

Alibaba Cloud

Identity as a service User Guide

Document Version: 20220322

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.
2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.
3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.
4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).
5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.
6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
 Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 Danger: Resetting will result in the loss of user configuration data.
 Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 Warning: Restarting will cause business interruption. About 10 minutes are required to restart an instance.
 Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: If the weight is set to 0, the server no longer receives new requests.
 Note	A note indicates supplemental instructions, best practices, tips, and other content.	 Note: You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click Settings > Network > Set network type .
Bold	Bold formatting is used for buttons, menus, page names, and other UI elements.	Click OK .
<code>Courier font</code>	Courier font is used for commands	Run the <code>cd /d C:/window</code> command to enter the Windows system folder.
<i>Italic</i>	Italic formatting is used for parameters and variables.	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] or [a b]	This format is used for an optional value, where only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	This format is used for a required value, where only one item can be selected.	<code>switch {active stand}</code>

Table of Contents

1.IT Administrator Guide	05
1.1. Logon	05
1.2. Applications	05
1.2.1. Provision Account To Application	05
1.2.2. Add an Application	08
1.3. Users	10
1.3.1. Groups	10
1.3.2. Organizations	16
1.3.3. Accounts	24
1.3.4. Account Management	33
1.4. Authentication	36
1.4.1. Application Authorize	36
1.4.2. Policy Server	39
2.Regular Users	46
2.1. Common Operations	46
2.2. Logon	48
2.3. Settings	50

1.IT Administrator Guide

1.1. Logon

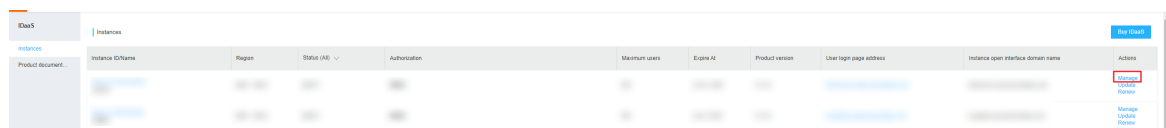
This topic describes how to log on to the IDaaS console after activating IDaaS.

Prerequisites

You have activated IDaaS and initialized the instance.

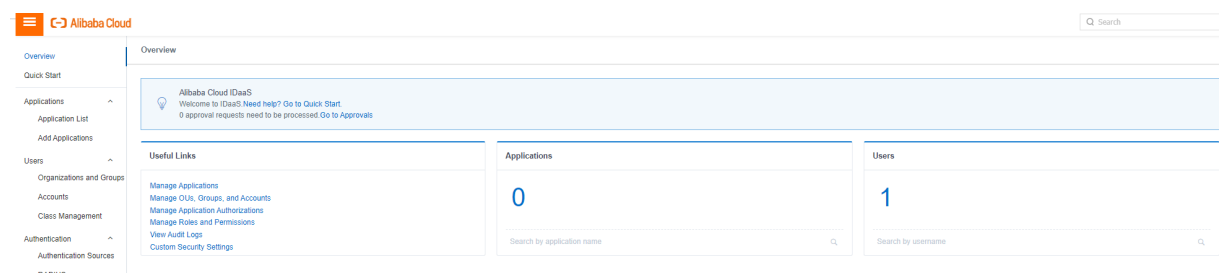
Procedure

1. Log on to the [IDaaS console](#).
2. On the **Instance List** page, find the target IDaaS instance and click **Manage** in the Actions column.



Results

You can choose **Menu > My Applications** to access the page.



1.2. Applications

1.2.1. Provision Account To Application

This topic describes how to provision the account information to the application in the IDaaS console.

Background

Before you push account information to the SP application, IT administrators must make SCIM configurations.

SCIM provisioning must be configured and enabled so that the IDaaS console pushes account information to SP applications. The same rule applies to account groups and organizations. If you want the IDaaS console to provision the information of both accounts and account groups to SP applications, you must configure and enable SCIM provisioning for both accounts and account groups.

Procedure

1. Log on to the IDaaS console as an IT administrator. For more information, see [Logon](#) in Administrator Guide.
2. In the left-side navigation pane, choose **Applications > Application List**.


3. Find the target application and click **Details** in the Actions column.

Application List Add Application

Application List

This page allows the administrator to manage applications. Once added to IDaaS, applications support single sign-on and user provisioning. After an application is added to IDaaS, make sure to enable the application and authorize application access to users. The page also provides detailed information about applications, including SSO URLs, application accounts, user provisioning settings, authorization settings, and audit logs.

Search by application name 🔍

Application Logo	Application Name	Application ID	Device Type	Application Status	Actions
	JWT	20200313110953GDMJ2Dy8pejwB	Web Application	✔	Authorize Details ▲

Application Information

Details of the application

[View Details](#) [Modify Application](#)

[Delete Application](#)

Authentication Information

Single sign-on (SSO) URLs

[IDaaS-initiated SSO URL](#)

[SP-initiated SSO URL](#)

Account Information - Provisioning

Modify SCIM settings and provision OUs and groups to the application.

[Provision OUs](#) [Configure SCIM](#)

Account Information - Account Linking

Application accounts that are linked with IDaaS accounts.

[View Application Accounts](#)

Authorization Information

Groups and accounts that are authorized to manage the application.

[Authorize](#)

Audit Information

View detailed operation logs about the application.

[View Logs](#) [View Provisioning Records](#)

API

Whether to apply open system API

☐ [API Key](#) [API Secret](#)

4. In the **Account Information - Provision** section, click **Configure SCIM**.

Note If the **Account Information - Application Accounts** section is displayed, click **Provision** to switch to the **Account Information - Provision** section.

5. On the **Configure SCIM** page, click the tab to select the target object to be provisioned and configure the parameters.

The following objects can be provisioned: **accounts** and **organizations**. Here the console acts as a client to provision account information to third-party business systems.

Parameter	Description
Application Name	The application with provisioning configured.
SCIM Service URL	The URL to receive account information, such as <code>http://jzyt.idp-local.com/api/application/cs_multibrowser/scim/account_password</code> .
Enable	Specifies whether to enable SCIM provisioning. If you turn on this switch, the organization will be pushed to authorized applications when you manually push an organization.
Protocol Type	The type of the authentication protocol used to verify requests. Valid values: <ul style="list-style-type: none"> Basic OAuth2
Username	If the Protocol Type is set to Basic, enter the administrator username.

Parameter	Description
Password	If the Protocol Type is set to Basic, enter the administrator password.
oauth_url	If the Protocol Type is set to OAuth2, enter the OAuth URL.
client_id	If the Protocol Type is set to OAuth2, enter the client ID.
client_secret	If the Protocol Type is set to OAuth2, enter the client key.

Configure SCIM (JWT) ×

Account

组织机构

Application Name

JWT

* SCIM Service URL

http://demo.com/api/application/scim/account

The URL is used to receive provisioning information. For example, http://xxx.com/api/application/scim/account

Enable

☐ No

Once enabled, when you create, modify, or delete an account, the account information will be automatically updated in the corresponding application.

Protocol Type

☒ Basic ☐ OAuth2

The type of authentication protocol that is used to verify requests.

* Username

test

The administrator name provided by BASIC.

Admin Password

.....

The administrator password provided by BASIC.

Save

Cancel

6. Click **Save**.

1.2.2. Add an Application

This topic describes how to add a third-party application and integrate single sign-on (SSO) into the application in the IDaaS console.

Background

IT administrators can add application systems in the IDaaS console and integrate single sign-on into application systems. After you add an application and provision the account information, you can log on to the application system from the IDaaS console in a single sign-on manner.

Procedure

1. Log on to the IDaaS console as an IT administrator. For more information, see [Logon](#) in Administrator Guide.
2. In the left-side navigation pane, choose **Applications > Add Applications**.

Note You can click **All**, **Standard Protocols**, or **Custom Templates** tab to find the application to be added.

Application Logo	Application Name	Application ID	Tag	Description	Application Type	Actions
	C/S Application	plugin_cs_oidc	CS, PC, OIDC	After wake-up application, it passes parameters to it through the oidc protocol to realize login, which is suitable for applications that can receive and parse the parameters of the oidc protocol.	PC Client	Add Application
	CAS	plugin_cas_apereo	SSO, CAS	CAS (central authentication service, version 2.0) is an open source single sign on protocol based on challenge and response. It is widely used in the enterprise when the network between the integrated client and the server is smooth. It has the advantages of simple integration and strong scalability.	Web Application, Mobile Application	Add Application
	JWT	plugin_jwt	SSO, JWT	JWT (JSON web token) is an open standard based on JSON declared in network application environment. IDaaS uses JWT for single sign on (SSO) of distributed sites. JWT single sign on is based on asymmetric encryption. IDaaS encrypts the user's status and information with private key. After passing it to the application, the application decrypts and verifies it with public key. The usage scenarios are very extensive and the integration is simple.	Web Application, Mobile Application, PC Client	Add Application
	OAuth2	plugin_oauth2	OAuth2	OAuth is an open resource authorization protocol. Applications can obtain token access through OAuth, Token, and carry the token to the server to request user resources. Application can use OAuth application template to realize unified identity management.	Web Application	Add Application

3. Find the target application from the application template list and click **Add Application** in the Actions column.

Note You can search for an application with the application name.

Application Logo	Application Name	Application ID	Tag	Description	Application Type	Actions
	Alibaba Cloud RAM-User SSO	plugin_aliyun	SSO, SAML, Aliyun	Based on SAML protocol, IDaaS single sign on to the alidocs console is realized. To use this template, it is necessary to create a ram sub account for each user in RAM. The IDaaS account and ram sub account are mapped to realize single sign on to ram.	Web Application	Add Application
	Alibaba Cloud RAM-Role SSO	plugin_aliyun_role	SSO, SAML, Aliyun	Based on SAML protocol, IDaaS single sign on to the alidocs console is realized. Using this template, RAM roles need to be created in RAM, and there is no need to create ram sub accounts for each user. IDaaS accounts and ram roles can be mapped to achieve single sign on to ram.	Web Application	Add Application
	JWT	plugin_jwt	SSO, JWT	JWT (JSON web token) is an open standard based on JSON declared in network application environment. IDaaS uses JWT for single sign on (SSO) of distributed sites. JWT single sign on is based on asymmetric encryption. IDaaS encrypts the user's status and information with private key. After passing it to the application, the application decrypts and verifies it with public key. The usage scenarios are very extensive and the integration is simple.	Web Application, Mobile Application, PC Client	Add Application
	OAuth2	plugin_oauth2	OAuth2	OAuth is an open resource authorization protocol. Applications can obtain token access through OAuth, Token, and carry the token to the server to request user resources. Application can use OAuth application template to realize unified identity management.	Web Application	Add Application
	SAML	plugin_saml	SSO, SAML	SAML (security assertion markup language, version 2.0) is based on XML protocol. It uses security token including assertion to transfer identity information between the authorizer (IDaaS) and the token consumer (application), and achieves single sign-on targeting cross-domain network. SAML is mature authentication protocol, which is widely used in public and private cloud at home and abroad.	Web Application	Add Application
	SAP GUI	plugin_sap_gui	SSO, C/S	SAP GUI is a graphical user interface used by SAP users to access SAP system. SAP is the world's leading enterprise software provider, whose products widely include ERP, CRM, data analysis, HR, logistics, travel, finance and other aspects. With 18000 global partners, SAP is widely distributed in 25 different industries, providing digital management solutions for various stages of enterprises.	PC Client	Add Application
	Salesforce	plugin_salesforce	SSO	Salesforce is widely used public cloud CRM platform (Customer Relationship Management) in the world. It provides enterprises with efficient business capabilities such as case management, task management, event dynamic upgrading, etc. IDaaS supports single sign-on to salesforce website through SAML protocol.	Web Application	Add Application
	WordPressSaml	plugin_wordpress_saml	SSO, SAML, CMS	WordPress is the most widely used CMS (content management system) in the world. It allows tens of millions of technical or non-technical personnel to produce and manage various types of websites through a very powerful plug-in system and a convenient and natural operation interface. From business websites and government pages to personal blogs and theme forums, WordPress supports a variety of forms. IDaaS supports single sign on to WordPress website through SAML protocol.	Web Application	Add Application

4. In the Add Application dialog box that appears, configure the parameters as required.

Notice The parameters will vary depending on the application. The Add Application dialog box will list these parameters.



The application is added. You can see the new application on the **Application List** page. By default, the new application is enabled.

