IAM 5.0 FAQs

Issue 01

Date 2025-11-28

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2025. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions


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

Notice

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

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

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

Contents

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

1 Permissions Management

1.1 What Can I Do If I Cannot Find a Specific Service in a Custom Identity Policy or Cannot Find a System-defined Identity Policy for a Specific Service During Authorization?

Symptom

The administrator cannot find a specific service when creating a custom identity policy on the new IAM console, or cannot find permissions for a specific service when assigning system-defined identity policies to users, groups, agencies, or trust agencies on the new IAM console.

Possible Causes

- The entered service name or identity policy name is incorrect.
- The service for which permissions are assigned does not support identity policies of IAM, so you cannot find that service when creating a custom identity policy or cannot find any system-defined identity policies for that service. For details, see **Cloud Services for Using Identity Policies and Trust Agencies**.

Solution

- Check the service name on the management console or in the help center, and view the actions supported by custom and system-defined identity policies provided by the service in **Identity Policy Authorization**.
- On the old IAM console, assign system-defined roles, system-defined policies, and custom policies to users, groups, or agencies to meet permissions management requirements.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

1.2 How Do I Grant Cloud Service Permissions in the EU-Dublin Region to IAM Users?

Symptom

You have enabled cloud services in the **EU-Dublin** region as an administrator, and need to authorize IAM users in your account to use cloud services in this region.

Users access cloud services in the **EU-Dublin** 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 Huawei Cloud's default regions and the **EU-Dublin** 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**.

Procedure

Step 1 Log in to Huawei Cloud as an administrator, click  on the console homepage, and select the **EU-Dublin** region.

Step 2 On the console of the **EU-Dublin** region, choose **Management & Deployment** > **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 **Authorize** in the row that contains the user group created in **Step 3**.

Step 5 In the identity policy list, select identity policies to be attached 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**. IAM user authorization for the **EU-Dublin** region is completed.

----End

After the authorization, log in to the Huawei Cloud console as an IAM user, switch to the **EU-Dublin** region, and use cloud resources as specified by the assigned permissions.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

1.3 Why Have Permissions Granted to a User Not Been Applied?

Symptom

Permissions granted to an IAM user on the new IAM console have not been applied.

Troubleshooting

1. Cause: Permissions granted to the IAM user were incorrect.

   Solution: Check and modify the permissions granted to the IAM user. For details, see **Assigning Permissions to an IAM User** or **Creating a User Group and Assigning Permissions**. For details about permission details, see **Identity Policy Authorization**.

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

   Solution: View the system-defined permissions granted to the IAM user and check whether there is any statement that denies the actions. For details, see **Identity Policy Syntax**.

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

   Solution: Add the user to the group that has been granted the permissions. For details, see **Adding Users to or Removing Users from a User Group**.

4. Cause: The granted permissions will be applied 15 to 30 minutes after the authorization.

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

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

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

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.

Solution

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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Prerequisites

You have already created an IAM user. For details, see **Creating an IAM User**.

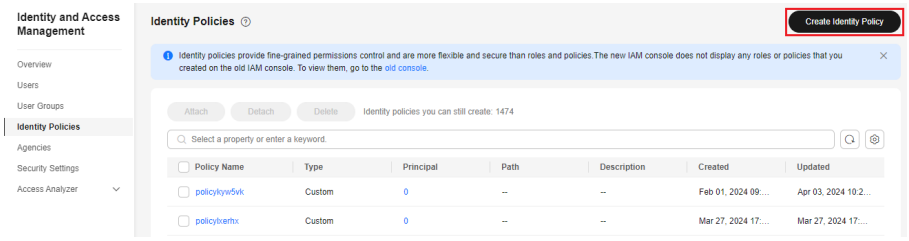
Procedure

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 In the navigation pane on the left, choose **Identity Policies**. In the upper right corner, click **Create Identity Policy**.

Figure 1-1 Creating a custom identity policy



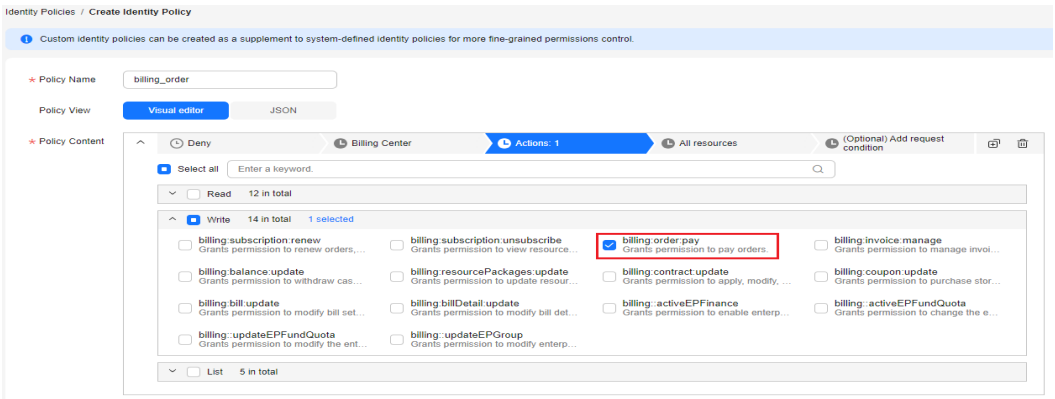
Step 4 Enter a policy name: **billing_order**.

Step 5 Select **Visual editor** for **Policy View**.

Step 6 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. Select **billing**.
  c. In the **Actions** pane, expand the **Write** area, and select action **billing:order:pay**.

  Figure 1-2 Configuring permissions to disallow order payment



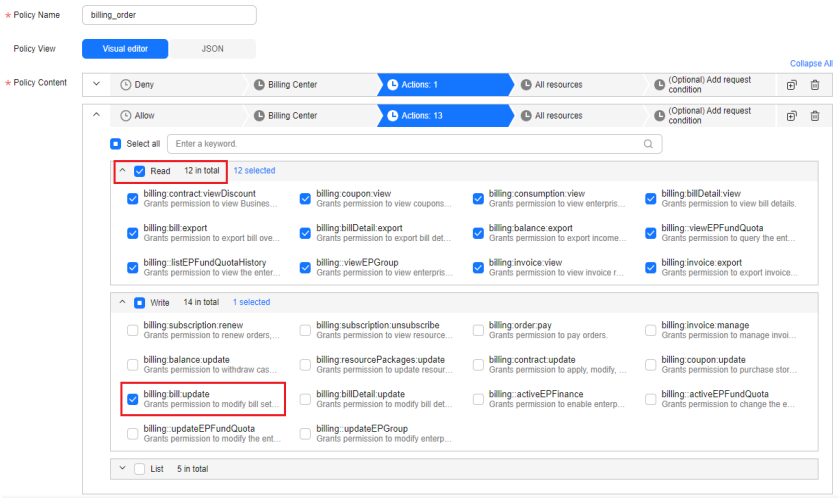
  d. Select **All resources** for **Resources**.
- Configuring permissions to allow order placement

a. Select **Allow**.

b. Select **billing**.

c. In the **Actions** pane, expand the **Write** area, select action **billing:bill:update**, and select all the actions in the **Read** area.

Figure 1-3 Configuring permissions to allow order placement



d. Select **All resources** for **Resources**.

Step 7 Set a description for the identity policy, for example, **Permissions to place orders but disallow order payment**.

Step 8 Click **OK**.

Step 9 Attach the custom identity policy to the created IAM user.

NOTE

You can attach custom identity policies to a user in the same way you attach system-defined identity policies. For details, see **Assigning Permissions to an IAM User**.

When the IAM user logs in and goes to the **Unpaid Orders** page of the Billing Center, the **Pay** button is grayed out in the **Operation** column.

Figure 1-4 Setting successful (Pay button grayed out)

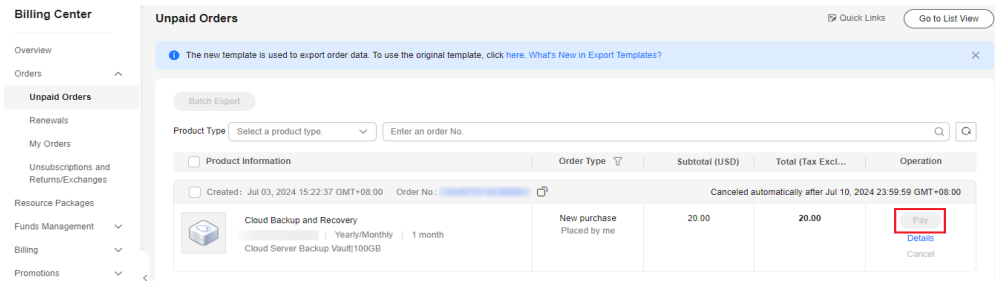
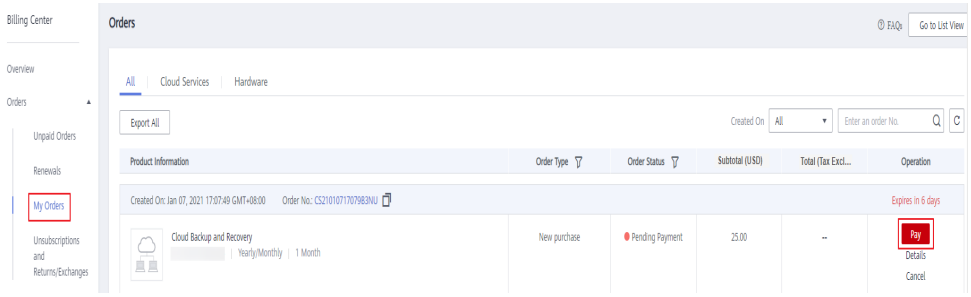


Figure 1-5 Setting failed (Pay button available)



----End

1.5 What Can I Do If I Cannot Find the Action in an Error Message During Policy-based Authorization?

Symptom

The administrator assigns system-defined or custom policies to an IAM user. After the IAM user performs an action beyond the authorization scope, the system displays a message indicating that the action is denied. However, the action mentioned in the message cannot be found in the assigned system-defined or custom policies.

