Identity and Access Management

FAQs

Issue	01
Date	2022-09-30

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

HUAWEI 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 User Groups and Permissions Management.... 1
1.1 Why Can't I Find Permissions for a Cloud Service?.... 1
1.2 How Do I Grant Cloud Service Permissions in the Cloud Alliance Regions to IAM Users?.... 1
1.3 Why Permissions Granted to a User Do Not Take Effect?.... 3
1.4 How Can I Grant an IAM User Permissions to Place Orders But Disallow Order Payment?.... 4
2 IAM User Management.... 8
2.1 Why Does IAM User Login Fail?.... 8
2.2 How Do I Control IAM User Access to the Console?.... 9
3 Security Settings.... 10
3.1 How Do I Enable Login Verification?.... 10
3.2 How Do I Disable Login Verification?.... 11
3.3 How Do I Change the Verification Method for Performing Critical Operations?.... 12
3.4 How Do I Disable Operation Protection?.... 15
3.5 How Do I Bind a Virtual MFA Device?.... 17
3.6 How Do I Obtain a Virtual MFA Verification Code?.... 18
3.7 How Do I Unbind or Remove a Virtual MFA Device?.... 19
3.8 Why Does MFA Authentication Fail?.... 21
3.9 Why Am I Not Getting the Verification Code?.... 21
3.10 Why Is My Account Locked?.... 22
3.11 Why Doesn't My API Access Control Policy Take Effect?.... 23
3.12 Why Do I Still Need to Perform MFA During Login After Unbinding the Virtual MFA Device?.... 24
4 Passwords and Credentials.... 26
4.1 What Should I Do If I Forgot My Password?.... 26
4.2 How Do I Change My Password?.... 30
4.3 How Do I Obtain an Access Key (AK/SK)?.... 30
4.4 What Should I Do If I Have Forgotten My Access Key (AK/SK)?.... 31
4.5 What Are Temporary Security Credentials (AK/SK and Security Token)?.... 31
4.6 How Do I Obtain a Token with Security Administrator Permissions?.... 32
4.7 How Do I Obtain an Access Key (AK/SK) in the Cloud Alliance Regions?.... 33
5 Project Management.... 35
5.1 What Are the Differences Between IAM and Enterprise Management?.... 35
5.2 What Are the Differences Between IAM Projects and Enterprise Projects?.... 36

5.3 What Are the Differences Between IAM Users and Enterprise Member Accounts?....37

6 Agency Management.... 39

6.1 How Can I Obtain Permissions to Create an Agency?.... 39

7 Account Management....40

7.1 Why Does Account Login Fail?....40

7.2 What Are the Relationships Between a Huawei Cloud Account, HUAWEI ID, IAM User, and Federated User?.... 42

7.3 What Are the Possible Causes of a HUAWEI ID Upgrade Failure?.... 45

7.4 Can I Log In with My Huawei Cloud Account After Upgrading It to a HUAWEI ID?....46

8 Others.... 47

8.1 How Do I Obtain a User Token Using Postman?....47

8.2 Why Is the Field-Level Help Always Displayed?....49

8.3 How Do I Disable Autofill Password on Google Chrome?....50

8.4 Region and AZ.... 51

8.5 How Do I Apply for the Permissions to Access Resources in a Cloud Alliance Region Using My Huawei Cloud Account or HUAWEI ID?.... 51

1 User Groups and Permissions Management

1.1 Why Can't I Find Permissions for a Cloud Service?

Symptom

You cannot find permissions for a specific cloud service when you assign permissions to a user group or an agency on the IAM console.

Possible Causes

- The service is not supported by IAM. No permissions are available for the service in IAM. For the cloud services supported by IAM, see **Supported Cloud Services**.
- The service name or permission name is incorrect.

Solutions

- **Submit a service ticket** and request to register permissions for the specific service in IAM.
- Check the service name on the management console or in the help center, and view the system-defined permissions provided by the service in **System-defined Permissions**.

1.2 How Do I Grant Cloud Service Permissions in the Cloud Alliance Regions to IAM Users?

Symptom

The administrator has enabled cloud services in the **CN-Hong Kong**, **AP-Singapore**, **CN East-Shanghai1**, **LA-Sao Paulo1**, **LA-Mexico City1**, **LA-Mexico City2**, **AF-Johannesburg**, or **LA-Santiago** cloud alliance region, and need to authorize IAM users to use cloud services in this region.

Users access cloud services in the cloud alliance region as virtual users authorized through federated authentication. They are not real users who exist in the cloud service system, and need to be authorized in the Huawei Cloud's default regions and the **CN-Hong Kong**, **AP-Singapore**, **CN East-Shanghai1**, **LA-Sao Paulo1**, **LA-Mexico City1**, **LA-Mexico City2**, **AF-Johannesburg**, or **LA-Santiago** cloud alliance region, respectively.

Prerequisites

- You have created an IAM user in a default region of Huawei Cloud and added the user to a user group. For example, you have created IAM user **User-001** and added them to user group **UserGroup-001**. For details, see **Creating an IAM User** and **Adding Users to or Removing Users from a User Group**.
- If this is the first time to grant cloud service permissions for IAM users in the cloud alliance regions, you need to use an account rather than an IAM user with administrator permissions to perform authorization operations.

Procedure

Step 1 Log in to Huawei Cloud as an administrator, click 📍 on the console homepage, and select the **CN-Hong Kong**, **AP-Singapore**, **CN East-Shanghai1**, **LA-Sao Paulo1**, **LA-Mexico City1**, **LA-Mexico City2**, **AF-Johannesburg**, or **LA-Santiago** region.

Step 2 On the console, choose **Management & Governance** > **Identity and Access Management**.

Step 3 On the IAM console, choose **User Groups** from the navigation pane, and click **Create User Group** in the upper right corner to create a group with the same name (**UserGroup-001**).

Step 4 On the **User Groups** page, click **Modify** in the row that contains the user group created in **3**.

Step 5 In the **Group Permissions** area, click **Attach Policy** in the row that contains the target region for user authorization, select desired permissions, and click **OK**.

The permissions assigned to this group will also apply to IAM users in the user group in Huawei Cloud.

Step 6 Click **OK** to complete the authorization for IAM users in the **CN-Hong Kong**, **AP-Singapore**, **CN East-Shanghai1**, **LA-Sao Paulo1**, **LA-Mexico City1**, **LA-Mexico City2**, **AF-Johannesburg**, or **LA-Santiago** cloud alliance region.

----End

After the authorization is complete, log in to the Huawei Cloud console as an IAM user. Select the **CN-Hong Kong**, **AP-Singapore**, **CN East-Shanghai1**, **LA-Sao Paulo1**, **LA-Mexico City1**, **LA-Mexico City2**, **AF-Johannesburg**, or **LA-Santiago** cloud alliance region and use cloud resources based on the assigned permissions.

1.3 Why Permissions Granted to a User Do Not Take Effect?

Symptom

Permissions that you grant to an IAM user do not take effect.

Troubleshooting

1. Cause: Incorrect permissions were granted to the user group to which the user belongs.

   Solution: Ask the administrator to modify the permissions granted to the user group to which the IAM user belongs. For details, see **Modifying User Group Permissions**. For details about permissions, see **System-defined Permissions**.

2. Cause: Actions are denied by the permissions granted to the user.

   View the system-defined permissions granted to the IAM user and check whether there is a policy statement that denies the action. For details, see **Policy Syntax**. If the system-defined permissions cannot meet your requirements, create a custom policy to allow the action. For details, see **Creating a Custom Policy**.

3. Cause: The IAM user has not been added to the user group with permissions assigned.

   Solution: Add the user to the target user group as the administrator. For details, see **Adding Users to a User Group**.

4. Cause: For a regional service, the user group is not assigned with permissions in specific regions.

   Assign permissions to the user group in specific regions. If you have assigned the user only permissions for a default region-specific project, the user does not have permissions for the subprojects. In this case, assign permissions for the required subproject. For details, see **Assigning Permissions to a User Group**.

5. Cause: The IAM user has not switched to the region where the user has been authorized to use cloud resources.

   Remind the user to switch to the region where the user is authorized to use cloud resources. For details, see **Switching Regions**.

6. Cause: If the administrator has granted OBS permissions to the user, the permissions will take effect 15 to 30 minutes after the authorization.

   Check the permissions after 15 to 30 minutes and try again.

7. Cause: The browser cache has not been cleared for a long time.

   Clear the browser cache and try again.

8. Cause: The service (such as OBS) provides separate permissions control.

   Grant the user permissions by referring to the service documentation. For example, see **Introduction to OBS Permission Control**.

9. Cause: If you have granted permissions to a user in both IAM and Enterprise Management, the permissions for enterprise projects may not take effect. IAM

authentication takes precedence over Enterprise Management authentication. If an IAM user has the **ECS ReadOnlyAccess** permission for all resources and enterprise project A, the user can view all ECS resources.

Modify the permissions of the user on the IAM console.

Related FAQ

Symptom: You have granted an IAM user only required permissions but the user has more permissions.

Possible causes:

1. The required permissions you granted to the IAM user have dependency permissions, which are automatically assigned so that the required permissions can take effect for the user.
2. You have granted other permissions to the IAM user in Enterprise Project Management. If you manage projects and users using IAM, cancel the permissions configured there. For details, see **Deleting Enterprise Projects That Are Managed by a User**.

1.4 How Can I Grant an IAM User Permissions to Place Orders But Disallow Order Payment?

Symptom

You want to grant an IAM user permissions to place orders but disallow the user to pay for the orders.

Solutions

However, the system permissions of the Billing Center registered with IAM cannot meet your requirements. You need to create a custom policy containing the required permissions and use the policy to grant permissions to the IAM user.

Prerequisites

You have already created IAM user A and user group B and you have added the user to the user group. For details, see **Creating an IAM User**.

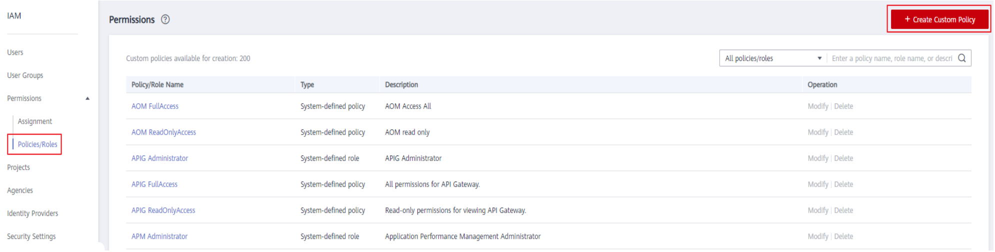
Procedure

Step 1 Log in to the HUAWEI CLOUD management console.

Step 2 On the management console, hover the mouse pointer over the username in the upper right corner, and choose **Identity and Access Management** from the drop-down list.

Step 3 On the IAM console, choose **Permissions** > **Policies/Roles** from the navigation pane, and click **Create Custom Policy** in the upper right corner.

Figure 1-1 Creating a custom policy



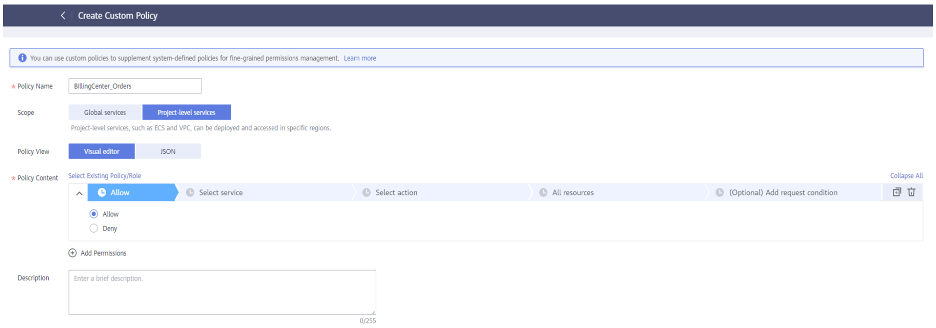
Custom policies available for creation: 200

Policy/Role Name	Type	Description	Operation
AOM FullAccess	System-defined policy	AOM Access All	Modify | Delete
AOM ReadOnlyAccess	System-defined policy	AOM read only	Modify | Delete
APIG Administrator	System-defined role	APIG Administrator	Modify | Delete
APIG FullAccess	System-defined policy	All permissions for API Gateway.	Modify | Delete
APIG ReadOnlyAccess	System-defined policy	Read-only permissions for viewing API Gateway.	Modify | Delete
APM Administrator	System-defined role	Application Performance Management Administrator	Modify | Delete

Step 4 Set the policy name to **BillingCenter_Orders**.

Step 5 Set the scope to **Project-level services**.

Figure 1-2 Setting the scope



You can use custom policies to supplement system-defined policies for fine-grained permissions management.

* Policy Name: BillingCenter_Orders

Scope: Project-level services

Project-level services, such as ECS and VPC, can be deployed and accessed in specific regions.

Policy View: Visual editor

* Policy Content: Allow

● Allow
○ Deny

Description

Step 6 Select **Visual editor**.

Step 7 In the **Policy Content** area, configure permissions that allow the user to place orders but disallow the user to pay for the orders.

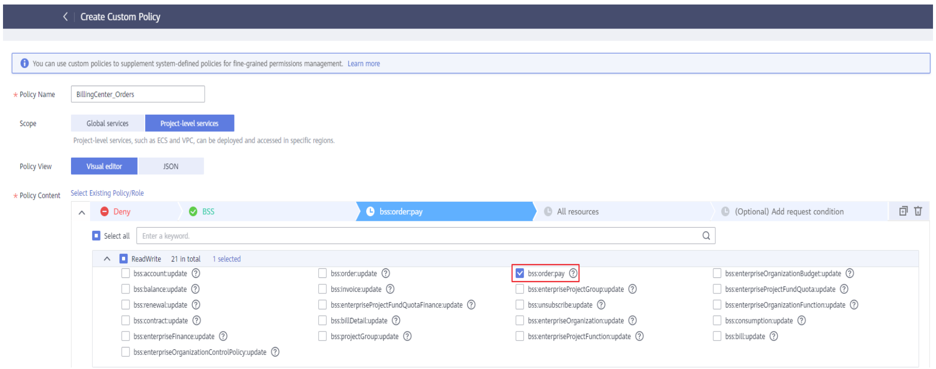
- Configuring permissions to disallow order payment

  a. Select **Deny**.

  b. For the cloud service, select **BSS (BSS)**.

  c. In the **Select action** step, expand the **ReadWrite** area, and select the action **bss:order:pay**.

Figure 1-3 Configuring permissions to disallow order payment



You can use custom policies to supplement system-defined policies for fine-grained permissions management.

* Policy Name: BillingCenter_Orders

Scope: Project-level services

Project-level services, such as ECS and VPC, can be deployed and accessed in specific regions.

Policy View: Visual editor

* Policy Content: Deny | BSS | bss:order:pay

ReadWrite 21 in total 1 selected

☐ bss:account:update ☐ bss:order:update ☑ bss:order:pay ☐ bss:enterpriseOrganizationBudget:update
☐ bss:balance:update ☐ bss:invoice:update ☐ bss:enterpriseProjectGroup:update ☐ bss:enterpriseProjectFundQuota:update
☐ bss:renewal:update ☐ bss:enterpriseProjectFundQuotaFinance:update ☐ bss:unsubscribe:update ☐ bss:enterpriseOrganizationFunction:update
☐ bss:contract:update ☐ bss:billDetail:update ☐ bss:enterpriseOrganization:update ☐ bss:consumption:update
☐ bss:enterpriseFinance:update ☐ bss:projectGroup:update ☐ bss:enterpriseProjectFunction:update ☐ bss:bill:update
☐ bss:enterpriseOrganizationControlPolicy:update

  d. Set the resource type to **All**.