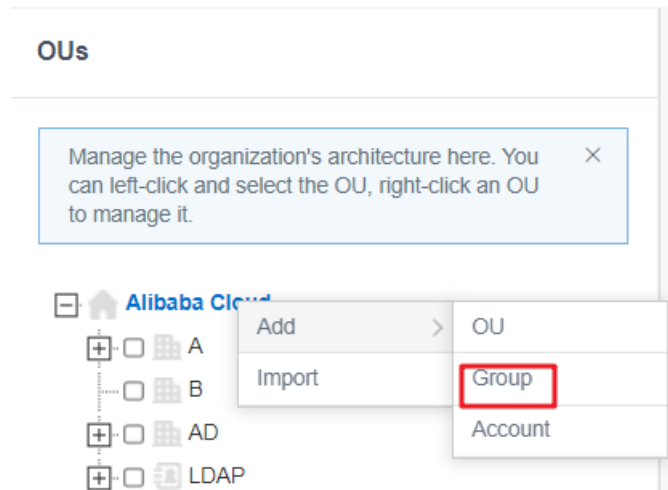
Authorize an application

1.3.1. Groups

Create a group

Procedure

- > Document Version: 20220322



4. In the **Create Group** dialog box that appears, click the **Group Attributes** tab and configure the following parameters.

Parameter	Description
Parent OU	The parent node of the group.
Name	The name the group.
External ID	The external ID of the group. The external ID is the unique ID of a group in IDaaS. If you do not specify this parameter, it is automatically generated by IDaaS.
Description	The description of the group.

Create Group
×

Group Attributes Extended Attributes Mutually Exclusive Groups

Parent OU Alibaba Cloud

* Name Enter a name

External ID Enter an external ID

Description Enter a description

Submit Close

5. If you have defined extended attributes in the data dictionary, click the **Extended Attributes** tab

to add attributes.

Create Group

×

Group Attributes

Extended Attributes

Mutually Exclusive Groups

The extended attributes. Fields marked with asterisks (*) are required.

B

Submit

Close

6. If the new group and an existing group are mutually exclusive, select the existing group on the **Mutually Exclusive Groups** tab.

Create Group

×

Group Attributes

Extended Attributes

Mutually Exclusive Groups

Q Search by name

<input type="checkbox"/>	Name	Type	Description	Directory
<input type="checkbox"/>	111111	User-created Group		
<input type="checkbox"/>	team1	User-created Group		
<input type="checkbox"/>	team2	User-created Group		

Total 3 items

<

1

>

Goto

1

Submit

Close

7. After configuring the parameters, click **Submit**.

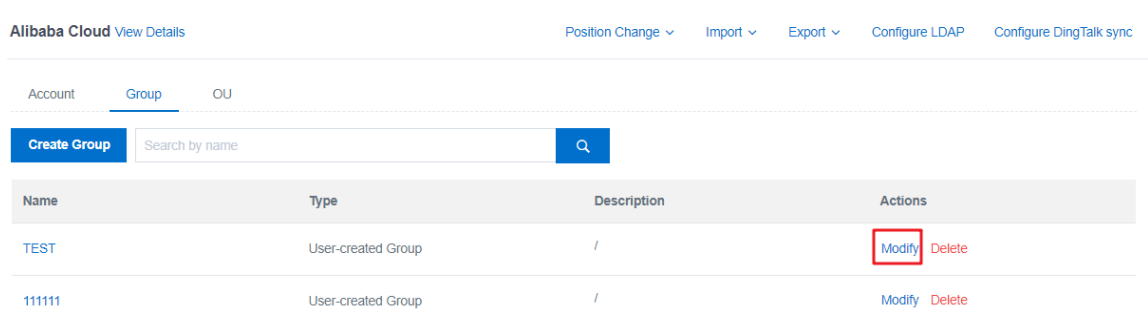
The new organization is displayed on the **Group** tab of the parent organization on the right. It is enabled by default.

Modify a group

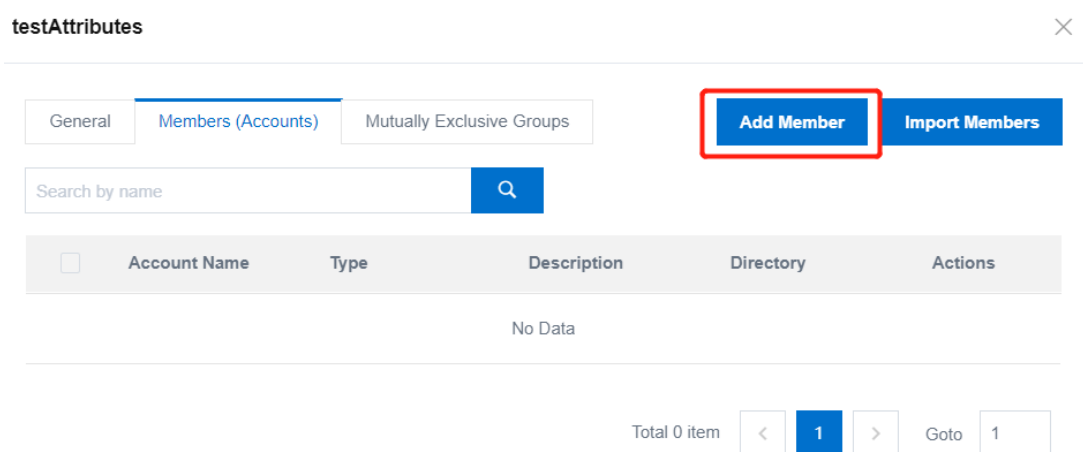
You can modify the attributes of an existing group at any time, such as the name, account members, group members, and mutually exclusive groups.

Procedure


1. Log on to the IDaaS console as an IT administrator. For more information, see [Logon](#) in Administrator Guide.
2. In the left-side navigation pane, choose **Users > Organizations and Groups**.
3. In the OUs window on the left, find the organization to which the group to be modified belongs and click its name.
4. In the organization information window on the right, click the **Group** tab.
5. In the group list, find the target group and click **Modify** in the Actions column.




6. In the Group Attributes dialog box that appears, modify the general attributes as specified in steps 4, 5, and 6 in the **Create a group** section and then click **OK**.
7. View and modify the account members and mutually exclusive groups of the current group on the **Member (Accounts)** and **Mutually Exclusive Groups** tabs.
 - o Add account members
 - a. On the **Members (Accounts)** tab, click **Add Members**.



- b. On the Add Members dialog box that appears, select the accounts to be added to the group.


 **Note** You cannot select members of mutually exclusive groups for the current group here.

← Add Members ×

Search by username 

<input type="checkbox"/>	Account Name	Type	Description	Directory
<input type="checkbox"/>	demoUser1	User-created Account		
<input type="checkbox"/>	C57D5C42-DE66-4E6C-905E-968A96872678	Provisioned Account		
<input type="checkbox"/>	4F1441C3-3AC6-4D96-9FBA-16F26DF84C72	Provisioned Account		
<input type="checkbox"/>	lin0512	User-created Account		
<input type="checkbox"/>	dt11567251533	Provisioned Account		
<input type="checkbox"/>	dt21328822228	Provisioned Account		
<input type="checkbox"/>	dt14756111111	Provisioned Account		
<input type="checkbox"/>	dt36002607117	Provisioned Account		
<input type="checkbox"/>	dt21310658399	Provisioned Account		
<input type="checkbox"/>	dt97296248448	Provisioned Account		

- c. Click OK.

 **Note** You can remove members on the **Members (Accounts)** tab by clicking Remove or Batch Remove.

- o Add mutually exclusive groups
 - a. On the **Mutually Exclusive Groups** tab, click **Add Mutually Exclusive Group**.

testAttributes ✕

General
Members (Accounts)
Mutually Exclusive Groups

☐

Name	Type	Description	Directory	Actions
No Data				

Total 0 item

- b. In the **Add Mutually Exclusive Group** dialog box that appears, select the groups to be added.


← Add Mutually Exclusive Group ✕

☐

Name	Type	Description	Actions
<input type="checkbox"/> TEST2	User-created Group		阿里云IDAAS

Total 1 item

- c. Click **OK**.

 **Note** You can remove mutually exclusive groups on the **Mutually Exclusive Groups** tab by clicking **Remove** or **Batch Remove**.

Delete a group or remove a group from an organization

You can delete a group that is no longer needed from the root node of its parent organization. You can only delete a group that does not contain any members. Therefore, you must delete members before this operation.

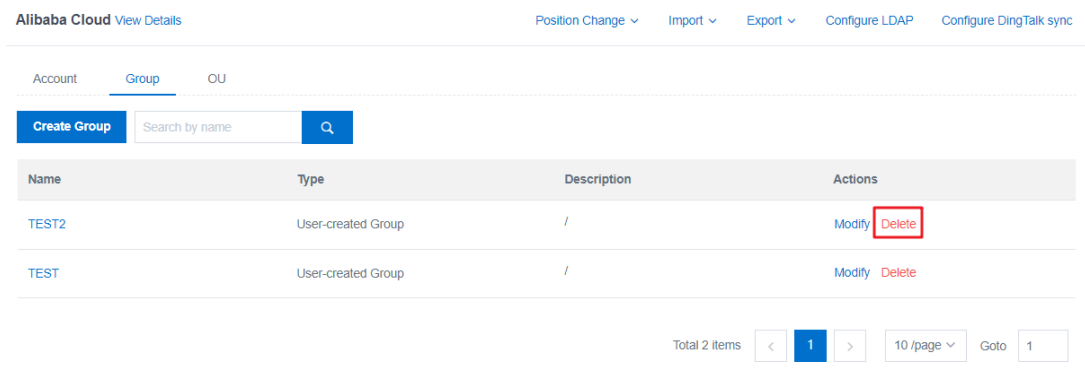
For a group that belongs to a non-root node, you can remove it from the parent organization to detach its affiliation with the organization. After removing a group that belongs to a non-root node from the parent organization, you can further remove it from the root node.

Procedure

1. Log on to the IDaaS console as an IT administrator. For more information, see [Logon](#) in Administrator Guide.
2. In the left-side navigation pane, choose **Users > Organizations and Groups**.
3. You can determine whether to delete a group or remove a group:
 - o **Delete a group**

○ Delete a group

- In the OUs window on the left, click the root node for the target organization.
- On the **Group** tab, search for the group to be deleted and click **Delete** in the Actions column.



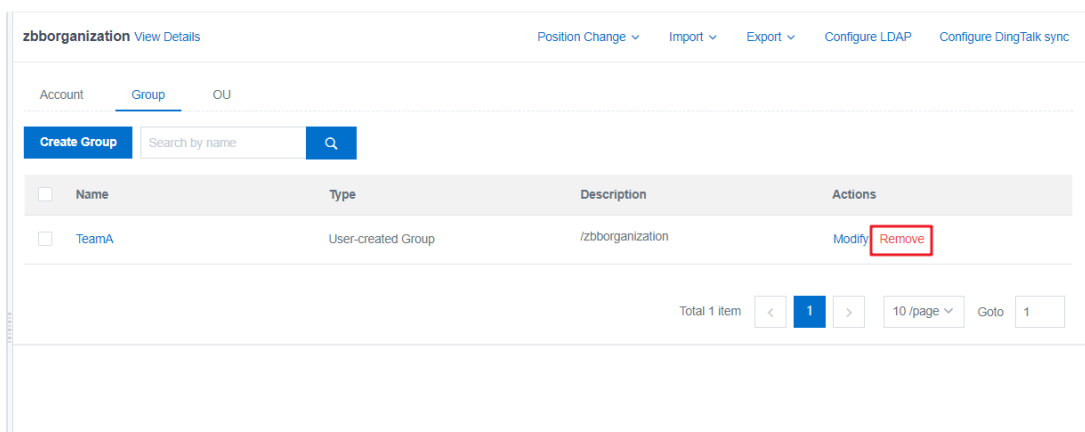
- In the **System Prompt** message that appears, click **OK**.

Note You can only delete a group that does not contain any members.

- In the **Incremental Provisioning** dialog box that appears, perform provisioning operations after you delete the group.

○ Remove a group

- In the OUs window on the left, find the organization to which the group to be removed belongs and click its name.
- On the **Group** tab, find the group to be removed and click **Remove** in the Actions column.



- In the **System Prompt** message that appears, click **OK**.

