# Alibaba Cloud

Identity as a service SSO Configuration

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", "Alibaba Cloud. The names owned by Alibaba Cloud and/or its affiliates 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.Best Practices	05
1.1. Implement single sign-on for JIRA or Confluence	05
1.2. WordPress-SAML application usage	10
1.3. Implement single sign-on for Salesforce	16
2.Standard Protocol Template Usage Guide	24
2.1. C/S Applications User Manua	24
2.2. OAuth2.0 Application User Manual	25
2.3. Form Autofill Template User Manual	33

# **1.Best Practices**

# 1.1. Implement single sign-on for JIRA or Confluence

This topic describes how to use the SAML protocol to implement single sign-on for JIRA or Confluence in the IDaaS console. We demonstrate single sign-on for the Alibaba Cloud console here.

## Background

Employees of an enterprise need to access JIRA or Confluence in their daily work. They must enter the logon URLs of applications, account names, and passwords upon each logon. If multiple similar applications are involved, they must record multiple pairs of usernames and passwords and repeated logons are time-consuming.

## Solution

IDaaS can implement single sign-on for JIRA or Confluence. Employees can access all authorized applications through single sign-on.

### 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**. Find the SAML application and click **Add Application** in the Actions column.

C-) Alibaba Cloud				Q Search Billing Ticket ICP Enterprise Support	Alibaba Cloud 🖬 🖇	R,	EN
Iverview	Add Application	n					
Quick Start	All Standar	d Protocols Cust	om Templates				
Applications ^ Application List Add Applications	Add Ap W This pi Applica	pplications age contains the appl ation templates can b	ication templates pro e divided into two typ	vided by (DasiS. The administrator can add applications to IDaaS based on these templates. et. One type supports standard protocols that you can use to implement SSO, such as JVIT, CAS, and SAML. The other is customized and provides APIs for SSO or user provisioning.			1
Organizations and Gr	Search by appl	ication name		<b>a</b>			
Accounts	Application L ogo	Application Nam e	Tag	Description	Application Type	Act	tions
class Management	C-)	阿里云RAM-用户 SSO	SSO, SAML, 阿里 云	基于 SAML 协议,实现由 IDaaS 单点量原则同量云控制给;使用该模拟,需要在RAM中力每个用户单始创建RAM子预户,IDaaS预户间RAM子预户通过移封实现单点量原则RAM,	Web Application	Add atic	d Applic an
Authentication Source	開設式RAM 角色     SSO、SAML 同型     ます SAML 防災、家気由 Dass 単点理及到同量式控制法: 使用读描版、需要RAM中始温RAM角色,不需要为每个用户单指绘温RAM子预户, Dass所产(RRAM角色量)]排射实现单点理及到RAM.					Add atic	d Applic an
Certificates	♀ CS相序 C5, PC, ODC 論擬任先活運过ODChWo角机将進身数实现登录,送用于可以接受解析ODChWo角数的应用。					Add atic	d Appli an
thorization ^	C	CAS(标准)	SSO, CAS	CAS(Central Authentication Service。集中式认证服务,版本 2.0)是一种基于挑战、应答的开展单点整要协议。在集成客户编和服务施之间网络摄畅的情况下广泛在企业中使用,有集成增便,扩展性强的优点。	Web Application, Mob Application	le Add atic	d Applic an
Application Authoriza	J	JWT	SSO, JWT	JWT(JSON Web Token)最石码临步用环境再调的一种基于 JSON 的开放方角,IDaaS 使用 JWT 进行分布式站船的单点重要(SSO),JWT 单点重要基于非对称如果,由 IDaaS 将用户状态和信息使用私用如果,给邀给 应用品,应用使用公明解离并进行验证,使用场展非常广泛,集成简单,	Web Application, Mob Application, PC Client	le Add atic	d Applic an
Operation Logs	O.	OAuth2	OAuth2	OAun 是一个开始的资源规划协议,应用可以通过 OAun 获取到今碑 access_loken,并携带令牌来服务装造求用户签置。应用可以使用 OAun 应用模板来说现她一身份管理。	Web Application	Add atic	d Applic an
Logon and Logout Lo	S	SAML	SSO, SAML	SAML(Security Assertion Markup Language,安全解解标记面解,版本 2.0) 基于 XML 协议,使用包含解释(Assertion)的安全令律,在提权方(IOaaS)和谐振方(应用)之间传递是份信息,实现基于网络跨域的单点 登录。SAML 协议观成编的认证协议,在期内外的公教方积私构云中有非常广泛的运用。	Web Application	Add atic	d Applic an
Approvals	-	SAP GUI	SSO, C/S	SAP GU愿SAP用户用于访问SAP系统的图形用户界面(Graphical User Interface), SAP 显世界初先的企业软件提供商,其简品范畴包含 ERP、CRM、数据分析、HR、物流、差缺、金融爆発方面,拥有1万9千个全球合作伙伴,广泛各布在25个不同的行业中,为余映各阶段企业组织数字化想理解成方案。	PC Client	Add atic	d Applic an
User Provisioning	salesjowe	Salesforce	SSO, SAML, CR M	Salesforce 展在世界范围内广泛使用的公寓云 CRM 平台(Customer Relationship Management,整户关系管理系统),它为企业提供了事例管理。任务管理、事件动态升级等能改的微业能力,IDaaS 划场面过 SAML 协议 单位量源到 Salesforce 网站。	Web Application	Add atic	d Applic an
Sessions	<b>W</b>	WordPress-SAML	SSO, SAML, CM S	WordPross 显金世界最初广泛使用的 CMS(Content Management System,內容管理系统),它還过非解凝大的指針系统的方便自然的描述作两氮,允许千万技术综容技术人员生产,管理各种类型的网站。从黄业网站、政府 页面到个人爆集,主题记坛、WordPross 所变地的形式非常多样。IDaas 发抖圈过 SAML 协议单点型原到 WordPross 网站。	Web Application	Add atic	d Applic an
My Messages 😋 ettings 🛛 🗸				Todal 13 dams	2 > 10 /page	Goto	1

3. Click Add SigningKey. Configure the parameters and click Submit.

Add Application (SAML	)						×
Import SigningKey	Add SigningKey						
Alias		Serial Number		Validity pe riod	Key Algori thm	Algorithm length	Actions
			No Data				
Add Cigning Kou							
Add SigningKey							×
*Name	Enter a name						
- Norrice							
Department	Enter a department na	me					
Company	Enter a company name	9					
* Country	Select						~
+ Dravince	Entor a province name						
* Province	Enter a province name						
City	Enter a city name						
*Key Size	Select						~
* Validity	Select						~
	Submit Cancel						

4. Export the SigningKey file.

Find the new SigningKey in the SigningKey list and click Export in the Actions column. Open the exported file in a text editor. Obtain the -- BEGIN CERTIFICATE-- -- END CERTIFICATE -- information.

		Q Search	Billing	Ticket	ICP	Enterprise	Support	Alibaba Cloud	Þ þ	₩ EN	0
Add Application (SAML)											
Export SigningKey	×	SigningKey									
You can export SigningKey in the following file formats.Imp ort the certificate in the application requiring single sign on.		Serial Numl	er				Validity pe riod	Key Algori thm	Algorithm length	Actions	s
DER Encoded Binary X.509 (.CER)(D)     Base64 Encoded X.509 (.CER)(S)		1422762525	144370953					RSA	2048	Select Export	
<mark>ОК</mark> Сал	cel										

5. Configure miniOrange Single Sign On for Confluence.

Configure SP Base URL.

Set SP Base URL and SP Entity ID to your Confluence information. Use the default values for other parameters.

M Include Sign	iing Certificate in Metadata					
Include signing or	toficate in the SAML Metadata to inform IdP that SP has ogned rep	est. To disable signing request, please uncheck this value and also uncheck Send Signed Requests in Configure IDP section.				
Include Encryption Certificate in Metadata						
include encryption	centurate in the priori methodical cost anony the row or excitibit vis	erupes.				
Save						
OR						
these values below to add JIRA as	ervice provider/relying party in your Identity Provider:					
P Entity ID / Issuer	http://	0.250.122.24:8080	Сору			
CS URL	http://	10.250.122.24.8080/plugins/servlet/sami/auth	Сору			
ingle Logout URL	http://	10.250.122.24/8080/plugins/servlet/sami/logout	Сору			
udience URI	http://	10.250.122.24:8080	Сору			
ecipient URL	http://	10.250.122.24/8080/plugins/servlet/sami/auth	Copy			
estination URL	http://	10.250.122.24.8080/plugins/servlet/sami/auth	Copy			
ertificate	Downi Note: # SAMLA	oad Show Cestificate Details The IDF requires lagred request, the IdP will need this cestificate to validate requests, It is also used to decrypt encrypted satisfurs from the IDF. After download, open in notepail to copy certificate. You can configure your own certificates from here.	Серу			
nfigure Service Provider URL	(Optional)					
SP Base URL:	http://10.250.122.24/8080					
	If your site is behind a proxy you can mudify SP base URL for Sing	e lign-On to wark.				
SP Entity ID:	http://10.250.122.24.8080					
	Set the Entity ID for the Service Provider. If not provided, JRA has	URL will be used by default.				

