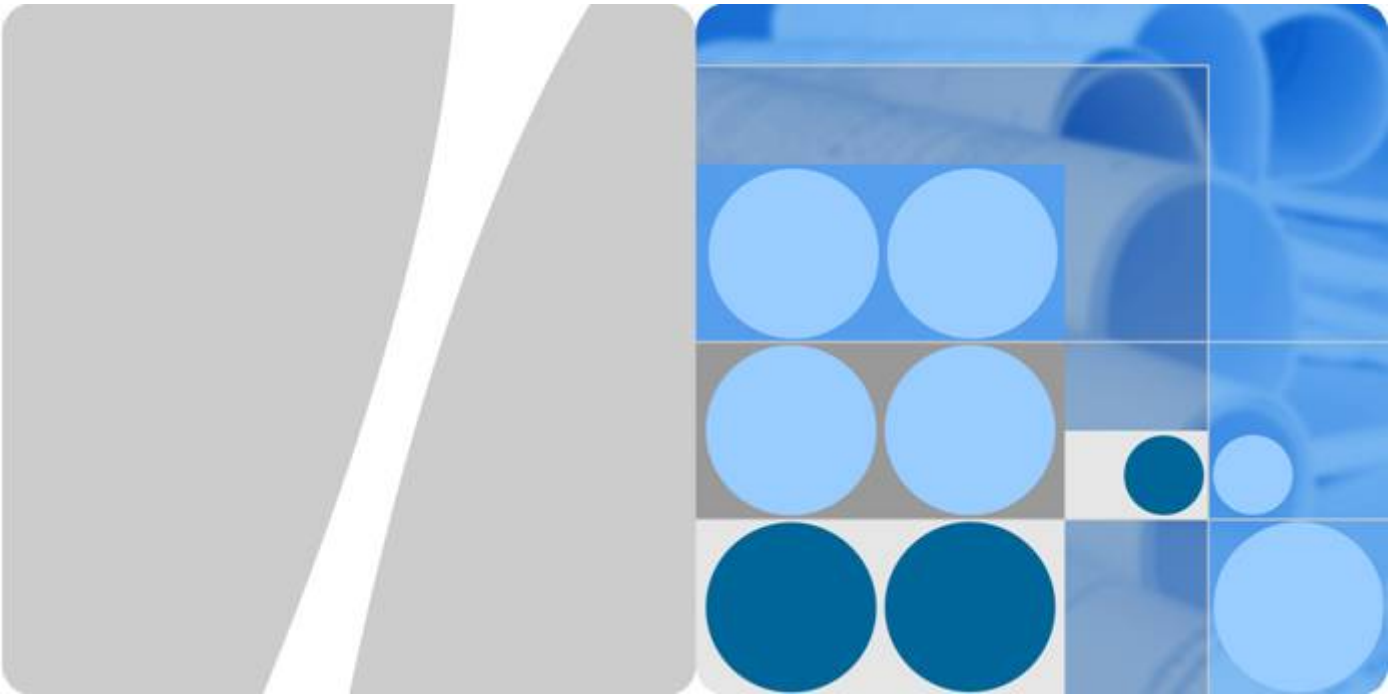

Identity and Access Management

My Credentials

Date **2020-10-30**

Contents

1 My Credentials

The **My Credentials** page is used to manage your security credentials, such as the mobile number, email address, and login password.

To access cloud resources 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 the mouse pointer over the account name in the upper right corner and choose **My Credentials** from the drop-down list.

Step 2 View your credentials on the **My Credentials** page.

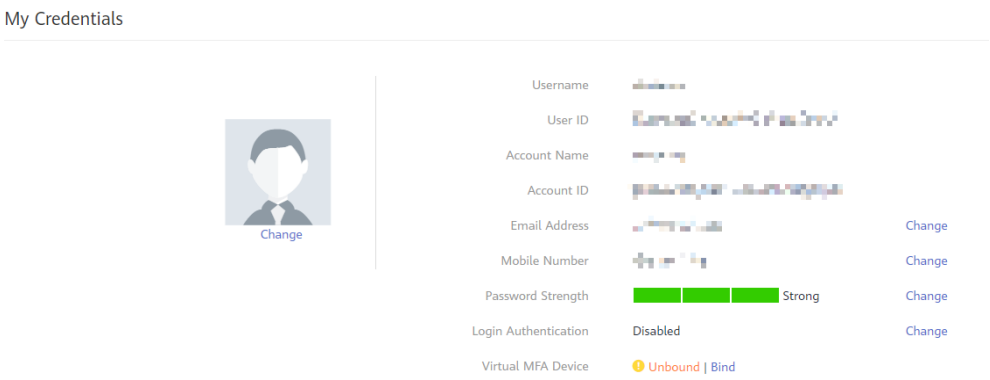

Table 1-1 Credential information

Parameter	Description
Username	Name used for logging in to the cloud system.
User ID	ID of the user, which is automatically generated by the cloud system.

Parameter	Description
Account Name	Automatically created upon successful registration of an entity (such as an enterprise). The account pays bills for the use of cloud resources.
Account ID	ID of the account, which is automatically generated by the cloud system.
Email Address	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 email address, click **Change** on the right.
Mobile Number	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 mobile number, click **Change** on the right.
Password Strength	Strength of the login password. To change the password, click **Change** on the right.
Login Authentication	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 cloud system.
Virtual MFA Device	Virtual MFA-based login authentication can be enabled only after you have bound a virtual MFA device.
Projects	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.
Project list	List of projects you can access. A project must be specified when you call native OpenStack APIs.
Access Keys	Long-term identity credentials used for accessing the system through APIs. You can create a maximum of two access keys.

----End

2 Changing the Password, Email Address, and Mobile Number

You can change your login password, email address, mobile number, avatar, and login authentication mode on the **My Credentials** page. IAM users can change their passwords on this page if they remember their passwords. If IAM users forget their passwords, they can contact the administrator to reset their passwords on the Identity and Access Management (IAM) console.

Procedure

Step 1 On the management console, hover the mouse pointer over the account name 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, you can configure password settings by choosing **Account Settings** > **Password Policy** in IAM, such as the minimum number of characters a password must contain.

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**.

NOTE

- 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 the mouse pointer over the account name 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.

----End

4 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 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, 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.

Federated users can only create temporary access credentials (temporary AK/SKs and security tokens).

Creating an Access Key

1. On the management console, hover the mouse pointer over the account name 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.

   NOTE

   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. For security purposes, keep your access keys secure and change them periodically. 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 row containing the access key you want to delete.
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 access keys of IAM users are lost or accidentally disclosed, IAM users can delete them on the **My Credentials** page or contact the administrator to delete them in IAM.