My Credentials

Issue 01

Date 2025-11-06

HUAWEI

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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 My Credentials (New)

1.1 My Credentials

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

When you access Huawei Cloud using APIs, you need to use your security credentials, such as the account name, account ID, and IAM user ID. You can view them on the new console. You can also manage your login credentials, access keys (AKs/SKs), and multi-factor authentication (MFA) devices on this page.

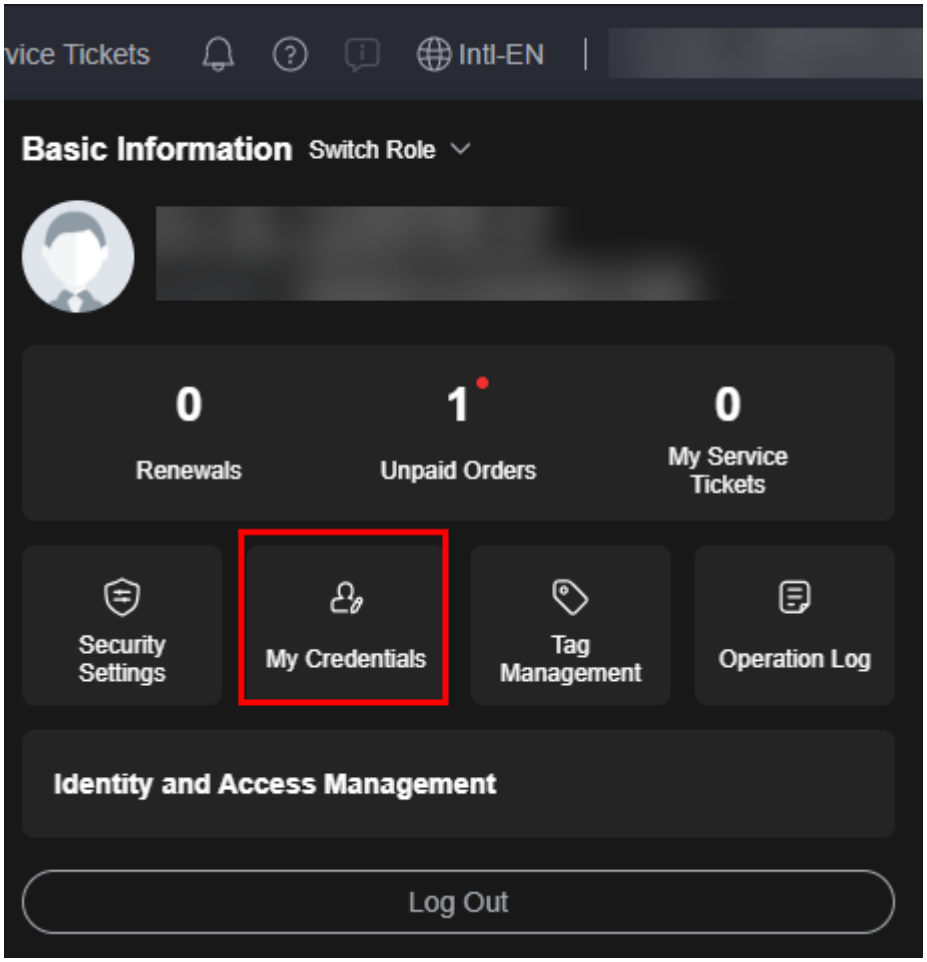
Constraints

If an IAM user needs to view and modify My Credentials, the user must be granted required permissions. For details about the actions, see **IAM Actions Supported by Identity Policy-based Authorization**.

Viewing My Credentials

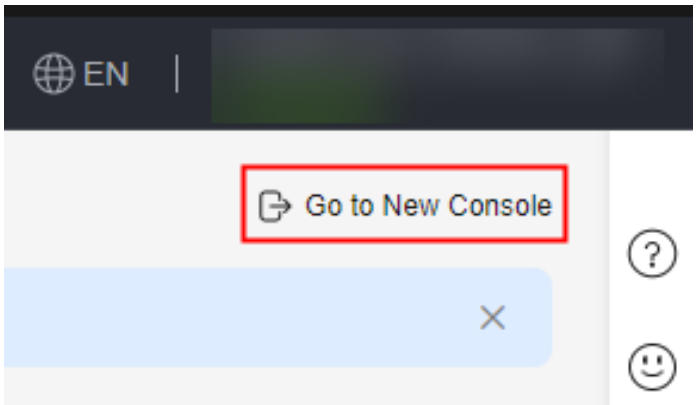
Step 1 Log in to the **Huawei Cloud console**, hover over the username in the upper right corner, and choose **My Credentials** from the drop-down list.

Figure 1-1 Choosing My Credentials



Step 2 Click **Go to New Console**.

Figure 1-2 Accessing My Credentials on the new console



Step 3 On the **My Credentials** page, view **login credentials**, **access keys**, and **MFA**.

Table 1-1 Credential information

Parameter		Description
Identity Credentials	IAM Username	The username used by an IAM user to log in to Huawei Cloud.
	IAM User ID	The ID of the IAM user, which is automatically generated by Huawei Cloud. The IAM user ID cannot be modified.
	Account Name	The name of an account, which is automatically created upon successful registration of an entity (such as an enterprise). The account pays bills for the use of cloud resources in the account. Resources of different accounts are isolated.
	Account ID	The ID of an account, which is automatically generated by Huawei Cloud. The account ID cannot be modified.
Login Credentials		The password used for logging in to the console. You can reset the login password and view the expiration date and the last time it was changed.
Access Keys		A pair of an access key ID (AK) and secret access key (SK) of users. You can create a maximum of two pairs. AKs/SKs are used to sign API requests.
Multi-Factor Authentication (MFA)		MFA requires users to enter a verification code, insert a hardware device, or provide a fingerprint, PIN, or facial information in addition to the username and password for logging in to the console. MFA provides higher security for your account and resources.

----End

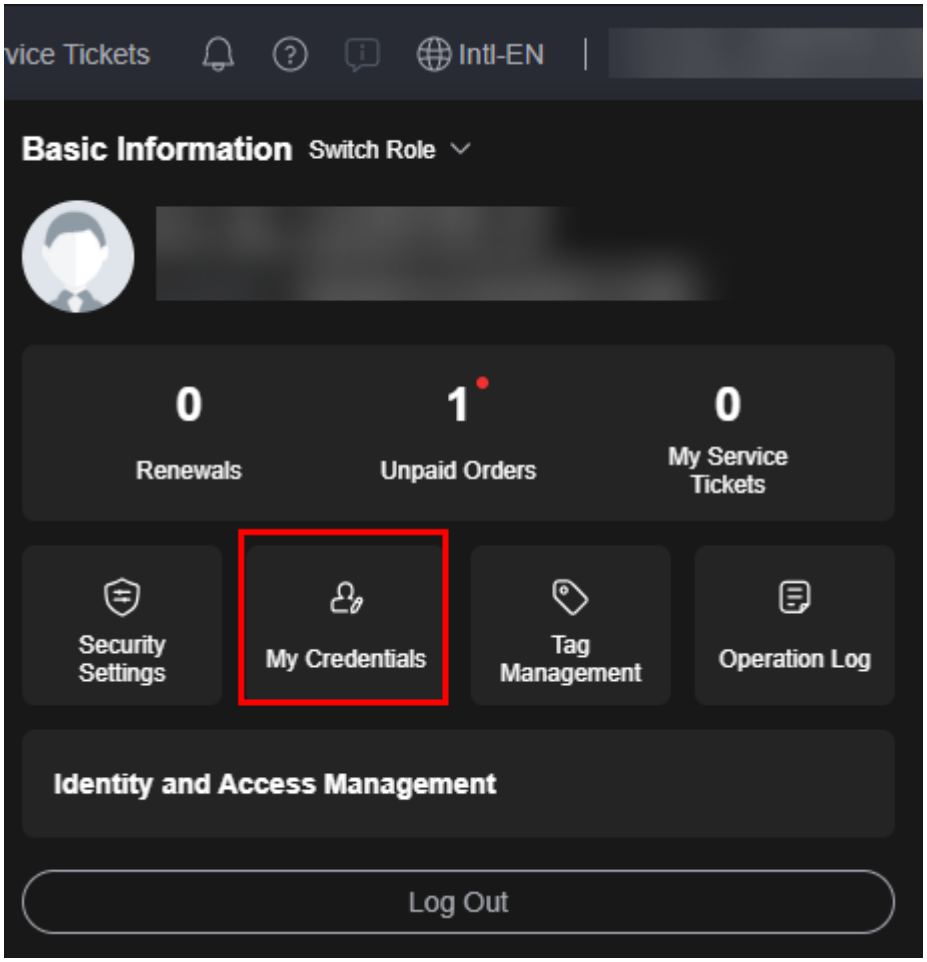
1.2 Login Credentials

A login credential refers to the password you use to log in to the console. An IAM user with required permissions can change the password and view the password expiration time and the last time it was changed on the **My Credentials** page.

