My Credentials

Issue	01
Date	2024-04-15

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

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

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

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

1 My Credentials

You can manage your security credentials on the **My Credentials** page.

To access the cloud platform using APIs, obtain security credentials (such as the account name and project ID) on the **API Credentials** page. On the **Access Keys** page, you can manage access keys (AK/SK) used for API access.

Procedure

Step 1 On the management console, hover over the username in the upper right corner and choose **My Credentials** from the drop-down list.

Step 2 On the **My Credentials** console, view your **API credentials** and **access keys**.

Table 1-1 Credential information

Parameter		Description
API Credentials	IAM User Name	Username used by an IAM user to log in to the cloud platform.
	IAM User ID	ID of the IAM user, which is automatically generated by the cloud platform. The IAM user ID cannot be modified.
	Account Name	Automatically created upon successful registration. Resources of different accounts are isolated.
	Account ID	ID of the account, which is automatically generated by the cloud platform. The account ID cannot be modified.
	Project ID	ID of a project, which is automatically generated by the cloud platform. The project ID cannot be modified.
	Projects	Group and isolate resources (including compute, storage, and network resources) across physical regions. A project can be a department or a project group. All your resources are managed by project.

Parameter	Description
Access Keys	Access key ID/Secret access key (AK/SK) pairs used for API access. You can create a maximum of two access keys.

----End

2 API Credentials

You can view your username, user ID, account name, account ID, and project IDs on the **API Credentials** page. A project ID uniquely identifies a region where cloud resources are deployed. It is required when you call APIs to manage cloud resources, such as creating a Virtual Private Cloud (VPC).

Procedure

Step 1 On the management console, hover over the username in the upper right corner and choose **My Credentials** from the drop-down list.

Step 2 Choose **API Credentials** from the navigation pane, and then view your IAM username, IAM user ID, account name, account ID, and project IDs.

----End

3 Access Keys

An access key comprises an access key ID (AK) and secret access key (SK). AK is used together with SK to sign requests cryptographically, ensuring that the requests are secret, complete, and correct.

After logging in to the management console, users authorized by the administrator can create and delete access keys on the **My Credentials** page.

If an IAM user does not have permissions to log in to the management console, the administrator of the user can manage access keys for the user in IAM.

NOTE

The credentials that an IAM user can use depend on the access type specified for the user. Select the access type that user will need to use.

- If the user **accesses cloud services only by using the management console**, specify the access type as **Management console access** and the credential type as **Password**.
- If the user **accesses cloud services only through programmatic calls**, specify the access type as **Programmatic access** and the credential type as **Access key**.
- If the user **needs to use a password as the credential for programmatic access** to certain APIs, specify the access type as **Programmatic access**.
- If the user needs to **perform access key verification** when using certain services in the console, specify the access type as "**Programmatic access** + **Management console access**" and the credential type as "**Access Key** + **Password**". For example, the user needs to perform access key verification when creating a data migration job in the Cloud Data Migration (CDM) console.

Important Notes

1. You can create a maximum of two access keys with identical permissions and unlimited validity. **Each access key can be downloaded only once when created.** Keep your access keys secure and change them periodically for security purposes. To change an access key, delete it and create a new one.
2. Federated users can only create temporary access credentials (temporary AK/SKs and security tokens). .
3. If you are an administrator, you can view the AK of an IAM user on the user details page. The SK is kept by the user.

Creating an Access Key

Step 1 On the management console, hover over the username in the upper right corner and choose **My Credentials** from the drop-down list.

Step 2 Choose **Access Keys** from the navigation pane.

Step 3 Click **Create Access Key**.

NOTE

- You can create a maximum of **two** access keys. **The quota cannot be increased**. If you already have two access keys, you can only delete an access key and create a new one.
- To change an access key, **delete it** and create a new one.

Step 4 Download the access key file.

After the access key is created, view the AK in the access key list and view the SK in the downloaded CSV file.

NOTE

- Download the access key file and keep it properly. If the download page is closed, you will not be able to download the access key. However, you can create a new one.
- Open the CSV file in the lower left corner, or choose **Downloads** in the browser and open the CSV file.
- Keep your access keys secure and change them periodically for security purposes. To change an access key, delete it and create a new one.

----End

Deleting an Access Key

If your access keys are forgotten or leaked, delete them on the **My Credentials** page or contact the administrator to delete them in IAM.

NOTE

Deleted access keys cannot be restored. Make sure that the deleted access keys have not been used for more than one week.

Step 1 On the **Access Keys** page, locate the access key to be deleted and click **Delete** in the **Operation** column.

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

----End

Enabling/Disabling an Access Key

Access keys are enabled by default once being created. To disable an access key, perform the following steps:

Step 1 On the **Access Keys** page, locate the access key to be disabled and click **Disable** in the **Operation** column.

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

----End

The method of enabling an access key is similar to that of disabling an access key.

Viewing Access Keys

You can view the access key ID, status, and creation time in the **Access Keys** area.