My Credentials

Issue 08

Date 2021-10-30

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Notice

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

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

Security Declaration

Vulnerability

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

Contents

1 My Credentials

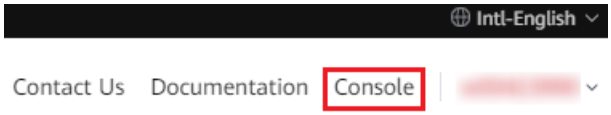
You can manage your security credentials on the **My Credentials** page.

To access Huawei Cloud 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

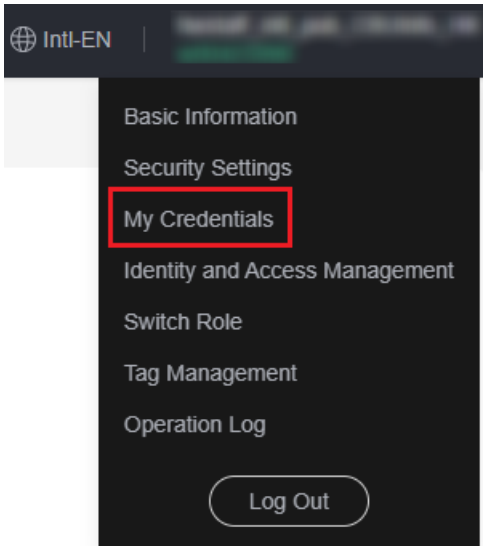
Step 1 Log in to Huawei Cloud and click **Console** in the upper right corner.

Figure 1-1 Accessing the console



Step 2 On the management console, hover over the username in the upper right corner and choose **My Credentials** from the drop-down list.

Figure 1-2 Choosing My Credentials



Step 3 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 Huawei Cloud.
	IAM User ID	ID of the IAM user, which is automatically generated by Huawei Cloud. The IAM user ID cannot be modified.
	Account Name	Automatically created upon successful registration of an entity (such as an enterprise). The account pays bills for the use of cloud resources under the account. Resources of different accounts are isolated.
	Account ID	ID of the account, which is automatically generated by Huawei Cloud. The account ID cannot be modified.
	Project ID	ID of a project, which is automatically generated by Huawei Cloud. 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.
Access Keys		Access key ID/Secret access key (AK/SK) pairs used for API access. You can create a maximum of two access keys.

NOTE

If you have logged in as a federated user, you are a virtual IAM user.

- You do not have an IAM user name or user ID.
- You only have a temporary access key. For details, see **Temporary Access Key (for Federated Users)**.

----End

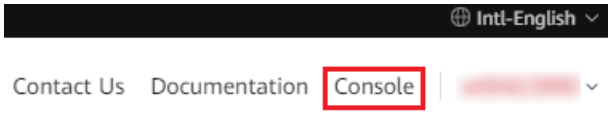
2 API Credentials

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

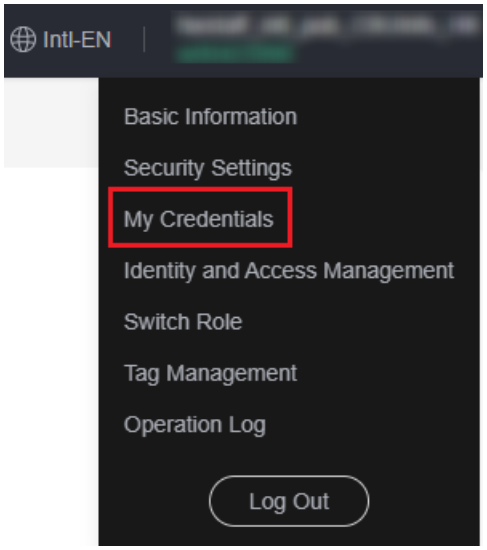
Step 1 Log in to Huawei Cloud and click **Console** in the upper right corner.