Changing the Login Password

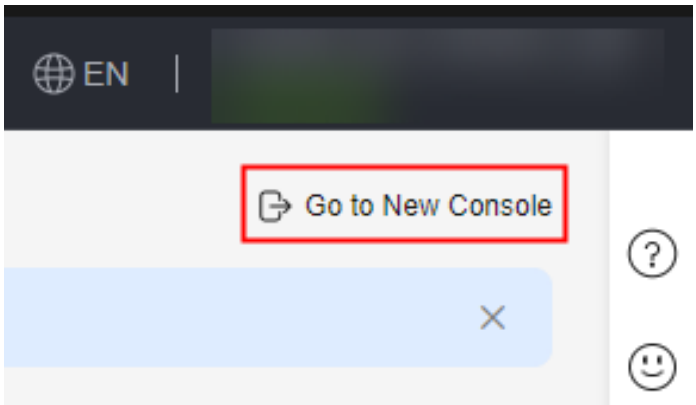
Step 1 Log in to the **Huawei Cloud console**, hover over the username in the upper right corner, and choose **My Credentials** from the drop-down list.

Figure 1-3 Choosing My Credentials



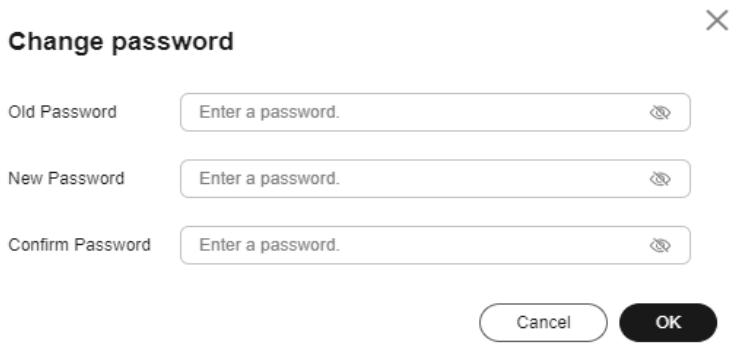
Step 2 Click **Go to New Console**.

Figure 1-4 Accessing My Credentials on the new console



Step 3 Click next to **Configured**. In the displayed dialog box, enter the old password and new password and confirm the new password. Click **OK**.

Figure 1-5 Changing the login password



----End

1.3 Access Keys

An access key comprises an AK and SK and is used as a long-term identity credential to **sign your Huawei Cloud API requests**. 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 can manage access keys for the user in IAM. For details, see **Managing Access Keys for an IAM User**.

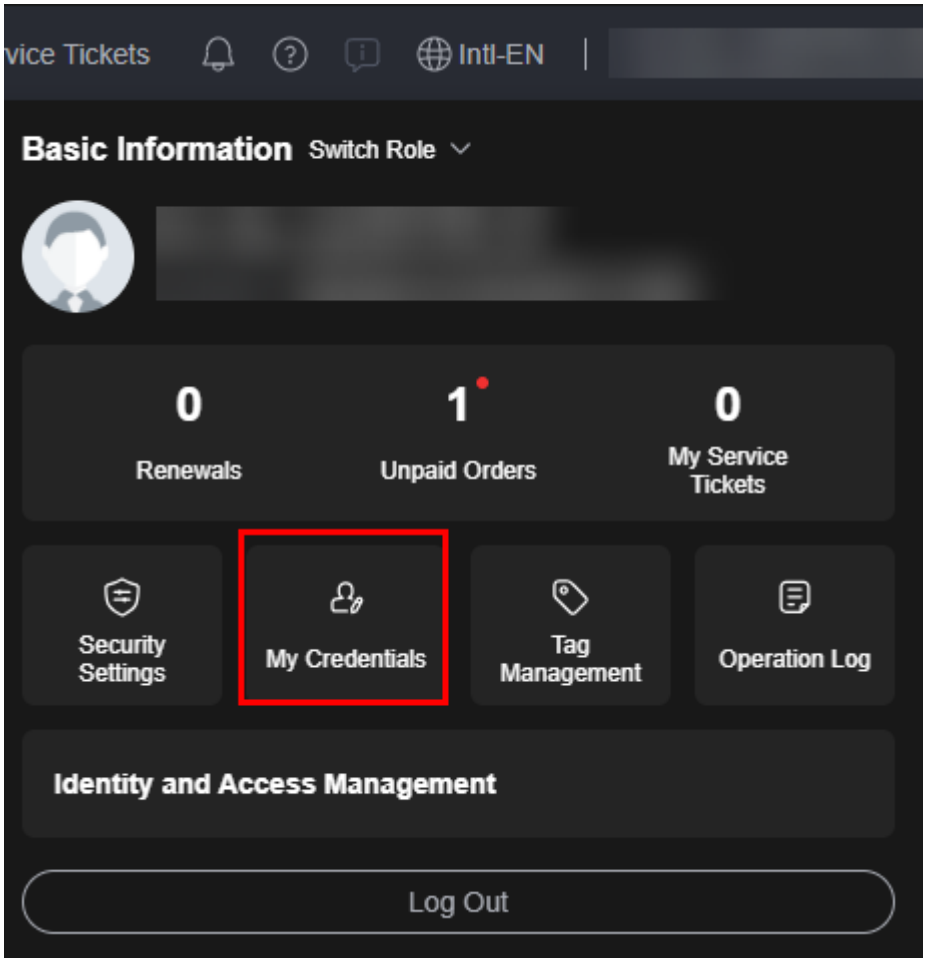
Important Notes

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. If you cannot manage your access keys, request the **administrator** to perform either of the following operations:
   - Manage your access keys. For details, see **Managing Access Keys for an IAM User**.
   - Assign the required permissions to you. For details about how to assign permissions, see **Assigning Permissions to an IAM User**.
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 Access Keys

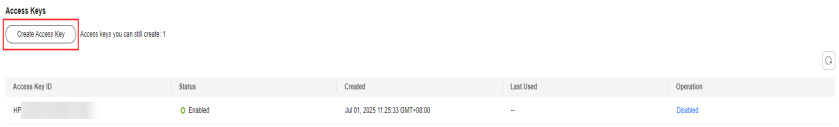
Step 1 Log in to the **Huawei Cloud console**, hover over the username in the upper right corner, and choose **My Credentials** from the drop-down list.

Figure 1-6 Choosing My Credentials



Step 2 In the **Access Keys** area, click **Create Access Key**.

Figure 1-7 Creating access keys



NOTE

- You cannot change the created access keys. To change the access keys, delete them and create a new pair.
- It is not recommended to create access keys for the root user. If you have to do so, be aware of the security risks.

Step 3 Click **Download Access Key** to generate and download the access keys.

After the access keys are created, view the access key ID (AK) 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 SK. However, you can create a new access key pair.
- You can open the access key file in the "Downloads" of the browser.
- For account security, keep your access keys secure and rotate them regularly by deleting old access keys and generating new ones. When deleting access keys, check if the access keys have not been used for a period of time so that the deletion does not affect your services.

----End

Deleting Access Keys

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

CAUTION

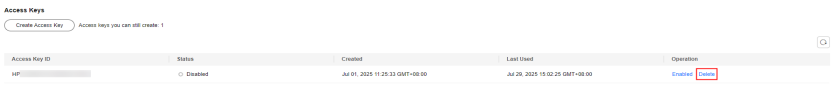
Deleted access keys cannot be restored. Make sure that they have not been used for more than one week.