Possible Causes

This action is defined in an identity policy, not a policy.

Solution

- Solution 1: You can use identity policy-based authorization and select the identity policy action mentioned in the displayed message.
- Solution 2: If you only want to use policy-based authorization, you need to find the alias of an identity policy action and add it to the policy.

Before using the second solution, you need to understand the validation logic of policies and identity policies shown in **Figure 1-6**.

Figure 1-6 Validation logic of policies and identity policies

Comprehensive evaluation result		Identity policy evaluation result		
		Explicit deny	Allow	Implicit deny
Policy evaluation result	Explicit deny	Explicit deny	Explicit deny	Explicit deny
	Allow	Explicit deny	Allow	Allow
	Implicit deny	Explicit deny	Allow	Implicit deny

User-defined permissions
Final decision: Deny
Final decision: Allow

For details about the differences between explicit deny and implicit deny, see **Policies** and **Identity Policy-based Authorization**. If the comprehensive

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

evaluation result is implicit deny, the system denies the action. Example error message:

```
"error_msg": "User: xxx is not authorized to perform action ecs:cloudServers:get on resource ecs:cn-north-5:yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy:instance:zzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzz because no identity-based policy allows the ecs:cloudServers:get action."
```

If the comprehensive evaluation result is explicit deny, the system denies the action. Example error message:

```
"error_msg": "User: xxx is not authorized to perform action ecs:cloudServers:get on resource ecs:cn-north-5:yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy:instance:zzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzz with an explicit deny in an identity-based policy."
```

The message describes which action is denied on what resources, but whether this action is defined in a policy or identity policy is not fixed. This is determined by IAM based on the evaluation logic shown in **Figure 1-7**.

Figure 1-7 Evaluation logic

Source of action in the error message		Identity policy evaluation result		
		Explicit deny	Allow	Implicit deny
Policy evaluation result	Explicit deny	Identity policy	Policy	Policy
	Allow	Identity policy	N/A	N/A
	Implicit deny	Identity policy	N/A	Identity policy

User-defined permissions
Final decision: Deny
Final decision: Allow

If you only use policy-based authorization and perform actions beyond the authorization scope, the results of both policy and identity policy evaluation are implicit deny, so the action in the displayed message is defined in an identity policy. In this case, if you do not want to use identity policy-based authorization but you cannot find the action in a policy, it means this identity policy action has an alias (different from the identity policy action name) in the policy and all you need to do is to add that alias to the policy. For details about the mapping between identity policy actions and their aliases, see **Identity Policy Authorization** of the corresponding cloud service.

1.6 How Are Identity Policies Compatible with Policies?

The role/policy-based authorization model and identity policy-based authorization model are independent from each other but the way of using them is similar.

You are advised to use only identity policies to manage authorization of new accounts for more secure and fine-grained permission control. You may use both roles/policies and identity policies for permissions management of existing accounts. This means an IAM principal can be granted multiple permissions, including system-defined roles, system-defined policies, custom policies, system-defined identity policies, and custom identity policies. These permissions can take effect at the same time. System-defined roles are a coarse-grained authorization strategy provided by IAM to assign permissions based on users' job responsibilities. They are not changeable and you can choose whether to use roles for authorization based on service requirements. System-defined policies, custom

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

policies, system-defined identity policies, and custom identity policies are fine-grained for permissions management.

When using policies and identity policies, it is important to select required actions. Using IAM as an example. For details about all actions supported by IAM, see **Permissions and Supported Actions**. The "Actions Supported by Policy-based Authorization" describes the policy actions supported by IAM APIs. The "Actions Supported by Identity Policy-based Authorization" describes the identity policy actions supported by IAM APIs. To be compatible with APIs that support only policy actions, certain identity policy actions that can call these APIs are added to IAM identity policies. Among these identity policy actions, some of their names are changed while some are not. We call the actions whose names are changed the alias of the identity policy actions.

Table 1-1 lists the policy actions that are added to identity policies without changing their names. **Table 1-2** lists the policy actions that are added to identity policies with their names changed.

Table 1-1 Actions that are added to identity policies without changing their names

Identity Policy Action	Access Level	Policy Action
iam:identityProviders:listMappings	List	iam:identityProviders:listMappings
iam:identityProviders:getMapping	Read	iam:identityProviders:getMapping
iam:identityProviders:createMapping	Write	iam:identityProviders:createMapping
iam:identityProviders:deleteMapping	Write	iam:identityProviders:deleteMapping
iam:identityProviders:updateMapping	Write	iam:identityProviders:updateMapping
iam:identityProviders:listProtocols	List	iam:identityProviders:listProtocols
iam:identityProviders:getProtocol	Read	iam:identityProviders:getProtocol
iam:identityProviders:createProtocol	Write	iam:identityProviders:createProtocol
iam:identityProviders:deleteProtocol	Write	iam:identityProviders:deleteProtocol
iam:identityProviders:updateProtocol	Write	iam:identityProviders:updateProtocol
iam:securityPolicies:getProtectPolicy	Read	iam:securityPolicies:getProtectPolicy

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Identity Policy Action	Access Level	Policy Action
iam:securityPolicies:updateProtectPolicy	Write	iam:securityPolicies:updateProtectPolicy
iam:securityPolicies:getPasswordPolicy	Read	iam:securityPolicies:getPasswordPolicy
iam:securityPolicies:updatePasswordPolicy	Write	iam:securityPolicies:updatePasswordPolicy
iam:securityPolicies:getLoginPolicy	Read	iam:securityPolicies:getLoginPolicy
iam:securityPolicies:updateLoginPolicy	Write	iam:securityPolicies:updateLoginPolicy
iam:securityPolicies:getConsoleAclPolicy	Read	iam:securityPolicies:getConsoleAclPolicy
iam:securityPolicies:updateConsoleAclPolicy	Write	iam:securityPolicies:updateConsoleAclPolicy
iam:securityPolicies:getApiAclPolicy	Read	iam:securityPolicies:getApiAclPolicy
iam:securityPolicies:updateApiAclPolicy	Write	iam:securityPolicies:updateApiAclPolicy

Table 1-2 Mapping between identity policy actions and policy actions

Identity Policy Action	Access Level	Policy Action (Alias of Identity Policy Action)
iam::listAccessKeys	List	iam:credentials:listCredentials
iam::createAccessKey	Write	iam:credentials:createCredential
iam::getAccessKey	Read	iam:credentials:getCredential
iam::updateAccessKey	Write	iam:credentials:updateCredential
iam::deleteAccessKey	Write	iam:credentials:deleteCredential
iam:projects:list	List	iam:projects:listProjects
iam:projects:create	Write	iam:projects:createProject
iam:projects:listForUser	List	iam:projects:listProjectsForUser
iam:projects:update	Write	iam:projects:updateProject
iam:groups:list	List	iam:groups:listGroups
iam:groups:create	Write	iam:groups:createGroup

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Identity Policy Action	Access Level	Policy Action (Alias of Identity Policy Action)
iam:groups:get	Read	iam:groups:getGroup
iam:groups:delete	Write	iam:groups:deleteGroup
iam:groups:update	Write	iam:groups:updateGroup
iam:groups:removeUser	Write	iam:permissions:removeUserFromGroup
iam:groups:listUsers	List	iam:users:listUsersForGroup
iam:groups:checkUser	Read	iam:permissions:checkUserInGroup
iam:groups:addUser	Write	iam:permissions:addUserToGroup
iam:users:create	Write	iam:users:createUser
iam:users:get	Read	iam:users:getUser
iam:users:update	Write	iam:users:updateUser
iam:users:list	List	iam:users:listUsers
iam:users:delete	Write	iam:users:deleteUser
iam:users:listGroups	List	iam:groups:listGroupsForUser
iam:users:listVirtualMFADevices	List	iam:mfa:listVirtualMFADevices
iam:users:createVirtualMFADevice	Write	iam:mfa:createVirtualMFADevice
iam:users:deleteVirtualMFADevice	Write	iam:mfa:deleteVirtualMFADevice
iam:users:getVirtualMFADevice	Read	iam:mfa:getVirtualMFADevice
iam:users:bindVirtualMFADevice	Write	iam:mfa:bindMFADevice
iam:users:unbindVirtualMFADevice	Write	iam:mfa:unbindMFADevice
iam:identityProviders:list	List	iam:identityProviders:listIdentityProviders
iam:identityProviders:get	Read	iam:identityProviders:getIdentityProvider
iam:identityProviders:create	Write	iam:identityProviders:createIdentityProvider
iam:identityProviders:delete	Write	iam:identityProviders:deleteIdentityProvider

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Identity Policy Action	Access Level	Policy Action (Alias of Identity Policy Action)
iam:identityProviders:update	Write	iam:identityProviders:updateIdentityProvider
iam:identityProviders:getSAMLMetadata	Read	iam:identityProviders:getIDPMetadata
iam:identityProviders:createSAMLMetadata	Write	iam:identityProviders:createIDPMetadata
iam:identityProviders:getOIDCConfig	Read	iam:identityProviders:getOpenIDConnectConfig
iam:identityProviders:createOIDCConfig	Write	iam:identityProviders:createOpenIDConnectConfig
iam:identityProviders:updateOIDCConfig	Write	iam:identityProviders:updateOpenIDConnectConfig
iam:users:listLoginProtectSettings	List	iam:users:listUserLoginProtects
iam:users:getLoginProtectSetting	Read	iam:users:getUserLoginProtect
iam:users:updateLoginProtectSetting	Write	iam:users:setUserLoginProtect
iam:quotas:list	List	iam:quotas:listQuotas
iam:quotas:listForProject	List	iam:quotas:listQuotasForProject

Table 1-2 lists policy actions that are aliases in the identity policy authorization. For example, you can create the following identity policy with the **iam:identityProviders:listMappings** action in **Table 1-1** allowed on the new IAM console to call the API **GET /v3/OS-FEDERATION/mappings** to list mappings of an identity provider. For details, see **Creating a Custom Identity Policy**.