Configure the IDP parameters on the second tab.

id Identity Provider	
ep 3: Configure IDP	
ck on Import From Metadata to feto	h IDP's settings from IDP metadata URL or XML file OR copy the URLs from Step 2 below to setup IDP details.
ed help with the configuration? You (	can reach out to us using Support and avail free support to setup the app. You can also submit a support request using our website's contact us form or write to us at info@xecurity.com
IDP Name*	
	This IDP Name will be shown in the togin wedget to users.
IDP Entity ID / Issuec"	http://10.250.100.169-8080
	Enter the Entity ID or tosuer value of your Identity Provider. You can find its value in the entity/D abritude of Entity/D escriptor tag in IdP Metadata XMI, the
Send Signed Requests	*
	It is recommended to keep If checked, Uncheck, only if your KIP is not accepting Bigned SAMI. Request.
SSO Binding Type	Use HTTP-Redirect Binding for SSO @ Use HTTP-Post Binding for SSO
Single Sign On URL*	http://10.250.100.169.8080
	Enter the Single Sign-on Service endpoint of your identity Provider. You can find its value in SingleSignCintlevice tay (Binding type: InTTP-Redirect) in idP-Metadata XMI. No.
SLO Binding Type:	
Single Logout URL	
	Enter the Single Logout Service endpoint of your identity Provider. You can find its value in SingleLogoutService tag in IdP-Metadata XML Ne. Leave blank if SLO not supported by ISP
NameID Format	um.oasis.names.tc:SAML2.0.nameid-format.persistent
IDP Signing Certificate."	Commentation     C

#### Parameter description

- IDP Name: Specify a name as needed.
- IDP Entity ID/Issuer: Enter the portal URL of the IDaaS user account.
- Send Signed Requests: Select this field.
- SSO Binding Type: Select the first option.
- Single Sign On URL: Enter the portal URL of the IDaaS user account.

- NameID Format: Select SAML:2.0 nameid-format persistent. The value must be consistent with that on IDaaS.
- IDP Signing Certificate: Enter the SigningKey information obtained in the preceding operation.
- 6. Configure SAML settings on IDaaS.

Application Logo	SAML
	⊕Upload File     ■
	The image size must be less than 1 MB.
Application ID	idaas-cn-0pp1mb0e705saml
SigningKey	722e0dfd0149304c31dcafdbfd6852f8qNKdmq4Pw5Y
*Application Name	SAML
*Application Type	Web Application
*IDaaS IdentityId	Enter the IDaaS IdentityId
	IDaaS IdentityId is required
*SP Entity ID	Enter the SP entity ID
	SP Entity ID is required
*SP ACS URL (SSO Location)	Enter the SP ACS URL
SP Logout URL	Enter an SP logout URL
*NameIdFormat	Select ~
*Binding	POST ~
Assertion	Assertion Attribute key - +
7 tempores	Assertion property. When the value is set, the value is placed in the SAML assertion. The name is a custom name and the value is the attribute value of t he account.
Sign Assertion	● No

#### Parameter description

- SP Entity ID: Enter SP Base URL for your Confluence information. The value must be consistent with that in Confluence.
- IDaaS IdentityId: the portal URL of the IDaaS user account. The value must be consistent with that of IDP Entity ID/Issuer specified in the preceding operation.
- NameIdFormat: Select SAML:2.0 nameid-format persistent. The value must be consistent with that in Confluence.
- SP ACS URL (SSO Location): Obtain the SP ACS URL information from SP Base URL.
- 7. Enable and authorize the application on IDaaS.

Application List					Add Application			
Application List ↓ This page allows the administrator to manage applications. Once added t After an application is added to IDaaS, make sure to enable the application	o IDaaS, applications support single sign-on and uses in and authorize application access to users. The pag	r provisioning. ge also provides detailed in	formation about applications, including SSO URLs, a	application accounts, user pr	$\times$ rovisioning settings, authorization settings, and audit logs.			
Search by application name		Q						
Application L ogo Application Name	Application ID		Device Type	Applicat	tion Stat Actions			
S. JIRA	idaas-cn-0pp1mb0e705saml		Web Application		Authorize Details •			
Application Information	Authentication Information		Account Information - Provisioning		Account Information - Account Linking			
Details of the application View Details Modify Application Deteler Application	Single sign-on (SSO) URLs. IDaaS-initiated SSO URL		Modify SCIM settings and provision OUs and gro Provision OUs Configure SCIM	oups to the application.	Application accounts that are linked with IDaaS accounts. View Application Accounts			
Authorization Information	Audit Information		API					
Groups and accounts that are authorized to manage the application. Authorize	View detailed operation logs about the application View Logs View Provisioning Records		Whether to apply open system API  API Key API Secret					
Authorize OUs or Groups by Application Grant	Application Access by OU or Grou	up Grant App	lication Access by Account A	Authorize Accounts	s by Application Authorize Application by Class			
Application Authorization This page provides the administrator with m For example, the administrator can select a	Application Authorization          Image: Specific and the administrator with multiple ways to authorize application access.         Image: Specific and Specific and Specific and authorize multiple OUs and groups to access the application. Alternatively, they can select an account and grant the account access to multiple OUs and groups to access the application. Alternatively, they can select an account and grant the account access to multiple OUs and groups to access the application.							
Applications (1)		OUs and Group	os (787) Authorized: 0					
JIRA	٩	📠 : OU 🚲 : Gi	roup					
JIRA	>	Search by grou	id name					
1	Fotal 1 item < 🚹 >	Alibaba	a Cloud o1					

8. Log on the IDaaS console as the authorized user. Add an application account for the application.

The application account is the account used in JIRA or Confluence.

IDaa S				Add Application	Account
IDaaS	Application Accounts				
				Application	JIRA ~
Menu -	Sub-account list Sub-account approval				Select an application.
My Applications				IDaaS Account	
All Applications	Add Application Account Search by application name		٩		
Application Accounts	Application L Application Name			Application Ac count	Application Account
Settings ^	ogo Application Hanny				
Two-factor	SAP GUI	Approved	demoUser2		Note: This application account uses the Manual linking mode. You must enter the valid username to I og on to the application system.
Authentication	Salesforce		demoUser2		
Messages					Save
Logs	Autofill ross				

9. The IT administrator reviews and approves the new application account.

😑 🕞 Alibaba Clour	8			Q Search	Billing Ticket ICP Enterprise Suppor	t Alibaba Cloud 🖾 🎝 🗑 EN
Overview	Approvals					
Quick Start	Application Account Approvals					
Applications ^						
Application List	Approvals					
Add Applications	When a user attempts to log on to an applic	and process approval requests, when new approval requestation through SSO, an application account is required as the	in identity. If the Account Linking Type of the application is s	t the navigation pane. et to Manual and the user has not been assigned an ap	plication account before, an approval request is s	ubmitted to link an application account to the
Users ^	After the request is approved, the application	r can men process the request on this page. In account is used to log on to the application during SSO.				
Organizations and Gr						
Accounts		dion Name Pending ~ Q Search				
Class Management	IDaaS Account (Applicant)	Application Account	Application Name	Application Time	Approval Status	Actions
Authentication ^	demol iser2	demo	JIRA	2020-05-28 20:18:18		View Details Approve
Authentication Source						Disapprove Neview
RADIUS						Total 1 Rem
Certificates						
Authorization ^						
Policy Servers						
Application Authoriza						
Audit ~						
More ^						
Approvals 🚯						

10. Log on to JIRA or Confluence from the IDaaS console in a single sign-on manner.

You click the application icon on the My Applications page and log on to JIRA or Confluence in a single sign-on manner.

IDaaS	My Applications			
Menu ^	Web Applications			
My Applications				
All Applications Application Accounts Settings	J	salesforce		SAML
My Account Two-factor Authentication	JWT1 Account not Added	Salesforce	SAP GUI	JIRA
Messages Logs	[-]	Ο	[-]	J
	RAM - Role-based SSO Account not Added	OAUTH OAuth2 Account not Added	RAM - User-based SSO Account not Added	JWT JWT Account not Added

# 1.2. WordPress-SAML application usage

## WordPress-SAML applications

WordPress-SAML applications are used to implement single sign-on for WordPress.

#### 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**. Find the SAML application and click **Add Application** in the Actions column.
- 3. Click Add SigningKey. Configure the parameters and click Submit.

Add A	Add Application (WordPress-SAML)										
Imp	oort SigningKey	Add SigningKey									
Alia	S		SerialNumber		ValidityDa ys	KeyAlgori thm	Key Size	Actions			
				No Data							

4. Find the new SigningKey in the SigningKey list and click **Select** in the Actions column. Configure the parameters and click Submit.

Application Logo		
	⊕Upload File     ■	
	The image size must be less than 1 MB.	
Application ID	idaas-cn-0pp1mb0e705wordpress_saml	
SigningKey	89c2834f51d3ceb586e5e0930385a22cVVOJklLTMd1	
* Application Name	WordPress-SAML	
*Application Type	Web Application	
IDaaS IdentityId	Enter the IDaaS IdentityId	
	IDaaS IdentityId is required	
*SP Entity ID	Enter the SP entity ID	
	SP Entity ID is required	
SP ACS URL (SSO Location)	Enter the SP ACS URL	
SP Logout URL	Enter an SP logout URL	
NameldFormat	urn:oasis:names:tc:SAML:2.0:nameid-format:persistent	~
*Binding	POST	~
Sign Assertion	No	
* Account Linking	○账户关联 (系统按主子账户对应关系进行手动关联,用户添加后需要管理员审批)	
туре	○账户映射(系统自动将主账户名称或指定的字段映射为应用的子账户)	
	Submit Cancel	

**?** Note Set IDaaS IdentityId to a value as needed and this value must be consistent with that in WordPress. Set SP Entity ID, SP ACS URL, and NameIdFormat to the values obtained from WordPress.

