

# Identity and Access Management

## User Guide

**Issue** 18  
**Date** 2021-07-30



**Copyright © Huawei Technologies Co., Ltd. 2024. All rights reserved.**

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

## **Trademarks and Permissions**



HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

## **Notice**

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

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

## **Huawei Technologies Co., Ltd.**

Address: Huawei Industrial Base  
Bantian, Longgang  
Shenzhen 518129  
People's Republic of China

Website: <https://www.huawei.com>

Email: [support@huawei.com](mailto:support@huawei.com)

# Security Declaration

## Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process*. For details about this process, visit the following web page:

<https://www.huawei.com/en/psirt/vul-response-process>

For vulnerability information, enterprise customers can visit the following web page:

<https://securitybulletin.huawei.com/enterprise/en/security-advisory>

---

# Contents

---

<b>1 Service Overview</b>	<b>1</b>
1.1 What Is IAM?	1
1.2 IAM Features	1
1.3 Identity Management	2
1.4 Permissions	4
1.5 Personal Data Protection Mechanism	12
<b>2 Getting Started</b>	<b>14</b>
2.1 Getting Started with IAM	14
2.2 Creating a Security Administrator	15
2.3 Creating a User Group and Assigning Permissions	17
2.4 Creating a User and Adding the User to a User Group	17
2.5 Logging In as an IAM User	20
<b>3 User Guide</b>	<b>21</b>
3.1 IAM Users	21
3.1.1 Creating a User	21
3.1.2 Managing IAM Users and Permissions	24
3.1.3 Viewing and Modifying User Information	26
3.1.4 Modifying User Permissions	27
3.1.5 Switching Projects or Regions	28
3.2 User Groups and Authorization	28
3.2.1 Creating a User Group and Assigning Permissions	28
3.2.2 Viewing and Modifying User Group Information	29
3.2.3 Assigning Dependency Roles	30
3.3 Permissions	30
3.3.1 Fine-Grained Policies	30
3.3.2 Policy Syntax	31
3.3.3 Creating a Custom Policy	35
3.3.4 Custom Policy Use Cases	37
3.4 Account Settings	40
3.5 Projects	42
3.6 Agencies	43
3.6.1 Account Delegation	43

3.6.1.1 Delegating Resource Access to Another Account.....	43
3.6.1.2 Creating an Agency (by a Delegating Party).....	44
3.6.1.3 (Optional) Assigning Permissions to an IAM User (by a Delegated Party).....	45
3.6.1.4 Switching Roles (by a Delegated Party).....	46
3.6.2 Cloud Service Delegation.....	47
3.6.3 Deleting or Modifying Agencies.....	47
3.7 Identity Providers.....	48
3.7.1 Introduction.....	48
3.7.2 Application Scenarios of Virtual User SSO and IAM User SSO.....	49
3.7.3 Virtual User SSO via SAML.....	50
3.7.3.1 Overview of Virtual User SSO via SAML.....	50
3.7.3.2 Step 1: Create an IdP Entity.....	52
3.7.3.3 Step 2: Configure the Enterprise IdP.....	56
3.7.3.4 Step 3: Configure Identity Conversion Rules.....	56
3.7.3.5 Step 4: Verify the Federated Login.....	59
3.7.3.6 (Optional) Step 5: Configure a Federated Login Entry in the Enterprise IdP.....	59
3.7.4 IAM User SSO via SAML.....	60
3.7.4.1 Overview of IAM User SSO via SAML.....	60
3.7.4.2 Step 1: Create an IdP Entity.....	61
3.7.4.3 Step 2: Configure the Enterprise IdP.....	64
3.7.4.4 Step 3: Configure an External Identity ID.....	65
3.7.4.5 Step 4: Verify the Federated Login.....	66
3.7.4.6 (Optional) Step 5: Configure a Federated Login Entry in the Enterprise IdP.....	66
3.7.5 Virtual User SSO via OpenID Connect.....	67
3.7.5.1 Overview of Virtual User SSO via OpenID Connect.....	67
3.7.5.2 Step 1: Create an IdP Entity.....	68
3.7.5.3 Step 2: Configure Identity Conversion Rules.....	71
3.7.5.4 (Optional) Step 3: Configure Login Link in the Enterprise Management System.....	74
3.7.6 Syntax of Identity Conversion Rules.....	74
3.8 MFA Authentication and Virtual MFA Device.....	80
3.9 Auditing.....	80
3.9.1 IAM Operations That Can Be Recorded by CTS.....	81
3.9.2 Viewing Audit Logs.....	83
<b>4 FAQs.....</b>	<b>85</b>
4.1 How Do I Enable Login Authentication?.....	85
4.2 How Do I Bind a Virtual MFA Device?.....	86
4.3 How Do I Obtain MFA Verification Codes?.....	87
4.4 How Do I Unbind a Virtual MFA Device?.....	88
4.5 Why Does IAM User Login Fail?.....	88
4.6 How Do I Control IAM User Access to the Console?.....	88
4.7 Differences Between IAM and Enterprise Management.....	89
4.8 What Are the Differences Between IAM Projects and Enterprise Projects?.....	91

---

4.9 How Can I Obtain Permissions to Create an Agency?.....	92
4.10 What Can I Do If Text Box Prompt Information Does Not Disappear?.....	93
4.11 How Do I Disable Password Association and Saving on Google Chrome?.....	93
4.12 How Do I Grant Cloud Service Permissions in the EU-Paris Region to IAM Users?.....	94
4.13 How Do I Obtain an Access Key (AK/SK) in the EU-Paris Region?.....	95
<b>A Change History.....</b>	<b>97</b>

# 1 Service Overview

---

[What Is IAM?](#)

[IAM Features](#)

[Identity Management](#)

[Permissions](#)

[Personal Data Protection Mechanism](#)

## 1.1 What Is IAM?

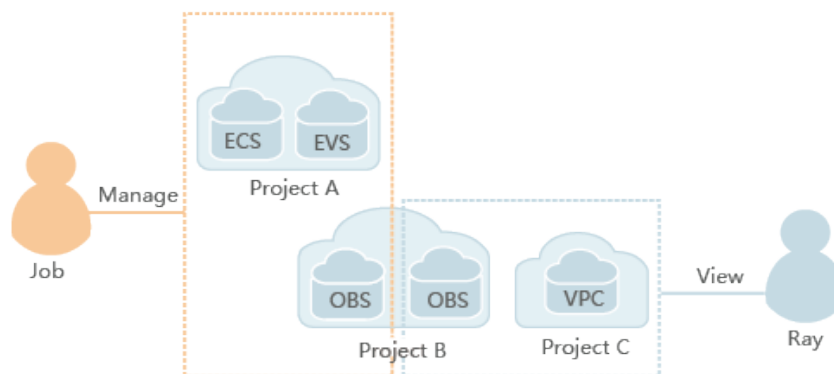
Identity and Access Management (IAM) provides identity authentication, permissions management, and access control. With IAM, you can create users for individuals, systems, and applications in your enterprise and grant permissions to these users to manage your resources. Each user has their own security credentials, and you do not need to share your API password or access keys with them. You can configure security policies to ensure account security and eliminate information security risks.

## 1.2 IAM Features

IAM provides the following basic functions:

- Refined permissions management

You can control user access to different projects and grant different permissions to users for the same project. For example, you can grant some users permissions to manage Object Storage Service (OBS), and grant other users only the permissions to read data from OBS.

**Figure 1-1** Permissions management model

- Simplified authorization  
You can authorize users in just two steps:
  - a. Plan user groups according to users' responsibilities and grant permissions to each user group.
  - b. Add a user to the user group that matches the user's responsibilities.
- Federated identity authentication  
Federated identity authentication enables users in your identity authentication system to access your resources through single sign-on (SSO).
- Delegation of resource access to another account or a specific cloud service  
You can delegate your operation permissions to a cloud service or another account so that the cloud service or account can access your resources.
- User authentication and authorization for other cloud services  
Users can be authenticated by IAM to access other services, for example, Relational Database Service (RDS), Cloud Trace Service (CTS), and OBS, based on assigned permissions.
- Security policy management  
You can set multi-factor authentication (MFA), login authentication and password policies, and an access control list (ACL) to keep user information and system data secure.

## 1.3 Identity Management

You can manage users in your account and their security credentials. In addition, you can configure identity federation so that users in other systems can access the cloud platform through SSO.

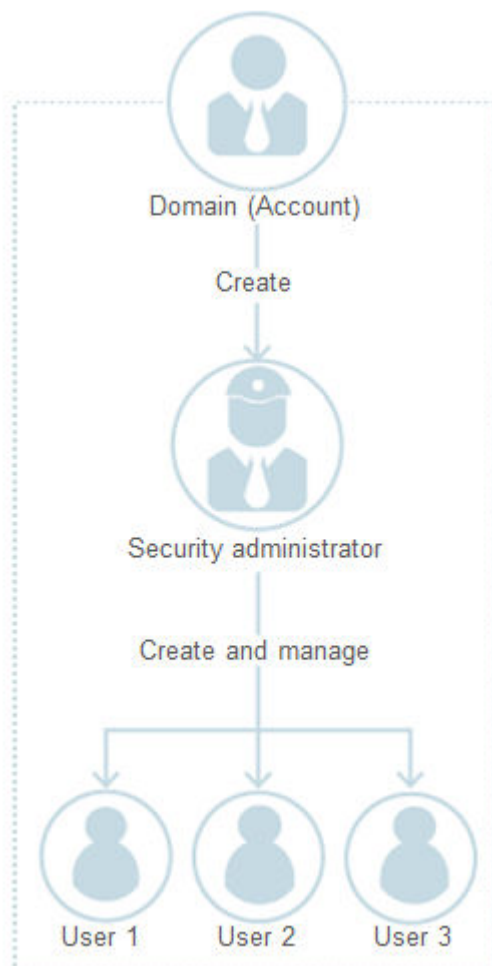
### Domain

A domain, also called an "account", is created upon successful registration with the cloud platform. The domain has full access permissions for its cloud services and resources.



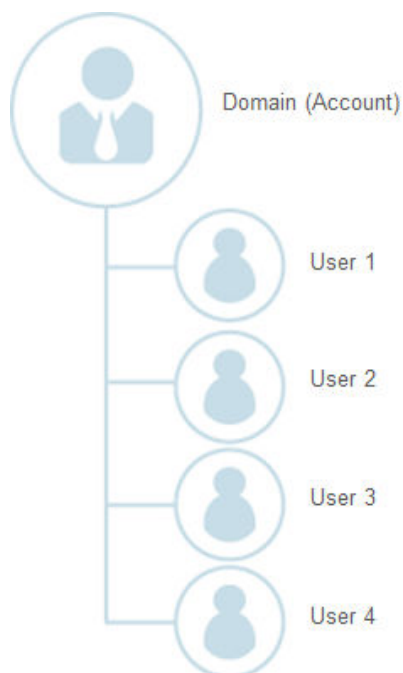
For security purposes, create a security administrator and grant them **Security Administrator** permissions to manage users and their permissions in your account.

**Figure 1-2** Account management model



## User

You or other administrators can create users for employees, systems, or applications in IAM. The users can log in to the console or access APIs using their own identity credentials (passwords and access keys).

**Figure 1-3** Relationship between an account and users

## Federated User

Federated users access the cloud platform through identity federation.

After being authenticated by an identity provider (IdP), users can access resources in a service provider (SP) without needing re-authentication.

- IdP: a system that authenticates user identities. In identity federation, the identity authentication system of an enterprise, for example, the enterprise management system, is the IdP.
- Service provider: a system that provides services.

Identity federation allows users in an IdP to access the cloud platform by using the users' security credentials in the IdP. IAM does not need to generate new security credentials for the users. In this way, SSO is implemented.

## 1.4 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 1-1** lists all the system-defined permissions for IAM.

**Table 1-1** 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	<a href="#">Content of the FullAccess Policy</a>
IAM ReadOnlyAccess	Read-only permissions for IAM. Users with these permissions can only view IAM data.	System-defined policy	<a href="#">Content of the IAM ReadOnlyAccess Policy</a>
Security Administrator	IAM administrator with full permissions, including permissions to create and delete IAM users.	System-defined role	<a href="#">Content of the Security Administrator Role</a>

Role/Policy Name	Description	Type	Content
Agent Operator	IAM operator (delegated party) with permissions to switch roles and access resources of a delegating party.	System-defined role	<a href="#">Content of the Agent Operator Role</a>
Tenant Guest	Read-only permissions for all services except IAM.	System-defined policy	<a href="#">Content of the Tenant Guest Role</a>
Tenant Administrator	Administrator permissions for all services except IAM.	System-defined policy	<a href="#">Content of the Tenant Administrator Role</a>

**Table 1-2** 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 1-2** 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

<b>Operation</b>	<b>Security Administrator</b>	<b>Agent Operator</b>	<b>FullAccess</b>	<b>IAM ReadOnlyAccess</b>
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
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

<b>Operation</b>	<b>Security Administrator</b>	<b>Agent Operator</b>	<b>FullAccess</b>	<b>IAM ReadOnlyAccess</b>
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
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

Operation	Security Administrator	Agent Operator	FullAccess	IAM ReadOnlyAccess
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 1-3** 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

Operation	Security Administrator	Agent Operator	FullAccess	IAM ReadOnlyAccess
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": [  
        ".*:get*",  
        ".*:list*",  
        ".*:head*"  
      ],  
      "Effect": "Allow"  
    }  
  ]  
}
```

## Content of the Tenant Administrator Role

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