1.3.2. Organizations

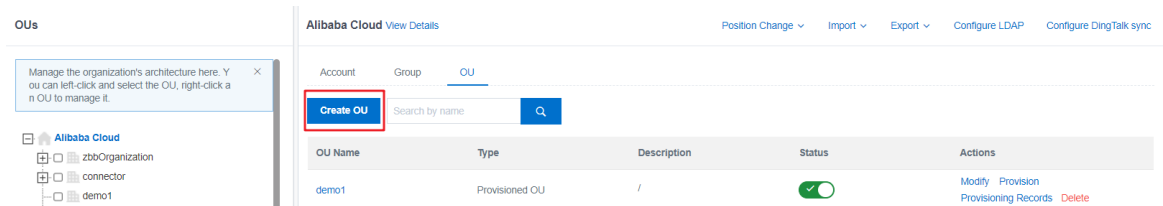
This topic describes how to create, modify, disable or enable, and delete organizations in the IDaaS console.

Create an organization

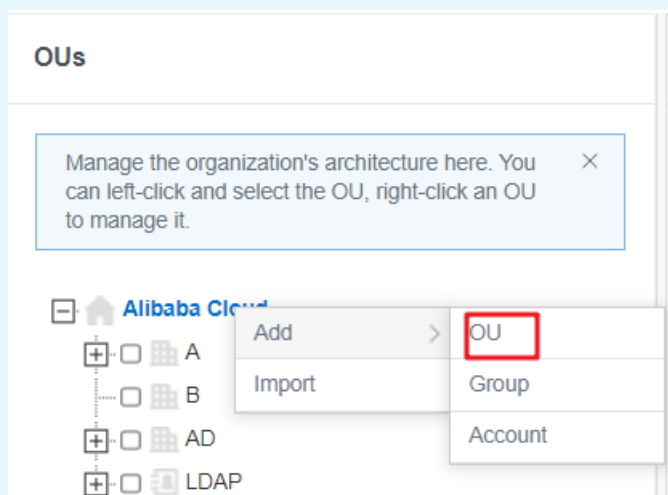
You can create an organization under the root node (company) or a child node (existing organization) of an organization.

Procedure

1. Log on to the IDaaS console as an IT administrator. For more information, see [Logon](#) in Administrator Guide.
2. In the left-side navigation pane, choose **Users > Organizations and Groups**.
3. In the OUs window on the left, find the parent node for the organization to be created and click its name.
4. In the parent node organization information window on the right, click the **OU** tab. Click **Create OU**.




Note Note: You can also right-click the parent node in the left window and choose **Add > OU** from the shortcut menu.



5. In the **Create OU** dialog box that appears, click the **OU Attributes** tab and configure the following parameters.

Parameter	Description
Parent OU	The parent node of the organization.

Parameter	Description
Type	<p>The type of the organization. Valid values:</p> <ul style="list-style-type: none">◦ Organization◦ Department <div> Note An organization is generally associated with an administrative region. A department is generally a functional organization. An organization is usually divided into multiple departments.</div>
Administrative Region	The administrative region of the organization. It is in the format of province + city + county.
Name	The name of the organization.
External ID	The external ID of the organization. The external ID is the unique ID of an organization in IDaaS and cannot be modified after it is specified. If you do not specify this parameter, it is automatically generated by IDaaS.
Description	The description of the organization.
SN	The serial number of the organization among same-level objects in the organization tree.

Create OU×

OU Attributes

Extended Attributes

Parent OU

Alibaba Cloud

* Type

Select

An organization is usually divided into multiple departments by administrative region.

Administrative Region

Select an administrative region

* Name

Enter an OU name

External ID

Enter an external ID

If you enter an external ID, it must be unique. If you do not enter a value, a default value will be generated, and you cannot modify it.

Description

Description

The OU description.

SN

0

Represents the location of the OU in the OU list.

Submit

Close

6. If you have defined extended attributes in the data dictionary, click the **Extended Attributes** tab to add attributes.

Create OU×

OU Attributes

Extended Attributes

The extended attributes. Fields marked with asterisks (*) are required.

dingtalkInstan
celd

dingtalkCropId

dingtalkDepart
mentId

Submit

Close

- After configuring the parameters, click **Submit**.
- In the **Incremental Provisioning** dialog box that appears, perform **LDAP Provisioning**, **Application Authorization**, and **SCIM Provisioning**.

Incremental Provisioning×

① **LDAP Provisioning**
Provision data to all LDAPs.

② **Application Authorization**
Application permissions of the parent OU or group are automatically inherited.

③ **SCIM Provisioning**
Use SCIM to provision data to authorized applications.

Provision Result

Successes: 0
Failures:

Note:

Next

Cancel

Incremental Provisioning

1

LDAP Provisioning

Provision data to all LDAPs.

2

Application Authorization

Application permissions of the parent OU or group are automatically inherited.

3

SCIM Provisioning

Use SCIM to provision data to authorized applications.

Application permissions of the parent OU or group are automatically inherited. The details are as follows:

J

JWT

DefaultAppforConnector

J

JWT

DefaultAppfor58connector

J

JWT

JWT

Total 3 items

<

1

>

Next

Cancel

Incremental Provisioning

1

LDAP Provisioning

Provision data to all LDAPs.

2

Application Authorization

Application permissions of the parent OU or group are automatically inherited.

3

SCIM Provisioning

Use SCIM to provision data to authorized applications.

Available applications with provision configured:

-

Available applications without provision configured:

☐ DefaultAppforConnector

☐ DefaultAppfor58connector

OK

Cancel

The organization is created. It is enabled by default. The new organization is displayed in the OUs window on the left or on the OU tab of the parent node on the right.

OUs

Manage the organization's architecture here. You can left-click and select the OU, right-click a n OU to manage it.

Alibaba Cloud

zbbOrganization

connector

demo1

demo

Alibaba Cloud View Details

Position Change Import Export Configure LDAP Configure DingTalk syn

Account Group OU

Create OU Search by name

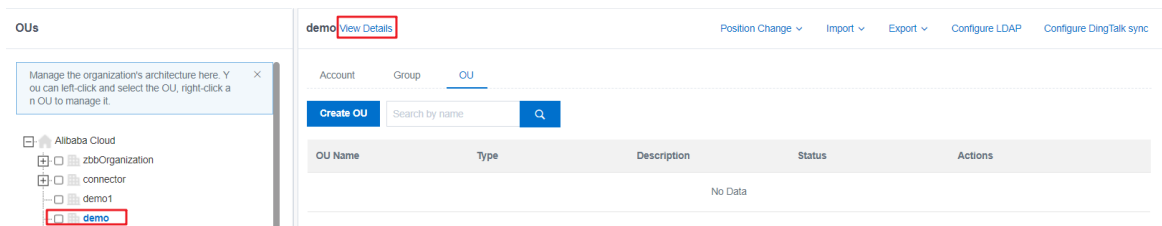
OU Name	Type	Description	Status	Actions
demo	User-created OU	/	<div><div></div></div>	<div>Modify Provision Provisioning Records Delete</div> <div>Modify Provision</div>

Modify an organization

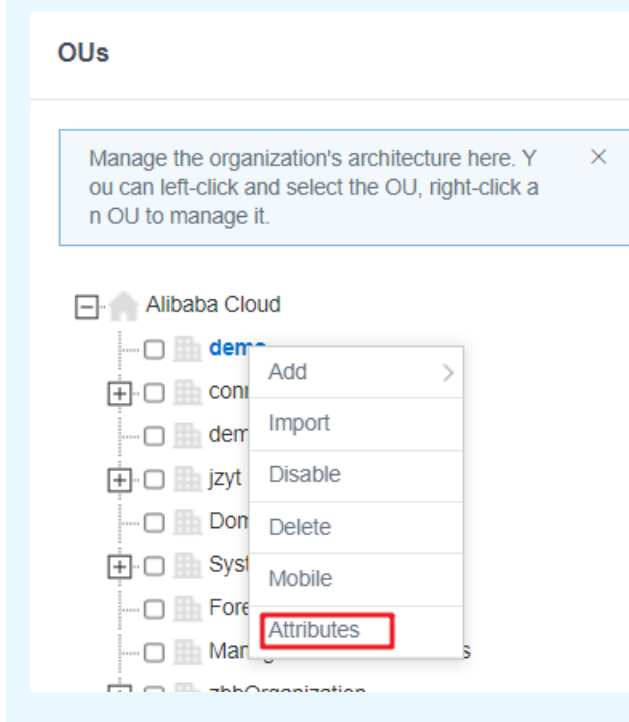
You can modify the attributes of an existing organization at any time.

Procedure

1. Log on to the IDaaS console as an IT administrator. For more information, see [Logon](#) in Administrator Guide.
2. In the left-side navigation pane, choose **Users > Organizations and Groups**.
3. In the OUs window on the left, find the parent node for the organization to be modified and click its name.
4. In the parent node organization information window on the right, click the **View Details**.



Note You can also right-click the target organization in the left window and choose **Attributes** from the shortcut menu.



5. On the **OU Attributes** tab, configure parameters as specified in steps 5 and 6 in the [Create an organization](#) section.
6. Click **OK**.
7. In the **Incremental Provisioning** dialog box that appears, perform **LDAP Provisioning**, **Application Authorization**, and **SCIM Provisioning**.

Disable or enable an organization

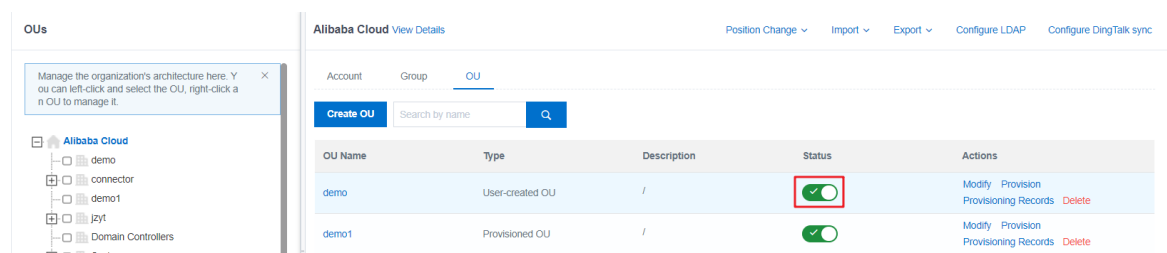
If you do not want to use an organization, you can disable it. A disabled organization is not displayed in the OUs window, but you can enable it again on the **OU** tab of the parent node.

Procedure

1. Log on to the IDaaS console as an IT administrator. For more information, see [Logon](#) in Administrator Guide.
2. In the left-side navigation pane, choose **Users > Organizations and Groups**.
3. In the OUs window on the left, find the parent node for the organization to be disabled and click its name.

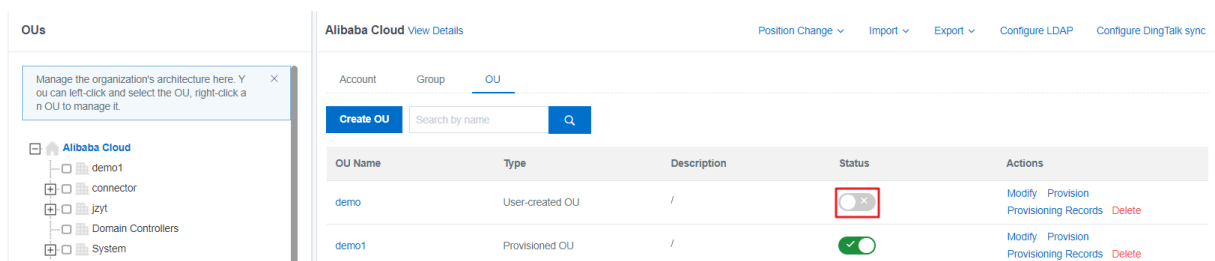
Note You can also right-click the target organization in the left window and choose **Disable** from the shortcut menu. After this operation, go directly to step 6.

4. In the parent node organization information window on the right, click the **OU** tab.
5. Find the target organization and turn off the Enable switch in the Status column.



6. In the **System Prompt** message that appears, click **OK**.

The disabled organization is still displayed on the **OU** tab of the parent node. You can enable this organization again by turning on the Enable switch in the Status column.



