

Identity and Access Management

User Guide

Date **2023-05-30**

Contents

1 Service Overview.....	1
1.1 What Is IAM?.....	1
1.2 Basic Concepts.....	3
1.3 Functions.....	7
1.4 Supported Cloud Services.....	9
1.5 Personal Data Protection.....	13
1.6 Permissions.....	15
1.7 Notes and Constraints.....	22
2 Getting Started.....	25
2.1 Before You Start.....	25
2.2 Step 1: Create User Groups and Assign Permissions.....	27
2.3 Step 2: Create IAM Users and Log In.....	29
3 User Guide.....	33
3.1 Before You Start.....	33
3.2 IAM Users.....	36
3.2.1 Creating an IAM User.....	36
3.2.2 Assigning Permissions to an IAM User.....	39
3.2.3 Logging In as an IAM User.....	40
3.2.4 Viewing or Modifying IAM User Information.....	41
3.2.5 Deleting an IAM User.....	46
3.2.6 Changing the Login Password of an IAM User.....	47
3.2.7 Managing Access Keys for an IAM User.....	47
3.3 User Groups and Authorization.....	49
3.3.1 Creating a User Group and Assigning Permissions.....	49
3.3.2 Adding Users to or Removing Users from a User Group.....	53
3.3.3 Deleting a User Group.....	55
3.3.4 Viewing or Modifying User Group Information.....	56
3.3.5 Revoking Permissions of a User Group.....	59
3.3.6 Assigning Dependency Roles.....	60
3.4 Permissions Management.....	61
3.4.1 Basic Concepts.....	61
3.4.2 Roles.....	62

3.4.3 Policies.....	63
3.4.3.1 Policy Content.....	63
3.4.3.2 Policy Syntax.....	64
3.4.3.3 Authentication Process.....	69
3.4.4 Authorization Records.....	70
3.4.5 Custom Policies.....	72
3.4.5.1 Creating a Custom Policy.....	72
3.4.5.2 Modifying or Deleting a Custom Policy.....	78
3.4.5.3 Custom Policy Use Cases.....	79
3.4.5.4 Cloud Services that Support Resource-Level Authorization Using IAM.....	82
3.5 Projects.....	83
3.6 Agencies.....	85
3.6.1 Account Delegation.....	85
3.6.1.1 Delegating Resource Access to Another Account.....	85
3.6.1.2 Creating an Agency (by a Delegating Party).....	86
3.6.1.3 (Optional) Assigning Permissions to an IAM User (by a Delegated Party).....	88
3.6.1.4 Switching Roles (by a Delegated Party).....	90
3.6.2 Cloud Service Delegation.....	91
3.6.3 Deleting or Modifying Agencies.....	93
3.7 Security Settings.....	94
3.7.1 Security Settings Overview.....	94
3.7.2 Basic Information.....	95
3.7.3 Critical Operation Protection.....	95
3.7.4 Login Authentication Policy.....	104
3.7.5 Password Policy.....	106
3.7.6 ACL.....	108
3.8 Identity Providers.....	109
3.8.1 Introduction.....	109
3.8.2 Identity Federation via SAML.....	111
3.8.2.1 Configuration of SAML-based Federated Identity Authentication.....	111
3.8.2.2 Step 1: Create an IdP Entity.....	114
3.8.2.3 Step 2: Configure Identity Conversion Rules.....	118
3.8.2.4 (Optional) Step 3: Configure a Federated Login Entry in the Enterprise IdP.....	121
3.8.3 Identity Federation Via OpenID Connect.....	122
3.8.3.1 Configuration of OpenID Connect-based Federated Identity Authentication.....	122
3.8.3.2 Step 1: Create an IdP Entity.....	123
3.8.3.3 Step 2: Configure Identity Conversion Rules.....	128
3.8.3.4 (Optional) Step 3: Configure a Federated Login Entry in the Enterprise IdP.....	130
3.8.4 Syntax of Identity Conversion Rules.....	131
3.9 MFA Authentication and Virtual MFA Device.....	137
3.9.1 MFA Authentication.....	137
3.9.2 Virtual MFA Device.....	138

3.10 Viewing IAM Operation Records.....	141
3.10.1 Enabling CTS.....	141
3.10.2 Viewing IAM Audit Logs.....	144
3.11 Quotas.....	145
4 FAQs.....	147
4.1 User Groups and Permissions Management.....	147
4.1.1 Why Can't I Find Permissions for a Cloud Service?.....	147
4.1.2 Why Permissions Granted to a User Do Not Take Effect?.....	147
4.2 IAM User Management.....	149
4.2.1 Why Does IAM User Login Fail?.....	149
4.2.2 How Do I Control IAM User Access to the Console?.....	150
4.3 Security Settings.....	150
4.3.1 How Do I Enable Login Verification?.....	150
4.3.2 How Do I Disable Login Verification?.....	151
4.3.3 How Do I Change the Verification Method for Performing Critical Operations?.....	152
4.3.4 How Do I Disable Operation Protection?.....	153
4.3.5 How Do I Bind a Virtual MFA Device?.....	155
4.3.6 How Do I Obtain a Virtual MFA Verification Code?.....	157
4.3.7 How Do I Unbind or Remove a Virtual MFA Device?.....	157
4.3.8 Why Does MFA Authentication Fail?.....	158
4.3.9 Why Am I Not Getting the Verification Code?.....	159
4.3.10 Why Is My Account Locked?.....	159
4.3.11 Why Do I Still Need to Perform MFA During Login After Unbinding the Virtual MFA Device?.....	160
4.4 Passwords and Credentials.....	161
4.4.1 How Do I Reset My Password?.....	161
4.4.2 How Do I Change My Password?.....	162
4.4.3 How Do I Obtain an Access Key (AK/SK)?.....	163
4.4.4 What Should I Do If I Have Forgotten My Access Key (AK/SK)?.....	163
4.4.5 What Are Temporary Security Credentials (AK/SK and SecurityToken)?.....	163
4.4.6 How Do I Obtain a Token with Security Administrator Permissions?.....	164
4.5 Agency Management.....	165
4.5.1 How Can I Obtain Permissions to Create an Agency?.....	165
4.6 Others.....	166
4.6.1 Why Is the Field-Level Help Always Displayed?.....	166
4.6.2 How Do I Disable Autofill Password on Google Chrome?.....	166
4.6.3 Region and AZ.....	167
5 Change History.....	169

1 Service Overview

- [1.1 What Is IAM?](#)
- [1.2 Basic Concepts](#)
- [1.3 Functions](#)
- [1.4 Supported Cloud Services](#)
- [1.5 Personal Data Protection](#)
- [1.6 Permissions](#)
- [1.7 Notes and Constraints](#)

1.1 What Is IAM?

Identity and Access Management (IAM) provides permissions management to help you securely control access to your cloud services and resources.

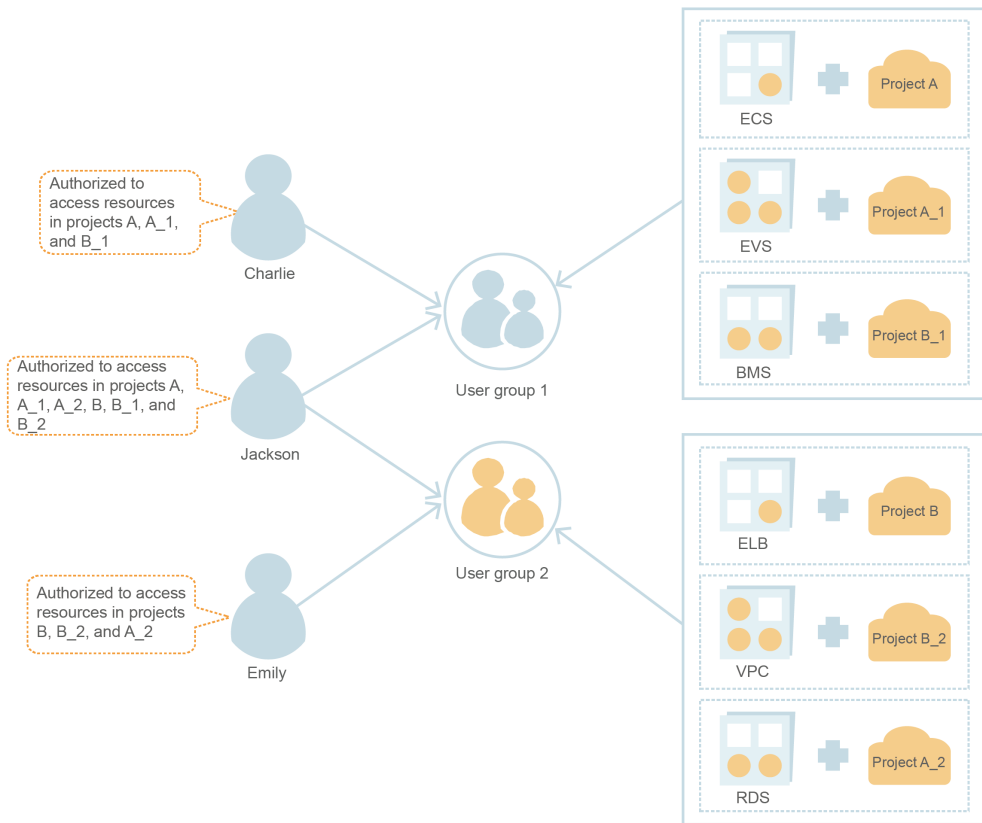
Advantages

Fine-grained access control for resources

When you successfully register with the cloud platform, your account is automatically created. Your account has full access permissions for your cloud services and resources.

If you create multiple resources on the cloud platform, such as Elastic Cloud Servers (ECSs), Elastic Volume Services (EVs), and Bare Metal Servers (BMSs), for different teams or applications in your enterprise, you can use your account to create IAM users for the team members or applications and grant them permissions required to complete specific tasks. The IAM users use their own usernames and passwords to log in to the cloud platform and access resources in your account.

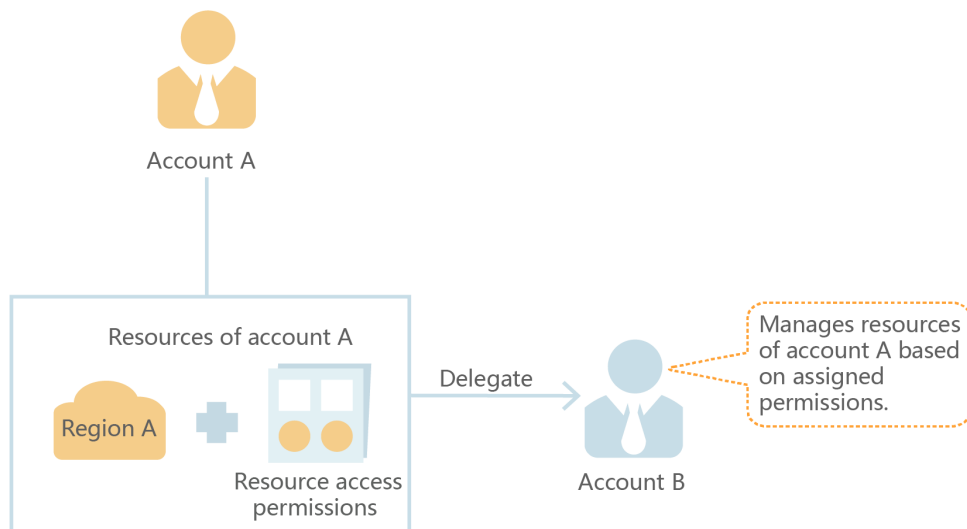
In addition to IAM, you can use Enterprise Management to control access to cloud resources. Enterprise Management supports more fine-grained permissions management and enterprise project management. You can choose either IAM or Enterprise Management to suit your requirements.



Cross-account resource access delegation

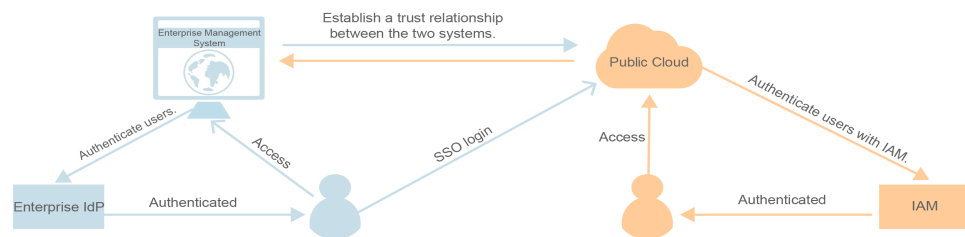
If you create multiple resources on the cloud platform, you can delegate another account to manage some of your resources for efficient O&M.

For example, you can create an agency for a professional O&M company to enable the company to manage specific resources with the company's own account. If the delegation changes, you can modify or revoke the delegated permissions at any time. In the following figure, account A is the delegating party, and account B is the delegated party.



Federated access to the cloud platform with existing enterprise accounts (identity federation)

If your enterprise has an identity system, you can create an identity provider (IdP) in IAM to provide single sign-on (SSO) access to the cloud platform for employees in your enterprise. The identity provider establishes a trust relationship between your enterprise and the cloud platform, allowing the employees to access the cloud platform using their existing accounts.



Access Methods

You can access IAM using either of the following methods:

- **Management console**
Access IAM through the management console — a browser-based visual interface.
- **REST APIs**
Access IAM using REST APIs in a programmable way.

1.2 Basic Concepts

The following are basic concepts that you need to understand before you get started with the IAM service.

Account

An account is created after you successfully register with the cloud platform. Your account has full access permissions for your cloud resources. You can use the account to reset user passwords and assign permissions.

IAM User

You can use your account to create IAM users and assign permissions for specific resources. Each IAM user has their own identity credentials (password or access keys) and uses cloud resources based on assigned permissions.

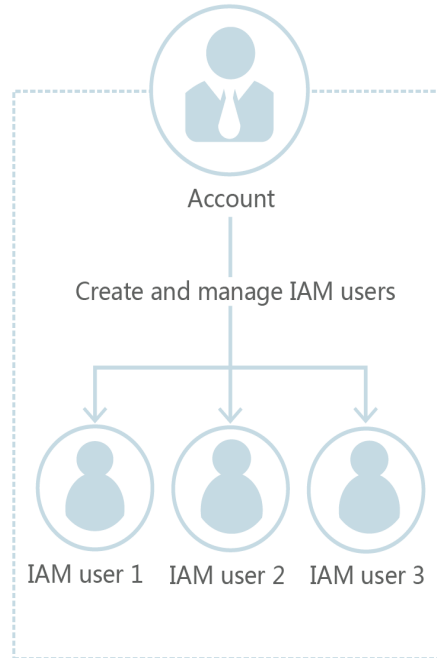
If an IAM user forgets their password, the user can reset the password by referring to "How Do I Reset My Password?" in the *Identity and Access Management FAQs*.

Relationship Between an Account and Its IAM Users

An account and its IAM users have a parent-child relationship. IAM users are created by an account, and they only have the permissions granted by the

account. The account can modify or revoke the IAM users' permissions at any time.

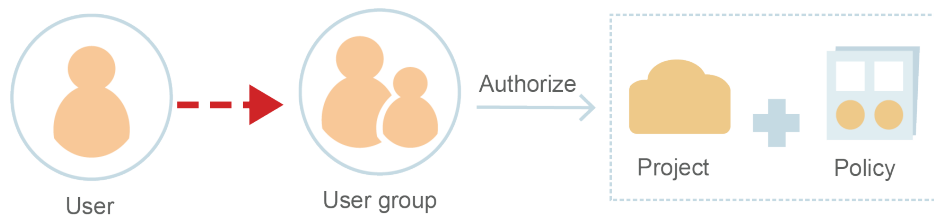
Figure 1-1 Account and IAM users



Authorization

Authorization is the process of granting required permissions for a user to perform specific tasks. After a system-defined or custom policy is assigned to a user group, users in the group inherit the permissions defined by the policy to manage resources.

Figure 1-2 Authorization process



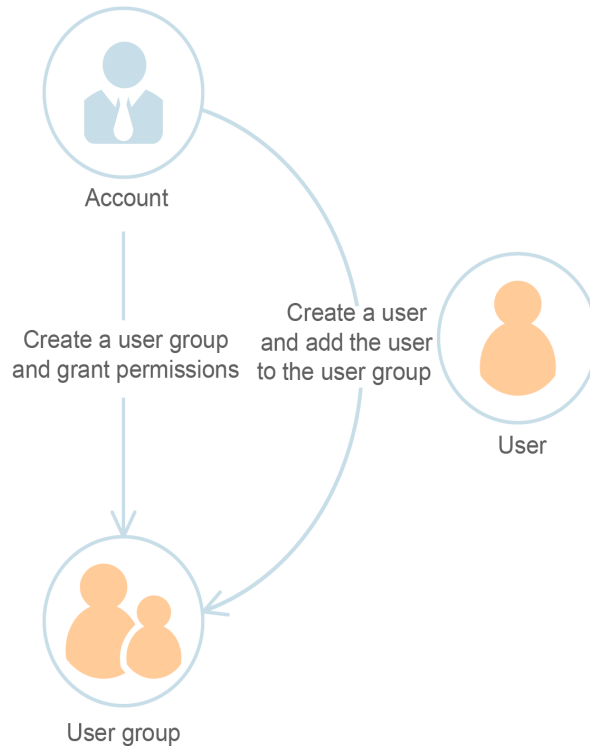
User Group

An IAM user group is a collection of IAM users. User groups let you specify permissions for multiple users, which can make it easier to manage the permissions for those users. IAM users added to a user group automatically obtain the permissions assigned to the group. If a user is added to multiple user groups, the user inherits the permissions from all these groups.

There is a default user group **admin**. It has all the permissions required to use all of the cloud resources. IAM users in this group can perform operations on all

resources, including but not limited to creating user groups and users, assigning permissions, and managing resources.

Figure 1-3 User group and users



Permissions

You can grant permissions by using roles and policies.

- **Roles:** A coarse-grained authorization strategy provided by IAM to assign permissions based on users' job responsibilities. Only a limited number of service-level roles are available for authorization.
- **Policies:** A fine-grained authorization strategy that defines permissions required to perform operations on specific cloud resources under certain conditions. This type of authorization is more flexible and is ideal for least privilege access. For example, you can grant users only permission to manage ECSs of a certain type. IAM supports both system-defined and custom policies.
 - A **system-defined policy** defines the common actions of a cloud service. System-defined policies can be used to assign permissions to user groups, and cannot be modified. If you need to assign permissions for a specific service to a user group or agency on the IAM console but cannot find corresponding policies, it indicates that the service does not support permissions management through IAM.
 - Custom policies function as a supplement to system-defined policies. You can create custom policies using the actions supported by cloud services for more refined access control. You can create custom policies in the visual editor or in JSON view.

Figure 1-4 Example permissions

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "apm:*:*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

Credentials

Credentials confirm the identity of a user when the user accesses the cloud platform through the console or APIs. Credentials can be either a password or access keys. You can manage your own credentials and your IAM users' credentials.

- Password: A common credential for logging in to the management console or calling APIs.
- Access key: An access key ID/secret access key (AK/SK) pair, which can only be used to call APIs. Each access key provides a signature for cryptographic authentication to ensure that access requests are secret, complete, and correct.

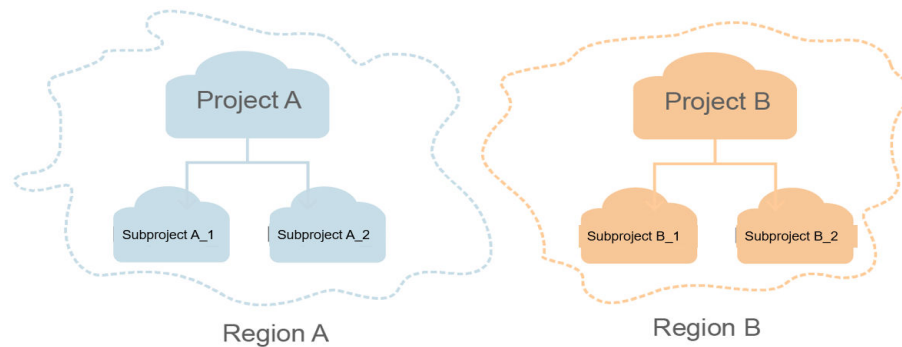
Virtual MFA Device

A virtual MFA device is an application that generates 6-digit verification codes in compliance with the Time-based One-time Password Algorithm (TOTP) standard. MFA devices can be hardware- or software-based. The cloud platform only supports software-based virtual MFA devices, which are application programs running on smart devices such as mobile phones.

Project

A region corresponds to a project. Default projects are defined to group and physically isolate resources (including computing, storage, and network resources) across regions. You can grant users permissions in a default project to access all resources in the region associated with the project. If you need more refined access control, you can create subprojects under a default project and create resources in subprojects. Then you can assign required permissions for users to access only resources in specific subprojects.

Figure 1-5 Projects



Enterprise Project

Enterprise projects allow you to group and manage resources across regions. Resources in enterprise projects are logically isolated from each other. An enterprise project can contain resources of multiple regions, and you can easily add resources to or remove resources from enterprise projects.

Agency

A trust relationship that you can establish between your account and another account or a cloud service to delegate resource access.

- Account delegation: You can delegate another account to implement O&M on your resources based on assigned permissions.
- Cloud service delegation: Services on the cloud platform interwork with each other, and some cloud services are dependent on other services. You can create an agency to delegate a cloud service to access other services.

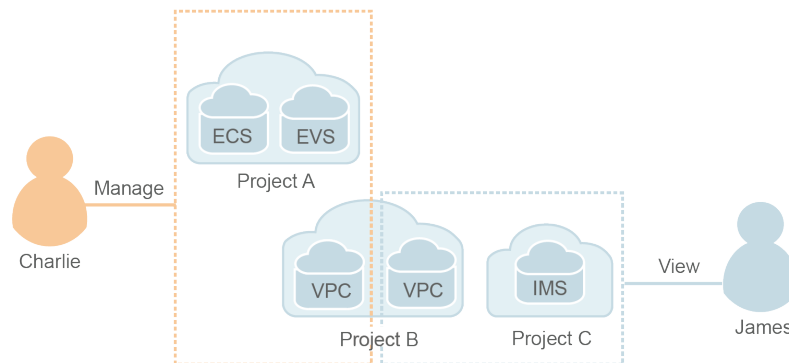
1.3 Functions

IAM provides a variety of functions for you to secure access to your resources.

Refined Permissions Management

You can grant IAM users permissions to manage different resources in your account. As shown in the following figure, you can grant Charlie permission to manage Virtual Private Cloud (VPC) resources in project B, and only grant James permission to view VPC resources in project B.

Figure 1-6 Permissions management model



Secure Access

Instead of sharing your password with others, you can create IAM users for employees or applications in your organization and generate identity credentials for them to securely access specific resources based on assigned permissions.

Critical Operation Protection

IAM provides login protection and critical operation protection, making your account and resources more secure. When you or users created using your account log in to the console or perform a critical operation, you and the users need to complete authentication by email, SMS, or virtual MFA device.

User Group-based Permissions Assignment

With IAM, you do not need to assign permissions to single users. Instead, you can manage users by group and assign permissions to the specified group. Each user then inherits permissions from their groups. To change the permissions of a user, you can remove the user from the original groups or add the user to other groups.

Project-based Resource Isolation

You can create subprojects in a region so that resources in that region can be isolated from each other.

Federated Identity Authentication

Enterprises with identity authentication systems can access the cloud platform through single sign-on (SSO), eliminating the need to create users on the cloud platform.

Resource Management Delegation

You can delegate more professional, efficient accounts or other cloud services to manage specific resources in your account.

Account Security Settings

Login authentication and password policies and access control list (ACL) improve security of user information and system data.

Eventual Consistency

Results of your IAM operations, such as creating users and user groups and assigning permissions, may not take effect immediately because data is replicated across different servers in the cloud platform's data centers around the world. Ensure that the operation results have taken effect before you perform any other operations that depend on them.

1.4 Supported Cloud Services

IAM provides identity authentication and permissions management for other services. Users created in IAM can access these services based on assigned permissions. For all permissions of the services supported by IAM, see [Permissions](#). For services that are not supported by IAM, you can only use your account to access these services.

The following lists the IAM-supported services and table heading descriptions.

- **Service:** Name of a cloud service that supports permissions management using IAM.
- **Scope:** The region where access permissions for a service can be assigned using IAM.
 - **Global regions:** Services deployed for all regions. Permissions for these services must be assigned in global regions. Users do not need to switch regions when they access these services.
 - **Specific regions:** Services deployed for specific regions are called project-level services. Permissions for these services need to be assigned in specific regions and take effect only for these regions. Users need to switch to one of these regions when they access the services.
- **Console:** Whether a service supports permissions management using the IAM console.
- **API:** Whether a service supports permissions management using APIs.
- **Agency:** Whether a service can be delegated to access and manage other cloud services on your behalf.
- **Policy:** Whether a service supports policy-based permissions management. A policy is a set of permissions defining the operations that can be performed on specific cloud resources.

NOTE

√: supported; x: not supported

Compute

Service	Scope	Console	API	Agency	Policy
Elastic Cloud Server (ECS)	Specific regions	√	√	√	√
Bare Metal Server (BMS)	Specific regions	√	√	√	√
Auto Scaling (AS)	Specific regions	√	√	x	√
Image Management Service (IMS)	Specific regions	√	√	√	√
Cloud Container Engine (CCE)	Specific regions	√	√	x	√
FunctionGraph	Specific regions	√	√	√	x

Storage

Service	Scope	Console	API	Agency	Policy
Elastic Volume Service (EVS)	Specific regions	√	√	x	√
Object Storage Service (OBS)	Global regions	√	√	√	√
Cloud Backup and Recovery (CBR)	Specific regions	√	√	x	√

Network

Service	Scope	Console	API	Agency	Policy
Virtual Private Cloud (VPC)	Specific regions	√	√	x	√
Elastic Load Balance (ELB)	Specific regions	√	√	x	√
Domain Name Service (DNS)	Global regions	√	√	x	x
NAT Gateway	Specific regions	√	√	x	√

Database

Service	Scope	Console	API	Agency	Policy
Relational Database Service (RDS)	Specific regions	√	√	x	√
Document Database Service (DDS)	Specific regions	√	x	x	√
Distributed Database Middleware (DDM)	Specific regions	√	√	x	√
Data Replication Service (DRS)	Specific regions	√	√	x	x
Data Admin Service (DAS)	Specific regions	√	x	x	x

Security

Service	Scope	Console	API	Agency	Policy
Web Application Firewall (WAF)	Specific regions	√	x	x	x
Host Security Service (HSS)	Specific regions	√	x	x	x
Database Security Service (DBSS)	Specific regions	√	x	x	√
Container Guard Service (CGS)	Specific regions	√	x	x	√

Management & Deployment

Service	Scope	Console	API	Agency	Fine-Grained Policy
Identity and Access Management (IAM)	Global regions	√	√	x	√
Cloud Eye	Specific regions	√	√	x	x
Cloud Trace Service (CTS)	Specific regions	√	√	x	x
Log Tank Service (LTS)	Specific regions	√	√	x	√
Application Performance Management (APM)	Specific regions	√	√	x	√
Application Operations Management (AOM)	Specific regions	√	√	x	√

Application

Service	Scope	Console	API	Agency	Policy
ServiceStage	Specific regions	√	√	x	x
Distributed Cache Service (DCS)	Specific regions	√	√	x	√
Simple Message Notification (SMN)	Specific regions	√	√	x	x
API Gateway	Specific regions	√	√	x	x

EI

Service	Scope	Console	API	Agency	Fine-Grained Policy
ModelArts	Specific regions	√	√	√	√
MapReduce Service (MRS)	Specific regions	√	√	x	√
Data Warehouse Service (DWS)	Specific regions	√	√	√	√
Data Lake Insight (DLI)	Specific regions	√	√	x	x
Cloud Search Service (CSS)	Specific regions	√	√	√	x
Graph Engine Service (GES)	Specific regions	√	√	√	x

Migration

Service	Scope	Console	API	Agency	Policy	Enterprise Project
Server Migration Service (SMS)	Global regions	√	x	x	√	x

1.5 Personal Data Protection

To prevent personal data (such as the username, password, and mobile number) from being accessed by unauthorized entities or individuals, IAM encrypts the data before storing it, controls access to the data, and can check all operations performed on the data from operation logs.

Personal Data

[Table 1-1](#) lists the personal data generated or collected by IAM.

Table 1-1 Personal data

Type	Source	Modifiable	Mandatory
Username	<ul style="list-style-type: none"> Entered when you create a user on the management console. Entered when you call an API. 	No	Yes Usernames are used to identify users.
Password	<ul style="list-style-type: none"> Entered when you create a user, modify user credentials, or reset the password on the management console. Entered when you call an API. 	Yes	No You can also choose AK/SK authentication.
Email address	Entered when you create a user, modify user credentials, or change the email address on the management console.	Yes	No
Mobile number	Entered when you create a user, modify user credentials, or change the mobile number on the management console.	Yes	No
AK/SK	Created on the My Credentials page or the IAM console.	No AK/SK cannot be modified, but they can be deleted and created again.	No AK/SK are used to sign the requests sent to call APIs.

Personal Data Storage

IAM uses encryption algorithms to encrypt sensitive user data before storing it.

- Usernames and AKs are non-sensitive data and are stored in plaintext.
- Passwords, email addresses, mobile numbers, and SKs are sensitive data and are encrypted before storage.

Access Control

Personal data is stored in the IAM database after being encrypted. A whitelist is configured to control access to the database.

MFA Authentication

You can enable login protection and critical operation protection by choosing **Security Settings > Critical Operations**. If you enable these functions, users under your account must verify their identity by SMS, email, or virtual MFA device before they log in or perform a critical operation.

API Constraints

- AK/SK authentication is required for calling APIs. You can create an access key (AK/SK) and download the file containing the access key. If you are unable to locate the file, you can create an access key again and download the file. Do not share your access key with anyone else.
- IAM does not provide APIs for batch querying and modifying personal data.

Operation Logs

IAM logs all personal data operations, including adding, modifying, querying, and deleting personal data. It uploads operation logs to CTS, and allows users to query only their own operation logs.

1.6 Permissions

If you need to assign different permissions for IAM to employees in your organization, IAM is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you secure access to your resources.

With IAM, you can create IAM users under your account, and assign permissions to these users to control their access to specific resources. For example, you can grant permissions to allow certain project planners in your enterprise to view IAM data but disallow them to perform any high-risk operations, for example, deleting IAM users and projects. For all permissions of the services supported by IAM, see "Permissions".

IAM Permissions

New IAM users do not have any permissions assigned by default. You need to first add them to one or more groups and attach policies or roles to these groups. The users then inherit permissions from the groups and can perform specified operations on cloud services based on the permissions they have been assigned.

IAM is a global service deployed for all regions. When you set the authorization scope to **Global services**, users have permission to access IAM in all regions.

You can grant permissions by using roles and policies.

- **Roles:** A coarse-grained authorization strategy provided by IAM to assign permissions based on users' job responsibilities. Only a limited number of service-level roles are available for authorization. Cloud services depend on each other. When you grant permissions using roles, you also need to attach any existing role dependencies. Roles are not ideal for fine-grained authorization and least privilege access.
- **Policies:** A fine-grained authorization strategy that defines permissions required to perform operations on specific cloud resources under certain conditions. This type of authorization is more flexible and is ideal for least privilege access. For example, you can grant users only permission to manage ECSs of a certain type. A majority of fine-grained policies contain permissions for specific APIs, and permissions are defined using API actions. For the API actions supported by IAM, see "Identity and Access Management API Reference > Permissions Policies and Supported Actions."

Table 1-2 lists all the system-defined permissions for IAM.

Table 1-2 System-defined permissions for IAM

Role/Policy Name	Description	Type	Content
FullAccess	Full permissions for all services that support policy-based authorization. Users with these permissions can perform operations on all services.	System-defined policy	Content of the FullAccess Policy
IAM ReadOnlyAccess	Read-only permissions for IAM. Users with these permissions can only view IAM data.	System-defined policy	Content of the IAM ReadOnlyAccess Policy
Security Administrator	IAM administrator with full permissions, including permissions to create and delete IAM users.	System-defined role	Content of the Security Administrator Role
Agent Operator	IAM operator (delegated party) with permissions to switch roles and access resources of a delegating party.	System-defined role	Content of the Agent Operator Role
Tenant Guest	Read-only permissions for all services except IAM.	System-defined policy	Content of the Tenant Guest Role
Tenant Administrator	Administrator permissions for all services except IAM.	System-defined policy	Content of the Tenant Administrator Role

Table 1-3 lists the common operations supported by system-defined permissions for IAM.

 **NOTE**

Tenant Guest and **Tenant Administrator** are basic roles provided by IAM and do not contain any specific permissions for IAM. Therefore, the two roles are not listed in the following table.

Table 1-3 Common operations supported by system-defined permissions

Operation	Security Administrator	Agent Operator	FullAccess	IAM ReadOnlyAccess
Creating IAM users	Supported	Not supported	Supported	Not supported
Querying IAM user details	Supported	Not supported	Supported	Supported
Modifying IAM user information	Supported	Not supported	Supported	Not supported
Querying security settings of IAM users	Supported	Not supported	Supported	Supported
Modifying security settings of IAM users	Supported	Not supported	Supported	Not supported
Deleting IAM users	Supported	Not supported	Supported	Not supported
Creating user groups	Supported	Not supported	Supported	Not supported
Querying user group details	Supported	Not supported	Supported	Supported
Modifying user group information	Supported	Not supported	Supported	Not supported
Adding users to user groups	Supported	Not supported	Supported	Not supported
Removing users from user groups	Supported	Not supported	Supported	Not supported
Deleting user groups	Supported	Not supported	Supported	Not supported
Assigning permissions to user groups	Supported	Not supported	Supported	Not supported

Operation	Security Administrator	Agent Operator	FullAccess	IAM ReadOnlyAccess
Removing permissions of user groups	Supported	Not supported	Supported	Not supported
Creating custom policies	Supported	Not supported	Supported	Not supported
Modifying custom policies	Supported	Not supported	Supported	Not supported
Deleting custom policies	Supported	Not supported	Supported	Not supported
Querying permission details	Supported	Not supported	Supported	Supported
Creating agencies	Supported	Not supported	Supported	Not supported
Querying agencies	Supported	Not supported	Supported	Supported
Modifying agencies	Supported	Not supported	Supported	Not supported
Switching roles	Not supported	Supported	Supported	Not supported
Deleting agencies	Supported	Not supported	Supported	Not supported
Granting permissions to agencies	Supported	Not supported	Supported	Not supported
Removing permissions of agencies	Supported	Not supported	Supported	Not supported
Creating projects	Supported	Not supported	Supported	Not supported
Querying projects	Supported	Not supported	Supported	Supported
Modifying projects	Supported	Not supported	Supported	Not supported

Operation	Security Administrator	Agent Operator	FullAccess	IAM ReadOnlyAccess
Deleting projects	Supported	Not supported	Supported	Not supported
Creating identity providers	Supported	Not supported	Supported	Not supported
Importing metadata files	Supported	Not supported	Supported	Not supported
Querying metadata files	Supported	Not supported	Supported	Supported
Querying identity providers	Supported	Not supported	Supported	Supported
Querying protocols	Supported	Not supported	Supported	Supported
Querying mappings	Supported	Not supported	Supported	Supported
Updating identity providers	Supported	Not supported	Supported	Not supported
Updating protocols	Supported	Not supported	Supported	Not supported
Updating mappings	Supported	Not supported	Supported	Not supported
Deleting identity providers	Supported	Not supported	Supported	Not supported
Deleting protocols	Supported	Not supported	Supported	Not supported
Deleting mappings	Supported	Not supported	Supported	Not supported
Querying quotas	Supported	Not supported	Supported	Not supported

If an IAM user wants to manage the access keys of other IAM users, see [Table 3](#). For example, if IAM user A wants to create an access key for IAM user B, IAM user A must have the Security Administrator or FullAccess permission.

Table 1-4 Access key operations supported by system-defined policies or roles

Operation	Security Administrator	Agent Operator	FullAccess	IAM ReadOnlyAccess
Creating access keys (for other IAM users)	Supported	Not supported	Supported	Not supported
Querying access keys (of other IAM users)	Supported	Not supported	Supported	Supported
Modifying access keys (for other IAM users)	Supported	Not supported	Supported	Not supported
Deleting access keys (for other IAM users)	Supported	Not supported	Supported	Not supported

Content of the FullAccess Policy

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

Content of the IAM ReadOnlyAccess Policy

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "iam:*get*",
        "iam:*list*",
        "iam:*check*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

Content of the Security Administrator Role

```
{
  "Version": "1.0",
```



```
"Statement": [  
  {  
    "Action": [  
      "iam:agencies:*",  
      "iam:credentials:*",  
      "iam:groups:*",  
      "iam:identityProviders:*",  
      "iam:mfa:*",  
      "iam:permissions:*",  
      "iam:projects:*",  
      "iam:quotas:*",  
      "iam:roles:*",  
      "iam:users:*",  
      "iam:securitypolicies:*"  
    ],  
    "Effect": "Allow"  
  }  
]
```

Content of the Agent Operator Role

```
{  
  "Version": "1.0",  
  "Statement": [  
    {  
      "Action": [  
        "iam:tokens:assume"  
      ],  
      "Effect": "Allow"  
    }  
  ]  
}
```

Content of the Tenant Guest Role

```
{  
  "Version": "1.1",  
  "Statement": [  
    {  
      "Action": [  
        "obs:*:get*",  
        "obs:*:list*",  
        "obs:*:head*"  
      ],  
      "Effect": "Allow"  
    },  
    {  
      "Condition": {  
        "StringNotEqualsIgnoreCase": {  
          "g:ServiceName": [  
            "iam"  
          ]  
        }  
      },  
      "Action": [  
        "obs:*:get*",  
        "obs:*:list*",  
        "obs:*:head*"  
      ],  
      "Effect": "Allow"  
    }  
  ]  
}
```

Content of the Tenant Administrator Role

```
{  
  "Version": "1.1",
```

```

"Statement": [
  {
    "Action": [
      "obs:*:*"
    ],
    "Effect": "Allow"
  },
  {
    "Condition": {
      "StringNotEqualsIgnoreCase": {
        "g:ServiceName": [
          "iam"
        ]
      }
    },
    "Action": [
      "obs:*:*"
    ],
    "Effect": "Allow"
  }
]

```

1.7 Notes and Constraints

The following table lists the quotas of various resources on IAM. For details, see "How Do I Increase My Quota?" in the *Identity and Access Management User Guide*.