Step 1 In the **Access Keys** area, locate the access keys you want to delete and click **Disable** in the **Operation** column.

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

Step 3 Click **Delete** in the **Operation** column of the disabled access keys. Ensure that the deletion will not affect your services.

Figure 1-8 Deleting access keys



Step 4 Enter **DELETE** and click **OK**.

----End

Enabling/Disabling Access Keys

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

Step 1 In the **Access Keys** area, locate the access keys you want to disable and click **Disable** in the **Operation** column.

Step 2 Click **OK**.

----End

The method of enabling access keys is similar to that of disabling access keys.

Viewing Access Keys

You can view the access key ID, status, creation time, and last used time on the access keys area.

1.4 MFA Devices

Multi-Factor Authentication

Multi-factor authentication (MFA) provides an additional layer of protection on top of the username and password. If you add an MFA device, users need to enter a verification code, insert a hardware device, or pass the identity verification with fingerprint, PIN, or facial information, in addition to the username and password when they are logging in to the management console.

MFA Device Types

IAM supports the following MFA types:

- Virtual MFA: A virtual MFA device generates verification codes based on the Time-based One-time Password Algorithm (TOTP). IAM supports only software-based virtual MFA devices. The applications that implement TOTP are virtual MFA devices, which can run on mobile devices (such as mobile phones). After a virtual MFA device is added, users need to enter verification codes generated from virtual MFA devices in addition to their credentials during login.
- Security key: A more secure authentication method that can replace passwords. Huawei Cloud supports security keys based on the FIDO2 authentication protocol. Once security keys are enabled, you can utilize fingerprints, facial recognition, or PIN from devices like computers and smartphones, along with FIDO2-compliant security key devices, to perform multi-factor authentication. For instance, once a security key (like Yubikey) supporting the FIDO2 protocol is activated, you must plug it into the computer and tap it for authentication. When using a Windows Hello security key, you will need to verify your identity with fingerprints, PIN, or facial recognition.

Application Scenarios

MFA authentication is mainly used for login protection. You can bind both virtual MFA devices and security keys to an account or IAM user. You can select either of them for authentication. You can add only one virtual MFA device and a maximum of eight security keys to each root user or IAM user.

Login protection: When you or an IAM user under your account logs in to the console, you or that user needs to perform MFA authentication in addition to entering the username and password. This can improve the account security.

Notes and Constraints

- An IAM user can have only one virtual MFA device added.
- An IAM user can have a maximum of eight security keys added.

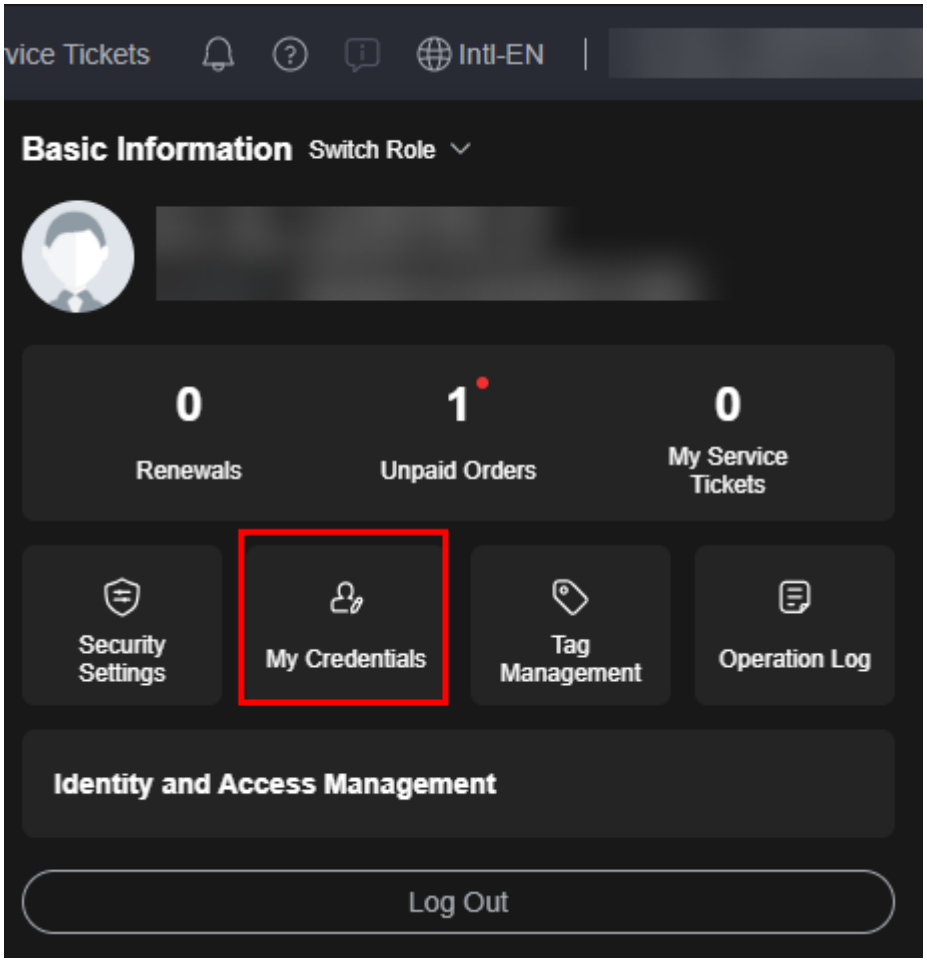
Adding a Virtual MFA Device

Before adding a virtual MFA device, you need to install an authenticator app (such as Google Authenticator and Microsoft Authenticator) on your mobile device.

After you add an MFA device for your Huawei Cloud account or IAM users, login protection is automatically enabled and the verification method is set to MFA verification. IAM users can add virtual MFA devices on the **My Credentials** page of the new console.

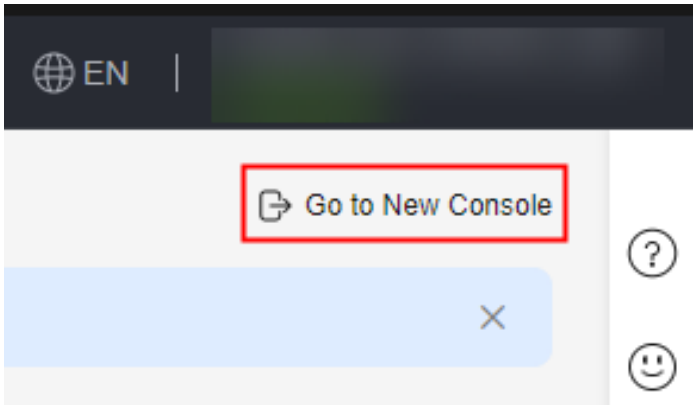
Step 1 Log in to the **Huawei Cloud console**, hover over the username in the upper right corner, and choose **My Credentials** from the drop-down list.

Figure 1-9 Choosing My Credentials



Step 2 Click **Go to New Console**.

Figure 1-10 Accessing My Credentials on the new console



Step 3 In the **Multi-Factor Authentication (MFA)** area, click **Add MFA Device**.

Step 4 Enter the device name. Only letters, digits, hyphens (-), and underscores (_) are allowed.

Step 5 Select an MFA device. Select **Virtual MFA** for **Device Type** and click **Next**.

Step 6 Add a virtual MFA device to your MFA application by scanning the QR code or entering the secret key.

- Scanning the QR code

  Open the MFA application on your mobile phone, and use the application to scan the QR code displayed on the **Add MFA Device** page. Then, the MFA application automatically adds the virtual MFA device.

- Entering the secret key

  Open the MFA application on your mobile phone, and enter the secret key.

  NOTE

  An MFA device can be manually added only using time-based one-time passwords (TOTP). You are advised to enable automatic time setting on your mobile device.

Step 7 View the dynamic codeson the home page of the MFA application. The codes are updated every 30 seconds.

Step 8 On the **Add MFA Device** page, enter two consecutive dynamic codes obtained from the virtual MFA device and click **OK**.