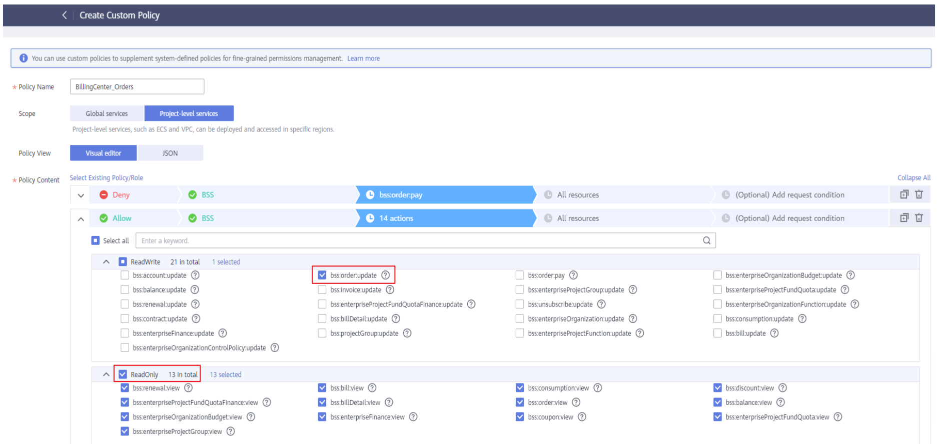
- Configuring permissions to allow order placement

  a. Select **Allow**.

b. For the cloud service, select **BSS (BSS)**.

c. In the **Select action** step, expand the **ReadWrite** area, select the action **bss:order:update**, and select all the actions in the **ReadOnly** area.

Figure 1-4 Configuring permissions to allow order placement



Create Custom Policy

You can use custom policies to supplement system-defined policies for fine-grained permissions management. Learn more

* Policy Name: BillingCenter_Orders

Scope: Global services | **Project-level services**

Project-level services, such as ECS and VPC, can be deployed and accessed in specific regions.

Policy View: **Visual editor** | JSON

* Policy Content: Select Existing Policy/Role — Collapse All

Deny	BSS	bss:order:pay	All resources	(Optional) Add request condition
Allow	BSS	14 actions	All resources	(Optional) Add request condition

□ Select all — Enter a keyword.

ReadWrite 21 in total 1 selected

- □ bss:account:update
- □ bss:balance:update
- □ bss:renewal:update
- □ bss:contract:update
- □ bss:enterpriseFinance:update
- □ bss:enterpriseOrganizationControlPolicy:update
- ☑ bss:order:update
- □ bss:invoice:update
- □ bss:enterpriseProjectFundQuotaFinance:update
- □ bss:billDetail:update
- □ bss:projectGroup:update
- □ bss:order:pay
- □ bss:enterpriseProjectGroup:update
- □ bss:unsubscribe:update
- □ bss:enterpriseOrganization:update
- □ bss:enterpriseProjectFunction:update
- □ bss:enterpriseOrganizationBudget:update
- □ bss:enterpriseProjectFundQuota:update
- □ bss:enterpriseOrganizationFunction:update
- □ bss:consumption:update
- □ bss:bill:update

☑ ReadOnly 13 in total 13 selected

- ☑ bss:renewal:view
- ☑ bss:enterpriseProjectFundQuotaFinance:view
- ☑ bss:enterpriseOrganizationBudget:view
- ☑ bss:enterpriseProjectGroup:view
- ☑ bss:bill:view
- ☑ bss:billDetail:view
- ☑ bss:enterpriseFinance:view
- ☑ bss:consumption:view
- ☑ bss:order:view
- ☑ bss:coupon:view
- ☑ bss:discount:view
- ☑ bss:balance:view
- ☑ bss:enterpriseProjectFundQuota:view

d. Set the resource type to **All**.

Step 8 Set a description for the policy, for example, "Permissions to place orders but disallow order payment."

Step 9 Click **OK**.

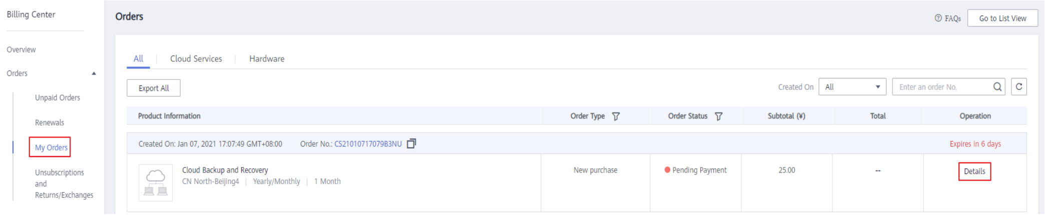
Step 10 Attach the policy to user group B. Users in the group inherit the permissions defined in this policy.

NOTE

You can attach custom policies to a user group in the same way you attach system-defined policies. For details, see **Creating a User Group and Assigning Permissions**.

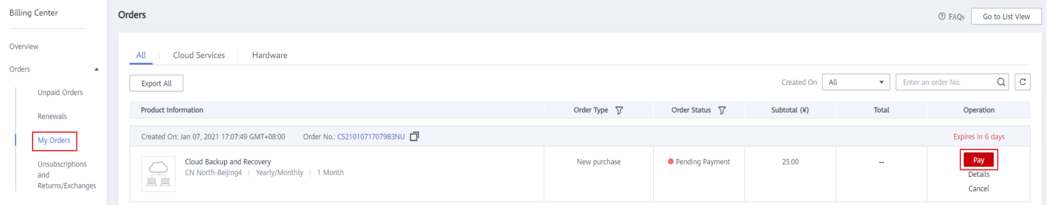
Step 11 When the IAM user logs in and goes to the **My Orders** page of the Billing Center, the **Pay** button is not displayed in the **Operation** column.

Figure 1-5 My Orders page displayed if permissions are granted successfully



Product Information	Order Type	Order Status	Subtotal (¥)	Total	Operation
Created On: Jan 07, 2021 17:07:49 GMT+08:00 Order No.: CS21010717079B3NU					Expires in 6 days
Cloud Backup and Recovery CN North-Beijing4 | Yearly/Monthly | 1 Month	New purchase	Pending Payment	25.00	--	Details

Figure 1-6 My Orders page displayed if permissions failed to be granted



Product Information	Order Type	Order Status	Subtotal (¥)	Total	Operation
Created On: Jan 07, 2021 17:07:49 GMT+08:00 Order No.: CS21010717079B3NU					Expires in 6 days
Cloud Backup and Recovery CN North-Beijing4 | Yearly/Monthly | 1 Month	New purchase	● Pending Payment	25.00	--	Pay Details Cancel

----End

2 IAM User Management

2.1 Why Does IAM User Login Fail?

Symptom

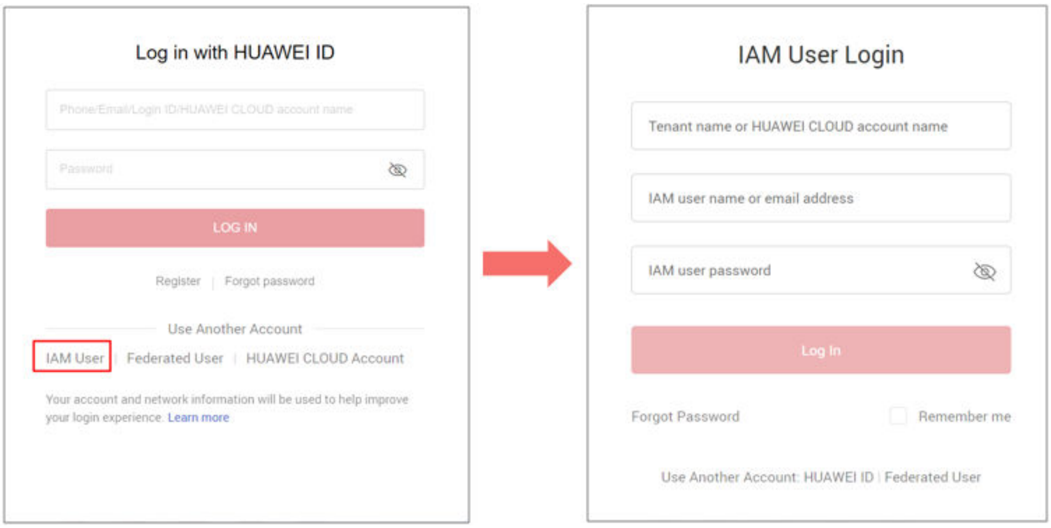
An IAM user fails to log in and sees a message indicating that the username or password is incorrect or login from the current device is not allowed due to the access control rules set by the administrator.

Troubleshooting

- **Incorrect username or password**

  a. You selected an incorrect login entry.

     Click **IAM User** on the login page.


Log in with HUAWEI ID
Phone/Email/Login ID/HUAWEI CLOUD account name
Password
LOG IN
Register | Forgot password
Use Another Account
IAM User | Federated User | HUAWEI CLOUD Account
Your account and network information will be used to help improve your login experience. Learn more
IAM User Login
Tenant name or HUAWEI CLOUD account name
IAM user name or email address
IAM user password
Log In
Forgot Password
Remember me
Use Another Account: HUAWEI ID | Federated User

  b. Incorrect tenant name/Huawei Cloud account name or IAM username.

Enter the correct tenant name/Huawei Cloud account name and IAM username. If you do not know your IAM user name or the name of the account used to create the IAM user, contact the administrator.

c. Incorrect password.

Enter the correct password. If you have forgotten your password, reset it by referring to **How Do I Reset My Password?**

d. You did not clear the browser cache after changing or resetting the password.

Clear the browser cache and log in again.

- **Login from the current device is not allowed due to the access control rules set by the administrator.**

a. The administrator has set access control rules on the IAM console to limit Huawei Cloud access to specific IP address ranges, IPv4 CIDR blocks, or VPC endpoints.

Solution: Contact the administrator to check the ACL rules on the console and log in to Huawei Cloud from an allowed device, or ask the administrator to modify the ACL rules. For details, see **Access Control**.

2.2 How Do I Control IAM User Access to the Console?

To ensure user information and system security, you can configure an ACL that allows user access only from specific IP addresses.

Procedure

Step 1 Log in to the IAM console.

Step 2 In the navigation pane, choose **Security Settings** > **ACL**.

NOTE

The ACL will take effect only for the IAM users you have created using your account.

Step 3 Click the **Console Access** tab, and set IP addresses or IPv4 CIDR blocks that are allowed to access the console.

- **IP Address Ranges**: Allow users to access the system using IP addresses in specific ranges.
- **IPv4 CIDR Blocks**: Allow users to access the system using specific IPv4 CIDR blocks.

  For example: **10.10.10.10/32**.

NOTE

If you specify both **IP Address Ranges** and **IPv4 CIDR Blocks**, users are allowed to access the system if their IP addresses meet the conditions specified by either of the two parameters.

Step 4 Click **Save**.

----End

3 Security Settings

3.1 How Do I Enable Login Verification?

To ensure account security, you are advised to enable login verification.

After you enable this function, you and IAM users created using your account need to enter verification codes generated by the bound virtual MFA device, SMS verification codes, or email verification codes on the **Login Verification** page during login.

If you disable this function, you and the IAM users only need to enter the account name/username and password during login.

Procedure

- Enabling login verification for an IAM user on the IAM console as an administrator

Step 1 In the navigation pane, choose **Users**.

Step 2 Click **Security Settings** in the row containing the target user.

Step 3 On the **Security Settings** tab, in the **Login Protection** area, select a verification method and enter a verification code.

Step 4 Click **OK**.

----End

- Enabling login verification for yourself (account administrator) on the **Security Settings** page

  Perform the following steps if your Huawei Cloud account has not been upgraded to a HUAWEI ID. To enable login verification for a HUAWEI ID, go to the **HUAWEI ID website**.

Step 1 Hover the mouse pointer over the username in the upper right corner and choose **Security Settings** from the drop-down list.

Step 2 Click the **Critical Operations** tab, and click **Enable** next to **Login Protection**.

Step 3 On the **Login Protection** page, select **Enable**, select a verification method, and enter a verification code.

Step 4 Click **OK**.

----End

Related Operations

You can change the login verification method of your IAM users or account:

- To change the login verification method of an IAM user, go to the user list on the IAM console, click **Security Settings** in the row that contains the user, click ✎ next to **Verification Method** under **Login Protection**, and then change the verification method.
- To change the login verification method of your account, go to the **Security Settings** page. On the **Critical Operations** tab, click **Change** next to **Login Protection**, and then change the verification method.

3.2 How Do I Disable Login Verification?

To ensure account security, you are advised to enable login verification.

After you enable this function, you and IAM users created using your account need to enter verification codes generated by the bound virtual MFA device, SMS verification codes, or email verification codes on the **Login Verification** page during login.

If you disable this function, you and the IAM users only need to enter the account name/username and password during login.

Disabling IAM User Login Verification as an Administrator

- An administrator can disable login verification for an IAM user on the IAM console as follows:

Step 1 In the navigation pane, choose **Users**.

Step 2 Click **Security Settings** in the row containing the target user.

Step 3 On the **Security Settings** tab page, click ✎ next to **Verification Method** under **Login Protection**, and select **Disabled**.

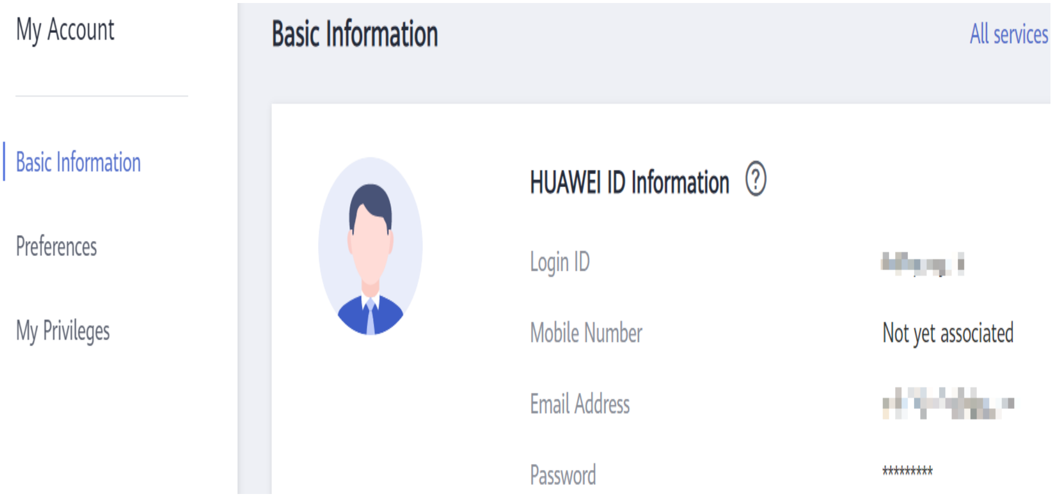
Step 4 Click **OK**.

