# Alibaba Cloud

Identity as a service User Guide

Document Version: 20220322

C-J Alibaba Cloud

### 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.

- You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloudauthorized 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 and/or its affiliates 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
A 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.
O 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.
디) 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.
⑦ Note	A note indicates supplemental instructions, best practices, tips, and other content.	Onte: 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.
Courier font	Courier font is used for commands	Run the cd /d C:/window command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	bae log listinstanceid Instance_ID
[] or [a b]	This format is used for an optional value, where only one item can be selected.	ipconfig [-all -t]
{} or {a b}	This format is used for a required value, where only one item can be selected.	switch {active stand}

# 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	<mark>0</mark> 8
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.

IDaa S	Interest									Buy (DaaS
Product document	Instance ID/Name	Region	Status (All) 🗸	Authorization	Maximum users	Expire At	Product version	User login page address	Instance open interface domain name	Actions
				-						Manage Update Renov
				-						Manage Update Renov

### Results

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

😑 🕞 Alibaba Cloud	I				Q Search			
Overview	Overview							
Quick Start								
Applications ^ Application List	Albaha Cixad DasS Witkoms to IDuaS Need Net/7 Os to Ouic/ Start e aprovime topicad in need to be processed. Gis to Approvals							
Add Applications								
Users ^	Useful Links	Applications		Users				
Organizations and Groups	Manage Applications							
Accounts	Manage OUs, Groups, and Accounts	0		1				
Class Management	Manage Application Authorizations Manage Roles and Permissions							
Authentication ^	View Audit Logs Custom Security Settings	Search by application name		Search by username				
Authentication Sources								

# 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.

- 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.

pplication List					Add Application
After an appl	lows the administrator to manage applicatio	ns. Once added to IDaaS, applications support single sign on able the application and authorize application access to users.		bout applications, including SSO URLs, applic	$\ \times$ ation accounts, user provisioning settings, auth
earch by application na	ame		٩		
Application Logo	Application Name	Application ID	Device Type	Application Status	Actions
J	JWT	20200313110953GDMJ2Dy8pejwt8	Web Application		Authorize Details
Application Infor	mation	Authentication Information	Account Information - Provisionir	ng Account Infor	mation - Account Linking
Details of the appl View Details Delete Application	etails Modify Application IDaaS-initiated SSO URL		Modify SCIM settings and provision he application. Provision OUs Configure SCIM	S.	counts that are linked with IDaaS account on Accounts
Authorization Inf	formation	Audit Information	API		
Groups and accou application. Authorize	unts that are authorized to manage the	View detailed operation logs about the application. View Logs View Provisioning Records	Whether to apply open system API	rret	

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

Once 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 http://jzyt.idp- local.com/api/application/cs_multibrowser/scim/ account_password.
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	<ul> <li>The type of the authentication protocol used to verify requests. Valid values:</li> <li>Basic</li> <li>OAuth2</li> </ul>
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.

X

Configure SCIM (JWT)

Account	组织机构
Application Name	JWT
* SCIM Service	http://demo.com/api/application/scim/account
UNE	The URL is used to receive provisioning information. For example, http://xxx.com/api/application/sci m/account
Enable	NO
	Once enabled, when you create, modify, or delete an account, the account information will be autom atically 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	
1 40011010	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.

C-) Alibaba Clou	d			Q Search	Expenses	Tickets ICP	Enterprise	Support	Official Site	₽_	ġ <b>.</b> ()	EN
verview uick Start pplications ^ Application List	This page	ion templates can be divid			d applications to IDaaS based on these Is that you can use to implement SSO		AS, and SAML.	The other is	customized ar	d provides	APIs for SS	: 60 or use
Add Applications	Search by application	on name			Q							
organizations and Groups	Application Logo	Application Name	Application ID	Тад	Description			Applic	ation Type		Action	
Accounts Management Class Management		C/S Application	plugin_cs_oidc	CS, PC, OIDC	After wake-up application, it pass protocol to realize login, which is receive and parse the parameters	suitable for applic	ations that can	c PC Cli	ent		Add Ap	plication
hentication ^ Authentication Sources RADIUS	Ccus	CAS	plugin_cas_apereo	SSO, CAS	CAS (central authentication servir single sign on protocol based on used in the enterprise when the n client and the server is smooth. It integration and strong scalability.	challenge and res network between t t has the advantag	ponse. It is wide he integrated	y Web A Applic	pplication, Mob ation	ile	Add Ap	plication
Certificate Management norization ^ Policy Servers Application Authorization	J	TWL	plugin_jwt	SSO, JWT	JWT (JSON web token) is an ope declared in network application e single sign on (SSO) of distribute on asymmetric encryption. IDA as information with private key. After application decrypts and verifies i scenarios are very extensive and	nvironment. Idaas id sites. JWT singl s encrypts the use passing it to the a it with public key.	uses JWT for e sign on is base r's status and application, the The usage	Web A	pplication, Mob ation, PC Client		Add Ap	plication
lit × re ×	OALTH	OAuth2	plugin_oauth2	OAuth2	OAuth is an open resource autho obtain token access through OAu the server to request user resourc application template to realize un	th_ Token, and ca ces. Application ca	irry the token to an use OAuth	Web A	pplication		Add Ap	plication