### Configure WordPress-SAML

WordPress-SAML runs in a PHP environment and you must set up a PHP environment. The procedure is as follows:

- 1. Download WampServer from the official website and decompress it.
- 2. Download WordPress from the official website and decompress it to the www directory of WampServe.

📕   🗹 📕 =	www							_	
文件 主页	共享	查看							~
★ 固定到" 复制 快速访问"	<mark>亡</mark> 粘贴	<ul> <li>▲ 剪切</li> <li>■ 复制路径</li> <li>☑ 粘贴快捷方式</li> </ul>	移动到 复制到 <b>制除</b> 重命名	▲ 新建项目・ ① 轻松访问・ 新建 文件夹	<ul> <li>✓</li> <li>✓</li> <li>届性</li> <li>⊘</li> <li>の</li> <li>历史记</li> </ul>	<ul> <li>         → 全部选择         <ul> <li></li></ul></li></ul>			
	剪贴板		组织	新建	打开	选择			
$\leftarrow$ $\rightarrow$ $\checkmark$ $\uparrow$	]	这台电脑 > Wind	lows (C:) > wamp > www					~ Ū	搜索"www",
📙 桌面	*	^ 名称	^	修改日期	A	类型	大小		
🔖 下载	*	wampla	naues	2019/6	/10 17:06	文件夹			
🔃 文档	*	wampth	iemes	2019/6,	/10 17:06	文件夹			
🔚 图片	*	wordpress	ess	2019/6,	/10 17:22	文件夹			
la OneDrive		add_vho	ost.php	2016/8,	/16 18:02	PHP 文件	18 KB		
		favicon.	ico	2010/12	2/31 9:40	图标	198 KB		
🍤 这台电脑		index.pl	hp	2016/8,	/16 18:03	PHP 文件	30 KB		
挶 3D 对象		test_soc	:kets.php	2015/9,	/21 17:30	PHP 文件	1 KB		
📱 视频		testmys	ql.php	2016/5,	/17 15:58	PHP 文件	1 KB		
📙 图片		📓 wordpre	ess-5.2.1.zip	2019/6,	/10 17:14	WinRAR ZIP 压缩文件	11,836 KB		
📔 文档									
🔖 下载									
1 音乐									
▶ 桌面									
🗊 Windows	s (C:)								

- 3. Create a WordPress account in MySQL.
- 4. On the WordPress welcome page, set the username and password.

## 欢迎

欢迎使用著名的WordPress五分钟安装程序! 请简单地填写下面的表格,来开始使用这个世界上最具扩展性、最强大的个人信息发布平台。

需要信息								
您需要填写一些基本信息。无需担心填错,这些信息以后可以再次修改。								
站点标题								
用户名								
	用户名只能含有字母、数字、空格、下划线、连字符、句号和"@"符号。							
密码	195 隐藏							
	强							
	重要: 您将需要此密码来登录, 请将其保存在安全的位置。							
您的电子邮件								
	请仔细检查电子邮件地址后再继续。							
对搜索引擎的可见性	□ 建议搜索引擎不索引本站点							
	搜索引擎将本着自觉自愿的原则对待WordPress提出的请求。并不是所有搜索引擎都会遵守这类请求。							
安装WordPress								

- 5. Click Install WordPress in the lower-left corner.
- 6. Download miniorange-saml-20-single-sign-on.4.8.23 and decompress it to the

|--|

📕   🗹 📕 =	plugins							-		$\times$
文件 主页	共享	查看								^ ?
★ 固定到" 复制 快速访问"	おいたのでは、	剪切 复制路径 粘贴快捷方式	移动到 复制到	★ ■ 動除 重命名	□ 1 新建项目・ ① 轻松访问・ 新建 文件夹	<ul> <li>✓</li> <li>✓</li> <li>届性</li> <li>✓</li> <li>Ø历史记录</li> </ul>	<ul> <li>全部选择</li> <li>全部取消</li> <li>反向选择</li> </ul>			
	剪贴板		组织	只	新建	打开	选择			
$\leftarrow \rightarrow \checkmark \uparrow$	> 这	台电脑 > Wind	lows (C:) → wan	np > www >	wordpress > wp-con	tent⇒ plugins		~ Ŭ	搜索"plu	. P
📙 桌面	* ^	名称	^		修改日期	类型	大小			
📜 下载	*	📕 akismet			2019/5/22 2:25	文件夹				
📔 文档	*	📜 miniora	nge-saml-20-sin	gle-sign-on	2019/6/10 17:25	文件夹				
🔚 图片	*	hello.ph	р		2019/3/19 1:19	PHP 文件	3 KB			
\land OneDrive		index.pl	hp		2014/6/5 23:59	PHP文件	1 KB			
🍤 这台电脑										
📙 3D 对象										
🚪 视频										
📙 图片										
📔 文档										
📜 下载										
▶ 音乐										

7. Restart the php environment and choose Restart All Services. Then install and enable miniOrange: Log on to WordPress and click Plug-ins. Click Enable for miniOrange and then refresh the page.

語											
🔞 🔂 test 🛡 0	③ 合 test 季 ○ + \$n@t 篇, admin ■										
@ 仪表盘	插件 安装插件		显示选项 ▼ 帮助 ▼								
★ 文章	全部 (3)   息用 (1)   未息用 (2) 授素已安装的										
9)媒体	批量操作 🔹 应用		3个项目								
<ul> <li>■ 贝皿</li> <li>■ 评论</li> </ul>	□ 插件	图像描述									
🔊 外观	Akismet Anti-Spam 信用 删除	由千百万人使用,Akismet可能是保护您的贴点免受垃圾评论 <b>的世界上最好的方式</b> 。它会不断地保护您的贴点。使用方式:激活Ak 密钥。	cismet插件,然后转到Akismet设置页面来设置您的API								
★ 插件 <b>已安装的插件</b> 安装插件	<ul> <li>miniOrange SSO using SAML 2.0 停用</li> </ul>	4.1.2版本   田Automattic   王朝1919] miniOrange SAML 2.0 SSO enables user to perform Single Sign On with any SAML 2.0 enabled Identity Provider. 4.8.23版本   由miniOrange   访问循件主页									
Plugin Editor 🏜 用户	□ 你好多莉 应用 删除	这不是普遍的插件,它家庭看一代人帮望和热情,浓缩或Louis Armstrong的四个字:你好,多考,在应用后,在忽站点后台每个页 英文原版台词。 1.7.2版本   由Matt Mullenweg   查看详情	國的右上角都可以看到一句来自《何红娘》音乐剧的								
E CT	□ 插件	能像描述									
iminiOrange SAML 2.0 SSO	批量操作 * 应用		3个项目								

8. The miniOrange SAML item is displayed on the page.



9. Record the values of SP-EntityID/Issuer, ACS (Assertion Consumer Service) URL, and NameID format on the Identity Provider tab. Enter them on the Add Application (WordPress) page.

Application Logo	OUpload File The image size must be less than 1 MB.							
Application ID	idaas-cn-0pp1mb0e705wordpress_saml							
SigningKey	89c2834f51d3ceb586e5e0930385a22cVVOJklLTMd1							
*Application Name	WordPress-SAML							
*Application Type	Web Application							
IDaaS IdentityId	Enter the IDaaS IdentityId							
	IDaaS IdentityId is required							
*SP Entity ID	Enter the SP entity ID							
	SP Entity ID is required							
SP ACS URL (SSO Location)	Enter the SP ACS URL							
SP Logout URL	Enter an SP logout URL							
NameldFormat	urn:oasis:names:tc:SAML:2.0:nameid-format:persistent	~						
* Binding	POST	~						
Sign Assertion	No							
*Account Linking Type	○账户关联 (系统按主子账户对应关系进行手动关联,用户添加后需要管理员审批) ○账户映射 (系统自动将主账户名称或指定的字段映射为应用的子账户)							
	Submit Gancei							

10. Set IDaaS IdentityId to a value as needed and this value must be consistent with that on the Service Provider tab in WordPress. Download the .cer file from the IDaaS console and copy the file information to the X.509 Certificate field on the Service Provider tab in WordPress.

Identity Provider	Service Provider	Sign in Settings	Attribute/Role Mapping	Help & FAQ	Licensing Plans			
Configure Servi	ce Provider							
Enter the information	n gathered from your Id	entity Provider						
Identity Provider Na	me*: 123							
IdP Entity ID or Issuer *: http://idass-local.com/idass								
SAML Login URL *: http://idass-local.com/idass								
X.509 Certificate *:	BI MIIC6j BhMC0 DTE5M	BEGIN CERTIFICATE MIIC6jCCAdKgAwiBAgile8oMA971gp0wDQYJKoZIhvcNAQEFBQAwNTELMAkGA1UE BhMCQQ4xDzANBgNVBAgMBuWbm+W3nTEVMBMGA1UEAxMMd29yZFByZXNzNjEwMB4X DTE5MDYxMDA4MDEyNFoXDTIwMDYwOTA4MDEyNFowNTELMAkGA1UEBhMCQ04xDzAN						
NOTE: Format of the certificate: BEGIN CERTIFICATE XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX								
Response Signed:	red: Check if your IdP is signing the SAML Response. Leave checked by default.							
Assertion Signed:	ssertion Signed: Check if the IdP is signing the SAML Assertion. Leave unchecked by default.							
	Si	ive Test conf	guration					

11. After the configuration is complete, add an application account for the WordPress-SAML application. This application account is the email address for the account in WordPress. Then you can log on to WordPress from the IDaaS console in a single sign-on manner.