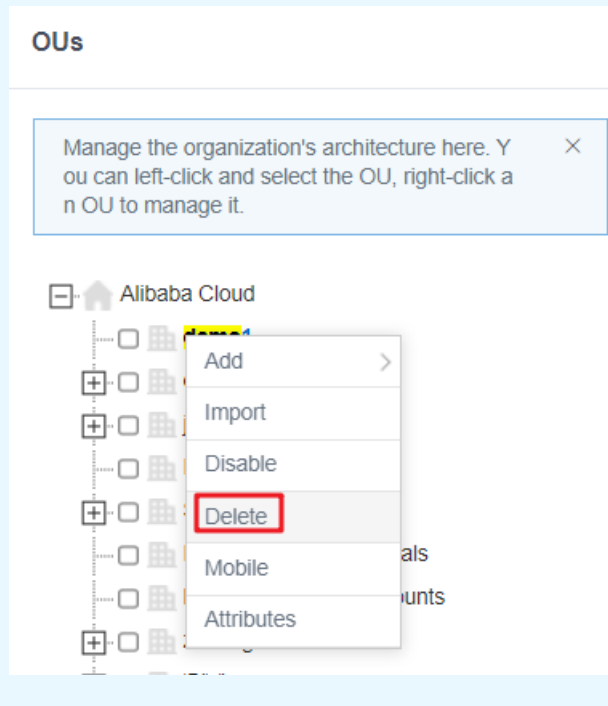
Delete an organization

You can delete an organization that is no longer needed. When you delete an organization, its default group is also deleted. You can only delete an organization that does not contain any members except the default group.

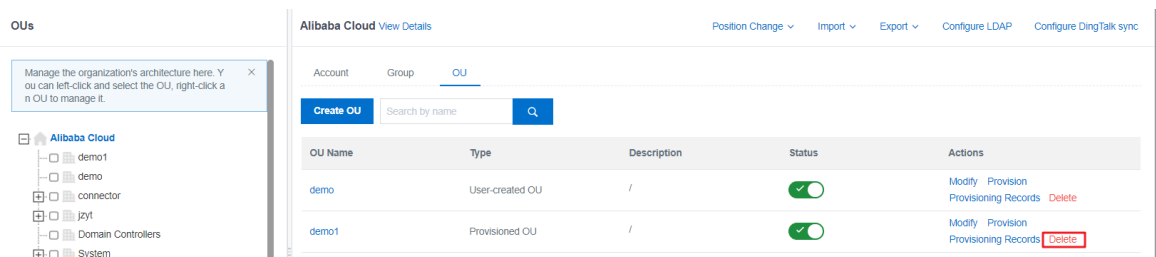
Procedure

1. Log on to the IDaaS console as an IT administrator. For more information, see [Logon](#) in Administrator Guide.
2. In the left-side navigation pane, choose **Users > Organizations and Groups**.
3. In the OUs window on the left, find the parent node for the organization to be deleted and click its name.

Note You can also right-click the target organization in the left window and choose **Delete** from the shortcut menu. After this operation, go directly to step 6.



4. In the parent node organization information window on the right, click the **OU** tab.
5. Find the target organization, and click **Delete** in the Actions column.



6. In the **System Prompt** message that appears, click **OK**.
7. In the **Incremental Provisioning** dialog box that appears, perform **LDAP Provisioning**, **Application Authorization**, and **SCIM Provisioning**.

1.3.3. Accounts

This topic describes how to create, modify, move, and delete an account in the IDaaS console.

Create an account (new recruit)

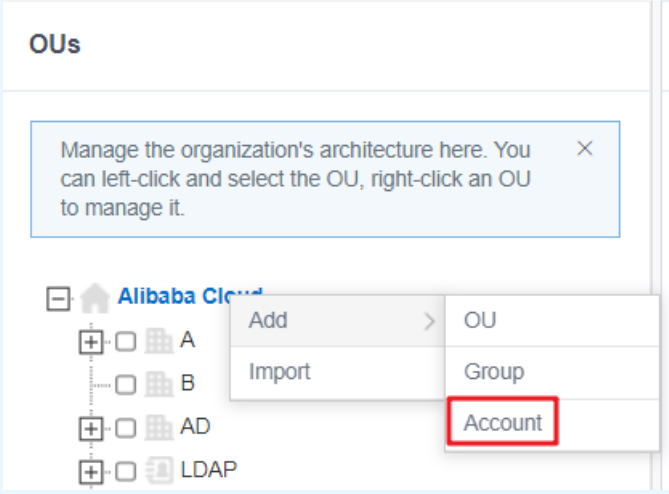
You can create an account for a new recruit in the IDaaS console.

Procedure

1. Log on to the IDaaS console as an IT administrator. For more information, see [Logon](#) in Administrator Guide.
2. In the left-side navigation pane, choose **Users > Organizations and Groups**.

3. In the OUs window on the left, find the organization to which the account to be created belongs and click its name.

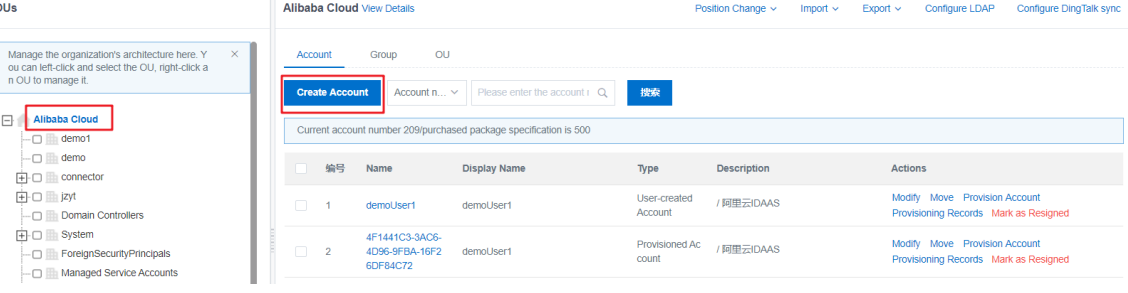
Note You can also right-click the target organization in the left window and choose **Add > Account** from the shortcut menu. After this operation, go directly to step 5.



The screenshot shows the 'OUs' (Organizational Units) window on the left. A message box states: 'Manage the organization's architecture here. You can left-click and select the OU, right-click an OU to manage it.' Below this, a tree view shows the hierarchy under 'Alibaba Cloud'. A right-click context menu is open over the 'Alibaba Cloud' node, showing options: 'Add', 'Import', 'Group', and 'Account'. The 'Account' option is highlighted with a red rectangle.

4. In the parent node organization information window on the right, click the Account tab. Click **Create Account**.

Note You can also choose **Position Change > Enroll** in the top navigation bar of the right window.





The screenshot shows the 'Alibaba Cloud View Details' window. The 'Account' tab is selected. A 'Create Account' button is highlighted with a red rectangle. Below the button, a table lists existing accounts:

编号	Name	Display Name	Type	Description	Actions
1	demoUser1	demoUser1	User-created Account	/ 阿里云IDAAS	Modify Move Provision Account Provisioning Records Mark as Resigned
2	4F1441C3-3AC6-4D96-9FBA-16F2-6DF84C72	demoUser1	Provisioned Account	/ 阿里云IDAAS	Modify Move Provision Account Provisioning Records Mark as Resigned

The 'Enroll' button in the top navigation bar is also highlighted with a red rectangle in the second screenshot.

5. In the **Create Account** dialog box that appears, click the **Account Attributes** tab and configure the following parameters.

Parameter	Description
Parent OU	The parent node of the account.

Parameter	Description
Display Name	The display name or alias of the account. It must be 2 to 18 characters in length.
Account Name	The logon name of the account. The name can contain uppercase letters, lowercase letters, digits, hyphens (-), underscores (_), and periods (.). It must be 4 to 18 characters in length.
Password	The password of the account. The password must contain uppercase letters, lowercase letters, digits, and special characters. It must be six or more characters in length.
Email	<p>The email address associated with the account.</p> <p> Note The email address or phone number is required.</p>
Phone Number	<p>The mobile phone number associated with the account.</p> <p> Note The email address or phone number is required.</p>
External ID	The external ID of the account. The external ID is the unique ID of an account in IDaaS. If you do not specify this parameter, it is automatically generated by IDaaS.
Expires On	The expiration date of the account. If you do not specify this parameter, the default expiration date is used.
Remarks	The remarks for the account.

Create Account

Account Attributes

Extended Attributes

Parent Groups

Parent OU

Alibaba Cloud

* Account Name

Enter an account name

An account name can contain Uppercase Letter, Lowercase Letter, Digit, Hyphen (-), Underscore (_), Period (.). The password must be at least 4 characters in length.

* Display Name

Enter a display name

* Password

Enter a password

The password must contain uppercase letters, lowercase letters, digits, and special characters.; The password must be at least 6 characters in length.

Email

Enter a valid email address

Optional. Specify a phone number or an email address, or both.

Phone Number

+86

Enter a valid phone number

Optional. Specify a phone number or an email address, or both.

External ID

Enter an external ID

The unique identifier of this account in IDaaS. If you do not specify an ID, the system automatically generates a value.

Expires On

Select an expiration date

Optional. If you do not specify this parameter, the default expiration date (December 31, 2116) will be used.

Remarks

Enter remarks

The user remarks.

Submit

Close

- If you have defined extended attributes in the data dictionary, click the **Extended Attributes** tab to add attributes.

Create Account

Account Attributes

Extended Attributes

Parent Groups

The extended attributes. Fields marked with asterisks (*) are required. [Data Dictionary](#) to add or enable one.

dingtalkInstanceId

dingtalkCropId

dingtalkUserId

dingtalkUnionId

dingtalkPosition

dingtalkAvatar

Submit

Close

7. Click the **Parent Groups** tab to select parent groups for the account.

Create Account

Account Attributes

Extended Attributes

Parent Groups

Note: Make sure the selected group and the existing parent groups of this account are not mutually exclusive.

Search by name

<input type="checkbox"/>	Name	Type	Description	Directory
<input type="checkbox"/>	TeamA	User-created Group		
<input type="checkbox"/>	TEST2	User-created Group		
<input type="checkbox"/>	TEST	User-created Group		

Total 3 items

<1>

Goto

1

Submit

Close

8. After configuring the parameters, click **Submit**.
9. In the **Incremental Provisioning** dialog box that appears, perform **LDAP Provisioning**, **Application Authorization**, and **SCIM Provisioning**.

Incremental Provisioning

1 LDAP Provisioning

2 Application Authorization

3 SCIM Provisioning

Provision data to all LDAPs.

Application permissions of the parent OU or group are automatically inherited.

Use SCIM to provision data to authorized applications.

Provision Result

Successes: 0

Failures:

Note:

Next

Cancel

Incremental Provisioning

1 LDAP Provisioning

2 Application Authorization

3 SCIM Provisioning

Provision data to all LDAPs.

Application permissions of the parent OU or group are automatically inherited.

Use SCIM to provision data to authorized applications.

Application permissions of the parent OU or group are automatically inherited. The details are as follows:

JJWT

DefaultAppforConnector

JJWT

JWT

JJWT

DefaultAppfor58connector

Total 3 items

<

1

>

Next

Cancel

> Document Version: 20220322

29

Incremental Provisioning ✕

✓ **LDAP Provisioning**
 Provision data to all LDAPs.

✓ **Application Authorization**
 Application permissions of the parent OU or group are automatically inherited.

3 **SCIM Provisioning**
 Use SCIM to provision data to authorized applications.

Available applications with provision configured:

-

Available applications without provision configured:

☐ DefaultAppforConnector
☐ JWT

☐ DefaultAppfor58connector

OK
Cancel

The new account is displayed on the **Account** tab of the parent organization on the right.

Modify an account

You can modify the attributes of an existing account at any time, such as the display name, associated email address or phone number, expiration data, external ID, and parent group.

Procedure

1. Log on to the IDaaS console as an IT administrator. For more information, see [Logon](#) in Administrator Guide.
2. In the left-side navigation pane, choose **Users > Organizations and Groups**.
3. In the OUs window on the left, find the organization to which the account to be modified belongs and click its name.
4. In the parent node organization information window on the right, click the **Account** tab.
5. Find the target account from the account list and click **Modify** in the Actions column.

Data Dictionary

Organizations and Groups

This page allows the administrator to manage information about OUs, departments, groups, and accounts. It also supports file uploads and user provisioning with AD/LDAP to import data. The administrator can manage OUs and groups by simply right-clicking on a node in the left-side organizational chart, or select a node and add members to the node on the right-side of the page.

OUs

Manage the organization's architecture here. You can left-click and select the OU, right-click a node to manage it.