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

C-J Alibaba Clo	ud				Q Bearch Expenses Tickets ICP Enterprise S	upport Official Site 💽	<b>∆'</b> ⑦ EN
arview	Add Application						
k Start	All Standard Pr	rotocols Custom Tem	plates				
cations ^ upplication List udd Applications s ^ organizations and Groups uccounts Management	W This pag	on templates can be divide			splications to IDaaS based on these templates. If you can use to implement SBO, such as XVIT, CAS, and SAML. The other is customized and provides APIs for SBO or user provisioning.		>
lass Management	Application Logo	Application Name	Application ID	Tag	Description	Application Type	Actions
ntication ^	C-)	Alibaba Cloud RAM - User SSO	plugin_aliyun	SSO, SAML, Aliyun	Based on SAML protocol, IDA as single sign on to the alicoud console is realized. To use this template, it is necessary to create a ram sub account for each user in RAM. The IDA as account and ram sub account are mapped to realize single sign on to ram.	Web Application	Add Application
ADIUS ertificate Management	C-)	Alibaba Cloud RAM - Role SSO	plugin_aliyun_role	SSO, SAML, Aliyun	Based on SAML protocol, IDA as single sign on to the allcloud 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. IDA as accounts and ram roles can be mapped to achieve single sign on to ram.	Web Application	Add Application
rization ^	J	JWT	plugin_jwt	SSO, JWT	VMT LGX0 web been is an open standard based on JSON idicated in intervolt application environment. Idiaat uses JMT for indige sign at (SSO) id distributed in the IAV standard standard and intervoltation with private key. After passing it to the application, the application discryptis and verifies it with public key. The usage scenarios are very ententive and the intergration is simple.	Web Application, Mobile Application, PC Client	Add Application
v	<b>O</b> MUTH	OAuth2	plugin_oauth2	OAuth2	O/uth is an open resource authorization protocol. Applications can obtain token access through O/uthToken, and carry the token to the server to request user resources. Application can use O/uth application template to realize unified identity management.	Web Application	Add Application
, v 18	S	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 (Daas) and the token comsumer (application), and activeves single sign-on targetting cross-domain networks: SAML is markur authentication protocol, which is widely used in public and private could a time and attraves.	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, logitatic, tavel, tinance and other aspects. With 1000 global partners, SAP is widely distributed in 5 different industries, providing digital management solutions for various stages of enterprises.	PC Client	Add Application
	<i></i>	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. (Daa8 supports single sign-on to salesforce website through SAML protocol.	Web Application	Add Application
	W	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 veloates through a very powerful pip-y system and a converient and natival operative interface. From business weblies and operement pages to personal blog and theme forums, WordPress supports a variety of forms.	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.

? Note Parameters marked with asterisks are required.

	Add Application					Add Application (JA	NT)
Start	All Standard Pr	otocols Custom Temp	dates				The image size must be less than 1 MB.
tions ^						Application ID	idaas-ap-southeast-1-\$3g\$lod8sw8plugm_jwt
d Applications	This page				applications to IDaaS based on these templates.	* Application Name	JNT.
					at you can use to implement SSO, such as JWT, CA	* Application Type	🗹 Web Application 🔯 Mobile Application 💆 PC
counts Management							Web app <sup>1</sup> and PC client will only be displayed in the user's web using environment, and 'mobile app <sup>1</sup> will only be displayed in the user's client. If you want to dis apps in multiple environments, check multiple.
ss Management	Application Logo	Application Name	Application ID	Тад	Description	* redirect_uri	Enter the application SSO URL. For example, http://www.coc.com/ssolparse.
ication ^	(-)	Alibaba Cloud RAM - User SSO	plugin_aliyun	SSO, SAML, Aliyun	Based on SAML protocol, IDA as single sign on t account and ram sub account are mapped to rea		The URL is used by the service provider to receive SSO parameters. In an SSO, IDaaS sends the kL_baten parameter to this URL in a CET request. The service provider uses the IDaaS-provided public key to verify the id_baten parameter. You can view the public key on the application details page. If the verification is successful, IDaaS can then obtain user internation from the service provider.
IUS ficate Management	<b>C</b> -)	Alibaba Cloud RAM - Role SSO	plugin_allyun_role	SSO, SAML, Aliyun	Based on SAML protocol, IDA as single sign on t accounts for each user. IDA as accounts and ran	Target_link_url	The URL that users will be directed to after logon. For example, http://www.coc.com/service/message.
ation ^	J	JWT	plugin_jwl		JWT (JSON web token) is an open standard bas sign on is based on asymmetric encryption. IDA with public key. The usage scenarios are very ex		Optional: The target URI of the service provider after the JV/T SSO is successful. This URL usually points to a secondary menu. If specified, a parameter name target_init_uris used to pass this value. If not specified and a target_linit_uri parameter exists in the request, the parameter will be passed accordingly.
ation Authorization		OAuth2	plugin_cauth2	OAuth2	OAuth is an open resource authorization protoco Application can use OAuth application template t	SSO Binding	REDIRECT Single sign on request mode, redirect is get type
	Suc	SAML	plugin_sami	SSO, SAML	SAML (security assertion markup language, vers (IDaaS) and the token consumer (application) an and private cloud at home and ateroad.	Include user token	Does the id_loken contain the user access_loken?
	-	SAP GUI	plugin_sap_gui		SAP GUI is a graphical user interface used by So data analysis, HR, logistics, travel, finance and o for various stages of enterprises.	ID_Token Validity	600 The validity period of kt_token. Unit: seconds.
	<b>\$</b>	Salesforce	plugin_salesforce		Salesforce is widely used public cloud CRM platt management, task management, event dynamic	Display Application	Whether to display the application on the user homepage after a user is authorized to access the application.
	0	WordPressSaml	plugin_wordpress_saml	SSO, SAML, CMS	WordPress is the most widely used CMS (conter types of websites through a very powerful plug-in theme forums, WordPress supports a variety of t	Account Linking Type	O Account association (the system performs manual association in line with corresponding relationship between the main-account and sub-account and odministrator approval is required after the user is added)
	F	Form Submit	plugin_aes256	SSO, AES256	Form submit can simulate a login mode in which application is stored locally in IDaaS using aes25 support transformation can use form filling to ach not applicable.		Account mapping (the system automatically maps the main account name or specified field to the application's sub-account)
	0	DDtalk		DingTalk	It is a free communication and cooperation platfo		

5. Click Submit.

### Results

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

### What to do next

Authorize an application

# 1.3. Users 1.3.1. Groups

This topic describes how to create, modify, and remove or delete groups in the IDaaS console.

### Create a group

You can add a group under an organization to manage (provision) multiple accounts or groups at a same. A group can contain other groups or accounts as its members. All members in a group can be provisioned as a whole.

- 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, right-click the organization to which the group to be created belongs and choose Add > Group from the shortcut menu.

 OUs

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

 Import

 Alibaba Clence

 Add
 OU

 Import
 Group

 AD
 Account

 Import
 Import

 Import
 Import

 Import
 Import

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 Attrib	outes	Extend	ed Attributes	Mutually Exclusive Groups
Parent OU	Alibab	a Cloud		
* Name	Entera	a name		
External ID	Entera	an external II	)	
Description	Entera	a description		
	Subr	nit Cl	ose	

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	s (*) are required.	
В			
Su	bmit Close		

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

Cı	reate Gro	oup			×
	Group A	ttributes	Extended Attributes	Mutually Exclusive Groups	
	Q Sear	ch by name			
		Name	Туре	Description	Directory
		111111	User-created	Group	
		team1	User-created	Group	
		team2	User-created	Group	
	Submit	Close		Total 3 items <	1 > Goto 1

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.

- 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.