```

    }
  },
  "Action": [
    "**:*:*"
  ],
  "Effect": "Allow"
}
]
}

```

## 1.5 Personal Data Protection Mechanism

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 records all operations performed on the data.

### Personal Data

**Table 1-4** lists the personal data collected or generated by IAM.

**Table 1-4** Personal data

Type	Source	Modifiable	Mandatory
Username	<ul style="list-style-type: none"> <li>Entered when a user is created.</li> <li>Entered when an API is called.</li> </ul>	No	Yes Usernames are used to identify users.
Password	<ul style="list-style-type: none"> <li>Entered during user creation, credential modification, or password resetting.</li> <li>Entered when an API is called.</li> </ul>	Yes	No You can choose between password- and AK/SK-based authentication.
Email address	Entered during user creation or credential or email address modification.	Yes	No
Mobile number	Entered during user creation or credential or mobile number modification.	Yes	No

Type	Source	Modifiable	Mandatory
AK (access key ID)/SK (secret access key)	Generated during credential setting on the <b>My Credentials</b> page or the IAM console.	No You cannot modify AK/SK, but you can delete AK/SK and create a new one.	No AK/SK are used to sign the requests sent to call APIs.

## Personal Data Storage

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

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

## Access Control

Personal data is stored in the IAM database after being encrypted. Access to the database is controlled through a whitelist.

## API Constraints

- AK/SK authentication is required for API calling. You can obtain AK/SK only when they are created. If you have not obtained an AK/SK or have lost the obtained AK/SK, create a new one by using the console or calling an API. For security purposes, do not share your AK/SK with anyone.
- IAM does not provide APIs for batch querying and modifying personal data.

## Logs

IAM records all personal data operations, including adding, modifying, querying, and deleting personal data, and uploads them to Cloud Trace Service (CTS). You can query operation logs at any time.

# 2 Getting Started

---

[Getting Started with IAM](#)

[Creating a Security Administrator](#)

[Creating a User Group and Assigning Permissions](#)

[Creating a User and Adding the User to a User Group](#)

[Logging In as an IAM User](#)

## 2.1 Getting Started with IAM

Your account has full access to your resources. For security purposes, create a security administrator and perform routine management as the security administrator.

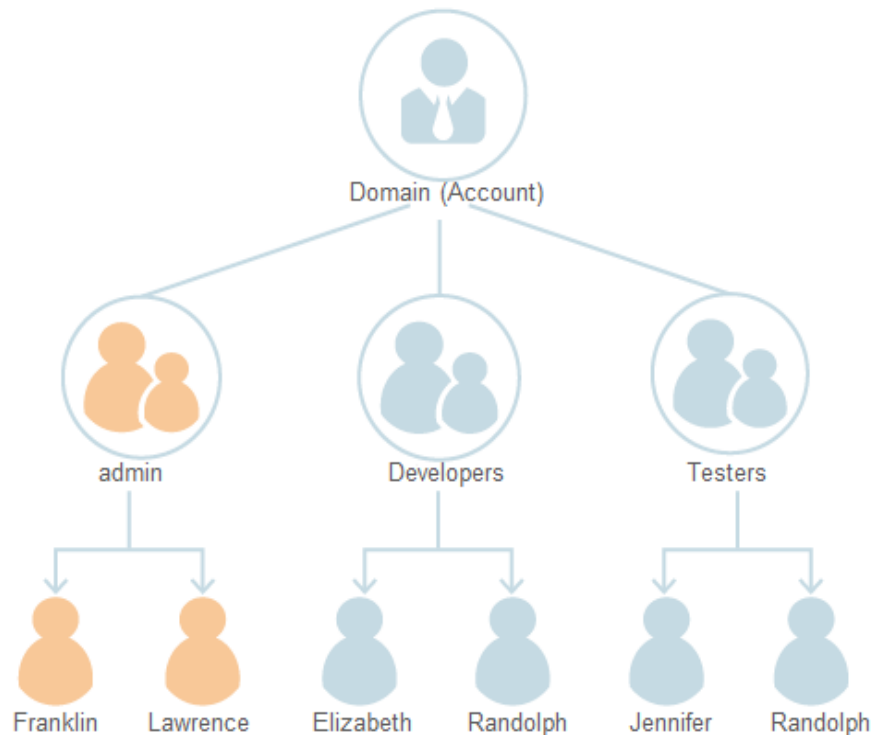
If a user needs to access resources in your account, you can create an IAM user and a user group as the security administrator, grant the required permissions to the user group, and add the user to the user group. The user inherits the permissions of the user group and has their own security credentials (username/password) to access resources in your account.

### Example

The following is an example of how to use IAM.

Assume that there are three user groups in your enterprise: security administrators (**admin**), developers, and testers. Each user group can contain multiple users, and a user can belong to multiple user groups.

Figure 2-1 User management model



1. Create a security administrator **Franklin** and add **Franklin** to the default user group **admin**.
2. Log in as **Franklin**, create another security administrator **Lawrence**, and add **Lawrence** to the default user group **admin**.
3. Log in as **Franklin** or **Lawrence**, create user groups **Developers** and **Testers**, and grant the required permissions to each user group.
4. Log in as **Franklin** or **Lawrence**, create developers **Elizabeth** and **Randolph**, and add them to the **Developers** user group. Then create tester **Jennifer**, and add **Jennifer** and **Randolph** to the **Testers** user group.
5. Users **Elizabeth**, **Jennifer**, and **Randolph** log in using their own credentials.

**NOTE**

Security administrators and users are IAM users who have different permissions depending on the user groups to which they belong. All IAM users have their own security credentials (username and password) to log in to the system.

## 2.2 Creating a Security Administrator

For security purposes, create a security administrator and manage users in your account as the security administrator.

**NOTE**

Only Cloud Alliance users with the administrator rights can create and manage users in IAM. Other users must use [Cloud Customer Space](#) to create users. On the **Rights** page, click **Add user**. For details, see [Adding a user](#). More help about the Cloud Customer Space can be found on [Flexible Engine assistance](#).

## Procedure

**Step 1** Choose **Management & Deployment > Identity and Access Management**.

**Step 2** In the navigation pane, choose **Users**.

**Step 3** On the **Users** page, click **Create User**.

**Step 4** On the **Create User** page, enter a username.

**Step 5** Select **API password** for **Credential Type**.

### NOTE

- You can use the API password to log in to the management console and to access resources with development tools (such as APIs, CLI, and SDKs) that support password authentication. The security administrator will manage users, so you are advised to select for **Credential Type**.
- You can also access resources using access keys together with development tools (including APIs, CLI, and SDKs) that support key authentication.

**Step 6** In the **User Groups** area, select **admin** from the drop-down list.

**Step 7** Click **Next**.

**Step 8** Then specify **API Password Type** as **Set now**.

### NOTE

If you create the security administrator for yourself, select **Set now** for **API Password Type**. If you create the security administrator for another user, select **Set by user** for **API Password Type** so that the user can set their own password.

**Step 9** Select **API Password Reset** to require the security administrator to change the password at first login. This option is enabled by default. Keep it enabled for security purposes.

**Step 10** Enter the email address, mobile number, and API password, and enter the password again.

### NOTE

- The email address and mobile number will be used as credentials of the security administrator.
- The password must meet the following requirements:
  - Must contain 6 to 32 characters.
  - Complies with the [password policy](#).
  - Must contain at least two types of the following: uppercase letters, lowercase letters, digits, and special characters (~!?,.,;:\_'"(){}/<>@#\$\$%^&\*+|\= and spaces).
  - 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**.

**Step 11** Click **OK**.

----End

## 2.3 Creating a User Group and Assigning Permissions

As a security administrator, you can create user groups and grant them permissions.

### Procedure

**Step 1** Choose **Management & Deployment > Identity and Access Management**.

**Step 2** In the navigation pane, choose **User Groups**.

**Step 3** On the **User Groups** page, click **Create User Group**.

**Step 4** Enter a user group name.

**Step 5** (Optional) Enter a description for the user group.

#### NOTE

To enable users to directly view their permissions, set a description for the user group. For example, if you assign the **Security Administrator** role to a user group, you can set any description in the **Description** text box. For example: **Security Administrator: Permissions for creating, deleting, and modifying users as well as granting permissions to users**. For details about the permissions for all cloud services, see [Permission Description](#).

**Step 6** Click **OK**.

The user group is displayed in the user group list.

**Step 7** Click **Modify** in the **Operation** column of the row that contains the user group.

**Step 8** In the **Group Permissions** area, click **Attach Policy** in the **Operation** column of the row that contains the target project.

#### NOTE

Permissions granted to the user group take effect only for the current project. If you need to grant permissions for multiple projects to the user group, click **Attach Policy** in the row that contains each project and grant permissions.

**Step 9** Attach policies to the user group.

#### NOTE

You can enter a keyword to quickly find the target policy.

**Step 10** Click **OK**.

----End

## 2.4 Creating a User and Adding the User to a User Group

As a security administrator, you can create a user and add the user to a user group. The user automatically inherits the permissions of the user group.

 **NOTE**

Only Cloud Alliance users with the administrator rights can create and manage users in IAM. Other users must use [Cloud Customer Space](#) to create users. On the **Rights** page, click **Add user**. For details, see [Adding a user](#). More help about the Cloud Customer Space can be found on [Flexible Engine assistance](#).

## Procedure

**Step 1** Choose **Management & Deployment > Identity and Access Management**.

**Step 2** In the navigation pane, choose **Users**. Then click **Create User**.

**Step 3** On the **Create User** page, enter a username.

**Step 4** Specify the credential type.

Credential Type	Scenario
API password	<ul style="list-style-type: none"> <li>Used to log in to the management console.</li> <li>Used together with development tools (such as APIs, CLI, and SDK) that support password authentication to access cloud services.</li> </ul>
Access key	Used together with development tools (such as APIs, CLI, and SDK) that support key authentication to access cloud services.

**Step 5** Select a user group from the drop-down list in the **User Groups** area.

 **NOTE**

- You can enter a keyword to quickly find the target user group.
- You can add a user to multiple user groups.

Perform the subsequent operation based on the credential type you select in [Step 4](#).

Credential Type	Follow-up Operation
API password	Go to <a href="#">6</a> .
Access key	<p>Click <b>OK</b>. The user is created, and an access key is automatically generated for the user.</p> <p><b>NOTE</b> Access keys are credentials used for identity authentication in IAM. You can download access keys only when they are generated.</p>

**Step 6** Click **Next**. Then specify **API Password Type**.



API Password Type	Description	Follow-up Operation
Set by user	The system will send a one-time login URL to the user. The user can set a password by clicking on the one-time login URL sent over email.	<ol style="list-style-type: none"> <li>1. Enter an email address for receiving the login link.</li> <li>2. (Optional) Enter a mobile number.</li> </ol>
Automatically generated	The system will generate a random 10-character password after you click <b>OK</b> . The user can use development tools (such as APIs, CLI, and SDK) that support password authentication to access cloud services.	<ol style="list-style-type: none"> <li>1. (Optional) Enter an email address.</li> <li>2. (Optional) Enter a mobile number.</li> </ol>
Set now	Set a password now.	<ol style="list-style-type: none"> <li>1. (Optional) Enter an email address.</li> <li>2. (Optional) Enter a mobile number.</li> <li>3. Set a password and enter it again.</li> </ol> <p><b>NOTE</b> The password must meet the following requirements:</p> <ul style="list-style-type: none"> <li>• Must contain 6 to 32 characters.</li> <li>• Complies with the <a href="#">password policy</a>.</li> <li>• Must contain at least two types of the following: uppercase letters, lowercase letters, digits, and special characters (~`!?,.,;:_'"(){}[]/&lt;&gt;@#\$\$%^&amp;*+ \= and spaces).</li> <li>• Cannot be the username or the username spelled backwards. For example, if the username is <b>A12345</b>, the password cannot be <b>A12345</b>, <b>a12345</b>, <b>54321A</b>, or <b>54321a</b>.</li> </ul>

**Step 7** Select **API Password Reset** to require the user to change the password at first login. This option is enabled by default. Keep it enabled for security purposes.

**Step 8** Click **OK**.

The user is created successfully.

----End

## 2.5 Logging In as an IAM User

You can log in to the cloud platform as an IAM user and access cloud services based on granted permissions.

### Background

If either of the following has been configured on **Security Settings > Login Authentication Policy**, you will see the **Login Verification** page after login:

- **Recent Login Information** has been enabled.
- **Custom Information** has been configured.

### Procedure

- Step 1** On the login page of Orange Cloud for Business, click **API Login** in the upper right corner.
- Step 2** Enter **Domain name, Username/Email address/Mobile number**, and **API password**, and click **Log In**.

#### NOTE

- **Domain Name** is set when you register with Orange Cloud for Business. **Username** is the name of a user created in IAM.
- If this is your first login, change your initial password on the **First Login** page. To ensure account security, change your password periodically.
- Enter a verification code on the **Login Verification** page if login authentication has been enabled.

If the login is successful, the management console is displayed.

----End

# 3 User Guide

---

- [IAM Users](#)
- [User Groups and Authorization](#)
- [Permissions](#)
- [Account Settings](#)
- [Projects](#)
- [Agencies](#)
- [Identity Providers](#)
- [MFA Authentication and Virtual MFA Device](#)
- [Auditing](#)

## 3.1 IAM Users

### 3.1.1 Creating a User

If you need to share resources in your account to other users, you can create users by using the console or by calling an API, and set security credentials and required permissions for the users. The users can then access the cloud platform through the management console or by calling APIs.

#### NOTE

Only Cloud Alliance users with the administrator rights can create and manage users in IAM. Other users must use [Cloud Customer Space](#) to create users. On the **Rights** page, click **Add user**. For details, see [Adding a user](#). More help about the Cloud Customer Space can be found on [Flexible Engine assistance](#).

#### Procedure

- Step 1** In the navigation pane, choose **Users**.
- Step 2** On the **Users** page, click **Create User**.

**Step 3** On the **Create User** page, enter the username.

**Step 4** Specify the credential type.

Credential Type	Scenario
API password	<ul style="list-style-type: none"> <li>Used to log in to the management console.</li> <li>Used together with development tools (such as APIs, CLI, and SDK) that support password authentication to access cloud services.</li> </ul>
Access key	Used together with development tools (such as APIs, CLI, and SDK) that support key authentication to access cloud services.

**Step 5** In the **User Groups** area, select a user group from the drop-down list.

 **NOTE**

- You can enter a keyword to quickly find the target user group.
- You can add a user to multiple user groups.

Perform one of the following based on the credential type you selected in [Step 4](#).

Credential Type	Follow-up Operation
API password	Go to <a href="#">6</a> .
Access key	<p>Click <b>OK</b>. The user is created, and an access key is automatically generated for the user.</p> <p><b>NOTE</b> Access keys are credentials used for identity authentication in IAM. You can download access keys only when they are generated. If the user needs to use an access key for authentication in IAM but it has not been downloaded, the user can only create a new access key.</p>

**Step 6** Click **Next**. Specify **API Password Type**.

API Password Type	Description	Follow-up Operation
Set by user	<p>The system will send a one-time login URL to the user. The user can set a password by clicking on the one-time login URL sent over email.</p> <p>The URL is valid for 7 days. Remind the user to log in and set a password before the URL expires.</p>	<ol style="list-style-type: none"> <li>Enter an email address for receiving the login link.</li> <li>(Optional) Enter a mobile number.</li> <li>Click <b>OK</b>.</li> </ol>