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:identityProviders:listMappings"
      ]
    }
  ]
}
```

This is the same as creating a policy with the iam:identityProviders:listMappings action on the old IAM console. For details, see **Creating a Custom Policy**.

```
{
    "Version": "1.1",
    "Statement": [{
        "Effect": "Allow",
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
        "Action": [
            "iam:identityProviders:listMappings"
        ]
    }]
}
```

You can create the following identity policy that allows the **iam::listAccessKeys** action in **Table 1-2** on the new IAM console to call the API **GET /v3.0/OS-CREDENTIAL/credentials** to query permanent access keys.

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam::listAccessKeys"
      ]
    }
  ]
}
```

The policy effect above is the same as the following policy that allows the **iam:credentials:listCredentials** action on the old IAM console:

```
{
    "Version": "1.1",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "iam:credentials:listCredentials"
        ]
    }]
}
```

1.7 What Can I Do If I Cannot Find the Action in an Error Message During Enterprise Project Authorization?

Symptom

If you only used enterprise project authorization and tried to perform an operation, the system displayed an error message showing you the action you need to obtain permissions for. However, this action cannot be found during policy authorization.

Possible Causes

The API for querying the resources bound to all enterprise projects is explicitly denied by an identity policy or a mandatory access control policy (such as an SCP). In this case, the system shows only the denied identity policy action instead of the denied policy action. The following is an example:

An IAM user was not granted the policy action **ces:siteMonitorRule:list** permission on the new IAM console. When the user calls the API requiring this permission, the system displays "Policy doesn't allow **ces:remoteChecks:list** to be performed". The system prompt only shows **ces:remoteChecks:list**, instead of the identity policy action **ces:siteMonitorRule:list**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Solutions

- If you use enterprise project authorization, go the old IAM console and grant required permissions in the enterprise project view.
- If you do not need enterprise project authorization:
  - Go the new IAM console and create identity policies.
  - Go the old IAM console and create policies in the IAM project view.

1.8 Why Can Users with Permissions to View Resources in an Enterprise Project View All Resources of the Account?

Symptom

An administrator used enterprise project authorization to grant a user the permission to view only resources in an enterprise project, and then attached the identity policy for viewing resources to the user. As a result, the user can view all resources in enterprise project created under the account.

Possible Causes

The identity policy allows the user to view all resources of the account.

Solutions

If you want the user to view only the resources allowed by the enterprise project authorization, detach the identity policy.

1.9 What Should I Do If Permissions Are Not Working as Expected When "NotAction" Is Used in an Identity Policy?

Symptom

An administrator created an identity policy on the new IAM console and used a deny statement with "NotAction" to exclude an action of a cloud service. However, the action of another cloud service is also excluded from the deny statement. For example, a member account in an organization has all cloud service permissions, and is attached with an identity policy with a deny statement containing "NotAction" to exclude a VPC action. This identity policy neither denies the VPC action nor the EIP action. The following is the identity policy used in this example:

```
{
    "Version": "5.0",
    "Statement": [{
        "Effect": "Deny",
        "NotAction": [
            "VPC:*:*"
        ]
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
    }]
}
```

Possible Causes

Some actions' aliases of a cloud service are the action names of another cloud service. The aliases are used to adapt the actions on the new console with those on the old one. For example, EIP uses the names of some VPC actions as aliases of EIP actions. For identity policy authentication, such actions are the same. VPC actions are regarded as EIP actions in "NotAction", so both are excluded from the deny statement.

Solutions

In the preceding scenario, to allow cloud service A's action and deny cloud service B's action, you will need two deny statements, one with "NotAction" for service A's action, and another for service B's action. For example, if you want to allow a VPC action and deny an EIP action, you can use "NotAction" to exclude the VPC action from the deny statement and then add another deny statement for the EIP action. The following is an example identity policy:

```
{
    "Version": "5.0",
    "Statement": [{
            "Effect": "Deny",
            "NotAction": [
                "VPC:*:*"
            ]
        },
        {
            "Effect": "Deny",
            "Action": [
                "EIP:*:*"
            ]
        }
    ]
}
```

1.10 Which Cloud Services Support the Global Condition Key G:CalledVia?

The following services support the global condition key **g:CalledVia**.

Table 1-3 Cloud services that support g:CalledVia

Cloud Service Name	Principal
Anti-DDoS Service (AAD)	service.AAD
IAM Access Analyzer	service.AccessAnalyzer
Application Operations Management (AOM)	service.AOM
API Gateway (APIG)	service.APIG
Auto Scaling	service.AS

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Cloud Service Name	Principal
Billing Center	service.BILLING
Cloud Bastion Host (CBH)	service.CBH
Cloud Backup and Recovery (CBR)	service.CBR
Cloud Connect	service.CC
Cloud Container Engine (CCE)	service.CCE
Content Delivery Network (CDN)	service.CDN
Cloud Eye	service.CES
Cloud Firewall (CFW)	service.CFW
Cloud Native Anti-DDoS Advanced (CNAD)	service.CNAD
Cloud Operations Center (COC)	service.COC
CodeArts	service.CODEARTS
CodeArts Pipeline	service.CodeArtsPipeline
Cloud Service Engine (CSE)	service.CSE
Cloud Secret Management Service (CSMS)	service.CSMS
Cloud Search Service (CSS)	service.CSS
Cloud Trace Service (CTS)	service.CTS
DataArts Studio	service.DataArtsStudio
Database Security Service (DBSS)	service.DBSS
Direct Connect (DC)	service.DCAAS
Distributed Cache Service (DCS)	service.DCS
Document Database Service (DDS)	service.DDS
Dedicated Hardware Security Module (DHSM)	service.DHSM
Data Lake Insight (DLI)	service.DLI
Domain Name Service (DNS)	service.DNS
Data Replication Service (DRS)	service.DRS
Data Security Center (DSC)	service.DSC
GaussDB(DWS)	service.DWS
Elastic IP (EIP)	service.EIP

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Cloud Service Name	Principal
Elastic Load Balance (ELB)	service.ELB
Enterprise Project Management Service (EPS)	service.EPS
Enterprise Router	service.ER
Elastic Volume Service (EVS)	service.EVS
Global Accelerator	service.GA
GaussDB	service.GaussDB
TaurusDB	service.GaussDBforMySQL
Host Security Service (HSS)	service.HSS
Identity and Access Management (IAM)	service.IAM
IAM Identity Center	service.IdentityCenter
Image Management Service (IMS)	service.IMS
IoT Device Access (IoTDA)	service.IoTDA
Key Management Service (KMS)	service.KMS
Key Pair Service (KPS)	service.KPS
Log Tank Service (LTS)	service.LTS
MapReduce Service (MRS)	service.MRS
NAT Gateway	service.NAT
Object Storage Migration Service (OMS)	service.OMS
Organizations	service.Organizations
Private Certificate Authority (PCA)	service.PCA
Resource Access Manager (RAM)	service.RAM
Relational Database Service (RDS)	service.RDS
Resource Formation Service (RFS)	service.RF
	service.RFStackSets
	service.RFStackSetsOrgMember
Resource Governance Center (RGC)	service.RGC
Config	service.RMSMultiAccountSetup
	service.RMSConforms

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Cloud Service Name	Principal
	service.RMSRemediation
SSL Certificate Manager (SCM)	service.SCM
SecMaster	service.SecMaster
ServiceStage	service.ServiceStage
Simple Message Notification (SMN)	service.SMN
Server Migration Service (SMS)	service.SMS
Software Repository for Container (SWR)	service.swr
Tag Management Service (TMS)	service.TMS
Virtual Private Cloud (VPC)	service.VPC
VPC Endpoint (VPCEP)	service.VPCEP
Web Application Firewall (WAF)	service.WAF
Workspace	service.Workspace

RFS and Config each have multiple principals.

RFS:

- You can use **service.RF** to assume a cloud service agency and create, update, or delete resources based on the cloud service defined in the template for cross-service access request forwarding.
- You can use **service.RFStackSets** to assume a cloud service agency and query OU and member account information in Organizations. The administrator can obtain temporary credentials of the trust agencies assumed by member accounts in IAM.
- You can use **service.RFStackSetsOrgMember** to assume a cloud service agency and create trust agencies for member accounts and add policies to the trust agencies in IAM for RFS management.

Config:

- You can use **service.RMSMultiAccountSetup** to create a service-linked agency in IAM for creating or updating organization conformance rules and packages for cross-service access request forwarding. You can also use this principal to assume a cloud service agency and send resource change notifications through SMN or dump resource snapshots to OBS.
- You can use **service.RMSConforms** to create a service-linked agency in IAM for creating or updating conformance packages for cross-service access request forwarding.
- You can use **service.RMSRemediation** to create a service-linked agency in IAM for creating or updating remediation configurations for cross-service access request forwarding.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

1.11 How Do I Handle Access Denied by Identity Policies?

IAM displays error messages for access denied by identity policies attached to users. They can identify the cause of the denied access errors and resolve them based on the error messages.

Implicit Deny and Explicit Deny

Access denied errors appear when IAM explicitly or implicitly denies an authorization request.