----End

Disabling Administrator Login Verification

Check whether the current account is a HUAWEI ID or Huawei Cloud account by hovering over the login account name in the upper right corner and clicking **Basic Information** from the drop-down list. If **HUAWEI ID Information** is displayed in the **Basic Information** area, the current account is a HUAWEI ID. Otherwise, the current account is a Huawei Cloud account. Disable login verification for a HUAWEI ID by performing the operations described in **Disabling the login** verification function for a Huawei ID. Disable login verification for a Huawei Cloud account by performing the operations described in Disabling login verification for yourself (account administrator).

Figure 3-1 HUAWEI ID information



HUAWEI ID Information

Login ID	[redacted]
Mobile Number	Not yet associated
Email Address	[redacted]
Password	*********

- Disabling the login verification function for a HUAWEI ID

  Choose Huawei Account Center > **Account & Security** > **Security Verification** > **Two-step verification**, click **Disable**, and enter the verification information to disable login protection.

- Disabling login verification for yourself (account administrator) on the **Security Settings** page

Step 1 Hover the mouse pointer over the username in the upper right corner and choose **Security Settings** from the drop-down list.

Step 2 Click the **Critical Operations** tab, and click **Change** next to **Login Protection**.

Step 3 On the **Login Protection** page, select **Disable**.

Step 4 Click **OK**.

----End

3.3 How Do I Change the Verification Method for Performing Critical Operations?

Symptom

If operation protection is enabled, users under your account can proceed with a critical operation, such as deleting a resource and creating an access key, only after the users or the specified person completes verification.

The verification is valid for 15 minutes and you do not need to be verified again when performing critical operations within the validity period.

- To change the verification method from **Self-verification** to **Verification by another person**, see Self-verification.

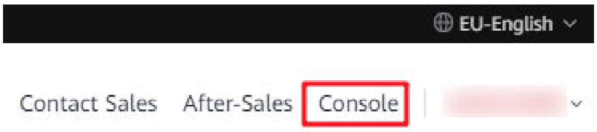
- To change the verification method from **Verification by another person** to **Self-verification** or to change the mobile number or email address for verification, see **Verification by another person.**

Procedure

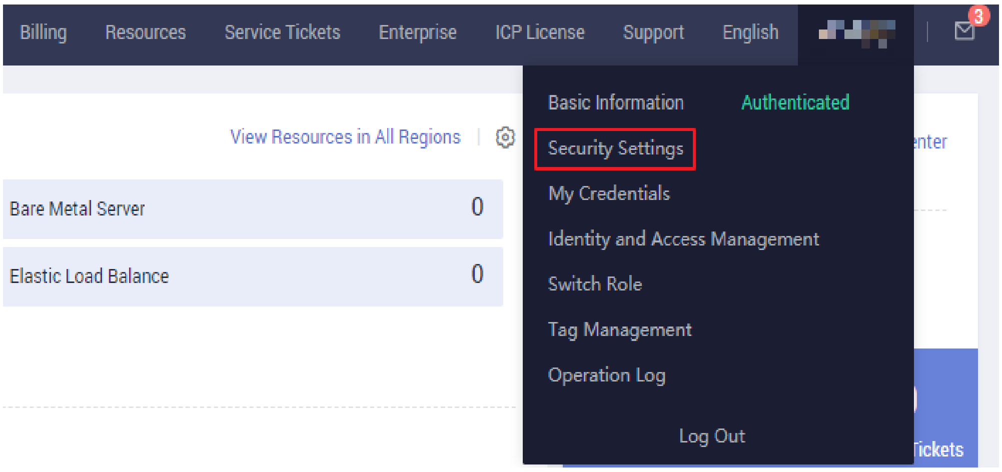
- **The current verification method is Self-verification.**

Step 1 Log in to the management console.

Figure 3-2 Logging in to the management console



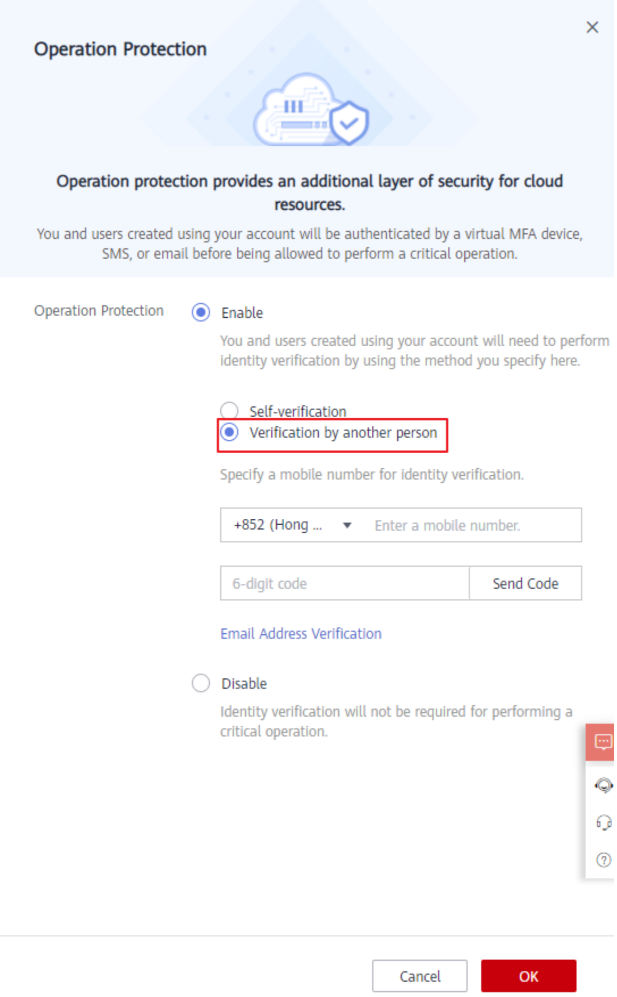
Step 2 On the management console, hover the mouse pointer over the username in the upper right corner, and choose **Security Settings** from the drop-down list.



Step 3 On the **Security Settings** page, click the **Critical Operations** tab, and click **Change** next to **Operation Protection**.

Step 4 On the **Operation Protection** page, select **Verification by another person**, enter the mobile number or email address for verification, and enter the verification code.

Figure 3-3 Operation protection settings



Operation Protection

Operation protection provides an additional layer of security for cloud resources.

You and users created using your account will be authenticated by a virtual MFA device, SMS, or email before being allowed to perform a critical operation.

Operation Protection ● Enable

You and users created using your account will need to perform identity verification by using the method you specify here.

○ Self-verification

● Verification by another person

Specify a mobile number for identity verification.

+852 (Hong ... Enter a mobile number.

6-digit code Send Code

Email Address Verification

○ Disable

Identity verification will not be required for performing a critical operation.

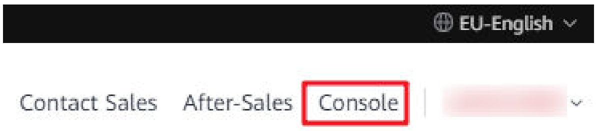
Step 5 Click **OK**.

----End

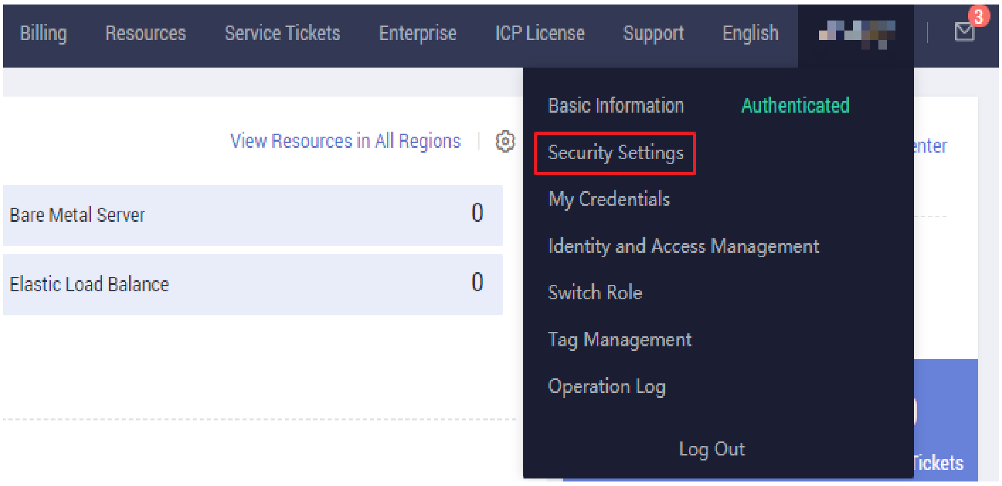
- **The current verification method is Verification by another person.**

Step 1 Log in to the management console.

Figure 3-4 Logging in to the management console



Step 2 On the management console, hover the mouse pointer over the username in the upper right corner, and choose **Security Settings** from the drop-down list.



Step 3 On the **Security Settings** page, click the **Critical Operations** tab, and click **Change** next to **Operation Protection**.

Step 4 On the **Operation Protection** page, select **Disable** and click **OK**. Enter the verification code and click **OK**.

Step 5 On the **Critical Operations** tab page, click **Enable** next to **Operation Protection**.

Step 6 On the **Operation Protection** page, select **Self-verification** or **Verification by another person**.

If you select **Verification by another person**, complete verification to ensure that the verification method is available.

- **Self-verification**: You or IAM users themselves perform verification when performing a critical operation.
- **Verification by another person**: The specified person performs verification when you or an IAM user performs a critical operation. Only SMS and email verification is supported.

Step 7 Click **OK**.

----End

3.4 How Do I Disable Operation Protection?

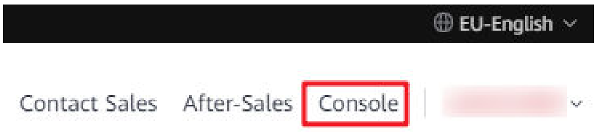
Symptom

If operation protection is enabled, users under your account can proceed with a critical operation (such as deleting a resource and creating an access key) only after the users or the specified person completes verification. To disable operation protection, perform the following procedure.

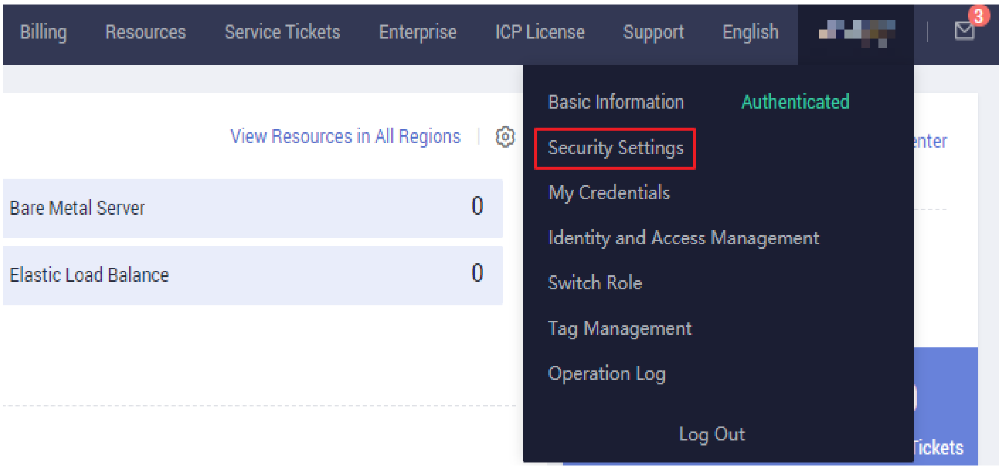
Procedure

Step 1 Log in to the management console.

Figure 3-5 Logging in to the management console



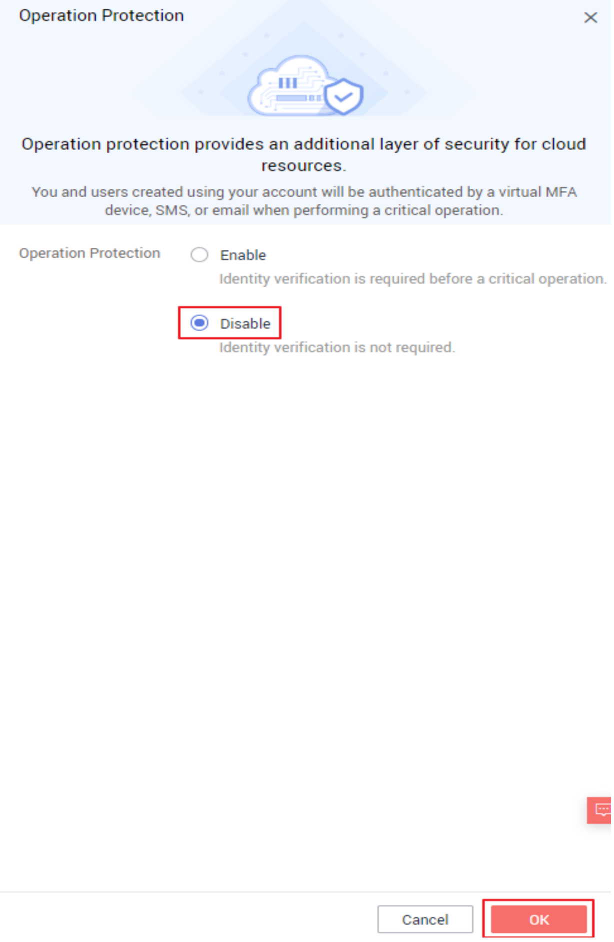
Step 2 On the management console, hover the mouse pointer over the username in the upper right corner, and choose **Security Settings** from the drop-down list.



Step 3 On the **Security Settings** page, click the **Critical Operations** tab, and click **Change** next to **Operation Protection**.

Step 4 Select **Disable** and click **OK**. Enter the verification code and click **OK**.

Figure 3-6 Disabling operation protection



Operation Protection

Operation protection provides an additional layer of security for cloud resources.

You and users created using your account will be authenticated by a virtual MFA device, SMS, or email when performing a critical operation.

Operation Protection ○ Enable
Identity verification is required before a critical operation.

● Disable
Identity verification is not required.

----End

3.5 How Do I Bind a Virtual MFA Device?

Multi-factor authentication (MFA) adds an extra layer of protection on top of your username and password. After MFA authentication is enabled, you need to enter verification codes after your username and password are authenticated. MFA, together with your username and password, ensures the security of your account and resources.

MFA devices can be based on hardware or software. However, IAM supports only virtual MFA devices.

A virtual MFA device is an application that generates 6-digit codes in compliance with the Time-Based One-Time Password Algorithm (TOTP). MFA applications can run on mobile devices (including smartphones) and are easy to use.

Prerequisites

You have installed an MFA application (for example, Google Authenticator) on your mobile phone.

Procedure

- **Huawei Cloud account or IAM user**

Step 1 On the management console, hover the mouse pointer over the username in the upper right corner, and choose **Security Settings** from the drop-down list.

Step 2 On the **Critical Operations** tab, click **Bind** next to **Virtual MFA Device**.

Step 3 Set up the MFA application by scanning the QR code or entering the secret key.

- Scan the QR code

  Open the MFA application on your mobile phone, and use the application to scan the QR code displayed on the **Bind Virtual MFA Device** page. Your account is then added to the application.

- Enter the secret key

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

NOTE

To ensure that you can perform MFA-based verification successfully, confirm that you have enabled the automatic time setup option on your mobile phone.

Step 4 View the verification code on the MFA application. The code is automatically updated every 30 seconds.

Step 5 On the **Bind Virtual MFA Device** page, enter two consecutive verification codes and click **OK**.

