My Credentials

Issue  01
Date  2020-03-17
# Contents

1 My Credentials .......................................................................................................................... 1  
2 Changing the Credentials ......................................................................................................... 4  
3 Viewing the Project Name and ID ............................................................................................ 7  
4 Managing Access Keys ............................................................................................................... 8
The My Credentials page is used to manage security credentials, such as your mobile number, email address, and password.

To access the cloud system using the console or APIs, you need to obtain security credentials (such as the account name and project ID) on the My Credentials page. On this page, you can also change the login password and manage access keys (AK/SK).

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** View your credentials on the My Credentials page.
### Table 1-1 Credential information

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Username used for logging in to the cloud system.</td>
</tr>
<tr>
<td>User ID</td>
<td>ID of the user, which is automatically generated by the cloud system.</td>
</tr>
<tr>
<td>Account Name</td>
<td>Automatically created upon successful registration of an entity (such as an enterprise). The account pays bills for the use of cloud resources.</td>
</tr>
<tr>
<td>Account ID</td>
<td>ID of the account, which is automatically generated by the cloud system.</td>
</tr>
<tr>
<td>Email Address</td>
<td>The email address bound to the user. It can be used to log in to the system, reset the login password, receive verification codes, and push notifications. To change the bound email address, click <strong>Change</strong> on the right.</td>
</tr>
<tr>
<td>Mobile Number</td>
<td>The mobile number bound to the user. It can be used to log in to the system, reset the login password, receive verification codes, and push notifications. To change the bound mobile number, click <strong>Change</strong> on the right.</td>
</tr>
<tr>
<td>Password Strength</td>
<td>Strength of the login password. To change the password, click <strong>Change</strong> on the right.</td>
</tr>
<tr>
<td>Login Authentication</td>
<td>Login authentication based on virtual MFA device, SMS, and email is supported. If this option is enabled, you will need to enter a verification code in addition to the username and password when logging in to the system.</td>
</tr>
<tr>
<td>Virtual MFA Device</td>
<td>Virtual MFA-based login authentication can be enabled only after you have bound a virtual MFA device.</td>
</tr>
<tr>
<td>Projects</td>
<td>Projects group and isolate resources (including compute, storage, and network resources) across physical regions. A project can be a department or a project group. For more refined resource management, you can create subprojects under a specific region and purchase resources in the subprojects.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Project list</td>
<td>List of projects you can access. A project must be specified when you call native OpenStack APIs.</td>
</tr>
<tr>
<td>Access Keys</td>
<td>Long-term identity credentials used for accessing the system through APIs. You can create a maximum of two access keys.</td>
</tr>
</tbody>
</table>

---End
You can change your login password, email address, mobile number, avatar, and login authentication mode on the My Credentials page. Users can change their passwords on this page if they remember their current passwords. If the password of an IAM user is forgotten, contact the administrator to reset the password on the Identity and Access Management (IAM) console.

**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 page, change the email address, mobile number, password, avatar, or login verification method.
The method of changing the email address and mobile number is similar to that of changing the password. The following example shows how to change the password.

- **Changing the password**
  a. Click **Change** next to **Password Strength**.
  b. Select email address or mobile number verification.

  ![NOTE]
  The two verification modes are available only if you have bound an email address and mobile number.
  c. Enter the verification code.
  d. Enter the old password and new password, and enter the new password again.

  ![NOTE]
  - The password cannot be the username or the username spelled backwards. For example, if the username is **A12345**, the password cannot be **A12345**, **a12345**, **54321A**, or **54321a**.
  - For account security, the administrator can configure password settings by choosing **Account Settings > Password Policy** in IAM, such as the minimum number of characters a password must contain. For details, see **Password Policy**.

  e. Click **OK**.

- **Changing the login verification method**
  a. Click **Change** next to **Login Authentication**. On the **Change Verification Method** page, select a verification method, and enter the verification code.
  b. Click **OK**.
Virtual MFA-based login authentication can be enabled only after you have bound a virtual MFA device.

After login authentication is enabled, you need to enter a verification code generated by a virtual MFA device, an SMS verification code, or an email verification code on the Login Verification page when logging in to the system.

To disable login authentication, select Disabled next to Verification Method, and click OK.

- Changing the avatar
  a. On the My Credentials page, click Change below the avatar.
  b. Click Upload and select a picture.
  c. Click OK.

--- End
3 Viewing the Project Name and ID

A project ID is the ID of a region in which resources are accessible to a user. If you need to specify a project name and ID when calling APIs to manage cloud resources, for example, creating a Virtual Private Cloud (VPC), you can obtain the project name and ID on the My Credentials page.

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 page, click the Projects tab and view project IDs.

Figure 3-1 Project IDs

----End
Managing 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, all users can create and delete their 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.

Federated users cannot create access keys, but they can create temporary access credentials (temporary AK/ SK and SecurityToken). For details, see What Are Temporary Security Credentials (AK/ SK and Security Token)?

Creating an Access Key

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

2. On the My Credentials page, click the Access Keys tab.
3. Click Create Access Key, and enter the verification code.
No verification code is required if you have not bound an email address or a mobile number.

4. Click OK to generate an access key and download it.

NOTE

You can create a maximum of two access keys with unlimited validity. Keep your access keys secure and change them periodically for security purposes. To change an access key, delete it and create a new one.

Deleting an Access Key

1. On the Access Keys tab page, click Delete in the same row as the access key.
2. Enter the verification code, and click Yes.

NOTE

- No verification code is required if you have not bound an email address or a mobile number.
- If your access keys are forgotten or leaked, delete them on the My Credentials page or contact the administrator to delete them in IAM.

Enabling/Disabling an Access Key

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

1. On the Access Keys tab page, click Disable in the same row as the target access key.
2. Enter the verification code, and click Yes.

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