API Password Type	Description	Follow-up Operation
Automatically generated	The system will generate a random password after you click <b>OK</b> . The user can use development tools (such as APIs, CLI, and SDK) that support password authentication to access cloud services.	<ol style="list-style-type: none"> <li>1. (Optional) Enter an email address.</li> <li>2. (Optional) Enter a mobile number.</li> <li>3. Click <b>OK</b>.</li> <li>4. Download the password file.</li> </ol>
Set now	Set a password now.	<ol style="list-style-type: none"> <li>1. (Optional) Enter an email address.</li> <li>2. (Optional) Enter a mobile number.</li> <li>3. Set a password and enter it again.</li> </ol> <p><b>NOTE</b> The password must meet the following requirements:</p> <ul style="list-style-type: none"> <li>- Must contain 6 to 32 characters.</li> <li>- Must contain at least two types of the following: uppercase letters, lowercase letters, digits, and special characters (~!?,,;:_'"(){}[]/&lt;&gt;@#\$\$%^&amp;*+ \= and spaces).</li> <li>- Cannot be the username or the username spelled backwards. For example, if the username is <b>A12345</b>, the password cannot be <b>A12345</b>, <b>a12345</b>, <b>54321A</b>, or <b>54321a</b>.</li> <li>- Cannot contain the user's mobile number or email address.</li> </ul> <ol style="list-style-type: none"> <li>4. Click <b>OK</b>.</li> </ol>

 **NOTE**

- The user can log in to the cloud platform using the username, mobile number, or email address.
- If the user forgets the password, the user can reset it using the bound email address or mobile number.

**Step 7** If you select **Automatically generated** or **Set now**, choose whether to require password reset when the user logs in. For security purposes, do not deselect this option.

**Step 8** Click **OK**.

The user is created successfully.

----End

## Related Operations

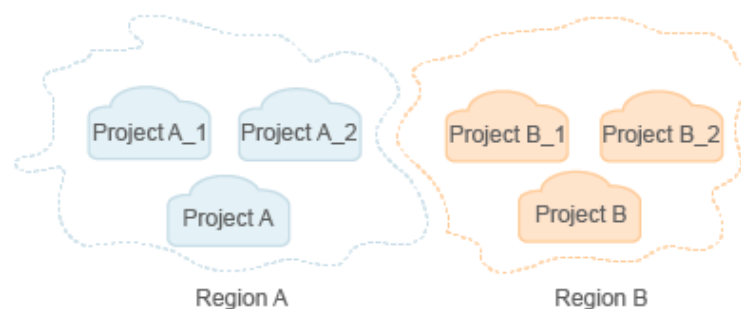
- View and modify information about the user, including the user status, email address, mobile number, user groups, and logs.
- In the user list, click **Delete** in the row that contains the user you want to delete and click **Yes**.

## 3.1.2 Managing IAM Users and Permissions

As a security administrator, you can grant permissions to a user group and add users to it. The users inherit the permissions of the user group and can access the cloud platform based on assigned permissions.

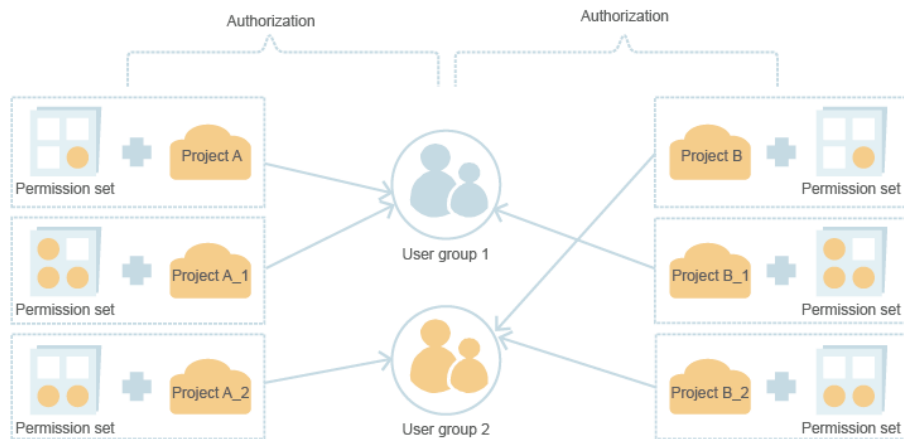
**Step 1** Create projects in a region to isolate resources.

**Figure 3-1** Project isolating model



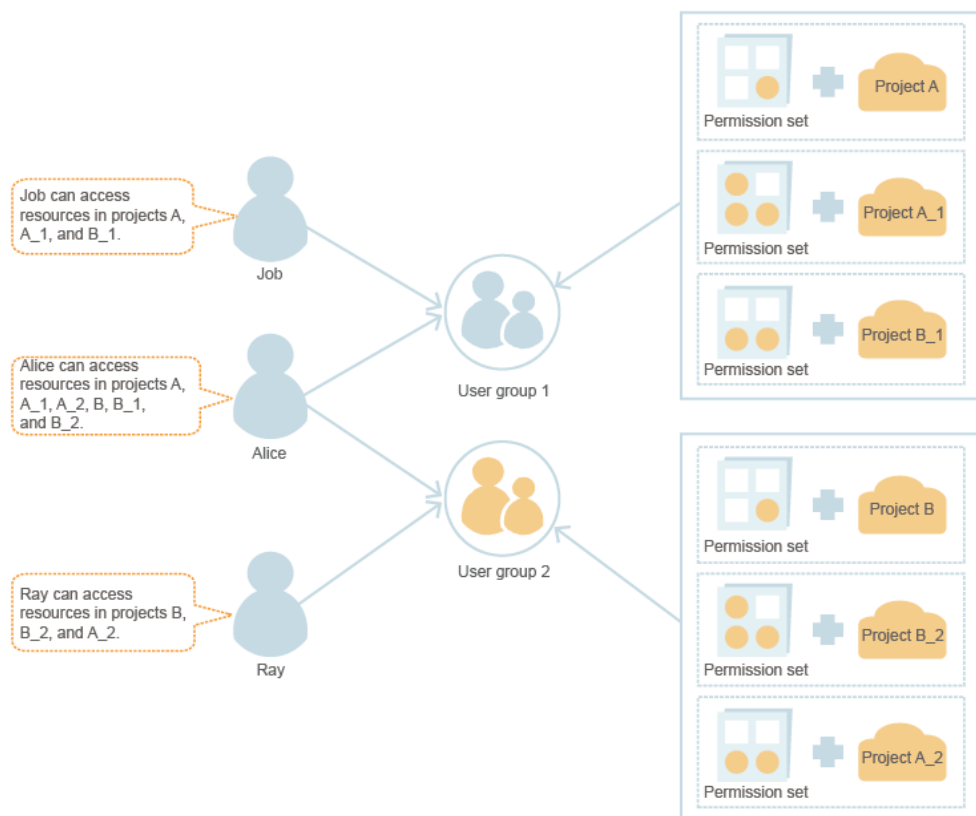
**Step 2** Plan user groups according to user responsibilities and grant the required permissions to the user groups.

**Figure 3-2** User group authorization model



**Step 3** Create users and add them to the corresponding user groups.

**Figure 3-3** User authorization model



**Step 4** Log in as the users and access the cloud platform based on assigned permissions.

----End

## 3.1.3 Viewing and Modifying User Information

### Viewing User Information

In the user list, view the detailed information about a user, including the basic information, user groups, and logs.

### Modifying User Information

Click **Modify** in the **Operation** column of the row that contains the target user.

- **Status:** A user is enabled by default after being created. You can change the status of a user to **Disabled** if you will no longer use it.
- **Login Authentication**
  - **Virtual MFA device:** Change the login authentication mode to virtual MFA device only if the user has been bound to an MFA device. The user needs to enter an MFA verification code during login.
  - **SMS:** Change the login authentication mode to SMS only if the user has been bound to a mobile number. The user needs to enter an SMS verification code during login.
  - **Email:** Change the login authentication mode to email only if the user has been bound to an email address. The user needs to enter an email verification code during login.
- **Email Address, Mobile Number, and Description**
- **Virtual MFA Device:** Bind an MFA device to or unbind an MFA device from the user.
- **User Groups:** Add the user to or remove the user from one or more user groups.

 **NOTE**

You can enter a keyword to quickly find the target user group.

### Setting User Credentials

In the user list, click **Set Credentials** in the **Operation** column of the row that contains the target user to change the API password or manage access keys.

Credential Type	Generation Method	Description	Application Scenario
API password	Set by user	The user can set a password by clicking on the one-time login URL sent over email.	Resetting the API password of a user who has been associated with an email address and needs to use the password to log in to the management console.



Credential Type	Generation Method	Description	Application Scenario
	Automatically generated	The system automatically generates a 10-character API password. <b>NOTE</b> You can download the password after clicking <b>OK</b> when the user is created.	Resetting the password of a user who uses a development tool (such as APIs, CLI, and SDK) that supports password authentication to access the cloud platform.
	Set now	Set an API password for the user.	Setting a password for a user.
Access key	Created by a user or security administrator	Create or delete access keys in the <b>Access Keys</b> area. <b>NOTE</b> Each user can have a maximum of two access keys, which are valid for 360 days. To ensure account security, keep the access keys properly.	Creating or deleting access keys of users who access the cloud platform using access keys.

- **Password Reset:** If you select **Automatically generated** or **Set now**, you can choose whether to require password reset when the user logs in. For security purposes, do not deselect this option.
- Resetting the failed login count  
In the user list, click **Reset Failed Login Count** in the **Operation** column of the row that contains the target user to reset the failed login count and unlock the user.

 **NOTE**

If your domain account is locked, contact technical support. (The domain account cannot be modified.)

### 3.1.4 Modifying User Permissions

You can modify user permissions using either of the following methods:

- Change the user groups to which a user belongs on the **Modify User** page. Choose this method if you want to modify the permissions of a single user. For details, see [Viewing and Modifying User Information](#).
- Modify the permissions of a user group or change the users included in the user group. Choose this method if you want to modify the permissions of multiple users. For details, see [Viewing and Modifying User Group Information](#).

## 3.1.5 Switching Projects or Regions

Resources in different projects or regions are isolated. You can access resources only in the projects or regions for which you have been granted permissions. If you do not have permissions for the current project or region, switch to another project or region which you have been authorized to access.

### Procedure

- Step 1** Log in to the management console.
- Step 2** In the upper left corner, select the project or region you want to access from the drop-down list.

After switching to the target project or region, you can access resources in the project or region.

----End

## 3.2 User Groups and Authorization

### 3.2.1 Creating a User Group and Assigning Permissions

You can plan user groups based on user responsibilities and grant the required permissions to the user groups. Users inherit permissions from the user groups to which they belong.

### Procedure

- Step 1** In the navigation pane, choose **User Groups**.
- Step 2** On the **User Groups** page, click **Create User Group**.
- Step 3** Enter a user group name.
- Step 4** (Optional) Enter a description for the user group.

#### NOTE

To enable users to directly view their permissions, set a description for the user group. For example, if you assign the **Security Administrator** role to a user group, you can set any description in the **Description** text box. For example: **Security Administrator: Permissions for creating, deleting, and modifying users as well as granting permissions to users.** For details about the permissions for all cloud services, see [Permissions](#).

- Step 5** Click **OK**.  
The user group is displayed in the user group list.
- Step 6** Click **Modify** in the **Operation** column of the row that contains the newly created user group.
- Step 7** In the **Group Permissions** area, click **Attach Policy** in the **Operation** column of the row that contains the target project.

 **NOTE**

Permissions granted to the user group take effect only for the current project. If you need to grant permissions for multiple projects to the user group, click **Attach Policy** in the row that contains each project and grant permissions.

**Step 8** Attach policies to the user group.

 **NOTE**

You can enter a keyword to quickly find the target policy.

**Step 9** Click **OK**.

----End

### 3.2.2 Viewing and Modifying User Group Information


As a security administrator, you can view and modify the basic information, permissions, and users of a user group. You can modify users' permissions by changing the groups to which the users belong.

#### Procedure

**Step 1** In the navigation pane, choose **User Groups**.

**Step 2** In the user group list, view or modify user group information.

- Viewing user group information

In the user group list, click  next to the target user group to view its details, including the basic information, permissions, and users.

- Modifying user group information

Click **Modify** in the **Operation** column of the row that contains the target user group to go to the **Modify User Group** page.

 **NOTE**

- For the default user group, you can only manage its users and cannot modify its basic information or permissions.
- If the name of a user group has been configured in the identity conversion rules of an IdP, modifying the user group name will cause the identity conversion rules to fail. Exercise caution when performing this operation.

User Group Information	Modification Method
Group Permissions	<ol style="list-style-type: none"> <li>1. Click <b>Attach Policy</b> in the <b>Operation</b> column of the row that contains the project for which you want to grant permissions to the user group.</li> <li>2. On the displayed <b>Attach Policy</b> page, select required policies.</li> <li>3. Click <b>OK</b>.</li> </ol>


User Group Information	Modification Method
Group Members	<ul style="list-style-type: none"> <li>- Adding a user In the <b>Group Members</b> area, select a user from the drop-down list.</li> <li><b>NOTE</b> You can enter a keyword to quickly find the target user.</li> <li>- Removing a user In the <b>Group Members</b> area, remove a user from the user group.</li> </ul>

----End

### 3.2.3 Assigning Dependency Roles

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 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** Click  next to the role to view the 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 5** Click **OK**.

----End

## 3.3 Permissions

### 3.3.1 Fine-Grained Policies

A fine-grained policy is a set of permissions that define operations allowed to be performed on specific cloud services. A policy can contain multiple permission sets. After a policy is attached to a user group, users in the user group inherit the permissions of the policy. IAM implements fine-grained access control based on the permissions defined by policies.

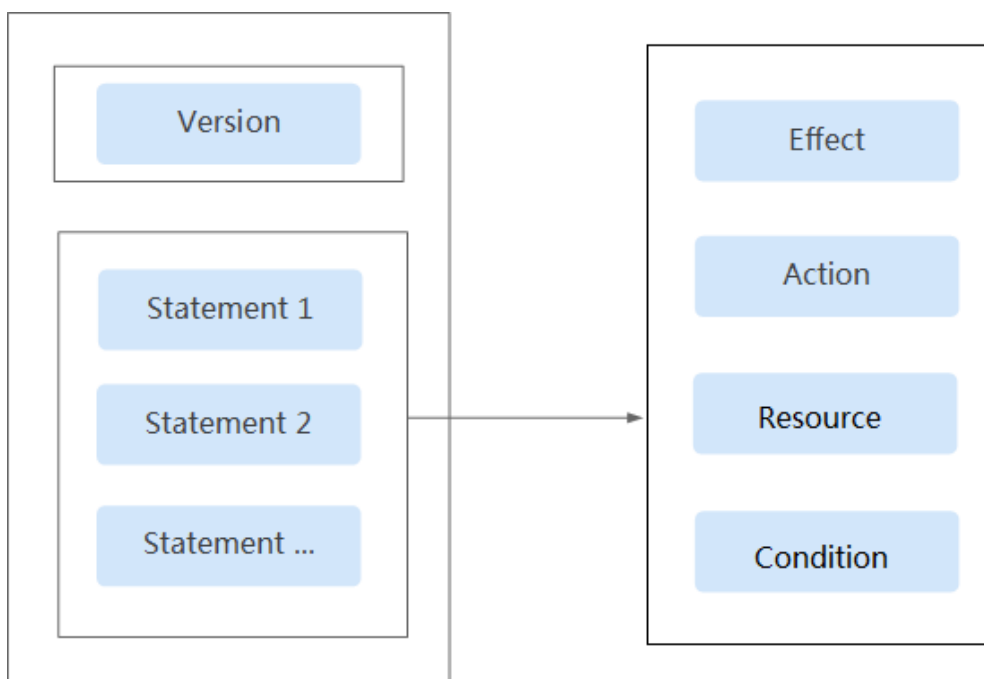
IAM supports two types of policies:

- System-defined policies: define the common permissions preset in the cloud platform, which are typically read-only or administrator permission for different cloud services such as ECS. System-defined policies can only be used for authorization and cannot be modified.
- Custom policies: created and managed by users to supplement system-defined policies.

### 3.3.2 Policy Syntax

#### Policy Content

A fine-grained policy consists of the policy version (the **Version** field) and statement (the **Statement** field).



- **Version:** Distinguishes between role-based access control (RBAC) and fine-grained policies.
  - **1.0:** RBAC policies, which are preset in the system and used to grant permissions for each service as a whole. After such a policy is granted to a user, the user has all permissions of the corresponding service.
  - **1.1:** Fine-grained policies, which enable more refined authorization based on service APIs. Users granted permissions of such a policy can only perform specific operations on the corresponding service. Fine-grained policies include system-defined and custom policies.
    - System-defined policies: read-only and administrator permissions for different services.
    - Custom policies: created and managed by users to supplement system-defined policies. For example, you can create a custom policy to allow users only to modify ECS specifications.
- **Statement:** Detailed information about a policy, containing the **Effect** and **Action** elements as well as the **Resource** and **Condition** elements.

- Effect  
The valid values for **Effect** include **Allow** and **Deny**. In a custom policy that contains both Allow and Deny statements, the Deny statements take precedence.
- Action  
The value can be one or more resource operations.  
The value format is *Service name.Resource type.Action*, for example, **vpc:ports:create**.
- Resource  
Resources on which the policy takes effect.  
Format: *Service name.Region.Account ID.Resource type.Resource path*. An asterisk (\*) means all based on its position in the resource path.  
Example:
  - **obs:\*:\*:bucket:\***: All OBS buckets
  - **obs:\*:\*:object:my-bucket/my-object/\***: All objects in the **my-object** directory of the **my-bucket** bucket
- Condition  
Conditions determine when a policy takes effect. A condition consists of a condition key and operator. Condition keys (see the documentation of the relevant cloud service) are either **global** or service-level and are used in the **Condition** element of a policy statement. Global condition keys (starting with **g:**) are available for operations of all services, while service-level condition keys (starting with a service abbreviation name such as **obs:**) are available only for operations of the corresponding service. An operator is used together with a condition key to form a complete condition statement.  
Format: *Condition operator:{Condition key:[Value 1, Value 2]}*  
Example:
  - **StringEndWithIfExists":{"g:UserName":["specialCharactor"]}**: The statement is valid for users whose names end with **specialCharactor**.

**Table 3-1** Global condition keys

Global Condition Key	Type	Description
g:CurrentTime	Time	Time when an authentication request is received. The time is expressed in the format defined by ISO 8601, for example, <b>2012-11-11T23:59:59Z</b> .
g:DomainName	Character string	Domain name

Global Condition Key	Type	Description
g:ProjectName	Character string	Project name
g:ServiceName	Character string	Service name
g:UserId	Character string	User ID
g:UserName	Character string	Username

 **NOTE**

- *Service name*: indicates a product name, such as **ecs**, **evs**, or **vpc**. Only lowercase letters are allowed.
- *Resource type* and *Action*: The values are case-insensitive, and wildcards (\*) are allowed. A wildcard (\*) can represent all or part of information about resource types and actions for the specific service.

### Example Policies

- A policy can define a single permission, such as the permission required to query ECS details.