An implicit deny means that the access is not explicitly authorized by an administrator. The error message may contain the following information:

```
User: ${principal} is not authorized to perform: ${action} on resource: ${resource} because no ${policy_type} policy allows the ${action} action.
```

An explicit deny means that the access is explicitly restricted by an administrator. The error message may contain the following information:

```
User: ${principal} is not authorized to perform: ${action} on resource: ${resource} with an explicit deny in the ${policy_type} policy.
```

${principal}	Principal
${action}	Action of the request
${resource}	Resources to be accessed
${policy_type}	Policy type

Example Error Information

- **Implicit Deny in a Policy or Identity Policy**

  No policy or identity policy that explicitly allows the access is attached to the principal.

  Check whether the policy or identity policy attached to the principal contains an Allow statement for the specific action. You can contact the IAM administrator to add the Allow statement.

  ```
  User: ${principal} is not authorized to perform: ${action} on resource: ${resource} because no identity-based policy allows the ${action} action.
  ```

- **Explicit Deny in a Policy or Identity Policy**

  A policy or identity policy that explicitly denies the access is attached to the principal.

  Check whether the policy or identity policy attached to the principal contains a Deny statement for the specific action. You can contact the IAM administrator to delete the Deny statement.

  ```
  User: ${principal} is not authorized to perform: ${action} on resource: ${resource} with an explicit deny in an identity-based policy.
  ```

- **Implicit Deny in a Resource Policy**

  No resource policy explicitly allows the access to the resource.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Check whether the resource policy contains an Allow statement for the specific action. You can contact the administrator to obtain the permissions.

```
User: ${principal} is not authorized to perform: ${action} on resource: ${resource} because no resource-based policy allows the ${action} action.
```

- **Explicit Deny in a Resource Policy**

  A resource policy explicitly denies the access to the resource.

  Check whether the resource policy contains a Deny statement for the specific action. You can contact the administrator to delete the restriction.

  ```
  User: ${principal} is not authorized to perform: ${action} on resource: ${resource} with an explicit deny in a resource-based policy.
  ```

- **Implicit Deny in a Trust Policy**

  No trust policy in the trust agency explicitly allows the access.

  Check whether a trust policy in the trust agency contains the Allow statement for the specific operation. You can contact an administrator to add the Allow statement to the trust policy. Alternatively, check the principal who assumes the agency.

  ```
  User: ${principal} is not authorized to perform: ${action} on resource: ${resource} because no agency trust policy allows the ${action} action.
  ```

- **Explicit Deny in a Trust Policy**

  A trust policy in the trust agency explicitly denies the access.

  Check whether a trust policy in the trust agency contains a Deny statement for the specific action. You can contact the administrator to delete the restriction.

  ```
  User: ${principal} is not authorized to perform: ${action} on resource: ${resource} with an explicit deny in the agency trust policy.
  ```

- **Implicit Deny in a Session Policy**

  No session policy in the agency session explicitly allows the access.

  Check whether a session policy in the agency session contains an Allow statement for the specific action. You can contact the administrator to obtain the permissions.

  ```
  User: ${principal} is not authorized to perform: ${action} on resource: ${resource} because no session policy allows the ${action} action.
  ```

- **Explicit Deny in a Session Policy**

  A session policy in the agency session explicitly denies the access.

  Check whether a session policy in the agency session contains a Deny statement for the specific action. You can contact the administrator to delete the restriction.

  ```
  User: ${principal} is not authorized to perform: ${action} on resource: ${resource} with an explicit deny in a session policy.
  ```

- **Implicit Deny in an SCP**

  No service control policy (SCP) that explicitly allows the access is attached to the tenant, organization root, or organization unit where the principal belongs.

  Check whether the SCP attached to the tenant, organization root, or organization unit where the principal belongs lacks the Allow statement for the specific action. You can contact an organization administrator to obtain the required permissions.

  ```
  User: ${principal} is not authorized to perform: ${action} on resource: ${resource} because no service control policy allows the ${action} action.
  ```

- **Explicit Deny in an SCP**

An SCP that explicitly denies the access is attached to the tenant, organization root, or organization unit where the principal belongs.

Check whether the SCP attached to the tenant, organization root, or organization unit where the principal belongs contains the Deny statement for the specific action. You can contact an organization administrator to delete the restriction.

```
User: ${principal} is not authorized to perform: ${action} on resource: ${resource} with an explicit deny in a service control policy.
```

2 IAM User Management

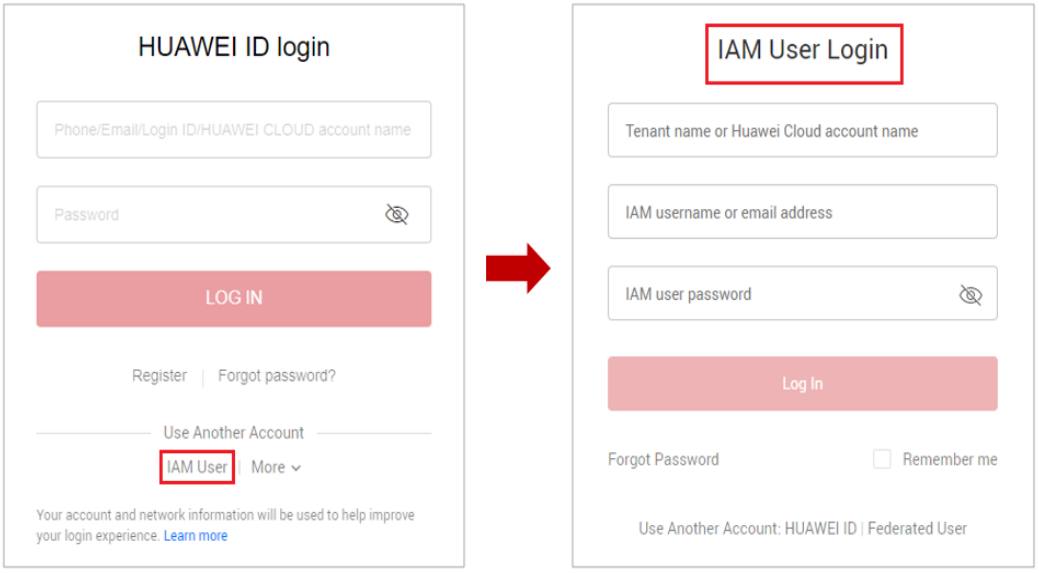
2.1 Why Does IAM User Login Fail?

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. Cause: The login entry is incorrect.
     Solution: Click **IAM User** on the login page.



  b. Cause: Incorrect mobile number/email address/account name/Huawei Cloud account or IAM username.
     Solution: Enter the correct mobile number/email address/account name/Huawei Cloud account and IAM username. If you do not know your IAM

username or the name of the account used to create the IAM user, contact the administrator.

c. Cause: The password is incorrect.

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

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

Solution: 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.**

  Cause: The administrator has set access control rules on the IAM console to limit access from specific IP address ranges, IP addresses, or IPv4 CIDR blocks to Huawei Cloud.

  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 on the left, choose **Security Settings**, and select the **Login Authentication Policy** tab.

NOTE

This setting is applied only for the IAM users created using your account.

Step 3 On the **Login Authentication Policy** tab, enter IP address ranges or IPv4 CIDR blocks that are allowed to access the console.

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

  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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

3 Security Settings

3.1 How Do I Enable Login Authentication?

To ensure account security, you are advised to bind an MFA device to enable login authentication.

After you bind an MFA device, MFA authentication is required for you or IAM users created using your account on the **Login Verification** page during their logins.

After you unbind the MFA device, you and your IAM users only need to enter the account name or username and password to log in.

Procedure

Step 1 Log in to the IAM console. In the navigation pane on the left, choose **Users**.

Step 2 Click a username to go to the user details page.

Step 3 Select the **Security Settings** tab and find **Multi-factor Authentication (MFA)**.

Step 4 Click **Add MFA Device**.

Step 5 Enter a device name. Only letters, digits, hyphens (-), and underscores (_) are allowed.

Step 6 Add a virtual MFA device by referring to **Adding a Virtual MFA Device**, or add a hardware MFA device by referring to **Adding a Hardware MFA Device**.

----End

3.2 How Do I Disable Login Authentication?

To ensure account security, you are advised to bind an MFA device to enable login authentication.

After you bind an MFA device, MFA authentication is required for you or IAM users created using your account on the **Login Verification** page during their logins.

After you unbind the MFA device, you and your IAM users only need to enter the account name or username and password to log in.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Procedure

Step 1 Log in to the IAM console. In the navigation pane on the left, choose **Users**.

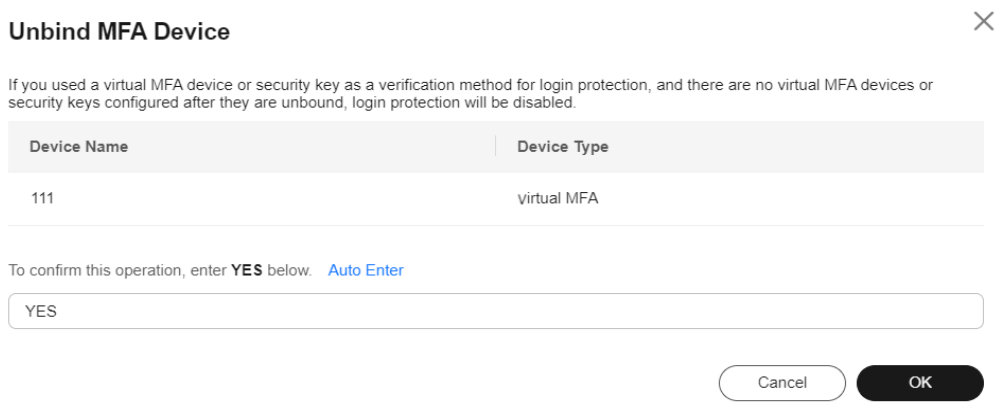
Step 2 Click a username to go to the user details page.