----End

- **HUAWEI ID**

Step 1 On the management console, hover the mouse pointer over the username in the upper right corner, and choose **Security Settings** from the drop-down list.

Step 2 Click the **Critical Operations** tab, and click **Bind** next to **Virtual MFA Device**.

Step 3 On the HUAWEI ID website, choose **Account & security**, and bind a virtual MFA device in the **Security verification** area.

----End

Related FAQs

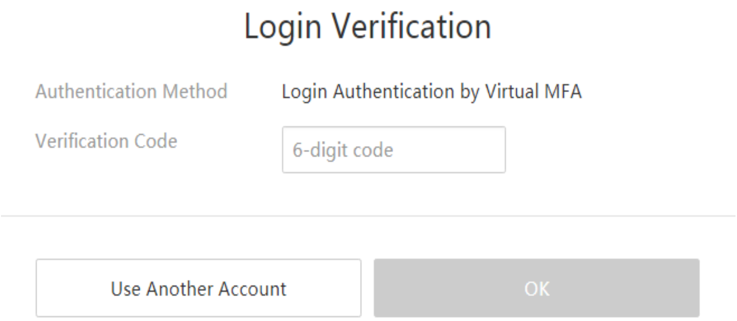
How Do I Obtain a Virtual MFA Verification Code?

How Do I Unbind or Remove a Virtual MFA Device?

Why Does MFA Authentication Fail?

3.6 How Do I Obtain a Virtual MFA Verification Code?

If you enable virtual MFA–based login protection or operation protection, you need to provide MFA verification codes when you log in to the cloud platform or perform a critical operation. The following figure shows the login verification page.



Open the bound MFA application and view the verification codes displayed for your account.

NOTE

If the verification fails, resolve the problem by referring to **Why Does MFA Authentication Fail?**

3.7 How Do I Unbind or Remove a Virtual MFA Device?

- If the virtual MFA device bound to your account is available, you can unbind the MFA device by referring to **Unbinding a Virtual MFA Device**.
- If the virtual MFA device bound to your account is unavailable, you cannot unbind the MFA device, but you can remove it by referring to **Removing the Virtual MFA Device**.

IAM users can bind another virtual MFA device on the **Security Settings** page. For details, see **How Do I Bind a Virtual MFA Device?**

Unbinding a Virtual MFA Device

1. Log in to the management console.
2. Hover the mouse pointer over the username in the upper right corner and choose **Security Settings** from the drop-down list.
3. On the **Critical Operations** tab, click **Unbind** next to **Virtual MFA Device**.

   NOTE

   If you have upgraded your Huawei Cloud account to a HUAWEI ID, you will be redirected to **Account & security** of the HUAWEI ID website. In the **Security verification** area, click **Disassociate** in the **Authenticator** row.
4. Enter verification codes generated by the MFA application.
5. Click **OK**.

Removing the Virtual MFA Device

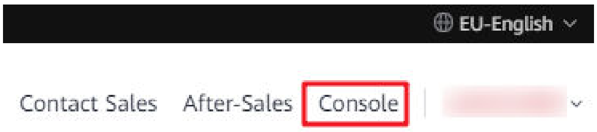
- Huawei Cloud account or HUAWEI ID: If your mobile phone is unavailable or the bound virtual MFA device has been deleted from your phone, **submit a**

service ticket by choosing **Identity and Access Management** > **Security Settings** to remove the virtual MFA device from your account.

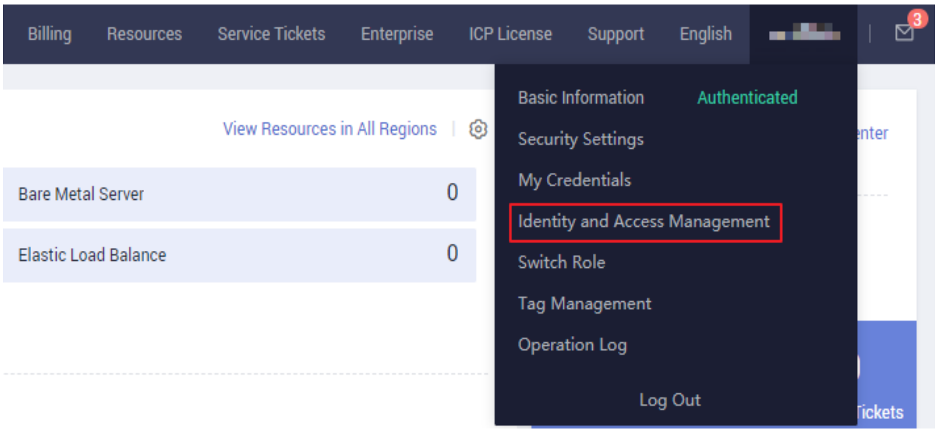
- IAM user: If your mobile phone is unavailable or the bound virtual MFA device has been deleted from your phone, request the **administrator** to remove the virtual MFA device. The procedure of removing a virtual MFA device is as follows:

1. Log in to the management console.

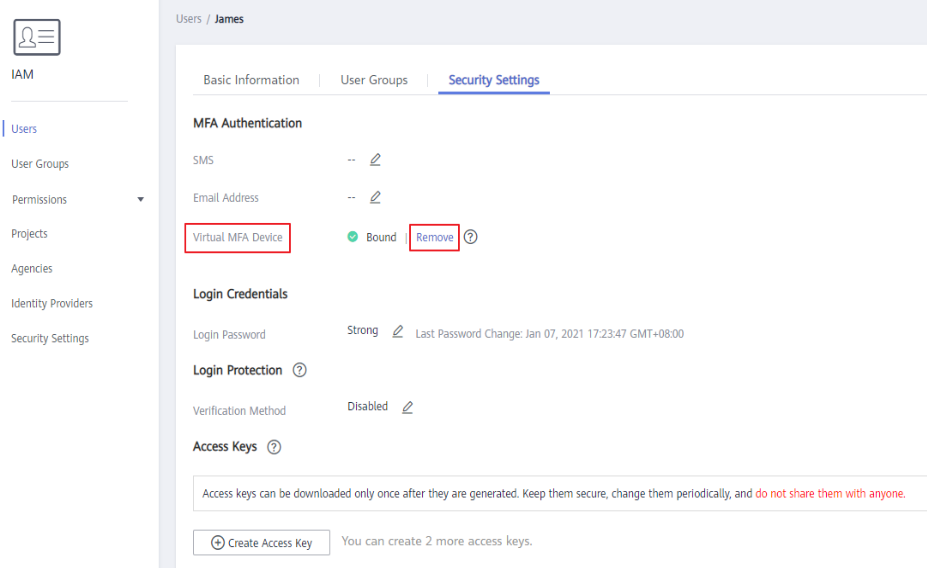
Figure 3-7 Logging in to the management console



2. On the management console, hover the mouse pointer over the username in the upper right corner, and choose **Identity and Access Management** from the drop-down list.



3. Log in to the IAM console.
4. On the **Users** page, click **Security Settings** on the right of the target user.
5. On the **Security Settings** tab page, click **Remove** next to **Virtual MFA Device**.



MFA Authentication

SMS --

Email Address --

Virtual MFA Device Bound | Remove

Login Credentials

Login Password Strong Last Password Change: Jan 07, 2021 17:23:47 GMT+08:00

Login Protection

Verification Method Disabled

Access Keys

Access keys can be downloaded only once after they are generated. Keep them secure, change them periodically, and do not share them with anyone.

You can create 2 more access keys.

6. Click **Yes**.

3.8 Why Does MFA Authentication Fail?

Symptom

MFA authentication fails when you log in or perform a critical operation, or bind or unbind a virtual MFA device.

Possible Causes

- The verification codes are incorrect.
- The verification codes have expired.
- The verification codes belong to another account.
- When you bound a virtual MFA device again after unbinding the previous one, you did not add your account to the MFA device.
- The generation of MFA verification codes is subject to the time. If the time difference between your mobile phone and the virtual MFA device is greater than 30 seconds, the MFA verification codes generated on your mobile phone will fail the verification.

Solutions

- Enter the correct verification codes.
- The verification codes are automatically updated every 30 seconds. Enter two consecutive verification codes.
- Ensure that the account name displayed above the verification code on the authenticator is the same as the name of the account used to request MFA authentication.
- To bind a virtual MFA device again, delete your account information in the MFA device, and then add your account to it.
- Ensure that the time on your mobile phone is the same as the time on the virtual MFA device, and try again. (You do not need to consider the time zone on your mobile phone, because the MFA authentication will be based on UTC time.)

3.9 Why Am I Not Getting the Verification Code?

When you bind or change the mobile number or email address or reset the password, you need to obtain a verification code for authentication. If you cannot obtain the code, perform the operations described in this section.

Why Am I Not Getting the SMS Verification Code?

- Check whether the mobile number you entered is correct. If it is incorrect, enter the correct mobile number and try again.
- Check whether your mobile service has been suspended due to arrears. If it has been suspended, clear the outstanding amount and try again after your

mobile service is resumed. You can also change the mobile number associated with your account.

- Check whether the SMS containing the verification code has been filtered or blocked as a junk message. If this happens, disable the SMS message filtering or blocking function.

  NOTE

  Check whether there are messages containing a verification code sent by HUAWEI CLOUD in junk or spam messages.

- In some scenarios, SMS messages may not be delivered due to network issues. In this case, send a verification code again or try again later. Alternatively, install the SIM card in another phone and try again.

If the fault persists after you perform the preceding operations, try email or virtual MFA verification.

If both your mobile phone and email address cannot receive the verification code, contact customer service.

Why Am I Not Getting the Email Verification Code?

- Check whether the email address you entered is correct. If it is incorrect, enter the correct email address and try again.
- Check whether your mailbox is normal and check the junk mail folder.
- Add the following email addresses to the whitelist: **noreplyhk01@mail01.huawei.com** and **noreplydl01@mail01.huawei.com**.
- Mails may not be delivered due to network issues. In this case, send a verification code again or try again later.

If the fault persists after you perform the preceding operations, try SMS or virtual MFA verification.

If both your mobile phone and email address cannot receive the verification code, contact customer service.

3.10 Why Is My Account Locked?

Symptom

- When you log in to the system, a message is displayed, indicating that your account is locked and can be used to log in again after 15 minutes.
- When you call an API (such as the API used to **obtain a user token**) whose request parameters include a password, the following response is displayed:

```
{
   "error": {
      "code": 401,
      "message": "The account is locked.",
      "title": "Unauthorized"
   }
}
```

Possible Causes

Your account is locked for 15 minutes due to security exceptions, for example, you have entered incorrect passwords multiple times, or the account has been frequently used for login from different locations.

Solutions

- If your account is locked due to misoperations, wait for 15 minutes and try again. Do not log in or enter the password within this period.
- If you have forgotten your login password, reset it. For details, see **What Should I Do If I Forgot My Password?**
- If the account is locked for no reason, change the password. For details, see **How Do I Change My Password?**

3.11 Why Doesn't My API Access Control Policy Take Effect?

Symptom

You have set an API access control policy, but IAM users who do not meet the policy requirements can still access Huawei Cloud using APIs.

Solutions

1. The API access control policy has not taken effect yet.

   API access control policies take effect within **2 hours** once set.

2. API access control is not supported in your current region.

   Currently, API access control is not supported in **CN North-Beijing4**. You can switch to another region.

   NOTE

   The API for obtaining an IAM user token (using a password) is not affected by the API access control policy.

3. API access control does not take effect for OBS.

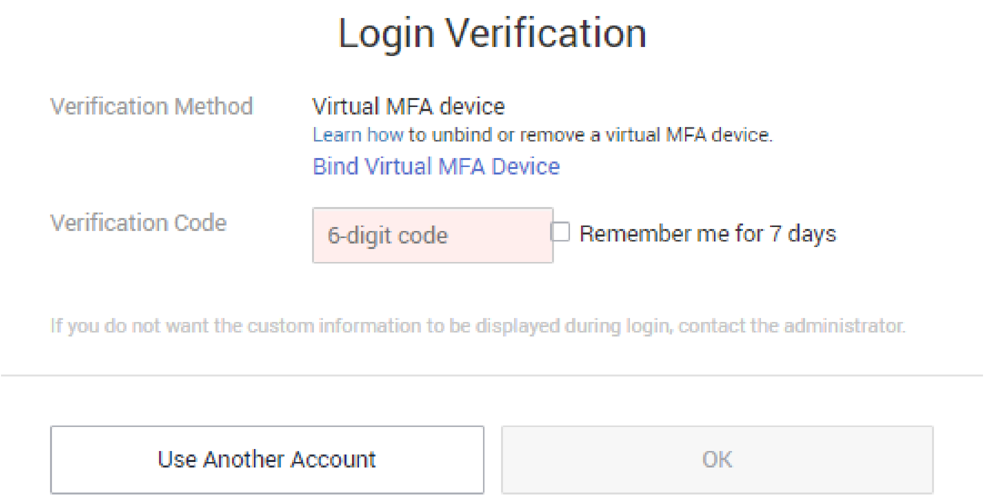
   OBS does not support API access control policies. To restrict access to OBS resources, see **Restricting Bucket Access to Specified IP Addresses**.

If none of the preceding scenarios apply, modify your API access control policy. If the policy still does not take effect, **submit a service ticket** by choosing **Identity and Access Management** > **Account Security Settings** and specifying "API access control".

3.12 Why Do I Still Need to Perform MFA During Login After Unbinding the Virtual MFA Device?

Symptom

You have unbound or removed the virtual MFA device, but you still need to verify your identity through MFA when logging to Huawei Cloud.



Login Verification

Verification Method: Virtual MFA device
Learn how to unbind or remove a virtual MFA device.
Bind Virtual MFA Device

Verification Code: 6-digit code □ Remember me for 7 days

If you do not want the custom information to be displayed during login, contact the administrator.

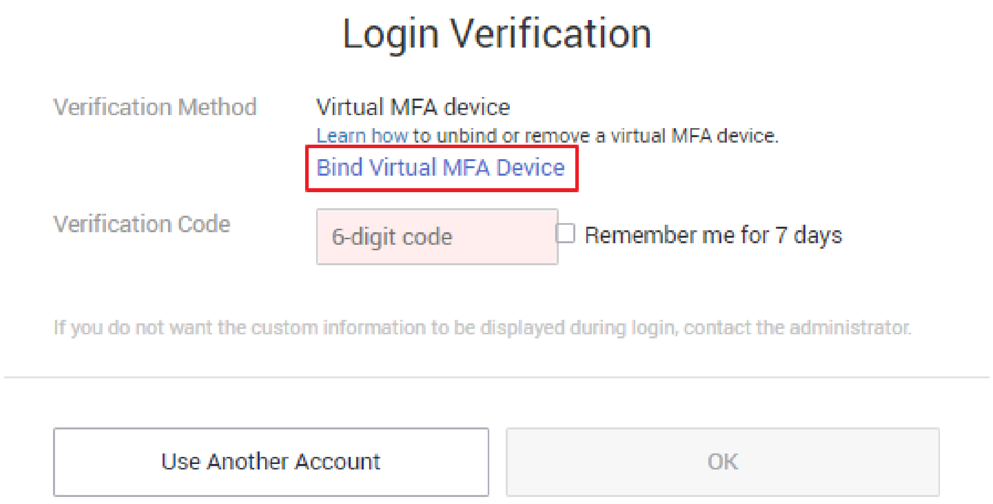
Possible Causes

Although the virtual MFA device has been unbound or removed, the login protection is still enabled. Login verification is still required.