```

{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ecs:servers:list",
        "ecs:servers:get",
        "ecs:serverVolumes:use",
        "ecs:diskConfigs:use",
        "ecs:securityGroups:use",
        "ecs:serverKeypairs:get",
        "vpc:securityGroups:list",
        "vpc:securityGroups:get",
        "vpc:securityGroupRules:get",
        "vpc:networks:get",
        "vpc:subnets:get",
        "vpc:ports:get",
        "vpc:routers:get"
      ]
    }
  ]
}

```

```
    ]
  }
]
}
```

- A policy can define multiple permissions, such as the permissions required to lock ECSs and create Elastic Volume Service (EVS) disks.

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ecs:servers:lock",
        "evs:volumes:create"
      ]
    }
  ]
}
```

- The following example shows how to use wildcards (\*) to define full permissions for Image Management Service (IMS) resources.

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "ims:*:*",
        "ecs:*:list",
        "ecs:*:get",
        "evs:*:get"
      ],
      "Effect": "Allow"
    }
  ]
}
```

- The following is an example policy that forbids users whose names start with **TestUser** to view OBS buckets **TestBucket\***.

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

 **NOTE**

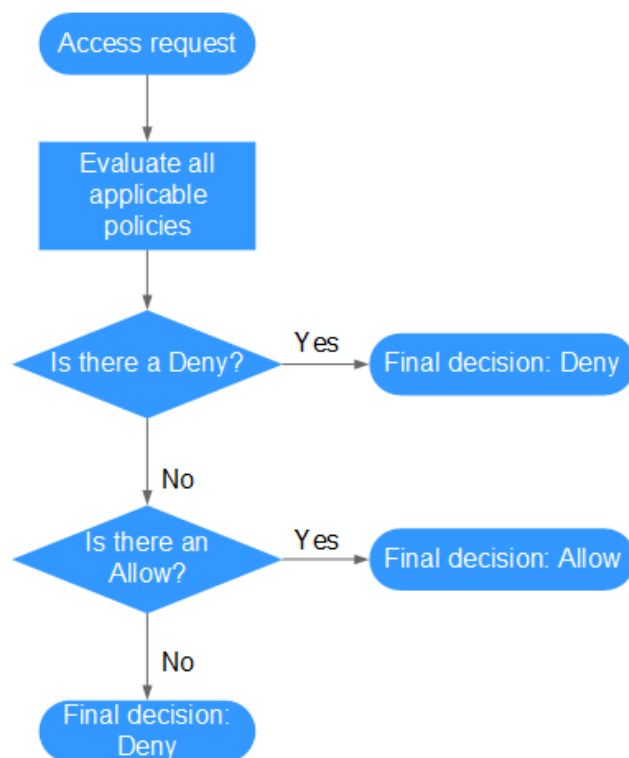
Currently, only certain cloud services support resource-based authorization. For services that do not support this function, you cannot create custom policies containing resource types.



## Authentication Process

IAM authenticates users according to the permissions granted to the users. The following diagram shows the authentication process.

**Figure 3-4** Authentication process



### NOTE

The actions in each policy bear the OR relationship.

1. A user accesses the system and initiates an operation request.
2. The system evaluates all the permissions policies assigned to the user.
3. The system looks for explicit Deny permissions in these policies. If the system finds an explicit Deny that applies, it returns a decision of Deny, and the authentication ends.
4. If no explicit Deny is found, the system looks for Allow permissions that would apply to the request. If the system finds an explicit Allow permission that applies, it returns a decision of Allow, and the authentication ends.
5. If no explicit Allow permission is found, the system returns a decision of Deny, and the authentication ends.

### 3.3.3 Creating a Custom Policy

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

## Creating a Custom Policy in the Visual Editor

**Step 1** On the IAM console, choose **Policies** in the navigation pane, and click **Create Custom Policy**.

**Step 2** Enter a policy name.

**Step 3** Select **Visual editor**.

**Step 4** 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.

3. Select actions.
4. Select all resources, or select specific resources by specifying their paths.
5. (Optional) Add request conditions by specifying condition keys, operators, and values.

**Table 3-2** Condition parameters

Name	Description
Condition Key	A key in the <b>Condition</b> element of a statement. There are global and service-level condition keys. Global condition keys (starting with <b>g:</b> ) are available for operations of all services, while service-level condition keys (starting with a service abbreviation name such as <b>obs:</b> ) are available only for operations of the corresponding service.
Operator	Used together with a condition key 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.

**Step 5** (Optional) Switch to the JSON view and modify the policy content in the JSON format.

 **NOTE**

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

**Step 6** (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 7** (Optional) Enter a brief description for the policy.

**Step 8** Click **OK**.

**Step 9** Attach the policy to a user group. Users in the group then inherit the permissions defined in the policy.

----End

## Creating a Custom Policy in JSON View

**Step 1** On the IAM console, choose **Policies** in the navigation pane, and click **Create Custom Policy**.

**Step 2** Enter a policy name.

**Step 3** Select **JSON**.

**Step 4** (Optional) Click **Select Existing Policy**, and select a policy to use it as a template, such as **VPC Admin**.

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

**Step 6** Modify the statement in the template.

- **Effect:** Set it to **Allow** or **Deny**.
- **Action:** Enter the actions provided in the API actions table of the EVS service, for example, **evs:volumes:create**.

### NOTE

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

**Step 7** (Optional) Enter a brief description for the policy.

**Step 8** Click **OK**. If the policy list is displayed, the policy is created successfully.

**Step 9** Attach the policy to a user group. Users in the group then inherit the permissions defined in the policy.

----End

## 3.3.4 Custom Policy Use Cases

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

Use the following method to assign permissions of the **FullAccess** policy to a user but also forbid the user from accessing CTS. Create a custom policy for denying access to the service, and attach the two policies to the group to which the user belongs. Then, the user will be able to perform all operations on all services except CTS.

Example policy denying access 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

- Use the following method to assign permissions of the **ECS FullAccess** policy to a user but also forbid the user from deleting ECSs. Create a custom policy denying the **ecs:cloudServers:delete** action, and attach this custom policy together with the system-defined **ECS FullAccess** policy to the group to which the user belongs. Then, the user will be able to perform all operations on ECS except deleting ECSs.

Example policy denying ECS deletion:

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ecs:cloudServers:delete"
      ]
    }
  ]
}
```

- Use the following method to assign permissions of the **OBS ReadOnlyAccess** policy to all IAM users but also forbid certain users from viewing specific resources, for example, forbidding users whose names start with **TestUser** from viewing buckets whose names start with **TestBucket**. Create a custom policy for denying the operation, and attach both the **OBS ReadOnlyAccess** policy and the custom policy to the groups to which the users belong. Then, the users will be able to view only buckets whose names do not start with **TestBucket**.

Example policy forbidding 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": {
        "StringStartsWith": {
          "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

To grant permissions for accessing specific services, 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, Application Operations Management (AOM), and ELB.

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

- 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, AOM, and ELB.

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

```
{
  "Action": [
    "ecs:*:*",
    "evs:*:*",
    "vpc:*:*",
    "aom:*:*",
    "elb:*:*"
  ],
  "Effect": "Deny"
}
```

## 3.4 Account Settings

Users with **Security Administrator** permissions can configure a login authentication policy, API password policy, and ACL to keep your user information and system secure.

### Procedure

**Step 1** Set the login authentication policy.

1. In the navigation pane, choose > **Login Authentication Policy**.
2. In the **Account Lockout** area, enter the idle duration, maximum number of invalid login attempts, and lockout duration.

If the number of login attempts reaches the specified upper limit within the specified duration, the user will be locked for a period of time. For example, if a user fails to log in for 3 consecutive times within 10 minutes, the user will be locked for 15 minutes. The user can log in again after 15 minutes.

3. In the **Account Disabling** area, select **Disable account upon login if it is not used within the validity period**, and set the user validity period. If the user does not access the cloud platform through the management console or APIs within the validity period, the user will be disabled.

The account disabling setting is for security purposes. If a user is disabled, resources in the account will not be affected and the user can contact the administrator to enable the user again.

4. In the **Session Timeout** area, set the session timeout that will apply if you or users created using your account do not perform any operations within a specific period. The timeout ranges from 15 minutes to 24 hours, and the default value is 15 minutes. If a user does not perform any operation within the specified duration, the user needs to log in again.

5. In the **Recent Login Information** area, select **Display last login information upon successful login**.

Users will be able to view the login information, such as the time of the last login, on the **Login Verification** page.

6. In the **Custom Information** area, set custom information that will be displayed upon successful login.

Users will be able to view this custom information on the **Login Verification** page.

7. Click **Save**.

**Step 2** Set the password policy.

1. In the navigation pane, choose > **Password Policy**.
2. In the **Password Composition & Reuse** area, do as follows:

- Set **Minimum Number of Characters**.

 **NOTE**

By default, a password must contain at least 6 characters.

- Select **Restrict consecutive identical characters** and set the maximum number of consecutive identical characters that can be contained in a password. The value ranges from 1 to 32.
  - Select **Disallow previously used passwords** and set the number of recent passwords disallowed. The value ranges from 1 to 10.
3. In the **Password Expiration** area, select **Prompt password change 15 days before expiration and force password change upon expiration**, and set the password validity period.

Users must change their password when the password has expired.

 **NOTE**

The password must meet the following requirements:

- Must contain 6 to 32 characters.
  - Must contain at least two types of the following: uppercase letters, lowercase letters, digits, and special characters (~`!?,;,:-'"(){}[]/<>@#\$\$%^&\*+|\= and spaces).
  - 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**.
  - Cannot contain the user's mobile number or email address.
4. In the **Minimum Password Age** area, select **Allow a password to be changed only after it is used for a specified time** and set the minimum password age.
- Users can change their password only when the specified period has expired.
5. Click **Save**.

**Step 3** Set the ACL.

1. In the navigation pane, choose > **ACL**.
2. On the **ACL** page, enter the allowed IP address ranges or IPv4 CIDR blocks.
  - **IP Address Ranges**: only allow users to access the system using IP addresses in specified ranges.
  - **IPv4 CIDR Blocks**: only allow users of specified IPv4 CIDR blocks to access the system. For example: **10.10.10.10/32**.

 **NOTE**

- The ACL takes effect only for users under your account.
- You can click **Restore Defaults** to restore the allowed IP address ranges to the default value, **0.0.0.0-255.255.255.255**, and to clear **IPv4 CIDR Blocks**.
- If both **IP Address Ranges** and **IPv4 CIDR Blocks** are set, users are allowed to access the system if their IP address meets the conditions specified by either of the two parameters.

3. Click **Save**.

----End

## 3.5 Projects

Projects are used to group and isolate OpenStack resources, including compute, storage, and network resources. A project can be a department or a project team. Resources in your account must be managed under projects. As a security administrator, you can access IAM, and create projects in a region to manage resources.

### Procedure

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

**Step 2** On the **Projects** page, click **Create Project**.

**Step 3** On the **Create Project** page, select a region from the **Region** drop-down list.

**Step 4** Set **Project Name**.

#### NOTE

- The project name format is *Region Name\_Project Name*. *Region Name* cannot be modified.
- The project name can only contain letters, digits, hyphens (-), and underscores (\_). The length of *Region Name\_Project Name* cannot exceed 64 characters.

**Step 5** (Optional) Enter a description for the project.

**Step 6** Click **OK**.

The project list is displayed, and the newly created project is in the **Normal** state.

----End

### Follow-Up Procedure

Assigning permissions for a specific project

In the **Group Permissions** area on the **Modify User Group** page, locate the row that contains the target project, and click **Attach Policy**. In the displayed dialog box, select the required permission sets for the project. For details, see [Creating a User Group and Assigning Permissions](#).

