotas

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

**Step 2** Hover the cursor over **Resources** on the top menu bar and choose **My Quotas**.

The **Quotas** page is displayed.

**Figure 6-7** My quotas



**Step 3** View the used and total quota of each type of resources on the displayed page.

If a quota cannot meet your service requirements, click **Increase Quota** to change it.

**----End**

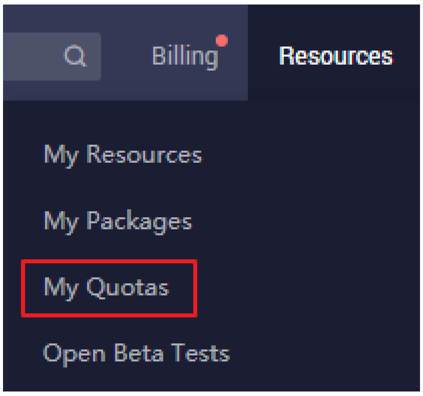
## Increasing Quotas

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

**Step 2** Hover the cursor over **Resources** on the top menu bar and choose **My Quotas**.

The **Quotas** page is displayed.

**Figure 6-8** My quotas



**Step 3** Click **Increase Quota**.

**Step 4** On the displayed **Create Service Ticket** page, configure parameters as required.

In the **Problem Description** area, fill in the content and reason for the increase.

**Step 5** Configure the parameters, select **I have read and agree to the user need to know**, and click **Submit**.

**----End**

# 7 Monitoring and Auditing

## 7.1 Using Cloud Eye to Monitor DEW

### 7.1.1 Metrics Supported by DEW

This section describes the monitoring metrics supported by DEW. The following describes the functions, namespaces, monitoring metrics, and dimensions.

#### Description

This section describes basic monitoring metrics reported by DEW to Cloud Eye. You can use Cloud Eye to view these metrics and alarms generated for DEW.

#### Namespaces

Key management: SYS.KMS

Secret management: SYS.CSMS

**NOTE**

A namespace is an abstract collection of resources and objects. Multiple namespaces can be created in a single cluster with the data isolated from each other. This enables namespaces to share the same cluster services without affecting each other.

## DEW Monitoring Metrics

**Table 7-1** Monitoring metrics of key management

| ID | Name | Description | Value Range | Unit | Conversion Rule | Dimension | Monitoring Period (Original Metric) |
|---|---|---|---|---|---|---|---|
| delkey_remaing_time | Remaining time of the key | Remaining time before the scheduled deletion of a key | ≥ 0 hours | Hour | N/A | key_id | 5 minutes |
| matrial_remaing_time | Remaining validity period of the key material | Remaining validity period of an imported key material | ≥ 0 hours | Hour | N/A | key_id | 5 minutes |

**Table 7-2** Monitoring metrics of secret management

| ID | Name | Description | Value Range | Unit | Conversion Rule | Monitored Object (Dimension) | Monitoring Period (Original Metric) |
|---|---|---|---|---|---|---|---|
| del_secret_remaining_time | Remaining time for scheduled secret deletion | Time remaining until a secret is deleted | ≥ 0 hours | Hour | N/A | secret_id | 5 minutes |

## Dimensions

| Key | Value |
|---|---|
| key_id | Key ID<br>You can obtain the value by referring to **Querying the Key List**. |
| secret_id | Secret ID<br>You can obtain the value by referring to **Querying a Secret**. |

# 7.1.2 Events Supported by DEW

## Description

Event monitoring provides event data reporting, query, and alarm reporting. You can create alarm rules for both system events and cloud events. Cloud Eye will generate an alarm for you once an event occurs.

## Namespace

Key management: SYS.KMS

Secret management: SYS.CSMS

## Events Supported By DEW

**Table 7-3** Events supported by KMS

| Event Name | Event ID | Severity | Description | Handling Suggestion | Impact |
|---|---|---|---|---|---|
| Disabling a key | disableKey | Major | A key is disabled and cannot be used. | If the customer needs to disable the key, no action is required. However, if the key is disabled by mistake, the customer needs to log in to the DEW console and enable it again. | Services may be affected if the key is being used. |

| Event Name | Event ID | Severity | Description | Handling Suggestion | Impact |
|---|---|---|---|---|---|
| Scheduling the deletion of a key | scheduleKeyDeletion | Minor | A key is scheduled to be deleted and cannot be used. | If the customer needs to delete the key, no action is required. However, if the deletion of the key is scheduled by mistake, the customer needs to log in to the DEW console, cancel the scheduled deletion, and enable the key again. | Services may be affected if the key is being used. |
| Retiring a grant | retireGrant | Major | A grant is retired and the key cannot be used. | If the customer needs to cancel the key grant, no action is required. However, if the grant is canceled by mistake, the customer needs to log in to the DEW console and create the grant again. | Services may be affected if the key is being used. |
| Revoking a grant | revokeGrant | Major | A grant is revoked and the key cannot be used. | If the customer needs to cancel the key grant, no action is required. However, if the grant is canceled by mistake, the customer needs to log in to the DEW console and create the grant again. | Services may be affected if the key is being used. |