Category	Item	Quota	Adjustable
User	IAM users	50	Yes
	Characters allowed in a username	32	No
	Groups to which a user can be added	10	No
	AK/SK pairs that a user can create	2	No
	Virtual MFA devices that can be associated with a user	1	No
	Permissions (including system-defined permissions and custom policies) that can be assigned to a user for enterprise projects	500	Yes

Category	Item	Quota	Adjustable
User group	User groups	20	Yes
	Characters allowed in a user group name	64	No
	Users that can be added to a user group	IAM users who have been created using your account	No
	Permissions (including system-defined permissions and custom policies) that can be assigned to a user group for IAM projects	200	Yes
	Permissions (including system-defined permissions and custom policies) that can be assigned to a user group for enterprise projects	500	Yes
Project	Subprojects in each region	10	Yes
Policy	Characters allowed in a policy name	64	No
Custom policy	Custom policies	200	Yes
	Characters per policy	6,144	No
	Statements per policy	8	No
	Actions per statement	100	No
	Resources per statement	10	No
	Conditions per statement	10	No

Category	Item	Quota	Adjustable
Agency	Agencies	50	Yes
	Characters allowed in an agency name	64	No
	Permissions (including system-defined permissions and custom policies) that can be assigned to an agency	200	Yes
Identity provider	Quantity	10	Yes
	Characters that can be contained in an identity provider name	64	No
	Mapping rules of all identity providers in an account	20	Yes

2 Getting Started

[2.1 Before You Start](#)

[2.2 Step 1: Create User Groups and Assign Permissions](#)

[2.3 Step 2: Create IAM Users and Log In](#)

2.1 Before You Start

Reading this document will help you to:

- Create Identity and Access Management (IAM) users.
- Create user groups based on your organization's business functions.
- Assign permissions to user groups.
- Create IAM users for employees in your organization.
- Enable IAM users to log in to the cloud platform.

Prerequisites

You already have an account. If you do not have an account, create one.

Example Scenario

A website development company has three functional teams. With IAM, the company's administrator can create only one account and then use this account to create IAM users for employees and assign permissions based on their job responsibilities.

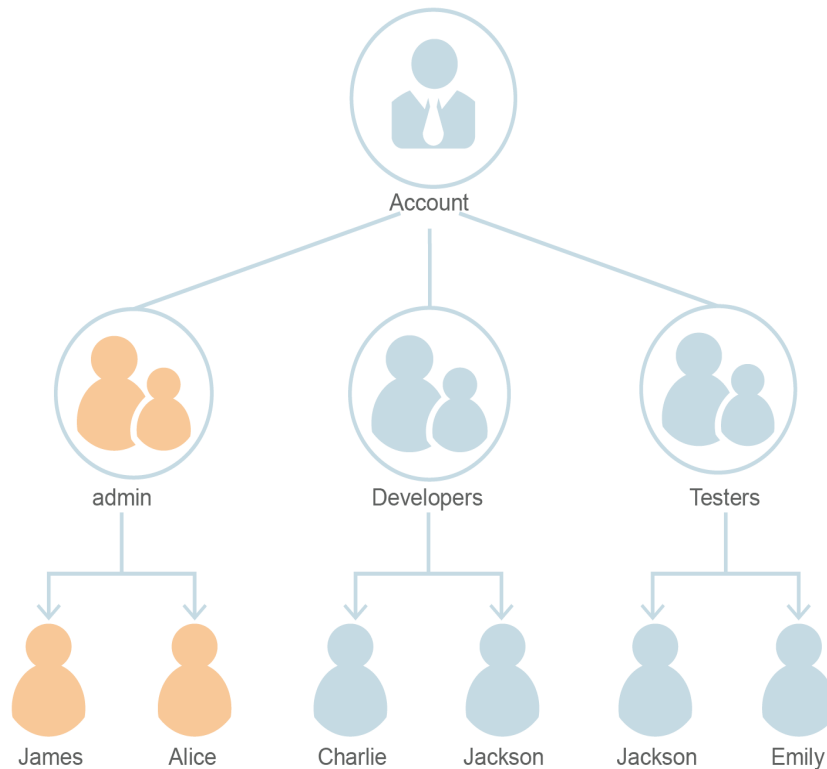
The following uses the company as an example to show how to use IAM to manage permissions.

Organizational Structure

- Management team (**admin** group in [Figure 2-1](#)): manages employees and resources, assigns permissions, and allocates resources. The team members include James and Alice.
- Development team (**Developers** group in [Figure 2-1](#)): develops websites. The team members include Charlie and Jackson.

- Test team (**Testers** group in [Figure 2-1](#)): tests websites. The team members include Jackson and Emily. Jackson develops and tests websites, so he needs to join both the **Developers** and **Testers** groups to obtain the required permissions.

Figure 2-1 User management model



User Groups and Required Resources

- **admin** group: manages user permissions using IAM.
- **Developers** group: develops websites using Elastic Cloud Server (ECS), Elastic Load Balance (ELB), Virtual Private Cloud (VPC), Relational Database Service (RDS), Elastic Volume Service (EVS), and Object Storage Service (OBS).
- **Testers** group: performs functional and performance testing on websites by using the Application Performance Management (APM) service.

User Management Process

1. The company's administrator logs in to the cloud platform, creates user groups **Developers** and **Testers**, and grants them permissions. For details, see [2.2 Step 1: Create User Groups and Assign Permissions](#).
2. The administrator creates IAM users for members of the three functional teams. The members then log in to the cloud platform as IAM users. For details, see [2.3 Step 2: Create IAM Users and Log In](#).

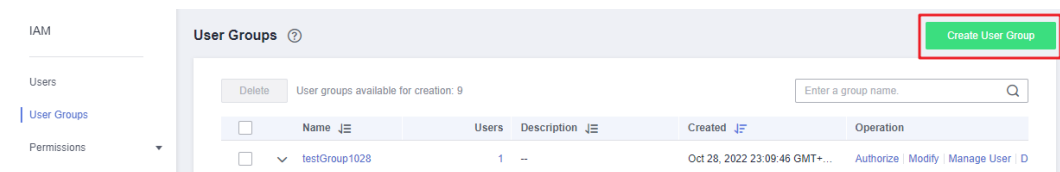
2.2 Step 1: Create User Groups and Assign Permissions

A company has three functional teams, including the management (**admin** group), development, and test teams. After the company administrator creates an account, the default group **admin** is automatically generated and has full permissions for all cloud services. The administrator only needs to create another two groups in IAM for the development and test teams, respectively.

Creating User Groups

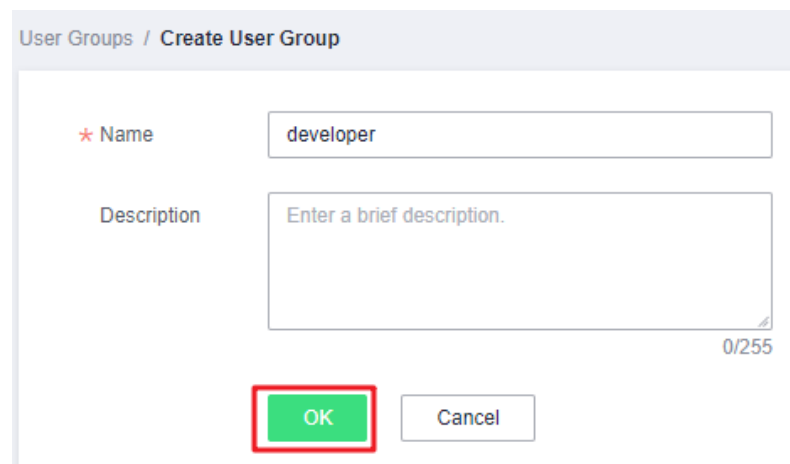
- Step 1** Log in to the management console and choose **Identity and Access Management**.
- Step 2** On the IAM console, choose **User Groups** and click **Create User Group**.

Figure 2-2 Creating a user group



- Step 3** Enter **Developers** for **Name**, and click **OK**.

Figure 2-3 Setting the user group information



- Step 4** Repeat steps **Step 2** and **Step 3** to create the **Testers** group.
- End

Assigning Permissions to User Groups

Developers in the company need to use ECS, RDS, ELB, VPC, EVS, and OBS, so the administrator needs to assign the required permissions to the **Developers** group to enable access to these services. Testers in this company need to use APM, so the administrator needs to assign the required permissions to the **Testers** group to enable access to the service. After permissions are assigned, users in the two

groups can access the corresponding services. **For details about the permissions of all cloud services, see "Permissions".**

Step 1 Determine the permissions policies to be attached to each user group.

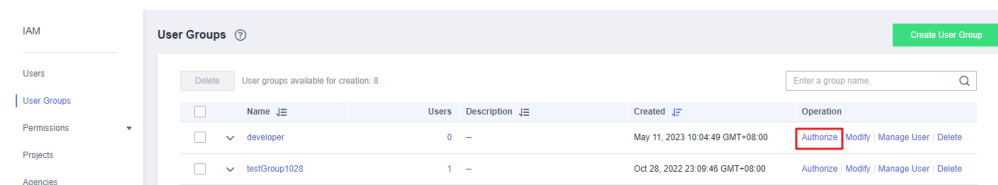
Determine the policies (see [Table 2-1](#)). Regions are geographic areas where services are deployed. If a project-level service policy is attached to a user group for a project in a specific region, the policy takes effect only for that project.

Table 2-1 Required permissions policies

User Group	Cloud Service	Region	Policy or Role
Developers	ECS	Specific regions	ECS Admin
	RDS	Specific regions	RDS Admin
	ELB	Specific regions	ELB Admin
	VPC	Specific regions	VPC Administrator
	EVS	Specific regions	EVS Admin
	OBS	Global	OBS Buckets Viewer
Testers	APM	Specific regions	APM Admin

Step 2 In the user group list, click **Authorize** in the row containing the user group **Developers**.

Figure 2-4 Authorizing a user group



Step 3 Assign permissions to the user group for region-specific projects.

1. All the services in [Table 2-1](#) except OBS are deployed in specific projects. Select desired permissions for project-level services and click **Next**.
2. Specify the scope as **Region-specific projects**, select an authorized region, and click **OK**.

Then users in the **Developers group** can access the specified project-level services in authorized regions but do not have permissions to access the services in other regions.

Step 4 Assign permissions to the user group for the global service project.

1. Select OBS Buckets Viewer and click **Next**.
2. Specify the scope as **Global service project** and click **OK**.

Step 5 Repeat steps 2 to 5 to attach the **APM Admin** role to the **Testers** group.

----End

2.3 Step 2: Create IAM Users and Log In

Create IAM users for employees and add the users to the user groups created in the previous section. Each IAM user has their own password to log in to the cloud platform, and can use resources based on the assigned permissions.

Creating IAM Users

Step 1 Choose **Users** from the navigation pane, and click **Create User**.

Step 2 Specify the user details and access type. To create more users, click **Add User**. A maximum of 10 users can be created at a time.

Figure 2-5 Configuring user information

The screenshot shows the 'Create User' interface. At the top, there are three steps: 1. Set User Details, 2. (Optional) Add User to Group, and 3. Finish. Below the steps, there is a section for 'User Details' with a note: 'The username and email address can be used as login credentials.' Below this note is a table with the following columns: Username, Email Address, Mobile Number, Description, External Identity ID, and Operation. The table contains two rows of input fields for each column. At the bottom of the table, there is an 'Add User' button and a note: 'Users available for addition: 8'.

NOTE

- Users can log in to the cloud platform using the username, email address, or mobile number.
- If users forget their password, they can reset it through email address or mobile number verification. If no email addresses or mobile numbers have been bound to users, users need to request the administrator to reset their passwords.

Table 2-2 User information

Parameter	Description
Username	Username that will be used to log in to the cloud platform, for example, James and Alice . This field is required.
Email Address	Email address of the IAM user that can be used as a login credential. IAM users can bind an email address after they are created. This field is required if you have selected Set by user for Credential Type .
Mobile Number	Mobile phone number of the IAM user that can be used as a login credential. IAM users can bind a mobile number after they are created. This field is optional.
Description	Additional information about the IAM user. This field is optional.

Figure 2-6 Setting the access type

★ Access Type

- Programmatic access**
Allows access to SberCloud services only by using development tools, such as APIs, CLI, and SDKs, and requires an access key or password. [Learn more](#)
- Management console access**
Allows access to SberCloud services only by using the management console and requires a password.

★ Credential Type

- Access key**
You can download the access key after you create the user.
- Password**
 - Set now**
.....
 - Require password reset at first login**
 - Automatically generated**
A password will be automatically generated. You can download the password file and provide it to the user.
 - Set by user**
A one-time login URL will be emailed to the user. The user can then click on the link to set a password.

★ Login Protection

- Enable (Recommended)**
Complete identity verification by to log in to the system.
- Disable**

- **Programmatic access:** Select this option to allow the user to access cloud services using development tools, such as APIs, CLI, and SDKs. You can generate an **access key** or set a **password** for the user.
- **Management console access:** Select this option to allow the user to access cloud services using the management console. You can set or generate a password for the user or request the user to set a password at first login.

NOTE

- If the user **accesses cloud services only by using the management console**, select **Management console access** for **Access Type** and **Password** for **Credential Type**.
- If the user **accesses cloud services only through programmatic access**, select **Programmatic access** for **Access Type** and **Access key** for **Credential Type**
- If the user **needs to use a password as the credential for programmatic access** to certain APIs, select **Programmatic access** for **Access Type** and **Password** for **Credential Type**
- If the user needs to **perform access key verification** when using certain services in the console, such as creating a data migration job in the Cloud Data Migration (CDM) console, select **Programmatic access** and **Management console access** for **Access Type** and **Access key** and **Password** for **Credential Type**.

Table 2-3 Setting the credential type and login protection

Credential Type and Login Protection	Description
Access key	After you create the user, you can download the access key (AK/SK) generated for the user. Each user can have a maximum of two access keys.

Credential Type and Login Protection		Description
Password	Set now	Set a password for the user and determine whether to require the user to reset the password at first login. If you are the user, select this option and set a password for login. You do not need to select Require password reset at first login .
	Automatically generated	The system automatically generates a login password for the user. After the user is created, download the EXCEL password file and provide the password to the user. The user can then use this password for login. This option is available only when you create a single user.
	Set by user	A one-time login URL will be emailed to the user. The user can click on the link to log in to the console and set a password. If you do not use the IAM user, select this option and enter the email address and mobile number of the IAM user. The user can then set a password by clicking on the one-time login URL sent over email. The login URL is valid for seven days .
Login Protection	Enable (Recommended)	If login protection is enabled, the user will need to enter a verification code in addition to the username and password during login. Enable this function for account security. You can choose from SMS-, email-, and virtual MFA-based login verification.
	Disable	To enable login protection for an IAM user after creation, see "Viewing or Modifying IAM User Information" in the <i>Identity and Access Management User Guide</i> .

Step 3 (Optional) Click **Next** to add the users to specific user groups.

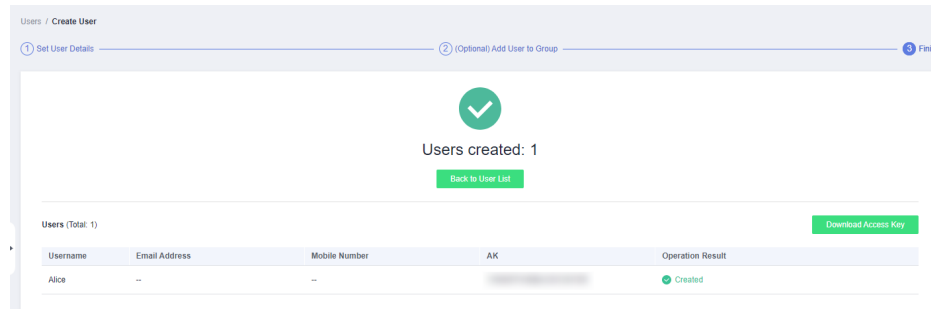
- The users will inherit the permissions assigned to the user groups.
- You can also create new groups as required.

 **NOTE**

The default user group **admin** has the administrator permissions and the permissions required to use all cloud resources. For mapping between the company employees and user groups, see [Figure 2-1](#).

Step 4 Click **Create**. If you have specified the access type as **Programmatic access** (see [Table 2-3](#)), you can download the access keys on the **Finish** page.

Figure 2-7 Users created successfully



Step 5 Repeat steps **Step 1** through **Step 4** to create users Charlie, Jackson, and Emily, and add them to the corresponding groups.

----End

IAM User Login

After creating users (for example, **James, Alice, Charlie, Jackson, and Emily**), the administrator needs to provide the account name, IAM user names, and IAM users' initial passwords to corresponding employees. Employees can use their own usernames and passwords to access the cloud platform.

Step 1 Click **IAM User Login** on the login page, and then enter your **Account name, IAM user name or email, and Password**.

Step 2 Click **Log In**.

----End

3 User Guide

- [3.1 Before You Start](#)
- [3.2 IAM Users](#)
- [3.3 User Groups and Authorization](#)
- [3.4 Permissions Management](#)
- [3.5 Projects](#)
- [3.6 Agencies](#)
- [3.7 Security Settings](#)
- [3.8 Identity Providers](#)
- [3.9 MFA Authentication and Virtual MFA Device](#)
- [3.10 Viewing IAM Operation Records](#)
- [3.11 Quotas](#)

3.1 Before You Start

Intended Audience

The Identity and Access Management (IAM) service is intended for administrators, including:

- 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 (with permissions to access IAM)

If you want to view, audit, and track the records of key operations performed on IAM, enable Cloud Trace Service (CTS). For details, see [3.10.1 Enabling CTS](#).

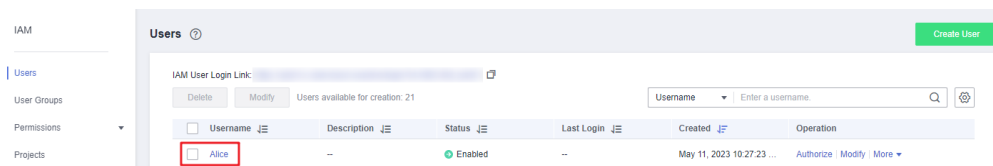
Account

An account has full permissions to access the resources under the account.

IAM User

You can create users in IAM as the administrator and assign permissions for specific resources. IAM users can log in to the cloud platform using their account name, usernames, and passwords, and then use resources based on assigned permissions. IAM users do not own resources.

Figure 3-1 IAM user created by the administrator

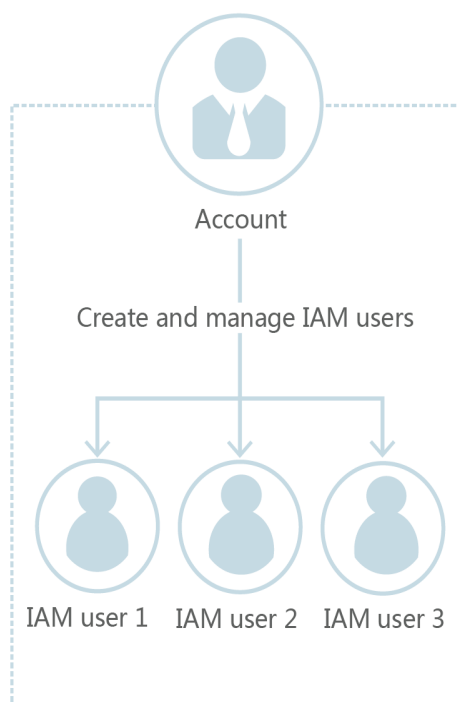


Relationship Between an Account and Its IAM Users

An account and its IAM users share a parent-child relationship. The account owns the resources and has full permissions for these resources.

IAM users are created by the account administrator, and only have the permissions granted by the administrator. The administrator can modify or revoke the IAM users' permissions at any time.

Figure 3-2 Relationship between an account and its IAM users

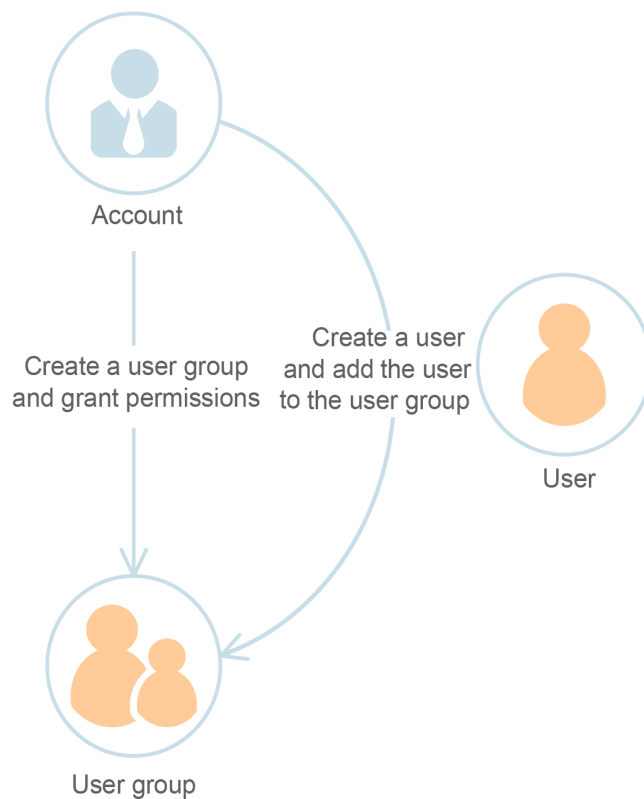


User Group

You can use user groups to assign permissions to IAM users. By default, new IAM users do not have permissions. To assign permissions to new users, add them to one or more groups, and grant permissions to these groups. The users then inherit permissions from the groups to which the users belong, and can perform specific operations on cloud services.

The default user group **admin** has all permissions required to use all of the cloud resources. Users in this group can perform operations on all the resources, including but not limited to creating user groups and users, modifying permissions, and managing resources.

Figure 3-3 User group



Permission

IAM provides common permissions for different services, such as administrator and read-only permissions. New IAM users do not have any permissions assigned by default. The administrator must add them to one or more groups and attach permissions policies or roles to these groups so that the IAM users can inherit permissions from the groups. Then the IAM users can perform specific operations on cloud services.

- Roles: a type of coarse-grained authorization mechanism that defines service-level permissions based on user responsibilities. There are only a limited number of roles for granting permissions to users. When using roles to grant permissions, you also need to assign dependency roles. Roles are not an ideal choice for fine-grained authorization and secure access control.

- **Policies:** a type of fine-grained authorization mechanism that defines permissions required to perform operations on specific cloud resources under certain conditions. This mechanism allows for more flexible policy-based authorization on a principle of least privilege (PoLP) basis. For example, you can grant Elastic Cloud Server (ECS) users only the permissions required for managing a certain type of ECS resources.

3.2 IAM Users

3.2.1 Creating an IAM User

If you are an **administrator** and have created multiple resources on the cloud platform, such as Elastic Cloud Servers (ECSs), Elastic Volume Service (EVS) disks, and Bare Metal Servers (BMSs), you can create IAM users grant them permissions required to perform operations on specific resources. You do not need to share the password of your account.

By default, new IAM users do not have permissions. You can assign permissions to new users, or add them to one or more groups and grant permissions to these groups by referring to **Assigning Permissions to a User Group** so that the users can inherit the permissions of the groups. The users then can perform specific operations on cloud services as specified by the permissions.

The default user group **admin** has all permissions required to use all of the cloud resources. Users in this group can perform operations on all the resources, including but not limited to creating user groups and users, modifying permissions, and managing resources.

 **NOTE**

If you delete a user and create a new user with the same name, you need to grant the required permissions to the new user again.

Procedure

- Step 1** Log in to the IAM console as the administrator.
- Step 2** Choose **Users** from the left navigation pane and click **Create User** in the upper right corner.
- Step 3** Specify the user information on the **Create User** page. To create more users, click **Add User**. You can add a maximum of 10 users at a time.

Table 3-1 User details

Parameter	Description
Username	This parameter is user-defined and cannot be the same as that of any other account or any IAM user in the account.

Parameter	Description
Email Address	This parameter is user-defined and cannot be the same as that of any other account or any IAM user in the account. It can be used to authenticate the IAM user and reset the password.
Mobile Number	This parameter is user-defined and cannot be the same as that of any other account or any IAM user in the account. It can be used to authenticate the IAM user and reset the password.
External Identity ID	Identity of an enterprise user in IAM user SSO. If you want to configure Identity Federation via SAML for an IAM user, External Identity ID of a maximum of 128 characters is mandatory.

Step 4 Specify Access Type.

Table 3-2 Access types

Access Type	Description
Programmatic access	Allows users to access cloud services using development tools such as APIs, CLI, and SDKs.
Management console access	Allows users to access cloud services through the management console. A password is mandatory for login.

Step 5 Specify Credential Type.

Table 3-3 Credential types

Credential Type	Description
Access key	After creating the user, you can download the access key (AK/SK) generated for the user. Each user can have a maximum of two access keys.
Password	Set now Set a password for the user and determine whether to require the user to reset the password at first login. If you are the user, select this option and set a password for login. You do not need to select Require password reset at first login .
	Automatically generated The system automatically generates a login password for the user. After the user is created, you can download the EXCEL password file and provide the password to the user. The user can then use this password for login. This option is available only when you create a single user.

Credential Type		Description
	Set by user	A one-time login URL will be emailed to the user. The user can click on the link to log in to the console and set a password. If you do not use the IAM user, select this option and enter the email address and mobile number of the IAM user. The user can then set a password by clicking on the one-time login URL sent over email. The login URL is valid for seven days .

Table 3-4 Recommended configurations

Management console access	Programmatic access	Credential type	Recommended Access Type	Recommended Credential Type
Select	Deselect	There are no special requirements.	Management console access	Password
Deselect	Select	There are no special requirements.	Programmatic access	Access key
Deselect	Select	A password is required as a credential for programmatic access (required by some APIs).	Programmatic access	Password
Select	Deselect	The access key (entered by the IAM user) needs to be verified on the console. For example, the user needs to perform access key verification before creating a data migration job in the Cloud Data Migration (CDM) console.	Programmatic access and management console access	Password and key

Step 6 Configure login protection. This parameter is available only when you have selected **Management console access** for **Access Type**.

- **Enable (Recommend):** The user needs to enter a verification code in addition to the username and password during login. Enable this function for account security.
You can choose from SMS-, email-, and virtual MFA-based login verification.
- **Disable:** The user does not need to enter a verification code for login. If you want to enable login protection after the user is created, see [Login Protection](#).

Step 7 Click **Next**. Select the user group to which the user is to be added, and add the user to the user group. The user will have the permissions assigned to the user group.

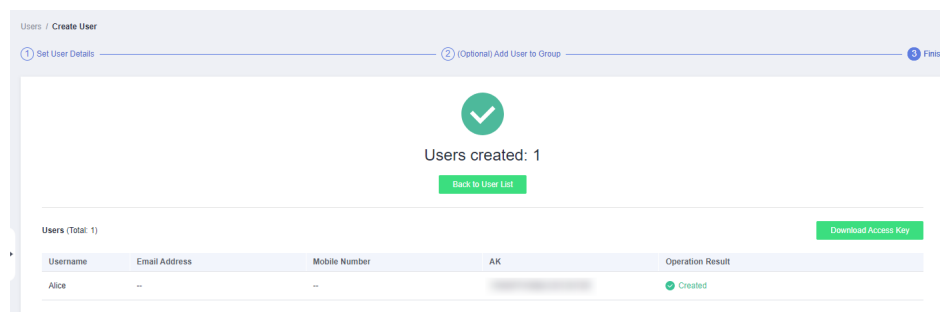
 **NOTE**

- You can also create a new group and add the user to that group.
- If the user will be an administrator, add the user to the default group **admin**.
- You can add a user to a maximum of 10 user groups.

Step 8 Click **Create**.

- If you have selected **Access key** for **Credential Type** in **5**, you can download the access key on the **Finish** page.
- If you have selected **Password > Automatically generated** for **Credential Type** in **Step 4**, you can download the password file on the **Finish** page.

Figure 3-4 Users created successfully



----End

3.2.2 Assigning Permissions to an IAM User

IAM users created without being added to any groups do not have any permissions. The administrator can assign permissions to these IAM users on the IAM console. After authorization, the users can use cloud resources in your account as specified by their permissions.

Constraints

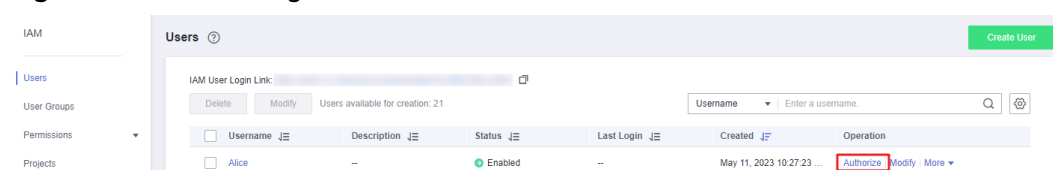
A maximum of 500 permissions (including system-defined permissions and custom policies) can be assigned to each IAM user for enterprise projects.

Procedure

Step 1 Log in to the IAM console as the administrator.

Step 2 In the user list, click **Authorize** in the row that contains the target user.

Figure 3-5 Authorizing an IAM user

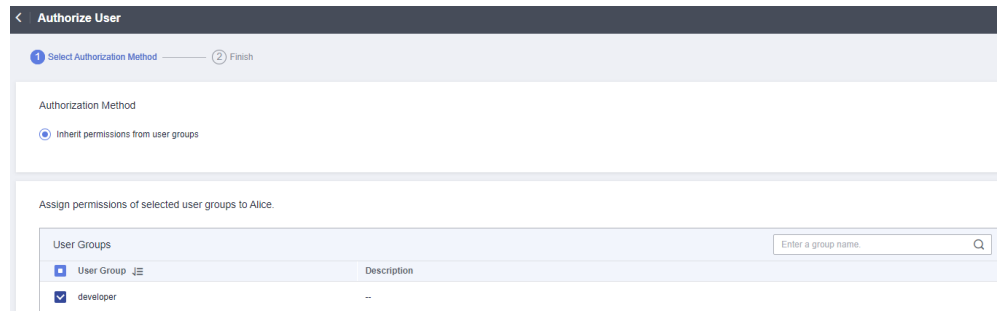


Step 3 On the **Authorize User** page, select an authorization mode and permissions.

- **Inherit permissions from user groups:** Add the IAM user to certain groups to inherit their permissions.

If you select this option, select the user groups to which the user will belong.

Figure 3-6 Inheriting permissions from user groups



- **Select permissions:** Directly assign specific permissions to the IAM user. You can assign permissions directly to IAM users only when Enterprise Project is enabled.

If you select this option, select permissions, click **Next** in the lower right, and then go to **Step 4**.

NOTE

- If you add an IAM user to the default group **admin**, the user becomes an administrator and can perform all operations on all cloud services.
- If you add a user to multiple user groups, the user inherits the permissions that are assigned to these groups.
- **For details on the system-defined permissions of all cloud services supported by IAM, see "System-defined Permissions".**
- If you have enabled enterprise management, you cannot create projects in IAM.

Step 4 On the **Select Scope** page, select enterprise projects that the IAM user can access. You do not need to perform this step if you have selected **Inherit permissions from user groups**.

Step 5 Click **OK**.

You can go to the **Permissions > Authorization** page and view or modify the permissions of the IAM user.

----End

3.2.3 Logging In as an IAM User

To log in as an IAM user, you can choose **IAM User Login** on the login page or obtain the IAM user login link from the administrator.

Method 1: Logging In by Clicking IAM User Login

Step 1 Click **IAM User Login** on the login page, and then enter your account name, IAM user name or email address, and password.

- **Account name:** The name of the account that was used to create the IAM user. You can obtain the account name from the **administrator**.

- **IAM user name or email:** The username or email address of the **IAM user**. You can obtain the username and password from the **administrator**.
- **Password:** The password of the IAM user.

Step 2 Click **Log In**.

NOTE

- If you have not been added to any group, you do not have permissions for accessing any cloud services. In this case, contact the administrator and request for required permissions (see [3.3.1 Creating a User Group and Assigning Permissions](#) and [3.3.2 Adding Users to or Removing Users from a User Group](#)).
- If you have been added to the default group **admin**, you have administrator permissions and you can perform all operations on all cloud services.

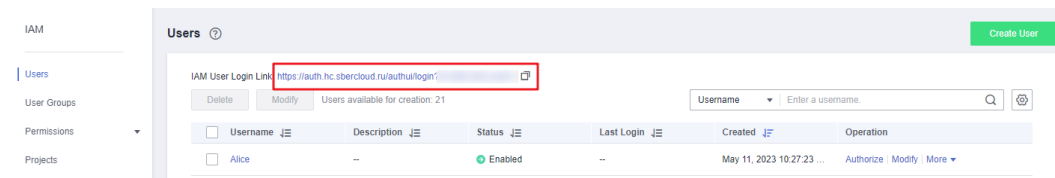
----End

Method 2: Logging In Using the IAM User Login Link

You can obtain the IAM user login link from the administrator and then log in using this link. When you visit the link, the system displays the login page and automatically populates the account name. You only need to enter your username and password.

Step 1 Obtain the IAM user login link from the administrator, who can copy the login link from the IAM console.

Figure 3-7 IAM user login link



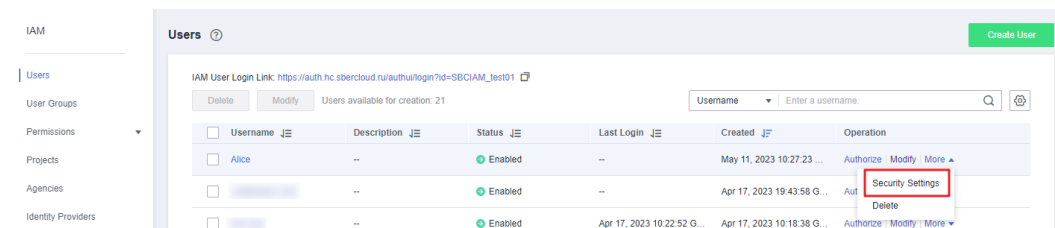
Step 2 Paste the link into the address bar of a browser, press **Enter**, and enter the IAM user name/email address and password, and click **Log In**.

----End


3.2.4 Viewing or Modifying IAM User Information

As an administrator, you can modify the basic information about an IAM user, change the security settings of the user and the groups to which the user belongs, and view or delete the assigned permissions. To view or modify user information, click **Security Settings** in the row containing the IAM user.

Figure 3-8 Going to the IAM user security settings page



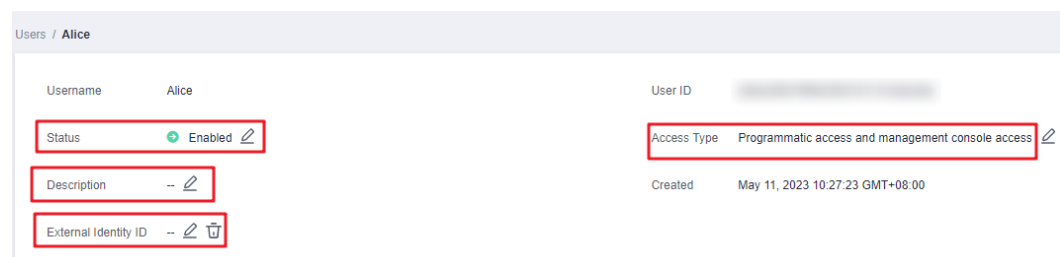


To adjust the item columns displayed on the list, click . The **Username** and **Operation** columns are displayed by default, and the **Status** column cannot be removed. You can also select **Description**, **Last Login**, **Created**, **Access Type**, **Virtual MFA Status**, **Password Age**, **Access Key (Status, Age, and AK)**, and **External Identity ID**.

Basic Information

You can view the basic information of each IAM user. The username, user ID, and creation time cannot be modified.

Figure 3-9 Modifying the status, access type, description, and external identity ID of an IAM user



- **Status:** New IAM users are enabled by default. You can set **Status** to **Disabled** to disable an IAM user. A disabled user is no longer able to log in to the cloud platform through the management console or programmatic access.
- **Access Type:** You can change the access type of the IAM user.

NOTE

- Pay attention to the following when you set the access type of an IAM user:
 - If the user **accesses cloud services only by using the management console**, specify the access type as **Management console access** and the credential type as **Password**.
 - If the user **accesses cloud services only through programmatic calls**, specify the access type as **Programmatic access** and the credential type as **Access key**.
 - If the user **needs to use a password as the credential for programmatic access** to certain APIs, specify the access type as **Programmatic access** and the credential type as **Password**.
 - If the user needs to **perform access key verification** when using certain services in the console, specify the access type as **Programmatic access** and **Management console access** and the credential type as **Access Key** and **Password**.
- If the access type of the user is **Programmatic access** or both **Programmatic access** and **Management console access**, deselecting **Programmatic access** will restrict the user's access to cloud services. Exercise caution when performing this operation.
- **Description:** You can modify the description of the IAM user.
- **External Identity ID:** Identifies an enterprise user in federated login using SSO.