#### Notes

1. The URL of the local WordPress application is 127.0.0.1 or localhost. You can modify the URL on **Settings** page.

You will need the following information to configure your IdP. Copy it and keep it handy:

SP-EntityID / Issuer	http://127.0.0.1/wordpress/wp-content/plugins/miniorange-saml-20-single- sign-on/
ACS (AssertionConsumerService) URL	http://127.0.0.1/wordpress/
Audience URI	http://127.0.0.1/wordpress/wp-content/plugins/miniorange-saml-20-single- sign-on/
NameID format	urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
Recipient URL	http://127.0.0.1/wordpress/
Destination URL	http://127.0.0.1/wordpress/
Default Relay State (Optional)	Available in the <b>premium</b> version
Certificate (Optional)	Available in the <b>premium</b> version

🔞 📸 wordpress 😔	1 투 0 🕂 新建	
🚳 仪表盘	常规选项	
★ 文章	站点标题	wordpress
■ 页面	副标题	又一个WordPress站点
♥ 评论		用简洁的文字描述本站点。
<ul><li>▶ 外观</li><li>▶ 插件 1</li></ul>	WordPress地址(URL)	http://127.0.0.1/wordpress
🎍 用户	站点地址(URL)	http://127.0.0.1/wordpress
		如果您想 <u>让您的站点主贞与WordPress安禄自录不同</u> ,请在此输入地址。
常規	管理邮件地址	test@mail.com
jung 阅读 讨论	成员资格	
媒体 固定链接 隐私	新用户默认角色	订阅者 >
inniOrange SAML 2.0 SSO	站点语言 😡	简体中文 ✓
● 收起菜单	时区	×上海 v
>日优选 ※ <u>70岁老中</u>	医!治疗肝病,不能错过这个好方法	##8 = 1977 同一時11 2016 ま =

2. If you cannot modify the miniOrange settings, click the link in the red rectangle in the following figure to log on to miniOrange.

		host/wordpress/w	p-admin/admin.php	?page=mo_sam	_settings&tab=config						
	前 test ■ 0 + ::	暗표대 LindUser P	ortal API 🗧 JSONG	333解析及信云 🕻	企业权信 🧾 九州云梅					嵵,	
	429 仪表盘	(Warning: <u>PHP openss</u>	<u>el extension</u> is not instal	led or disabled)							
	📌 文章	Account Setup	Identity Provider	Service Provid	er Attribute/Role Mapping	Help & FAQ	Licensing Plans				
	9〕媒体								Support		
	■ 页面 <b>-</b> 评论	Prese Departure August and another and the another ano							Need any help? We can help you with configuring your Ider Just send us a query and we will get back to you soon.		
	🔊 外观	You will need the	following information	to configure your	figure your IdP. Copy it and keep it handy:				Enter your email		
<	★ 插件 ▲ 用户	SP-EntityID / Issuer		h	http://localhost/wordpress/wp-content/plugins/miniorange-saml-20-single- sign-on/				Write your query here		
`	<b>⊁</b> 工具	ACS (AssertionConsumerService) URL Audience URI NameID format			http://localhost/wordpress/						
	■ 後年 ① miniOrange SAML /				http://localhost/wordpress/wp-content/plugins/miniorange-saml-20-single- sign-on/ urnoasisnamestc:SAML:1.1:nameid-formatemailAddress					提交	
	2.0 SSO ● 收起菜单										
		Recipient URL		h	http://localhost/wordpress/						
		Destination UF	RL	h	tp://localhost/wordpress/						
		Default Relay	State (Optional)	h	http://localhost/wordpress/						
		Certificate (Op	tional)	C	ownload (Register to download th	e certificate)			73 第	数活 Windows <sup></sup> 封"设置"以激活 Windows	

# 1.3. Implement single sign-on for Salesforce

This topic describes how to use the SAML protocol to implement single sign-on for Salesforce in the IDaaS console.

## Background

Salesforce is a customer relationship management (CRM) software service provider based in San Francisco, USA. It was founded in 1999 and provides a customer relationship management platform for on-demand applications. Salesforce supports single sign-on with the SAML protocol.

#### 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 Application**. Find the Salesforce application and click Add Application in the Actions column.

😑 C-J Alibaba Cloud	ł		Q	Search	Expenses Tickets ICP Enterprise S	Support Official Site 돈	1 🗘 🕐 EN 🌔
Overview	OAUTH	OAuth2	plugin_oauth2	OAuth2	obtain to ken access through OAuth_Token, and carry the token to the server to request user resources. Application can use OAuth application template to realize unified identity management.	Web Application	Add Application
Applications ^ Application List Add Applications	SAME	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 (Dasa) and the token consumer (application) and achieves single sign-on targetting cross- domain network. SAML is mature authentication protocol, which is widely used in public and private load at home and abroad.	Web Application	Add Application
Users ^ Organizations and Groups Accounts Management	-	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 wedly include ERP, CRM, data analysis, HR, logistics, travel, finance and other aspects. With 18000 global partners, SAP is widely distributed in 25 different industries, providing digital management solutions for various stages of enterprises.	PC Client	Add Application
Class Management Authentication ^ Authentication Sources	-	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 ucgrading, etc. Daas supports single sign-on to salesforce website through SAML protocol.	Web Application	Add Application
RAUIUS Certificate Management Authorization ^ Policy Servers Application Authorization		WordPressSaml	plugin_wordpress_saml	SSO, SAML, CMS	WordPress is the most widely used CMS (content management system) in the word. It allows tens of millions of technical or non- technical presonnel to produce and manage various types of websites through a very powerful plug-in system and a convenient and natural operation interface. From business websites and government pages to personal blogs and theme forums, WordPress supports a variety of forms. (DasS supports single sign on to WordPress website through SML protocol.	Web Application	Add Application
Audit × More × Settings ×	FORM	Form Submit	plugin_aes256	SSO, AES256	Form submit can simulate a login mode in which users enter their user name and password on the login page and submit them through the form. The accurd password of the application is stored locally in DaaS using aex526 encryption algorithm. Many old systems, systems that do not support transformation can use form filing to during users that do not support transformation can use form filing to during users that do not support transformation can use form filing to during users that do not support transformation can use form filing to during users that do not support transformation can use form filing to during users that do not support transformation can use form filing to during users of the during transformation can use form filing to during users that do not support transformation can use form filing to during users that do not support transformation can use form filing to during users that do not support transformation can use form filing to during users that do not support transformation can use form filing to during users that do not support transformation can use form filing to during users that do not support transformation can use form filing to during users that do not support transformation can use form filing to during users that do not support transformation can use form filing to during users that do not support transformation can use form filing to during users that do not support transformation can use form filing to during users that do not support transformation can use form filing to during users transformation can use form filing to during users that do not support transformation can use form filing to during users that do not support transformation can use form filing to during users that do not support transformation can use form filing to during users that do not support transformation can use form filing to during users that do not support transformation can use form filing to during users that do not support transformation can users that do not support transform	Web Application	Add Application

3. Find an existing SigningKey. You can add a SigningKey first if there are no existing SigningKeys. Click Export in the Actions column. Export a .cer certificate locally.

Import SigningKey       Add SigningKey         Alias       SerialNumber       ValidityDa ys       KeyAlgori thm       Key Size       Actions         CN=1, ST=1, C=CN       1842960145345832170       180       RSA       2048       Select Export	A	Add Application (Salesforce)								
AliasSerialNumberValidityDa ysKey Algori thmKey SizeActionsCN=1, ST=1, C=CN1842960145345832170180RSA2048Select Export		Import SigningKey Add SigningKey								
CN=1, ST=1, C=CN 1842960145345832170 180 RSA 2048 Select Export		Alias	SerialNumber	ValidityDa ys	KeyAlgori thm	Key Size	Actions			
		CN=1, ST=1, C=CN	1842960145345832170	180	RSA	2048	Select Export			

4. Log on to Salesforce as an administrator. Click Settings in the upper-right corner.



5. In the left-side navigation pane, choose Identity > Single Sign-On Settings. Find SAML Single Sign-On Settings and click New.

	Q, Search Setup
Setup Home Object	tt Manager 🗸
PLATFORM TOOLS	
> Apps	Strup
> Feature Settings	Single sign on Settings
> Einstein	
> Objects and Fields	Single Sign-On Settings
> Process Automation	Configure single sign-on in order to authenticate users in salesforce.com from external environments. Your organization has the following options available for single sign-on:
> User Interface	Federated authentication, a single sign-on method that uses SAML assertions sent to a Salesforce endpoint.
> Custom Code	Edit SAML Assertion Validator
> Environments	Federated Single Sign-On Using SAML
> User Engagement	SAMLEnabled
> Integrations	
> Notification Builder	SAML Single Sign-On Settings New from Metadata File New from Metadata URL
SETTINGS	Ne SAML Single Sign-On Settings
> Company Settings	
> Data Classification	
✓ Identity	
Auth. Providers	
Identity Provider	
Identity Verification	
Identity Verification History	
Login Flows	
Login History	
OAuth Custom Scopes	
Single Sign-On Settings	

6. Go to the SAML Single Sign-On Settings page.

	Save Save & New Cancel			-
Name		API Name	1	
SAML Version	2.0			
Issuer		Entity ID		
Identity Provider Certificate	选择文件 未选择任何文件			
Request Signing Certificate	Generate self-signed certificate V			
Request Signature Method	RSA-SHA256 V			
Assertion Decryption Certificate	Assertion not encrypted V			
SAML Identity Type	Assertion contains the User's Salesforce username     Assertion contains the Federation ID from the User object     Assertion contains the User object     Assertion contains the User object			
SAML Identity Location	Identity is in the Nameldentifier element of the Subject statement     Identity is in an Attribute element			
Identity Provider Login URL				
Custom Logout URL				
Custom Error URL				
Single Logout Enabled				
st-in-time User Provisioning				

- **Name**: the name of the SAML single sign-on configuration. You can enter a name as needed.
- Issuer: Note that this value must be the same as that of IDaaS IdentityId in IDaaS.
- Entity ID: Set it to https://SAML.Salesforce.com.
- Identity Provider Certificate: Select the certificate file exported from IDaaS.
- **Request Signing Certificate**: Use the default value.
- Request Signature Method: Set it to RSA-SHA1.
- Assertion Decryption Certificate: Select Assertion unencrypted.
- SAML Identity Type: Select Assertion contains User's Salesforce username.
- **SAML Identity Location**: Select Identity is in the NameIdentifier element of the Subject statement.
- Leave Identity Provider Login URL, Customer Logout URL, and Custom Error URL empty.