**Table 7-4** Events supported by CSMS

| Event Name | Event ID | Severity | Description | Handling Suggestion | Impact |
|---|---|---|---|---|---|
| Performing operations on secrets to be deleted | operateDeletedSecret | Major | A user attempts to perform operations on a secret scheduled to be deleted by calling APIs. | Cancel the schedule deletion of the secret. | Secrets deleted upon scheduled deletion cannot be restored. |

## 7.1.3 Creating an Alarm Rule for Metrics and Events

You can set DEW alarm rules to customize the monitored objects and notification policies, and set parameters such as the alarm rule name, monitored object, metric, threshold, monitoring period, and whether to send notifications. This helps you learn the DEW protection status in a timely manner.

### Prerequisites

A key or secret instance has been created.

### Procedure

**Step 1** Log in to the **Cloud Eye console**.

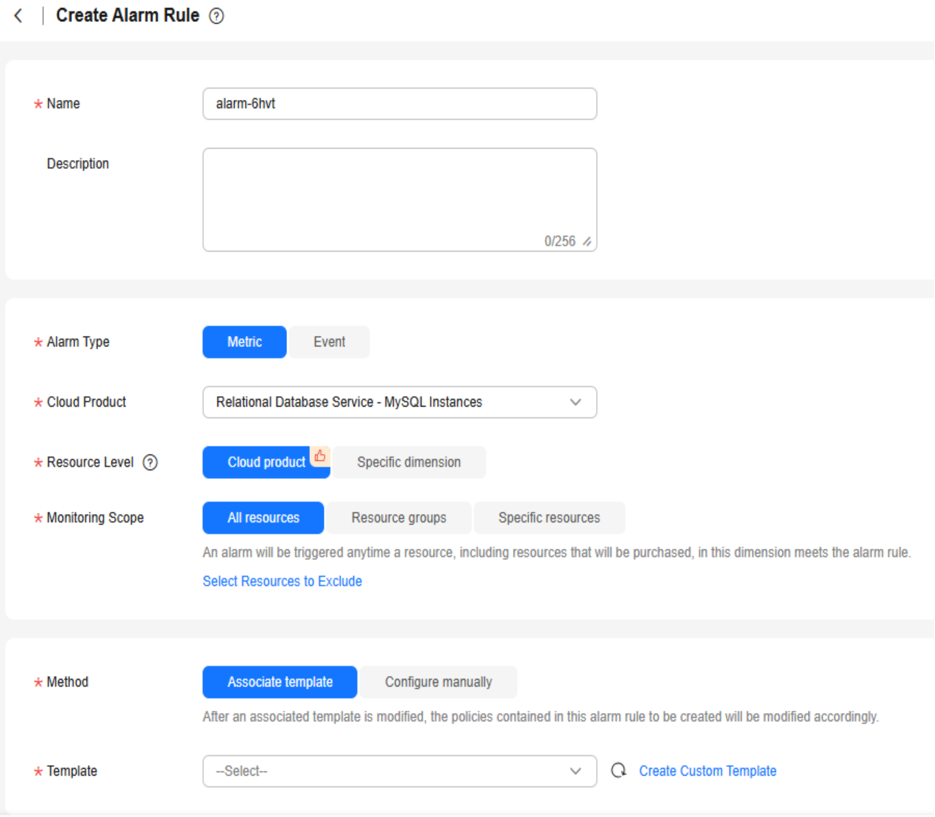
**Step 2** Click 📍 in the upper left corner and select a region or project.

**Step 3** In the navigation pane on the left, choose **Alarm Management** > **Alarm Rule**.

**Step 4** In the upper right corner of the page, click **Create Alarm Rule**.

**Step 5** Enter the alarm rule information, as shown in **Figure 7-1**. For details about alarm rule information, see **Table 7-5**.

**Figure 7-1** Setting DEW monitoring alarm rules



Create Alarm Rule

* Name: alarm-6hvt

Description: 0/256

* Alarm Type: Metric | Event

* Cloud Product: Relational Database Service - MySQL Instances

* Resource Level: Cloud product | Specific dimension

* Monitoring Scope: All resources | Resource groups | Specific resources

An alarm will be triggered anytime a resource, including resources that will be purchased, in this dimension meets the alarm rule.