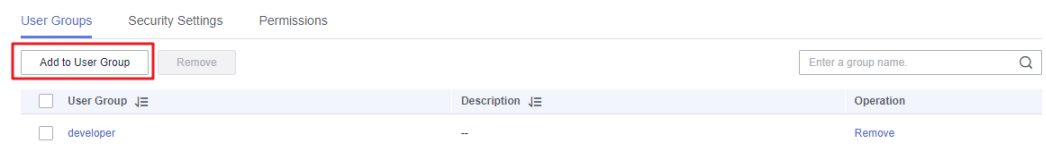
User Groups

An IAM user inherits permissions from the groups to which the user belongs. **You can change the permissions assigned for an IAM user by changing the groups to which the user belongs to.** To modify the permissions of a user group, see [3.3.4 Viewing or Modifying User Group Information](#).

Your account belongs to the default group **admin**, which cannot be changed.

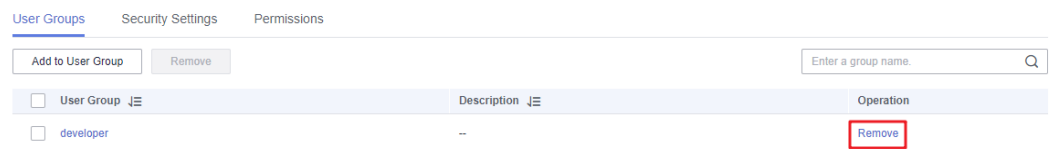
- Click **Add to User Groups**, and select one or more groups to which the user will belong. The user then inherits permissions of these groups.

Figure 3-10 Adding the user to user groups



- Click **Remove** on the right of a user group and click **Yes**. The user no longer has the permissions assigned to the group.

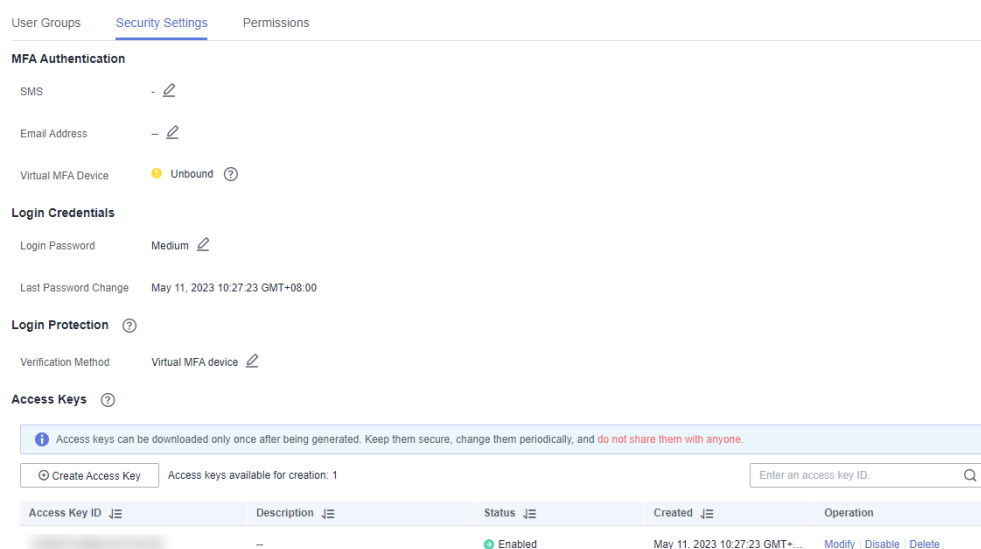
Figure 3-11 Removing the user from a user group



Security Settings

As an administrator, you can modify the MFA device, login credential, login protection, and access keys of an IAM user on this page. If you are an IAM user and need to change your mobile number, email address, or virtual MFA device, see [3.7.1 Security Settings Overview](#).

Figure 3-12 IAM user security settings



- **MFA Authentication:** You can change the multi-factor authentication (MFA) settings of an IAM user on the **Security Settings** page.
 - Change the mobile number or email address of the user.

 **NOTE**

The mobile number and email address of the IAM user cannot be the same as those of your account or other IAM users.

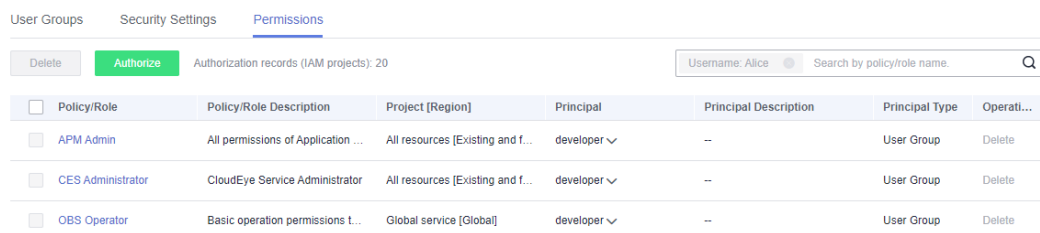
- Remove the MFA device from the user. For more information about MFA authentication and virtual MFA device, see [3.9 MFA Authentication and Virtual MFA Device](#).
- **Login Credentials:** You can change the login password of the IAM user. For more information, see [3.2.6 Changing the Login Password of an IAM User](#).
- **Login Protection:** You can change the login verification method of the IAM user. Three verification methods are available: virtual MFA device, SMS, and email.

This option is disabled by default. If you enable this option, the user will need to enter a verification code in addition to the username and password when logging in to the console.
- **Access Keys:** You can manage access keys of the IAM user. For more information, see [3.2.7 Managing Access Keys for an IAM User](#).

Permissions

You can view or delete permissions of IAM users. To modify permissions of IAM users, see [User Groups](#).

Figure 3-13 Permissions assigned to an IAM user



Policy/Role	Policy/Role Description	Project [Region]	Principal	Principal Description	Principal Type	Operati...
<input type="checkbox"/> APM Admin	All permissions of Application ...	All resources [Existing and f...	developer v	--	User Group	Delete
<input type="checkbox"/> CES Administrator	CloudEye Service Administrator	All resources [Existing and f...	developer v	--	User Group	Delete
<input type="checkbox"/> OBS Operator	Basic operation permissions t...	Global service [Global]	developer v	--	User Group	Delete

To view all authorization records under your account, see [3.4.4 Authorization Records](#).

 **NOTE**

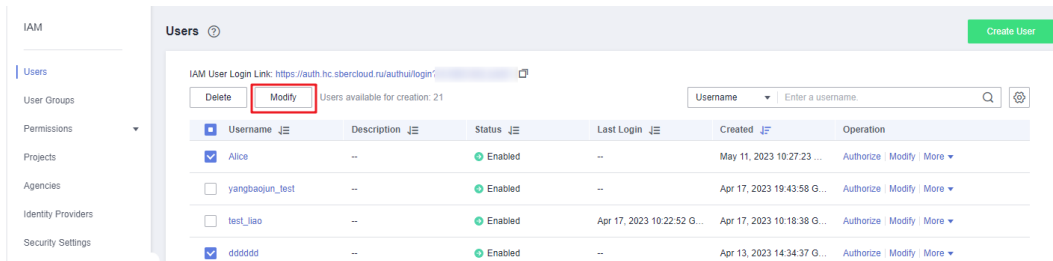
Deleting the permissions of an IAM user will delete the permissions assigned to the group to which the user belongs. All users in the group will no longer have the permissions. Exercise caution when performing this operation.

Batch Modifying IAM User Information

IAM allows you to batch modify the status, access type, and verification method of IAM users. The following describes how to batch modify the status of IAM users. The methods of modifying other information about users are similar to this method.

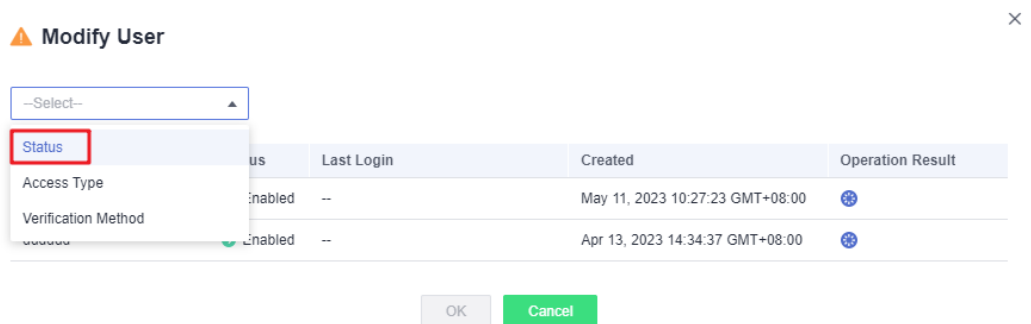
- Step 1** Log in to the IAM console. In the navigation pane, choose **Users**.
- Step 2** In the user list, select the users whose information you want to modify, and click **Modify** above the user list.

Figure 3-14 Modifying user information



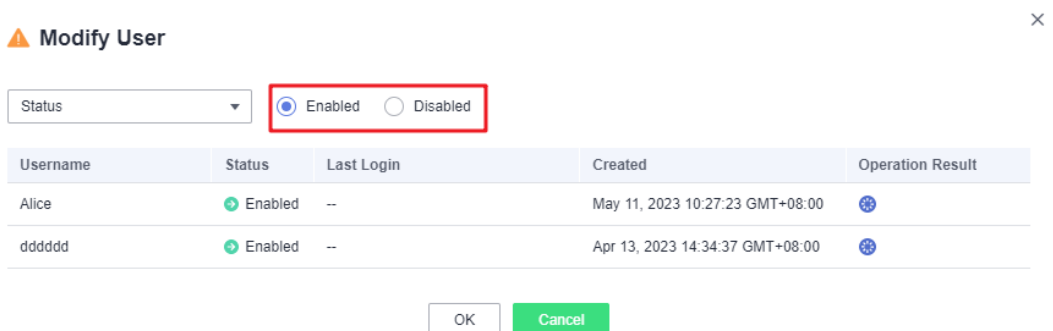
- Step 3** Select the attribute you want to modify. In this example, select **Status** from the drop-down list.

Figure 3-15 Selecting the status attribute



- Step 4** Select the target status to be configured for the selected IAM users.

Figure 3-16 Selecting the target status



NOTE

Make sure that this user is no longer in use. Disabling an active user may affect services.

- Step 5** Click **OK**.

- Step 6** In the displayed dialog box, click **OK** to confirm the change.
- End

3.2.5 Deleting an IAM User

CAUTION

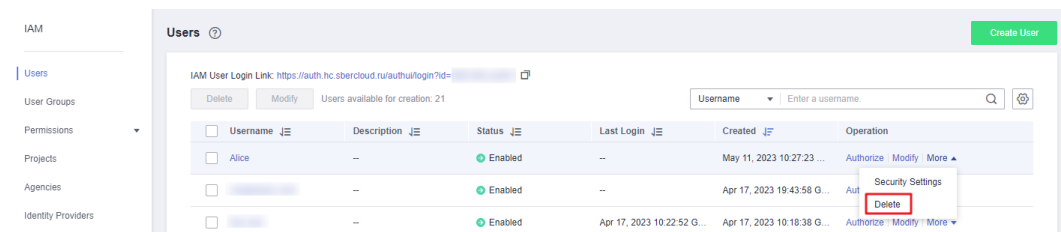
After an IAM user is deleted, they can no longer log in and their username, password, access keys, and authorizations will be cleared and cannot be recovered.

- Make sure that the users to be deleted are no longer needed. If you are not sure, disable them rather than delete them so that they can be enabled if any service failures occur. To disable an individual IAM user, see [Basic Information](#). To disable multiple IAM users at a time, see [Batch Modifying IAM User Information](#).
- To remove an IAM user from a user group, see [3.3.2 Adding Users to or Removing Users from a User Group](#).

Deleting an IAM User

- Step 1** Log in to the IAM console. In the navigation pane, choose **Users**.
- Step 2** Choose **More > Delete** in the row containing the IAM user you want to delete, and click **Yes**.

Figure 3-17 Deleting an IAM user

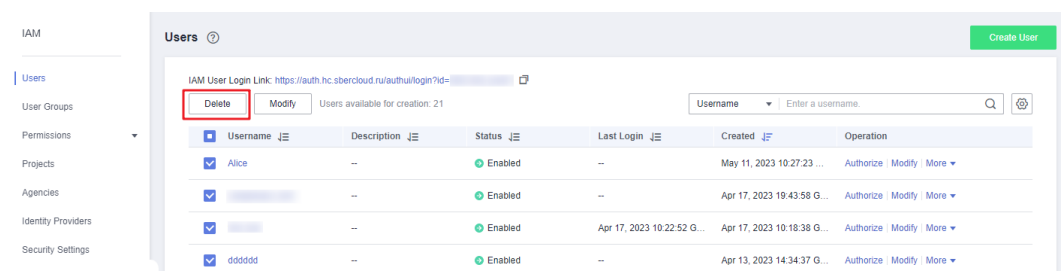


----End

Batch Deleting IAM Users

- Step 1** Log in to the IAM console. In the navigation pane, choose **Users**.
- Step 2** In the user list, select the users to be deleted and click **Delete** above the user list.

Figure 3-18 Batch deleting IAM users



Step 3 In the displayed dialog box, click **Yes**.

----End

3.2.6 Changing the Login Password of an IAM User

As an administrator, you can reset the password of an IAM user if the user has forgotten the password and no email address or mobile number has been bound to the user.


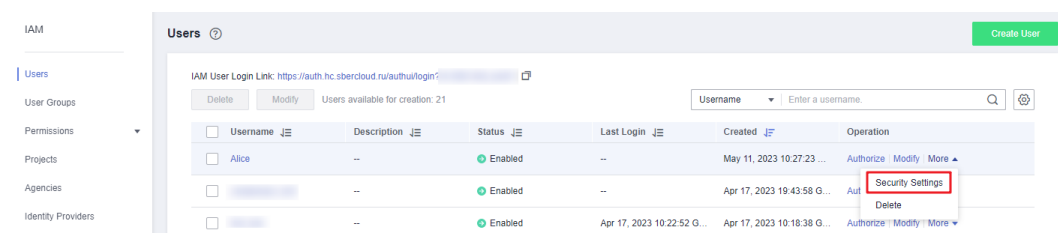
To reset the login password of an IAM user, click **Security Settings** in the row containing the user, click  next to **Login Password** in the **Login Credentials** area, and select a password type.

Figure 3-19 Changing the password of an IAM user



 **NOTE**

- You can reset the password of an IAM user on the **Security Settings** page.
- IAM users can change their passwords on the **Account Settings** tab.
- **Set by user:** A one-time login URL will be emailed to the user. The user can then click on the link to set a password.
- **Automatically generated:** A password will be automatically generated and then sent to the user by email.
- **Set now:** You set a new password and send the new password to the user.

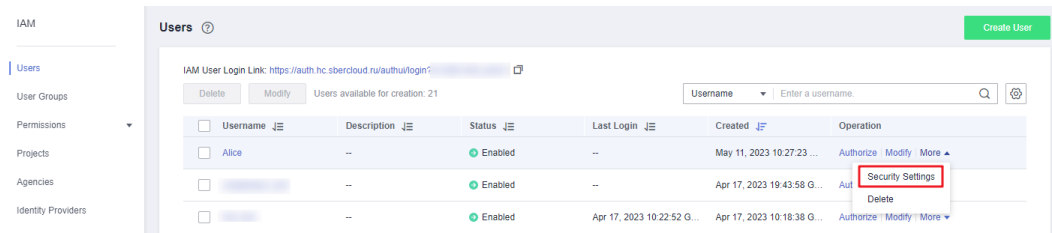
3.2.7 Managing Access Keys for an IAM User

An access key consists of an access key ID (AK) and secret access key (SK) pair. You can use an access key to access the cloud platform using development tools, including APIs, CLI, and SDKs. Access keys cannot be used to log in to the console. AK is a unique identifier used in conjunction with SK to sign requests cryptographically, ensuring that the requests are secret, complete, and correct.

As an administrator, you can manage access keys for IAM users who have forgotten their access keys and do not have access to the console.

Choose **More > Security Settings** in the row containing the IAM user, and then create or delete access keys in the **Access Keys** area.

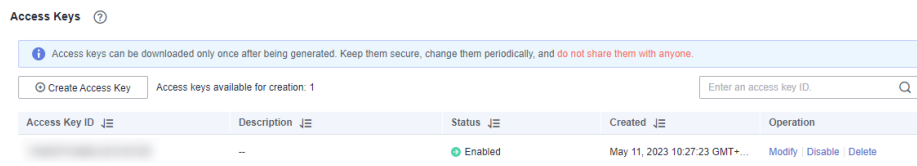
Figure 3-20 Managing access keys for an IAM user



NOTE

- Federated users can only create temporary access credentials (temporary AK/SKs and security tokens).
- If a user is authorized to use the console, the user can manage access keys on the **My Credentials** page.
- Access keys are identity credentials used to call APIs. The account administrator and IAM users can only use their own access keys to call APIs.
- Creating an access key
 - a. Click **Create Access Key**.

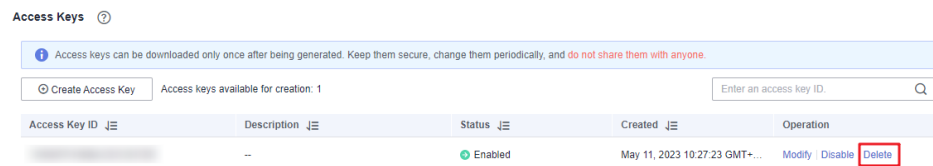
Figure 3-21 Creating an access key



NOTE

- Each user has a maximum of two access keys, and the access keys are permanently valid. For security purposes, change the access keys of IAM users periodically.
- b. (Optional) If operation protection is enabled, you need to enter a verification code or password.
 - c. Click **OK**. An access key is automatically generated. Download the access key and provide it to the user.
- Deleting an access key
 - a. In the access key list, click **Delete** in the row containing the access key to be deleted.

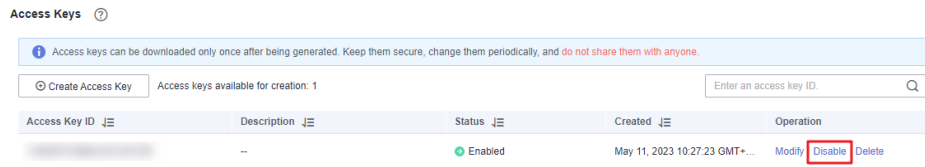
Figure 3-22 Deleting an access key



- b. (Optional) If operation protection is enabled, you need to enter a verification code or password.
- c. Click **Yes**.

- Enabling/Disabling an access key
New access keys are enabled by default. To disable an access key, perform the following steps:
 - a. In the access key list, click **Disable** in the row containing the access key you want to disable.

Figure 3-23 Disabling an access key



- b. (Optional) If operation protection is enabled, you need to enter a verification code or password, and click **Yes**.
The method of enabling an access key is similar to that of disabling an access key.

3.3 User Groups and Authorization

3.3.1 Creating a User Group and Assigning Permissions

As an administrator, you can create user groups, and grant them permissions by attaching policies or roles. Users you add to the user groups inherit permissions of the policies or roles. IAM provides general permissions (such as administrator or read-only permissions) for each cloud service, which you can assign to user groups. Users in the groups can then use cloud services based on the assigned permissions. For details, see [3.2.2 Assigning Permissions to an IAM User](#). For details about the system-defined permissions of all cloud services, see "Permissions".

Prerequisites

Before creating a user group, learn about the following:

- Understand the [basic concepts](#) of permissions.
- **Know permissions provided by IAM.**

Creating a User Group

- Step 1** Log in to the IAM console as the administrator.
- Step 2** On the IAM console, choose **User Groups** from the navigation pane, and click **Create User Group** in the upper right corner.

Figure 3-24 Creating a user group



Step 3 On the displayed page, enter a user group name.

Step 4 Click **OK**.

 **NOTE**

You can create a maximum of 20 user groups. To create more user groups, increase the quota by referring to [3.11 Quotas](#)

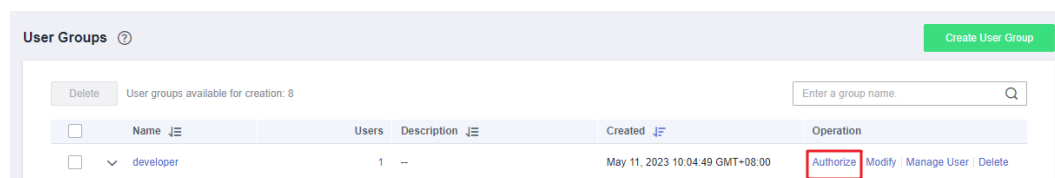
----End

Assigning Permissions to a User Group

To assign permissions to a user group, do as follows. To revoke permissions of a user group, see [3.3.5 Revoking Permissions of a User Group](#).

Step 1 In the user group list, click **Authorize** in the row that contains the created user group.

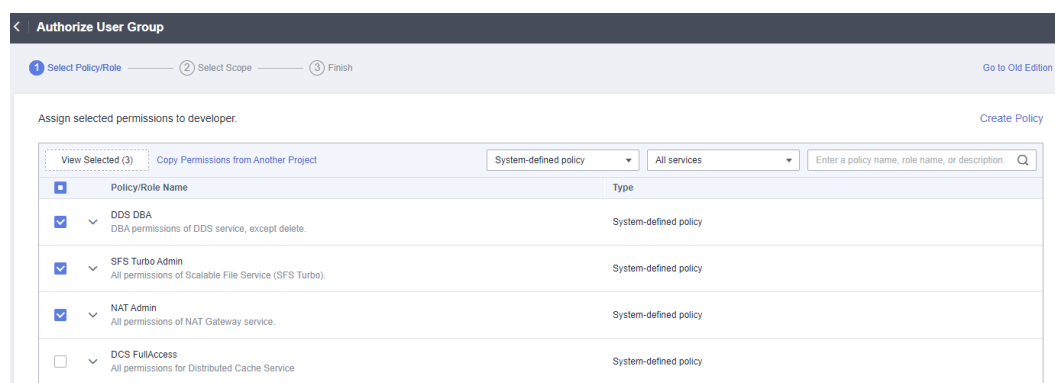
Figure 3-25 Going to the user group authorization page



Step 2 On the **Authorize User Group** page, select the permissions to be assigned to the user group and click **Next**.

If the system-defined policies do not meet your requirements, click **Create Policy** in the upper right to create custom policies. You can use them to supplement system-defined policies for refined permissions control. For details, see [3.4.5.1 Creating a Custom Policy](#).

Figure 3-26 Selecting permissions



Step 3 Specify the scope. The system automatically recommends an authorization scope for the permissions you selected. [Table 3-5](#) describes all the authorization scopes provided by IAM.

Table 3-5 Authorization scopes

Scope	Description
All resources	IAM users can use the resources in all region-specific projects and the global service project in your account as specified by the permissions.
Enterprise projects	IAM users can use the resources in the enterprise projects you select, as specified by the permissions. This option is available only when the enterprise project function has been enabled. For details about enterprise projects, see "Enterprise Management" in the <i>Enterprise Management User Guide</i> .
Region-specific projects	IAM users can use the resources in the region-specific projects you select, as specified by the permissions. If some of the selected permissions belong to global services, the system automatically sets the authorization scope of these permissions to All resources . Selected permissions for project-level services will apply to the region-specific projects you select.
Global services	IAM users can use global services as specified by the permissions. Global services are deployed with no physical regions specified. IAM users do not need to specify a region when accessing these services, such as Object Storage Service (OBS) and Content Delivery Network (CDN). If some of the selected permissions belong to project-level services, the system automatically sets the authorization scope of these permissions to All resources . Selected permissions for global services will apply to the global services.

Step 4 Click **OK**.

----End

Table 3-6 lists the common permissions. For the complete list of service-specific permissions, see [Permission Description](#).

 **NOTE**

- If you add a user to multiple groups, the user will inherit all the permissions that have been assigned to the groups.

Table 3-6 Common permissions

Category	Policy/Role Name	Description	Authorization Scope
General administration	FullAccess	Full permissions for services supporting policy-based access control.	All

Category	Policy/Role Name	Description	Authorization Scope
Resource management	Tenant Administrator	Administrator permissions for all services except IAM.	All
Viewing resources	Tenant Guest	Read-only permissions for all resources.	All
IAM user management	Security Administrator	Administrator permissions for IAM.	Global services
Computing O&M	ECS Admin	Administrator permissions for ECS.	Region-specific projects
	CCE FullAccess	Administrator permissions for Cloud Container Engine (CCE).	Region-specific projects
	BMS FullAccess	Administrator permissions for Bare Metal Server (BMS).	Region-specific projects
	IMS Admin	Administrator permissions for Image Management Service (IMS).	Region-specific projects
	AutoScaling FullAccess	Administrator permissions for Auto Scaling (AS).	Region-specific projects
Network O&M	VPC Admin	Administrator permissions for Virtual Private Cloud (VPC).	Region-specific projects
	ELB Admin	Administrator permissions for Elastic Load Balance (ELB).	Region-specific projects
Database O&M	RDS FullAccess	Administrator permissions for Relational Database Service (RDS).	Region-specific projects
	DDS FullAccess	Administrator permissions for Document Database Service (DDS).	Region-specific projects

Category	Policy/Role Name	Description	Authorization Scope
	DDM FullAccess	Administrator permissions for Distributed Database Middleware (DDM).	Region-specific projects
Security O&M	WAF Administrator	Administrator permissions for Web Application Firewall (WAF).	Region-specific projects
	CGS FullAccess	Administrator permissions for Container Guard Service (CGS).	Region-specific projects
	KMS Administrator	Administrator permissions for Key Management Service (KMS), which has been renamed Data Encryption Workshop (DEW).	Region-specific projects
	DBSS FullAccess	Administrator permissions for Database Security Service (DBSS).	Region-specific projects

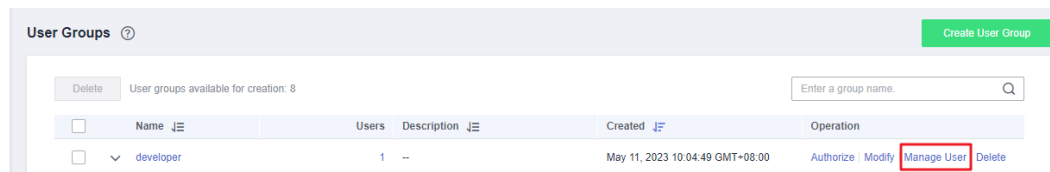
3.3.2 Adding Users to or Removing Users from a User Group

A user inherits permissions from the groups to which the user belongs. To change the permissions of a user, add the user to a new group or remove the user from an existing group.

Adding Users to a User Group

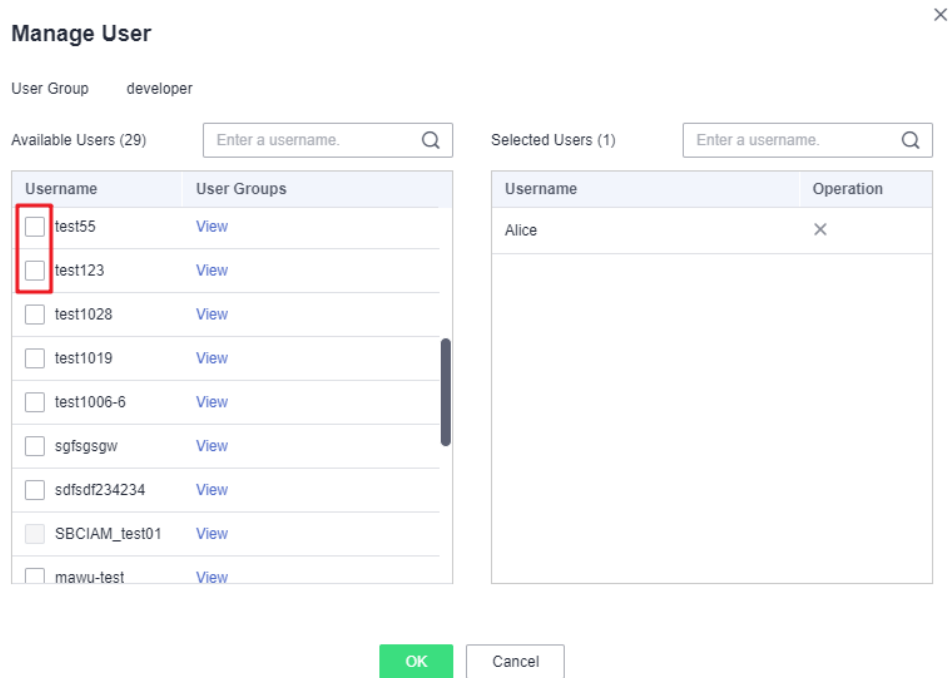
Step 1 In the user group list, click **Manage User** in the row containing the target user group.

Figure 3-27 Managing users



Step 2 In the **Manage User** dialog box, select the usernames to be added.

Figure 3-28 Selecting users



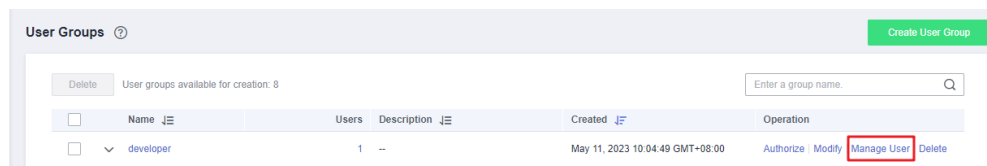
Step 3 Click **OK**.

----End

Removing Users from a User Group

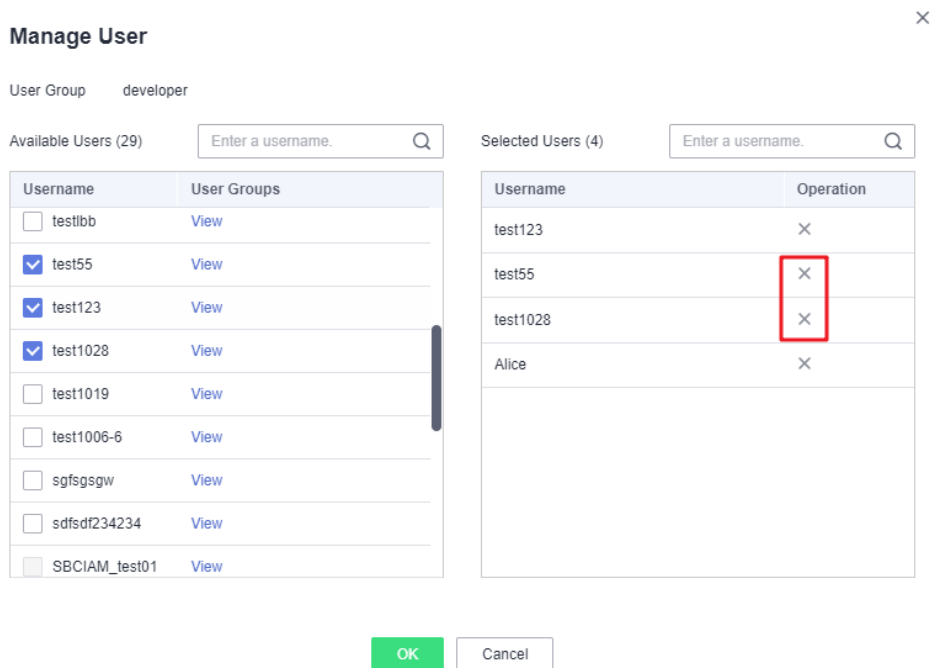
Step 1 In the user group list, click **Manage User** in the row containing the target user group.

Figure 3-29 Managing users



Step 2 In the **Selected Users** area, click **x** in the row containing the usernames to be removed and click **OK**.

Figure 3-30 Removing users from a user group



----End

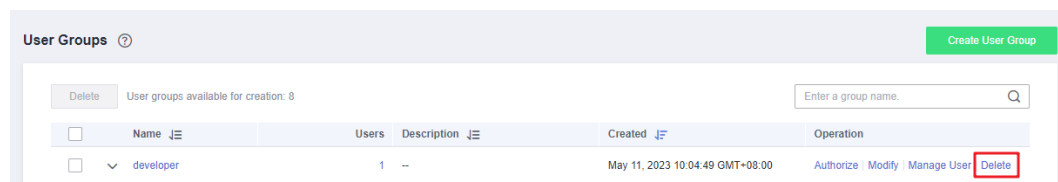
3.3.3 Deleting a User Group

Procedure

To delete a user group, do the following:

- Step 1** Log in to the IAM console. In the navigation pane, choose **User Groups**.
- Step 2** In the user group list, click **Delete** in the row that contains the user group to be deleted.

Figure 3-31 Deleting a user group



- Step 3** In the displayed dialog box, click **Yes**.

----End

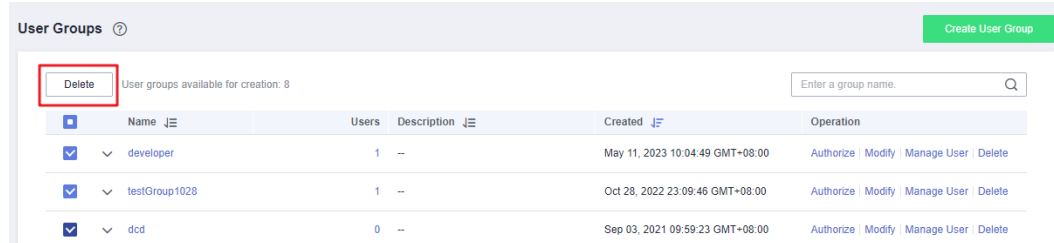
Batch Deleting User Groups

To delete multiple user groups at a time, do the following:

- Step 1** Log in to the IAM console. In the navigation pane, choose **User Groups**.

Step 2 In the user group list, select the user groups to be deleted and click **Delete** above the list.

Figure 3-32 Batch deleting user groups



Step 3 In the displayed dialog box, click **Yes**.

----End

3.3.4 Viewing or Modifying User Group Information

Viewing User Group Information


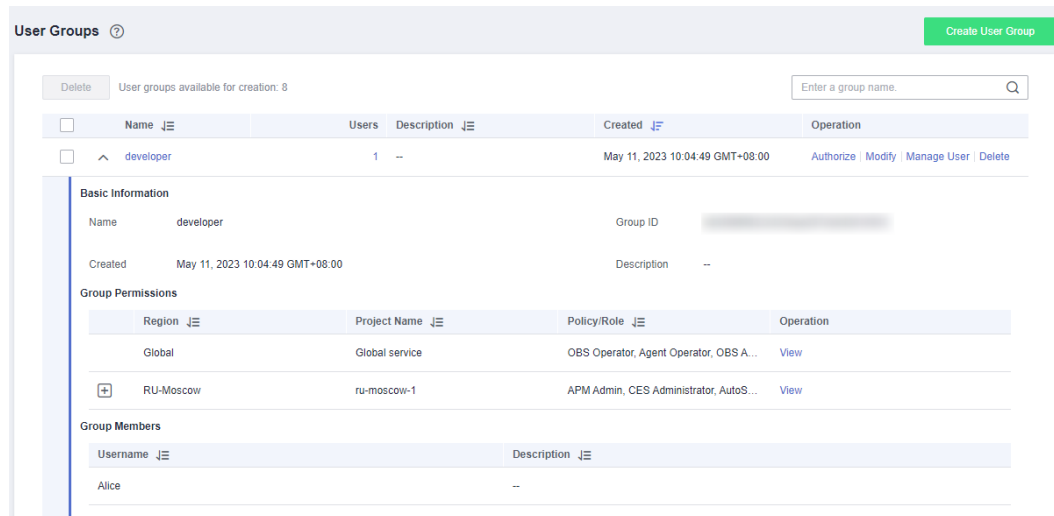
In the user group list, click  next to a user group to view its basic information, assigned permissions, and managed users.

Figure 3-33 Viewing user group information



Modifying User Group Permissions

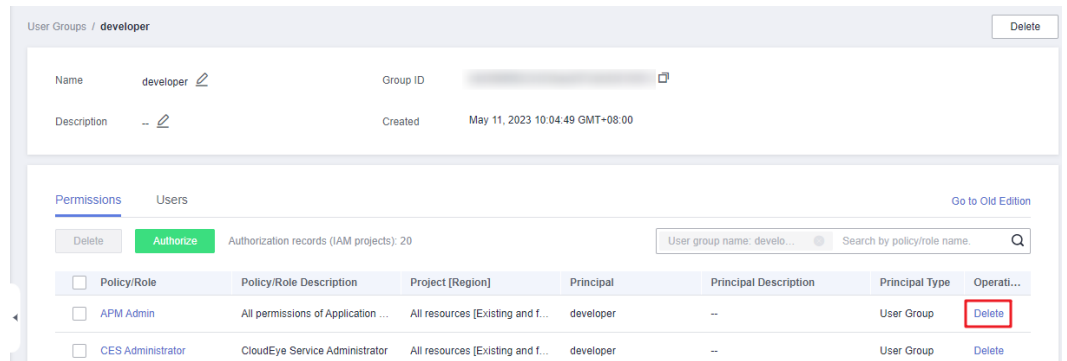
View or modify user group permissions.

 **NOTE**

- Modifying the permissions of a user group affects the permissions of all users in the user group. Exercise caution when performing this operation.
 - Permissions of the default user group **admin** cannot be modified.
1. Click the name of a user group (for example, **Developers**) to go to the details page, and view the group permissions on the **Permissions** tab.