Alibaba Cloud View Details		Position Change V Impo	t v Export v Configure LDAP	Configure DingTalk sync
Account Group OU				
Create Group Search by name		Q		
Name	Туре	Description	Actions	
TEST	User-created Group	1	Modify Delete	
111111	User-created Group	1	Modify Delete	

- 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.
  - Add account members
    - a. On the Members (Accounts) tab, click Add Members.

General	Members (Accounts)	Mutually Exclu	sive Groups	Add Member	Import Membe
earch by n	ame		Q		•
	Account Name	Туре	Description	Directory	Actions
			No Data		
			Total	0 item < 1	Goto 1

×

# 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.

4	Add	Members	

Search by	username	Q			
couldr's y					
	Account Name	Туре	Description	Directory	
	demoUser1	User-created Account			
	C57D5C42-DE66-4E6C-905E -968A96872678	Provisioned Account			
	4F1441C3-3AC6-4D96-9FBA- 16F26DF84C72	Provisioned Account			
	lin0512	User-created Account			
	dt11567251533	Provisioned Account			
	dt21328822228	Provisioned Account			
	dt14756111111	Provisioned Account			
	dt36002607117	Provisioned Account			
	dt21310658399	Provisioned Account			
	dt97296248448	Provisioned Account			
					_

### c. Click OK.

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

### • Add mutually exclusive groups

a. On the Mutually Exclusive Groups tab, click Add Mutually Exclusive Group.

testAttribute	s				×
General	Members (Accounts)	Mutually Exclusive	Groups	Add Mut	ually Exclusive Group
Search by na	ame	C	2		
	Name	Туре	Description	Directory	Actions
			No Data		
			Total (	Ditem < 1	> Goto 1

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

•	- Add Mu	utually Exclusive Group				$\times$
	Search by	y name	Q			
		Name	Туре	Description	Actions	
		TEST2	User-created Group		阿里云IDAAS	
	ок	Cancel		Total 1 item <	1 > Goto 1	

### 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.

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

Alibaba Cloud View Details		Position Change ~	Import ~ Export ~	Configure LDAP Configure DingTalk sy
Account Group OU				
Create Group Search by name	Q			
Name	Туре	Description		Actions
TEST2	User-created Group	1		Modify Delete
TEST	User-created Group	1		Modify Delete
			Total 2 items	1 > 10 /page ~ Goto 1

c. In the System Prompt message that appears, click OK.

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

- d. In the **Incremental Provisioning** dialog box that appears, perform provisioning operations after you delete the group.
- Remove a group
  - a. In the OUs window on the left, find the organization to which the group to be removed belongs and click its name.
  - b. On the Group tab, find the group to be removed and click Remove in the Actions column.

bborganization View Details		Position Change V In	nport ~ E	Export 🗸	Configure LDAP	Configure DingTalk syn
Account Group OU						
Create Group Search by name	Q					
Name	Туре	Description			Actions	
TeamA	User-created Group	/zbborganization			Modify Remove	]
			Total 1 item	< 1	> 10 /pa	ge∨ Goto 1

c. 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.

OUs	Alibaba Cloud View Details			ition Change ~ Import ~	Export ~ Configure LDAP	Configure DingTalk sync
Manage the organization's architecture here. Y × ou can left-click and select the OU, right-click a n OU to manage it.		oup OU arch by name Q				
Alibaba Cloud     E-      E-	OU Name	Туре	Description	Status	Actions	
connector     demo1	demo1	Provisioned OU	1		Modify Provision Provisioning Re-	

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

OUs		
0 0	nization's architectur I select the OU, right-	
Alibaba C	Add	> OU Group
⊕ □ ● AD ⊕ □ ● LDA	ι	Account

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
	<ul> <li>The type of the organization. Valid values:</li> <li>Organization</li> <li>Department</li> </ul>
Туре	<b>Note</b> An organization is generally associated with an administrative region. A department is generally a functional organization. An organization is usually divided into multiple departments.
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
* Туре	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 gene rated, 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		$\times$
OU Attributes	Extended Attributes	
The extended	attributes. Fields marked with asterisks (*) are required.	
dingtalkInstan celd		
dingtalkCropId		
dingtalkDepart mentId		
	Submit Close	

- 7. After configuring the parameters, click **Submit**.
- 8. 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.	<ul> <li>Application Authorization 3</li> <li>Application permissions of the pare nt OU or group are automatically in herited.</li> </ul>	SCIM Provisioning Use SCIM to provision data to auth orized applications.
Provision Result		
Successes: 0 Failures:		
Note:		
		Next Cancel

ncremental Provisioning		>
Provision data to all LDAPs.	2 Application Authorization 3 Application permissions of the pare nt OU or group are automatically in herited.	SCIM Provisioning Use SCIM to provision data to autorized applications.
Application permissions of the parent	OU or group are automatically inherited. T	he details are as follows:
Just DefaultAppforConnector	JWT	
DefaultAppfor58connector		
	То	tal 3 items < 1 >
		Next Cancel
ncremental Provisioning		
· · ·	Application Authorization — 3	SCIM Provisioning
	Application Authorization — 3 Application permissions of the pare nt OU or group are automatically in herited.	SCIM Provisioning
LDAP Provisioning (	Application permissions of the pare nt OU or group are automatically in herited.	SCIM Provisioning Use SCIM to provision data to aut
LDAP Provisioning     Provision data to all LDAPs.	Application permissions of the pare nt OU or group are automatically in herited.	SCIM Provisioning Use SCIM to provision data to aut
LDAP Provisioning (     Provision data to all LDAPs.     Available applications with provision c	Application permissions of the pare nt OU or group are automatically in herited.	SCIM Provisioning Use SCIM to provision data to aut orized applications.

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	Alibaba Cloud View	Details	Pos	sition Change ~ Import ~	Export ~	Configure LDAP	Configure DingTalk syn
Manage the organization's architecture here. Y $\qquad \times \qquad$ ou can left-click and select the OU, right-click a n OU to manage it.	Account Gro	·					
Alibaba Cloud	Create OU Sea	arch by name Q					
± com zbbOrganization	OU Name	Туре	Description	Status		Actions	
connector     demo1	demo	User-created OU	I			Modify Provision Provisioning Record	ts Delete
- 🗆 🏢 demo						Modify Provision	

### 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.

OUs	demo View Deta	ils		Position Change ~	Import ~	Export ~	Configure LDAP	Configure DingTalk sync
Manage the organization's architecture here. Y $\qquad \times$ ou can left-click and select the OU, right-click a	Account	Group OU						
n OU to manage it.	Create OU	Search by name						
Alibaba Cloud	OU Name	Туре	Description	Stat	us		Actions	
connector     demo1     demo				No Data				

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

	nization's architectur nd select the OU, rig it.	
Alibaba Clo	ud	
🗋 📠 dem	Add	1
🕂 🗆 🏦 coni	,	-
🗆 🏦 dem	Import	
🛓 🗆 🔝 jzyt	Disable	
🗋 Don	Delete	
🕂 🗆 🔝 Syst	Mobile	
🗋 🛄 Fore	Attaitester	-
	Attributes	

- 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.