Select Resources to Exclude

* Method: Associate template | Configure manually

After an associated template is modified, the policies contained in this alarm rule to be created will be modified accordingly.

* Template: --Select--

Create Custom Template

**Table 7-5** Parameters for setting DEW alarm rules

| Parameter | Description | Example Value |
|---|---|---|
| Name | Name of the rule. The system generates a random name and you can modify it. | alarm-blc7 |
| Description | Description of the rule. | - |
| Alarm Type | Type of the alarm rule. The value can be **Metric** or **Event**. | Metric |
| Cloud Product | Select the cloud product you want to monitor. This parameter is available only when you set **Alarm Type** to **Metric**.<br>Select **Key Management Service** or **Credential Management Service** from the drop-down list box. | Key Management Service |

| Parameter | Description | Example Value |
|---|---|---|
| Resource Level | Resource level of the monitored object. The resource level of the alarm rule. This parameter is available only when you set **Alarm Type** to **Metric**. You can select **Cloud product** (recommended) or **Specific dimension**.<br>**NOTE**<br>If you set this parameter to **Cloud product**, metrics across dimensions, such as disk usage and CPU usage, can be configured in the same alarm rule. If you select **Specific dimension**, only metrics of the specified dimension can be configured for the same alarm rule. | KMS key |

| Parameter | Description | Example Value |
|---|---|---|
| Monitoring Scope | Monitoring scope the alarm rule applies to.<br>● **All resources**: An alarm will be triggered if any resource of the current cloud product meets the alarm policy. To exclude resources that do not need to be monitored, click **Select Resources to Exclude**.<br>● **Resource groups**: An alarm will be triggered if any resource in the resource group meets the alarm policy. To exclude resources that do not need to be monitored, click **Select Resources to Exclude**.<br>● **Specific resources**: Click **Select Specific Resources** to select resources.<br>**NOTE**<br>● If **Alarm Type** is set to **Metric**, you can select **All resources**, **Resource groups**, or **Specific resources**.<br>● If **Alarm Type** is set to **Event** and **Event Type** is set to **System event**, you can configure the monitoring scope. | Resource |
| Group | When **Monitoring Scope** is set to **Resource groups**, you need to select a group. If no resource group meets you needs, click **Create Resource Group** to create one.<br>After selecting a resource group from the drop-down list, you can click **View Resources in a Group** to view the details of resources in the group. After an alarm rule is configured, the group cannot be modified. | - |

| Parameter | Description | Example Value |
|---|---|---|
| Instance | When **Monitoring Scope** is set to **Specific resources**, you need to select the monitored objects for the alarm rule.<br>Click **Select Specific Resources** to select desired resources. | - |
| Event Type | Set this parameter if **Alarm Type** is set to **Event**. You can select **System event** or **Custom event**. | System event |
| Event Source | Set this parameter if **Alarm Type** is set to **Event**.<br>● If **Event Type** is set to **System event**, select the cloud service that generates the event from the drop-down list.<br>● If **Event Type** is set to **Custom event**, the event source must be the same as the reported field and written in the *<Service>***.***<Item>* format. | Cloud Secret Management Service |
| Method | Available options include **Associate template**, **Use existing template**, and **Configure manually**.<br>**NOTE**<br>After an associated template is modified, the policies contained in this alarm rule to be created will be modified accordingly. | Associate template |
| Template | Template to be associated. You can import a template. | - |

| Parameter | Description | Example Value |
|---|---|---|
| Alarm Policy | Set this parameter if **Method** is set to **Configure manually**.<br>● When you set **Alarm Type** to **Metric**, whether to trigger an alarm depends on whether the data in consecutive periods reaches the threshold. For example, an alarm is triggered if the average CPU usage is 80% or higher for three consecutive 5-minute periods.<br>● When you set **Alarm Type** is to **Event** and a specific event occurs, an alarm is triggered. For example, an alarm is triggered if a VM is restarted. | - |
| Alarm Notifications | Specifies whether to notify users when alarms are triggered. Notifications can be sent by email, text message, or HTTP/HTTPS message. | Enabled |
| Notification Recipient | Specifies the method of sending alarm notifications. You can select **Notification group** or **Topic subscription**.<br>● Notification Group: Specifies the notification group that needs to send alarm notifications.<br>● Topic: A topic is used to publish messages and subscribe to notifications. If the required topic is unavailable, create one first and add subscriptions to it. | Notification Group |