Solutions

- When logging in to Huawei Cloud, bind a virtual MFA device again and use it to verify your identity.

  Click **Bind Virtual MFA Device** in the **Login Verification** dialog box. For details, see **How Do I Bind a Virtual MFA Device?**.



Login Verification

Verification Method: Virtual MFA device

Learn how to unbind or remove a virtual MFA device.

Bind Virtual MFA Device

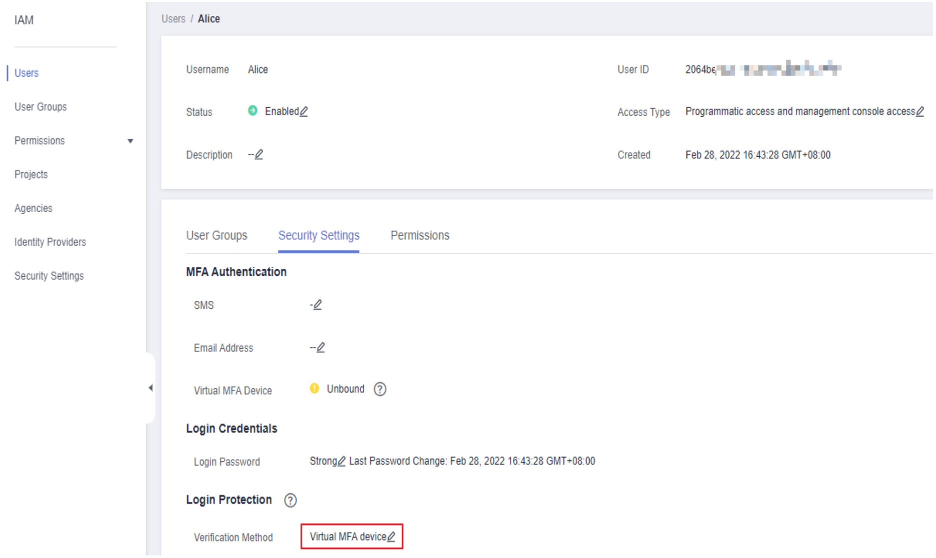
Verification Code: 6-digit code □ Remember me for 7 days

If you do not want the custom information to be displayed during login, contact the administrator.

- If you are an IAM user, request the administrator to change your login verification mode to mobile number or email address, and then log in again.

  If you are an administrator, log in to the IAM console, click the username to go to the user details page, and change the login verification mode on the **Security Settings** tab page.

Figure 3-8 Virtual MFA authentication



Username	Alice	User ID	2064b6[redacted]
Status	Enabled	Access Type	Programmatic access and management console access
Description	--	Created	Feb 28, 2022 16:43:28 GMT+08:00

MFA Authentication

SMS: -

Email Address: --

Virtual MFA Device: Unbound

Login Credentials

Login Password: Strong Last Password Change: Feb 28, 2022 16:43:28 GMT+08:00

Login Protection

Verification Method: Virtual MFA device

4 Passwords and Credentials

4.1 What Should I Do If I Forgot My Password?

If you are an IAM user and forgot your password, reset the password by referring to **Resetting the Password of an IAM User**.

If you forgot the password of your account, reset the password by referring to **Resetting the Password of an Account**.

📖 NOTE

This section describes how to retrieve the password of an IAM user, Huawei Cloud account, or HUAWEI ID.

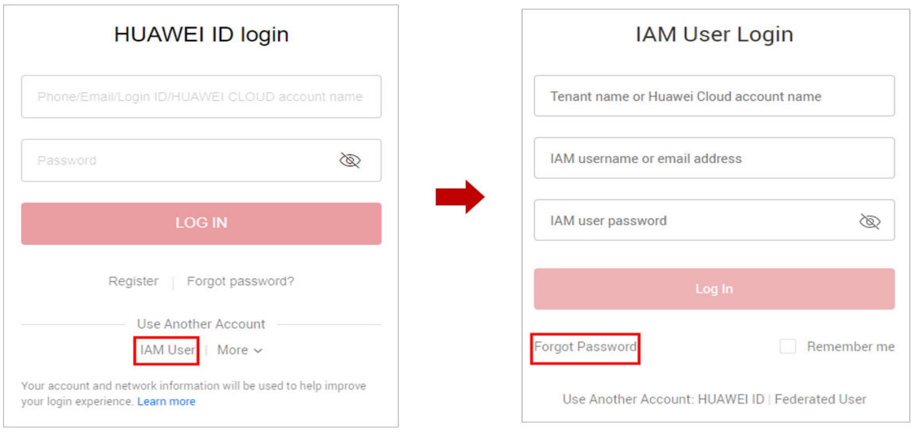
If an error message is displayed indicating that the account is invalid or not supported during password retrieval, this means the account is not an IAM user, Huawei Cloud account, or HUAWEI ID. Check whether the entered account name is correct. If you do not have a HUAWEI ID, create one and use it to enable Huawei Cloud services. For details, see **Registering a HUAWEI ID and Enabling Huawei Cloud Services**.

Resetting the Password of an IAM User

If you are an IAM user and have not bound an email address or mobile number, you cannot change the password by yourself. You need to contact the administrator to **reset your password**.

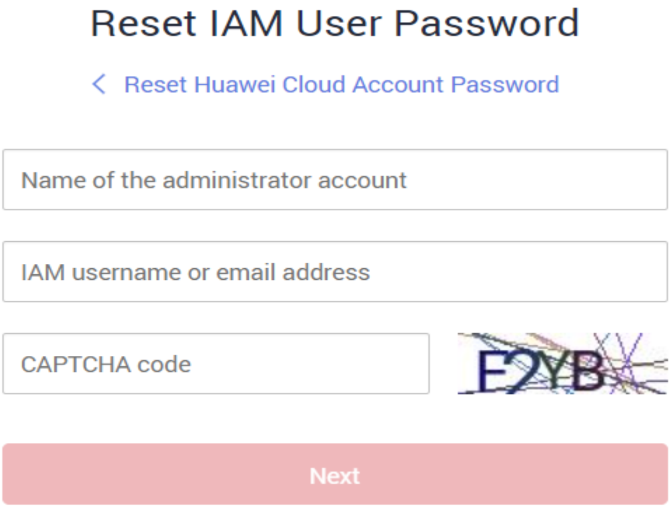
Step 1 On the HUAWEI ID login page, click **IAM User**. On the displayed login page, click **Forgot Password**.

Figure 4-1 IAM user login page


HUAWEI ID login
Phone/Email/Login ID/HUAWEI CLOUD account name
Password
LOG IN
Register | Forgot password?
Use Another Account
IAM User | More
Your account and network information will be used to help improve your login experience. Learn more
IAM User Login
Tenant name or Huawei Cloud account name
IAM username or email address
IAM user password
Log In
Forgot Password
Remember me
Use Another Account: HUAWEI ID | Federated User

Step 2 Enter the administrator account, IAM username or email address, and verification code.

Figure 4-2 Resetting IAM user password


Reset IAM User Password
Reset Huawei Cloud Account Password
Name of the administrator account
IAM username or email address
CAPTCHA code
E2YB
Next

NOTE

- Account: Created upon successful registration with Huawei Cloud. The account has full access permissions for all of its cloud services and resources and makes payments for the use of these resources. After account login, you will see the account marked **Enterprise administrator** on the **Users** page.
- IAM user: Created using your account. IAM users can log in to Huawei Cloud using the account name, username, and password, and then use resources based on assigned permissions. IAM users do not own resources and cannot make payments.
- If you are an IAM user and have not bound an email address or mobile phone number to your account, ask the administrator to reset your password. For details, see **Changing the Login Password of an IAM User**.

Step 3 Select a verification method, enter the verification code, and click **Next**.

NOTE

- Ensure that the mobile number or email address you entered is correct, or the password cannot be reset.
- If you do not receive the verification code, see **Why Am I Not Getting the Verification Code?**

Step 4 Enter a new password, confirm it, and click **OK**.

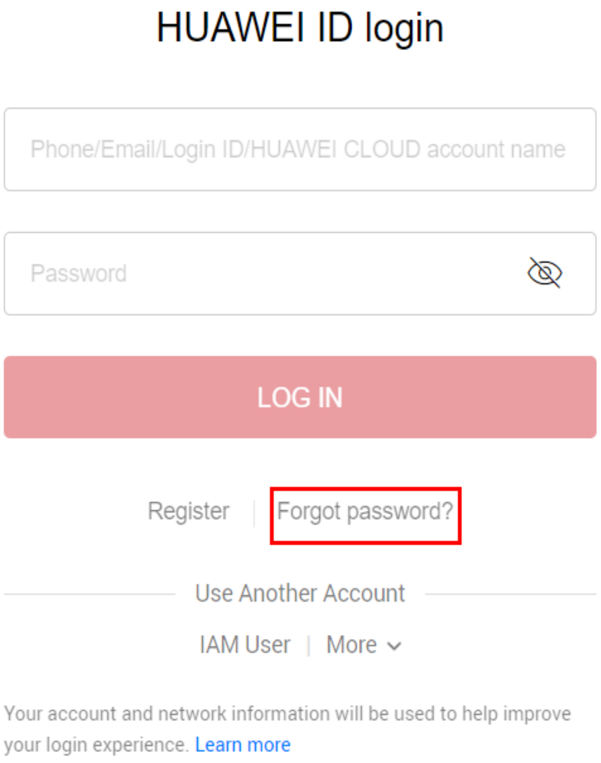
Step 5 Click **Log In** or wait to be redirected to the login page and use the new password to log in.

----End

Resetting the Password of an Account

Step 1 On the login page, click **Forgot password**.

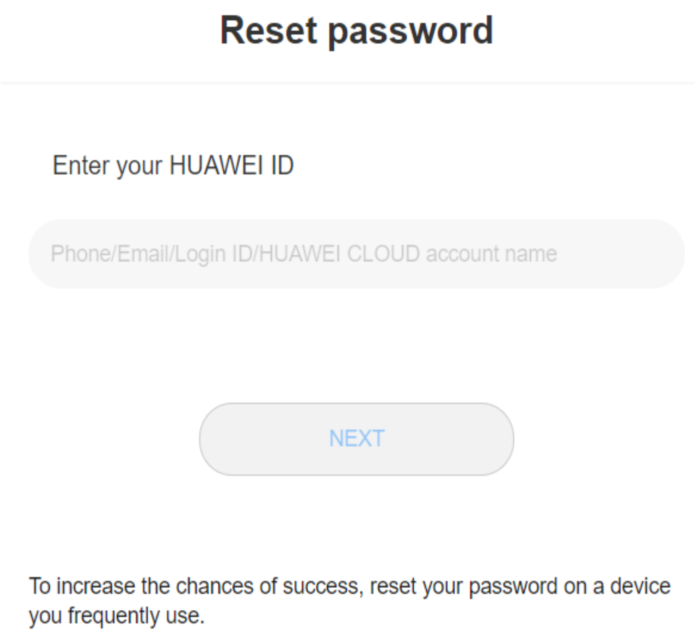
Figure 4-3 Resetting the HUAWEI ID password



HUAWEI ID login
Phone/Email/Login ID/HUAWEI CLOUD account name
Password
LOG IN
Register
Forgot password?
Use Another Account
IAM User
More
Your account and network information will be used to help improve your login experience. Learn more

Step 2 Enter your login ID, the mobile number, or the email address used to create your HUAWEI ID, and click **NEXT**.

Figure 4-4 Resetting the password



Reset password

Enter your HUAWEI ID

To increase the chances of success, reset your password on a device you frequently use.

Step 3 Get the verification code in step **Step 2**.

Step 4 Enter the verification code and click **NEXT**.

NOTE

- If you do not receive the verification code, see **Why Am I Not Getting the Verification Code?**
- For Huawei Cloud accounts, if the mobile number is unavailable, contact customer service at +86 4000-955988 (Chinese Mainland) or +85 2800-931122 (Hong Kong, China), or **submit a service ticket**.
- For HUAWEI IDs, if the mobile number or email address is unavailable, **change the mobile number or email address bound to your HUAWEI ID** first and then use the new mobile number or email address to reset the password.

Step 5 (Optional) Reset the password of a HUAWEI ID using either of the following methods:

- Register a HUAWEI ID on the official Petal Mail website for free. After the registration is complete, the phone number will be used as your security phone number.

  ⚠ CAUTION

  The newly registered account cannot use the resources of the original HUAWEI ID account.

- Reset the password of the original HUAWEI ID account.
  a. If the password is to be reset on a non-frequently used device, verification is required. Select an appropriate verification method and click **NEXT**.
  b. Fill in the following information for verification:

- Phone number real-name information
- Security information
  - Basic information
  - Historical information
  - Device information

Then, submit the information for verification. If the password still cannot be reset, **change your account**. The results will be sent to you by SMS. If the appeal is approved, **reset the password** within 24 hours.

Step 6 Enter a new password, confirm it, and click **OK**.

Step 7 (Optional) Reset the password of a HUAWEI ID by adding MFA to the HUAWEI ID account. For details, see **MFA Authentication and Virtual MFA Device**.

Step 8 Click **RETURN NOW** and use the new password to **log in to Huawei Cloud**.

----End

4.2 How Do I Change My Password?

- If you remember your password and want to change it, do as follows:
  - **Huawei Cloud account**: Change the password on the **Basic Information** page of My Account.
  - **HUAWEI ID**: Change the password on HUAWEI Account center. To do so, go to the **Basic Information** page of My Account, and click **Manage** next to **HUAWEI ID Information**. You are automatically redirected to the **Account & security** page of HUAWEI Account center. Reset the password in the **Security center** area.
  - **IAM user**: Hover the mouse pointer over the username in the upper right corner of the console and choose **Security Settings**. Then change the password on the **Basic Information** tab.
- If you have forgotten your password:
  - Reset your password by following the instructions in **What Should I Do If I Forgot My Password?**
  - If you are an IAM user and have not bound any email address or mobile number to your account, **request the administrator to reset your password**.

4.3 How Do I Obtain an Access Key (AK/SK)?

- If you have a password for logging in to the management console, log in to the console, move the pointer to the username in the upper right corner and select **My Credentials** from the drop-down list. Choose **Access Keys** in the left navigation pane and you can view the access key ID (AK) in the access key list. You can obtain the secret access key (SK) from the downloaded .csv file. For more information, see **Access Keys**.

- If you do not a password for logging in to the management console, request the administrator to create an access key for you on the IAM console. For more information, see **Managing Access Keys for an IAM User**.

4.4 What Should I Do If I Have Forgotten My Access Key (AK/SK)?

If you have forgotten your original access key, create a new access key and use it to replace the original in-use access key. Ensure that services are not affected and then delete or disable the original access key. For details, see **Access Keys**.

NOTE

- Each IAM user can create a maximum of two access keys. The quota cannot be increased.
- If you are an IAM user, move the pointer to the account name 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 IAM users who have been granted the required permissions can manage access keys.
- If you cannot manage your access keys:
  - Request the **administrator** to manage your access keys. For details, see **Managing Access Keys for an IAM User**.
  - Request the **administrator** to assign required permissions to you or disable access key management. For details, see **Assigning Permissions to an IAM User** or **Access Key Management**.