Click Save.

7. After you configure the SAML settings, the SAML details will be displayed with the name that you specified. You must the value of Salesforce Login URL for later use.

Single Sign-On Settin	gs
SAML Single Sign-On Set	ttings
	Edit Delete Clone Download Metadata SAI
Name	1
SAML Version	2.0
Issuer	1
Identity Provider Certificate	CN=1, ST=1, C=CN Expiration: 24 Nov 2020 11:27:00 GMT
Request Signing Certificate	SelfSignedCert 28May2020 114740
Request Signature Method	RSA-SHA256
Assertion Decryption Certificate	Assertion not encrypted
SAML Identity Type	Username
SAML Identity Location	Subject
Identity Provider Login URL	
Custom Logout URL	
Custom Error URL	
Single Logout Enabled	
Just-in-time User Provisioning	
User Provisioning Enab	bled
Endpoints View SAML endpoints for your organization, cor	nmunities, or custom domains.
Your Organization	
Login U	JRL https://login.salesforce.com?so=00D2x000004uc8r
OAuth 2.0 Token Endp	pint https://login.salesforce.com/services/oauth2/token?so=00D2x000004uc8r
	Edit Delete Clone Download Metadata SAM

Note: You also can click the SAML name to view the value of Salesforce Login URL on the preceding page.

SAML Si	ngle Sigr	n-On Settings		New New from Metadata File New from Metadata URL
Action	Name	SAML Version	Issuer	Entity ID
Edit   De	1	2.0	1	https://ap17.lightning.force.com/lightning/setup/SingleSignOn/page?address=%2F0LE%2Fe%3FretURL%3D%25.

8. Find Single Sign-On Settings and click Edit.

Setup Single Sign-On Settings
Single Sign-On Settings
Configure single sign-on in order to authenticate users in salesforce.com from external environments. Your organization has the following options available
Federated authentication, a single sign-on method that uses SAML assertions sent to a Salesforce endpoint.
Edit SAML Assertion Validator
Federated Single Sign-On Using SAML
SAML Enabled

9. Select the SAML Enabled check box and click Save.

SETUP Single Sign-On Settings	
Single Sign-On Settings	
	Save
Federated Single Sign-On Using SAML	
	Save

10. Return to the Add Application (Salesforce) page of the IDaaS console. Find the target SingingKey and click Select in the Actions column to configure the SAML parameters.

Application Logo	© Upload File The image size must be less than 1 MB.
Application ID	
SigningKey	
*Application Name	Enter an application name
*Application Type	
*IDaaS IdentityId	Enter the IDaaS IdentityId
	IDaaS IdentityId is required
*SP Entity ID	Enter the SP entity ID
	SP Entity ID is required
*SP ACS URL (SSO Location)	Enter the SP ACS URL
SP Logout URL	Enter an SP logout URL
*NameIdFormat	Select
*Binding	Select
Sign Assertion	No
*Account Linking Type	
	Submit Cancel

- Set IDaaS IdentityId to the value of Issue specified in Salesforce.
- Set SP ACS URL(SSO Location) to the Salesforce logon URL.

Note The URL format is https://login.Salesforce.com?so=<Your organization ID>. If you are not sure about your organization ID in Salesforce, go to the Company Profile > Company Information page of Salesforce.

11. Enable and authorize the application.

😑 🕞 Alibaba Cloud	i				Q Search	Billing Tic	ket ICP Enterprise	Support Albaba Cloud 🖾	і ф <b>.</b> ж ем
Overview	Application	n List							Add Applicati
Quick Start Applications Application List	♀ A ∏ A	pplication List his page allows the administrator to manage applications. Once added t ifter an application is added to IDaaS, make sure to enable the application	o IDaaS, applications support single sign-on and user on and authorize application access to users. The pag	provisioning. e also provides detailed i	nformation about applications, including SSO URLs, application acco	unts, user pro	vvisioning settings, autho	rization settings, and audit logs.	
Add Applications	Search by	application name		۹					
Users ^ Organizations and Gr	Application ogo	on L Application Name	Application ID		Device Type	Applicati us	ion Stat	Actions	
Accounts	Laboratore	Salesforce	idaas-cn-0pp1mb0e705salesforce		Web Application			Authorize Details +	
Class Management	Appli	ication Information	Authentication Information		Account Information - Provisioning		Account Information	- Account Linking	
Authentication Source RADIUS Certificates	Detail View	Is of the application Details Modify Application Delete Application	Single sign-on (SSO) URLs. DaaS-initiated SSO URL		Modify SCIM settings and provision OUs and groups to the appl Provision OUs Configure SCIM	ication.	Application accounts that are linked with IDaaS accounts.		ts.
Authorization									
Policy Servers Application Authoriza	Autho	orization Information	Audit Information		API				
Audit ~	Group	ps and accounts that are authorized to manage the application.	View detailed operation logs about the application. View Logs View Provisioning Records		Whether to apply open system API				
Settings ~									
😑 🕞 Alibat	ba Cloud	1						Q Se	arch
Overview	_	Application Authorization							
Quick Start		Authorize OUs or Groups by Application G	rant Application Access by OU or Gr	oup Grant Ap	pplication Access by Account Authorize Acc	ounts by	Application A	Authorize Application by	Class
Applications Application Li: Add Applicatio	st ons	Application Authorization This page provides the administrator w For example, the administrator can sel	vith multiple ways to authorize applica ect an application and authorize mult	ition access. iple OUs and gro	ups to access the application. Alternatively, the	y can sel	ect an account ar	id grant the account acc	cess to multi
Users Organizations	and Gr	Applications (1)		OUs and Grou	ups (787) Authorized: 0				
Accounts	Salesforce		٩		Group				
Class Manage	ement	Salesforce	>	Search by gro	oup name				
Authentication	^	1		🖃 🗆 🥼 Aliba	ba Cloud				
Authentication	n Source		Total 1 item < 1 >	⊡ li ab	mo1 c				

12. Add an application account and log on to Salesforce in a single sign-on manner.

Application List					Add Application				
Application List									
Search by application frame a									
Application L ogo Application Name		Application ID	Device Type	Application Stat us	Actions				
Salesforce		idaas-cn-0pp1mb0e705salesforce	Web Application		Authorize Details •				
Application Information		Authentication Information	Account Information - Provisioning	Accou	unt Information - Account Linking				
Details of the application		Single sign-on (SSO) URLs.	Modify SCIM settings and provision OUs and groups to the application	ition. Applic	ation accounts that are linked with IDaaS accounts.				
View Details Modify Application	Delete Application	IDaaS-initiated SSO URL	Provision OUs Configure SCIM	View A	Application Accounts				
Authorization Information		Audit Information	API						
Groups and accounts that are authorized	to manage the application.	View detailed operation logs about the application.	Whether to apply open system API						
Authorize		View Logs View Provisioning Records	API Key API Secret						

Application List / Application	Accounts						
← Application Accoun	ts					Link Ace	counts Batch Import Batch Export
Application Accounts Sub account refers to t for example: there is a pplication is created, if	he identity of the user in the specified app main account Zhang San (user name Zha account mapping is selected, the default p	ication system. Master account refers to the ngsan) in IDaa5. In the enterprise BPM app rrimary account and sub account are comple	account in idaas. During single sign on, i blication system, the user name of this use tely the same, without configuration. If ac	laas will transfer the corresp r is agoodman, that is, the s count association is selected	onding sub account to the application system b account should be agoodman, which is ass , manual sub account creation and primary su	which needs to exist and be recognizable i ociated with the main account Zhangsan. < b account association need to be performed	$\times$ the application system, $\label{eq:basic} {\rm br}  (>$ account association method; when the a $t$ here,
Salesforce							
Search by IDaaS account nam	me						
IDaaS Account	Display Name	Application Account	Application Account Password	Linked	Approval Status	Linked At	Actions
				lo Data			
							fotal 0 item < 1 > Goto 1
Link Account	s						×
100.4	IDeeC Asses						
*IDaaS Accou	nt IDaas Accou	m					
Application	Application A	coount					
Account	Application	CCOUTIL					
	Save F	Return					
IDaa S						Messages 🕕	demoUser2 + 🔲 Language v
IDaa S	My Applications						
My Applications	Web Applications						
All Applications Application Accounts							
Settings ^		JWT	OAUTH			JWT	salesforce
My Account Two-factor	RAM - Role-based SSO Account not Added	JWT1 Account not Added	OAuth2 Account not Ad	led	RAM - User-based SSO Account not Added	JWT Account not Added	Salesforce
Authentication Messages							
Logs		F	1				
	C/S_applications	Autofill					
	Mobile Applications						

If all the preceding steps are successful, you have logged on to Salesforce in a single sign-on manner.