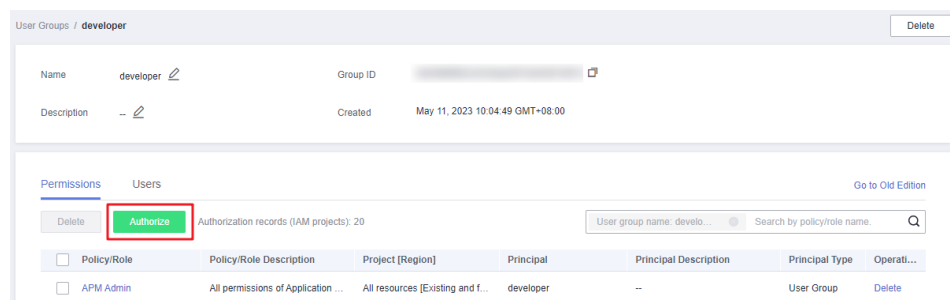
2. Click **Delete** in the row that contains the role or policy you want to delete.

Figure 3-34 Deleting an assigned permission



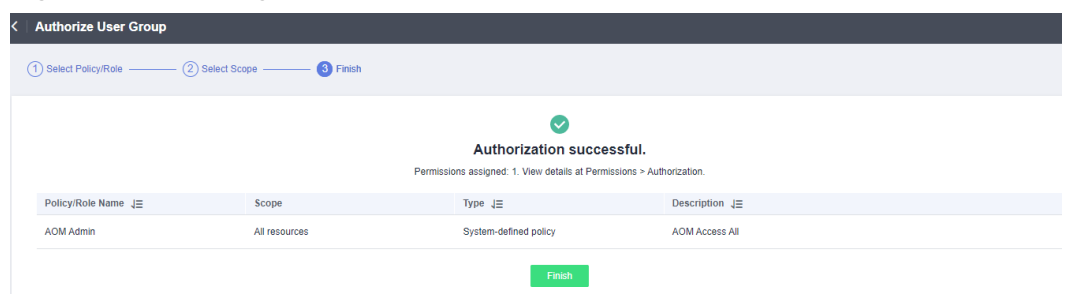
3. Click **Yes**.
4. On the **Permissions** tab, click **Authorize**.

Figure 3-35 Assigning permissions to a user group



5. Select desired permissions and a scope, and click **OK**.
6. Click **Back**. Then view the group permissions on the **Permissions** tab.

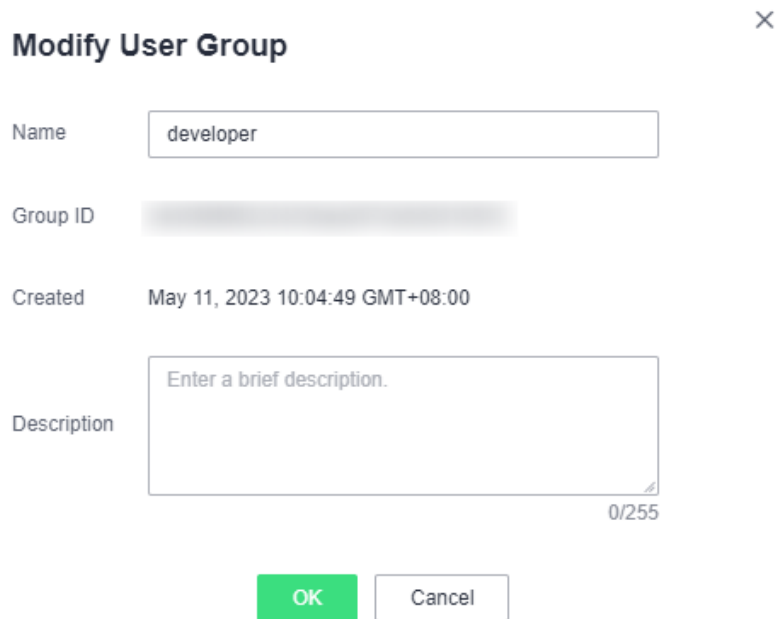
Figure 3-36 Clicking Back



Modifying a User Group Name and Description

In the user group list, click **Modify** in the row containing the user group whose name and description you want to modify, and modify the name and description.

Figure 3-37 Modifying the user group name and description



Modify User Group ✕

Name

Group ID

Created **May 11, 2023 10:04:49 GMT+08:00**

Description

0/255

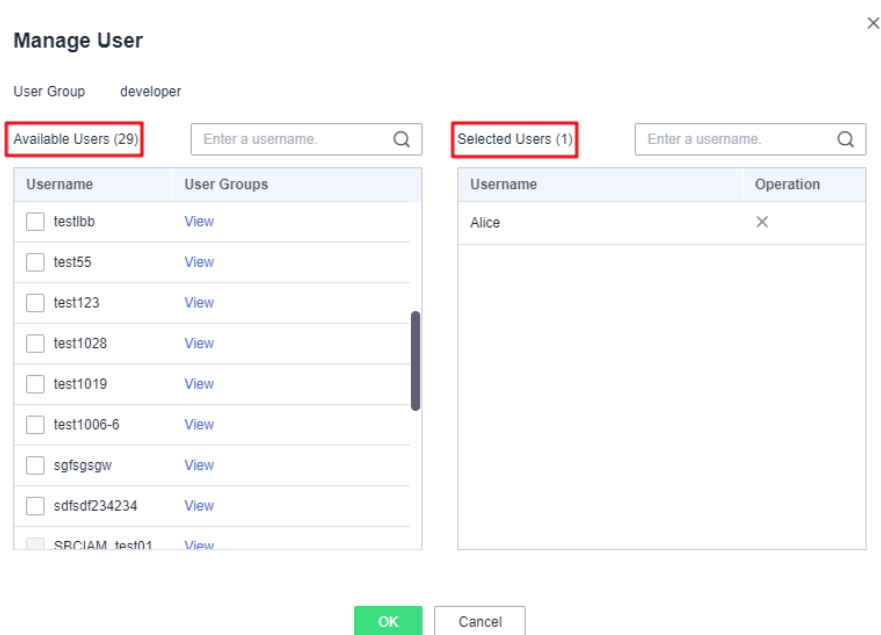
 **NOTE**

If a user group name has been configured in the identity conversion rules of an identity provider, modifying the user group name will cause the identity conversion rules to fail. Exercise caution when performing this operation.

Managing Users

Step 1 In the user group list, click **Manage User** in the row containing the user group you want to modify.

Figure 3-38 Managing Users



Manage User ✕

User Group **developer**

Available Users (29)

Username	User Groups
<input type="checkbox"/> testlibb	View
<input type="checkbox"/> test55	View
<input type="checkbox"/> test123	View
<input type="checkbox"/> test1028	View
<input type="checkbox"/> test1019	View
<input type="checkbox"/> test1006-6	View
<input type="checkbox"/> sgfsgsgw	View
<input type="checkbox"/> sdfsd234234	View
<input type="checkbox"/> SRCIAM_test01	View

Selected Users (1)

Username	Operation
Alice	<input type="button" value="X"/>

Step 2 In the **Available Users** area, select users you want to add to the user group.

Step 3 In the **Selected Users** area, remove users from the user group.

----End

 **NOTE**

For the default group **admin**, you can only manage its users and cannot modify its description or permissions.

3.3.5 Revoking Permissions of a User Group

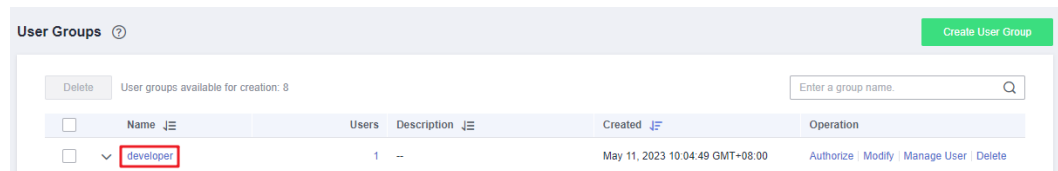
Procedure

To revoke a policy or role attached to a user group, do the following:

Step 1 Log in to the IAM console. In the navigation pane, choose **User Groups**.

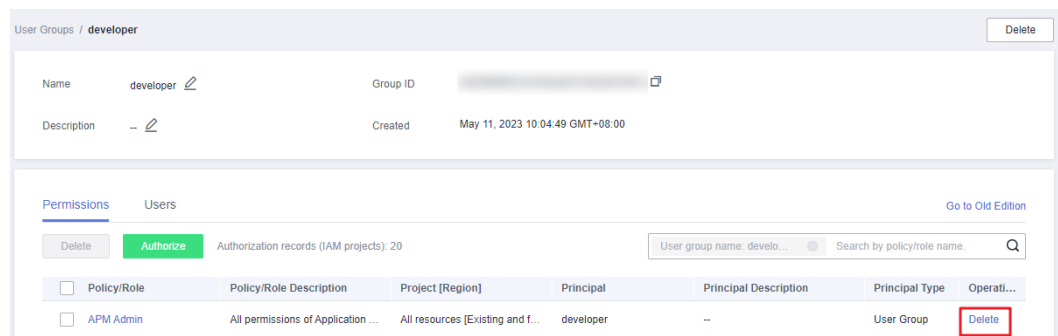
Step 2 Click the name of the user group to go to the group details page.

Figure 3-39 Clicking a user group name



Step 3 On the **Permissions** tab, click **Delete** in the row that contains the role or policy you want to delete.

Figure 3-40 Revoking permissions



Step 4 In the displayed dialog box, click **Yes**.

----End

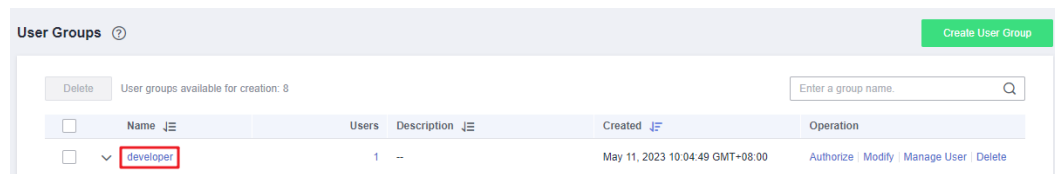
Batch Revoking Permissions of a User Group

To revoke multiple policies or roles attached to a user group, do as follows:

Step 1 Log in to the IAM console. In the navigation pane, choose **User Groups**.

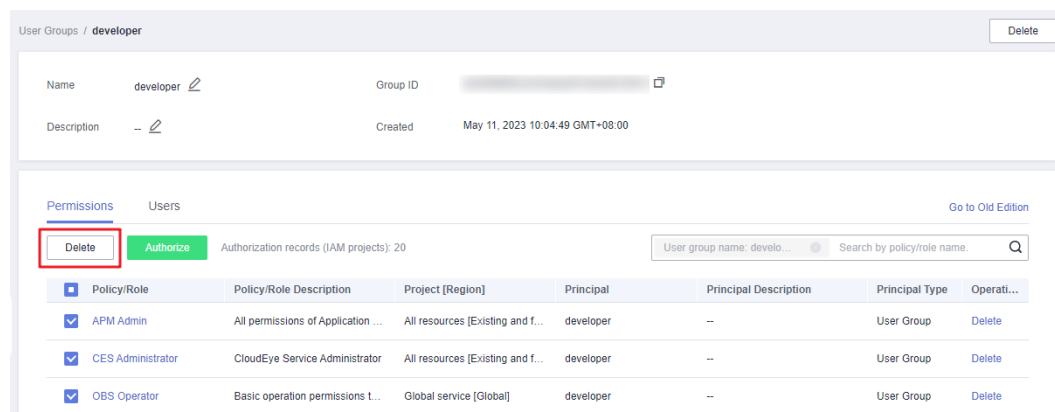
Step 2 Click the name of the user group to go to the group details page.

Figure 3-41 Viewing a user group



Step 3 On the **Permissions** page, select the roles or policies you want to delete and click **Delete** above the list.

Figure 3-42 Batch revoking permissions



Step 4 In the displayed dialog box, click **Yes**.
----End

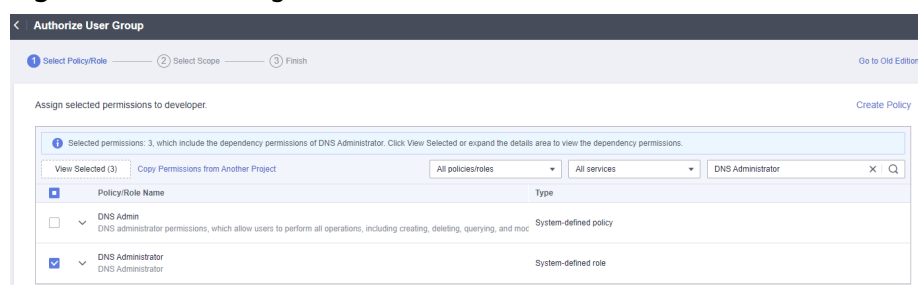
3.3.6 Assigning Dependency Roles

Cloud services interwork with each other. Roles of some services take effect only if they are assigned along with roles of other services.

Procedure

- Step 1** Log in to the IAM console as the administrator.
- Step 2** In the user group list, click **Authorize** in the row that contains the created user group.
- Step 3** On the displayed page, search for a role in the search box in the upper right corner.
- Step 4** Select the target role. The system automatically selects the dependency roles.

Figure 3-43 Selecting a role




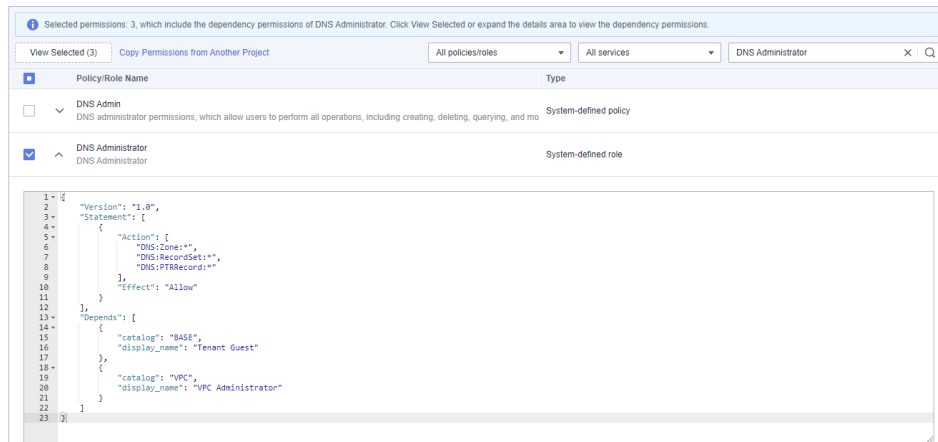
Step 5 Click  next to the role to view the dependencies.

Figure 3-44 Viewing dependencies



For example, the **DNS Administrator** role contains the **Depends** parameter which specifies the dependency roles. When you assign the **DNS Administrator** role to a user group, you also need to assign the **Tenant Guest** and **VPC Administrator** roles to the group for the same project.

Step 6 Click **OK**.

----End

3.4 Permissions Management

3.4.1 Basic Concepts

Permission

By default, IAM users do not have permissions. To assign permissions to IAM users, add them to one or more groups, and attach policies or roles to these groups. The users then inherit permissions from the groups to which the users belong, and can perform specific operations on cloud services.

Permission Type

You can grant users permissions by using roles and policies.

- **Roles:** a type of coarse-grained authorization mechanism that defines service-level permissions based on user responsibilities. IAM provides a limited number of roles for permissions management. When using roles to grant permissions, you also need to assign dependency roles. Roles are not an ideal choice for fine-grained authorization and secure access control.
- **Policies:** a type of fine-grained authorization mechanism that defines permissions required to perform operations on specific cloud resources under certain conditions. This mechanism allows for more flexible policy-based authorization and secure access control. For example, you can grant ECS users only the permissions required for managing a certain type of ECS resources.

IAM supports both [system-defined policies](#) and [custom policies](#).

System-Defined Policy

A system-defined policy defines the common actions of a cloud service. System-defined policies can be used to assign permissions to user groups, and they cannot be modified. **For details about the system-defined policies of all cloud services, see "Permissions".**

If there are no system-defined policies for a specific service, it indicates that IAM does not support this service.

Custom Policy


You can create custom policies using the actions supported by cloud services to supplement system-defined policies for more refined access control. You can create custom policies in the visual editor or in JSON view.

3.4.2 Roles

Roles are a type of coarse-grained authorization mechanism that defines service-level permissions based on user responsibilities. IAM provides a limited number of roles for permissions management.

Services on the cloud platform interwork with each other. Roles of some services take effect only if they are assigned along with roles of other services. For more information, see [3.3.6 Assigning Dependency Roles](#).

Role Content

When using roles to assign permissions, you can select a role and click  to view the details of the role. This section uses the **DNS Administrator** role as an example to describe the role content.

```
{
  "Version": "1.0",
  "Statement": [
    {
      "Action": [
        "DNS:Zone:*",
        "DNS:RecordSet:*",
        "DNS:PTRRecord:*"
      ],
      "Effect": "Allow"
    }
  ],
  "Depends": [
    {
      "catalog": "BASE",
      "display_name": "Tenant Guest"
    },
    {
      "catalog": "VPC",
      "display_name": "VPC Administrator"
    }
  ]
}
```

Parameter Description

Table 3-7 Parameter description

Parameter		Description	Value
Version		Role version.	1.0: indicates role-based access control.
Statement	Action	Operations to be performed on the service.	Format: " <i>Service name:Resource type.Operation</i> ". DNS:Zone:* : Permissions for performing all operations on Domain Name Service (DNS) zones.
	Effect	Determines whether to allow or deny the operations defined in the action.	<ul style="list-style-type: none"> • Allow • Deny NOTE If a role grants both Allow and Deny effects for the same action, the Deny takes precedence.
Depends	catalog	Name of the service to which a dependency role belongs.	Service name. Example: BASE and VPC .
	display_name	Name of the dependency role.	Role name. NOTE When you assign the DNS Administrator role to a user group, you also need to assign the Tenant Guest and VPC Administrator roles to the group for the same project. For more information about dependencies, see "Permissions".

3.4.3 Policies

3.4.3.1 Policy Content


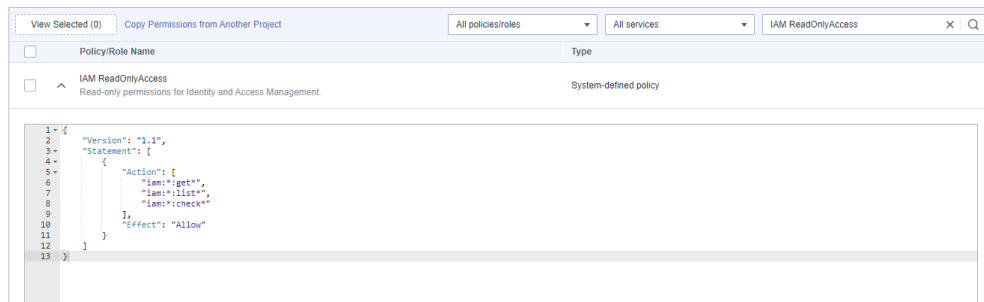
When you assign permissions to a user group, you can click  on the left of a policy name to view its details. This section uses the system-defined policy **IAM ReadOnlyAccess** as an example.

Figure 3-45 Content of the IAM ReadOnlyAccess policy



```

{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "iam:*get*",
        "iam:*list*",
        "iam:*check*"
      ],
      "Effect": "Allow"
    }
  ]
}

```

3.4.3.2 Policy Syntax

The following uses a custom policy for OBS as an example to describe the syntax.

```

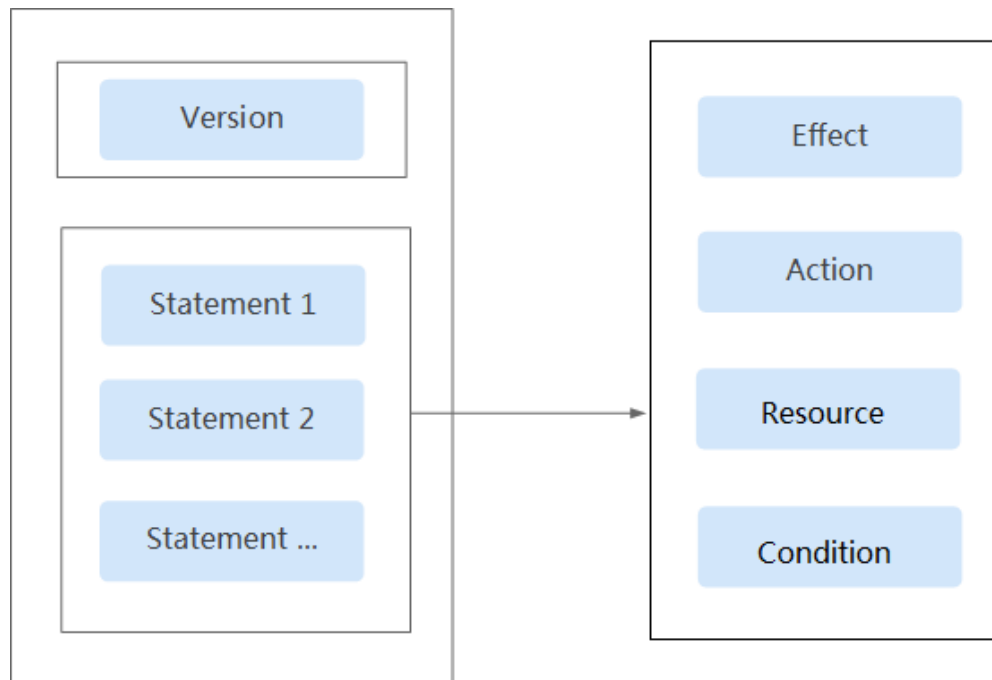
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "obs:bucket:ListAllMyBuckets",
        "obs:bucket:HeadBucket",
        "obs:bucket:ListBucket",
        "obs:bucket:GetBucketLocation"
      ],
      "Condition": {
        "StringEndWithIfExists": {
          "g:UserName": [
            "specialCharactor"
          ]
        },
        "Bool": {
          "g:MFAPresent": [
            "true"
          ]
        }
      },
      "Resource": [
        "obs:*:*:bucket:*"
      ]
    }
  ]
}

```

Policy Structure

A policy consists of a version and one or more statements (indicating different actions).

Figure 3-46 Policy structure



Policy Parameters

Policy parameters include **Version** and **Statement**, which are described in the following table. You can create custom policies by specifying the parameters. For details, see [3.4.5.3 Custom Policy Use Cases](#).

Table 3-8 Policy parameters

Parameter		Description	Value
Version		Policy version.	1.1 : indicates policy-based access control.
Statement	Effect	Determines whether to allow or deny the operations defined in the action.	<ul style="list-style-type: none"> Allow Deny <p>NOTE If an action has both Allow and Deny effects, the Deny effect takes precedence.</p>
	Action	Operations to be performed on the service.	Format: " <i>Service name.Resource type.Operation</i> ". Wildcard characters (*) are supported, indicating all options. Example: obs:bucket:ListAllMybuckets: Permissions for listing all OBS buckets. View all actions of the service in its <i>API Reference</i> .

Parameter		Description	Value
	Condition	Determines when a policy takes effect. A condition consists of a condition key and an operator .	<p>Format: "<i>Condition operator</i>. {<i>Condition key</i>: [<i>Value 1</i>, <i>Value 2</i>]}"</p> <p>If you set multiple conditions, the policy takes effect only when all the conditions are met.</p> <p>Example:</p> <p>StringEndWithIfExists": {"g:UserName": ["specialCharactor"]}: The statement is valid for users whose names end with specialCharactor.</p>
	Resource	Resources on which the policy takes effect.	<p>Format: <i>Service name.Region.Account ID.Resource type.Resource path</i>. Wildcard characters (*) are supported.</p> <p>Example:</p> <ul style="list-style-type: none"> ● obs:*:bucket:*: All OBS buckets. ● obs:*:object:my-bucket/my-object/*: All objects in the my-object directory of the my-bucket bucket.

- **Condition key**

A condition key is a key in the **Condition** element of a statement. There are global and service-level condition keys.

- Global condition keys (starting with **g**;) apply to all operations. IAM provides common global condition keys and special global condition keys.
 - Common global condition keys: Cloud services do not need to provide user identity information. Instead, IAM automatically abstracts user information and authenticates users. For details, see [Common global condition keys](#).
 - Special global condition keys: IAM obtains condition information from cloud services for authentication.
- Service-level condition keys (starting with a service name abbreviation, for example, **obs**;) apply only to operations on the specified service. For details, see the user guide of the corresponding cloud service.

Table 3-9 Common global condition keys

Global Condition Key	Type	Description
g:CurrentTime	Time	Time when an authentication request is received. The time is in ISO 8601 format, for example, 2012-11-11T23:59:59Z .
g:DomainName	String	Account name.
g:MFAPresent	Boolean	Whether to obtain a token through MFA authentication.
g:MFAAge	Number	Validity period of a token obtained through MFA authentication. This condition must be used together with g:MFAPresent .
g:ProjectName	String	Project name.
g:ServiceName	String	Service name.
g:UserId	String	IAM user ID.
g:UserName	String	IAM user name.

- **Operator**

An operator (see [Operators](#)), a condition key, and a condition value together constitute a complete condition statement. A policy takes effect only when its request conditions are met. The operator suffix **IfExists** indicates that a policy takes effect if a request value is empty or meets the specified condition. For example, if the operator **StringEqualsIfExists** is selected for a policy, the policy takes effect if a request value is empty or equal to the specified condition value.

Table 3-10 Operators (String operators are not case-sensitive unless otherwise specified.)

Operator	Type	Description
StringEquals	String	(Case-sensitive) The request value is the same as the condition value.
StringNotEquals	String	(Case-sensitive) The request value is different from the condition value.
StringEqualsIgnoreCase	String	The request value is the same as the condition value.
StringNotEqualsIgnoreCase	String	The request value is different from the condition value.

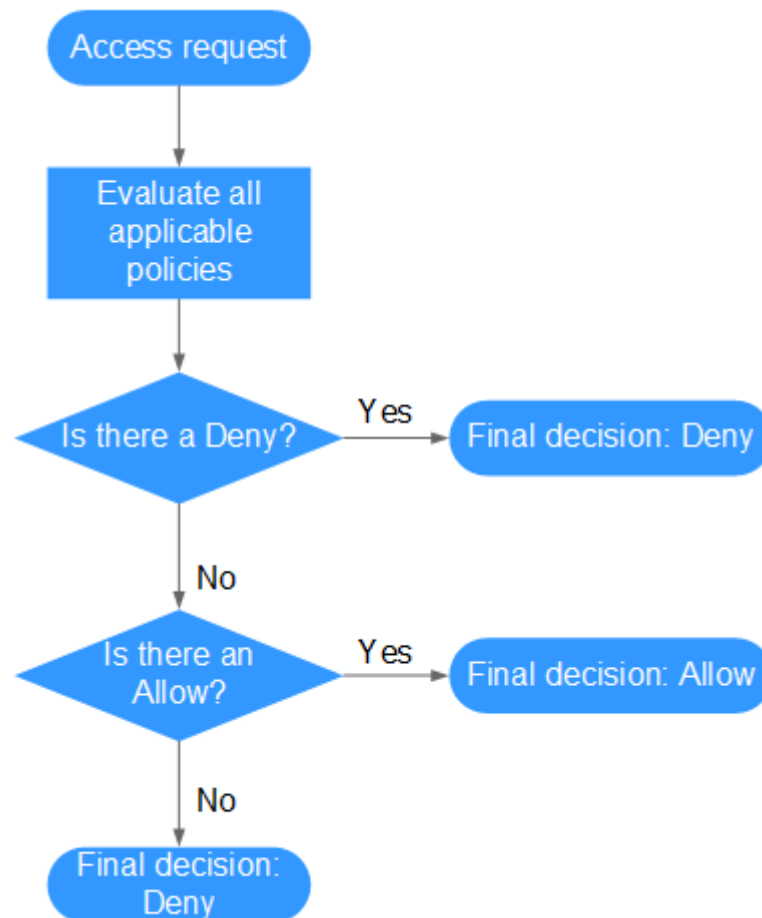
Operator	Type	Description
StringLike	String	The request value contains the condition value.
StringNotLike	String	The request value does not contain the condition value.
StringStartWith	String	The request value starts with the condition value.
StringEndWith	String	The request value ends with the condition value.
StringNotStartWith	String	The request value does not start with the condition value.
StringNotEndWith	String	The request value does not end with the condition value.
StringEqualsAnyOf	String	(Case-sensitive) The request value is the same as any of the configured condition values.
StringNotEqualsAnyOf	String	(Case-sensitive) The request value is different from all of the configured condition values.
StringEqualsIgnoreCaseAnyOf	String	The request value is the same as any of the configured condition values.
StringNotEqualsIgnoreCaseAnyOf	String	The request value is different from all of the configured condition values.
StringLikeAnyOf	String	The request value contains any of the configured condition values.
StringNotLikeAnyOf	String	The request value does not contain any of the configured condition values.
StringStartWithAnyOf	String	The request value starts with any of the configured condition values.
StringEndWithAnyOf	String	The request value ends with any of the configured condition values.
StringNotStartWithAnyOf	String	The request value does not start with any of the configured condition values.
StringNotEndWithAnyOf	String	The request value does not end with any of the configured condition values.
NumberEquals	Number	The request value is equal to the condition value.
NumberNotEquals	Number	The request value is not equal to the condition value.

Operator	Type	Description
NumberLessThan	Number	The request value is less than the condition value.
NumberLessThanEquals	Number	The request value is less than or equal to the condition value.
NumberGreaterThan	Number	The request value is greater than the condition value.
NumberGreaterThanEquals	Number	The request value is greater than or equal to the condition value.
NumberEqualsAnyOf	Number	The request value is equal to any of the configured condition values.
NumberNotEqualsAnyOf	Number	The request value is not equal to any of the configured condition values.
DateLessThan	Time	The request value is earlier than the condition value.
DateLessThanEquals	Time	The request value is earlier than or equal to the condition value.
DateGreaterThan	Time	The request value is later than the condition value.
DateGreaterThanEquals	Time	The request value is later than or equal to the condition value.
Bool	Boolean	The request value is equal to the condition value.
IpAddress	IP address	The request value is within the IP address range set in the condition value.
NotIpAddress	IP address	The request value is beyond the IP address range set in the condition value.
IsNullOrEmpty	Null	The request value is null or an empty string.
IsNull	Null	The request value is null.
IsNotNull	Null	The request value is not null.

3.4.3.3 Authentication Process

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

Figure 3-47 Authentication process



1. A user initiates an access request.
2. The system looks for a Deny among the applicable actions of the policies from which the user gets permissions. If the system finds an applicable Deny, it returns a decision of Deny, and the authentication ends.
3. If no Deny is found applicable, the system looks for an Allow that would apply to the request. If the system finds an applicable Allow, it returns a decision of Allow, and the authentication ends.
4. If no Allow is found applicable, the system returns a decision of Deny, and the authentication ends.

3.4.4 Authorization Records

View all authorization records under your account on the **Permissions > Authorization** page. You can filter records by policy/role name, username, user group name, agency name, IAM project, enterprise project (if it is enabled), and principal type (user, user group, and agency).

- Enterprise Project function enabled: View authorization records by IAM or enterprise project.
- Enterprise Project function not enabled: View authorization records by IAM project.

Figure 3-48 Enterprise Project function not enabled

Policy/Role	Policy/Role Description	Project (Region)	Principal	Principal Description	Principal Type	Operati...
Security Administrator	Full permissions for Identity an...	Global service [Global]	admin	Full permissions	User Group	Delete
Agent Operator	Permissions for switching role ...	All resources [Existing and f...	admin	Full permissions	User Group	Delete
Tenant Administrator	Tenant Administrator (Exclude ...	All resources [Existing and f...	admin	Full permissions	User Group	Delete

Viewing Authorization Records by IAM Project

When viewing authorization records by IAM project, select the following filter conditions:

- Policy/Role name:**
 To view the authorization records of a policy or role, select **Policy/Role name**, and enter a name. For details about the permissions of all cloud services, see "Permission Description".
- Username/User group name/Agency name:**
 To view the IAM project permissions assigned to a specific IAM user, user group, or agency, select **Username**, **User group name**, or **Agency name**, and enter a name.

NOTE

For IAM project-based authorization, you assign permissions by user group. If you query the authorization records of a specific user, the authorization records of the group to which the user belongs are displayed.

- IAM project:** The application scope of permissions. If you want to view authorization records of an IAM project, select **IAM project** and any of the following options:
 - Global service:** View authorization records of all global services.
 - All resources:** View authorization records of all projects, that is, the global service project and all region-specific projects (including projects created later).
 - Region-specific project:** View authorization records of a default project or subproject
- Principal type:** The type of objects that are authorized. There are three principal types: user, user group, and agency. In the IAM project view, filter records by user group or agency. If you select **User**, no records will be displayed.
- Enterprise project:** The name of an enterprise project. If you select **Enterprise project** and enter an enterprise project name, the **enterprise project view** is displayed.

Viewing Authorization Records by Enterprise Project

When viewing authorization records by enterprise project, select the following filter conditions:

- Policy/Role name:**
 To view the authorization records of a policy or role, select **Policy/Role name**, and enter a name. For details about the cloud service permissions supported

by enterprise projects, see "Cloud Service Permissions" in the *Enterprise Management User Guide*.

- **Username/User group name/Agency name:**

To view the enterprise project permissions assigned to a specific IAM user or user group, select **Username** or **User group name**, and enter a name.

 **NOTE**

- For enterprise project-based authorization, you assign permissions by user. If you query the authorization records of a specific user, the authorization records of the user and the user group to which the user belongs are displayed.
- **Enterprise project:** The name of an enterprise project, that is, the application scope of permissions. To view the authorization records of a specific enterprise project, select **Enterprise project**, and enter an enterprise project name.
- **Principal type:** The type of objects that are authorized. There are three principal types: user, user group, and agency.
- **IAM project:** The name of an IAM project or region. If you select **IAM project** and enter a project name, the **IAM project view** is displayed.

3.4.5 Custom Policies

3.4.5.1 Creating a Custom Policy

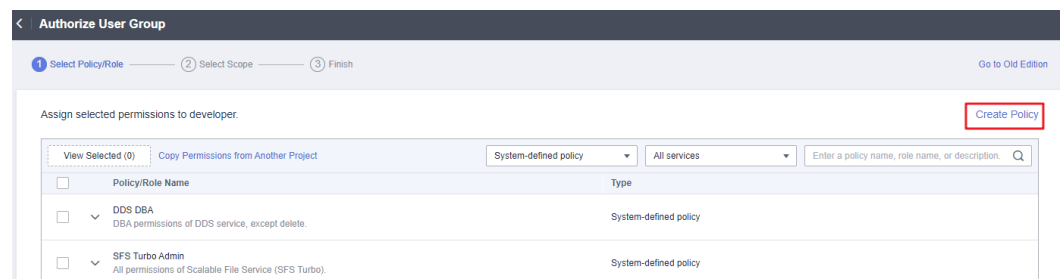
You can create custom policies to supplement system-defined policies and implement more refined access control.

You can create custom policies in either of the following ways:

- Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy syntax.
- JSON: Create a JSON policy or edit an existing one.

This section describes how to create custom policies on the **Permissions > Policies/Roles** page. You can also create custom policies during authorization (see [Figure 3-49](#)).

Figure 3-49 Creating a policy during authorization

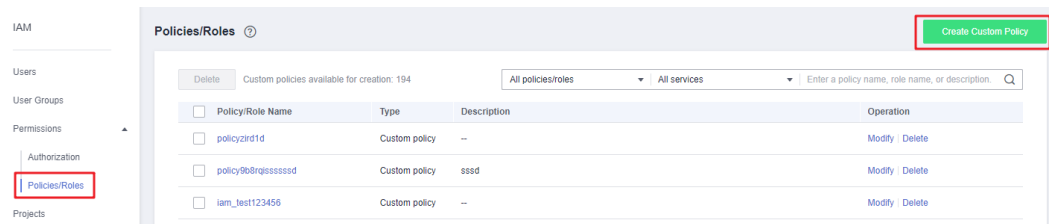


Creating a Custom Policy in the Visual Editor

Step 1 Log in to the IAM console.

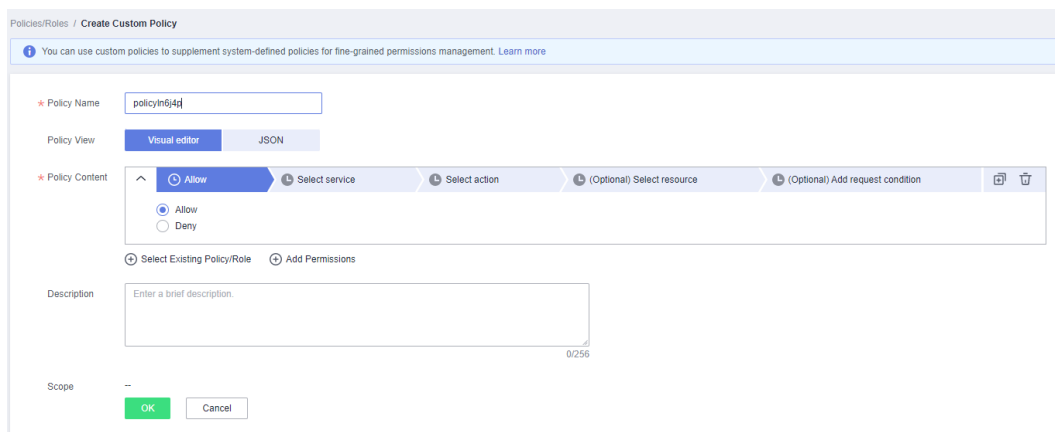
Step 2 On the IAM console, choose **Permissions > Policies/Roles** from the navigation pane, and click **Create Custom Policy** in the upper right corner.

Figure 3-50 Creating a custom policy



Step 3 Enter a policy name.

