



应用身份服务 身份管理服务公共云合集

文档版本: 20220707



法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。 如果您阅读或使用本文档,您的阅读或使用行为将被视为对本声明全部内容的认可。

- 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档,且仅能用 于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息,您应当严格 遵守保密义务;未经阿里云事先书面同意,您不得向任何第三方披露本手册内容或 提供给任何第三方使用。
- 未经阿里云事先书面许可,任何单位、公司或个人不得擅自摘抄、翻译、复制本文 档内容的部分或全部,不得以任何方式或途径进行传播和宣传。
- 由于产品版本升级、调整或其他原因,本文档内容有可能变更。阿里云保留在没有 任何通知或者提示下对本文档的内容进行修改的权利,并在阿里云授权通道中不时 发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠 道下载、获取最新版的用户文档。
- 4. 本文档仅作为用户使用阿里云产品及服务的参考性指引,阿里云以产品及服务的"现状"、"有缺陷"和"当前功能"的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引,但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的,阿里云不承担任何法律责任。在任何情况下,阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害,包括用户使用或信赖本文档而遭受的利润损失,承担责任(即使阿里云已被告知该等损失的可能性)。
- 5. 阿里云网站上所有内容,包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计,均由阿里云和/或其关联公司依法拥有其知识产权,包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意,任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外,未经阿里云事先书面同意,任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称(包括但不限于单独为或以组合形式包含"阿里云"、"Aliyun"、"万网"等阿里云和/或其关联公司品牌,上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司)。
- 6. 如若发现本文档存在任何错误,请与阿里云取得直接联系。

通用约定

格式	说明	样例
⚠ 危险	该类警示信息将导致系统重大变更甚至故 障,或者导致人身伤害等结果。	⚠ 危险 重置操作将丢失用户配置数据。
▲ 警告	该类警示信息可能会导致系统重大变更甚 至故障,或者导致人身伤害等结果。	
〔〕) 注意	用于警示信息、补充说明等,是用户必须 了解的内容。	大意 权重设置为0,该服务器不会再接受新 请求。
? 说明	用于补充说明、最佳实践、窍门等 <i>,</i> 不是 用户必须了解的内容。	⑦ 说明 您也可以通过按Ctrl+A选中全部文 件。
>	多级菜单递进。	单击设置> 网络> 设置网络类型。
粗体	表示按键、菜单、页面名称等UI元素。	在 结果确认 页面 <i>,</i> 单击 确定 。
Courier字体	命令或代码。	执行 cd /d C:/window 命令,进入 Windows系统文件夹。
斜体	表示参数、变量。	bae log listinstanceid
[] 或者 [alb]	表示可选项,至多选择一个。	ipconfig [-all -t]
{} 或者 {a b}	表示必选项,至多选择一个。	switch {active stand}

目录

1.EIAM 云身份服务	09
1.1. 产品简介	09
1.1.1. 什么是 IDaaS?	09
1.1.2. IDaaS 术语表	09
1.1.3. 应用场景	12
1.1.4. 产品计费	13
1.1.5. 1.x 旧版实例变更方案	13
1.1.6. 新旧版本功能对比	14
1.2. 产品特色	17
1.2.1. IDaaS "默认安全"设计	17
1.2.2. IDaaS "开发友好"设计	18
1.3. 快速上手	20
1.3.1. 1. 免费开通实例	20
1.3.2. 2. 创建账户	21
1.3.3. 3. 创建应用	22
1.3.4. 4. 首次单点登录!	24
1.4. 管理进阶	25
1.4.1. 身份提供方	25
1.4.1.1. 绑定钉钉-入方向	25
1.4.1.2. 绑定钉钉-出方向	32
1.4.1.3. 其他身份提供方	35
1.4.1.4. 字段映射	35
1.4.2. 账户	37
1.4.2.1. 创建账户/组织	37
1.4.2.2. 账户详情	37
1.4.2.3. 账户生命周期	38

1.4.2.4. 组织管理	39
1.4.2.5. 账户/组织同步	40
1.4.3. 开通应用	41
1.4.3.1. 应用开通说明	41
1.4.3.2. 1. 应用市场	42
1.4.3.3. 2. 标准协议	43
1.4.3.4.3. 自研应用	44
1.4.4. 应用管理	44
1.4.4.1. 基本配置	44
1.4.4.2. 单点登录通用说明	45
1.4.4.3. SAML 2.0 SSO 配置	46
1.4.4.3.1. SAML 2.0 SSO 配置	46
1.4.4.3.2. SAML 应用账户配置	48
1.4.4.3.3. SAML Attribute Statements 值填写规范	49
1.4.4.4. OIDC SSO 配置	49
1.4.4.4.1. OIDC SSO 配置	49
1.4.4.4.2. OIDC id_token 扩展值填写规范	51
1.4.4.5. 自研应用 SSO 配置	51
1.4.4.6. 高级:账户字段表达式	53
1.4.4.7. 应用授权	55
1.4.4.8. 账户同步 - IDaaS 同步到应用	55
1.4.4.9. 账户同步 - 应用同步给 IDaaS	57
1.4.4.10. 应用 API 开放	57
1.4.5. 登录	58
1.4.5.1. 登录方式	58
1.4.5.2. 二次认证	59
1.4.5.3. 密码策略	61
1.4.6. 日志	63

1.4.6.1. 管理/用户日志	63
1.4.6.2. 同步日志	63
1.4.7. 企业个性化	64
1.4.7.1. 企业信息	65
1.4.7.2. 短信/邮件内容	65
1.5. 用户指南	65
1.5.1. 通用登录页	65
1.5.2. 钉钉扫码登录	67
1.5.3. 门户页	68
1.5.4. 钉钉工作台访问门户	69
1.5.5. 用户自服务	71
1.5.6. OIDC Device Flow 设备模式登录流程	72
1.6. 开发指南	73
1.6.1. 接入单点登录	73
1.6.1.1. 自研应用接入 SSO	73
1.6.1.2. Java SpringBoot 自研应用接入 SSO 示例	78
1.6.2. 接入账户同步	80
1.6.2.1. 账户同步接入概述	80
1.6.2.2. 通讯录事件	84
1.6.2.3. Java 应用接入账户同步示例	90
1.6.3. 应用开发 API 对接	93
1.6.3.1. 应用开发 API 说明	93
1.6.3.2. 应用开发 API 列表	94
1.6.4. 开源代码参考	105
1.7. 其他	106
1.7.1. 常规资源限额	106
1.7.2. 常用应用配置	107
1.7.2.1. 阿里云用户 SSO	107

1.7.2.2. 阿里云角色 SSO	109
1.7.2.3. 腾讯云用户 SSO	112
1.7.2.4. 腾讯云角色 SSO	114
1.7.2.5. 华为云 SSO	117
1.7.2.6. 百度智能云用户 SSO	120
1.7.2.7. 百度智能云角色 SSO	123
1.7.2.8. 金山云角色 SSO	126
1.7.2.9. Salesforce SSO	129
1.7.2.10. JumpServer SSO	132
1.7.2.11. JIRA/Confluence SSO	136
1.7.2.12. Jenkins SSO	138
1.7.2.13. Splunk SSO	141
1.7.2.14. SonarQube SSO	144
1.7.2.15. 简道云 SSO	146
1.7.2.16. Salesforce SSO	150
1.7.2.17. Teambition SSO	152
1.7.2.18. WordPress miniOrange SAML	156
1.7.2.19. Bitbucket miniOrange SAML	161
1.7.2.20. Zabbix SSO	171
1.7.2.21. GitLab SSO By SAML	174
1.7.2.22. Redash SSO	177
1.7.2.23. Argo CD SSO	180
2.咨询反馈	184
3.IDaaS 旧版文档	185
3.1. 常见问题	185
3.2. 权限系统	185
3.2.1. 权限系统介绍	185
3.2.2. 最佳实践	187

3.2.2.1. 第三方业务系统接入权限系统	187
3.2.3. 自建权限系统	
3.2.3.1. 自建权限系统	189 190
3.2.3.2. 新增系统及系统详情	191
3.2.3.3. 资源管理	192
3.2.3.4. 角色管理	199
3.2.3.5. 授权管理	204
3.2.4. 权限系统API接口清单	213
3.2.5. 权限系统相关FAQ	235

1.EIAM 云身份服务

1.1. 产品简介

1.1.1. 什么是 IDaaS?

云身份服务 IDaaS(英文名:Alibaba Cloud IDentity as a Service,简称 IDaaS)是阿里云为企业用户提供的云原生的、经济的、便捷的、标准的身份、权限管理体系。

您可以使用 IDaaS,统一管理各应用中分散的账号,并集中分配应用访问控制权限,极大降低低效、重复的账号访问配置和运维消耗,解放生产力。

- <u>低门槛</u>:上手容易、免费开通、预算经济
- <u>云原生</u>:标准、安全、稳定
- 更开放:面向开发者、云产品深度集成、场景模板快速积累

欢迎 免费开通试用 使用。

核心能力

对管理者而言,IDaaS 提供一站式组织架构、账户全生命周期管理、应用接入实现单点登录(SSO),并控制账号所具备的权限等能力。

对用户而言,IDaaS 提供应用访问门户、独立登录体系、账号自服务能力。

⑦ 说明 您只需花费 10 分钟即可体验 IDaaS 核心能力,请参考 免费开通实例。

同时,IDaaS 允许应用和企业既有通讯录与 IDaaS 的账号体系打通。您可以将 IDaaS 当做企业账号管理系统来使用,也可仅将 IDaaS 当做不同账号体系之间的桥接。



CIAM 和 安全认证

除了上述企业管理场景外,IDaaS 同样支持 CIAM 和安全认证两款产品。

<u>CIAM 用户身份权限管理</u>(Customer Identity Access Management)是阿里云 IDaaS 为大型政企机构提供的、针对 C 端用户管理的产品,帮助政企打通信息系统内公民/ 会员身份孤岛,紧贴业务地提供身份中心。支持公共云和私有化部署。请参考文档: 什么是 IDaaS CIAM? 。

安全认证 是阿里云 IDaaS 提供的独立产品,针对当下认证安全隐患很普遍、认证集成方式割裂的现况,提供的一站式开发者工具,一套 SDK 实现号码认证、WebAuthn 生 物识别认证、短信登录、OTP 动态口令认证、IFAA 认证等无密码认证方式,方便安全。请参考文档:<mark>安全认证整体介绍。</mark>

1.1.2. IDaaS 术语表

产品相关

IDaaS

ldentity-as-a-Service,身份即服务,企业云身份管理中心,阿里云提供的云身份服务。

EIAM

Enterprise Identity Access Management,企业员工身份管理系统、传统意义上的统一身份认证平台、IAM 系统、4A 平台。面向企业内部 ToE 员工、实习生、临时工与 ToB 合作伙伴、供应商、门店职工的身份管理。阿里云提供的云身份服务。

CIAM

Customer Identity Access Management, 企业外部用户身份管理系统, 面向消费者、会员、公民市民等外部身份。阿里云提供的云身份服务。

身份管理服务公共云合集·EIAM 云身份 服务

国际化

指产品使用、界面、图片、文档、运营、支持的多语言化。IDaaS 目前支持中、英两种语言。

安全认证

安全认证。阿里云提供的身份认证服务,提供号码认证、IIFAA、WebAuthn、短信认证、OTP 等一揽子无密码登录方式,对接一套 SDK 即全部可用。

零信任

零信任是一套新兴网络架构,国内外普遍采用。零信任架构打破了原有的可信网络环境边界,要求所有服务访问均需要可信身份、合理授权,有效提高了整体网络架构安全 性和使用便捷性,在远程办公、多云架构、BYOD 等现代办公条件中应用。

公共云/私有化

公共云 IDaaS 是阿里云 IDaaS 提供的即开即用、灵活定价的云服务。管理员使用阿里云账户,即可立刻开通。 私有化 IDaaS 指代将 IDaaS 部署到您指定的环境中,无论部署在您的阿里云 VPC、AWS、还是线下机房等,均属与私有化范畴。

身份提供方

IdP

ldentity Provider, 身份提供方,即 IDaaS。源自于 SAML 协议中定义, IdP 为进行用户认证、鉴权,并返回 SAML Response 结果信息给 SP 的身份提供方,后通用化指统一 身份管理平台。在当前场景中, IDaaS 即是 IdP。

SP

Service Provider,服务提供方,即应用。源自于 SAML协议中定义,SP 为接收 IdP 返回结果的解析方,后通用化指接入 IdP 的应用。

AD 活动目录

微软 Active Directory,微软用于企业办公场景中,对组织、账户、权限进行管理的组件,可单独部署。由于其极广的适用性,很多现代应用也支持 AD 作为其账号体系。由 于 AD 普遍存在的体验和兼容性问题,通常企业会寻找其他身份方案,比如 IDaaS。

LDAP

Lightweight Directory Access Protocol,轻量级目录访问协议,最常用于和 AD、OpenLDAP 企业目录进行交互,但同样采用与 Apache Directory 等其他系统。

OpenLDAP

广泛使用的,基于 LDAP 协议的开源身份目录。

ADFS

Active Directory Federation Service, AD 联邦服务, Windows Server 的一个默认组件,用于加强传统 AD 在链接外部应用时不够灵活的弊端,使用麻烦、需要维护。

钉钉通讯录

IDaaS 增强钉钉通讯录的能力,实现钉钉通讯录到其他企业账号体系之间身份同步、身份提供等场景。

账户

组织架构

企业以部门为单位的树形结构。

组织

亦称组织机构、Organizational Unit、OU、部门等,企业树形组织架构中的节点,一般对应企业部门。

根组织节点

每个 IDaaS 实例只有一个根节点,对应企业本身,在 IDaaS 中可以修改根节点名称。

账户

每个用户理论上应有且只有一个 IDaaS 账户。账户可登录 IDaaS 应用门户,接入应用 SSO 后,亦可已授权登录应用。

账户生命周期管理

账户从创建(入职)到终止(离职)的全生命周期管理流程,包含禁用、锁定、移动、编辑等操作。

组

组是账户的集合,用于统一进行权限分配,设定同步范围。

同步

在 IDaaS 场景中,同步普遍指代账户、组织在不同系统之间的传递。同步可分为增量、全量,可分为即时、定时,还可按照出方向(从 IDaaS 同步到外部系统)、入方向 (外部系统同步到 IDaaS)划分。

SCIM

System for Cross-domain Identity Management,跨域身份管理系统,专用于不同系统之间账户、组织同步的国际通用规范,国内外有大量应用支持接收 SCIM 协议同步请 求,以实现不同系统身份的互用性 Interoperability。

应用

单点登录(SSO)

Single Sign-On。指用户仅需一次登录,即可访问全部应用的实现,在历史中根据应用变化,SSO 也有多种实现形态。在 IDaaS 的语境中,我们只把基于 SAML、OIDC 等标 准协议的身份联邦机制,称为单点登录。

IdP 发起的单点登录

ldP-init SSO。用户先访问到 IDaaS 应用门户,已处于登录状态后,然后访问应用触发的单点登录。在此流程中,请求由 IDaaS(ldP)发起。

SP 发起的单点登录

SP-init SSO。用户访问到应用,由应用判断是否要进行登录。如果需要登录,应跳转到 IDaaS(IdP)完成认证后,回跳到应用中。在此流程中,请求由 应用(SP)发起。

应用账户

Application User,指在单点登录时,已登录 IDaaS 账户在目标应用中所扮演的身份。举例:zhangsan(IDaaS 账户)在"运营平台"应用中是 admin(应用账户)。IDaaS 支持多种应用账户与 IDaaS 账户的关联方式。在同一个应用中,当同时可扮演多个身份时,用户需要选择一个身份进行访问。

签名/验签

基于非对称性加密算法,衍生出的常见使用。举例: IDaaS 在 OIDC SSO 时,对签发的 __id_token 使用 RSA-256 算法私钥签名,应用使用公钥验签,确保令牌未经伪造、 篡改。

加密/解密

基于对称或非对称加密算法实现。举例:IDaaS 应用进行同步时,IDaaS 支持将同步内容使用 AES-256 加密后传输。应用使用对称密钥,将内容解密后,才能获取到其中内 容,确保在不安全网络环境中内容私密性、准确性。

授权

主体(组织、账户)与客体(应用或其他资源)之间的权限分配。IDaaS 中可以统一分配所有接入应用的访问权限,实现企业统一权限管理。在 IDaaS 中,授权特定组织到 应用后,组织内账户才拥有访问应用的权限。

SAML

Security Assertion Markup Language 安全断言标记语言,基于 XML,全球使用广泛的单点登录协议,相较 OIDC 而言较为复杂。IDaaS 支持 SAML 2.0。

OIDC

OpenID Connect。OIDC 协议于 2014 年发布,结合了 OpenID 认证协议和 OAuth 2.0 授权协议的优势,是全球通用的现代身份联邦协议,用于实现 SSO、鉴权、委托认证等 场景。

JWT

JWT Json Web Token(RFC7519) 狭义上是一种基于 Json 的信息传输格式。由于传输的内容支持签名和加密,在中国 IAM 语境中,JWT 又经常代表一种简化的、部分基于 OIDC 隐式流的单点登录实现方式。

CAS

Central Authentication Service。全球通用的单点登录协议,支持 B/S 网页应用。

OAuth 2.0

授权协议,虽不是为了 SSO 设计,但也经常用于实现 SSO。由于 OIDC 协议基于 OAuth 2.0 协议实现,两者很多支持的模式是互通的。

access_token/id_token/refresh_token

access_token 是授权令牌,用于调用 ldP 提供的接口。

id_token 是身份令牌,可通过解析 id_token 内容,获取当前已登录账户信息。

refresh_token 是刷新令牌,在 access_token 令牌过期后,可以使用 refresh_token 获取新令牌。

OIDC/OAuth 客户端模式/客户端流

Client Credentials 模式,被授权方不是用户/账户,而是应用服务,用于应用获取调用对应资源/接口的权限。IDaaS 提供 client_id, client_secret 给应用,应用可借其换取 access_token,调用 IDaaS 指定接口。

OAuth 授权码模式/授权码流

Authorization Code 模式,被授权方是用户,应用通过授权码模式,可获取三方系统身份信息,并以该身份进行登录。常见的钉钉登录、微信登录等均采用授权码模式。

OAuth 设备模式/设备流

Device Flow,用于特定硬件设备中,在设备/终端不支持展示 IDaaS 登录页面时,允许用户在 PC/手机浏览器中访问 IDaaS 登录页,完成登录后,身份将传递到设备/终端, 完成登录。

登录

密码复杂度

企业下属账户的密码必须达到的复杂度要求。

懒加载

Lazy Loading、Just-in-time Provisioning,当用户登录时,若 IDaaS 中未找到身份信息,自动转发向企业原有身份体系发起认证请求,当认证通过,该账户信息在 IDaaS 中 保存。通常用于密码在原有系统中无法导入 IDaaS,只能使用懒加载逐步导入的场景。

二次认证 (MFA/2FA)

Multi-Factor Authentication 多因素认证、Two-Factor Authentication 双因素/二次认证,指在登录时需要提供多种身份认证因子,交叉确认访问者身份。由于密码天然的 安全弱点,通常用于加强账号+密码登录方式。IDaaS 中支持对账密认证开启短信、邮件或动态令牌(OTP)二次认证。

ОТР

One Time Password 动态口令,一次有效的验证码机制。最常用的 OTP 为 TOTP(Time-based One-Time Password),通常 30s 一变,服务端和客户端(APP)需提前对 齐种子、提前校对时间。在同一时间窗口内,客户端(APP)计算的动态口令(OTP)应与服务端一致,从而通过认证。

应用门户

IDaaS 提供的企业访问门户页,可在此页面发起到所有应用的单点登录。可收费进行定制。

1.1.3. 应用场景

IDaaS 可以打破身份孤岛,将不同部门、不同组织内的全生命周期应用账户管理起来,实现统一访问控制,允许企业成员使用一个账号畅游所有应用。

如下举例 3 个常见使用场景。欢迎 免费开通试用。

核心场景一、研发团队账户管理

当企业中研发、运维、IT 等团队人数达到数十人至数百人时,由于使用应用数量多,在应用的账户、密码管理上会出现瓶颈。

近些年账户权限导致的问题层出不穷,为了确保企业资产安全,往往只有团队管理者可对各系统账户进行管理。当应用较多时,针对各应用账户的改密、解锁、权限分配 等,日常会消耗掉管理人员可观的宝贵精力。

对追求精益求精的团队来讲,此类管理操作低效、重复、价值低,账户分散管理风险大、不可控。人工管理难以接受。

IDaaS 可以将研发、运维工作相关的应用尽数打通,实现一套账户登录、统一授权管理。安全价值高,配置简化,效率高。 常见的文档、任务管理、代码管理、接口管理、资源运维、日志告警、沟通交流等工作,全部可由 IDaaS 统一实现 SSO。**每个应用配置短至 5 分钟,即可开始使用。**

核心场景二、业务应用账户管理

IDaaS 支持员工、临时工、实习生、合作伙伴、生态公司等各类账户的统一管理,并统筹账户到业务、财务、HRSaaS、等各类企业应用的访问权限。

同时,企业可以将各类自研应用接入 IDaaS 统一进行访问控制。



核心场景三、企业账户连接器

若您正在使用 AD、钉钉、企业微信等企业账户,会发现系统和系统间、系统和应用间的账户难以打通。部分应用有自己的规范,无法按照 AD、钉钉的同步接口要求进行调整,导致账户变更需要在多点重复操作,容易导致错配、漏配问题,且消耗时间精力,是低价值重复劳动。

IDaa5 能作为桥梁,将不同体系中的身份贯通在一起,可以即时将钉钉、AD 的变更同步给所有企业身份源,或将其他应用中的变更同步给钉钉、AD。

每个身份源都会有字段映射、字段缺失、失败处理、时间策略等难题,IDaaS 通过极其简单的配置,提供强大的、整套的身份连接和转化能力,帮助企业弥合身份间的孤岛。



1.1.4. 产品计费

```
知阶段不计费。
记aaS 预期22年6月完成商业化,部分现暂时免费的功能,届时需升级到【企业版】,才可继续使用。
DaaS 2.0 会提供如下版本:
• 免费版。DaaS 提供大量免费能力,无用户数限制,可免费实现大量身份场景。
• 企业版。按用户数预付费。使用 IDaaS 当做企业的云身份管理中心时采用。预算管理方便。
免费版
IDaaS 不限制账户数,您尽可以把全量账户导入进来,IDaaS 不会对此收费。
部分常见应用在 IDaaS 中可免费使用。欢迎前往 IDaaS 控制台 中查看。若您还未有 IDaaS 实例,欢迎 免费开通。
企业版 包年包月 - 按用户数预付费
按用户数预付费是最常见的计费方式,便于理解和计算。
账户数一定的情况下,所有功能全部开放。预付费普适于需要准确预算规划的企业。
使用 IDaaS 作为企业身份管理中心的客户,普遍应采用企业版。
暂未上线,预期于7月底前开始计费。
```

1.1.5.1.x 旧版实例变更方案

感谢各位客户对阿里云 IDaaS 的认可和支持!

为了提供更优秀的服务,我们进行了一系列重大优化,包括技术架构、产品定位、计费体系等多方面,旨在能为您长期提供云原生的、经济的、标准的服务,由此推出 IDaaS 新版本。

由于更新内容非常丰富<u>,</u>新版本是不兼容更新<u>,旧有 1.x 版本无法自动升级至新版。部分不常用功能不在新版支持,且不支持自动迁移工具。</u>

我们提供 新旧版本功能对比,并邀请您 免费开通新版,亲自体验对比版本差异。请参照如下内容,自由判断接下来最适合的处理方案。我们会积极提供对应支持。

新客户请使用新版,更易用、更灵活、更经济。

周期规划

新旧版本交替重要时间点规划如下:

时间点

事件

22年02月	 2.0 新版公测上线,新购入口切换为新版。 旧版本新购入口关闭。 旧版本不再更新功能,但仍可以使用(既有旧版客户可新购、升级、续费等,参考下方处理方案)。
22年03月	2.0 商业化,提供优质稳定的服务,并不断迭代增强。
22 年 06 月	1.x 免费版不再可见,请1.x 免费版客户在 6 月前迁移到新版使用。
23 年 03 月	1.x 标准版续费入口关闭。
23年09月	1.x 标准版停止服务,所有实例不再可用。

既有 1.x 版本客户的变更方案

既有 1.x 免费版客户

22 年 9 月 1 日起, 旧版本免费版实例将不再可见。

新版本具备更多免费能力,请所有旧版本免费版客户尽早迁移至新版本。

既有 1.x 标准版客户

诉求	处理方案
希望换新版本使用	请客户参照 新旧版本功能对比,评估新版本能力是否满足需求。 • 若对新版满意,请直接使用新版。新版本暂时可免费使用。 • 您可提交申请表单(暂未开放)。我们会在新版开始收费前,完成余额迁移的订正工作。 提交表格后,我们会主动联系,讨论迁移策略。
希望新购旧版本(新购)	只针对已有旧实例的客户开放。 在 23 年 3 月前,客户可提交申请表单(暂未开放),由我们进行特殊处理,允许客户购买旧 版本。
希望续费旧版本(续费)	我们建议标准版客户尽早迁移至新版本。 但您在 23 年 3 月前仍可以为旧实例继续续费,但最终到期时间不能晚于服务终止时间(预计 23 年 9 月)。
希望升配旧版本(升配)	既有实例可以继续升配,不受影响。 例如 100 -> 300 用户。
不再希望使用	若经由权衡,新版无法满足使用诉求,不再希望使用 IDaaS,请您提交工单,IDaaS 团队将协 助售后小二,帮助您进行剩余时间折算退款处理。

1.x 标准版会继续提供的服务

支持	我们仍会保障现有服务的可靠安全,SLA 保障不变,且会进行安全补丁修复,重大 BUG 更 新。
不再支持	需求咨询、工单支持、新功能更新等业务咨询、支持、售后诉求。

既有 1.x 专属版客户

既有专属版客户实例不受此次更新影响。您可以持续使用既有专属版实例,没有时间限制。 我们会持续提供专属版实例支持。

从版本的持续更新考虑,我们仍建议您考虑迁移到更经济、更敏捷的新版本中。您可以关注 更新记录,或联系我们一对一沟通。

1.1.6. 新旧版本功能对比

本文档用于提供新旧版本功能差异的粗粒度说明,用于判断新版功能是否满足需求的初步材料。 在 2021 年新版本规划的过程中,我们统计了旧版所有功能的使用频率,取其中高频使用的部分,并综合产品规划方向、开发难度等因素综合考量,划定了当前版本功能。 对于最常用的 20% 功能,进行了大幅功能使用简化、配置丰富化、标准化的工作。对于最不常用的功能,我们对功能进行了削减,少量不常用功能不再支持。 在 2022 年,我们会将夯实基础、丰富场景、提高安全作为 IDaaS 的主要发展目标。 新版会优先提供有如下特点的功能:

- 旧版高频使用的功能
- 对身份安全保障有提升
- 符合产品长期定义方向
- 通用身份基础能力
- 研发支持难度

更多功能正在开发中。

无论表格对照结论如何,我们都建议您免费开通新版实例,并尝试新版的体验和能力。

功能对照表

大模块	功能模块	子模块	1.x 旧版本	2.x 新版本
实例		多免费实例	不支持	支持,最多创建 3 个实例,超出需要申请。
		实例释放	不支持	支持
概览页			支持	暂不支持。 预计 22 年下半年支持。
		积累应用模板	不支持	支持
	应用市场	预集成 SSO 模板	不支持	支持,新版操作极大简化
		一对一配置文档	不支持	支持
		应用列表	支持	支持
		应用生命周期	支持	支持
应用		子账户管理	支持	支持
	应用管理	单点登录配置	支持	支持
		应用授权	支持,在独立授权菜单中支持。	支持,在应用管理中支持。
		应用同步 - 自研接入	支持	支持,接口有重新定义,需对接。
		应用同步 - 预集成模板	支持,例如支持 RAM 子账户同 步。	开发中, 暂无预集成同步模板。
		账户列表	支持	支持
	账户管理	账户生命周期	支持	支持。暂时不支持"离职"操作、 过期设置。
		离职操作	支持	不支持
		实名认证	支持	不支持
		僵尸账号	支持	不支持
账户		单个账户同步	支持	开发中,暂不支持触发单个账户同 步。
		组织树形管理	支持	支持
		组织生命周期管理	支持	支持
	组织架构	组织同步	支持	支持

		账户属于多组织	支持	暂不支持。 预计 22 年上半年支持。
	分类管理	按属性值分配权限	支持	不支持
		登录方式模板	支持	支持
	登录方式/认证源	查看登录方式列表	支持	支持
		登录方式生命周期管理	支持	支持
ЮШ		登录方式列表	 支持列表如下: 钉钉 支付宝 微信 企业微信 LDAP 短信 	支持列表如下: • 短信 • 钉钉 LDAP, 企业微信、微信等认证 源, 预计 22 年上半年支持。
	安全设置	全局二次认证	支持,TOTP 和短信	支持,OTP、邮件和短信。
		登录安全	支持	支持
	密码策略	密码安全	支持	支持
	RADIUS		支持	不支持
	证书管理		支持	不支持
		授权菜单	支持	不支持,应用授权在应用管理中完 成,无独立菜单。
		按应用授权在医政股	支持	支持
将 权	应用授权	按应用授权账户	支持	支持
AT 52	授权时限		暂不支持。预计 22 年下半年支 持。	
		反向授权	支持	不支持
	权限系统	进行三方应用	支持	开发中暂不支持。
审计	用户日志	查看用户日志列表	不支持,过去用户和管理日志混淆	支持
		查看管理日志列表	支持	支持
	同步中心	钉钉通讯录导入	支持	支持,且极大简化了操作
	消息中心		支持	不支持
其他	审批中心		支持	不支持
	开发者角色		支持	不支持
	移动端应用门户		支持	不支持
	管理操作风控	关键操作风控强制验证	不支持	支持

1.2. 产品特色

1.2.1. IDaaS "默认安全"设计

阿里云 IDaaS 是阿里云安全团队设计、实现的身份产品,采用"默认安全"的产品设计。

"<u>默认安全</u>"的设计理念:在"<u>可用性</u>"和"安全性"难以两全的场景中,IDaaS 会优先保障"安全性",在此基础上,尽可能追求"<u>易用性</u>"。虽然不同行业的安全要求 不一,我们无法承诺 IDaaS 的默认配置符合所有行业的标准、更不意味着"绝对安全",但我们追求最大程度上的"<u>开箱即安全</u>"。

安全是生命线,企业身份体系是信息安全的紧要核心,也是外部攻击的主要进攻点。我们会尽可能地,按照高标准,提供安全、可信、可靠的安全身份服务。 举例一:默认开启二次认证

使用密码虽然有难以克服的安全隐患,但由于其方便用、好实现,仍然是大量应用的主要身份验证方式之一。

二次认证是针对密码认证场景的最直接的安全兜底方式。当进行了密码登录后,还需要额外进行一次短信/邮箱验证,才能访问服务。 为了保障企业的账号安全,IDaaS 实例默认开启二次认证,所有账户访问应用,均需要进行二次认证,确认身份无误后,才能放行。

因此,所有接入 IDaaS SSO 的应用,即刻受到 IDaaS 二次认证的安全保障。

■员已开启:	二次认证。
"保障您的! E成身份验	账户安全,请您选择如下认证方式之一,纟 证。
选择短信	验证码
IDaaS将向 脸证码。	您账户的手机号+8 3发送
选择邮箱	脸证码
lDaaS将向 发送验证码	您账户的邮箱 :om 。

高级:智能模式

同时,为了避免多次登录时反复二次认证的麻烦,IDaaS 默认开启【智能模式】。【智能模式】将综合当前设备访问环境和账户状况,判断当前是否需要二次认证。

若您正常办公,可能很多天都无需二次认证,IDaaS 以此保障安全登录的易用性。

举例二:管理控制台操作风控

管理员的操作拥有比用户操作远远更大的权限。一旦管理员账户被盗用,其恶意行为将造成远远更大的负面影响。当子管理员进行一些影响面较大的敏感操作时,也应该由 负责人确认后进行,以此保障局面可控,流程合规。

阿里云 IDaaS 为管理侧关键管理操作,利用阿里云多年沉淀的风控体系,判断当前管理者的账号状态和访问环境。一旦操作风险超过阈值,将会触发风控验证,需要阿里云 账号绑定的手机号进行二次认证。

短信验证			×
当前绑定手	机号: 1700 100000		
36	设证码: 6位数字	获取短信验证码	
5		确定	取消

IDaaS 在如下操作中预置了风控埋点,覆盖了对访问、对开发、对数据最敏感的一些场景。

- 删除实例
- 批量删除账户
- 删除应用
- 密钥轮转
- … 等十余类操作

举例三: 应用默认手动授权

> 文档版本: 20220707

使用 IDaaS 进行企业身份管理,除了 SSO 带来的便捷和安全性,另一大核心价值,是由统一分配权限管理带来的。当所有访问均通过 IDaaS 进行 SSO,就可以非常方便地在 IDaaS 中分配应用访问权限。

阿里云 IDaaS 默认所有应用均需要手动进行授权。

授权范围	手动授权	~
	若选择"手动授权",	需要在 应用授权 中进行权限分配。

新创建出来的应用,在管理员明确其授权范围前,无人可以访问。以最小权限原则,避免应用访问权限的泛滥问题。

举例四: 密码策略安全性

当不得不使用密码登录时,密码的安全策略就派上了用场。

IDaaS 默认支持密码登录,为了保障登录的基本安全性,我们推荐了一系列较为通用的安全配置,作为实例初始化默认配置。

密码长度				
10	密码最少字符数			
复杂度				
🔽 必须包含	大写字母			
🔽 必须包含	必须包含小写字母			
🔽 必须包含	必须包含数字			
🔽 必须包含	🖌 必须包含特殊字符 (! @ # \$ % & * ~)			
🔽 不能包含	用户名			
□ 不能包含	显示名称或其拼音			
□ 不能包含	手机号			
□ 不能包含	邮箱前缀			

我们默认一套相对安全性较高的复杂度配置,以尽可能为身份安全提供高标准、高规范。默认的复杂度为:

- 最少 10 位
- 必须包含大写字母
- 必须包含小写字母
- 必须包含数字
- 必须包含特殊字符
- 不能包含账户名。

您可以对此策略进行调整,以达成业务需求和安全性之间的平衡。

举例五:默认签名、默认加密

在进行跨域请求时,无论是否使用 HTTPS,都无法 100% 真正保障跨域请求在网络传输中的安全性。

为了达到真正端到端的安全防护,IDaaS 在全局采用 HTTPS 的基础上,额外提供了业务层面的"签名层"和"加密层",默认开启。

签名层:在进行跨域请求时,对请求内容使用私钥进行签名,允许接收方使用公钥验证信息,确保信息在传输过程中不被篡改。在部分 SSO 场景、出方向账户同步场景中 使用。

加密层:支持同步信息的端对端加解密,默认加密后同步数据,且默认不同步密码信息,避免疏漏操作导致的信息泄露。未来会支持 SAML SSO 全过程加密,让 SSO 达到 金融级、政务级的高级别安全要求。

是否加密	✓ 业务政场/JIdX 若勾选,业务数据将使用加解密密钥加密后传输。详情参考 接收 IDaaS 同步事件。				
加解密钥	06f7c3d9fe3f6f65b5291c9c8dcbb7d0ff2ff1355d31d4a8c129b9e3f	C 生成密钥			
	AES256加密密钥,Hex编码格式。您可以指定加解密钥,或自动由 IDaaS 生成。				
是否同步密码	□ 同步密码				
	勾选是,则会在特定事件的数据中传递明文密码。 若同时勾选加密,则密码会和业务数据一起加密传输。				

1.2.2. IDaaS "开发友好"设计

虽然有诸多企业身份管理的场景价值可通过简单的配置实现,中大型企业想要完整地使用 IDaaS 的价值,仍往往需要与 IDaaS 进行开发对接,以实现部分系统身份数据的识 别和互通。我们深刻认识到"开发友好"对企业采用现代云身份服务的重要性。

为了方便企业开发者,IDaaS 提供了一系列围绕开发者的功能,以方便对接,降低门槛,真正实现适用于不同企业的普惠服务。

功能一:围绕应用开发组织能力

为了便于管理和理解,开发者对接的全部功能,全部围绕着 IDaaS 中的应用展开。

[→ 登录统一: 单点登录接入

实现单点登录,用户即可使用 IDaaS 账户登录业务应用。访问控制可以在 IDaaS 中通过授权统一管理。 请应用开发人员参照《单点登录通用说明》,即可快速对接。

- 聚户统一: 账户同步接入 实现账户同步, 即可实现账户管理—处传改, 兑处生效, 方便快速, IDaaS 支持出、入两个方向的账号同步, 请应用开发人员参照(IDaaS 同步到应用), 确定方案, 开始集成。
- lDaaS 支持出、入两个方向的账号向步,请应用并发入负参照《lDaaS 同步到应用》,偏定方来,并如果说。
- 权限统一 未来版本 当前版本暂不支持,敬请期待。

面向应用,我们开放如下能力允许开发对接:

场景	核心能力	说明
登录统一	单点登录 SSO	实现应用将登录统一托管给 IDaaS,全企业所有应用统一登录入口、登录体验。
账户统一	账户/组织同步	通过入方向(应用同步到 IDaaS)和出方向(IDaaS 同步到应用)同步配置,实现身份信息的 互联互通、统一管理。
权限统一	权限系统管理	可以直线基于 RBAC 的应用内菜单、按钮、数据等权限在 IDaaS 中统一托管和统一授权。 暂未上线,敬请期待。

分散不好管理,集中易于对接。全部需开发对接功能都在应用管理菜单中陈列,一次性即可配置完成。

云身份服务 / 厄							
← 自研	应用						
通用配置	登录访问	账户同步	API 开放				

功能二:代码开源

IDaaS 提供了一系列针对 SSO 接入、OIDC 设备流对接、账户同步接入等场景的样本代码,以便于开发者下载、查看、复用,详情请查看:开源代码参考。

功能三: SDK 与样例代码

针对不同场景,IDaaS 提供管理说明文档、开发说明文档和 SDK 及样本代码,汇总如下:

场景	管理说明文档	开发说明文档	样本代码
应用接入 SSO	自研应用 SSO 配置	自定应用接入 SSO	应用接入 SSO Java 样本代码 Github 开源 - 自研应用接入示例
IDaaS 同步到应用	账户同步-IDaaS 同步到应用	账户同步接入概述 通讯录事件说明	应用接入同步示例 Github 开源 - 接收事件并同步到 RAM 示例
IDaaS 开放 API	应用 API 开放	应用开发 API 说明 应用开发 API 列表	阿里云 IDaaS API 开发者平台 详情参考下段说明。

特色:开放 API SDK 下载和样例代码

针对 IDaaS 开放的 API, IDaaS 提供尽可能多语言(Java/Python/Go/PHP/C#/C++/TypeScript)的 SDK 下载使用和示例代码。

可以前往 阿里云 IDaaS API开发者平台,在左侧可切换到不同接口,在右侧可选择对应语言【下载完整工程】,参照其中代码实现 SDK 安装、应用和调用。



功能四: API 在线调试

IDaaS 对外开放的 API 均提供在线调试能力,可直接在浏览器中录入参数、动态渲染样本代码、并直接执行查看结果。

在 <mark>阿里云 IDaaS API 开发者平台</mark> 的 【API 调试】菜单中,在中间可填写真实的接口调用参数,调用完成后,可以在右侧【调用结果】标签查看返回参数。若调用创建账户、 修改组织信息等接口,也可以在对应的 IDaaS 实例中查看实际变化效果。



1.3. 快速上手

1.3.1.1.免费开通实例

IDaaS 快速上手教程会引导您创建账户、配置应用、并完成第一次应用单点登录。

IDaaS 2.0 实例开通免费,其中大量功能均可免费使用,部分功能收费(请参考 产品计费)。开通没有审批流程,您可即开即用,畅享 IDaaS 提供的服务。

请访问 阿里云 IDaaS 控制台,来到 EIAM 云身份服务 新版 2.0 实例列表页。

应用身份服务





实例创建会瞬时完成。创建成功后,点击实例 ID 或【访问控制台】,前往 IDaaS 管理控制台。



您已完成实例创建,请前往下一步: 2. 创建账户。

1.3.2.2.创建账户

IDaaS 是企业的云上账号中心,您可以在 IDaaS 中管理企业组织架构和各类企业账号,包括产研、运维、人力、销售等各部门人员、临时员工、外包人员等。

```
IDaaS 中的账户,可以通过统一登录体系,访问到所有其具备权限的企业应用中。
```

☰ (-) 阿里云 ☆	工作台 ◎ 杭州 ~	Q 授索	费用	E IN ICP	备案 企业	支持 Ap	op En (, A ()	84 👩
云身份服务	云身份服务 / 账户						版本更新记录	IDaaS支持群	帮助文档
快速入门	账户								导入
身份提供方	IDaaS 中管理的账户可以通过 https:	//, unidaas.com 登录i	用户门户或 SSO 到应	用.					
80°									
应用	组织结构	账户 组织							
登录 日志	- 阿里云 IDaaS	創建務户 全部状态 >	账P名 〜 请!	ŧλ		Q		包含节点下全部務	r ()
个性化	如元前38.36.2018	□ 账户名	显示名	手机号	邮箱	未源	账户状态	操作	
		□ test 2				白琥	🕑 正常	禁用 编辑	ł
		11.11.11.11.11.11.11.11.11.11.11.11.11.		每页显	8 10 V	共1条数据	< ±-	頁 1 下一	页 >

添加账户

请您来到【账户】菜单,点击页面上【创建账户】按钮,按照表单提示,进行手动账户添加。

身份管理服务公共云合集·EIAM 云身份 服务

63A2/11/			>
• 所属组织			
Q. 阿里云 IDaaS			\sim
·账户名			
请输入账户名			
用于登录和唯一标识的账户名,不可修改。可包含英文字母、数字、。			
• 密码			
请输入密码	0	C 自动生	成
、 长度至少10位,必须包含大写字母、小写字母、数字、特殊字符、不得包含账户名。 置。	可在登	录 - 密码策略	中配
手机			
中国 +86 🏾 请输入手机号			
中国+86 ✓ 请输入手机号 建议填写。可用于登录、找回密码、二次认证等流程。若不填写,可能导致一些流标	呈阻断。		
中国+86 ∨ 衛編入手机号 建议请写。司用于登录、找回密码、二次认证等流程。若不填写,可能导致一些流体 鮮瑞	呈阻断。		
中国+86 ∨ (福祉入手机号 建议酒写,可用于登录、找回密码、二次从证等流程。若不填写,可能导致一些流射 鮮瑞 (福祉入鮮福地址)	呈阻断。		
中国+86 ∨ (建築入手机号 建议调写,可用于登录、找回密码、二次从证等流程。若不填写,可能导致一些流材 邮箱 (建築入邮箱地址 建议调写,可用于登录、找回密码、二次从证等流程。若不填写,可能导致一些流行	呈阻断。		
中田+86 ∨ (猪输入手机号 建议项写,可用于量录,找回图码,二次认证等流程。若不填写,可能导致一些流柱 绑箱 请输入都箱地址 建议填写,可用于量录,找回密码、二次认证等流程。若不填写,可能导致一些流柱 显示者	呈阻断。		

? 说明

除了手动添加外,IDaaS 支持一系列组织和账户的导入方式,请参考:账户/组织同步。

下一步

恭喜您完成了第一个账户的添加!

您已可以通过实例的登录页, 登录到账户的访问门户中。实例登录页地址可在【账户】页面上方查看。 请前往下一步: 3.创建应用。

1.3.3.3.创建应用

应用是 IDaaS 中承载业务应用、系统、服务的载体。通过应用,可实现到应用的单点登录(SSO)以及和 IDaaS 应用之间的账户同步。

本文将以配置【阿里云用户 SSO】应用为例,实现 IDaaS 账户登录到阿里云控制台。

添加应用

请您前往【应用】菜单,点击【添加应用】,来到【应用市场】。

IDaaS 中预集成了一系列常用企业软件应用模板,进行了深度配置优化,可一键添加,配置简单。

⑦ 说明 对于市面上其他应用和自研应用,可以使用【标准协议】和【自研应用】模板进行接入。



【阿里云用户 SSO】应用是市场中的第一个,点击添加应用,确认应用名称后,会自动跳转到配置页。

• 应用名称	阿里云用户SSO	
	应用的显示名称。	

配置单点登录

单点登录(SSO)流程需要 IDaaS 与应用之间进行交互,需要在两端进行简单配置。

⑦ 说明

【阿里云用户 SSO】背后使用 SAML 2.0 协议,SAML 2.0 有十余个常用参数可配置,较为繁琐。而 IDaaS 为您提供了一键式配置方式,配置难度接近于无。

在 IDaaS 中的配置

开通应用后,页面会跳转到单点登录配置页,并将所有参数填充好。

1	四田二田白。こう	

、 r J 工	4/11/	000	
通用配置	登录访问	账户同步 API 开放	
单点登录	应用账户	授权	
单点登录配置	已启用		
不知道怎么配	置? 请参考	封接文档。	
• 阿里云主账号	ID	默认前端获取当前 uid。 望实现 SSO 的目标阿里云主账户 ID。	
• 应用账户	[IDaaS账户名 点登录时,将选中项作为账户标识,传递给业务系统	×
授权范围	[手动授权 选择"手动授权",需要在 <u>应用授权</u> 中进行权限分配	~
隐藏高级配置 🗸			
RAM默认域名		example.onlaiyun.com	
	F	AM 支持修改默认域名。若自定义,需要在此填写,	以作呼应。

请参考字段说明:

字段名	说明
阿里云主账号 ID	配置单点登录到阿里云指定主账号下。
应用账户	设定单点登录时使用的账户标识。 默认使用:I <u>DaaS 账户名</u> 。详细说明请参考:SAML 应用账户配置。
授权范围	设定哪些账户可访问当前应用。 默认使用: <u>手动授权</u> 。详细说明请参考:单点 登录通用说明 。
RAM 默认域名	一般无需填写。当 RAM 中配置了辅助域名时才需填写。

出于快速上手的目的,当前我们建议无需修改,直接点击保存。 在页面下方,有【应用配置信息】章节,请直接在其中【下载 metadata】文件。文件中包含了所有单点登录配置信息,下一步中在 RAM 中上传即可。

在 访问控制 RAM 中的配置

🥐 说明

前提:由于上一步中默认选择使用 IDaaS 账户名作为应用账户,请先确认第 2 步创建的 IDaaS 账户名与 RAM 对应的用户名一致。若没有,请先创建 RAM 用户。若希望 能灵活关联应用账户,请查看 SAML 应用账户配置。

请点击链接前往 RAM SSO 配置页,切换到【用户 SSO】标签,点击编辑。

三〇阿里云	ÂΙ	作台				Q 搜索		费用	工单	ICP
RAM 访问控制 ^{概览}		RAM 访问控制 / SSO SSO 管理	管理							
身份管理 . 用户 用户组 角色	^	 阿里云支持基于 阿里云目前支持 1. 通过角色 S 2. 通过用户 S 	SAML 2.0 的 两种 SSO 型 SO,企业可 SO,企业员	的 SSO(Sing 登录方式: J以在本地 IdP S工在登录后,:	le Sign On,单点登录), 中管理员工信息,无需进行 将以 RAM 用户身份访问阿	也称为身份联合登录。 阿里云和企业 ldP 间的用 里云。	户同步,企业员工将使用:	指定的 RAI	VI 角色来	·登录阿
设置 SSO 管理		角色 SSO 用	户 SSO							
 	~	SSO 登录设置 SSO 功能状态 元数照文档 ス約ML 服务提供方元数II 編助域名	∠ 编辑 据 URL	关印 末」 http	利 上传 ps://signin.aliyun.com/se	ıml/SpMetadata.xml?ter	nantiD=15136823594490)78 🗗		

将 SSO 功能开启,并上传刚才在 IDaaS 配置过程中下载的文件。

IDaaS 单点登录 – 应用配置信息

阿里云 RAM - SSO 管理 - 用户 SSO



点击【确定】后,配置完成。您已经可以使用 IDaaS 账号单点登录【阿里云用户 SSO】应用。

下一步引导您体验单点登录。请前往最后一步: 4. 首次单点登录!。

1.3.4.4.首次单点登录!

您已经完成了上手配置。请体验效果,使用 IDaaS 账户,登录用户门户,并单点登录(SSO)到阿里云控制台。

登录门户

实例的门户访问地址可以在【快速上手】【账户】等菜单查看,亦可在实例列表页中【用户门户】列查看。 请在浏览器打开门户访问地址,来到 IDaaS 登录页。

	中文 🗸
阿里云 IDaaS	
账户名、手机号或邮箱 请输入登录信息	
密码 请输入密码	\odot
登录	
其他登录方式	
••• 使用短信验证码登录	

IDaaS 支持多样登录方式,管理员可以在【登录】菜单中管理。

请您使用教程第 2 步中创建的账号,进行登录,来到 IDaaS 用户门户页。

单点登录!

用户在 IDaaS 门户中,能看到所有管理员配置完成、并为其分配好权限的应用。

点击该应用,即可发起单点登录跳转请求。尝试点击【阿里云用户 SSO】应用,即会在新的标签页中登录到阿里云中。

IDaaS 应用门户 _{阿里云 IDaaS}



恭喜!您已经体验了 IDaaS 最核心的流程。请您后续参考进阶文档,导入更多账号,创建更多应用!

1.4. 管理进阶

1.4.1. 身份提供方

1.4.1.1. 绑定钉钉-入方向

实现场景

IDaaS 中有【身份提供方】概念,用于管理企业常见的、现有的身份系统和 IDaaS 之间的联动。 钉钉作为阿里云产品,和 IDaaS 之间有着天然的集成,绑定钉钉的配置流程非常简单,您只需要扫码并授权,2 分钟即可完成绑定。通过极其简便的配置可实现如下能力:

分类	实现能力
账户	 將钉钉通讯录全量同步到 IDaaS 监听钉钉通讯录事件, 增量同步有变动的数据到 IDaaS 全量或增量同步数据到钉钉(请看绑定钉钉-出方向)
登录	● 钉钉扫码登录 IDaaS 或 IDaaS 中的应用
应用	 在钉钉工作台单点登录到 IDaaS 中的应用 在钉钉工作台自动创建单点登录到 IDaaS 中的应用(暂不支持)

绑定钉钉的两种方案

您可以在【身份提供方】菜单中,将钉钉添加为 IDaaS 的身份提供方,并在过程中开启所有相关能力。 针对从钉钉导入数据的场景, IDaaS 支持两种方案:

方案	说明
	采用钉钉三方企业应用方案,扫码授权即可完成配置。 优势: • 配置极简,开通方便。
<u>三方应用方案(快速绑定钉钉)</u>	⑦ 说明 配置过程无需您填写任何信息,仅需扫码授权,即可全部配置完成。
	劣势:无法批量获取到用户的手机号和邮箱,需管理员填写或用户在登录时授权。
	在三方应用方案的基础上,需要钉钉管理员创建钉钉一方应用,开放对应权限,并将信息配置 到 IDaaS。 优势:
<u>一方应用方案(钉钉高级配置)</u>	 权限灵活,可获取到完整的用户信息。 劣势: 配置周期较长。

快速绑定钉钉

在【快速入门】或【身份提供方】菜单中,点击【快速绑定钉钉】,即可开始快速绑定钉钉-入方向流程。

三()阿里云	\$ Ift 2 KM ~	Q HR SRE IN K
云身份服务	云身份服务 / 快速入门	
DIA BER	快速入门	
导台提供方	欢迎体验 IDaaS 云身份服务	
16.m	IDasS 原用量云原生企业账号管理中心,为成企提供单步整备,访问任期	等安全、俚语的业务很多份管理服务。
应用	如果包括 (DeaS 10 北京本省户) 清查省文档 1×10000000万里。	
爱臣	上美学時代表 应应下方关键代表, 在他于你快速上工作用Dask	
日市	2.3 Mar 2.3	
个性化	2 *	*
	继续现有账号系统	实现应用单点整块
	快速导入账号,并展用影响的登录方式。	2 🔅 🐓 🗙 🗘 🖬 🗶 🖙 🗶 🤟
	16089621111 A	HIB RAM SSO
	入力1的 ③	前社应即市场 接入自耕应用
	曲方向 ③	

第一步 选择场景

在第一步中,选择希望和钉钉实现的场景能力,若无偏好,可直接下一步。

1 绑定配置	2 扫码开通	3) 扫码绑定
同步目标	Q. 阿里云 IDaaSdddd く	
	导入通讯录中的数据并置于该节点下,可在第二步中授权通讯录的导入范围。	
増量同步 ⑦	この日本日本	
UUHHER ()	この第月	
更多设置	☑ 數数一次全量同步	
	完成原定后,导入钉钉通讯录授权范围内的全部数据。首次增量同步崩建议进行一次全量同步。	

能力说明

- 同步目标: 钉钉的通讯录数据将会导入到 IDaaS 的这个节点之下。
- 增量同步: 启用后, IDaaS 调用钉钉接口, 监听钉钉通讯录事件。钉钉通讯录有变动, 可实时将变动数据同步到 IDaaS 中。
- 从钉钉导入的账户,IDaaS 会默认使用其钉钉 userld 与 IDaaS 账户进行匹配(可在字段映射中自定义规则),如果匹配成功,将覆盖更新,否则将创建账户。
- 建议在增量同步前进行一次全量同步,否则部分数据可能会同步失败。
- 单条记录无法导入,不影响其他数据导入。
- 失败信息可在【同步日志】中查看。
- **打钉扫码登录:** 勾选后, 会在【登录】菜单中创建【钉钉扫码登录】, 并处于启用状态, 可直接扫码登录。
- **触发一次全量同步:** 勾选后, 将在完成绑定后导入钉钉通讯录授权范围内的全部数据。

第二步 扫码开通

在第二步中,请钉钉管理员扫描二维码,为钉钉企业开通【阿里云 IDaaS】三方免费应用。

绑定钉钉-入方向		×
✓ #定配置	د <u>عبر المجامع</u> عبر المجامع (٤)	扫码绑定
	時使用 <u>111雪提売账号</u> 扫码。 开港 (D <u>ass 应用</u> <u>若己开造</u> ,可重输进入最后一步。	
	distributionersities distributionersities	(
上一步 輸从已升鐵应用,	N-19 REA	

钉钉扫码后,将跳转到应用开通页面,如下图所示完成开通流程。



? 说明

在完成绑定后,如需调整同步到 IDaaS 的钉钉通讯录范围,请在 钉钉管理后台-应用管理 中的【阿里云IDaaS】应用中调整,IDaaS 在同步时以该应用的授权范围为准。

(>) 切好管理后台					DINER 🗳 MARKA
小杨科技		工作台 > 应用管理			
(2.775)				1日 か公用語	🔀 HHIEM
12 首先					
创 通讯录	٠	The size	1 2018人專	🗐 tikat	😑 H#
88 IM18	^				
应用管理					
连接圈			хэя	🟠 金月園	<mark>)</mark> #9
⊕ 钉钉专业版 →===	*	_		_	
∠ 增值服务	÷	交 ^朱 晋	2 XX10	支付重(办公)	道驗助手
0 <u>2488</u>	*	6 1988	① 小麦杏枝	(二) 第5日	
日 酸芳酮	-				122
◎ 安全与权限	Ŧ	(十)从服用中心器的			19/10

第三步 扫码绑定

最后第三步,请钉钉管理员在【阿里云 IDaaS】应用中点击【钉钉管理员扫码绑定】按钮,扫描第三步中的二维码并确认,即可完成绑定。此时IDaaS 会根据配置执行全量 同步或增量同步,钉钉用户也可以扫码登录 IDaaS。

绑定钉钉-入方向		×
→ 網定配置		
	请在 <u>打打</u> 中打开 IDaaS 应用,并点击页面上的 <u>扫码感觉</u> 再次扫码先成配置	
		ſ
上-步 〇 等待相至中	R76	

管理钉钉身份提供方

绑定钉钉后,会自动跳转到【身份提供方】菜单中。您可在此处对与身份提供方联动的不同功能进行管理。

☰ (-) 阿里云 🛛 🗢	工作台 및 杭州 ∨	Q 搜索	费用 工单 ICP 备案	企业支持 🗗 🖸 📋	· ⑦ 简体	0
云身份服务	云身份服务 / 身份提供方			IDaaS 讨论区 III	DaaS 支持群 帮助	文档
快速入门	身份提供方					
身份提供方	绑定企业的其他身份提供方(ldP Identity Provider),包括钉钉、AD、企业微信、飞书等,	实现账户同步、代理认证等功能。请参考文档身	分提供方。			
账户	快速爆走打打 > 其他身份提供方					
应用						
登录	小杨科技 ② 导入成功 画看详情 ×				删除	
日志	Corpia: aingaa ideob					
个性化		JIDaaS 増量同步 已启起			已禁用 🚺	
		(*: /戸)主云 IUaas 査看日志 触发同步	修改配置	抗重获取贝工于机械、邮相等个人取励信息。	修改配置	

查看导入状态

- <u>导入提示</u>:若您绑定时选择了【同步通讯录 导入 IDaaS】,那么会在页面上提示【正在导入中...】。点击【查看详情】,即可跳转到【同步任务】中查看进度。
- <u>手机号/邮箱缺失处理</u>:同步完成后,会在【身份提供方】页面进行提示。导入进来的账户即可使用钉钉扫码登录 IDaaS 或应用。但刚导入的账户缺失手机号/邮箱,我 们会建议用户补充手机号/邮箱,否则包含二次认证、找回密码等相关功能将不可用。详情查看: 钉钉扫码登录。

修改同步目标

如果需要修改同步目标,请在修改后手动触发全量同步,核对组织架构是否符合预期。

钉钉扫码登录

 若您绑定时选择【钉钉扫码登录 - 启用】, IDaaS 会在【登录】菜单中创建钉钉扫码登录方式。您可以在【身份提供方】或【登录】菜单中对功能进行管理。用户可以前 往登录页进行钉钉扫码登录。详情查看: 钉钉扫码登录。

绑定多个钉钉

IDaaS 支持绑定多个钉钉通讯录,只需用不同的钉钉企业管理员,按照上述扫码开通流程即可完成。

多企业管理的情况下,您可能希望不同企业账户同步到不同的目标节点,以作区分。例如希望将钉钉企业 A 和企业 B 通讯录导入 IDaaS 中统一管理,我们建议您先在 IDaaS 组织架构根节点下,创建 A 组织和 B 组织,并在绑定钉钉时,指定企业 A 同步到组织 A, 企业 B 到组织 B。

但反过来,一个钉钉企业只能绑定一个 IDaaS 实例。若您同一个钉钉企业绑定多个 IDaaS 实例的需求,请等待后续版本更新支持。

开启钉钉高级配置

完成绑定钉钉后,可以按需在身份提供方页开启钉钉高级配置。开启高级配置后可以获取到完整的钉钉用户信息,以及未来支持的在钉钉工作台自动创建 IDaaS 中的应用、 实现单点登录。

	工作台 및 杭州 → Q 投	s 書用 工年	a ICP 备案 企业 支持 💀 🖸 🗯 📜	· ② ③ 简体 ③
云身份服务	云身份服务 / 身份提供方		IDaaS 讨论区	IDaaS 支持群 帮助文档
快速入门	身份提供方			
身份提供方	绑定企业的其他身份提供方(ldP ldentity Provider),包括钉钉、AD、企业微信、飞书等,实现账户	同步、代理认证等功能。请参考文档· <mark>身份提供方</mark> 。		
見	快速爆造钉钉 > 其他身份提供方			
应用				
登录	小杨科技			删除
日志	Corpla: aling830271 = control = = = control = = =			G
个性化		増量同步 已启用 C		已禁用
	ana, muss/umusuomanyumusustum and/minususteen a	查看日志 触发同步 修改配置	RUMBRAR スエナルで、即用サイト体別相応。	修改配置

第一步 选择场景

第一步中	, 目則晢个廾放[
			(3) (183)(28	×
 	在同步时可以就能员工手机号、邮箱等 未来这時	· UTHERXHI	J 100000	I
_梦 U	则建应用	広田信息和墨利いる		
市二丁中	需安符1111中的/	业用信息能直到 IDd	d5 Ψ。	~
目目局级配直	Î.	•		X
✓ 选择场景	ł	2 创建应用		分配权限
请在灯灯开放平台	會中创建企业内部应用,复制应用	配置信息并填写到下方,查 看 文档		
Corpld	ding9d1d 📕 🗖 🖷 📕			
кррКеу	请在钉钉应用详情的 <u>应用信息</u> 8	天取。		
AppSecret				
	请在钉钉应用详情的应用信息。	天职。		4
⊥# 下- 录 钉钉开	-步 Rm 放平台-企业内部	¹⁷ 开发,点击【创建	应用】,填写企业	内部应用的基本信息
全业内部用发	41111 ±11111	 0 		(947.024)
nnan Ehe	4.001R 0458 HS8005	a	1928 - Similianagendi	ineres a
næ,		1977. #121413: 2022.05.08	HSettab.5%	
	- in in in its	REMO: 20220121	HSBBER	
	- 😒 EWARTARA	004A.2	HSettab.Sij	
	 — — —	GARA:	16508(23)	
创建企业内部	应用	×		
应用类型	2: • H5微应用 🔿 小程序			
• 応田名称	5: demo			
* 应用名称	R: demo			
* 应用名称 * 应用描述	 オートレージョン・オート・オート・オート・オート・オート・オート・オート・オート・オート・オート	: 注登录。 		
● 应用名称 ● 应用描述 应用图称	8: demo g: demo成用在IDaaS的单。 ;:	: 199. 		
 ◎ 应用各利 ◎ 应用描述 ◎ 应用图标 	 demo demo应用在IDaaS的单点 iii ja_LIfs/PG/PNG检击、244 	: 2登录。 		
• 应用名称 • 应用描述 应用图称	 8: demo 8: demo旅用在IDaaS的单点 6: 原本 第二代3FG/PNG指式, 24G 以口約天面角回転 	: 2登录。 		
 ・ 应用名称 ・ 应用描述 ・ 应用图构 	 k: demo g: demolt/用在iDaaS的单点 示: 点上代5/PG/PNG指式、24G 以内的无面角面标 直着面積が認知 > 	: 2登录。 		
 ・应用总称 ・应用删述 应用图频 ・开发方式 	 オートレージョン・シーン・シーン・シーン・シーン・シーン・シーン・シーン・シーン・シーン・シー	: 2世界。 9240ps以上、1:1、2MB 11服务商开发		
。应用名称 。应用描述 应用图称	 オートレージョン・ション・ション・ション・ション・ション・ション・ション・ション・ション・シ	: 2登录。 2240ps以上, 1:1、2M8 U服务商开发 取消 确定的时		