Onte 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.

OUs	Alibaba Cloud View Details			ition Change ~ Import ~ Expo	rt v Configure LDAP Configure DingTalk sync
Manage the organization's architecture here. Y $\times$ ou can left-click and select the OU, right-click a n OU to manage it.	Account Grou	b OU			
Alibaba Cloud	OU Name	Туре	Description	Status	Actions
terror demo1	demo	User-created OU	I		Modify Provision Provisioning Records Delete
Domain Controllers	demo1	Provisioned OU	I		Modify Provision Provisioning Records Delete

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.

OUs	Alibaba Cloud View D	etails	Po	sition Change ~ Impor	t ~ Export ~	Configure LDAP	Configure DingTalk sync
Manage the organization's architecture here. Y × ou can left-click and select the OU, right-click a	Account Grou	p OU					
n OU to manage it.	Create OU Searc	ch by name Q					
Alibaba Cloud     demo1	OU Name	Туре	Description	Status		Actions	
	demo	User-created OU	I			Modify Provision Provisioning Reco	
Domain Controllers     Domain System	demo1	Provisioned OU	I			Modify Provision Provisioning Reco	

### 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.

- 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.

OUs	
Manage the organization's architecture here. Y $\times$ ou can left-click and select the OU, right-click a n OU to manage it.	
Alibaba Cloud	
Delete Mobile Attributes Unts	

- 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.

OUs	Alibaba Cloud View D	etails	Po	sition Change 🗸 Import 🗸 E	xport v Configure LDAP Configure DingTalk sync
Manage the organization's architecture here, Y × ou can left-click and select the OU, right-click a	Account Grou	o OU			
n OU to manage it.	Create OU Searc	h by name Q			
Alibaba Cloud	OU Name	Туре	Description	Status	Actions
C  connector	demo	User-created OU	1	$\checkmark \bigcirc$	Modify Provision Provisioning Records Delete
	demo1	Provisioned OU	1	$\checkmark \bigcirc$	Modify Provision Provisioning Records Delete
庄 🗆 🎰 System	B				11 M 10 M 10

- 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.

- 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.

OUs		
0 0	nization's architecture h select the OU, right-clio	
Alibaba Cl	Add >	OU
	Import	Group
÷. 🗆 🏬 AD		Account
🕂 🗆 🗐 LDA	P	

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

OUs	Alibaba Clou	d View Details		F	Position Change ~	Import ~	Export ~	Configure LDAP	Configure DingTalk sync
Manage the organization's architecture here. Y × ou can left-click and select the OU, right-click a n OU to manage it.	Account Create Acco Current acco			拨款					
- C III demo	编号	Name	Display Name	Туре	Description		Actio	ons	
i izyt □ III Domain Controllers	□ 1	demoUser1	demoUser1	User-created Account	/ 阿里云IDAAS			fy Move Provision isioning Records Ma	
C      System     SereignSecurityPrincipals     Managed Service Accounts	2	4F1441C3-3AC6- 4D96-9FBA-16F2 6DF84C72	demoUser1	Provisioned Ac count	<sup>C</sup> / 阿里云IDAAS			fy Move Provision isioning Records Ma	

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

OUs	Alibaba C	loud View Details		P	osition Change ~	Import ~	Export ~	Configure LDAP	Configure DingTalk sync
Manage the organization's architecture here. Y × ou can left-click and select the OU, right-click a n OU to manage it.	Account Create A	Group OL			Enroll Move Mark as Resigned				
Alibaba Cloud			ased package specification is 5		Description				
🔁 🗆 🛄 connector		号 Name	Display Name	Туре	Description		Actio		
+-  Domain Controllers	□ 1	demoUser1	demoUser1	User-created Account	/ 阿里云IDAAS			ly Move Provision. sioning Records Ma	
Comparison of the system     Comparison of the system     Comparison of the system of the syste	2	4F1441C3-3AC6- 4D96-9FBA-16F2 6DF84C72	demoUser1	Provisioned Ac count	/ 阿里云IDAAS			y Move Provision sioning Records Mar	

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.

ParameterDescriptionDisplay NameThe display name or alias of the account. It must be 2 to 18 characters in length.Account NameThe 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.PasswordThe 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.EmailThe email address associated with the account.Phone NumberThe mobile phone number associated with the account.Phone NumberThe 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 OnThe expiration date of the account. If you do not specify this parameter, the default expiration date is used.RemarksThe remarks for the account.		
Display Name       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, lowercase letters, digits, and special characters. It must be six or more characters in length.         Email       The email address associated with the account.         Phone Number       The mobile phone number associated with the account.         Phone Number       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.	Parameter	Description
Account Namecontain uppercase letters, lowercase letters, digits, hyphens (-), underscores (_), and periods (_). It must be 4 to 18 characters in length.PasswordThe password of the account. The password must contain uppercase letters, lowercase letters, digits, and special characters. It must be a six or more characters in length.EmailThe email address associated with the account.Phone NumberThe mobile phone number associated with the account.Phone NumberThe email address or phone number is required.External IDThe external ID of the account. The external ID ass. If you do not specify this parameter, it is automatically generated by IDaas.Expires OnThe expiration date of the account. If you do not specify this parameter, the default expiration date of the account.	Display Name	
Passwordmust contain uppercase letters, lowercase letters, digits, and special characters. It must be six or more characters in length.EmailThe email address associated with the account. ⑦ Note The email address or phone number is required.Phone NumberThe mobile phone number associated with the account. ⑦ Note The email address or phone number is required.External IDThe 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 OnThe expiration date of the account. If you do not specify this parameter, the default expiration date is used.	Account Name	contain uppercase letters, lowercase letters, digits, hyphens (-), underscores (_), and periods
EmailImage: Note of the email address or phone number is required.Phone NumberThe mobile phone number associated with the account.Phone NumberImage: Note of the email address or phone number is required.External IDThe 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 OnThe expiration date of the account. If you do not specify this parameter, the default expiration date is used.	Password	must contain uppercase letters, lowercase letters, digits, and special characters. It must be
number is required.         Phone Number       The mobile phone number associated with the account.         ⑦ Note The email address or phone number is required.         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.		The email address associated with the account.
Phone Numberaccount.? Note The email address or phone number is required.External IDExternal IDExpires OnThe expiration date of the account. If you do not specify this parameter, it is automatically generated by IDaaS.The expiration date of the account. If you do not specify this parameter, the default expiration date is used.	Email	
When a basis of the second s		· · · · ·
External IDthe unique ID of an account in IDaaS. If you do not specify this parameter, it is automatically generated by IDaaS.Expires OnThe expiration date of the account. If you do not specify this parameter, the default expiration date is used.	Phone Number	
Expires On       specify this parameter, the default expiration date is used.	External ID	the unique ID of an account in IDaaS. If you do not specify this parameter, it is automatically
<b>Remarks</b> The remarks for the account.	Expires On	specify this parameter, the default expiration
	Remarks	The remarks for the account.