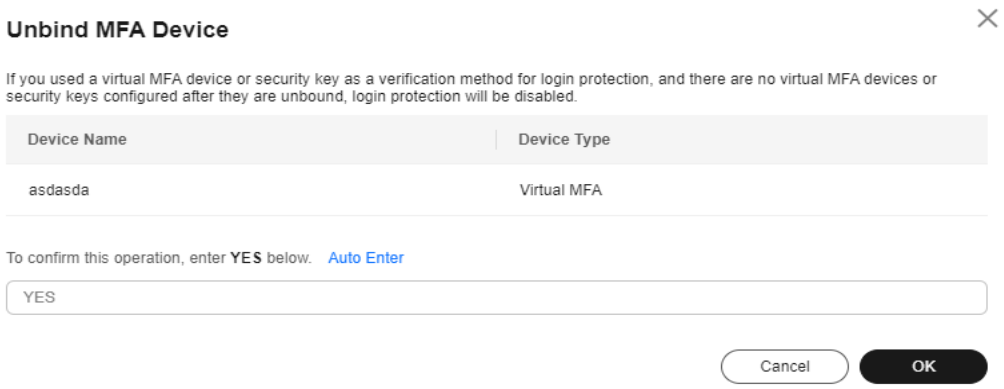
----End

Removing a Virtual MFA Device

Step 1 In the **Multi-Factor Authentication (MFA)** area, locate the MFA device and click **Unbind** in the **Operation** column.

Step 2 In the displayed dialog box, enter **YES**.

Figure 1-11 Confirming unbinding



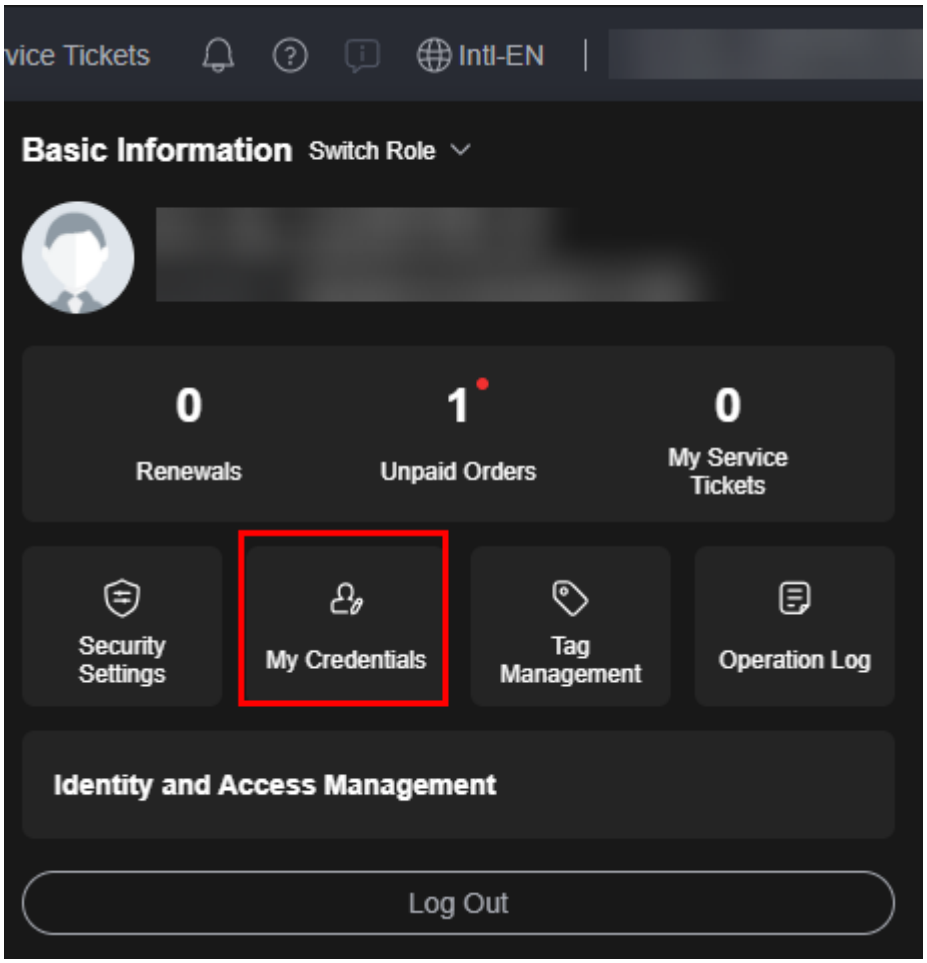
Step 3 Click **OK**.

----End

Binding a Security Key

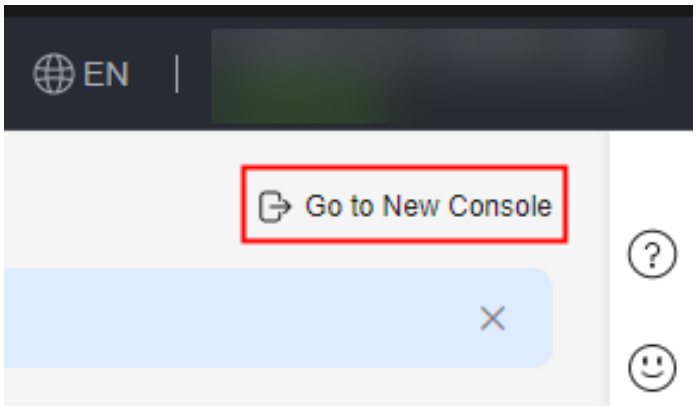
Step 1 Log in to the **Huawei Cloud console**, hover over the username in the upper right corner, and choose **My Credentials** from the drop-down list.

Figure 1-12 Choosing My Credentials



Step 2 Click **Go to New Console**.

Figure 1-13 Accessing My Credentials on the new console



Step 3 In the **Multi-Factor Authentication (MFA)** area, click **Add MFA Device**.

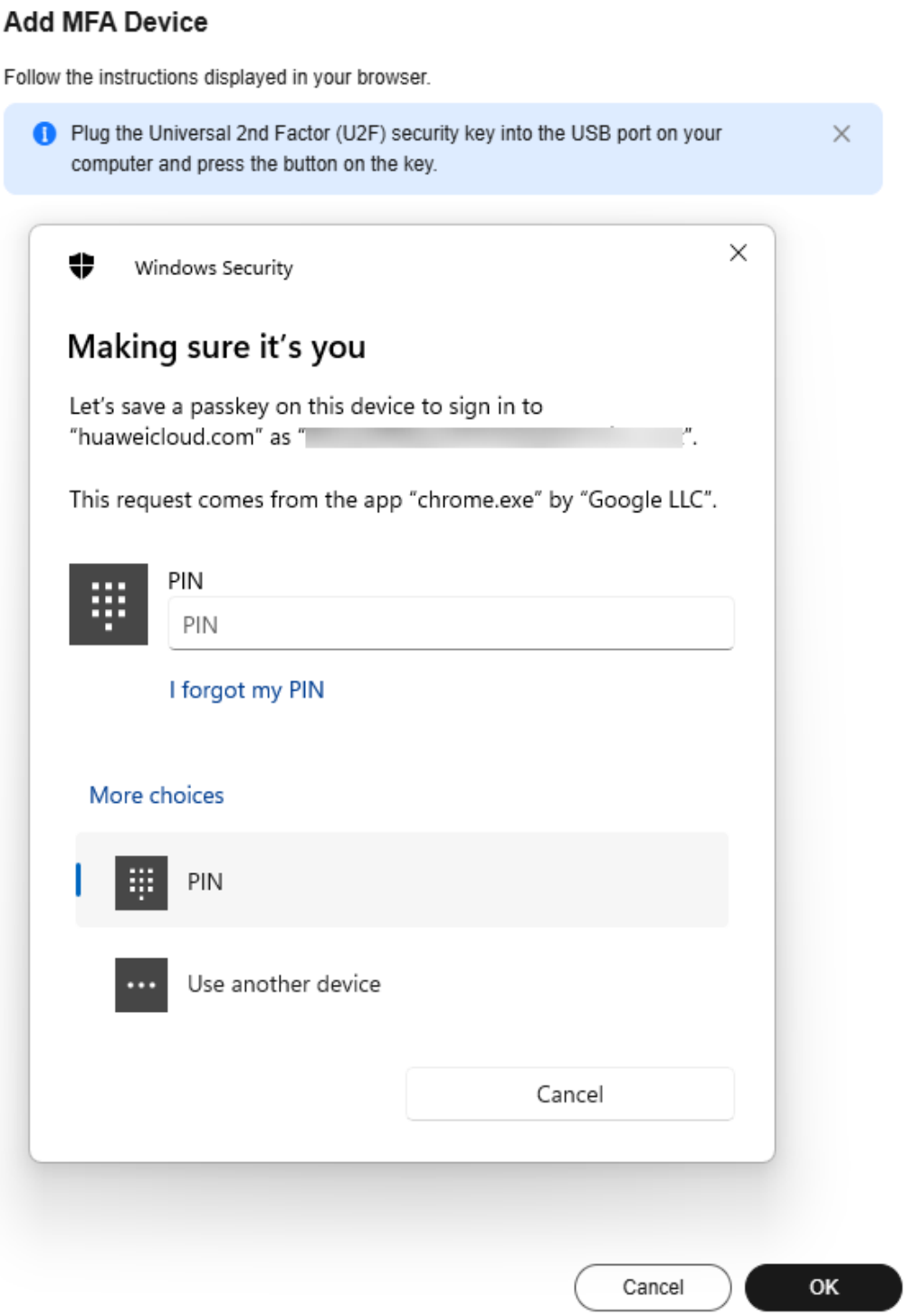
Step 4 On the displayed page, enter a device name. Only letters, digits, hyphens (-), and underscores (_) are allowed.