完成创建后,将自动跳转到钉钉的应用详情页。依次将 AppKey 和 AppSecret 复制粘贴到 IDaaS 中。

▶ 钉钉开放平台	首页 成用开发 > 开放能力 > 开发工具 阿爾云 基本信息 开发文档 返回旧版 Q 小杨科技 退出	
< 返回企业内部开发 demo (HSOUTE) 企 基础信息 へ	应用信息 femo demo demo demo demo demo gala	
成用信息 开发管理 权限管理 ♀ 成用功能	应用凭证 AgentId AppSecret 16g 1g dingwgoff 1g 1g WFLIDyKDj12cM8whSspjLbUper9U1ctdj82TNF7et 1g	
消息推送 酷应用扩展 事件与回调 登录与分享	删除应用 删除操作不可逆,该应用所有信息将被删除,请谨慎操作. 概除	
山 安全与监控		

完成填写后,点击【连接钉钉】,IDaaS 将测试和钉钉的连接,如果所填信息正确,则可以进入下一步。

 一 函料 	2 创建应用	3 分配权限	
请在 钉钉开放	8平台 中创建企业内部应用,复制应用配置信息并填写到下方。 或着 文档		
orpld	ding5d1de68		
ррКеу	ding a griff a gala a		
	请在钉钉应用详情的 <u>应用信息</u> 获取。		
ppSecret	WEUD 11, and and and the first them to set the test of tes		
	请在钉钉应用评情的 应用色思 获取。		

第三步 分配权限

在第三步中,您需要在当前的钉钉应用中分配权限。点击【权限管理】,分别在【通讯录管理】和【应用管理】中勾选全部权限,并点击【批量申请】。

> 钉钉开放平台	首页 应用开发	攴 ~	开放能力 ~	开发工具	阿里云	基本信息	开发文档	返回旧版	↓ 小杨科技	退出
< 返回企业内部开发	权限范围									
HSW近用 HSW近用	注:接口权限是以应 用范围和适用类型, 请选择权限范围:()	2用维度(部分接) 泰加通讯	数受权, 鼓励应用(□需要付费或达到) 录接□权限后生效	使用尽可能多的热 特定条件后才可修)	妾囗,实现跟钉 更用。	「钉核心能力的≦	全面互通。并不是所有接口都	8可以直接开通	i使用,具体参照接	口的使
应用信息	 全部员工 授权部门: 	部分员工	_							
开发管理	全部员工 + 添加	bo							4	
权限管理	请输入权限或接口的名	3称进行	搜索						→ 批量申	请 (10)
消息推送	全部		权限信息		接口		权限点code		全部 _{筛选 Q} 状态	操作
酷应用扩展	2 通讯录管理		企业员工手机号信	息			fieldMobile		未开通	申请权 限
登录与分享	OA审批		邮箱等个人信息				fieldEmail		未开通	申请权 限
业 安全与监控 ▲	考勤				获取部门	羊情 🕒				
监控中心 ⑦ 部署与发布	消息通知 硬件		通讯录部门信息调	卖权限	获取指定) 列表 □ 获取部门3	用户的所有父部门 列表 🕒	qyapi_get_departmer	nt_list	未开通	申请权 限
版本管理与发布	智能人事				获取指定部列表 🗋 查看更多	邵门的所有父部门				
	日志				设置高管标	黄式 🗋				
	^{立王9} 钉钉运动		维护通讯录的接口	口访问权限	创建部门 更新部门 删除部门	6 6	qyapi_manage_addre	sslist	未开通	申₩
	应用管理身份验证				查看更多					\odot

权限范围请选择【全部员工】。如需调整同步到 IDaaS 的钉钉通讯录范围,请在 钉钉管理后台-应用管理 中的【阿里云IDaaS】应用中调整,IDaaS 在同步时以该应用的授权 范围为准。

完成授权后,在 IDaaS 中点击【确认已授权】按钮,IDaaS 将检查该应用是否拥有钉钉通讯录管理权限,检查通过则完成了配置,此时 IDaaS 即可获取员工手机号、邮箱等 信息。

钉钉高级配置		×
→ 选择场景		
请在打打开放平台	中进入应用评情,在 权限整理 中分配 通讯设备理 和 应用管理 的 全部权限,按权范围选择 全部处工,查看文档	
L->> 1011	2960 803	

? 说明

如果您希望只有 IDaaS 可以请求该钉钉应用,请在该钉钉应用页面的【开发管理】中填写【服务器出口IP】:

112.124.239.96,112.124.239.101,112.124.239.100,112.124.239.99,112.124.239.98,112.124.239.97,112.124.239.105,112.124.239.104,112.124.239.103,112.124.239.102,112.124.239.104,112.124.239.103,112.124.239.102,112.124.239.104,112.124.239.104,112.124.239.102,1124.239.102,1124.239.102,1124.239.102,1124.239.102,1124.239.102,1124.239.102,1124.239.102,1124.239.102,1124.239.102,1124.239.102,1124.239.102,1124.239.1024.239.124.239.1024.239.124.239.1024.239.124.239.1024.239.124.239.1024.23

▶訂訂开放平台	3	前の 前用开設、 开放能力、 开放工具 阿服云 基本信息 开設文档
< 返回企业内部开发		
demo HSMC2PE		开发管理 在开想病,需要在开設者后台能運服务提出CIP,应用該贡辱。7%要多
C MALICUS	•	 · 开发模式 ·
应用信息		● 「1220日76 ○ PRANUUSK 需要表示开发工具进行功能开发
开发管理		服务器出LIP
权职管理		112.124.239.96,112.124.239.101,112.124.239.100,112.124.239.99,112.124.239.98,112.124.239.97,112.124.239.105,112.124.239.105,112.124.239.105,112.124.239.105,112.124.239.105,112.124.239.102
C1 应用功能	*	《周田打打服务课本PEED会注户列展、多个PEE以下展开、支持用一个"每通配物的PEE比
满意推送		*应用盖页地址
動应用扩展		请输入
事件与回阅		增給,AhttpRhttpstf:SEDMEHER, SDhttps://www.dingtalk.com
由于该应用当	主要用	3于同步数据而不用于员工日常使用,【应用首页地址】

第四步 调整字段映射(可选)

如果您希望将钉钉手机号、邮箱信息作为 IDaaS 账户的用户名、手机号等,或者将手机号相同的钉钉用户与 IDaaS 账户进行绑定,可以在 <mark>字段映射</mark> 中进行配置。

1.4.1.2. 绑定钉钉-出方向

介绍绑定钉钉-出方向的操作步骤。

快速绑定钉钉

在【快速入门】或【身份提供方】菜单中,点击【快速绑定钉钉】,即可开始快速绑定钉钉-出方向流程。

☰ 〔→)阿里云 ゅ	a 王作俗 章 机州 ~	Q 找求 费用 工单 H
云身份服务	云身份服务 / 快速入门	
快速入门	快速入门	
身份提供方	双道体验 IDaaS 云身份服务	
账户	Das5 是阿里云原主企业账号管理中心,为政企提供单示登录。	边问拉利等安全、便播的业务级身份管理服务。
应用	如用想是 IDeeS 1.0 宅地本面户, 请查看文档 1.x 已收买的安里;	ne.
建 业	上手装儲行各 克成下方关键任务,有助于包括道上手使用D.	85
日本		
个性化	< ●	
	惯定现有账号系统	实现应用单点强采
	快速导入账号,并整用现有的抽屉方式。	a 🔗 🧔 🛟 🕉 🗘 🔽 🛯 🗶 🥆 📼
	telestingsTHT A	开酬 RAM SSO
	入方向 ③ 网络动物副植方	前往应用市场 接入白研应用
	HUDIN (D AL DAAS FEBRUARIES FT	

第一步 创建应用

在第一步中,您需要在 IDaaS 中填写以下信息:



- 显示名: 用户在登录、使用 IDaaS 时可能看到。
- <u>Corpld</u>:在 钉钉开放平台-首页 获取。

9400370, 880894-88, 85	(((((((((((((((((((((((((((((((((((((((🔊 944 C	
	的合数理则进行如何。	Could dealed auguste	
Jac SWRItty開版用		APT ILEANE - 201900013401362.000000 公告 「面相目的に」开始なな相目的(500-6512) 「面相目的に」开始なな相目的(520-529) (回目的に」开始なな相目的(520-529) (回目的に」」 デ教育会の相目的(520-529) (回目的に) (520-52) (100-100) (06/17 06/17 06/12
	REGIMA	【■映画は】开発まな和単新(509-5-15) ← 5 cconnee 括景化集成方案,降低开发成 6 critt中和原用要素和	65/20
		RETAINS	5.575%man 运费化集成方案,降低开发成3 。01077年8月1日

<u>AppKey/AppSecret</u>.

○ 在 钉钉开放平台-企业内部开发 中创建应用。

> 钉钉开放平台	前页 <u>原現开設</u> → 开設能:	b > 开放工具 同語云 数4回巻 开放文紙	2019-105	0 (1604)8 3
全业内部开发	钉钉应用 #####	v 8		((#04))
@ 1713608	ANDER OVER HSDEER		1988 - Mathema	
# Ift				
6 FIEL	 demois/8020ad358/0229. 	SS版人: ** * 単四時刊: 2022.06.06	H5如应用	
	Image: 100 jean 10	008A: •	HSIDEET	
		信用人: 11日 創訂時刊: 2022.04.29	HSRIDER	
	15点 (15) (15) (15) (15) (15) (15) (15) (15)	0080A:	H5/8/201	

◦ 在应用详情中获取 AppKey/AppSecret。

	NY GREN LINNA INTE DEP MAR	THEY BEACH O AND I AN
	应用信息 demo demoliflesDauStymo建界。	84
оное лаян оран С алон оное	应用凭证 Apartori We L doging line = = =	Ngalawi Militadi at a sa a a a a a a a a a
2019/02 2015/07-20 2017-02/20 2017-02/20 2017-02/20	删除应用 maantrife, maanthaansama, maantri, ma	12
al \$25000 -		0

您还需要将以下信息填到到钉钉中:

 CORRE 	:00	20 B MA V			이 아이는 이 가 가 가 가 가 가 가 가 가 가 가 가 가 가 가 가 가 가
Decise .		2000年 - 00000 身份提供方			0028315-26万向
sesian. ter CH		ACCOUNTS OF MANAGEMENT OF MANY PARTY, 1997, 40, 52 ACCOUNTS OF MANY PARTY.	n 708 Ilberte	NEX CROW, REAL MARKING,	ORGEN OFFICER NEWPORE
13					NO CALEND NO. CALEND ALEXAN PROVIDER.
185		ENGL9	Sana 💽	RMM Gal Mate	- Copiel Relation and a commentation and a commentation and a commentation and
		Compare solution of			NOCCONFICIE CARANTER, EXTENSION AND AND AND AND AND AND AND AND AND AN
		135228 (h): Nep-threfaille-algorithm over (0112228)	128 C	RENOL WARD	Vagheer.
		123 Complete JUDI alt			MARKER WELLCHARTERSTORMEN, MICH WELLCHARTERSTORMEN, MICH WELLCHARTERSTORMEN, MICH WELL MICH WELLCHARTERSTORMEN, MICH WELLCHARTERSTORMENT, MICH WELLCHARTERS
		III victorateuteuteuteute infitéééé	Cine 👅	RENER GROUP	NNECTORINE () NOCCONTRACTOR () () NOCCONTRACTOR () () () () () () () () () () () () ()
		best Owner 1 of			_
					2-2

• 回调域名:填写到应用详情中的登录与分享-回调域名。该字段用于钉钉扫码登录,如果不填写将无法使用钉钉扫码登录到 DaaS。

> 钉钉开放平台	百次 約用井敷 ~ 井田能力 > 井助工具 同能品 基本協参 井敷之地	1000 0 94646 1 800
 с. акала . кона . 	接入及录 actions (in AnArgidoCollectus, 7885 - 1999년 	
 <u>他</u>但其新 和件句描述 2 秋句が本 	接入分享 10.58954、23	46 42
41 安全地設設 ~ 12(2中心	105 539	Ē
◎ 2番526 ~ 図本管理526年	Android 9 %	ం

 应用首页地址:填写到应用详情中的登录与分享-回调域名。配置该字段后,用户在钉钉控制台点击该应用时(在版本管理与发布中可以设置应用的可见范围),可以 单点登录到 IDaaS 应用门户。



? 说明

如果您希望只有 IDaaS 可以请求该钉钉应用,请在该钉钉应用页面的【开发管理】中填写【服务器出口IP】:

112.124.239.96,112.124.239.101,112.124.239.100,112.124.239.99,112.124.239.98,112.124.239.97,112.124.239.105,112.124.239.104,112.124.239.103,112.124.239.104,1124.239.104,11

> 钉钉开放平台	首页 <u>成明研設</u> ~ 开放能力 ~ 开发工具 阿里云 基本信息 开发文档
< 返回企业内部开发	
demo HSRGT	开发管理 在开发期,需要在开放者后台配置服务器出口PP、应用趋页等。 了解更多
0 356668 ·	◆开发模式
应用信息	 ● 升-2004円 ● 状体理由技 需要使用开发工具进行动相开致
开发管理	服务器出口IP
权限管理	112.124.239.96,112.124.239.101,112.124.239.100,112.124.239.99,112.124.239.98,112.124.239.97,112.124. 239.105,112.124.239.104,112.124.239.103,112.124.239.102
C 应用功能	▲ 调用打打服务调API的的合法IPF测索,多个IP通识;"隔开,支持等一个小型通能符的IP相式
消息推送	*应用首页地址
酷应用扩展	湖柏入
哪件与回调	博输入httpIIIhttpIIIhttps开头的网边链接,如https://www.dingtalk.com

第二步 分配权限

在第二步中,您需要在当前的钉钉应用中分配权限。点击【权限管理】,分别在【通讯录管理】和【应用管理】中勾选全部权限,并点击【批量申请】。权限范围请选择 【全部员工】。



完成授权后,在 IDaaS 中点击【下一步】按钮,IDaaS 将检查该应用是否拥有钉钉通讯录管理权限,检查通过则完成了配置。



第三步 选择场景

在第三步中,选择希望和钉钉实现的场景能力。



能力说明

• <u>同步目标</u>:同步来源所选的 IDaaS 的账户/组织数据将会导入到钉钉的这个节点之下。【目标节点】需要填写钉钉部门 ID,可以在 钉钉管理后台 中编辑部门时可以看到, 钉钉根部门的 ID 默认为 1。

унижность						100000	(55120.F
-1-ME8128	2	日本語 > 参口管理					
e mu.g		部门管理				811188	
		CORD REPORTS				4070.440	
10 ER		(#8/07) (##0/8/07)				• DH 10444	240
3 MR. 4		\$10,040 B	162588	2.8	16(3488898		PORTOTION DE LA CONTRACTA DE L
		446448	10		2.0	 上現型(3) 	14848
PERMIT		► □ 15735	2		#8		
新加速		0.0286	5		2.0	CHIE:	
智能人事		0 8239	2		#R	80	
外部联系人							
ACCESSION DATE:						电话	
10100-510-2						70/7EX	
内部運和決定置							
S Ifte							bies/(30
-							-109817189178-00
• ()() • Ann							
<1 (13)438							5X77 #819 \$225

- <u>增量同步</u>: 启用后,当 IDaaS 账户/组织数据有变动时,将实时将变动数据同步到钉钉通讯录中。导出到钉钉的账户,IDaaS 会根据第四步【字段映射】中的【映射标 识】与钉钉用户进行匹配(可在字段映射中自定义规则),如果匹配成功,将覆盖更新,否则将创建账户。
- **钉钉扫码登录:** 勾选后, 会在【登录】菜单中创建【钉钉扫码登录】, 并处于启用状态, 用户可直接扫码登录。

🗋 警告

建议使用小范围的数据(或非生产环境)进行测试验证,完成验证后再扩大节点范围,以免因配置有误影响钉钉的数据。

第四步 字段映射

如果您在钉钉中已存在存量数据,需要 IDaaS 账户/组织和钉钉用户/部门绑定,或者希望使用 IDaaS 中账户的某些数据作为钉钉用户的数据,例如将 IDaaS 账户的显示名作 为钉钉用户的姓名,则需要在第四步配置字段映射。

Same Same Same Same		10H 2 H-4 -		Q ME.	#1.2	a cras co on 8 10	6' W	0 0 mm	6
	19.15	3.86488 / 900/7		\$5.880025793					×
		快速入门		(2) status	(2) anes —	arss			
	Rð	NUMBER OVER STREEM						-	
		DASSING THE DESCRIPTION OF THE PARTY OF THE		BADDE CAS PERFORMENT	CALIFORNIA CONTRACTOR	OR CASES/CONTRACTOR	7109.0		
				80					
		2333220 04733201, 00100023000ml		ocm	#4520	2314		391	
				t A MR spitecensit	0.075L ~	104	~ ©	1211 1 100	
		THE REAL PROPERTY AND A DESCRIPTION OF A	201004400	1.345.534 COUNTS	2010	P6	v o	51 H	
		URDAN, PROBABERTZ,	□ ⊕ C ⊕ X O B K ↔	- ALL DAR	8838	214	~ ©	16 N 1 16 D	
• and Citi and • and € Citi and • and • and € Citi and • and • and • and • and		RANARD V	NER MAN LID	were (KENNE) Optimizero	8898 ×	uati	~ ©	10. NO	
H H H H COT MM 1 MM N COT MM 1 MM N N				- 88990					
Circle Visit Visit All Bill State State State State State - State				005					
■ 200				0070	INVESTIGA.	754		81	
				M 350 Splippingstonel/Honeme	20110 V	the	~ @	201 000	
				- 84974					
60, 01/609 000, 0700				60,01000 000,0	COLUMN TO A COLUMNT TO A COLUMN TO A COLUMNT TO A COLUMNTA A COLUMNT TO A COLUMNT TO A COLUMNTA A COLUMNT TO A COLUMNTA A COLUMNT T				

□ 注意

如果需要使用 IDaaS 账户登录专属钉,钉钉用户的 userid 字段必须使用 IDaaS 账户的 userid 字段。

IDaaS 默认支持钉钉的名称、手机号、邮箱、职位、工号等字段值的自定义,如果您需要使用其他字段(比如办公地点),您可以【添加字段】。



• <u>字段名称</u>:仅在 IDaaS 中显示使用。

● **字段标识**:需要使用钉钉字段名称,在当前身份提供方中唯一。以上图为例,办公地点的字段标识是 work_place。更多钉钉字段请看 钉钉用户的全部字段、钉钉部门的 全部字段。

更多字段映射的说明请查看文档字段映射。

如果确认字段映射的配置准确,可以选择【保持,且立即同步】,此时将执行一次全量同步,将第三步所选的 IDaaS 数据同步到钉钉;如果您暂不确定字段映射的配置是否 准确,可以选择【仅保持,暂不同步】,后续在该身份提供方的【修改配置-字段映射】中修改。

↓ 注意
 使用增量同步前需至少进行过一次全量同步,否则可能导致增量同步失败。

1.4.1.3. 其他身份提供方

阿里云 IDaaS 会在未来版本中提供原生的 AD、OpenLDAP、企业微信、飞书等常见身份提供方的天然联动,敬请期待。

1.4.1.4. 字段映射

使用字段映射可以管理不同账号系统和 IDaaS 账户/组织的对应关系。本文档介绍字段映射的基本概念和操作。

基本概念

通过【字段映射】能力,您可以在两个层面实现 IDaaS 账户与外部账号的一致性:

- <u>账户层面</u>:通过账户绑定关系将账户的状态保持一致。以导入钉钉通讯录为例,如果某个钉钉用户与 IDaaS 账户建立了绑定关系,在钉钉删除该用户时,在 IDaaS 中也 会删除对应的账户。
- <u>字段层面</u>:在账户绑定关系的基础上,通过**字段映射关系**将账户的**信息**保持一致。以导入钉钉通讯录为例,如果将钉钉用户的企业邮箱作为 IDaaS 账户的显示名,当钉 钉用户的企业邮箱修改时, IDaaS 账户的显示名也会修改。

? 说明

只有在删除 IDaaS 账户/组织/组后,才可删除绑定关系;组织也支持绑定和字段映射,但暂不支持映射标识。

字段映射入口

- 您可以通过两个入口配置字段映射:
- **创建时:** 在创建身份提供方时(除了绑定钉钉-入方向之外),在创建流程中可以配置字段映射。
- 修改时: 在身份提供方页面中, 点击【修改配置】后, 在弹窗内可切换至【字段映射】模块。

☰ (-)阿里云 🖙	〕 I作台 ② 杭州 → Q 授系 商用 I单 ICP 留案 企业 支持 🔂 🗋 🍦 🤉 ⑦ 商	陈 🌔
云身份服务	云身份服务 / 身份提供方 IDaaS 讨论区 IDaaS 支持群	帮助文档
快通入门	身份提供方	
身份提供方	据定企业的其他身份提供方(ldP ldentity Provider),包括打钉、AD、企业做信、飞书等,实现账户同步、代理认证等功能。诱参考文档身份提供方。	
账户	快速确定到打 > 其他身份提彻方	
应用		
登录	小杨科技 @##	8.
日志		8
个性化		
	Elizet (mpx)/ 「 Legy indeducen (Elizet 2 view of 1 National Content of 1 Nationa	牧配置

映射标识

您可以指定一个【映射标识】来建立账户绑定关系,如果字段映射两边的值相同则进行绑定,主要适用于绑定已在使用的存量账号。例如,从钉钉导入用户到 IDaaS 时,假 设映射标识如下图所示,如果钉钉用户的企业邮箱 zh***@example.com 和某个 IDaaS 账户的邮箱相同,这两个账户会进行绑定,绑定成功后账户的状态和信息将保持一 致;如果和所有的 IDaaS 账户的邮箱都不相同,则会创建 IDaaS 账户并进行绑定。

在此处配置钉钉通讯录字段到 IDaaS 账户/组	织字段的对应关系,例如将	将钉钉用户的工号作为 IDaaS 账户的账户将	8、了解更多	
<u>Þ</u>				
IDaaS 字段	映射规则	字段值		操作
显示名 user.displayName	造择字段 ~	员工名称	~ @	澤加 移映
手机区号 user.phoneRegion	选择字段 🗸	国际电话区号	~ (?)	添加 移除
手机 映射标识 user.phoneNumber	选择字段 🗸	手机号码 (雲开启高级配置)	~ @	添加 移時
邮箱 获得打获 获 user.email	选择字段 🗸	个人邮箱 (電开启高级配置)	~ 0	添加 移种
织				
IDaaS 字段	映射规则	字段值		操作
* 组织名称	法释定的 🌙	部门名称	~ @	35.hn \$2.00

不同的身份提供方支持不同的字段作为映射标识,您可以根据业务需求设置其中一个作为映射标识。您也可以不设置或取消设置。

映射规则

IDaaS 目前支持两种方式进行字段映射:

- 选择字段:选择同步来源中的某个字段,直接将它的值作为同步目标对应字段的值。IDaaS针对不同的身份提供方会有不同的字段范围,如果您所需要的字段不在范围内,可使用表达式进行设置。
- 表达式:通过表达式自定义所需的值,并将它作为同步目标对应字段的值。使用表达式可以灵活地兼容多种场景,例如将钉钉的邮箱前缀作为 IDaaS 账户名,或者使用不在 IDaaS 【选择字段】范围内的字段。以下为表达式的常见用法:
- 使用字段范围之外的字段:
 - 钉钉用户岗位: idpUser.title
 - 钉钉用户办公地点:idpUser.work_place
 - 钉钉部门负责人: idpOrganizationalUnit.org_dept_owner
 - 钉钉的全部字段请参考《钉钉用户字段》、《钉钉部门字段》。
提取邮箱的前缀作为字段值:

- 使用钉钉邮箱前缀: SubstringBefore(idpUser.email,"@")
- 使用 AD UPN 前缀:Subst ringBef ore(idpUser.userPrincipalName,"@")
- 使用固定值: Trim("myString")

? 说明

IDaaS 表达式中的字段格式为"idp"+"User/OrganizationUnit"+"."+"身份提供方中的字段名"(入方向)或"IDaaS 中的字段名"(出方向),如 idpUser.userld。更多表达式样例和语法请查看 高级:账户字段表达式。

针对不希望进行映射的字段,可以点击【移除】按钮,此时映射规则将变为【不映射】,在同步时将不会同步该字段的数据。

1.4.2. 账户

1.4.2.1. 创建账户/组织

IDaaS 支持如下账户创建方式:

账户创建方式	描述
从身份提供方中导入	当前支持钉钉。操作参考: <mark>绑定钉钉</mark> 。 接下来会支持:AD、OpenLDAP、企业微信、飞书等常见身份提供方。
OpenAPI 开发对接导入	IDaaS 开放账户管理 OpenAPI 供开发者调用,可用该系列接口批量导入账户。
手动创建	管理员在控制台中逐一创建。操作参考: <mark>2. 创建账户</mark> 。
Excel 导入	暂不提供。

由于 IDaaS 不按照账户数计费, 您尽可以将企业/团队所有账户导入进来, 统一管理。

导入后,即可在【账户】菜单中,对账户/组织进行统一管理。

	工作台 👱 杭州 🗸	Q 搜索	费用 工!	单 ICP 备案 企	业 支持 App	Þ Ó	☐ ⑦ 简体	Ģ
云身份服务	云身份服务 / 账户				52	ā本更新记录	IDaaS支持群 帮助	文档
快速入门	账户						导入	
身份提供方	IDaaS 中管理的账户可以通过 https:	// lev.aliyunidaas.com 登录用户门户	或 SSO 到应用。					
账户								
应用	组织结构	账户 组织						
登录			7		0			~
日志	▼ 阿里云 IDaaS	□健康尸 全部状念 ◇	3 ∨ 请输入		Q	~ t	1317日(二元中省6	3
个性化		□ 账户名	显示名 手机	1号 邮箱	来源 账	户状态	操作	
		□ test ⊘			自建 🥝)正常	禁用│编辑│ :	
		批量删除		每页显示 10	✓ 共1条数据	< 上一页	1 下一页 >	

1.4.2.2. 账户详情

IDaaS 允许管理员总览指定账户详情,并对账户进行状态变更。

从【账户】菜单中,找到希望查看详情的账户,点击该行账户名,或从右侧选择【详情】菜单,进入到账户详情页。

```
⑦ 说明详情页字段信息展示不脱敏,拥有管理员权限即可单独查看除密码外的所有账户信息。
```

身份管理服务公共云合集·EIAM 云身份 服务



账户信息

基本信息

账户核心信息,账户在创建和编辑时需要填写的基础内容。

其他信息

账户元数据,包括创建来源、时间、近期使用情况等。

已绑定账户

管理已绑定的三方账户,可以查看绑定信息。若用户希望更换绑定信息,管理员也可以操作解绑,允许用户重新绑定。

? 说明

由钉钉导入进来的账户,默认绑定钉钉 userld,且无法解绑。

查看权限

管理员可以查看在当前的授权策略下,当前账户可以访问哪些应用。

状态变更

在上方导航条右侧,可以对账户进行如下操作:

- 重置密码
- 禁用/启用账户
- 解锁账户
- 删除账户

若希望了解账户状态,请查看 账户生命周期。

修改密码

管理员可以修改指定账户的密码,密码需要符合复杂度设置。 亦可使用密码【自动生成】按钮,自动生成符合复杂度要求的密码。

若希望将新密码发给团队成员,可以一键复制账户名和密码,便于分享。

修改密码			×
• 密码			
请输入密码	Q	C	自动生成
长度至少10位,必须包含大写字母、小写字母、数字。 名、可在 登录 - 密码策略 中配置。	、特殊字	符、不	得包含账户
□ 复制账号密码			
	确定		取消
	muna		40/13

1.4.2.3. 账户生命周期



正常状态

账户创建后即处于正常状态,可正常使用所有功能。

禁用状态

当账户有风险或短期离职,可以将账户禁用。只能通过控制台或 OpenAPI 进行账户启用/禁用操作,禁用不会影响账户的任何数据。

处于禁用状态下的账户,任何功能都无法使用。

锁定状态

锁定

同一账户,5分钟内连续使用密码登录失败10次,会锁定5分钟。锁定期间将无法登录。

解锁

解锁的方式有两种:

- 等待 5 分钟自动解锁。
- 管理员在【账户】菜单中将账户解锁。

1.4.2.4. 组织管理

IDaaS 中可以进行企业树形组织架构管理,等同于钉钉中【部门】、AD 中【OU OrganizationalUnit 组织机构】。管理员可以将钉钉、AD 等现有体系中的组织架构树完整导 入进 IDaaS。

组织架构主要用于:

- 1. <u>查看</u>。与企业实际结构贴合,便于查看和管理。
- 2. 授权。IDaaS 允许对组织节点进行授权,授权后节点下所有账户均会拥有对应权限。
- 3. 回步。指定同步范围,将指定节点下的组织或账户同步出去,或由外部同步到目标节点下。

基本组织管理

请来到【账户】菜单。左侧会展示组织架构树,右侧展示组织的下属账户或子级组织。



请您点击选择左侧组织节点进行管理。默认会选中【根组织】,并在右侧展示根组织下的账户和组织列表。 在右侧切换到组织列表,对组织可以进行如下操作:

- 创建
- 编辑/移动
- 删除

创建/编辑/移动

点击【创建组织】按钮,弹出如下表单。只需选择 新组织所属的上级组织 并填写 名称,即可创建成功。

Q. 阿里z	5 IDaaS			~
注:分配账号	号归属的组织,	默认在当前节	点下创建。	
 APR APR - Rev (FAx) 				
• 组织名称				

进行名称编辑时,针对字段进行修改即可,进行组织移动时,选择要移动到的父组织。

删除组织

在删除组织时,若组织有下级组织或账户,默认无法删除。

若明确删除的影响范围,确认希望强制删除,可以勾选【强制删除子级组织和账户】,确定即可将当前节点及下属所有信息全部删除。通常用于误导入删除场景、测试转生 产数据清空场景等,删除无法恢复,请您谨慎操作。



账户 - 组织 关系

账户必须要归属于一个、且仅一个组织节点。 账户创建时可以指定其所属组织节点,后续允许变更。

1.4.2.5. 账户/组织同步



IDaaS 既可以作为可信身份信息来源,将数据分发给相关方;也可以作为桥梁,将不同体系中的账户、组织连接起来。

IDaaS 将同步分为两个方向:

- <u>入方向</u>:同步进入 IDaaS。
- **出方向**:由 IDaaS 同步到相关方。

两个方向可以串联起来,实现在 AD 或钉钉中的数据变更,通过 IDaaS 传递给所有相关方。

入方向同步

IDaaS 支持的入方向同步方式如下:

入方向同步方式	对接方	描述
从身份提供方同步	ldP 身份提供方	当前支持钉钉。操作参考: <mark>绑定钉钉</mark> 。 接下来会支持:AD、OpenLDAP、企业微信、飞书等常见身份提供方。
Developer API 开发对接	应用 - 自研应用	为了便于应用接入,IDaaS 提供了一套理解简单、接入容易的开发者 API,供自研应用调用。 详情请参考: <mark>应用开发 API 说明</mark> 。
OpenAPI 开发对接(暂不支持)	应用 - 云产品	IDaaS 开放账户管理 OpenAPI 供开发者调用,可用该系列接口批量导入账户。
SCIM 标准协议 (暂不支持)	应用 - 部分国际	部分国际应用支持 SCIM 协议(System for Cross-domain Identity Management,跨域身份 管理)。IDaaS 未来会支持 SCIM 协议直接对接。
懒加载(暂不支持)	多种	懒加载(Lazy Loading、JIT Provisioning)对接后,会随着用户的登录,逐步将每个账户同 步进入 IDaaS。

出方向同步

IDaaS 支持的出方向同步方式如下:

出方向同步方式	对接方	描述
---------	-----	----

由 IDaa5 推送	应用 - 自研	IDaaS 支持主动向应用按照 IDaaS 固定格式推送数据。 • 当前仅支持 IDaaS 自定义格式数据推送 • 暂不支持 SCIM 协议推送数据给应用 • 市场中部分应用提供了固定同步接口, IDaaS 会在未来预集成,可方便地一键配置使用
从 IDaaS 拉取(暂不支持)	应用 - 自研	当前版本未支持。 未来版本会支持:应用主动调用 Developer API,批量获取账户和组织信息,进行同步。
同步给身份提供方(暂不支持)	IDP 身份提供方	当前版本未支持。 未来版本会支持:钉钉、AD、OpenLDAP、企业微信、飞书等常见身份提供方。

1.4.3. 开通应用

1.4.3.1. 应用开通说明

应用是 IDaaS 中承载业务应用、系统、服务的载体。通过应用,可实现到应用的单点登录(SSO)以及和 IDaaS 应用之间的账户同步。

IDaaS 中将应用分为如下几个类型:

优先顺序	接入类型	类型说明
1	1. 应用市场	IDaaS 预集成的应用模板,快速开通使用,省时省事。会不断补充。
2	2. 标准协议	不在应用市场中,但支持标准 SAML、OIDC 等协议的三方应用。通过标准化配置即可使用。
3	3. 自研应用	不在应用市场中,且不支持标准协议,但可以按照 IDaaS 提供的标准研发对接的应用。
4	老旧兼容未来版本	针对上述方案都无法支持的应用,IDaaS 提供密码代填能力,安全存储密码,实现 SSO 的效果。

当您有应用希望接入 IDaaS,实现统一访问、统一账户管理时,请您按照下图流程判断应采用的接入类型。



应用市场

👎 🏟 🦊	× 🖬	aws	0	K	M	-
(-) 🗖 🧼			Ø	Ŵ	e	Ø

IDaaS 为市面常见的应用,提供了预集成模板,在应用市场中允许搜索开通,并快速配置单点登录和同步。

? 说明

说明:IDaaS 应用市场不直接开通或购买应用,仅提供 IDaaS 对应用的身份连接服务。您仍需要自行搭建或购买想使用的应用。

当您希望接入新应用时,应首先查看应用在市场中是否有预集成。使用预集成模板可以为您节省大量配置时间。 请前往【应用】菜单,点击【添加应用】,来到应用市场,搜索您希望接入的应用名称。

应用身份服务

云身份服务 / 庭用 / 添加应用		版本更新记录 IDaaS支持群 帮助文档
← 添加应用		
应用市场 标准协议 自研应用		
如果没有找到你想使用的应用,请告诉我们,我们将在 24	小时内联系您沟道需求,进行排期。	
搜索我的应用 Q		
▶ 阿里云角色SSO 永久免费	○ 阿里云用户SSO 永久免费	腾讯云用户SSO 限时免费 ☺
阿里云角色SSO应用模板,通过应用账户名方式生成 阿里云云角色名arn。	RAM用户SSO,用户自己选择账号名属性取值方式。 并支持自定义RAM辅助域名	腾讯云用户SSO应用模板,支持用户自己选择NamelD属 性取值生成方式。
SSO	SSO	\$\$O
添加应用	添加应用	添加证用
● 勝田元角色SSO 回封单质 ◎	後次元田户SSO 国时免费の	Salasforma
器讯云角色SSO应用模板,通过应用账户名方式生成 腾讯云角色Sarn。	华为云IAM用户SSO	Salesforce 作为全世界最知名的综合类 CRM SaaS 提供 商,拥有完善的云计算技术和经过专家设计的客户管理软 作。
SSO	SSO	SSO
添加应用	35.00位 <i>用</i>	湖泊加坡 用

? 说明

若未搜索到结果,希望您可以在 讨论区 中将接入需求提交给我们,我们会根据紧急性和重要性排期进行接入。与此同时,请您检查应用是否可以使用标准单点登录协议 接入。

1.4.3.3.2. 标准协议

企业身份管理体系有国际通用的、普遍使用的身份管理协议。成熟的企业软件,往往参照国际通用标准协议,便于其客户与自己的 ldP (在我们的语境中,ldP 就是 lDaaS) 进行集成。

IDaaS 允许任意支持标准协议的应用,通过配置对接单点登录。

云身份服务 / 应用 / 添加应用		版本更新记录	IDaaS支持群	帮助文档
← 添加应用				
应用市场 标准协议 自研应用				
若在应用市场中未找到目标应用。而该应用支持标准协议接 如何判断是否支持协议?	入,可通过标准协议,实现单点登录。			
 ▲ SAML 2.0 SAML 基于 XML协议, 使用音会亲言 (Assertion) 約 安全會場, 在現权方 (DaaS) 和助長方 (皿用) 之间 传递身份信息, 実現基于用适用域的单点登录。 ▲ SSD ▲ MIR用 	ODC ODC 4000 Connect 約時時, 0DC = (identity, Authentication) + 0Auth 2.0, Dass 使用 0DC 进 行分析试验的原始重要(SSO)。 SSO Automm			

使用标准协议的优势

对于应用而言,支持标准协议有以下价值:

- 更成熟。对标准身份协议的支持,是企业应用成熟的重要表征。
- 更通用。不锁定企业账号体系。对接一套标准协议,允许客户自行选择最适合的身份提供方。
- 更安全。自研协议几乎肯定存在安全问题。国际标准协议经由严格的发布流程,场景完整、安全有保障。

? 说明

对接标准协议仅需很短时间。若您是企业应用厂商,且希望对接标准,可以联系我们提供帮助。同时,我们会将您的企业应用上架到 IDaaS 应用市场中,获取精准的公众曝光。

IDaaS 支持的标准协议

标准协议名	说明
OIDC	发布于 2014 年,OIDC(OpenID Connect)协议在现代身份体系中具备最佳的配置集成体验和表现,其在 OAuth 2.0 授权协议基础上叠加了 基于 JWT 格式的 id_token,兼容认证和授权场景。
SAML 2.0	发布于 2005 年,SAML 2.0 仍是全世界最常见的单点登录协议,绝大部分成熟企业应用均支持 SAML 对接。由于历史原因,其底层基于 XML 实现,在一些边缘场景中适应性较差。
OAuth 2.0 未来版本	发布于 2012 年,OAuth 2.0(RFC 6749)是最通用的授权代理协议。协议中将授权(AS)和资源(RS)区分,具备轻便灵活的特点。常见微 信登录、钉钉扫码登录等,均使用 OAuth 2.0 协议实现。

|--|

您可以在搜索引擎或应用文档中,检索" {{应用名}} 单点登录 " 或" {{application_name}} SSO ",检查您希望接入的应用,是否支持单点登录标准协议。

若应用支持标准协议,您可以在 讨论区 中将接入需求提交给我们,我们将在很短的时间内,上架应用到应用市场中,便于您和后续客户的使用。

1.4.3.4. 3. 自研应用

企业常会有一系列自研应用,以支撑自己独特的业务流程。

管理员可以在 IDaaS 中添加自研应用,并参照 IDaaS 提供的对接文档,开发进行接入。

云身份服务 / 应用	1 / 添加应用	版本更新记录	IDaaS支持群	帮助文档
← 添加原	Z用			
应用市场	标准协议 自研应用			
IDaaS 为您的企	业自研应用开放接入能力。请了解如下三类递进的接入能力,并创建应用开始对接。			
添加自研应用	l			
[→ 登录統- 实现单点 请应用开	-: 单点登录接入 显示, 用户即可使用 (DaaS 账户登录业务应用, 访问控制可以在 IDaaS 中通过授权统一管理。 发人员参照《单点登录排入文码》,即可快速对接。			
L 账号统 实现账户 IDaaS 3	一: 账号同步接入 同步,却可实现账户管理一处排弦、允虻主攻、方使快速。 排述、入再个方向的账号同步,编回用并发人员参照(<mark>账户同步接入文档)</mark> ,确定方案,并始集成。			
	- 未来版本 1875文件, 歌调期待。 1884回。			

自研应用的接入层次

IDaaS 允许企业的自研应用身份体系与 IDaaS 进行三个层次的接入,我们建议您从上到下,依次检查对接需求:

接入层次	说明	价值
<u>第一层: 登录统一</u>	实现单点登录(SSO)。通过接入 OIDC 协议,配置应用账户和应用授权,允许 IDaaS 中的企业账户单点登录到应用中。 开发文档:自研应用接入单点登录。	员工一套账户,畅游所有应用。 统一授权、统一管理、统一行为审计。
<u>第二层:账户统一</u>	实现账户同步。通过对接 IDaaS 同步接口,打通身份孤岛。 开发文档:自研应用接入账户同步。	实现账户管理一处修改、处处生效,管理方 便快捷,极大减少低效工作。
第三层: 权限统一 (暂不支持)	实现权限托管。通过对接 IDaa5 标准灵活的 RBAC 模型,将应用内角色、菜单、功能等权限托 管在 IDaaS 中,并统一授权管理。	实现对访问控制的细粒度管理,统一统筹企 业内信息访问的权限内容。 减少自研应用复杂高昂的权限系统研发成 本。

1.4.4. 应用管理

1.4.4.1. 基本配置

每个应用都有一些跨功能、或与功能平行的配置,统一在通用配置中进行管理。

当前版本中,	管理员可以开启/关闭接口访问状态,	并对密钥进行轮转。

	±400 € 400 ×				Q	商用	Ξŧ	ICP \$88	22	立 35	Ð	53	¢, А	0	⊕ ≈	× ()	ł
云身份服务	元 月 代開発 / 泉均 / 1	NORTH / PERSONAL										Ded	2010	iDauS (\$)	907 N	R0.72.68	
快速入门	← 阿里云用	户 SSO													8/0	624	
身份错误方	通用配置 登录	的间 电中国步	API 开放														
92.00	Davis 九星周开坡 SSO.	电外带能力输口,使用用	REDRIG BUTS	dient.id, dient.sec	ret Milliand												
88	dient.id	aga microst =1 af															
9.R		+ 1850 client_secret															
Ва	基础信息																8
个性化	< 6/80 0	$\exp(r(\alpha \mathbf{L}^{\mathbf{n}} _{1}))$	$-2\pi V = 0$														1
	692.437	网络白刺															
	* 5008#	阿里亚印哈 SSO															
	896899	(为 PAGAFG 悟点、大小不服 曲例7.物理時,	22 IME,													

接口访问

IDaaS 对每个应用,均可配置开启一系列接口,供不同功能场景来调用。包含:

- 基于 OIDC 协议的单点登录相关接口
- 账户同步相关接口
- 权限托管相关接口 未来版本

这些场景接口,均需共用这里的 client_id 和 client_secret,获取到 access_token 访问令牌后,才能获权调用。

? 说明

```
提示:想要获取具备对应接口权限的 access_token,您不仅需要在此开启应用接口访问,还需确保每个功能的正确配置。例:若希望调用同步接口,您需要确保【账户
同步】中对应功能同样处于启用状态。
```

当前版本中,管理员可以开启/关闭接口访问状态,并对密钥进行轮转。

密钥轮转

每个应用均支持自定义周期的密钥轮转。

为了支持最灵活的密钥轮转,IDaaS 中每个应用可最多拥有两个 client_secret ,同时至少有一个处于启用状态。

在轮转并行期间,您可以保持两套 client_secret 均处于有效状态,直到您确定旧有 client_secret 已不再使用,即可安全删除。

IDaaS 为应用开放 SSO、同步等能力接口,使用前需启用接口访问,通过下方 client_id, client_secret 进行接口鉴权。



出于安全因素考量,我们推荐每3个月(或按照具体合规要求)进行一次密钥轮转。过程如下:

- 1. 当需要轮转时,创建新的 client_secret。
- 2. 应用对接,将新的 client_secret 替换老的 client_secret。
- 3. 禁用老 client_secret。在禁用时,会提示当前 client_secret 最近一次的使用时间,您可再次确认已无人使用后,完成禁用。
- 4. 验证应用运行是否受到影响。
- 5. 确认无影响后,可删除历史 client_secret。

基础信息

字段名	说明
应用 ID	应用资源标识 ID。暂仅供参考使用。不可更改。
创建来源	应用创建时使用的创建模板。不可更改。 取值有三种:应用模板/标准协议/自研应用。
应用名称	应用显示名称。
应用图标	应用显示图标。必须为 PNG/JPG 格式,大小不超过 1 MB。建议使用 256*256 像素方形图标。

1.4.4.2. 单点登录通用说明

若您希望实现单点登录(SSO),首先需要完成单点登录配置。

本篇文档说明以下通用的单点登录配置,每个应用均需选择:

- <u>单点登录状态</u>
- 应用账户
- 授权范围

详细配置步骤,针对不同应用模板类型,请参考文档:

应用模板类型	协议	参考文档

应用市场预集成模板	SAML 2.0	3. 创建应用
标准协议 - SAML	SAML 2.0	SAML 2.0 SSO 配置
标准协议 - OIDC	OIDC	OIDC SSO 配置
自研应用	OIDC	自研应用 SSO 配置

单点登录状态

应用开通后,所有功能均处于禁用状态。为了配置方便,前端会自动将单点登录状态变更到【启用】,您仍需要点击保存,状态才会真正变更。

关闭单点登录功能的应用,将不会显示在用户门户中。

授权范围

规范应用的可使用人群范围,有以下两个选项:

选项	说明
全员可访问	在 IDaaS 中的所有账户,均可访问该应用,无需额外授权。
手动授权	需要在应用的【应用授权】标签中,手动分配可访问应用的组织和账户。详情参考 应用授权。

1.4.4.3. SAML 2.0 SSO 配置

1.4.4.3.1. SAML 2.0 SSO 配置

单点登录流程需要 IDaaS 与应用之间进行交互,所以需要在两端进行配置。

当前文档以 SAML 2.0 标准协议为例进行配置说明。

```
    ⑦ 说明
    若您希望了解 IDaaS 中支持的 SSO 协议,请前往: 2. 标准协议。
```

IDaaS 侧配置

快捷方式:上传应用配置文件

部分应用在 SSO 配置页面,能够将配置信息 met adat a 一键下载,并在 IDaaS 中上传;或提供公开接口,允许 IDaaS 将配置信息拉取过来。

上传应用 metadata 或输入应用 metadata 地址: 解析

应用 metadata 为应用侧生成的 SSO 配置文件。 若已有 metadata,直接导入,可自动填充下方 SSO 参数,简单快捷。

IDaaS 即可获取到配置 SSO 的所有信息,预填充进表单。无需管理员手动配置,确认保存即可完成。

IDaaS 侧配置字段说明

	字段	说明	举例
	<u>单点登录地址</u> ACS URL	应用的 SAML SSO 核心地址,与 IDaaS 交互 处理单点登录请求。	https://signin.example.com/1021*****48 13/saml/SSO
基本配置(必填)	<u>应用唯一标识</u> SP Entity ID	应用在 IDaa5 中的标识,通常在应用侧获 取,格式通常为应用 URI。若应用侧没有要 求,直接复用单点登录地址即可。	https://signin.example.com/1021*****48 13/saml/SSO
	应用账户	SAML 协议中将应用账户称为 NamelD。请 参考:SAML 应用账户配置。	选择:使用 IDaaS 账户名(Username)

	授权范围	请参考:单点登录通用说明。	选择: 全员可访问
	<u>默认跳转地址</u> Default RelayState	IDP 发起 SSO 登录成功后,应用自动跳转的 地址。在 SAML Response 中会在 RelayState 参数中传递,应用读取后实现跳 转。	应用内二级菜单页。 http://www.example.com/menu/mana ge
	NameID 格式NameIDFormat	SAML Response 中指定账户标识 NamelD 字段格式。很多应用不对 NamelDFormat 进行处理,所以一般无需修改。	选择:1.0 Unspecified
	<u>Binding 格式</u> Binding	Binding 字段指定了双方请求的方式。目前 只支持 Redirect - POST , 一般无需修改。	选择:Redirect - POST
高级配置(选填)	<u>是否对断言签名</u> Sign Assertion	IDaaS 会为所有 SAML 请求签名,暂不支持 修改。	-
	<u>签名算法</u> Signing Algorithm	签名使用的非对称算法,当前仅支持 RSA- SHA256 算法,一般无需修改。	选择:RSA-SHA256
	<u>账户字段</u> Attribute Statements	在 SAML Response 中,可以将额外用户字 段(例如邮箱、显示名等)返回给应用解 析。参考 SAML Attribute Statements 值填 写规范。	-
	<u>SS0发起方</u>	用户访问由应用发起,还是支持门户发起。	只允许应用发起
	登录发起地址	若【SSO发起方】设置为【支持门户和应用 发起】, 可填写登录发起地址。门户页访问 应用时, IDaaS 会跳转到本地址, 应即刻自 动向 IDaaS 发起 SAMLRequest 登录请求。	-

应用侧配置

快捷方式:上传 IDaaS 配置文件

为了便于应用侧配置,IDaaS 支持将配置信息一键下载。

应用配置信息

IdP 元数据	https://inkqc4cn.dev.aliyunidaas.com/api/v2/app_mgf2jgmpcexwy2wn245mluusa/sami2/meta / 全下数
IdP Metadata	若应用支持 metadata 配置信息上传/规取,可以节鉴大量配置步骤,请在应用 550 配置中寻找最否有 metadata 工作能力。
IdP 唯一标识	https://inkqc4cn.dev.aliyunidaas.com/api/v2/app_mgf2jqmpcexwy2wnz45mluusa/sami2/meta び
IdP Entity ID	IDaaS 在应用中的标识,需要将值填写在应用单点登录配置中。
IdP SSO 地址	https://inkqc4cn.dev.allyunidaas.com/login/app/app_migf2jqmpcexwy2wnz45mluusa/sami2/sso Ø
IdP Sign-in URL	SAML 协议支持 SP 发起单点登录,可能需要填写此地站在应用配置中,由 DaaS 提供,可以直接访问该地址,进行应用登录。
单点退出地址	智不变持
SLO URL	SAML 协议支持单点退出,可能需要填写此地址在应用配置中。由 印aaS 提供。
公钥证书 Certificate	BEGIN CERTIFICATE MIEFTCCA/24wiF8/giSFSHid2DMIDJB9/DDY28R4/MA0GCSqGSIb3DQEBCwUA MIGSMScwu/DVTVQGDDB5h-HBRWinZJacWTMr2V4G3xyd256NDVTDHV1CZExKTA
	下载.cer证书后导入至 salesforce "身份提供商证书"字段中。
	G复制证书内容 业下载证书.cer文件

部分应用配置 SSO 时,支持 met adata 信息上传。可将 IDaaS 配置文件上传,或将 met adata 地址填写至应用侧。无需手动配置,即可完成对接。

应用侧配置字段说明

应用侧需要配置 IDaaS 的信息,完成对接。

IDaaS 会在单点登录配置页中,集中展示所有应用侧可能需要使用的信息,方便配置。具体字段说明如下:

字段名称	说明	示例
<u>IDP 唯一标识</u> IDP Entity ID	IDaaS 在应用中的标识。可能需要将值填写在应用侧 SSO 配置中。	https://xxxxx.aliyunidaas.com
IDP 发起 SSO 地址 IDP-init SSO URL	SAML 协议支持 SP 发起单点登录,可能需要填写此地址在应 用配置中。	https://xxxx.aliyunidaas.com.cn/saml/idp/saml1
<u>单点退出地址</u> 未来版本 SLO URL	SAML 协议支持单点登出。若希望实现此功能,需要填写此地 址在应用配置中。	-

<u>公钥证书</u> Certificate	IDaaS 发送的单点登录结果,会自动携带一个电子签名。应 用可以使用这里的公钥,对结果验签,确认结果是 IDaaS 发 出,确保安全。	BEGIN CERTIFICAT E MIIDEjCCAfqgAwiBAgIHAYnNmX60izANBgkqhkiG9w0BAQs FADApMRowGAYDVQQD
----------------------------	--	--

1.4.4.3.2. SAML 应用账户配置

SAML 在进行单点登录时,会将用户身份信息传递于 SAMLResponse 的 NamelD 字段中,或存在与其他字段。 配置应用账户,即是配置使用哪类值,当做账户的身份标识信息。

最常用的设定为 IDaaS【账户名】或 IDaaS【邮箱】。

单点登录配置项

应用账户 Name ID	IDaaS 账户 / 账户名 へ			
itanic ib	IDaaS 账户	>	✓ 账户名	
授权范围	应用账户	>	邮箱	\sim
	优先应用账户	>		
显示高级配置 ✔ 跳转地址、签名、额外账户	表达式			

您可以在如下四种规则中进行选择:

选项	说明	
	指定当前应用单点登录时,使用 IDaaS 账户信息作为应用身份标识。选择此项,需确保进行单点登录的账户,在 IDaaS 和应用中用户名完全一致,否则 会导致失败,甚至账户错乱。	
1. <u>IDaaS 账户</u>	这是最常用的配置。避免为每个 IDaaS 账户单独配置应用账户,省时省力。	
	可选子选项有两个:	
	• IDaaS 账户名(Username)	
	● I <u>DaaS 邮箱(Email)</u>	
	管理员需要指定当前应用 SSO 时每个 IDaaS 账户使用的应用账户。未指定,则无法单点登录。	
	例如:IDaaS 中有账户名为 test_user,希望登录应用为 admin,可通过手动配置完成。配置方式参考 SAML 应用账户配置。	
<u>2.应用账户</u>	若应用使用人数较少,可使用此配置,获得最大灵活度。	
	可选子选项有一个:	
	 ● <u>应用账户</u> 	
	结合了前两个选项的优点。允许管理员手动配置应用账户,并优先使用。配置方式参考 SAML 应用账户配置。当未配置应用账户时,默认使用 IDaaS 身 份标识信息,作为兜底方案。	
<u>3.优先应用账户</u>	可选子选项有两个:	
	● <u>次选 IDaa5 账户名(Username)</u>	
	● 次选 IDaaS 邮箱 (Email)	
	若应用账户具备特定规则,可以配置表达式。	
4.表达式	例如,应用将每个账户的邮箱前缀作为账户名。	
	无可选子选项。表达式较为复杂,请咨询 IDaaS 团队提供配置。	
	<u>リ潮入农込式规则。</u>	

手动添加应用账户

若在单点登录表单的 应用账户 选项中,选择 应用账户 或 优先应用账户 ,则可以手动配置不同账户在访问该应用时的身份。

点击【添加应用账户】,弹出表单。

添加应用账户	×
按账户名搜索 ∨ test	
已选	
test	账户访问应用时所使身份。例如 admin,manager等
	-0.42 Y022

在表单上方搜索找到 IDaaS 账户,点选后,在下方为其添加应用账户,举例:admin、root 、手机号码、zhangsan 等。保存即完成。

🥐 说明

您同时可以为一个 IDaaS 账户设置多个应用账户。在发起单点登录时,用户可选择其中一个进行登录。

1.4.4.3.3. SAML Attribute Statements 值填写规范

类型	填写值	说明
	<u>user.username</u>	账户名
	<u>user.displayName</u>	显示名称
亦是	<u>user.phone</u>	手机号
交重 	<u>user.email</u>	邮箱
	<u>user.status</u>	用户状态,取值:enabled/disabled
	appUser.username	应用账户
常量	使用 "" 英文双引号, 引号中填写常量。	
表达式	高级功能,可以灵活地将值进行拼接、变化。 具体功能请咨询 IDaaS 团队。	

1.4.4.4. OIDC SSO 配置

1.4.4.4.1. OIDC SSO 配置

当前文档以 OIDC 标准协议为例进行单点登录配置说明。

```
    ⑦ 说明
    如您希望了解 IDaaS 中支持的 SSO 协议,请前往: 2.标准协议。
```

IDaaS 对 OIDC 不同模式的支持

```
您可在如下模式中多选:
```

模式	支持说明
<u>客户量模式</u> client_credentials	IDaaS 使用 OIDC 客户端模式,允许应用的 client_id, client_secret 来到 IDaaS 换取服务端令牌,调用 IDaaS 应用开放的 Developer API。
	客户端模式无需勾选,若应用【通用配置 - 接口访问】启用,则模式开启。
<u>授权码模式</u> authorization_code	IDaaS 中 OIDC 应用最普适的登录模式。应用将登录委托给 IDaaS,并解析 IDaaS 返回的 id_token,完成登录校验。

全牌刷新模式 refresh_token	支持使用 refresh_token 对 access_token、id_token 进行刷新的模式,以延长会话有效时间。通常与授权码模式一起使用。
<u>设备模式</u> device	设备模式常用于非 B/S 架构的应用接入。当设备不便于直接展示 IDaaS 登录页时,允许用户使用浏览器辅助完成登录流程。

常规的 B/S 网页端企业应用,我们建议您勾选 授权码 + 令牌刷新 模式。

非 B/S 应用,建议勾选 设备 + 令牌刷新 模式。

? 说明

提示:OIDC 其他模式 IDaaS 暂不支持,如有需求,请前往 <mark>讨论区</mark> 告诉我们。

IDaaS 侧配置

	字段	说明	举例
	模式	为应用选择要使用的模式。	多选: 授权码模式 多选: 令牌刷新模式
基本配置(必填)	登录 Redirect URIs	Redirect URI 白名单。应用在请求登录时会携带 redirect_uri 参数,该值 需要在白名单中,IDaaS 才会在认证完成后发起跳转。	http://www.example.com/oidc /sso http://www.example.com/oidc /sso2
	授权范围	请参考:单点登录通用说明。	选择:全员可访问
高级配置(选填)	<u>用户信息范围</u> <u>SCODES</u>	 用户登录后,使用用户信息端点可以获取到的已登录用户信息。 openid email phone profile 	多选: openid 多选: email 多选: profile
	PKCE	【授权模式】中勾选【授权码模式】时可选。启用后,授权码模式会使用 更安全的 PKCE 扩展流程。	默认不勾选
	<u>Code Challenge</u> 生成方式	开启【PKCE】后可选。PKCE 扩展中 Code Challenge 的生成方式。若未 勾选开启 PKCE,则不会显示。	-
	<u>access_token</u> 有效期	access_token 用于请求 IDaaS 接口。默认 2 小时有效。过期后需要使用 refresh_token 刷新,或重新登录。	2 小时
	i <u>d_token</u> 有效期	id_token 用于鉴别用户身份,JWT 格式,允许应用使用公钥自行验证用户 身份。过期后需要使用 refresh_token 刷新,或重新登录。 id_token 格式请参考:IDaaS 中的各类 token。	10 小时
	<u>refresh_token</u> 有效期	用于获取新的 access_token 和 id_token。refresh_token 过期后,用户 需要重新登录。	30 天
	<u>扩展 id_token</u> 字段	可以通过扩展 id_token 中的 payload 字段,将用户的非敏感基本信息返 回,以免需要反复调用用户信息端点。参考 OIDC id_token 扩展值填写规 范。 注意:payload 中添加的字段公开可见,请按需使用。	-
	<u>id_token</u> 签名算法	id_token 签名使用的非对称算法,当前仅支持 RSA-SHA256 算法。	RSA-SHA256
	<u>SSO 发起方</u>	用户访问由应用发起,还是支持门户发起	只允许应用发起

登录发起地址	若【SSO 发起方】设置为【支持门户和应用发起】,可填写登录发起地 址,即 IDaa5 发起 SSO 请求访问的应用地址。该地址接收到请求,应即 刻转向 IDaa5 / authorize 授权端口。	-
--------	--	---

应用侧配置

OIDC 协议允许应用侧通过一系列 IDaaS 开放的标准接口,完成登录认证整套流程。

开放的接口说明如下:

字段名	说明	示例
lssuer	id_token 中标记令牌来源的字段。同时是下述接口的 baseUrl。	https://xxxxx.aliyunidaas.com.cn/oidc1
<u>发现端点</u> Discovery	用于获取当前 IDaaS 支持的各端点信息和支持的模式、参数信息,可公开 访问。	https://xxxxx.aliyunidaas.com.cn/oidc1/.well-known/openid- configuration
授权端点 Authorization	应用发起单点登录的地址。	https://xxxx.aliyunidaas.com.cn/oidc/authorize
<mark>全脾端点</mark> Token	应用在单点登录过程中,拿到 授权码 code 后,从后端发去换取 token 的 接口地址。	https://xxxx.aliyunidaas.com.cn/oidc/token
<u>验签公钥端点</u> JWKS	用于验证 id_token、完成 SSO 流程的公钥端点。公钥暂不支持轮转。	https://xxxx.aliyunidaas.com.cn/oidc1/jwks
<u>用户信息端点</u> Userinfo	登录后,使用 access_token 获取用户基本信息的端点。	https://xxxx.aliyunidaas.com.cn/oidc1/userinfo
<u>退出端点</u> (暂不支持) SLO	用户注销 IDaaS 主登录态。	-