- Alibaba Cloud
 - demo1
 - demo
 - connector
 - jzyt
 - Domain Controllers

Alibaba Cloud View Details Position Change ▾ Import ▾ Export ▾ Configure LDAP Configure DingTalk sync

Account
Group
OU

Create Account
Account n...
Please enter the account name
搜索

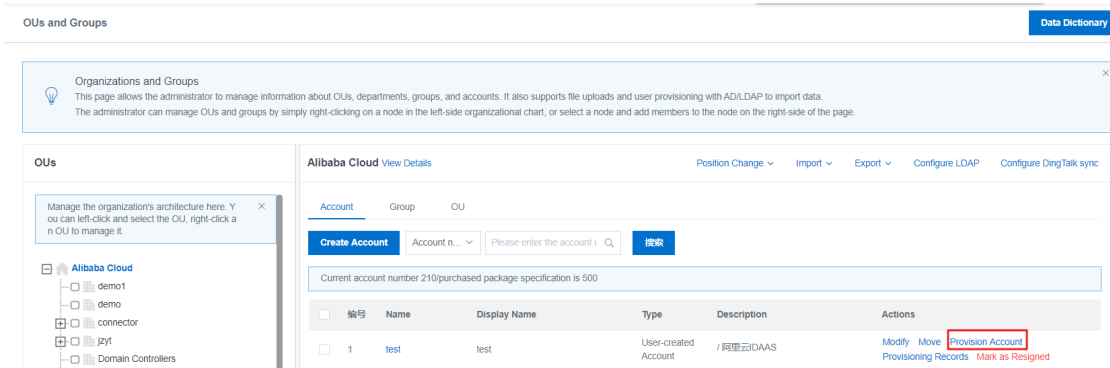
Current account number 210/purchased package specification is 500

编号	Name	Display Name	Type	Description	Actions
1	test	test	User-created Account	/ 阿里云IDaaS	Modify Move Provision Account Provisioning Records Mark as Resigned

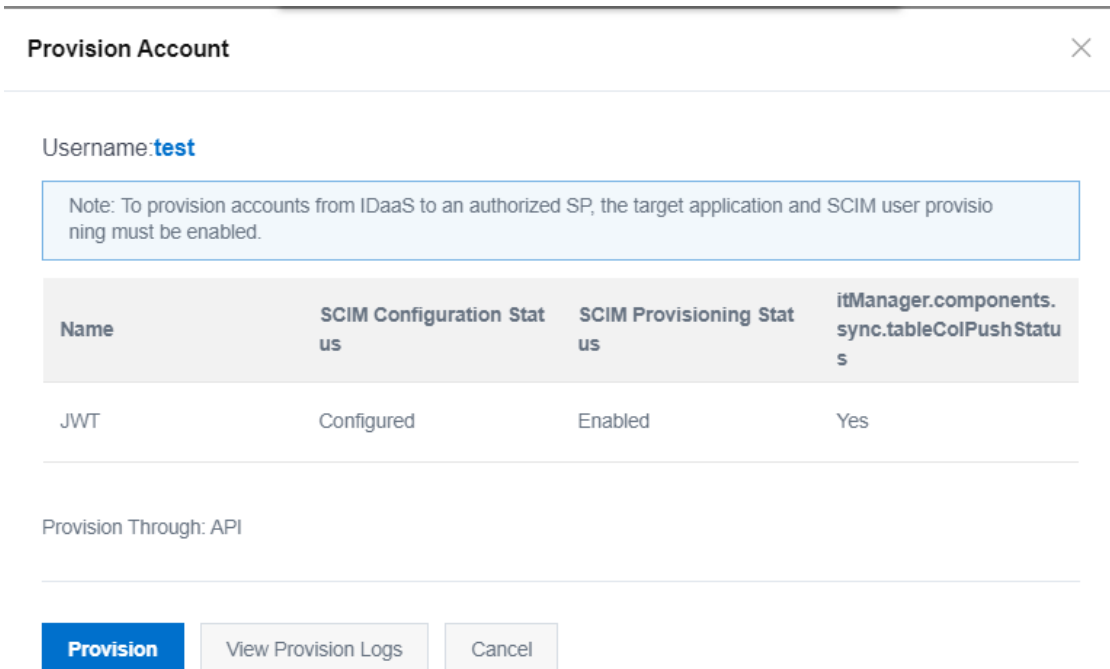
? **Note** You can search for an account with the account name or display name.

6. In the Account Attributes dialog box that appears, modify the account attributes as specified in steps 5, 6, and 7 in the [Create an account](#) section.

7. After configuring the parameters, click **Submit**.
8. After modifying the account attributes, you can provision the latest account information to the applications that the current organization has been authorized to access.
 - i. Go to the parent node organization information window.
 - ii. Click the **Account** tab. Find the target account and click **Provision Account** in the Actions column.



- iii. In the **Provision Account** dialog box that appears, select the applications to receive the provisioned account from the authorized third-party systems.



- iv. Click **Provision**.
- v. Check the provisioning record.

Move an account

You can move an account from an organization to another.

Procedure

1. Log on to the IDaaS console as an IT administrator. For more information, see [Logon](#) in Administrator Guide.
2. In the left-side navigation pane, choose **Users > Organizations and Groups**.
3. In the OUs window on the left, find the organization to which the account to be moved belongs and click its name.

Note You can also choose **Position Change > Move** in the top navigation bar of the right window. Search for the target account and click **Move** in the Actions column. After this operation, go directly to step 5.

4. In the parent node organization information window on the right, click the **Account** tab. Find the target account and click **Move** in the Actions column.

The screenshot shows the 'Organizations and Groups' management interface. On the left, a tree view shows the 'Alibaba Cloud' organization selected. The main area displays the 'Account' tab for the 'Alibaba Cloud' organization. A table lists accounts, with the 'test' account selected. The 'Move' action is highlighted in the 'Actions' column for the 'test' account.

编号	Name	Display Name	Type	Description	Actions
1	test	test	User-created Account	/ Alibaba Cloud	Modify Move Provision Account Provisioning Records Mark as Resigned
2	demoUser1	demoUser1	User-created Account	/ Alibaba Cloud	Modify Move Provision Account Provisioning Records Mark as Resigned

5. In the Account Move dialog box that appears, select the destination organization to which the account to be moved belongs in the Move To list.

The screenshot shows the 'testMove' dialog box. On the left, a tree view shows the 'Alibaba Cloud' organization selected. The main area displays the 'Move To' list with 'Alibaba Cloud' selected. The right pane shows the 'Current OU' and 'Target OU' fields, both set to 'Alibaba Cloud'. Below, there are tables for 'Available Applications Before Move' and 'Available Applications After Move', showing application details like Name, ID, and Device Type.

Name	ID	Device Type
DefaultAppforConnector	idaas-cn-0pp1mb0e705jw3	Data Provisioning
JWT	idaas-cn-0pp1mb0e705jw3	Web Application
DefaultAppfor58connector	idaas-cn-0pp1mb0e705jw2	Data Provisioning

6. Confirm the authorization application information after the move operation and click **Move**.

Mark an account as resigned

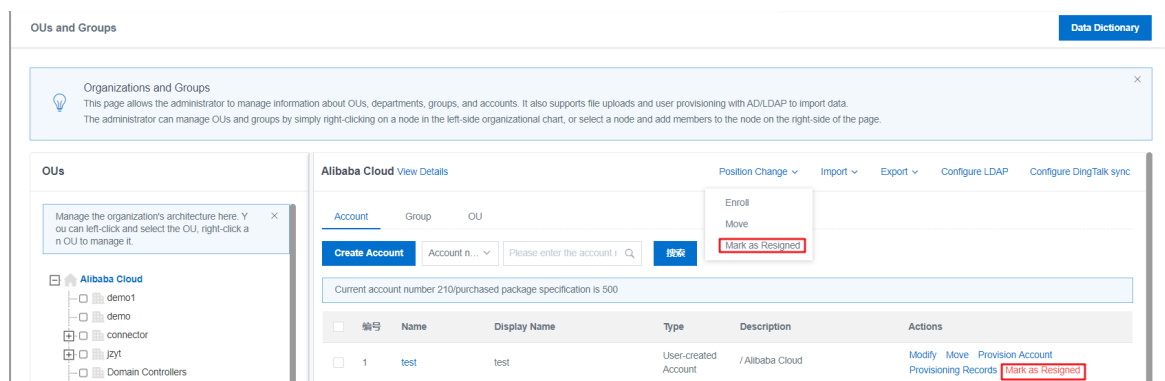
You can mark the account for a resigned employee as resigned.

Procedure

1. Log on to the IDaaS console as an IT administrator. For more information, see [Logon](#) in Administrator Guide.
2. In the left-side navigation pane, choose **Users > Organizations and Groups**.
3. In the OUs window on the left, find the root node for the target organization and click its name.

Note You can also choose **Position Change > Mark as Resigned** in the top navigation bar of the right window. Search for the target account and click **Mark as Resigned** in the Actions column. After this operation, go directly to step 6.

4. Click the **Account** tab. Search for the target account.
5. Click **Mark as Resigned** in the Actions column.



6. In the **System Prompt** message that appears, click OK.
7. In the **Incremental Provisioning** dialog box that appears, perform **LDAP Provisioning**, **Application Authorization**, and **SCIM Provisioning**.

1.3.4. Account Management

This topic describes how to manage an account on the Accounts page of the IDaaS console. You can view account details, enable or disable two-factor authentication, reset the password, enable or disable an account, and delete an account.

Procedure

1. Log on to the IDaaS console as an IT administrator. For more information, see [Logon](#) in Administrator Guide.
2. In the left-side navigation pane, choose **Users > Accounts**.
3. Select the account type by clicking the **Personal Account** or **Developer Account** tab.
4. Find the target account from the account list.

Note You can search for an account by using the associated email address, associated phone number, and account name.

Accounts

Personnel Account

Resigned Accounts

Real Name authentication

Accounts

This page allows the administrator to disable accounts, reset account passwords, enable two-factor authentication, and delete accounts. It also provides details about each account, including information about related devices, permissions, status, attributes, and OUS.

Account n...

Please enter the account n

Select enable status

Select expiration status

Search

Current account number 210/purchased package specification is 500

Username	Display Name	Email	Phone Number	Enabled or not	Expiration Status	Two-factor Authentication	Actions
test	test		-	<div><div></div></div>	Normal	<div><div></div></div>	<div>Account Details</div> <div>Reset Password</div> <div>Mark as Resigned</div>
demoUser1	demoUser1		-	<div><div></div></div>	Normal	<div><div></div></div>	<div>Account Details</div> <div>Reset Password</div> <div>Mark as Resigned</div>
C57D5C42-DE66-4E6C-905E-968A96872678	demoUser2		-	<div><div></div></div>	Normal	<div><div></div></div>	<div>Account Details</div> <div>Reset Password</div> <div>Mark as Resigned</div>
4F1441C3-3AC6-4D96-9FBA-16F26DF84C72	demoUser1		-	<div><div></div></div>	Normal	<div><div></div></div>	<div>Account Details</div> <div>Reset Password</div> <div>Mark as Resigned</div>

5. Perform the following operations as needed:

- View account details.
 - a. Find the target account and click **Account Details** in the Actions column.
 - b. The Account Details page consists of the following tabs:
 - **Account Information**: displays the general information, extended information, certificate information, and bound third-party account for the current account.
 - **Available Applications**: displays the applications that the current account is authorized to access.
 - **Application Account**: displays the application accounts created for the current account.
 - **OUs and Groups**: displays the OU list and group list to which the current account belongs.
 - **Devices**: displays the authenticated devices associated with the current account.
 - **Report**: generates an operation report for the current account.

Accounts / Account Details

← Account Details (test)

Account Information

Available Applications

Application Account

OUs and Groups

Devices

Report

Real-name authentication information

General Information

Username

test

Display Name

test

Email

Phone Number

(+86)undefined

Account Status

Normal

Directory

/

Account Type

User-created Account

External ID

790474142897347631

Created At

2020/5/22 下午3:03:00

Expiration Date

2116-12-31(Modify)

Two-factor Authentication

禁用

Extended Information

dingtalkInstanceid

dingtalkCropid

dingtalkUserid

dingtalkUnionid

dingtalkPosition

dingtalkAvatar

Certificate Information

Expires On

2023-05-22

Certificate Created At

2020/5/22 下午3:03:03

SubjectDN

CN=test, L=BJ, ST=BJ, O=IDSMANAGER, OU=IDaaS, C=CN

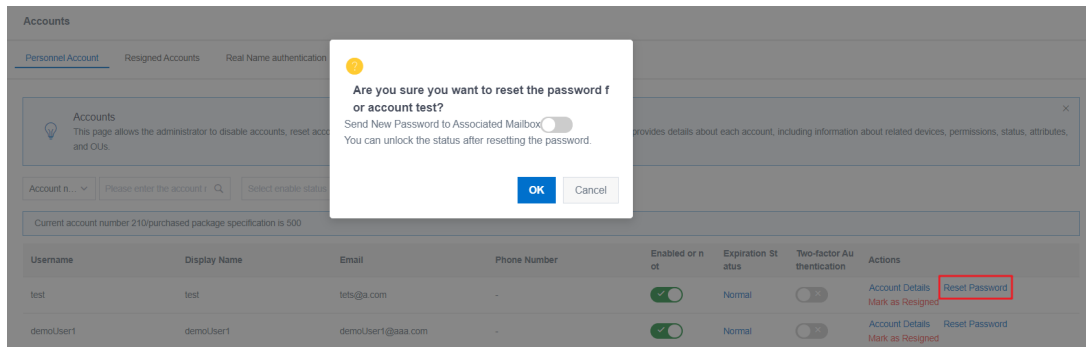
Third-party Accounts

- c. In the General Information section of the Account Information page, you can click **Modify** set **Expiration Time** for the current account.