Figure 2-1 Accessing the console



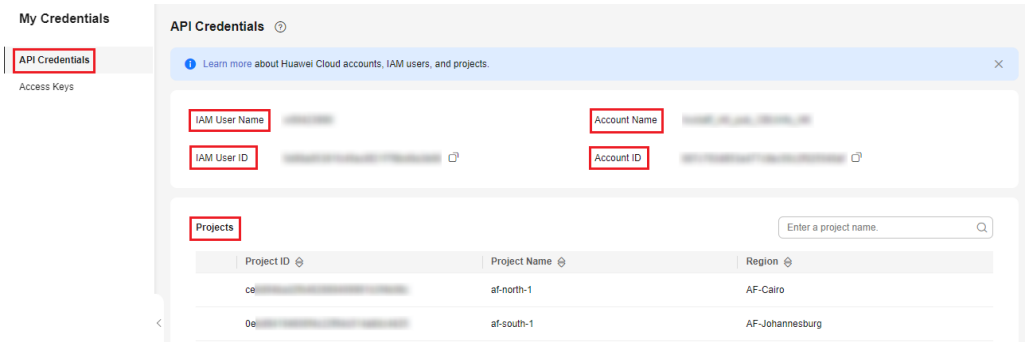
Step 2 On the management console, hover over the username in the upper right corner and choose **My Credentials** from the drop-down list.

Figure 2-2 Choosing My Credentials



Step 3 Choose **API Credentials** from the navigation pane, and then view your IAM username, IAM user ID, account name, account ID, and project IDs.

Figure 2-3 Viewing API credentials



NOTE

- If the region and project you want to view are not displayed, click **Console** in the upper left corner, switch to the desired region, and go to the **API Credentials** page again.
- If you have logged in as a federated user, you are a virtual IAM user and you do not have an IAM user name or user ID.

----End

3 Access Keys

An access key comprises an access key ID (AK) and secret access key (SK), and is used as a long-term identity credential to **sign your requests for Huawei Cloud APIs**. 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. For details, see **Managing Access Keys for an IAM User**.

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** and the credential type as **Password**.
- 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

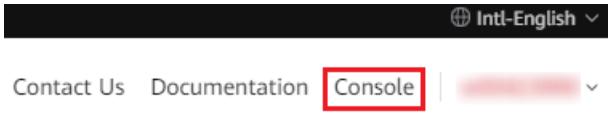
1. You can create a maximum of two access keys with identical permissions and unlimited validity. **Each access key can be downloaded only once when created.** Keep your access keys secure and change them periodically for security purposes. To change an access key, delete it and create a new one.
2. Federated users can only create temporary access credentials (temporary AK/SKs and security tokens). For details, see **Temporary Access Key (for Federated Users)**.

3. If you are an IAM user, move the pointer to the username in the upper right corner of the management console, choose **Security Settings**, click the **Critical Operations** tab, and check the enabling status of the **Access Key Management** feature.
   - Disabled: All IAM users under the account can manage (create, enable, disable, and delete) their own access keys.
   - Enabled: Only the administrator can manage users' access keys.
4. If you cannot manage your access keys, request the **administrator** to perform either of the following operations:
   - Manage your access keys (see **Managing Access Keys for an IAM User**).
   - Grant the permissions you require (see **Assigning Permissions to an IAM User**) or enable access key management (see **Access Key Management**).
5. 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

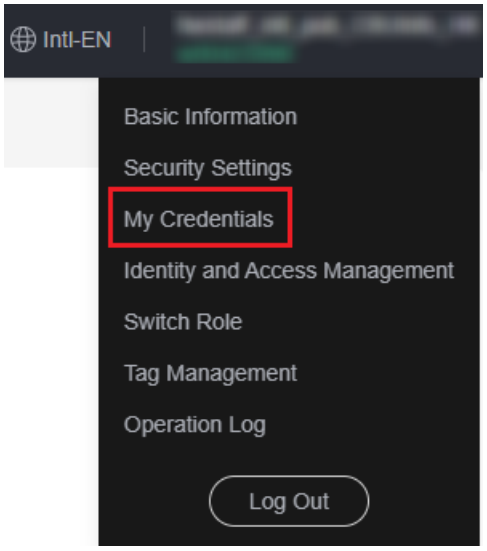
Step 1 Log in to Huawei Cloud and click **Console** in the upper right corner.