1.4.4.4.2. OIDC id_token 扩展值填写规范

类型	填写值	说明
变量	<u>user.username</u>	账户名
	<u>user.displayName</u>	显示名称
	<u>user.phone</u>	手机号,不包含国际区号
	<u>user.email</u>	邮箱
	<u>user.status</u>	用户状态,取值:enabled/disabled
常量	使用 "" 英文双引号,引号中填写常量。	
表达式	高级功能,可以灵活地将值进行拼接、变化。 具体功能请咨询 IDaaS 团队。	

1.4.4.5. 自研应用 SSO 配置

IDaaS 支持企业自研应用接入,实现单点登录。

为了应用接入的简易型和安全性,自然应用接入需要通过 OIDC 授权码模式。为了简化理解、便于上手,IDaaS 对配置项进行了极大程度的简化。

IDaaS 侧配置

在 IDaaS 侧,仅需将应用处理单点登录请求的地址填写到 【登录 Redirect URIs】中,其他选项保持默认,即可完成基本配置。

	字段	说明	举例
基本配置(必填)	登录 Redirect URI	Redirect URI 白名单。应用在请求登录时会 携带 redirect_uri 参数,该值需要在白名单 中,IDaaS 才会在认证完成后发起跳转。	http://www.example.com/oidc/sso http://www.example.com/oidc/sso2
	授权范围	请参考:单点登录通用说明。	选择:全员可访问
高级配置(选填)	<u>用户信息范围</u> SCODES	 用户登录后,使用用户信息端点可以获取到 的已登录用户信息。 openid email phone profile 	多选: openid 多选: email 多选: profile
	access_token 有效期	access_token 用于请求 IDaaS 接口。默认 2 小时有效。过期后需要使用 refresh_token 刷新,或重新登录。	2 小时
	<u>id_token</u> 有效期	id_token 用于鉴别用户身份, JWT 格式, 允 许应用使用公钥自行验证用户身份。过期后 需要使用 refresh_token 刷新, 或重新登 录。 id_token 格式请参考: IDaaS 中的各类 token。	10 小时
	refresh_token 有效期	用于获取新的 access_token 和 id_token。 refresh_token 过期后,用户需要重新登 录。	30 天
	扩展 id_token 字段	可以通过扩展 id_token 中的 payload 字 段,将用户的非敏感基本信息返回,以免需 要反复调用用户信息端点。注意: payload 中添加的字段公开可见,请按需使用。	-
	<u>SS0 发起方</u>	OIDC 协议天然支持应用发起。 若选择 支持门户和应用发起 ,则必须填 写下个字段:门户登录发起地址。	支持门户和应用发起
	登录发起地址	IDaaS 发起 SSO 请求时,访问的应用地址。 该地址接收到请求,应即刻发起 /authorize 授权端口请求。	http://www.example.com/oidc/login

应用侧配置

OIDC 协议允许应用侧通过一系列 IDaaS 开放的标准接口,完成登录认证整套流程。

开放的接口说明如下:

字段名	说明	示例
Issuer	id_token 中标记令牌来源的字段。同时是下述接口的 baseUrl。	https://xxxxx.aliyunidaas.com.cn/oidc1
<mark>发现端点</mark> Discovery	用于获取当前 IDaaS 支持的各端点信息和支持的模式、参数 信息,可公开访问。	https://xxxxx.aliyunidaas.com.cn/oidc1/.well- known/openid-configuration
授权端点 Authorization	应用发起单点登录的地址。	https://xxxxx.aliyunidaas.com.cn/oidc/authorize
<u>令脾端点</u> Token	应用在单点登录过程中,拿到 授权码 code 后,从后端发去 换取 token 的接口地址。	https://xxxxx.aliyunidaas.com.cn/oauth2/token

令脾品销端点 Revocation	将已生效的特定令牌注销掉。	https://xxxx.aliyunidaas.com.cn/oauth2/revoke
<u>验签公钥端点</u> JWKS	用于验证 id_token、完成 SSO 流程的公钥端点。公钥可能会 轮转。	https://xxxxx.aliyunidaas.com.cn/oidc1/slo
<u>用户信息端点</u> Userinfo	登录后,使用 access_token 获取用户基本信息的端点。	https://xxxxx.aliyunidaas.com.cn/oidc1/userinfo
退出鐵点 SLO	用户注销 IDaaS 主登录态。	-

对接详情请参考文档: 自研应用接入 SSO。

1.4.4.6. 高级:账户字段表达式

基础说明

IDaaS 內置了表达式引擎,在 SAML和 OIDC 应用中,支持使用高级表达式,向返回信息中添加新的参数。当目标应用需接受额外参数,且参数需要进行某种转化、拼接、判 断时,可使用表达式实现。 与此类似,可以使用同样防范,在配置与身份提供方间同步的字段映射时,也可使用表达式实现字段值自定义赋值。

+

本篇文档下方列有常见示例,帮助快速理解使用场景和方法。

full_phone

以 OIDC 为例,在 SSO 配置中,支持扩展返回的 id_token 信息。在扩展值中,可填写高级表达式,以达成特定处理目标。

扩展 id_token

Join("-", user.phoneRegion, user.phone)

可以通过扩展 id_token 中的 payload 字段,将用户的非敏感基本信息返回,便于操作。注意:payload 中添加的字段公开可见,请按需使用。

表达式分为两部分:

1. 模型,包含 User (对应 IDaaS 账户)和 AppUser (对应 应用账户)两种。

2. <u>函数</u>,代表执行逻辑关系。

模型说明

1. User

下列字段在 IDaaS 的 User 模型中, 可使用类似 user.username 、 user.lockExpireTime 的引用方式。

属性	说明
username	用户名
displayName	用户显示名
passwordSet	密码是否已设置
phoneRegion	手机地区编号,示例:中国区号为 "86",不带 "00" 或 "+"
phoneNumber	手机号码
email	邮箱
userSourceT ype	来源类型,取值为: build_in、ding_talk、ad、ldap、idp_auto_build
userSourceld	来源ID
status	用户状态,取值为:enabled、disabled
accountExpireTime	账户过期时间,UNIX纪元时间,单位毫秒
registerTime	用户注册时间,UNIX纪元时间,单位毫秒

身份管理服务公共云合集·EIAM 云身份 服务

lockExpireTime	锁定过期时间,UNIX纪元时间,单位毫秒
updateTime	最近一次更新时间,UNIX纪元时间,单位毫秒
description	描述

2. App User

下列字段在 IDaaS 的 AppUser 模型中,可使用类似 appUser.username 引用方式。

属性	说明
username	应用账号用户名

3. IdP User

ldP User 模型应用于与身份提供方进行同步时,举例:钉钉的办公地点字段: idpuser.work_place 。

具体字段请查看对应身份提供方文档,例如钉钉的钉钉帮助文档-用户详情。

函数说明

以下为我们开放的常用函数及说明:

函数名	函数定义	说明
Append	Append(str1, str2,, strn)	拼接输入参数为新的字符串,等于 str1+str2+
Join	Join(source1, source2,, sourceN, separator)	将多个源值拼接为一个字符串,源值间用分隔符分隔。
<u>Coalesce</u>	Coalesce(source1, source2,, sourceN, defaultValue)	返回输入参数中第一个非空参数,若参数都为空,则返回null,其中空指非 null 且参数长度大 于 0。
IFE	IFF(condition, whenTrue, whenFalse)	三目运算。根据condition的结果返回不同的值,为 true 时返回whenTrue,为 false 时返回 whenFalse。
<u>IsNull</u>	IsNull(value)	当 value 为 null 即缺失时,输出为 true。
IsNullOrEmpty	IsNullOrEmpty(value)	当 value 为 null 或空字符串时,输出为 true。
Now	Now()	返回表示当前 UTC DateTime 的字符串,格式为 yyyy-MM-dd'T'HH:mm:ssXXX
<u>StringReplace</u>	StringReplace("hello \$VariableName", VariableName, ReplaceString)	普通字符串替换。
<u>Trim</u>	Trim(source)	去除源值字符串前后的空白字符。
<u>ToLower</u> <u>ToUpper</u>	ToLower(source) ToUpper(source)	字符串变为全大写或全小写。
<u>Substring</u>	Substring(source, fromIndex, endIndex)	返回字符串的子字符串,即子字符串下标地址为 [fromindex, endindex]。
SubstringBefore	SubstringBefore(source, subString)	返回 subString 之前的字符串。

参考示例

效果	表达式示例
取用户名,拼接固定 "@example.com"。	Append(user.username, "@example.com")
当邮箱不为空,返回邮箱。 当邮箱为空时,取手机号。	Coalesce(user.email, user.phoneNumber)

当手机号为空时,默认填写固定手机号。	IFF(IsNullOrEmpty(user.phoneNumber), "1888888****", user.phoneNumber)
将手机号地区和手机号以 - 拼接。	Join(user.phoneRegion, user.phoneNumber, "-")
返回包含显示名的自定义欢迎信息。	StringReplace("hello \$DisplayName", "\$DisplayName", user.displayName)
将手机号中间四位用 * 脱敏返回。	Append(SubString(user.phoneNumber, 0, 4), "****", SubString(user.phoneNumber, 8, 10))
提取邮箱中的用户名。	SubstringBefore(user.email, "@")

1.4.4.7. 应用授权

应用授权用于指定哪些组织或账户具备访问权限。

没有权限的账户,将无法访问当前应用。

? 说明

```
前提:IDaaS 应用单点登录配置中,可设置该应用为【全员可访问】。该选项下,无需配置应用授权,且手动授权无效。若需指定授权范围,请将该配置默认为【手动
授权】。
```

管理授权

管理员可来到【应用】菜单,点击待操作应用名称,选择【登录访问】-【授权】标签查看应用的授权关系,并进行添加授权、取消授权。

🥐 说明

```
当应用授权给组织后,组织内所有账户均会拥有权限,但 IDaaS 不会单独记录应用到账户的授权关系。 您可以前往【账户】【账户详情】【查看权限】,确认账户是否
拥有特定权限。
```

云身份服务 / 应用 / 酒	加应用 / SAML协议	版本更新记录 IDaaS支持群 帮助文档
← SAML协	议	抽用应用
通用配置 单点	登录 账户同步	
单点登录 应用账	户 授权	
添加授权 账户	◇ 技账户名援索 ◇ 请输入	
主体	主体类型	操作
test	死亡/20	取消授权
11 批量取消		毎页显示: 20 > 共1条数器 < 上一页 1 下一页 >

添加授权

点击【添加授权】,弹出表单。

质加应用授权	×
添加应用授权后, 被授权方将可以访问应用。	
<u>账户</u> 组织	
按账户名提案 > 请输入	
已选	
₩° ✓	清空
test	×
	保存授权 取消

在表单上方搜索找到 IDaaS 组织或账户, 点选后, 会出现在下方列表中供确认。

确认无误,即可确认添加。

1.4.4.8. 账户同步 - IDaaS 同步到应用

IDaaS 支持与应用之间的组织/账户双向同步。具体支持方式请参考:账户/组织同步。 IDaaS 允许将 IDaaS 中账户一次性同步给应用,也支持即时将增量变更进行通知。

云身份服务 / 应用 / 添加应用 / OIDC 应用 ← OIDC 应用 通用配置 登录访问 账户同步 API 开放 同步范围设定 ~ 保存 IDaaS 同步到应用 已禁用 🔵 请来到【账户同步】页面,开启同步功能,并配置 同步范围。 设定同步范围后,应用只能获取到 IDaaS 指定节点下的组织/账户信息。 推送配置 请来到【同步到应用】标签。 IDaaS 推送到应用
 論登公钥講
 https://pra-eiam-api-cn-hangzhou.aliyun-inc.com/v2/idaas_wkeft

 1471gugy(anii/provisioning/jwks の
 の

 点
 请点开链接,获取公钥信息,可以通过程序调用公钥端点,动态获取。
 出口 IP 112.124.239.96/27 び 若您的网络有请求 IP 限制,请将 IDaaS 的出口 IP 列表加入您的白名单中。 * 同步接收地 https://... 请输入您接收同步请求的地址,我们将向该地址发送请求信息。 址 是否加密 型务数据加密 若勾选,业务数据将使用加解密密切加密后传输。详情参考接收 (DaaS 同步事件。) AES256加密密钥,Hex编码格式。您可以指定加解密钥,或自动由 IDaaS 生成。 是否同步密码 🗌 同步密码 一 勾选是,则会在特定事件的数据中传递明文密码。 若同时勾选加密,则密码会和业务数据一起加密传输。 □ 账户解锁 🗌 账户移动 □ 30 5000 金號 取消全选 需要订阅对应的账户变更事件,才会触发事件回调,默认全部订阅,可随时调整。 事件类型定义请参考: IDaaS 同步到应用。

保存 测试连接 ⑦ ─镭推送 ⑦

首先请进行基本的推送配置,字段说明如下:

字段名	说明	示例
同步范围	将指定 IDaaS 组织机构下的主体变更进行推送,且通过接口只能获取到该组织机构下的数据。	选择:阿里云 IDaaS
验签公钥端点	同步请求会携带签名,接收方需要从 IDaaS 获取到公钥信息,并对同步请求进行验证。	-
出口 IP	请将 IDaaS 出口 IP 在您的安全设置中加白,保障 IDaaS 请求可顺利抵达接收方。	
同步接收地址	填写您接收同步请求的地址。 该地址需要按照开发文档,实现包括测试链接、接收账户、接收组织等一系列能力。详情参考 开发文档 - 账户同步 - 由 IDaaS 推送。	http://www.example.com/accounts/pr ovision
是否加密	若勾选是,业务数据将使用加解密密钥加密后传输。当数据需要从公网传输时,为了保障数据 传输安全,强烈建议开启。	选择:否
加解密钥	用于业务数据加密的密钥。 可由 IDaaS 生成,也可自行生成填写进来。	2fdc67ca538cc9500bcad6518390feb937 b58e9102b00bffb30a292112fdf626
是否同步密码	 勾选是,则会在特定事件的数据中传递明文密码,事件包括: 创建账户 密码变更(修改密码、重置密码等) 若同时勾选了业务数据加密,则密码会和业务数据一起加密传输。 	选择:否

配置了数据推送后,还可以选择性地订阅希望关注的变更事件,获取即时变更推送。

回调事件	□ 账户创建	组织机构创建
	□ 账户删除	4 组织机构删除
	账户基础信息更新	修改组织机构基础信息
	账户密码更新	□ 组织机构下移入账户
	账户禁用	□ 组织机构下移出账户
	账户启用	组织机构更新父组织
	账户锁定	
	账户解锁	
	账户变更组织机构	
	全选 取消全选 需要订阅对应的账户变更事	件,才会触发事件回调。默认全部订阅,可随时调整。
	事件类型定义请参考: 开发	文档 - 账户同步 - 由 IDaaS 推送 。

IDaaS 中定义了十余种账户/组织变更事件,分为增量事件和全量事件。详情参考 通讯录事件。 配置完成后,在同步功能启用状态下,您可以:

- 测试连接 , 验证连接正确、网络通顺、请求能正确处理。
- 一键推送 , 尝试发起全量同步。

 保存
 測试连接 ⑦
 一键推送 ⑦

为正确接收 IDaaS 发出的事件请求,您需要先对照 账户同步接入概述 完成对接开发。

1.4.4.9. 账户同步 - 应用同步给 IDaaS

企业可能希望使用应用作为账号管理源,并将信息即时同步给 IDaaS。

具体支持方式请参考:账户/组织同步。

IDaaS 对企业的应用开发者开放 API 供调用,以实现账户/组织信息的导入和同步,详情请参考 应用 API 开放。

1.4.4.10. 应用 API 开放

IDaaS 为应用开发者开放应用 Developer API 供调用。

目前可借此实现账户/组织同步到 IDaaS, 实现新员工入职、离职、转岗等生命周期管理。

IDaaS 管理员拥有应用管理的最高权限,可以指定应用的 API 开放与否、开放范围。

开放 API

可在【API开放】标签中为指定应用开启/关闭接口调用。

通用配置 登录访问 账户同步 API 开放

请参考 应用 Developer API 对接说明 。

API 开放 已禁用

启用后,将在【通用配置】标签中获取到的 client_id 、 client_secret 提供给应用开发者,在正确设定权限后,即可调用接口。

接口权限

管理员可为指定应用分配其调用的接口权限。

```
? 说明
```

注意:与阿里云 OpenAPI 不同, IDaaS 开放的 Developer API 依赖于 IDaaS 中应用的密钥,并在 IDaaS 应用管理中分配接口调用权限。Developer API 权限不依赖于 RAM。

在【API开放】标签中,可以勾选场景,场景对应的接口将开放可调用。

ł	安口权	Z限			
		功能场景	权限名	积限值	对应接口
	~	账户/组织	查询账户信息	umalibabaidaas:scope:user:read_all	获取能户信息: GetUser 通过外部DG教教账户D: GetUserIdByExternalld 查询账户列表: ListUsers 获取能户密码策略: GetUserPasswordPolicy
		账户/组织	管理用户	um:alibaba:idaas:scope:user:manage_all	创建账户: CreateUser 修改账户信息: PatchUser 删除账户: DeleteUser
		账户/组织	查询机构信息	urn:allbabe-idaes:scope:organizational_unit:read_all	我取組织信息:GetOrganizationalUnit 通过外部D获取组织D: GetOrganizationalUnitIdByExternalId 重调组织列表:ListOrganizationalUnits 获取组织先代节点列表:ListOrganizationalUnitParentIds
		账户/组织	管理机构	urn:alibaba:idaas:scope:organizational_unit:manage_all	创建组织: CreateOrganizationalUnit 修改组织信息: PatchOrganizationalUnit 删除组织: DeleteOrganizationalUnit

数据权限

与此同时,【账户同步】菜单中设定的【同步范围】亦将生效,限定可操作的数据范围。

同步范围设定 前往编辑

Alibaba Cloud IDaaS

应用调用 API 进行创建/查询等操作,仅可在指定的【同步范围】内进行操作。

【同步范围】需要前往【账户同步】标签中进行管理。

开发对接

对接文档请参考:应用开发 API 说明。

IDaaS 提供多种语言的 SDK, 您可以在 阿里云 OpenAPI 开发者门户 下载/查看调用样例,并直接尝试调用接口查看效果。

1.4.5. 登录

1.4.5.1. 登录方式

IDaaS 允许用户使用多种常见登录方式,安全便捷地访问应用。



登录方式

IDaaS 系统自带两种登录方式:

系统登录方式	说明
IDaaS 账户密码登录	默认启用。 使用 IDaaS 中存储的账户名和密码登录。若没有账户名或密码(例如刚从钉钉导入),则无法使用。
IDaaS 短信验证码登录	默认处于禁用状态,需要开启。 账户需要有手机号才能使用。 可以查看短信内容,但内容不能修改。 当前版本不收取短信费用。

添加登录方式

IDaaS 中提供的其他登录方式,均需要基于【身份提供方】配置进行开启。 当管理员添加身份提供方时,可能会有相关的登录能力自动添加为登录方式。 例如,绑定钉钉时,若管理员勾选启用钉钉扫码登录,则会自动创建钉钉扫码登录方式,可以直接使用。



若绑定时没有启用,在【身份提供方】菜单中,仍然可以随时开启功能。首次开启后,仍会自动创建对应的登录方式。

测试 Corpld: dingd00	● 导入初始化 宣看详情 × d2e7 f7214b	5469 🗿	删除
扫码登录 通过 https://i 进行扫码登录	已启用	同步對 IDaaS (特入 IDaaS) 増量回調 已品用 (の) 目标组织: 阿里云 IDaaS 全者日志 - 細拉取	应用自动上钉(暂不支 持) "DaaS 中支持 SSO 的应用, 钉钉控制台自动创建。

【身份提供方】菜单中的登录相关状态,会与【登录方式】菜单中保持一致。

例如:当在【身份提供方】菜单中关闭了钉钉扫码登录,【登录方式】中对应的状态亦会关闭。

禁用登录方式

登录方式禁用后将无法使用,且不会显示在登录页中。

登录配置

```
      针对 IDaaS 登录进行基础配置。

      登录配置

      优先登录方式 注: IDaaS 登录页立即展示的登录方式,可在页面切换至其他登录方式。

      团aaS 账等医畅登录
      >

      登录有双期 注: 在测宽器中登录 IDaaS 的会话级持时间,超出时间后,IDaaS 需要重新登录。

      8
      小时 

      不活跃重叠 注: 登录会话中君用户无任何操作,经过指定时长后,再次使用需要重新登录。

      2
      小时
```

参数说明如下:

参数	说明	示例
优先登录方式	IDaaS 登录页默认首选的登录方式,可在页面切换至其他登 录方式。	IDaaS 账户名密码登录
登录有效期	在浏览器中登录 IDaaS 的会话保持时间。超出时间后,IDaaS 一定需要重新登录。	8 小时
不活跃重登	登录会话中若用户无任何操作,经过指定时长后,再次使用 需要重新登录。	2 小时

1.4.5.2. 二次认证

IDaaS 支持在使用密码登录后,要求用户进行二次认证,提高管理安全性,满足合规要求。

```
⑦ 说明
为了保障您的使用安全性,二次认证能力默认开启。
```

云身份服务 / 登录
登录
通用配置 二次认证 密码策略
IDaaS 支持在账密登录后,开启二次认证。请参考文档 二次认证。
二次认证配置 已开启
开启模式
常开模式 每次登录都需要二次认证
> 9040-481-7
● 智能候式 不必每次登录都二次认证。IDaaS 会灵活进行判断。
二次认证方式
□ OTP 动态口会
使用 Google 认证器 APP 或其他常用 OTP APP 进行二次认证。
✓ 短信验证码
若账户没有手机号,则无法使用该方式。短信暂不收费。 宣看短信内容
✓ 邮件验证码
若账户没有邮箱,则无法使用该方式。 查看邮箱内容

开启模式

IDaaS 支持两种二次认证开启模式。

模式	说明
智能模式【推荐】	开启后,IDaaS 会根据上下文自行判断是否需要进行二次认证,在保障安全的基础上,降低用户使用复杂度,是 IDaaS 的特色能力。
常开模式	开启后,用户每次登录都需要进行二次认证。

二次认证方式

IDaaS 支持多种二次认证方式,管理员可多选同时开启。

方式	说明
0TP 动态口令	使用 Google 认证器等三方 APP 完成绑定,输入 6 位动态口令以完成二次认证。 用户需要先成功登录 IDaaS 应用门户,并在账户管理中,绑定 OTP 后,才能使用 OTP 二次认证登录。
短信验证码	发送 6 位验证码短信到 IDaaS 账户手机号。若账户没有手机号,则无法使用该方式。 短信暂不收费。 可前往【个性化】菜单查看短信内容。
邮箱验证码	发送 6 位验证码邮件到 IDaaS 账户邮箱。若账户没有邮箱,则无法使用该方式。 可前往【个性化】菜单查看邮件内容。

? 说明

提示:若 IDaaS 账户既无手机号也无邮箱,管理员开启二次认证后,用户将无法通过二次认证。 建议管理员确保所有 IDaaS 账户均能使用至少一种二次认证方式,再开 启功能。

开启后,所有 IDaaS 账户均可使用。用户可在二次认证环节自行选择使用方式。参考下图:

< 返回
二次认证 - 选择方式
管理员已开启二次认证。 为了保障您的账户安全,请您选择如下认证方式之一,继续 完成身份验证。
选择短信验证码 没有手机号
IDaaS将向您账户的手机号发送验证码。
选择邮箱验证码 没有邮箱
IDaaS将向您账户的邮箱发送验证码。
无法登录? 请联系您的企业管理员。

1.4.5.3. 密码策略

IDaaS 允许管理员对密码相关策略进行集中管理,包含:

- 密码复杂度
- 找回密码

密码复杂度

密码是网络安全中最薄弱环节之一。越复杂的密码安全性越高。

登录

通用配置 二次认证 密码策略

配置密码相	配置密码相关策略。保存后,所有密码新增或变更均会进行检查。			
预设复杂度模	板			
无限制	低复杂	常见	推荐	高复杂
密码长度				
10	密码最少字符	守数		
复杂度				
✔ 必须包含	大写字母			
✔ 必须包含	必须包含小写字母			
🖌 必须包含	必须包含数字			
✓ 必须包含	特殊字符 (!@	#\$%&*~	~)	
✔ 不能包含	不能包含用户名			
□ 不能包含	显示名称或其拼	† 音		
□ 不能包含	不能包含手机号			
□ 不能包含	邮箱前缀			

为了便于场景选择,在【登录】菜单【密码策略】标签中, IDaaS 提供了 5 类预置复杂度模板,说明如下:

复杂度模板	模板内容
无限制	最少 4 位。
低复杂	最少 6 位,必须包含小写字母,数字。
常见	最少 8 位,必须包含大写字母、小写字母、数字。
推荐	最少 10 位,必须包含大写字母、小写字母、数字、特殊字符。不能包含账户名。
高复杂	最少 16 位,必须包含大写字母、小写字母、数字、特殊字符。不能包含账户名、显示名及其拼音、手机号或邮箱前缀。

您可选择其中一个模板,在此基础上调整配置,或直接自定义配置,保存后即可生效。

变更复杂度后,既有密码不受影响,新密码需遵守复杂度限制。

忘记密码

用户在登录时可能忘记密码,IDaaS 提供用户自助服务完成新密码设定。

	云身份服务 / 登录
	谷录
	通用配置 二次认证 密码策略
	复杂度 忘记密码
	忘记密码
	开启忘记密码
	■ 展示忘记密码 开启后,登录流程中,允许用户使用忘记密码功能。
	身份验证方式
<	□ 短信验证 通过短信身份验证找回密码。查看短信内容
_	■ 邮箱验证 通过邮箱身份验证找回密码。查看邮箱内容

功能默认未启用。在管理员侧,通过【密码策略】【忘记密码】标签,可勾选开启忘记密码开启能力。开启后,使用密码登录的页面下方会出现【忘记密码】链接。

中文 🗸
•
账户名、手机号或邮箱
密码
忘记密码?
登录
其他登录方式

用户通过该链接,可通过短信或邮箱验证的方式进行身份认证。 手机号、邮箱皆为空时,账户的密码无法找回,请联系管理员重新设置。

置。
获取验证码
下一步

而后即可设定新密码。

返回	设置新密码	
请您设置新密码。	3	
		ø
长度至少 10 位, 特殊字符,不得f	必须包含大写字母、小写 包含账户名。	字母、数字、
		完成

为了保障身份安全,设定密码时,该近期使用过的的密码不能再次使用。

1.4.6. 日志

1.4.6.1. 管理/用户日志

IDaaS 会将数十种管理员、用户的关键操作记录在日志中,便于后续审计、追溯和分析。

在 IDaaS 中, 管理操作和用户行为会分开查询。管理员可以在【日志】菜单中分别查看。

⑦ 说明提示:日志会保存 180 天。

管理员可以根据 事件发生时间范围 和 事件类型 进行检索。

云身份服务	時 / 日志						更新日志	IDaaS 支持群	帮助文档
日志	能作 用户行为 同步	日志							
2022-0	02-10 17:45:08 20:	22-02-17 17:45:08	■ 近一周 〜	全部事件类	<u>u</u> ~				
	时(11)		操作者	事件类型		操作对象			
^	2022-02-17 17:38:38		root	启用应用配置		OIDC 协议			
	 操作者 操作者 操作者 操作者 型 操作不着 型 操作 操作 条 操作 条 () 操作 	1021806970344 RAM 册户 root 100.68.65.13 OpenAPI Unknown Unknown	813		 事件 事件 ID 秋季件 ID 少季件 ID 事件特別 事件件括果 操作対象 対象 OIDC 协议 対象 OIDC 协议 対象 対象 対象 対象 対象 	evnt_aaaac7yh 2022-02-17 17: 原用应用应量 成20 (個用) app_mhark 应用 OIDC 协议	vwro6pwmm	wiigjif2smkgeqru dds3rj7r4e4	nydyq
~	2022-02-17 17:38:29		root	禁用应用同步		OIDC 协议			
~	2022-02-17 17:37:08		root	启用二次认证					
~	2022-02-17 17:37:06		root	启用二次认证					

1.4.6.2. 同步日志

由于同步日志的类型特殊,IDaaS 将同步日志单独记录、展示。

 在当前版本中,不同同步方式下,同步日志的记录情况如下:

 入方向
 出方向

 记录同步日志
 ・ 从身份提供方同步
 ・ 由 IDaaS 推送给应用

 ・ 由 IDaaS 推送给身份指示
 ・ 由 IDaaS 推送给身份指示

 正家向多口志
 • M 穿顶旋状刀向多
 • 由 IDaaS 推送给身份提供方(暂不支持)

 不记录向步日志,但会记录为管理或用户日志
 • OpenAPI
 • Developer API(暂不支持)

 • SCIM API(暂不支持)
 • 应用从 IDaaS 拉取

? 说明

提示:部分操作可能会同时记录同步日志和管理或用户日志。

任务执行

【任务】是同步日志的集合。

理论上,当一次操作导致多条数据同步时,IDaaS 会将该批次同步结果聚合为【任务】,方便查看执行状态和结果。

日志										
管理操作	用户行为	同步日志								
任务执行	日志详情									
查看批次	《任务的执行情	况,若要查看	单条记录,请前往	日志详情。						×
开始时间	→ 结束时间	Q	过滤同步方向	~ izi	结果	×				
同步方	向 相关	方类型 相	11关方名称	发起时间	结束时间	触发方式	结果	结果描述	操作	
入方向	身份	提供方 派	则试钉钉	2020-10-10 10:00:00	-	手动触发	进行中 🖒	已完成导入 18 个组织机构,5 个账 户,进行中		
出方向	应用	ß	立用	2020-10-10 10:00:00	2020-10-1	D自动触发	部分失败	从钉钉全量拉取 10 个组织, 18 个账 户,其中3个组织, 3个账户失败。	详情 重推	

触发任务记录的事件

触发模块	记录任务的情况	只有日志的情况
身份提供方 IdP	 从 ldP 批量导入(定时/手动) 一次性全量同步到 ldP(暂不支持) 	 IdP 单条数据变更同步到 IDaaS IDaaS 单条数据变更同步到 IdP
应用	• 一次性批量将账户同步给应用	● IDaaS 中单条数据变更触发的同步事件
账户	 手动触发同步组织或账户 (暂不支持) 	

同步任务状态

状态	说明
成功	当次所有同步请求全部成功执行。
失败	当次所有同步请求全部失败,可能由于网络原因。
部分成功	该批次请求中部分失败,可以查看详情。
进行中	同步任务仍在进行中。列表每 5 秒刷新一次。
初始化	一般在执行的时候出现异常,导致同步未执行。 出现该状态时,可以重新触发同步任务。 属于罕见异常。

日志详情

管理员可以查看每条同步数据的状态和详情,并进行检索。

日志							
管理操作	用户行为	同步日志					
任务执行	日志详情						
音 查看每个	同步请求的执行	情况。					
时间开始	> 时间截止	Q	防肉・	结果	~ 选择相关任	' ў	·
					机机 题 ID	aaS 2021年12月31日17:26:0! 、	•
时间	同步方向	相关方类型	相关方名称	触发方式	同步对象	同步类型	结果
2020-10-1 10:00:00)入方向	身份提供方	测试钉钉	自动触发	TestUser (账户)	创建	成功
2020-10-1 10:00:00	出方向	应用	自研应用A	自动触发	TestUser (账户)	修改	失败 🔮

若同步请求失败,可以查看失败原因。原因订正后,您可以通过两种方式处理此次异常:

● 手动变更。前往对应系统,手动将此次要同步的数据进行更正。

重新推送。在同步来源重新触发推送尝试。注意避免造成数据重复。

1.4.7. 企业个性化

1.4.7.1. 企业信息

管理员可以在【个性化】菜单中设定自己的企业信息。

云身份服务 / 个	性化			
个性化				
企业信息	短信模板	邮件模板		
在 IDaaS 界面	上个性化显示您	的企业信息。		
企业图标	2 上 企业图柄 必须为F	2 传 网/JPG 格式,大小不超过 1	MB。建议使用 256*256 像素方形	图标。
企业名称	阿里z 企业名称	(IDaaS 《将会显示在【登录页面】和【	× 组织机构根节点】中。	
设定后,在	组织根节	点和登录页中,会	有对应体现。	
组织	限节点	Ā	登录页	

85/1019	
阿里云 IDaaS 测试企业	*
产品测试部门	阿里云 IDaaS 测试企业
	账户名、手机号或邮箱 test
	· ····· ⑥
	**

1.4.7.2. 短信/邮件内容

在【个性化】菜单中可以查看 IDaaS 会向最终用户发送的短信和邮件内容。

```
若对应功能开启,并由用户的特定操作触发,则会发送短信/邮件。详情请参考控制台页面。
```

云身份服务 / 个性化		更新日志 IDaaS 支持	寺群 帮助文档
个性化			
企业信息 短信機	板 邮件模板		
查看 IDaaS 向用户发送的	的短信配置。		
模板名称	触发条件	短信内容	操作
短信验证码登录	管理员开启短信验证码登录方式后,用户选择该方式 登录时。	尊敬的用户XXX,您正在登录阿里云 IDaaS,验证码为:XXXXX, 5分钟内有效。	暂不支持 编辑
短信二次认证	管理员开启短信二次认证后,用户使用账密登录,选 择短信二次认证时。	尊敬的用户XXX,您正在阿里云 IDaaS 中进行二次认证,验证码 为:XXXXX,5分钟内有效。	暂不支持 编辑
换绑手机号、新手 机号验证	账户当前已有手机号,用户进行换绑操作,需要对新 手机号进行验证。	尊敬的用户XXX,您正在阿里云 IDaaS 中绑定新的手机,验证码 为:XXXXX,5分钟内有效。	暂不支持 编辑

곗 说明

```
提示:当前 IDaaS 可以免费发送相关短信/邮件。
在未来版本中,会支持自定义短信网关、邮件网关,并开放内容编辑,敬请期待。
```

1.5. 用户指南

1.5.1. 通用登录页

IDaaS 提供通用登录页,允许终端用户使用 IDaaS 账户,登录 IDaaS 用户门户,或直接登录对接好的应用。

⑦ 说明 提示:每个 IDaaS 实例有不同的登录页地址,可在【快速入门】【账户】【登录】等菜单查看。

登录流程



上图中的 3 个特殊步骤说明如下:

特殊步骤#	步骤名称	说明
1	二次认证	仅限于密码登录方式。详情参考: <mark>二次认证</mark> 。
2	强制密码修改	当前尚未开放强制密码修改功能,敬请期待。
3	选择应用账户	仅限于 SP 发起的 SSO 流程时登录场景,登录后需要选择使用的应用身份,发起 SSO。

登录页



⑦ 说明

提示:登录页图标和企业名称可以在企业信息中管理。

二次认证页

□次认证 – 选择方式		< 道田 二次认证 - 知	豆信验证码
为了保障您的账户安全,请您选择如下认证方式之 -,继续完成身份验证。		短信检证码已经发送至手机号	183****2637, 请查收。
38 48 49 /0 30 JT TT		请输入验证码	重发(46a)
285年201日381年5月 DasS 将向您账户的手机号 183****2637 发送 检证码。		收不到知信? 试试 语音接收,	或其他认证方式。
	L,	上一步: 选择方式	输认
选择邮件验证码 无法使用 您当前账户并未绑定邮箱,无法使用邮件验证码二 次认证。			
无法登录? 请联系您的企业管理员。			

详情参考: 二次认证。

选择应用账户

同一个 IDaaS 账户访问同一个应用,可能有多个不同的身份可以扮演。可通过添加多个应用账户实现。详情参考:SAML 应用账户配置。

在进行应用 SP 发起 SSO 时,若发现已登录 IDaaS 账户有多个应用账户可选择,会请用户选择其中一个,进行访问。

< 返回	
请选择应用账户	
您正在尝试登录应用 阿里云控制台。 管理员为您配置了多个应用账户。请选择一个, SSO。	,进行
ram_admin1	~

登录异常情况

场景	针对功能	异常说明
人机验证	只针对账户名+密码登录。	在同一浏览器中, 当登录失败一次后, 在成功前的所有账密登录, 均需要使用人机验证。
账户锁定	只针对账户名+密码登录。	同一个账户,5分钟内连续登录失败10次,会将账户锁定。 若账户有多个可登录标识(例如间隔使用户名和手机号登录),失败次数会跨标识累积。 解锁方式如下: • 等待5分钟自动解锁。 • 管理员在[账户]菜单中将账户解锁。 • 走完忘记密码流程,自动解锁。(暂不支持)
<u>短信/邮件</u> 验证码限制	在登录、二次认证、找回密码等流程中通 用。	 60 秒可以发送一次,短信和邮件单独计时。 同一验证码可以尝试 3 次输入, 3 次均失败后,验证码失效。用户需要获取新验证码。

1.5.2. 钉钉扫码登录

```
? 说明
```

前提:IDaaS 管理员已经绑定钉钉,且钉钉扫码登录处于开启状态。操作详情查看:绑定钉钉。

选择钉钉扫码登录

在用户登录页,选择【其他登录方式】中【钉钉扫码登录】选项,跳转到钉钉二维码展示页面。请用户使用钉钉扫描二维码。

🤊 说明

注意: 若未看到【钉钉扫码登录】选项, 请管理员前往【登录】菜单, 确认您是否启用了钉钉扫码登录功能。



扫码后两种情况

使用钉钉扫码登录时,共有如下两种情况。

情况一、正常扫码登录

当 IDaaS 中存在该钉钉身份的绑定信息时,弹出如下界面。确认即可完成登录。



取消登录

情况二、IDaaS 无法识别用户身份

非钉钉导入的账户,需要手动绑定钉钉和 IDaaS 的账户身份,才能扫码登录成功。

扫码确认后,网页会跳转到下图界面,选择【绑定已有 IDaaS 账户】,触发 IDaaS 账户身份验证流程。

用户需要使用任何 <u>非钉钉扫码</u> 方式,进行身份验证,验证通过后会将钉钉账户与 IDaaS 账户进行绑定,并登录成功。

后续登录无需再次绑定。

±± ± ± ± ± ± ± ± ± ± ± ± ±	Ф х ∨
阿里云 IDaaS 测试企业	阿里云 IDaaS 测试企业
● IDaaS 中末找到您的第三方账户信息。	③ 您正在将微软账户绑定 IDaaS 账户。请先验证 IDaaS 身份,通过后自动绑定。
请选择如下选项继续操作: 绑定已有IDaaS账户	账户名、手机号或邮箱 test
进行 IDaaS 账户认证,成功后自动绑定。	密码 ⓒ
注册 IDaaS 新账户 督未开放 注册新的 IDaaS 账户,自动与当前账户绑定。	登录
	其他登录方式
	··· 使用短信验证码登录
	▼ 麦加潮试 无法使用 ②

1.5.3. 门户页

IDaaS 用户门户是企业的统一访问入口。我们建议企业用户将此页面保存为书签,作为业务应用访问入口。

所有企业用户可在此查看其被授权访问的企业应用,并一键访问,实现 SSO。



? 说明

提示:经由应用发起的 SSO 流程,登录后会直接跳回到应用中,不会来到门户页。 通过登录页直接登录的情况下,才会来到门户页,用户可自行选择后续 SSO 到哪个 应用。

我的应用

在【我的应用】菜单中, 会显示当前 IDaa5 账户已被授权可访问的应用。若为空, 请联系管理员进行 3. 创建应用 和 应用授权。

若应用数量较多,可通过应用名称进行模糊搜索,快速查找目标应用。

针对不同应用的可选应用账户数量,可能出现以下 3 种情况:

情况	说明
<u>情况一</u> 有且仅有一个应用账户	用户可顺利 SSO 到应用,无需额外步骤。
<u>情况二</u> 无应用账户	若 IDaaS 无法识别 SSO 应使用的身份标识,界面会提示【暂无应用账户】,无法进行 SSO。 此类情况需要联系管理员解决。暂不支持用户发起添加应用账户的申请。
<u>情况三</u> 有多个应用账户	同一个 IDaaS 账户访问同一个应用,可能有多个不同的身份可以扮演。可通过添加多个应用账户实现。 在门户页进行 SSO 时(IdP 发起的 SSO),若发现有多个应用账户可选择,会跳转到应用账户选择页。请用户选择其中一个, 进行访问。

登出

IDaaS 用户登录态有四种登出方式:

登出方式	说明
超出登录有效期	可配置。详情参考 <mark>登录方式</mark> 。
超时不适跃	可配置。详情参考 <mark>登录方式</mark> 。
手动退出	在 IDaaS 门户中,也通过右上角的【登出】按钮,退出 IDaaS 登录态。
<u>关闭浏览器</u>	当前浏览器完全关闭后,登录态会自动失效。

登出后,后续访问任何应用,均需要重新登录。

钉钉工作台中访问门户页

若通过扫码开通的方式 绑定钉钉 后,除了网页登录外,企业用户可以在钉钉工作台中免登 IDaaS 用户门户,并继续 SSO 到任何与 IDaaS 对接的 SSO 应用。详情参考:钉钉工 <mark>作台访问门</mark>户。

1.5.4. 钉钉工作台访问门户

IDaaS 中 <mark>绑定钉钉</mark> 的流程,即是钉钉企业三方应用的开通流程。

开通的过程中,管理员会分配 IDaaS 应用在钉钉通讯录中的使用范围。该使用范围内的账户,可以同步到 IDaaS 中,也可以在钉钉工作台中直接访问 IDaaS 门户。

下图以云效举例说明。



绑定 IDaaS 账户

所有从钉钉导入 IDaaS 的账户,均无需绑定,可直接访问钉钉工作台中的 IDaaS 门户。

非钉钉扫入的 IDaaS 账户,若尚未绑定钉钉 userId ,则需要先进行账户绑定。

绑定时,使用 <u>非钉钉登录</u>的方式验证身份,完成后即可访问。

```
后续访问无需再次绑定。
       未找到对应账户
                                       验证身份
                      中文 🗸
                                                   中文 レ
            <
                                         $
     阿里云 IDaaS 测试企业
                                  阿里云 IDaaS 测试企业
 IDaaS 中未找到您的第三方账户信息。
                               😐 您正在将微软账户绑定 IDaaS 账户。请先验证
                                 IDaaS 身份,通过后自动绑定。
 请选择如下选项继续操作:
                                账户名、手机号或邮箱
                                test
  绑定已有IDaaS账户 ____
  进行 IDaaS 账户认证,成功后自动绑定。
                                密码
                                                    0
  注册 IDaaS 新账户 暂未开放
  注册新的 IDaaS 账户,自动与当前账户绑定
                                       其他登录方式
                               --- 使用短信验证码登录
                               ▶ 表扣测试 无法使用 ⑦
```

一键获取钉钉手机号/邮箱

从钉钉中导入的账户,缺失手机号/邮箱,会导致部分 IDaaS 关键功能不可用(二次认证、找回密码等)。

从钉钉工作台进入到 IDaaS 门户,会在页面上方提示,可以一键授权获取手机号/邮箱。

用户同意后,IDaaS 可以获取到当前用户的手机号/邮箱信息,并自动填充进当前账户。

IDaaS 用F	口户主页	钉钉个人	「信息授权页
 请点击下方的应用进行 应用情况有疑议,请罪 	前单点登录。若对 🕺 🍾	 请点击下方的应用 应用情况有疑议, 	进行单点登录。若对 ⁵ × 清联系管理员。
 您当前未填写手机号利用。请一键投权。 用。请一键投权。 用 用 用 用 用 用 用 点 <l< th=""><th>和納賴, 部分功能无法使</th><th>IEE RAM ram_salmin1 文 网钉科技 申请茲 以下权限 ク 获取你的个人基本信 ク 获取你的个人基本信 グ 我取你的手机号 図 我已阅读并同意 用户 取消</th><th> 第6 送売可能が 表記の利能が 見欠ひ込む 免許 </th></l<>	和納賴, 部分功能无法使	IEE RAM ram_salmin1 文 网钉科技 申请茲 以下权限 ク 获取你的个人基本信 ク 获取你的个人基本信 グ 我取你的手机号 図 我已阅读并同意 用户 取消	 第6 送売可能が 表記の利能が 見欠ひ込む 免許

1.5.5. 用户自服务

IDaaS 用户登录至门户后,可在【我的账户】菜单,对当前登录账户进行基本信息查看和编辑。

IDaaS 应用门户 阿里云 IDaaS 测试企业			
我的应用	我的账户		
我的账户	基础信息		
	账户名	test	
	显示名	test	修改
	安全信息		
	手机	未擱定	绑定手机号
	邮箱 ①	未绑定	绑定邮箱
	密码		修改密码
	三方登录绑定		
	() () () () () () () () () () () () () (未绑定	绑定

? 说明

提示:【我的账户】菜单在钉钉 IDaaS 应用中不可见。仅可在 PC 端浏览器中使用。

可管理信息如下:

字段名	说明
账户名	用于登录和唯一标识的账户名,可修改。 提示:从钉钉扫入的账户,账户名初始为空。从 IDaaS 中创建的账户,账户名为必填。
显 <u>示名</u>	账户的显示昵称,通常为姓名。
<u> 手机</u>	强烈建议填写。可用于登录、找回密码、二次认证等流程。 提示:若开启二次认证,手机和邮箱均未填写时,账户无法登录。
邮箱	建议填写。可用于登录、找回密码、二次认证等流程。 提示:若开启二次认证,手机和邮箱均未填写时,账户无法登录。
<u>密码</u>	密码复杂度可由管理员配置。
三方登录缆定	绑定外部企业身份,允许用户使用该身份进行登录。在此可进行绑定、解绑等操作。若账户从身份提供方导入创建,则默认绑定,无法解绑。 提示:当前支持钉钉身份,未来会支持企业微信、飞书、AzureAD 等其他企业级身份源。
OTP 绑定	当管理员启用 OTP 二次认证后,用户可在此绑定 OTP。

1.5.6. OIDC Device Flow 设备模式登录流程

在 OIDC 协议支持的模式中,专有一类 Device Flow 设备模式,允许各类终端或硬件,通过 IDaaS 完成登录流程。

由于终端的显示模式可能受限,无法内置登录页面,OIDC设备模式将用户的登录流程与设备分开,允许用户使用外部浏览器,完成登录。

? 说明

提示:本文档讲解 OIDC 设备模式的场景与流程,详细接口文档请参考:OIDC Decive Flow 接口说明。

系统间时序图如下:



步骤一、登录准备

登录准备阶段无需用户参与,终端/设备与 IDaaS 进行交互,获取到 用户口令 user_code 设备口令 device_code 登录地址 verification_url 。

其中, 用户口令 和 登录地址 需要展示给用户,并请用户在任意浏览器中打开 登录地址 ,输入 用户口令 ,进行登录流程。



⑦ 说明

提示:若设备允许,可以将用户口令拼接在登录地址: {{verification_url}}?user_code={{user_code}},并提供超链接,或生成为二维码。用户在访问该地址时,将无需 手动输入 user_code,省时便捷。

在获取到上述信息后,终端应开始到 IDaaS 的轮询请求,获取登录结果。 步骤二、浏览器登录授权

用户打开登录地址 verification_url 后,将按照下图顺序进行操作,完成登录。
PC 端 device code 口令输入界面		PC 端应用授权确认页面	PC 端结果页
*		*	\bigcirc
IDaaS – 设备登录		IDaaS – 确认授权	认证授权完成
 您正在进行【测试应用】的设备登录。 请输入设备上显示的口令,以开始认证流程。 		请您确认授权登录应用【阿里云 SSL VPN】。	设备端应已登录完成。 请 <u>返回设备路</u> ,进行后续操作。
8819 xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	→ IDaaS 登录流程	តាំ៤៩៩៩ រូបនានេក	

登录成功后,用户可切换回终端/设备查看结果。终端/设备发起的轮询将会返回认证成功信息,其中包含用户的 id_token。

可以使用 IDaaS OIDC 应用中提供的 JWKS 端点,获取应用的公钥信息,并使用公钥进行验签,确定登录有效,拿到用户标识,顺利登录。

1.6. 开发指南

1.6.1. 接入单点登录

1.6.1.1. 自研应用接入 SSO

1. 背景介绍

IDaaS 采用标准的 OIDC 协议授权码模式来支持常规企业自研应用接入。

? 说明

兼容 OAuth: OIDC(OpenID Connect)1.0 协议是基于 OAuth2.0 协议之上建立了用户身份层,所以只要符合OIDC协议本身就是符合 OAuth2.0 协议规范的。OIDC 授权码 流和 OAuth2.0 一致,区别是 OIDC 对用户信息端点进行了标准化,并在 Token 端点会返回用户的 ID Token。

授权码流程介绍



2. 对接 SSO

2.1. 创建自研(或OIDC协议)应用

请参考自研应用 SSO 配置 创建应用。

곗 说明

默认情况下 client_id 与 application_id 一致,以 "app_" 开始,长度约 26 个字符, client_secret 是以 cs 开始的随机字符串,长度在 44 ~ 46 字符之间。

2.2. 请求授权端点 Authorization Endpoint

请参照如下示例,在授权端点地址 Authorization Endpoint 的基础上,拼装出 URL 访问地址,在浏览器中发起跳转。

{{授权端点 Authorization Endpoint}}?
client_id=app_***&
redirect_uri=http%3A%2F%2Flocalhost%3A3000%2F***&
response_type=code&
scope=openid&
state=525f49cc-***

字段	示例	说明
client_id	app_michs7r4fwfcost66osh346pye	Client ID
scope	openid	授权 scope , openid 表示接收入以下字段: sub , jti , iss , iat , nbf , exp , aud , at_hash
response_type	code	所有 B/S 网页应用,均推荐采用授权码流,固定为 code。
redirect_uri	http://localhost:3000/user/oauth2/aliy unidaas/callback	接入应用的重定向地址,用于接收入IDaaS返回的授权码 code
state	525f49cc-87c4-4655-b79c-4c4f971b1ad1	state 是应用自己生成的随机字符串,建议长度 32 位以上。state 值将在返回授权码 code 时带回给应用,应用应验证 state 值是否与发起时一致,以确保同一会话,以规避 XSRF 安全 漏洞。



用户登录成功后,浏览器会 302 跳转回redirect_uri,并在 URL参数中携带 code 和 state 参数。

{{redirect_uri}}? code=CO***& state=525f49cc-***

字段	示例	说明
code	COE59pkCTm4A9nmowJUsfsfarGEaiShj3TuDc7NCzLCYu9	授权码
state	525f49cc-87c4-4655-b79c-4c4f971b1ad1	授权时传入的 state 一致

2.4. 请求令牌端点 Token Endpoint

上一	步接收到 code 授权码,	并验证请求合法	(验证 state	与发起请求传入的	的一致)后	, 应用的后端服务,	应使用获得的 code 向令牌	端点 (Token Endpoint))发起 POST
请求	,请求示例如下:								



grant_type	是	authorization_code	固定填写 authorization_code 即可。
code	是	n0esc3NRze7LTCu7iYzS6a5acc3f0ogp4	即上一步中返回的授权码 code。
client_id	是	app_miharkwwro6pwmmdds3rj7r4e4	IDaaS 默认使用 client_secret_post 模式验证调用方合理性。在此模式下,需要将 client_id, client_secret 作为 POST 参数传递给 IDaaS,进行调用方身份验证。
client_secret	是	CSAuycr3yWHNn8bEmdkox8ppbKJfXUWMPQ9av tqRozS1V1	出于安全考量,client_secret 任何情况下都不应存储在前端。
redirect_url	是	http%3A%2F%2Fwww.example.com%2Fsso%2 Fcallback	即上一步使用的 redirect_uri, 重新传入以保障请求连续性。

响应结果如下:

"token_type": "Bearer",

"access_token": "ATM4SoVDqWgUJHLu3Bg6qF2hccE6cvjKXiKdiJ2Dc8RJZSbzpBDXPZK3gPhGxQs16s3s7MsZ46fEyiYTWG7EGFKi9uzGjRALaRLecPutBLzzQQRVUt6pbuarCbq5hFRj e6bzsrW4jTehhCtZM5JneEfcSQ2ViSDVZGNNtMKAA6v7KTeubZrTaWNzosNMyzGXoD4rqPBwF9FsYqwACQ4aJrt9NnS3NpgDKoMtqEQs5TfDsCYMKYmp7Z73F2BJz89jzN1utEbnuj3HnvyRQPC ismDiXjS8EPvoUZBrUBMhrnzYmMcT9KmzKoC12sQjDRQYqgPVxQyMKwQKwwHWXV7stEXnoSt524GW8HVrF3WRsM2N1Ykod1irCz7ZasSwk3ZS5mtn6fcSp8NH8",

"expires_in": 1200,

"expires_at": 1644843164,

"id_token": "eyJraWQiOiJLRVkyVHkxcUw2dTIxTkdLbWNjdjNqd2ZkMm5kbWd0UVBuYWciLCJhbGciOiJSUzIINiJ9.eyJzdWIiOiJlc2VyX3V5dmVmb3RqbjdrcGJlamZteG9vczNydG1 tIiwianRpIjoiand0X2FhYWFjN3h5aGNsYWM2YXFrZ3RqYXhzdGh3NXlvdG4IZDc3cG1raSIsImlzcyI6Imh0dHBzOi8vcHJlLWVpYW0tYXBpLWNuLWhhbmd6aG91LmFsaXllbi1pbmMuY29tL3 YyL21kYWFzX2JxZ2xkdnpwcGEyYWw2aTZhYzVxemphcWpxL2FwcF9taHlsZ28zaWFpcmpxamR4NWVvcDZ1YWY2NC9vaWRjIiwiaWF0IjoxNjQ0DQxOTY1LCJuYMYi0jE2NDQ4NDESNjUsImV4c CIGMTYONDg0MjI2NswiYXVk1joiYXBwX2loeWxnbzNpYW1yanFq2Hg1ZW9wNnVh2jM0IiwiYXRfaGFzaCI611hIRWFHcElvb005enZRWGFNekNORUEifQ.abebHwo5z0i92-Q0K0_B38jyfxjzV LpRIK858UsOehe_GZB6KOE11zQOS1jBB7CwZCdQJpqIIrUxqQopwjvHRSfA-04_cc4sXDpZYXodeVRXUiv1kYB1b4gZ-hstcEleh_5jJj1dpoGPBsjTTHjp43EgDx1-8M-8ePF3zXZAfqxCjjro GgB9qXtSreRAIUh50DViyHYRSAis7CNdP7jKG1dU1UNSGwXWNyRcgVaCqL05gCh0LhHrutMXDy8pcKzdXHQMMBaHF-rGkkGd1p4q9KqwjkpzakcWieRmPa2UUXLdQgK1Pgzc5F7mE-fvsvVfMYf h_3gRIadj-frOIRFChA" }

对结果中的 id_token 解析如下:

```
{
    "kid": "KEY2Ty1qL6u21NGKmccv3jwfd2ndmgtQPnag",
    "alg": "RS256"
}.{
    "sub": "user_uyvefotjn7kpbejfmxoos3rtmm",
    "jti": "jwt_aaaac7xyhclac6aqkgtjaxsthw5yotn5d77pmki",
    "iss": "https://pre-eiam-api-cn-hangzhou.aliyun-inc.com/v2/idaas_bqgldvzppa2al6i6ac5qzjaqjq/app_mhy1go3iairjqjdx5eop6uaf34/oidc",
    "iat": 1644841965,
    "nbf": 1644841965,
    "nbf": 1644842265,
    "aud": "app_mhy1go3iairjqjdx5eop6uaf34",
    "at_hash": "XHEAGpMooM9zvQXAMzCNEA"
}.[Signature]
```

对于 id_token 中的字段受应用被授权的 scope 而定。

2.5. 通过程序解析 id_token

id_token 是一种 JWT (JSON Web T oken)令牌,使用签名方法创建也就是 JWS (JSON Web Signat ure),对于JWT 的解析可以参见<mark>https://jwt.io/libraries</mark> 找到合适的库,下面以 Java 库:org.bit bucket.b_c:jose4j 为例介绍如何使用。

首先加入对应的Maven依赖:

```
<dependency>
<groupId>org.bitbucket.b_c</groupId>
<artifactId>jose4j</artifactId>
<version>0.7.12</version>
</dependency>
```

解析示例如下:

[{]

import org.jose4j.jwk.JsonWebKey; import org.jose4j.jwk.JsonWebKeySet; import org.jose4j.jwt.JwtClaims; import org.jose4j.jwt.consumer.JwtConsumer; import org.jose4j.jwt.consumer.JwtConsumerBuilder; public class IdTokenTest { public static void main(String[] args) throws Exception { String issuer = "https://eiam-api-cn-hangzhou.aliyuncs.com/v2/idaas_padyrlux3mphrlsex4uonyqhxu/app_mkif4dwlpeh6dns4pxpzbasqmu/oidc"; String appId = "app_mkif4dwlpeh6dns4pxpzbasqmu"; String jwkJson = "{\n" + " \"keys\": [\n" + " {\n" + " \"ktv\": \"RSA\",\n" + " \"e\": \"AOAB\",\n" ... \"use\": \"sig\",\n" + " \"kid\": \"KEY2H82C2at57itnW4onT3p1ySjwH4nirjCk\",\n" + " \"n\": \"w7Jl3fAUJp_9GuxVXb9Jb_QsOA4lnXR5OD4kF4QbleBiDiH8_MThrFi9k2MB6YMkSzf5JfIkpAS3JCqZ7k6Wooydp4pzaZNZAk3SGzdsa022RmAT" + "-Iayi4Yj6J9tSdTQCjwh2XkzzsIxA_Hla8rWiQ8Vhw1" "-7QArgObfe67nsR7LxD55MFLxk9FU0NWLEjRR1GhrQGE_0LUuGWtCJG1r1e6aKquyswfxxAr3Rvj8QGIeJrG0R1Pv8m8d1_50dULhB7149VqjM6D98WFjab0U2SNv0UIRE ZXTcS4p-2QNm_1egYRRpJEY_00FZqNSYsmErMGepYhO_61KoGqd8cphWQ\"\n" + " }\n" + "]\n" + "}"; $\texttt{String jwt} = \texttt{"eyJraWQiOiJLRVkySDgyQzJhdDU3aXRuVzRvblQzcDF5U2p3SDRuaXJqQ2siLCJhbGciOiJSUzIlNiJ9.eyJzdWIiOiJ1c2VyX2R0NmtqNnlmNjRjZjR3amFrbnBi$ eGpjd3V11iwianRpIjoiand0X2FhYWFkYWllYTc2eWg1cW0zcm11bnoyeGg0eHd5aTJzZHBoNjR6aSIsImlzcyI6Imh0dHBzOi8vZWlhbS1hcGktY24taGFuZ3pob3UuYWxpeXVuY3MuY29tL3Y yL2lkYWFzX3BhZHlybHV4M21waHJsc2V4NHVvbnlxaHh1L2FwcF9ta2lmNGR3bHBlaDZkbnM0cHhwemJhc3FtdS9vaWRjIiwiaWF0IjoxNjUzNjMwMDQxLCJuYmYiOjE2NTM2MzAwNDEsImV4cC I6MTY1M2Y2MDM0MSwiYXVkIjoiYXBwX21raWY0ZHdscGV0NmRuczRweHB6YmFzcW11IiwibmFtZSI6InRlc3QiLCJwcmVmZXJyZWRfdXNlcm5hbWUi0iJ0ZXN0IiwidXBkYXRlZF9hdCI6MTY1M z y 0 DU5 MH0.pAs UNB80 kdp i x JM2 RfL j7 Pa 31 ts Jy 144a 1 j VI l v d 0 xw0 t PULAwr Fx nB0 X 3 e 0 x89 h UGC d v W1 9 F0 90 - 5 kT7L - RER0w J y 2 9 N Kq r V NB na Rw INR Z ye Y LR V u r WM Z 0 D Q z - V 0 U Ld 9 ra M 1 a 0 rM_i2f_SoWFs1gPFtYh_ijUARHISi7Q3q93ZfAuY8Lq2Nq07QunmDbosvioUd5wJG7WCxW5XXZYDUQe9p5IEYd1MSvnWuTOLbg7rKn0Vm4dNYGWjz1WuoAyCsc_QxOCgpmQ_2czoqPeN-SvPJAQ2 CykLk7DSnGpABw1aNrjDidLS9Beqsga9VDCth86sk_01yTZOaORtUrfVTtQ"; JsonWebKeySet jsonWebKeySet = new JsonWebKeySet(jwkJson); JwtConsumer jwtConsumer = createJwtConsumer(jsonWebKeySet, issuer, appId); JwtClaims jwtClaims = jwtConsumer.processToClaims(jwt); System.out.println(jwtClaims); } public static JwtConsumer createJwtConsumer(JsonWebKeySet jsonWebKeySet, String issuer, String appId) { final JwtConsumerBuilder jwtConsumerBuilder = new JwtConsumerBuilder(); jwtConsumerBuilder.setExpectedIssuer(issuer); jwtConsumerBuilder.setRequireIssuedAt(); jwtConsumerBuilder.setRequireExpirationTime(); jwtConsumerBuilder.setAllowedClockSkewInSeconds(60); jwtConsumerBuilder.setExpectedAudience(appId); jwtConsumerBuilder.setVerificationKeyResolver((jws, nestingContext) -> { final String signKeyId = jws.getKeyIdHeaderValue(); for (JsonWebKey jsonWebKey : jsonWebKeySet.getJsonWebKeys()) { if (signKeyId.equals(jsonWebKey.getKeyId())) { return jsonWebKey.getKey(); throw new RuntimeException("Cannot find verification key: " + signKeyId); return jwtConsumerBuilder.build(); } }