| Parameter | Description | Example Value |
|---|---|---|
| Notification Policies | Set this parameter if **Alarm Notifications** is set to **Notification policies**. You can specify the notification group, window, template, and other parameters in a notification policy. | - |
| Notification Group | Set this parameter if **Alarm Notifications** is set to **Notification groups**. | - |
| Recipient | Set this parameter if **Alarm Notifications** is set to **Topic subscriptions**. You can select an account contact or a topic to receive alarm notifications.<br>● The account contact is the mobile phone number and email address of the registered account.<br>● The topic is a specific event type for publishing messages or subscribing to notifications. If the required topic is unavailable, create one and add subscriptions to it. | - |
| Notification Template | Set this parameter if **Alarm Notifications** is set to **Notification groups** or **Topic subscriptions**. You can select an existing one or create one. | - |
| Notification Window | Set this parameter if **Alarm Notifications** is set to **Notification groups** or **Topic subscriptions**.<br>Cloud Eye sends notifications only within the notification window you specified. | 00:00-8:00 |
| Time Zone | Time zone for the alarm notification window. By default, it matches the time zone of the client server, but can be manually configured. | - |

| Parameter | Description | Example Value |
|---|---|---|
| Trigger Condition | Condition for triggering the alarm notification. Select **Generated alarm** when an alarm is generated or **Cleared alarm** when an alarm is triggered, or both. | Generated alarm |

**Step 6** Click **Create**. In the displayed dialog box, click **OK**.

**----End**

## 7.1.4 Viewing Metric and Event Monitoring Data

You can view DEW metrics on Cloud Eye to learn about the DEW protection status in a timely manner and set protection policies based on the metrics.

### Prerequisites

DEW has been interconnected with Cloud Eye, that is, alarm rules have been set on Cloud Eye. For details about how to set alarm monitoring rules, see **Setting Alarm Rules**.

### Viewing Metric Monitoring Data

**Step 1** Log in to the **Cloud Eye console**.

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

**Step 3** In the navigation pane on the left, choose **Cloud Service Monitoring**.

**Step 4** Search for **KMS** or **CSMS**, click the dashboard name to view the service monitoring details.

**Step 5** Locate the target key or secret instance and click **View Metric** in the **Operation** column.

**----End**

### Viewing Event Monitoring Data

**Step 1** Log in to the **Cloud Eye console**.

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

**Step 3** In the navigation pane on the left, choose **Event Monitoring**.

**Step 4** On the displayed page, view all system events and custom events over the last 24 hours.

You can view events in the last 1 hour, last 3 hours, last 12 hours, last 1 day, last 7 days, or last 30 days. Alternatively, you can set a custom time range to view events triggered within that period.

**Table 7-6** Event monitoring list

| Parameter | Description |
|---|---|
| Event Type | Event type, which can be either system event or custom event. |
| Event Name | User operation that triggered an event, such as login and logout.<br>For details about the system events supported by DEW, see **7.1.2 Events Supported by DEW**. |
| Event Source | Service the event is generated for. |
| Quantity | Number of times that the event is reported in the selected period. |
| Last Occurred At | Time when the event last occurred. |
| Operation | You can view the monitoring graph and create alarm rules. |

**Step 5** Locate the event type to be viewed and click **View Graph** in the **Operation** column.

**Step 6** Locate a specific event and click **View Event** in the **Operation** column.

**----End**

# 7.2 Using CTS to Audit DEW

## 7.2.1 Operations supported by CTS

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

**Table 7-7** KMS operations supported by CTS

| Operation | Resource Type | Event Name |
|---|---|---|
| Creating a key | CMK | createKey |
| Creating a DEK | CMK | createDataKey |
| Creating a plaintext-free DEK | CMK | createDataKeyWithout-Plaintext |
| Enabling a key | CMK | enableKey |
| Disabling a key | CMK | disableKey |
| Encrypting a DEK | CMK | encryptDatakey |
| Decrypting a DEK | CMK | decryptDatakey |

| Operation | Resource Type | Event Name |
|---|---|---|
| Scheduling the deletion of a key | CMK | scheduleKeyDeletion |
| Canceling the scheduled deletion of a key | CMK | cancelKeyDeletion |
| Generating a random number | RNG | genRandom |
| Modifying the key alias | CMK | updateKeyAlias |
| Modifying the key description | CMK | updateKeyDescription |
| Prompting risks about key deletion | CMK | deleteKeyRiskTips |
| Importing key materials | CMK | importKeyMaterial |
| Deleting key materials | 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 tags in batches | CMK | batchCreateKmsTags |
| Deleting tags in batches | CMK | batchDeleteKmsTags |
| Enabling key rotation | CMK | enableKeyRotation |
| Modifying the key rotation interval | CMK | updateKeyRotationInterval |