Step 5 Select an MFA device. Select **Security key** for **Device Type**.

Step 6 Click **Next**.

Step 7 Select an authentication method for Windows Hello, such as PIN, face, or fingerprint.

Figure 1-14 Setting up Windows Hello



NOTE

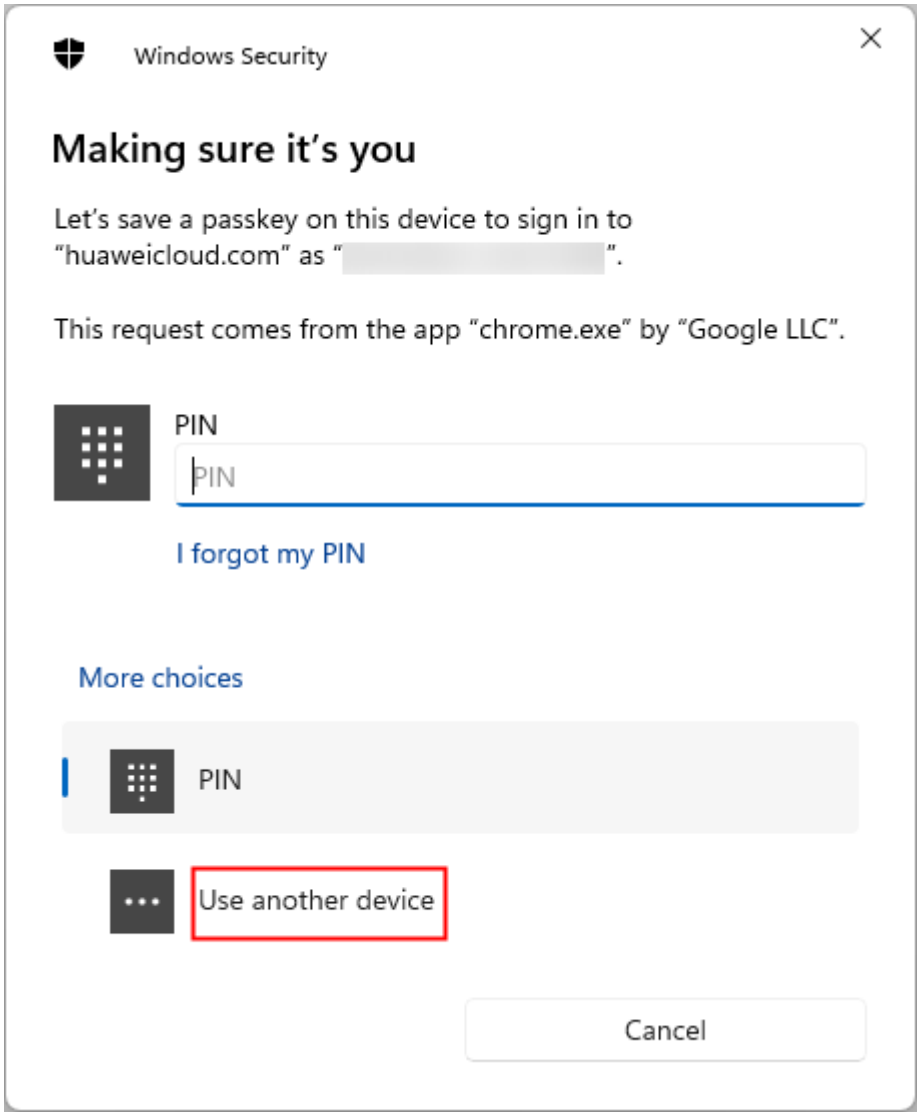
If your Windows device does not support enabling facial recognition and fingerprint, options such as **Face** and **Fingerprint** will not appear. FIDO2 will show you the options according to the authentication types supported by your device.

Step 8 Enter the PIN (or recognize the face or fingerprint). After the system authentication is successful, a dialog box is displayed, indicating that the binding is successful. Click **OK**. The security key will be displayed in the MFA device list.

Figure 1-15 MFA device added

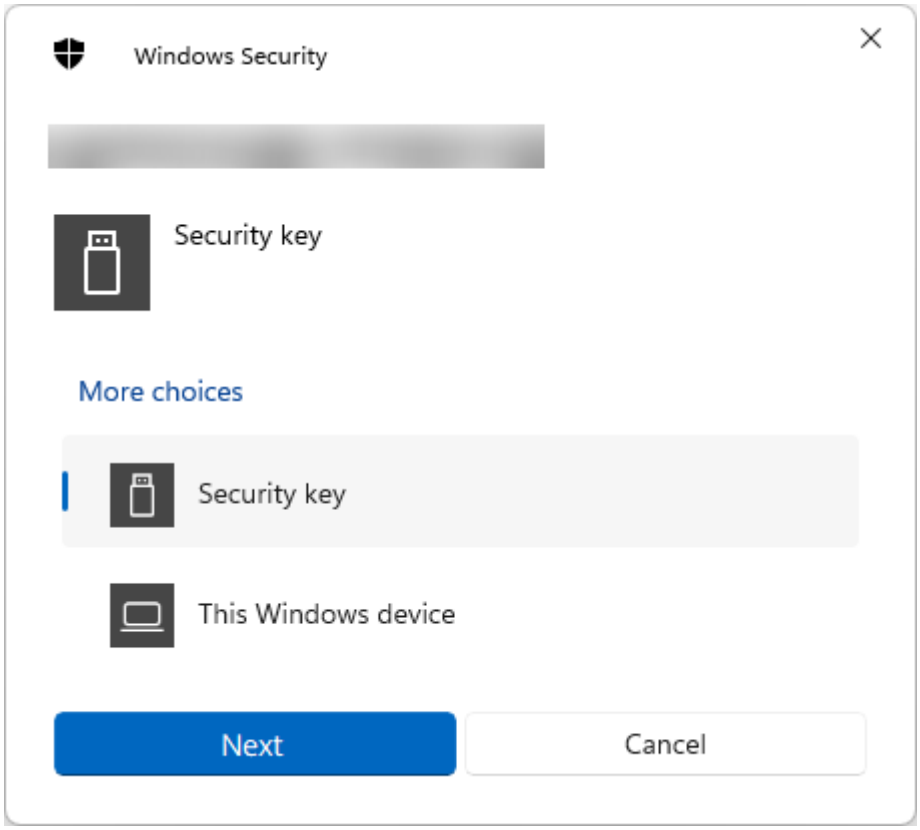
Step 9 To set up a FIDO2 security key, select **Use another device** in the dialog box and plug the security key into the USB port of your computer.

