

Alibaba Cloud

Identity as a service Best Practice

Document Version: 20220322

Legal disclaimer

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

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

Document conventions









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

Table of Contents

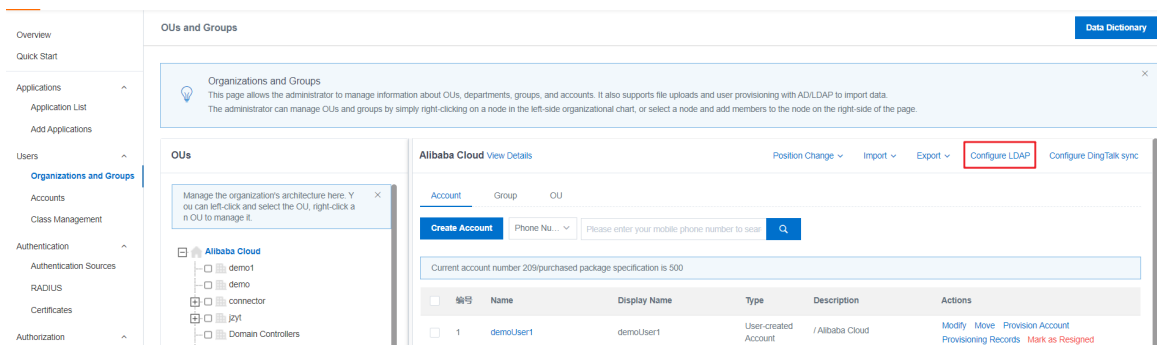
1.Account Provision	05
1.1. LDAP Provision Configuration	05