Step 3 Select the **Security Settings** tab and find **Multi-factor Authentication (MFA)**.

Step 4 Locate the MFA device and click **Unbind** in the **Operation** column.

Step 5 In the displayed dialog box, enter **Yes** to confirm unbinding. The following describes how to unbind an MFA device.

Figure 3-1 Confirming unbinding



Step 6 Click **OK**.

----End

3.3 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 you enable MFA-based login authentication, you need to enter a verification code after authenticating your username and password. MFA devices, together with your username and password, ensure the security of your account and resources.

MFA devices can be hardware-or software-based. A virtual MFA device is an application that generates 6-digit verification codes in compliance with the time-based one-time password (TOTP) standard. MFA applications can run on mobile devices (including smartphones) and are easy to use.

Prerequisites

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

Procedure

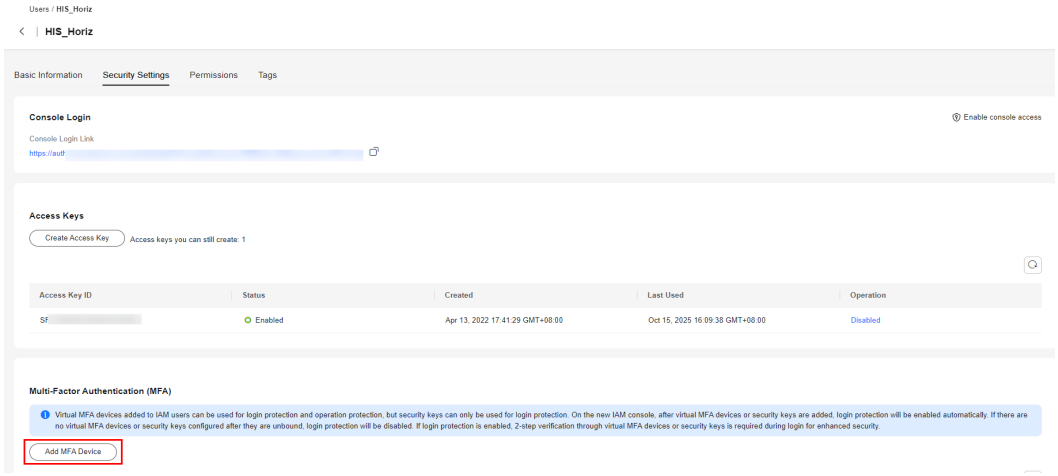
Step 1 Log in to the IAM console. In the navigation pane on the left, choose **Users**.

Step 2 Click a username to go to the user details page.

Step 3 Select the **Security Settings** tab and find **Multi-factor Authentication (MFA)**.

Step 4 Click **Add MFA Device**.

Figure 3-2 Adding an MFA device



Step 5 Enter a device name. Only letters, digits, hyphens (-), and underscores (_) are allowed.

Step 6 Select an MFA device.

Step 7 Click **Next** to go to the **Set MFA Device** step.

Step 8 Add an MFA device by scanning the QR code or entering the secret key.

- Scanning the QR code

  Open the MFA application and scan the QR code displayed in the **Set MFA Device** step. Then the user is added to the MFA device.

- Entering the secret key

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

  NOTE

  The user can be manually added only with time-based one-time passwords (TOTP). You are advised to enable automatic time setting on your mobile phone.

Step 9 In the **Set MFA Device** step, enter two consecutive verification codes and click **OK**.

Step 10 View the dynamic codes for MFA on the MFA App. The codes are automatically updated every 30 seconds.

----End

Related FAQs

3.4 How Do I Obtain a Virtual MFA Verification Code?

3.5 How Do I Unbind a Virtual MFA Device?

3.7 Why Does MFA Authentication Fail?

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

3.4 How Do I Obtain a Virtual MFA Verification Code?

After a virtual MFA device is added, you need to enter an MFA verification code when logging in to the console.

You can open the virtual MFA device on your mobile phone and get the verification code displayed under your user account. Then enter the code on the login page.

NOTE

If the verification fails, resolve the problem by referring to **3.7 Why Does MFA Authentication Fail?**

3.5 How Do I Unbind a Virtual MFA Device?

You can unbind a virtual MFA device as needed.

If you need MFA authentication again, you can bind a virtual MFA device on the **Security Settings** page. For details, see **3.3 How Do I Bind a Virtual MFA Device?**.

Procedure

Step 1 Log in to the IAM console. In the navigation pane on the left, choose **Users**.

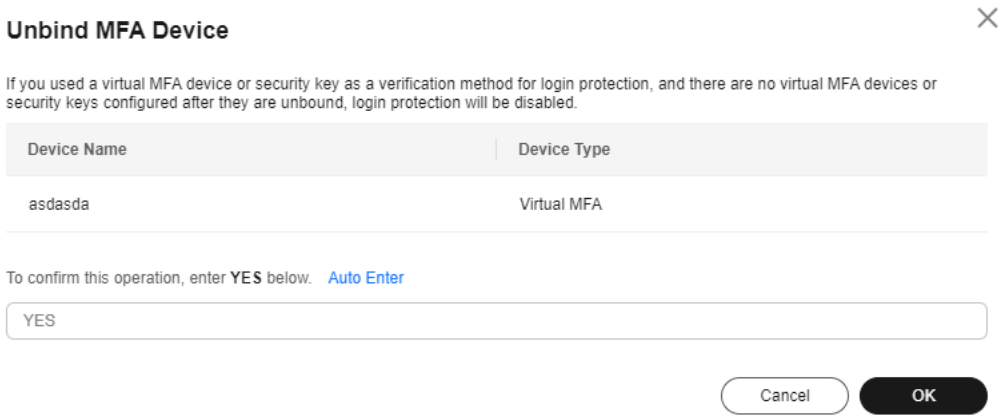
Step 2 Click a username to go to the user details page.

Step 3 Select the **Security Settings** tab and find **Multi-factor Authentication (MFA)**.

Step 4 Locate the virtual MFA device and click **Unbind** in the **Operation** column.

Step 5 In the displayed dialog box, enter **Yes** to confirm unbinding.

Figure 3-3 Confirming unbinding



Step 6 Click **OK**.

----End

3.6 What Should I Do If My MFA Device Is Lost?

- If your mobile phone is lost, you deleted the virtual MFA application, or the security key of your Huawei Cloud or HUAWEI ID is lost, call the customer service hotline 4000-955-988 to report the issue. The customer service personnel will reset the MFA device for you as soon as possible.
- If your mobile phone is lost, you deleted the virtual MFA application, or the security key of your IAM user is lost, contact the administrator to remove the MFA device.

Unbinding a Virtual MFA Device

Step 1 Log in to the **new IAM console** and choose **Users** in the navigation pane.

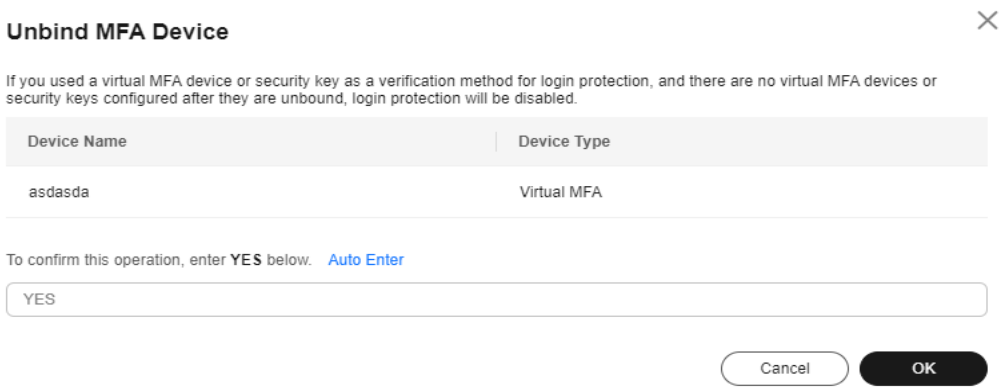
Step 2 Click a username to go to the user details page.

Step 3 Click the **Security Settings** tab and find **Multi-factor Authentication (MFA)**.

Step 4 Locate the virtual MFA device and click **Unbind** in the **Operation** column.

Step 5 In the displayed dialog box, enter **YES**.

Figure 3-4 Confirming unbinding



Step 6 Click **OK**.

----End

Unbinding a Security Key

Step 1 Log in to the **new IAM console** and choose **Users** in the navigation pane.

Step 2 Click a username to go to the user details page.

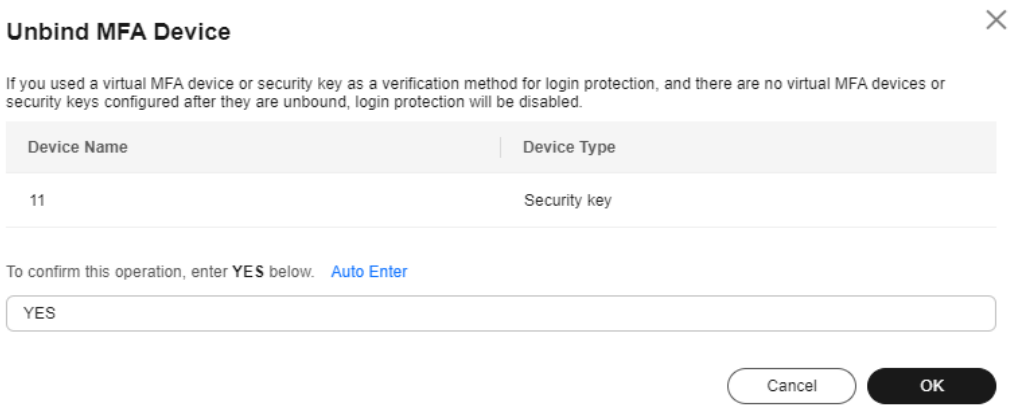
Step 3 Click the **Security Settings** tab and find **Multi-factor Authentication (MFA)**.