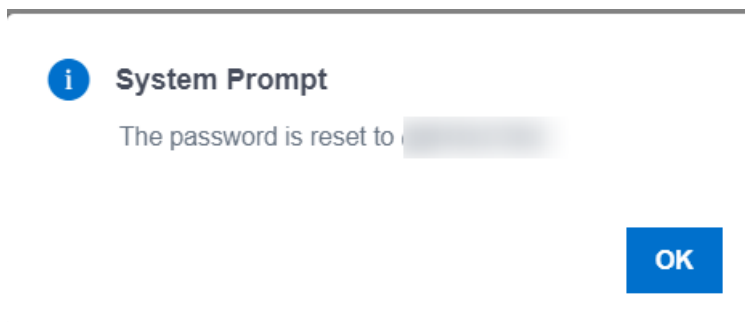
- Enable or disable two-factor authentication.

Find the target account and turn on or off the switch in the **Two-factor Authentication** column to enable or disable two-factor authentication.

- Reset the password.
 - a. Find the target account and click **Reset Password**.
 - b. In the dialog box that appears, select **Send New Password to Associated Mailbox** (ignore this option if there is not an email address specified for the account) and click **OK**.

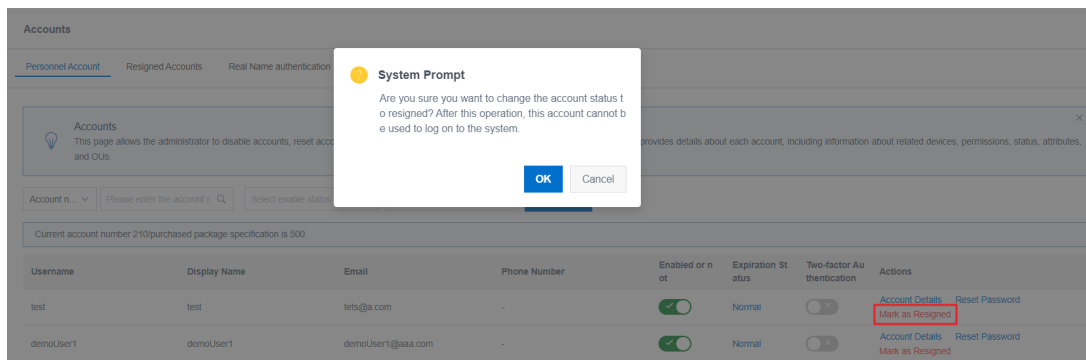


The account password is reset. A System Prompt message is displayed to indicate the new password.



- Enable or disable an account.
 - For an account in the **Disabled** state, you can turn on the **Enable** switch to enable it.
 - For an account in the **Normal** state, you can turn off the **Enable** switch to disable it.
- Mark an account as resigned.
 - a. Find the target account and click **Mark as Resigned**.

b. In the **System Prompt** message that appears, click **OK**.



Note You can also make an account as resigned on the Account tab of the OUs and Groups page. For more information, see [Mark an account resigned](#).

1.4. Authentication

1.4.1. Application Authorize

This topic describes how to grant permissions in the IDaaS console. You can authorize groups by application or authorize applications by group.

Prerequisites

Confirm that you have completed the following tasks:

- [Add an application](#)
- [Create a group](#)

Authorize groups by application

This operation determines which organizations or groups can access an application.

Procedure

1. Log on to the IDaaS console as an IT administrator. For more information, see [Logon](#) in Administrator Guide.
2. In the left-side navigation pane, choose **Authorization > Application Authorization**.
3. Click the **Authorize OUs or Groups by Application** tab.

Application Authorization

[Authorize OUs or Groups by Application](#)
[Grant Application Access by OU or Group](#)
[Grant Application Access by Account](#)
[Authorize Accounts by Application](#)
[Authorize Application by Class](#)

Application Authorization
This page provides the administrator with multiple ways to authorize application access. For example, the administrator can select an application and authorize multiple OUs and groups to access the application. Alternatively, they can select an account and grant the account access to multiple applications.

Applications (5)

- DefaultAppforConnector
- CAS(标准)
- DefaultAppfor58connector
- JWT1
- JWT

OUs and Groups (774) Authorized: 1

- Alibaba Cloud
 - demo1
 - demo
 - connector
 - jzyt
 - Domain Controllers
 - System
 - ForeignSecurityPrincipals

- Select the target application in the **Applications** list on the left.

Note You can search for an application with the application name.

- Select the organizations and groups allowed to access the current application in the OUs and Groups list on the right.

Note You can search for a group with the group name.

Authorize applications by group

This operation determines which applications the members of a group can access.

Procedure

- Log on to the IDaaS console as an IT administrator. For more information, see [Logon](#) in Administrator Guide.
- In the left-side navigation pane, choose **Authorization > Application Authorization**.
- Click the **Grant Application Access by OU or Group** tab.

Application Authorization

[Authorize OUs or Groups by Application](#)
[Grant Application Access by OU or Group](#)
[Grant Application Access by Account](#)
[Authorize Accounts by Application](#)
[Authorize Application by Class](#)

OUs and Groups(774)

- Alibaba Cloud
 - demo1
 - demo
 - connector
 - jzyt
 - Domain Controllers
 - System
 - ForeignSecurityPrincipals
 - Managed Service Accounts
 - zbbOrganization
 - 测试V1-4
 - 测试V2

Applications (5) Authorized: 3

<input type="checkbox"/>	Application Name	Application ID
<input checked="" type="checkbox"/>	DefaultAppforConnector	idaas-cn-0pp1mb0e705jw3
<input type="checkbox"/>	CAS(标准)	idaas-cn-0pp1mb0e705cas_apereo
<input checked="" type="checkbox"/>	DefaultAppfor58connector	idaas-cn-0pp1mb0e705jw2
<input type="checkbox"/>	JWT1	idaas-cn-0pp1mb0e705jw1
<input checked="" type="checkbox"/>	JWT	idaas-cn-0pp1mb0e705jw

- Select the target group in the OUs and Groups list on the left.

Note You can search for a group with the group name.

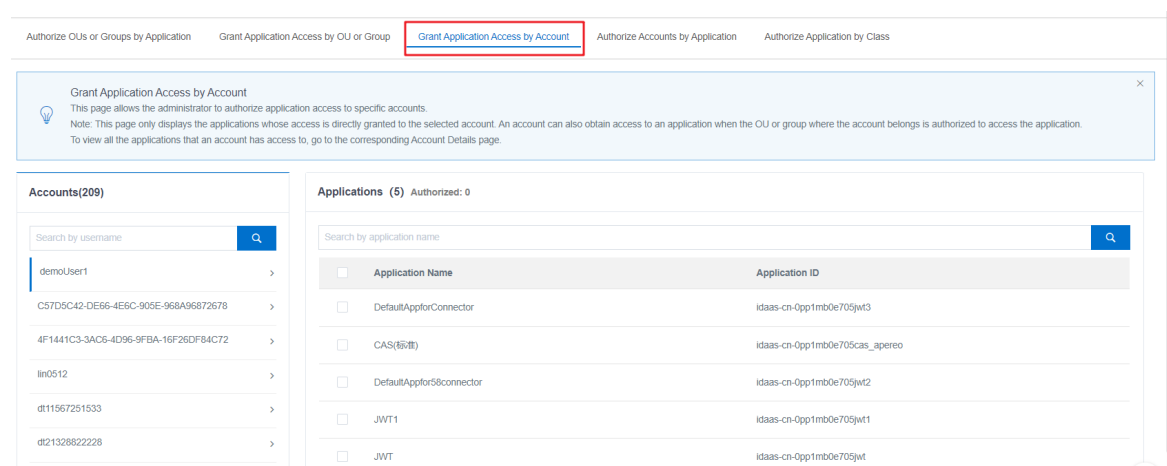
5. Select the applications that the members of the group can access in the Applications list on the right.

Authorize applications by account

This operation determines which applications an account can access.

Procedure

1. Log on to the IDaaS console as an IT administrator. For more information, see [Logon](#) in Administrator Guide.
2. In the left-side navigation pane, choose **Authorization > Application Authorization**.
3. Click the **Grant Application Access by Account** tab.



4. You can perform a fuzzy or exact search in the Accounts list on the left.

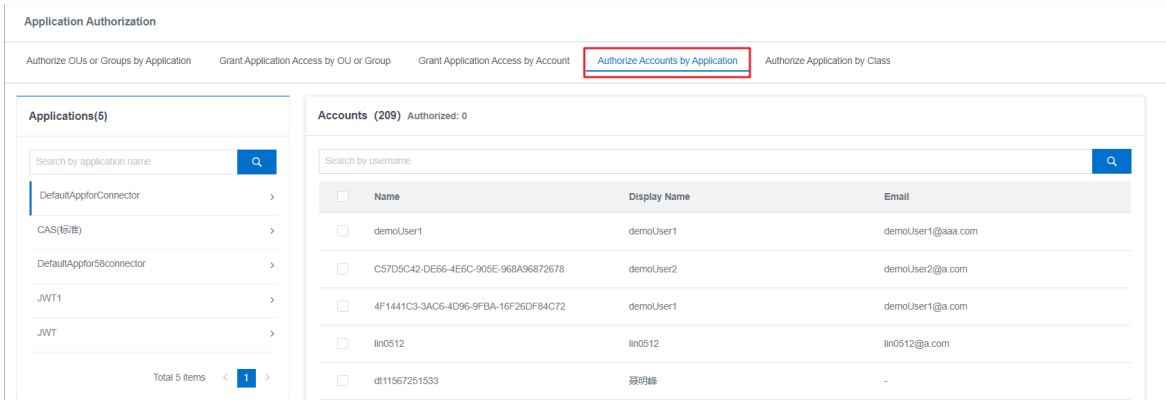
Note You can search for an application with the application name in the Applications list on the right.

Authorize accounts by application


This operation determines which accounts can access an application.

Procedure

1. Log on to the IDaaS console as an IT administrator. For more information, see [Logon](#) in Administrator Guide.
2. In the left-side navigation pane, choose **Authorization > Application Authorization**.
3. Click the **Authorize Accounts by Application** tab.



4. You can perform fuzzy or exact search in the Applications list on the left.

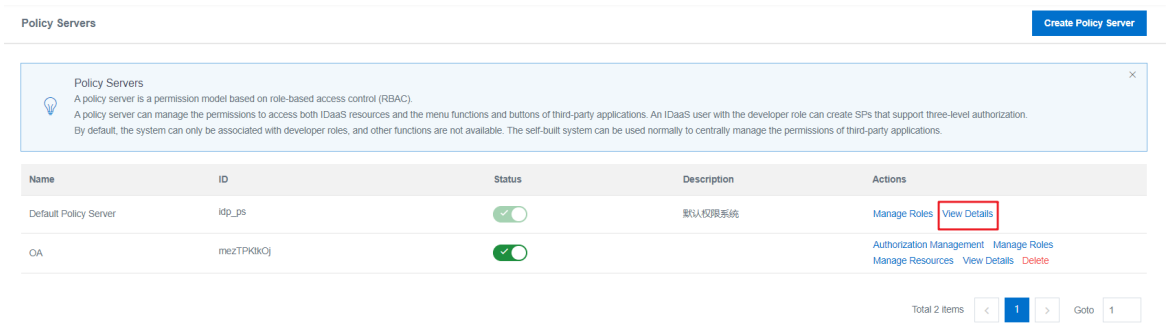
 **Note** You can search for an account with the account name in the Accounts list on the right.

1.4.2. Policy Server

This topic describes how to maintain policy servers in the IDaaS console, such as view details, perform administrator query, and manage roles.