Figure 1-16 Using another device



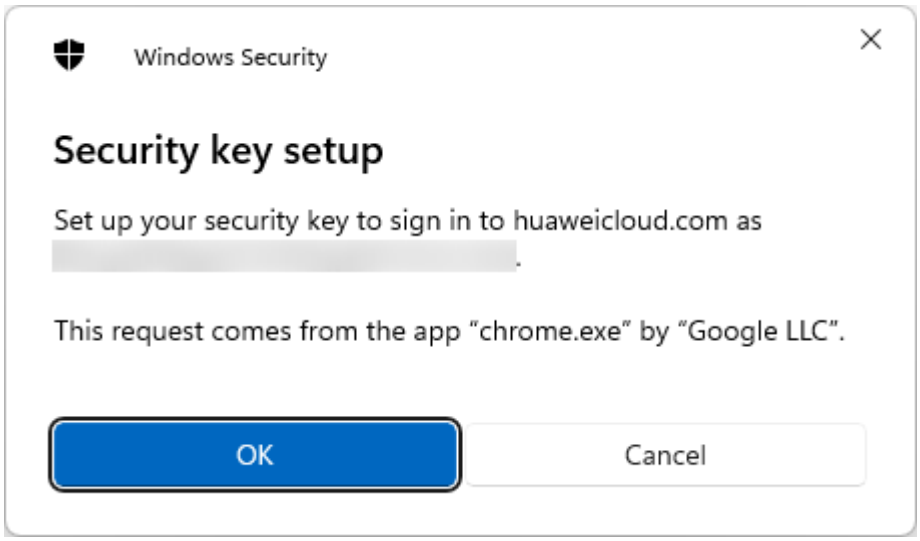
Step 10 In the displayed dialog box, select **Security key** and click **Next**.

Figure 1-17 Selecting the security key



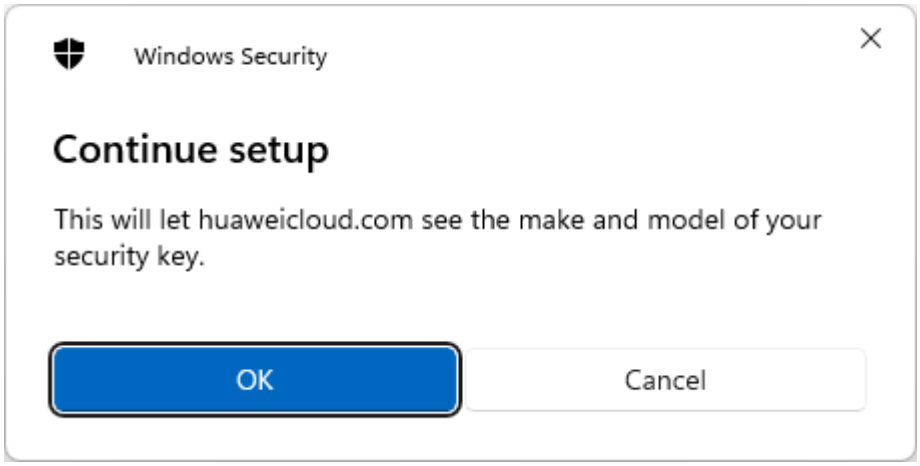
Step 11 Click **OK** to confirm the settings.

Figure 1-18 Confirming the settings



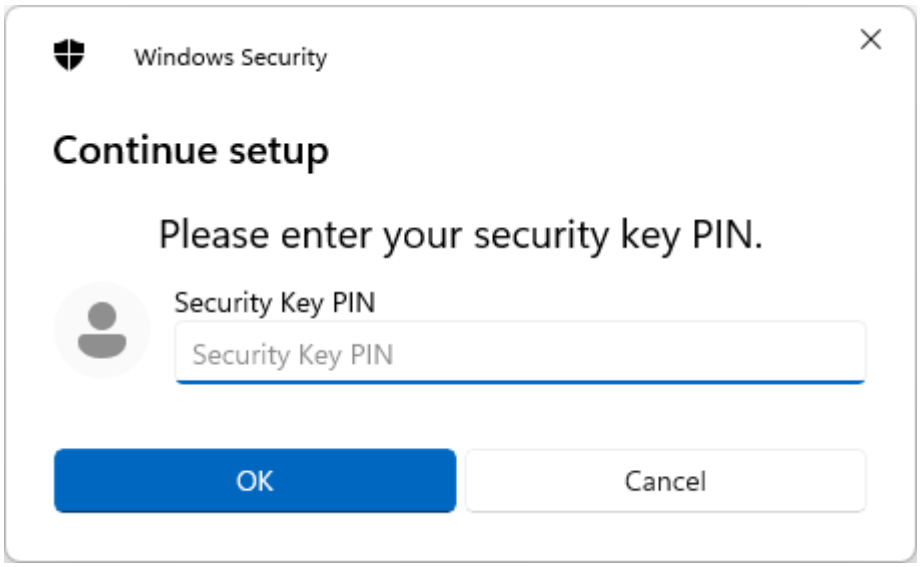
Step 12 Click **OK** to install the security key.

Figure 1-19 Installing the security key



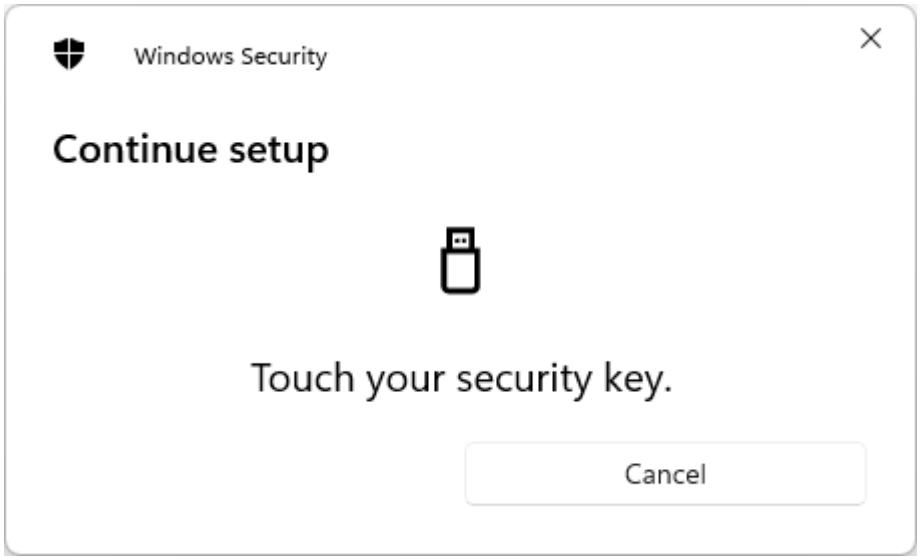
Step 13 Enter the PIN of the security key and click **OK**.

Figure 1-20 Entering the PIN



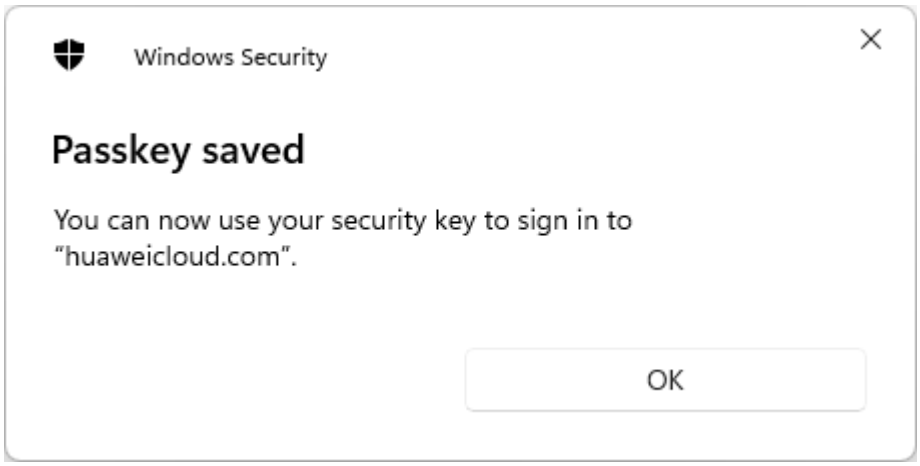
Step 14 Touch the security key.