Account Attrib	outes	Extended Attributes	Parent Groups	
Parent OU	Alibaba C	loud		
Account Name	Enter an a	account name		
		t name can containUppe at least 4 characters in le	ercase Letter、Lowercase Letter、Digit、Hyphen (-)、Underscore (_)、Period (.)、The passv length.	NOI
Display Name	Enter a di	isplay name		
Password	Enter a pa	assword		
	The passwo		case letters, lowercase letters, digits, and special characters.; The password must be at least	t 6
Email	Enter a va	alid email address		
	Optional. S	pecify a phone number	or an email address, or both.	
Phone Number	+86	✓ Enter a valid phon	ie number	
	Optional. S	pecify a phone number	or an email address, or both.	
External ID	Enter an e	external ID		
	The unique	e identifier of this accourt	nt in IDaaS. If you do not specify an ID, the system automatically generates a value.	
	Select an	expiration date	1	
Expires On	Optional. If	you do not specify this	parameter, the default expiration date (December 31, 2116) will be used.	
Expires On				
Expires On Remarks	Enter rem	narks		

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

C	eate Account	$\times$
	Account Attributes Extended Attributes Parent Groups	
	The extended attributes. Fields marked with asterisks (*) are required. Data Dictionary to add or enable one.	
	ngtalkInstance	
	ngtalkCropId	
	ngtalkUserid	
	ngtalkUnionId	
	ngtalkPosition	
	ngtalkAvatar	
	Submit Close	

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

С	reate Acc	count					$\times$
	Account	Attributes	Extended Attributes	Parent Groups			
	Note: Ma	ake sure the sele	ected group and the existing pa	arent groups of this ac	count are not mutually exclusi	ve.	
	Search by	/ name		Q			
		Name	Туре		Description	Directory	
		TeamA	User-crea	ited Group			
		TEST2	User-crea	ited Group			
		TEST	User-crea	ited Group			
	Submit	Close			Total 3 items	< 1 > Goto	1

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

			A				· ·	
	DAP Provisioning rovision data to all LDAPs.	- (2)	Application	ion Authorizat on permissions group are auto	of the pare		provision dat	a to au
Pro	ovision Result							
	Successes: 0 Failures:							
	Note:							
						Next	Cance	1
						I TEA	Cance	-1
							Cance	•
crem	nental Provisioning						Cance	
	nental Provisioning	- 2	Applicati	ion Authorizat	ion — (3			
) LC		- 2	Application	ion Authorizat on permissions group are auto	of the pare	SCIM Provis	sioning provision dat	
) LC Pr	DAP Provisioning		Application nt OU or herited.	on permissions group are auto	of the pare omatically in	SCIM Provis Use SCIM to orized applic	sioning provision data ations.	
Pr App	DAP Provisioning rovision data to all LDAPs.	arent OU	Application nt OU or herited.	on permissions group are auto are automatica	of the pare omatically in ally inherited. Th	SCIM Provis Use SCIM to orized applic	sioning o provision dat ations. s follows:	
Apj	DAP Provisioning rovision data to all LDAPs. plication permissions of the pa	arent OU	Application nt OU or herited.	on permissions group are auto are automatica	of the pare omatically in ally inherited. The	SCIM Provis Use SCIM to orized applic the details are a	sioning o provision dat ations. s follows:	
App	DAP Provisioning rovision data to all LDAPs. plication permissions of the pa	arent OU	Application nt OU or herited.	on permissions group are auto are automatica	s of the pare omatically in ally inherited. The Default	SCIM Provis Use SCIM to orized applic the details are a	sioning o provision dat ations. s follows:	

Incremental Provisioning ×								
LDAP Provisioning     Provision data to all LDAPs.	Application Authorization — 3 Application permissions of the pare nt OU or group are automatically in herited.	SCIM Provisioning Use SCIM to provision data to auth orized applications.						
Available applications with provision con	figured:							
Available applications without provision of DefaultAppforConnector	configured:	nector						
		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.

- 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.

Organizations and Groups This page allows the administrator to manage inforr The administrator can manage OUs and groups by							
OUs	Alibaba Cloud View Details		P	osition Change ~	Import v Export v	Configure LDAP	Configure DingTalk sy
Manage the organization's architecture here, Y $\qquad \times$ ou can left-click and select the OU, right-click a n OU to manage it.	Account Group Create Account Account	OU n    Please enter the account	unti Q, 推察				
Alibaba Cloud     demo1	Current account number 210/pu	irchased package specification is	500				
□   demo  demo  connector	编号 Name	Display Name	Туре	Description	Ac	tions	
	1 test	test	User-created Account	/ 阿里云IDAAS		odify Move Provision ovisioning Records M	

- **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.

OUs and Groups	Data Dictional Data Dictional									
Organizations and Groups This page allows the administrator to manage information about CUs, 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	Position Change 🗸	Import ~	Export ~	Configure LDAP	Configure DingTalk sync					
Manage the organization's architecture here. Y × ou can left-click and select the OU, right-click a n OU to manage it.	Account Group OU Create Account Account	Please enter the account r Q	搜索							
E Mibaba Cloud	Current account number 210 purchased package specification is 500									
C  demo temo temo temo temo temo temo temo t	编号 Name	Display Name	Туре	Description		Actio	ns			
Izyt     Domain Controllers	1 test	test	User-created Account	/ 阿里云IDAAS			y Move Provision sioning Records Ma			

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

Provision Account ×									
Username: <b>test</b> Note: To provision accounts from IDaaS to an authorized SP, the target application and SCIM user provining must be enabled.									
	Name	SCIM Configuration Stat	SCIM Provisioning Stat us	itManager.components. sync.tableColPushStatu s					
	JWT	Configured	Enabled	Yes					
	Provision Through: API Provision View Pro	vision Logs Cancel							

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

### Move an account

You can move an account from an organization to another.