Step 4 Click **Unbind** in the **Operation** column of the target security key.

Step 5 In the displayed dialog box, enter **YES**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 3-5 Confirming unbinding



Step 6 Click **OK**.

----End

3.7 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 code is incorrect.
- The verification code has expired.
- The verification code belongs 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 code generated on your mobile phone will fail the verification.

Solution

- Enter the correct verification code.
- The verification code is automatically updated every 30 seconds. Enter two consecutive verification codes.
- Ensure that the account name displayed above the verification code on the MFA App 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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

on your mobile phone, because the MFA authentication will be based on UTC time.)

3.8 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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

3.9 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.

Cause

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.

Solution

- 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 **4.1 What Should I Do If I Forgot My Password?**
- If the account is locked for no reason, change the password. For details, see **4.2 How Do I Change My Password?**

3.10 What Can I Do If the System Displays a Message Indicating that the MFA Device Already Exists When I Attempt to Add It?

Symptom

On the new IAM console, you can choose **Users** in the left navigation pane and click **Security Settings** in the **Operation** column of the row containing the target user. In the **Multi-Factor Authentication (MFA)** area, click **Add MFA Device**, enter the device name, and click **Next**. Then the message **Virtual MFA device already exists.** is displayed.

Cause

- An MFA device has already been bound to the user. Each user can only have one MFA device bound.
- The virtual MFA device with the same name has been bound to another user in the account. The virtual MFA device name must be unique in the account.

Solution

On the new IAM console, choose **Users** > **Security Settings**. In the **Multi-Factor Authentication (MFA)** area, check whether an MFA device has been bound to the user or whether an MFA device with the same name has been bound to another user in the account.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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, **sign up for a HUAWEI ID and enable Huawei Cloud services**.

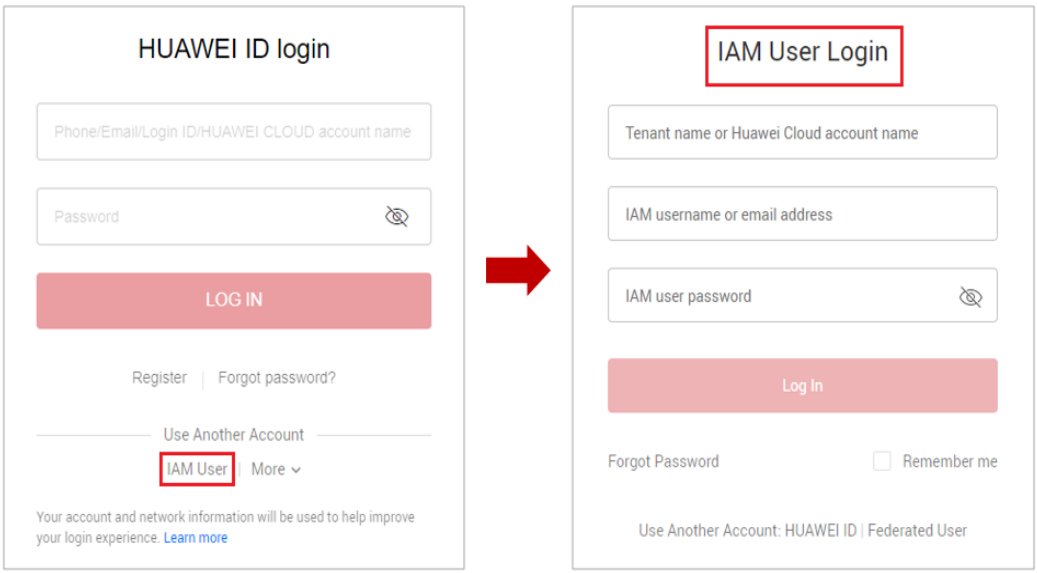
Resetting the Password of an IAM User

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**.

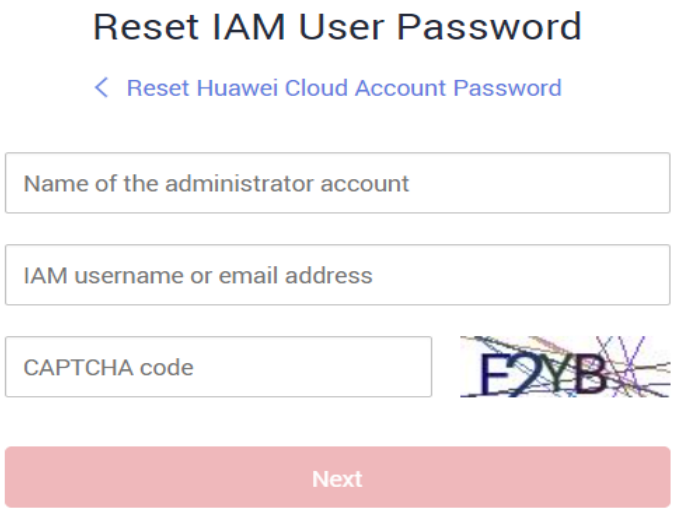
 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 4-1 Forgetting the password of an IAM user



Step 2 Enter the name of the administrator account, IAM username or email address, and CAPTCHA code.

Figure 4-2 Specifying IAM user details



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 login using an account, you will see the root user marked **Enterprise administrator** on the **Users** page of the IAM console.
- 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, contact the administrator to **reset your password**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 3 Select a verification method (account name, email address, or mobile number), complete the identity verification, and click **Next**.

NOTE

- Ensure that the mobile number or email address you entered is correct, or the password cannot be reset.
- If you cannot get the verification code, rectify this issue by referring to **3.8 Why Am I Not Getting the Verification Code?**

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

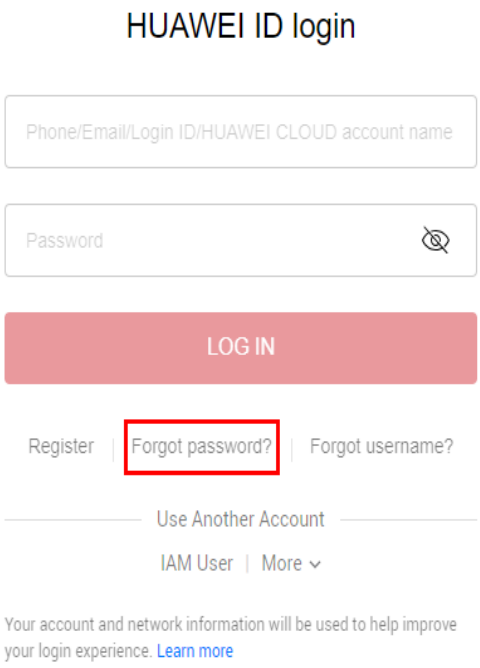
Step 5 Click **Log In** or wait to be redirected to the login page and use the new password to log in.

----End

Resetting the Password of an Account

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

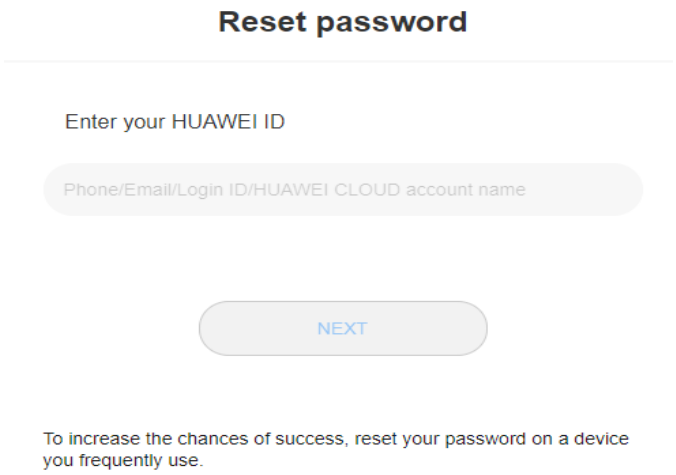
Figure 4-3 Forgetting the password of an account



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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 4-4 Specifying account details



Step 3 Get the verification code sent to the mobile number or email address you entered in **Step 2**.

NOTE

- If you cannot get the verification code, rectify this issue by referring to **3.8 Why Am I Not Getting the Verification Code?**
- If the mobile number or email address of the account is unavailable, contact customer service at +852-800-931-122 (Hong Kong, China).

Step 4 Perform the verification and click **NEXT**.

Step 5 Enter a new password, confirm it, and click **OK**.

HUAWEI ID is a unified identity that you can use to access all Huawei services. If the preceding steps do not work, you can reset the password of your HUAWEI ID from the following link:

https://consumer.huawei.com/en/support/content/en-us00770241/

Step 6 Click **RETURN NOW** and **log in to Huawei Cloud** using the new password.

----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, choose **My Credentials** from the drop-down list, click **Go to New Console**, and change your password in the **Login Credentials** area.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- If you have forgotten your password:
  - Reset your password by following the instructions in **4.1 What Should I Do If I Forgot My Password?**
  - If you are an IAM user, **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. Click **Go to New Console** in the upper right corner 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 have a password for logging in to the management console and the access key is lost or needs to be reset, request the administrator to **create an access key on the IAM console** and send it to you.

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

If you have forgotten your access key, you can delete it and create a new one. For details, see **Creating Access Keys**.