Figure 1-21 Touching the security key



Step 15 Click **OK** in the displayed dialog box indicating that the hardware MFA device is added. The security key will be displayed in the MFA device list.

Figure 1-22 MFA device added



----End

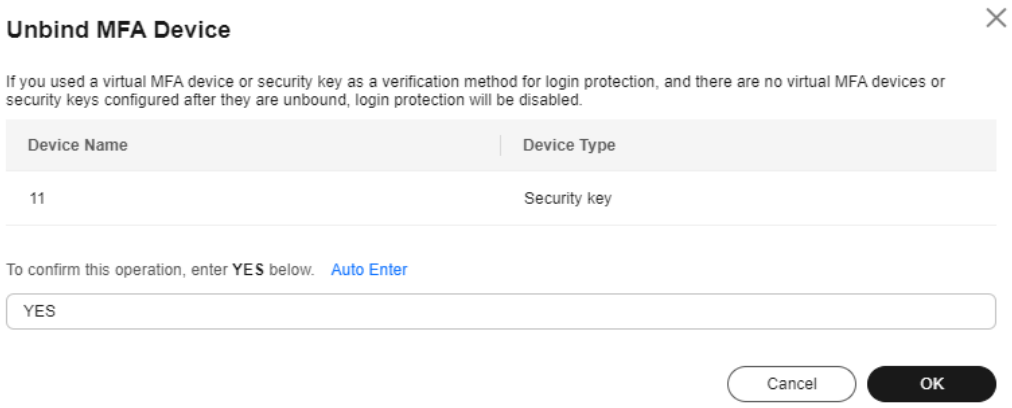
Unbinding a Security Key

You can unbind a security key on the console as an IAM user or using your account.

Step 1 In the **Multi-Factor Authentication (MFA)** area, locate the target security key and click **Unbind** in the **Operation** column.

Step 2 In the displayed dialog box, enter **YES**.

Figure 1-23 Confirming unbinding



Step 3 Click **OK**.

----End

2 My Credentials (Old)

2.1 My Credentials

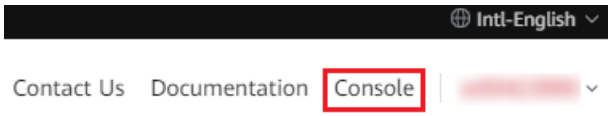
You can manage your security credentials on the **My Credentials** page.

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

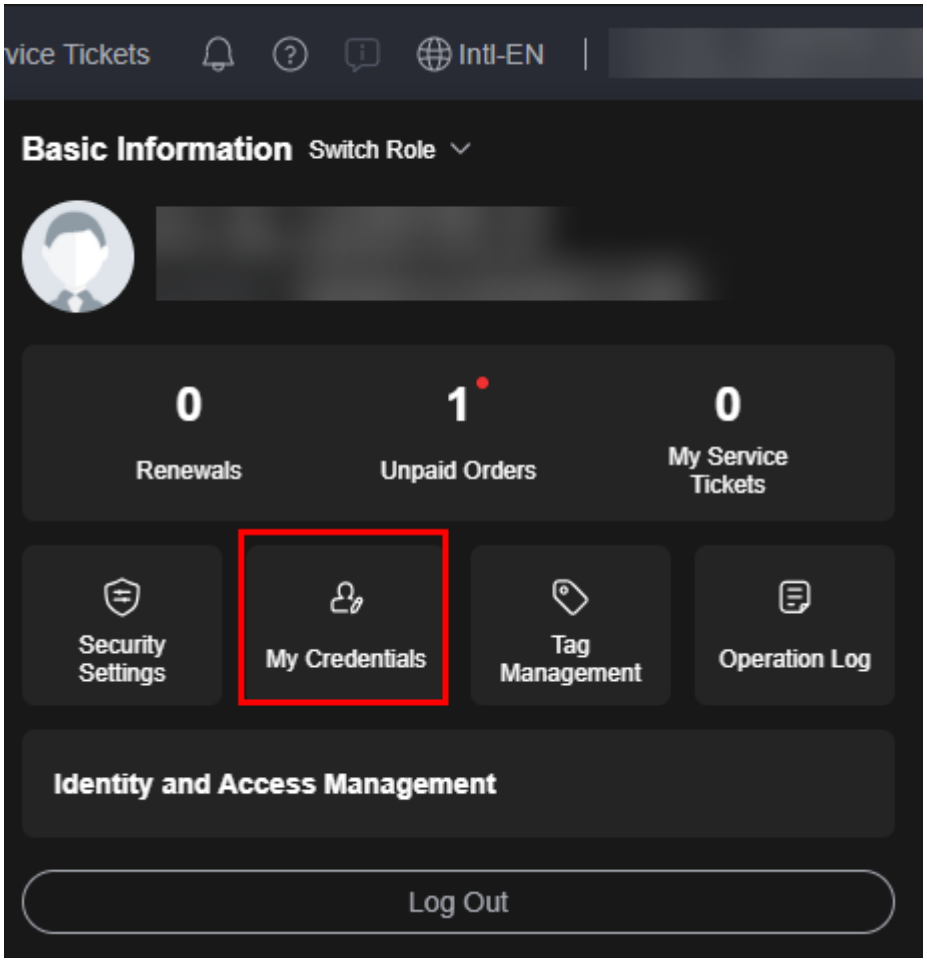
Step 1 Log in to Huawei Cloud and click **Console** in the upper right corner.

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

Table 2-1 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.

Parameter		Description
	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 **2.4 Temporary Access Key (for Federated Users)**.

----End

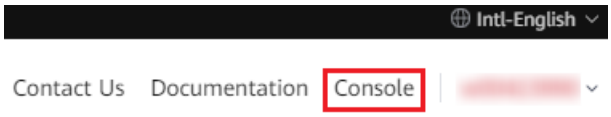
2.2 API Credentials

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

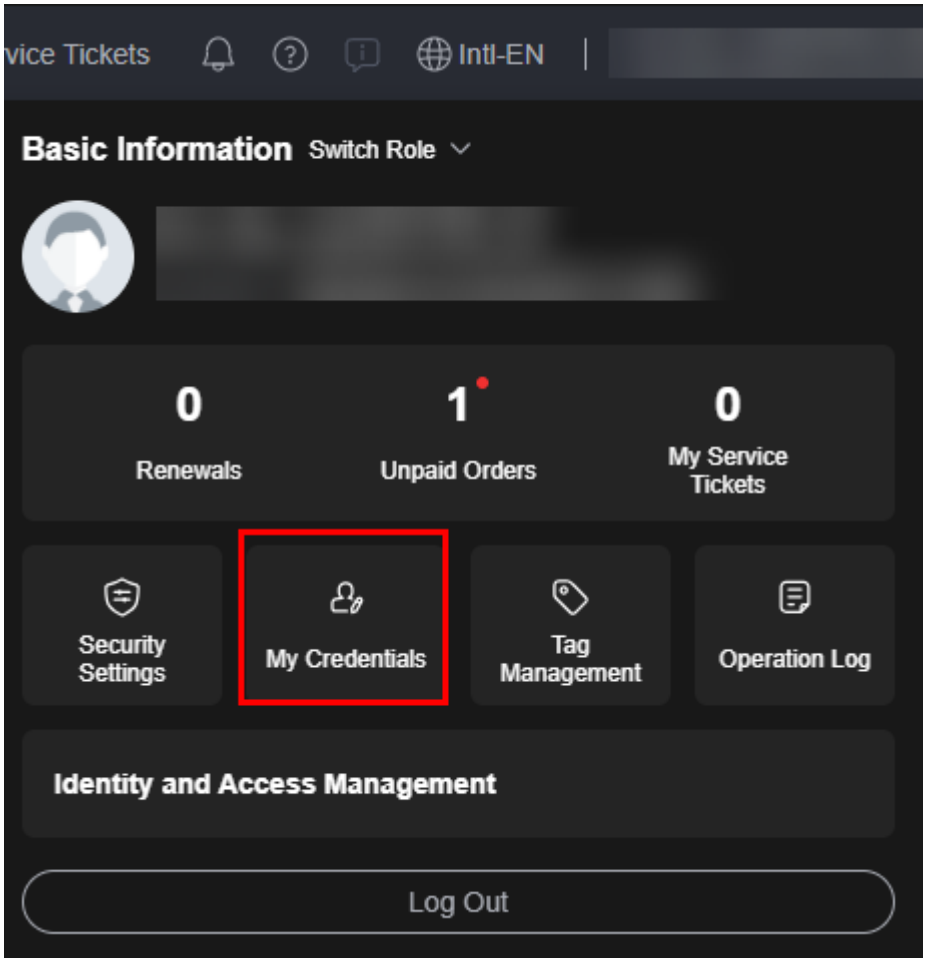
Step 1 Log in to Huawei Cloud and click **Console** in the upper right corner.