<sup>&</sup>gt; Document Version: 20220322

- 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.

OUs and Groups	Us and Groups								
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	Alibaba Cloud View Details		P	Position Change ~ Import ~	Export      Configure LDAP Configure DingTalk sync				
Manage the organization's architecture here. Y × ou can left-click and select the OU, right-click a n OU to manage it.	Account Group C	Please enter the account r Q		Erroll Move Mark as Resigned					
Alibaba Cloud	Current account number 210/purc	hased package specification is 500							
C D demo	编号 Name	Display Name	Туре	Description	Actions				
	□ 1 test	test	User-created Account	/ Alibaba Cloud	Modify Move Provision Account Provisioning Records Mark as Resigned				
System     ForeignSecurityPrincipals	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.

testMove				$\times$
				_
Move To:	Current OU: (/ Alibaba Cloud)			
Alibaba Cloud  Alibaba Cloud  Comparison  demo  connector  demo	Target OU: (/)	ization to this account will be revoked, and the acc	count will be authorized to manage the appli	
	Available Applications Before Move:			1
⊕ m  -m  -m	Name	ID	Device Type	İ
	DefaultAppforConnector	idaas-cn-0pp1mb0e705jwt3	Data Provisioning	
	JWT	idaas-cn-0pp1mb0e705jwt	Web Application	
	DefaultAppfor58connector	idaas-cn-0pp1mb0e705jwt2	Data Provisioning	
<u>⊕</u> - <u>⊞</u>	Available Applications After Move:			
	Name	ID	Device Type	
	DefaultAppforConnector	idaas-cn-0pp1mb0e705jwt3	Data Provisioning	
	JWT	idaas-cn-0pp1mb0e705jwt	Web Application	
	DefaultAppfor58connector	idaas-cn-0pp1mb0e705jwt2	Data Provisioning	
	Retain the account linking corresponding to the	e application that this account is authorized to ma	inage before and after the move.	
	Move Cancel			

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.

OUs and Groups			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	Alibaba Cloud View Details	Position Change ~ Import ~ Ex	port - Configure LDAP Configure DingTalk sync						
Manage the organization's architecture here. Y × ou can left-click and select the OU, right-click a n OU to manage it.	Account Group OU  Create Account Account  Please enter the account I Q.  BioR	Enroll Move Mark as Resigned							
Alibaba Cloud	Current account number 210/purchased package specification is 500	Description	Actions						
connector     controllers     Domain Controllers	1 test     User-c     Accourt		Modify Move Provision Account Provisioning Records Mark as Resigned						

- 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 a	dministrator to disable accounts, re	set account passwords, enable two-facto	or authentication, and delete accounts. If	also provides details abou	t each account, ind	cluding information	about related devices, permissions, status, attributes,	
and OUs.								
Account n v Please enter th	ne account r Q Select enabl	e status V Select expiration	status V Q Search					
Current account number 210/pur	chased package specification is 50	0						
Username	Display Name	Email	Phone Number	Enabled or n ot	Expiration St atus	Two-factor Au thentication	Actions	
test	test				Normal	×	Account Details Reset Password Mark as Resigned	
demoUser1	demoUser1		-		Normal	×	Account Details Reset Password Mark as Resigned	
C57D5C42-DE66-4E6C-905E-96 96872678	BA demoUser2				Normal	×	Account Details Reset Password Mark as Resigned	
4F1441C3-3AC6-4D96-9FBA-16F 6DF84C72	2 demoUser1		-	$\bigcirc \bigcirc$	Normal	×	Account Details Reset Password Mark as Resigned	

- 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	Account / Account Details									
← Account D	← Account Details (test)									
Account Information	Available Applications	Application Account	OUs and Groups	Devices	Report	Real-name authentication info	ormation			
General Information										
Username	test		Display Name	test			Email			
Phone Number	(+86)undefined		Account Status	Normal			Directory	T		
Account Type	User-created Account		External ID	79047414	12897347631		Created At	2020/5/22 下午3:03:00		
Expiration Date	2116-12-31(Modify) Two-factor Authentication 禁刑									
Extended Information										
dingtalkInstanceId			dingtalkCropId				dingtalkUserld			
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=ID	SMANAGER, OU=IDaaS, (	C=CN							
Third-party Accounts										88
miru-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**.

Accounts								
Accounts	esigned Accounts Real Name auther	Are you sure you v or account test? Send New Password to A	vant to reset the password f ssociated Mailbox		t each account, in		about related devices, permissions, sta	× tus, attributes,
	enter the account r Q Select enable		OK Cancel					
Username	Display Name	Email	Phone Number	Enabled or n ot	Expiration St atus	Two-factor Au thentication	Actions	
test	test	tets@a.com			Normal		Account Details Reset Password Mark as Resigned	
demoUser1	demoUser1	demoUser1@aaa.com			Normal		Account Details Reset Password Mark as Resigned	

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

	i System Prompt The password is reset to	
		ОК
0	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**.

A	ccounts							
P	ersonnel Account Resigned Acc	counts Real Name authentication	System Prompt	to change the account status t				
	Accounts This page allows the admi and OUs.	inistrator to disable accounts, reset acc	o resigned? After this o e used to log on to the :		provides details abou	it each account, in	cluding information	$\ensuremath{\times}$ about related devices, permissions, status, attributes,
/	Account n			OK Cancel				
	Current account number 210/purcha	ised package specification is 500						
	Username	Display Name	Email	Phone Number	Enabled or n ot	Expiration St atus	Two-factor Au thentication	Actions
	lest	test	tets@a.com			Normal		Account Details Reset Password Mark as Resigned
	demoUser1	demoUser1	demoUser1@aaa.com			Normal	<b>O</b> ×	Account Details Reset Password Mark as Resigned

(?) 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.

- 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   |
|  | tor with multiple ways to authorize application access.<br>n 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)                       | OUs and Groups (774) Authorized: 1   |
| Search by application name             | Q 💼 : 00 🐠 : Group   |
| DefaultAppforConnector                 | > Search by name   |
| CAS(标准)                                | > Cloud Alibaba Cloud  |
| DefaultAppfor58connector               | > — 🐨 🖿 demo   |
| JWT1                                   |  |
| JWT                                    | Domain Controllers      Domain Controllers      System   |
|  | GreignSecurityPrincipals   |

4. Select the target application in the Applications list on the left.

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

5. 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

- 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 OU or Group tab.