Figure 3-51 Entering a policy name



Step 4 Select a scope based on the type of services related to this policy. For more information about service types, see "Permissions".

- **Global services:** Select this option if the services to which the policy is related must be deployed in the Global region. When creating custom policies for globally deployed services, specify the scope as **Global services**. Custom policies of this scope must be attached to user groups for the global service project.
- **Project-level services:** Select this option if the services to which the policy is related must be deployed in specific regions. When creating custom policies for regionally deployed services, specify the scope as **Project-level services**. Custom policies of this scope must be attached to user groups for specific projects except the global service project.

For example, when creating a custom policy containing the action **evs:volumes:create** for EVS, specify the scope as **Project-level services**.

NOTE

A custom policy can contain actions of multiple services that are globally accessible or accessible through region-specific projects. To define permissions required to access both global and project-level services, create two custom policies and specify the scope as **Global services** and **Project-level services** respectively.

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

Step 6 Set the policy content.

1. Select **Allow** or **Deny**.

2. Select a cloud service.

 **NOTE**

- Only one cloud service can be selected for each permission block. To configure permissions for multiple cloud services, click **Add Permissions**, or switch to the JSON view (see [Creating a Custom Policy in JSON View](#)).
 - A custom policy can contain permissions for either global or project-level services. To define permissions required to access both global and project-level services, enclose the permissions in two separate custom policies for refined authorization.
3. Select actions.
 4. (Optional) Select all resources, or select specific resources by specifying their paths.

Table 3-11 Resource type

Parameter	Description
Specific	<p>Permissions for specific resources. For example, to define permissions for buckets whose names start with TestBucket, specify the bucket resource path as OBS:*:*:bucket:TestBucket*.</p> <p>NOTE</p> <ul style="list-style-type: none"> - Specifying bucket resources Format: "OBS:*:*:bucket:<i>Bucket name</i>". <p>For bucket resources, IAM automatically generates the prefix of the resource path: obs:*:*:bucket:. For the path of a specific bucket, add the <i>bucket name</i> to the end. You can also use a wildcard character (*) to indicate any bucket. For example, obs:*:*:bucket:* indicates any OBS bucket.</p> <ul style="list-style-type: none"> - Specifying object resources Format: "OBS:*:*:object:<i>Bucket name or object name</i>". <p>For object resources, IAM automatically generates the prefix of the resource path: obs:*:*:object:. For the path of a specific object, add the <i>bucket name/object name</i> to the end of the resource path. You can also use a wildcard character (*) to indicate any object in a bucket. For example, obs:*:*:object:my-bucket/my-object/* indicates any object in the my-object directory of the my-bucket bucket.</p>
All	Permissions for all resources.

5. (Optional) Add request conditions by specifying condition keys, operators, and values.

Table 3-12 Condition parameters

Name	Description
Condition Key	A key in the Condition element of a statement. There are global and service-specific condition keys. Global condition keys (starting with g:) are available for operations of all services, whereas service-specific condition keys (starting with a service abbreviation name such as obs:) are available only for operations of the corresponding service. For details, see the user guide of the corresponding cloud service.
Operator	Used together with a condition key and condition value to form a complete condition statement.
Value	Used together with a condition key and an operator that requires a keyword, to form a complete condition statement.

Figure 3-52 Adding a request condition

Table 3-13 Global condition keys

Global Condition Key	Type	Description
g:CurrentTime	Time	Time when an authentication request is received. The time is in ISO 8601 format, for example, 2012-11-11T23:59:59Z .
g:DomainName	String	Account name.
g:MFAPresent	Boolean	Whether to obtain a token through MFA authentication.
g:MFAAge	Number	Validity period of a token obtained through MFA authentication. This condition must be used together with g:MFAPresent .
g:ProjectName	String	Project name.

Global Condition Key	Type	Description
g:ServiceName	String	Service name.
g:UserId	String	IAM user ID.
g:UserName	String	IAM user name.

Step 7 (Optional) Switch to the JSON view and modify the policy content in JSON format.

NOTE

If the modified policy content is incorrect, check and modify the content again, or click **Reset** to cancel the modifications.

Step 8 (Optional) To add another permission block for the policy, click **Add Permissions**. Alternatively, click the plus (+) icon on the right of an existing permission block to clone its permissions.

Step 9 (Optional) Enter a brief description for the policy.

Step 10 Click **OK**.

Step 11 Attach the policy to a user group. Users in the group then inherit the permissions defined in this policy.

NOTE

You can attach custom policies to a user group in the same way as you attach system-defined policies. For details, see [3.3.1 Creating a User Group and Assigning Permissions](#).

----End

Creating a Custom Policy in JSON View

Step 1 Log in to the IAM console.

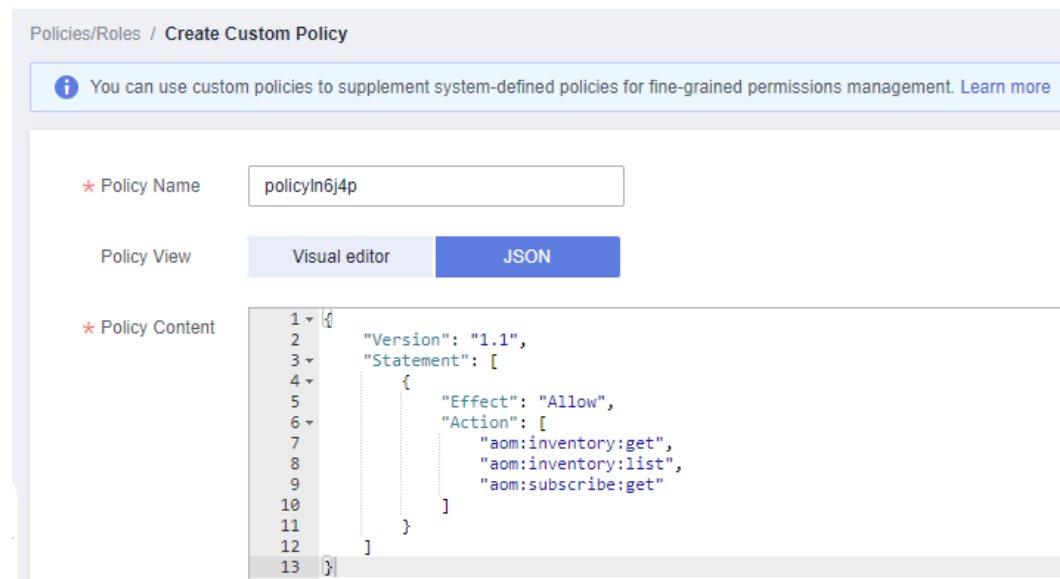
Step 2 On the IAM console, choose **Permissions > Policies/Roles** from the navigation pane, and click **Create Custom Policy** in the upper right corner.

Figure 3-53 Creating a custom policy



Step 3 Enter a policy name.

Figure 3-54 Entering a policy name



Step 4 Select a scope based on the type of services related to this policy. For more information about service types, see "Permissions".

- **Global services:** Select this option if the services to which the policy is related must be deployed in the Global region. When creating custom policies for globally deployed services, specify the scope as **Global services**. Custom policies of this scope must be attached to user groups for the global service project.
- **Project-level services:** Select this option if the services to which the policy is related must be deployed in specific regions. When creating custom policies for regionally deployed services, specify the scope as **Project-level services**. Custom policies of this scope must be attached to user groups for specific projects except the global service project.

For example, when creating a custom policy containing the action **evs:volumes:create** for EVS, specify the scope as **Project-level services**.

NOTE

A custom policy can contain actions of multiple services that are globally accessible or accessible through region-specific projects. To define permissions required to access both global and project-level services, create two custom policies and specify the scope as **Global services** and **Project-level services** respectively.

Step 5 Select **JSON** for **Policy View**.

Step 6 (Optional) Click **Select Existing Policy/Role**, and select a policy/role to use it as a template, for example, select **EVS Admin**.

NOTE

If you select multiple policies, all of them must have the same scope, that is, either **Global services** or **Project-level services**. To define permissions required to access both global and project-level services, enclose the permissions in two separate custom policies for refined authorization.

Step 7 Click **OK**.

Step 8 Modify the statement in the template.

- **Effect:** Set it to **Allow** or **Deny**.
- **Action:** Enter the actions listed in the API actions table (see [Figure 3-55](#)) of the EVS service, for example, **evs:volumes:create**.

Figure 3-55 API actions

Permission	API	Action
Listing Users	GET /v3/users	iam:users:listUsers

 **NOTE**

The version of each custom policy is fixed at **1.1**.

Step 9 (Optional) Enter a brief description for the policy.

Step 10 Click **OK**. If the policy list is displayed, the policy is created successfully. If a message indicating incorrect policy content is displayed, modify the policy.

Step 11 Attach the policy to a user group. Users in the group then inherit the permissions defined in this policy.

 **NOTE**

You can attach custom policies to a user group in the same way as you attach system-defined policies. For details, see [3.3.1 Creating a User Group and Assigning Permissions](#).

----End

3.4.5.2 Modifying or Deleting a Custom Policy

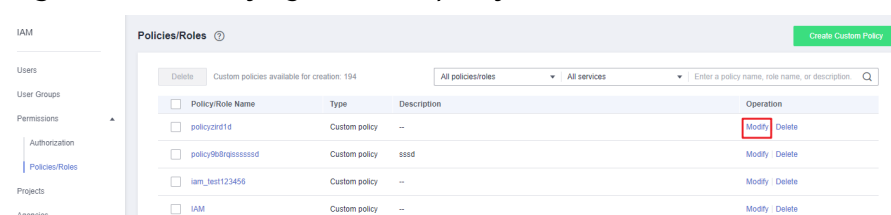
You can modify or delete custom policies.

Modifying a Custom Policy

Modify the name, description, or content of a custom policy.

1. In the left navigation pane on the IAM console, choose **Permissions** > **Policies/Roles**.
2. Locate the custom policy you want to modify and click **Modify** in the **Operation** column, or click the custom policy name to go to the policy details page.

Figure 3-56 Modifying a custom policy



3. Modify the name or description of the policy as required.

4. Modify the policy content by following the instructions provided in [Creating a Custom Policy in the Visual Editor](#) as required.
5. Click **OK** to save the modifications.

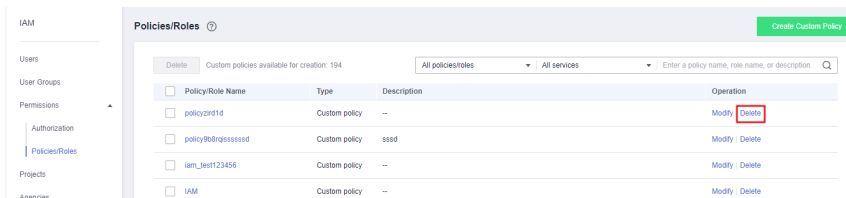
Deleting a Custom Policy

NOTE

Only custom policies that are not attached to any user groups or agencies can be deleted. If a custom policy has been attached to certain user groups or agencies, detach the policy and then delete it.

1. In the left navigation pane on the IAM console, choose **Permissions > Policies/Roles**.
2. In the row containing the custom policy you want to delete, click **Delete**.

Figure 3-57 Deleting a custom policy



3. Click **Yes**.

3.4.5.3 Custom Policy Use Cases

Using a Custom Policy Along with Full-Permission System-Defined Policies

If you want to assign full permissions to a user but disallow them from accessing a specific service, such as Cloud Trace Service (CTS), create a custom policy for denying access to CTS and then attach this custom policy together with the **FullAccess** policy to the user. As an explicit deny in any policy overrides any allows, the user can perform operations on all services except CTS.

Example policy denying access only to CTS:

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "cts:*:*"
      ]
    }
  ]
}
```

NOTE

- **Action:** Operations to be performed. Each action must be defined in the format "*Service name:Resource type:Operation*".
For example, **cts:*:*** refers to permissions for performing all operations on all resource types of CTS.
- **Effect:** Determines whether to deny or allow the operation.

Using a Custom Policy Along with a System-Defined Policy

- If you want to assign full permissions to a user but disallow them from creating BMSs, create a custom policy denying the **bms:servers:create** action and then attach this custom policy together with the **BMS FullAccess** policy to the user. As an explicit deny in any policy overrides any allows, the user can perform all operations on BMS except creating BMSs.

Example policy denying BMS creation:

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "bms:servers:create"
      ]
    }
  ]
}
```

- If you want to assign OBS read-only permissions to all users but disallow certain users from viewing specific resources, for example, disallow users whose names start with **TestUser** from viewing buckets whose names start with **TestBucket**, create a custom policy denying such operations and attach this custom policy together with the OBS ReadOnlyAccess policy to those users. As an explicit deny in any policy overrides any allows, certain users cannot view buckets whose names start with **TestBucket**.

Example policy denying users whose names start with **TestUser** from viewing buckets whose names start with **TestBucket**:

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "obs:bucket:ListAllMybuckets",
        "obs:bucket:HeadBucket",
        "obs:bucket:ListBucket",
        "obs:bucket:GetBucketLocation"
      ],
      "Resource": [
        "obs:*:bucket:TestBucket*"
      ],
      "Condition": {
        "StringStartWith": {
          "g:UserName": [
            "TestUser"
          ]
        }
      }
    }
  ]
}
```

NOTE

Currently, only certain cloud services (such as OBS) support resource-based authorization. For services that do not support this function, you cannot create custom policies containing resource types.

Using Only a Custom Policy

You can create a custom policy and attach only the custom policy to the group to which the user belongs.

- The following is an example policy that allows access only to ECS, EVS, VPC, ELB, and Application Operations Management (AOM).

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow"
      "Action": [
        "ecs:*:*",
        "evs:*:*",
        "vpc:*:*",
        "elb:*:*",
        "aom:*:*"
      ]
    }
  ]
}
```

- The following is an example policy that allows only IAM users whose names start with **TestUser** to delete all objects in the **my-object** directory of the bucket **my-bucket**.

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "obs:object:DeleteObject"
      ],
      "Resource": [
        "obs:*:*:object:my-bucket/my-object/*"
      ],
      "Condition": {
        "StringStartWith": {
          "g:UserName": [
            "TestUser"
          ]
        }
      }
    }
  ]
}
```

- The following is an example policy that allows access to all services except ECS, EVS, VPC, ELB, AOM, and APM.

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "*"
      ]
    },
    {
      "Action": [
        "ecs:*:*",
        "evs:*:*",
        "vpc:*:*",
        "elb:*:*",
        "aom:*:*",
        "apm:*:*"
      ],
      "Effect": "Deny"
    }
  ]
}
```

```
} ]
```

3.4.5.4 Cloud Services that Support Resource-Level Authorization Using IAM

If you want to grant an IAM user permissions for specific resources, **create a custom policy** that contains permissions for the resources, and attach the policy to the user. The user then only has the permissions for the specified resources. For example, to grant an IAM user permissions for buckets whose names start with **TestBucket**, create a custom policy, specify the resource path as **OBS::*:bucket:TestBucket***, and attach the policy to the user.

The following table lists the cloud services that support resource-level authorization and the supported resource types.

Table 3-14 Cloud services that support resource-level authorization and the supported resource types

Service	Resource Type	Resource Name
Elastic Cloud Server (ECS)	instance	ECS
Elastic Volume Service (EVS)	volume	EVS disk
Object Storage Service (OBS)	bucket	Bucket
	object	Object
Software Repository for Container (SWR)	chart	chart
	repository	Repository
	instance	Instance
Data Lake Insight (DLI)	queue	DLI queue
	database	DLI database
	table	DLI table
	column	DLI column
	datasourceauth	DLI security authentication information
	jobs	DLI job
Graph Engine Service (GES)	graphName	GES graph name
	backupName	GES backup name
Distributed Message Service (DMS)	rabbitmq	RabbitMQ instance
	kafka	Kafka instance
GaussDB(DWS)	cluster	Cluster

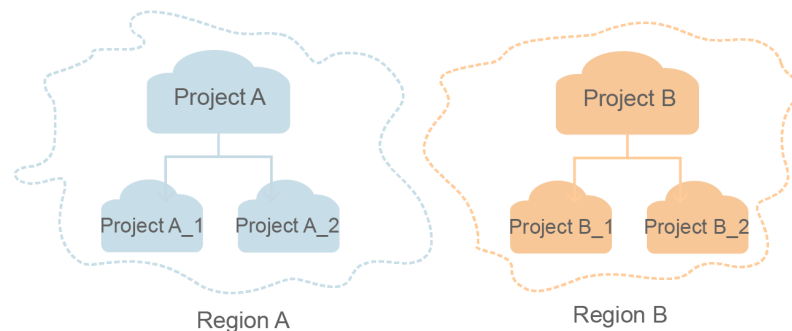
3.5 Projects

Projects are used to isolate resources (including compute, storage, and network resources) among physical regions. A project is provided for each region by default, and permissions are assigned based on projects.

For more refined access control, create subprojects under a project and create resources in the subprojects. Then, provide users with permissions to access resources in specific subprojects.

IAM projects are different from enterprise projects. For details about their differences, see Identity and Access Management > FAQs > Project Management > What Are the Differences Between IAM Projects and Enterprise Projects?

Figure 3-58 Project isolation



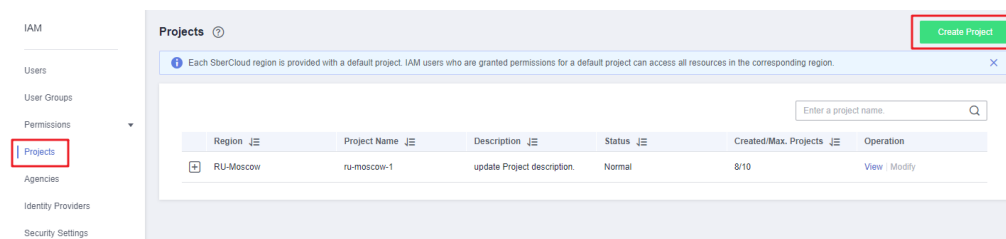
NOTE

- Resources cannot be transferred across IAM projects.
- You cannot create projects in IAM after enabling the Enterprise Project function.

Creating a Project

Step 1 In the left navigation pane on the IAM console, choose Projects and click **Create Project**.

Figure 3-59 Creating a project



Step 2 Select a region in which you want to create a subproject.

Step 3 Enter a project name.

NOTE

- The project name will be in the format "*Name of the default project for the selected region_Custom project name*". The name of default projects cannot be modified.
- The project name can only contain letters, digits, hyphens (-), and underscores (_). The total length of the project name cannot exceed 64 characters.

Step 4 (Optional) Enter a description for the project.

Step 5 Click **OK**.

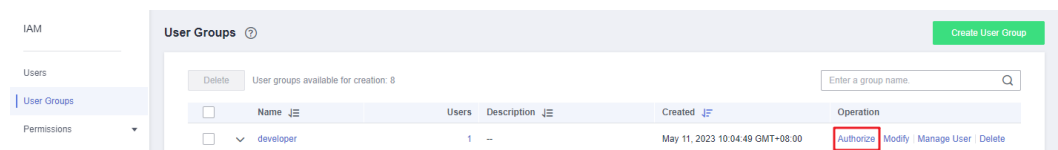
----End

Granting a User Group Permissions for a Project

You can assign permissions based on projects to control access to resources in specific projects.

Step 1 In the user group list, click **Authorize** in the row containing the target user group.

Figure 3-60 Managing permissions



Step 2 On the **Authorize User Group** page, select the policies or roles to be attached to the user group and click **Next**.

Step 3 Specify the authorization scope. If you select **Region-specific projects**, select one or more projects.

Step 4 Click **OK**.

NOTE

For more information about user group authorization, see [3.3.1 Creating a User Group and Assigning Permissions](#).

----End

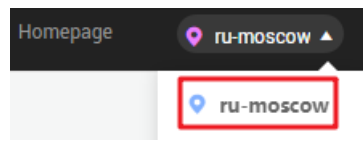
Switching Regions or Projects

For project-level services, switch to a region or project in which you have been authorized to access cloud services. You do not need to switch regions or projects for global services.

Step 1 Log in to the management console.

Step 2 Go to a project-level cloud service page. Click the drop-down list box in the upper left corner of the page and select a region.

Figure 3-61 Switching to a specific region or project



----End

3.6 Agencies

3.6.1 Account Delegation

3.6.1.1 Delegating Resource Access to Another Account

The agency function enables you to delegate another account to implement O&M on your resources based on assigned permissions.

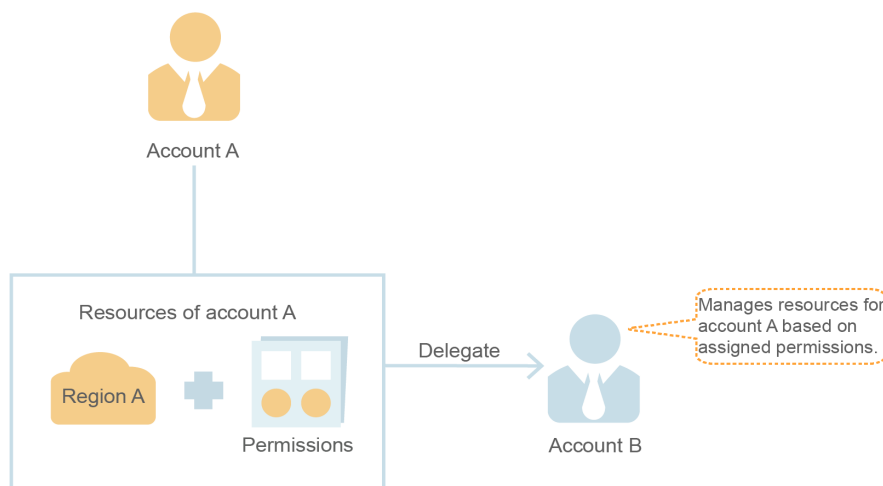
NOTE

You can delegate resource access only to accounts. The accounts can then delegate access to IAM users under them.

The following is the procedure for delegating access to resources in one account to another account. Account A is the delegating party and account B is the delegated party.

Step 1 Account A creates an agency in IAM to delegate resource access to account B.

Figure 3-62 (Account A) Creating an agency

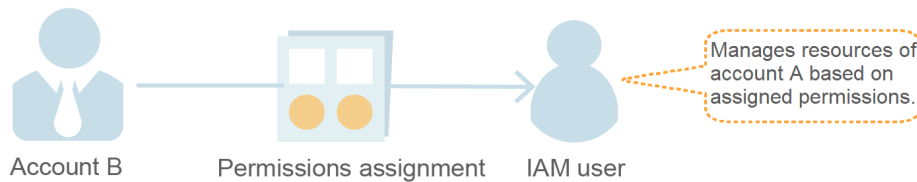


Step 2 (Optional) Account B assigns permissions to an IAM user to manage specific resources for account A.

1. Create a user group, and grant it permissions required to manage account A's resources.

2. Create a user and add the user to the user group.

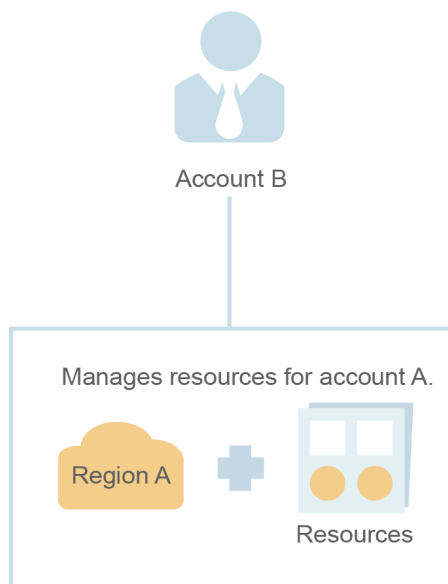
Figure 3-63 (Account B) Authorizing an IAM user to manage delegated resources



Step 3 Account B or the authorized user manages account A's resources.

1. Log in to account B's account and switch the role to account A.
2. Switch to region A and manage account A's resources in this region.

Figure 3-64 (Account B) Switching the role



----End

3.6.1.2 Creating an Agency (by a Delegating Party)

By creating an agency, you can share your resources with another account, or delegate an individual or team to manage your resources. You do not need to share your security credentials (the password and access keys) with the delegated party. Instead, the delegated party can log in with its own account credentials and then switches the role to your account and manage your resources.

Prerequisites

Before creating an agency, complete the following operations:

- Understand the **basic concepts** of permissions.

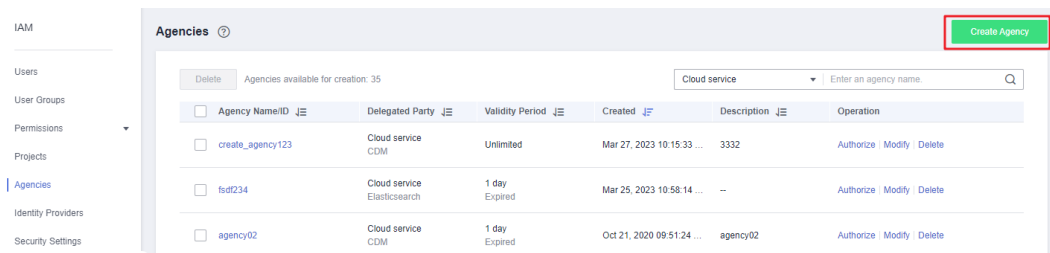
- Determine the "permissions" to be assigned to the agency, and check whether the permissions have dependencies. For more details, see [Assigning Dependency Roles](#).

Procedure

Step 1 Log in to the IAM console.

Step 2 On the IAM console, choose **Agencies** from the navigation pane, and click **Create Agency** in the upper right corner.

Figure 3-65 Creating an agency



Step 3 Enter an agency name.

Figure 3-66 Setting the agency name

Agencies / Create Agency

* Agency Name:

* Agency Type: Account
Delegate another SberCloud account to perform operations on your resources.
 Cloud service
Delegate a cloud service to access your resources in other cloud services.

* Delegated Account:

* Validity Period:

Description:

0/255

Step 4 Specify the agency type as **Account**, and enter the name of a delegated account.

NOTE

- **Account:** Share resources with another account or delegate an individual or team to manage your resources. The delegated account can only be an account, rather than an IAM user or a federated user.
- **Cloud service:** Delegate a specific service to access other services. For more information, see [3.6.2 Cloud Service Delegation](#).

Step 5 Set the validity period and enter a description for the agency.

Step 6 Click **Next**.

Step 7 Select the policies or roles to be attached to the agency, click **Next**, and select the authorization scope.

 **NOTE**

- Assigning permissions to an agency is similar to assigning permissions to a user group. The two operations differ only in the number of available permissions. For details about how to assign permissions to a user group, see [Assigning Permissions to a User Group](#).
- Agencies cannot be assigned the **Security Administrator** role. For account security, grant permissions required to agencies based on the principle of least privilege.

Step 8 Click **OK**.

 **NOTE**

After creating an agency, provide your account name, agency name, agency ID, and agency permissions to the delegated party. The delegated party can then switch the role to your account and manage specific resources based on the assigned permissions.

----End

3.6.1.3 (Optional) Assigning Permissions to an IAM User (by a Delegated Party)

When a trust relationship is established between your account and another account, you become a delegated party. By default, only your account and the members of the **admin** group can manage resources for the delegating party. To authorize IAM users to manage these resources, assign permissions to the users.

You can authorize an IAM user to manage resources for all delegating parties, or authorize the user to manage resources for a specific delegating party.

Prerequisites

- A trust relationship has been established between your account and another account.
- You have obtained the name of the delegating account and the name and ID of the created agency.

Procedure

Step 1 Create a user group and grant permissions to it.

1. On the **User Groups** page, click **Create User Group**.
2. Enter a user group name.
3. Click **OK**.
4. In the row containing the user group, click **Authorize**.
5. Create a custom policy.

 **NOTE**

This step is used to create a policy containing permissions required to manage resources for a specific agency. If you want to authorize an IAM user to manage resources for all agencies, go to [Step 1.6](#).

- a. On the **Select Policy/Role** page, click **Create Policy** in the upper right corner of the permission list.
- b. Enter a policy name.
- c. Select **JSON** for **Policy View**.
- d. In the **Policy Content** area, enter the following content:

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "iam:agencies:assume"
      ],
      "Resource": {
        "uri": [
          "/iam/agencies/b36b1258b5dc41a4aa8255508xxx..."
        ]
      },
      "Effect": "Allow"
    }
  ]
}
```

 **NOTE**

- Replace *b36b1258b5dc41a4aa8255508xxx...* with the agency ID obtained from a delegating party. Do not make any other changes.
 - For more information about permissions, see [3.4 Permissions Management](#).
- e. Click **Next**.
 6. Select the policy created in the previous step or the **Agent Operator** role and click **Next**.
 - Custom policy: Allows a user to manage resources only for a specific agency.
 - **Agent Operator** role: Allows a user to manage resources for all agencies.
 7. Specify the authorization scope.
 8. Click **OK**.

Step 2 Create an IAM user and add the user to the user group.

1. On the **Users** page, click **Create User**.
2. On the **Create User** page, enter a username.
3. For the access type, select **Management console access** and **Set by user**.
4. Enable login protection and click **Next**.
5. Select the user group created in [Step 1](#) and click **Create**.

 **NOTE**

After the authorization is complete, the IAM user can switch to the account of the delegating party and manage specific resources under the account.

----End

Related Operations

The delegated account or the authorized IAM users can **switch their roles** to the delegating account to view and use its resources.

3.6.1.4 Switching Roles (by a Delegated Party)

When an account establishes a trust relationship with your account, you become a delegated party. You and all the users you have authorized can switch to the delegating account and manage resources under the account based on assigned permissions.

Prerequisites

- A trust relationship has been established between your account and another account.
- You have obtained the delegating account name and agency name.

Procedure

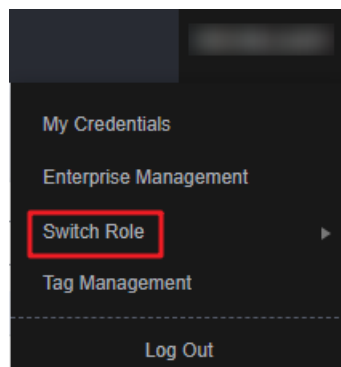
- Step 1** Log in to the management console using your account or log in as the IAM user created in **Step 2**.

 **NOTE**

The IAM user created in **Step 2** of **3.6.1.3 (Optional) Assigning Permissions to an IAM User (by a Delegated Party)** can switch roles to manage resources for the delegating party.

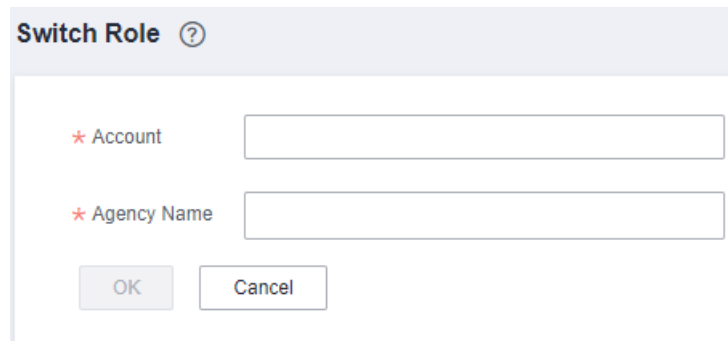
- Step 2** Hover the mouse pointer over the username in the upper right corner and choose **Switch Role**.

Figure 3-67 Switching the role



- Step 3** On the **Switch Role** page, enter the account name of the delegating party.

Figure 3-68 Entering the account name and agency name of the delegating party



NOTE

After you enter the account name, the agencies created under this account will be automatically displayed after you click the agency name text box. Select an authorized one from the drop-down list.

Step 4 Click **OK** to switch to the delegating account.

----End

Follow-Up Procedure

To return to your own account, hover the mouse pointer over the username in the upper right corner, choose **Switch Role**, and select your account.

3.6.2 Cloud Service Delegation

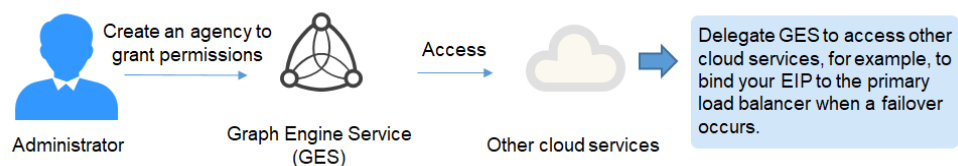
Services on the cloud platform interwork with each other, and some cloud services are dependent on other services. To delegate a cloud service to access other services and perform resource O&M, create an agency for the service.

IAM provides two methods to create a cloud service agency:

1. **Creating a cloud service agency on the IAM console**

The following takes a Graph Engine Service (GES) agency as an example. The agency allows GES to use other cloud services, for example, to bind your EIP to the primary load balancer if a failover occurs.

Figure 3-69 Cloud service delegation



2. **Automatically creating a cloud service agency to use certain resources**

The following takes Scalable File Service (SFS) as an example to describe the procedure for automatically creating a cloud service agency:

- a. Go to the SFS console.

- b. On the **Create File System** page, enable static data encryption.
- c. A dialog box is displayed requesting you to confirm the creation of an SFS agency. After you click **OK**, the system automatically creates an SFS agency with **KMS CMKFullAccess** permissions for the current project. With the agency, SFS can obtain KMS keys for encrypting or decrypting file systems.
- d. You can view the agency in the agency list on the IAM console.

Creating a Cloud Service Agency on the IAM Console

Step 1 Log in to the IAM console.

Step 2 On the IAM console, choose **Agencies** from the navigation pane, and click **Create Agency**.

Step 3 Enter an agency name.

Figure 3-70 Cloud service agency name

The screenshot shows the 'Create Agency' form in the IAM console. The form is titled 'Agencies / Create Agency' and contains several fields:

- Agency Name:** A text input field containing 'Cloud Agency'.
- Agency Type:** Two radio button options: 'Account' (unselected) and 'Cloud service' (selected). Below 'Account' is the text 'Delegate another SberCloud account to perform operations on your resources.' Below 'Cloud service' is the text 'Delegate a cloud service to access your resources in other cloud services.'
- Cloud Service:** A dropdown menu with 'CDM' selected.
- Validity Period:** A dropdown menu with 'Unlimited' selected.
- Description:** A text area with the placeholder text 'Enter a brief description.' and a character count '0/255' at the bottom right.

At the bottom of the form are two buttons: 'Next' (green) and 'Cancel' (white).

Step 4 Select the **Cloud service** agency type, and then select a service.

Step 5 Select a validity period.

Step 6 (Optional) Enter a description for the agency to facilitate identification.

Step 7 Click **Next**.

Step 8 Select the permissions to be assigned to the agency, click **Next**, and specify the authorization scope.

Step 9 Click **OK**.

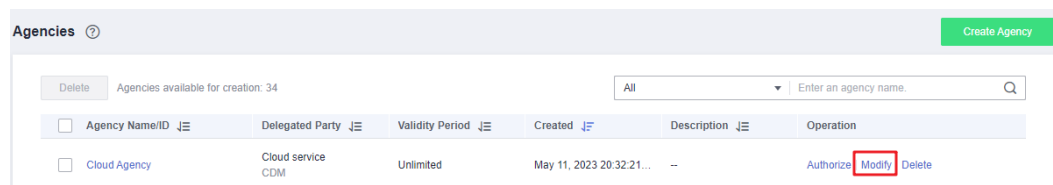
----End

3.6.3 Deleting or Modifying Agencies

Modifying an Agency

To modify the permissions, validity period, and description of an agency, click **Modify** in the row containing the agency you want to modify.

Figure 3-71 Modifying an agency



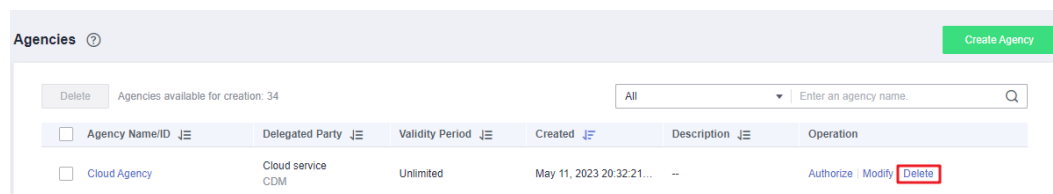
NOTE

- You can change the cloud service, validity period, description, and permissions of cloud service agencies, but you cannot change the agency name and type.
- Modifying the permissions of cloud service agencies may affect the usage of certain functions of cloud services. Exercise caution when performing this operation.

Deleting an Agency

To delete an agency, click **Delete** in the row containing the agency to be deleted and click **Yes**.

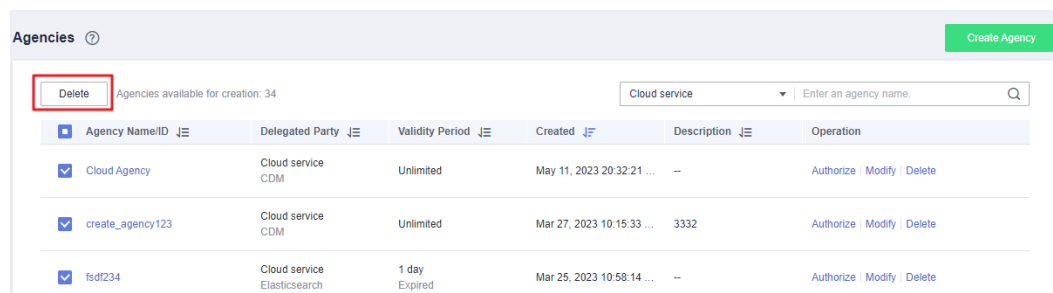
Figure 3-72 Deleting an agency



Batch Deleting Agencies

To delete multiple agencies, select the agencies to be deleted in the list and click **Delete** above the list.

Figure 3-73 Batch deleting agencies



 NOTE

After you delete an agency, all permissions granted to the delegated accounts will be revoked.

3.7 Security Settings

3.7.1 Security Settings Overview

You can configure the account settings, critical operation protection, login authentication policy, password policy, and access control list (ACL) on the **Security Settings** page. For details, see [3.7.2 Basic Information](#), [3.7.3 Critical Operation Protection](#), [3.7.4 Login Authentication Policy](#), [3.7.5 Password Policy](#), and [3.7.6 ACL](#). This chapter describes how to access the **Security Settings** page and who is the intended audience.

Intended Audience

[Table 3-15](#) lists the intended audience of different functions provided on the **Account Security Settings** page and their access permissions for the functions.

Table 3-15 Intended audience

Function	Intended Audience
Basic Information	IAM users: Full access
Critical Operations	<ul style="list-style-type: none"> • Administrator: Full access • IAM users: No access
Login Authentication Policy	<ul style="list-style-type: none"> • Administrator: Full access • IAM users: Read-only access
Password Policy	<ul style="list-style-type: none"> • Administrator: Full access • IAM users: Read-only access
ACL	<ul style="list-style-type: none"> • Administrator: Full access • IAM users: No access

Accessing the Security Settings Page

- You and all IAM users created using your account can access the **Security Settings** page from the management console.
 - a. Log in to the IAM console.

- b. In the left navigation pane, choose **Security Settings**.

3.7.2 Basic Information

As an account administrator, both you and your IAM users can manage basic information on this page.

NOTE

- A mobile number or an email address can be bound only to one account or IAM user.
- Only one mobile number, email address, and virtual MFA can be bound to an account or IAM user.

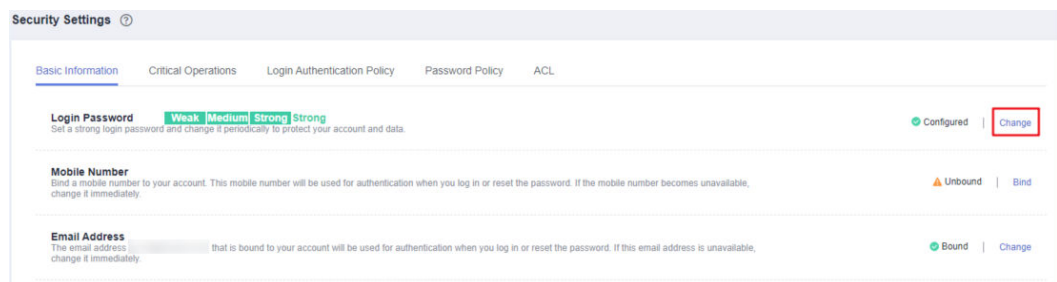
Changing the Login Password, Mobile Number, or Email Address

The methods for changing the login password, mobile number, and email address are similar. To change the login password, do as follows:

Step 1 Go to the [Security Settings](#) page.

Step 2 Click the **Basic Information** tab, and click **Change** in the **Login Password** row.

Figure 3-74 Changing the login password



Step 3 (Optional) Select email address or mobile number verification, and enter the verification code.

NOTE

If neither email address nor mobile number is bound, no verification is required.

Step 4 Enter the old password and new password, and enter the new password again.

NOTE

- The password cannot be the username or the username spelled backwards. For example, if the username is **A12345**, the password cannot be **A12345**, **a12345**, **54321A**, or **54321a**.
- To prevent password cracking, the administrator can configure the password policy to define password requirements, such as minimum password length. For details, see [3.7.5 Password Policy](#).

Step 5 Click **OK**.

----End

3.7.3 Critical Operation Protection

Only an **administrator** can configure critical operation protection, and IAM users can only view the configurations. If an IAM user needs to modify the

configurations, the user can request the administrator to perform the modification or grant the required permissions.

 **NOTE**

Federated users do not need to verify their identity when performing critical operations.

Virtual MFA Device

An MFA device generates 6-digit verification codes in compliance with the Time-based One-time Password Algorithm (TOTP). MFA devices can be hardware- or software-based. Currently, only software-based virtual MFA devices are supported, and they are application programs running on smart devices such as mobile phones.

This section describes how to bind a virtual MFA device. If you have installed another MFA application, add a user by following the on-screen prompts. For details about how to bind or remove a virtual MFA device, see [3.9.2 Virtual MFA Device](#).

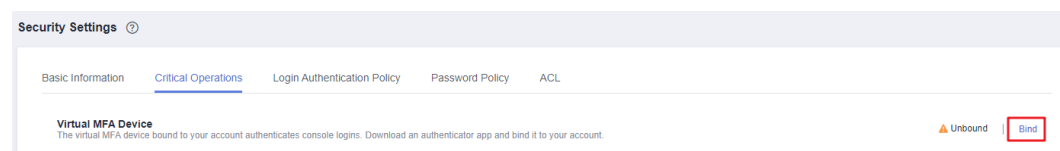
 **NOTE**

Before binding a virtual MFA device, ensure that you have installed an MFA application on your mobile device.

Step 1 Go to the [Security Settings](#) page.

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

Figure 3-75 Virtual MFA Device

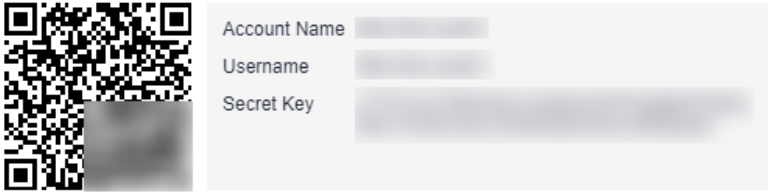


Step 3 Set up the MFA application by scanning the QR code or manually entering the secret key.

Figure 3-76 Binding a virtual MFA device

Bind Virtual MFA Device

1 **Step 1: Set up the authenticator app.**
Open the authenticator app on your mobile phone and scan the QR code or enter the secret key.



2 **Step 2: Enter the MFA verification codes.**
Enter two consecutive MFA verification codes generated on the app.

* Verification Code 1

* Verification Code 2

You can bind a virtual MFA device to your account by scanning the QR code or entering the secret key.

- Scanning the QR code
Open the MFA application on your mobile phone, and use the application to scan the QR code displayed on the **Bind Virtual MFA Device** page. Your account or IAM user is then added to the application.
- Manually entering the secret key
Open the MFA application on your mobile phone, and enter the secret key.

NOTE

Your account is manually added using the time-based algorithm. Ensure that automatic time setting has been enabled on your mobile phone.

Step 4 View the verification codes 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

Login Protection

After login protection is enabled, you and IAM users created using your account will need to enter a verification code in addition to the username and password during login. Enable this function for account security.

For the account, only the account administrator can enable login protection for it. For IAM users, both the account administrator and other administrators can enable this feature for the users.


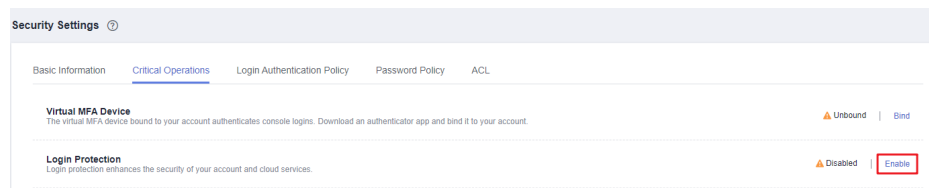
- (Administrator) Enabling login protection for an IAM user**
 To enable login protection for an IAM user, go to the **Users** page and choose **More > Security Settings** in the row that contains the IAM user. In the **Login Protection** area on the displayed **Security Settings** tab, click  next to **Verification Method**, and select a verification method from SMS, email, or virtual MFA device.
- Enabling login protection for your account**
 To enable login protection, click the **Critical Operations** tab on the **Security Settings** page, click **Enable** next to **Login Protection**, select a verification method, enter the verification codes, and click **OK**.

Figure 3-77 Enabling login protection



Operation Protection

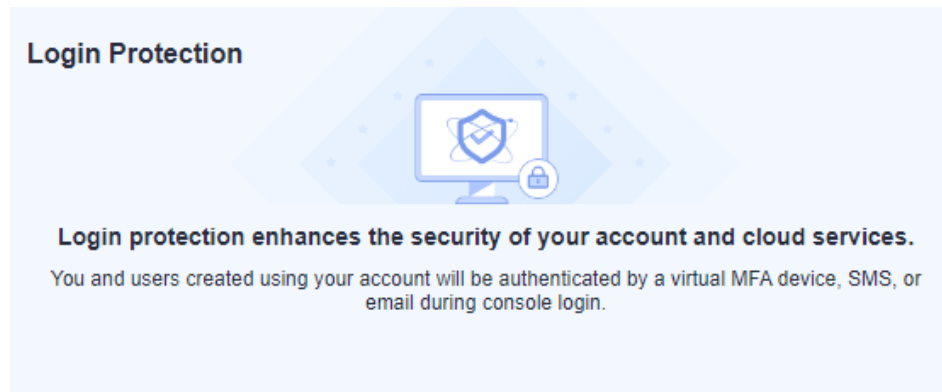
- Enabling operation protection**
 After operation protection is enabled, you and IAM users created using your account need to enter a verification code when performing a critical operation, such as deleting an ECS. This function is enabled by default. To ensure resource security, keep it enabled.
 The verification is valid for 15 minutes and you do not need to be verified again when performing critical operations within the validity period.

Step 1 Go to the **Security Settings** page.

Step 2 On the **Critical Operations** tab, locate the **Operation Protection** row and click **Enable**.

Step 3 Select **Enable**.

Figure 3-78 Configuring operation protection



Login Protection Enable
Identity verification will be required during login.

Disable
Identity verification will not be required during login.

Verification Method

Email address ()

Verification Code

Step 4 Click **OK**.

----End

- **Disabling operation protection**

If operation protection is disabled, you and IAM users created using your account do not need to enter a verification code when performing a critical operation.

Step 1 Go to the [Security Settings](#) page.

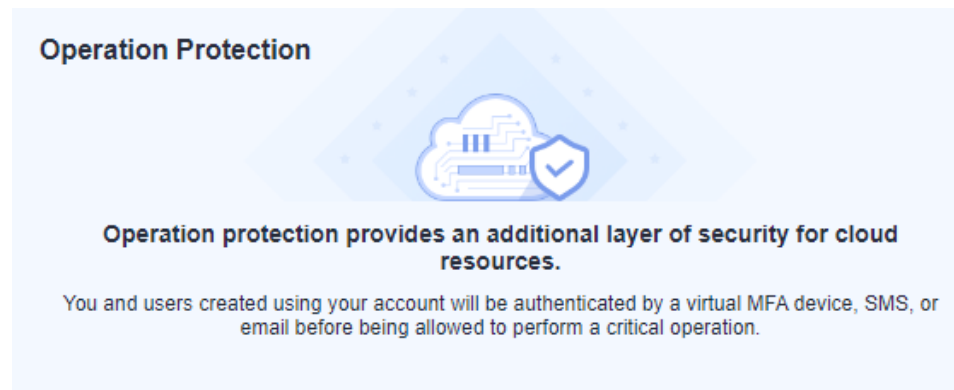
Step 2 On the **Critical Operations** tab, locate the **Operation Protection** row and click **Change**.

Figure 3-79 Disabling operation protection



Step 3 Select **Disable** and click **OK**.

Figure 3-80 Disabling operation protection



- Operation Protection
- Enable
You and users created using your account will need to perform identity verification by using the method you specify here.
 - Disable
Identity verification will not be required for performing a critical operation.

Step 4 Enter a verification code.

- **Self-verification:** The administrator who wants to disable operation protection completes the verification. SMS, email, and virtual MFA verification are supported.
- **Verification by another person:** The specified person completes the verification. Only SMS and email verification are supported.

Step 5 Click **OK**.

----End

NOTE

- Each cloud service defines its own critical operations.
- When IAM users created using your account perform a critical operation, they will be prompted to choose a verification method from email, SMS, and virtual MFA device.
 - If a user is only associated with a mobile number, only SMS verification is available.
 - If a user is only associated with an email address, only email verification is available.
 - If a user is not associated with an email address, mobile number, or virtual MFA device, the user will need to associate at least one of them before the user can perform any critical operations.
- You may not be able to receive email or SMS verification codes due to communication errors. In this case, you are advised to use a virtual MFA device for verification.
- If operation protection is enabled, IAM users need to enter verification codes when performing a critical operation. The verification codes are sent to the mobile number or email address bound to the IAM users.

Access Key Management

- **Enabling access key management**

After access key management is enabled, only the administrator can create, enable, disable, or delete access keys of IAM users. This function is disabled by default. To ensure resource security, enable this function.

To enable access key management, click the **Critical Operations** tab on the **Security Settings** page, and click in the **Access Key Management** row.

- **Disabling access key management**

After access key management is disabled, all IAM users can create, enable, disable, or delete their own access keys.

To enable access key management, click the **Critical Operations** tab on the **Security Settings** page, and click in the **Access Key Management** row.

Information Self-Management

- **Enabling information self-management**

By default, information self-management is enabled, indicating that all IAM users can manage their own **basic information** (login password, mobile number, and email address). Determine whether to allow IAM users to manage their own information and what information they can modify.

To enable information self-management, click the **Critical Operations** tab on the **Security Settings** page, and click **Enable** next to **Information Self-Management**. Select **Enable**, select the information types that IAM users can modify, and click **OK**.

- **Disabling information self-management**

After you disable information self-management, only administrators can manage their own **basic information**. If IAM users need to modify their login password, mobile number, or email address, they can contact the administrator. For details, see **3.2.4 Viewing or Modifying IAM User Information**.

To disable information self-management, click the **Critical Operations** tab on the **Security Settings** page, and click **Change** in the **Information Self-Management** row. In the displayed pane, select **Disable** and click **OK**.

Critical Operations

The following tables list the critical operations defined by each cloud service.

Table 3-16 Critical operations defined by cloud services

Service Type	Service	Critical Operation
Compute	Elastic Cloud Server (ECS)	<ul style="list-style-type: none"> • Stopping, restarting, or deleting an ECS • Resetting the password for logging in to an ECS • Detaching a disk • Unbinding an EIP

Service Type	Service	Critical Operation
	Bare Metal Server (BMS)	<ul style="list-style-type: none"> ● Stopping or restarting a BMS ● Resetting the BMS password ● Detaching a disk ● Unbinding an EIP
	Auto Scaling (AS)	Deleting an AS group
Storage	Object Storage Service (OBS)	<ul style="list-style-type: none"> ● Deleting a bucket ● Creating, editing, or deleting a bucket policy ● Configuring an object policy ● Creating, editing, or deleting a bucket ACL ● Configuring access logging ● Configuring URL validation ● Creating or editing a bucket inventory
	Elastic Volume Service (EVS)	Deleting an EVS disk
	Cloud Backup and Recovery (CBR)	<ul style="list-style-type: none"> ● Deleting a vault ● Deleting a backup ● Restoring a backup ● Deleting a policy ● Dissociating a resource ● Accepting a backup
Network	Domain Name Service (DNS)	<ul style="list-style-type: none"> ● Modifying, disabling, or deleting a record set
	Virtual Private Cloud (VPC)	<ul style="list-style-type: none"> ● Releasing or unbinding an EIP ● Deleting a shared bandwidth ● Batch releasing or unbinding EIPs

Service Type	Service	Critical Operation
	Elastic Load Balance (ELB)	<ul style="list-style-type: none"> ● Classic load balancers <ul style="list-style-type: none"> - Deleting a load balancer - Deleting a listener - Deleting a certificate - Disabling a load balancer ● Shared load balancers <ul style="list-style-type: none"> - Deleting a load balancer - Deleting a listener - Deleting a certificate - Removing a backend server - Unbinding an EIP - Unbind a public or private IPv4 address - Unbinding an IPv6 address - Removing from IPv6 shared bandwidth
	Elastic IP (EIP)	<ul style="list-style-type: none"> ● Deleting a shared bandwidth ● Releasing or unbinding an EIP ● Releasing or unbinding EIPs
Management & Deployment	Identity and Access Management (IAM)	<ul style="list-style-type: none"> ● Disabling operation protection ● Disabling login protection ● Changing the mobile number ● Changing the email address ● Changing the login password ● Changing the login authentication method ● Deleting an IAM user ● Disabling an IAM user ● Deleting an agency ● Deleting a user group ● Deleting a policy ● Deleting permissions ● Creating an access key ● Deleting an access key ● Disabling an access key ● Deleting the project ● Modifying the status of access key management

Service Type	Service	Critical Operation
Application	Distributed Cache Service (DCS)	<ul style="list-style-type: none"> Resetting the password of a DCS instance Deleting a DCS instance Clearing DCS instance data
Database	RDS for MySQL	<ul style="list-style-type: none"> Resetting the administrator password Deleting a DB instance Deleting a database backup Switching between primary and standby DB instances Changing the database port Deleting a database account Deleting a database Unbinding an EIP Downloading a full backup
Databases	Document Database Service (DDS)	<ul style="list-style-type: none"> Resetting the password Restarting or deleting a DB instance Restarting a node Switching the primary and secondary nodes of a replica set Deleting a security group rule Enabling IP addresses of shard and config nodes Restoring the current DB instance from a backup Restoring an existing DB instance from a backup

3.7.4 Login Authentication Policy

The **Login Authentication Policy** tab of the **Security Settings** page provides the **Session Timeout**, **Account Lockout**, **Account Disabling**, **Recent Login Information**, and **Custom Information** settings. These settings take effect for both your account and the IAM users created using the account.

Only the **administrator** can configure the login authentication policy, and IAM users can only view the configurations. If an IAM user needs to modify the configurations, the user can request the administrator to perform the modification or grant the required permissions.

Session Timeout

Set the session timeout that will apply if you or users created using your account do not perform any operations within a specific period.

Figure 3-81 Session Timeout

Session Timeout

Log out if no operations are performed within .

The timeout ranges from 15 minutes to 24 hours, and the default timeout is 1 hour.

Account Lockout

Set a duration to lock users out if a specific number of unsuccessful login attempts has been reached within a certain period. You cannot unlock your own account or an IAM user's account. Wait until the lock time expires.

Figure 3-82 Account Lockout

Account Lockout Takes effect for both you and IAM users created using your account

Lock the account for minutes if login attempts fail within minutes.

The administrator can set the time for resetting the account lockout counter, maximum number of unsuccessful login attempts, and account lockout duration.

- Time for resetting the account lockout counter: The value ranges from 15 to 60 minutes, and the default value is **15 minutes**.
- Maximum number of unsuccessful login attempts: The value ranges from 3 to 10, and the default value is **5**.
- Lockout duration: The value ranges from 15 to 30 minutes, and the default value is **15 minutes**.

Account Disabling

Set a validity period to disable IAM users if they have not accessed the cloud platform using the console or APIs within a certain period.

This option is disabled by default. The validity period ranges from 1 to 240 days.

If you enable this option, the setting will take effect only for IAM users created using your account. If an IAM user is disabled, the user can request the administrator to enable their account again.

Recent Login Information

Configure whether you want the system to display the previous login information after you log in. If incorrect login information is displayed on the **Login Verification** page, change your password immediately.

This option is disabled by default and can be enabled by the administrator.

Custom Information

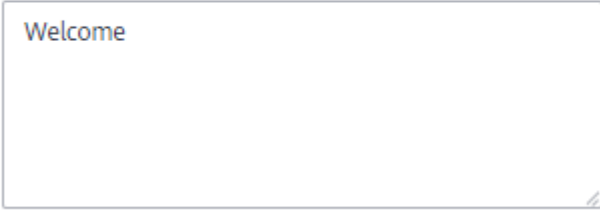
Set custom information that will be displayed upon successful login. For example, enter the word **Welcome**.

No information is displayed by default, and the administrator can set custom information that will be displayed.

Figure 3-83 Custom Information

Custom Information

Display custom information upon login.



A screenshot of a web interface showing a text input field. The field is rectangular with a thin border and contains the word "Welcome" in a light blue font. Below the field, the text "7/60" is visible, likely indicating a character count or a page number.

You and all the IAM users created using your account will see the same information upon successful login.

3.7.5 Password Policy

The **Password Policy** tab of the **Security Settings** page provides the **Password Composition & Reuse**, **Password Expiration**, and **Minimum Password Age** settings.

Only the **administrator** can configure the password policy, and IAM users can only view the configurations. If an IAM user needs to modify the configurations, the user can request the administrator to perform the modification or grant the required permissions.

You can configure the password policy to ensure that IAM users create strong passwords and rotate them periodically. In the password policy, you can define password requirements, such as minimum password length, whether to allow consecutive identical characters in a password, and whether to allow previously used passwords.

Password Composition & Reuse

Figure 3-84 Password Composition & Reuse

Password Composition & Reuse

Must contain at least of the following character types: uppercase letters, lowercase letters, digits and special characters.

Minimum Number of Characters

Restrict consecutive identical characters

Max. Number of Consecutive Identical Characters

Disallow previously used passwords

Number of Recent Passwords Disallowed

- Ensure that the password contains 2 to 4 of the following character types: uppercase letters, lowercase letters, digits, and special characters. By default, the password must contain at least 2 of these character types.
- Set the minimum number of characters that a password must contain. The default value is 6 and the value range is from 6 to 32.
- (Optional) Enable the **Restrict consecutive identical characters** option and set the maximum number of times that a character is allowed to be consecutively present in a password. For example, value **1** indicates that consecutive identical characters are not allowed in a password.
- (Optional) Enable the **Disallow previously used passwords** option and set the number of previously used passwords that are not allowed. For example, value **3** indicates that the user cannot set the last three passwords that the user has previously used when setting a new password.

Changes to the password policy take effect the next time you or your IAM users change passwords. IAM users created later will also adhere to the updated password policy.

Password Expiration

Set a validity period for passwords so that users need to change their passwords periodically. The users will be prompted to change their passwords 15 days before password expiration. Expired passwords cannot be used to log in to the cloud platform.

This option is disabled by default. The validity period ranges from 1 to 180 days.

The changes will take effect immediately for your account and all IAM users under your account.

NOTE

After the password expires, users need to set a new password through the URL sent by email. The new password must be different from the old password.

Minimum Password Age

To prevent password loss due to frequent password changes, you can set a minimum period after which users are allowed to make a password change.

This option is disabled by default. If you enable this option, you can set a period from 0 to 1440 minutes.

The changes will take effect immediately for your account and all IAM users under your account.

3.7.6 ACL

The **ACL** tab of the **Security Settings** page provides the **IP Address Ranges**, **IPv4 CIDR Blocks**, and **VPC Endpoints** settings for allowing user access only from specified IP address ranges, IPv4 CIDR blocks, or VPC endpoints.

Only the **administrator** can configure the ACL. If an IAM user needs to configure the ACL, the user can request the administrator to perform the configuration or grant the required permissions.

Access type:

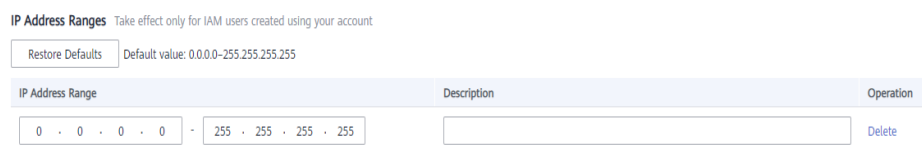
- **Console Access** (recommended): The ACL takes effect only for IAM users who are created using your account and have access to the console.
- **API Access**: The ACL controls users' API access through API Gateway and takes effect only for IAM users two hours after you complete the configuration.

NOTE

- You can configure a maximum of 200 access control items.

IP Address Ranges

Figure 3-85 IP Address Ranges



Specify IP address ranges from 0.0.0.0 to 255.255.255.255 to allow access to the cloud platform. The default value is **0.0.0.0–255.255.255.255**. If this parameter is left blank or the default value is used, your IAM users can access the management console from anywhere.

IPv4 CIDR Blocks

Specify IPv4 CIDR blocks to allow access to the cloud platform. For example, set **IPv4 CIDR block** to **10.10.10.10/32**.

VPC Endpoints

Specify VPC endpoints, such as **Occad098-b8f4-495a-9b10-613e2a5exxxx**, to allow API-based access to the cloud platform. If access control is not configured, you can access APIs from all VPC endpoints by default.

 **NOTE**

- User access is allowed if any of **IP Address Ranges**, **IPv4 CIDR Blocks**, and **VPC Endpoints** is met.
- To restore **IP Address Ranges** to the default settings (0.0.0.0–255.255.255.255) and clear the settings in **IPv4 CIDR Blocks** and **VPC Endpoints**, click **Restore Defaults**.

3.8 Identity Providers

3.8.1 Introduction

The cloud platform provides identity federation based on Security Assertion Markup Language (SAML) or OpenID Connect. This function allows users in your enterprise management system to access the cloud platform through single sign-on (SSO).

IAM supports two types of identity federation:

- **Web SSO:** Browsers are used as the communication media. This authentication type enables common users to access the cloud platform using browsers.
- **API calling:** Development tools (such as OpenStack Client and ShibbolethECP Client) are used as the communication media. This authentication type enables enterprise users and common users to access the cloud platform by calling APIs.

Basic Concepts

Table 3-17 Basic concepts

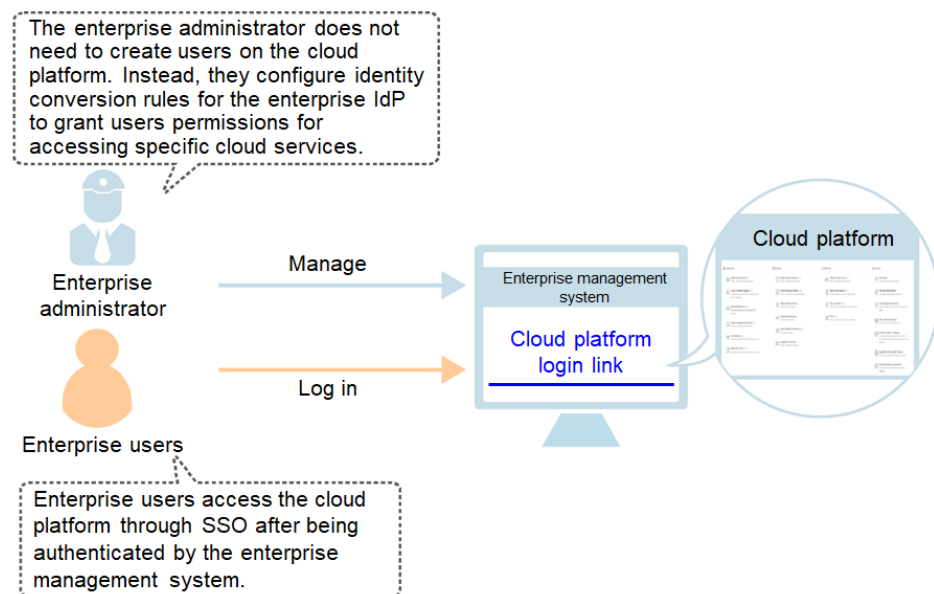
Concept	Description
Identity provider (IdP)	An IdP collects and stores user identity information, such as usernames and passwords, and authenticates users during login. For identity federation between an enterprise and the cloud platform, the identity authentication system of the enterprise is an identity provider and is also called "enterprise IdP". Popular third-party IdPs include Microsoft Active Directory Federation Services (AD FS) and Shibboleth.
Service Provider (SP)	A service provider establishes a trust relationship with an IdP and provides services based on the user information provided by the IdP. For identity federation between an enterprise and the cloud platform, the cloud platform is a service provider.

Concept	Description
Identity federation	Identity federation is the process of establishing a trust relationship between an IdP and SP to implement SSO.
Single sign-on (SSO)	SSO allows users to access a trusted SP after logging in to the enterprise IdP. For example, after a trust relationship is established between an enterprise management system and the cloud platform, users in the enterprise management system can use their existing accounts and passwords to access the cloud platform through the login link in the enterprise management system.
SAML 2.0	SAML 2.0 is an XML-based protocol that uses securityTokens containing assertions to pass information about an end user between an IdP and an SP. It is an open standard ratified by the Organization for the Advancement of Structured Information Standards (OASIS) and is being used by many IdPs. For more information about this standard, see SAML 2.0 Technical Overview . The cloud platform implements identity federation in compliance with SAML 2.0. To successfully federate users to the cloud platform, ensure that your enterprise IdP is compatible with this protocol.
OpenID Connect	OpenID Connect is a simple identity layer on top of the Open Authorization 2.0 (OAuth 2.0) protocol. IAM implements identity federation in compliance with OpenID Connect 1.0. To successfully federate users to the cloud platform, ensure that your enterprise IdP is compatible with this protocol.
OAuth 2.0	OAuth 2.0 is an open authorization protocol. The authorization framework of this protocol allows third-party applications to obtain access permissions.

Advantages of Identity Federation

- Easy identity management
As an administrator, you only need to create accounts for your employees in your enterprise management system. The employees can use their own accounts to access both the enterprise management system and the cloud platform.
- Simplified operations
Employees can log in to the cloud platform from the enterprise management system.

Figure 3-86 Advantages of identity federation



Precautions

- Ensure that your enterprise IdP server and the cloud platform use Greenwich Mean Time (GMT) time in the same time zone.
- The identity information (such as email address or mobile number) of federated users is stored in the enterprise IdP. Federated users are mapped to the cloud platform as virtual identities, so their access to the cloud platform has the following restrictions:
 - Federated users do not need to perform a 2-step verification when performing critical operations even though **critical operation protection** (login protection or operation protection) is enabled.
 - Federated users cannot create access keys with unlimited validity, but they can obtain temporary access credentials (access keys and securityTokens) using user or agency tokens.

If a federated user needs an access key with unlimited validity, they can contact the account administrator or an IAM user to create one. An access key contains the permissions granted to a user, so it is recommended that the federated user request an IAM user in the same group to create an access key.

3.8.2 Identity Federation via SAML

3.8.2.1 Configuration of SAML-based Federated Identity Authentication

This section describes the process and configuration of SAML-based federated identity authentication between an enterprise IdP and the cloud platform.

CAUTION

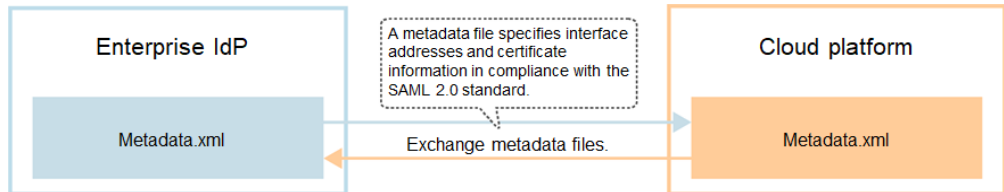
Ensure that your enterprise IdP supports SAML 2.0.

Configuring Federated Identity Authentication

To implement federated identity authentication between an enterprise management system and the cloud platform, complete the following configuration:

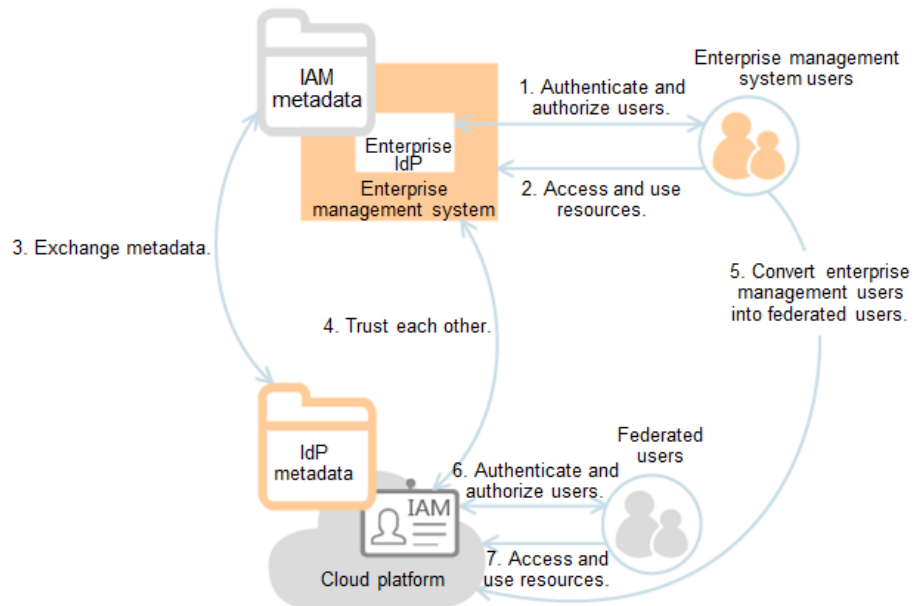
1. **Establish a trust relationship and create an identity provider:** Exchange the metadata files of the enterprise IdP and the cloud platform.

Figure 3-87 Metadata file exchange model



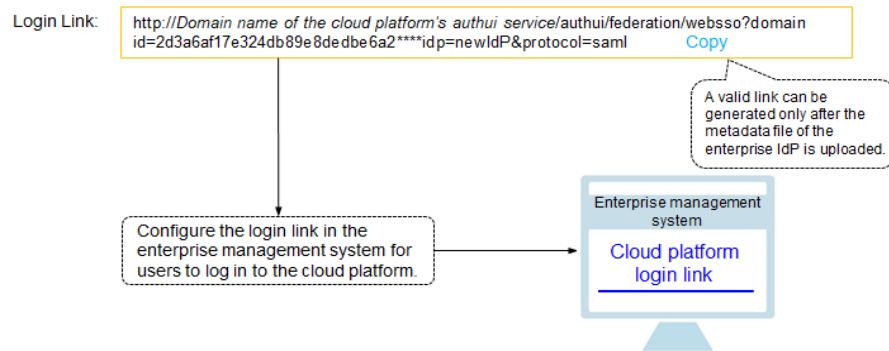
2. **Configure identity conversion rules:** Map the users, user groups, and permissions in the enterprise IdP to the cloud platform (see Figure 3-88).

Figure 3-88 User identity conversion model



3. **Configure a login link:** Configure a login link in the enterprise management system to allow users to access the cloud platform through SSO.

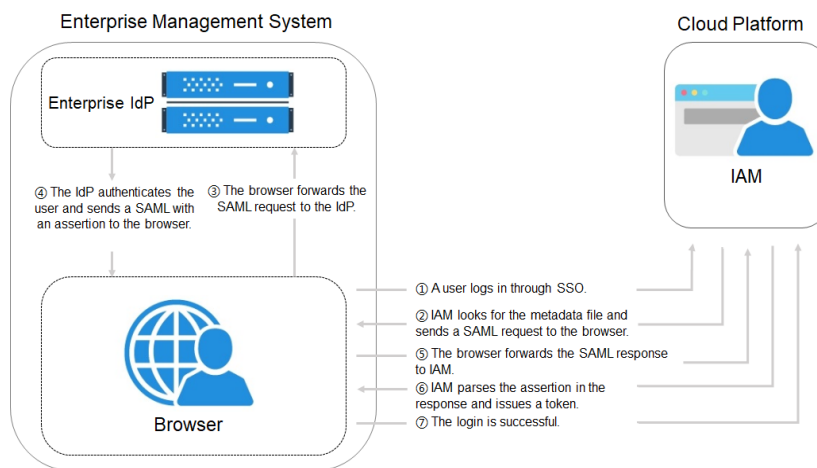
Figure 3-89 SSO login model



Process of Federated Identity Authentication

Figure 3-90 shows the interaction between an enterprise management system and the cloud platform after a user initiates an SSO request.

Figure 3-90 Process of federated identity authentication



NOTE

To view interactive requests and assertions with a better experience, you are advised to use Google Chrome and install the SAML Message Decoder plug-in.

The process of federated identity authentication is as follows:

1. A user uses a browser to visit the login link of the identity provider, and the browser sends an SSO request to the cloud platform.
2. The cloud platform searches for a metadata file based on the login link, and sends a SAML request to the browser.
3. The browser forwards the SAML request to the enterprise IdP.
4. The user enters their username and password on the login page displayed in the enterprise IdP. After the enterprise IdP authenticates the user's identity, it constructs a SAML assertion containing the user information, and sends the assertion to the browser as a SAML response.
5. The browser responds and forwards the SAML response to the cloud platform.

6. The cloud platform parses the assertion in the SAML response, and issues a token to the user after identifying the group to which the user is mapped, according to the configured identity conversion rules.
7. If the login is successful, the user accesses the cloud platform successfully.

 **NOTE**

The assertion must carry a signature; otherwise, the login will fail.

3.8.2.2 Step 1: Create an IdP Entity

To establish a trust relationship between an enterprise IdP and the cloud platform, upload the metadata file of the cloud platform to the enterprise IdP, and then create an IdP entity and upload the metadata file of the IdP on the IAM console.

Prerequisites

- The enterprise administrator has created an account in the cloud platform, and has created user groups and assigned permissions to the group in IAM. For details, see [3.3.1 Creating a User Group and Assigning Permissions](#). The user groups created in IAM will be mapped to federated users so that the federated users can obtain the permissions of the user groups to use cloud resources.
- The enterprise administrator has read the help documentation of the enterprise IdP or has understood how to use the enterprise IdP. Configurations of different enterprise IdPs differ greatly, so they are not described in this document. For details about how to obtain the enterprise IdP's metadata file and how to upload the cloud platform's metadata to the enterprise IdP, see the IdP documentation.

Establishing a Trust Relationship Between the Enterprise IdP and the Cloud Platform

The metadata file of the cloud platform needs to be configured in the enterprise IdP to establish a trust relationship between the two systems.

Step 1 Download the metadata file of the cloud platform.

- Web SSO: Visit <https://Domain name of the authui service on the cloud platform/authui/saml/metadata.xml>, right-click on the page, choose **Save As**, and set a file name, for example, **websso-metadata.xml**.
- SSO via API calling: Visit <https://Endpoint address of a region/v3-ext/auth/OS-FEDERATION/SSO/metadata>, right-click on the page, choose **Save As**, and set a file name, for example, **api-metadata-region.xml**.

The cloud platform provides different API gateways for users in different regions to call APIs. To allow users to access resources in multiple regions, download metadata files of all these regions.

Step 2 Upload the metadata file to the enterprise IdP server. For details, see the help documentation of the enterprise IdP.

Step 3 Obtain the metadata file of the enterprise IdP. For details, see the help documentation of the enterprise IdP.

----End

Creating an IdP Entity on the Cloud Platform

Create an Idp entity and configure the metadata file in IAM.

Step 1 Log in to the IAM console, choose **Identity Providers** from the navigation pane, and click **Create Identity Provider** in the upper right corner.

Step 2 Specify the name, protocol, SSO type, status, and description of the IdP entity.

Table 3-18 Basic parameters of an IdP

Parameter	Description
Name	IdP name, which must be unique globally. You are advised to use the domain name.
Protocol	IdP protocol. The system supports SAML and OpenID Connect IdPs. For details about how to configure OpenID Connect-based identity federation, see 3.8.3 Identity Federation Via OpenID Connect .
SSO Type	IdP type. An account can have only one type of IdP. <ul style="list-style-type: none"> Virtual user: After a user logs in to the cloud platform as a federated user, the system automatically creates a virtual identity for the user. An account can have multiple IdPs of the virtual user type. IAM user: After a user logs in to the cloud platform as a federated user, the system automatically maps the external identity ID to an IAM user so that the federated user has the permissions of the mapped IAM user. An account can have only one IdP of the IAM user type. If you select the IAM user SSO, ensure that you have created an IAM user and set the external identity ID. For details, see 3.2.1 Creating an IAM User.
Status	IdP status. The default value is Enabled .

 **NOTE**

The IdP name must be unique under your account. You are advised to use the domain name.

Step 3 Click **OK**.

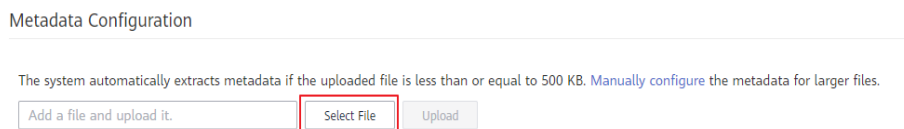
----End

Configuring the Metadata File of the IdP

To configure the metadata file of the enterprise IdP obtained in [Step 3](#) on the cloud platform, you can upload the metadata file or manually edit metadata on the IAM console. For a metadata file larger than 500 KB, manually configure the metadata. If the metadata has been changed, upload the latest metadata file or edit the existing metadata to ensure that the federated users can log in to the cloud platform successfully.

- **Upload a metadata file.**
 - a. Click **Modify** in the row containing the IdP.
 - b. Click **Select File** and select the metadata file of the enterprise IdP.

Figure 3-91 Uploading a metadata file



- c. Click **Upload**. The metadata extracted from the uploaded file is displayed. Click **OK**.
 - If the uploaded metadata file contains multiple IdPs, select the IdP you want to use from the **Entity ID** drop-down list.
 - If a message is displayed indicating that no entity ID is specified or the signing certificate has expired, check the metadata file and upload it again, or configure the metadata manually.
 - d. Click **OK**.
- **Manually configure metadata.**
 - a. Click **Manually configure**.
 - b. In the **Configure Metadata** dialog box, set the metadata parameters, such as **Entity ID**, **Signing Certificate**, and **SingleSignOnService**.

Parameter	Man dato ry	Description
Entity ID	Yes	The unique identifier of an IdP. Enter the value of entityID displayed in the enterprise IdP's metadata file. If the metadata file contains multiple IdPs, choose the one you want to use.
Protocol	Yes	The SAML protocol is used for identity federation between an enterprise IdP and SP.
NameIdFormat	No	Enter the value of NameIdFormat displayed in the IdP metadata file. It specifies the username identifier format supported by the IdP, which is used for communication between the IdP and federated user.

Parameter	Man datory	Description
Signing Certificate	Yes	Enter the value of <X509Certificate> displayed in the IdP metadata file. A signing certificate is a public key certificate used for signature verification. For security purposes, enter a public key containing at least 2,048 bits. The signing certificate is used during identity federation to ensure that assertions are credible and complete.
SingleSignOnService	Yes	Enter the value of SingleSignOnService displayed in the IdP metadata file. This parameter defines how SAML requests are sent during SSO. It must support HTTP Redirect or HTTP POST.
SingleLogoutService	No	Enter the value of SingleLogoutService displayed in the IdP metadata file. This parameter indicates the address to which federated users will be redirected after logging out their sessions. It must support HTTP Redirect or HTTP POST.

The following example shows the metadata file of an enterprise IdP and the manually configured metadata.

Figure 3-92 Metadata file of an enterprise IdP