NOTE

If you cannot manage your access keys, request your **administrator** to:

- **Create an access key on the IAM console** and send it to you.
- **Assign required permissions to you**.

4.5 Why Can't I Add a Security Key Device?

Symptom

An IAM user encounters an error when adding a security key device, and cannot bind the security key for login protection.

Possible Causes

- You do not have the permission to add a security key.
- Your device does not support security keys.
- Your browser version is too early.

Solutions

- Check whether your IAM user has the required permissions for security keys. For example, to add a security key, you need the **iam:mfa:enableV5** action.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

To delete a security key, you need the **iam:mfa:disableV5** action. To list security keys, you need the **iam:mfa:listMFADevicesV5** action.

- Check whether Windows Hello has been enabled in Windows settings. You will need to pass identity verification with your fingerprint, PIN, or facial information. Another option for identity verification is hardware devices that support FIDO2.
- Check whether you are using the latest version of your browser. The latest Google Chrome is recommended. Ensure that your browser does not contain any plugins incompatible with WebAuthn. Disable all incompatible plugins and try again.

4.6 How Do I Obtain an Access Key (AK/SK) in the EU-Dublin Region?

Symptom

You have enabled cloud services in the **EU-Dublin** region as an administrator. You and IAM users in your account need to use access keys in this region for encryption and signing.

Users access cloud services in the **EU-Dublin** 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 **EU-Dublin** 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 **EU-Dublin** region as an administrator. To create an access key for yourself, go to 2.

1. Log in to Huawei Cloud as an administrator, click  on the console homepage, and select the **EU-Dublin** region.
2. On the console of the **EU-Dublin** region, choose **Management & Deployment** > **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 in the **EU-Dublin** region as an administrator.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

2. On the **Users** page, locate the IAM user created in **4.6 How Do I Obtain an Access Key (AK/SK) in the EU-Dublin Region?** and click **Security Settings** in the **Operation** column.
3. On the user details page, select the **Security Settings** tab and click **Create Access Key**.
4. (Optional) Enter a description for the access key.
5. Click **OK**.
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.
   - You and the IAM user can use the access key only in the **EU-Dublin** region.
7. (Optional) Provide the access key to the IAM user.

----End

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

5 Agency Management

5.1 How Can I Obtain Permissions to Create a Trust Agency?

Symptom

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

Possible Causes

You do not have permissions to use IAM.

Only the following users can use IAM:

- Account root user (with permissions to access all services, including IAM)
- IAM users added to the **admin** group (with full permissions for all services, including IAM)
- IAM users with **IAMFullAccessPolicy** permissions (IAM administrator, with permissions to access IAM)

Solution

- Request the administrator to **create a trust agency**.
- Request the administrator to **assign required permissions to you**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

5.2 What Can I Do If I Cannot Access the Consoles and APIs of Some Cloud Services After I Switch to a Trust Agency?

Symptom

An account (delegating account) creates a trust agency for another account (delegated account). After switching to the trust agency, the delegated account cannot access the consoles and APIs of some cloud services.

Possible Causes

- The cloud service does not support trust agencies. For details about services that support trust agencies, see **Cloud Services for Using Identity Policies and Trust Agencies**.
- The cloud service supports trust agencies, but permissions required for accessing cloud services are not assigned to the switched trust agency.
- The cloud service supports trust agencies and required permissions are assigned to the switched trust agency, but the console or API of the cloud service indirectly accesses other cloud services that do not support trust agencies.

Solution

- If the cloud service does not support trust agencies, you can create an agency and assign permissions required for accessing cloud services to the agency. For details about the differences between trust agencies and agencies, see **Trust Policy**.
- If the cloud service supports trust agencies, assign permissions required for accessing cloud services to the switched trust agency.
- If the cloud service indirectly accesses other cloud services that do not support trust agencies, create an agency and assign permissions required for accessing cloud services to the agency.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

6 Account Management

6.1 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.

Solution

- 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 6-1**. Otherwise, choose **Huawei Cloud Account**, as shown in **Figure 6-2**.
- If you are an IAM user, log in by choosing **IAM User** on the login page. If the login fails, see **2.1 Why Does IAM User Login Fail?**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 6-1 Logging in using a HUAWEI ID

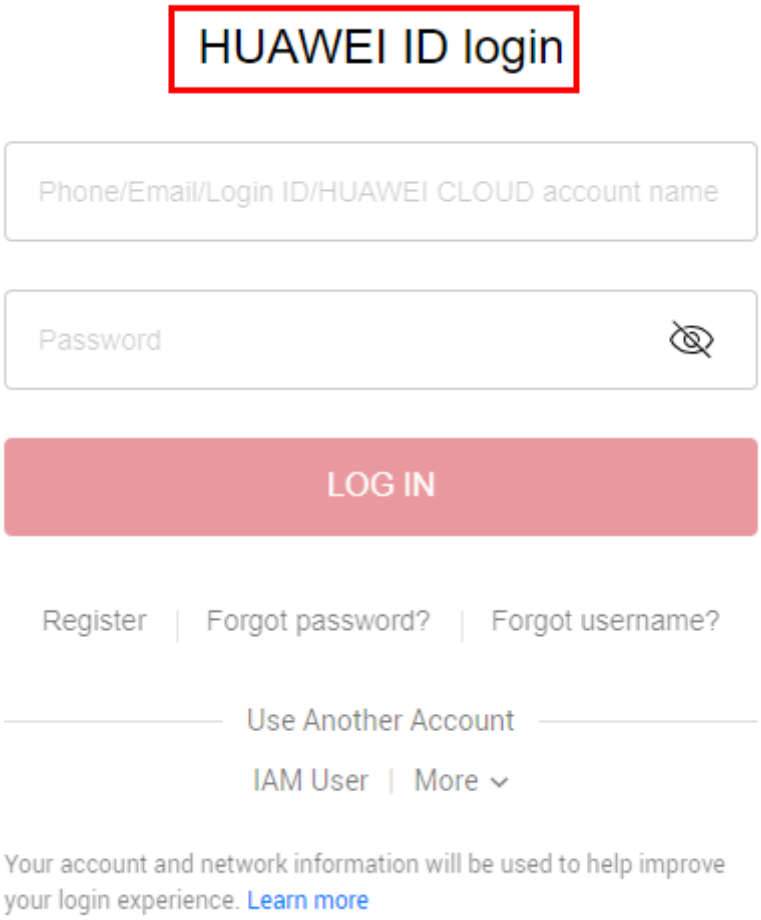
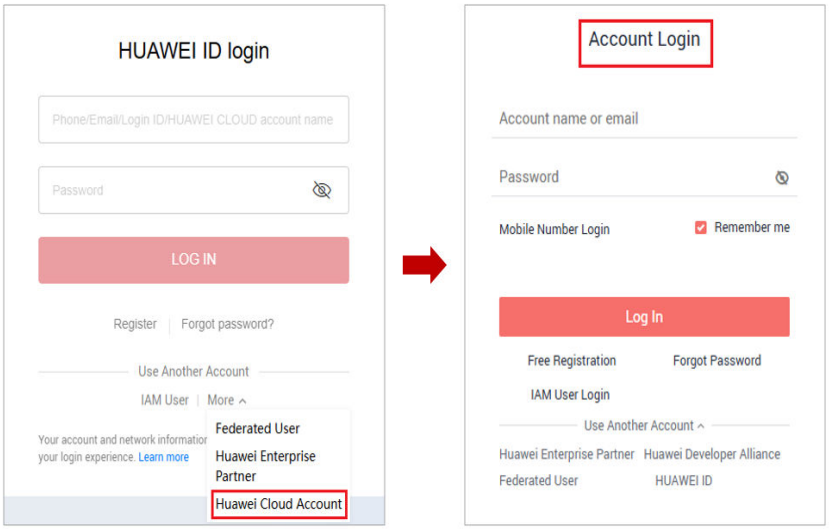


Figure 6-2 Logging in using a Huawei Cloud account



 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- 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.

6.2 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

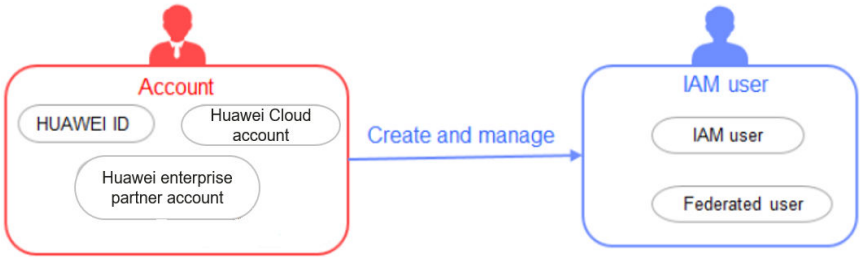
The Huawei Cloud account system consists of two types of accounts:

- **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.

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

If you are an IAM user created by an account, you can log in to Huawei Cloud through the **IAM User** entry and use resources and cloud services based on the permissions granted by the account.