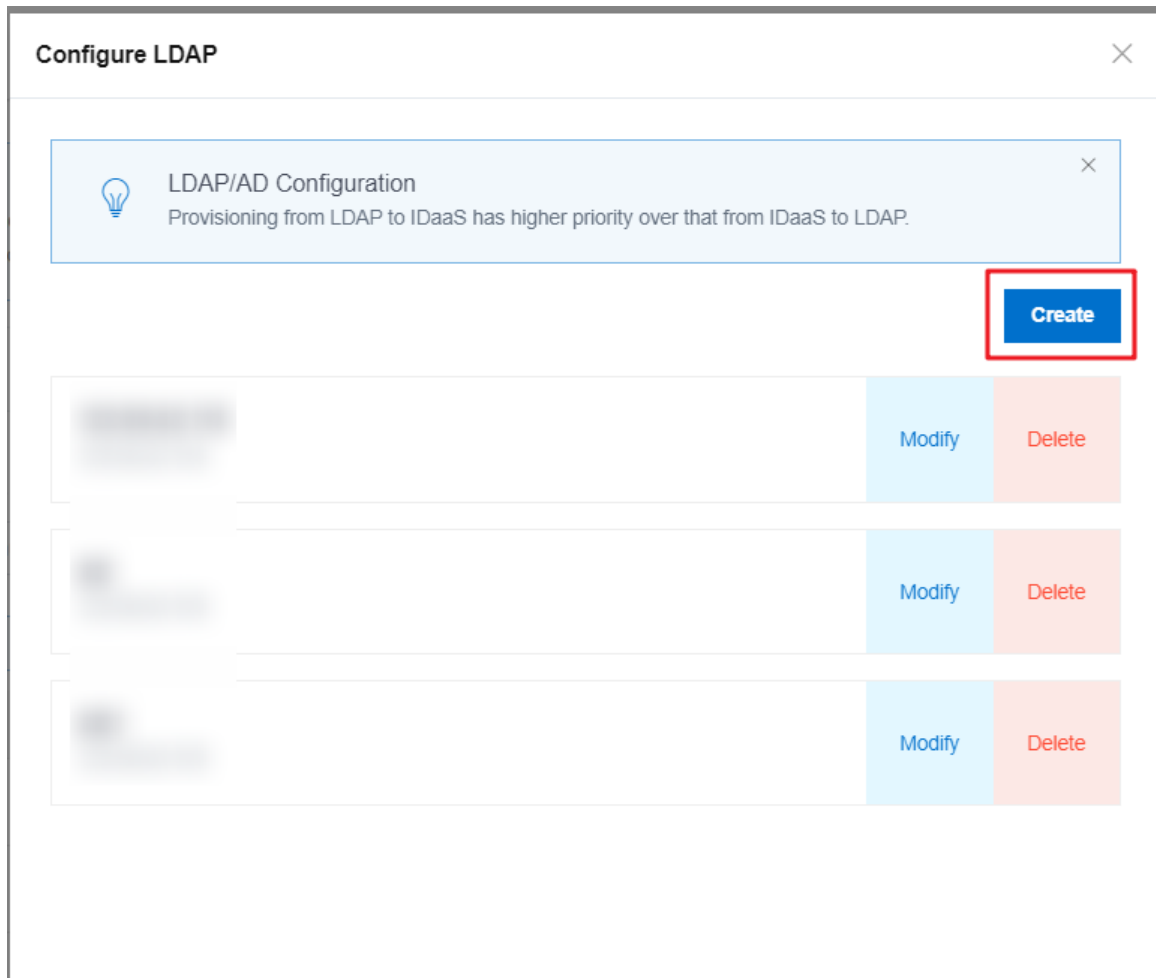
1.Account Provision

1.1. LDAP Provision Configuration

Step 1: Configure LDAP

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. Click **Configure LDAP** in the top navigation bar of the parent node organization information window. Click **Create** in the Configure LDAP dialog box that appears. Set **Provision from IDaaS to LDAP** to **Enable** and configure the other parameters.





i. **Server Connection tab**

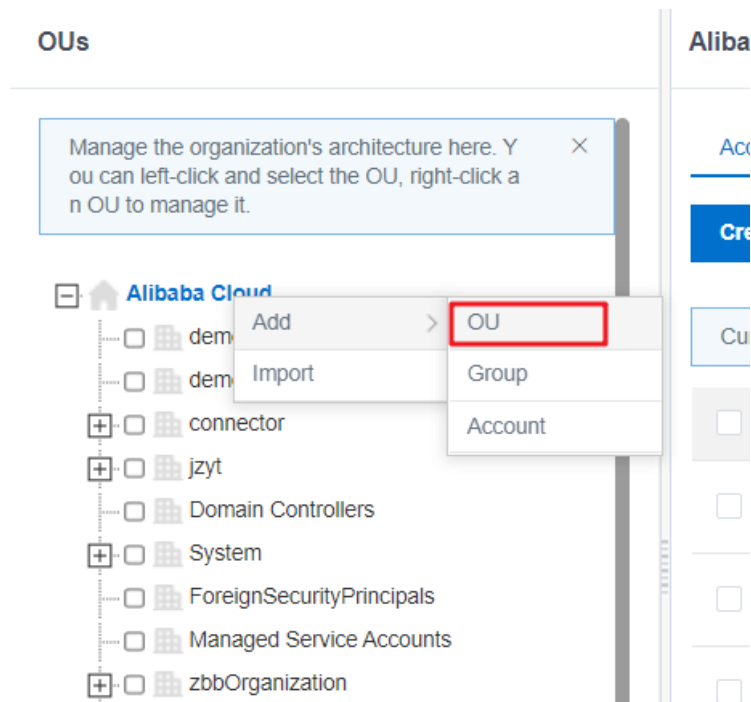
- AD/LDAP Name
- Server Address and Port Number
- Base DN
- Connection Method
- Administrator DN and Password
- Select Type
- Owned OU node

ii. **Field Matching Rules tab**

- Username
- External ID
- Password Attribute
- User Unique ID
- Phone Number
- Email

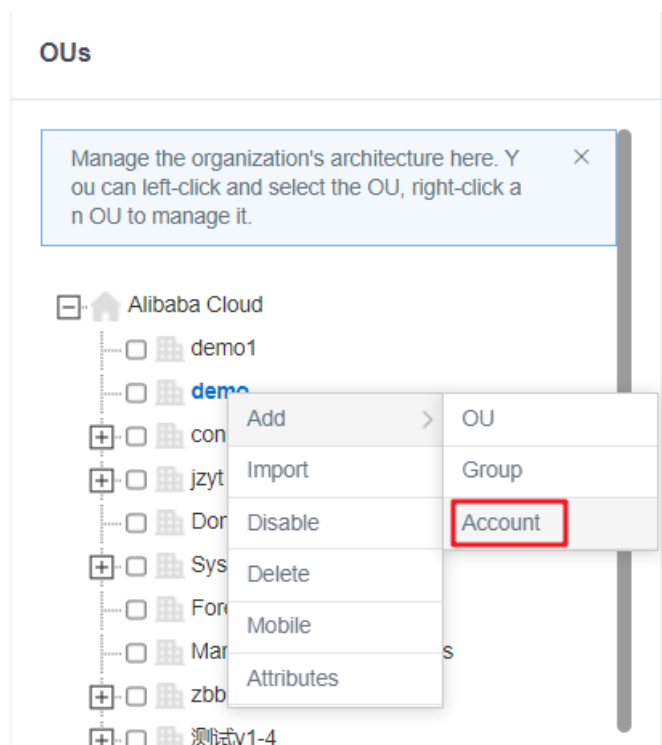
Step 2: Create an organization

Click Create OU on the OU tab of the OUs and Groups page to create an organization.