```
<EntityDescriptor xmlns="urn:oasis:names:tg:metadata">
  <IDPSSODescriptor protocolSupportAliases="urn:oasis:names:tg:SAML:2.0:protocol">
    <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
      <X509Data>
        <X509Certificate>MIIDBTCCBgkrBq1D18Fq8t8q969A00Cg5q5I3DQ8CwKACBxIAAgpVAPTTphoY4KeeK7yJaw55b3d3d8E3j3c2vWb0RtU1v7Tt12M8F3A4nb0R41wT1d188F93A4G4AM8Hd0VQVQ0x5I
        </X509Data>
      </KeyInfo>
    </IDPSSODescriptor>
  </EntityDescriptor>
  <SingleLogoutService Binding="urn:oasis:names:tg:SAML:2.0:bindings" Location="https://chaanyao01.com/saml/urn:oasis:names:tg:SAML:2.0:assertion" />
  <SingleSignOnService Binding="urn:oasis:names:tg:SAML:2.0:bindings" Location="https://chaanyao01.com/saml/urn:oasis:names:tg:SAML:2.0:assertion" />
  <NameIDFormat urn:oasis:names:tg:SAML:2.0:nameid-format:emailAddress />
  <NameIDFormat urn:oasis:names:tg:SAML:2.0:nameid-format:ipersistent />
  <NameIDFormat urn:oasis:names:tg:SAML:2.0:nameid-format:transient />
  <SingleLogoutService Binding="urn:oasis:names:tg:SAML:2.0:bindings HTTP-Redirect" Location="https://chaanyao01.com/saml/urn:oasis:names:tg:SAML:2.0:assertion" />
  <SingleSignOnService Binding="urn:oasis:names:tg:SAML:2.0:bindings HTTP-POST" Location="https://chaanyao01.com/saml/urn:oasis:names:tg:SAML:2.0:assertion" />
  <Attribute Name="https://schemas.xmlsoap.org/2003/09/identity/claims/Name" NameFormat="urn:oasis:names:tg:SAML:2.0:attribute-format:uri" FriendlyName="Name" xmlns="urn:oasis:names:tg:SAML:2.0:assertion"/>
  <Attribute Name="https://schemas.xmlsoap.org/2003/09/identity/claims/Name" NameFormat="urn:oasis:names:tg:SAML:2.0:attribute-format:uri" FriendlyName="Name" xmlns="urn:oasis:names:tg:SAML:2.0:assertion"/>
  <Attribute Name="https://schemas.xmlsoap.org/2003/09/identity/claims/Name" NameFormat="urn:oasis:names:tg:SAML:2.0:attribute-format:uri" FriendlyName="Name" xmlns="urn:oasis:names:tg:SAML:2.0:assertion"/>
  <Attribute Name="https://schemas.xmlsoap.org/2003/09/identity/claims/Name" NameFormat="urn:oasis:names:tg:SAML:2.0:attribute-format:uri" FriendlyName="Name" xmlns="urn:oasis:names:tg:SAML:2.0:assertion"/>
  </IDPSSODescriptor>
</EntityDescriptor>
```

- c. Click **OK**.
- Click **OK** to save the settings.

Verifying the Federated Login

Step 1 Click the login link displayed on the IdP details page and check if the login page of the enterprise IdP server is displayed.

1. On the **Identity Providers** page, click **View** in the **Operation** column of the identity provider. Copy the login link displayed on the identity provider details page and visit the link using a browser.

2. If the login page is not displayed, check the metadata file and configurations of the enterprise IdP server.

Step 2 Enter the username and password of a user that was created in the enterprise management system.

- If the login is successful, add the login link to the enterprise's website.
- If the login fails, check the username and password.

 **NOTE**

Federated users can only access the cloud platform by default. To assign permissions to federated users, configure identity conversion rules. For more information, see [3.8.2.3 Step 2: Configure Identity Conversion Rules](#).

----End

Related Operations

- Viewing IdP information: In the IdP list, click **View** in the row containing the IdP, and view its basic information, metadata, and identity conversion rules.

 **NOTE**

To modify the configuration of an IdP, click **Modify** at the bottom of the details page.

- Modifying an IdP: In the IdP list, click **Modify** in the row containing the IdP, and then change its status or modify the description, metadata, or identity conversion rules.
- Deleting an IdP: In the IdP list, click **Delete** in the row containing the IdP, and click **Yes** in the displayed dialog box.

Follow-Up Procedure

- In the **Identity Conversion Rules** area, configure identity conversion rules to map enterprise IdP users to IAM user groups and assign permissions to the users. For details, see [3.8.2.3 Step 2: Configure Identity Conversion Rules](#).
- Configure the enterprise management system to allow users to access the cloud platform through SSO. For details, see [3.8.2.4 \(Optional\) Step 3: Configure a Federated Login Entry in the Enterprise IdP](#).

3.8.2.3 Step 2: Configure Identity Conversion Rules

Federated users are named **FederationUser** by default on the cloud platform. These users can only access the cloud platform and they do not have any other permissions. You can configure identity conversion rules on the IAM console to achieve the following:

- Display enterprise users with different names on the cloud platform.
- Grant enterprise users permissions to use cloud resources by mapping these users to IAM user groups. Ensure that you have created the required user groups. For details, see [3.3.1 Creating a User Group and Assigning Permissions](#).

 **NOTE**

- Modifications to identity conversion rules will take effect only after the federated users log in again.
- To modify the permissions of a user, modify the permissions of the user group to which the user belongs. Then restart the enterprise IdP for the modifications to take effect.

Prerequisites

An IdP entity has been created, and the login link of the IdP is accessible. (For details about how to create and verify an IdP entity, see [3.8.2.2 Step 1: Create an IdP Entity](#).)

Procedure

If you configure identity conversion rules by clicking **Create Rule**, IAM converts the rule parameters to the JSON format. Alternatively, you can click **Edit Rule** to configure rules in JSON format. For details, see [3.8.4 Syntax of Identity Conversion Rules](#).

- **Creating Rules**
 - Choose **Identity Providers** from the navigation pane.
 - In the IdP list, click **Modify** in the row containing the IdP.
 - In the **Identity Conversion Rules** area, click **Create Rule**. Then, configure the rules in the **Create Rule** dialog box.

Table 3-19 Parameter description

Parameter	Description	Remarks
Username	Username of federated users to be displayed on the cloud platform.	<p>To distinguish federated users from users of the cloud platform, it is recommended that you set the username to "FederationUser-IdP_XXX". <i>IdP</i> indicates an IdP name, for example, AD FS or Shibboleth. <i>XXX</i> indicates a custom name.</p> <p>NOTICE</p> <ul style="list-style-type: none"> • The username of each federated user must be unique in the same IdP. Identical federated user names under the same identity provider will be identified as the same IAM user on the cloud platform. • The username can only contain letters, digits, spaces, hyphens (-), underscores (_), and periods (.). It cannot start with a digit and cannot contain the following special characters: ", \", \\, \n, \r

Parameter	Description	Remarks
User Groups	User groups to which the federated users will belong on the cloud platform.	The federated users will inherit permissions from their user groups. NOTE The user group name can only contain letters, digits, spaces, hyphens (-), underscores (_), and periods (.). It cannot start with a digit and cannot contain the following special characters: ", \", \\, \n, \r
Rule Conditions	Conditions that a federated user must meet to obtain permissions from the selected user groups.	Federated users who do not meet these conditions cannot access the cloud platform. You can create a maximum of 10 conditions for an identity conversion rule. The Attribute and Value parameters are used for the enterprise IdP to transfer user information to the cloud platform through SAML assertions. The Condition parameter can be set to empty , any_one_of , or not_any_of . For details about these parameters, see Syntax of Identity Conversion Rules . NOTE <ul style="list-style-type: none"> An identity conversion rule can have multiple conditions. It takes effect only if all of the conditions are met. An IdP can have multiple identity conversion rules. If a federated user does not meet any of the rules, the user will not be allowed to access the cloud platform.

For example, set an identity conversion rule for administrators in the enterprise management system.

- Username: **FederationUser-IdP_admin**
 - User group: **admin**
 - Rule condition: **_NAMEID_** (attribute), **any_one_of** (condition), and **000000001** (value).
Only the user with ID 000000001 is mapped to IAM user **FederationUser-IdP_admin** and inherits permissions from the **admin** user group.
- d. In the **Create Rule** dialog box, click **OK**.
 - e. On the **Modify Identity Provider** page, click **OK**.
- **Editing Rules**
 - a. Log in to the cloud platform as an administrator, and go to the IAM console. Then, choose **Identity Providers** from the navigation pane.

- b. In the IdP list, click **Modify** in the row containing the IdP.
- c. In the **Identity Conversion Rules** area, click **Edit Rule**.
- d. Edit the identity conversion rules in JSON format. For details, see [3.8.4 Syntax of Identity Conversion Rules](#).
- e. Click **Validate** to verify the syntax of the rules.
- f. If the rule is correct, click **OK** in the **Edit Rule** dialog box, and click **OK** on the **Modify Identity Provider** page.
If a message indicating that the JSON file is incomplete is displayed, modify the statements or click **Cancel** to cancel the modifications.

Verifying Federated User Permissions

After configuring identity conversion rules, verify the permissions of federated users.

Step 1 Log in as a federated user.

On the **Identity Providers** page of the IAM console, click **View** in the row containing the IdP. Copy the login link displayed on the IdP details page, open the link using a browser, and then enter the username and password used in the enterprise management system.

Step 2 Check that the federated user has the permissions assigned to their user group.

For example, configure an identity conversion rule to map federated user **ID1** to the **admin** user group so that **ID1** will have full permissions for all cloud services. On the management console, select a cloud service, and check if you can access the service.

----End

Related Operations

Viewing identity conversion rules: Click **View Rule** on the **Modify Identity Provider** page. The identity conversion rules are displayed in JSON format. For details about the JSON format, see [Syntax of Identity Conversion Rules](#).

3.8.2.4 (Optional) Step 3: Configure a Federated Login Entry in the Enterprise IdP

Configure the login link of the IdP in the enterprise management system so that enterprise users can use this link to access the cloud platform.

Prerequisites

- An IdP entity has been created, and the login link of the identity provider is accessible. (For details about how to create and verify an IdP entity, see [3.8.2.2 Step 1: Create an IdP Entity](#).)
- The login link of the identity provider has already been configured in the enterprise management system for logging in to the cloud platform.

Procedure

Step 1 Log in to the IAM console, and choose **Identity Providers** from the navigation pane.

Step 2 Click **View** in the row containing the IdP.

Step 3 Copy the login link.

Step 4 Add the following statement to the page file of the enterprise management system:

```
<a href="<Login link>"> Login entry </a>
```

Step 5 Log in to the enterprise management system using your enterprise account, and then click the configured login link to access the cloud platform.

----End

3.8.3 Identity Federation Via OpenID Connect

3.8.3.1 Configuration of OpenID Connect–based Federated Identity Authentication

This section describes the process and configuration of OpenID Connect–based federated identity authentication between an enterprise IdP and the cloud platform.

Configuring Federated Identity Authentication

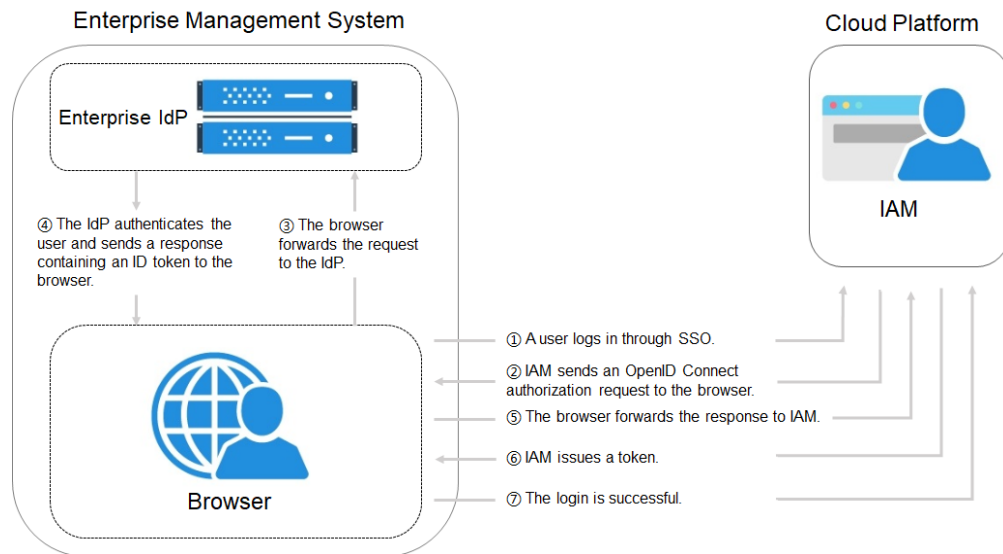
To implement federated identity authentication between an enterprise management system and the cloud platform, complete the following configuration:

1. **Establish a trust relationship and create an identity provider:** Create OAuth 2.0 credentials in the enterprise IdP, and create an identity provider on the cloud platform.
2. **Configure identity conversion rules:** Map the users, user groups, and their permissions in the enterprise IdP to the cloud platform.
3. **Configure a login link:** Configure a login link in the enterprise management system to allow users to access the cloud platform through SSO.

Process of Federated Identity Authentication

Figure 3-93 shows the interaction between an enterprise management system and the cloud platform after a user initiates an SSO request.

Figure 3-93 Process of federated identity authentication



The process of federated identity authentication is as follows:

1. A user uses a browser to open the login link obtained from IAM, and then the browser sends an SSO request to the cloud platform.
2. The cloud platform searches for identity provider configurations based on the login link, and sends an OpenID Connect authorization request to the browser.
3. The browser forwards the authorization request to the enterprise IdP.
4. The user enters their username and password on the login page displayed in the enterprise IdP. After the enterprise IdP authenticates the user's identity, it constructs an ID token containing the user information, and sends the ID token to the browser as an OpenID Connect authorization response.
5. The browser responds and forwards the authorization response to the cloud platform.
6. The cloud platform parses the ID token in the authorization response, and issues a token to the user after identifying the group to which the user is mapped, according to the configured identity conversion rules.
7. If the login is successful, the user accesses the cloud platform successfully.

3.8.3.2 Step 1: Create an IdP Entity

To establish a trust relationship between an enterprise IdP and the cloud platform, create an IdP entity and configure authorization information on the IAM console, and set the user redirect URLs and create OAuth 2.0 credentials in the enterprise IdP.

Prerequisites

- The enterprise administrator has created an account in the cloud platform, and has created user groups and assigned permissions to the group in IAM. For details, see [3.3.1 Creating a User Group and Assigning Permissions](#). The user groups created in IAM will be mapped to federated users so that the

federated users can obtain the permissions of the user groups to use cloud resources.

- The enterprise administrator has read the help documentation of the enterprise IdP or has understood how to use the enterprise IdP. Configurations of different enterprise IdPs differ greatly, so they are not described in this document. For details about how to obtain an enterprise IdP's OAuth 2.0 credentials, see the IdP help documentation.

Creating OAuth 2.0 Credentials in the Enterprise IdP

Step 1 Set redirect URLs in the enterprise IdP so that users can be redirected to the OpenID Connect IdP on the cloud platform.

Step 2 Obtain OAuth 2.0 credentials of the enterprise IdP.

NOTE

The configurations vary depending on the enterprise IdP. For details about the required configurations, see the documentation of the enterprise IdP.

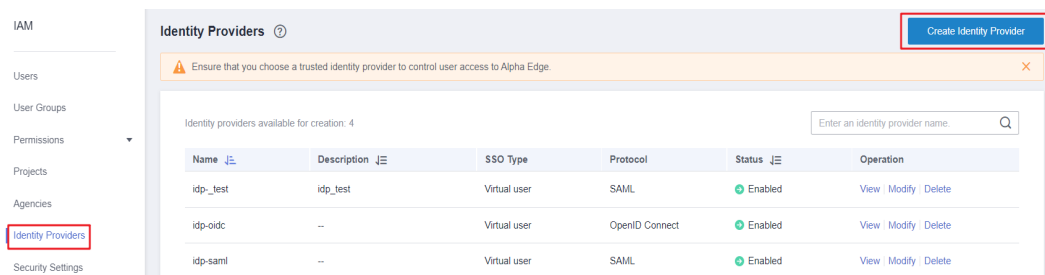
----End

Creating an IdP Entity on the Cloud Platform

Create an IdP entity and configure authorization information in IAM.

Step 1 Log in to the IAM console, choose **Identity Providers** from the navigation pane, and click **Create Identity Provider** in the upper right corner.

Figure 3-94 Creating an IdP entity



Step 2 Enter an IdP name, select **OpenID Connect** and **Enabled**, and click **OK**.

NOTE

The IdP name must be unique under your account.

----End

Configuring Authorization Information on the Cloud Platform

Step 1 Click **Modify** in the **Operation** column of the row containing the IdP you want to modify.

Step 2 Select an access type.

Table 3-20 Access type description

Access Type	Description
Programmatic access and management console access	<ul style="list-style-type: none"> • Programmatic access: Federated users can use development tools (including APIs, CLI, and SDKs) that support key authentication to access the cloud platform. • Management console access: Federated users can log in to the management console by using their own usernames and passwords. Select this access type if you want users to access the cloud platform through SSO.
Programmatic access	Federated users can only use development tools (including APIs, CLI, and SDKs) that support key authentication to access the cloud platform.

Step 3 Specify the configuration information.

Table 3-21 Configuration information

Parameter	Description
Identity Provider URL	<p>URL of the OpenID Connect IdP. Specify this parameter as the value of issuer in the Openid-configuration.</p> <p>NOTE Openid-configuration indicates a URL defined in OpenID Connect, containing configurations of an enterprise IdP. The URL format is https://{base URL}.well-known/openid-configuration, where <i>base URL</i> is defined by the enterprise IdP. For example, the Openid-configuration of Google is https://accounts.google.com/.well-known/openid-configuration.</p>
Client ID	ID of a client registered with the OpenID Connect IdP. The client ID is an OAuth 2.0 credential created in the enterprise IdP .
Authorization Endpoint	<p>Authorization endpoint of the OpenID Connect IdP. Specify this parameter as the value of authorization_endpoint in the Openid-configuration.</p> <p>This parameter is required only if you set Access Type to Programmatic access and management console access.</p>

Parameter	Description
Scopes	Scopes of authorization requests. openid is selected by default. This parameter is required only if you set Access Type to Programmatic access and management console access . Enumerated values: <ul style="list-style-type: none"> • openid • email • profile
Response Type	Response type of authorization requests. The default value is id_token . This parameter is required only if you set Access Type to Programmatic access and management console access .
Response Mode	Response mode of authorization requests. The options include form_post and fragment . form_post is recommended. This parameter is required only if you set Access Type to Programmatic access and management console access.
Signing Key	Public key used to sign the ID token of the OpenID Connect IdP. For account security purposes, change the signing key periodically.

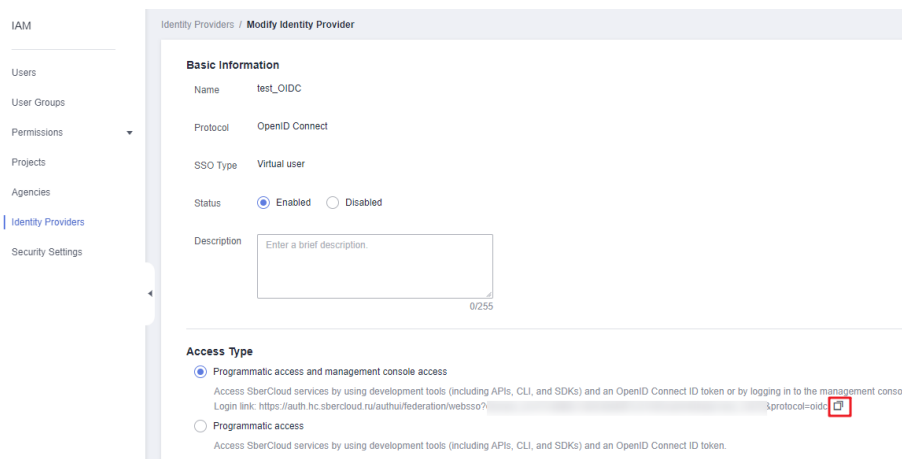
Step 4 Click **OK**.

----End

Verifying the Federated Login

Step 1 Click the login link displayed on the IdP details page and check if the login page of the enterprise IdP server is displayed.

1. On the **Identity Providers** page, click **Modify** in the **Operation** column of the IdP.
2. Copy the login link displayed on the **Modify Identity Provider** page and visit the link using a browser.

Figure 3-95 Copying the login link

3. If the enterprise IdP login page is not displayed, check the configurations of the IdP and the enterprise IdP server.

Step 2 Enter the username and password of a user that was created in the enterprise management system.

- If the login is successful, add the login link to the enterprise's website.
- If the login fails, check the username and password.

NOTE

Federated users can only access the cloud platform by default. To assign permissions to federated users, configure identity conversion rules. For more information, see [3.8.3.3 Step 2: Configure Identity Conversion Rules](#).

----End

Related Operations

- Viewing IdP information: In the IdP list, click **View** in the row containing the IdP, and view its basic information, metadata, and identity conversion rules.

NOTE

To modify the configuration of an IdP, click **Modify** at the bottom of the details page.

- Modifying an IdP: In the IdP list, click **Modify** in the row containing the IdP, and then change its status or modify the description, metadata, or identity conversion rules.
- Deleting an IdP: In the IdP list, click **Delete** in the row containing the IdP, and click **Yes** in the displayed dialog box.

Follow-Up Procedure

- Configure identity conversion rules to map enterprise IdP users to IAM user groups and assign permissions to the users. For details, see [3.8.3.3 Step 2: Configure Identity Conversion Rules](#).
- Configure the enterprise management system to allow users to access the cloud platform through SSO. For details, see [3.8.3.4 \(Optional\) Step 3: Configure a Federated Login Entry in the Enterprise IdP](#).

3.8.3.3 Step 2: Configure Identity Conversion Rules

Federated users are named **FederationUser** by default on the cloud platform. These users can only access the cloud platform and they do not have any other permissions. You can configure identity conversion rules on the IAM console to achieve the following:

- Display federated users with different names on the cloud platform.
- Grant federated users permissions to use cloud resources by mapping these users to IAM user groups. Ensure that you have created the required user groups. For details, see [3.3.1 Creating a User Group and Assigning Permissions](#).

NOTE

- Modifications to identity conversion rules will take effect only after the federated users log in again.
- To modify the permissions of a user, modify the permissions of the user group to which the user belongs. Then restart the enterprise IdP for the modifications to take effect.

Prerequisites

An IdP entity has been created, and the login link of the identity provider is accessible. (For details about how to create and verify an IdP entity, see [3.8.3.2 Step 1: Create an IdP Entity](#).)

Procedure

If you configure identity conversion rules by clicking **Create Rule**, IAM converts the rule parameters to the JSON format. Alternatively, you can click **Edit Rule** to configure rules in JSON format. For details, see [3.8.4 Syntax of Identity Conversion Rules](#).

- **Creating Rules**
 - a. Choose **Identity Providers** from the navigation pane.
 - b. In the IdP list, click **Modify** in the row containing the IdP.
 - c. In the **Identity Conversion Rules** area, click **Create Rule**. Then, configure the rules in the **Create Rule** dialog box.

Table 3-22 Parameter description

Parameter	Description	Remarks
Username	Username of federated users to be displayed on the cloud platform.	<p>To distinguish federated users from users of the cloud platform, it is recommended that you set the username to "FederationUser-IdP_XXX". <i>IdP</i> indicates an IdP name, for example, AD FS or Shibboleth. <i>XXX</i> indicates a custom name.</p> <p>NOTICE</p> <ul style="list-style-type: none"> The username of each federated user must be unique in the same IdP. Identical federated user names under the same IdP will be identified as the same IAM user on the cloud platform. The username can only contain letters, digits, spaces, hyphens (-), underscores (_), and periods (.). It cannot start with a digit and cannot contain the following special characters: ", \", \\, \n, \r
User Groups	User groups to which the federated users will belong on the cloud platform.	<p>The federated users will inherit permissions from the groups to which they belong.</p> <p>NOTE</p> <p>The user group name can only contain letters, digits, spaces, hyphens (-), underscores (_), and periods (.). It cannot start with a digit and cannot contain the following special characters: ", \", \\, \n, \r</p>
Rule Conditions	Conditions that a federated user must meet to obtain permissions from the selected user groups.	<p>Federated users who do not meet these conditions cannot access the cloud platform. You can create a maximum of 10 conditions for an identity conversion rule.</p> <p>NOTE</p> <ul style="list-style-type: none"> An identity conversion rule can have multiple conditions. It takes effect only if all of the conditions are met. An IdP can have multiple identity conversion rules. If a federated user does not meet any of the rules, the user will not be allowed to access the cloud platform.

For example, set an identity conversion rule for administrators in the enterprise management system.

- Username: **FederationUser-IdP_admin**
- User group: **admin**
- Rule condition: **_NAMEID_** (attribute), **any_one_of** (condition), and **00000001** (value).

Only the user with ID 000000001 is mapped to IAM user **FederationUser-IdP_admin** and inherits permissions from the **admin** user group.

- d. In the **Create Rule** dialog box, click **OK**.
- e. On the **Modify Identity Provider** page, click **OK**.
- **Editing Rules**
 - a. Log in to the cloud platform as an administrator, and go to the IAM console. Then, choose **Identity Providers** from the navigation pane.
 - b. In the IdP list, click **Modify** in the row containing the IdP.
 - c. In the **Identity Conversion Rules** area, click **Edit Rule**.
 - d. Edit the identity conversion rules in JSON format. For details, see [3.8.4 Syntax of Identity Conversion Rules](#).
 - e. Click **Validate** to verify the syntax of the rules.
 - f. If the rule is correct, click **OK** in the **Edit Rule** dialog box, and click **OK** on the **Modify Identity Provider** page.

If a message indicating that the JSON file is incomplete is displayed, modify the statements or click **Cancel** to cancel the modifications.

Verifying Federated User Permissions

After configuring identity conversion rules, verify the permissions of federated users.

Step 1 Log in as a federated user, such as user **ID1**.

On the **Identity Providers** page of the IAM console, click **View** in the row containing the IdP. Copy the login link displayed on the IdP details page, open the link using a browser, and then enter the username and password used in the enterprise management system.

Step 2 Check that the federated user has the permissions assigned to their user group.

For example, configure an identity conversion rule to map federated user **ID1** to the **admin** user group so that **ID1** will have full permissions for all cloud services. On the management console, select a cloud service, and check if you can access the service.

----End

Related Operations

Viewing identity conversion rules: Click **View Rule** on the **Modify Identity Provider** page. The identity conversion rules are displayed in JSON format. For details about the JSON format, see [Syntax of Identity Conversion Rules](#).

3.8.3.4 (Optional) Step 3: Configure a Federated Login Entry in the Enterprise IdP

Configure the login link of the IdP in the enterprise management system so that enterprise users can use this link to access the cloud platform.

Prerequisites

- An IdP entity has been created, and the login link of the identity provider is accessible. (For details about how to create and verify an IdP entity, see [3.8.3.2 Step 1: Create an IdP Entity](#).)
- The login link of the IdP has already been configured in the enterprise management system for logging in to the cloud platform.

Procedure

Step 1 Log in to the IAM console, and choose **Identity Providers** from the navigation pane.

Step 2 Click **View** in the row containing the IdP.

Step 3 Copy the login link.

Step 4 Add the following statement to the page file of the enterprise management system:

```
<a href="<Login link>"> Login entry</a>
```

Step 5 Log in to the enterprise management system using your enterprise account, and then click the configured login link to access the cloud platform.

----End

3.8.4 Syntax of Identity Conversion Rules

An identity conversion rule is a JSON object which can be modified. The following is an example JSON object:

```
[
  {
    "local": [
      {
        "<user> or <group> or <groups>"
      }
    ],
    "remote": [
      {
        "<condition>"
      }
    ]
  }
]
```

Parameter description:

- **local**: Identity information of a federated user mapped to IAM. The value of this field can contain placeholders, such as **{0...n}**. The attributes **{0}** and **{1}** represent the first and second remote attributes of the user information, respectively.
- **remote**: Information about a federated user of the IdP. This field is an expression consisting of assertion attributes and operators. The value of this field is determined by the assertion.
 - **condition**: Conditions for the identity conversion rule to take effect. The following three types of conditions are supported:

- **empty:** The rule is matched to all claims containing the attribute type. This condition does not need to be specified. The condition result is the argument that is passed as input.
- **any_one_of:** The rule is matched only if any of the specified strings appear in the attribute type. The condition result is Boolean, not the argument that is passed as input.
- **not_any_of:** The rule is not matched if any of the specified strings appear in the attribute type. The condition result is Boolean, not the argument that is passed as input.

NOTICE

The user information mapped to IAM can only contain letters, digits, spaces, hyphens (-), underscores (_), and periods (.), and cannot start with a digit.

Examples of the empty Condition

The **empty** condition returns character strings to replace the local attributes **{0..n}**.

- In the following example, the username of a federated user will be "the value of the first remote attribute+space+the value of the second remote attribute" in IAM, that is, *FirstName LastName*. The group to which the user belongs is the value of the third remote attribute *Group*. This attribute has only one value.

```
[
  {
    "local": [
      {
        "user": {
          "name": "{0} {1}"
        }
      },
      {
        "group": {
          "name": "{2}"
        }
      }
    ],
    "remote": [
      {
        "type": "FirstName"
      },
      {
        "type": "LastName"
      },
      {
        "type": "Group"
      }
    ]
  }
]
```

If the following assertion (simplified for easy understanding) is received, the username of the federated user will be **John Smith** and the user will only belong to the **admin** group.


```
{FirstName: John}
{LastName: Smith}
{Group: admin}
```

- If a federated user will belong to multiple user groups in IAM, the identity conversion rule can be configured as follows:

In the following example, the username of a federated user will be "the value of the first remote attribute+space+the value of the second remote attribute" in IAM, that is, *FirstName LastName*. The groups to which the user belongs are the value of the third remote attribute *Groups*.

```
[
  {
    "local": [
      {
        "user": {
          "name": "{0} {1}"
        }
      },
      {
        "group": "{2}"
      }
    ],
    "remote": [
      {
        "type": "FirstName"
      },
      {
        "type": "LastName"
      },
      {
        "type": "Groups"
      }
    ]
  }
]
```

If the following assertion is received, the username of the federated user will be **John Smith** and the user will belong to the **admin** and **manager** groups.

```
{FirstName: John}
{LastName: Smith}
{Groups: [admin, manager]}
```

Examples of the "any one of" and "not any of" Conditions

Unlike the **empty** condition, the **any one of** and **not any of** conditions return Boolean values. These values will not be used to replace the local attributes. In the following example, only **{0}** will be replaced by the returned value of the first **empty** condition in the **remote** block. The value of **group** is fixed as **admin**.

- The username of the federated user in IAM is the value of the first remote attribute, that is, *UserName*. The federated user belongs to the **admin** group. This rule takes effect only for users who are members of the **idp_admin** group in the IdP.

```
[
  {
    "local": [
      {
        "user": {
          "name": "{0}"
        }
      },
      {
        "group": {
          "name": "admin"
        }
      }
    ]
  }
]
```

```

    }
  ],
  "remote": [
    {
      "type": "UserName"
    },
    {
      "type": "Groups",
      "any_one_of": [
        "idp_admin"
      ]
    }
  ]
}
]

```

- If a federated user will belong to multiple user groups in IAM, the identity conversion rule can be configured as follows:

The username of the federated user in IAM is the value of the first remote attribute, that is, *UserName*. The federated user belongs to the **admin** and **manager** groups. This rule takes effect only for users who are members of the **idp_admin** group in the IdP.

```

[
  {
    "local": [
      {
        "user": {
          "name": "{0}"
        }
      },
      {
        "group": {
          "name": "admin"
        }
      },
      {
        "group": {
          "name": "manager"
        }
      }
    ],
    "remote": [
      {
        "type": "UserName"
      },
      {
        "type": "Groups",
        "any_one_of": [
          "idp_admin"
        ]
      }
    ]
  }
]

```

- The following assertion indicates that the federated user John Smith is a member of the **idp_admin** group. Therefore, the user can access the cloud platform.

```
{UserName: John Smith}
{Groups: [idp_user, idp_admin, idp_agency]}
```

- The following assertion indicates that the federated user John Smith is not a member of the **idp_admin** group. Therefore, the rule does not take effect for the user and the user cannot access the cloud platform.

```
{UserName: John Smith}
{Groups: [idp_user, idp_agency]}
```

Example Condition Containing a Regular Expression

You can add **"regex": true** to a condition to calculate results using a regular expression.

This rule takes effect for any user whose username ends with **@mail.com**. The username of each applicable federated user is *UserName* in IAM and the user belongs to the **admin** group.