输出示例如下:

```
JWT Claims Set:{sub=user_dt6kj6yf64cf4wjaknpbxjcwuu,
    jti=jwt_aaaadaiea76yh5qm3rmunz2xh4xwyi2sdph64zi,
    iss=https://eiam-api-cn-hangzhou.aliyuncs.com/v2/idaas_padyrlux3mphrlsex4uonyqhxu/app_mkif4dwlpeh6dns4pxpzbasqmu/oidc,
    iat=1653630041,
    exp=1653630341,
    aud=app_mkif4dwlpeh6dns4pxpzbasqmu,
    name=test,
    preferred_username=test,
    updated_at=1653628590
    }
```

由此获取到 IDaaS 中已登录身份信息,验证后,应用可顺利登录。

3. 其他设置

3.1. OIDC Discovery 应用发现端点说明

OIDC应用的 issuer 格式如下:

https://<idaas-api-domain>/v2/<instance_id>/<application_id>/oidc

IDaaS 支持 OpenID Connect Discovery 1.0 标准,在 issuer 后再加上 /.well-known/openid-configuration 就是该应用的 OIDC 发现端点地址。

端点	说明
authorization_endpoint	授权端点
device_authorization_endpoint	设备模式 需要标准OIDC应用支持该功能,自研应用暂时不支持设备码流登录
token_endpoint	令牌端点
revocation_endpoint	令牌吊销端点
userinfo_endpoint	用户信息端点
jwks_uri	JWK公钥端点

OIDC Discovery中 scopes_supported 与 claims_supported 有对应关系,对应的 claims_supported 清单如下表所示:

字段	scope	说明
sub	openid	用户的 userId
jti	openid	JWT ID
iss	openid	JWT签发的 issuer
iat	openid	JWT签发时间
nbf	openid	JWT有效开始时间
exp	openid	JWT过期时间
aud	openid	ClientID
at_hash	openid	AccessToken 哈希
phone_number	phone	电话号码,比如 +86 130 1234 5678
phone_number_verified	phone	电话号码是否被验证过,目前默认电话号码是已验证
email	email	电子邮箱, 比如 al***@example.com
email_verified	email	电子邮箱是否被验证过,目前默认电子邮箱是已验证
name	profile	用户显示名
preferred_username	profile	用户的 username
updated_at	profile	用户资料最后更新时间

3.2. 令牌端点支持的认证方式

根据 OIDC 协议指明,IDaaS 提供灵活性,允许以下 4 种不同方式进行身份验证。

在发现端点中返回的字段 token_endpoint_auth_methods_supported 指定了支持的认证方法。

取值	说明
none	用于 Public 客户端, 通过 none 认证方式认证时 grant_type 不能是 client_credentials
client_secret_basic	按规范 RFC 6749 - The OAuth 2.0 Authorization Framework 实现
client_secret_post	按规范 RFC 6749 - The OAuth 2.0 Authorization Framework 实现
client_secret_jwt	按规范 OpenID Connect Core 1.0 实现

上一步接收到 code 授权码,并验证请求合法(验证 state 与发起请求传入的一致)后,应用的后端服务,应使用获得的 code 向令牌端点(Token Endpoint)发起 POST 请求,请求示例如下:

以 client_secret_basic 为例, 令牌端点请求样例为:

POST /token HTTP/1.0 Host: api.aliyunidaas.com Authorization: Basic YXBwX21pY2hzN3I0*******cHll0kNTKioqKioq

grant_type=authorization_code&
code=COE59pkCTm4J******arGEaiShj7NCzLCYu9

更多说明参看 OIDC Core 1.0 规范。

3.3. 应用 ClientSecret 轮转

请参考基本配置中密钥轮转章节说明。

相关标准

- RFC6749 The OAuth 2.0 Authorization Framework https://datatracker.ietf.org/doc/html/rfc6749
- RFC6750 The OAuth 2.0 Authorization Framework: Bearer Token Usage https://datatracker.ietf.org/doc/html/rfc6750
- RFC7009 OAuth 2.0 Token Revocation https://datatracker.ietf.org/doc/html/rfc7009
- RFC7515 JSON Web Signature (JWS) https://datatracker.ietf.org/doc/html/rfc7515
- RFC7517 JSON Web Key (JWK) https://datatracker.ietf.org/doc/html/rfc7517
- RFC7518 JSON Web Algorithms (JWA) https://datatracker.ietf.org/doc/html/rfc7518
- RFC7519 JSON Web Token (JWT) https://datatracker.ietf.org/doc/html/rfc7519
- RFC7636 Proof Key for Code Exchange by OAuth Public Clients https://datatracker.ietf.org/doc/html/rfc7636
- RFC8252 OAuth 2.0 for Native Apps https://datatracker.ietf.org/doc/html/rfc8252
- RFC8628 OAuth 2.0 Device Authorization Grant https://datatracker.ietf.org/doc/html/rfc8628
- OpenID Connect Core 1.0
 https://openid.net/specs/openid-connect-core-1_0.html
 OpenID Connect Discovery 1.0
 - https://openid.net/specs/openid-connect-discovery-1_0.html

1.6.1.2. Java SpringBoot 自研应用接入 SSO 示例

本篇文档以 Java SpringBoot 为例, 讲解作为自研应用与 IDaaS 的对接。 若您希望了解对接原理和调用流程,请参考自研应用接入 SSO。

IDaaS 自研应用采用 OIDC 授权码模式,该模式向下兼容 OAuth 2.0 协议授权码模式,所以可以采用 OAuth 工具包 spring-boot-starter-oauth2-client 完成对接开发。

该工具包封装了所有的 OIDC 授权码模式调用流程和 id_token 解析过程,使用起来非常简单。

1. 引入工具包

在 pom.xml 中增加依赖: spring-boot-starter-oauth2-client , 示例如下:

<pre><pre>></pre></pre>
<groupid>org.springframework.boot</groupid>
<artifactid>spring-boot-starter-parent</artifactid>
<version>2.4.1</version>
<properties></properties>
<java.version>8</java.version>
<dependencies></dependencies>
<dependency></dependency>
<proupid>org.springframework.boot</proupid>
<artifactid>spring-boot-starter-web</artifactid>
<dependency></dependency>
<proupid>org.springframework.boot</proupid>
<pre><artifactid>spring=boot=starter=oauth2=client</artifactid></pre>

2. 配置 IDaaS 信息

将 client_id , client_secret 及 issuer 在 application.properties 中配置:

```
spring.security.oauth2.client.registration.aliyunidaas.client-id=app_***
spring.security.oauth2.client.registration.aliyunidaas.client-secret=CS***
spring.security.oauth2.client.provider.aliyunidaas.issuer-uri=<issuer>
```

上述信息,均可在应用创建后获取,请参考自研应用接入 SSO。

3. 配置 Security 需要 OAuth 认证

import org.springframework.security.config.annotation.web.builders.HttpSecurity; import org.springframework.security.config.annotation.web.configuration.EnableWebSecurity; import org.springframework.security.config.annotation.web.configuration.WebSecurityConfigurerAdapter; @EnableWebSecurity public class SecurityConfig extends WebSecurityConfigurerAdapter { @Override protected void configure(HttpSecurity http) throws Exception { http.authorizeRequests() .anyRequest().authenticated() .and()

.oauth2Login();

```
}
```

```
}
```

4. 获取 User 信息

工具包为自动完成所有的授权调用和 id_token 验证机制。

通过注入 @AuthenticationPrincipal OAuth2User user 即可获得最终的用户信息:

```
import org.springframework.security.core.annotation.AuthenticationPrincipal;
 import org.springframework.security.oauth2.core.user.OAuth2User;
 import org.springframework.web.bind.annotation.GetMapping;
  import org.springframework.web.bind.annotation.RestController;
  @RestController
 public class SampleController {
        @GetMapping("/user")
       public OAuth2User user(@AuthenticationPrincipal OAuth2User user) {
             return user;
        }
 }
最后可尝试在 /user 端点输出用户信息 :
                                                                    û 🖈 💿 🗯 🍥 :
  ← → C (i) localhost:8080/user
{"authorities":[{"authority":"ROLE_USER","attributes":
{"sub":"user_uyvefotjn7kpbejfmxoos3rtmm","email":"hatter@example.com","
email_verified":true,"name":"Hatter
Jiang","preferred_username":"hatter","updated_at":1644889269}}],"attrib
utes":
("sub":"user_uyvefotjn7kpbejfmxoos3rtmm","email":"hatter@example.com","
email_verified":true,"name":"Hatter
Jiang","preferred_username":"hatter","updated_at":1644889269},"name":"u
ser_uyvefotjn7kpbejfmxoos3rtmm")
使用这些用户信息,直接将用户登录,即可完成 SSO 过程。
```

若应用部署在代理之后

如果将应用部署在代理后面,比如阿里云SLB、Nginx等,在测试时可能会发现如下情况下:

- 用户访问 https://www.example.com
- OIDC登录跳转时产生的 redirect_uri 变成了 http://127.0.0.1:8080/oauth2/authorization/aliyunidaas 这样的形式,会导致登录不了。

如果需要解决这个问题,就需要修改 SpringBoot 生成 redirect_uri 的逻辑,具体方法是:

1. 在 SpringBoot 中配置增加配置项

server.forward-headers-strategy = NATIVE

2. 如果用户有使用阿里云SLB则需要在SLB高级配置中勾选"通过 X-Forwarded-Proto 头字段获取 SLB 的监听协议",如下图所示:



3. 如果用户在SLB与应用之间有Nginx代理,则需要在代理上配置:

proxy_set_header Host \$host; proxy_set_header X-Forwarded-Proto \$proxy_x_forwarded_proto;

4. 如果用户直接通过Nginx以HTTPS方式提供服务,则需要配置:

proxy_set_header Host \$host;
proxy_set_header X-Forwarded-Proto https;

如果您使用了他们代理类服务或软件,需要自行查找配置,最终需要确保SpringBoot收到的请求中传入了正确的 Host 及 X-forwarded-Proto 这两个HTTP Header。

相关参考资料:

https://tools.ietf.org/html/rfc7239 https://docs.nginx.com/nginx/admin-guide/web-server/reverse-proxy/ https://docs.spring.io/spring-boot/docs/current/reference/html/howto.html#howto.webserver.use-behind-a-proxy-server

1.6.2. 接入账户同步

1.6.2.1. 账户同步接入概述

背景介绍 IDaaS 支持自研应用对接,实现 IDaaS 到应用的组织/账户同步。 若希望实现应用到 IDaaS 的账户同步,请参考 <u>应用开发 API 说明。</u> 应用同步配置请参考:<u>账户同步 - IDaaS 同步到应用</u>。本篇文档介绍应用按照 IDaaS 规范完成账户同步对接。



 一致性依赖:可能有一系列相关方,依赖于您的应用中的身份数据,进行营销或验证,由此希望能够及时地从 IDaaS 同步账户的变化。例如在用户入职时,在 IDaaS 中创 建账户,HR 应用需要近乎同时创建账户,才不会耽搁入职流程。可以通过订阅 账户创建 事件实现。

● **实时性要求**:您的应用需要及时响应用户的操作。例如用户登录系统后修改了手机后,你的应用需要及时更新该用户的手机号,可以通过订阅 账户更新 事件实现。

事件回调机制说明

以上是两个简单的使用场景,开发者可以根据不同需求,订阅不同的事件,进行不同的处理。 为了满足客户的快速对接需求,我们提供了一套由 IDaaS 定义的、集成便捷、传输安全的 IDaaS 到应用同步方式,应用可以快速对接,接收同步请求。 这套机制通过事件回调机制实现。 在 IDaaS 中,您需要配置关注的事件(例如账户创建),当对应事件触发后,将自动向事件订阅者通过 HTTP POST 发送同步请求。 事件分为两个部分: • 订阅事件:在 IDaaS 管理控制台完成,配置关注的 IDaaS 事件。 • 接收事件:需要开发者按照要求,进行对接。 订阅事件 在 IDaaS 中创建应用后,可以前往【账户同步】菜单,进行应用账户同步配置。 通用配置 单点登录 账户同步

地用配直 半点豆水 赋广问少

同步到应用 同步到 IDaaS 具体配置方式,请参考账户同步 - IDaaS 同步到应用。

在下方配置中,您可以勾选当前应用关注的回调事件。

```
□ 账户创建
                          _____组织创建
回调事件
             □ 账户删除
                          _____组织删除
             □ 账户基础信息更新 □ 组织更新
             ── 账户密码更新
                          _____组织移动
             账户禁用
             □ 账户启用
             ── 账户锁定
             □ 账户解锁
             □ 账户移动
             全选 取消全选
             需要订阅对应的账户变更事件,才会触发事件回调。默认全部订阅,可随时调整。
             事件类型定义请参考: IDaaS 同步到应用
```

当事件发生时,IDaaS 将向应用发出请求。

接收回调

当事件发生时, IDaaS 会向配置的 同步接收地址 发送 POST 请求。

请求参数参考如下:

Content-Type: application/json;charset=utf-8

//IDaaS post 请求body体示例。应用拿到参数后进行验签

"event":"eyJhbGciOiJIUZ11NiISInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjMONTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKxwRJSMeKKF2QT4fwpMeJf 36POk6yJV_adQssw5c"

所有参数均在 event 字段中传递,传递的内容是包含签名的 JWT 格式 (参考 RFC 7515 JWS),

事件格式

您需要使用各语言的通用开源工具,对 JWT 信息进行解析。 出于测试目的,您也可以将 JWT 格式值粘贴到 https://jwt.io/,以直接查看其包含内容。 event 值包含两大部分, header 和 payload . header 举例:

```
{
    "kid": "KEYH1zR7XLCGcHw1hzhkCqVjnuyaAJUf6yMR",
    "typ": "JWT",
    "alg": "RS256"
}
```

payload **举例:**

```
{
  "iss":"urn:alibaba:idaas:app:event",
   "sub":"idaas-121313",
   "aud":"app_12131313",
   "exp":1640966400,
  "iat":1640966400,
  "jti": "cNetm90D5bXqfVfdvqGMYw",
   "dataEncrypted":false,
   "cipherData":"",
   "plainData":{
     "aliVid":1231313, //阿里云账号Vid
    "instanceId":"实例ID", //实例id
     "eventVersion":"V1.0", //版本号
     "eventData":[
      {
"eventId":"", //事件id
"eventType":"", //事件类型
:"":==":121313, //事件努
        "eventType":"", //事件突坐
"eventTime":121313, //事件实际发生的事件
"bizId":"业务数据id", //业务数据id。若是组织,则为组织id
"bizData":{} //具体的数据详情,不同事件类型该字段不同。可参考通讯录事件
       }
    ]
  }
}
```

其中包含的字段具体如下:

	参数名称	参数位置	参数类型	参数说明
header	alg	header	String	固定值:RS256 代表采用SHA-256的RSA签名
	kid	header	String	IDaaS 颁发的公私钥对 key ID。 验签时需要使用该 kid 对应的公钥。 IDaaS 暂不支持同步用公私钥轮转,同步公私钥信息不会变化。
payload	iss	payload	String	固定值: urn:alibaba:idaas:app:event 代表是由 IDaaS 发起的事件订阅通知。
	sub	payload	String	客户的 IDaaS 实例 id
	aud	payload	String	客户的 IDaaS 应用 id
	ехр	payload	Long	event 的过期时间,单位 ms,默认为创建时间之后 30 分钟。 若当前时间超过过期时间,应用解析时应该报错,判断过期。
	iat	payload	Long	event 的创建时间,单位 ms。若当前时间早于创建时间,应用解析时应该报 错,判断无效。
	data_encrypted	payload	Boolean	事件数据是否为加密传输。
	cipher_data	payload	String	开启加密时不为空。 该字段是加密后密文事件数据,需解密后查看内容。
	plain_data	payload	Object	关闭加密时不为空。 包含所有事件数据。

数据验签

请先对 JWT 验签,确认对应 event 事件信息是由 IDaaS 签发。若不进行验证,任何人都将可以仿造请求。

您可以通过同步菜单中的 验签公钥端点 ,获取到验签 JWT 使用的公钥信息,并使用其对发送给应用的事件内容进行有效来源验证。我们推荐您使用对应开发语言的开源 JWT 工具包进行验签工作。不在此赘述。

IDaaS 推送到应用

验签公钥端点

 https://pre-eiam-api-cn-hangzh
 2mlpq5rp

 4w
 ark
 dds3rj7r4e4/provisioning/jwks の

 请点开链接,获取公钥信息。可以通过程序调用公钥端点,动态获取。

数据解密(可选)

IDaaS 支持对推送的事件数据进行加密传输,加密后字段将在 payload 中 cipher_data 字段传递。

f.
"cipher_data": "ZePq7ckODWnL54vqZc3kTw0vF7tjvIRZjqqy/gZm9oTEt71WMufD9sw1mHzZkniSqyDGQpkmMRLCXz9gzRJ4BY2RroLUPQW8ZDPSfmJKEf2m2w6wY1twoR1nHLoFCVh
ravsvN0afBqmxd3eK5tHd05Ze6ML0XS3fqxqH61dGAm2mwecvAFPRrKVeg6JXBYUvA2Uu6dmC0P3y938kFdhodD13005MBIqWghq569wYvVjKMFMcnsZqmGGKXN0vRFhg+SR16sr24b1X/gQDbN
$\tt qy MDICB9k3QMe09d0odw NEwvgxbf1v4Pby CRX1P9U074nDQaWROWZFp1E7qP/JMy3pBr0pxW+hJS9u/Zpvj/hvLlhBTAZkmhAkDKx1ryztqrgJbr4VOUv8mlqxWjDK4I7VZugODJMSwi1HdjXL+$
wlMzPMOeH8rkDFU+b5VH3dsxg3hZ64Ukd7exB62QyyeIJpfk0d57xw8UACiSsXadexQYpJPDycVdmJ7FAmIhxbJ8I6w9Kcv9U5sKybUz1YA8tONAw=="
}

开启该特性后,您可以自主填写加密密钥,也可由 IDaaS 生成密钥。IDaaS 发出事件回调请求前,会使用该密钥将请求数据全部加密后传输。

是否加密	✓ 业务数据加密				
	若勾选,业务数据将使用加解密秘钥加密后传输。详情参考 接收 IDaaS 同步事件	•			
加解密钥	4f2c82f82ed4711b441854ca8a14df83ac44d77192297528e48 C 4	主成密钥			

AES256加密秘钥,Hex编码格式。您可以指定加解密钥,或自动由 IDaaS 生成。

IDaaS 会使用 AES-256 算法对称加密,并采用 JWE 格式对事件进行加密。

应用需要使用同样的密钥解密,才能获取同步数据。

开发对接可以参考 Java 应用接入账户同步示例。

响应返回

应用需负责按照 IDaaS 规范,返回事件处理结果。IDaaS 将记录结果,并依照返回信息进行后续处理。

执行成功

若请求处理一切正常,必须返回 event ld 及对应的结果,格式如下:

返回字段	数据类型	描述
successEvents	Array	同步成功,返回该事件
skippedEvents	Array	同步跳过(场景举例:应用接收到删除账户事件,但账户在应用系统中已不存在,则可以返回 跳过。)
failedEvents	Array	同步失败,返回该事件
retriedEvents	Array	同步重试,若返回,该事件将重试。最大重试次数5次
-eventid	String	事件 ID, 必须返回 IDaaS 当次事件 ID。 不发送或传输错误 event ld 将触发重试。
-event Code	String	错误码,IDaaS 将记录结果,便于排查问题。您可自定义 event Code。
-eventMessage	String	错误描述,IDaaS 将记录结果原因,便于排查问题。您可自定义 eventMessage。

正常返回结果示例:

{		
	"succes	sEvents": [
	{	
		"eventId": "事件ID",
		"eventCode": "SUCCESS",
		"eventMessage": "SUCCESS"
	}	
],	
	"skippe	dEvents": [
	{	
		"eventId": "事件ID",
		"eventCode": "跳过code",
		"eventMessage": "跳过描述"
	}	
],	
	"failed	Events": [
	{	
		"eventId": "事件ID",
		"eventCode": "错误code",
		"eventMessage": "错误描述"
	}	
],	
	"retrie	dEvents": [
	{	<i>+ u</i>
		"eventId": "爭忤ID",
		"eventCode": "错误code",
		"eventMessage": "
	}	
	1	
}		

🗘 注意

收到请求后,需要在10秒内以HTTP 200状态码响应该请求,否则IDaaS 会视此次推送失败并以1s、5s、10s、10s、10s的间隔重新推送事件,最多重试5次。

执行失败

若处理失败,返回 HTTP 状态码必须是 4XX 或者 5XX。 处理失败后返回的参数如下:

参数名称	数据类型	描述
error	String	错误码
error_description	String	错误描述

针对通用,建议参考如下错误码返回:

错误码	http状态码	描述
invalid_token	403	jws token校验不合法
too_many_request	429	业务方处理繁忙返回该错误后,idaas会进行流控策略进行降 级处理
internal_error	500	内部错误,idaas会自动重试

异常返回结果示例

```
{
"error": "invalid_token",
"error_description": "jws token校验不合法"
}
```

1.6.2.2. 通讯录事件

基础说明

本文档用于开发者对接 IDaaS 应用同步的能力,并详细列明了具体事件参数。 若您希望了解对接原理和调用流程,请参考 账户同步接入概述。 我们可以将所有 IDaaS 中通讯录事件分为两大类。 一、测试事件

管理员在完成应用同步配置后,可通过【测试连接】按钮,检查配置是否成功。

使用该功能,应用能够接收特殊的测试事件。

二、增量事件

增量事件指由 IDaaS 中发生的变化自动触发的操作。

通常用于 IDaaS 和应用之间数的持续、增量的同步。

三、全量事件

全量事件指管理员从 IDaaS 页面明确手动触发的同步操作。

通常用于将 IDaaS 中数据一次性导入至应用中。

事件清单

事件模块	事件类型	类型代码				
测试事件	测试连接	urn:alibaba:idaas:app:event:common:test				
	账户创建	urn:alibaba:idaas:app:event:ud:user:create				
	账户删除	urn:alibaba:idaas:app:event:ud:user:delete				
	账户基础信息更新	urn:alibaba:idaas:app:event:ud:user:update_info				
	账户密码更新	urn:alibaba:idaas:app:event:ud:user:update_password				
	账户禁用	urn:alibaba:idaas:app:event:ud:user:disable				
通讯录 "一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一	账户启用	urn: alibaba: idaas: app: event: ud: user: enable				
	账户锁定	urn:alibaba:idaas:app:event:ud:user:lock				
	账户解锁	urn:alibaba:idaas:app:event:ud:user:unlock				
	账户移动	urn:alibaba:idaas:app:event:ud:user:update_primary_ou				
	组织创建	urn:alibaba:idaas:app:event:ud:organizational_unit:create				
	组织删除	urn:alibaba:idaas:app:event:ud:organizational_unit:delete				
	组织更新	urn:alibaba:idaas:app:event:ud:organizational_unit:update				
	组织移动	urn:alibaba:idaas:app:event:ud:organizational_unit:update_parent_organizational_u nit				
通讯录	全量推送组织	urn:alibaba:idaas:app:event:ud:organizational_unit:push				
全量事件	全量推送账户	urn:alibaba:idaas:app:event:ud:user:push				

数据安全性

所有的账户/组织事件,IDaaS均会将完整的账户/组织信息作为参数,传递给事件监听方。 若数据中有敏感信息,推荐通过 HTTPs加密通道或勾选【业务数据加密】,对传输过程进行保护。 测试连接 测试配置信息的连通性,验证验签和加密能力。 一键测试时是单独的事件订阅类型:um:alibaba:idaas:app:event:common:test

请求参数验签后 payload 示例:

1								
	"iss":	"urn:alibaba:idaas:app:event",						
	"sub":	"idaas_rhhoqmlnyu3cv7ow657gyvurky",						
	"aud":	"app_mjavzivahje6zxkbc4i2bierdu",						
	"exp":	1648711369,						
	"iat":	1648709570,						
	"jti":	"bNRrCYrqXjqe8B1xweqlZw",						
	"dataEr	ncrypted": false,						
	"cipher	Data": "",						
	"plainI	Data": {						
	"inst	anceId": "idaas_rhhoqmlnyu3cv7ow657gyvurky",						
	"alit	Jid": 1519714049632764,						
	"ever	ntVersion": "V1.0",						
	"ever	ntData": [
		{						
		"eventId":"evnt_aaaac766x2somw2ptotoyk6ag6bmfkt5xpqprpq",						
		"eventType":"urn:alibaba:idaas:app:event:common:test",						
		"eventTime":"1648709509849",						
		"bizId":"evnt_aaaac766x2somw2ptotoyk6ag6bmfkt5xpqprpq",						
		"bizData":"{\"bizData\":\"req_xxxxxxxsdfsdfsfd\"}"						
		}						
]							
	}							
}								

应用成功接收后,应用侧必须在返回请求,并确保字段 successEvents 中 eventId 与请求中保持一致。

否则测试请求将失败。

{ "successEvents": [}], "skippedEvents": [{
 "eventId": "",
 "eventCode": "",
 "eventMessage": "" } "failedEvents": [{
 "eventId": "",
 "eventCode": "",
 "eventMessage": "" }], "retriedEvents": ["ret" {
 "eventId": "",
 "eventCode": "",
 "eventMessage": "" 1 }

账户创建

通过该事件订阅员工入职。

事件类型: urn:alibaba:idaas:app:event:ud:user:create

解析后的 bizData 示例:

应用身份服务

{

"password": "ssGp96", "userId": "user_4alcbywzc7jy1231u2sr1jsw7i", "username": "zhangsan", "displayName": "张三", "passwordSet": true, "phoneRegion": "",
"phoneNumber": "155****5620",
"phoneVerified": false, "email":"zh***@163.com", "emailVerified": false, "userExternalId": "user_4alcbywzc7jyl23lu2sr1jsw7i", "userSourceType": "build_in", "userSourceId": "idaas_rhhoqmlnyu3cv7ow657gyvurky", "status": "enabled", "accountExpireTime": "-1", "registerTime": "1648531553621", "lockExpireTime": "-1", "createTime": "1648531553621", "updateTime": "1648531553621", "description": "", "primaryOrganizationalUnitId": "ou_bvluxnp2ef36uupdwob6km34a4", "organizationalUnits": [{ "organizationalUnitId": "ou_bvluxnp2ef36uupdwob6km34a4", "organizationalUnitName": "研发部", "primary": true }]

}

参数说明:

参数	字段类型	说明
userld	String	用户唯一id
username	String	用户名
displayName	String	显示名称,一般为用户姓名
passwordSet	boolean	是否设置密码
phoneRegion	String	手机号区号
phoneNumber	String	手机号
phoneVerified	boolean	手机号是否验证过,暂时不进行验证。
email	String	邮箱
emailVerified	boolean	邮箱是否验证过,暂时不进行验证。
userExternalid	String	外部id。若是自建账户则和 userld 一致;若是外部同步的账户,则为来源的用户id。如来源是 钉钉,则为钉钉的userld。
userSourceT ype	String	来源类型,若为自建账户,则为 "build_id"。
userSourceld	String	来源类型 id
password	String	密码。若同步应用开启同步密码,且用户设置密码,会传该值
status	String	状态: enabled-启用, disabled-禁用
account ExpireT ime	Long	用户过期时间
registerTime	Long	注册时间

lockExpireTime	Long	锁定到期时间。即到该时间点则解锁
createTime	Long	创建时间
updateTime	Long	修改时间
description	String	描述
primaryOrganizationalUnitId	String	所属主组织机构
organizationalUnits	List	所属组织机构列表
-organizationalUnitId	String	所属组织机构唯一id
-organizationalUnitName	String	所属组织机构名称。
-primary	boolean	所属主组织机构。true-所属主组织机构,false-非主组织机构

账户删除

当员工离职时,通讯录发生变更,可订阅该事件。

事件类型: urn:alibaba:idaas:app:event:ud:user:delete

解析后的 bizData 示例: 同账户创建。

账户基础信息更新

若员工基本信息发生变更。如手机号,邮箱,姓名等发生变更,应用需要及时收到变更的信息,可通过订阅该事件。

事件类型:urn:alibaba:idaas:app:event:ud:user:update_info

解析后的 bizData 示例: 同账户创建。

账户密码更新

当账户密码发生变更时,如:管理员重置密码,用户修改密码。应用可通过订阅此事件,收到账户最新密码。

注意:在订阅该事件时,同时还需要,才会生效。否则不同步。请参考 账户同步 - IDaaS 同步到应用。

事件类型: urn:alibaba:idaas:app:event:ud:user:update_password

解析后的 bizData 示例: 同账户创建。

账户启用

账户状态发生变更,从禁用状态修改为启用状态,可订阅该事件。

事件类型: urn:alibaba:idaas:app:event:ud:user:enable

解析后的 bizData 示例:同账户创建。

账户禁用

账户状态发生变更,从启用状态修改为禁用状态,可订阅该事件。

事件类型: urn:alibaba:idaas:app:event:ud:user:disable

解析后的 bizData <mark>示例:同账户创建。</mark>

```
账户锁定
```

账户状态发生变更,如输错多次密码,导致账号锁定,暂不可用,可订阅该事件。

事件类型: urn:alibaba:idaas:app:event:ud:user:lock

解析后的 bizData 示例:同账户创建。

账户解锁

账户状态发生变更,由锁定状态变为正常状态,可订阅该事件。

事件类型: urn:alibaba:idaas:app:event:ud:user:unlock

解析后的 bizData 示例:同账户创建。

账户移动

账户所属主组织机构变更,可订阅该事件。

事件类型: urn:alibaba:idaas:app:event:ud:user:update_primary_ou

解析后的 bizData 示例: 同账户创建

组织创建

可通过该事件订阅创建组织机构。

事件类型: urn:alibaba:idaas:app:event:ud:organizational_unit:create

解析后的 bizData 示例:

{

- "organizationalUnitId": "ou_dqdvxesykpfhig2kvgrzpeoeyu",
- "organizationalUnitName": "组织部",
- "parentId": "ou_dqdvxesykpdfasdfaseoeyu",
 "organizationalUnitExternalId": "ou_dqdvxesykpfhig2kvgrzpeoeyu",
- "organizationalUnitSourceType": "build_in",
- "organizationalUnitSourceId": "idaas_rhhoqmlnyu3cv7ow657gyvurky",
- "createTime": "1648451475209",
- "updateTime": "1648451475209",
- "description":"自建" }

参数说明:

参数	字段类型	说明
organizationalUnitId	String	组织唯一id
organizationalUnitName	String	组织名称。
parentId	String	父级组织机构id
organizationalUnitExternalId	String	外部id,若组织是自建的则是 organizationalUnitId。若是外部同步进来的,如来源于钉钉,则是钉钉的部门id。
organizationalUnitSourceType	String	来源类型
organizationalUnitSourceld	String	来源类型id
createTime	Long	创建时间
updateTime	Long	修改时间,同lastUpdatedTime
description	String	描述

组织删除

可通过该事件订阅删除组织机构。

事件类型: urn:alibaba:idaas:app:event:ud:organizational_unit:delete

解析后的 bizData 示例:同组织创建。

组织更新

可通过该事件订阅修改组织机构基础信息,如组织机构名称。

事件类型: urn:alibaba:idaas:app:event:ud:organizational_unit:create

解析后的 bizData 示例:同组织创建。

组织移动

可通过该事件订阅组织机构更新父组织机构。

事件类型: urn:alibaba:idaas:app:event:ud:organizational_unit:update_parent_organizational_unit

解析后的 bizData 示例:同组织创建。

全量推送组织机构

事件类型: urn:alibaba:idaas:app:event:ud:organizational_unit:push

解析后的 bizData 示例: 同组织创建。

全量推送账户

事件类型: urn:alibaba:idaas:app:event:ud:user:push

解析后的 bizData 示例:同组织创建。

1.6.2.3. Java 应用接入账户同步示例

本篇文档以 Java 为例,讲解作为应用与 IDaaS 的对接。 若您希望了解对接原理和调用流程,请参考 账户同步接入概述。 接入账户同步可能需要处理两点:

● 验签

解密(可选)

进行完上述过程后,即可获取到该次事件的请求内容,应用自行处理即可。

1. 验签

参考 账户同步 - IDaaS 同步到应用 中操作,从应用同步配置中获取公钥端点。

驗签公钥送点 https://pre-eiam-api-cn-hangzhou.aliyun-inc.com/v2/idaas_wwxgovp6fag2mlpq5rp4w5pgrm/app_mig7

```
JI編点 pnwavgy6cyqilynwkkqa7m/provisioning/jwks 日
请点开链接,获取公钥信息。可以通过程序调用公钥端点,动态获取。
```

在本文档示例中,提供了直接从公钥端点获取公钥的 Java 工具类。若您所选开发语言需要公钥信息,可能需要您点开公钥端点,获取公钥内容,转化成 .pem 文件格式存储 在本地。

公钥示例:

<dependency> <groupId>org.bitbucket.b_c</groupId> <artifactId>jose4j</artifactId> <version>0.7.9</version>

</dependency>

工具类代码如下,用于从 IDaaS 公钥端点获取公钥并验签,您可以直接复制使用:

import org.apache.commons.codec.binary.StringUtils; import org.jose4j.jwk.JsonWebKey; import org.jose4j.jwk.JsonWebKeySet; import org.jose4j.jwt.consumer.JwtConsumer; import org.jose4j.jwt.consumer.JwtConsumerBuilder; import org.jose4j.lang.JoseException; import java.io.ByteArrayOutputStream; import java.io.IOException; import java.io.InputStream; import java.net.URL; import java.net.URLConnection; import java.nio.charset.StandardCharsets; import java.util.concurrent.ConcurrentHashMap; import java.util.concurrent.ConcurrentMap; public class JwtUtil { private final static ConcurrentMap<String, JsonWebKeySet> IDAAS_SIGN_JWK_SET_MAP = new ConcurrentHashMap<>(); public static JwtConsumer createJwtConsumerFromUrl(String jwkUrl, String appId) { try { final JsonWebKeySet jsonWebKeySet = getJsonWebKeySetByUrl(jwkUrl); return createJwtConsumer(jsonWebKeySet, appId); } catch (Exception e) { throw new RuntimeException("Fetch JWKs from url failed: " + e.getMessage() + ", " + jwkUrl, e); } 3 public static JwtConsumer createJwtConsumer(JsonWebKeySet jsonWebKeySet, String appId) { final JwtConsumerBuilder jwtConsumerBuilder = new JwtConsumerBuilder(); jwtConsumerBuilder.setExpectedIssuer("urn:alibaba:idaas:app:event"); jwtConsumerBuilder.setRequireExpirationTime(); jwtConsumerBuilder.setRequireJwtId(); jwtConsumerBuilder.setRequireIssuedAt(); jwtConsumerBuilder.setRequireExpirationTime(); jwtConsumerBuilder.setMaxFutureValidityInMinutes(1); jwtConsumerBuilder.setAllowedClockSkewInSeconds(120); jwtConsumerBuilder.setExpectedAudience(appId); jwtConsumerBuilder.setVerificationKeyResolver((jws, nestingContext) -> { final String signKeyId = jws.getKeyIdHeaderValue(); for (JsonWebKey jsonWebKey : jsonWebKeySet.getJsonWebKeys()) { if (StringUtils.equals(jsonWebKey.getKeyId(), signKeyId)) { return jsonWebKey.getKey(); } throw new RuntimeException ("Cannot find verification key: " + signKeyId); return jwtConsumerBuilder.build(); } synchronized private static JsonWebKeySet getJsonWebKeySetByUrl(String jwkUrlString) throws IOException, JoseException { JsonWebKeySet jsonWebKeySet = IDAAS_SIGN_JWK_SET_MAP.get(jwkUrlString); if (isonWebKevSet == null) { jsonWebKeySet = innerGetJsonWebKeySetByUrl(jwkUrlString); IDAAS_SIGN_JWK_SET_MAP.put(jwkUrlString, jsonWebKeySet); return jsonWebKeySet; } private static JsonWebKeySet innerGetJsonWebKeySetByUrl(String jwkUrlString) throws IOException, JoseException { final URL jwkUrl = new URL(jwkUrlString); final URLConnection urlConnection = jwkUrl.openConnection(); urlConnection.setConnectTimeout(50000); urlConnection.setReadTimeout(50000); final String jwkSetJson = new String(readAll(urlConnection.getInputStream()), StandardCharsets.UTF 8); return new JsonWebKeySet(jwkSetJson); public static byte[] readAll(InputStream inputStream) throws IOException { final byte[] buffer = new byte[1024 * 8]; final ByteArrayOutputStream baos = new ByteArrayOutputStream(); for (int len; ((len = inputStream.read(buffer)) != -1);) { baos.write(buffer, 0, len); return baos.toByteArray(); } }

调用示例代码:

//公钥->IDaaS应用同步配置里,访问应用公钥端点后获取到。

String publicKey = "{ \n "

- \"keys\": [\n" + "
- + " {\n"
- + " \"kty\": \"RSA\",\n"
- + **"** \"e\": \"AQAB\",\n"
- + " \"use\": \"sig\",\n" + "
- \"kid\": \"KEYHH4yFa1cpZdrs1HqNo1nJ7nM2FR3595P1\",\n" + "
- \"n\": \"oy_xxxxxxxxxxxxxxxxxxxxxxxxxx95d1padSEABqIbcTKcnlTaET3WHaR"
- + "-3MvsooeZWluv94GQEp-U2jzMladgTqBl_7KPjUk0dwrZbob_8pOLX5UQMF70o_nH5-H5EyL9-yGGhFA4oeuA"
- + "-b73qXShxP7eHs5xTT1kiYEu2NE3rBZdtrRWUIC_hlDvZMtyWF0Pwm3dpLiwCcllgcKvVuSEXyCBj6Gjevn3_clguVQ2kHlNOVyNn6Ky1iGQJzXctJCEJ5fnBRs4XZZbPNSc iYMD2-___cRdbYPtGyyuoEAfouw\"\n"
 - + " }\n" + "]\n"
 - + "}";;
- //应用ID->应用列表中,找到对应的应用ID

String appId = "app_mjavzivahje6zxxxx";

//JwtUtil->下面已提供JwtUtil工具类 JwtConsumer jwtConsumer = JwtUtil.createJwtConsumer(new JsonWebKeySet(publicKey),appId);

//JWT**验签后,获取到**payload

//event参数值->接口接收到的参数值 JwtClaims jwtClaims = jwtConsumer.processToClaims("event参数的值"); //**获取到具体的**payload Map<String, Object> map = jwtClaims.getClaimsMap(); //接下来,根据具体的数据,做对应的业务处理

2. 解密(可选)

数据解密

若应用开启业务数据加密,事件数据将通过 cipher_data 加密传递,业务方需要解密,以获取到同步数据。

IDaaS 支持自主填写加密密钥,也可由 IDaaS 生成。

是否加密	✓ 业务数据加密			
	若勾选,业务数据将使用加解密秘钥加密后传输。详情参考 接收 IDaaS 同步事件 。			
加解密钥	4f2c82f82ed4711b441854ca8a14df83ac44d77192297528e4{ C 生成密钥			
	AES256加密秘钥,Hex编码格式。您可以指定加解密钥,或自动由 IDaaS 生成。			

将密钥复制出来, 解密时使用。

新增 Maven 依赖:

<dependency> <groupId>org.bitbucket.b_c</groupId> <artifactId>jose4j</artifactId> <version>0.7.9</version> </dependency> <dependency> <groupId>org.bouncycastle</groupId> <artifactId>bcprov-jdk15on</artifactId> <version>1.70</version> </dependency>

解密示例代码:

public String decrypte(String cipherData, String key) throws JoseException { String alg = "AES";

// **生成使用密钥生成** KeySpec

SecretKeySpec secretKeySpec = new SecretKeySpec(Hex.decode(key), alg); JsonWebKey jsonWebKey = JsonWebKey.Factory.newJwk(secretKeySpec);

JsonWebEncryption receiverJwe = new JsonWebEncryption();

// 设定加解密机制

AlgorithmConstraints algConstraints = new AlgorithmConstraints(AlgorithmConstraints.ConstraintType.PERMIT, new String[]{"dir"}); receiverJwe.setAlgorithmConstraints(algConstraints);

AlgorithmConstraints encConstraints = new AlgorithmConstraints (AlgorithmConstraints.ConstraintType.PERMIT, new String[]{"A256GCM", "A192GCM", "A128GCM"}); ${\tt receiverJwe.setContentEncryptionAlgorithmConstraints (encConstraints);}$

// 传入密钥和密文

receiverJwe.setKey(jsonWebKey.getKey()); receiverJwe.setCompactSerialization(cipherData);

// 返回解密内容

return new String(receiverJwe.getPlaintextBytes(), StandardCharsets.UTF_8);

}

1.6.3. 应用开发 API 对接

1.6.3.1. 应用开发 API 说明

1. 概述

本文档为 IDaaS 对外提供的组织和账户相关的 API 文档,开发者可根据该文档进行集成 IDaaS 账户组织数据的操作管理。

接口分四部分:

- 1. 获取认证令牌接口,所有其他接口,均依赖令牌调用。
- 2. <u>账户查询和管理接口</u>
- 3. <u>组织查询和管理接口</u>
- 4. 获取同步范围接口,账户/组织管理需在指定的同步范围内。

2. 接口调用方式

接口认证

IDaaS 开放的大部分接口,均需要先获取 access_token,才能调用。

请参照 ,从应用的【通用配置】中 ,获取 client_id 和 client_secret ,并进一步 获取令牌。

? 说明

注意:与阿里云 OpenAPI 不同, IDaaS 应用开放的 Developer API 依赖于 IDaaS 中应用的密钥,并在 IDaaS 应用管理中分配接口调用权限。Developer API 权限不依赖于 RAM。

SDK、样例代码 和调试

推荐您使用 SDK 调用接口。

通过 阿里云 OpenAPI 开发者门户,IDaaS 支持如下便捷 SDK 相关操作:

- 在线查看 接口文档
- 在线 调试接口
- 各语言 SDK 下载/安装(Java/Python/Go/PHP/C#/C++/TypeScript)
- 各语言、各接口 SDK 调用 示例代码



您可以在 调试接口 页面,通过【下载完整工程】,参考 SDK 安装方法和调用示例。

SDK 版本选择: 升级版 SDK	原版 SDK	查看两者区别
-------------------	--------	--------

								SUK 1	问题, 泉古 〇 0	21
	📕 Java	📕 Java (异	步) 🖪 TypeScript	° GO Go	🕐 PHP	🔁 Python	🕓 C#	C + C++		
48	lines			▷ 运行示例	1 T	载完整工程	₽ 复制	SDK 依赖信息●	获取 AK♂	
1	// This f	ile is auto-g	enerated, don't edit i	t. Thanks.						ī
2	package o	om.aliyun.sam	ple;							

API 调用

作为备选方案, IDaaS 同时支持您使用对应的开发/测试工具,直接调用 API。请您参考文档:应用开发 API 列表。

接口列表

接口详情请查看: 应用开发 API 列表。

分类 场景 接口列表 权限值【在应用管理中设置	1
---	---

令牌	获取令牌	• 获取令牌: GenerateToken	-
	账户管理接口	 创建账户: CreateUser 更新账户: PatchUser 删除账户: DeleteUser 	urn:alibaba:idaas:scope:user: manager_all
XIX /	账户查询接口	 获取账户信息: Get User 查询账户列表: List Users 获取账户密码策略: Get UserPasswordPolicy 	urn:alibaba:idaas:scope:user:r ead_all
	组织管理接口	 创建机构: CreateOrganizationalUnit 部分修改机构信息: PatchOrganizationalUnit 删除机构: DeleteOrganizationalUnit 	urn: alibaba: idaas: scope: organi zational_unit: manager_all
道教	组织查询接口	 获取机构信息: GetOrganizationalUnit 查询机构列表: ListOrganizationalUnits 获取机构祖先列表: ListOrganizationalUnitParentIds 	urn: alibaba: idaas: scope: organi zational_unit: read_all
同步范围	获取同步范围	● 获取同步范围: GetApplicationProvisioningScope	-

1.6.3.2. 应用开发 API 列表

通用接口说明

请求域名

所有接口请求的域名为: eiam-developerapi.cn-hangzhou.aliyuncs.com

通用参数

参数名称	数据类型	参数位置	是否必填	描述
instance_id	String	path	是	实例 ID
application_id	String	path	是	应用 ID

以上两个参数在请求 URL 中以路径变量的方式统一传递。

每个 IDaaS 接口均会验证传入信息和当前访问令牌权限是否一致。

通用错误码信息

所有接口调用错误的时候 http 状态码都应该返回 4XX 或者 5XX。 错误调用后返回的参数如下:

参数名称	数据类型	描述
error	String	错误码
error_description	String	错误描述

通用错误码:

错误码	http状态码	描述
invalid_token	400	access_token 无效
application_disabled	403	应用处于禁用状态
application_api_disabled	403	应用开放API处于禁用状态
permission_denied	403	接口缺少授权
application_not_found	404	应用不存在

internal_error	500	内部错误
----------------	-----	------

请您针对上述错误信息,统一处理 IDaaS 接口返回的错误信息。

一、获取 token

1.1. 获取 access_token

IDaaS 通过 OAuth Client Credentials 客户端模式提供应用获取服务令牌的接口。

该模式暂不支持令牌刷新机制。当令牌过期后,请获取新令牌。

IDaaS 获取令牌的接口支持多种传递密钥的方式,以下以 client_secret_post 为例。

接口说明

- POST /v2/\${instance_id}/\${application_id}/oauth2/token
- token 默认有效时长 20 分钟。

请求参数

参数名称	数据类型	参数位置	是否必填	描述
instance_id	String	path	是	实例ID
application_id	String	path	是	应用ID
client_id	String	query	是	客户端D
client_secret	String	query	是	客户端密钥
grant_type	String	query	是	授权方式,填client_credentials

请求样例

curl -X POST \

https://\${spDomain}/v2/\${instance_id}/\${application_id}/users \

-H 'cache-control: no-cache' \setminus

-H 'content-type: application/x-www-form-urlencoded' $\$

-d 'grant_type=client_credentials&client_id=app_001&client_secret=xxxx'

正确响应样例

```
"token_type": "Bearer",
"access_token": "ATxxxx",
"expires_in": 1200,
"expires_at": 1653441402
```

}

{

二、账户查询/管理

2.1 创建账户

接口说明

• POST /v2/\${instance_id}/\${application_id}/users

限定在同步范围内创建新账户。

请求参数

参数名称	数据类型	参数位置	是否必填	描述
Authorization	String	header	是	格式: Bearer \${access_token}
username	String	body	是	账号名称
displayName	String	body	是	账户显示名称
password	String	body	是	密码

身份管理服务公共云合集·EIAM 云身份 服务

email	String	body	否	邮箱
emailVerified	Boolean	body	否	邮箱是否已验证
phoneRegion	String	body	否	手机国家代码
phoneNumber	String	body	否	手机号
phoneNumberVerified	Boolean	body	否	手机号是否已验证
userExternalId	String	body	否	关联的外部ID
primaryOrganizationalUnitId	String	body	是	主组织ID
description	String	body	否	描述

响应参数

参数名称	数据类型	描述
userid	String	账户ID

错误码

错误码	http状态码	描述
ResourceDuplicated.xxxx	400	参数xxxx已存在
MissingParameter.xxxx	400	缺少参数xxxx
InvalidParameter.xxxx	400	参数xxxx无效
OrganizationUnitIdNotInScopes	400	主组织不在授权范围内或不存在
UserEmailAlreadyExist	400	账户邮箱已存在
UserPhoneNumberAlreadyExist	400	账户手机号已存在

请求样例

{
 "username":"zhangsanl",
 "displayName":"李四",
 "description":"我的账号",
 "primaryOrganizationalUnitId": "ou_001",
 "userExternalId": "user_001",
 "phoneRegion": "86",
 "phoneNumberV:rified": true,
 "mailVerified": true,
 "password": "\$sfdsfl2AAfa_"
}

正确响应样例

{ "userId": "user_001" }

2.2 修改账户

接口说明

• Patch /v2/\${instance_id}/\${application_id}/users/\${userId}

• 部分修改账户信息,参数为空,则认为不做更新,否则更新,不存在的参数会被忽略

```
• 限定在应用设定的同步范围内。
```

请求参数

参数名称	数据类型	参数位置	是否必填	描述
Authorization	String	header	是	格式:Bearer \${access_token}
userld	String	path	是	账户ID
username	String	body	否	账号名称
displayName	String	body	否	账号显示名称
userExternalId	String	body	否	账户外部 ID
email	String	body	否	邮箱,
emailVerified	Boolean	body	否	邮箱是否已验证
phoneRegion	String	body	否	手机国家代码,默认中国,即 "86"。
phoneNumber	String	body	否	手机号
phoneNumberVerified	Boolean	body	否	手机号是否已验证
description	String	body	否	描述

响应参数

无。响应 200 代表成功。

请求样例

{
 "username":"才和gsanl",
 "displayName":"李四",
 "description":"我的账号,
 "userExternalId": "user_Ool",
 "phoneRegion": "86",
 "phoneNumber": 1560000****",
 "phoneNumberVerified": true,
 "emailVerified": true
 }
}

错误响应样例

```
{
    "error": "ResourceNotFound.User",
    "error_description": "The specified User resource: user_001 not found."
}
```

2.3 获取账户信息

接口说明

- GET /v2/\${instance_id}/\${application_id}/users/\${userld}
- 获取账户信息。
- 限定在应用设定的同步范围内。

```
请求参数
```

参数名称	数据类型	参数位置	是否必填	描述
Authorization	String	header	是	格式: Bearer \${access_token}

身份管理服务公共云合集·EIAM 云身份 服务

应用身份服务

userld	String	path	是	账户ID

响应参数

11=> M				
参数名称	数据类型	参数位置	是否必填	描述
userld	String	body	是	账户ID
username	String	body	是	账户账号
displayName	String	body	是	账户显示名称
email	String	body	否	邮箱
emailVerified	Boolean	body	否	邮箱是否已验证
phoneRegion	String	body	否	手机国家代码
phoneNumber	String	body	否	手机号
phoneNumberVerified	Boolean	body	否	手机号是否已验证
userExternalId	String	body	是	关联的外部ID
userSourceT ype	String	body	是	来源类型
userSourceld	String	body	是	来源ID
status	String	body	是	启用/禁用状态,值为 "enabled"/"disabled"。
accountExpireTime	Long	body	否	账户过期时间
registerTime	Long	body	否	账户注册时间
lockExpireTime	Long	body	否	锁定过期时间
createTime	Long	body	否	创建时间
updateTime	Long	body	否	最近一次更新时间
organizationalUnits	List	body	是	账户所在机组织表
organizationalUnitId	String	body	是	组织ID
organizationalUnitName	String	body	是	组织名称
• primary	Boolean	body	是	是否主组织
description	String	body	否	描述

正确响应样例

应用身份服务

{ "userId":"1234567",

"username":"xxxx", "displayName":"xxxxx", "email":"t****@example.com", "emailVerified": true, "phoneRegion":"86",
"phone":"1560000****",
"phoneNumberVerified": true, "userExternalId":"xxxx", "userSourceType":"xxxx", "userSourceId":"xxxx", "accountExpireTime":-1, "registerTime":1653551629139, "lockExpireTime":-1, "createTime":1653551629139, "updateTime":1653551629139, "description":"xxxxxx", "organizationalUnits":[{ "organizationalUnitId":"123", "organizationalUnitName": "xxx", "primary": true }] }

错误响应样例

{

"error": "ResourceNotFound.User", "error_description": "The specified User resource: user_001 not found."

}

2.4 查询账户列表

接口说明

- GET /v2/\${instance_id}/\${application_id}/users
- 获取账户基础信息列表。
- 限定在应用设定的同步范围内。

请求参数

参数名称	数据类型	参数位置	是否必填	描述
Authorization	String	header	是	格式:Bearer \${access_token}
organizationalUnitId	String	query	否	组织ID
pageNumber	Integer	query	否	开始读取的位置,默认为1
pageSize	Integer	query	否	本次读取最大记录数,范围1到100

响应参数

参数名称	数据类型	参数位置	是否必填	描述
totalCount	Integer	body	是	数据总条数
users	List			
• userld	String	body	是	账户ID
• username	String	body	是	账号名称
displayName	String	body	是	账户显示名
• email	String	body	否	邮箱
• emailVerified	Boolean	body	否	邮箱是否已验证

身份管理服务公共云合集·EIAM 云身份 服务

• phoneRegion	String	body	否	手机国家代码
phoneNumber	String	body	否	手机号
phoneNumberVerified	Boolean	body	否	手机号是否已验证
• userExternalId	String	body	是	关联的外部ID
• userSourceType	String	body	是	来源类型
userSourceld	String	body	是	来源ID
• status	String	body	是	状态
accountExpireTime	Long	body	否	账号过期时间
• registerTime	Long	body	否	账户注册时间
• lockExpireTime	Long	body	否	锁定过期时间
createTime	Long	body	否	创建时间
• updateTime	Long	body	否	最近一次更新时间
• description	String	body	否	描述

正确响应样例

{ "totalCount": 100, "users":[{ "userId":"1234567", "username":"xxxx", "displayName":"xxxxx", "passwordSet": true, "email":"t****@example.com", "emailVerified": true, "phoneRegion":"86", "phone":"1560000****", "phoneNumberVerified": true, "userExternalId":"xxxx", "userSourceType":"xxxx", "userSourceId":"xxxx", "accountExpireTime":-1, "registerTime":1653551629139, "lockExpireTime":-1, "createTime":1653551629139, "updateTime":1653551629139, "description":"xxxxxx' }] }

错误响应样例

```
{
  "error": "invalid_token",
  "error_description": "Access token expired or has been revoked"
}
```

2.5 查询账户密码策略

接口说明

- GET /v2/\${instance_id}/\${application_id}/users/_/actions/getUserPasswordPolicy
- 获取账户密码策略。
- 限定在应用设定的同步范围内。

请求参数

应用身份服务

身份管理服务公共云合集·EIAM 云身份 服务

参数名称	数据类型	参数位置	是否必填	描述
Authorization	String	header	是	格式: Bearer \${access_token}

响应参数

参数名称	数据类型	参数位置	描述
activeCycle	Integer	body	密码周期,单位秒,默认-1,永不失效
minLength	Integer	body	密码最小长度
reservationCount	Integer	body	保存密码最近次数,不能设置为最近使用过 的密码
passwordComplexityItem	List		
containUpperCase	Boolean	body	是否包含大写字母
containLowerCase	Boolean	body	是否包含小写字母
• containNumber	Boolean	body	是否包含数字
containSpecialChar	Boolean	body	是否包含特殊字符
• emailCheck	Boolean	body	是否进行密码不能包含邮箱检测
• usernameCheck	Boolean	body	是否进行"密码不能包含账户名的检测"
displayNameCheck	Boolean	body	是否进行"密码不能包含显示名检测"
phoneCheck	Boolean	body	是否进行"密码不能包含手机号检测"

正确响应样例

```
{
   "instanceId": "idaas_h6pmuhzub3vbdp3exsyabvn33m",
   "passwordComplexityItem": {
        "containUpperCase": true,
        "containNumber": true,
        "containSpecialChar": true,
        "emailCheck": true,
        "displayNameCheck": true,
        "displayNameCheck": true,
        "phoneCheck": true
    },
    "activeCycle": -1,
    "minLength": 16,
    "reservationCount": 10
}
```

错误响应样例

```
{
  "error": "invalid_token",
  "error_description": "Access token expired or has been revoked"
}
```

三、组织管理和查询

```
3.1 创建新组织
```

接口说明

- POST /v2/\${instance_id}/\${application_id}/organizationalUnits
- 在指定组织下创建新组织。
- 限定在应用设定的同步范围内。

请求参数

参数名称	数据类型	参数位置	是否必填	描述
Authorization	String	header	是	格式:Bearer \${access_token}
organizationalUnitName	String	body	是	组织名称
parentId	String	body	是	父组织ID
organizationalUnitExternalId	String	body	ጽ	组织的外部ID 不指定则与生成的组织ID一样
description	String	body	是	描述

请求样例

{

```
"organizationalUnitName":"it部",
```

"parentId":"ou_xxxss01", "description":"1234567", "organizationalUnitExternalId": "xxxx" }

正确响应样例

```
{
    "organizationalUnitId": "ou_001"
```

```
}
```

错误响应样例

```
{
```

"error":"MissingParameter.OrganizationalUnitName", "error_description":"The specified parameter:OrganizationalUnitName is required!"

```
}
```

3.2 获取指定组织信息

接口说明

- GET /v2/\${instance_id}/\${application_id}/organizationalUnits/\${organizationalUnitId}
- 获取指定组织的信息。
- 限定在应用设定的同步范围内。

请求参数

参数名称	数据类型	参数位置	是否必填	描述
Authorization	String	header	是	格式:Bearer \${access_token}
organizationalUnitId	String	path	是	组织ID

响应参数

参数名称	数据类型	描述
instanceld	String	实例ID
organizationalUnitId	String	组织ID
organizationalUnitName	String	组织名称
parentId	String	上级组织ld
organizationalUnitExternalId	String	组织外部ID

organizationalUnitSourceType	String	来源类型, build_in[自建],ding_talk[钉钉导入],ad[AD导 入],ldap[LDAP导入]
organizationalUnitSourceId	String	来源D
createTime	Long	创建时间
updateT ime	Long	最近一次更新时间
description	String	描述

正确响应样例

{
 "organizationalUnitId": "1234567",
 "organizationalUnitName": "it部",
 "parentId": "xxx",
 "organizationalUnitExternalId": "xxxx",
 "organizationalUnitSourceType": "xxxx",
 "organizationalUnitSourceId": "xxxx",
 "createTime":1653550138462,
 "updateTime":1653550138462,
 "description": "xxxxxx"
}

3.3 更新组织信息

接口说明

• PATCH /v2/\${instance_id}/\${application_id}/organizationalUnits/\${organizationalUnitId}

- 修改组织信息。
- 限定在应用设定的同步范围内。

请求参数

参数名称	数据类型	参数位置	是否必填	描述
Authorization	String	header	是	格式: Bearer \${access_token}
organizationalUnitId	String	path	是	组织ID
organizationalUnitName	String	body	否	组织名称
description	String	body	否	描述

请求样例

- {
- "organizationalUnitName": "it部", "description":"xxxxxx"
- "description
 }

正确响应样例

{

}

"instanceId": "idaas_h6pmuhzub3vbdp3exsyabvn33m",
"organizationalUnitId": "ou_lloqvor2jbexeafkjwwx34vzha",
"organizationalUnitName": "dsad1111sas1xc",
"parentId": "ou_penjtomawyoo1622uc6316boea",
"organizationalUnitExternalId": "fsddfsf",
"organizationalUnitSourceType": "build_in",
"organizationalUnitSourceId": "idaas_001",
"createTime": 1653550138462,
"updateTime": 1653550138462,
"description": "fdsfsfs"

错误响应样例

{
 "error": "invalid_token",

"error_description": "Access token expired or has been revoked"
}

3.4 查询组织列表

接口说明

- GET /v2/\${instance_id}/\${application_id}/organizationalUnits/
- 查询组织列表。
- 限定在应用设定的同步范围内。

请求参数

参数名称	数据类型	参数位置	是否必填	描述
Authorization	String	header	是	格式:Bearer \${access_token}
parentId	String	query	是	父组织 ID
pageNumber	Integer	query	否	开始读取的位置,默认为1
pageSize	Integer	query	否	本次读取最大记录数,1到100

正确响应样例

```
[{
"organizationalUnitId": "1234567",
```

```
"organizationalUnitName": "it部",
"parentId": "ou_xx01",
"organizationalUnitExternalId": "fsddfsf",
"organizationalUnitSourceType": "build_in",
"organizationalUnitSourceId": "idaas_001",
"createTime":1653551629139,
"updateTime":1653551629139,
"description":"xxxxxx"
}]
```

错误响应样例

{
 "error": "invalid_token",

"error_description": "Access token expired or has been revoked"

3.5 删除组织

接口说明

}

- DELETE /v2/\${inst ance_id}/\${applicat ion_id}/organizat ionalUnits/\${organizat ionalUnitId}
- 删除指定组织。
- 限定在应用设定的同步范围内。

请求参数

参数名称	数据类型	参数位置	是否必填	描述
Authorization String		header	是 格式:Bearer \$access	
organizationalUnitId	String	path	是	组织ID

正确响应样例

```
无。响应 200 代表成功。
```

错误响应样例

```
{
   "error": "invalid_token",
   "error_description": "Access token expired or has been revoked"
```

```
}
```

3.6 查询先代组织

接口说明

- GET /v2/\${instance_id}/\${application_id}/organizationalUnits/\${organizationalUnitId}/parentIds
- 查询指定组织的先代节点列表。
- 限定在应用设定的同步范围内。

请求参数

参数名称	数据类型	参数位置	是否必填	描述
Authorization	String	header	是	格式: Bearer \${access_token}
organizationalUnitId	String	path	是	组织ID

正确响应样例

```
{
    "parentIds": [
```

```
"ou_penjtomawyocl622uc63i6boea"
```

```
}
```