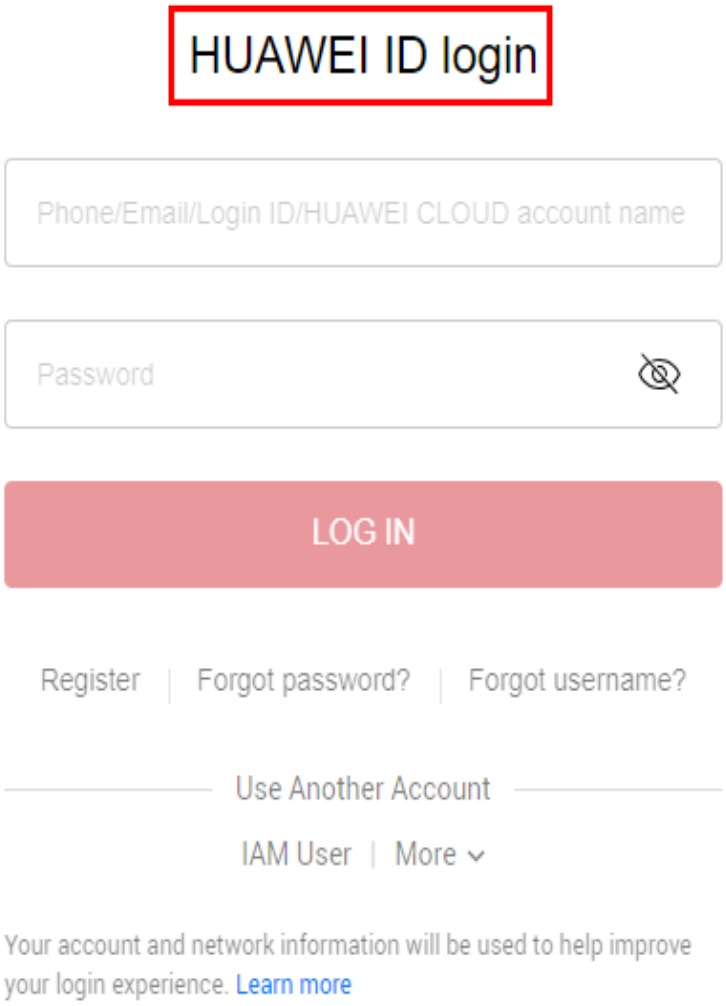
 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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.



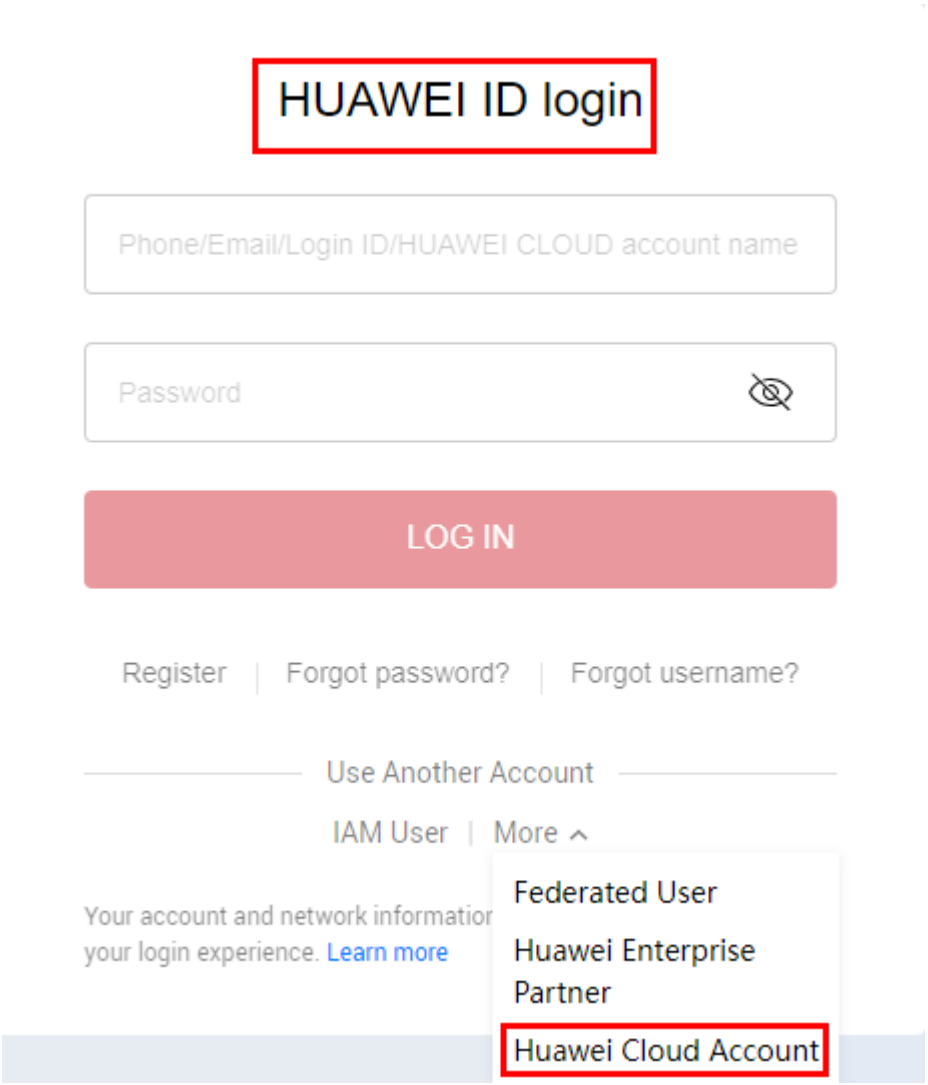
Huawei Cloud Account

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

Registration: To improve login experience, we have unified our account system. You can only register HUAWEI IDs on Huawei Cloud from October 30, 2021.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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



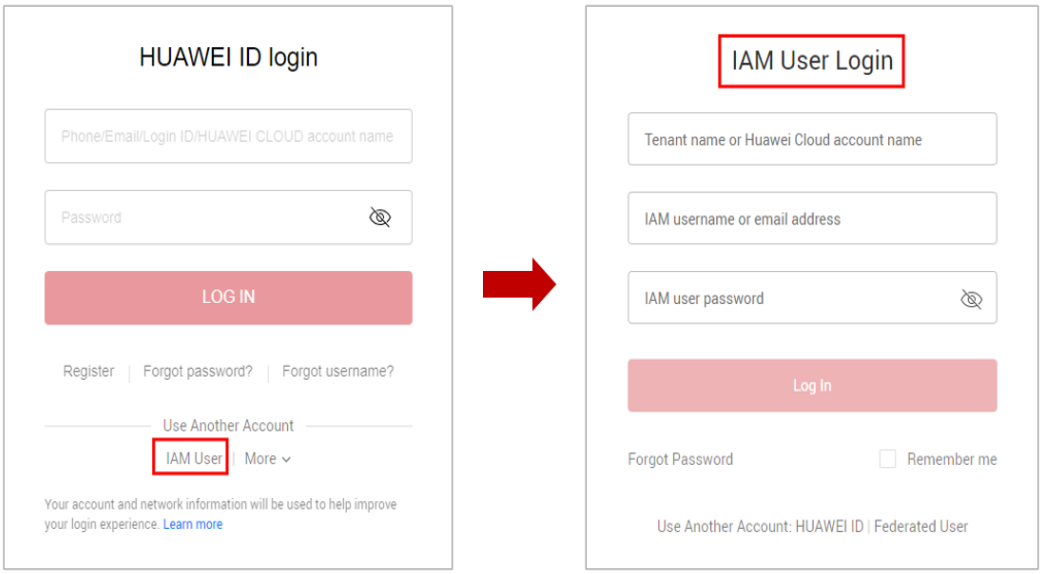
IAM User

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**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.



Other

If you already have a **Huawei enterprise partner account**, you can use this account to log in to Huawei Cloud and access Huawei Cloud resources.

6.3 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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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.

6.4 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.

6.5 What Can I Do If the Account Root User Does Not Have Permissions?

Symptom

The account root user cannot access Huawei Cloud console or APIs, with a message indicating insufficient permissions.

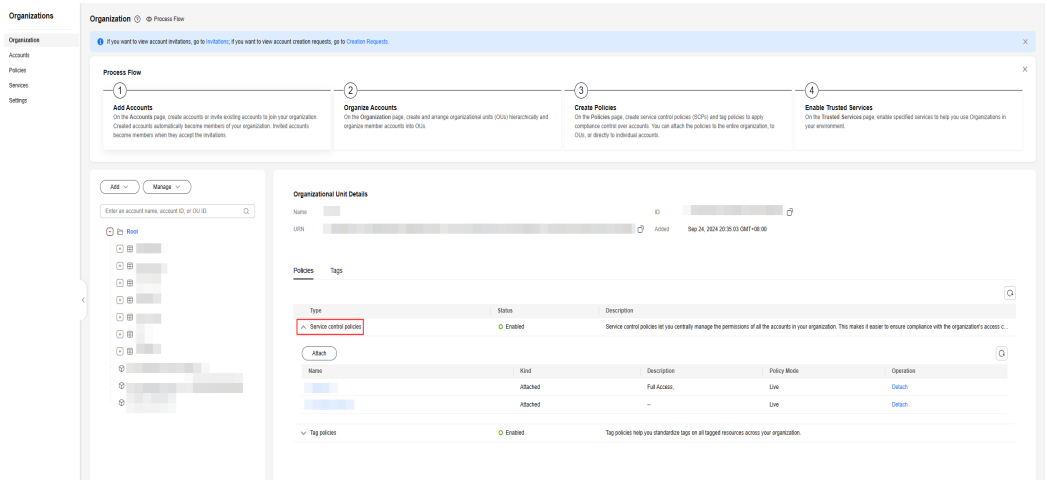
Possible Causes

Your account may be a member of an organization and the organization administrator may have set service control policies (SCPs) to restrict access permissions of your account root user.

Solutions

Go to the Organizations console to check the SCPs attached to your account, and contact the organization administrator to modify the SCPs or detach them.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.


Organizations
Organization
Accounts
Policies
Services
Settings
Organization
Process Flow
Process Flow
1
Add Accounts
2
Organize Accounts
3
Create Policies
4
Enable Trusted Services
Add
Manage
Root
Organizational Unit Details
Policies
Tags
Type
Status
Description
Service control policies
Enabled
Attach
Name
Kind
Description
Policy Mode
Operation
Attached
Full Access
Live
Detach
Tag policies
Enabled