View file system details

- 1. Log on to the IDaaS console as an IT administrator. For more information, see [Logon](#) in Administrator Guide.
- 2. In the left-side navigation pane, choose **Authorization > Policy Servers**.
- 3. Find the target policy server and click **View Details**.



4. The **View Details** page consists of the General Information and API Information sections.

View Details (IDaaS权限系统) ×

General Information

Name	IDaaS权限系统
ID	idp_ps
Description	默认权限系统
Status	Enabled
Enable SSO	No
Enable OTP	No
Enable QR Code Logon	No
Members	209
Roles	4
Permissions	39
Created By:	SYSTEM
Created At	2020-04-21 11:11

API Information

AppKey	
AppSecret	

全部显示

×

Create a policy server

1. Log on to the IDaaS console as an IT administrator. For more information, see [Logon](#) in Administrator Guide.
2. In the left-side navigation pane, choose **Authorization > Policy Servers**.
3. Click **Create Policy Server** in the upper-right corner of the page.

Policy Servers

Create Policy Server

Policy Servers

A policy server is a permission model based on role-based access control (RBAC).
A policy server can manage the permissions to access both IDaaS resources and the menu functions and buttons of third-party applications. An IDaaS user with the developer role can create SPs that support three-level authorization.
By default, the system can only be associated with developer roles, and other functions are not available. The self-built system can be used normally to centrally manage the permissions of third-party applications.

Name	ID	Status	Description	Actions
Default Policy Server	ldp_ps	<div><div></div></div>	默认权限系统	Manage Roles View Details
OA	mezTPKikOj	<div><div></div></div>		Authorization Management Manage Roles Manage Resources View Details Delete

Total 2 items

<1>

Goto1

4. In the **Create Policy Server** dialog box that appears, enter a server name and click **OK**.

Create Policy Server

*

Name

Name

*

系统ID

2HAKyq2n3e

The unique identifier of the policy server.

Description

Enter a description of the policy server

OK

Cancel

5. The new policy server is displayed on the Policy Servers page, with the **View Details**, **Manage Role**, **Manage Resources**, **Authorization Management**, **Modify**, and **Delete** available in the Actions column and the **Enable** switch available in the Status column.

Policy Servers

Create Policy Server

Policy Servers

A policy server is a permission model based on role-based access control (RBAC).
A policy server can manage the permissions to access both IDaaS resources and the menu functions and buttons of third-party applications. An IDaaS user with the developer role can create SPs that support three-level authorization.
By default, the system can only be associated with developer roles, and other functions are not available. The self-built system can be used normally to centrally manage the permissions of third-party applications.

Name	ID	Status	Description	Actions
Default Policy Server	ldp_ps	<div><div></div></div>	默认权限系统	Manage Roles View Details
HR	2HAKyq2n3e	<div><div></div></div>		Authorization Management Manage Roles Manage Resources View Details Modify Delete
OA	mezTPKikOj	<div><div></div></div>		Authorization Management Manage Roles Manage Resources View Details Delete

Total 3 items

<1>

Goto1

Manage roles

1. Log on to the IDaaS console as an IT administrator. For more information, see [Logon](#) in Administrator Guide.

2. In the left-side navigation pane, choose **Authorization > Policy Servers**.

3. Find the new policy server and click **Manage Roles** in the Actions column.

Policy Servers

Create Policy Server

Policy Servers

A policy server is a permission model based on role-based access control (RBAC).
A policy server can manage the permissions to access both IDaaS resources and the menu functions and buttons of third-party applications. An IDaaS user with the developer role can create SPs that support three-level authorization.
By default, the system can only be associated with developer roles, and other functions are not available. The self-built system can be used normally to centrally manage the permissions of third-party applications.

Name	ID	Status	Description	Actions
Default Policy Server	idp_ps		默认权限系统	Manage Roles View Details
OA	mezTPKIKOj			Authorization Management Manage Roles Manage Resources View Details Delete

Total 2 items

< 1 >

 Goto 1

4. On the Manage Roles page, you can perform the following tasks.
- o Create a role.
 - a. On the Manage Roles page, click **Create**.

Policy Servers / OA

← Manage Roles

Manage Roles

The policy servers in IDaaS support role-based access control (RBAC). A role can be associated with a range of permissions. Accounts assigned to a role have all the permissions of the role. This page allows the administrator to create, delete, or modify roles in the policy server.

Create

Import

Search by role name

<input type="checkbox"/>	Role	Permission ID	Permissions	Description	Status	External ID	Actions
<input type="checkbox"/>	role2	role2	0			role2	Add Permission Authorized to person Modify Delete
<input type="checkbox"/>	role1	role1	0			role1	Add Permission Authorized to person Modify Delete
<input type="checkbox"/>	Batch Delete						

Total 2 items

< 1 >

 Goto 1

- b. In the **Create Role** dialog box that appears, configure the following parameters.
- a. **Role**: the name of the role. The name must be unique.
 - b. **Permission ID**: the permission ID of the role.
 - c. **Status**: specifies whether to enable the role.
 - d. **Description**: the description of the role.

Create Role✕

* Role

Role

The specified name already exists.

* Permission ID

Permission ID

A permission ID is the unique identifier of a role or permission in IDaaS. Third-party systems can use permission IDs to identify and differentiate roles and permissions. A permission ID can contain only letters, digits, and underscores (_).

Status

Enable

Enable

Description

Enter a role description

Enter a description of the role.

Submit

- c. After configuring the parameters, click **Submit**.
- o Grant the role permissions.
 - a. On the Manage Roles page, find the target role and click **Add Permission**.

b. On the **Resources** tab of the **Manage Roles** page, select permissions to be grant.

Policy Servers / OA

← Manage Roles

Manage Roles

The policy servers in IDaaS support role-based access control (RBAC). A role can be associated with a range of permissions. Accounts assigned to a role have all the permissions of the role. This page allows the administrator to create, delete, or modify roles in the policy server.

Create Import Search by role name

Role	Permission ID	Permissions	Description	Status	External ID	Actions
<input type="checkbox"/> role3	role3	0			d57d6ed863d902eae3d050...	Add Permission Authorized to person Modify Delete
<input type="checkbox"/> role2	role2	0			role2	Add Permission Authorized to person Modify Delete
<input type="checkbox"/> role1	role1	0			role1	Add Permission Authorized to person Modify Delete
<input type="checkbox"/> Batch Delete						

Total 3 items < 1 > Goto 1

Policy Servers / HR

← Authorization Management

Authorized by person Authorize by role **idManager.v1.2.ps.authorizationManager.importRolePrivilege**

Authorization Management

Role authorization is a permission model Based on RBAC (Role-Based Access Control). You can manage both the system permissions of IDaaS and the level 2 and Level 3 authorization of third-party applications (developer role is required).

Role list (1)

role3

Total 1 item < 1 >

Associated with permissions **Authorize to account**

如果取消关联父级节点,对应的子级节点都会取消关联

HR

- ☐ ResourceA
- ☐ ResourceB
- ☐ ResourceC

Save


After the permissions have been granted, the number of permissions granted is displayed in the **Permissions** column of the role on the **Manage Roles** page.

- Modify a role.
 - a. On the **Manage Roles** page, find the target role and click **Modify**.
 - b. On the **General** tab of the **Manage Roles** page, you can modify the parameters of the role as needed.
 - c. After modifying the parameters, click **Save**.
- Delete a role
 - a. On the **Manage Roles** page, find the target role and click **Delete**.

Note The default role cannot be deleted.

- b. In the **System Prompt** message that appears, click **OK**.
- Batch delete roles.

- a. On the Manage Roles page, select the target roles and click **Batch Delete** at the bottom.

 **Note** The default role cannot be deleted.

- b. In the **System Prompt** message that appears, click **OK**.

2.Regular Users

2.1. Common Operations

This topic describes how to perform common operations in the IDaaS console, including logon-free applications, application management, and associating application accounts.

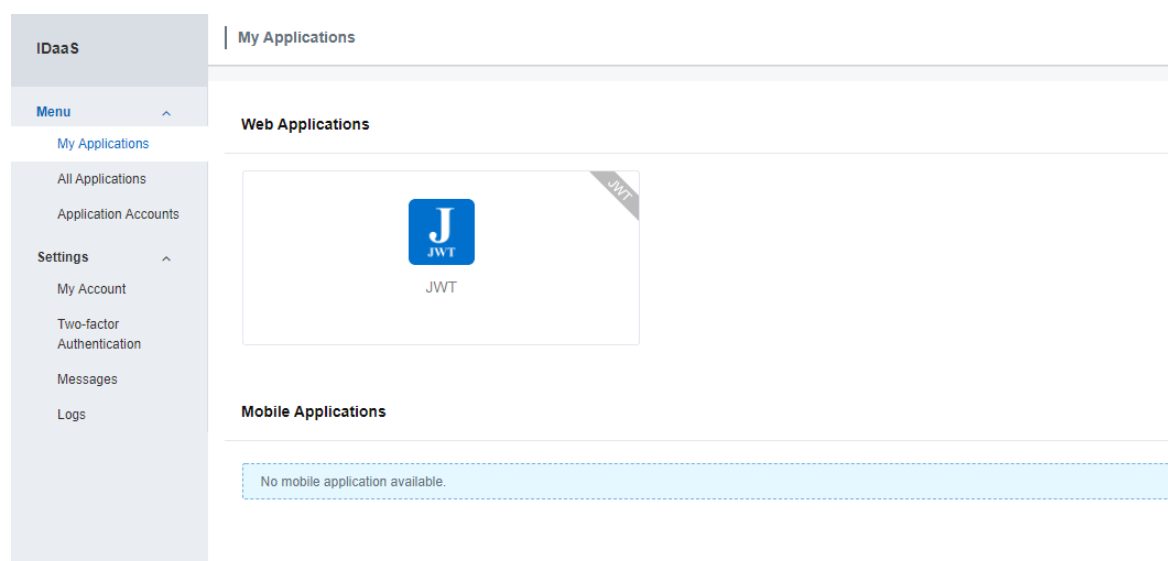
Logon-free applications

After logging on the IDaaS console as a common user, the My Applications page displays logon-free applications. Logon-free applications are generally enterprise-related applications. The IT administrator can configure single sign-on for these applications. To implement logon-free access to applications, you must perform the following operations after the IT administrator grants your account the application access permissions:

- Associate application accounts
- Enable applications

Procedure

1. Log on to the IDaaS console as a common user. For more information, see [Logon](#) in User Guide.
2. On the **My Applications** page, click a logon-free application to access the application.






Application management

On the All Applications page, you can maintain the information of applications displayed on the logon-free application page.

Procedure

1. Log on to the IDaaS console as a common user. For more information, see [Logon](#) in User Guide.
2. In the left-side navigation pane, choose **Menu > All Applications**.

IDaaS	Applications				
Menu My Applications All Applications Application Accounts Settings My Account Two-factor Authentication Messages Logs	Search by application name <input type="text"/> <input type="button" value="Q"/>				
	Application Logo	Application Name	Application ID	Application Type	Actions
		DefaultAppforConnector	idaas-cn-0pp1mb0e705jw3	DATA_SYNC	View Logs
		DefaultAppforS8connector	idaas-cn-0pp1mb0e705jw2	DATA_SYNC	View Logs
		JWT	idaas-cn-0pp1mb0e705jw1	WEB	View Logs

3. View application operation logs. In the left-side navigation pane, choose **Settings > Logs**.


IDaaS	Logs			
Menu My Applications All Applications Application Accounts Settings My Account Two-factor Authentication Messages Logs	All Logs <input type="text"/>			
	Log Type	Time	Content	IP
	Logon	2020/5/22 下午4:54:51		106.11.34.14
	Application Log	2020/5/22 下午1:59:40		106.11.34.14
	Application Log	2020/5/22 下午1:58:45		106.11.34.14
	Application Log	2020/5/22 下午1:57:20		106.11.34.14
	Application Log	2020/5/22 下午12:08:03		106.11.34.14
	Logon	2020/5/22 下午12:07:46		106.11.34.14
	Application Log	2020/5/22 下午12:04:42		106.11.34.14
	Application Log	2020/5/22 下午12:04:13		106.11.34.14
	Logon	2020/5/22 下午12:04:13		106.11.34.14
	Application Log	2020/5/22 下午12:04:13		106.11.34.14

Associate application accounts

If you want to log on to the application in a single sign-on manner after the IT administrator grants your account access permissions for a new application, you must associate an application account with the application.