错误响应样例

```
{
```

```
"error": "invalid_token",
"error_description": "Access token expired or has been revoked"
```

```
}
```

四、获取应用同步范围(可选)

4.1. 获取应用同步范围

IDaaS 中可为应用设定一个或多个组织为同步范围,所有对账户/组织的操作,均需要在同步范围内。

可以通过当前接口,获取当前应用的同步范围组织列表。

接口说明

• GET /v2/\${instance_id}/\${application_id}/provisioningScope

获取应用同步范围

请求参数

参数名称	数据类型	参数位置	是否必填	描述
Authorization	String	header	是	格式: Bearer \${access_token}

响应参数

参数名称	数据类型	描述
organizationalUnitIds	List <string></string>	组织ID列表

请求样例

```
curl -X POST \
https://${spDomain}/v2/${instance_id}/${application_id}/provisioningScope \
-H 'authorization: Bearer ${access_token}'
```

正确响应样例

```
{
   "organizationalUnitIds": [
    "ou_001"
  ]
}
```

1.6.4. 开源代码参考

阿里云 IDaaS 开源代码库: https://github.com/aliyunidaas

阿里云 IDaaS 将一系列集成样例代码开源,供企业应用的开发者对接使用。

如下为开源代码库。每个库中,都有完整的配置使用、开发说明,请参考:

库名	说明	链接
java-spring-oidc-sample	应用参照 OIDC 协议(授权码模式)实现 SSO 的样例,最常用的接入方法,也即 IDaaS 中自 研应用接入方法。	https://github.com/aliyunidaas/java- spring-oidc-sample
java-spring-saml-sample	应用参照 SAML 协议实现 SSO 的样例。	https://github.com/aliyunidaas/java- spring-saml-sample
java-device-code-flow-sample	应用参照 OIDC 协议(设备流)实现 SSO 的样例,用于设备端无浏览器情况下的安全登录。	https://github.com/aliyunidaas/java- device-code-flow-sample
java-fc-ram-user-push-sample	使用阿里云函数计算(Function Compute)作为中转服务,实现 IDaaS 同步账户到 RAM 中。	https://github.com/aliyunidaas/java-fc- ram-user-push-sample
java-sync-sdk	应用接收 IDaaS 同步推送的基础 SDK。	https://github.com/aliyunidaas/java- sync-sdk
java-fc-sync-sdk	在 java-sync-sdk 基础上,函数计算接收 IDaaS 同步的参考代码。	https://github.com/aliyunidaas/java-fc- sync-sdk

1.7. 其他

1.7.1. 常规资源限额

为了保障公共云资源不被恶意或无意浪费,IDaaS 对所有实例(免费或付费)均具有如下默认资源限制。

以下限制目的仅在于规避非正常使用场景造成的浪费,普遍情况下不应触发限制。

若您为正常使用情况且超配额(如确实有超出 1万用户数、500 个组织等),请联系我们为您提高配额。

限额项	数量	说明
创建实例数	3	每个阿里云账户最多可创建 3 个 IDaaS 实例
实例账户数	10000	每个实例最多 10000 个账户,超出请联系我们提额。
实例组织数	500	每个实例最多 500 个账户,超出请联系我们提额。
组织深度	10	最多 10 层组织嵌套
登录方式数	10	最多 10 种登录方式
应用数	1000	每个实例最多 1000 个应用
应用同步范围对象数	10	最多设置 10 个组织和组作为同步范围对象。
应用下单个主账户的最大应用账户数	5	每个账户针对一个应用,最多可扮演 5 个不用的应用账户。
钉钉 IdP 数量	20	身份提供方中可创建的最大钉钉 IdP 数量
入方向其他 IdP 数量	30	除了钉钉以外的其他所有入方向 IdP
出方向其他 IdP 数量	50	除了钉钉以外的其他所有出方向 IdP

少部分老版本实例的限额与上不同,若有出入,可联系我们处理。

곗 说明

随着增强完善,IDaaS 未来可能介绍新的配额项,并可能根据市场反馈对已有项目进行调整。

1.7.2. 常用应用配置

1.7.2.1. 阿里云用户 SSO

本文为您介绍如何在 IDaaS 中配置阿里云用户单点登录。使用用户SSO,您的企业成员将以 RAM 用户访问阿里云。

应用简介

阿里云——阿里巴巴集团旗下公司,是领先的云计算及人工智能科技公司。提供免费试用、云服务器、云数据库、云安全、云企业应用等云计算服务,以及大数据、人工智 能服务、精准定制基于场景的行业解决方案。免费备案,7x24 小时售后支持,助企业无忧上云。

操作步骤

- 一、创建应用
- 1. 登录 IDaaS管理控制台。
- 2. 前往 应用-添加应用-应用市场,搜索到阿里云用户 SSO 应用模板。点击添加应用。

C→ 阿里云用户SSO	永久免费
RAM用户SSO,用户自己选择账号名属性取值方式,并支持 辅助域名	自定义RAM
SSO	
添加应用	

3. 确认应用名称,即可完成添加。

添加应用 - 阿里;	云用户SSO	×
• 应用名称	阿里云用户SSO 应用的显示名称。	
		立即添加

二、配置应用单点登录

1. 添加应用后,将自动跳转到应用单点登录配置页,您将在此处进行配置。

云身份服务 / 应用 /	添加雇用 / 阿里云用户SSO	
← 阿里云)	用户SSO	
通用配置 单	点 登录 账户同步	
用应 泰登高单	海市 授权	
单点登录配置 已		
不知道怎么配置? 词	育参考 IDaaS 配置 SAML 单点登录。	
* 阿里云主账号Uid	阿里元主聚号Ud 阿里元主聚号Ud	
• 应用账号名履性	IDaa5账户名 应用账号名篇性获取方式,采用user.username or appUser.username	\sim
阿里云RAM辅助城名	道example.onlaiyun.com 阿亚云RAM制的给名	
授权范围	手动 <mark>短权</mark> 若选择"手动起权",需要在 <mark>应用股权</mark> 中进行权限分配。	\sim

2. 输入阿里云主账号 id (账号 id 可在 阿里云控制合 首页-头像或账号中心获取)。选择应用账号名属性,用户进行单点登录时,将以该字段作为主键,对应至阿里云中的 RAM 用户,从而实现在阿里云中的登录。如果仅用于测试,建议 授权范围 选择 全员可访问,暂时跳过为 IDaaS 账号分配权限的步骤。

裁用	工単	ICP 备案	企业	支持	App	۶.,	۵	A	?	简体	0
				idaas 账号 I 主财	_***** D: 102	19	1	a	1		
				甚	本资料		实名	认证		安全谈	200
)态及最 0欠票,	新資讯。 増加域多	与业内大牛司 1委托、 回购1	取对面。 等功能	☞ 50 ④ 10 日 18	T全管控 词控制 ccessKe I荷返利	*y 管理 后台					
				草体	好设置						
目云対象	存储OSS	敏感数据保持	中功能定				退出	澄录			

3. 在 应用配置信息中,下载 IdP 元数据,保存到电脑中。此文件用于建立阿里云对 IDaaS 的信任关系。

应用配置信息

三、在阿里云中配置用户 SSO

- 1. 登录阿里云 RAM 控制台。
- 2. 在左侧导航栏中,单击 SSO管理。
- 3. 在 用户 SSO 页签 下,可查看当前 SSO 登录设置相关信息。
- 4. 点击编辑,开启 SSO 功能状态,上传步骤二中在 IDaaS 下载的 IdP 元数据,无需开启辅助域名。

×

5. 点击确定,即可完成配置。

編相 SSO 登录设置 SSO Raletts © ● 开启 ○ 关闭 元期英文地 ① LOS ① ▲昭始茲 ⑦ ○ 开启 ● 关闭

四、在阿里云中配置子用户权限(可选)

您可能拥有存量的阿里云子用户,或希望将 IDaaS 中账户同步至阿里云(详见文档:账户同步),此时请按需在左侧菜单栏的 **用户** 中为用户分配权限,以便用户拥有恰当 的权限访问阿里云的资源。如果仅为了测试单点登录能力,请忽略此步骤。

用户	1								
800	Q 输入管理名、显示名、用户 ID 起 AccessKey ID								
	用户登录名称/型示名称	備注	最后登录时间 11	创建时间 14	18/3				
	Neiro Selecter Alfred and an			2022年2月9日 00:56:45	添加到用户相 添加权限 删除				
	and Distance Income The Association			2022年1月19日 14:17:00	Sasaning Sasan Bu				
	and a second			2021年12月25日 21:04:52	and the second second				

五、尝试SSO

您已经可以开始阿里云用户 SSO。有如下两种发起模式。

1. 从 IDaaS 发起(IdP发起):使用已拥有阿里云用户 SSO 应用权限的 IDaaS 账户,登录到 IDaaS 应用门户页,点击页面上的图标,即可发起单点登录,成功登录至阿里云。

IDaaS 应用门户 _{阿里云 IDaaS}



2. 从阿里云发起(SP发起):使用匿名浏览器,打开阿里云登录页,点击下方 RAM用户登录,输入阿里云用户名并点击 下一步 按钮。

••	扫码登录	Ø) 账号密码登录
	密码登录		
	••••		
		登录	
		忘记电码 忘记登录名	5 免费注册
目它務急方式	<u>a a a a a</u>		RAM用户登录
具它登录万式	2 10 🔍 🖉 🔮		KAM用叶豆菜


3. 此时将出现提示页面,点击使用企业账号登录按钮或复制登录链接,如果您已登录 IDaaS 应用门户,则可直接登录至阿里云;否则将跳转至 IDaaS 的登录页,在 IDaaS 中完成登录后自动完成阿里云的登录。



1.7.2.2. 阿里云角色 SSO

本文为您介绍如何在 IDaaS 中配置阿里云用户单点登录。使用角色 SSO,您不必为企业或组织中的每一个成员都创建一个 RAM 子账户。

应用简介

阿里云——阿里巴巴集团旗下公司,是领先的云计算及人工智能科技公司。提供免费试用、云服务器、云数据库、云安全、云企业应用等云计算服务,以及大数据、人工智 能服务、精准定制基于场景的行业解决方案。免费备案,7x24 小时售后支持,助企业无忧上云。

操作步骤

一、创建应用

1. 登录 IDaaS管理控制台。

2. 前往 应用-添加应用-应用市场,搜索阿里云角色 SSO 应用模板。点击添加应用。

□ 阿里云角色SSO	永久免费
阿里云角色SSO应用模板,通过应用账户名方式生成阿里云; am。	云角色名
SSO	
添加应用	
3. 确认应用名称, 即可完成添加。	

添加应用 - 阿里	云角色SSO	×
• 应用名称	阿里云角色SSO	
	应用的显示名称。	
		立即添加

二、配置应用单点登录

1. 添加应用后,将自动跳转到应用单点登录配置页,您将在此处进行配置。

云身份	服务 /	应用 /	添加应用		阿里云角色SSO
\leftarrow	阿旦	シスト	角色SS	50	С

通用配置	单点登录	账户同步	
東亞法華	应用账户	授权	
单点登录配置	已启用	0	
不知道怎么配	置? 请参考 ID	aaS 配置 SAML 单点登录。	
* 阿里云主账号U	lid 同	阿里云主账号UId 里云主账号UId	
* 阿里云 身 份提住	南名称	物准备在阿里云RAM处创建的身份提供商名称 在荷里云RAM处创建的身份提供商名称	
• 应用账号名属的	ŧ ش	应用账号名 用账号名圜性获取方式,采用appUser.username	\sim
授权范围	若	手动接权 选择"手动接权",需要在 应用接权 中进行权限分配。	\sim

2. 输入阿里云主账号 id(账号 id 可在 阿里云控制台 首页 - 头像或账号中心获取)。

填写您准备在阿里云创建的身份提供商名称(只允许英文字母、数字、特殊字符--_,不能以特殊字符开头或结尾),需与步骤三中的一致。 选择应用账号名属性,用户进行单点登录时,将以该字段作为主键,对应至阿里云中的子用户,从而实现在阿里云中的登录。 如果仅用于测试,建议 **授权范围** 选择 **全员可访问**,以便跳过为 IDaaS 账号分配权限的步骤。

费用 工单	ICP 备案	企业	支持	App	D_	٥.	Ä	0	简体	0
			idaas 账号 I 主题	D: 102	10	-	6	•		
			Ш	本资料		实名	认证		安全设	iπ.
1态及最新资讯,: 10欠重,增加域名	5业内大牛匪 委托、回购4	D对面。 等功能	 ● 5 ○ 12 <l< td=""><td> 全管控 何控制 CCESSKe 荐返利 </td><td>ry 管理 后台</td><td></td><td></td><td></td><td></td><td></td></l<>	全管控 何控制 CCESSKe 荐返利	ry 管理 后台					
			至 6	好设置						
目云对象存储OSS	收感数据保护	中功能定				退出	登录			

3. 在 应用配置信息中,下载 IdP 元数据,保存到电脑中。此文件用于建立阿里云对 IDaaS 的信任关系。

应用配置信息
IdP 元数据 https://・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
4. 在 单点登录-应用账户 中, 点击 添加应用账户。
云身份服务 / 应用 / 添加应用 / 阿田云角色SSO
← 阿里云角色SSO
通用配置 单点整量 账户同步
单点量录 应用操作 授权
什么愿应用班户? 请参考应用账户。
● 您当前配置【使用 IDaaS 账户名】,如下应用账户配置均不会主效。如需变更,请前往 無 <u>希望录</u> 配置。
活血应用医产 接致产名提案 ∨ 消给入
IDaas 账户名 应用账户 添加时间

5. 选择需要使用阿里云角色 SSO 的账户,为其添加应用账户。应用账户名需要和阿里云角色名称完全一致。如果一个 IDaaS 账户对应多个阿里云角色,可以创建多个应用账户。

添加应用账户			×
按账户各搜索 > 清给入			
已透			
xiaoming	账户访问应用时所使券份。例如 admin,manager等。		
		保存 取得	ģ

- 三、在阿里云中配置角色 SSO
- 1. 登录阿里云 RAM 控制台。
- 2. 在左侧导航栏中,单击 **SSO管理**。
- 3. 在 角色 SSO 页签 下, 可查看当前 SSO 登录设置相关信息。
- 4. 点击 创建身份提供商 按钮。

应用身份服务

RAM 访问控制 / SSO 御理	
SSO 管理	
9 阿里克共務署 F3ML 218 950 (Single Sign On, 無希望與), 也除为舟谷散会建美 阿里五部設式時時 50 登里办式: 1. 處式命令50 公会可以在本部 60 中發展为工程表, 无電曲行時里式的企业 60 向的用户同步, 企业员工称使用指定的 6AM 2. 處式用户 550、企业员工在登录后, 将以 RAM 用户条合切同将里面。	/ 由色宇登洞网第五:
角色 SSO 用户 SSO	
SAML OIDC	
在企业 ldP 方配置时, 诱使用如下阿里云 SAML 账务提供商元数据 URL: https://signin.aliyun.com/saml-nole/sp-metada	ata.ml digg
6029602046	
身份提供商名称 备注	会]建 合于问
5. 填写身份提供商名称(需和步骤二中的身份提供商名称一致)	,上传步骤二中在 IDaaS 下载的 IdP 元数据,点击确定,完成身份提供商的创建。
RAM 访问控制 / SSO 管理 / SAML	
← 创建身份提供商	
* 身份提供商类型	
SAMIL 在您的承号与符合 SAML2.0 规范的身份提供有之间建立信任。	
* 身份提供肯名称 ①	
Ø1+	
mu	
 一切期間ではの 	
「山水山へへ」 (J	
T	
上传文件	
Hada: BISUA	
四、在阿里云中配置身份提供商权限	
1 在左側呈航栏中 单击 身份管理-角色	
2 占击创建备备 洗择身份提供商	
1 选择类型 2 配置角色 3 创建完成	
选择可值实体类型	
0 阿里云教号 安信云来号下的子用户可以通过扮演该RAM角色来访问您的云资源、受信云来号可以是当前云来号, 也可以是其他云来号	
〇 阿里云級务 受信云服务可以通过扮演RAM角色来访问您的云资源	
● 身份提供商 号份提供商 号份提供商助制,通过设置SSO可以实现从企业本地账号系统登录阿里云控制台,帮您解决企业的统一	
用户登录认证要求	
3. 填写角色名称(需和步骤二中的应用账户名一致),选择步骤	三中创建的身份提供商,按需填写其他配置,点击完成。
创建角色 ×	
✓ 选择类型 3 创建完成 ▲	
已洗塔可倾车体举型	
身份提供商	
* 角色名称	
允许英文字母、数字或"",字符数成小于等于 64 个	
偏注	

4. 此时也完成角色的创建。您可以为您的角色分配权限,通过该角色单点登录到阿里云的 IDaaS 账户都会拥有相同权限。

>文档版本:20220707

条件关键词 条件判定方式 值

上一步 完成 关闭

身份提供商类型
 SAML
 选择身份提供商
 请选择
 限制条件

创建角色	×
 送择类型 —— · 配置角色 — · 3 · 创建完成 · · ·	

🔗 角色创新	建成功!
为确保角色的正常使用,建	议您继续为此角色添加权限
为角色虚权	精确授权

五、尝试SSO

您已经可以开始阿里云角色 SSO。

1. 使用已拥有阿里云角色 SSO 应用权限的 IDaaS 账户,登录到 IDaaS 应用门户页,点击页面上的图标,即可发起单点登录。

iDaaS 应用门户 _{阿里云 IDaaS}	
我的应用	我的应用
我的账户	请点击下方的应用进行单点登录。若希望修改应用内容,
	捜索应用 Q
	< 阿里云角色SSO 阿里云用户SSO
	saml0011,saml001 danfer

2. 如果 IDaaS 账户拥有两个或以上的应用账户(阿里云角色),则需要选择一个应用账户进行单点登录。

应用则	长户选择
念正在尝试登录应用【阿里 置了多个应用账户。请选择	云角色SSO】, 管理员为您副 一个进行 SSO。
saml0011	\checkmark
ā	角定

3. 选择合适的应用账户并点击确定,即以角色的身份单点登录至阿里云。

1.7.2.3. 腾讯云用户 SSO

本文为您介绍如何在 IDaaS 中配置腾讯云用户单点登录。使用用户SSO,您的企业成员将以 CAM 子用户访问腾讯云。

应用简介

腾讯云为数百万的企业和开发者提供安全稳定的云计算服务,涵盖云服务器、云数据库、云存储、视频与CDN、域名注册等全方位云服务和各行业解决方案。

操作步骤

一、创建应用

1. 登录 IDaaS管理控制台。

2. 前往 应用-添加应用-应用市场,搜索到腾讯云用户 SSO 应用模板。点击添加应用。



3. 确认应用名称,即可完成添加。

添加应用 - 腾讯;	×	
* 应用名称	瞬讯云用户SSO 应用的显示名称。	
		立即等加

二、配置应用单点登录

1. 添加应用后,将自动跳转到应用单点登录配置页,您将在此处进行配置。

I. 添加应用/	百,将日 动跳转到应用甲 只 豆求配直贝,	1003
云身份服务 / 应用 / 添加	应用 / 鹏讯云用⊨SSO	
← 腾讯云用户	SSO	
通用配置 单点登	▶ 账户同步	
单点登录 应用账户	授权	
单点登录配置 已启用		
不知道怎么配置? 请参考	IDeaS 配置 SAML 单点登录。	
* 勝讯云主账号Uid	第3元云主账号Uid 第3元元士账号Uid	
• 应用账号名属性	Deas账户名	~
	应用账号名置性获取方式,采用user.username or appUser.username	
授权范围	手动授权	~

若洗経"手动授权"、需要在 ☆用授权 中进行权限分配。

2. 输入腾讯云主账号 id(账号 id 可在<mark>腾讯云控制台</mark>首页或账号中心获取)。

选择应用账号名属性,用户进行单点登录时,将以该字段作为主键,对应至腾讯云中的子用户,从而实现在腾讯云中的登录。

如果仅用于测试,建议 **授权范围** 选择 **全员可访问**,以便跳过为 IDaaS 账号分配权限的步骤。

			🕜 小程序	99+ 如如账号 -	备案			悪用 ▼	💽 👻
						账号 ID	: 10000 =)		
	ALL	的名句使用有细数	12689月,126日35			*# ک بتر چ	計信息 5认证(已本		
	第号ID 実名认证	1000000000000000000000000000000000000				按 57 应 必	金い田		
访问管理	Ŧ		新増	用户 漆加权限		口标	5		
用户数 2		用户组 1	^{角色} 12			- 安	16.5E 2管控		

3. 在 应用配置信息中,下载 IdP 元数据,保存到电脑中。此文件用于建立腾讯云对 IDaaS 的信任关系。

应用配置信息

三、在腾讯云中配置用户 SSO

1. 登录腾讯云 CAM 控制台。

- 2. 在左侧导航栏中,单击 **身份提供商-用户 SSO**。
- 3. 在用户 SSO 管理页面可查看当前用户 SSO 状态和配置信息。
- 4. 开启用户SSO, 上传步骤二中在 IDaaS 下载的 IdP 元数据, 点击保存, 即可完成配置。

SSO 登录设置				
用户 SSO ①				
SSOIDLX ·	O SAML OIDC			
SAML服务提供商元数据 URL	https://cloud.tencent.com	/saml/SpMetada	ata xml?tenantiD:	90 M
身份提供南元款据文档	metadataDocument.xml	重新上传		
	保存 取消			

四、在腾讯云中配置子用户权限

您可能拥有存量的腾讯云子用户,或希望将 IDaaS 中账户同步至腾讯云(详见文档:账户同步),此时请按需在用户列表 中为子用户分配权限,以便子用户拥有恰当的权限访问腾讯云的资源。如果仅为了测试单点登录能力,请忽略此步骤。

用户	列	ŧ					CAMPER	·(E43364) (2
G		如何有有效多位的? 20月前日2月20日初期4日息	进行安全升限保护,忽可以收出列的	NP左肩下拉拐钮 (►) 查看用户的界份安全状态	. Emternations	您也可以收出用户就进入用户的	658+±±048.	
t	ani	ESR/F +				探求用户名/D/Sec	add/于机/邮稿/编注(多关键闭空相隔开	Q. ¢
		Rras	用作类型	服号印	0323344	关联结查	设作	
	,		主教品	100000		G. 15	拉权 更多操作 ▼	
	,	atachong	子用户	1000 🔐 🛯 👘	an 11 an 11	D.	如何 王乐说作 *	
	,	xiaoming	子用≏	1000	PERCENT		授权 更多操作 ▼	

五、尝试SSO

您已经可以开始腾讯云用户 SSO。有如下两种发起模式。

1. 从 IDaaS 发起(IdP发起):使用已拥有腾讯云用户 SSO 应用权限的 IDaaS 账户,登录到 IDaaS 应用门户页,点击页面上的图标,即可发起单点登录,成功登录至腾讯 云。

IDaaS 应用门户 阿重云 IDaaS	
我的应用	我的应用
我的账户	请示由下方的应用进行曲点破录。若希望惨改应用内容,请联系管理员。

2. 从腾讯云发起(SP发起):使用匿名浏览器,打开腾讯云登录页,点击下方 子用户,直接点击用户 SSO 登录 按钮,此时如果您已登录 IDaaS 应用门户,则可直接登录至腾讯云;否则将跳转至 IDaaS 的登录页,在 IDaaS 中完成登录后自动完成腾讯云的登录。



1.7.2.4. 腾讯云角色 SSO

本文为您介绍如何在 IDaaS 中配置腾讯云角色单点登录。使用角色 SSO,您不必为企业或组织中的每一个成员都创建一个 CAM 子用户。

应用简介

腾讯云为数百万的企业和开发者提供安全稳定的云计算服务,涵盖云服务器、云数据库、云存储、视频与CDN、域名注册等全方位云服务和各行业解决方案。

操作步骤

- 一、创建应用
- 1. 登录 IDaaS管理控制台。
- 2. 前往 应用-添加应用-应用市场,搜索到腾讯云角色 SSO 应用模板。点击添加应用。

🔗 腾讯云角	色SSO	限时免费 ③
腾讯云角色SSOE am。	2用模板,通过应用账户名方式	生成腾讯云角色名
SSO		
添加应用		
3. 确认应)	用名称,即可完成	添加。
添加应用 - 腾讯;	云角色SSO	
添加应用 - 腾讯; • 应用名称	云角色SSO 時雨云角色SSO	
添加应用 - 腾讯; • 应用名称	云角色SSO 随讯云角色SSO 应用的显示名称。	

二、配置应用单点登录

1. 添加应用后,将自动跳转到应用单点登录配置页,您将在此处进行配置。

应用身份服务

大学の後端 (20月 / 2010年) 第日に近後2500
 「第日にご 単の設計 第日に近後2500
 「第日にご 単の設計 知り何歩

 のの設計 単の数計 取り何歩

 のの設計 配用にデー 使の

 「第日にご 単のいる 記言 SAAL 総合登录。

 「第日に立た後年いは

 第日にご 単のいる 記言 SAAL 総合登录。

 「第日に立た後年いは

 「第日に立た後年いは

 「第日に立た後年のには

 「第日に立た後年のには

 「第日に立た後年のには

 「第日に立た後年のには

 「第日に立た後年ののその

 「第日についますの方方、第月時の以りによりの時のに

 「第日についますの方方、第月時の以りによりの時のに

 「第日についますの方方、第月時の以りによりの時のに

 「第日についますの方方、第月時の以りによりの時のに

 「第日についますの方方、第月時の以りによりの時ののに

 「第日についますの方方、第月時の以りによりの時ののに

 」

 「第日についますの方方、第月時の以りによりの時ののに

 「第日についますの方方、第月時の以上のにの時間に

 「第一についますの方方、第月時の以上のにの時間に

 「第一についますの方方、第月時の別によりの時ののに

 「第一についますの方方、第月時の別によりの時ののに

 「第一についますの」

 「第二についますの」

 「第二についますの」

 「第二についますの」

 「「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

 「」

2. 输入腾讯云主账号 id (账号 id 可在<mark>腾讯云控制台</mark>首页或账号中心获取)。

填写您准备再腾讯云创建的身份提供商名称(腾讯云中支持3-128个数字、大小写字母、和+=,.@_-),需与步骤三中的一致。 选择应用账号名属性,用户进行单点登录时,将以该字段作为主键,对应至阿里云中的子用户,从而实现在阿里云中的登录。 如果仅用于测试,建议 授权范围 选择 全员可访问,以便跳过为 IDaaS 账号分配权限的步骤。

					⊠ ²²	集团账号	- 留案			费用 ▼	0	
								<mark>。</mark> 账号ID:	10000 =			
	HARRIEK.	NMBUCH+	18000000	9, 10092				2 #*	始息 31年(已2			
	「 乐号ID	100000						··· · · · · · · · · · · · · · · · · ·				
访问管	· 买名(). 里	业 已实名	立的影響	新畑	用户 漆	的复数		分佈	1世理 E			
用户数 2	_	用户组 1		^{角色} 12				\$† 项目 □ 安全	1管理 1管控			

3. 在 应用配置信息中,下载 IdP 元数据,保存到电脑中。此文件用于建立腾讯云对 IDaaS 的信任关系。

et marine /drate				
	6373	HE 2	慶/合	44
	125.1	サロル		~ <u>~</u> ^

4. 在 单点登录-应用账户 中, 点击 添加应用账户。

云身份很多 / 应用 / 源加应用 / 网讯云角色SSO			1
← 腾讯云角色SSO			
通用配置 单点量录 账户同步			
单示登录 应用账户 授权			
什么是应用账户? 请参考 应用账户。			
◎ 您当前配置【使用 IDeaS 账户名】,如下应用账户配置均不	5会生效。如雾安更,请前往 单点登录 配置。		
※加加田市户 按照户名提示 ∨ 清单入			
DaaS 账户编	应用账户	(#t6181#)	
xiaoming	123	2022-02-11 15:7:36	
xiaoming	abc001	2022-02-11 15:7:36	
ILEBRIT			●页显示 20 ∨ 共2条数据

5. 选择需要使用腾讯云角色 SSO 的账户,为其添加应用账户。应用账户名需要和腾讯云角色名称完全一致。如果一个 IDaaS 账户对应多个腾讯云角色,可以创建多个 应用账户。

添加应用账户			×
按账户名搜索 > 丙油入			
已進			
xiaoming	账户访问放用时所使身份。例如 admin,manager等。		
		保存	取消

三、在腾讯云中配置角色 SSO

- 1. 登录腾讯云 CAM 控制台。
- 2. 在左侧导航栏中,单击 **身份提供商-角色 SSO**。
- 3. 在角色 SSO 管理页面中 新建身份提供商。

角	色SSO							
	○ 身色世界的(必) 時期現象 報告正式時期子 MAL2 85 00 Grope sept On: 券 有量量),通过 IP 务与敏速的外期回 ² 可置数均分的空機用正規則,換正日和定时所用 550 量差方式・ 1 音楽 550、地域になる年以 PP 電影和工程機能、表面正確和形式形成金 54 PP 時時間可考,企业加工事業工程能的 CAN 最高量型規模正式: 2 用P 550、換形正規工 IP 電影的 SAAN 整定性 ODC 全球商金会运用PP 時期完 CAN 用PODIE文系。会运用P量品任、使用家 CAN 用PP 的间期表示。							
	aner the							
	提供商名称	提供商类型	PRESID	最后更新时间	操作			
	aboldP	SAML	2022-02-21 21:54:59	2022-02-21 21:54:59	89			

4. 填写身份供应商名称(需和步骤二中的身份提供商名称一致),上传步骤二中在 IDaaS 下载的 IdP 元数据,点击下一步,完成身份提供商的创建。

1 配置提供	商信息	> 21	审阅并完成		
(供賣問題)・	O SAML				
1份提供商名称•					
注					
)附属文档 •			10	建文件	

四、在腾讯云中配置身份提供商权限

1. 在左侧导航栏中,单击 **角色**。

选择角色	载体	×
	腾讯云产品服务 接权云服传通过角色使用物的云流源	>
8	時代云集中 授权主张号或者其他主张号通过角色使用您的云资源	>
Ēð	身份提供商 接段腾讯云外部用户身份(如企业用户目录)使用物的云波源	>

3. 选择步骤三中创建的身份提供商,按需填写其他配置,点击下一步。

← 新建自定义角色

1 输入的	自色载体值息 > ② 配置角色策略	> ③ 审阅	
身份提供商	请选择身份提供商 👻		
控制台访问	允许当前角色访问控制台		
使用条件	52	茶件	
			暫无政損
	共口顶		
	初婚使用条件		
ᡯ᠆᠊ᢔ			

4. 选择您希望该角色拥有的权限。通过该角色单点登录到腾讯云的 IDaaS 账户都会拥有该权限。完全选择后点击下一步。

← 新建自定义角色

第월 (共 685 奈)			已總罪0束	
2家芽語名称/語法/描述		Q	2018/0	加速失望
1888	保路关型 T			
AdministratorAccess 這種種九件位量運動产丸后有用作及其67月,就身相关的信息,云服务资。	教記問題	^		
ReadOnhAccess 读用能力许可用使力问称内方所有支持使口袋量的或使得很量的的支援表。	FT-12.9480			
OCIoudResourceFullAccess 这项能力计设管理和户与所有正面表现户。(他了CAM包括高公所有50限。	预采用器			
OCloudFinanceFulAccess 家族医力学の質問がつれ始め相当的内容。例如: の形、开展。	技巧推断			
OcloudAAFullAccess	IS O MIN			

5. 填写角色的名称等基本信息(名称需和步骤二中的应用账户名一致),并进行审阅,完成创建角色。

五、尝试SSO

您已经可以开始腾讯云角色 SSO。

1. 使用已拥有腾讯云角色 SSO 应用权限的 IDaaS 账户,登录到 IDaaS 应用门户页,点击页面上的图标,即可发起单点登录。

IDaaS 应用门户 ^{同里云 IDaas}

我的应用	我的应用
我的账户	调点由下方的应用进行单点登录。若希望修改应用内容,调联系管理员。
	\bigotimes
	< 開讯云角色SSO
	abc001,123

2. 如果 IDaaS 账户拥有两个或以上的应用账户(腾讯云角色),则需要选择一个应用账户进行单点登录。

近任至刘蓉将成出【解加公用6220】, 复加	里贝为您配
了多个应用账户。请选择一个进行 SSO。	
abc001	~

3. 选择合适的应用账户并点击确定,即以角色的身份单点登录至腾讯云。

1.7.2.5. 华为云 SSO

本文为您介绍如何在 IDaaS 中配置华为云用户单点登录。使用 SSO,您的企业成员可以使用企业账号单点登录华为云,这一过程在华为云中称为联邦身份认证。 操作步骤

- 一、创建应用
- 1. 登录IDaaS管理控制台
- 2. 前往 应用-添加应用-应用市场,搜索到华为云用户 SSO 应用模板。点击添加应用。

 ・ 単为云用户SSO 半为云IAM用户SSO 	限时免费 ⑦
550	
^{≫加∞用} 1.确认应用名称,即可完成添加。	

添加应用 - 华为:	云用户SSO	×
* 应用名称	华为云用户SSO 应用的显示名称。	
		立即添加

二、配置应用单点登录

1. 添加应用后,将自动跳转到应用单点登录配置页,您将在此处进行配置。

云身份服务 / 应用	/ 潘加迪用 / 华为云用户SSO
← 华为云	和户SSO
诵用配置	单点答录 账户同步
单点登录 应	
单点登录配置	
不知道怎么配置?	· 诱参考 IDeaS 配置 SAML 单点登录。
* 应用账户名	IDaa5既户名
* 37064/2783=88885	
UND PLAN ACT	初始代登录地址,华为云仪支持SP发起登录的应用SSO,需要填写此地址才可登录
授权范围	手动授权 🗸
	若选择"手动授权",需要在 <u>加用授权</u> 中进行权限分配。
2. 输入初始	3化登录地址(该地址在下文第三步中获取)。
选择应用账号	}名属性,用户进行单点登录时,将以该字段作为主键,对应至华为云中的 IAM 用户,从而实现在华为云中的登录。
如果仅用于测	JI江,建议 投 仪 氾 固 选择 全 页 リ 访 问 , 以 便 跳 过 为 IDaaS 账 号 分 配 权限 的 步骤。
3. 仕 22 用 8	近直信息 甲,下载 IQP 元数据,保存到电脑甲。此义件用于建立华内云对 IDaas 的信任关系。
应用配置信	急
IdP 元数排	
IdP Meta	Cata 石业用文存 metacata 配置信息工作/拉联,可以节有大重配置步骤。 消任业用 SSU 配置平寻找定合有 metacata 工作服力。
三、在华	为云中配置用户 SSO
1. 登录 <mark>华为</mark>	J국 IAM 控制台。
2. 在左侧导	身航栏中,单击 身份提供商 。
3. 点击 创致	皇身份提供商。
身份提供商 ⑦ ▲ ₩#191025022975	+ and so show
您还可以很建2个身份提供商。	WWA-Antomina carines Q
新御 正 aniariSAML	Mill (2) INN Mill (2) Mill - SAMA Q ADI Ref (42) (80)
4. 填写名称	R,并点击确定。
身份提供商 / 创建	2 身份提供商
* 名称	
* this	SaMi
*状态(
描述	济输入身份提供向信息。
	NEX
5. 点击修3	次身份提供商 ,或在 身份提供商列表 页面中点击 修改。
/ 12 1	
创建鸟	9份提供商业功。请咐往州改会份提供商页面完美容的身份提供商信息。
CONTRA	
	5岁后口动天时底闪起。

6. 在 元数据配置 点击添加文件,选择在步骤二中在 IDaaS 下载的 IdP 元数据,并点击上传文件,确认元数据配置(一般无需修改)。复制 登录链接,回填到上文第二步中 IDaaS 应用详情中的 初始化登录地址。完成后,点击确定按钮,完成身份提供商的创建。

基本信息	
名称	idaassaml
协议	SAML
状态	 ● 商用 ○ #用
描述	1998.A.34918300928.
	0255
登录链接	https://auth.huaweicloud.com/authui/federation/websso et anning of a flage index of a flage
登录链接	https://with huaveicloud.com/authul/edention/websu
型录链接 元数据配 】 系统将从(https://aux/huseeicloud.com/aufu/infederation/websoury on an and an an and an and an and an and an and an and a
登录链接 元数据配 系统统从(idp-app	Ntps://aux/huseeicoud.com/aufu/infederation/vectory.com/aux/huseeicoud.com/aux/huseeicou
 登录链接 元数据高器 系统端从(idp-app ○ 上传班 	https://aux/huseecioud.com/aufu/infederation/websions on a man and a man an a man and a man and a man and a man an
登录链接 元数据配理 素級能从(idp-app ● 上传訳 ✓ 已	https://aux/huseeicoud.com/aufu/federator/websourgenting.interformeranting.interform
☆求研接 二数据配	http://www.htusencloud.com/wwfederator/wdefarco/wdefar ####################################
並示碼接 元数据配引 系统共从1 (idp-app ② 上供 ② 上供 ② 上供 ③ 身份转換 認述可以的	https://aux/htusencicoud.com/aufu/federator/wieder Referenceanterator/wiedera
 ・	https://aux/huseencloud.com/au/fu/federation/websus_series_ass Sector_sector_asseries_asseries_asseries_asseries_asseries_asseries_asseries_asseries_asseries_asseries_asseries Sector_asseries_asseries_asseries_asseries_asseries_asseries_asseries_asseries_asseries_asseries_asseries_asse
空泉磁接 示数据配計 ぶらまい (idp-app ② 上作 ③ 上作 ③ 一 ③ 一 ③ 上 ③ 一 ③ 上 ③ 上 ③ 上 ③ 上 ③ 上 ③ 上 ③ 二 ③ 二 ③ 二 ③ 二 ③ 二 ③ 二 ③ 二 ③ 二 ③ 二 ③ 二 ④ 二 ⑤ 二 ⑥ 二 ⑤ 二 ⑥ 二 ⑤ 二 ⑤ 二 ⑤ 二 ⑥ 二 ⑥ 二 ⑤ 二 ⑤ 二 ⑤ 二 ⑤ 二 ⑤ 二 ⑤ 二 ⑤ 二 ⑤ 二 ⑥ 二 ⑤ 二 ⑤ 二 ⑥ □ □ ⑥ 二 ⑥ 二 ⑥ 二 ⑥ □ □ ⑥ 二 ⑥ 二 ⑤ 二 ⑤ 二 ⑤ 二 ⑤ 二 ⑤ 二 ⑥ 二 ⑥ 二 ⑥ 二 ⑦ 二 ⑥ 二 ⑥ 二 ⑦ □ □ ⑦ 二 ⑦ □ □ ⑦ □ □ □ □ □ □ □ □ □	Mites Jaux husencicus consultative deeration vieces or an

四、尝试SSO

您已经可以开始华为云用户 SSO。有如下两种发起模式。

1. 使用已拥有华为云用户 SSO 应用权限的 IDaaS 账户,登录到 IDaaS 应用门户页,点击页面上的图标,即可发起单点登录,以联邦用户的身份登录至华为云。

IDaaS 应用门户 _{阿里云 IDaaS}	
我的应用	我的应用
我的账户	请点击下方的应用进行单点登录。若希望修改应用内容,
	援索应用 Q
	иудля-550 Падафиясан-550
	未配置应用账户 saml0011,saml001

2. 使用匿名浏览器,打开华为云登录页,点击下方 企业联邦用户。

扫码登录		密码登录
华	《为帐号登	录
13 19		
		Ì
	登录	
	注册 忘记密	码
	使用其他帐号登	录
AM用户 企业联邦用 华为云帐号	沪华为官网帐	号 华为企业合作伙伴
初门为您提供华为帐号服 1提升登录体验, 了解更	务,在登录过程中! 多	会使用到您的帐号和网络信

输入 原华为云账号名/租户名,选择身份提供商,并点击前往登录按钮。

扫码登录		密码登录
企	业联邦身	份登录
yan 🔳 🚥		
idaassaml		~
		记住登录信息
	前往登录	ŧ

4. 点击后,如果您已登录 IDaaS 应用门户,则可以联邦用户的身份直接登录至华为云;否则将跳转至 IDaaS 的登录页,在 IDaaS 中完成登录后自动完成华为云的登录。

五、配置身份转换规则

在以联邦用户的身份单点登录到华为云后,用户在华为云中的用户名默认为"FederationUser",且**联邦用户仅能访问华为云,没有任何权限**。您可以在华为云 IAM 控制 台配置身份转换规则,实现:

• 企业管理系统用户在华为云中显示不同的用户名。

赋予企业管理系统用户使用华为云资源的权限。

详情请查看华为云官方文档:《步骤2:配置身份转换规则》

1.7.2.6. 百度智能云用户 SSO

本文为您介绍如何在 IDaaS 中配置百度智能云用户 SSO(对应百度智能云中的IAM用户联合)。使用用户SSO,您的企业成员将以子用户访问百度智能云。

应用简介

百度智能云致力于为企业和开发者提供全球领先的人工智能、大数据和云计算服务,加速产业智能化转型升级。

操作步骤

- 一、创建应用
- 1. 登录 IDaaS管理控制台。
- 2. 前往 应用-添加应用-应用市场,搜索到 百度智能云用户 SSO 应用模板。点击 添加应用。



3. 确认应用名称,即可完成添加。

二、在 IDaaS 中配置 SSO

1. 在单点登录配置页中, 您需要录入百度智能云的主账号 ID

单点登录配置 已启用		
不知道怎么配置? 请参考	对接文档。	
・百度智能云 主账号 ID	希望实现 SSO 的目标百度胃能云主账户 ID。	
百度智能云 辅助域名	example.login.bce.baidu.com 如果您在百度智能云IAM用户联合企义了辅助城名,则需要在此进行填写,并保持一致。	
* 应用账户	Daas 解户名 单点型录时,将选中项作为影户研订,传递给百度鲜能云。	
授权范围	全最可访问	

您可以使主账号登录百度智能云, 在"用户中心"查看您的主账号 ID

	〇百	度智能元 控制台总》	名 全局 >			Q	88	 *	Ä	备案	工単	文档	企业	支持	财务	生态	H ^
Ŧ	体信息 h	19957 Homan Garcil	账户ID: 联系人:	Toasii Inden (N. 1.4) - 2 - 4-30 af7] Trigi	一模行业分类: 二级行业分类:			移动应用 系统	Ħ		主营业务 网站地址			 日 74 2 用户 3 安全 3 安全 3 多用F 	ゆりばは 中心 人证 9访问控制	E	覆 个人认证
														切换身	169		山 退出

2. 其他选项保持默认,点击保存即可完成 IDaaS 侧的全部 SSO 配置。

🤊 说明

提示 应用账户:默认使用 IDaaS 账户名作为应用登录标识。应用中用户名必须要和 IDaaS 账户名保持一致,才能完成 SSO。若希望灵活配置,请参考 单点配置通用说 明 - 应用账户 进行配置。 授权范围:若希望指定可访问应用的 IDaaS 账户,请参考 单点配置通用说明 - 应用账户 进行配置。

3. 在页面下方的【应用配置信息】中,即包含了百度智能云完成 SSO 配置所需要的参数,下载 ldP 元数据,保存至本地,在后续流程中将会使用。

应用配置信息	
IdP 元数据	https://aliyunidaas.com/api/v2/app_mividtiffw64hiqw4wop7bhg34/sami2/meta の
IdP Metadata	室田支持 metadata 配置信息上传/拉眼,可以节質大量配置步骤。请在应用 SSO 配置中寻线是否有 metadata 上传能力。
IdP 唯一标识	https://saliyunidaas.com/api/v2/app_mividtiffwb4hiqw4wop7bhg34/sami2/meta 资
IdP Entity ID	IDaaS 在应用中的标识。需要将值填写在应用单点登录配置中。
IdP SSO 地址	https://ici-acallyunidaas.com/login/app/app_mivldtiffwbdhiqwdwop7bhg34/saml2/sso ♂
IdP Sign-in URL	SAML协议支持 SP 我起串点登录,可能需要填写此地址在应用配置中。由 IDaas 提供。可以直接访问该地址,进行应用登录。
单点退出地址	智不支持
SLO URL	SAML协议支持单点退出,可能需要填写此地址在应用配置中。由 IDaaS 提供。
公钥证书 Certificate	BEGIN CERTIFICATE MIIETICCA/2qAwlBAgISHTWxz2KCeECsDy8Ji+vo92z9MA0GCSqGSlb3DQEBCwUA MIGSMScwJQYDVQQDD85hcH8fbWI2bGR0aWZmd2l0aGkxdzR3b3A3YmhnMzQxKTAn
三、配置百	度智能云

1. 使用主账号,登录百度智能云,点击右上角的头像,在弹出的菜单中,点击"多用户访问控制",如下图所示:

=	🗘 百度智能云	控制台总览	全局 🗸				Q	33 C;	ч ,	备案	Τ#	文档	企业	支持	财务	生态	Н ^
đ	林信息 h ^{您好} h boxers		账户ID: 联系人:	75862 168 ± 38 1.5 ± 8 ± 408017. ⊋*3		一级行业分类: 二级行业分类:		移	力应用 充		主营业务: 网站地址:			 用户中/ 一用户中/ 一 安全认う (多用户) 切换身(■ ■■ ひ 証 訪问控制 分	6	个人认证
2	在左侧导航椅	兰栏中,选	₅择【外部账号	号接入】【IAM用户联合】,	打开如下图所示界面												

多用户访问控制			IAM用户联合	
概览			基于SAML 2.0协议	义用户联合设置
用户管理	~			_
组管理			功能状态:	
策略管理			ldP元数据:	上传
角色管理			SP元数据:	https://console.bce.baidu.com/api/iam/account/saml/spmeta/7 💷 🛛 💷 🖄 💷 🖄 💷 💷 💷 📼
外部帐号接入	^			
• IAM角色联合			辅助域名:	编辑
• IAM用户联合				
操作记录(公测中)				
3. 将"功能状态"	,修	改为周	3月,同时上传之前下载的)IdP 元数据,如下图所示:
IAM用户联合				

基于SAML 2.0协议用户联合设置 ① 开启IAM用户联合后,所有子用户将使用企业账号联合登录的方式登录控制台,子用户管理中的控制台登录设置将不再生效

功能状态:	
ldP元数据:	idp-app_mizo77gk7hag6vtph35v6t7vpe-meta.xml ×
SP元数据:	https://console.bce.baidu.com/api/iam/account/sami/spmeta/7t 🔐 " 🗰 🐭 🖿 🖬 🐨 🖬 🖉 "
辅助域名:	编辑
â	

? 说明

注意:如果您在"百度智能云-IAM用户身份联合"中,开启了辅助域名,您需要将辅助域名,填写到阿里云IDaaS中。

四、在百度智能云中创建子用户

创建百度智能云子用户(如果您有存量的百度智能云子用户,可以跳过此步骤),如下图所示:录入子用户的用户名(账号名建议与IDaaS中的账号名一致,如果不一致, 您还需要在IDaaS中,通过"应用账号"来建立映射关系),开启控制台密码访问,并按照要求设置子用户的密码

多用户访问控制	用户中心 / 子用户						
概览	子用户管理 ?						①帮助文档
用户管理 ^	子用户登录链接: http://	danfer2song.login.bce					
• 子用户	+ 创建子用户		创建于用户			× .	请输入用户名或AccessKey进行搜索 Q
* 消息接收人	用户名	密码	* 用户名			时间	操作
组管理	danfer	20 1	备注			2-03-16 20:11:25	编辑权限 禁用 删除 管理
策略管理			访问方式	☐ 编程访问 自动生成AccessKey, 子用户通过API或SDK工具访问			_
角色管理				✓ 控制台密码访问 子用户使用账号密码登录云控制台			< 1 >
外部帐号接入 ~		_		手动输入 自动生成 绑定内网账号			
操作记录(公测中)			* 新密码				
密钥报告			*确认密码				
设置				■要求用户下次登录时必须重置密码			
			快速授权	(其他权限可创建后添加)			
					教会 取当		
					THE PARTY		

五、尝试SSO

您已经可以尝试百度智能云用户 SSO。

IDP 发起

请用已授权使用 "百度智能云用户 SSO"的 IDaa5 账户, 登录到 IDaa5 门户页, 点击页面上 "百度智能云用户 SSO"图标, 发起 SSO。

IDaaS 应用门户 阿里云 IDaaS	
我的应用	我的应用
我的账户	構造市下方的应用进行单点登录。若希望修改应用内容,请联系管理员。 「 「 「 「 「 定 「 客 」 こ こ 名 二 二 二 二 二 二 二 二 二 二 二 二 二

SP 发起

请在匿名浏览器中,打开"百度智能云子账号"登录页,登录页的URL,可以在【多用户访问控制】【子用户】【子用户管理】页面中查看,如下图所示:

多用户访问控制	用户中心 / 子用户								
概范	子用户管理 ?	了用户管理 ?							
用户管理 ^	子用户登录链接: http://#uf(算篇v)	a.login.boe.baidu.com 自定义							
• 子用户	+ 创建子用户						请输入用户名或AccessKey进行搜索	Q	
* 消息接收人	用户名	密码	说明	状态 🖌	所在组	创建时间	操作		
组管理	danfer	已设置 修改		● 活跃		2022-03-16 20:11:25	编辑权限 禁用 删除 管理		
策略管理									
角色管理							<	•	
外部帐号接入 🗸 🗸									

点击"使用企业账号登录,"则会跳转到 IDaaS 进行登录。如果用户尚未登录 IDaaS ,则 IDaaS 会引导用户进行登录 。

()百度智能云 子用户登录	< 返回百度智能云首页
	English
	<u>ま账号</u> ・ ・ は、 : ・ : - : : : 使用 <u>企业账号登录</u> 使用其他子用户登录 使用主账户登录

IDaaS 认证用户通过后,将直接登录到 百度智能云 中。

1.7.2.7. 百度智能云角色 SSO

本文为您介绍如何在 IDaa5 中配置百度智能云角色 SSO(对应百度智能云中的IAM角色联合)。使用角色 SSO,您不必为企业或组织中的每一个成员都创建一个百度智能云 子用户。

应用简介

百度智能云致力于为企业和开发者提供全球领先的人工智能、大数据和云计算服务,加速产业智能化转型升级。

```
一、创建应用
```

- 1. 登录 IDaaS管理控制台。
- 2. 前往 应用-添加应用-应用市场,搜索到百度智能云角色 SSO 应用模板。点击添加应用。

```
    ● 百度智能云角色 SSO 限时免费 ②
    ■ 百度智能云教力于为企业和开发者提供全球领先的人工智能、大教编和云计算影务,加迪产业智能化转型升处,本模板用于 IDaaS 登录到百度智能云,并作为百度智能云的角色进行访问。
    ● SSO
    ● SMD应用
```

3. 确认应用名称,即可完成添加。

二、在 IDaaS 中配置 SSO

1. 在单点登录配置页中,您需要录入百度智能云的主账号 ID

单点登录配置 日											
不知道怎么配置? 请参考 对接文档。											
• 百度智能云 主账号 [[0										
	希望实现 SSO 的目标百度销能云主账户 ID。										
* 身份提供商名称	AliyunIDaaSRole										
	在百度智能云 IAM 角色聚合中创建的身份提供商名称。										
* 应用账户	应用账户										
	单点登录时,将选中项作为角色标识,传递给百度哲能云。										
授权范围	全员可访问										
	一 若选择"手动授权",需要在 <mark>应用授权</mark> 中进行权限分配。										

您可以使主账号登录百度智能云, 在"用户中心"查看您的主账号 ID

I 🗘	百度智能云 控制台总览	全局 ~			Q	82	₽,	¥ 8	案 工	1 文档	企业	支持	财务	生态	H ^
基本信息	1897 Hommanaett	账户ID: 联系人:	Teatrine – Altri z venet7 T ¹ €	一级行业分类: 二级行业分类:			移动应F 系统	3	主営业	务: 趾:		 日 日	リテレン い し い い の 行 知 知 の に の に の の の の の の の の の の の の の の	8	8 个人认证
												切换身	HB		り退出

2. 身份提供商名称,需要与百度智能云【IAM角色联合】中的身份提供商名称保持一致,例如: AliyunIDaaSRole

3. 其他选项保持默认,点击保存即可完成 IDaaS 侧 全部 SSO 配置。

? 说明

提示 应用账户:默认使用 IDaaS 账户名作为应用登录标识。应用中用户名必须要和 IDaaS 账户名保持一致,才能完成 SSO。若希望灵活配置,请参考 单点配置通用说 明 - 应用账户 进行配置。 授权范围:若希望指定可访问应用的 IDaaS 账户,请参考 单点配置通用说明 - 应用账户 进行配置。

4. 在页面下方的【应用配置信息】中,即包含了百度智能云完成 SSO 配置所需要的参数,下载 ldP 元数据,保存至本地,在后续流程中将会使用。

立用配置信息							
IdP 元数据	https://valereen.aliyunidaas.com/api/v2/app_mivldtiffwb4hiqw4wop7bhg34/saml2/meta ロ 」で載						
IdP Metadata	若应用支持 metadata 配置信息上传/拉取,可以节省大量配置步骤。请在应用 SSO 配置中寻找是否有 metadata 上传能力。						
IdP 唯一标识	tps:// 🚛 🚛 aliyunidaas.com/api/v2/app_mivldtiffwb4hiqw4wop7bhg34/saml2/meta 司						
IdP Entity ID	laaS 在应用中的标识。需要将值填写在应用单点登录配置中。						
IdP SSO 地址	https://读读读读aliyunidaas.com/login/app/app_mivldtiffwb4hiqw4wop7bhg34/saml2/sso 问						
IdP Sign-in URL	SAML 协议支持 SP 发起单点登录,可能需要填写此地址在应用配置中。由 IDaaS 提供。可以直接访问该地址,进行应用登录。						
单点退出地址	暂不支持						
SLO URL	SAML 协议支持单点退出,可能需要填写此地址在应用配置中。由 IDaaS 提供。						
公钥证书 Certificate	BEGIN CERTIFICATE MIIEFTCCAv2gAwlBAgISHTwxr2KCeECsDy8JI+vo92z9MA0GCSqGSIb3DQEBCwUA MIGSMScwJQYDVQQDDB5hcHBfbWl2bGR0aWZmd2l0aGlxdzR3b3A3YmhnMzQxKTAn						

三、配置百度智能云

1. 使用主账号,登录百度智能云,点击右上角的头像,在弹出的菜单中,点击"多用户访问控制",如下图所示:

🗧 🗘 百度智能云	控制台总览 全局 >	Q III 😅 🛱	7 备案 工单 文档	企业 支持 财务 生态 Η ^
基本信息 加 bms.set	戦户D: [75a62: 15.45 m. 25. 15.15 m. 25. 45.45 m. 27] 取扱人: ついの (15.15 m. 25.15 m. 25.45 m. 25.25 m. 2	移动应用系统	主营业务: 网站地址:	・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
2. 在左侧导航	栏栏中,选择【外部账号接入】【IAM角色联合】,打开如下图所示界面			
多用户访问控制	用户中心 / 外診厥号接入			
概范	外部账号接入			
用户管理 ~				
组管理 策略管理	百度智能云基于SAML2.0协议,支持用户使用企业已有身份顶(UP)联合认证,并通过控制台或层端指动问云资源,以实现单点显录。 百度智能云当约支持4秒将式的联合认证:			收起说明

角色管理	 IAM角色联告:企业员工(客户)/ IAM用户联合:企业员工(客户)/ 	A外部身份源认证通过后,以IAM角色身份访问云资源; A外部身份源认证通过后,以IAM子用户身份访问云资源。更多详情请	参考: 外部账号接入		
外部帐号接入 个					
• IAM角色联合	+ 身份提供者				Q
• IAM用户联合	身份提供商名称	身份提供商描述	创建时间	操作	
操作记录(公测中)			and the second sec		

3. 添加"身份提供者",打开如下界面,名称填写"AliyunIDaaSRole",务必与IDaaS中配置的名称保持一致;选择步骤二中下载的 ldP 元数据,进行上传。

添加身份提供者				×
类型:	SAML			
名称:				
描述:				
元数据文件:			选择文件	
	74	actor	町当	

4. 点击"确定",你可以在列表中,查看到您添加的"身份服务提供者"。

多用户访问控制	用户中	(产中心 / 务部期号接入										
概览	外	部账号接入										
用户管理 ~												
组管理		百度智能云基于SAML 2.0协议。支持用户使用企业已有身份	能能云基于SAML 2.0协议,支持用户使用企业已有身份调(MP)联合认证,并通过控制台或是编程均问云资源,以实现单点管录。									
策略管理		目成指输云当你支持这种形式创建合认证: 1. JAM的面包各个。今月有一家合叫人被骂各次到了证循计师。以JAA的面包条价治问示需要:										
角色管理		2. IAM用户联合:企业员工(客户)从外部身份源认证通过后,	以IAM子用户身份访问云资源,更多详情请参考:外部账号接入									
外部帐号接入 ^												
• IAM角色联合		+ 身份提供者					Q					
• IAM用户联合	射	分提供商名称	身份提供商描述	创建时间	操作							
操作记录(公测中)	Aliy	JuniDaaSRole		2022-03-17 17:23:59	删除							

四、在百度智能云中创建角色

1. 创建百度智能云角色(如果您有存量的百度智能云子用户,可以跳过此步骤),选择【多用户访问控制】【角色管理】【增加角色】,打开如下界面

多用户访问控制	用户中心 / 角色管理	/ 新建角色							
概览 用户管理 ~	基本信息								
组管理	*角色名称:	DemoSSORole							
策略管理	备注:	测试单点登录							
角色管理									
外部帐号接入 ~									
操作记录(公测中)									
密钥报告	角色载体								
设置									
	* 载体类型:	 中建智能无限号 使用智能五主子用户代入到AM角色访问其他宽广云资源,角色载体可以是当你云散号,也可以是其他云散号 							
	* 载体实体:	AliyuniDaaSRole 🗸 如还没有身份供应着,应该这里去倒建							
	限制条件:	+ jānāsēt							

2. 输入角色名称,例如: DemoSSORole,角色载体-载体类型,选择外部账号,载体主体选择之前创建的身份服务提供者: AliyuniDaaSRole。您可以为该角色赋予一些权限

五、在 IDaaS 中为用户关联角色

返回 IDaaS 管理控制台

 选择【应用】菜单,在应用列表中,找到步骤一中创建的应用"百度智能云角色 SSO",点击【管理】按钮,接着选择【单点登录】【应用账户】页签,点击"添加应 用账户"按钮,弹出如下对话框:

云身份服务	云身份服务 / 应用 / 添加应用 / 百度智能云角色 SSO						IDaaS ittiBIX
快速入门	← 百度智能云角色 SSO						
身份提供方 账户	通用配置 单点登录						
应用	单点登录 应用账户 接权						
登录 日志	什么是应用账户? 请参考 应用账户。						
个性化	 ● 如果忽然震使用【IOesS账户名】,应用账户属性的 添加应用账户 20 按照户名说家 >> danfer 	漆加应用账户			×		
	Daws 账户名	按账户名搜索 > danfer				操作	
		已透					
		danfer 📲 👘	DemoSSORole				
				_			
				&#F</td><td>HI3H</td><td></td><td></td></tr></tbody></table>			

40227 20 ¥ #14226 < ±-2 1 T-3 >

2. 搜索并选择一个用户,为其添加应用账号,账号名称为步骤四中创建的角色名称"DemoSSORole",然后保存。您可以在应用账户列表中,查看到您刚刚添加的应用账 号。 云身份服务 / 应用 / 添加应用 / 百 云身份服务 Dass 171977 Dass WHITH A ANNUMBER 快速入门 最份透明方 所件 費果 日志 个性化 就用应用 ← 百度智能云角色 SSO 道用配置 **单点致**承 单点致录 应用账户 把权 什么是应用账户?请参考应用账户。 ● 如果也配置使用【DasS所户名】、应用所户届社配置后不会生效:如果交更、清晰注单#型委 配置 anger / Brage / Bra Daws Romes (5.10月)间 应用账户 遺作 201

六、尝试550

您已经可以尝试 百度智能云角色 SSO。

IDP 发起

请用上一步中关联了百度智能云角色"DemoSSORole"的 IDaaS 账户,登录到 IDaaS 门户页,点击页面上 "百度智能云用户 SSO" 图标,发起 SSO。

IDaaS 应用门户 阿里云 IDaaS								
我的应用	我的应用							
我的账户	请点击下方的应用进行单点显录,若希望修改应用内容,请联系管理员。							
您将以"DemoSSORol	建築範囲 Q 正教報告告 SSO DemeSSORdee e" 的身份,登录到百度智能云中,如下图所示:	Q	89	£	备案	文档	支持	生志 D~
DemoSSORole								安全认证
有权限的服务 子用户无权限或使用ACL模式配置,	廣駅系系統管理交機以							

1.7.2.8. 金山云角色 SSO

本文为您介绍如何在 IDaaS 中配置金山云用户单点登录。使用角色 SSO,您不必为企业或组织中的每一个成员都创建一个子用户。

应用简介

金山集团旗下云计算企业,提供云计算、大数据、人工智能、边缘计算等服务,精准定制适用于企业级市场的解决方案。

操作步骤

- 一、创建应用
- 1. 登录 IDaaS管理控制台。

```
2. 前往 应用-添加应用-应用市场,搜索金山云角色 SSO 应用模板。点击添加应用。
```

```
    ▲山云角色 SSO 限的免费 ⊙
    金山東胡斯下云计寶企业, 提供云计算、大数据、人工智能、边缘计算等服务, 精准定制适用于企业级市场的解决方案。
    SSO
```