**Table 7-8** CSMS operations supported by CTS

| Operation | Resource Type | Event Name |
|---|---|---|
| Creating a secret | Secret | createSecret |
| Updating a secret | Secret | updateSecret |
| Deleting a secret | Secret | forceDeleteSecret |
| Creating a scheduled deletion for a secret | Secret | scheduleDelSecret |

| Operation | Resource Type | Event Name |
|---|---|---|
| Canceling the scheduled deletion of a secret | Secret | restoreSecretFromDeletedStatus |
| Creating a secret status | Secret | createSecretStage |
| Updating a secret status | Secret | updateSecretStage |
| Deleting a secret status | Secret | deleteSecretStage |
| Creating a secret version | Secret | createSecretVersion |
| Downloading a secret backup | Secret | backupSecret |
| Restoring a secret backup | Secret | restoreSecretFromBackupBlob |
| Updating the secret version | Secret | putSecretVersion |
| Secret rotation | Secret | rotateSecret |
| Creating a secret event | Secret | createSecretEvent |
| Updating a secret event | Secret | updateSecretEvent |
| Deleting a secret event | Secret | deleteSecretEvent |
| Creating a resource tag | Secret | createResourceTag |
| Deleting a resource tag | Secret | deleteResourceTag |

**Table 7-9** KPS operations supported by CTS

| Operation | Resource Type | Event Name |
|---|---|---|
| Creating or importing an SSH key pair | Key pair | createOrImportKeypair |
| Deleting an SSH key pair | Key pair | deleteKeypair |
| Importing a private key | Key pair | importPrivateKey |
| Exporting a private key | Key pair | exportPrivateKey |
| Binding an SSH key pair | Key pair | bindKeypair |
| Unbinding an SSH key pair | Key pair | unbindKeypair |
| Clearing a private key | Key pair | clearPrivateKey |

**Table 7-10** Dedicated HSM operations supported by CTS

| Operation | Resource Type | Event Name |
|---|---|---|
| Purchasing an HSM instance | HSM | purchaseHsm |
| Configuring an HSM instance | HSM | createHsm |
| Deleting an HSM instance | HSM | deleteHsm |

## 7.2.2 Viewing CTS Traces in the Trace List

### Scenarios

Cloud Trace Service (CTS) records operations performed on cloud service resources. A record contains information such as the user who performed the operation, IP address, operation content, and returned response message. These records facilitate security auditing, issue tracking, and resource locating. They also help you plan and use resources, and identify high-risk or non-compliant operations.

### What Is a Trace?

A trace is an operation log for a cloud service resource, tracked and stored by CTS. Traces record operations such as adding, modifying, or deleting cloud service resources. You can view them to identify who performed operations and when for detailed tracking.

### What Is a Management Tracker and Data Tracker?

A management tracker identifies and associates with all your cloud services, recording all user operations. It records management traces, which are operations performed by users on cloud service resources, such as their creation, modification, and deletion.

A data tracker records details of user operations on data in OBS buckets. It records data traces reported by OBS, detailing user operations on data in OBS buckets, including uploads and downloads.

### Constraints

- Before the organization function is enabled, you can query the traces of a single account on the CTS console. After the organization function is enabled, you can only view multi-account traces on the **Trace List** page of each account, or in the OBS bucket or the **CTS/system** log stream configured for the management tracker with the organization function enabled.
- You can only query operation records of the last seven days on the CTS console. They are automatically deleted upon expiration and cannot be manually deleted. To store them for longer than seven days, configure

transfer to Object Storage Service (OBS) or Log Tank Service (LTS) so that you can view them in the OBS buckets or LTS log streams.

- After creating, modifying, or deleting a cloud service resource, you can query management traces on the CTS console 1 minute later and query data traces 5 minutes later.
- Data traces are not displayed in the trace list of the new version. To view them, you need to go to the old version.

## Prerequisites

1. **Register with Huawei Cloud and complete real-name authentication.**

   If you already have a Huawei Cloud account, skip this step. If you do not have one, do as follows:

   a. Log in to the **Huawei Cloud official website**, and click **Sign Up**.

   b. Sign up for a HUAWEI ID as prompted. For details, see **Signing Up for a HUAWEI ID and Enabling Huawei Cloud Services**.

      Your personal information page is displayed after the registration completes.

   c. Complete individual or enterprise real-name authentication by referring to **Real-Name Authentication**.

2. **Grant permissions for users.**

   If you log in to the console using a Huawei Cloud account, skip this step.

   If you log in to the console as an IAM user, first contact your CTS administrator (account owner or a user in the **admin** user group) to obtain the **CTS FullAccess** permissions. For details, see **Assigning Permissions to an IAM User**.

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

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

**Step 2** In the navigation pane, choose **Trace List**.

**Step 3** In the time range drop-down list above the trace list, select a desired query time range: **Last 1 hour**, **Last 1 day**, or **Last 1 week**. You can also select **Custom** to specify a custom time range within the last seven days.