Figure 3-1 Accessing the console



Step 2 On the management console, hover over the username in the upper right corner and choose **My Credentials** from the drop-down list.

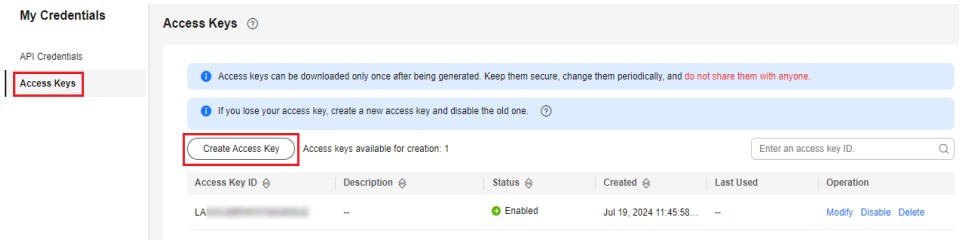
Figure 3-2 Choosing My Credentials



Step 3 Choose **Access Keys** from the navigation pane.

Step 4 Click **Create Access Key**.

Figure 3-3 Creating an 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.
- For newly created access keys, the last used time is the same as the creation time, but will change the next time you use them.

Step 5 Download the access key file.

After the access key is created, view the access key ID (AK) in the access key list in the access key list and view the secret access key (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

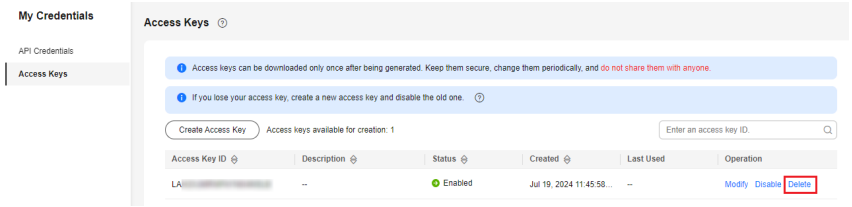
If your access keys are forgotten or leaked, delete them on the **My Credentials** page or contact the administrator to delete them in IAM.

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.

Figure 3-4 Deleting an access key



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.

4 Temporary Access Key (for Federated Users)

A temporary access key is an identity credential that **has temporary access permissions**. It consists of an access key ID (AK) and a 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 their own **temporary access key** on the **My Credentials** page. Only federated users can create a temporary access key on the **My Credentials** page. For accounts and IAM users, see **Access Keys**.

If a user cannot log in to the console or does not have permissions to visit the **My Credentials** page, the administrator can manage **permanent access keys** for the user in IAM.

If you are a federated user, you are advised to use a temporary access key.

Differences Between Temporary and Permanent Access Keys

Temporary and permanent access keys work almost in the same way and only have slight differences.

Table 4-1 Differences between temporary and permanent access keys

Item	Temporary Access Keys	Permanent Access Keys
Validity period	15 minutes to 24 hours	Unlimited validity
Quantity	Unlimited and can be generated repeatedly	2 access keys for each IAM user

Item	Temporary Access Keys	Permanent Access Keys
Creation method	Generated dynamically, cannot be embedded into applications or stored for later use, and must be generated again after expiration. For details, see **Creating a Temporary Access Key**.	--
Credential management	Cannot be deleted, enabled, or disabled and will be automatically invalidated and cleared when they expire.	Can be deleted, enabled, and disabled by the administrator on the IAM console.

Precautions

1. To ensure account security, keep the temporary access key secure and set a proper validity period for it.
2. 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 a Temporary 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 **Permanent Access Key** from the navigation pane.

Step 3 In the upper right corner of the page, set a validity period **from 15 minutes to 24 hours.**

Step 4 Click **Generate** in the **Operation** column.

After the access key is created, view the AK, SK, and STS token in the access key list.

NOTE

When you refresh the **Temporary Access Key** page, the AK, SK, and STS token content are cleared, but they will stay valid before they expire. Keep the access key properly.

----End