Procedure

1. Log on to the IDaaS console as a common user. For more information, see [Logon](#) in User Guide.
2. In the left-side navigation pane, choose **Menu > Application Accounts**.
3. On the **Application Accounts** page, click **Add Application Account**.

IDaaS	Application Accounts				
Menu My Applications All Applications Application Accounts Settings My Account Two-factor Authentication Messages Logs	Sub-account list Sub-account approval				
	Add Application Account <input type="text"/> <input type="button" value="Q"/>				
	Application Logo	Application Name	Approval Status	IDaaS Account	Application Account
		JWT	Approved	lin0512	lin0512 Delete

Total 1 item < 1 > Go to 1

4. In the **Add Application Account** dialog box that appears, configure the following parameters:
 - o **Application**: the application to be associated.

Note The association operation varies depending on the account association method configured when the IT administrator added the application.

- If manual association (account association or account mapping) is configured, you must provide the correct username. The association will only be successful after being approved by the IT administrator. The IT administrator also can directly associate the application for you.
- When automatic association (account + password) is configured, you must provide the correct username and password. The association will only be successful after you pass the background authentication.

- **Application Account**: the username of the application account.
- **Application Account Password** and **Confirm Password**: the password of the application account. The two parameters are only required when automatic association is configured for the application.

The screenshot shows the IDaaS console interface. On the left is a sidebar with 'Menu' and 'Settings'. The main area displays 'Application Accounts' with a table listing applications. A modal window titled 'Add Application Account' is open on the right. It contains the following fields:

- Application**: A dropdown menu with 'JWT' selected.
- IDaaS Account**: A text input field containing 'in0512'.
- Application Account**: A text input field containing 'test'.

Below the fields is a note: "Note: This application account uses the Auto linking mode. The system uses the IDaaS account username or the specified field as the application username." At the bottom of the modal is a blue 'Save' button.

Note You can associate an application with multiple application accounts. Select an application account to grant logon-free access.

5. Click Save.

After application accounts have been associated and the application has been enabled, you can access the application with an application account without having to log on.

2.2. Logon


This topic describes how to log on to the IDaaS console as a common user.

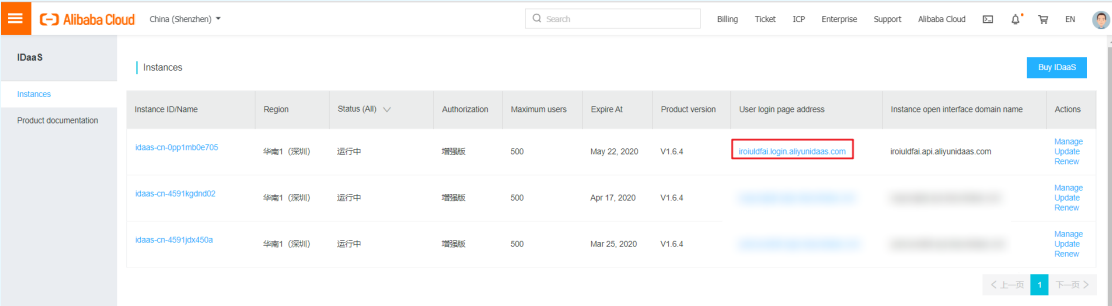
Common users are employee accounts created or imported by an IT administrator. They are end users of the IDaaS console. After creating a common user account, the IT administrator assigns application permissions to the account and configures the logon authentication method.

Common users can log on to the IDaaS console with portal addresses, view the applications that they are authorized to access on the authentication-free applications page, and associate applications with application accounts. After associated with application accounts, common users can access applications in a single sign-on manner.

Login from a PC

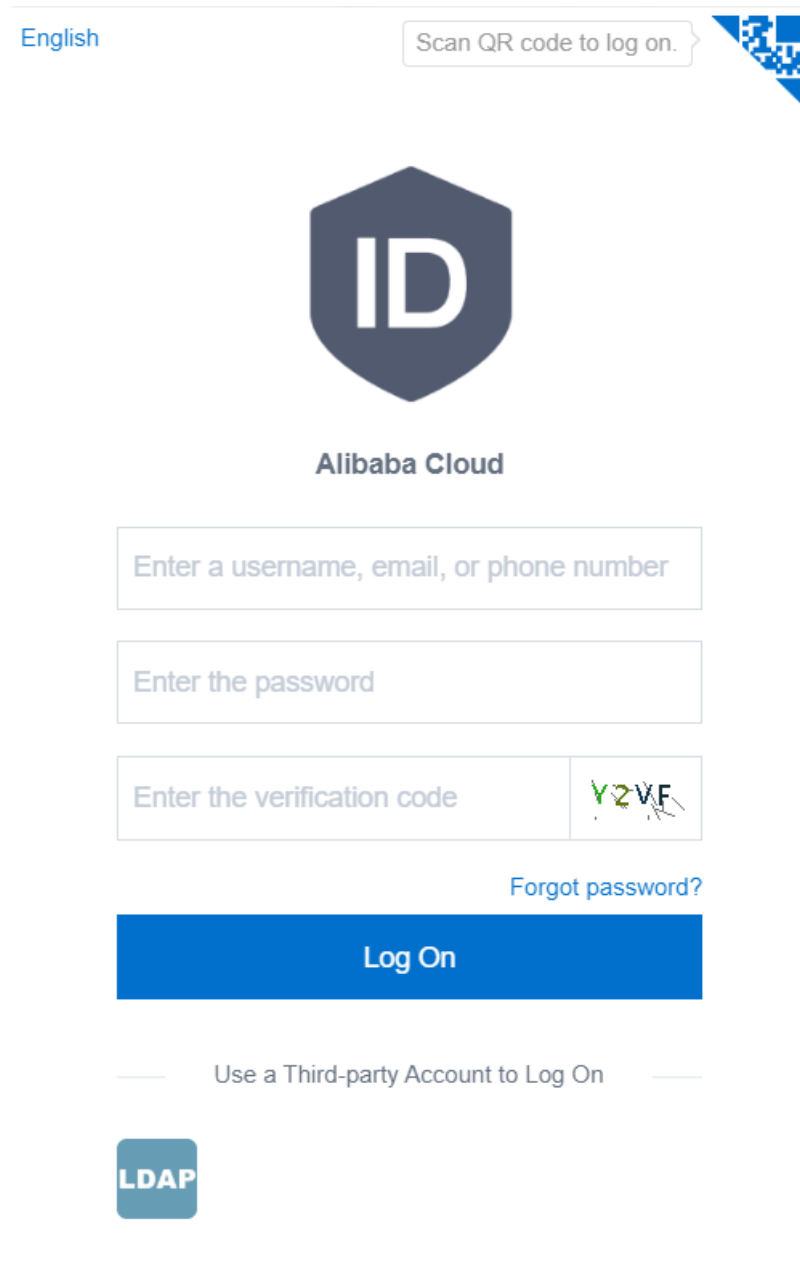
1. Access the IDaaS portal address from a PC browser.

 **Note** The portal address is provided by the IT administrator. The IT administrator can query the view portal addresses on the [Instance List](#) page.



Instance ID/Name	Region	Status (All)	Authorization	Maximum users	Expire At	Product version	User login page address	Instance open interface domain name	Actions
idaas-cn-0pptmb0e705	华东1 (深圳)	运行中	增权版	500	May 22, 2020	V1.6.4	iroudtfai login.aliyundaa.com	iroudtfai.api.aliyundaa.com	Manage Update Renew
idaas-cn-4591kgnd02	华东1 (深圳)	运行中	增权版	500	Apr 17, 2020	V1.6.4			Manage Update Renew
idaas-cn-4591jdx450a	华东1 (深圳)	运行中	增权版	500	Mar 25, 2020	V1.6.4			Manage Update Renew

2. Enter the mobile phone number, account username, or email address and password, and then complete authentication on the login page.



English

Scan QR code to log on.

ID

Alibaba Cloud

Enter a username, email, or phone number

Enter the password

Enter the verification code

Forgot password?

Log On

Use a Third-party Account to Log On

LDAP

2.3. Settings

This topic describes common settings of the IDaaS console including account settings, two-factor authentication settings, and viewing messages and logs.

Account settings

You can view the complete information of the current account on the **My Account** page.

Procedure


1. Log on to the IDaaS console as a common user. For more information, see [Logon](#) in User Guide.
2. In the left-side navigation pane, choose **Settings > My Account**.
3. Configure the following settings as needed:
 - o On the **Account Security** tab, you can change the **Login Password** of the account and bind

- On the **Account Security** tab, you can change the **Logon Password** of the account and bind an **Email** or **Phone Number**.

Note The bound mobile phone number can be used for logon through the phone number and password or through an SMS verification code. The bound email can be used for logon through the email address and password or for password retrieval.


My Account

Account Security General Information Certificate Third-party Accounts




Logon Password
This password is used to protect your account information and ensure logon security.

Change



Email *****@a.com
This email account is used to log on to IDaaS, reset the password, and receive messages from IDaaS.

Bound Change



Phone Number 166****1074
This phone number is used to log on to IDaaS, reset the password, and receive messages from IDaaS.

Bound Change

- On the **General Information** tab, you can view the applications and application accounts of the user account, and modify the **Display Name**.

My Account

Account Security **General Information** Certificate Third-party Accounts

Applications

3

Application Accounts

1

Username

lin0512

Display Name

lin0512

Save

- On the **Certificate** tab, you can view your certificate and the certificate password. You can also download your certificate locally.

My Account

Account Security General Information **Certificate** Third-party Accounts

Certificate

Expire At	2023-05-12 14:30
Generated At	2020-05-12 14:30
SubjectDN	CN=lin0512, L=BJ, ST=BJ, O=IDSMANAGER, OU=IDaa S, C=CN

[Download](#) [View Certificate Password](#)

- If the IT administrator has enabled external authentication and the external authentication source can be bound, you can bind third-party accounts on the **Third-party Accounts** tab.

Two-factor authentication

Common users can set whether to enable two-factor authentication. After two-factor authentication is enabled, common user can only log on to webpages after completing two-factor authentication with the push notification or dynamic token received on their mobile phones.

The following two-factor authentication methods are supported:

- **Mobile App authentication:** Two-factor authentication is implemented through the IDaaS App. The following authentication methods are supported:
 - Mobile terminals receive push notifications for two-factor authentication or scan QR codes for two-factor authentication.
 - Six-digit OTP codes displayed on mobile terminals are used for offline two-factor authentication, such as when push notifications cannot be received on mobile phones.
- **SMS verification code authentication:** Two-factor authentication is implemented with SMS verification codes.

Procedure

1. Log on to the IDaaS console as a common user. For more information, see [Logon](#) in User Guide.
2. In the left-side navigation pane, choose **Settings > Two-factor Authentication**.
3. Configure the following settings as needed:
 - On the **Two-factor Authentication** tab, you can select the **Enable** check box for two-factor authentication or select **Mobile App** or **SMS Verification Code** from the **Authenticate With** drop-down list.

- On the **Devices** tab, you can view all bound devices, discover and delete suspicious devices, or show QR codes and bind them to devices.

View messages and logs

Common users can view messages sent from the IDaaS console such as notices and announcements. Message that have been viewed are listed in read messages. Message that have been deleted are listed in deleted messages.

Procedure

- Log on to the IDaaS console as a common user. For more information, see [Logon](#) in User Guide.
- In the left-side navigation pane, choose **Settings > Messages**. On this page, you can view all messages.
 - The **Unread** tab lists all unread messages. You can **View** or **Delete** unread messages.
 - The **Read** tab lists all read messages. You can **View** or **Delete** read messages.
 - The **Deleted** tab lists all deleted messages. You can **View** deleted messages.

- In the left-side navigation pane, choose **Settings > Logs**. On this page, you can view all logs. You can filter logs by operation type.

Logs

All Logs

Log Type	Time	Content	IP
Logon	2020/5/22 下午4:54:51		106.11.34.14
Application Log	2020/5/22 下午1:59:40		106.11.34.14
Application Log	2020/5/22 下午1:58:45		106.11.34.14
Application Log	2020/5/22 下午1:57:20		106.11.34.14
Application Log	2020/5/22 下午12:08:03		106.11.34.14
Logon	2020/5/22 下午12:07:46		106.11.34.14
Application Log	2020/5/22 下午12:04:42		106.11.34.14
Application Log	2020/5/22 下午12:04:13		106.11.34.14
Logon	2020/5/22 下午12:04:13		106.11.34.14
Application Log	2020/5/22 下午12:04:13		106.11.34.14