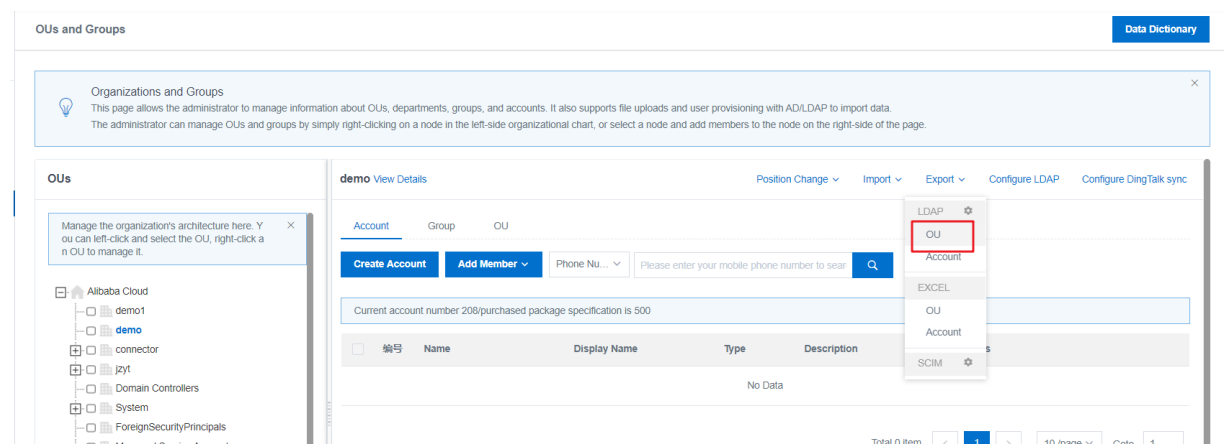
Step 3: Create an account

Click Create Account on the Account tab of the OUs and Groups page to create an account for the new organization.



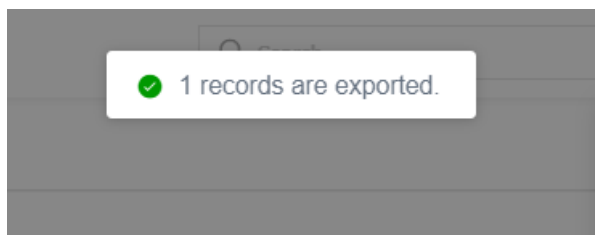
Step 4: Provision the new organization

In the left-side navigation pane, choose Users > OUs and Groups > Export > LDAP > OU to provision the new organization to the configured LDAP server.



[illegible]

Click OK. The following message is displayed after a successful operation.



Step 5: Provision the new account

Before provisioning the account, you must confirm that the organization to which the account belongs exists in the LDAP server. In the left-side navigation pane, choose Users > OUs and Groups > Export > LDAP > Account to provision the new account to the configured LDAP server.

The screenshot displays the 'Organizations and Groups' management interface. On the left, the 'Organizations and Groups' sidebar shows a tree structure under 'Alibaba Cloud' with 'demo' selected. The main panel shows the 'demo View Details' page. The 'Account' tab is active, displaying a table with one account: 'demoUser1'. A red box highlights the 'demoUser1' row. A dropdown menu is open, showing 'Account' selected. The 'Export Accounts (To LDAP)' dialog is open, showing the 'Batch Export' tab. The 'Select ADs to which you want to import data' section has '23.56.42.118' selected. The 'Select OUs to export' section has 'demo' selected. The 'demoViewDetails' table is visible in the background, showing the account details for 'demoUser1'.

You can export a single account on the Export One tab.

Export Accounts (To LDAP)

Batch Export

Export One

Select ADs to which you want to import data. If no AD is available, configure LDAP first.

☒

23.56.42.118

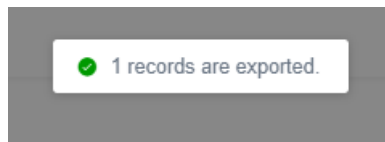
☐ AD ☐ AD1

To import a single account, you must search for the account first.

demoUser1

Name	Type	Actions
demoUser1	User-created Account	<div>Export to LDAP</div>

The following message is displayed after a successful operation.



Step 6: View the provisioned account in the LDAP server

Log on to the LDAP server by using the LDAP connection tool. Refresh the page and view the provisioned account, as shown in the following figure.