### Related Operations

- Viewing project details
  - a. View the projects of the corresponding region in the project list.
  - b. Click **View** in the **Operation** column of the row that contains the target project.  
View project details and the users bound to the project.



 NOTE

After you add a user to a user group that has been granted permissions for a specific project, the user inherits permissions of the group and is associated with the project. The user can switch to this project to access resources in it.

- c. Click **View Permissions** in the **Operation** column of the user permission list.

View the permissions of the user for the project.

- Modifying project information
  - a. In the project list, expand the region where the target project resides.
  - b. Click **Modify** in the **Operation** column of the row that contains the target project. In the displayed **Modify Project** dialog box, modify **Project Name** and **Description**.

 NOTE

The project name format is *Region Name\_Project Name*. *Region Name* cannot be modified.

- Deleting a project
  - a. Click **Delete** in the row that contains the project you want to delete.

 NOTE

Only subprojects created in a region can be deleted. The default project of the region cannot be deleted.

- b. Enter the password and verification code.
- c. Click **Yes**.

In the project list, the status of the project changes to **Deleting**.

 NOTE

After resources in the project are deleted, the project is deleted completely.

- For details about how to switch between projects, see [Switching Projects or Regions](#).

## 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.

- Step 1** (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.

**Step 2** 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.

----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 or 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.

**Step 3** Enter an agency name.

**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 [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 [Managing IAM Users and Permissions](#).
- Agencies cannot be assigned the **Security Administrator** role. For account security purposes, only grant the required permissions to the agency based on the principle of least privilege (PoLP).

**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 .
5. 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. Select **Management console access** for **Access Type** and then select **Set by user** for **Credential Type**.
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. The IAM users that are granted agency permissions can switch to the delegating account and manage resources under the account based on the granted permissions.

## Prerequisites

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

## Procedure

- Step 1** Log in to the console using your account or log in as the IAM user created in [Step 2](#).

 **NOTE**

The IAM user created in [Step 2](#) of [\(Optional\) 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**.

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

 **NOTE**

After you enter the 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

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**
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 .
- Step 2** On the IAM console, choose **Agencies** from the navigation pane, and click **Create Agency**.
- Step 3** Enter an agency name.
- 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 **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.

#### 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**.

# 3.7 Identity Providers

## 3.7.1 Introduction

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

### Basic Concepts

**Table 3-3** 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 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 , is a service provider.
Identity federation	Identity federation is the process of 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 , users in the enterprise management system can use their existing accounts and passwords to access through the login link in the enterprise management system.

Concept	Description
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 <a href="#">SAML 2.0 Technical Overview</a> . implements identity federation in compliance with SAML 2.0. To successfully federate your enterprise users with , ensure that your enterprise IdP is compatible with this protocol.

### Advantages of Identity Federation

- Easy identity management  
With an identity provider, the administrator can manage workforce identities outside of and give these external workforce identities permissions to use resources on .
- Simplified operations  
Workforce users can use their existing accounts in the enterprise to access through SSO.

### Precautions

- Ensure that your enterprise IdP server and 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 as virtual identities, so their access to 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.

## 3.7.2 Application Scenarios of Virtual User SSO and IAM User SSO

IAM supports two SSO types: virtual user SSO and IAM user SSO. This section describes the two SSO types and their differences, helping you to choose an appropriate type for your business.

## Virtual User SSO

After a federated user logs in to , the system automatically creates a virtual user and assigns permissions to the user based on identity conversion rules. Virtual user SSO is recommended if:

- To reduce management costs, you do not want to create and manage IAM users on the cloud platform.
- You want to assign permissions for cloud resources based on the user groups or attributes in your local enterprise IdP. Permission changes in the local enterprise IdP can be synchronized to the cloud platform by adjusting the user groups or attributes locally.
- Your enterprise has branches and may require multiple enterprise IdPs. These IdPs need to access the same account. You need to configure multiple IdPs in for identity federation.

## IAM User SSO

After a federated user logs in to , 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. IAM user SSO is recommended if:

- The cloud products you use do not support virtual user SSO.
- You do not need virtual user SSO and want to simplify the IdP configuration.

## Differences Between Virtual User SSO and IAM User SSO

The differences between virtual user SSO and IAM user SSO are described as follows:

1. Identity conversion: Virtual user SSO uses **identity conversion rules** while IAM user SSO uses external identity IDs for identity conversion. An IdP user will be mapped to an IAM user if the **IAM\_SAML\_Attributes\_xUserId** value of the IdP user is the same as the external identity ID of the IAM user. When you use IAM user SSO, make sure that you have set **IAM\_SAML\_Attributes\_xUserId** in the IdP and **External Identity ID** in the SP to the same value.
2. User identity in IAM: In virtual user SSO, the IdP user does not have a corresponding IAM user in the IAM user list. After the IdP user logs in, the system automatically creates a virtual user for it. In IAM user SSO, the IdP user has a IAM user mapped by external identity ID on the IAM console.
3. Permissions assignment in IAM: In virtual user SSO, the permissions of the IdP user are defined by the identity conversion rule. In IAM user SSO, the IdP user inherits the permissions of the user group which the mapped IAM user belongs to.

## 3.7.3 Virtual User SSO via SAML

### 3.7.3.1 Overview of Virtual User SSO via SAML

supports identity federation with Security Assertion Markup Language (SAML), which is an open standard that many identity providers (IdPs) use. During identity federation, functions as a service provider (SP) and enterprises function as IdPs.



This section describes how to configure identity federation and how identity federation works.

---

**⚠ CAUTION**

Ensure that your enterprise IdP supports SAML 2.0.

---

## Configuring Identity Federation

The following describes how to configure your enterprise IdP and to trust each other.

1. **Create an IdP entity and establish a trust relationship:** Create an IdP entity for your enterprise on . Then, upload the metadata file to the enterprise IdP, and upload the metadata file of the enterprise IdP to .
2. **Configure the enterprise IdP:** Configure enterprise IdP parameters to determine what information can be sent to .
3. **Configure identity conversion rules:** Configure identity conversion rules to determine the IdP user identities and permissions on .
4. **Verify the federated login:** Check whether the enterprise user can log in to through SSO.
5. **(Optional) Configure a federated login entry:** Configure the login link (see ) in the enterprise IdP to allow enterprise users to be redirected to from your enterprise management system.

## How Identity Federation Works

shows the identity federation process between an enterprise management system and .

**📖 NOTE**

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

As shown in , the process of identity federation is as follows:

1. A user opens the login link generated after the IdP creation in the browser. The browser sends an SSO request to .
2. authenticates the user against the metadata file of the enterprise IdP and constructs 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. After the enterprise IdP authenticates the user's identity, it constructs a SAML assertion containing the user details and sends the assertion to the browser as a SAML response.
5. The browser responds and forwards the SAML response to .
6. parses the assertion in the SAML response, identifies the IAM user group mapping to the user based on the identity conversion rules, and issues a token to the user.

7. The SSO login is successful.

 **NOTE**

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

### 3.7.3.2 Step 1: Create an IdP Entity

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

#### Prerequisites

You have read the documentation of the enterprise IdP or have 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 metadata file of to the enterprise IdP, see the IdP help documentation.

#### Establishing a Trust Relationship Between the Enterprise IdP and

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

- Step 1** Upload the metadata file to the enterprise IdP server. For details, see the help documentation of the enterprise IdP.
- Step 2** Obtain the metadata file of the enterprise IdP. For details, see the help documentation of the enterprise IdP.

----End

#### Creating an IdP Entity on

To create an IdP entity on the IAM console, do as follows:

- Step 1** Log in to the , 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 3-4** 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. supports SAML and OpenID Connect protocols. For details about OpenID Connect-based identity federation, see <a href="#">Virtual User SSO via OpenID Connect</a> .

Parameter	Description
SSO Type	IdP type. An account can have only one type of IdP. The following describes the virtual user type. Virtual user SSO: After a federated user logs in to , the system automatically creates a virtual user for the federated user. An account can have multiple IdPs of the virtual user type.
Status	IdP status. The default value is <b>Enabled</b> .

**Step 3** Click **OK**.

----End

## Configuring the Metadata File of the Enterprise IdP on

To configure the metadata file of the enterprise IdP in , 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 successfully.

### NOTE

For details about how to obtain the metadata file of an enterprise IdP, see the help documentation of the enterprise IdP.

- **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.
  - 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	Mandatory	Description
Entity ID	Yes	The unique identifier of an IdP. Enter the value of <b>entityID</b> displayed in the enterprise IdP's metadata file.  If the metadata file contains multiple IdPs, choose the one you want to use.
Protocol	Yes	Protocol used for identity federation between an enterprise IdP and SP.  The protocol is selected by default.
NameIdFormat	No	Enter the value of <b>NameIdFormat</b> 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.  If you configure multiple values, uses the first value by default.
Signing Certificate	Yes	Enter the value of <b>&lt;X509Certificate&gt;</b> 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.  If you configure multiple values, uses the first value by default.
SingleSignOnService	Yes	Enter the value of <b>SingleSignOnService</b> displayed in the IdP metadata file.  This parameter defines how SAML requests are sent during SSO. It must support HTTP Redirect or HTTP POST.  If you configure multiple values, uses the first value by default.

Parameter	Mandatory	Description
SingleLogoutService	No	Enter the value of <b>SingleLogoutService</b> 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.  If you configure multiple values, uses the first value by default.

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

**Figure 3-5** Metadata file of an enterprise IdP

```
<EntityDescriptor xmlns="urn:oasis:names:iso:15958-2" id="idp" xsi:type="urn:oasis:names:iso:15958-2:IDPEntityDescriptor">
  <EntityDescriptor xmlns="urn:oasis:names:iso:15958-2" id="idp" xsi:type="urn:oasis:names:iso:15958-2:IDPEntityDescriptor">
    <KeyDescriptor use="signature">
      <KeyInfo xmlns="urn:oasis:names:iso:15958-2" use="signature">
        <X509Data>
          <X509Certificate href="#idp-cert" type="certificate" />
        </X509Data>
      </KeyInfo>
    </KeyDescriptor>
    </EntityDescriptor>
    <SingleLogoutService binding="urn:oasis:names:iso:15958-2:binding:HTTP-POST" location="https://idp.example.com/oidc/logout" />
    <SingleLogoutService binding="urn:oasis:names:iso:15958-2:binding:HTTP-POST" location="https://idp.example.com/oidc/logout" />
    <Attribute xmlns="urn:oasis:names:iso:15958-2" name="idp:assertion" type="boolean" />
    <Attribute xmlns="urn:oasis:names:iso:15958-2" name="idp:assertion" type="boolean" />
    <Attribute xmlns="urn:oasis:names:iso:15958-2" name="idp:assertion" type="boolean" />
    <Attribute xmlns="urn:oasis:names:iso:15958-2" name="idp:assertion" type="boolean" />
  </EntityDescriptor>
</EntityDescriptor>
```

c. Click **OK**.

## Related Operations

- Viewing IdP information: In the IdP list, click **View** in the row containing the IdP, and view its basic information, metadata configuration, 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 the enterprise IdP: Configure enterprise IdP parameters to determine what information can be sent to .
- Configure identity conversion rules: In the **Identity Conversion Rules** area, configure identity conversion rules to establish a mapping between enterprise users and IAM user groups. In this way, enterprise users can obtain the

corresponding permissions in . For details, see [Step 3: Configure Identity Conversion Rules](#).

- Verify the federated login: Check whether the enterprise user can log in to through SSO. For details, see [Step 4: Verify the Federated Login](#).

### 3.7.3.3 Step 2: Configure the Enterprise IdP

You can configure parameters in the enterprise IdP to determine what information will be sent to . authenticates the federated identity and assigns permissions based on the received information and identity conversion rules.

## Common Parameters in an Enterprise IdP

**Table 3-5** Common parameters in an enterprise IdP

Parameter	Description	Scenario
IAM_SAML_Attributes_redirected_url	Target URL which the federated user will be redirected to	During SSO login, the federated user will be redirected to a .
IAM_SAML_Attributes_domain_id	Account ID of to be federated with the enterprise IdP	This parameter is mandatory in the enterprise IdP-initiated federation.
IAM_SAML_Attributes_idp_id	Name of the IdP entity created on	This parameter is mandatory in the enterprise IdP-initiated federation.

### 3.7.3.4 Step 3: Configure Identity Conversion Rules

After an enterprise IdP user logs in to , authenticates the identity and assigns permissions to the user based on the identity conversion rules. You can customize identity conversion rules based on your service requirements. If you do not configure identity conversion rules, the username of the federated user on is **FederationUser** by default, and the federated user can only access by default.

You can configure the following parameters for federated users:

- Username: Usernames of federated users in .
- User permissions: Permissions assigned to federated users in . You need to map the federated users to IAM user groups. In this way, the federated users can obtain the permissions of the user groups to use resources. Ensure that user groups have been created. For details about how to create a user group, see [Creating a User Group and Assigning Permissions](#).

#### NOTE

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

## Prerequisites

- The enterprise administrator has created an account in , and has created user groups and assigned permissions to the group in IAM. For details, see [Creating a User Group and Assigning Permissions](#).
- An IdP has been created in . For details, see [Step 1: Create an IdP Entity](#).

## Procedure

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

- **Creating Rules**
  - a. Log in to the as the administrator. In the navigation pane, choose **Identity Providers**.
  - 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 3-6** Parameter description

Parameter	Description	Remarks
Username	Username of federated users in .	<p>To distinguish federated users from , it is recommended that you set the username to <b>FederationUser-IdP_XXX</b>. <i>IdP</i> indicates an IdP name, for example, AD FS or Shibboleth. <i>XXX</i> indicates a custom name.</p> <p><b>NOTICE</b></p> <ul style="list-style-type: none"> <li>• The username of each federated user must be unique in the same IdP. Federated users with the same usernames in the same IdP will be mapped to the same IAM user in .</li> <li>• 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</li> </ul>
User Groups	User groups which the federated users belong to in .	The federated users will inherit permissions from the groups to which they belong. You can select a user group that has already been created.

Parameter	Description	Remarks
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 . You can create a maximum of 10 conditions for an identity conversion rule.</p> <p>The <b>Attribute</b> and <b>Value</b> parameters are used for the enterprise IdP to transfer user information to through SAML assertions. The <b>Condition</b> parameter can be set to <b>empty</b>, <b>any_one_of</b>, or <b>not_any_of</b>. For details about these parameters, see <a href="#">Syntax of Identity Conversion Rules</a>.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>• An identity conversion rule can have multiple conditions. It takes effect only if all of the conditions are met.</li> <li>• An IdP can have multiple identity conversion rules. If a federated user does not meet any of the conditions, the user will be denied to access .</li> </ul>

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 as the administrator. In the navigation pane, choose **Identity Providers**.
    - 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 [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.

## 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](#).

### 3.7.3.5 Step 4: Verify the Federated Login


#### Verifying the Federated Login

Federated users can initiate a login from the IdP or SP.