4.5 What Are Temporary Security Credentials (AK/SK and Security Token)?

Temporary Security Credentials

Temporary security credentials include temporary access keys (AK/SK) and security tokens. They only have **temporary access permissions** and are slightly different from permanent security credentials.

Differences Between Temporary and Permanent Security Credentials

The following table provides the differences between the two types of security credentials.

Table 4-1 Credential differences

Item	Temporary Credentials	Permanent Credentials
Validity period	15 minutes to 24 hours	Unlimited validity

Item	Temporary Credentials	Permanent Credentials
Number of credentials	Unlimited	2 credentials for each IAM user
Obtaining method	Call the API used to **obtain a temporary access key**.	Create an access key on the **My Credentials** page.
Usage	Cannot be embedded into applications or stored for later use, and must be obtained again after expiration.	N/A

Advantages of Temporary Security Credentials

Temporary security credentials are useful to grant federated users only required permissions with a specific validity period.

Usage of Temporary Security Credentials

An access key must be used together with a security token. When you use temporary security credentials for authentication, add the **x-security-token** field to the request header. For details, see **API Request Signing Guide**.

4.6 How Do I Obtain a Token with Security Administrator Permissions?

A token is an access credential issued to an IAM user to bear its identity and permissions. When calling the APIs of IAM or other cloud services, you can use this API to obtain a user token for authentication.

Permissions of a token are determined by permissions of the user who obtains the token. Only users who have been assigned the **Security Administrator** role can obtain a token with **Security Administrator** permissions.

Methods

- Account administrator: Create an IAM user, assign the **Security Administrator** role to the user, and then call the API used to **obtain a user token**. The obtained token has the **Security Administrator** permissions.
- IAM user: Request the administrator to assign you the **Security Administrator** role, and then obtain a token.

Security Administrator Permissions

Table 4-2 Security administrator permissions

Permission Name	Scope	Description
Security Administrator	Global	Administrator permissions for IAM, including but not limited to the following permissions: ● Creating, modifying, and deleting IAM users ● Creating, modifying, and deleting user groups, and granting them permissions ● Creating, modifying, and deleting custom policies ● Creating and modifying projects ● Creating, modifying, and deleting agencies ● Creating, modifying, and deleting identity providers ● Configuring account security settings

4.7 How Do I Obtain an Access Key (AK/SK) in the Cloud Alliance Regions?

Symptom

The administrator has enabled the **CN-Hong Kong**, **AP-Singapore**, **CN East-Shanghai1**, **LA-Sao Paulo1**, **LA-Mexico City1**, **LA-Mexico City2**, **AF-Johannesburg**, or **LA-Santiago** cloud alliance region. The account and IAM users need to use access keys for encryption and signing in the selected region.

Users access cloud services in the cloud alliance region as virtual users authorized through federated authentication. They are not real users who exist in the cloud service system, and need to obtain an access key in Huawei Cloud's default regions and the **CN-Hong Kong**, **AP-Singapore**, **CN East-Shanghai1**, **LA-Sao Paulo1**, **LA-Mexico City1**, **LA-Mexico City2**, **AF-Johannesburg**, or **LA-Santiago** cloud alliance region, respectively.

The procedure below guides you through creating a permanent access key for yourself as an administrator or for your IAM users. Both you and your IAM users can create temporary access keys on the **My Credentials** page.

Procedure

Step 1 Create an IAM user in the **CN-Hong Kong**, **AP-Singapore**, **CN East-Shanghai1**, **LA-Sao Paulo1**, **LA-Mexico City1**, **LA-Mexico City2**, **AF-Johannesburg**, or **LA-Santiago** cloud alliance region as an administrator. To create an access key for yourself, go to **Step 2**.

1. Log in to Huawei Cloud as an administrator, click 📍 on the console homepage, and select the **CN-Hong Kong**, **AP-Singapore**, **CN East-**

Shanghai1, **LA-Sao Paulo1**, **LA-Mexico City1**, **LA-Mexico City2**, **AF-Johannesburg**, or **LA-Santiago** region.

2. On the console, in the selected region, choose **Management & Governance** > **Identity and Access Management**.
3. In the navigation pane of the IAM console, choose **Users**.
4. Click **Create User** in the upper right corner.
5. On the **Create User** page, set user information. For details, see **Creating an IAM User**.

   To identify the entity that uses an access key, create an IAM user with the same name as the corresponding IAM user or your account.
6. Click **OK**.

Step 2 Obtain an access key for the IAM user.

1. Log in to the IAM console as an administrator and select the **CN-Hong Kong**, **AP-Singapore**, **CN East-Shanghai1**, **LA-Sao Paulo1**, **LA-Mexico City1**, **LA-Mexico City2**, **AF-Johannesburg**, or **LA-Santiago** cloud alliance region.
2. On the **Users** page of the IAM console, click **Security Settings** in the **Operation** column of the row that contains the IAM user created in **1**.
3. On the **Security Settings** tab of the IAM user details page, click **Create Access Key**.
4. (Optional) Enter a description for the access key.
5. Click **OK**. The access key is created.
6. Download the access key file.

   NOTE

   - Each user can have a maximum of two access keys with unlimited validity. To ensure account security, keep them properly.
   - The administrator and IAM users can use the access key only in the **CN-Hong Kong**, **AP-Singapore**, **CN East-Shanghai1**, **LA-Sao Paulo1**, **LA-Mexico City1**, **LA-Mexico City2**, **AF-Johannesburg**, or **LA-Santiago** cloud alliance region.
7. (Optional) Provide the access key to the IAM user.

----End

5 Project Management

5.1 What Are the Differences Between IAM and Enterprise Management?

Enterprise Management enables enterprises to manage cloud resources by project and organization level. It includes enterprise project, accounting, application, and personnel management. IAM is an identity management service that provides identity authentication, permissions management, and access control.

You can use both IAM and Enterprise Management to manage users and access permissions. Enterprise Management also allows accounting and application management, and supports more fine-grained authorization for resource usage. It is recommended for medium- and large-sized enterprises. For more information about Enterprise Management, see **Enterprise Management User Guide**.

Differences Between IAM and Enterprise Management

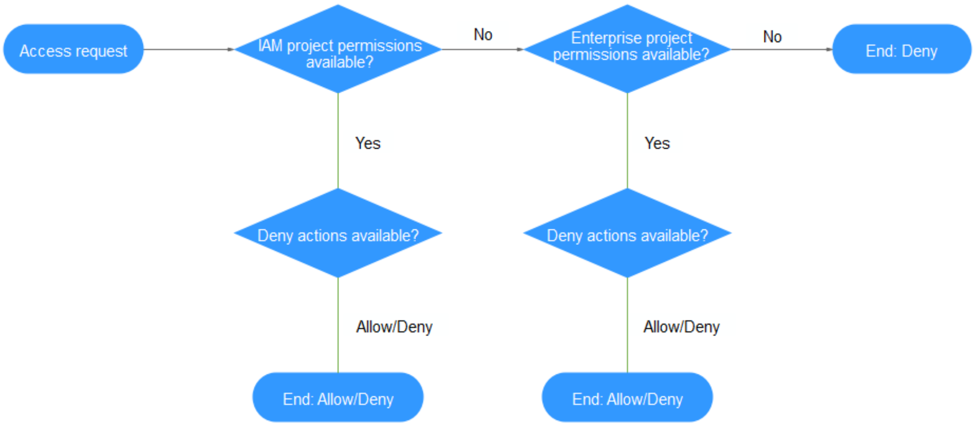
- Enabling method
  - IAM is free of charge and you can use it immediately after you register with Huawei Cloud.
  - Enterprise Management is a resource management service on Huawei Cloud. After registering with the system, you need to apply for enabling Enterprise Management. For details, see **Enabling Enterprise Center**.
- Resource isolation
  - Using IAM, you can create multiple projects in a region to isolate resources, and authorize users to access resources in specific projects. For details, see **Projects**.
  - Using Enterprise Management, you can create enterprise projects to isolate resources across regions. Enterprise Management makes it easy for you to assign permissions for specific cloud resources. For example, you can add an Elastic Cloud Server (ECS) to an enterprise project, and assign permissions to a user for managing the ECS in the project. The user then can manage only this ECS.
- Supported services

- For details about services supported by IAM, **Supported Cloud Services**.
- For details about services supported by Enterprise Management, see **Supported Cloud Services**.

Authentication Process

When a user initiates an access request, the system authenticates the request based on the actions in the policies attached to the group to which the user belongs. The following figure shows the authentication process.

Figure 5-1 Request authentication process



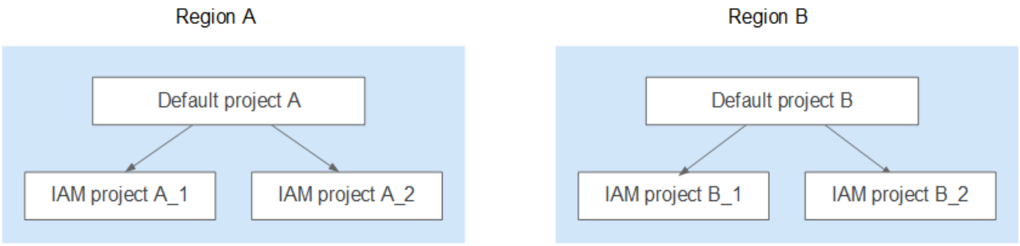
1. A user initiates an access request.
2. The system searches for IAM project permissions and then searches for matched actions in the permissions.
3. If a matched Allow or Deny action is found, the system returns an authentication result (Allow or Deny). Then the authentication is completed.
4. If no matched actions are found in IAM project permissions, the system continues to search for enterprise project permissions and matched actions.
5. If a matched Allow or Deny action is found, the system returns an authentication result (Allow or Deny). Then the authentication is completed.
6. If no matched actions are found, the system returns a Deny. Then the authentication is completed.

5.2 What Are the Differences Between IAM Projects and Enterprise Projects?

IAM Projects

IAM projects can group and physically isolate resources. Resources cannot be transferred between IAM projects, but can only be deleted and then created or purchased again.

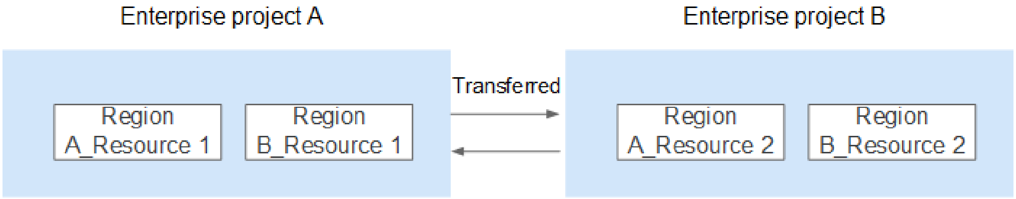
For details about IAM projects, see **Projects**.



Enterprise Projects

Enterprise projects can group and logically isolate resources. An enterprise project can contain resources from different regions, and resources can be transferred between enterprise projects. Enterprise Management makes it easy for you to assign permissions for specific cloud resources. For example, you can add an Elastic Cloud Server (ECS) to an enterprise project, and assign permissions to a user for managing the ECS in the project. The user then can manage only this ECS. You cannot create projects in IAM after enabling Enterprise Management.

For details about enterprise projects, see **Creating an Enterprise Project**.



5.3 What Are the Differences Between IAM Users and Enterprise Member Accounts?

IAM Users

IAM users are created using an account in IAM or Enterprise Management (**User Management** page). They are managed and granted permissions by the account. **Bills generated by the IAM users' use of resources are paid by the account.**

In an enterprise, if there are multiple employees who need to use the resources purchased from Huawei Cloud through an account, the account can be used to create IAM users for these employees and assign permissions to the users for using resources. The IAM users have their own passwords for accessing the resources under the account.

For details about how to create an IAM user, see **Creating an IAM User**.

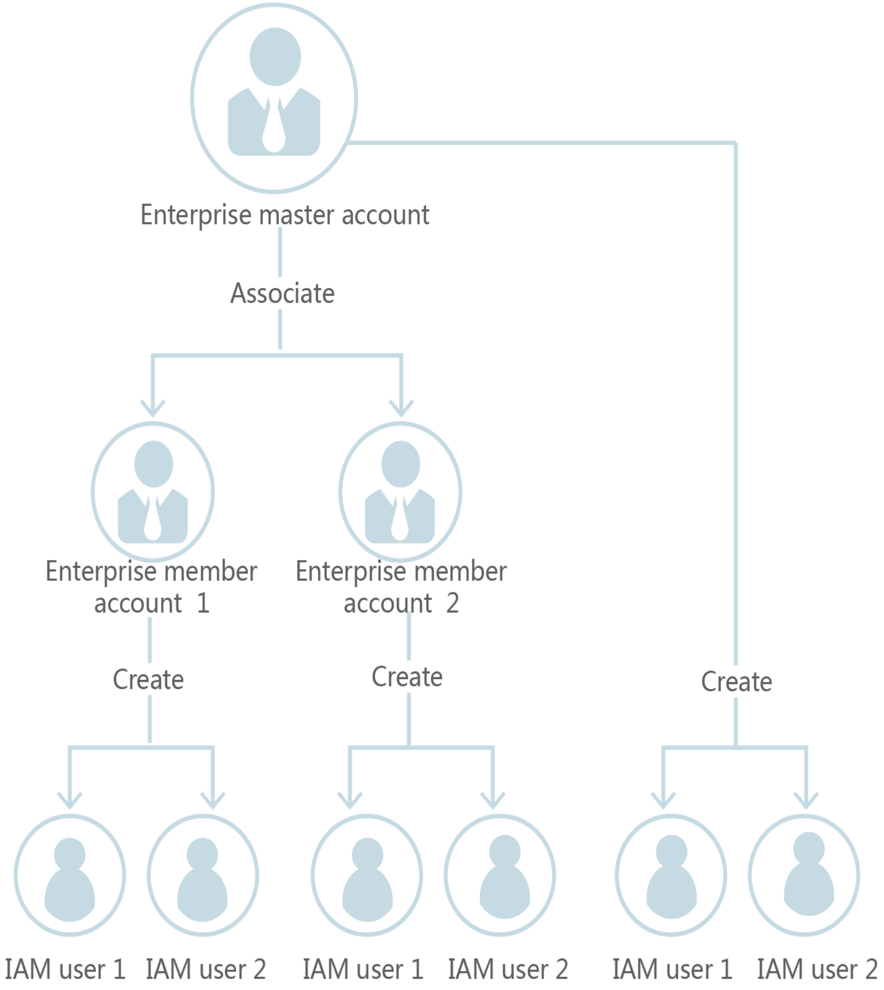
Enterprise Member Accounts

Both enterprise master accounts and member accounts are generated upon successful registration with Huawei Cloud. **Accounting Management** of Enterprise Management allows multiple Huawei Cloud accounts to be associated with each other for accounting purposes. You can create a hierarchical organization and a master account, add member accounts to this organization, and associate them with the master account.

The master account can allocate funds to member accounts so that the member accounts can use the funds to **manage resources**.

Both the master account and member accounts can create IAM users to control access to specific resources. An account can only manage its own IAM users but cannot manage the IAM users created by other accounts.

For details about how to create a member account, see **Creating a Member Account**.



6 Agency Management

6.1 How Can I Obtain Permissions to Create an Agency?

Symptom

You do not have permissions for creating an agency on the IAM console.

Possible Causes

You do not have permissions to use IAM.