# 2.Standard Protocol Template Usage Guide

## 2.1. C/S Applications User Manua

The OIDC protocol can be used to pass in parameters for logon after the program has been enabled. This method only applies to applications that can receive and parse OIDC protocol parameters.

#### Procedure

1. In the left-side navigation pane, choose **Applications > Add Applications**. Find the C/S program and click **Add Application** in the Actions column.

♥ To set up SS	O with a client/server application, you must install IDP-Agent.
Application Logo	
	⊕Upload File
	The image size must be less than 1 MB.
<ul> <li>Application Name</li> </ul>	C/S_applications
Executable File	For example, abc.exe.
	The executable file that starts the client/server application.
Executable File Path	For example, C:\User\AppData\abc\
	Executable File Path
Parameters	For example, d=idp&m=code.
	The parameters that are needed when starting the client/server application.

**?** Note To implement single sign-on for C/S applications, you must install the IDP-Agent plug-in locally.

- Application Name: required. Specify a name as needed.
- Executable File: the name of the executable file for startup.
- Executable File Path: the path of the C/S application file on the local computer.
- 2. Enable and Authorize the application. By default, Authorize Groups by Application is selected.

ol Template Usage Guide

Application Log o Application Name	Application ID	Device Type	Application	Status Actions	
C/8_applications	idaas-cn-0pp1mb0e705cs_oidc	PC Client		Authorize Details 🔺	
Application Information	Account Information - Provisioning	Account Information - Accou	nt Linking	Authorization Information	
Details of the application View Details Modify Application Delete Application	Modify SCIM settings and provision OUs and groups to on. Provision OUs Configure SCIM	o the applicati Application accounts that are li View Application Accounts	nked with IDaaS accounts.	Groups and accounts that are authorized to manage the applicatio n. Authorize	
Audit Information Wew detailed operation logs about the application. Wew Logs View Provisioning Records	API Whether to apply open system API API Key API Secret				
Authorize OUs or Groups by Application Grant Application Access by OU or Group Grant Application Access by Account Authorize Accounts by Application Authorize Application by Class					
Application Authorization This page provides the administrator wit For example, the administrator can sele	h multiple ways to authorize application ac ct an application and authorize multiple OI	ccess. Us and groups to access the application	on. Alternatively, they can sele	ct an account and grant the account access to multiple	
Applications (1)	OUs ar	nd Groups (787) Authorized: 0			
C/S_applications	Q	OU 🚲 : Group			
C/S_applications	> Search	h by group name			
• Total 1	item < 1 >	Alibaba Cloud			

- 3. Log on to the IDaaS console as a common user. For more information, see Logon in User Guide.
- 4. Click the C/S application icon on the My Application page.

IDaaS					Messages 🚺	demoUser2
IDaaS	My Applications					
Menu ^	Web Applications					
My Applications						
All Applications						0
Application Accounts	<b>C-D</b>	J	[-]	J		8
Settings ^	DAM Dala based SSO	DA/T4	DAM, Lines bened SCO	DACE	C/C emplicatio	
Two-factor Authentication	Account not Added	Account not Added	Account not Added	Account not Added	C/S_applicatio	ns
Messages						
Logs	Mobile Applications					

After the application account has been added, you can click the C/S application icon on the My Application page to perform single sign-on.

# 2.2. OAuth2.0 Application User Manual

OAuth2 is an open protocol for resource authorization. Applications can obtain access tokens through OAuth and use the tokens to request user resources from the server. Applications can use the OAuth application for centralized authentication.

#### 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 Application**.
- 3. Find the OAuth2 application and click Add Application in the Actions column.

Application Logo	© Upload File The image size must be less than 1 MB.
Application ID	idaas-cn-0pp1mb0e705oauth2
* Application Name	OAuth2
* Application Type	Web Application If you select Web Application or PC Client, the application is displayed in Web browsers. If you select Mobile Application, the application is displayed in mobile applications. If you select Data Provisioning, the application is used for data provisioning only and not visible to users. To display the application in multiple environments, select multiple check boxes.
* Redirect URI	http://www.baidu.com
Allow callback subdomains	If enabled, the RedirectURI passed when the SP initiates single sign-on can enable the subdomain of the currently configured Redirect URI add ress.
SP HomePageURL	The home page of the application. You can manually initiate SSO.
* GrantType	authorization_code ~
	autnonzation_code: autnonzation code mode (log on to obtain the code and then obtain the token), standard OAuth2 process; implicit: simplifie d mode (in the redirect_uri Hash delivery token) is used to verify the legality of third parties.
Access_Token有效期 Validity	7200 The validity period of Access_Token有效期. Unit: seconds. Default is 7,200.
Refresh Token Validity	604800 The validity period of Refresh Token. Unit: seconds. Default is 604,800.

4. View the details of the OAuth2 application and obtain the values of AppKey, AppSecret, and Authorize URL.

Application Details (0	DAuth2)
Application Logo	OAUTH
Application ID	idaas-cn-0pp1mb0e705oauth2
Application Name	OAuth2
Client Id	bc57d9ab8f22805a1c2cd5add5a252cerX5s4dcAPJx
Client Secret	
Redirect URI	http://www.baidu.com
Allow callback subdomains	Yes
SP HomePageURL	
GrantType	authorization_code
Authorize URL	https://iroiuldfai.login.aliyunidaas.com/oauth/authorize?response_type=code&scope=read&client_id=bc57d9ab8f22805a1c2cd5add5a252cerX5
	s4dcAPJx&redirect_uri=http%3A%2F%2Fwww.baidu.com&state=ikzzx9j4
Access_Token有效期 Validity	7200Seconds
Refresh Token Validity	604800Seconds
Application Status	Enable
Created By	idaas_manager
Created At	2020-05-28 18:09

5. Open the Authorize URL in your browser and use the authorized account to log on. After successful logon, you will be redirected to the webhook address. Extract the value of the code parameter from the address bar of the browser.

	D		
	Alibaba Cloud		
	Email/Phone/Username		
	Password		
	Please Enter Captcha		
	Forgot Password?		
	Login		
	Other login methods		
		X	

6	話      話      話      話      「      話      話      話      「      話     話      話      話      話      話     話	-下, 你 C 合	就知道 う☆	× +	百度 (	https://www.baidu.com	/:code=PyEBcua	ustate=ikzzx9j4				
新闻	hao123	地图	视频	贴吧	学术	更多		]				
									Bai <sup>*</sup> @ 百度			
										 രി	百度一下	

- 6. Use Postman to send a POST request to http://{IDaaS\_server}/oauth/token? grant\_type=authorization\_code&code={code}&client\_id={AppKey}&client\_secret= {AppSecret}&redirect\_uri={redirect\_uri}
  - Replace {IDaaS\_server} with the IP address of the IDaaS server.



• Replace {code} with the value of the code parameter obtain in step 5.

**Notice** The value of the code parameter can only be used once.

• Replace {AppKey} and {AppSecret} with the values obtained in step 4.

Application Details (C	)Auth2)
Application Logo	OAUTH
Application ID	idaas-cn-0pp1mb0e705oauth2
Application Name	OAuth2
Client Id	bc57d9ab8f22805a1c2cd5add5a252cerX5s4dcAPJx
Client Secret	
Redirect URI	http://www.baidu.com
Allow callback subdomains	Yes
SP HomePageURL	
GrantType	authorization_code
Authorize URL	https://iroiuldfai.login.aliyunidaas.com/oauth/authorize?response_type=code&scope=read&client_id=bc57d9ab8f22805a1c2cd5add5a252cerX5
	s4dcAPJx&redirect_uri=http%3A%2F%2Fwww.baidu.com&state=ikzzx9j4
Access_Token有效期 Validity	7200Seconds
Refresh Token Validity	604800Seconds
Application Status	Enable
Created By	idaas_manager
Created At	2020-05-28 18:09

- Replace {redirect\_uri} with the value of Redirect URL that you specified in step 3.
- 7. The IDaaS server returns the access token, which can be used to access IDaaS server resources.
- 8. Use Postman to send a GET request to http://{IDaaS\_server} /api/bff/v1.2/oauth2/userinfo? access\_token={access\_token}

**Note** v1.2 indicates the version. Replace it with the actual version. If no version number is written in js, enter v1 here. If a version number is written in js, enter that value here.