**Step 4** The search box above the trace list supports advanced queries. Combine one or more filters to refine your search.

**Table 7-11** Trace filtering parameters

| Parameter | Description |
|---|---|
| Read-Only | After selecting the **Read-Only** filter, you can select either **Yes** or **No** from the drop-down list.<br>● **Yes**: filters read-only operation traces, for example, resource query operations. This option is available after **Read-Only Trace Reporting** has been enabled in the **Configuration Center** and at least one read-only trace has been triggered.<br>● **No**: filters non-read-only operation traces, such as creating, modifying, and deleting resources. |
| Trace Name | Name of a trace.<br>The entered value is case-sensitive and requires an exact match. Fuzzy matching is not supported.<br>For details about the operations that can be audited for each cloud service, see **Supported Services and Operations**.<br>Example: **updateAlarm** |
| Trace Source | Cloud service name abbreviation.<br>The entered value is case-sensitive and requires an exact match. Fuzzy matching is not supported.<br>Example: **IAM** |
| Resource Name | Name of a cloud resource involved in a trace.<br>The entered value is case-sensitive and requires an exact match. Fuzzy matching is not supported.<br>If the cloud resource involved in the trace does not have a resource name or the corresponding API operation does not involve the resource name parameter, leave this field empty.<br>Example: **ecs-name** |
| Resource ID | ID of a cloud resource involved in a trace.<br>The entered value is case-sensitive and requires an exact match. Fuzzy matching is not supported.<br>Leave this field empty if the resource has no resource ID or if resource creation failed.<br>Example: *{VM ID}* |
| Trace ID | Value of the **trace_id** parameter for a trace reported to CTS.<br>The entered value requires an exact match. Fuzzy matching is not supported.<br>Example: **01d18a1b-56ee-11f0-ac81-******1e229** |

| Parameter | Description |
|---|---|
| Resource Type | Type of a resource involved in a trace.<br>The entered value is case-sensitive and requires an exact match. Fuzzy matching is not supported.<br>For details about the resource types of each cloud service, see **Supported Services and Operations**.<br>Example: **user** |
| Operator | User who triggers a trace.<br>Select one or more operators from the drop-down list.<br>If the value of **trace_type** in a trace is **SystemAction**, the operation is triggered by the service and the trace's operator may be empty. |
| Trace Status | Select one of the following options from the drop-down list:<br>● **normal**: The operation succeeded.<br>● **warning**: The operation failed.<br>● **incident**: The operation caused a fault that is more serious than a normal failure, for example, causing other faults. |
| Enterprise Project ID | ID of the enterprise project to which a resource belongs.<br>To check enterprise project IDs, go to the Enterprise Project Management Service (EPS) console and choose **Project Management** in the navigation pane.<br>Example: **b305ea24-c930-4922-b4b9-******1eb2** |
| Access Key | Temporary or permanent access key ID.<br>To check access key IDs, hover over your username in the upper right corner of the console and select **My Credentials** from the pop-up list. On the displayed page, choose **Access Keys** in the navigation pane.<br>Example: **HSTAB47V9V*******TLN9** |

**Step 5** On the **Trace List** page, you can also export and refresh the trace list, and customize columns to display.

- Enter any keyword in the search box and press **Enter** to filter desired traces.
- Click **Export** to export all traces in the query result as an .xlsx file. The file can contain up to 5,000 records.
- Click ⟳ to view the latest information about traces.
- Click ⚙ to customize the information to be displayed in the trace list. If **Auto wrapping** is enabled (●), excess text will move down to the next line; otherwise, the text will be truncated. By default, this function is disabled.

**Step 6** (Optional) On the **Trace List** page of the new edition, click **Old Edition** in the upper right corner to switch to the **Trace List** page of the old edition.

**----End**

## Viewing Traces in the Trace List of the Old Edition

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

**Step 2** In the navigation pane, choose **Trace List**.

**Step 3** Each time you log in to the CTS console, the new edition is displayed by default. Click **Old Edition** in the upper right corner to switch to the trace list of the old edition.

**Step 4** In the upper right corner of the page, set a desired query time range: **Last 1 hour**, **Last 1 day**, or **Last 1 week**. You can also click **Customize** to specify a custom time range within the last seven days.