二、配置应用单点登录

1. 添加应用后,将自动跳转到应用单点登录配置页,您将在此处进行配置。

^{3.} 确认应用名称,即可完成添加。

应用身份服务

单点登录配置 已启月		
不知道怎么配置? 请参	考对接文档。	
* 金山云 主账号 ID	14.00	
	希望实现 SSO 的目标金山云主账户 ID。	
* 身份提供商名称	AliyunIDaaS	
	在金山云【访问控制】【SSO 管理】中创建的身份提供商的名称。	
* 应用账户	应用账户	\sim
	单点登录时,将选中项作为角色标识,传递给金山云。	
授权范围	全员可访问	\sim
	若选择"手动授权",需要在 应用授权 中进行权限分配。	

2. 配置下列信息:

金山云主账号ID,在金山云控制台-账号及安全中获取。

ශ	金山云	控制台首页				English	备案	消息	文档	工单 ~	企业 ~	费用 ~	a na serie de la compañía de la comp	~	
≣		·管理		账号及安全											
⊜	・ 账号	及安全	♀ ● 您尚未进行实名认证,购买使用本公司服务需要先进行实名认证。 立即认证												
⊕	 实名 	认证		甘士次約 修订										1	
	 消息 	接收管理		登录账号■□□■■未实名		所属行业				所在地区					
⊘				账号ID ■■■■■		产品名称				详细地址					
9						网站地址									
			-												
0				安全设置											
♥				账号安全级别:低											
Ĭ				♥ 登录密码	安全性高的密码可以	使账户更安全,建议您定期更	奂密码。						修改		
				手机号绑定	您已绑定手机号 + 🖡	,	安全手机制	弓,可以找[回密码, 但;	不能用于登录。			修改		

身份提供商名称,需要与金山云【SSO管理】中的身份提供商名称保持一致,如果没有身份提供商,请先参考步骤三,例如:AliyunIDaaSRole。

\Diamond	金山	云 控制部	白首页					English	备案	消息	文档 エ	単〜 í	企业 ~	费用 ~	auiou001	
≣		访问控制			SSO管理											
₿	•	概览		•	如果您的企业或组织	织已有内网账号体系,金山云	为企业用户提供SSOI	功能,您不必在金山云!	账户中为每一	位组织成员	创建子用户,	通过 IdP 身(份验证的外部	8用户可直接访问	可您的金山云	÷
⊕	•	人员管理	^		资源。 1.金山云支持基于:	SAML 2.0 的联合身份验证来	实现与企业内网账号的	的互通,点击查看详情。								
٨		子用户			2.企业IdP的配置,	需要使用金山云的SAML服务	提供商元数据,点击	下载。								
0		用户组			向冲白八垣供支											
0		权限管理	^		创建分价提供商											
0		授权		Œ	身份提供商名称	备注		KRN			创建时间		更新时间]	操作	
Ø		策略			dia kaominina						10.00	2.2.1	100	- Dec	删除	
0	•	项目管理														
	•	SSO管理														
	•	角色管理														
		设置	^													
		安全设置		*												

其他选项保持默认,点击保存即可完成 IDaaS 侧全部 SSO 配置。

⑦ 说明

应用账户:默认使用 IDaaS 账户名作为应用登录标识。应用中用户名必须要和 IDaaS 账户名保持一致,才能完成 SSO。 若希望灵活配置,请参考 单点配置通用说明 - 应 用账户 进行配置。 授权范围:若希望指定可访问应用的 IDaaS 账户,请参考 单点配置通用说明 - 应用账户 进行配置。

三、在金山云中创建身份提供商

下载ldP元数据,在 应用配置信息中,下载 ldP 元数据,保存到电脑中。此文件用于建立金山云对 IDaaS 的信任关系。

身份管理服务公共云合集·EIAM 云身份 服务

应用配置信息

IdP 元数据	https://w星科星aliyunidaas.com/api/v2/app_mi6a7d2uunacdlgr3zra4r3l3q/saml2/meta 回 业下载 IDaaS 作为身份服务提供商的元数据,你需要将元数据下载,并上传到金山云的身份服务提供商中。						
IdP 唯一标识	https:// 『『『『』』aliyunidaas.com/api/v2/app_mi6a7d2uunacdlgr3zra4r3l3q/saml2/meta 口 IDaaS 作为身份服务提供商的唯一标识,同时也是 SAML 响应和断言的签发者。						
IdP SSO 地址	https://= 📭 🌆 aliyunidaas.com/login/app/app_mi6a7d2uunacdlgr3zra4r3l3q/saml2/sso 🗗 IDaaS 提供的用于金山云发起单点登录的地址,用户也可以直接访问该地址,发起金山云 SSO 。						
单点退出地址	暂不支持 IDaaS 提供的用于金山云发起单点登出的地址。						
公钥证书	BEGIN CERTIFICATE MIIEFTCCAv2gAwlBAgISITiUE5Mpqx2U5Bo55kJtoCUyMA0GCSqGSlb3DQEBCwUA MIGSMScwJQYDVQQDDB5hcHBfbWk2YTdkMnV1bmFjZGxncjN6cmE0cjNsM3ExKTAn						
	下载或复制证书,并导入或粘贴到应用中。						
	□ 复制证书内容 业下载证书.cer 文件						
1. 登录访问金山云管理控制台	o						
. 选择左侧菜单SSO 管理 。							
. 在SSO管理页面中单击创建身份提供商校钮							

- 4. 在弹窗中输入**身份提供商名称**和备注,上传元数据文档。
- 元数据文档由企业IdP提供
- 一般为XML格式,包含ldP的登录服务地址、用于验证签名的公钥及断言格式等信息
- 5. 单击提交,完成创建。

四、在金山云中创建角色

- 1. 登录访问金山云管理控制台。
- 2. 在左侧导航栏,单击**角色管理**。
- 3. 在角色管理界面,单击新建角色。
- 在新建角色页面中,设置授权实体类型为身份提供商。
- 5. 输入角色名称和备注。
- 6. 在设置载体信息,选择身份提供商。
- 7. 单击**下一步**,完成角色创建。
- 五、在 IDaaS 中为用户关联角色

配置应用账户,选择需要使用金山云角色 SSO 的账户,为其添加应用账户。**应用账户名需要和金山云角色名称完全一致。**如果一个 IDaaS 账户对应多个金山云角色,可 以创建多个应用账户。



六、尝试SSO

您已经可以开始金山云角色 SSO。

1. 使用已拥有金山云角色	SSO 应用权限的 IDaaS 账户,登录到 IDaaS 应用门户页,点击页面上的图标,即可发起单点登录。	
我的应用	我的应用	
我的账户	请点击下方的应用进行单点登录。若希望修改应用内容,请联系管理员。	
	▲山云桷色 Q × ▲山云桷色 SSO AliYunRole.Aliyun_r	
	每页显示: 10 V 共1条数据 〈 上一页 1 下一页	>
浙ICP备12022327号-58		
2. 如果 IDaaS 账户拥有两	个或以上的应用账户(金山云角色),则需要选择一个应用账户进行单点登录。	
应用则	长户选择	

本文为您介绍如何在 IDaaS 中配置 Salesforce 单点登录。 应用简介

\$ 1040 (2.0

Salesforce是一家创建于 1999 年的客户关系管理(CRM)软件服务提供商,总部设于美国旧金山,可提供随需应用的客户关系管理平台。

```
操作步骤
```

```
一、创建应用
```

```
请管理员前往【应用】【应用市场】,搜索到 Salesf orce 应用模板。确认应用名后,即可完成添加流程。
```

 \sim

Salesforce	限时免费 ⑦						
Salesforce 作为全世界最知名的综合类 CRM SaaS 提供商,拥有完善的云计算技术和经过专家设计的 客户管理软件。							
SSO							
添加应用							

1.7.2.9. Salesforce SSO

您正在尝试登录应用【金山云角色 SSO】,管理员为您 配置了多个应用账户。请选择一个进行 SSO。

确定

```
添加后,会自动来到 SSO 配置页。
```

```
IDaaS 中 Salesforce 应用 SSO 配置页面下方,包含了一系列 Salesforce 完成配置所需要的参数。
```

応	⊞	ᇒ	æ	信	e
122		D U	_		

https://inkqc4cn.dev.aliyunidaas.com/api/v2/app_mihoejhckjwq66z6xygihw6mia/sam12/meta の 主下載 若屈用支持 metadata 配置信息上传/拉取,可以节省大量配置步骤,请在应用 SSO 配置中号技是否有 metadata 上传能力。
https://inkqc4cn.dev.aliyunidaas.com/api/v2/apg_mihcejhckjwq66z6xygihw6mia/saml2/meta の IDaaS 在应用中的标识。需要将值填写在应用单点包录配置中。
https://inkqc4cn.dev.aliyunidaas.com/login/app_mihcejhckjwq66z6xygihw6mia/sami2/soo ⑦ SAML 协议支持 SP 发起单点登录,可能需要填写此地址在应用配置中,由 IDaaS 提供,可以直接访问该地址,进行应用登录,
暂不支持 SAML 协议支持单点退出,可能需要填写此地址在应用配置中,由 IDaaS 提供。
BEGIN CERTIFICATE MIETFCCAv2a/wiBagiY98pX0sHskEm00gIKST8MIh0VMA0GCSqGSib3DQEBCwUA MIGSMSK-vUQ70QGDB8h-eHBUW/072VqdGNandsNgZ6Ninh52ladzZtaWExiXTan
下载 .cer 证书后导入至 salesforce "身份提供商证书"字段中。
☑复制证书内容 坐下载证书 .cer 文件

点击【下载证书 .cer 文件】进行下载,在后续步骤中上传到 Salesforce 中。

二、配置 Salesforce

1. 前往单点登录设置

请在新的浏览器标签中登录 Salesforce 管理后台。通过右上角齿轮按钮,来到设置。



导航前往【设置】【身份】【单点登录设置】菜单。

设	置
>	公司设置
>	数据分类
~	身份
	OAuth 自定义范围
	单点登录设置
	登录历史
	登录流

? 说明

提示:若无法打开页面或无响应,可尝试切换浏览器尝试。部分浏览器会阻止跨域 Cookie,导致页面无法展示。在此情况下,参照页面提示,可以切换到 Salesforce Classic 中编辑和查看。

2. 进行 SAML 配置

在【SAML单点登录设置】中,点击【新建】,来到配置表单。

 SAML单点登录设置
 新建
 元数据文件的新增功能
 元数据 URL 的新增功能

 无 SAML单点登录设置
 无 SAML单点登录设置

页面配置较多,但大部分保持默认即可。您只需将 IDaaS 中 SSO 配置页【应用配置信息】中信息配置进来。 关键字段包括:

字段	别称	说明
<u>姓名</u>	-	固定值:IDaaS,可随意填写。
<u>API 名称</u>	-	固定值:IDaaS,可随意填写。
颁发人	IDP Entity ID	又称为 IDP Entity ID。 从 IDaaS SSO 配置页【应用配置信息】中获取 IdP 唯一标识 ,两方必须保持一致。
<u> 实体 ID</u>	SP Entity ID	又称为 SP Entity ID。 必须固定为:http://saml.salesforce.com,两方必须保持一致。
<u>身份提供商证书</u>	公钥证书	从 IDaaS SSO 配置页【应用配置信息】中下载 公钥证书 获得。在此上传。

		从 IDaaS SSO 配置页【应用配置信息】中获取 IdP SSO 地址 。
身份供应商登录 URL(选填)	ldP Sign-in URL、SAML SSO URL 等	当您希望实现 SP 发起 SSO 时需填写。当进行 SP 发起 SSO 时,Salesforce 将向该地址发送 SAML Request 请求,发起单点登录请求。

参考下图配置示例:

此页面的帮助 🔞 SAML 单点登录设置 保存 保存并新建 取消 i 声明解密证书 声明未加密 😒 SAML身份类型 。 声明包含用户的 Salesforce 用户名 。 声明包含来自用户对象的联盟 ID 。 声明包含来自用户对象的时户 ID SAML 身份位置 身份在主题声明的 Nameldentifier 元素中 身份在属性元素中 服务提供商发起的请求绑定 HTTP POST HTTP 重新引导 ・ 身份提供商登录 URL https://xxxx.aliyunidaas.com.cn/saml/idp/salesforce1 自定义注销 URL 自定义错误 URL 单点注销已启用 - 必填信息 即时用户配置 已启用用户配置 保存 保存并新建 取消

点击保存后,跳转到配置详情页。请您将页面下方展示的【登录 URL】复制出来,后续需填写到 IDaaS 中。

```
        議点

        音看贵组织、Experience Cloud 站点或自定义域的 SAML 端点。

        當島 URL

        杜ps:// my.salesforce.com/services/auth/sp/saml2/logout

        OAuth 2.0 标记端点

        Htps:// my.salesforce.com/services/auth/sp/saml2/logout
        my.salesforce.com/services/auth/sp/saml2/logout
```

SSO 配置完成,但默认处于未启用状态。

3. 启用 SAML SSO

您需要重新返回到 Salesforce【单点登录配置】菜单中,点击【编辑】按钮,勾选【SAML 已启用】,保存完成。

单点登录设置

配置单点登录,以便从外部环境验证 salesforce.com 中的用户。您的组织对单点登录

委返验证是一种使用从 salesforce.com 发送到据点的 Web 服务调用的单点登录方
 联合验证是一种使用发送到 Salesforce 端点的 SAML 声明的单点登录方法。

		编辑 SAML 声明验证器	
委派验证			_
禁用使用 Salesforce 凭据登录	() i		
使用 SAML 的联合单点登录	Ł		_
SAML 已启用			\$

三、在 IDaaS 中配置 SSO

切换回 IDaaS 页面。

在创建完 Salesforce 应用后,应跳转到 SSO 配置页。在表单中填写从 Salesforce 中获取的【登录 URL】。

云身份服务 / 应用 / 添加应用 / Salesforce							
\leftarrow Salesforc	← Salesforce						
通用配置 单点	登录 账户同步						
单点登录 应用账户	5 授权						
单点登录配置 已启用							
不知道怎么配置? 请参	考 IDaaS 配置 SAML 单点登录 。						
* Salesforce城名	Salesforce城名 Salesforce城名						
• 应用账户名	□DaaS販户名 > 应用账户名属性值生成方式						
授权范围	手动授权 ✓ 若选择"手动授权",需要在 应用授权 中进行权限分配。						

其他选项保持默认,点击保存即可完成全部 SSO 配置。

⑦ 说明							
应用账户:用于 SSO 的身份标识, 问】	可参考 SAML 应用账户配置 进行配置。	授权范围:	出于安全考量,	默认需要手动授权。	若在进行前期测试,	可修改为	【全员可访

四、尝试 SSO

您已经可以尝试 Salesforce SSO。

请用已授权使用 Salesforce 的 IDaaS 账户,登录到 IDaaS 门户页,点击页面上 Salesforce 图标,发起 SSO,检查配置结果。

IDaaS	门户页
企业名称	A I



1.7.2.10. JumpServer SSO

本文为您介绍如何在 IDaaS 中配置 JumpServer 单点登录。

应用简介

JumpServer 是全球首款开源的堡垒机,使用 GNU GPL v2.0 开源协议,是符合 4A 规范的运维安全审计系统。

? 说明

JumpServer 支持多种协议,IDaaS 基于 SAML 2.0 协议与其对接,提供应用模板。 JumpServer 于 2021 年 12 月 16 日,发布 v2.17.0,开始支持 SAML 2.0 协议。若您的 版本不支持,可使用 IDaaS OIDC 协议模板与 JumpServer 支持的 OIDC 认证方式进行对接。

操作步骤

一、创建 IDaaS 应用

请管理员前往【应用】【应用市场】,搜索到 JumpServer 应用模板。确认应用名后,即可完成添加流程。

JumpServ	ver
JumpServer 是全球首 v2.0 开源协议,是符合	款开源的堡垒机,使用 GNU GPL 4A 规范的运维安全审计系统。
SSO 添加应用	
添加后,会自动来到	到 SSO 配置页。
配置 SSO	
您只需要将 JumpSe 单点登录配置	erver 根域名填写进来。
不知道怎么配置?请	参考 IDaaS 配置 SAML 单点登录。
* Jumpserver 根域名	https://{{JumpServer_DOMAIN}}/ 请填写 JumpServer 警看根域名。
应用账户 Name ID	使用 IDaaS 账户 账户名 (Username) > 单点登录时,将退中项作为账户标识,传递给业务系统。 >
授权范围	全员可访问 ~ 若选择"手动限权",而要在 <u>应用</u> 限权 中进行权限分配。

其他选项保持默认,点击【保存】即可完成全部 SSO 配置。

? 说明

```
应用账户:默认使用 IDaa5 账户名作为应用登录标识。 若希望灵活配置,请参考 SAML 应用账户配置 进行配置。 授权范围:改为全员可用。若希望指定可访问应用的
IDaa5 账户,请参考 应用授权 进行配置。
```

获取 JumpServer 配置信息

配置页下方的【应用配置信息】中, 只需将【IdP元数据】地址复制出来即可。

应用配置信息

```
    下列信息可能在应用中配置单点登录时使用。
    IDP metadata URL <u>https://xxxx.allyunidaas.com.cn/sami/metadata</u> II <u>と下載</u>

        志屈用支持 metadata 配置信息上传/拉取,可以节省大量配置步骤。

        诸在应用 SSO 配置中寻找是否有 metadata 上传能力。
```

二、JumpServer 中配置 SSO

为 JumpServer 配置 SSO 非常简单。

生成证书

SAML协议依赖证书,由于 JumpServer 不支持自己生成证书,所以需要单独生成。您可以使用 SSL 工具生成公私钥(可搜索市面方案),或使用 <mark>本链投</mark> 生成。

以使用链接生成为例,在页面表单中填写信息(随意填写内容即可,建议尽可能如实填写,内容会在证书中有所体现),点击【Generate Self-Signed Certs】按钮生成证 书。

Private Key	ß	X.509 cert	в
FixxCXZEZ7+TSkglguVeZQUrKd5szUECQQCxodeXhcQe88l8aTXhNo wKUQRE5Es DHXTmJ9xDewzgogYZLiotsf9/gzEASgog5QScAtgCQtQturg/ZipKod AkEA89J2 tVSWMyeC/akZ8D9IPWJaaKyN8SD7/UkwUG6xYsdoywYpABc/i/Z/B ISwgnBUXg IIRkbq1XZiwKFCV4ZQA== END PRIVATE KEY	G H JO	BEGIN CERTIFICATE MILCLICCAZeadwiBAqiBADANBakqhkiG9wQBAQQFADAQMQswCQYI YQQGEwJICZEL MAKGAIUECAwCIKMXCZAJBaNYBAQMAk5DMQswCQYDYQQDDAJQ QZASEWQYMIAXMIQX MITMXMIRaFWQYMZAXMIQXMITMXMIRaMDQxCZAJBaNYBAYTAnYZMQ wCQYDYQQIDAJQ QZELMAKGAIUECawCIKMXCZAJBaNYBAMMAk5DMIGfMAQQCSqGSI	Q 2 2 2 4

将私钥【Private Key】内容复制在本地,保存为 .pem 文件。将【X.509 cert】公钥保存为 .cer 文件。

在接下来配置中,需要将这两个文件上传。

配置 JumpServer

请在新的浏览器标签中使用管理员账号登录 JumpServer 后台。

通过	【系统设置】	【认证设置】,	来到认证方式配置页。	点击【SAML2认证】	的【启用】	按钮。

Server FIT2CLOUD 100年 第五品牌						
- 公 仪表盘	系统设置					
營 用户管理 🛛 🗸	基本设置	邮件设置	LDAP	认证设置	消息订阅	终端设置
ロ 资产管理 へ	i	认证方式				
资产列表				CAS 认证	启用	
网域列表 系统用户				OIDC 认证	启用	
命令过滤				企业微信 认证	启用	
平台列表				\$T\$T (1)7	白田	
				1313 W144	airo	
				毛书 认证	启用	
				RADIUS 认证	启用	
7 五路管理			S	iSO Token 认证	启用	
				SAML2 认证	启用	
0° 5 4910 1		其它				
				忘记密码 URL		
			启	用登录跳转提示		
			14		_	10.00
					重重	爆交

配置表单参数较多,但大多无需关注。您只需关注如下参数:

参数	说明		
<u>SP 密钥</u>	即上一步生成的私钥 Private Key,文件上传 .pem。		
<u>SP 证书</u>	即上一步生成的公钥证书 X.509 cert,上传 .cer 文件。		
开启 SAML2 认证	勾选即可。		
IDP metadata URL	填写 IDaaS 中提供的元数据地址。		
<u>高级设置</u> strict	将 strict 的值改为 false 。 提示:将 strict 设定为 false 。 SAML 配置描述不清,只得如此配置过滤。我们会即时跟进 JumpServer 官网说明,尽可 能提供完整、安全的 SAML 服务。若您对安全性要求较高,请使用 OIDC 协议配置 JumpServer。		

参考下图配置效果:

应用身份服务

基本	
开启 SAML2 认证	8
证书	
SP 密钥	选择文件 jumpserver.pem
	SP 证书和密钥 是用来和 IDP 加密通信的
SP 证书	选择文件 jumpserver.cer
do ikk	上传证书密钥后保存, 然后宣看 SP Metadata 宣看
参数	
IDP metadata URL	
	从远端地址中加载 IDP Metadata
IDP metadata XML	
	IDP metadata URL 和 IDP metadata XML参数二选一即可,IDP metadata URL的优先级高
* 高级配置	j∋
	3 - "en": { 4
	5 "displayname": "JumpServer",
	7 }
	<pre>8 }, 9 "strict": false,</pre>
其它	
同步注销	
总是更新用户信息	
* 用户属性映射	Э.
	1 - 1
	<pre>2 "username": "username", 3 "email": "email"</pre>
	4 }
	映射关系 {idp: sp}
	重量 機交

JumpServer 配置完成,请点击页面下方【提交】。

您已可以尝试使用 IDaaS 账户登录 JumpServer。

三、尝试 SSO

您已经可以尝试 Jenkins SSO。

JumpServer 既支持 IDP(IDaaS 门户)发起 SSO,也支持 SP(应用) 发起 SSO。

⑦ 说明

```
注意:JumpServer 默认支持【自动创建账户】(Just-in-time Provisioning),单点登录时,若 JumpServer 中不存在指定应用账户,则会直接创建,不会拒绝访问。请
在 IDaaS 中管理 JumpServer 访问权限。
```

IDP 发起

请用已授权使用 JumpServer 的 IDaaS 账户,登录到 IDaaS 门户页,点击页面上 JumpServer 图标,发起 SSO。

IDaaS 门户页 企业名称 A



SP 发起

请在匿名浏览器中,打开 JumpServer 登录页,点击下方【SAML2】认证。



使用 IDaaS 账户验证通过后,将直接登录到 JumpServer 中。

1.7.2.11. JIRA/Confluence SSO

本文为您介绍如何在 IDaaS 中配置 JIRA 单点登录。

应用简介

JIRA 是 Atlassian公司出品的项目与事务跟踪工具,被广泛应用于缺陷跟踪、客户服务、需求收集、流程审批、任务跟踪、项目跟踪和敏捷管理等工作领域。JIRA中配置灵 活、功能全面、部署简单、扩展丰富。

? 说明

- JIRA 7.12 及以下版本,使用【SAML身份验证】菜单完成 SSO 配置。JIRA 7.13 及以上版本,使用【SSO 2.0】菜单完成配置。配置内容相近,可统一参考。
- 部分版本 JIRA 没有自带 SSO 配置,请使用 JIRA 【插件】市场,通过安装插件解决。 JIRA 与 Confluence 配置相近,可统一参考。
- 示例中针对 Jira Server v7.12 版本配置。

操作步骤

一、IDaaS 中创建应用

请管理员前往【应用】【应用市场】,搜索到 At lassian JIRA 应用模板。确认应用名后,即可完成添加流程。



添加后, 会自动来到 SSO 配置页。

IDaaS 中 JIRA 应用 SSO 配置页【应用配置信息】中,包含了 JIRA 完成配置所需要的参数。

应用配置信息



二、配置 JIRA

1. 前往单点登录设置

请在新的浏览器标签中登录 JRA 管理后台。通过右上角菜单,来到系统。



导航前往【安全】【SAML身份验证】菜单。

安全	
项目角色	
全局权限	
密码策略	
用户会话	
SAML身份验证	
记住我登录	

开启单点登录。

配置用户登录方式

身份验证方法 〇 登录表

用户通过在登录窗体中输入他们的用户名和密码登录。 SAML单一登录 用户使用SAML身份提供者登录。

? 说明

提示:启用 SAML单一登录,需要先配置好 JIRA/Confluence 访问环境的 HTTPs。

2. 进行 SAML 配置

在【SAML SSO 2.0】设置中,只需要填写 3 个 IDaaS 在【应用配置信息】中提供的参数,即可保存完成配置。

字段	别称	说明
单一登录颁发者	IDP Entity ID	从 IDaaS SSO 配置页【应用配置信息】中获取。
身份提供者单一登录 URL	ldP Sign-in URL、SAML SSO URL 等	从 IDaaS SSO 配置页【应用配置信息】中获取。 JIRA 将向该地址发送 SAML Request 请求,发起单点登录请求。
<u>X.509 证书</u>	公钥证书	从 IDaaS SSO 配置页【应用配置信息】中复制出来,后续使用。

参考下图配置示例:

配置用户登录方式



将页面下方展示的 认定消费者服务 URL 观众 URL (实体 ID) 复制出来,在下一步中填写到 IDaaS中,完成双向配置。

另外,若您希望使用 IDaaS 账户直接登录 JIRA,跳过门户页(即 SP 发起单点登录流程),请复制登录模式中的 登录链接 ,可将其保存为 JIRA 登录书签,并在团队内分发。

```
SAML SSO 2.0行为
登录模式 ● 作为编数身份验证使用SAML
同<sup>中</sup>场用度以登录者意念。他们可以使用单一标志型表 - 逝江身份接供者或感<mark>是 ZS语用</mark>

○ 作为首要身份验证使用SAML

在他们的间面用原生型杂类率时,重定向词定意用个到口P。仍允许REST和其它读求,了展更多信息
```

三、在 IDaaS 中配置 SSO

切换回 IDaaS 页面。

在创建完 JIRA 应用后,应跳转到 SSO 配置页。在表单中填写从 JIRA 中获取的 认定消费者服务 URL 和 观众URL (实体ID)。

不知道怎么配置? 请参考 对我文档。 ・ 以定消费者服务 URL https://47.94.230.179-8443/plugins/serviet/samiconsumer 应用的 SAML SSO 标心地址、与 IDaaS 交互处理中点量承请求、在 JIPA 配置中获取。 ・ 观众URL(家体ID) https://47.94.230.179-8443 应用在 IDaaS 中的标识、在 JIPA 配置中获取。 ・ 应调账户 // / / / / / / / / / / / / / / / / / /	单点登录配置	已启用 🦲
・认定消費者服务 URL https://47.94.230.179:8443/plugins/servlet/samticonsumer 原用的 SAML SSO 核心地址。与 IDaaS 交互处理单点登录请求。在 JIRA 配置中获取。 ・或众URL(读体ID) https://47.94.230.179:8443 原用在 IDaaS 中的标识。在 JIRA 配置中获取。 ・範囲账户 IDaaS 整户名 単点登录时,将选中项作为账户标识。传递输业务系统。	不知道怎么配置?	请参考对接文档。
届用的 SAML SSO 核心地址, 与 IDaaS 交互处理单点登录请求,在 JIRA 配置中获取。 ・寬介URL(葉体ID) Intrp://47.94.230.179-8443 面用在 IDaaS 中的時限,在 JIRA 配置中获取。 ・直周骶P ・直周骶P	• 认定消费者服务 U	RL https://47.94.230.179:8443/plugins/servlet/samlconsumer
* 寛公URL(袁体ID) https://4734.230.179.8443 应用在: (DaaS 中約時況,在,JIRA 配置中校取。 · 应用账户 iDaaS 账户名 · 文 单点登录时,将流中项作为账户标识,传递给业务系统。		应用的 SAML SSO 核心地址,与 IDaaS 交互处理单点登录请求。在 JIRA 配置中获取。
应用在 IDaoS 中的标识,在 JIRA 配置中获取, ・ 应用账户 単点登录时,将造中项作为账户标识,传递给业务系统。	* 观众URL(实体ID)	https://47.94.230.179:8443
 ・直閉賬户 DaaS 账户名 単点登录时,将选中项作为账户标识,传递给业务系统, 		应用在 IDaaS 中的标识。在 JIRA 配置中获取。
单点登录时,将选中项作为账户标识,传递给业务系统。	• 应用账户	IDaaS 账户名
		单点登录时,将选中项作为账户标识,传递给业务系统。
授权范围 全员可访问 🗸	授权范围	全员可访问 🗸

为了便于测试,【授权范围】可暂时选择【全员可访问】。

其他选项保持默认,点击保存即可完成全部 SSO 配置。

? 说明

应用账户:默认使用 IDaaS 账户名作为应用登录标识。应用中用户名必须要和 IDaaS 账户名保持一致,才能完成 SSO。若希望灵活配置,请参考 SAML 应用账户配置 进行 配置。

授权范围:默认全员可用。若希望指定可访问应用的 IDaaS 账户,请参考 单点登录通用说明 进行配置。

四、尝试 SSO

您已经可以尝试 JIRA SSO。

IDP 发起

请用已授权使用 JIRA 的 IDaaS 账户,登录到 IDaaS 门户页,点击页面上 JIRA 图标,发起 SSO,检查配置结果。

SP 发起

请使用刚才复制出来的 登录链接 ,在浏览器中打开。若未登录,将跳转到 IDaaS 登录页进行登录。

验证通过后,将直接登录到 JIRA 中。

参考链接

适用于 JIRA 数据中心应用程序的 SAML SSO sso-for-atlassian-server-and-data-center/version-history https://docs.atlassian.com/software/jira/docs/api/REST/7.6.1/#api/2/user-createUser

1.7.2.12. Jenkins SSO

本文为您介绍如何在 IDaaS 中配置 Jenkins 单点登录。

应用简介

Jenkins 是开源 Cl&CD 软件领导者,是基于 Java 开发的一种持续集成工具,用于监控持续重复的工作,旨在提供一个开放易用的软件平台,使软件项目可以进行持续集成。

? 说明

提示:Jenkins 的 SSO 配置非常便捷,无需填写详细参数,只需将两方的地址互相配置,即可完成。简单易配。

操作步骤

一、添加 Jenkins 应用

请管理员前往【应用】【应用市场】,搜索到 Jenkins 应用模板。确认应用名后,即可完成添加流程。

lenkins	限时免费 ③
Jenkins是开源CI&CD软件领导者,提供超过1000个 构建、部署、自动化,满足任何项目的需要。	`插件来支持
SSO	
添加应用	

添加后,会自动来到 SSO 配置页。

配置 SSO

您只需要将 Jenkins 根域名填写进来。请注意,域名最后不要以 / 结尾,否则会产生冲突。

应用身份服务

单点登录配置	已启用 🛑	
不知道怎么配置?	请参考对接文档。	
* Jenkins 服务地址	http://39.105.33.121:7300	
	请填写 Jenkins 服务的地址。	
* 应用账户	IDaaS 账户名	~
	单点登录时,将选中项作为账户标识,传递给 Jenkins。	
授权范围	全员可访问	\sim
	若选择"手动授权",需要在应用授权中进行权限分配。	

为了便于测试,【授权范围】可暂时选择【全员可访问】。

点击【保存】即可完成全部 SSO 配置。

⑦ 说明

- 应用账户:默认使用 IDaaS 账户名作为应用登录标识。Jenkins 支持【自动创建账户】,单点登录时,若 Jenkins 中不存在指定账户,则会直接创建出来。若希望 灵活配置,请参考 SAML 应用账户配置进行配置。
- 授权范围:若希望指定可访问应用的 IDaaS 账户,请参考 单点登录通用说明 进行配置。

获取 Jenkins 配置信息

配置页下方的【应用配置信息】中,包含了 Jenkins 完成配置所需要的参数。

您无需关注其他参数含义,只需要将【ldP 元数据】链接复制出来即可,后续步骤将在 Jenkins 中粘贴。

 IdP 元数据
 https://exdh7lcn.aliyunidaas.com/api/v2/app_miuwj6yqy/6ppdkyut7lco3ha/saml2/meta の シ下数

 IdP Metadata
 若应用支持 metadata 配置信息上传/拉取,可以节省大量配置步骤。请在应用 SSO 配置中寻找是否有 metadata 上传能力。

二、Jenkins 中配置 SSO

为 Jenkins 配置 SSO 非常简单。

1. 安装 SAML 插件

Jenkins 官方支持 SAML SSO 插件,安装即可使用。

请在新的浏览器标签中使用管理员账号登录 Jenkins 后台。通过左上角菜单,来到插件管理。

🏘 Jenkins	
Dashboard → eiam_t	est
🚔 新建任务	
鵗 用户列表	
🔁 构建历史	
淤 系统管理 →	系统配置
鵗 我的视图	🏠 系統配置
● 打开 Blue Ocean	💥 全局工具配置
S Lockable Resources	🕌 插件管理
🋅 新建视图	📕 节点管理
	安全

切换到【可选插件】标签,搜索【SAML】插件。勾选后选择安装。

Q SAM	L]	
可更新	可选插件	已安装	高级	
Install	Name ↑			
	SAML			
	认证和用户管	管理		
	This plugin	enables use	of a SA	ML 2.0 authentication source for single sign-on support.

页面会提示安装进度,等待直到完成。

? 说明

在安装的过程中,可能会遇到前置插件版本需要更新,可能需要手动重启 Jenkins 服务生效。请参照页面提示重启即可。

安装完成后,请前往【系统配置】页,访问【全局安全配置】。

🏘 Jenkins Q 查找 쯜 新建任务 管理Jenkins 鵗 用户列表 新版本的 Jenkins (2.319.2) 可以**下载 (变更记录)**。 🔁 构建历史 🐡 系统管理 鵗 我的视图 系統配置 会 打开 Blue Ocean 系统配置 配置全局设置和路径 Nuckable Resources 📄 新建视图 🕌 插件管理

		• •	添加、删除、禁用或启用Jenkins功能扩展插
构建队列	^		件。 ▲ 可用册新
队列中没有构建任务			
构建执行状态	^	安全	
1 空闲			
2 空闲			全局安全配置 Jenkins 安全,定义谁可以访问或使用系统。

在【安全域】配置项中,应该出现【SAML 2.0】这一选项,代表安装成功。

安全域
 Jenkins专有用户数据库 允许用户注册
O SAML 2.0
○ Servlet容器代理
 Unix user/group database
O None

2. 进行 SAML 配置

选择【SAML 2.0】,进行 Jenkins SAML 配置。

配置表单参数较多,但都无需关注。您只需关注一部分: <u>表单最上方的【IdP Met adat</u>
--

IdP Metadata URL	6
https://exdł .aliyunidaas.com/api/v2/app_mluwj5yqy	:3ha/saml2/meta
URL to take the IdP Metadata from	
Refresh Period	6
0	
Minutes between downloads of the IdP Metadata	
	Validate IdP Metadata URL

请将 IDaaS 中【IdP 元数据】粘贴到这里,并点击【Validate IdP Metadata URL】进行数据验证。

```
Jenkins 配置完成,请点击页面下方【保存】。
```

```
? 说明
保存配置生效后,Jenkins 自己的管理员登录即刻失效,只能由 IDaaS 登录。若配置错误,您将被锁定在外。
若被锁定在外,请您通过命令行暂时禁用 Jenkins 的安全配置,完成配置修复后,再重新启用。
```

三、尝试 SSO

您已经可以尝试 Jenkins SSO。

Jenkins 既支持 IDP(IDaaS 门户)发起 SSO,也支持 SP(应用)发起 SSO。

? 说明

```
Jenkins 支持【自动创建账户】(Just-in-time Provisioning),单点登录时,若 Jenkins 中不存在指定应用账户,则会直接创建,不会拒绝访问。请在 IDaaS 中管理
Jenkins 访问权限。
```

IDP 发起

请用已授权使用 Jenkins 的 IDaaS 账户,登录到 IDaaS 门户页,点击页面上 Jenkins 图标,发起 SSO。

应用身份服务

IDaaS 应用门户
 Albaha Clourt



SP 发起

请在匿名浏览器中,打开 Jenkins 任意页面。若未登录,将跳转到 IDaaS 登录页进行登录。

验证通过后,将直接登录到 Jenkins 中。

1.7.2.13. Splunk SSO

本文为您介绍如何在 IDaaS 中配置 Splunk 单点登录。

应用简介

Splunk 可收集、索引和利用所有应用程序、服务器和设备生成的快速移动型计算机数据。

? 说明

Splunk 的 SSO 配置非常便捷,无需填写详细参数,只需将两方的地址互相配置,并将 IDaaS 应用账户对应上 Splunk 组名,即可完成。

操作步骤

一、配置 Splunk 应用

请管理员前往【应用】【应用市场】, 搜索到 Splunk 应用模板。确认应用名后, 即可完成添加流程。



添加后,会自动来到 SSO 配置页。

配置 SSO

您只需要将 Splunk 服务地址填写进来。请注意, 域名最后不要以 / 结尾, 否则会产生冲突。

单点登录配置	己島用
不知道怎么配置	? 请参考 对接文档 。
* Splunk 服务地址	https://example.com:8000
	Splunk 服务地址是必填字段 以 http:// 或 https:// 开始的域名或 IP 地址,包含端口号,最后不要以 / 结束。
• 应用账户	应用账户
	只支持【应用账户】。您需要单独为每个账户配置应用中角色。应用账户名与 Splunk 中组名—3
授权范围	全员可访问
	若选择"手动授权",需要在 应用授权 中进行权限分配。

为了便于测试,【授权范围】可暂时选择【全员可访问】。

```
点击【保存】即可完成全部 SSO 配置。
```

```
⑦ 说明
应用账户:您需要单独为每个账户配置 Splunk 应用中所扮演的身份。应用账户名与 Splunk 中组名一致。Splunk 组的配置见下方。
授权范围:若希望指定可访问应用的 IDaaS 账户,请参考 单点配置通用说明 - 应用账户 进行配置。
```

获取 Splunk 配置信息

配置页下方的【应用配置信息】中,包含了 Splunk 完成配置所需要的参数。

您无需关注其他参数含义,只需要下载【IdP 元数据】即可。后续要将该文件上传至 Splunk 中。



二、Splunk 中配置 SSO

为 Splunk 配置 SSO 非常简单。

1. 进行 SAML 配置

来到 Splunk 管理后台,前往【设置】【验证方法】菜单,外部验证机制选择 SAML。



点击 SAML Settings 进行 SSO 配置。



点击右上角【SAML 配置】按钮,打开 SAML 配置表单。

SAML 配置	×
为 Splunk 配置 SAML。 了龢	更多信息 ピ
从 Splunk 下载 SPMetadata	并将其添加到您的 SAML 环境以连接到 Splunk。
SP 元数据文件	下载文件
通过浏览将身份提供程序 (ld	P) 元数据导入到 XML 文件中,或将信息复制并粘贴到"元数据内容"文本框中。
元数据 XML 文件	选择文件
元数据内容	
	应用
常规设置	
单一登录 (SSO) URL ?	https://exdh7lcn.aliyunidaas.com/login/app/app_mixoag6kvrnhi373eyny565rla/saml2/sso
单一注销 (SLO) URL ?	可选
IdP 证书路径 [?]	idpCert.pem
	如果将 IdP 证书储存在 \$SPLUNK_HOME/etc/auth/idpCerts 下,请留空
IdP 证书链?	
	取消保存

将刚才下载的文件上传至【元数据 XML文件】后,所有的字段信息将自动填充。

您需要额外配置一个字段:常规设置中的【实体 ID】字段。该字段固定值为 splunkEntityId 即可。

常规设置	
单一登录 (SSO) URL ?	https://exdh7lcn.aliyunidaas.com/login/app/app_mixoag6kvrnhl373eyny565rla/saml2/sso
单一注销 (SLO) URL ?	可选
ldP 证书路径 [?]	ldpCert.pem
	如果将 IdP 证书储存在 \$SPLUNK_HOME/etc/auth/idpCerts 下,请留空
IdP 证书链 [?]	
复制证书?	
发行人 ID ?	$https://exdh7lcn.aliyunidaas.com/api/v2/app_mixoag6kvrnhl373eyny565rla/saml2/metaaliyunidaas.com/api/v2/app_mixoag6kvrnhl374eyny565rla/saml2/metaaliyunidaas.com/api/v2$
实体 ID ?	splunkEntityId
签名验证请求	

点击保存,完成 SSO 配置。

🥐 说明

注意:保存配置生效后,Splunk自己的管理员登录即刻失效,只能由 IDaaS 登录。若配置错误,您将被锁定在外。

2. 配置 Splunk 组

在进行 SSO 时,IDaaS 所携带的应用账户信息,需要与 Splunk 的组名保持一致。

在刚才 SAML 配置的页面,点击【新组】,进行组创建。



为了测试的目的,在新弹出的表单中,命名组名为 admin,并选择 admin 角色。真实情况下,请您按需分配角色。

添加时间

新建SAML 组				×
组名	admin			
Solunk 角色	可用项目	全部添加 »	选定的项目	< 全部删除
Spiank AB	admin		admin	
	can_delete			
	power			
	splunk-system-role			
	licar			
				取消保存

保存即可。

3. 在 IDaaS 中添加应用账户

回到 IDaaS 控制台,在应用管理中,切换到应用账户标签。

	aJ j도 mj	ц, 11	四市官	连中,	977¥3	-11-22 (71) (62 /	101/202	0
< >> >> >> >> >> >> >>> >>> >>>>>>>>>>		ipiise						
地内配具	車 魚 豆 束 应用账户	授权						
什么最应用账	(户? 请参考 应	用账户。						
 如果您配 	董使用【IDaaS	·账户名】, 8	如用账户属性配	置后不会生效	;如鼎变更,	请前往 单点登录	配置。	
添加应用账户	按账户	名搜索 >	请输入					
DaaS	账户名				应用账户			
							9	

搜索到希望使用 Splunk 的账户,并为其指定 admin 为 SSO 时使用的应用账户。

潏	添加应用账户						×
	按账户名搜索 ∨	michael					
3	已选						
	michael Mich	iael	admin				
						保存	取消

确认后,即可使用该账户尝试 Splunk SSO。

三、尝试 SSO

您已经可以尝试 Splunk SSO。

Splunk 既支持 IDP(IDaaS 门户) 发起 SSO,也支持 SP(应用) 发起 SSO。

IDP 发起

请用已授权使用 Splunk 的 IDaaS 账户,登录到 IDaaS 门户页,点击页面上 Splunk 图标,发起 SSO。

IDaaS 应用门户 Alibaba Cloud			
我的应用	我的应用		
我的账户	请点击下方的应用进行单点登录。若希望修改应用内容,请联系管理员。		
	搜索应用	Q.	
	>		
	Splunk Enterpri se	Jenkins	Elastic Stack
	admin	未配置应用账户	未配置应用账户

SP 发起

请在匿名浏览器中,打开 Splunk 服务地址。若未登录,将跳转到 IDaaS 登录页进行登录。

验证通过后,将直接登录到 Splunk 中。

1.7.2.14. SonarQube SSO

本文为您介绍如何在 IDaaS 中配置 SonarQube 单点登录。

应用简介

SonarQube 是一个开源的代码质量管理系统,支持超过 25 种语言,提供重复代码、编码标准、单元测试、代码覆盖率、代码复杂度、潜在Bug、注释和软件设计报告。

? 说明

```
注意: SonarQube 8.x+ 版本中,系统原生提供 SAML 2.0 的 SSO 支持。我们推荐您使用 8.x 以上版本。若您当前使用版本低于 8.0,或您需要启用 SAML 的高级安全功
能(签名、加密传输等),可能需要额外安装免费/付费插件。可以参考 sonar-auth-saml 或 SonarQube - MiniOrange 等外部插件。本文档中, SonarQube 版本为 9.2
社区版。
```

操作步骤

一、创建应用

请管理员前往【应用】【应用市场】,搜索到 SonarQube 应用模板。确认应用名后,即可完成添加流程。





添加后,会自动来到 SSO 配置页。

配置 SSO
您只需要将 SonarQube 服务地址填写进来。

单点登录配置 ^{8用}	
① 不知道怎么配置? 请参考	IDaaS 配置 SAML 单点登录。
* SonarQube 服务地址	https:// <sonarqube_url></sonarqube_url>
	请填写 SonarQube 服务地址。
应用账户	使用 IDaaS 账户 v 账户名(Username) v
Name ID	单点登录时,将选中项作为账户标识,传递给业务系统。
授权范围	全员可访问 ~
	若选择"手动授权",需要在 <mark>应用授权</mark> 中进行权限分配。
	保存

为了便于测试, 【授权范围】可暂时选择【全员可访问】。 其他选项保持默认, 点击【保存】即可完成全部 SSO 配置。

? 说明

应用账户:默认使用 IDaa5 账户名作为应用登录标识。SonarQube 支持【自动创建账户】,单点登录时,若 SonarQube 中不存在指定账户,则会直接创建出来。 若希 望灵活配置,请参考 <mark>SAML 应用账户配置</mark> 进行配置。 若希望指定可访问应用的 IDaa5 账户,请参考<mark>应用授权</mark> 进行配置。

配置页面下方,包含了一系列 SonarQube 完成配置所需要的参数。

应用配置信息						
1 下列信息可能在	下列信息可能在应用中配置单点登录时使用。					
IdP 元数据 IdP Metadata	据 https://xxxx.allyunidaas.com.on/saml/metadata び 上下載 者应用发射 metadata 設置信息上传/拉旗、可以节客大量配置步骤。 请在应用 SSO 配置中寻找是否有 metadata 上传能力。					
ldP 唯一标识 ldP Entity ID	https://xxxxx.aliyunidaas.com.cn ① Daas 在应用中的标识,需要将值填写在应用单点登录配置中。					
ldP SSO 地址 ldP Sign-in URL	https://xxxxx.aliyunidaas.com.cn/sami/idp/sami1 占 SAML 协议获得 SP 发起着点登录,可能需要填写此地址在应用配置中,由 IDaaS 提供,可以直接协同该地址,进行应用登录。					
单点退出地址 SLO URL	暂不支持。 SAML 协议支持单点退出,可能需要填写此地址在应用配置中。由 IDaaS 提供。					
公钥证书 Certificate	BEGIN CERTIFICATE MIDEjCCAfqgAwiBAgirA/nhmX80izANBgkqhkiG9w0BAQsFADApMR owGAYDVQQD ExPHLXRisQAy(YXV0aGiuZy6jbjELMAkgAtUEBhMCQ04w+lhcNMjExMT EIMDg0NTQ2					
	复制内容 下载证书.cer文件					
从中您需要获取	IdP 唯一标识	IdP SSO 地址	和	公钥证书	三个参数。	

二、配置 SonarQube

请在新的浏览器标签中使用管理员账号登录 SonarQube 后台。

通过【Administration】【Security】, 来到 SAML 配置页。

Administration					
Configuration - Securit	y - Projects - System Marketplace				
General Settings					
Edit global settings for thi	s SonarQube instance.				
ALM Integrations	SAML				
Analuia Caana	In order to enable SAML authentication, the property	'sonar.core.serverBaseURL' must be set to the public URL			
Avaryors GCOpe	Enabled				
External Analyzers	Enable SAML users to login. Value is ignored if provider				
General	D, login url, certificate, login, name attributes are not lefined.				
	Key: sonar.auth.saml.enabled	Reset Default: False			
Housekeeping					
JaCoCo					
Languages	Application ID				
Languages	Identifier of the application. Key: sonar.auth.saml.applicationId	sonarqube			
New Code		(default)			
SCM					
Security					
Technical Debt	Provider Name				
	Key: sonar.auth.saml.providerName	SAML			

字段	IDaaS 中字段名称	说明
----	-------------	----

Enabled	-	启用。
ApplicationID	-	固定值为 "sonarqube"
Provider Name	-	建议填写为"使用阿里云 IDaaS SSO"
Provider ID	ldP 唯一标识 ldP Entity ID	从 IDaaS SSO 配置页【应用配置信息】中获取。
SAML Login URL	ldP SSO 地址 ldP SSO URL	从 IDaaS SSO 配置页【应用配置信息】中获取。
Provider Certificate	公钥证书 Certificate	从 IDaaS SSO 配置页【应用配置信息】中获取。
SAML user name attribute	-	填写 username 即可。
SAML user email attribute	-	填写 username 即可。

将以上配置保存,即可使用 SonarQube SSO。

三、尝试 SSO

您已经可以尝试 SonarQube SSO。

SonarQube 既支持 IDP(IDaaS 门户)发起 SSO,也支持 SP(应用)发起 SSO。

🥐 说明

注意:SonarQube 支持【自动创建账户】(Just-in-time Provisioning),单点登录时,若 SonarQube 中不存在指定应用账户,则会直接创建,不会拒绝访问。请在 IDaaS 中管理 SonarQube 访问权限。

IDP 发起

请用已授权使用 SonarQube 的 IDaaS 账户,登录到 IDaaS 门户页,点击页面上 SonarQube 图标,发起 SSO。

IDaaS 门户页 企业名称 A



SP 发起

请在匿名浏览器中,打开 SonarQube 登录页。若未登录,将跳转到 IDaaS 登录页进行登录。

Log In to SonarQube

💪 Log ir	with SAML
Login	
Password	
	Log in Cancel

验证通过后,将直接登录到 SonarQube 中。

1.7.2.15. 简道云 SSO

本文为您介绍如何在 IDaaS 中配置 简道云 单点登录。

应用简介

简道云是一个零代码轻量级应用搭建平台,旨在满足企业/部门的个性化管理需求。简道云提供 300+ 免费应用模板,提供表单、流程、仪表盘、知识库等核心功能。通过拖 拉拽的操作方式,管理员用户可以搭建出符合自身需求的管理应用(如生产管理、销售管理、人事 OA 等)。

? 说明

提示:简道云 SSO 功能仅在简道云【企业版】开放。若需升级或有特需,请联系简道云进行升级。

操作步骤

一、创建应用

请管理员前往【应用】【应用市场】,搜索到 简道云 应用模板。确认应用名后,即可完成添加流程。

■ 简道云	限时免费 ③
简道云量一个零代码经量级应用搭罐平台,旨在满足企业/部门的个性化管理需求。IDaaS 可以点 的 SSO。	:現到简道云
sso	
添加加速用	

添加后,会自动来到 SSO 配置页。

二、在 IDaaS 中配置 SSO

切换回 IDaaS 页面。

在简道云【企业信息】【基础信息】【账号模式】栏中,复制【CorpID】。

基础信息							
简道云企业名称 Lid	▶•: 修改						
账号模式 🕢 Corp	共観式 如原明定第三方平台、点此咨询 MD <u>[14471 後3:4/x012351df2</u>]						
企业账号URL htt	ps://www.jiandaoyun.com/Nij+414ws 類別 預览 当前企业专属的登录入口						
	的改						
将【CorpiD】填写到表单中。							
不知道怎么配置? 请参考 对施文档。							
* 简道云 CorpID	E CorpiD (1)						
* 应用账户	优先应用账户, 次选 IDaaS 账户各 > 单点型更时, 持造中场作为服户标识, 传递给业资系统。 >						
授权范围	全员可访问	~					
	若选择"手动授权",需要在 应用授权 中进行权限分配。						

为了便于测试,【授权范围】可暂时选择【全员可访问】。

其他选项保持默认,点击保存即可完成 IDaaS 侧 全部 SSO 配置。

? 说明

- 应用账户:默认使用 IDaaS 账户名作为应用登录标识。应用中用户名必须要和 IDaaS 账户名保持一致,才能完成 SSO。若希望灵活配置,请参考 SAML 应用账户 配置 进行配置。
- 授权范围:若希望指定可访问应用的 IDaaS 账户,请参考 单点登录通用说明进行配置。

在页面下方的【应用配置信息】中,即包含了简道云完成 SSO 配置所需要的参数。

应用配置信息

IdP 元数据 IdP Metadata	https://aliyunidaas.com/api/v2/app_mivldtifkv64hiqv4wop7bhg34/saml2/meta			
IdP 唯一标识	https://s,laliyunidaas.com/api/v2/app_mivldtiffwb4hiqw4wop7bhg34/saml2/meta			
IdP Entity ID	IDaaS 在应用中的标识。需要将值填写在应用单点登录意图中。			
IdP SSO 地址	https://www.aliyunidaas.com/login/app/app_mividtiffwb4hiqw4wop7bhg34/sami2/sso 可			
IdP Sign-in URL	SAML协议支持 SP 发起单点登录,可能需要填写此地站在应用配置中。由 IDaas 提供。可以直接访问该地址,进行应用登录。			
单点退出地址	暂不支持			
SLO URL	SAML协议支持单点退出,可能需要填写此地址在应用配置中。由 iDaaS 提供。			
公钥证书 Certificate	BEGIN CERTIFICATE MIESTICCA-V2gAwtBAGISTTwo2KC6ECsDy8II+v992z9MA0QCSqGSIb3DQEBCwUA MIGSMScwUrgUV02QDBSA-hEBEW12bGR6aWZnd2DaGladzR3B3A3YminMAQ2KTAn			

三、配置 简道云

1. 前往单点登录设置

请在新的浏览器标签中登录 简道云 管理后台。通过右上角菜单,来到企业管理。

 🔁 If	怡						BRXING		0	0
		我的待办		0		4	(5	Michael Grant	R	itaten
		0		我发起的	我处理的	的 抄送我的	发起新流机	个人设置 企业管理		
	我的应用 ©						Q 输入名称未进来	版本购买		
								退出		
	「「「」」「「」」「「」」「」」「「」」「」」「「」」「」」「」」「」」「」」	備道云高级	功能介绍							

导航前往【企业信息】【高级设置】【单点登录】选项。

业工作台 设置 给企业成员设计默认的工作台样式
服务号集成
▲ 金承 应用于企业账号URL和发布给成员的内链接中 如何配置?
单点登录。
▲ 田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田

2. 进行 SAML 配置

点击【配置】按钮,弹出配置表单。

将 IDaaS 【应用配置信息】中的参数全部填写到配置表单中。

字段	别称	说明
SAML 2.0 Endpoint	IdP SSO 地址 IdP Sign-in URL	从 IDaaS SSO 配置页【应用配置信息】中获取。 简道云 将向该地址发送 SAML Request 请求,发起单点登录请求。
Issuer URL	ldP 唯一标识 ldP Entity ID	从 IDaaS SSO 配置页【应用配置信息】中获取。
<u>SAML 加密算法</u>	签名算法	选择 SHA-256。
IDP 公钥	公钥证书 Certificate	从 IDaaS SSO 配置页【应用配置信息】中复制出来,后续使用。

参考下图配置示例:

配置单点登录	\times
请选择单点登录配置方式 ● SAML 20 ○ 自定义接口	
请从支持 SAML 认证协议的身份认证服务商中获取以下信息进行填写 SAML 2.0 Endpoint (HTTP)*	
https://·引作在maliyunidaas.com/login/app/app_mivldtiffwb4hiqw4wop7bhg3 IdP 公钥	
BEGIN CERTIFICATE MIEFTCCAv2gAwiBAgISHTvxr2KCeECsDy8JI+vo92z9MA0GCSqGSIb3DQEBCw UA	
SAML加密算法	
SHA-256 🗸	
Issuer URL*	
$https://\ensuremath{\mathcal{A}}_{\mathcal{A}}^{*}f_{\mathcal{A}}^{*} \wedge f_{\mathcal{A}}^{*} diyunidaas.com/api/v2/app_mivldtiffwb4hiqw4wop7bhg34/s$	
如何配置? 取消 保存	

点击保存后,展示出详细 SSO 信息。

東登录	(开) 应用于企业账号URL和发布给成员的内链接中 如何配置?			
	SAML 2.0 Endpoint	https://xxxxx.cloud-idaas.com/saml/idp/jiandaoyun		
	认证返回地址	https://www.jiandaoyun.com/sso/saml/61de470cbc03b40008551df2	复制	
	Metadata 地址	https://www.jiandaoyun.com/sso/saml/61de470cbc03b40008551df2	下载	
	简道云登出地址	https://www.jiandaoyun.com/sso/saml/61de470cbc03b40008551df2	复制	
	修改配置 清空配置			

单点登录配置完成。

3. (可选)创建简道云账户

IDaaS SSO 到简道云,默认使用 IDaaS 账户名作为标识,与简道云账户的【编号】属性值需要完全对应,才能完成 SSO。对应关系可通过 IDaaS 单点登录的【应用账户】字 段灵活配置。

若 IDaaS 账户尚未有对应的简道云账户,单点登录会失败报错。

可以在 简道云【通讯录】菜单内,添加账户,指定编号与 IDaaS 账户对应,激活后即可使用。



四、尝试 SSO

您已经可以尝试 简道云 SSO。

IDP 发起

请用已授权使用 简道云 的 IDaaS 账户,登录到 IDaaS 门户页,点击页面上 简道云 图标,发起 SSO,检查配置结果。



SP 发起

请在匿名浏览器中,打开 简道云 登录页,点击【单点登录】页签下的"登录"按钮,则会跳转到 IDaaS 进行登录。如果用户尚未登录 IDaaS ,则 IDaaS 会引导用户进行登录



验证通过后,将直接登录到 简道云 中。

1.7.2.16. Salesforce SSO

This article introduces Salesforce SSO configuration on IDaaS.

App Introduction

Salesforce is a SaaS software which provides customer relationship management software and applications focused on sales, customer service, marketing automation, analytics, and application development.

Configuration Steps

1. Create Application

Please direct to Applications - Add Application - Marketplace and find Salesforce template. After confirming the application's name, a new app would be created.



You will be automatically redirected to SSO configuration page.

Below, IDaaS provides a series of attributes needed on Salesforce side.

Application Settings



Download the certificate to be uploaded on Salesforce later.

2. Configure Salesforce SSO

2.1. Go to SSO Settings

Please login salesforce admin panel. Visit Settings from the gear icon at the top right.



Navigate to SETTINGS - Identity - Single Sign-on Settings.

SETTINGS

- > Company Settings
- > Data Classification

✓ Identity

Auth. Providers
 Identity Provider
 Identity Provider Event Log
 Identity Verification
 Identity Verification History
 Login Flows
 Login History
 OAuth Custom Scopes
 Single Sign-On Settings
 Security

? 说明

If this page is not responsive, please try another browser. Some browsers forbids cross site cookies, which might cause display problems. When that happens, you may switch to Salesforce Classic as the page would suggest.

2.2. SAML Configuration

Click New.

SAML SI	ngle Sign-Or	n Settings	New New from Metadata File New from Metadata URL
Action	Name	SAML Version	Issuer
E-010-0	and in case of	- 24	the second se

There are quite a few things an the form, but we only need to pay attention to the following:

Attribute	Alias	Comments
<u>Name</u>	-	Fixed Value: IDaaS。You may enter as you wish.
<u>API Name</u>	-	Fixed Value: IDaaS。You may enter as you wish.
lssuer	IDP Entity ID	AKA IDP Entity ID. Retrieved from IDaaS Application Settings.
Entity ID	ESP Entity ID	AKA SP Entity ID. Retrieved from IDaaS Application Settings.
Identity Provider Certificate	Public Key Certificate	Retrieved from IDaaS Application Settings.
Identity Provider Login URL	Also called IdP Sign-in URL SAML SSO URL etc.	Retrieved from IDaaS Application Settings.

After you successfully save, it redirects to settings page. Please copy the Login URL and later paste it into IDaaS.

Endpoints									
View SAML endpoints	for your org, Ex	perience	Cloud sites,	or custor	m dor	nains.			
Your Organization									
	Login URL	https://			sale	esforce.co	m		
	Logout URL	https://		1	y.sale	esforce.co	m/service	es/auth/sp/saml2/logout	
OAuth 2.0 Tol	ken Endpoint	https://		a	y.sale	esforce.co	m/service	es/oauth2/token	
				E	dit	Delete	Clone	Download Metadata	SAML Assertion Validator

2.3. Enable SAML SSO

You need to go back into the Salesforce SSO configuration and enable this setting. Clieck on Edit on the SSO main page, and enable SAML SSO.

3. Configure SSO in IDaaS

Go backto IDaaS page.

Paste the Login URL from Salesforce.

SSO Enabled

For information	about how to configure SSO settings, see Configure SSO $_{\circ}$	
• Login URL	https://xxxxx.my.salesforce.com	
-	SAML ACS URL provided by Salesforce. Presented on its SSO co	onfiguration page.
* App User	App User	\sim
	When SSO, the selected attribute will be IDaaS account's role/us	ser in that applicatio
Authorize	All Users	~
	If you select Manual, you need to go to Authorize to assign nerro	nissions

For ease of testing, choose All Users for Authorization.

Save to complete all configurations.

4. Try

You may now try to SSO Salesforce.

Please use an authorized user to login IDaaS user portal. Click on the Salesforce icon to initiate SSO.

