ALIBABA CLOUD

Alibaba Cloud

Identity as a service

FAQ

Document Version: 20220322

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 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**.
`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 list --instanceid` *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.FAQ for Account Provision

1. If there are two service systems with the same account name, how will they be provisioned to the IDaaS console? How will the accounts be provisioned to the IDaaS console if a user has account names in two service systems?

The accounts of a service system carry a unique ID when they are provisioned to the IDaaS console. The IDaaS console determines whether it is the same account based on the unique ID. If the two IDs are the same, IDaaS will associate the two accounts. If the two IDs are different, IDaaS will create another account.

IDaaS provides user accounts and application accounts and retains their association relations. Two application accounts can be mapped to a single user account with the same attributes.

> **Note** The unique ID is generally the email address or mobile phone number bound to an account.

2. What methods can be used to provision accounts? What are the differences between these methods?

IDaaS supports the following two methods to provision accounts:

- Service systems can use SCIM-based APIs provided by IDaaS to provision accounts to the IDaaS console.
- The IDaaS console can use APIs provided by the SP to provision APIs created in IDaaS to the SP.

The two methods differ in which side receives the transferred accounts and which side provides APIs.

> **Note** APIs must be developed based on the SCIM protocol.

2.What is Single Sign-on?

Single sign-on (SSO) means that you can access multiple mutually trusted application systems with only one logon. The single sign-on service in IDaaS is used for authentication of different applications of the same company. Users can access all added applications with only one logon.

The single sign-on service in IDaaS is applicable to the following scenarios:

IDP initiation

IDP initiation is also called IDaaS initiation. You log on to the IDaaS console and then can log on to applications (SPs) from the IDaaS console.

1. On the IDaaS logon page, you enter the username and password to log on to the IDaaS console.
2. The browser sends an IDaaS logon request carrying the username and password.
3. After you pass the authentication, the IDaaS console creates a primary session returns the application list.
4. You log on to the IDaaS console and can view the application list.
5. You click the SP1 application icon from the application list.
6. The browser sends a request carrying the ID of the SP1 application to the IDaaS console for generating a secondary token for the SP1 application.
7. The IDaaS console generates a secondary token based on the received information and returns the secondary token to the browser.
8. The browser sends a logon request carrying the secondary token to the SP1 application.
9. The SP1 application system parses and authenticates the secondary token. After a successful authentication, the system will create a secondary session and return the successful logon page.
10. The SP1 single sign-on is successful and the browser displays the SP1 homepage.

> **Note** Steps (11) to (16) of the preceding figure demonstrate the single sign-on process of the SP2 application system, which is similar to that of the SP1 application system. After a primary session is created, this process can be used to implement single sign-on of any applications.

SP initiation

SP initiation includes two cases.

- Access the SP page

  You access the SP page, send a Redirect or POST request for redirection with an authentication protocol such as SAML or CAS from the IDaaS console to the SP application. This process allows for centralized authentication of the SP application.

  The following example demonstrates the SP-initiated single sign-on process by using the SAML protocol.

  i. You access the SP resource page.
  ii. The browser requests resources from the SP system.
  iii. The SP system generates a SAML authentication request and returns it to the browser.
  iv. The browser sends a SAML authentication request for access to the IDaaS SSO URL.

v. IDaaS verifies the SAML authentication request information.

> **Note** If you have logged on to the IDaaS console, go directly to step i.

vi. You are redirected to the IDaaS logon page.

vii. You enter the IDaaS account and password.

viii. The browser sends a username + password request for logon to the IDaaS console.

ix. You log on to the IDaaS console. IDaaS analyzes the SAML authentication request information, obtains other information, and then generates response token data.

x. IDaaS returns the response token data for the SAML request to the browser.

xi. The browser uses the SAML response data to access the SP authentication URL.

xii. The SP system uses the public key to verify the SAML response data.

xiii. The SP system returns the SP resource URL to the browser after a successful authentication.

xiv. The browser accesses the SP resource page.

xv. The SP system returns the SP resource page.

xvi. You log on to the SP resource page.

- Access an SP resource

  You access an SP resource and are redirected to the IDaaS SSO URL. After a successful IDaaS authentication, the SP system will return the logon page carrying the redirect_url parameter of the request event. After you log on to the SP system, the SP system returns the SP resource page to the browser.

  i. You access the SP resource page.

  ii. The browser requests resources from the SP system.

  iii. The SP system checks your logon status.

  > **Note** If you have logged on to the IDaaS console, go directly to step i.

  iv. You are redirected to the IDaaS SSO URL.

  v. The SP system returns the logon page carrying the redirect_url parameter of the request event.

  vi. You enter the IDaaS account and password.

  vii. The browser sends a username + password request for logon to the IDaaS console.

  viii. The IDaaS console authenticates the account.

  ix. The IDaaS console returns the deeplinking and id_token data to the browser.

  x. The browser sends the data to the SP system for verification.

  xi. The SP system uses the public key to verify the id_token.

  xii. The SP system returns the deeplinking URL to the browser and creates a session.

  xiii. You can view the SP resource page.

Later authentication

The SP system uses IDaaS for later authentication.

1. You access the SP1 logon page.

2. The browser requests the SP1 logon page.
3. The SP1 system returns the logon page.
4. You can view the SP1 logon page.
5. You enter the username and password for logon.
6. The browser sends a logon request carrying the username and password to the SP1 system.
7. The SP1 system sends the username and password to IDaaS for logon authentication.
8. After a successful authentication, IDaaS will generate a primary token and then return the primary token, application list, and user information to the SP1 system.
9. You log on to the SP1 system and the browser obtains the successful SP1 logon page.
10. You can view the successful SP1 logon page with the application list displayed.
11. You click the SP2 application icon for single sign-on from the application list displayed on the SP1 system.
12. The browser sends a request carrying the primary token and the ID of the SP2 system to IDaaS for generating a secondary token.
13. IDaaS returns the secondary token and redirect URL of the SP2 system.
14. The browser sends a request carrying the secondary token to the SP2 system for accessing the redirect URL.
15. The SP2 system parses the secondary token and returns the successful SP2 logon page.
16. You can view the successful SP2 logon page.

Logon redirection

You access the SP system page and are redirected to the IDaaS logon page for centralized authentication. After a successful logon, IDaaS will return a JWT token to the SP system page for implementing single sign-on. The JWT token carries information such as the application list and a secondary token for accessing another SP application.

1. You access the SP1 logon page.
2. The browser requests the SP1 logon page.
3. The SP1 system returns the redirect URL.
4. The browser accesses the redirect URL.
5. IDaaS returns to the logon page.
6. The browser sends a request carrying the username, password, and the ID of the SP1 system to IDaaS for logon.
7. After a successful local authentication, IDaaS will create a primary session and return a JWT token which contains the application list and a secondary token to the browser.
8. After receiving the information, the browser will verify the JWT token and parse the secondary token, and then send a request to the SP1 system for authentication and logon.
9. The SP1 system obtains and parses the secondary token, creates a secondary session, and returns the successful logon page to the browser.
10. You can view the successful SP1 logon page.
11. After logging on to the SP1 system, you access the SP2 logon page.
12. The browser requests the SP2 logon page.

13. The SP2 system returns the redirect URL.
14. The browser accesses the redirect URL.
15. IDaaS directly generates a secondary token of the SP2 system based on the application ID and returns the token to the browser Because IDaaS has created a master session for you.
16. The browser sends a request carrying the secondary token to the SP2 system.
17. The SP2 system parses the secondary token, creates a secondary session, and returns the successful logon page to the browser.
18. You can view the successful SP2 logon page.