# Alibaba Cloud

# Identity as a service Unified Authentication

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.

- 1. 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
<u>↑</u> 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.
C) 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.
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.Third-party Authentication Source Access	05
1.1. LDAP as Authentication Source	05

# 1.Third-party Authentication Source Access

## 1.1. LDAP as Authentication Source

This topic describes how to add LDAP authentication sources and use user accounts in AD to log on to IDaaS.

#### 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 Authentication > Authentication Sources.
- 3. In the upper-right corner of the Authentication Sources page, click Add Authentication Source. Find LDAP and click Add Authentication Source in the Actions column. Configure the parameters in the dialog box that appears.

E C-) Alibaba Cloud	ł		Q Search		Billing Ticket ICP	Enterprise S	upport Alibaba Ck	ud 🖭	Q, A	EN	0
Overview Quick Start	Authentication Sou	urces				Add DingTalk :	authentication source	Add	Authenticati	on Source	
Applications ^ Application List Add Applications	Authentic IDaaS sup After you h	cation Sources ports external authentication sources. You can use thir have enabled external authentication sources, IDaaS a	d-party authentication systems to authenticate users. For exam llows users to log on through third-party authentication systems	ple, DB, LDAP, and	d DingTalk.					>	£
Users ^ Organizations and Groups	Search by authentik	ication source name	٩								
😑 C-J Alibaba Clo	bud		Q Search	Expenses	Tickets ICP Ent	erprise Suppor	t Official Site	ΣÂ	•	EN	0
Overview Quick Start	← Add A	uthentication Source									
Applications ^ Application List	Search by author	Authentication Source Name	Identifier		Description				Action	s	
Add Applications	$\Box$	Enterprise wechat micro	wechatenterprise_micro		Log in with enter	prise wechat and n	nicro application	/	dd Authenti، Source	ication e	
Organizations and Groups	赵	Alipay login	alipay		Login with Alipay	scan code		,	Add Authenti Source	ication	-
Class Management		DDTalk micro APP	ddtalk_micro		Login with DDTa	k micro APP		,	Add Authenti Source	ication	-
Authentication ^	<b>2</b>	Wechat QR code	wechat		Scan wechat QR	code to login		1	Add Authenti Source	ication e	-
RADIUS Certificate Management		DDTalk QR code	ddtalk		Scan DDTalk QF	code to login		4	Add Authenti Source	ication	-
Authorization ^	LDAP	LDAP	ldap		Use LDAP (such	as ad domain) for	authentication	_	Add Authenti Source	ication e	
Application Authorization		SMS login	sms		Login with SMS	ogin		4	Add Authenti Source	ication e	-
More	$\bigcirc$	Enterprise wechat QR code	wechat_enterprise		Login with enter	rise wechat QR co	de	4	Add Authenti Source	ication	
Settings ~											

Set LDAP URL to the IP address + port number of the AD domain.

Set LDAP Base, LDAP Account, and LDAP account password to the values of AD.

Set Filter Condition to (sAMAccountName=\$username\$).

Add Authenticatio	n Source (LDAP)	$\times$
* Name	LDAP	
* LDAP URL	Idap://	
	LDAP server connection address, For example, Idap://127.0.0.1:389/	
	IPv6 address host IP needs to be placed in brackets, such as: Idap://[0000:0000:0000:0000:00	
	00:0000:0001]:389/	
* LDAP Base	dc=xxx,dc=com	
	LDAP will authenticate the account under this node,For example, dc=idsmanager,dc=com	
* LDAP Account	cn=Manager,dc=xxx,dc=com	
	The management authority of the base filled in above is required, For example, cn=Manager, dc=	-
	userName,dc=com	
* LDAP Account Password	LDAP Account Password	
	The password corresponding to LDAP account.	
Filter Condition	Enter a condition to query users	
	Replace the username in LDAP with \$username\$. For example, (sAMAccountName=\$username)	n
	e\$). \$username\$ is a fixed value in IDaaS.	
LDAP Encryption Algorithm	NONE V	
	The encryption algorithm of the LDAP password. If the LDAP password is not encrypted, select	
	NONE.	
Verify with userPassword		

4. In the left-side navigation pane, choose Users > Organizations and Groups. Click Configure LDAP in the right window to configure LDAP settings. If you have configured the LDAP authentication source, skip this step.