1.7.2.17. Teambition SSO

本文为您介绍如何在 IDaaS 中配置 Teambition 单点登录。

应用简介

Teambition 是阿里巴巴旗下的团队协作工具,通过项目和任务的可视化管理来支撑企业团队协作,适合产品、研发、设计、市场、运营、销售、HR 等各类团队,让企业协 同化繁为简,轻松愉悦。

? 说明

操作步骤

一、创建应用

- 1. 登录 IDaaS管理控制台。
- 2. 前往应用-添加应用-应用市场,搜索到 Teambition 应用模板。点击添加应用。

```
▼ Teambition 限的免费 ③
阿里巴巴旗下团队协作工具,通过项目和任务的可视化管理来支厚企业
团队协作、适合产品、研发、设计、市场、运营、销售、HR 等各类团
队、让企业协同化繁为简,轻松愉悦。
SSO
添加应用
```

3. 确认应用名称,即可完成添加。

添加后,会自动来到 SSO 配置页。在SSO 配置页的 应用配置信息中,包含了 Teambition 完成配置所需要的参数。

並用配置信息	
IdP 元数据 IdP Metadata	https://viewiewiewiewiewiewiewiewiewiewiewiewiewi
IdP 唯一标识	https://i.ee.uliyunidaas.com/api/v2/app_mividtiffwbdhiqw4wop7bhg34/saml2/meta ♂
IdP Entity ID	IDaaS 在应用中的标识,需要将值项写在应用单点登录配置中。
IdP SSO 地址	https://www.aliyunidaas.com/login/app/app_mivldtiffwb4hiqw4wop7bhg34/sam12/sso 了
IdP Sign-in URL	SAML协议支持 SP 发起单点登录,可能需要填写此地址在应用配置中。由 IDaas 提供,可以直接访问该地址,进行应用登5
单点退出地址	智不支持
SLO URL	SAML协议支持单点退出,可能需要填写此地址在应用配置中。由 IDaaS 提供。
公明证书 Certificate	BEGIN CERTIFICATE MIETTCCA/24wiB4/2615HTww2KCeECED/98/#+v9229MAGGCSqGSib3DQEBCwUA MIGSMSww0/QVDQDDB5hcH8BWW2bcR0aWZmd20aGkdz83b3A3YmhnMr2zkTAn

二、配置 Teambition

1. 前往单点登录设置

请在新的浏览器标签中登录 Teambition,按照下图所示,进入管理后台。



导航前往基础-企业身份认证选项,将展示SAMLSSO配置。

基础	Ŧ	SAML SSO 配置 配置 SAML 后,可以在登起汽面通过 SSO 方式登录		🗇 查看文档
		36.000F28		
成员管理 企业设置 回 自定义字段	*	① 添加并验证域名后,所有企业邮粮后拨为该域名的成员将会被引导到你所配置的 SAML SSO 页面中登录		×
□ 企业标签		域名验证	④ 添加并验证域名	🔎 开启实名认证担保 🕕 🚺 查看文档
☑ 任务类型				
🖯 日程类型				
📋 企业日历		暂无域名		
□ 企业优先级				
应用	+			
权限	+			
安全	+			

点击 **添加配置**,打开如下所示对话框。

身份管理服务公共云合集·EIAM 云身份 服务

SAML SSO 配置 X X
登陆名称
请输入 SSO 登陆显示名称
SSO 地址
https://example.teambition.com/
在 SSO 选项下,滚动至 SAML 2.0 Endpoint 便可以找到 SAML 2.0 URL
IdP 公钥 (选填)
填写 ldP 公钥 SAMI 加密始法
SHA-1 V
lssurer URL (选填)
http://
IdP SLO 地址 (选填)
http://
用户从 Teambition 登出后,可以通过触发 idP 的 SLO 地址,登出所有 SAML 应用
②如何配置 SAML SSO ? 查看文档 保存

2. 进行 SAML 配置

点击 配置 按钮,弹出配置表单。

将 IDaaS 应用配置信息 中的参数全部填写到配置表单中。

字段	别称	说明
登录名称		建议填写为: 阿里云 IDaaS
550 地址	ldP SSO 地址 ldP Sign-in URL	从 IDaaS SSO 配置页 应用配置信息 中获取。
IdP 公钥	公钥证书 Certificate	从 IDaaS SSO 配置页 应用配置信息 中复制出来,填写到文本框中。
SAML 加密算法	签名算法	选择 SHA-256。
Issuer URL	ldP 唯一标识 ldP Entity ID	从 IDaaS SSO 配置页 应用配置信息 中获取。

参考下图配置示例:

应用身份服务

SAML SSO 配置	\times
登陆名称	
阿里云 IDaaS	
SSO 地址	
https://wgfpfem.aliyunidaas.com/login/app/app_miyfqd35gvnisnzprpvik6fge	da/s
在 SSO 选项下,滚动至 SAML 2.0 Endpoint 便可以找到 SAML 2.0 URL	
IdP 公钥 (选填)	
BEGIN CERTIFICATE MIIEFTCCAv2gAwlBAgISbjtXkIhCEitXICXdmm9LVoG8MA0GCSqGSIb3DQEBC wUA MIGSMScwJQYDVQQDDB5hcHBfbWI5ZnFkMzVndm5pc256cHJwdmIrNmZn	•
SAML 加密算法	
SHA-256 ~	
Issurer URL (选填)	
https://هوالمانعة:https://هوالمانعة:https://هوالمانعة:https://هوالمانعة:https://هوالمانعة:https://هوالمانعة:https://هوالمانعة:https://هوالمانعة:https://هوالمانعة:https://هوالمانعة:https://هوالمانعة:https://هوالمانعة:https://هوالمانعة:https://هوالمانعة:https://	am
IdP SLO 地址 (选填)	
http://	
用户从 Teambition 登出后, 可以通过触发 idP 的 SLO 地址,登出所有 SAML 应用	
②如何配置 SAML SSO ? 直看文档 探	存

点击保存后,展示出详细 SSO 信息。

SAML SSO 配置 配置 SAML 后,可以在登时	顶面通过 SSO 方式登录
登陆名称	阿里云 IDaaS
SSO 地址	https://www.ilian.aliyunidaas.com/login/app/app_miyfqd35gvnisnzprpvik6fgda/saml2/sso
认证返回地址	https://account.teambition.com/saml/62335- b= 1 === i = i = i = 301226==-08/callback 🗍
Metadata 地址	https://account.teambition.com/saml/62000; و: المَعَانَ المَعَانَ المَعَانَ المَعَانَ المَعَانَ المَ
Teambition 登出地址	https://account.teambition.com/logout 🗍
编辑 清空配置	

复制上图中的 认证返回地址,下一步需要将该地址需要填写到 IDaaS 中。

三、在 IDaaS 中配置 SSO

切换回 IDaaS 页面。

在创建完 Teambition 应用后,应跳转到 SSO 配置页。将上一步复制的地址,填写到表单中的 Teambition 认证返回地址。

单点登录配置 已启用						
不知道怎么配置? 请参考 对接文档。						
* Teambition 认证返回地 址	https://account.teambition.com/saml/ <your_corp_id>/callback IDaaS 回响 Teambition 的地址,Teambition 在该地址接收SAML服育</your_corp_id>					
* 应用账户	DaaS 账户名 ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~	~				
授权范围	全员可访问 ~ √ 若选择"手动接权",需要在 <u>应用赚权</u> 中进行权限分配。	~				

其他选项保持默认,点击保存即可完成全部 SSO 配置。

? 说明

提示 应用账户:默认使用 IDaaS 账户名作为应用登录标识。应用中用户名必须要和 IDaaS 账户名保持一致,才能完成 SSO。若希望灵活配置,请参考 单点配置通用说 明 - 应用账户 进行配置。 授权范围:默认全员可用。若希望指定可访问应用的 IDaaS 账户,请参考 单点配置通用说明 - 应用账户 进行配置。

四、尝试 SSO

您已经可以尝试 Teambition SSO。

IDP 发起

请用已授权使用 Teambition 的 IDaaS 账户,登录到 IDaaS 门户页,点击页面上 【Teambition 】图标,发起 SSO。

IDaaS 应用门户 阿里云 IDaaS	
我的应用	我的应用
我的账户	请点击下方的应用进行单点登录。若希望修改应用内容,请联系管理员。
	搜索应用 Q Family Teambiltion

SP 发起

Teambition需要先进行域名绑定和验证,才可以在登录界面显示外部的SAML认证源,进而从SP发起登录,如下图所示。

① 添加并验证域名后,所有企业邮箱后缀为该域名的成员将会被引导到你所配置的 SAML SSO 页面中登录				;
域名验证		⑦ 添加并验证域名	, 开启实名认证担保 ①	🗇 查看文档
	暂无域名			

请参考 Teambition 官方文档 https://thoughts.teambition.com/share/5ff6ab616d745600469814b4 ,完成域名绑定操作,绑定成功后,访问Teambition,直接在登录 页面点击「使用 SSO 登录」或者点击「第三方账号登录」中的「SSO」都会触发到 阿里云 IDaaS 进行登录。

teambition	teambition
	单点登录 SSO
密码 ① 忘记察告?	输入企业邮箱,使用你的企业帐号登录
登录	
使用 微信 登录 (使用 数6 登录 (使用 550 登录) 第三方第号登录	登录
还没有帐号? 注册新帐号	使用 Teambition 账号

1.7.2.18. WordPress miniOrange SAML

本文为您介绍如何在 IDaaS 中配置 WordPress 单点登录。

应用简介

WordPress

? 说明

注意: WordPress 需要额外插件才能实现 SSO, 例如: SAML Single Sign On - SAML SSO Login, 该插件支持 WordPress 3.7及更高版本。本篇文档中 WordPress 版本为 5.9.2。在 WordPress 中通过 配置请参考文档: https://plugins.miniorange.com/saml-single-sign-on-sso-wordpress-using-custom-idp

操作步骤

- 一、配置 IDaaS 应用
- 1. 登录 IDaaS管理控制台。

2. 前往 应用-添加应用-应用市场,搜索到 WordPress miniOrange 应用模板。点击 添加应用。



3. 确认应用名称,即可完成添加。

二、在 IDaaS 中配置 SSO

您只需要将 WordPress 服务地址填写进来,注意结尾不要以"/"结尾。

半点豆水配直 0.4/0		
不知道怎么配置? 请参考	》对接文档。	
* WordPress 服务地址	http:// <your_domain> WordPress 服务地址,不能以""范尾</your_domain>	
* 应用账户	IDaaS 账户名 单点登录时,将选中项作为账户标识,传递给业务系统。	~
援权范围	金克可访问 若选择"手动线权",需要在 <u>应用操权</u> 中进行权限分配。	~

其他选项保持默认,点击 保存 即可完成全部 SSO 配置。

? 说明

应用账户:默认使用 IDaaS 账户名作为应用登录标识。WordPress 支持 自动创建账户,单点登录时,若 WordPress 中不存在指定账户,则会直接创建出来。若希望灵 活配置,请参考 单点配置通用说明 - 应用账户 进行配置。 授权范围:默认全员可用。若希望指定可访问应用的 IDaaS 账户,请参考 单点配置通用说明 - 应用账户 进行 配置。

查看配置页下方的 应用配置信息中,包含了 WordPress 完成配置所需要的参数。

应用配置信息						
IdP 元数据 IdP Metadata	https://i.ealalyunidaas.com/api/v2/app_mixpu3hqp4fpka3e67lqicb2ly(saml2/meta の 上下載 岩島用支持 metadata 配置信息上传/拉敏,可以节管大量配置步骤,請在息用 550 配置中寻找是否有 metadata 上传能力。					
IdP 唯一标识 IdP Entity ID	https://www.aliyunidaas.com/api/v2/app_mixpu3hqp4fpka3e67/lqjcb2ly/saml2/meta 凸 DaaS 在应用中的标识。需要将值属写在应用单点型变配置中。					
IdP SSO 地址 IdP Sign-in URL	https://i.g.i.g.ialyunidaas.com/login/app/app_mixpu3hqp4fpka3e67lqjcb2ly/saml2/sso ♂ SAML 协议支持 SP 发起师师登录,可能需要項写此地址在应用配置中,由 IDaas 提供,可以直接访问该地址,进行应用登录。					
单点退出地址 SLO URL	智不支持 SAML 协议支持单点退出,可能需要填写此地址在应用配置中。由 IDaaS 提供。					
公钥证书 Certificate	BEGIN CERTIFICATE MIETICCA/254wiRAgiSUNBpic/GU/MKEXHett2X/vgDMA0GC5qGSIB3DQEBC/wUA MIGSMS&0/UVQQDDB5hetf8fbWildetHwikGzwa2EztTY3bHfq212bHfq22bHfq212bHfq22bHfq212bHfq22bHfq212bHfq22b					
	下载或复制证书,并导入或粘贴到应用中。					
	日本語の「日本語」である「日本語」である「日本語」である「日本語」である「日本語」である「日本語」である「日本語」である「日本語」である「日本語」である。					
从中您需要获取	IdP 元数据 IdP 唯一标识 IdP SSO 地址 和 公钥证书 四个参数。					

三、WordPress 中配置 SSO

1. 安装插件

WordProcess 插件市场中有多款用于实现单点登录的插件,搜索 SAML Single Sign On,在搜索列表中,选择 SAML Single Sign On - SAML SSO Login 插件(该插件 由 miniOrange 提供),点击 **立即安装**。

应用身份服务

添加插件 上侧	ŧ					▶帮助 ▼
投放结果 特色 然	N 1987 Kan				关脚字 ~ SAML Single Sign On	
						22个项目
$\mathbf{\mathbf{G}}$	SAML Single Sign On – SAML SSO Login WordPess SSO S (PM:: minOrange		Login using WordPress Users (WP as SAML IDP) Login with Word #?#:: miniCrange	立即安装 更多评情	OneLogin SAML SSO	2的安装 更多详情
★★★★ (146) 8,000+个已启用安装版	↓ ● 读描件兼容于均当前使用的	近更新: 2同前 WordPress版本 700+个已应用安装数	✔ 说描件兼容于恋当的印	最近現新: 2問前 明的WordPress版本 ★★★★★(13) 6,000+个已回用安装数	最近更新 ✓ 该插件 教 容于您当你伊耶的Word	Mf: 1月前 IPress版本
Ċ	Single Sign On for Windows Single Sign On fPB: minDrange	①即改独 更SiFt柄 EZPZ SP	EZPZ SAMI, SP Single Sign On (SSO) EZPZ SP makes L 作者: Overt Software Solutions ITD	DERM DESKA	OAuth Single Sign On – SSO (OAuth Client) WerdPress SIO S 카페는 minChange	2即安禁 更多详情
★★★★★ (2) 60+个已启用安装数	最 未在想的WordPh	近距額: 3月前	未在物的	最近更新:1年前 (ordPress総本中測试 2,000+个已信用安装数	欄近要網 ✔ 该插件兼容于您当新使用的Word	Wi: 3周前 Press版本

插件安装成功之后,在 插件-安装插件 列表中,找到 miniOrange SSO using SAML 2.0 插件,启用该插件。

@ 仪表盘	插件 安娜神		显示选项 🔻 💽 帮助 🔻
📌 文章	全部(3) 已合用(1) 木合用(2) 最近合	用过(1) 自动理解(2)(3)	搜索已安装的插件
93 wik	批攝操作 く 应用		4个项目
🗐 页面	□ 插件	施送	白动更新
🏴 評论	Akismet 反垃圾评论被成功删除。		
🎤 外窥	miniOrange SSO using SAML 2.0	miniOrange SAM, plugin allows ssortogin using Azure, Azure B2C, Okta, ADFS, Keycloak, Onelogin, Salesforce, Google Apps (Issuite), Salesforce, Shibboleth, Centrity, Ping, Auth0 and other Identity Providers. It acts as a SAM, Service Provider which can be configured	10 店用自动更新
🖆 插件	唐用 删除	establish a trust between the plugin and DP to securely authenticate and login the user to WordPress site. 43 17075 LTPP	
已安装的新鲜		are taken i fear - munoranile i 2280-00	

2. 配置 SSO

启用插件之后,WordPress 将在左侧导航栏中增加菜单 miniOrange SAML 2.0 SSO,点击该菜单,即可进入编辑页面,如下图所示:

	mi	niOrang	e SSO u	sing SA	AML 2.0						P	remium Pla	ns Upgrade N	low
ア ~ 						Service Pro	vider Setup	Service Pro	vider Metadat	a Attribu	te/Role Mappi	ng Redi	irection & SSO	Links Add-Ons
♥ 评论 ▶ 外观		Q Sea	rch and seled	t your IDP										
▶ 摘件 ▲ 用户 <i>▶</i> 工具		Classlink	OneLogin	Centrify	PingFederate	Shibboleth 2	Shibboleth 3	AbsorbLMS	Gluu Server	JumpCloud	IdentityServer	Degreed	CyberArk	Duo
E 设置		FusionAuth	SecureAuth	NetlQ	Fonteva	SURFconext	PhenixID	Authanvil	Bitium	CA Identity	OpenAM	Oracle	PingOne	RSA SecureID
Plugin Configuration Premium Plans Add-Ons							SimpleSAMLph p	wso2	Custom IDP					

在 Service Provider Set up 标签内,搜索 Cust om IDP,如下图所示:

	Service Provider Setup	Service Provider Metadata	Attribute/Role Mapping	Redirection & SSO Links	Add-Ons
Q Custom IDP					
		Custom IDP			

在搜索结果中,点击 Custom IDP 图标,打开下图所示界面,可以通过 上传IDP元数据 和 手动填写IDP元数据 两种方式,配置IdP信息。

● 上传IDP元数据

选择 Upload IDP Metadata 页签

应用身份服务

Configure Service Provide	r		
	Enter IDP Metadata Manually	OR	Upload IDP Metadata
Identity Provider Name :	AliyunIDaaS		
Upload Metadata :	选择文件未选择任何文件		1. Upload
		OR	
Enter metadata URL :	https://-gipter.aliyunidaas.com/api/v	2/app_mivtvakxby	한 Fetch Metadata

字段	IDaaS 中字段名称	说明				
Identity Provider Name		输入一个名字,例如: AliyunIDaaS ,这个名字将在WordPress 登录页中显示。				
<u>Upload Metadata</u>	IdP 元数据	从 IDaaS 单点登录配置页 应用配置信息 中获取,对应 " IdP 元数据" ,您可以将元数据下载到本地之后,然后 在当前页面进行上传。				
Enter metadata URL	iur metauata	从 IDaaS 单点登录配置页 应用配置信息 中获取,对应"IdP 元数据"配置项中的URL。				

● 手动填写IDP元数据

将 IDaaS 中获取到的信息填写进入表格中。参数对照如下:

Configure Service Provide	er 🕐				
	Enter IDP Metadata Manually	OR	Upload IDP N	Metadata	
Identity Provider Name :					
luentity Provider Name .	AliyunIDaaS				
IdP Entity ID or Issuer :	https://wglj=fin_n.aliyunidaas.com/api/va	2/app_mivtvakxbyk	tqo247g5jliu6uu/san	nl2/meta	
	Note: You can find the EntityID in Your IdP-Metadata XML file enclosed in EntityGescriptor tag having attribute as entityID				
SAML Login URL :	https://%jf_f_tan.aliyunidaas.com/login,	/app/app_mivtvakx	byktqo247g5jliu6uu,	/saml2/sso	
	Note: You can find the SAML Login URL in Your IdP-Metadata XML file enclosed in SingleSignOnService tag (Binding type: HTTP-Redirect)				
X.509 Certificate :	BEGIN CERTIFICATE MIIEFTCGAv2gAwiBAgISWuP97eXkCYpE+blqbySAL452MA0GCSqGSIb3DQEBCwUA MIGSMScWQYDYQQDDB5hcH8fbWl2dHZha3hieWt0cW8yNDdnNWpsaXU2dXUxkTAn BgNVBAsMIGlkYWFzX2thcHcydHd0d2xr2Zzoc21sdDRuc2ZxdHk0MRwwGgYDVQQK				
	Note : Format of the certificate - BEGIN CERTIFICATE X0X000000000000000000000000000000				
Character encoding :	Note : Uses iconv encoding to convert X509 certi	ficate into correct enco	ding.		
	Save Test Co	nfiguration			
字段	IDaaS 中字段名称	说明			
dentity Provider Name		输入-	一个名字,例如:	AliyunIDaaS	,这个名字将在 WordPress 登录页

从 IDaaS SSO 配置页 **应用配置信息** 中获取,对应" IdP 唯一标识"

IdP entity ID or Issuer

ldP 唯一标识

IdP Entity ID

SAML Login URL	ldP SSO 地址 ldP Sign-in URL	从 IDaaS SSO 配置页 应用配置信息 中获取,对应" IdP SSO 地址"
X.509 Certificate	公钥证书 Certificate	从 IDaaS SSO 配置页 应用配置信息 中获取,对应 " IdP 公钥证书"

3. 配置属性映射(可选)

只有付费版的 miniOrange SAML SSO 插件,才支持配置属性映射。选择 Attribute/Role Mapping 页签,如下图所示:

Service Provider Setup Service Provider Metadata Attribute/Role Mapping Redirection & SSO Links Add-Ons

Attribute Mapping @		
Username (required) :	NamelD	W
Email (required) :	NamelD	
First Name :	Enter attribute name for First Name	
Last Name :	Enter attribute name for Last Name	
Group/Role :	Enter attribute name for Group/Role	
Map Custom Attributes	Customized Attribute Mapping means you can map any attribute of the IDP to the usermeta table of your database.	

目前支持的属性映射:

WordPress 属性名	IDaaS SAML 断言中的属性名	说明
Email	email	如果 IDaaS 中,用户的邮箱存在,则会在SAML断言中,通过 email 属性传递给 WordPress。
First Name	-	暂不支持
Last Name	-	暂不支持
Group/Role	-	暂不支持
-	displayName	如果 IDaaS 中,用户的显示名存在,则会在SAML断言中,通过 displayName 属性传递给 WordPress。

4. 配置登录页 SSO 链接(可选)

通过 miniOrange SAML SSO 插件,可以配置是否在登录页面显示单点登录的链接,您可以在 Redirection & SSO Links 页签进行配置,具体请参考官方文档 https://plugins.miniorange.com/saml-single-sign-on-sso-wordpress-using-custom-idp。

Service Provider Setup Service Provider Metadata Attribute/Role Mapping Redirection & SSO Links Add-Ons

Option 1: Use a Single Sign-On button [®]				
Add a Single Sign-On button on the Wo	rdpress login page			
Customize Single Sign-On But	tton	W		
Shape	Theme	Size of the Button		
Round	Button Color: #17a2b8	Width: 200 - +		
Rounded Edges	Button Text: Login with #IDP#	Height: 50 - +		
Square	Font Color: #ffffff	Curve: 5 - +		
O Long Button with Text	Font Size: 20 - +			

四、尝试 SSO

您已经可以尝试 WordPress SSO。

WordPress 既支持 IDP(IDaaS 门户)发起 SSO,也支持 SP(应用)发起 SSO。

注意:WordPress 支持 **自动创建账户**(Just-in-time Provisioning),单点登录时,若 WordPress 中不存在指定应用账户,则会直接创建,不会拒绝访问。请在 IDaaS 中管 理 WordPress 访问权限。

IDP 发起

请用已授权使用 WordPress 的 IDaaS 账户,登录到 IDaaS 门户页,点击页面上 WordPress 图标,发起 SSO。

IDaaS 应用门户 阿里云 IDaaS	
我的应用	我的应用
我的账户	请点击下方的应用进行单点登录。若希望修改应用内容,请联系管理员。
	理変応用 Q WordPress 大配電応用販户

SP 发起

请在匿名浏览器中,打开 WordPress 登录页,点击 Login with AliyunIDaaS,则会跳转到 IDaaS 进行登录。如果用户尚未登录 IDaaS ,则 IDaaS 会引导用户进行登录 。

Login with AliyunIDaaS				
OR				
用户名或电子邮箱地址				
密码 (1)				
□记住我 登录				

验证通过后,将直接登录到 WordPress 中。

1.7.2.19. Bitbucket miniOrange SAML

本文为您介绍如何在 IDaaS 中配置 Bit bucket miniOrange saml单点登录。

应用简介

Bit bucket

注意: Bit bucket 需要额外插件才能实现 SSO,例如: SAML Single Sign On - SAML SSO Login

本篇文档中 Bit bucket 版本为 6.0.3。在 Bit bucket 中通过 配置请参考文档: https://miniorange.com/atlassian/setup-saml-single-sign-on-sso-for-bit bucket#stepe

操作步骤

一、创建应用

- 1. 登录 IDaaS管理控制台。
- 2. 前往 应用-添加应用-应用市场,搜索到 Bit bucket miniOrange SAML 应用模板。点击 添加应用。

 Bitbucket miniOrange SAN Bitbucket 是一家源代码托管网站, 另 	/L 限时免费 ⑦ 尽用Mercurial和Git作为分布式版本控制系统,同时提供商业计划和免费账户。				
SSO					
漆加应用					
3. 确认应用名称,即可完成	添加。				
二、在 IDaaS 中配置	SSO				
您只需要将 Bit bucket 服务地」	业填写进来,注意结尾不要以"/"结尾。				
1.項马330配直 苗占癸己配罢 已白日	#				
不知道怎么配置? 请参	考对接文档。				
* Bitbucket 服务地址	http:// <your_domain></your_domain>				
	Bitbucket 服务地址, 注意:不能以 "/" 结尾				
* 应用账户	山口203 秋 一 五 单 占 登 录 时	~			
授权范围	全员可访问 ~				
若选择"手动授权",需要在 应用授权 中进行权限分配。					
其他选项保持默认,点击 保存 ● 应用账户:默认使用 IDaaS	[:] 即可完成全部 SSO 配置。 账户名作为应用登录标识。Bit bucket 支持 自动创建账户 ,单点登录时,若 Bit bucket 中不存在指定账户,则会直接创建出来。				
 若希望灵活配置,请参考 单 	点登录通用说明 进行配置。				
● 授权范围:默认全员可用。	若希望指定可访问应用的 IDaaS 账户,请参考 单点登录通用说明 进行配置。				
2. 获取 Bit bucket 配置信息					
配置页下方的 应用配置信息 。	中,包含了 Bit bucket 完成配置所需要的参数。				
应用配置信息					
IdP 元数据	https://esfz6rcn.aliyunidaas.com/api/v2/app_mi6f4xge4rkpysus62l4waujha/saml2/meta 回 业下载 IDaaS 作为身份服务提供商的元数据,你需要复制元数据的URL地址,并将其填写到 Bitbucket 的 SAML 配置中。				
IdP 唯一标识	https://esfz6rcn.aliyunidaas.com/api/v2/app_mi6f4xge4rkpysus62l4waujha/saml2/meta 回 IDaaS 作为身份服务提供商的唯一标识,同时也是 SAML 响应和断言的签发者。				
IdP 发起 SSO 地址	https://esfz6rcn.aliyunidaas.com/login/app/app_mi6f4xge4rkpysus62l4waujha/saml2/sso				
SLO 地址	暂不支持 IDaaS 提供的用于 Bitbucket 发起单点登出的地址。				
公钥证书	BEGIN CERTIFICATE MIIEFJCCAv6gAwIBAgITAJXJL7c+jDpiYM+czsTlkbkOaDANBgkqhkiG9w0BAQsF ADCBkjEnMCUGA1UEAwweYXBwX21pNmY0eGdlNHJrcHlzdXM2Mmw0d2F1amhhMSk w				
	下载或复制证书,并导入或粘贴到应用中。				
	□ 复制证书内容 业下载证书 .cer 文件				

从中您需要获取 ldP 元数据,ldP 唯一标识ldP, 发起 SSO 地址和公钥证书四个参数。

三、Bitbucket 中配置 SSO

1. 安装插件

Bit bucket 插件市场中有多款用于实现单点登录的插件,点击 **设置按钮-Manage apps**,搜索 "SAML Single Sign On",在搜索列表中,选择 "SAML Single Sign On - SAML SSO Login"插件(该插件由 miniOrange 提供),点击"立即安装"。

插件安装成功之后,在 User-installed apps 中可找到 SAML Single Sign On for Bitbucket。

Bitbucket Your we	ork Projects Repositories 🗸	Q Searc	ch for code, commits or repo
Administration			
Overview AccouNTS Users Groups Global permissions Authentication	Manage apps You can install, update, enable, and disable apps here. Find new apps. Filter visible apps	î Upload app 🕂 Build	a new app
SAML Single Sign On User Sync Authentication methods Avatars Audit log User Directories	Image: SAML Single Sign On for Bitbucket Image: SAML Single Sign On for Bitbucket Image: SSO for Atlassian Data Center Image: SSO for Atlassian Data Center Audit log Bitbucket update check Settings Enter safe mode The Universal Plugin Manager (v4.2.10) by Atlassian	IAL EXPIRING	Update Update
SYSTEM			

2. 配置 550

启用插件之后,Bitbucket 将在左侧导航栏中增加菜单 SAML Single Sign On,点击该菜单,即可进入编辑页面,如下图所示:

Bitbucket	Your work	Projects	Repositories 💙

Administration

Overview	SAML Single	Sign On Configuration 🗜	
ACCOUNTS Users	Identity Providers	IDaaS (SAML) abc (SAML) Add new IdP+	
Groups	Redirection	Settings for IdP (SAML)	
Global permissions Authentication	IdP Selection	Name *	
SAML Single Sign On	Advanced Page Templates System & Support	IDaaS Choose a unique name. This name is shown on the IdP selection page by default. Description	
User Sync			
Authentication methods			
Avatars		EIAM单点登录	
Audit log		Description for this IdP. This value is shown on the IdP selection page by default.	
User Directories		Wainhe *	
SYSTEM			
Server settings			
Database		IdPs are sorted using this property. The default IdP is the one with the lowest weight.	
Storage			
Application Navigator			
Application Links		CAMI IdD Matadata Sattings	
在 Identity Providers 标签内,点击 Ac	dd new ldp,如下图所示:		

Bitbucket
 Your work
 Projects
 Repositories

Administration

Overview	SAML Single Sign On Configuration		
ACCOUNTS			
Users	Identity Providers	IDaaS (SAML) abc (SAML) Add new IdP+	
Groups	Redirection	Settings for IdP (SAML)	
Global permissions	IdP Selection		
Authentication	Service Provider	Name *	
SAML Single Sign On	Advanced	IDaaS	
User Sync	Page Templates	Choose a unique name. This name is shown on the IdP selection page by default.	
Authentication methods	System & Support	Description	
Avatars		EIAM单点登录	
Audit log		Description for this IdP. This value is shown on the IdP selection have by default	
User Directories		Description for this full. This value is shown on the full selection page by default.	
SYSTEM		Weight *	
Server settings		10	
Database		IdPs are sorted using this property. The default IdP is the one with the lowest weight.	
Storage			
Application Navigator			
Application Links		CAMI IdD Matadata Sattings	

点击 Add new Idp 图标后,弹框,选择您的身份提供方 Other Idp。

	Choose Your Identity Provider	
	To help you add your IdP, there are some templates that you can use.	
	Select your Identity Provider *	_
	Select 🗸	,
	AuthAnvil	^
	OneLogin	Close Back Next \rightarrow
	Ping One	
Ad	Centrify	
Pag	Duo Access Gateway	
Sys	Salesforce	
	WSO2	
	OTHER	
	Other IdP	
	· · · · · · · · · · · · · · · · · · ·	·

选择完身份提供方后,填写Name,如下图,然后点击 Next 。

Choose Your Identity Provider

To help you add your IdP, there are some templates that you can use.

Select your Identity Provider *					
Other IdP	~				
Change the Authorities Durth rel *					
choose the Authentication Protocol					
SAML2	*				
For the differences and guidance on choosing the protocol, please see our KB article	here. If you are unsure, go with SAML2.				
Name *					
IDaaS-EIAM					
Choose a unique name. This name is shown on the IdP selection page by default.					
Description					
Description for this IdP. This value is shown on the IdP selection page by default.					
		Close	Back	Next →	

找到界面中的"SAML ldp Metadata Settings",可以通过"上传IDP元数据"和"手动填写IDP元数据"两种方式,配置ldP信息。

● 上传IDP元数据

下载列表,选择 I have ametadata URL 页签, "Metadata URL"填写 Idp元数据 地址。

SAML IdP Metadata Settings

Choose an option to import metadata I have a metadata URL	~	Þ	
Metadata URL			

Accept all HTTPS certificates including self-signed certificates

Reload metadata automatically after a day

Import Metadata

字段	IDaaS 中字段名称	说明
Name		输入一个名字,例如: AliyunIDaaS
Metadata URL	ldP 元数据 ldP Metadata	从 IDaaS 单点登录配置页 应用配置信息 中获取,对应" IdP 元数据",您可以将元数据下载到本地之后,然后在当前 页面进行上传。

导入完成后可看到如下图,修改Login Binding 方式为 REDIRECT。

Basic IdP Se	ttin	gs						
IdP Entity ID / Issuer *								
https://esfz6rcn.ali	yunida	aas.com/api/v2/app_mi6f4xge4rkpysus62l4waujha/sarr						
Unique identifier used	Unique identifier used in SAML messages. The message's value is matched against this value.							
Login Binding *		IdP REDIRECT Binding URL *						
REDIRECT	~	https://miii infinimaliyunidaas.com/login/app/app_mi6f4xge4rkpysus62l4waujha/saml2/sso						
		SAML requests are sent to this URL on the identity provider using the HTTP-REDIRECT binding.						
Logout Binding		•						
DISABLE	~	Note Single Logout is turned off for this IdP - complete the configuration if you wish to enable it.						
SAML binding used for logout		- учини на учи ни на						

Security Settings

Token Signing Certificates



● 手动填写IDP元数据

将 IDaaS 中获取到的信息填写进入表格中。参数对照如下:

Basic IdP Se	etting	gs			
IdP Entity ID / Issuer					
https://esfz6rcn.al	iyunida	as.com/api/v2/app_mi6f4xge4rkpysus62l4waujha/sarr			
Unique identifier used in SAML messages. The message's value is matched against this value.					
Login Binding *		IdP REDIRECT Binding URL •			
REDIRECT	~	https://a aliyunidaas.com/login/app/app_mi6f4xge4rkpysus62l4waujha/saml2/sso			
		SAML requests are sent to this URL on the identity provider using the HTTP-REDIRECT binding.			
Logout Binding		0 m/			
DISABLE	~	Note Single Logout is turned off for this IdP - complete the configuration if you wish to enable it.			
SAML binding used fo logout	r	, , , , , , , , , , , , , , , , , , ,			

Security Settings

Token Signing Certificates

Certificate *

MIIEF;CCAv6gAwlBAgITAJXJ17c+jDpjYH+czsTlkbkDaDANBgkqhkiG9w0BAQsFADCBkjEnKUGA1UEAwweYXBwX21phmY0a6d1NH3rcH1zdXH2 ^ Mmw0d2F1amhhMSkwJwYDUQQLDCBpZ6Fhc19weXhjUXR2dTMzYm30M243cWJYH3D1NnhtdTEcMBoGA1UECgwTQWxpYmFiYSBDbG91ZCB3RGFhUzER MA8GA1UECAwlMmllamlhDmcxCcAJBgWNBAYTAkHOM84XDTJyWDWyKE2DHDAwHF0xDTMyWDWyKE2DHDAwHF0xgZXJ32A1BgWNBAMHMmkrC9FaTZm MHnZTRya385c32VHJ33HHdhWhpOYTEPKCGALUECwmgaRWRTYWAF(H14Y2W04nLJ%Z12HDNXHFpcjHyZTZAbXUHABBgWNBAMH6FsxBJYHreg QzxddwQ52HNYVMxETAPBgWNBAKCFD02WppYMSnWq3ucQYDVQQEwJDTjCCAS1M0QY3KcZhVCM4QEBQADggEPADCCAQoCggEBAMdEwcB1PS Hut08PLPDLkpnYOJNRHsqGGjzpK91edE21cNkrvhKfqUf9SQL1mfMd7WHuZH0Bg5n1CczcN3b3Rf/c9Za6go3RpC

字段	IDaaS 中字段名称	说明
Identity Provider Name		输入一个名字,例如: AliyunlDaaS,这个名字将在 WordPress 登录页中显示。
ldP Entity ID / Issuer	IdP 唯一标识 IdP Entity ID	从 IDaaS SSO 配置页 应用配置信息 中获取,对应" IdP 唯 一标识"
Login Binding	SP发起请求方式	固定值:REDIRECT
Idp REDIRECT Binding URL	ldP SSO 地址 IdP Sign-in URL	从 IDaaS SSO 配置页 应用配置信息 中获取,对应" IdP SSO 地址"
<u>Certificate</u>	公钥证书 Certificate	从 IDaaS SSO 配置页 应用配置信息 中获取,对应" IdP 公 钥证书"

同时关闭 "Sign Authentication Requests"

Security Settings

Token Signing Certificates

Certificate *



选中 Service Provider,修改Entity Id为Bitbucket的域名

SAML Single	Sign On Configuration 🛛 🗜		Shc	w IdP Infor
Identity Providers Redirection IdP Selection Service Provider Advanced	Entity Id *	Þ	Reset to Default	
Page Templates System & Support	Signing and Encryption			

修改Protocal Binding方式为 POST。

Request settings

Nameld Format in Request				
NONE	~			
Nameld format to be added to the SAML Re	quest. Select NONE to not include a Name	d format.		
RelayState parameter name *				
RelayState	Reset to Defa	ult		
The URL originally requested by the user is t The value from this parameter should be ret Some IdPs are a bit quirky here and expect a	ransferred to the IdP in a parameter called urned by the IdP as it was sent. another parameter name, e.g. TARGET.	RelayState.		
Protocol Binding				
POST	~			
The SAML protocol binding to be used for the	ne SAML response. Set to NONE to exclude	the ProtocolBinding tag from the	SAML request. This may be necessar	y for some quirky IdPs
Use Base URL from Request				
Use the base URL from the current request in	n the SAML request. This makes sure SSO w	orks, even if the system is accesse	d by using another URL than the bas	e URL.
AuthnContextComparisonType				
none 🗸				
3. 配置属性映射				
若只进行单点登录,则在 Find user by B	litbucket attribute,选择对应的映	射规则即可。		
Attribute Mapping				
Find user by this Bitbucket attribute				
Username	~			
How should SAML SSO search in Bitbucket fo	or the user? By default, SAML SSO searches f	or the username.		
Attribute as received from IdP	Bitbucket Attribute	Transformations	Actions	
Use Name ID	Username		Edit 🖉 Delete i	Ť
Match attributes received from IdP with the o	corresponding application attributes in Bitbu	cket.		
4. 单点登录时同步配置(可选)			
选择 User Update Method 为 Update fr	om SAML-Attribute(Just-in-Time	Provisioning),如下图:		
User Creation and	Update			
Reactivate inactive users d	uring login			

Users that exist in a directory and are marked as inactive will be re-enabled after a successful SAML authentication.

ι	Jser Update Method		
	Update from SAML-Attributes (Just-in-Time Provisioning)	~	Þ
1			

Configure if and how users will be created and updated during login.

开启"Create New Users"

建议关闭 Update users not created by this app(关闭后,同步时修改只修改单点登录同步过来的用户)

User Creation and Update from SAML Attributes

Create New Users

Directory for the creation of new users

Bitbucket Internal Directory

Update users not created by this app

Update existing users with data from the SAML attributes above. If this is disabled, only users created by this app are updated during Single Sign On.

必须选择 组,同步后,账户会同步到对应的组下面。若不填此项,则同步过来的账户单点登录时无权限

Group Setting

Always add users to these groups

stash-users ×

Users are always added to these groups during SSO, in addition to the group names from the SAML response (if mapped above).

Create groups if they do not exist

Create groups from the SAML response if they don't exist yet. If not enabled, users will only be assigned to already existing groups!

Remove from Groups

Remove memberships that don't match the group list above or the values of the groups attribute of the SAML response. If enabled, **group memberships must be managed on the IdP**. Manual additions or removals will otherwise be overridden during SSO. The setting will only apply to users created by this app, **never** to the group memberships of **existing users and administrators**.

© ~

属性配置。账户同步时,必须有配置FullName 和Eamil的属性映射。如下图:

Attribute Mapping	
Find user by this Bitbucket attribute	
Username	*
How should SAML SSO search in Bitbucket for the	user? By default, SAML SSO searches for the username

Addibite as received non dr Didected Addibite Instrumento in addibite Edit // Delete Use Name ID Username Edit // Clear & displayName Full Name Edit // Clear & email E-Mail Address Edit // Clear &	^	ttribute as received fr	om IdP	Rithucket Attribute	Transformations	Actions			
displayNameFull NameEdit 🖉Clear 🔇emailE-Mail AddressEdit 🖉Clear 🔇		lse Name ID	onniar	Username	Tansiomations	Edit	0	Delete	T
email E-Mail Address Edit 🖉 Clear 😒	d	isplayName		Full Name		Edit	0	Clear	×
	P	mail		E-Mail Address		Edit	0	Clear	8
		less and				Luit	~ ~	Class	•

Match attributes received from IdP with the corresponding application attributes in Bitbucket.

目前支持的属性映射如下图:

Bitbucket 属性名	IDaaS SAML 断言中的属性名	说明
Username	username	如果 IDaaS 中,用户的用户名。若单点登录时,Use Name ID对应的不是Usename,则需要单独配置此映射

Add New Attribute Mapping 💙

Full Name	displayName	如果 IDaa5 中,用户的显示名存在,则会在SAML断言中,通 过 displayName 属性传递给 Bitbucket。
E-Mail Address	email	如果 IDaa5 中,用户的邮箱存在,则会在SAML断言中,通过 email 属性传递给 Bitbucket。

四、尝试 SSO

您已经可以尝试 Bitbucket SSO。

Bit bucket 既支持 IDP(IDaaS 门户) 发起 SSO,也支持 SP(应用) 发起 SSO。

注意:Bitbucket 支持 **自动创建账户**,单点登录时,若 Bitbucket 配置用户同步,则Bitbucket中不存在账户则会直接创建,不会拒绝访问。请在 IDaaS 中管理 Bitbucket 访 问权限。

IDP 发起

请用已授权使用 Bit bucket 的 IDaaS 账户,登录到 IDaaS 门户页,点击页面上 Bit bucket 图标,发起 SSO。

IDaaS 应用门户 阿里云 IDaaS	
我的应用	我的应用
我的账户	请点击下方的应用进行单点登录。若希望修改应用内容,请联系管理员。
	授索应用 Q
	Bitbucket miniOr ange SAML
	く 未配置应用账户

SP 发起

请在匿名浏览器中,打开 Bit bucket 登录页,点击 Login again with Single Sign On,则会跳转到 IDaaS 进行登录。如果用户尚未登录 IDaaS ,则 IDaaS 会引导用户进行 登录 。



验证通过后,将直接登录到 Bit bucket 中。

1.7.2.20. Zabbix SSO 本文为您介绍如何在 IDaaS 中配置 Zabbix 单点登录。
 应用简介

Zabbix 是一个基于 WEB 界面的提供分布式系统监视以及网络监视功能的企业级的开源解决方案。能监视各种网络参数,保证服务器系统的安全运营。

⑦ 说明

注意: 在 Zabbix 5.0+ 版本中,系统原生提供 SAML 2.0 的 SSO 支持。若您当前使用版本低于 5.0,可能需要额外插件才能实现 SSO,例如 Zabbix - MiniOrange, 配置 方式也会不同。本篇文档中 Zabbix 版本为 5.4。Zabbix 原生SAML 配置请参考文档: https://www.zabbix.com/document.ation/current/en/manual/web_interf.ace/frontend_sections/administration/authentication

操作步骤

一、配置 IDaaS 应用

请管理员前往【应用】【应用市场】,搜索到"Zabbix"应用模板,点击"添加应用"按钮,确认应用名后,即可完成应用创建。

Z	Zabbix	限时免费 ⑦
Zabbi 网络餐	x 是一个墓于 WEB 界面的提供分布式系统监视以及网络监视功能的企业级的开源解决方案。 参数,保证服务器系统的安全运营。	能监视各种
SSC		

创建应用成功后,会自动来到 SSO 单点登录配置页。

配置 SSO

您只需要将 Zabbix 服务地址填写进来,注意结尾不要以"/"结尾。

单点登录配置 已启	通 💶	
不知道怎么配置? 请教	参考 对接文档。	
* Zabbix 服务地址	https://zabbix.example.com Zabbix 服务地址URL,请注意:最后不要以 /* 结尾。	
* 应用账户	IDaaS 账户名 单点登录时,将进中项作为账户硕识,传递给业务系统。	\sim
援权范围	金质可访问 图选择"手动线灯",需要在 应用等权 中进行权限分配。	\sim

其他选项保持默认,点击【保存】即可完成全部 SSO 配置。

? 说明

```
应用账户:默认使用 IDaaS 账户名作为应用登录标识。Zabbix 支持【自动创建账户】,单点登录时,若 Zabbix 中不存在指定账户,则会直接创建出来。 若希望灵活配
置,请参考 单点配置通用说明 - 应用账户 进行配置。 授权范围:默认全员可用。若希望指定可访问应用的 IDaaS 账户,请参考 单点配置通用说明 - 应用账户 进行配
置。
```

获取 Zabbix 配置信息

配置页下方的【应用配置信息】中,包含了 Zabbix 完成配置所需要的参数。

应用配置信息

IdP 元数据 IdP Metadata	https://ijlaliyunidaas.com/api/v2/app_mixpu3hqp4fpka3e67lqicb2ly/saml2/meta 👩 👱 下載 若应用支持 metadata 武置信息上传/应取,可以行省大量武置步骤。等在应用 SSO 配置中寻找是否有 metadata 上传能力,
IdP 唯一标识 IdP Entity ID	https://i-jallyunidaas.com/api/v2/app_mixpu3hqp4fpka3e67lqicb2ly/saml2/meta j IDaaS 在应用中的标识,需要将值编写在应用单点登录起置中。
IdP SSO 地址 IdP Sign-in URL	https://ialiyunidaas.com/login/app/app_mixpu3hop4pka3e57djcb2ly/saml2/sso ④ SAML 协议支持 SP 发起单点登录,可能需要填写此地址在应用配置中,由 IDaas 提供,可以直接访问该地址,进行应用登录。
单点退出地址 SLO URL	智不支持 SAML协议支持单点退出,可能需要填写此地址在应用配置中。由 IDaaS 提供。
公钥证书 Certificate	BEGIN CERTIFICATE MIETFCCAr2gAwiBagSUNBpiCrQL/MKEXHctt2XrrgDMA0GC5qGSlibJ0QEBCwUA MIGSMSW20PUVQQDDB5hcHBWW4cHU2aHfwNG2wa2E2TT3bH5qr21ybHicxTAn
	下载或复制证书,并导入或粘贴到应用中。
	□复制证书内容 业下载证书 .cer 文件

从中您需要获取 IdP 唯一标识 IdP SSO 地址 和 公钥证书 三个参数。其中 公钥证书 需要您下载到本地。

二、Zabbix 中配置 SSO

1. 配置 SSO

请在新的浏览器标签中使用管理员账号登录 Zabbix 后台。

通过【Administration】【Authentication】【SAML Settings】, 来到 SAML 配置页。

Z	ABBIX		Authentication			
Zabt	oix docker	Q	Authentication HTTP:	settings LDAP se	ettings SAML settings •	
0	Monitoring	3	Enable SAI	ML authentication	✓	
				* IdP entity ID	https://wcj; * • • .aliyunidaas.com/api/v2/app_mixpu3hqp4fpka3e67lqjcb2ly/saml2/m	
=	Inventory		- :	SSO service URL	https://mmmailyunidaas.com/login/app/app_mixpu3hqp4fpka3e67lqjcb2ly/saml2	
	Reports			SLO service URL		
٩	Configurat	tion	• U:	sername attribute	username	
	Administra	ation		* SP entity ID	http://zabbix.example.com	
	General		s	P name ID format	urn:oasis:names:tc:SAML:2.0:nameid-format:transient	
	Proxies			Sign	✓ Messages	
	Authenticati	ion			✓ Assertions	
	User groups	5			AuthN requests	
	User roles				Logout responses	
	Users			Encrypt	Name ID	
	Media types	5			Assertions	
	Scripts		Ca	ase sensitive login		
	Queue			l	Update	

将 IDaaS 中获取到的信息填写进入表格中。参数对照如下:

字段	IDaaS 中字段名称	说明
Enable saml authentication		启用。
<u>IdP entity ID</u>	ldP 唯一标识 ldP Entity ID	从 IDaaS SSO 配置页【应用配置信息】中获取。
SSO service URL	ldP SSO 地址 ldP Sign-in URL	从 IDaaS SSO 配置页【应用配置信息】中获取。
<u>Username attribute</u>		填写 username 即可。
<u>SP entity ID</u>	-	固定填写为 Zabbix 服务地址。

将以上配置保存,将立刻生效。

2. 配置证书

您需要将 IDaaS 中下载的证书放置在 Zabbix 部署环境中的指定位置,Zabbix 才能用其解析 SAML SSO 请求。

请检查 zabbix.conf.php 文件中 \$SS0['IDP_CERT'] 配置。若未手动指定,其默认值应为 ui/conf/certs/idp.crt 。

请您做两件事:

- 1. <u>文件改名</u>。将从 IDaaS 下载的 .cer 证书文件,改名为 idp.crt 文件。后缀请直接修改即可。
- 2. <u>文件上传</u>。将 idp.crt 上传到上述指定位置。
- 重启 Zabbix 服务后,即可使用 SSO。

三、尝试 SSO

您已经可以尝试 Zabbix SSO。

Zabbix 既支持 IDP(IDaaS 门户)发起 SSO,也支持 SP(应用)发起 SSO。

注意:Zabbix 支持【自动创建账户】(Just-in-time Provisioning),单点登录时,若 Zabbix 中不存在指定应用账户,则会直接创建,不会拒绝访问。请在 IDaaS 中管理 Zabbix 访问权限。

IDP 发起

请用已授权使用 Zabbix 的 IDaaS 账户,登录到 IDaaS 门户页,点击页面上 Zabbix 图标,发起 SSO。

IDaaS 门户页 企业名称 A

我的应用	我的应用	
我的账户	● 请点击下方的应用进行单点登录。若对应用访问情况有疑议,请联系管理员。	×
	您当前未填写手机号和邮箱,部分功能无法使用。请前往我的账户填写。	×
	搜索应用 Zabbix testuser	

SP 发起

请在匿名浏览器中,打开 Zabbix 登录页,点击【Sign in with Single Sign-On(SAML)】,则会跳转到 IDaaS 进行登录。如果用户尚未登录 IDaaS ,则 IDaaS 会引导用户进 行登录 。

	ZABBIX
Use	rname
Pas	sword
<u> </u>	Remember me for 30 days
	Sign in
	Sign in with Single Sign-On (SAML)
	Help · Support

验证通过后,将直接登录到 Zabbix 中。

1.7.2.21. GitLab SSO By SAML

本文为您介绍如何在 IDaaS 中通过 SAML 协议,配置 Git lab 单点登录。

应用简介

Git Lab 是一个用于仓库管理系统的开源项目,使用Git作为代码管理工具,并在此基础上搭建起来的Web服务。

? 说明

GitLab 支持多种 SSO 协议,本文档介绍如何通过 SAML协议对接 GitLab。GitLab SAML官网文档: https://docs.gitlab.com/ee/integration/saml.html

操作步骤

一、配置 IDaaS 应用

请管理员前往【应用】【应用市场】,搜索到 GitLab 应用模板。确认应用名后,即可完成添加流程。

😝 GitLab SAML	限时免费 ⑦
GitLab 是一个用于仓库管理系统的开源项目,使用Git作为代码管理工具,并在此基础上搭建起; 务。	₩â9Web服
sso	
添加应用	

创建应用成功后,会自动来到 SSO 单点登录配置页。

配置 SSO

您只需要将 Git Lab 的服务地址填写进来,注意服务地址不要以"/"结尾

单点登录配置 已启用		
不知道怎么配置? 请参考	●对接文档。	
• GitLab 服务地址	http://gitab.example.com	
* 应用账户	URLID #1997ABL/URL_119112.851、HUNI-Y-1894、/ HENRL IDasS 账户名	\sim
410 4 17 745 980	单点型录时,将选中语作为账户标识,传递给业务系统。 	~
技权沿面	エルマシッド 若語修手动接収",需要在 应用接収 中进行权限分配。	

其他选项保持默认,点击【保存】即可完成全部 SSO 配置。

? 说明

应用账户:默认使用 IDaaS 账户名作为应用登录标识。GitLab 支持【自动创建账户】,单点登录时,若 GitLab 中不存在指定账户,则会直接创建出来。若希望灵活配置,请参考 单点配置通用说明 - 应用账户 进行配置。 授权范围:默认全员可用。若希望指定可访问应用的 IDaaS 账户,请参考 单点配置通用说明 - 应用账户 进行配置。

配置页面下方,包含了一系列 Git Lab 完成配置所需要的参数。

应用配置信息

IdP 元数据	https://:。ここのallyunidaas.com/api/v2/app_mivpoqqmz7zrsixcmlyxa25me4/saml2/meta 🧭 👱 下載		
IdP Metadata	若应用支持 metadata 配置信息上传/检察,可以符管大量配置步骤。 寄在应用 SSO 配置中符线是否有 metadata 上传能力。		
IdP 唯一标识	http://:aliyunidaas.com/api/V2/app_mivpoqqm27zrskxcmlyxa25me4/saml2/meta の		
IdP Entity ID	IDaaS 在应用中的标识。需要将值填写在应用单点包录配置中。		
IdP SSO 地址	https://www.allyunidaas.com/login/app/app_mlvpoqqmz7zrstxcmlyxa25me4/saml2/sso ⑦		
IdP Sign-in URL	SAML 协议支持 SP 发起希点登录,可能需要項写此地址在应用配置中,由 IDaaS 提供,可以直接访问该地址,进行应用登录。		
单点退出地址	智不支持		
SLO URL	SAML协议支持单点退出,可能需要填写此地址在应用配置中。由 iDaaS 提供。		
公钥证书 Certificate	BEGIN CERTIFICATE MIETCCAr2gAvir8Ag050x56R84bwQTJuvd2CZR/m63UUMA0GCSqGSIb3DQEBCwUA MIGSMSw3/QFUVQQDDB5nHeBRWIBzCd9xxV15N3byr2b4721seXihmMjVIzTCuXTAn		
	下载或复制证书,并导入或粘贴到应用中。		
	□复制证书内容 → 上下载证书 .cer 文件		

二、配置 Gitlab

根据 Git lab 官网文档,您需要在部署环境中编辑 git lab 配置文件。

若您使用 Omnibus 安装 Gitlab,请使用命令: sudo editor /etc/gitlab/gitlab.rb

#若您使用独立安装 Gitlab,请参考命令:

cd /home/git/gitlab

sudo -u git -H editor config/gitlab.yml

将如下信息补充进配置文件(参数按照 onmibus 安装方式提供。独立安装的参数与其一致,但格式不同,详情参考官网):

gitlab_rails['omniauth_enabled'] = true
gitlab_rails['omniauth_allow_single_sign_on'] = ['saml']
gitlab_rails['omniauth_block_auto_created_users'] = false
gitlab_rails['omniauth_auto_link_saml_user'] = true
gitlab_rails['omniauth_providers']=[
{
name: 'saml',
args: {
name: 'saml',
assertion_consumer_service_url:'http://gitlab.example.com/users/auth/saml/callback',
<pre>issuer:'http://gitlab.example.com/users/auth/saml',</pre>
idp_cert_fingerprint:'23:f8:77:03:fc:69:4c:da:ac:7e:4a:42:5a:87:5a:b3:ad:a8:d9:df',
idp_sso_target_url:'https://example.aliyunidaas.com/login/app/app_mivpoqqmz7zrs1xcmlyxa25me4/saml2/sso',
<pre>name_identifier_format:'urn:oasis:names:tc:SAML:2.0:nameid-format:persistent',</pre>
attribute_statements: {
nickname: ['username'],
},
},
label:'EIAM2.0'
}

如上参数中大部分无需调整, 仅有几项配置需要修改:

参数名	说明	示例
args.assertion_consumer_service_url	填写 GitLab 的断言消费地址,一般是 GitLab 服务地址后加 /users/auth/saml/callback	http://gitlab.example.com/users/auth/saml/callback

<u>args.</u> issuer	填写 GitLab 的身份标识,一般是 GitLab 服务地址后加 /users/auth/saml	http://gitlab.example.com/users/auth/saml
<u>args.</u> idp_sso_target_url	IdP SSO 地址,从 IDaaS 获得	https://example.aliyunidaas.com/login/app/app_mivp oqqmz7zrslxcmlyxa25me4/saml2/sso
args.idp_cert_fingerprint	ldp 公钥证书指纹。请您下载证书后,通过检查证书属性,获 取证书 SHA1 指纹。可能获取到的指纹信息并未按照冒号: 区隔,您可能需要手动处理。	23:f8:77:03:fc:69:4c:da:ac:7e:4a:42:5a:87:5a:b3:ad: a8:d9:df

配置完成后,使用命令重启 Gitlab。

若您使用 Omnibus 安装 Gitlab,请使用命令: sudo gitlab-ctl restart

若您使用独立安装 Gitlab, 请参考命令:
 # 运行 systemd 的系统
 sudo systemctl restart gitlab.target

允许 SysV init **的系统**

sudo service gitlab restart

重启后,在 Git lab 登录页下方,应出现【使用阿里云 IDaaS 账户登录】按钮。

配置完成。

三、尝试 SSO

您已经可以尝试 Git Lab SSO。

本文中 Git Lab 采用 SAML 协议, 既支持 IdP 发起(即从阿里云 IDaaS 发起) SSO, 也支持 SP 发起(即从 Git Lab 发起) SSO 流程。

IdP 发起

请用已授权使用 Git Lab 的 IDaaS 账户,登录到 IDaaS 门户页,点击页面上 Git Lab 图标,发起 SSO。



SP 发起

请在匿名浏览器中,打开 Gitlab 登录页,点击【阿里云 IDaaS】,则会跳转到 IDaaS 进行登录。如果用户尚未登录 IDaaS ,则 IDaaS 会引导用户进行登录 。

登录	注册
用户名或邮箱	
密码	
□记住我	忘记密码?
	录

尚未收到确认邮件? 重新发送确认邮件。

通过 阿里云 IDaaS

IDaaS 验证用户身份通过后,将直接登录到 Git Lab 中。

1.7.2.22. Redash SSO

本文为您介绍如何在 IDaaS 中配置 Redash 单点登录。

应用简介

Redash 是一款开源的 BI 工具,提供了基于 WEB 的数据库查询和数据可视化功能。

? 说明

Redash 支持通过 SAML 协议,实现单点登录,请参考官方文档: https://redash.io/help/user-guide/users/authentication-options#SAML-2-0

一、创建应用

请管理员前往【应用】【应用市场】, 搜索到"Redash"应用模板。点击"添加应用"按钮,确认应用名后,即可完成应用创建。



创建应用成功后,会自动来到 SSO 单点登录配置页。

二、在 IDaaS 中配置 SSO

将【Redash服务地址】填写到表单中。注意:Redash服务地址不可以"/"结尾。

单点登录配置	
不知道怎么配置?	请参考对投文档。
* Redash 服务地址	https:// <your_domain> Redash 服务地址, 注意: 不能以 "/" 结尾。</your_domain>
* 组织机构	default 组织机构ID,如果您在安装 Redash 时没有设置,那么默认值是:default 。
* 应用账户 <	IDaaS 邮箱 《 》 单点登录时,将透中项作为账户标识,传递给业务系统。
授权范围	手动授权

为了便于测试,【授权范围】可暂时选择【全员可访问】。

其他选项保持默认,点击保存即可完成 IDaaS 侧 全部 SSO 配置。

? 说明

提示 应用账户:默认使用 IDaaS 账户名作为应用登录标识。应用中配置IDaaS邮箱作为账户标识,才能完成 SSO。若希望灵活配置,请参考 单点配置通用说明 - 应用账 户 进行配置。 授权范围:若希望指定可访问应用的 IDaaS 账户,请参考 单点配置通用说明 - 应用账户 进行配置。

在页面下方的【应用配置信息】中,即包含了Redash完成 SSO 配置所需要的参数。

-	-	-		6.00	-
- h1/		m-	- 282	i =	
119		ы.	_		

IdP 元数据	https://。デザー=_aliyunidass.com/api/v2/app_mi56ezpm32ofzwka7wp5665wu/saml2/meta の 上下載 IDaaS 作为身份服务提供简的元政组,你需要接触元政组的URL地址,并将其填写到 Redash 的 SAML 配置中。
ldP 唯一标识	https://wj-ji === aliyunidass.com/api/v2/app_mi56ezpm32ofzwka7wp5665wu/saml2/meta ① IDaaS 作为身份最终提供简的唯一标识,同时也是 SAML 喻应和解言的悠波者。
IdP 发起 SSO 地址	https://aliyunidass.com/login/Japp/app_mi56ezpm32ofzrwka7wp56s5wu/sami2/sso 個 IDaaS 提供的用于 Redash 发起她点意思的地址,用户也可以直接的问题地址,发起 Redash SSO。
SLO 地址	智不支持 IDaaS 提供的用于 Redash 发起单点密始的地址。
公明证书	BGIN CERTIFICATE MIEFJCCA-VGAvilGAarJACDexSFVBdr7KW64a0aemmv98DANBgkqhbiG9w08AQsF ADCBigFMACUGA1UEAwwYBWX21pMT2en8BMEJxZnpv22thN3dwNT2zHX21MStw
	下载或援制正书,并导入或粘战到应用中。
	♂ 复制证书内容 业下载证书 .cer 文件

三、配置 Redash

1.