```
[
  {
    "local": [
      {
        "user": {
          "name": "{0}"
        }
      },
      {
        "group": {
          "name": "admin"
        }
      }
    ],
    "remote": [
      {
        "type": "UserName"
      },
      {
        "type": "Groups",
        "any_one_of": [
          ".*@mail.com$"
        ],
        "regex": true
      }
    ]
  }
]
```

Examples of Combined Conditions

Multiple conditions can be combined using the logical operator AND.

This rule takes effect only for the federated users who do not belong to the **idp_user** or **idp_agent** user group in the IdP. The username of each applicable federated user is *UserName* in IAM and the user belongs to the **admin** group.

```
[
  {
    "local": [
      {
        "user": {
          "name": "{0}"
        }
      },
      {
        "group": {
          "name": "admin"
        }
      }
    ],
    "remote": [
      {
        "type": "UserName"
      },
      {
        "type": "Groups",
        "not_any_of": [
          "idp_user"
        ]
      }
    ]
  }
]
```

```

    ]
  },
  {
    "type": "Groups",
    "not_any_of": [
      "idp_agent"
    ]
  }
]
}
]

```

The preceding rule is equivalent to the following:

```

[
  {
    "local": [
      {
        "user": {
          "name": "{0}"
        }
      },
      {
        "group": {
          "name": "admin"
        }
      }
    ],
    "remote": [
      {
        "type": "UserName"
      },
      {
        "type": "Groups",
        "not_any_of": [
          "idp_user",
          "idp_agent"
        ]
      }
    ]
  }
]
}

```

Examples of Combined Rules

If multiple rules are combined, the methods for matching usernames and user groups are different.

The name of a federated user will be the username matched in the first rule that takes effect, and the user will belong to all groups matched in all rules that take effect. A federated user can log in only if at least one rule takes effect to match the username. For easy understanding, username and user group rules can be configured separately.

In the following example, the rules take effect for users in the **idp_admin** group. The username of each applicable federated user is *UserName* in IAM and the user belongs to the **admin** group.

```

[
  {
    "local": [
      {
        "user": {
          "name": "{0}"
        }
      }
    ]
  }
]

```

```

    ],
    "remote": [
      {
        "type": "UserName"
      }
    ]
  },
  {
    "local": [
      {
        "group": {
          "name": "admin"
        }
      }
    ],
    "remote": [
      {
        "type": "Groups",
        "any_one_of": [
          "idp_admin"
        ]
      }
    ]
  }
]

```

The following assertion indicates that user John Smith is a member of the **idp_admin** group in the IdP and therefore meets the rules. The username of this user will be **John Smith** in IAM, and the user will belong to the **admin** group.

```

{UserName: John Smith}
{Groups: [idp_user, idp_admin, idp_agency]}

```

3.9 MFA Authentication and Virtual MFA Device

3.9.1 MFA Authentication

What Is MFA Authentication?

MFA authentication provides an additional layer of protection on top of the username and password. If you enable MFA authentication, users need to enter the username and password as well as a verification code before they can log in to the console.

MFA authentication can also be enabled to verify a user's identity before the user is allowed to perform critical operations.

MFA Authentication Methods

MFA authentication can be performed through SMS, email, and virtual MFA device.

Application Scenarios

MFA authentication is suitable for login protection and critical operation protection.

- Login protection: When you or an IAM user under your account logs in to the console, you and the user need to enter a verification code in addition to the username and password.
- Operation protection: When you or an IAM user under your account attempts to perform a critical operation, such as deleting an ECS resource, you and the user need to enter a verification code to proceed.

For more information about login protection and critical operation protection, see [3.7.3 Critical Operation Protection](#).

3.9.2 Virtual MFA Device

This section describes how to **bind** and **unbind** a virtual MFA device. If the bound virtual MFA device of an IAM user is deleted or the mobile phone on which it runs is unavailable, you can **remove** the virtual MFA device for the IAM user.

What Is a Virtual MFA Device?

An MFA device generates 6-digit verification codes in compliance with the Time-based One-time Password Algorithm (TOTP). MFA devices can be hardware- or software-based. Currently, software-based virtual MFA devices are supported. They are application programs running on smart devices such as mobile phones.

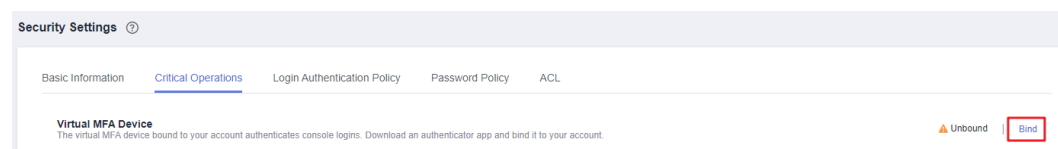
Binding a Virtual MFA Device

Install an authenticator app (such as Google Authenticator or Microsoft Authenticator) on your mobile device.

Step 1 Go to the [Security Settings](#) page.

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

Figure 3-96 Virtual MFA Device

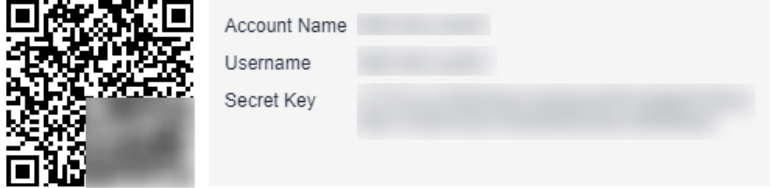


Step 3 Set up the MFA application by scanning the QR code or manually entering the secret key.

Figure 3-97 Binding a virtual MFA device

Bind Virtual MFA Device

1 **Step 1: Set up the authenticator app.**
Open the authenticator app on your mobile phone and scan the QR code or enter the secret key.



2 **Step 2: Enter the MFA verification codes.**
Enter two consecutive MFA verification codes generated on the app.

* Verification Code 1

* Verification Code 2

You can bind a virtual MFA device to your account by scanning the QR code or entering the secret key.

- Scanning the QR code
Open the MFA application on your mobile phone, and use the application to scan the QR code displayed on the **Bind Virtual MFA Device** page. Your account or IAM user is then added to the application.
- Manually entering the secret key
Open the MFA application on your mobile phone, and enter the secret key.

NOTE

Your account is manually added using the time-based algorithm. Ensure that automatic time setting has been enabled on your mobile phone.

Step 4 View the verification codes 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

Obtaining an MFA Verification Code

If virtual MFA-based login protection or operation protection is enabled, you need to enter an MFA verification code when you log in to the console or performing a critical operation.

Open the MFA application on your smart device, view the verification code displayed next to your account, and then enter the code on the console.

Unbinding a Virtual MFA Device

You can unbind the virtual MFA device as long as the mobile phone bound to the virtual MFA device is available and the virtual MFA device is still installed on your phone.

- Step 1** Go to the [Security Settings](#) page.
- Step 2** Click the **Critical Operations** tab, and click **Unbind** in the **Virtual MFA Device** row.
- Step 3** On the **Unbind Virtual MFA Device** page, enter a verification code generated by the MFA application.

Figure 3-98 Entering a virtual MFA verification code



- Step 4** Click **OK**.
- End

Removing the Virtual MFA Device

If the mobile phone of an IAM user is unavailable or the virtual MFA device has been deleted from the user's phone, as an **administrator**, you can remove the virtual MFA device by performing the following procedure:

- Step 1** Log in to the IAM console.
- Step 2** On the **Users** page, click **Security Settings** in the row containing the user for whom you want to remove the bound virtual MFA device.
- Step 3** On the **Security Settings** tab page, click **Remove** in the **Virtual MFA Device** row.
- Step 4** Click **Yes**.
- End

3.10 Viewing IAM Operation Records

3.10.1 Enabling CTS

CTS records operations performed on cloud resources in your account. The operation logs can be used to perform security analysis, track resource changes, perform compliance audits, and locate faults.

It is recommended that you enable the CTS service to record key IAM operations, such as creating and deleting users.

Procedure

- Step 1** Log in to the management console.
- Step 2** Click **Service List** and choose **Management & Deployment > Cloud Trace Service**.
- Step 3** Click **Trackers** in the navigation pane.
- Step 4** Click **Enable CTS**.
- Step 5** In the displayed dialog box, click **Enable**. The system automatically creates a tracker.

After you enable CTS, you can view the tracker information on the **Trackers** page.

----End

CTS records all operations performed on IAM, such as creating users and user groups. [Table 3-23](#) shows the IAM operations that can be recorded by CTS.

Table 3-23 IAM operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Login	user	login
Logging in as a user of the Cloud Alliance	user	cloudLoginBySaml
Login failure	user	loginFailed
Logout	user	logout
Logging in as a federated user	user	tenantLoginBySamlSuccess/ oidcLoginSuccess
(IAM user) Changing the password at first login, when the password will expire, or after the password expires	user	changePassword

Operation	Resource Type	Trace Name
Creating a user	user	createUser
Modifying user information	user	updateUser
Deleting a user	user	deleteUser
Creating an access key (AK/SK)	user	createCredential and addCredential
Deleting an access key (AK/SK)	user	deleteCredential
Disabling or enabling an access key (AK/SK)	user	changeCredentialStatus
Modifying an access key (AK/SK)	user	updateCredential
Changing the email address	user	modifyUserEmail
Changing the mobile number	user	modifyUserMobile
Changing the password	user	modifyUserPassword
Setting a password for a user (by the administrator)	user	setPasswordByAdmin
Creating a user group	userGroup	createUserGroup
Modifying a user group	userGroup	updateGroup and updateUserGroup
Deleting a user group	userGroup	deleteUserGroup
Adding users to a user group	userGroup	addUserToGroup and updateUser/ updateUserGroup
Removing users from a user group	userGroup	removeUserFromGroup and updateUser/ updateUserGroup
Unbinding a virtual MFA device	MFA	BindMFA
Binding a virtual MFA device	MFA	UnBindMFA
Creating a project	project	createProject
Modifying a project	project	updateProject
Deleting a project	project	deleteProject

Operation	Resource Type	Trace Name
Creating an agency	agency	createAgency
Modifying an agency	agency	updateAgency
Deleting an agency	agency	deleteAgency
Switching roles	agency	switchRole
	Token	createToken
Creating an identity provider	identityProvider	createIdentityProvider
Modifying an identity provider	identityProvider	updateIdentityProvider
Deleting an identity provider	identityProvider	deleteIdentityProvider
Uploading IdP metadata	identityProvider	updateMetaConfigure and uploadMetadataFile
Editing IdP metadata	identityProvider	updateMetaConfigure
Registering a mapping	mapping	createMapping
Updating a mapping	mapping	updateMapping
Deleting a mapping	mapping	deleteMapping
Registering a protocol	protocol	createProtocol
Updating a protocol	protocol	updateProtocol
Deleting a protocol	protocol	deleteProtocol
Creating a custom policy	role	createRole
Modifying a custom policy	role	updateRole
Deleting a custom policy	role	deleteRole
Assigning permissions to a user group under an account	roleGroupDomain	assignRoleToGroupOnDomain
Canceling permissions of a user group under an account	roleGroupDomain	unassignRoleToGroupOnDomain
Assigning permissions to a user group for a project	roleGroupProject	assignRoleToGroupOnProject
Canceling permissions of a user group for a project	roleGroupProject	unassignRoleToGroupOnProject

Operation	Resource Type	Trace Name
Updating the login authentication policy	domain	updateSecurityPolicies
Modifying the password policy	domain	updatePasswordPolicies
Modifying the ACL	domain	updateACLPolicies

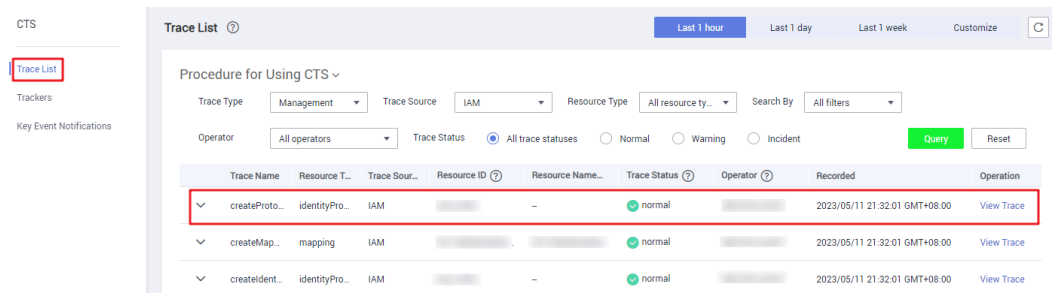
3.10.2 Viewing IAM Audit Logs

After CTS is enabled, it records key operations performed on IAM and other supported services. CTS retains operation records for the last 7 days.

Procedure

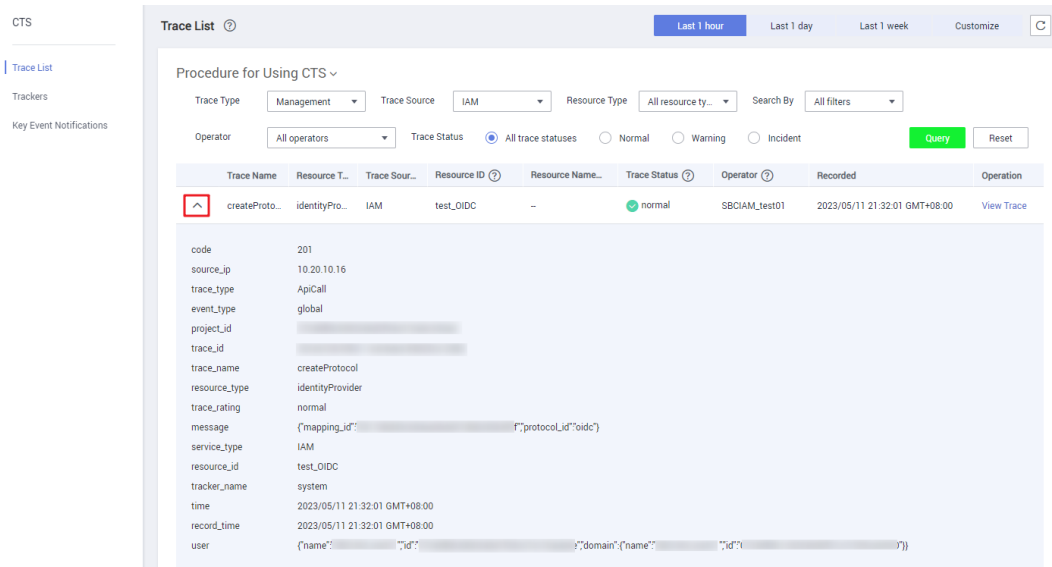
- Step 1** On the IAM console, perform an operation, such as creating a user named **CTS-Test**.
- Step 2** Log in to the CTS console and view the operation records of IAM.

Figure 3-99 Viewing IAM operation records



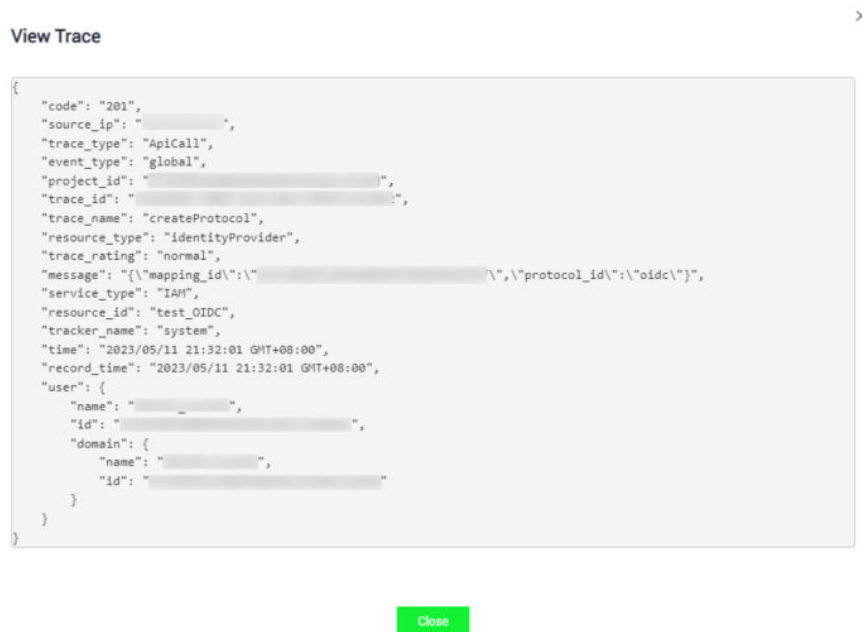
- Step 3** Click  next to a trace to view its basic information.

Figure 3-100 Viewing event basic information



Step 4 Click **View Trace** on the right of a trace to view the trace structure.

Figure 3-101 Viewing event details



----End



3.11 Quotas

What Is a Quota?

A quota is a limit on the quantity or capacity of a certain type of service resources that a user can use, for example, the maximum number of IAM users or user groups that you can create.

If the current resource quota cannot meet your service requirements, you can apply for a higher quota.

How Do I View My Quotas?

1. Log in to the management console.
2. Click  in the upper left corner and select a region and project.
3. Click  (the **My Quotas** icon) in the upper right corner.
The **Service Quota** page is displayed.
4. On the **Service Quota** page, view the used and total quotas of each type of resources.
If the quota cannot meet your service requirements, increase the quota.

How Do I Increase My Quota?

The system does not support online quota adjustment. To increase a quota, contact customer service by calling the hotline or sending an email. We will

process your request as soon as possible and will inform you of the processing progress by phone or email.

Before you contact customer service, prepare the following information:

- Account name, project name, and project ID
To obtain the preceding information, log in to the management console, click the username in the upper-right corner, and choose **My Credentials** from the drop-down list.
- Quota information, including:
 - Service name
 - Quota type
 - Required quota

Click [here](#) to obtain our service hotline and email address.

4 FAQs

- [4.1 User Groups and Permissions Management](#)
- [4.2 IAM User Management](#)
- [4.3 Security Settings](#)
- [4.4 Passwords and Credentials](#)
- [4.5 Agency Management](#)
- [4.6 Others](#)

4.1 User Groups and Permissions Management

4.1.1 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 name or permission name is incorrect.

Solutions

- Check the service name on the management console or in the help center, and view the system-defined permissions provided by the service in "Permissions".

4.1.2 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: Modify the permissions granted to the user group to which the IAM user belongs as the administrator. For details, see "Identity and Access Management > User Guide > User Groups and Authorization > Viewing or Modifying User Group Information". 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 "Identity and Access Management > User Guide > Permissions > Policies > Policy Syntax". If the system-defined permissions cannot meet your requirements, create a custom policy to allow the action. For details, see "Identity and Access Management > User Guide > Permissions > Custom Policies > 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 "Identity and Access Management > User Guide > User Groups and Authorization > Adding Users to or Removing Users from 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 "Identity and Access Management > User Guide > User Groups and Authorization > Creating a User Group and Assigning Permissions".
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 "Identity and Access Management > User Guide > Projects".
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: 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.

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 "Enterprise Management > User Guide > Personnel Management > Project Management > Managing Users in an Enterprise Project> Deleting Enterprise Projects That Are Managed by a User".

4.2 IAM User Management

4.2.1 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 Login** on the login page.
 - b. Incorrect account name or IAM user name.
Enter the correct 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 cloud platform 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 the cloud service platform from an allowed device, or ask the administrator to modify the ACL rules.

4.2.2 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

4.3 Security Settings

4.3.1 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

Step 1 On the IAM console, choose **Security Settings** in the navigation pane.

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.

4.3.2 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

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

Step 1 On the IAM console, choose **Security Settings** in the navigation pane.

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

4.3.3 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](#).

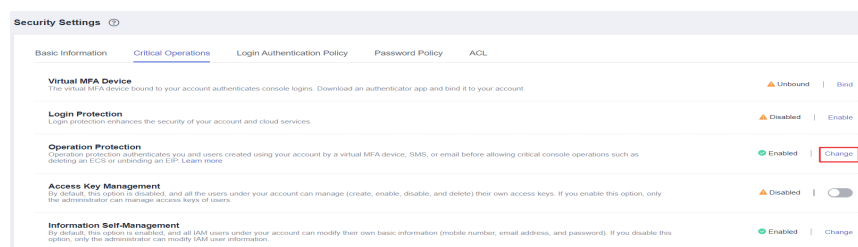
Procedure

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

Step 1 On the IAM console, choose **Security Settings** in the navigation pane.

Step 2 On the **Security Settings** page, click the **Critical Operations** tab, and click **Change** next to **Operation Protection**.

Figure 4-1 Security settings



Step 3 On the **Operation Protection** page, select **Verification by another person**, enter the mobile number or email address for verification, and enter the verification code.

Step 4 Click **OK**.

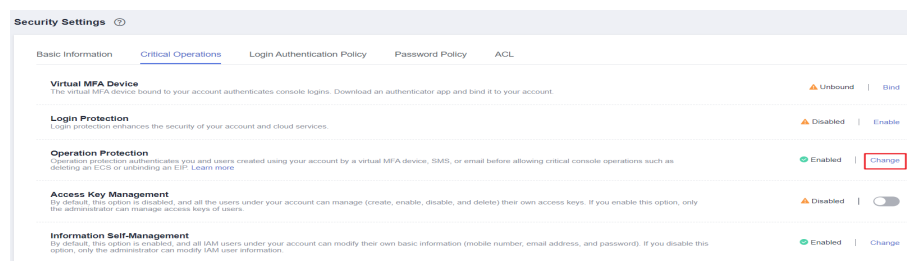
----End

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

Step 1 On the IAM console, choose **Security Settings** in the navigation pane.

Step 2 On the **Security Settings** page, click the **Critical Operations** tab, and click **Change** next to **Operation Protection**.

Figure 4-2 Security settings



Step 3 On the **Operation Protection** page, select **Disable** and click **OK**. Enter the verification code and click **OK**.

Step 4 On the **Critical Operations** tab page, click **Enable** next to **Operation Protection**.

Step 5 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 6 Click **OK**.

----End

4.3.4 How Do I Disable Operation Protection?

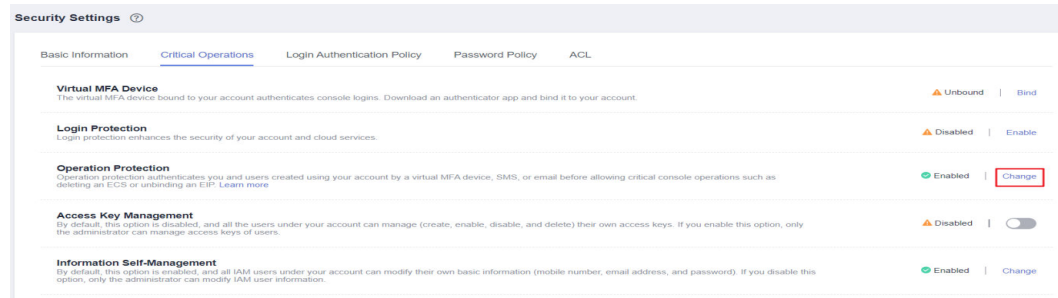
Symptom

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

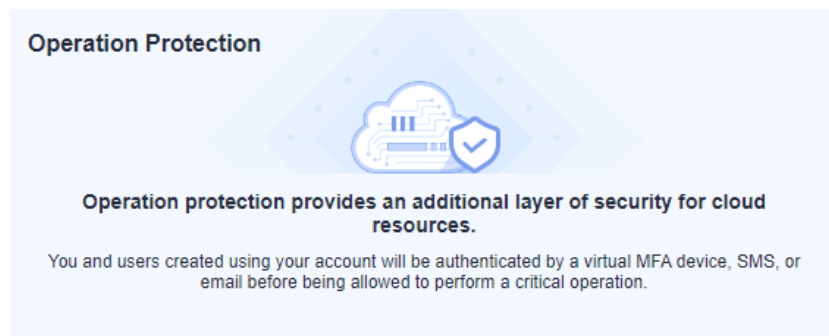
- Step 1** On the IAM console, choose **Security Settings** in the navigation pane.
- Step 2** On the **Security Settings** page, click the **Critical Operations** tab, and click **Change** next to **Operation Protection**.

Figure 4-3 Changing operation protection settings



- Step 3** Select **Disable** and click **OK**. Enter the verification code and click **OK**.

Figure 4-4 Disabling operation protection



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

① **Disable**
Identity verification will not be required for performing a critical operation.

②

Cancel

----End

4.3.5 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 you enable MFA-based login verification, you need to enter verification codes after authenticating your username and password. 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.

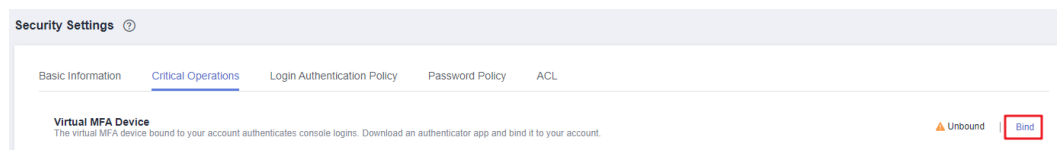
Prerequisites

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

Procedure

- Step 1** On the IAM console, choose **Account Security Settings** in the navigation pane.
- Step 2** On the **Account Settings** tab, click **Bind** next to **Virtual MFA Device**.

Figure 4-5 Virtual MFA Device

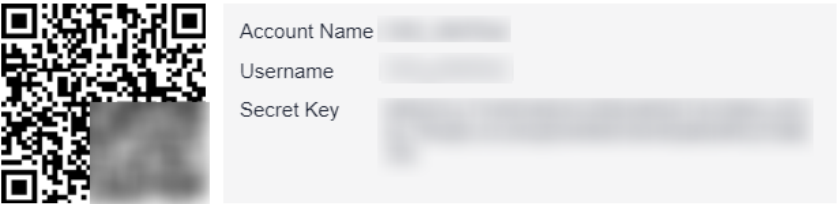


- Step 3** Set up the MFA application by scanning the QR code or entering the secret key.

Figure 4-6 Binding a virtual MFA device

Bind Virtual MFA Device

1 **Step 1: Set up the authenticator app.**
Open the authenticator app on your mobile phone and scan the QR code or enter the secret key.

The image shows a QR code on the left and a form on the right. The form has three fields: 'Account Name', 'Username', and 'Secret Key'.

2 **Step 2: Enter the MFA verification codes.**
Enter two consecutive MFA verification codes generated on the app.

* Verification Code 1

* Verification Code 2

- 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

Related FAQs

[4.3.6 How Do I Obtain a Virtual MFA Verification Code?](#)

[4.3.7 How Do I Unbind or Remove a Virtual MFA Device?](#)

[4.3.8 Why Does MFA Authentication Fail?](#)

4.3.6 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 [4.3.8 Why Does MFA Authentication Fail?](#)

4.3.7 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 [4.3.5 How Do I Bind a Virtual MFA Device?](#)

Unbinding a Virtual MFA Device

1. On the IAM console, choose **Security Settings** in the navigation pane.
2. On the **Critical Operations** tab, click **Unbind** next to **Virtual MFA Device**.
3. Enter verification codes generated by the MFA application.
4. Click **OK**.

Removing the Virtual MFA Device

If the mobile phone of an **IAM user** is unavailable or the bound virtual MFA device of the user has been deleted from the phone, the user can 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 IAM console.
2. On the **Users** page, click **Security Settings** on the right of the target user.
3. On the **Security Settings** tab page, click **Remove** next to **Virtual MFA Device**.
4. Click **Yes**.

4.3.8 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.)

4.3.9 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.
- 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.

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.
- 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.

4.3.10 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 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 [4.4.1 How Do I Reset My Password?](#)
- If the account is locked for no reason, change the password. For details, see [4.4.2 How Do I Change My Password?](#)

4.3.11 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 the cloud platform.

Login Verification

Verification Method Virtual MFA device
[Learn how to unbind or remove a virtual MFA device.](#)
[Bind Virtual MFA Device](#)

Verification 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. Therefore, login verification is still required.

Solutions

- When logging in to the management console, 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 [4.3.5 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 <input type="checkbox"/> Remember me for 7 days

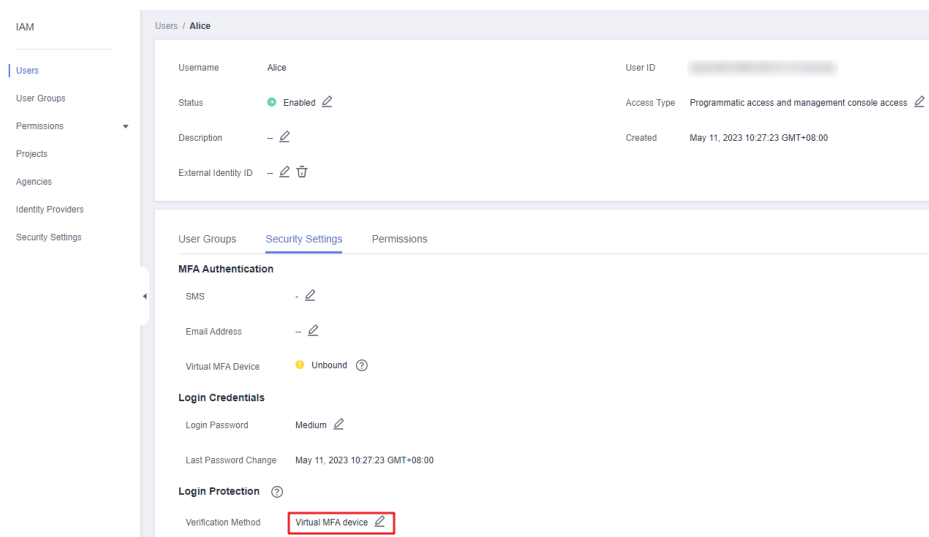
If you do not want the custom information to be displayed during login, contact the administrator.

Use Another Account

OK

- 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 4-7 Virtual MFA authentication



4.4 Passwords and Credentials

4.4.1 How Do I Reset My Password?

If you have forgotten the password of your IAM user or account, reset the password by referring to [Resetting IAM User Password or Account Password](#).

Resetting IAM User Password or Account 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 by following the instructions in "IAM Users" of the *User Guide*.

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

Step 2 Specify the account or IAM user for whom you want to reset the password, and enter the CAPTCHA code.

NOTE

- **Account:** Created upon successful registration with the cloud platform. The account has full access permissions for all of its cloud services and 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 the cloud platform using their account names, usernames, and passwords, and then use resources based on assigned permissions. IAM users do not own resources.
- 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 *User Guide* > "IAM Users" > "Changing the Login Password of an IAM User".

Step 3 Select account name/email address or mobile number verification, enter the verification information as prompted, and click **Next**.

NOTE

- Ensure that the mobile number or email address you entered is correct. Otherwise, the password cannot be reset.
- If you do not receive the verification code, see [4.3.9 Why Am I Not Getting the Verification Code?](#)

Step 4 Enter a new password, enter it again, and click **Next**.

Step 5 Click **Log In** to log in using the new password.

----End

4.4.2 How Do I Change My Password?

- If you remember your password and want to change it, do as follows:
 - **Account:** Change the password by referring to [Resetting IAM User Password or Account Password](#).
 - **IAM user:** On the IAM console, choose **Security Settings** in the left navigation pane and change the password on the **Basic Information** tab. For details, see "Changing the Login Password of an IAM User" in *Identity and Access Management User Guide*.
- If you have forgotten your password:
 - Reset your password by following the instructions in [4.4.1 How Do I Reset 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. For details, see "Changing the Login Password of an IAM User" in *Identity and Access Management User Guide*.

4.4.3 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 "Identity and Access Management > User Guide > IAM Users > Managing Access Keys for an IAM User".

4.4.4 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 *My Credentials*.

NOTE

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 "Identity and Access Management > User Guide > IAM Users > Managing Access Keys for an IAM User".
- request the administrator to assign required permissions to you or disable access key management. For details, see "Identity and Access Management > User Guide > IAM Users > Assigning Permissions to an IAM User" or "Identity and Access Management > User Guide > Security Settings > Critical Operation Protection".

4.4.5 What Are Temporary Security Credentials (AK/SK and SecurityToken)?

Temporary Security Credentials

Temporary security credentials include temporary access keys (AK/SK) and securityTokens. 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
Number of credentials	Unlimited	2 credentials for each IAM user
Obtaining method	Call the API used to obtain a temporary AK/SK.	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 securityToken. When you use temporary security credentials for authentication, add the **x-security-token** field to the request header.

4.4.6 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: <ul style="list-style-type: none"> • 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

4.5 Agency Management

4.5.1 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 "Identity and Access Management > User Guide > Agencies > Account Delegation > Creating an Agency (by a Delegating Party)".
- Contact the administrator to grant you the permissions for using IAM. For details, see "Identity and Access Management > User Guide > IAM Users > Assigning Permissions to an IAM User".

4.6 Others

4.6.1 Why Is the Field-Level Help Always Displayed?

When you register with or log in to the cloud platform, bind an 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.

- 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).

4.6.2 How Do I Disable Autofill Password on Google Chrome?

When you use Google Chrome to log in to the cloud platform 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


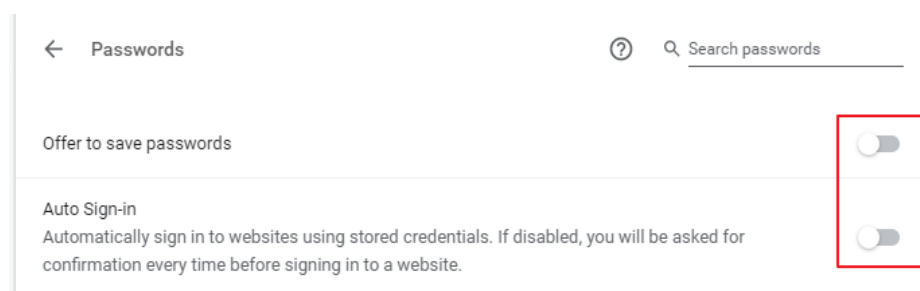

- Step 1** Open the Google Chrome browser, click  in the upper right corner of the browser, and choose **Settings**.
- Step 2** In the **Autofill** area, click **Passwords**.
- Step 3** Deselect **Offer to save passwords** and **Auto Sign-in**.

Figure 4-8 Deselecting Offer to save passwords and Auto Sign-in



----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.

4.6.3 Region and AZ

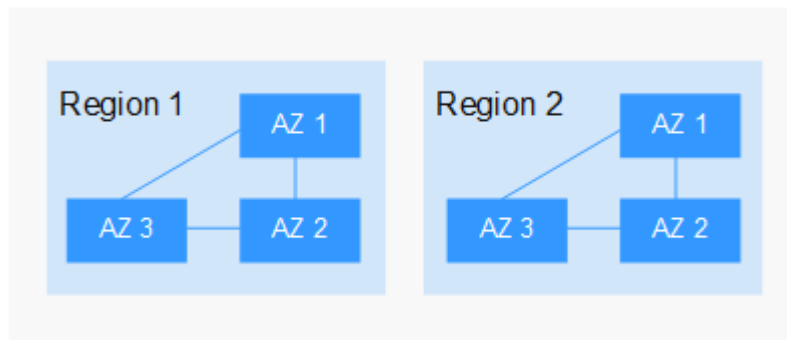
Concept

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

- A region is a physical data center, which is completely isolated to improve fault tolerance and stability. The region that is selected during resource creation cannot be changed after the resource is created.
- An AZ is a physical location where resources use independent power supplies and networks. A region contains one or more AZs that are physically isolated but interconnected through internal networks. Because AZs are isolated from each other, any fault that occurs in one AZ will not affect others.

[Figure 4-9](#) shows the relationship between regions and AZs.

Figure 4-9 Regions and AZs



Selecting a Region

Select a region closest to your target users for lower network latency and quick access.

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.

Regions and Endpoints

Before you use an API to call resources, specify its region and endpoint. For more details, see [Regions and Endpoints](#).

Before you use an API to call resources, specify its region and endpoint. Obtain the regions and endpoints from the operations administrator.

5 Change History

Table 5-1 Change history

Released On	Description
2023-05-30	<p>This issue is the sixth official release.</p> <p>Modified the following content:</p> <ul style="list-style-type: none"> • Added screenshots. • Added 1.4 Supported Cloud Services. • Added 3.4.4 Authorization Records. • Added 3.4.5.4 Cloud Services that Support Resource-Level Authorization Using IAM. • Added 4.1 User Groups and Permissions Management. • Added 4.3.10 Why Is My Account Locked? • Added 4.3.11 Why Do I Still Need to Perform MFA During Login After Unbinding the Virtual MFA Device? • Added 4.4.2 How Do I Change My Password? • Added 4.4.4 What Should I Do If I Have Forgotten My Access Key (AK/SK)? • Added 4.6.3 Region and AZ.
2023-03-22	<p>This issue is the fifth official release.</p> <p>Modified the following content:</p> <p>Added Table 3-16 in 3.7.3 Critical Operation Protection.</p>

Released On	Description
2022-11-30	<p>This issue is the fourth official release.</p> <p>Added the following content:</p> <ul style="list-style-type: none"> • Added 1.7 Notes and Constraints. • Added Table 2-3. • Added Step 5. • Added Procedure. • Added Batch Modifying IAM User Information. • Added Batch Deleting IAM Users. • Added Batch Deleting User Groups. • Added Batch Revoking Permissions of a User Group. • Added Batch Deleting Agencies. • Added Virtual MFA Device. • Added Access Key Management. • Added Information Self-Management. • Added Table 3-18. • Added 4.1.1 Why Can't I Find Permissions for a Cloud Service?. • Added 4.1.2 Why Permissions Granted to a User Do Not Take Effect?. • Added 4.3.3 How Do I Change the Verification Method for Performing Critical Operations?. • Added 4.4.2 How Do I Change My Password?. • Added 4.4.4 What Should I Do If I Have Forgotten My Access Key (AK/SK)?.
2021-07-30	<p>This issue is the third official release.</p> <p>Added section 3.8.3 Identity Federation Via OpenID Connect.</p>
2021-04-30	<p>This issue is the second official release.</p> <p>Updated all sections based on the product version.</p>
2020-02-26	<p>This issue is the first official release.</p>