Application Authorization		
Authorize OUs or Groups by Application Grant Application	Grant Application Access by OU or Group Grant Application Access by Account Authorize	e Accounts by Application Authorize Application by Class
OUs and Groups(774)	Applications (5) Authorized: 3	
Search by name Q	Search by application name	
Alibaba Cloud	Application Name	Application ID
demo	DefaultAppforConnector	idaas-cn-0pp1mb0e705jwt3
connector     jzyt     jzyt     Domain Controllers	□ CAS(标准)	idaas-cn-0pp1mb0e705cas_apereo
E System	<ul> <li>DefaultAppfor58connector</li> </ul>	idaas-cn-0pp1mb0e705jwt2
ForeignSecurityPrincipals     Managed Service Accounts     SubOrganization	JWT1	idaas-cn-0pp1mb0e705jwt1
<ul> <li>         ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・</li></ul>	TWL 💟	idaas-cn-0pp1mb0e705jwt

4. 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.

Authorize OUs or Groups by Application Grant	Application Ac	Cess by OU or Group Grant Application Access by Acce	Authorize Accounts by Application Authorize Application by Class		
Srant Application Access by Account          Itsis page allows the administrator to authorize application access to specific accounts.         Note:: This page only displays the applications whose access is directly granted to the selected account. An account can also obtain access to an application when the OU or group where the account belongs is authorized to access the application.        To view all the applications that an account has access to, go to the corresponding Account Details page.					
Accounts(209)		Applications (5) Authorized: 0			
Search by username	Q	Search by application name	٩		
demoUser1	>	Application Name	Application ID		
C57D5C42-DE66-4E6C-905E-968A96872678	>	DefaultAppforConnector	idaas-cn-0pp1mb0e705jwt3		
4F1441C3-3AC6-4D96-9FBA-16F26DF84C72	>	CAS(标准)	idaas-cn-0pp1mb0e705cas_apereo		
lin0512	>	DefaultAppfor58connector	idaas-cn-Opp1mb0e705jwt2		
dt11567251533	>	JWT1	idaas-cn-0pp1mb0e705jwt1		
dt21328622228	>	JWT	idaas-cn-0pp1mb0e705jwt		

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

Onte 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.

- 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.

Application Authorization						
Authorize OUs or Groups by Application Gran	nt Application Ac	ccess by OU or	Group Grant Application Access by Account	Authorize Accounts by Application	Authorize Application by Class	
Applications(5)	Account	s (209) Authorized: 0				
Search by application name	Q	Search b	y usemame		Q.	
DefaultAppforConnector	>		Name	Display Name	Email	
CAS(标准)	>		demoUser1	demoUser1	demoUser1@aaa.com	
DefaultAppfor58connector	>		C57D5C42-DE66-4E6C-905E-968A96872678	demoUser2	demoUser2@a.com	
JWT1	>		4F1441C3-3AC6-4D96-9FBA-16F26DF84C72	demoUser1	demoUser1@a.com	
JWT	>		lin0512	lin0512	lin0512@a.com	
Total 5 items <	1 >		dl11567251533	聂明峰		

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.

Policy Servers				Create Policy Serv
A policy server can m		ntrol (RBAC). sources and the menu functions and buttons of third-party appl nd other functions are not available. The self-butt system can t		
Name	ID	Status	Description	Actions
Default Policy Server	idp_ps		默认权限系统	Manage Roles View Details
OA	mezTPKlkOj			Authorization Management Manage Roles Manage Resources View Details Delete
				Total 2 items < 1 > Goto 1

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

 $\times$ 

#### 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				
	ermission model based on role-based access control			
<ul> <li>A policy server can n</li> </ul>		urces and the menu functions and buttons of third-party ap other functions are not available. The self-built system car		
,,				and a second party approximation
ame	ID	Status	Description	Actions
arrive .	15	ontes	Description	Patona
efault Policy Server	idp_ps	$\sim$ $\circ$	默认权限系统	Manage Roles View Details
efault Policy Server	idp_ps mezTPKIkOj		默认权限系统	Manage Roles View Details Authorization Management Manage Roles

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	11				
	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.

A policy server can m		(RBAC). ces and the menu functions and buttons of third-party ap ther functions are not available. The self-built system car		
Name	ID	Status	Description	Actions
	idp_ps		默认权限系统	Manage Roles View Details
Default Policy Server				
Default Policy Server	2HAkyq2n3e			Authorization Management Manage Roles Manage Resources View Details Modify Delete

## 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	arminalan madal hasad an rala hasad asaasa santu			
	permission model based on role-based access conti nanage the permissions to access both IDaaS reso	uror (RBAC). purces and the menu functions and buttons of third-party ap	plications. An IDaaS user with the developer role	can create SPs that support three-level authorization.
By default, the syste	m can only be associated with developer roles, and	d other functions are not available. The self-built system car	n be used normally to centrally manage the perm	issions of third-party applications.
Name	ID	Status	Description	Actions
Default Policy Server	idp_ps		默认权限系统	Manage Roles View Details
				Authorization Management Manage Roles
DA	mezTPKtkOi			Manage Resources View Details Delete

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

Policy S	ervers / OA						
← Ma	anage Roles						
Ŵ	Manage Roles The policy servers in IDaaS sup n the policy server.	oport role-based access control (RE	BAC). A role can be associated with	a range of permissions. Accounts a	ssigned to a role have all the permi	ssions of the role. This page allows	$\ensuremath{\times}$ is the administrator to create, delete, or modify roles i
Create	Import ~ Search by	role name			٩		
	Role	Permission ID	Permissions	Description	Status	External ID	Actions
	role2	role2	0			role2	Add Permission Authorized to person Modify Delete
	role1	role1	0			role1	Add Permission Authorized to person Modify Delete
	Batch Delete						
						То	tal 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

 $\times$ 

* 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 I etters, digits, and underscores (_).
Status	Enab
	Enable
Description	Enter a role description
	Enter a description of the role.
	Submit

- c. After configuring the parameters, click Submit.
- 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.