Figure 2-3 Accessing the console



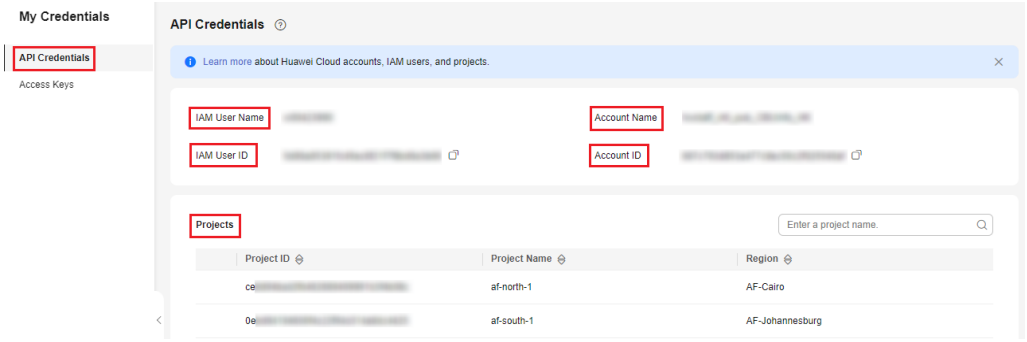
Step 2 On the management console, hover over the username in the upper right corner and choose **My Credentials** from the drop-down list.

Figure 2-4 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 2-5 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

2.3 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 cannot create access keys, but can create temporary access credentials (temporary AK/SK and security tokens). For details, see **Temporary Access Key (for Federated Users)**
3. If you are an IAM user, hover over 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 access keys** and send it to you.
   - Assign required permissions to you or change access key status. For details about how to assign permissions, see **Assigning Permissions to**

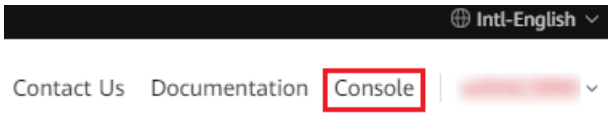
an IAM User. For details about how to change access key status, see Access Key Management.

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

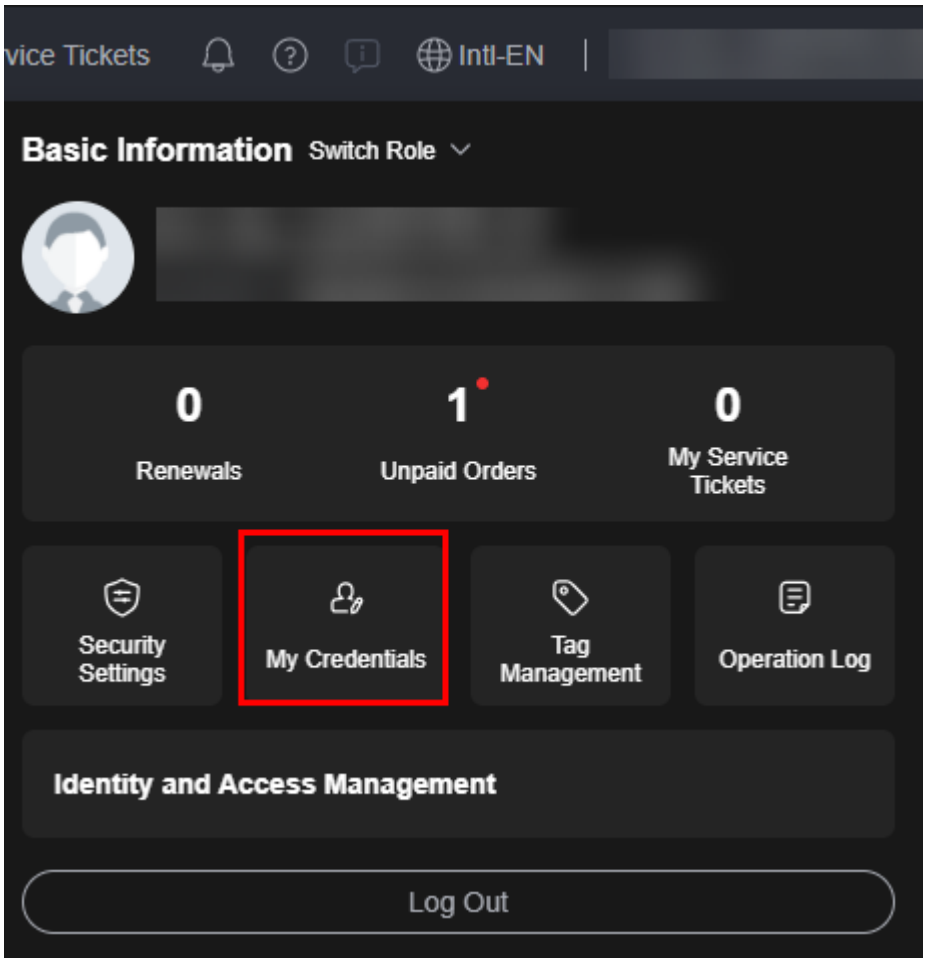
Step 1 Log in to Huawei Cloud and click **Console** in the upper right corner.

Figure 2-6 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 2-7 Choosing My Credentials

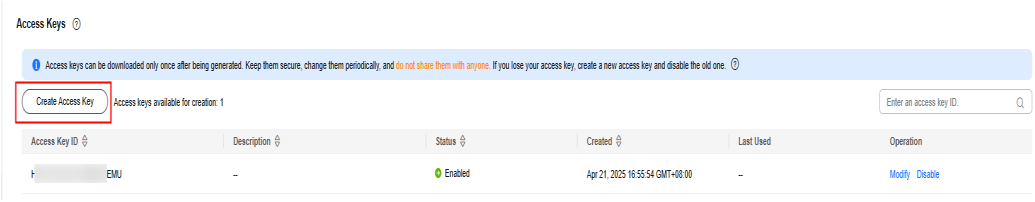


Step 3 Choose **Access Keys** from the navigation pane.

Step 4 Click **Create Access Key**.

If operation protection is enabled, you (the administrator) need to enter a verification code or password for identity authentication when creating an access key.

Figure 2-8 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 keys are created, view the access key ID (AK) 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.

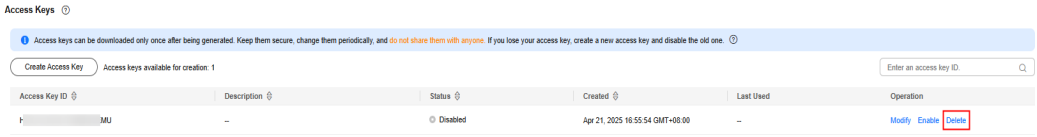
Step 1 On the **Access Keys** page, locate the access key to be deleted and click **Disable** in the **Operation** column.

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

Step 3 Click **Delete** in the **Operation** column of the disabled access key. Ensure that the deletion will not affect your services.

If operation protection is enabled, you (the administrator) need to enter a verification code or password for identity authentication when deleting an access key.

Figure 2-9 Deleting an access key



Step 4 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.

2.4 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 **2.3 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 2-2 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
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