**Step 5** Set filters to search for your desired traces.

**Table 7-12** Trace filtering parameters

| Parameter | Description |
|---|---|
| Trace Type | Select **Management** or **Data**.<br>● Management traces record operations performed by users on cloud service resources, including creation, modification, and deletion.<br>● Data traces are reported by OBS and record operations performed on data in OBS buckets, including uploads and downloads. |
| Trace Source | Select the name of the cloud service that triggers a trace from the drop-down list. |
| Resource type | Select the type of the resource involved in a trace from the drop-down list.<br>For details about the resource types of each cloud service, see **Supported Services and Operations**. |
| Operator | User who triggers a trace.<br>Select one or more operators from the drop-down list.<br>If the value of **trace_type** in a trace is **SystemAction**, the operation is triggered by the service and the trace's operator may be empty. |
| Trace Status | Select one of the following options:<br>● **Normal**: The operation succeeded.<br>● **Warning**: The operation failed.<br>● **Incident**: The operation caused a fault that is more serious than a normal failure, for example, causing other faults. |

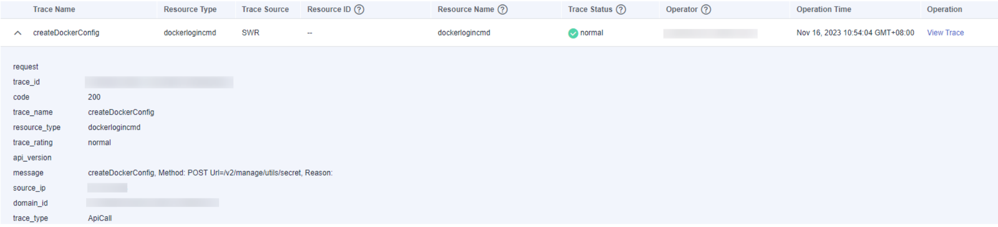
**Step 6** Click **Query**.

**Step 7** On the **Trace List** page, you can also export and refresh the trace list.

- Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5,000 records.

- Click ↻ to view the latest information about traces.

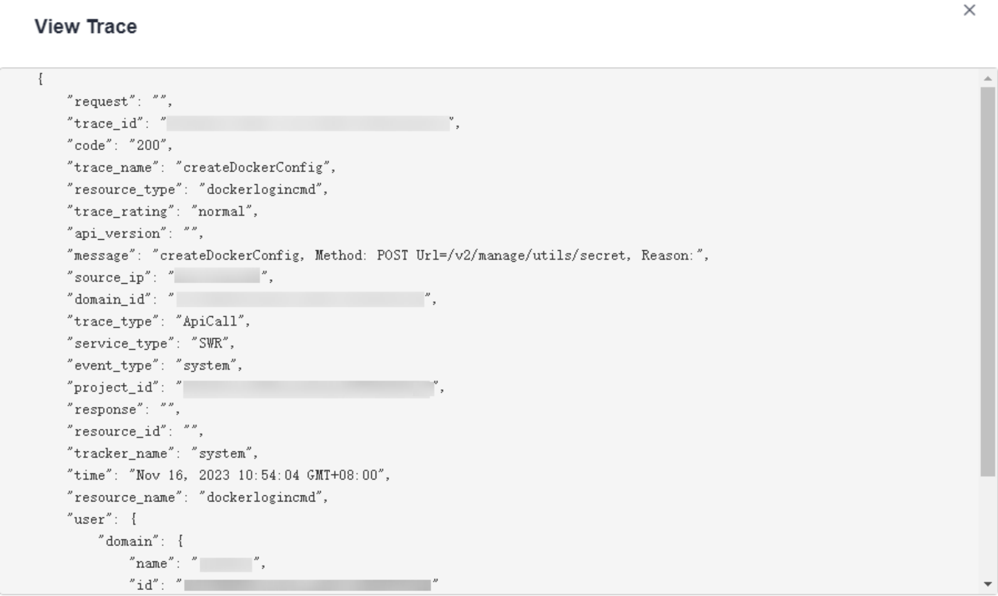
**Step 8** Click ∨ on the left of a trace to expand its details.



| Trace Name | Resource Type | Trace Source | Resource ID ⓘ | Resource Name ⓘ | Trace Status ⓘ | Operator ⓘ | Operation Time | Operation |
|---|---|---|---|---|---|---|---|---|
| ∧ createDockerConfig | dockerlogincmd | SWR | -- | dockerlogincmd | ✓ normal | [redacted] | Nov 16, 2023 10:54:04 GMT+08:00 | View Trace |

| | |
|---|---|
| request | |
| trace_id | [redacted] |
| code | 200 |
| trace_name | createDockerConfig |
| resource_type | dockerlogincmd |
| trace_rating | normal |
| api_version | |
| message | createDockerConfig, Method: POST Url=/v2/manage/utils/secret, Reason: |
| source_ip | [redacted] |
| domain_id | [redacted] |
| trace_type | ApiCall |

**Step 9** Click **View Trace** in the **Operation** column. The trace details are displayed.



View Trace

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

**Step 10** (Optional) On the **Trace List** page of the old edition, click **New Edition** in the upper right corner to switch to the **Trace List** page of the new edition.