Ma	nage Roles						
	Manage Roles The policy servers in I n the policy server.	DaaS support role-based access cont	trol (RBAC). A role can be associa	ated with a range of permissions. Acc	counts assigned to a role have all	the permissions of the role. This page allow	vs the administrator to create, delete, or modify ro
reate	Import ~	Search by role name			٩		
	Role	Permission ID	Permissions	Description	Status	External ID	Actions
	role3	role3	0		$\checkmark$	d87d6ed883d902eaeb3d050	Add Permission Authorized to person Modify Delete
	role2	role2	0			role2	Add Permission Authorized to person Modify Delete
	role1	role1	0		$\checkmark$	role1	Add Permission Authorized to person Modify Delete
y Se	rvers / HR					K	otar 3 items < 1 > Goto 1
		<i>l</i> anagement				K	dua di acinis e di acini di ac
Aut	horization N	Management tize by role					evi 2. ps. authorizationManager.ImportRolePri
Aut	thorization N by person Author Authorization Manag	rize by role	ole-Based Access Control. You ca	n manage both the system permissi	ons of iDaaS and the level 2 and		r v1.2.ps.authortzationManager.ImportRolePri
Aut orized	thorization N by person Author Authorization Manag Role authorization is a p	rize by role	ote-Based Access Control. You can Associated with permissions		ons of IDaaS and the level 2 and	tißfanager	r v1.2.ps.authortzationManager.ImportRolePri
Aut horized	thorization N by person Author Authorization Manag Role authorization is a p	rize by role		Authorize to account	ons of iDaaS and the level 2 and	tißfanager	r v1.2.ps.authortzationManager.ImportRolePri
Aut	thorization N by person <u>Author</u> Authorization Manag Role authorization is a p	tize by role	Associated with permissions 如果取得关联父报节点对应的	Authorize to account	ons of IDaaS and the level 2 and	tißfanager	r v1.2.ps.authortzationManager.ImportRolePri
Aut	thorization N by person <u>Author</u> Authorization Manage Role authorization is a p	errent erritission model Based on RBAC (Rc	Associated with permissions 如果取得关联父级节点、对应的	Authorize to account	ons of IDaaS and the level 2 and	tißfanager	r v1.2.ps.authortzationManager.ImportRolePri

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**.

⑦ 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.

⑦ 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.

IDaaS	My Applications
Menu ^	Web Applications
My Applications	
All Applications	
Application Accounts	J
Settings ^	JWT
My Account	JWT
Two-factor Authentication	
Messages	
Logs	Mobile Applications
	No mobile application available.

## **Application management**

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

- 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	Applicat	tions					
Menu ^	Search by	application name		۹			
All Applications	Application ogo	Application Name	Application ID	Application Type	Actions		
Application Accounts	J	DefaultAppforConnector	idaas-cn-0pp1mb0e705jwt3		View Logs		
My Account	J	DefaultAppfor58connector	idaas-cn-0pp1mb0e705jwt2		View Logs		
Two-factor Authentication	J	JWT	idaas-cn-0pp1mb0e705jwt		View Logs		
Messages Logs							

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

IDaaS	Logs			
Menu ^ My Applications	All Logs 🗸 🗸			
All Applications	Log Type	Time	Content	IP
Application Accounts	Logon	2020/5/22 下午4:54:51		106.11.34.14
Settings ^ My Account	Application Log	2020/5/22 下午1:59:40		106.11.34.14
Two-factor Authentication	Application Log	2020/5/22 下午1:58:45		106.11.34.14
Messages	Application Log	2020/5/22 下午1:57:20		106.11.34.14
Logs	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.

- 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	Sub-account list St	ub-account approval			
All Applications	Add Application Account	Search by application name	Q		
Application Accounts		]			
Settings ^	Application L ogo	ame Approval Status	IDaaS Account	Application Account	Actions
My Account Two-factor	J. JWT	Approved	lin0512	lin0512	Delete
Authentication Messages					Total 1 item < 1 > Goto 1
Logs					

- 4. In the Add Application Account dialog box that appears, configure the following parameters:
  - **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.

				Add Application A	Account	$\times$
IDaaS	Application Accounts			Application	JWT	~
Menu Applications	Sub-account list Sub-account appro	wal		Select an application.		
All Applications	Add Application Account Search by applic		م	IDaaS Account		
Application Accounts Settings	Application L ogo	Approval Status	IDaaS Account	Application Ac count	test	
Anna Anna Anna Anna Anna Anna Anna Anna	ego Antonio Autori	Approved	le0512		Note: This application account uses the <b>Auto</b> inking mode. The system uses the IDaaS account username or the specified field as the application in username.	
	◎ IDaaS 浙ICP督12022327号					

**?** 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.

# Logon from a PC

1. Access the IDaaS port al 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.

laaS	Instances									Buy IDaaS
stances oduct documentation	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-0pp1mb0e705	华南1 (深圳)	這行中	増强板	500	May 22, 2020	V1.6.4	iroluldfai login aliyunidaas.com	iroiuldfai.api.aliyunidaas.com	Manage Update Renew
	idaas-cn-4591kgdnd02	<b>徐南1(</b> 3冠川)	运行中	増强板	500	Apr 17, 2020	V1.6.4			Manage Update Renew
	idaas-cn-4591jdx450a	华南1 (深圳)	运行中	增强板	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 logon page.

nglish		Scan QR code	to log on.	3
		D		
	Alibak	a Cloud		
	Enter a username, er	nail, or phone	number	
	Enter the password			
	Enter the verification	code	NSNE	
		Forgo	t password?	
	Lo	g 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.

- 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 Logon Password of the account and hind

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 Ad	My Account					
Accour	Security General Information Certificate Third-party Accounts					
Ð	Logon Password This password is used to protect your account information and ensure logon security.	Change				
	Email I****2@a.com This email account is used to log on to IDaaS, reset the password, and receive messages from IDaaS. Boun	d Change				
	Phone Number 165****1074 This phone number is used to log on to IDaaS, reset the password, and receive messages from IDaaS.	d 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	y General Information Certificate Third	I-party Accounts	
	Applications	Application Accounts	
	3	1	
	0		
Username			
Display Name	lin0512		
	Save		

• On the **Cert if icat e** tab, you can view your certificate and the certificate password. You can also download your certificate locally.

I	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.

- 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.

Two-factor Authentication	
Two-factor Authentication D	evices
	scurity through two-factor authentication, select the following option:
Enable	
Authenticate With	Mobile App ~
	After you enable two-factor authentication, logon authentication based on the IDaaS app on your mobile terminal or SMS verification codes will be performed.
	Save

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

Two-factor Authentication							
Two-factor Authentication Devices							
enduser.v1.2.towFactor.device.tttle.list If you are using the internal network, you can use the IDaaS app on your mobile terminal to scan the QR code to enable OTP. Show QR Code							
Device Name	Device Type	Approval Status	Device Status	Created At	Actions		
No Data							
4						Þ	

## 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

- 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 > 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.

Messages						
Unread Read	Deleted					
Title	From	Q Search				
Title	From	Туре	Status	Created At	Actions	
			No Data			
•						Þ
					Total 0 item < 1 >	Goto 1

3. 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 v							
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				