OUs and Groups						Data Diction
Organizations and Groups This page allows the administrator to manage informati The administrator can manage OUs and groups by sim	on about OUs, departments, groups, and accounts. It also supports file uploads and user provisi ply right-clicking on a node in the left-side organizational chart, or select a node and add membe	ioning with AD/LDAP to ers to the node on the rig	import data. ght-side of the pa	ige.		
OUs	阿里云 IDAAS View Details	Position Change ~	Import ~	Export ~	Configure LDAP	Configure DingTalk syn
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 Phone Nu  Please enter your mobile phone number to sea	r Q	UDAP ¢ OU Account	]		

### Unified Authentication Third-party

ldent it y as a service

Authentication Source Access

≡	C-J Alibaba Clou	d				Expe	nses	Tickets	ICP	Enterprise	Support	Official Site	2	۵.	0	EN	0
Overvi	ew	OUs and Groups					Config	gure LE	AP								$\times$
Quick	Start																
Applic Ap Ac	ations ^	Organizations and Groups This page allows the administrator to manage info The administrator can manage OUs and groups t	rmation about OU: y simply right-clicki	, departments, groups ng on a node in the lef	, and accounts. It also t-side organizational (	o supp chart, i		₩ P	DAP/AD rovisioning	Configuratio from LDAP to	n IDaaS has hi	gher priority ove	r that fro	ım IDaaŝ	S to LDA	Creat	
Users	^	OUs	View Details												Ľ		
Or	ganizations and Groups																
Ac	counts Management	Manage the organization's architecture ×	Account	Group OU													
Cl	ass Management	OU, right-click an OU to manage it.	Create Accour	Account n V		count r											
Auther	ntication ^	間甲元のムムS															
Au	thentication Sources		Current accourt	t number 1/purchased	package specification	n is 10											
RA	DIUS		Number	Name	Display Name												
Ce	ertificate Management																
Author	ization ^			idaas_manager	Default administ	rator											
Po	licy Servers																
Ap	plication Authorization																
Audit	~																
More	· ·																
Setting	js ×																

#### Configure LDAP

 $\times$ 

Server Connection	Field Matching Rules Return
Connection	
AD/LDAP Name	Enter a name
<ul> <li>Server Address</li> </ul>	Enter a server address
Port Number:	Enter a port number
	If you enter an SSL port, the password changes will be provisioned to LDAP.
<ul> <li>Base DN</li> </ul>	Enter a Base DN, Example: dc=xxxx,dc=com
	This item cannot be changed after the addition is completed, because when the system synchronize s data with LDAP (or AD), if BaseDN changes, the organization directories of both parties cannot cor respond, resulting in data synchronization failure, to synchronize data from different directories, it is r ecommended to add multiple LDAP configurations.
Connection Method	SSL
	Use SSL to connect to LDAP Server.
Account	
Administrator DN	
	Enter the administrator DN. If DN is modified after synchronization, data synchronization shall be per formed again.
* Password:	•
	Enter the LDAP administrator password.
Туре	
Select Type	○ Windows AD
Location	
Owned OU node	Enter the OU UUID
	Data is imported into the node position of the organization in the system. If it is not filled in, it is impor ted into the root OU.

- 5. Create an account and provision the account to AD. You can connect to AD to view the provisioned account.
- 6. Click LDAP in the Use a Third-party Account to Log On section of the logon page. You are redirected to the Log On with LDAP Account page. Enter the provisioned account for logon. The password for the provisioned account here must be the AD domain password, instead of the password in IDaaS.

English		Scan QR cod	e to log on.	R
		D		
	Alik	baba Cloud		
	Enter a username,	, email, or phone	number	
	Enter the passwor	d		
	Enter the verification	on code	PLVG	
		Forg	ot password?	
		Log On		
	Use a Third-p	arty Account to Log	J On	
ſ				

	~	
Log On with LDAP Account		
demoUser		
v62x		
Submit		
Back		

After adding the LDAP authentication source, you can use the account and the password in AD to log on to the IDaaS console.

0