**----End**

## Helpful Links

- For details about the key fields in the trace structure, see **Trace Structure** and **Example Traces**.

# 8 Permissions Management

## 8.1 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:

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

- JSON: Edit JSON policies from scratch or based on an existing policy. For details about how to create custom policies, see **Creating a Custom Policy**. This section describes typical DEW custom policies.

### Example Custom Policies of DEW

- Example: authorizing users to create and import keys

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

- Example: denying deletion of key tags

  A deny policy must be used together with other policies. 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"
            ]
        }
```

```
  ]
}
```

# 8.2 Critical Operation Protection

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

## Constraints

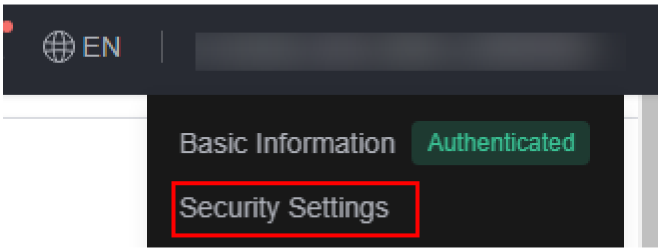
Only operations that are performed on the console are protected by this function.

## Enabling operation protection

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

**Step 2** On the console, locate the user name in the upper right corner, and select **Security Settings** from the drop-down list.

**Figure 8-1** Security settings



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

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

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

NOTE

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

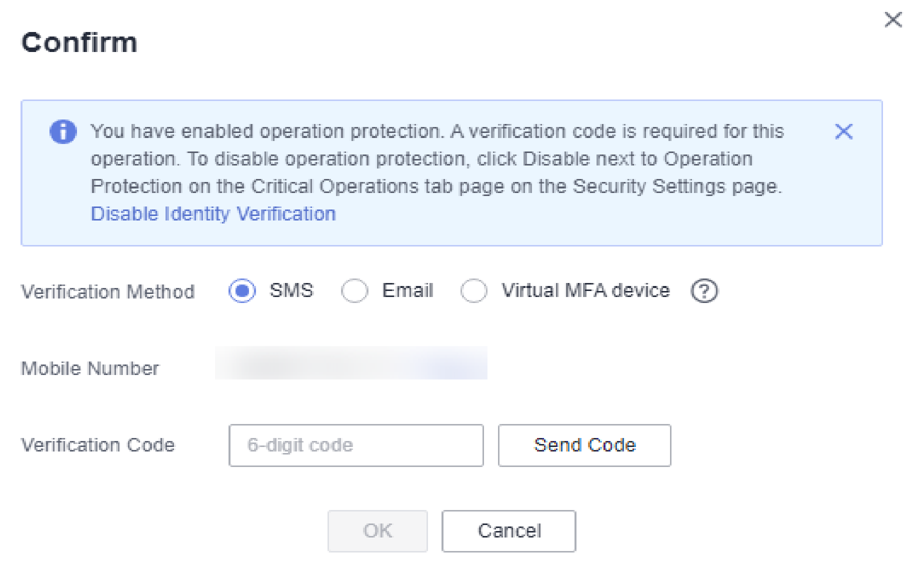
**----End**

## Verifying the Operation Protection

If you have enabled operation protection, there will be a verification when you perform critical operations such as viewing the secret value. Select a verification mode based on your bound information, as shown in **Figure 8-2**.

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

**Figure 8-2** Operation protection verification



Confirm

You have enabled operation protection. A verification code is required for this operation. To disable operation protection, click Disable next to Operation Protection on the Critical Operations tab page on the Security Settings page.
Disable Identity Verification

Verification Method ● SMS ○ Email ○ Virtual MFA device

Mobile Number

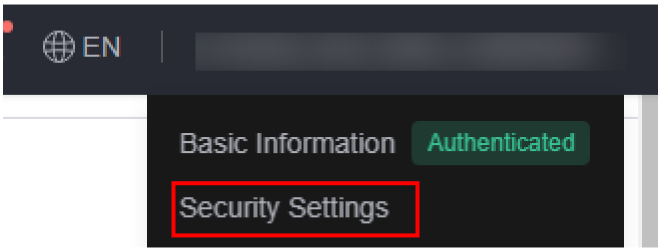
Verification Code 6-digit code

## Disabling Operation Protection

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

**Step 2** On the console, locate the user name in the upper right corner, and select **Security Settings** from the drop-down list.

**Figure 8-3** Security settings



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

**Step 4** On the **Operation Protection** page, choose **Disable**, click **OK**, and pass the verification.

**----End**