Only the following users can use IAM:

- Account administrator (with full permissions for all services, including IAM)
- IAM users added to the **admin** group (with full permissions for all services, including IAM)
- IAM users assigned the **Security Administrator** role or an **xxx FullAccess** policy (with permissions to access IAM)

Solutions

- Contact the administrator to create an agency. For details, see **Creating an Agency (by a Delegating Party)**.
- Contact the administrator to grant you the permissions for using IAM. For details, see **Assigning Permissions to an IAM User**.

7 Account Management

7.1 Why Does Account Login Fail?

Symptom

When you log in to IAM using an account, the system displays a message indicating that your account name or password is incorrect.

Possible Causes

- The login link is incorrect.
- The login ID is incorrect.
- The password is incorrect.

Solutions

- Use the correct login link and enter a HUAWEI ID or Huawei Cloud account. If you have already upgraded your account to a HUAWEI ID, choose **HUAWEI ID**, as shown in **Figure 7-1**. Otherwise, choose **Huawei Cloud Account**, as shown in **Figure 7-2**.
  - To log in as a federated user, see **Logging In to Huawei Cloud**.
  - If you are an IAM user, log in by choosing **IAM User** on the login page. If the login fails, see **Why Does IAM User Login Fail?**.

Figure 7-1 Logging in using a HUAWEI ID

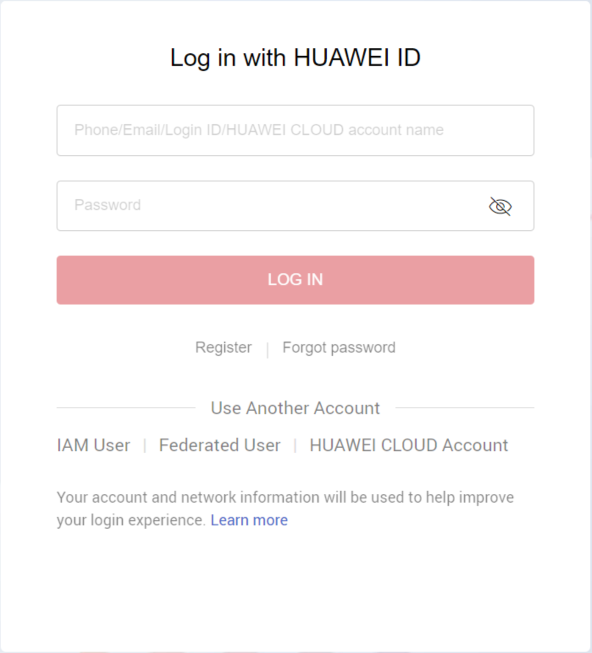
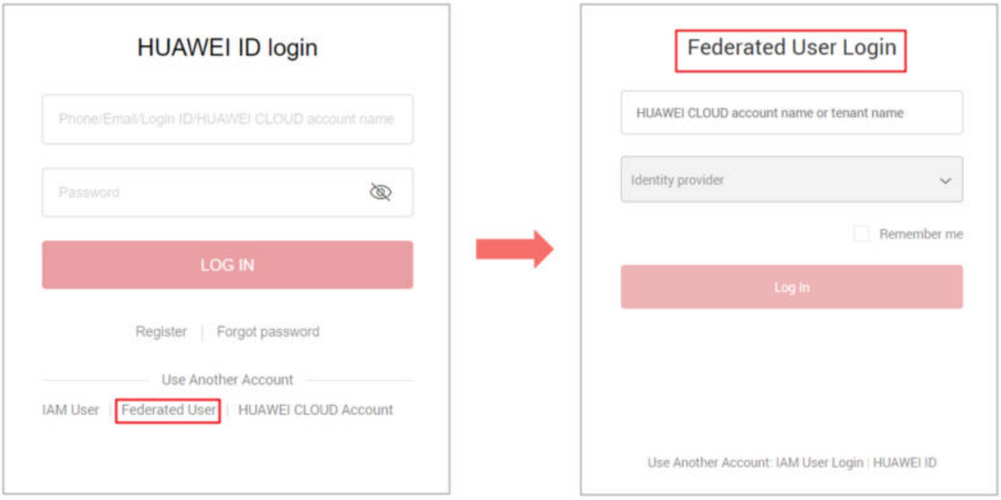

Log in with HUAWEI ID
Phone/Email/Login ID/HUAWEI CLOUD account name
Password
LOG IN
Register | Forgot password
Use Another Account
IAM User | Federated User | HUAWEI CLOUD Account
Your account and network information will be used to help improve your login experience. Learn more

Figure 7-2 Logging in using a Huawei Cloud account


HUAWEI ID login
Phone/Email/Login ID/HUAWEI CLOUD account name
Password
LOG IN
Register | Forgot password
Use Another Account
IAM User | Federated User | HUAWEI CLOUD Account
Federated User Login
HUAWEI CLOUD account name or tenant name
Identity provider
Remember me
Log In
Use Another Account: IAM User Login | HUAWEI ID

- When logging in with a HUAWEI ID, enter the **mobile number, email address, login ID, or Huawei Cloud account name**. When logging in with a Huawei Cloud account, enter the **name or email address of the account**.
  - If you have a HUAWEI ID, enter the mobile number or email address associated with the HUAWEI ID, or enter the login ID of this HUAWEI ID. For details, see **Logging In Using a HUAWEI ID**.
  - If you do not have a HUAWEI ID but have a Huawei Cloud account, which has not been upgraded to a HUAWEI ID, enter the Huawei Cloud account name.
- If you log in with a HUAWEI ID, enter the password of the HUAWEI ID. If you log in with a Huawei Cloud account, enter the password of the Huawei Cloud account.

7.2 What Are the Relationships Between a Huawei Cloud Account, HUAWEI ID, IAM User, and Federated User?

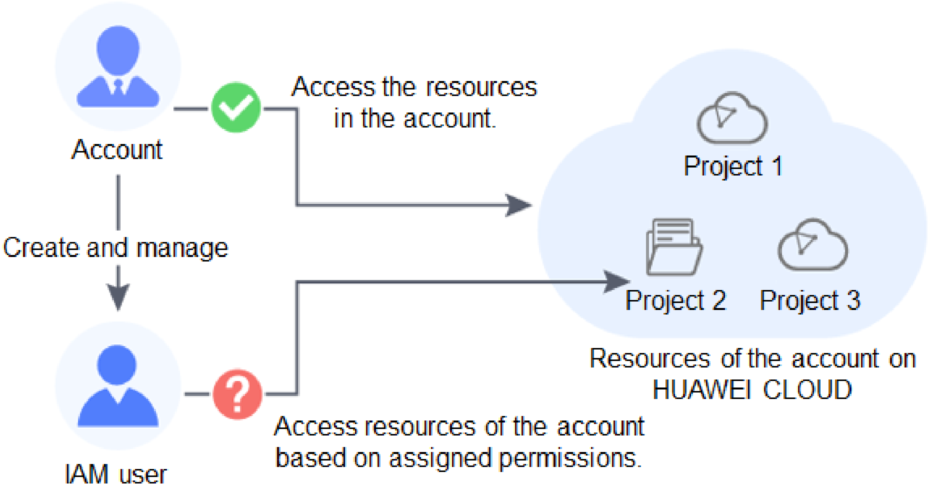
This section introduces the accounts used on Huawei Cloud and their relationships.

Account Types of Huawei Cloud

The Huawei Cloud account system consists of two types of accounts:

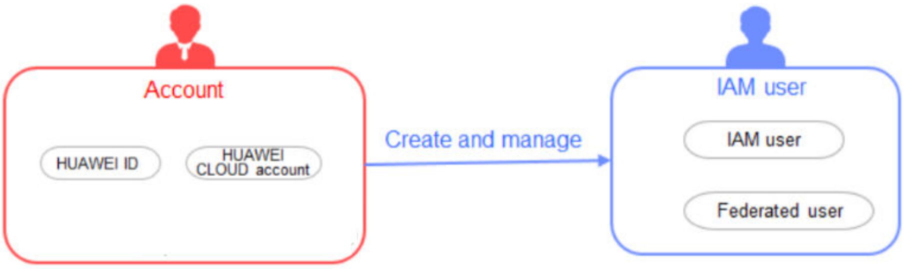
- **Accounts**: registered or created on Huawei Cloud. An account has the highest permissions on Huawei Cloud. It can access all of its resources and pays for the use of these resources. Accounts include HUAWEI IDs and Huawei Cloud accounts.
- **IAM users**: created and managed using an account in IAM. The account administrator grants permissions to IAM users and makes payment for the resources they use. IAM users use resources as specified by the permissions.

An account and its IAM users have a parent-child relationship.


Account
Access the resources in the account.
Create and manage
Project 1
Project 2
Project 3
Resources of the account on HUAWEI CLOUD
IAM user
Access resources of the account based on assigned permissions.

You can log in to Huawei Cloud using a HUAWEI ID or Huawei Cloud account, and use your resources and cloud services.

If you are an IAM user created by an account or a user of a third-party system that has established a trust relationship with Huawei Cloud, log in to Huawei Cloud through the corresponding page and then use resources and cloud services as specified by the permissions granted by the account.

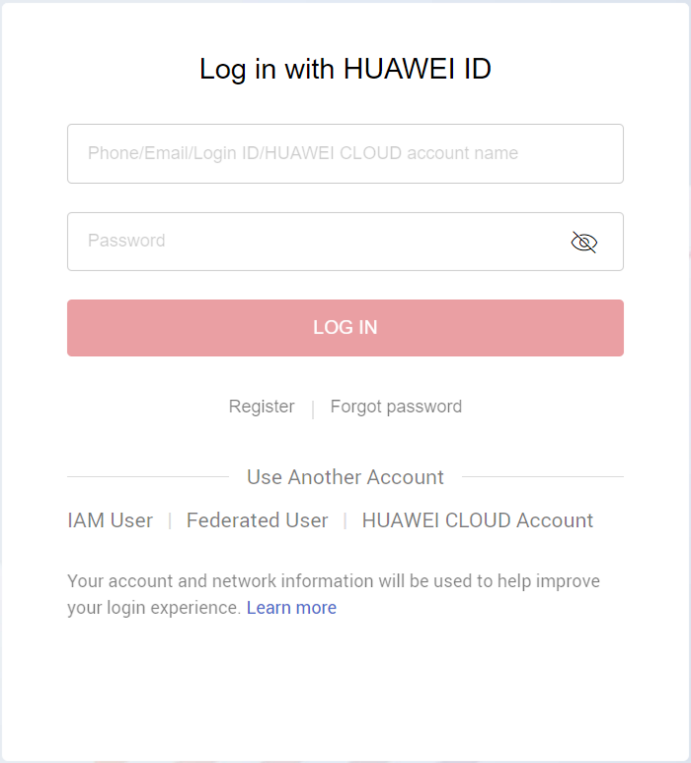


HUAWEI ID

You can register a HUAWEI ID to access all Huawei services, such as Huawei Cloud and Vmall.

Registration: Register a HUAWEI ID on any Huawei service website, such as the **HUAWEI ID website**.

Huawei Cloud login: Log in to Huawei Cloud by clicking **HUAWEI ID**. If this is the first time you log in to Huawei Cloud with a HUAWEI ID, enable Huawei Cloud services or bind the HUAWEI ID to your Huawei Cloud account by following the on-screen prompts.


Log in with HUAWEI ID

Phone/Email/Login ID/HUAWEI CLOUD account name

Password

LOG IN

Register | Forgot password

Use Another Account

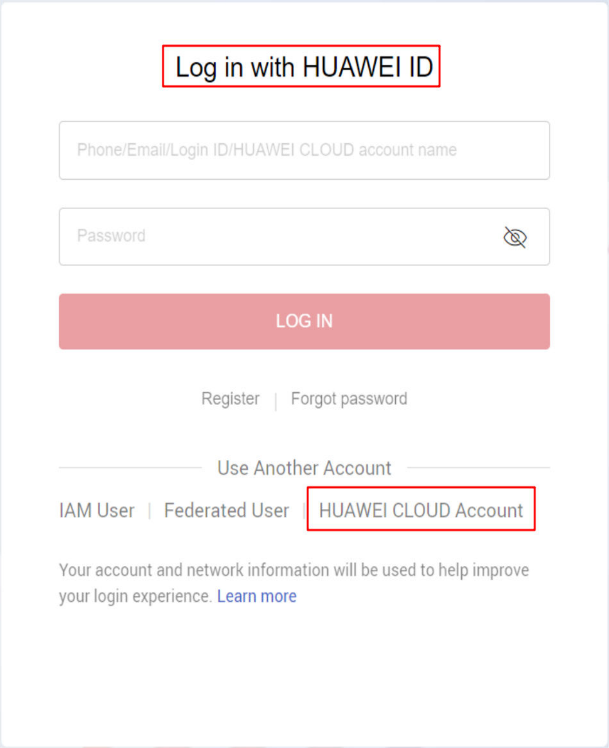
IAM User | Federated User | HUAWEI CLOUD Account

Your account and network information will be used to help improve your login experience. Learn more

Huawei Cloud Account

Huawei Cloud accounts can only be used to log in to Huawei Cloud.

Huawei Cloud login: Log in to Huawei Cloud by clicking **HUAWEI ID** or **Huawei Cloud Account**.


Log in with HUAWEI ID
Phone/Email/Login ID/HUAWEI CLOUD account name
Password
LOG IN
Register | Forgot password
Use Another Account
IAM User | Federated User | HUAWEI CLOUD Account

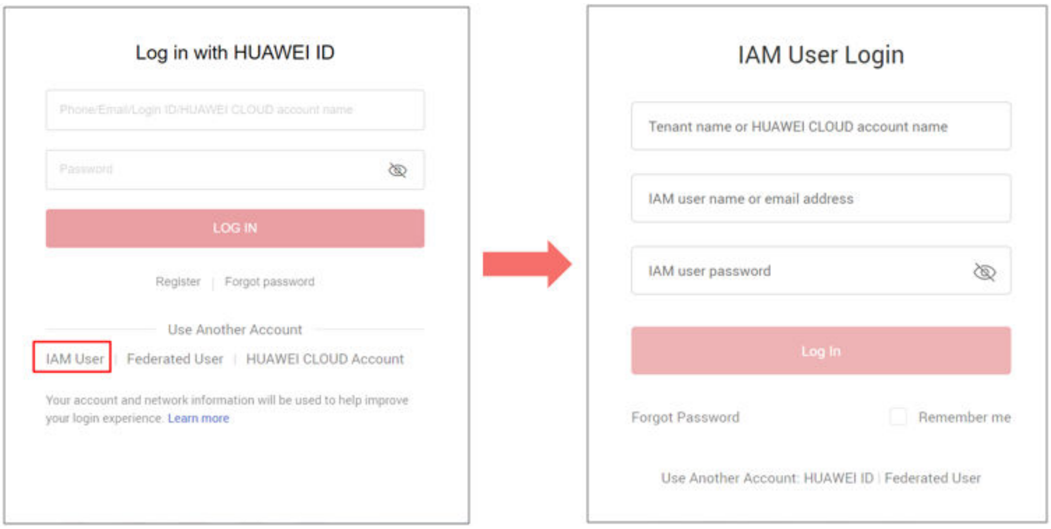
Your account and network information will be used to help improve your login experience. Learn more

IAM User

IAM users use Huawei Cloud resources as specified by the permissions granted by their account.

Creation: IAM users are created by an account in IAM. For details, see **Creating an IAM User**.

Huawei Cloud login: Log in to Huawei Cloud by clicking **IAM User**.