- Initiating a login from an IdP, for example, Microsoft Active Directory Federation Services (AD FS) or Shibboleth.
- Initiating a login from the SP. You can obtain the login link from the IdP details page on the IAM console.

The IdP-initiated login method depends on the IdP. For details, see the IdP help documentation. This section describes how to initiate a login from the SP.

**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. Click  to copy the login link displayed in the **Basic Information** area, 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.

----End

#### Redirecting to a Specified Region or Service

You can specify the target page which the federated user will be redirected to after login.

- Configuring the login link on the SP  
Combine the login link obtained from the console with the specified URL using the format **Login link&service=Specified URL**.
- Configuring the login link on the IdP  
Configure **IAM\_SAML\_Attributes\_redirect\_url** (the URL to be redirected to) in the SAML assertion of the enterprise IdP.

### 3.7.3.6 (Optional) Step 5: Configure a Federated Login Entry in the Enterprise IdP

Configure a federated login entry in the enterprise IdP so that enterprise users can use the login link to access .

## Prerequisites

- An IdP entity has been created on . For details about how to create an IdP entity, see [Step 1: Create an IdP Entity](#).
- The login entry for logging in to has been configured in the enterprise management system.

## Procedure

**Step 1** Log in to the . In the navigation pane, choose **Identity Providers**.

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

**Step 3** Copy the login link by clicking  in the **Login Link** row.

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

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

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

----End

## 3.7.4 IAM User SSO via SAML

### 3.7.4.1 Overview of IAM User SSO via SAML

supports identity federation with Security Assertion Markup Language (SAML), which is an open standard that many identity providers (IdPs) use. During identity federation, functions as a service provider (SP) and enterprises function as IdPs. SAML-based federation enables single sign-on (SSO), so employees in your enterprise can log in to as IAM users.

This section describes how to configure identity federation and how identity federation works.



Ensure that your enterprise IdP supports SAML 2.0.

---

## Configuring Identity Federation

The following describes how to configure your enterprise IdP and to trust each other.

1. **Create an IdP entity and establish a trust relationship:** Create an IdP entity for your enterprise on . Then, upload the metadata file to the enterprise IdP, and upload the metadata file of the enterprise IdP to .
2. **Configure the enterprise IdP:** Configure enterprise IdP parameters to determine what information can be sent to .
3. **Configure an external identity ID:** Establish a mapping between an IAM user and an enterprise user. When your enterprise IdP establishes SSO access to ,

the enterprise user can log in to as the IAM user with the specified external identity ID. For example, if an enterprise user **IdP\_Test\_User** is mapped to the IAM user **Alice**, the enterprise user **IdP\_Test\_User** will log in to as the IAM user **Alice**.

4. **Verify the federated login:** Check whether the enterprise user can log in to through SSO.
5. **(Optional) Configure a federated login entry:** Configure the login link (see ) in the enterprise IdP to allow enterprise users to be redirected to from your enterprise management system.

## How Identity Federation Works

shows the identity federation process between an enterprise management system and .

### NOTE

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

As shown in , the process of identity federation is as follows:

1. A user opens the login link generated after the IdP creation in the browser. The browser sends an SSO request to .
2. authenticates the user against the metadata file of the enterprise IdP and constructs 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. After the enterprise IdP authenticates the user's identity, it constructs a SAML assertion containing the user details and sends the assertion to the browser as a SAML response.
5. The browser responds and forwards the SAML response to .
6. parses the assertion in the SAML response, identifies the IAM user group mapping to the user based on the identity conversion rules, and issues a token to the user.
7. The SSO login is successful.

### NOTE

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

### 3.7.4.2 Step 1: Create an IdP Entity

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

## Establishing a Trust Relationship Between the Enterprise IdP and

Configure the metadata file of on the enterprise IdP to establish a trust.

- Step 1** Upload the metadata file to the enterprise IdP server. For details, see the help documentation of the enterprise IdP.

**Step 2** Obtain the metadata file of the enterprise IdP. For details, see the help documentation of the enterprise IdP.

----End

## Creating an IdP Entity on

To create an IdP entity on the IAM console, do as follows:

**Step 1** Log in to the , 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 3-7** 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. supports SAML and OpenID Connect protocols. For details about OpenID Connect-based identity federation, see <a href="#">Virtual User SSO via OpenID Connect</a> .
SSO Type	IdP type. An account can have only one type of IdP. The following describes the IAM user type. IAM user SSO: After a federated user logs in to , 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 <a href="#">Creating a User</a> .
Status	IdP status. The default value is <b>Enabled</b> .

**Step 3** Click **OK**.

----End

## Configuring the Metadata File of the Enterprise IdP on

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 successfully.

### NOTE

For details about how to obtain the metadata file of an enterprise IdP, see the help documentation of the enterprise IdP.

- **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.
  - 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** to save the settings.
- **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 <b>entityID</b> displayed in the enterprise IdP's metadata file. If the metadata file contains multiple IdPs, choose the one you want to use.
Protocol	Yes	Protocol used for identity federation between an enterprise IdP and SP. The protocol is selected by default.
NameldFormat	No	Enter the value of <b>NameldFormat</b> 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. If you configure multiple values, uses the first value by default.
Signing Certificate	Yes	Enter the value of <b>&lt;X509Certificate&gt;</b> 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. If you configure multiple values, uses the first value by default.

Parameter	Man datory	Description
SingleSignOnService	Yes	Enter the value of <b>SingleSignOnService</b> displayed in the IdP metadata file.  This parameter defines how SAML requests are sent during SSO. It must support HTTP Redirect or HTTP POST.  If you configure multiple values, uses the first value by default.
SingleLogoutService	No	Enter the value of <b>SingleLogoutService</b> 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.  If you configure multiple values, uses the first value by default.

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

**Figure 3-6** Metadata file of an enterprise IdP

```
<EntityDescriptor xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns="urn:oasis:names:specification:saml:2.0:metadata"
  <SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:specification:saml:2.0:protocol"
    <IDPSSODescriptor xmlns="urn:oasis:names:specification:saml:2.0:protocol"
      <SingleSignOnService Location="https://example.com/saml/2.0/SSO"
        <SingleLogoutService Location="https://example.com/saml/2.0/SLO"
          <Attribute xmlns="urn:oasis:names:specification:saml:2.0:attribute"
            </EntityDescriptor>
</EntityDescriptor>
```

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

### 3.7.4.3 Step 2: Configure the Enterprise IdP

You can configure parameters in the enterprise IdP to determine what information will be sent to . authenticates the federated identity and assigns permissions based on the received information.

**NOTE**

If the SSO type is IAM user, the enterprise IdP must have the **IAM\_SAML\_Attributes\_xUserId** assertion configured.

## Common Parameters in an Enterprise IdP

**Table 3-8** Common parameters in an enterprise IdP

Parameter	Description	Scenario
IAM_SAML_Attributes_xUserId	ID of an enterprise IdP user (federated user)	This parameter is mandatory when the SSO type is IAM user. Each federated user is mapped to an IAM user. The <b>IAM_SAML_Attributes_xUserId</b> of the federated user is the same as the external identity ID of the corresponding IAM user.
IAM_SAML_Attributes_redirected_url	Target URL which the federated user will be redirected to	During SSO login, the federated user will be redirected to .
IAM_SAML_Attributes_domain_id	Account ID of to be federated with the enterprise IdP	This parameter is mandatory in the enterprise IdP-initiated federation.
IAM_SAML_Attributes_idp_id	Name of the IdP entity created on	This parameter is mandatory in the enterprise IdP-initiated federation.

### 3.7.4.4 Step 3: Configure an External Identity ID

For the IAM user SSO type, you must configure an external identity ID for the IAM user which the federated user maps to on . The external identity ID must be the same as the **IAM\_SAML\_Attributes\_xUserId** value of the enterprise IdP user (federated user). You can create an IAM user and configure an external identity ID for it, or change the external identity ID of an existing IAM user.

- [Creating an IAM User and Configuring an External Identity ID](#)
- [Changing the External Identity ID of an Existing IAM User](#)

### Creating an IAM User and Configuring an External Identity ID

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

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

**Step 3** In the **User Details** area, configure an external identity ID. For details about other settings, see [Creating a User](#).

----End

## Changing the External Identity ID of an Existing IAM User

In the IAM user list, click a username or choose **More > Security Settings** in the row containing the user and change the external identity ID.

### 3.7.4.5 Step 4: Verify the Federated Login


#### Verifying the Federated Login

Federated users can initiate a login from the IdP or SP.

- Initiating a login from an IdP, for example, Microsoft Active Directory Federation Services (AD FS) or Shibboleth.
- Initiating a login from the SP (the cloud platform). You can obtain the login link from the IdP details page on the IAM console.

The IdP-initiated login method depends on the IdP. For details, see the IdP help documentation. This section describes how to initiate a login from the SP.

##### 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. Click  to copy the login link displayed in the **Basic Information** area, open the link using a browser, and then enter the username and password used in the enterprise management system.

##### Step 2 Check whether the federated user is logging in as an IAM user.

----End

#### Redirecting to a Specified Region or Service

You can specify the target page which the federated user will be redirected to after login.

- Configuring the login link on the SP  
Combine the login link obtained from the console with the specified URL using the format **Login link&service=Specified URL**.
- Configuring the login link on the IdP  
Configure **IAM\_SAML\_Attributes\_redirect\_url** (the URL to be redirected to) in the SAML assertion of the enterprise IdP.

### 3.7.4.6 (Optional) Step 5: Configure a Federated Login Entry in the Enterprise IdP

Configure a federated login entry in the enterprise IdP so that enterprise users can use the login link to access .

#### Prerequisites

- An IdP entity has been created on , and the login link for the IdP is available. For details, see [Step 1: Create an IdP Entity](#).




- The login entry for logging in to has been configured in the enterprise management system.

## Procedure

**Step 1** Log in to the . In the navigation pane, choose **Identity Providers**.

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

**Step 3** Copy the login link by clicking  in the **Login Link** row.

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

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

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

----End

## 3.7.5 Virtual User SSO via OpenID Connect

### 3.7.5.1 Overview of Virtual User SSO via OpenID Connect

This section describes how to configure identity federation and how identity federation works.

## Configuring Identity Federation

The following describes how to configure your enterprise IdP and to trust each other.

1. **Create an IdP entity and establish a trust relationship:** Create OAuth 2.0 credentials in the enterprise IdP. On , create an IdP entity and establish a trust relationship between the two systems.
2. **Configure identity conversion rules:** Configure identity conversion rules on to map the users, user groups, and permissions in the enterprise IdP to .
3. **Configure a federated login entry:** Configure the login link in the enterprise IdP to allow enterprise users to be redirected to from your enterprise management system.

## How Identity Federation Works

shows the identity federation process between an enterprise management system and .

The process of identity federation is as follows:

1. A user opens the login link obtained from the IAM console in the browser. The browser sends an SSO request to .
2. authenticates the user against the configuration of the enterprise IdP and constructs an OpenID Connect request to the browser.
3. The browser forwards the OpenID Connect 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 OpenID Connect response to .
6. parses the ID token in the OpenID Connect response, identifies the IAM user group mapping to the user based on the identity conversion rules, and issues a token to the user.
7. The SSO login is successful.

### 3.7.5.2 Step 1: Create an IdP Entity

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

#### Prerequisites

- The enterprise administrator has created an account in , and has created user groups and assigned them permissions in IAM. For details, see [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 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 <https://authui/oidc/redirect> and <https://authui/oidc/post> in the enterprise IdP so that users can be redirected to the OpenID Connect IdP in .

**Step 2** Obtain OAuth 2.0 credentials of the enterprise IdP.

----End

### Creating an IdP Entity on

Create an IdP entity and configure authorization information in IAM to establish a trust relationship between the enterprise IdP and IAM

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

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

#### NOTE

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

----End

## Configuring Authorization Information in

**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 3-9** Access type description

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

**Step 3** Specify the configuration information.

**Table 3-10** Configuration information

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

Parameter	Description
Scopes	Scopes of authorization requests. <b>openid</b> is selected by default. This parameter is required only if you set <b>Access Type</b> to <b>Programmatic access and management console access</b> . Enumerated values: <ul style="list-style-type: none"> <li>• openid</li> <li>• email</li> <li>• profile</li> </ul>
Response Type	Response type of authorization requests. The default value is <b>id_token</b> . This parameter is required only if you set <b>Access Type</b> to <b>Programmatic access and management console access</b> .
Response Mode	Response mode of authorization requests. The options include <b>form_post</b> and <b>fragment</b> . <b>form_post</b> is recommended. This parameter is required only if you set <b>Access Type</b> to <b>Programmatic access and management console access</b> .
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 identity provider.
2. Copy the login link displayed on the **Modify Identity Provider** page and visit the link using a browser.
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 management system.
- If the login fails, check the username and password.

 **NOTE**

Federated users can only access by default. To assign permissions to federated users, configure identity conversion rules for the IdP. For details, see [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 configuration, 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 [Step 2: Configure Identity Conversion Rules](#).
- Configure the enterprise management system to allow users to access through SSO. For details, see [\(Optional\) Step 3: Configure Login Link in the Enterprise Management System](#).

### 3.7.5.3 Step 2: Configure Identity Conversion Rules

Federated users are named **FederationUser** by default in . These users can only log in to 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 in .
- Assign permissions to enterprise users to use resources by mapping these users to IAM user groups. Ensure that you have created the required user groups. For details, see [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 which the user belongs to. 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 [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 [Syntax of Identity Conversion Rules](#).

- **Creating Rules**
  - a. Log in to the as the administrator. In the navigation pane, choose **Identity Providers**.
  - 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 3-11** Parameter description

Parameter	Description	Remarks
Username	Username of federated users in .	<p>To distinguish federated users from , it is recommended that you set the username to <b>FederationUser-IdP_XXX</b>. <i>IdP</i> indicates an IdP name, for example, AD FS or Shibboleth. <i>XXX</i> indicates a custom name.</p> <p><b>NOTICE</b></p> <ul style="list-style-type: none"> <li>• The username of each federated user must be unique in the same IdP. Federated users with the same usernames in the same IdP will be mapped to the same IAM user in .</li> <li>• 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</li> </ul>
User Groups	User groups which the federated users belong to in .	The federated users will inherit permissions from their user groups. You can select a user group that has already been created.
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 . You can create a maximum of 10 conditions for an identity conversion rule.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>• An identity conversion rule can have multiple conditions. It takes effect only if all of the conditions are met.</li> <li>• An IdP can have multiple identity conversion rules. If a federated user does not meet any of the conditions, the user will be denied to access .</li> </ul>

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 as the administrator. In the navigation pane, choose **Identity Providers**.
    - 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 [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. Click  to copy the login link displayed in the **Basic Information** area, 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](#).

### 3.7.5.4 (Optional) Step 3: Configure Login Link in the Enterprise Management System

Configure a federated login entry in the enterprise IdP so that enterprise users can use the login link to access .

#### Prerequisites

- An IdP entity has been created on . For details about how to create an IdP entity, see [Step 1: Create an IdP Entity](#).
- The login entry for logging in to has been configured in the enterprise management system.