Iter Hide data URLs All XHR CSS Img Media Font Doc WS Manifest Other   500 ms 1000 ms 1500 ms 2000 ms 2500 ms 3000 ms   ame × Headers Preview Response Timing   applys • General • • •   applys • • General • •   applys • • • • •   • • • • • <	Elements Console	e Sources Network Performance Memory Application Security Audits					
Iter       Hide data URLS All XHR S CSS Img Media Font Doc WS Manifest Other         500 ms       1000 ms       1500 ms       2000 ms       2500 ms       3000 ms       3500 ms         ame       × Headers       Preview Response Timing       V1       Image: Status Code: 2000 (from memory cache)       Request URL: https       b/idaas/1.1.0/js (app.js)       app.js         apply       status Code: 2000 (from memory cache)       Request Method: GET       Status Code: 2000 (from memory cache)       Referrer Policy: no-referrer-when-downgrade         Referer Policy: no-referrer-when-downgrade       Referrer Policy: no-referrer-when downgrade       Offline No throttling ▼         Iter       Hide data URLs All XHR S CSS Img Media Font Doc WS Manifest Other       100 ms       200 ms       200 ms       700 ms       800 m         100 ms       200 ms       300 ms       400 ms       V1.2       700 ms       800 m         ame       × Headers       Preview Response Cookies Timing       700 ms       700 ms       800 m         100 ms       200 ms       300 ms       400 ms       V1.2       700 ms       800 m         100 ms       200 ms       300 ms       400 ms       V1.2       700 ms       800 m         100 ms       200 ms       300 ms       400 ms       V1.2       7	🖲 🔕   🖿 🍟 🔍   View:	: 📰 🛬 🔲 Group by frame 🛛 🔲 Preserve log 💭 Disable cache 🗍 💭 Offline 🛛 No throttling 🔹					
500 ms       1000 ms       1500 ms       2000 ms       2500 ms       3000 ms       3500 ms         ame       ×       Headers       Preview       Response       Timing         appijs       • General       Request URL: https:       b/idaas/1.1.0/js       app.js         appijs       • General       Request URL: https:       forom memory cache)       Reduest Orbit         Returned       × Headers       Performance       Memory       Application       Security       Audits         Iter       • Hide data URLs       All       XHR       S CSS       Imp       400 ms       V1.2       600 ms       700 ms       800 ms	ilter 🛛	Hide data URLs All XHR JS CSS Img Media Font Doc WS Manifest Other					
ame × Headers Preview Response Timing   appjs General   chunk-vendorsjs appjs   appis Pequest URL: https   pois boistrapjs   mainjs Request URL: https://response   bootstrapjs   mainjs   version?productid=idaas&call   Referrer Policy: no-referrer-when-downgrade   version?productid=idaas&call   Proview   estimation   Oview: = Console   Sources   Network   Performance   Memeric   Norma   200 ms    400 ms <td< td=""><td>500 ms</td><td>1000 ms 1500 ms 2000 ms 2500 ms 3000 ms 3500 ms</td></td<>	500 ms	1000 ms 1500 ms 2000 ms 2500 ms 3000 ms 3500 ms					
ame × Headers Preview Response Timing     app.js   app.		v1					
app.js       ✓ General         chunk-vendors.js       Request URL: https         app.js       b/idaas/1.1.0/js         app.js       Request Wethod: GET         status Code: ● 200 (from memory cache)         main.js       Remote Address: 124.193.235.240:443         wersion?productId=idaas&call       Referrer Policy: no-referrer-when-downgrade         Image: Sources       Network         Performance       Memory         Application       Security         Audits       Image: Sources         Iter       Hide data URLs         Hide data URLs       All         200 ms       300 ms         400 ms       V1.2         600 ms       700 ms         800 m       700 ms         100 ms       200 ms         300 ms       400 ms         V1.2       600 ms         700 ms       800 m         100 ms       200 ms         100 ms       400 ms         400 ms       V1.2         600 ms       700 ms         800 m       700 ms         100 ms       400 ms         400 ms       V1.2         600 ms       700 ms         Request URL	ame	× Headers Preview Response Timing					
chunk-vendors.js   app.js   app.js   aplus_v2.js   bootstrap.js   main.js   version?productId=idaas&call.     Referrer Policy: no-referrer-when-downgrade     Clumk-vendors.js?v=1.2.12     version?js?v=1.2.12     request URL: https::   // frontend/itmanager/js/app. j; 2v=1.2.12   Request URL: https::   // frontend/itmanager/js/app. j; 2v=1.2.12	app.js	👻 General					
aplus_v2.js bootstrapjs main.js version?productd=idaas&call Status Code: ● 200 (from memory cache) Remote Address: 124.193.235.240:443 Referrer Policy: no-referrer-when-downgrade Referrer Policy: no-referrer Policy: no-referrer-when-downgrade Referrer Policy: no-referrer-when-downg	chunk-vendors.js app.js	Request URL: https b/idaas/1.1.0/js app.js Request Method: GET					
Bootstrap,s       Remote Address: 124.193.235.240:443         main,js       Version?productId=idaas&call         Referrer Policy: no-referrer-when-downgrade         Image: Sources       Network         Performance       Memory         Application       Security         Audits       Security         Iter       Hide data URLs         All       XHR         Sources       Network         Performance       Memory         Application       Security         Audits       Security         Iter       Hide data URLs         Mame       X         Headers       Preview         Request URL: https::       'frontend/itmanager/js/app.j;?v=1.2.12         Request URL: https::       'frontend/itmanager/js/app.j;?v=1.2.12	aplus_v2.js	Status Code:  200 (from memory cache)					
Imain,js       Referrer Policy: no-referrer-when-downgrade         Referrer Policy: no-referrer-when-downgrade         Imain,js         Referrer Policy: no-referrer-when-downgrade         Imain,js         Referrer Policy: no-referrer-when-downgrade         Referrer Policy: no-referrer-when-downgrade         Imain,js         Referrer Policy: no-referrer-when-downgrade         Referrer Policy: no-referrer-when-downgrade         Imain,js         Referrer Policy: no-referrer-when-downgrade         Referrer Policy: no-referrer-when Preserve log         Doms       200 ms         Sources       400 ms         V1.2       600 ms         Referrer Policy: no-referrer-when Preview Response Cookies Timing         Request URL: https::       'frontend/itmanager/js/app.j; 2v=1.2.12         Request URL: https::       'frontend/itmanager/js/app.j; 2v=1.2.12	bootstrap.js	Remote Address: 124.193.235.240:443					
Image: Sources Network   Network Performance   Memory Application   Security Audits     Iter Hide data   Uns Image: Sources   100 ms 200 ms   200 ms 300 ms   400 ms V1.2     600 ms   700 ms   800 ms   100 ms   200 ms   300 ms   400 ms   V1.2     600 ms   700 ms   800 ms     100 ms   200 ms   300 ms   400 ms   V1.2     600 ms   700 ms   800 ms   100 ms   200 ms   200 ms   300 ms   400 ms   V1.2   600 ms   700 ms   800 ms   100 ms   200 ms   200 ms   300 ms   400 ms   V1.2   600 ms   700 ms   800 ms   100 ms   200 ms   200 ms   200 ms   300 ms   400 ms   100 ms   200 ms   200 ms   300 ms   400 ms   100 ms   200 ms <td colspan="5">main.js varien?productid_idens@vall Referrer Policy: no-referrer-when-downgrade</td>	main.js varien?productid_idens@vall Referrer Policy: no-referrer-when-downgrade						
Iame       × Headers       Preview       Response       Cookies       Timing         ] app.js?v=1.2.12       v General         ] chunk-vendors.js?v=1.2.12       request       URL: https://ukerodoc.js/vendoc.js/v	R       Elements       Console       Sources       Network       Performance       Memory       Application       Security       Audits         ●       Image: Sources       Network       Performance       Memory       Application       Security       Audits         ●       Image: Sources       Network       Performance       Memory       Application       Security       Audits         Image: Sources       Image: Sources						
Iame     × Headers     Preview     Response     Cookies     Timing       ] app.js?v=1.2.12      General		- v1.2 -					
] app;s?v=1.2.12 vGeneral ] chunk-vendors;s?v=1.2.12 Request URL: https://frontend/itmanager/js/app.j.?v=1.2.12 Request Method: GET	lame	➤ Headers Preview Response Cookies Timing					
<pre>] chunk-vendorsjs?v=1.2.12 Request URL: https://frontend/itmanager/js/app.j?v=1.2.12 Request Method: GET</pre>	app.js?v=1.2.12 v General						
Request Method: GET	chunk-vendors.js?v=1.2.12	s?v=1.2.12 Request URL: https://frontend/itmanager/js/app.js?v=1.2.12					
		Request Method: GET					
Status Code: 🔿 304 Not Modified		Status Code: 🖷 304 Not Modified					
Remote Address: 47.104.68.11:443		Remote Address: 47.104.68.11:443					
Referrer Policy: no-referrer-when-downgrade		Referrer Policy: no-referrer-when-downgrade					

### API operations

- 1. Request URI: /oauth/token
  - Description: You can call this operation to obtain the access token.
  - Request parameters

Parameter	Туре	Required	Example	Description
code	String	Yes	vuQ3n6	The value of the code parameter in the callback after a successful logon.
client_id	String	Yes	oauth2 client_id	OAuth2 client_id
client_secret	String	Yes	oauth2 client_secret	OAuth2 client_secret
redirect_uri	String	Yes	http://example. com	The redirect URL

• Response parameters

Parameter	Туре	Example	Description
access_token	String	333ab704-abc0-48b3- 8af0-496eedd15383	The access token returned.
token_type	String	bearer	The type of the access token.
expires_in	String	7199	The expiration time of the access token.
scope	String	read	The granted permissions.

#### • Error codes

HTTP status code	Error code	Error message	Description
400	invalid_grant	Invalid authorization code: "code".	The error message returned because the value of the code parameter is invalid.
400	invalid_grant	Redirect URI mismatch.	The error message returned because the value of Redirect URI is invalid.
401	Unauthorized	Unauthorized	The error message returned because your access is not authorized.
403	Forbidden	Forbidden	The error message returned because your access was denied.
404	ResourceNotFound	ResourceNotFound	The error message returned when the specified resource does not exist.
415	Unsupport ed MediaT y pe	UnsupportedMediaTy pe	The error message returned because the media type is not supported.
500	InternalError	The request processing has failed due to some unknown error, exception or failure.	The error message returned because an internal error has occurred.

2. Request URI: /api/bff/v1.2/oauth2/userinfo

- Description: You can call this operation to obtain user details.
- Request parameters

Parameter	Туре	Required	Example	Description
access_token	String	Yes	333ab704-abc0- 48b3-8af0- 496eedd15383	The access token.