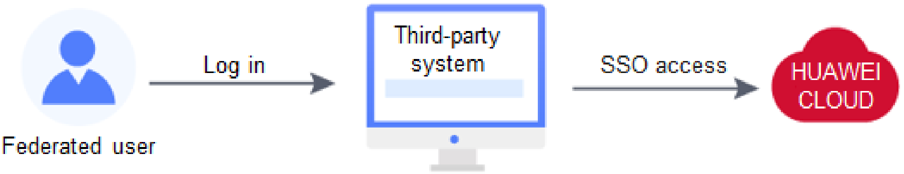

Log in with HUAWEI ID
Phone/Email/Login ID/HUAWEI CLOUD account name
Password
LOG IN
Register | Forgot password
Use Another Account
IAM User | Federated User | HUAWEI CLOUD Account
IAM User Login
Tenant name or HUAWEI CLOUD account name
IAM user name or email address
IAM user password
Log In
Forgot Password
Remember me
Use Another Account: HUAWEI ID | Federated User

Your account and network information will be used to help improve your login experience. Learn more

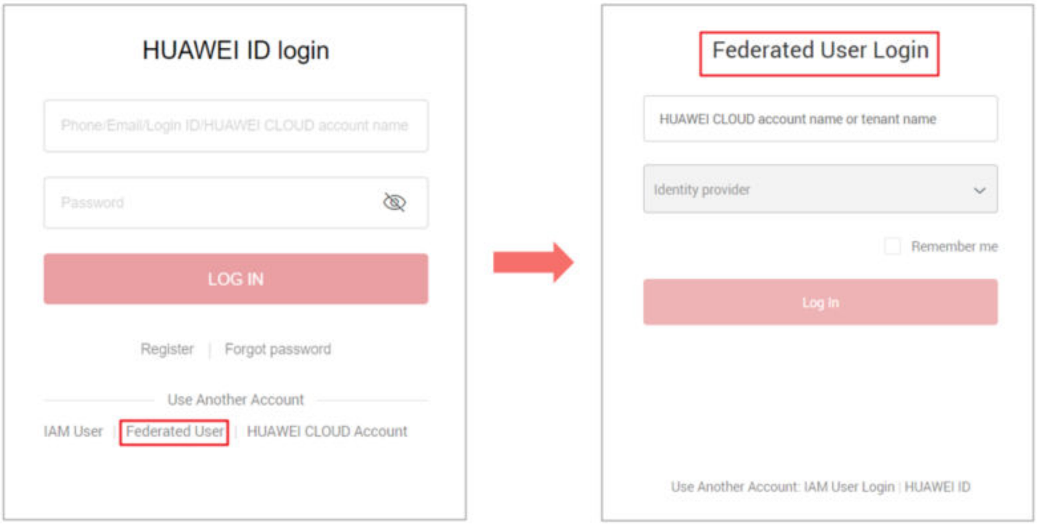
Federated User (Virtual User)

Federated users are registered with a third-party system that has established a trust relationship with Huawei Cloud. Users can log in to Huawei Cloud using third-party system accounts. For example, they can log in to a gaming platform using their social networking service (SNS) accounts.

Creation: When an enterprise user logs in to Huawei Cloud using an account of a third-party system, IAM automatically creates a virtual user (enterprise federated user). The third-party system corresponds to an identity provider that you have created in IAM. For details, see **Introduction to Identity Provider**.



Huawei Cloud login: Log in to Huawei Cloud by clicking **Federated User**.


HUAWEI ID login
Phone/Email/Login ID/HUAWEI CLOUD account name
Password
LOG IN
Register | Forgot password
Use Another Account
IAM User | Federated User | HUAWEI CLOUD Account
Federated User Login
HUAWEI CLOUD account name or tenant name
Identity provider
Remember me
Log In
Use Another Account: IAM User Login | HUAWEI ID

7.3 What Are the Possible Causes of a HUAWEI ID Upgrade Failure?

Symptom

Your Huawei Cloud account fails to be upgraded to a HUAWEI ID.

Possible Causes

1. Cause: You have registered a Huawei Cloud account and HUAWEI ID using the same mobile number or email address, and you have not used the HUAWEI ID to enable Huawei Cloud services.

Solution: Log out of your Huawei Cloud account, log in again using your HUAWEI ID, and associate your HUAWEI ID with your Huawei Cloud account.

2. Cause: You have registered **multiple** Huawei Cloud accounts and **one** HUAWEI ID, and used the HUAWEI ID to associate with or enable Huawei Cloud services. In this case, you cannot upgrade your Huawei Cloud accounts to HUAWEI ID.

   Solution: Log in using your Huawei Cloud account and ignore the upgrade notice.

3. Cause: You have registered a Huawei Cloud account and HUAWEI ID in different countries or regions using the same mobile number or email address. In this case, you cannot associate the account with the ID.

   Solution: Log in using your Huawei Cloud account and ignore the upgrade notice.

4. Cause: Your HUAWEI ID is frozen.

   Solution: Go to **HUAWEI ID website > Security center > Unfreeze account** to unfreeze your account, and try again.

5. Cause: Your mobile number has already been used to register a HUAWEI ID.

   Solution: Register a new HUAWEI ID on the **HUAWEI ID website**, and associate your Huawei Cloud account with the HUAWEI ID.

7.4 Can I Log In with My Huawei Cloud Account After Upgrading It to a HUAWEI ID?

- **If you have already registered a HUAWEI ID:**

  Log in using the mobile number, email address, or account name, but only if they are the same. For example, if the email addresses for your Huawei Cloud account and HUAWEI ID are different, you can log in with the mobile number of the Huawei Cloud account but not its email address.

- **If you have never registered a HUAWEI ID:**

  Log in using the same mobile number, email address, or account name.

8 Others

8.1 How Do I Obtain a User Token Using Postman?

Postman is a visual editing tool for building and testing API requests. It provides an easy-to-use user interface to send HTTP requests, including GET, PUT, POST, and DELETE requests. Postman allows you to modify parameters of HTTP requests and returns response to your requests.

A token is a user's access credential, which includes user identities and permissions. When you call an API to access cloud resources, a token is required for identity authentication.

Perform the procedure described in this section to obtain a user token using Postman. For details about the parameters, see **Obtaining a User Token**.

NOTE

- **Validity period of a token**

  The validity period of a token is **24 hours**. Cache your token to prevent frequent API calling. Ensure that the token is valid while you use it. Using a token that will soon expire may cause API calling failures.

  Obtaining a new token does not affect the validity of the existing token. However, the following operations will invalidate the existing token:

  - Deleting or disabling the IAM user
  - Changing the IAM user's password or access key
  - The IAM user's permissions are changed (due to outstanding payments, OBT application approval, or permission modification).
- **Obtaining a token**
  - If your Huawei Cloud account has been upgraded to a HUAWEI ID, you cannot obtain a token using the HUAWEI ID. However, you can create an IAM user, grant the user required permissions, and obtain a token as the user.
  - If you are a user of a third-party system, you cannot obtain a token by using the username and password that you use for federated identity authentication. Go to the Huawei Cloud login page, click **Forgot password**, click **Reset Huawei Cloud account password**, and set a password.

Prerequisites

You have installed and registered with Postman.

NOTE

- You are advised to install a Postman version that supports a header larger than 32 KB. Otherwise, a header overflow error may be reported.

Procedure

Step 1 Edit the request URL, header, and body of the API used to obtain a token for calling APIs.

- **Request URL**

  The request URL is in the format "**https://***IAM region and endpoint***/***API URI*".

  a. Obtain the IAM region and endpoint.

  b. Obtain the API URI from **Obtaining a User Token**.

     For example, the request URL in the **eu-west-101** region is **https://iam.myhuaweicloud.eu/v3/auth/tokens**.

  c. Select an API request method and enter the request URL in Postman.

- **Request Header**

  Set **key** to **Content-Type** and **value** to **application/json;charset=utf8**.

- **Request Body**

  Modify parameters in the example request body.

```
{
    "auth": {
        "identity": {
            "methods": [
                                "password"
                        ],
            "password": {
                "user": {
                    "domain": {
                        "name": "Account name"
                    },
                    "name": "IAM user name",
                    "password": "IAM user password"
                }
            }
        },
        "scope": {
            "domain": {
                "name": "Account name"
            }
        }
    }
  }
```

NOTE

For details about how to obtain the account name and IAM user name, see **Obtaining Account, IAM User, and Project Information**.

Step 2 Click **Send** to send the API request.

Step 3 View the token in the response header. You can use this token for authentication when you call other IAM APIs.

NOTE

- If error **401** is returned, the authentication has failed. Make sure that parameters in the request body are correct and send the request again.
- If error **400** is returned, the body format is incorrect. Check whether the body format complies with the JSON syntax. For details, see **Status Codes**.
- If "Header Overflow" is displayed, resolve the problem by referring to **Why Am I Seeing a Message Indicating Header Overflow When I Attempt to Use Postman to Obtain a Token?**

----End

Why Am I Seeing a Message Indicating Header Overflow When I Attempt to Use Postman to Obtain a Token?

Postman of V7.25.0, V7.26.0, or a later version cannot be used to obtain a user token due to configurations. The message "Header Overflow" will be displayed if you use any of these versions.

- **Solution 1**

  Use an earlier version of Postman, such as V 5.xx.

- **Solution 2:**

  Use curl to obtain a token and replace the text in bold with actual values:

  ```
  curl -ik -X POST -H 'Content-Type=application/json;charset=utf8' -d '{"auth": {"identity": {"methods":
  ["password"],"password": {"user": {"domain": {"name": "Account name"},"name": "IAM
  username","password": "IAM user password"}}},"scope": {"domain": {"name": "Account name"}}}}'
  https://iam.myhuaweicloud.eu/v3/auth/tokens
  ```

- **Solution 3**

  Pass an additional environment variable **NODE_OPTIONS=--max-http-header-size=16384 (16 KB)** to Postman to specify the maximum size of the HTTP header (in bytes).

  Run one of the following commands depending on your OS:

  – macOS

    ```
    NODE_OPTIONS=--max-http-header-size=16384 /Applications/Postman.app/Contents/MacOS/
    Postman
    ```

  – Linux

    ```
    NODE_OPTIONS=--max-http-header-size=16384 /path/to/Postman/Postman
    ```

  – Windows

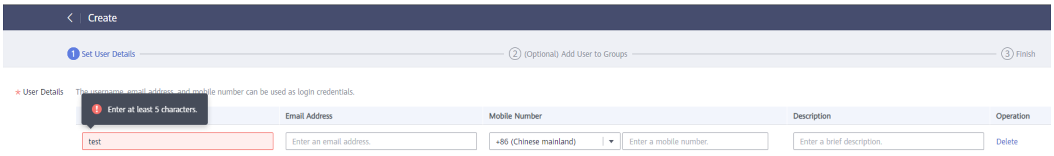
    ```
    set NODE_OPTIONS=--max-http-header-size=16384
    C:\users\<username>\AppData\local\Postman\Postman.exe
    ```

8.2 Why Is the Field-Level Help Always Displayed?

When you register with or log in to Huawei Cloud, bind a Huawei Cloud account, create a user, or reset or change the password, field-level help, such as "Enter at least 5 characters." is always displayed because you may be using Internet

Explorer 8 or an earlier version. In this case, fix the issue using the following methods.

Figure 8-1 Field-level help is always displayed



* User Details The username, email address, and mobile number can be used as login credentials.

Enter at least 5 characters.

test

Enter an email address.

+86 (Chinese mainland)

Enter a mobile number.

Enter a brief description.

- Upgrade the browser.

  Upgrade to Internet Explorer 9 or a later version.

- Use another browser.

  Use Mozilla Firefox (version 38.0 or later) or Google Chrome (version 43.0 or later).

8.3 How Do I Disable Autofill Password on Google Chrome?

When you use Google Chrome to log in to Huawei Cloud for the first time, a message will appear asking you to confirm whether you want to save the password. This is because **Offer to save passwords** and **Auto Sign-in** in the **Passwords** area of the **Settings** page in Google Chrome are selected by default after the Google Chrome browser is installed. If you confirm to save the password, the password will be automatically filled during your next login. To ensure the security of your account and password, perform the following operations to disable this function. This section uses Google Chrome 61.0.3163.100 as an example to describe how to disable this function.

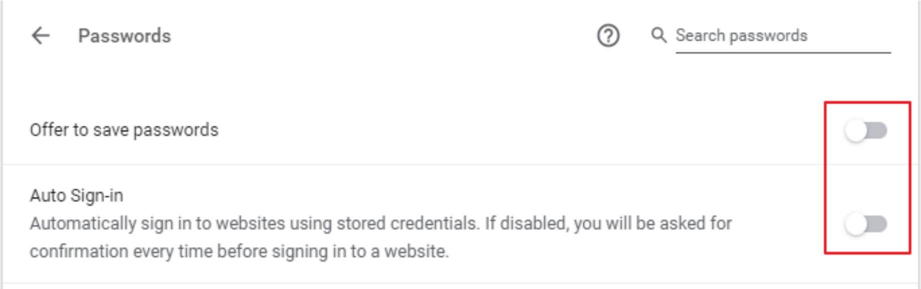
Procedure

Step 1 Open the Google Chrome browser, click ⋮ in the upper right corner of the browser, and choose **Settings**.

Step 2 In the **Autofill** area, click **Passwords**.

Step 3 Deselect **Offer to save passwords** and **Auto Sign-in**.

Figure 8-2 Deselecting Offer to save passwords and Auto Sign-in



Offer to save passwords ○

Auto Sign-in
Automatically sign in to websites using stored credentials. If disabled, you will be asked for confirmation every time before signing in to a website. ○

----End

Follow-up Procedure

To delete a saved password, in the **Saved Passwords** area, click ⋮ next to the password, and click **Remove**. The password will be deleted.

8.4 Region and AZ

Concept

A region and availability zone (AZ) identify the location of a data center. You can create resources in a specific region and AZ.

- Regions are divided based on geographical location and network latency. Public services, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP), and Image Management Service (IMS), are shared within the same region. Regions are classified into universal regions and dedicated regions. A universal region provides universal cloud services for common tenants. A dedicated region provides specific services for specific tenants.
- An AZ contains one or more physical data centers. Each AZ has independent cooling, fire extinguishing, moisture-proof, and electricity facilities. Within an AZ, computing, network, storage, and other resources are logically divided into multiple clusters. to support high-availability systems.

Selecting a Region

If your target users are in Europe, select the **EU-Dublin** region.

Selecting an AZ

When deploying resources, consider your applications' requirements on disaster recovery (DR) and network latency.

- For high DR capability, deploy resources in different AZs within the same region.
- For lower network latency, deploy resources in the same AZ.

8.5 How Do I Apply for the Permissions to Access Resources in a Cloud Alliance Region Using My Huawei Cloud Account or HUAWEI ID?

You can submit a service ticket to apply for required permissions to access resources in cloud alliance regions such as **CN-Hong Kong**, **AP-Singapore**, **CN East-Shanghai1**, **LA-Sao Paulo1**, **LA-Mexico City1**, **LA-Mexico City2**, **AF-Johannesburg**, or **LA-Santiago**.

Procedure

Step 1 **Submit a service ticket** and specify the cloud alliance region that you want to access.

Step 2 Wait for an approval email notification. After receiving the email, log in to the management console and click 📍 in the upper left corner to select the region you want to access.

----End