#### Procedure

**Step 1** Log in to the . In the navigation pane, choose **Identity Providers**.

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

**Step 3** Copy the login link by clicking  in the **Login Link** row.

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

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

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

----End

## 3.7.6 Syntax of Identity Conversion Rules

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

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

- **remote:** Information about a federated user in the identity provider system. 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 conditions are supported:
  - **empty:** The rule is matched to all claims containing the attribute type. This condition does not need to be specified.
  - **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.
- **local:** Identity information about a federated user mapped to the cloud system. 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.

## Examples of Identity Conversion Rule Conditions

The following examples illustrate how to use the **empty**, **any\_one\_of**, and **not\_any\_of** conditions in an identity conversion rule.

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

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

In this 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 the cloud system, 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.

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

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

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

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

In this 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 the cloud system, that is, *FirstName LastName*. The groups to which the user belongs are the value of the third remote attribute *Groups*.

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

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

- 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**.

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

```

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

```

The username of the federated user in the cloud system 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 identity provider system.

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

```

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

```

The username of the federated user in the cloud system 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 identity provider system.

- 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 system.

```

{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 system.

```

{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.

```

[
  {
    "local": [
      {
        "user": {

```

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

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

- Examples of combined conditions: Multiple conditions can be combined using the logical operator AND.

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

This rule takes effect only for the federated users who do not belong to the **idp\_user** or **idp\_agent** user group in the identity provider system. The username of each applicable federated user is *UserName* in the cloud system

and the user belongs to the **admin** group. 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.

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

```

```
        "type": "Groups",
        "any_one_of": [
          "idp_admin"
        ]
      }
    ]
  }
}
```

In this example, the rules take effect for users in the **idp\_admin** group. The username of each applicable federated user is *UserName* in the cloud system and the user belongs to the **admin** group.

The following assertion indicates that user John Smith is a member of the **idp\_admin** group in the identity provider system and therefore meets the rules. The username of this user will be **John Smith** in the cloud system, and the user will belong to the **admin** group.

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

## 3.8 MFA Authentication and Virtual MFA Device

### 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 perform operations.

MFA authentication can be enabled to verify a user's identity before the user is allowed to log in to the console.

### MFA Authentication Methods

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

### 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) standard. 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.

### Application Scenarios

MFA authentication verifies your identity during login. When you or an IAM user logs in to the console, you and the user need to enter a verification code in addition to the username and password.

## 3.9 Auditing

### 3.9.1 IAM Operations That Can Be Recorded by CTS

**Table 3-12** lists Identity and Access Management (IAM) operations that can be recorded by Cloud Trace Service (CTS).

**Table 3-12** IAM operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Obtaining a token	token	createTokenByPwd
Obtaining a token	token	createTokenByHwAccessKey
Obtaining a token	token	createTokenByToken
Obtaining a token	token	createTokenByAssumeRole
Login	user	login
Login failure	user	loginFailed
Logout	user	logout
Changing the password	user	changePassword
Creating a user	user	createUser
Modifying user information	user	updateUser
Deleting a user	user	deleteUser
Changing the password	user	updateUserPwd
Creating an access key (AK/SK)	user	addCredential
Deleting an access key (AK/SK)	user	deleteCredential
Changing the email address	user	modifyUserEmail
Changing the mobile number	user	modifyUserMobile
Changing the password	user	modifyUserPassword
Uploading a profile picture	user	modifyUserPicture
Changing the password of a user (by the administrator)	user	setPasswordByAdmin
Creating a user group	userGroup	createUserGroup
Updating a user group	userGroup	updateUserGroup
Deleting a user group	userGroup	deleteUserGroup

Operation	Resource Type	Trace Name
Adding a user to a user group	userGroup	addUserToGroup
Removing a user from a user group	userGroup	removeUserFromGroup
Creating a project	project	createProject
Modifying project information	project	updateProject
Changing project status	project	updateProjectStatus
Creating an agency	agency	createAgency
Modifying an agency	agency	updateAgency
Deleting an agency	agency	deleteAgency
Switching the role	user	switchRole
Registering an identity provider	identityProvider	createIdentityProvider
Updating an identity provider	identityProvider	updateIdentityProvider
Deleting an identity provider	identityProvider	deleteIdentityProvider
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
Granting permissions to a user group under a domain	roleGroupDomain	assignRoleToGroupOnDomain
Canceling permissions of a user group under a domain	roleGroupDomain	unassignRoleToGroupOnDomain
Granting permissions to a user group for a project	roleGroupProject	assignRoleToGroupOnProject
Delete permissions of a user group for a project	roleGroupProject	unassignRoleToGroupOnProject



Operation	Resource Type	Trace Name
Updating the login authentication policy	domain	updateSecurityPolicies
Updating the password policy	domain	updatePasswordPolicies
Updating the ACL	domain	updateACLPolicies
Unbinding a virtual MFA device	MFA	UnBindMFA

### 3.9.2 Viewing Audit Logs

After you enable CTS, it records key operations performed on IAM. You can view the operation records of the last 7 days on the CTS console.

#### Viewing IAM Audit Logs

- Step 1** Log in to the management console.
- Step 2** Click **Service List** in the upper part of the page and choose **Cloud Trace Service** under **Management & Deployment**.
- Step 3** In the navigation pane, choose **Trace List**.
- Step 4** Click **Filter** in the upper right corner of the trace list to set filter conditions.

The following filters are available:

- **Trace Source, Resource Type, and Search By**
  - Select a filter criteria from the drop-down list. Specifically, select **IAM** from the **Trace Source** drop-down list.
  - If you select **Trace name** for **Search By**, select a trace name.
  - If you select **Resource ID** for **Search By**, select or enter a resource ID.
  - If you select **Resource name** for **Search By**, select or enter a resource name.
- **Operator:** Select an operator (a user rather than domain).
- **Trace Status:** Available options include **All trace statuses**, **normal**, and **warning**.
- Specify the start time and end time for querying traces.

**Step 5** Click **Query**.

**Step 6** Expand the details of a trace, as shown in **Figure 3-7**.

**Figure 3-7** Expanding trace details

Trace Name	Resource Type	Trace Source	Resource ID	Resource Name	Trace Status	Operator	Recorded	Operation
batchCreateVolume	evs	EVS	--		normal		2021-03-16 15:37:13 GMT+08:00	<a href="#">View Trace</a>
<div style="border: 1px solid #ccc; padding: 5px;"> <p>Trace ID: 6c78de50-...-d0e3</p> <p>Trace Type: ApiCall</p> <p>Source IP Address: ...</p> <p>Generated: 2021-03-16 15:37:13 GMT+08:00</p> </div>								
createVolume	evs	EVS	c32fca8-d97d-4237-8...		normal		2021-03-16 15:37:10 GMT+08:00	<a href="#">View Trace</a>

**Step 7** Click **View Trace** in the **Operation** column. In the **View Trace** dialog box as shown in **Figure 3-8**, the trace details are displayed.

**Figure 3-8** Viewing a trace



----End

# 4 FAQs

---

[How Do I Enable Login Authentication?](#)

[How Do I Bind a Virtual MFA Device?](#)

[How Do I Obtain MFA Verification Codes?](#)

[How Do I Unbind a Virtual MFA Device?](#)

[Why Does IAM User Login Fail?](#)

[How Do I Control IAM User Access to the Console?](#)

[Differences Between IAM and Enterprise Management](#)

[What Are the Differences Between IAM Projects and Enterprise Projects?](#)

[How Can I Obtain Permissions to Create an Agency?](#)

[What Can I Do If Text Box Prompt Information Does Not Disappear?](#)

[How Do I Disable Password Association and Saving on Google Chrome?](#)

[How Do I Grant Cloud Service Permissions in the EU-Paris Region to IAM Users?](#)

[How Do I Obtain an Access Key \(AK/SK\) in the EU-Paris Region?](#)

## 4.1 How Do I Enable Login Authentication?

For account security purposes, you are advised to enable login authentication. After this function is enabled, users need to enter an SMS, MFA, or email verification code on the **Login Verification** page when logging in to the cloud system.

### Prerequisites

Users have bound a mobile number, email address, or **virtual MFA device** to their account.

## Procedure

- Enabling login authentication on the **Modify User** page of the IAM console

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

**Step 2** Click **Modify** in the **Operation** column of the row that contains the target user.

**Step 3** On the **Modify User** page, select a login verification method, and enter the verification code.

**Step 4** Click **OK**.

----End

- Enabling login authentication on the **My Credentials** page

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

**Step 2** On the **My Credentials** page, click **Change** next to **Login Authentication**.

**Step 3** On the **Change Verification Method** page, select a login verification method, and enter the verification code.

**Step 4** Click **OK**.

----End

## 4.2 How Do I Bind a Virtual MFA Device?

MFA authentication provides an additional layer of protection on top of the username and password. If MFA-based login authentication is enabled, you will need to enter a verification code after your username and password are authenticated. Together, these factors make your account and resources more secure.

MFA devices can be based on hardware or software. The cloud system supports only virtual MFA devices.

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

For more information, see [MFA Authentication and Virtual MFA Device](#).

### Prerequisites

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

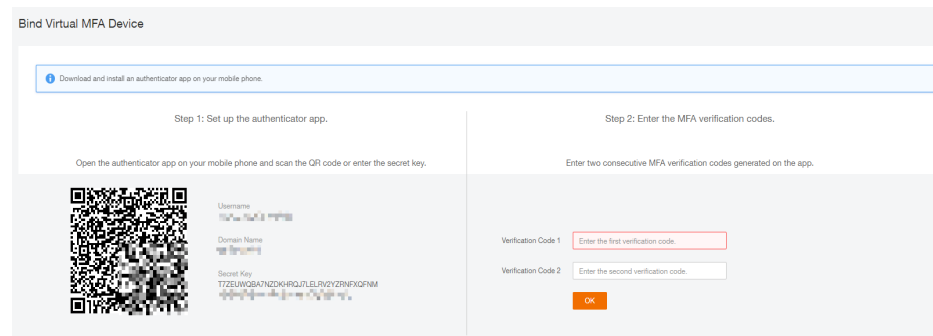
## Procedure

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

**Step 2** On the **My Credentials** page, click **Bind** next to the **Virtual MFA Device** parameter.

**Step 3** Go to the **Bind Virtual MFA Device** page.

**Figure 4-1** Binding a virtual MFA device



**NOTE**

The secret key is a one-time credential that you can use to obtain an MFA verification code. To ensure account security, do not share the secret key with anyone.

**Step 4** Add your account to an MFA application.

- Scanning the QR code  
Open the MFA application on your mobile phone, click the plus sign + on the application, and scan the QR code displayed on the **Bind Virtual MFA Device** page. Your account is then automatically added to the application, with the username and secret key displayed.
- Manually entering the secret key  
Open the MFA application on your mobile phone, click the plus sign + on the application, and manually enter the secret key displayed on the **Bind Virtual MFA Device** page.

**NOTE**

The manual entry function is time-based. Ensure that automatic time setup has been enabled on your mobile phone.

**Step 5** View the verification code on the MFA application. The code is automatically updated every 30 seconds.

**Step 6** On the **Bind Virtual MFA Device** page, enter two consecutive verification codes and click **OK** to bind the virtual MFA device.

----End

## 4.3 How Do I Obtain MFA Verification Codes?

After MFA-based login authentication is enabled, you need to enter an MFA verification code in addition to the username and password when logging in to the console. Open the bound MFA application and view the verification code displayed for your account.

## 4.4 How Do I Unbind a Virtual MFA Device?

You can unbind the virtual MFA device as long as the mobile phone used to bind the MFA device is available and the MFA application is still installed on the phone.

1. On the homepage of the cloud system, click **Console**.
2. Hover the mouse pointer over the username in the upper right corner and choose **My Credentials** from the drop-down list.
3. Click **Unbind** next to **Virtual MFA Device**.
4. Enter the verification code obtained from the virtual MFA device.
5. Click **OK**.

The virtual MFA device is unbound successfully.

## 4.5 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 by the access control rules set by the administrator.

### Troubleshooting

- **Incorrect username or password**
  - a. Possible cause: The domain name or IAM username is incorrect.  
Solution: Enter the correct domain name and IAM username. If you do not know the IAM username or the domain name, contact the administrator.
  - b. Possible cause: The password is incorrect.  
Solution: Enter the correct password (pay attention to letter cases).
  - c. Possible cause: You did not clear the browser cache after changing or resetting the password.  
Solution: Clear the browser cache and log in again.
- **Login from the current device is not allowed by the access control rules set by the administrator.**

Possible cause: The administrator has set access control rules on the IAM console to limit access from 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.

## 4.6 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**. On the displayed page, click **ACL**.

 **NOTE**

The ACL takes effect only for users created using your account.

**Step 3** Click the **ACL** tab, click **Console Access** and set allowed IP address ranges or IPv4 CIDR blocks.

- **IP Address Ranges:** Users can access the console only from specific IP address ranges.
- **IPv4 CIDR Blocks:** Users can access the console only from specific IPv4 CIDR blocks.

For example: **10.10.10.10/32**.

 **NOTE**

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

**Step 4** Click **Save**.

----End

## 4.7 Differences Between IAM and Enterprise Management

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

You can use both IAM and Enterprise Management to manage users and access permissions. Enterprise Management supports more fine-grained authorization for resource usage. It is recommended for medium- and large-sized enterprises.

### Differences Between IAM and Enterprise Management

- Enabling method
  - Identity and Access Management (IAM) is an identity management service on and is free of charge.
  - Enterprise Management is a resource management service on . After registering with the system, .
- Resource isolation
  - Using IAM, you can create multiple projects in a region to isolate resources, and authorize users to access resources in specific projects. For details, see "Projects" in *Identity and Access Management User Guide*.
  - Using Enterprise Management, you can create enterprise projects to isolate resources across regions. Enterprise Management makes it easy

for you to assign permissions for specific cloud resources. For example, you can add an Elastic Cloud Server (ECS) to an enterprise project, and assign permissions to a user to manage this ECS in the project. Then the user can manage only this ECS.

## Relationship Between Enterprise Management and IAM

- The functions of creating users and user groups are the same for IAM and Enterprise Management.
- If you have enabled Enterprise Management, you need to use the policies managed in IAM to assign permissions to user groups created in Enterprise Management. If the system-defined policies cannot meet your requirements, you can create custom policies in IAM. The custom policies will be synchronized to Enterprise Management and can be associated with user groups in both IAM and Enterprise Management.
- If you grant a user group with permissions in both IAM and Enterprise Management, users in the group will inherit permissions from the policies attached to the group in both IAM and Enterprise Management. Requests of these users will then be authenticated based on the actions in the attached policies.

- If the attached policies contain the same action, the action defined in IAM takes precedence. In the following example, the action creating ECSs is allowed in Enterprise Management but denied in IAM, then users are not allowed to create ECSs.

A policy attached in an IAM project contains the following action:

```
{
  "Action": [
    "ecs:cloudServers:create"
  ],
  "Effect": "Deny"
}
```

A policy attached in an enterprise project contains the following action:

```
{
  "Action": [
    "ecs:cloudServers:create"
  ],
  "Effect": "Allow"
}
```

- All different actions in the policies attached in IAM and Enterprise Management will take effect. In the following example, users are allowed to create and delete ECSs.

A policy attached in an IAM project contains the following action:

```
{
  "Action": [
    "ecs:cloudServers:create"
  ],
  "Effect": "Allow"
}
```

A policy attached in an enterprise project contains the following action:

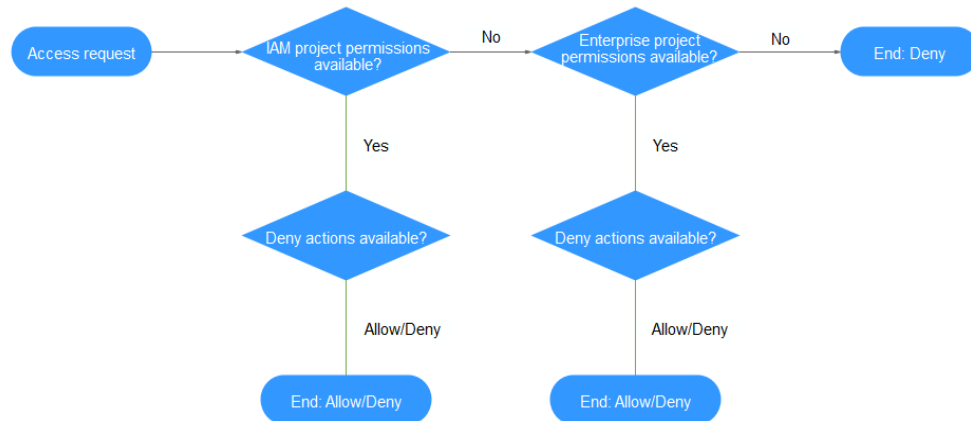
```
{
  "Action": [
    "ecs:cloudServers:delete"
  ],
  "Effect": "Allow"
}
```



## Authentication Process

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

**Figure 4-2** Request authentication process



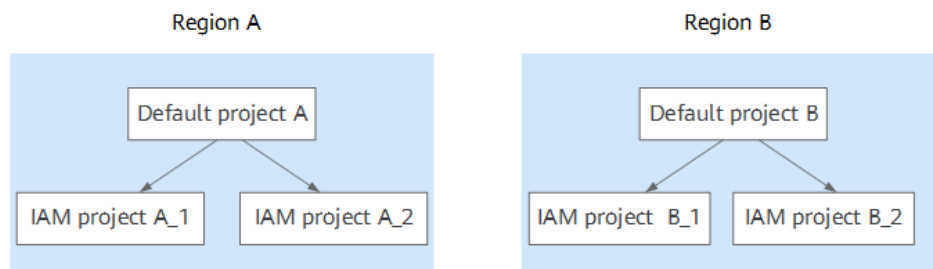
1. A user initiates an access request.
2. The system searches for IAM project permissions and then searches for matched actions in the permissions.
3. If a matched Allow or Deny action is found, the system returns an authentication result (Allow or Deny). Then the authentication is completed.
4. If no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

## 4.8 What Are the Differences Between IAM Projects and Enterprise Projects?

### IAM Projects

Projects are used to group and physically isolate resources in a region. Resources cannot be transferred between IAM projects. They can only be deleted and then provisioned again.

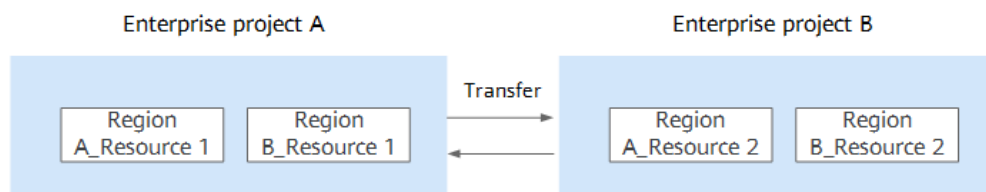
For details about how to use IAM projects, see "Projects" in the *Identity and Access Management User Guide*.



## Enterprise Projects

Enterprise projects 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 resources can be transferred between enterprise projects. Enterprise Management makes it easy for you to assign permissions for specific cloud resources. For example, you can add an Elastic Cloud Server (ECS) to an enterprise project, and assign permissions to a user to manage this ECS in the project. Then the user can manage only this ECS. You cannot create projects in IAM after enabling Enterprise Management.

For details about enterprise projects, see *Enterprise Management User Guide*.



## 4.9 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

- Request the administrator to create an agency. For details, see "Creating an Agency (by a Delegating Party)" in *Identity and Access Management User Guide*.
- Request the administrator to grant the permissions for using IAM.

## 4.10 What Can I Do If Text Box Prompt Information Does Not Disappear?


When you register with or log in to , bind , create a user, or reset or change the password, field-level help, such as "Enter at least 5 characters." is always displayed. This is because you may be using Internet Explorer 8 or an earlier version. You can address this issue using the following methods.

- Upgrade the browser.  
Upgrade to Internet Explorer 9 or later.
- Use another browser.  
Use Mozilla Firefox (version 38.0 or later) or Google Chrome (version 43.0 or later).

## 4.11 How Do I Disable Password Association and Saving on Google Chrome?


When you use Google Chrome to log in to 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. The following 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** Disable **Offer to save passwords** and **Auto Sign-in**.

----End

## Follow-Up Procedure

To delete a saved password record, in the **Saved Passwords** area, click  in the row containing the password record, and select **Remove** from the drop-down list. The records of websites, usernames, and passwords are deleted.

## 4.12 How Do I Grant Cloud Service Permissions in the EU-Paris Region to IAM Users?

### Symptom


The administrator has enabled cloud services in the **EU-Paris** region, and need to authorize IAM users to use cloud services in this region.

Users access cloud services in the **EU-Paris** region as virtual users authorized through federated authentication. They are not real users who exist in the cloud service system, and need to be authorized in Huawei Cloud's default regions and the **EU-Paris** region, respectively.

### Prerequisites

- You have created an IAM user in a default region of Huawei Cloud and added the user to a user group. For example, you have created IAM user **User-001** and added them to user group **UserGroup-001**. For details, see [Creating a User](#) and [Managing IAM Users and Permissions](#) .
- If this is the first time to grant cloud service permissions for IAM users in the **EU-Paris** region, you need to use an account rather than an IAM user with administrator permissions to perform authorization operations.

### Procedure

- Step 1** Log in to Huawei Cloud as an administrator, click  on the console homepage, and select the **EU-Paris** region.
- Step 2** On the console, choose **Management & Governance > Identity and Access Management**.
- Step 3** On the IAM console, choose **User Groups** from the navigation pane, and click **Create User Group** in the upper right corner to create a group with the same name (**UserGroup-001**).
- Step 4** On the **User Groups** page, click **Modify** in the row that contains the user group created in **3**.
- Step 5** In the **Group Permissions** area, click **Attach Policy** in the row that contains the target region for user authorization, select desired permissions, and click **OK**.  
The permissions assigned to this group will also apply to IAM users in the user group in Huawei Cloud.
- Step 6** Click **OK** to complete the authorization for IAM users in the **EU-Paris** region.

----End

After the authorization is complete, log in to the Huawei Cloud console as an IAM user. Select the **EU-Paris** region and use cloud resources based on the assigned permissions.

## 4.13 How Do I Obtain an Access Key (AK/SK) in the EU-Paris Region?

### Symptom


The administrator has enabled the **EU-Paris** region. The account and IAM users need to use access keys for encryption and signing in the selected region.

Users access cloud services in the **EU-Paris** region as virtual users authorized through federated authentication. They are not real users who exist in the cloud service system, and need to obtain an access key in Huawei Cloud's default regions and the **EU-Paris** region, respectively.

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

### Procedure

**Step 1** Create an IAM user in the **EU-Paris** region as an administrator. To create an access key for yourself, go to [Step 2](#).

1. Log in to Huawei Cloud as an administrator, click  on the console homepage, and select the **EU-Paris** region.
2. On the console, choose **Management & Governance > Identity and Access Management**.
3. In the navigation pane of the IAM console, choose **Users**.
4. Click **Create User** in the upper right corner.
5. On the **Create User** page, set user information. For details, see [Creating a User](#).

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

6. Click **OK**.

**Step 2** Obtain an access key for the IAM user.

1. Log in to the IAM console as an administrator and select the **EU-Paris** region.
2. On the **Users** page of the IAM console, click **Set Credentials** in the **Operation** column of the row that contains the IAM user created in [1](#).
3. On the **Set Credentials** page, click **Create Access Key**.
4. (Optional) Enter a description for the access key.
5. Click **OK**. The access key is created.
6. Download the access key file.

 **NOTE**

- Each user can have a maximum of two access keys with unlimited validity. To ensure account security, keep them properly.
- The administrator and IAM users can use the access key only in the **EU-Paris** region.

7. (Optional) Provide the access key to the IAM user.

----**End**

# A Change History

**Table A-1** Change history

Released On	What's New
2022-11-30	<p>This issue is the twentieth official release.</p> <p>This release incorporates the following changes:</p> <ul style="list-style-type: none"> <li>• Added section <a href="#">Why Does IAM User Login Fail?</a></li> <li>• Added section <a href="#">How Do I Control IAM User Access to the Console?</a></li> <li>• Added section <a href="#">Differences Between IAM and Enterprise Management.</a></li> <li>• Added section <a href="#">What Are the Differences Between IAM Projects and Enterprise Projects?</a></li> <li>• Added section <a href="#">How Can I Obtain Permissions to Create an Agency?</a></li> <li>• Added section <a href="#">What Can I Do If Text Box Prompt Information Does Not Disappear?</a></li> <li>• Added section <a href="#">How Do I Disable Password Association and Saving on Google Chrome?.</a></li> </ul>
2022-07-25	<p>This issue is the nineteenth official release.</p> <p>Incorporated the following change:</p> <p>Modified user creation descriptions in <a href="#">Creating a Security Administrator</a>, <a href="#">Creating a User and Adding the User to a User Group</a>, <a href="#">Creating a User</a>, and <a href="#">(Optional) Assigning Permissions to an IAM User (by a Delegated Party)</a>.</p>
2021-07-30	<p>This issue is the eighteenth official release.</p> <p>Incorporated the following changes:</p> <ul style="list-style-type: none"> <li>• Added section <a href="#">Permissions.</a></li> <li>• Added section <a href="#">Custom Policy Use Cases.</a></li> </ul>

Released On	What's New
2020-08-30	<p>This issue is the seventeenth official release.</p> <p>Incorporated the following changes:</p> <ul style="list-style-type: none"> <li>• Adjusted the structure of <b>Identity Providers</b>.</li> <li>• Added section <b>Virtual User SSO via OpenID Connect</b>.</li> </ul>
2020-03-31	<p>This issue is the sixteenth official release.</p> <p>Incorporated the following change:</p> <p>Added descriptions about the <b>Resource</b> and <b>Condition</b> elements in policy statements in <b>Policy Syntax</b>.</p>
2020-01-03	<p>This issue is the fifteenth official release.</p> <p>Incorporated the following change:</p> <p>Deleted the description about not allowing for the deletion of cloud service agencies in <b>Creating an Agency (by a Delegating Party)</b>.</p>
2018-08-30	<p>This issue is the fourteenth official release.</p> <p>Incorporated the following change:</p> <p>Added the description about <b>Session Timeout Policy</b> in <b>Account Settings</b>.</p>
2018-08-10	<p>This issue is the thirteenth official release.</p> <p>Incorporated the following change:</p> <ul style="list-style-type: none"> <li>• Added section <b>Personal Data Protection Mechanism</b>.</li> <li>• Added section <b>Auditing</b>.</li> </ul>
2018-06-29	<p>This issue is the twelfth official release.</p> <p>Incorporated the following change:</p> <p>Added description about the <b>Require Password Reset</b> option in section <b>Viewing and Modifying User Information</b>.</p>



Released On	What's New
2018-04-30	<p>This issue is the eleventh official release.</p> <p>Incorporated the following changes:</p> <ul style="list-style-type: none"> <li>● Added the operation of resetting the failed login count in <a href="#">Viewing and Modifying User Information</a>.</li> <li>● Added the operation of setting the session timeout duration in <a href="#">Account Settings</a>.</li> <li>● Added section <a href="#">How Do I Bind a Virtual MFA Device?</a></li> <li>● Added section <a href="#">How Do I Obtain MFA Verification Codes?</a></li> <li>● Added section <a href="#">How Do I Unbind a Virtual MFA Device?</a></li> <li>● Added section <a href="#">Permissions</a>.</li> </ul>
2018-02-09	<p>This issue is the tenth official release.</p> <p>Incorporated the following change:</p> <p>Added a table that describes agency types in <a href="#">Creating an Agency (by a Delegating Party)</a>.</p>
2017-10-27	<p>This issue is the ninth official release.</p> <p>Adjusted the document content structure. Added sections <a href="#">Service Overview</a> and <a href="#">Getting Started</a>.</p>
2017-10-15	<p>This issue is the eighth official release.</p> <p>Incorporated the following change:</p> <p>Deleted chapter "Permission Description." For details, see "Permission Description".</p>
2017-07-27	<p>This issue is the seventh official release.</p> <p>Incorporated the following change:</p> <ul style="list-style-type: none"> <li>● Added the description for the <b>CTS Administrator</b> permission.</li> <li>● Added the description for automatically extracting metadata and manually configuring metadata in <a href="#">Step 1: Create an IdP Entity</a>.</li> </ul>
2017-05-26	<p>This issue is the sixth official release.</p> <p>Incorporated the following change:</p> <p>Added <a href="#">Step 1: Create an IdP Entity</a>.</p>
2017-04-27	<p>This issue is the fifth official release.</p> <p>Incorporated the following change:</p> <ul style="list-style-type: none"> <li>● Added section <a href="#">Creating an Agency (by a Delegating Party)</a>.</li> <li>● Added section <a href="#">(Optional) Assigning Permissions to an IAM User (by a Delegated Party)</a>.</li> </ul>

Released On	What's New
2017-03-30	<p>This issue is the fourth official release.</p> <p>Incorporated the following change:</p> <ul style="list-style-type: none"> <li>● Added the description for the <b>Agent Operator</b> permission.</li> <li>● Added the description for the <b>RTS Administrator</b> permission.</li> <li>● Added the description for setting user credentials in <a href="#">Viewing and Modifying User Information</a>.</li> </ul>
2017-02-10	<p>This issue is the third official release.</p> <p>Incorporated the following change:</p> <p>Added the description for the <b>Guest</b> permission.</p>
2017-01-20	<p>This issue is the second official release.</p> <p>Incorporated the following changes:</p> <p>Added the description for the <b>MRS Administrator</b> permission.</p>
2016-12-30	<p>This issue is the first official release.</p>