• Response parameters

#### Sample responses

```
{
"success": true,
"code": "200",
"message": null,
"requestId": "59C5766B-C7F9-4DF6-B5E4-0F2A89942749",
"data": {
    "sub": "4982789226325725762",
    "ou_id": "5920417439492153461",
    "nickname": "admin",
    "phone_number": null,
    "ou_name": "PG China",
    "email": "sz@xxxx.com",
    "username": "admin_wli"
  }
}
```

#### Parameters for running the Spark Structured Streaming program

Parameter	Туре	Example	Description
sub	String	498278922632572576 2	The external ID of the account.
username	String	admin_wli	The username of the account.
nickname	String	admin	The nickname of the account.
email	String	sz@xxxx.com	The email address of the account.
phone_number	String	null	The phone number of the account.
ou_name	String	PG China	The name of the organization to which the account belongs.

Parameter	Туре	Example	Description
ou_id	String	592041743949215346 1	The external ID of the organization to which the account belongs.

#### • Error codes

HTTP status code	Error code	Error message	Description
401	Unauthorized	Unauthorized	The error message returned because your access is not authorized.
403	Forbidden	Forbidden	The error message returned because your access was denied.
404	ResourceNotFound	ResourceNotFound	The error message returned when the specified resource does not exist.
415	Unsupport ed MediaT y pe	UnsupportedMediaTy pe	The error message returned because the media type is not supported.
500	InternalError	The request processing has failed due to some unknown error, exception or failure.	The error message returned because an internal error has occurred.

## 2.3. Form Autofill Template User Manual

This topic describes how to use Form Autofill to implement single sign on for an application.

## Background

A company uses Application A as its website with high visits. The traditional access method is simple but poses security risks.

- Application A is frequently used in daily office work and repeated logons are time-consuming.
- There are security risks in Application A because verification codes are not used for logon authentication.

#### Solution

The Form Autofill application in IDaaS can be used to implement single sign-on and authentication for Application A.

> Document Version: 20220322

#### 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 Application. Find the Form Autofill application and click Add Application in the Actions column.

Overview	Add Application										
Quick Start	AB Standard Protocols Custom Templates										
Applications ^											
Application List Add Applications	Add Ap This pay Applicat	Add Applications This page contains the application templates provided by DasS. The administrator can add applications to DasS based on these templates. Applications the divided into two types. One type supports tendent protocols that you can use to implement SSO, such as JNT. CAS, and SAML. The other is customized and provides APIs for SSO or user provisioning.									
Users ^ Organizations and Groups	Search by applicat	Eesch by application name Q									
Class Management	Application Log o	Application Name	Tag	Description	Application Type	Actions					
Authentication ^	F	表单代填	SSO, AES256	思举代读可以推知用户在登录页输入用户名标签码,再通过思举编变的一种登录方式。应用的原母委码在 DasS 中使用 AES266 加密期述本地加密护编,很多旧系统,不交转后来认证的 议的系统成不交换改造的系统可以使用思举代做实现他一身份管理,思举中有限计验证码,CSRF token,能参考数的场展不适用,	Web Application	Add Applicati on					
RADIUS	No.	4J4J	钉钉固步	们打是由阿里巴巴出品,为中国政企量身打造的免费问题的作平台,们打同步应用是用来进行 (Dass 与针打之间间步的剩体,实现从 (Dass 同步数据我们打的资程。	Data Provisioning	Add Applicati on					
Authorization ^	M	阿里邮箱	SSO, 用户同步, SAM L, 阿里云, 診輔	基于 SAML协议,实现由 IDaaS 到阿盟加權的尊占提录和用户用户。	Web Application	Add Applicati on					
Policy Servers											

3. In the Add Application dialog box that appears, configure the following parameters:

	FORM	
	© Upload File	
	The image size must be less than 1 MB.	
* Application Name	Autofill	
* Application Type	Veb Application	
	If you select Web Application or PC Client, the application is displayed in Web browsers. If you select Mobile Application, the application in mobile applications. If you select Data Provisioning, the application is used for data provisioning only and not visible to users. To display ation in multiple environments, select multiple check boxes.	is displayed ay the applic
Logon URL	http://	Mobile
	The URL of the AES256 logon page. It must start with http:// or https://. For example, https://oa.xxxx.com/login. Select the Mobile check e logon pages.	box for mobil
* Form Submit URL	http://	
	The URL of the AES256 logon page after form submit. It must start with http:// or https://. For example, https://oa.xxxx.com/login.	
<ul> <li>Username Name Attribute</li> </ul>	usemameField	
	The name attribute of the username field.	
* Password Name	passwordField	
/ ttributo	The name attribute of the password field.	
Logon Button	submitField	
Humo / tenouto	The name attribute of the logon button.	
Other Logon Information	Other Logon Information	
	Optional. The other information that is needed in the logon form. For example, <input name="spt" type="hidden" value="123"/>	
Logon Success Page	IoginSuccessPage	//
	Logon Success Page	

\* Request Method 💿 POST 🕓 GET

- Form Submit URL: the logon URL of Application A.
- Username Name Attribute: the username for the logon URL.
- Password Name Attribute: the password for the logon URL.

- Request Method: the request method for the logon URL.
- Account Linking Method: Select Account and Password.
- 4. Enable and authorize the application.

Application L o	og Application Name	Application ID	Device Type	Application	Status Actions		
FORM	Autofili idaas-cn-0pp1mb0e705aes256		Web Application		Authorize Details 🔺		
Applicat	ion Information	Authentication Information	Account Information - Provisioning		Account Information - Account Linking		
Details o	f the application	Single sign-on (SSO) URLs.	Modify SCIM settings and provision OUs and groups to th on.	ne applicati	Application accounts that are linked with IDaaS accounts.		
View De	tails Modify Application Delete Application	IDaaS-Initiated SSO URL	Provision OUs Configure SCIM		View Application Accounts		
Authoriz	ation Information	Audit Information	API				
Groups a	and accounts that are authorized to manage the applicatio	View detailed operation logs about the application.	Whether to apply open system API				
Authoriz	9	View Logs View Provisioning Records	API Key API Secret				
Applica	ation Authorization						
Authoriz	e OUs or Groups by Application Grant Applic	cation Access by OU or Group Grant Application Acce	ess by Account Authorize Accounts by Applica	ation Aut	horize Application by Class		
Ŵ	Application Authorization This page provides the administrator with multiple	le ways to authorize application access.					
	For example, the administrator can select an ap	plication and authorize multiple OUs and groups to access	the application. Alternatively, they can select an ac	count and gra	nt the account access to multiple applications.		
Applic	Applications (1) OUs and Groups (787) Authorized: 0						
Autofi	1	Q 🔚 : OU 🕌 : Group					
Auto	tuli	> Search by group name					
	Total 1 item	< 1 > Alibaba Cloud					
		abc					

5. Bind the application account to the user account. The user account is the account used to access the IDaaS console, and the application account is the account for Application A.

Application List			Add Application
Application List This page allows the administrator to manage applications. Cnce as Atter an application is added to IDaaS, make sure to enable the app Search by application nume Application Log Application Log	ded to IDaaS, applications support single sign-on and user provisioning. Ication and authorce application access to users. The page also provides d Q Application ID	Setailed information about applications, including SSO URLs, application accound	× nts, user provisioning settings, authorization settings, and audit logs. on Status Actions
Autofil	idaas-cn-0pp1mb0e705aes256	Web Application	Authorize Details 🔺
Application Information Details of the application Vew Details Modify Application Delete Application	Authentication Information Single sign-on (SSC) URLs. IDeaS-imbated SSC URL	Account Information - Provisioning Modely SCM settings and provision OUs and groups to the application on operation OUs Configure SCM	Account Information - Account Linking Application accounts that are linked with (DasB accounts. View Application Accounts
Authorization Information	Audit Information	АРІ	
Orcups and accounts that are authorized to manage the applicatio n. Authorize	View detailed operation logs about the application. View Logs View Provisioning Records	Whether to apply open system API	

Application List / Application	on Accounts								
← Application Acc	ounts					U.	ink Accounts	Batch Import	Batch Export
Application Account Sub account refers to for example: there is a d: when the applicatio	s the identity of the user in the specifie main account Zhang San (user nam in is created, if account mapping is se	d application system. Master account refer e Zhangsan) in IDaaS. In the enterprise Bi lected, the default primary account and su	s to the account in idaas. During single sign PM application system, the user name of th b account are completely the same, without	i on, idaas will tr is user is agoodi configuration. If	ansfer the corresponding sub account to the application s man, that is, the sub account should be agoodman, which account association is selected, manual sub account crea	ystem, which needs to exis is associated with the mai ation and primary sub acco	st and be recognizable in account Zhangsan. sunt association need !	in the application < br / > account a to be performed h	× i system. issociation metho lere.
Autofill									
Search by IDaaS account nam	ne		٩						
IDaaS Account	Display Name	Application Account	Application Account Password	Linked	Approval Status	Linked At		Action	15
			No	Data					
							Total 0 item <	1	Goto 1

6. Log on to IDaaS as the common user authorized to access the application and click the icon to log on to Application A in a single sign-on manner.

IDaaS					Messages 1	demoUser2
IDaaS	My Applications					
Menu ^	Web Applications					
My Applications	Heb Applications					
All Applications		46		46		100
Application Accounts	<b>C D</b>		57		F	1
Settings ^		JWT		JWT	FORM	
My Account	RAM - Role-based SSO	JWT1	RAM - User-based SSO	JWT	Autofill	
Two-factor Authentication	Account not Added	Account not Added	Account not Added	Account not Added		
Messages						
Logs	Mobile Applications					
	No mobile application available.					

If all the preceding steps are successful, you have logged on to Application A in a single sign-on manner.