1.前往单点登录设置 使用管理员账号,登录 Redash ,在右上角【Settings】按钮,并选择 Settings 页签,打开如下界面:					
Dashboards 🗸 Queries 🗸 Alert	s Create 🗸		Search queries	۹ 🕜	😫 📄 admin 🗸
	Settings				
	Data Sources Users Groups Alert Destinations	Query Snippets Account			
		General			
		Date Format			
		DD/MM/YY V			
		Time Format			
		HH:mm V			
		Feature Flags			
		Enable experimental multiple owners support			
		Email query owners when scheduled queries fail			
		Enable multi-byte (Chinese, Japanese, and Korean) search for query names and descriptions (slower)			
		Anonymous Usage Data Sharing 😯			
		Help Redash improve by automatically sending anonymous usage data			
		Authentication 🛛			
在 Authentication 区域,勾	选【SAML Enabled】,将展开如下配置	鼠界面:			

SAML	
SAML Metadata URL	
SAML Entity ID	
SAML NameID Format	
Save	

2. 进行 SAML 配置。

将 IDaaS 【应用配置信息】中的参数全部填写到配置表单中。

|--|

SAML Metadata URL	IdP 元数据	从 IDaaS SSO 配置页【应用配置信息】中获取。 Redash 将从该元数据中解析出SSO地址发送 SAML Request 请求,发起单点登录请求。
SAML Entity ID	Redash服务地址	Redash服务地址。
SAML NameID Format	固定值	填写:urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress 。

参考下图配置示例:



四、尝试 SSO

您已经可以尝试 Redash SSO。

IDP 发起

请用已授权使用 Redash 的 IDaaS 邮箱账户,登录到 IDaaS 门户页,点击页面上 Redash 图标,发起 SSO,检查配置结果。

ViDaaS 应用门户 _{阿里云 IDaaS}	
我的应用	我的应用
我的账户	请点击下方的应用进行单点登录。若希望修改应用内容,请联系管理员。
	変 定 日
SP 发起	

请在匿名浏览器中,打开 Redash 登录页,点击【SAML Login】按钮,则会跳转到 IDaaS 进行登录。如果用户尚未登录 IDaaS ,则 IDaaS 会引导用户进行登录 。

Login to Redash SAML Login Email Password Login
Login to Redash SAML Login Email Basseord Log In
SAML Login Email Password Log In
Email Password Log In
Password Log in
Login
Log In

lDaaS 认证用户通过后,将直接登录到 Redash 中。

1.7.2.23. Argo CD SSO

本文为您介绍如何在 IDaaS 中配置 Argo CD 单点登录。

应用简介

Argo CD是用于Kubernetes的声明性GitOps连续交付工具。

一、创建应用

请管理员前往【应用】【应用市场】, 搜索到"Argo CD"应用模板。点击"添加应用"按钮,确认应用名后,即可完成应用创建。

AIGO CD		限时免费 ②		
Argo CD 是用于 Kubern Git 仓库作为定义所需应 的应用程序状态,应用程	etes 的声明性 GitOps 持续交付工具,遵循 用程序状态的真实来源。Argo CD 可在指定 序邮署可以在 Git 提交时跟踪对分支,标签	f GitOps 模式,该模式使用 的目标环境中自动部署所需 的更新,或固定到清单的特		
家加应用				
创建应用成功后,会	自动来到 SSO 单点登录配置页。			
一 在 IDaaS I	中配置 550			
复制Argo CD服务访问	可地址,例如:【https://argoco	d.example.com】。		
复制Argo CD服务访问	可地址,例如:【https://argoco	d.example.com】。		
复制Argo CD服务访问 单点登录配置 已和	可地址,例如:【https://argoco	d.example.com】。		
复制Argo CD服务访问 单点登录配置 已和 不知道怎么配置? 请	可地址,例如:【https://argoco 音用 参考 对援文档 。	d.example.com】。		
复制Argo CD服务访问 单点登录配置 已編 不知道怎么配置?请	问地址,例如:【https://argoco	d.example.com]。		
复制Argo CD服务访问 单点登录配置 已系 不知道怎么配置?请 * Argo CD 服务地址	可地址,例如:【https://argoco 音用 参考 对接文档。 https://argocd.example.com>	d.example.com]。		
复制Argo CD服务访问 单点登录配置 已編 不知道怎么配置?请 * Argo CD 服务地址	可地址,例如:【https://argoco 音用 参考 对接文档。 https://argocd.example.com> Argo CD 服务地址是必填字段	d.example.com]。		
复制Argo CD服务访问 单点登录配置 已編 不知道怎么配置? 请 * Argo CD 服务地址	可地址,例如:【https://argoco 音用 参考 对接文档。 https://cargocd.example.com> Argo CD 服务地址是必填字段 Argo CD 服务地址,注意:不能以*/*	d.example.com】。		
复制Argo CD服务访问 单点登录配置 已パ 不知道怎么配置? 请 ・Argo CD 服务地址 ・应用账户	同地址,例如:【https://argocoland 日本の 参考 对接文档。 https://cargocol.example.com> Argo CD 服务地址是必填字段 Argo CD 服务地址,注意:不能以 "/" IDaaS 账户名	d.example.com】。 结尾。		
复制Argo CD服务访问 単点登录配置 已和 不知道怎么配置? 请 ・Argo CD 服务地址 ・应用账户	J地址,例如:【https://argoco 副 参考 对接文档。	d.example.com】。 结尾。 传递给业务系统。		~
 复制Argo CD服务访问 単点登录配置 CJ 不知道怎么配置?请 ・Argo CD 服务地址 ・应用账户 授权范围 	可地址,例如:【 https://argocol B用 ● 参考 对接文档。 https://cargocol.example.com> Argo CD 服务地址是必填字段 Argo CD 服务地址 注意:不能以 "/" IDaaS 账户名 单点登录时,将选中项作为账户标识, 全员可访问	d.example.com】。 结尾。 传递给业务系统。		~

将【https://argocd.example.com】填写到表单中。
应用身份服务

单点登录 应用账F	ュ	
单点登录配置 已启月		
不知道怎么配置? 请参	考对接文档。	
* Argo CD 服务地址	https://argocd.example.com	
	Argo CD 服务地址,注意:不能以 "/" 结尾。	
应用账户	IDaaS 邮箱 ~	
	单点登录时,将选中项作为账户标识,传递给业务系统。	
受权范围	全员可访问 ~	
	若选择"手动授权",需要在 应用授权 中进行权限分配。	

为了便于测试,【授权范围】可暂时选择【全员可访问】。

其他选项保持默认,点击保存即可完成 IDaaS 侧 全部 SSO 配置。

? 说明

提示 应用账户:默认使用 IDaaS 邮箱作为应用登录标识。 IDaaS 邮箱必须包含,才能完成 SSO。若希望灵活配置,请参考 单点配置通用说明 - 应用账户 进行配置。 授 权范围:若希望指定可访问应用的 IDaaS 账户,请参考 单点配置通用说明 - 应用账户 进行配置。

在页面下方的【应用配置信息】中,即包含了Argo CD完成 SSO 配置所需要的参数。

应用配置信息	
IdP 元数据	https://www.aliyunidaas.com/api/v2/app_mividtiffwb4hiqw4wop7bhg34/sami2/meta 🗗 🔥 无數
IdP Metadata	哲应用支持 metadata 配置信息上传/控取,可以节省大量配置步骤,请在应用 SSO 配置中寻找是否有 metadata 上传能力。
IdP 唯一标识	https://www.aliyunidaas.com/api/v2/app_mivldtiffwb4hiqw4wop7bhg34/sami2/meta ♂
IdP Entity ID	IDaaS 在应用中的标识,需要将值填写在应用单点包录配置中。
IdP SSO 地址	https://;;;;;;;;;avaliyunidaas.com/login/app/app_mivldtiffwb4hiqw4wop7bhg34/saml2/sso ♂
IdP Sign-in URL	SAML 协议支持 SP 发起单点登录,可能需要填写此地址在应用配置中。由 IDaaS 提供,可以直接访问该地址,进行应用登录,
单点退出地址	智不支持
SLO URL	SAML协议支持单点退出,可能需要填写此地址在应用配置中。由 IDaaS 提供。
公钥证书 Certificate	BEGIN CERTIFICATE MIIEFTCCAv2gAwBAgGSHiwa72KCeECsDy81+vo9229MA0GCSqGSIb3DQEBCwUA MIGSMscv047V0QD0BShcH8tbW12bGR0wWZmc210aGiusztR3b3A3YmhnMr2xkTAn

三、配置 Argo CD

1. SAML 配置字段

将 IDaaS 【应用配置信息】中的参数全部填写到配置argocd-cm中。

字段	别称	说明
ssoURL	IdP 发起 SSO 地址	从 IDaaS SSO 配置页【应用配置信息】中获取。 Argo CD将向该地址发送 SAML Request 请求,发起单点登录请求。
ssolssuer	ldP 唯一标识 ldP Entity ID	从 IDaaS SSO 配置页【应用配置信息】中获取。
caData	公钥证书 Certificate	从 IDaaS SSO 配置页【应用配置信息】中复制出来,然后Base64之后使用。

2. 前往单点登录设置

编辑argocd-cm和配置data.dex.config部分:

kubectl edit configmap argocd-cm -n argocd

Please edit the object below. Lines beginning with a '#' will be ignored, $\ensuremath{\sharp}$ and an empty file will abort the edit. If an error occurs while saving this file will be # reopened with the relevant failures. # apiVersion: v1 data: dex.config: | connectors: - type: saml id: saml name: 阿里云IDaaS config: ssoURL: 阿里云IDaaS SAML 应用IdP发起SSO地址 entityIssuer: https://argocd.example.com/api/dex/callback caData: 阿里云IDaaS SAML 应用证书Base64之后的值 redirectURI: https://argocd.example.com/api/dex/callback usernameAttr: email emailAttr: email # optional ssoIssuer: 阿里云IDaaS SAML 应用IdP唯一标识 url: https://argocd.example.com kind: ConfigMap metadata: annotations: kubectl.kubernetes.io/last-applied-configuration: | {"apiVersion":"v1", "kind":"ConfigMap", "metadata": {"annotations": {}, "labels": {"app.kubernetes.io/name": "argocd-cm", "app.kubernetes.io/part-of"
:"argocd", "name": "argocd-cm", "namespace": "argocd"}
creationTimestamp: "2022-03-23T02:43:34Z" labels: app.kubernetes.io/name: argocd-cm app.kubernetes.io/part-of: argood name: argocd-cm namespace: argood resourceVersion: "124561" uid: 9e161ab5-807e-449a-8488-7e764b4ed349

保存配置,重启服务吗,开启单点登录。

您已经可以尝试 Argo CD SSO。

IDP 发起

请用已授权使用 Argo CD 的 IDaaS 账户,登录到 IDaaS 门户页,点击页面上 Argo CD 图标,发起 SSO,检查配置结果。

ViDaaS 应用门户 _{阿里云 IDaaS}		
我的应用	我的应用	
我的账户	请点击下方的应用进行单点登录。若希望修改应用内容,请联系管理员。	
	搜索应用 Q.	
	argo	
	Argo CDwo	
	未配置应用账户	
		1

SP 发起

请在匿名浏览器中,打开 Argo CD 登录页,点击【单点登录】页签下的"登录"按钮,则会跳转到 IDaaS 进行登录。如果用户尚未登录 IDaaS ,则 IDaaS 会引导用户进行登录 。



验证通过后,将直接登录到 Argo CD 中。

2.咨询反馈

欢迎使用如下资源与我们沟通:

1. 讨论区

若您对产品功能、使用实践、最佳方案等有疑问,请您前往 讨论区 提出您的疑问或建议,我们将在 24 小时内提供官方回复。

2. 服务群

若您关注 IDaaS,请钉钉扫码入群,群中会发布产品更新,行业趋势等公告。

若您有具体问题,群内金牌服务机器人会解答您的问题。

若您希望人工服务,请入群后提交需求咨询表单。我们会尽快为真实需求客户提供专属服务。



3. 面向付费客户

若您是 IDaaS 付费客户,且有问题希望咨询,请钉钉搜索账户 idaasgc 联系 IDaaS 运营同学,我们将为您提供专属服务。加好友请备注您的企业信息

3.IDaaS 旧版文档 3.1. 常见问题

产品FAQ

- 产品购买FAQ
- 产品相关FAQ
- 权限系统相关FAQ
- 账户同步常见问题
- 热点问题

阿里云应用对接

```
阿里云用户 SSO 配置完成后,原先RAM的登录入口就不能使用了吗?
是否支持单点登录到其他阿里云应用,如云效、云桌面?
针对用户SSO,子用户是否可以管理元数据文件?如果可以管理,子用户需要什么权限
钉钉对接
钉钉微应用的出口PP怎么填
```

```
配置完成后,测试连接通过,但是拉取不到账户和机构是为什么?
为什么可以拉取到钉钉的部门,但是拉取不到员工账户
钉钉同步配置,可以手动拉取。但注册回调后只增量同步了机构,但是没有同步账户
钉钉扫码登录,移动端确认后,页面一直在loading
```

如果您有其他问题和需求,欢迎 联系我们。您可通过"联系我们"中的钉钉群二维码直接入群咨询。

3.2. 权限系统

3.2.1. 权限系统介绍

本文主要介绍了RBAC授权模式,和IDaaS的权限系统的设计架构以及权限系统的主要功能。

一、RBAC模型

RBAC,基于角色的权限访问控制(Role-Based Access Control): RBAC的核心在于用户只和角色关联,而角色代表对了权限,是一系列权限的集合。 RBAC三要素:

- 用户:系统中所有的账户
- 角色: 一系列权限的集合(如: 管理员, 开发者, 审计管理员等)

• 权限:菜单,按钮,数据的增删改查等详细权限。

在RBAC中,权限与角色相关联,用户通过成为适当角色的成员而得到这些角色的权限。角色是为了完成各种工作而创造,用户则依据它的责任和资格来被指派相应的角色, 用户可以很容易地从一个角色被指派到另一个角色。角色可依新的需求和系统的合并而赋予新的权限,而权限也可根据需要而从某角色中回收。角色与角色的关系同样也存 在继承关系防止越权。

• 阿里云应用相关FAQ

钉钉相关FAQ

• 单占容寻概述

• 优点: 便于角色划分, 更灵活的授权管理; 最小颗粒度授权

二、设计架构

1. 授权架构

IDaaS权限系统的架构依赖于RBAC模型,无论是在功能设计思路还是在用户体验上,权限,角色,用户三者关联关系可灵活组合,从而实现精细化授权。 此外,我们不仅支持按角色授权,同时也支持按账户直接授权。让用户的授权变的更加便捷,尤其是人员较少的企业极为使用。我们满足各类授权方式,按需求可灵活 自由操作,极大地简化了权限分配的管理。



3.2.2. 最佳实践

3.2.2.1. 第三方业务系统接入权限系统

SP: 指第三方业务系统

IDaaS: 身份应用服务

本文主要介绍如何使用 IDaaS 权限系统,实现第三方业务系统与 IDaaS 的权限对接,从而实现权限的集中管理。如想了解更多 IDaaS 权限知识,请参考权限系统介绍



场景描述

我们简单构建一个与 IDaaS 对接的第三方业务系统 (OA 工作平台),其 OA 系统菜单如下所示。



准备工作

在 IDaaS 中新建 OA 权限系统

1)点击 【授权】-【权限系统】。

2) 点击【新增系统】起名,保存。

概范		权限系统				85540 88.592
快速入门						
应用 应用列表	^	校限系统 校限系统是基于RBAC (Role	a-Based Access Control,基于角色的访问控制)的权利	R模型。既可以管理 IDaaS 自身系统权限,也可以管理第三方应用的二三级接权	(需要开发者角色)。	×
添加应用		系统名称	系统ID	系统状态	描述	操作
用一日求 机构及组	Ŷ	默认权限系统	idp_ps		IDaaS默认权限系统	派加管理员 授权管理 角色管理 系统详情
账户管理		OA业务系统	VQ1EDutzID			授权管理 角色管理 权限资源 系统详情 修改 對時
жы. же	^					接权管理 角色管理 权限资源 系统详情 <mark>影除</mark>
认证源						授权管理 角色管理 权限资源 系统详情 整除
记书管理						接权管理角色管理权限注意系统详情停放 對除
授权 权限系统 应用授权)					共5会 < 1 > 誕至 1 页
审计 其它管理	č					

1、定义资源

设置

无论是某个功能、菜单、按钮的查看权、使用权,还是某些特定数据的访问权限,都属于一种资源(Resource)。资源支持嵌套树形结构。管理员在这里可以新增、导入、 删除、编辑资源,也可以为某资源关联到角色使用。

我们需要在 IDaaS 上定义 OA 系统的资源,构建权限树

资源创建方式在IDaaS中有2种:

- 手动创建,详细操作请参考 新增权限资源
- 表格批量导入,详细操作请参考 导入权限资源
- 第三方接口调用,<mark>权限系统API接口清单</mark>

创建好的权限树如下图所示

🖃 🗆 📃 机构人员管理 ┆ □ 艮 机构管理 白. 🗆 民 人员管理 白.口 民 工作台 ----- 🖳 审批 ---- 📃 🗏 日报周报 白 🛛 🕄 行政办公

2、定义角色

在 IDaaS 中定义(创建)角色方式有 3 中

- 手动创建,详细操作请参考 新增角色
- 表格批量导入,导入角色

第三方接口调用, 权限系统API接口清单
在这里我们可以定义 3 个角色作为示例
1) 普通用户,拥有【通讯录】【工作台】【行政办公】【项目管理】等基本权限
2) 系统管理员,拥有【系统管理】权限
3) HR 部门管理员,【机构人员管理】权限
当然,我们也可以灵活去分配各类角色以满足需求,如部门管理员,分级管理员等此外,我们在机构人员管理中也定义按钮资源,同样也可作为权限分配
在通讯录中,我们定义了董事长,总经理等数据,也可对数据进行权限分配

3、资源关联角色

当角色创建完成后,就需要对角色进行授权了,我们将步骤2中定义好的角色按需要进行权限关联即可,从而建立资源-角色对应关系。

我们支持角色资源授权方式有3种:

手动创建,详细操作请参考,按角色授权权限资源
 第三方接口调用,权限系统API接口清单
 详细的角色分配操作,请参考 授权管理

4、角色关联账户

角色权限关联好后,对账号进行关联。 给每个人关联上相应的角色信息 我们支持角色账号授权方式有3种:

• 手动创建,详细操作请参考角色管理按角色授权账户

表格批量导入,详细操作请参考 导入角色成员

● 第三方接口调用,<mark>权限系统API接口清单</mark>

详细的角色分配操作,请参考授权管理

到这里我们的授权环节就全部完成了。

5、登录及获取权限

当我们完成以上4个步骤之后,这是我们就可以使用一个账号来进行效果验证了。

比如:我们使用张三登录 IDaaS 。可以看见张三的首页有 OA 业务系统,点击图标进行单点登录。(这里我们默认 OA 系统已经和 IDaaS 实现 JWT 协议的单点登录,详细对 接,请参考: JWT 模板使用指南)这时候 IDaaS 会向 OA 系统发起单点登录请求,OA 系统通过解析,获取到张三账号信息。

这时,我们就需要来查询张三的权限了

通过调用 IDaaS 权限系统 API 接口(获取权限系统指定用户的角色和权限)来获取张三这个角色对应拥有的权限资源信息

6、SP 前端展示

当OA系统获取完成张三的权限信息后,按权限情况展示张三所拥有的菜单即可。这里会涉及 OA 系统的研发工作。具体前端展现方式按实际情况即可。通常会有两种方式: 1) 无权限的功能菜单不展示

2)所有功能菜单展示,但未授权的菜单不可使用,点击提示"无权访问"等之类提示信息。

7、鉴权

鉴权就是指,当用户访问某项功能时,判断是该用户否有其权限。

IDaaS 提供关于的相应 API 接口来服务于 SP 进行鉴权。我们可以使用用户的角色或是账户名称来进行鉴权。

例如,张三在登录到 OA 系统后,当他每次点击 OA 的功能菜单时,OA 系统使用通过之前定义好的菜单(权限 ID)向 IDaaS 询问是否有其权限,并将结果告知给 OA 系统。

详细的鉴权 API 请参考 ,权限系统API接口

如果您想了解更多 IDaaS 权限系统内容,请<mark>联系我</mark>们

3.2.3. 自建权限系统

本文主要介绍什么是自建权限系统

一、自建权限系统介绍

我们在前文介绍IDaaS权限系统时,讲到IDaaS也支持第三方业务系统的权限管理接入。所以,自建权限系统就是指:在IDaaS权限系统中,除默认系统之外,新创建的权限 系统。



当我们在第三方业务系统接入后,在IDaaS权限系统功能中,一样可以进行角色管理,授权管理,资源管理等详细操作说明请参考 <mark>新增系统及系统详情</mark>

资源管理 角色管理 授权管理

权限系统API接口清单

二、第三方系统接入流程

详细第三方接入流程请参考最佳实践: 第三方业务系统接入权限系统

3.2.3.1. 自建权限系统

本文主要介绍什么是自建权限系统

一、自建权限系统介绍

我们在前文介绍IDaaS权限系统时,讲到IDaaS也支持第三方业务系统的权限管理接入。所以,自建权限系统就是指:在IDaaS权限系统中,除默认系统之外,新创建的权限 系统。



当我们在第三方业务系统接入后,在IDaaS权限系统功能中,一样可以进行角色管理,授权管理,资源管理等详细操作说明请参考 新增系统及系统详情 资源管理 角色管理 授权管理 权限系统API按口清单

二、第三方系统接入流程 详细第三方接入流程请参考最佳实践: ^{第三方业务系统接入权限系统}

3.2.3.2. 新增系统及系统详情

本文介绍IT管理员如何在IDaaS控制台新增权限系统,以及权限系统的详情查看。

- 1. 以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考 IT管理员指南-登录。
- 2. 在左侧导航栏,单击**授权> 权限系统**。
- 3. 单击页面右上角的**新增系统**。

		Q 搜索文档、控制台、API、解决方案和资源	要用 工单 备	案 企业 支	時 官网	>_	Ϋ.	Ä	⑦ 简	体 🧯
权限系统									新增	系统
✔ 収限系统 权限系统是基于RBAC 既可以管理 IDaaS 自身 默认系统只能关联开发	(Role-Based Access Control,基于角 资源权限,也可以管理第三方应用的二 者角色,其它功能不可用;自建系统可	色的访问控制)的权限模型。 级菜单功能按田等资源权限;当授予某个 IDaaS 用户开发者权限 以正常使用,用于集中管理第三方应用的权限。	1, 在未来将可以创建出新的自	定义权限系统,以	し支持应用的三	级授权。				×
系统名称	系统ID	系统状态	描述	操	PF					
默认权限系统	idp_ps		默认权限系统	角	色管理系统	详情				

4. 在**新增系统**侧边页,填写系统名称点击确定。

新增系统		×
* 系统名称	系统名称	
* 系统ID	Mn28ntWVEE	
	系统唯一标识,不能重复	
描述	系统描述,备注信息	
	确定 取消	

5. 在新增系统操作下面可以看到系统详情、角色管理、资源管理、授权管理、修改、启用、删除。

权限系统				新增系统
权限系统 权限系统是基于 既可以管理 IDa 默认系统只能关	RBAC(Role-Based Access Control,基于 S 自身治源积艰,也可以管理第三方应用的 联开发者角色,其它功能不可用;自建系统	龟的访问控制) 的权限模型 二级亲单功能按钮等资源权限;当提予某个 IDaaS 用户开发# 可以正常使用,用于集中管理第二方应用的权限。	客权限,在 未来 将可以创建出新的i	自定义权限系统,以支持应用的三级授权。
系统名称	系统ID	系统状态	描述	操作
默认权限系统	idp_ps		默认权限系统	角色管理系统详情
测试系统	Mn28ntWVEE	\mathbf{x}		授权管理角色管理资源管理系统详情修改删除

查看系统详情

- 1. 以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考IT管理员指南-登录。
- 2. 在左侧导航栏, 单击授权 >权限系统。
- 3. 在IDaaS权限系统下,单击操作列中的**系统详情**。

权限系统					新增系统
₩ 权限系统 权限系统是基于	RBAC(Role-Based Access Control,基于	角色的访问控制)的权限模型。既可以管理 IDaaS 自身系统权限,	也可以管理第三方应用的二三	级授权 (需要开发者角色) 。	×
系统名称	系统ID	聚统状态	描述	操作	
默认权限系统	idp_ps		默认权限系统	添加管理员 授权管理 角	色管理系统详情

4. 在**系统详情**侧边页,查看IDaaS权限系统的基础信息和API信息。

系统详情 (IDaaS权限系统)

	基础信息
系统名称	IDaaS权限系统
系统ID	idp_ps
描述	默认权限系统
系统状态	已启用
启用SSO	否
启用OTP	否
启用扫码登录	否
已有成员	16
已有角色	7
已有权限	39
创建人	IDP
创建时间	2020-02-19 11:12
	API信息
AppKey	739b2d9d93a307aa2dbd70eb2a7c04adhFThixszQMZ

 AppKey
 739b2d9d93a307aa2dbd70eb2a7c04adhFThixszQMZ

 AppSecret
 xq5VrtkazZANOQcv7oefmqBQlb7f48T1YmuZ5swmST

3.2.3.3. 资源管理

本文介绍如何使用权限系统的资源管理功能,实现在IDaaS平台维护应用系统的资源信息。

以Ⅱ管理员账号登录云盾IDaaS管理平台。具体操作请参考Ⅲ管理员指南-登录。

- 2. 在左侧导航栏,单击**授权 > 权限系统**。
- 3. 新建一个权限系统,参考使用新增系统。
- 4. 选择新增的权限系统,点击资源管理。
- 5. 根据需要,执行以下功能。
 - 新增权限资源
 - 新增子级权限资源
 - 导入权限资源
 - 编辑权限资源
 - 删除权限资源

? 说明

```
资源区分类型原因:1.资源对应的是客户自己系统中的内容,如系统中可能存在左侧导航菜单,页面上有不同的button和API接口等,可以通过类型进行区分;2.
资源还包括系统中的数据,在IDaaS中创建数据资源,需要关联数据权限模型,通过数据权限模型来控制数据有哪些操作权限,比如有的数据只有新增权限,没有删
除权限等。
```

新增权限资源

1. 在权限资源页面, 点击新增资源

概览		权限系统 / 测试OA	系统						
快速入门		← 资源管理						新增资源	导入资源
应用	^								
应用列表 添加应用		☆源管理 无论是某个項	bi能、菜单、按钮的查看权、使F	用权,还是某些特定数据的访问权限,	都屬于一种资源(Resource)	。资源支持嵌套网形结构。管理员	在这里可以新增、导入、删除、编辑资源,1	也可以为某资源关联到角色使用	× I.
账户	^				_				
机构及组		请输入名称进行搜索			Q				
账户管理									
分类管理		资源名称	权限值	外部口	描述	路径	操作		
认证	^				暂无费	文据			
认证源									
RADIUS							共0条 < 1	> 10条页 > 跳至	1 页
证书管理									

2. 在新增资源侧边页,完成新增资源参数的配置

新增资源		\times
父级	I	
* 权限值	Accounts	
	权跟值是权限在当前权限系统中的唯一标识,第三方系统可以根据权限值来区分校限,仅支持英文、数字、下划线	Z
*显示名称	账户管理	
权限类型	● 菜单 ─ 按钮 ─ API ─ 数据 ─ 其它	
*显示顺序	1	
	请填写整数数字, 越小的数字越靠前	
描述	请填写描述信息	
	确定 取消	

3. 点击确定

创建成功后,会在资源管理页面展示创建的权限资源

权限系统	测试OA系统						
← 资源	〔 管理					新增资源	导入资源
Ŵ	资源管理 无论是某个功能、菜单、按钮的查看权、使用权,	还是某些特定数据的访问权限,都属于	—种资源 (Resource)	。资源支持嵌套树形结构。	管理员在这里可以新增、导入、删除、编辑资	源,也可以为某资源关联到角色使用	× B.
请输入名称	进行搜索		Q				
资源名称	权限值	外部ID	描述	路径	操作		
账户管理	Accounts	902d8e7ffc94512864a7b61304 d9b9d8juPnLMqq11j		1	新増資源 編輯 删除	ŧ	
					共1条 〈 1	> 10条/页 > 跳至	1 页

新增子级权限资源

1. 选择需要创建子级资源的资源,点击操作栏中的 新增资源

权限系统 / 测试0	A系统						
← 资源管理	1					新增资源	导入资源
☆ 源管理 元 论是果	【 个功能、菜单、按钮的查看权、使用权,;	还是某些特定数据的访问权限,都履	于一种资源(Resource),	,资源支持嵌套树形结构。	管理员在这里可以新增、导入、删除、编辑	资源,也可以为某资源关联到角色使	× Ħ.
请输入名称进行搜索			Q				
资源名称	权限值	外部ID	描述	路径	操作		
账户管理	Accounts	902d8e7ffc94512864a7b6130 d9b9d8juPnLMqq1lj	04	1	新増資源 編輯	除	
					共1条 〈	1 > 10 条页 > 跳至	1 页

2. 在新增资源侧边页,完成新增资源参数的配置

父级	/账户管理	
* 权限值	delete_account_button	
	权限值是权限在当前权限系统中的唯一标识,第三方系统可以根据权限值来区分权限,仅支持英文、数字、下划线	
*显示名称	删除账户按钮	
权限类型	○ 菜单 ● 按钮 ○ API ○ 数据 ○ 其它	
*显示顺序	2	
	请填写整数数字,越小的数字越靠前	_
描述	请填写描述信息	
	确定 取消	

- 资源管理							新均	資源	导入多
资源管理 无论是某个!	力能、菜单、按钮的查着权、使用权,美	至是某些特定数据的访问权限,都属于	—种资源 (Resource)	,资源支持嵌套树形结构。	管理员在这里可以新增、导入、	删除、编辑资源	1,也可以为某资源关照	到角色便用	1.
输入名称进行搜索			٩						
资源名称	权限值	外部ID	描述	路径	操作				
账户管理	Accounts	902d8e7ffc94512864a7b61304 d9b9d8juPnLMqq1lj		1	新增资源	编辑 删除			
删除账户按钮	delete_account_button	aaa63d176b572671ba9cc5d05 3bba3539ycMKGohut2		/账户管理	新增资源	编辑 删除			
					共2条	< 1	> 10条/页丶	跳至	1

导入权限资源

管理员可以在excel表格中维护权限资源的基本信息和层级关系,通过使用导入功能批量导入权限资源。

1. 在权限资源页面,点击导入资源

权限系统 / 测试OA系统								
← 资源管理							新增资源	导入资源
☆ 源管理 无论是某个功能、	菜单、按钮的查着权、使用权,还想	是某些特定数据的访问权限,都属于	—种资源 (Resource) ,	。资源支持嵌套树形结构。管理员在这	这里可以新 增、导入、删除、雏	错错资源,也可以为某资	源关联到角色便序	× ∃.
请输入名称进行搜索			Q					
资源名称	权限值	外部ID	描述	路径	操作			
账户管理	Accounts	902d8e7ffc94512864a7b61304 d9b9d8juPnLMqq1lj		I	新增资源 编辑	删除		
删除账户按钮	delete_account_button	aaa63d176b572671ba9cc5d05 3bba3539ycMKGohut2		/账户管理	新增资源 编辑	删除		
					共2条 <	1 > 10 9	彩页 〜 跳至	1 页

2. 下载 导入格式范例文档,并根据文档填写系统的所有权限资源的信息

导入资源	\times
当前导入系统 测试OA系统	
消先下载资源导入恰式泡例又档,依据肯定恰式导入蝴蝶合子按完望正确无误,召则有可能导致导入失败。	
导入文件	
导入文件 取消	

3. 点击上传文件,选择填写好的文件

导入资源				\times
当前导入系统	ti.测试OA系统			
• 下载导	入格式范例文档			
请先下载 致导入失	资源导入格式范例文档, 收。	根据指定格式导入确保各字段类型正 研	确无误, 否则有可能导	
导入文件	命上传文件			
导入文件	取消			
点击导入文件				~
点击导入文件 导入资源				×
京击导入文件 导入资源 当前导入系统	ō: 测试OA系统			×
点击导入文件 导入资源 当前导入系统	5. 测试OA系统			×
点击导入文件 导入资源 当前导入系统	٤: 测试OA系统 入格式范例文档			×
 点击导入文件 导入资源 当前导入系统 当前导入系统 1 1 1 第 市载号 満先下載 3 3 (長) (長)	8: 测试OA系统 入 格式范例文档 资源导入格式范例文档,	限据指定格式导入确保各字段类型正确	角无误,否则有可能导	×
 点击导入文件 与入资源 当前导入系統 3前导入系統 1前导入系統 3前导入系統 3前局、 <	 3: 测试OA系统 入格式范例文档 资源导入格式范例文档, * 收。 平上传文件 导入权限资源 xls (20 kb) 	限据指定格式导入确保各字段类型正确	角无误,否则有可能导	×

5. 系统会弹窗提示导入结果,并在资源管理页面展示导入成功的资源

权限系统 / 测试OA系统							
← 资源管理		系统提示	×			新增资源	导入资源
愛源管理 无论是某个功能、菜 前输入名称进行搜索	单、按钮的查看权、使用权,还是3	资源导入结果如下: 本次总共导入数据:3条 预建:3条 更新:0条 删除:0条 失败:0条		吉构。管理员在这里可以新增、导入、非	創除、编編資源,也可以为其	#资源关联到角色使F	×
资源名称	权限值		确定取消	操作			
账户管理	Accounts	902d8e7ffc94512864a7b61304 d9b9d8juPnLMqq1lj		新增资源	编辑删除		
删除账户按钮	delete_account_button	aaa63d176b572671ba9cc5d05 3bba3539ycMKGohut2	/账户管	理新增资源	编辑删除		
机构管理	organization			新增资源	编辑删除		
新增机构按钮	new_organization	000011	/机构管	理新增资源	编辑删除		
删除机构按钮	del_organization		/机构管	理新增资源	编辑删除		

编辑权限资源

1. 选择需要更新的权限资源,点击编辑

权限系统 / 测试OA系统								
← 资源管理							新增资源	导入资源
☆ 旅育管理 无论是某个功能、	菜单、按钮的查看权、使用权,i	还是某些特定数据的访问权限,都属于	—种资源(Resource),	。资源支持嵌套树形结构。	管理员在这里可以新增、导入、	删除、编辑资源	,也可以为某资源关联到角色使用	× I.
请输入名称进行搜索			Q					
资源名称	权限值	外部D	描述	路径	操作			
账户管理	Accounts	902d8e7ffc94512864a7b61304 d9b9d8juPnLMqq1lj		1	新增资源	编辑删除		
删除账户按钮	delete_account_button	aaa63d176b572671ba9cc5d05 3bba3539ycMKGohut2		/账户管理	新增资源	編輯 删除		
机构管理	organization	00001		T	新增资源	编辑 删除		
新增机构按钮	new_organization	000011		/机构管理	新增资源	编辑 删除		
删除机构按钮	del_organization	000012		/机构管理	新增资源	编辑 删除		
					共5条	< 1	> 10条/页 > 跳至	1

2. 在输入框中更新想要更新的内容, 点击确定

删除权限资源

1. 选择需要删除的权限资源,点击删除

🗘 注意

如果想要删除的资源下还存在子级资源,则不允许删除。需要确保资源下子级资源都已删除的情况下,才可以删除该资源

权限系统 / 测试OA系统									
← 资源管理								新增资源	导入资源
☆源管理 无论是某个功能、 永	乘单、按钮的查看权、使用权,还是	是某些特定数据的访问权限,都属于	一种资源(Resource)。资源支持	嵌套树形结构。管理员在这里可以	新増、导入、	删除、编	辑资源, 也可以	为某资源关联到角色使	× 用。
请输入名称进行搜索			Q						
资源名称	权限值	外部D	描述	路径	操作				
账户管理	Accounts	902d8e7ffc94512864a7b61304 d9b9d8juPnLMqq1lj	OA系统,账户管理菜单	T	新增资源	编辑	删除		
删除账户按钮	delete_account_button	aaa63d176b572671ba9cc5d05 3bba3539ycMKGohut2		/账户管理	新增资源	编辑	删除		
机构管理	organization	00001		I	新增资源	编辑	删除		
新增机构按钮	new_organization	000011		/机构管理	新增资源	编辑	删除		
					共4条	<	1	10条/页 > 跳至	1

2. 在弹出的对话框中,点击确定

3.2.3.4. 角色管理

- 1. 以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考 IT管理员指南-登录。
- 2. 在左侧导航栏,单击**授权 > 权限系统**。
- 3. 新建一个权限系统,参考 使用新增系统。
- 4. 选择新增的权限系统,点击角色管理
- 5. 根据需要,执行以下功能
- 新增角色
- 导入角色
- 导入角色成员
- 编辑角色
- 删除角色
- 批量删除角色
- ◎ 按角色授权权限资源
- 按角色授权账户

新增角色

1. 在角色管理页面,单击**新增角色**

权限系统 / ps2

	←角的	色管理									
	Ŵ	角色管理 IDaaS 的权限系统支持角色性	愛权模型 (RBAC) 。角色可以	关联到一系列指定权限上,拥有	有角色的账号则即可拥有所有对	应的权限。管理员可以在这里分	为指定权限系统的角色进行新增	1、删除、编辑、关联校	限等管理技	梨作。	×
	新增角色	请输入角色名称进行搜	家			Q					
		角色名称	状态	权限值	权限数	描述	外部ID	操作			
		121	已启用	321	4		24cc601e351078e3922	关联权限 授权到人	編輯	削除	
		开发	已启用	2	2		e9cd2932a3f8c7701e35	关联权限 授权到人	编辑 🖁	11除	
		测试	已启用	1	4		372f2538825bf3cf548e	关联权限 授权到人	编辑 🖁	削除	
		批量删除					ŧ	±3条 < 1	> 1	跳至 1	页
2. 在	E新增角1	色 侧边页,完成以下	配置。								
	i. 名称	:为角色命名。角色	名称应唯一。								
	ⅲ. 权限(⋯ ↓ ↓ ★	直: 设置角色的权限	值。								
	Ⅲ. 状念:	: 走台后用角色。 · 法加备免条注信自									
	11.1曲处	, 冰川用己苷注信忌	0								

新建角色	×
*角色名称	测试角色-管理员
	名称不能重复
* 权限值	admin
	权限值是角色/权限在当前系统中的唯一标识,第三方系统可以根据权限值来标记区分角 色/权限,仅支持英文、数字、下划线以及路径!/
状态	
	是否启用
描述	角色描述,备注信息
	角色描述备注信息
	提交

3. 完成配置后,单击**提交**。

导入角色

1. 在角色管理页面,点击 导入-导入角色

权限系统 / 测试OA系统								
← 角色管理								
	支持角色授权模型(RBAC)。	角色可以关联到一系列指定权际	限上,拥有角色的账号则即可排	用有所有对应的权限。管理员可	以在这里为指定权限系统的角色	9进行新增、删除、编辑、关联	权限等管理操作。	×
新增角色 导入 ~	请输入角色名称进行搜索			٩				
日 : 导入角色	权限值	权限数	描述	状态	外部ID	操作		
S7 OB BAILOR			暫決	无数据				
						共0条 < 1	> 跳至 1	页

`			6 4 .	请先下载角色档 将角色导入到当	各式模板,确保行 当前所选PS系统	各字段类型无误, 沖。	否则有可能导致导)	、失败,提示:当前操作为
;角色格式范'	例文档,并根	据文档填写角	色基本信息	导入文件	@上传3	文件		
					请导入.xlsJ 导入文代	文件 4 返回		
i上传文件,ì	选择填写好的	文件						
i导入文件 入角色侧边ī	页,确认导入	数据是否正确	<i>,</i> 确认无误后点击	i 确定上传导入				
						×		
入角色								
入角色 系统自动共振的问题	p您进行了数据 建清除所有校验	校验,请您先 不合格的数据,	处理不合法数据才f ,也可删除指定不f	能进行上传导入操 合格的校验数据。	於作,或者 重新 」	上传		
於角色 系统自动状态可以一顿 请输入角色名	的您进行了数据 建清除所有校验 名称进行搜索	校验,请您先 不合格的数据,	处理不合法数据才 ,也可删除指定不有 Q	能进行上传导入操 合格的校验数据。	¥作, 或者 <u>重新</u> ・ ・	上传 定上传导入		
於角色 系統自动状 您可以一餐 请输入角色名 角色名称	的感进行了数据 建清除所有校验 名称进行搜索 权限值	校验,请您先不合格的数据,	处理不合法数据才 ,也可删除指定不有 Q 外部D	^{能进行上传导入操} 合格的校验数据。 描述	¥作,或者 重新. 确 校验结果	上传 定上传导入 操作		
沃角色 系统自动并 您可以一餐 请输入角色名 角色名称 角色1	b您进行了数据 書清除所有校验 名称进行搜索 权限值 role1	校验,请您先 不合格的数据; 状态 启用	处理不合法数据才 ,也可删除指定不r Q 外部D role1	^{能进行上传导入操} 合格的校验数据。 描述	(作,或者重新) (件) (中) (中	上传 定上传导入 操作 移除		
 決角色 系统自动状 您可以一餐 请输入角色结 角色名称 角色1 角色2 	o您进行了数据 書清除所有校验 名称进行搜索 权限值 role1 role2	校验,请您先 不合格的数据	处理不合法数据才 ,也可删除指定不f Q 外部D role1 role2	^{設进行上传导入操} 合格的校验数据。 描述	(作,或者重新) (件) (中) (中	上传 定上传导入 操作 移除 移除		
 決角色 系統自动決 您可以一餐 请输入角色結 角色名称 角色1 角色2 角色3 	DS&进行了数据 對清除所有校验 名称进行搜索 名称进行搜索 role1 role2 role3	校验,请您先 不合格的数据	处理不合法数据式 ,也可删除指定不 外部D role1 role2 7745d818d 6342408ae 4dd07a594 408b3eRpf 0IM7SIL	將进行上传导入操 含格的校验数据。 描述	 株,或者重新。 確 校验结果 校验成功 校验成功 	上传 定上传导入 操作 移除 移除 移除		

权限系统	测试OA系统							
←角	色管理							
Ŵ	角色管理 IDaaS 的权限系统式	友持角色授权模型(RBAC)。兌	角色可以关联到一系列指定权限	限上,拥有角色的账号则即可拥	有所有对应的权限。管理员可	以在这里为指定权限系统的角色进行新地	曾、删除、编辑、关联权限等管理操作。	×
新增角的	善导入 ∽	请输入角色名称进行搜索			٩			
	角色名称	权限值	权限数	描述	状态	外部ID	操作	
	角色4	role4	0			819fd628b9d3c50b1438	关联权限授权到人编辑删除	
	角色3	role3	0			7745d818d6342408ae4d	关联权限授权到人编辑删除	
	角色2	role2	0			role2	关联权限授权到人编辑删除	
	角色1	role1	0			role1	关联权限授权到人编辑删除	
	批量删除						共4条 < 1 > 跳3	

导入角色成员

1. 在角色管理页面,点击 导入-导入角色成员

权限系统	/ 测试OA系统							
←角的	色管理							
$\mathbf{\nabla}$	角色管理 IDaaS 的权限系统支持	角色授权模型(RBAC)。	角色可以关联到一系列指定权网	艮上,拥有角色的账号则即可排	¥有所有对应的权限。管理员可	以在这里为指定权限系统的角色进行新华	^{名、} 删除、编辑、关联权限等管理操作。	×
新增角色	● 令入 ~ 前	射输入角色名称进行搜索			Q			
	导入角色 导入角色成员	权限值	权限数	描述	状态	外部ID	操作	
	用色4	role4	0			819fd628b9d3c50b1438	关联权限授权到人编辑。删除	
	角色3	role3	0			7745d818d6342408ae4d	关联权限授权到人编辑。删除	
	角色2	role2	0			role2	关联权限授权到人编辑。删除	
	角色1	role1	0			role1	关联权限授权到人编辑。删除	
	批量删除						共4条 < 1 > 跳至	1

2. 下载 角色成员格式范例文档,并根据文档填写角色基本信息

- 3. 点击上传文件,选择填写好的文件
- 4. 点击导入文件
- 5. 在导入角色侧边页,确认导入数据是否正确,确认无误后点击 确定上传导入

×

导入角色成员

系统自动为您进行	了数据校验,请您先处理	王不合法数据才能进行上传导	入操作,或者重新上					
传 您可以一键清除所有校验不合格的数据,也可删除指定不合格的校验数据。								
请输入账号名称或	角色名称进行搜索	Q 确症	主传导入 一键删除					
账号名称	角色名称	校验结果	操作					
ceshi1	角色1	校验成功	移除					
ceshi2	角色1	校验成功	移除					
ceshi5	角色1	校验成功	移除					
ceshi3	角色2	校验成功	移除					
ceshi4	角色2	校验成功	移除					
ceshi1		角色不存在	移除					
ceshi3		角色不存在	移除					

导入成功后, 会在角色管理页面选择角色, 点击 授权到人 按钮可查看导入的角色成员

权限系统 / 测试OA系统

← 角色管理

Ŵ	角色管理 IDaaS 的权限系统	范支持角色授权模型(RBAC)。f	角色可以关联到一系列指定权际	艮上,拥有角色的账号则即可拥	稍所有对应的权限。管理员可以很	在这里为指定权限系统的角色进行象	所增、删除、编辑、关联权限等管理操作。	×
新增角色	- 导入 ×	调输入角色名称进行搜索			Q			
	角色名称	权限值	权限数	描述	状态	外部ID	操作	
	角色4	role4	0			819fd628b9d3c50b1438	关联权限授权到人编辑删除	
	角色3	role3	0		\sim	7745d818d6342408ae4d.	··· 关联权限 授权到人 编辑 删除	
	角色2	role2	0		\sim	role2	关联权限授权到人编辑删除	
	角色1	role1	0		\sim	role1	关联权限 授权到人 编辑 删除	
	批量删除							
							共4条 〈 1 〉 跳至	

编辑角色

- 1. 在角色管理页面,定位到要操作的角色,单击其操作列下的**编辑**。
- 2. 在角色管理侧边页基本信息页签下,根据需要修改角色的配置属性。
- 3. 修改完配置后,单击**保存**。

删除角色

1. 在角色管理页面,定位到要操作的角色,单击其操作列下的**删除**。

↓ 注意 删除角色之前,需要先禁用该角色

2. 在**提示**对话框中,单击**确定**。

批量删除角色

1. 在角色管理页面,勾选要操作的角色,单击页面下面的**批量删除**。

2. 在**提示**对话框中,单击**确定**。

3.2.3.5. 授权管理

- 1. 以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考 IT管理员指南-登录。
- 2. 在左侧导航栏,单击**授权 > 权限系统**。
- 3. 新建一个权限系统,参考 使用新增系统。
- 4. 选择新增的权限系统,点击授权管理
- 5. 根据需要,执行以下功能
 - 按账户授权权限资源
 - 导入账户关联的权限资源
 - 按账户授权角色

 - 按角色授权权限资源
 - 按角色授权账户

按账户授权权限资源

1. 在授权管理页面,点击按人授权页签

权限系统 / 測试OA系统			
← 授权管理 该人授权 按角色授权			导入账号关联权限资源
授 <mark>収管理</mark> 接人授权是基于ACL (Access (Control List) 访问控	利列本就是用一个列来的形式来维护对某个资源的访问控制,例如:针对账号对其控制能访问管理哪些资源。	×
账号列表 (999)		授权到权限 授权到角色	
请输入账号进行搜索	Q	☞ 角色继承的权限资源 🕝 自身赋予的权限资源	×
ceshi4 ceshi1	>	□ ② 民 机构管理 □ ○ 民 新婚师场法法田 □ □ 民 新婚师场法法田	
ceshi2	>		
ceshi5	>	- □ 民 新増設产設田 - □ 民 新時設产設田	
ceshi3	>	□ ■ 編銀版户按钮	
	>	1417	-

2. 在左侧账号列表中选择账户, 点击授权到权限

权限系统 / 测试OA系统

○ 授权管理			
¥ 按人授权是基于ACL (Ac	cess Control List) 访问控	·阿表就是用一个列表的形式来维护对某个资源的访问控制,例如:针对账号对其控制能访问管理哪些资源。	
长号列表 (999)		授权到份限 授权到角色	
请输入账号进行搜索	Q	☑ 角色继承的权限资源 ☑ 自身繁子的权限资源	
ceshi4	>		
ceshi1	>	- 😪 民 新婚机构按钮 - 🗆 民 删除机构按钮	
ceshi2	>		
ceshi5	>		
ceshi3	>		
DDFDDDD	>	\$\$ 7	
lip00001			

② 说明 其中勾选上且置灰的权限资源,为账户继承自角色的权限资源,无法在该页面取消。如需取消,取消角色和账户的关联关系即可。

🔲 MAT 🔄 LA 🔄 MEA 🐪 NATE (188, 779,				U 1	>wix#]	LAUTO
	Q 搜索文档、控制台、API、解决方案和资源 费用 工单 备案 企业 支持 官网	Δ	. Ä	0	简体	9
- 反仪官坦						
安人授权 按角色授权			导,	联号关联	关权限资源	₿.
₩ 授权管理 按人授权是基于ACL (Access Control List) 访问	制列表就是用一个列表的形式来维护对某个资源的访问控制,例如:针对紫母对其控制能访问管理哪些资源。					×
账号列表 (999)	授权到权限 授权到角色					
请输入账号进行搜索 Q	☑ 角色继承的权限资源 🕜 自身赋予的权限资源				×	
ceshi4 >						
ceshi1 >	- 2 民 新婚机构按钮					
ceshi2 >						
ceshi5 >						
ceshi3 >	- ☞ 弐 豊勝策庁按钮					
DDFDDDD >	₩ ₽					
lin00001 >						
zb5253232 >						B\$
tect_1						

导入账户关联的权限资源

1. 在授权管理页面,点击页面右上角的 导入账号关联权限资源

权限系统 / 测试OA系统

← 授权管理

按人授权 按角色授权						导入账号关联权限	资源
₩ 授权管理 按人授权是基于ACL (Acces	s Control List) 访问控	制列表就是用一	个列表的形式来维护双	对某个资源的访问控制,例如:针对账号对其控	制能访问"管理哪些资源。		×
账号列表 (999)		授权到权	双限 授权到角	iê.			
请输入账号进行搜索	Q	请输入角的	色名称进行搜索		Q	添加关联 批量取消关	联
ceshi4	>		角色名称	权限值	描述	操作	
ceshi1	>		角色3	role3		取消关联	
ceshi2	>		角色2	role2		取消关联	
ceshi5	>		角色1	role1		取消关联	
ceshi3	>						
DDFDDDD	>					共3条 〈 1 〉 跳至 1	N
lin00001	>						

2. 点击下载导入账户关联权限资源格式范例文档,并根据范例填写文档

导入账号关联权限资源	(测试OA系统)

 \times

洗下载账户关理 示:当前操作为料	关权限资源格式模板 务账户导入到指定权	页,确保各字段 【限资源中。	送型无误,	否则有可能导	致导入失败,	提
导入文件	命上传文件					
	请导入.xls文件					
	导入文件	返回				

- 3. 点击上传文件,选择填写好的文件
- 4. 点击导入文件
- 5. 在导入角色侧边页,确认导入数据是否正确,确认无误后点击 确定上传导入

导入成功后,会	会在 授权管理-按人授权-	·授权到权限	页面展示账户	被授予的权限资源
---------	---------------	--------	--------	----------

权限系统 / 测试OA系统

← 授权管理

		导入账号关联权限资源
ontrol List) 访问控	制列来就是用一个列来的形式来维护对某个资源的访问控制,例如:针对账号对其控制能访问管理哪些资源。	×
	授权到权限 授权到角色	
Q	≥ 角色維承的权限资源 😪 自身繁子的权限资源	×
>		
>		
>		
>		
>		
>	\$ 77	
>		
	ontrol List) 访问控 Q > > > > > > >	http://Lsi) 坊间控制列来就是用一个列表的形式未维护对某个资源的访问控制,例如:针对账号对并控制能访问管理哪些资源。

按账户授权角色

1. 在授权管理页面, 点击按人授权页签

权限系统 / 测试OA系统

← 授权管理 _{按人授权} 按角色授权			导入账号关联权限资源
授权管理 按人授权是基于ACL (Acces	ess Control List) 访问控制	例表就是用一个列來的形式來維护对某个资源的访问控制,例如:针对账号对共控制能访问管理哪些资源。	×
账号列表 (999)		授权到权限 授权到角色	
请输入账号进行搜索	Q	≥角色缝承的积限资源 🖌 自身赋予的积限资源	×
ceshi4	>		
ceshi1	>	- 2 民 新培机构按钮 - D 民 删除机构按钮	
ceshi2	>	□□ 民 編編机构按钮	
ceshi5	>		
ceshi3	>		
DDFDDDD	>	保存	
lin00001	>		

2. 在左侧账号列表中选择账户,点击授权到角色

权限系统 / 測试OA系统

√ 授权管理 按人授权是基于ACL (Acc	ess Control List) 访问控	则列表就是用一个列表的形式来维护对某个	资源的访问控制,例如:针对账号对其把	空制能访问"管理哪些资源。	
号列表 (999)		授权到权限 授权到角色			
物入账号进行搜索	Q	请输入角色名称进行搜索	•	Q	添加关联 批量取消关
eshi4	>	角色名称	权限值	描述	操作
ceshi1	>	角色1	role1		取消关联
eshi2	>				
eshi5	>				共1条 〈 1 〉 跳至 1
eshi3	>				
DFDDDD	>				
in00001					

⑦ 说明 添加关联关系后,账户会自动继承角色的权限资源。

号列表 (999)		授权到权限 授权到角色	_		
f输入账号进行搜索	<u>م</u>	请输入角色名称进行搜索	17102 /4	Q	「「「「「」」「「」」「「」」「」」「「」」「」」「「」」「」」「」」「」」「
ceshi1	>	角色1	typeter	加述	探TF
eshi2	>		10121		AP.XEn.xe
eshi5	>				共1条 〈 1 〉 跳至 1
eshi3	>				
DFDDDD	>				
n00001	>				
联角色 (ceshi1)				×	
联角色(ceshi1) 请输入角色名称进行搜索		٩		×	
联角色 (ceshi1) 请输入角色名称进行搜索 角色名称		Q 权限值	描述	×	
联角色 (ceshi1) 请输入角色名称进行搜索 ● 角色名称 ● 角色2		Q 权限值 role2	描述	×	
联角色 (ceshi1) 请输入角色名称进行搜索 ▲ 角色名称 ▲ 角色3		マ 权限値 role2 role3	描述	×	
联角色 (ceshi1) 请输入角色名称进行搜索 ④ 角色名称 ④ 角色3 ④ 角色4		マ 权限値 role2 role3	描述	×	

点击取消关联,可删除账户和角色的关联关系

权限系统 / 测试OA系统

← 授权管理 放人授权 施角色授权				导入账号关联权限资源
授权管理 按人授权是基于ACL(Access Control List)访问]控制列表就是用一个列表的形式来维护对某个	资源的访问控制,例如:针对账号对共	空制能访问/管理哪些资源。	×
账号列表 (999)	授权到权限 授权到角色			
请输入账号进行搜索 Q	请输入角色名称进行搜索		Q	<mark>添加关联</mark> 批量取消关联
ceshi4 >	角色名称	权限值	描述	操作
ceshi1 >	角色3	role3		取消关联
ceshi2 >	角色2	role2		取消关联
ceshi5 >	角色1	role1		取消关联
ceshi3 >				
DDFDDDD				共3条 〈 1 〉 跳至 1 💦
lin00001 >				

○ 也可以勾选角色后,点击批量取消关联,批量删除账户和角色的关联关系

权	限系统	测试OA系统

← 授权管理						
按人授权 按角色授权					导入账号关联权限	長资源
₩ 授权管理 按人授权是基于ACL (Acces	ss Control List) 访问控	制列表就是用一个列表的形式来维护处	某个资源的访问控制,例如:针对账号对其	控制能访问/管理哪些资源。		×
账号列表 (999)		授权到权限 授权到角旗	<u> </u>			
请输入账号进行搜索	Q	请输入角色名称进行搜索		Q	添加关联 批量取消关	联
ceshi4	>	角色名称	权限值	描述	操作	
ceshi1	>	✔ 角色3	role3		取消关联	
ceshi2	>	角色2	role2		取消关联	
ceshi5	>	角色1	role1		取消关联	
ceshi3	>					
DDFDDDD	>				共3条 〈 1 〉 跳至 1	à.
lin00001	>					

按角色授权权限资源

1. 在授权管理页面, 点击按角色授权页签

权限系统 / 测试OA系统		
授权管理 角色授权是基于RBAC (Role-Based Access Control	,基于角色的访问控制)的权限模型。既可以管理 IDaaS 自身系统权限,也可以管理第三方应用的二三级授权(需要开发者角色)。	×
角色列表 (4)	关联到权限 授权到账号	
请输入角色进行搜索 Q		
角色2 >		
角色3 >		
角色4 >	- D 民 新増%/-按钮 - D 民 新始%/-按钮	
角色1 >		
共4条 < 1 >	保存	

2. 在左侧角色列表中选择角色,点击关联到权限

权限系统 / 测试OA系统			
← 授权管理 ^{按人授权} 按角色授权			
₩ 授权管理 角色授权是基于RBAC(Rd	ole-Based Access Contro	1, 基于角色的访问控制)的权限模型。既可以管理 IDaaS 自身系统权限,也可以管理第三方应用的二三级授权(需要开发者角色)。	×
角色列表(4)		关联到权限 接权到账号	
请输入角色进行搜索	Q		
		🗹 民 新増机构按钮	
角色2	>		
角色3	>		
每节4			
用巴4	,		
角色1	>		
		保存	
共 4	条 〈 1 〉		

3. 勾选想要授权给角色的权限资源,点击保存,即可授予角色权限资源

权限系统 / 测试OA系统

授权管理 角色授权是基于RBAC(Role-B	Based Access Control	,基于角色的访问控制)的权限模型。既可以管理 IDaaS 自身系统权限,也可以管理第三方应用的二三级授权(需要开发者角色)。	×
角色列表 (4)		关联到权限 授权到账号	
请输入角色进行搜索	Q		
角色2	>		
角色3	>	└-O 民 編編的构設田 └-O 民 新学管理	
角色4	>	- C 民 新婚账户按钮	
角色1	>		
共4条	< 1 →	保存	

按角色授权账户

1. 在授权管理页面, 点击按角色授权页签

权限系统 / 测试OA系统			
← 授权管理			
按人授权 按角色授权			
- 410417255TBB			
☆ 授权官理 角色授权是基于RBAC(F	Role-Based Access Contro	,基于角色的访问控制)的权限模型。既可以管理 IDaaS 自身系统权限,也可以管理第三方应用的二三级授权(需要开发者角色)。	
角色列表 (4)		关联到积限 授权到账号	
请输入角色进行搜索	Q		
角色2	>	- 🐨 民 新禅切构按钮 - 🗆 民 翻除机构按钮	
角色3	>		
角色4	>		
角色1			
		6 777	E
共,	4条 〈 1 〉		

2. 在左侧角色列表中选择角色,点击授权到账号

应用身份服务

权限系统 / 测试OA系统					
角色列表 (4)	关联到权限 授权到账号				
请输入角色进行搜索 Q	请编入账户名称进行搜索		٩		添加关联 批量取消关联
角色2 >	账号	昵称	邮箱	描述	操作
角色3 >	ceshi1	测试1	ceshi1@mail.com	外部同步账户	取消关联
角色4 >	ceshi2	测试2	ceshi2@mail.com	外部同步账户	取消关联
角色1 >	ceshi5	测试5	ceshi5@mail.com	外部同步账户	取遄关联
扶4옾 < <mark>1</mark> >					共3条 < 1 > 覲至 1 页

○ 点击添加关联,可选择账户,添加账户和角色的关联关系。

⑦ 说明 添加关联关系后,账户会自动继承角色的权限资源。

权限系统 / 测试OA系统

← 授权管理

按人授权 按角色授权

授权管理 角色規模基基子RBAC(Role-Based Access Control、基于角色的访问控制)的初期構態。 筋可以管理 (DasS 自身系统初度、也可以管理論二方应用的二三取接权 (需要开设者角色)。						
角色列表 (4)		关联到权限 接权到账号				
请输入角色进行搜索	Q	请输入账户名称进行搜索		Q		添加关联 批型取消关联
角色2	>	账号	昵称	解释	描述	操作
角色3	>	ceshi1	测试1	ceshi1@mail.com	外部同步账户	取消关联
角色4	>	ceshi2	测试2	ceshi2@mail.com	外部同步账户	取满关联
角色1	>	ceshi5	测试5	ceshi5@mail.com	外部同步账户	取满关联
共4象 < 1	>					共3条 〈 1 〉 跳至 1 页

P 88

添加关联	(角色1)			>	<	
请输入账	户名称进行搜索	Q				
	账号	昵称	邮箱	路径		
	test2020	test2020	test2020@163.com			
	lin107	lin107	lin107@a.com			
	admin2	admin2	admin2@as.nj			
	admin1	admin1	admin1@as.kk			
	user2	user2	user2@as.cd			
	user1	user1	user1@as.cd			
	54678567	54678567	54678567@com.cn			
	lin001	lip001	lin001@a.com			
	1001	H=4024	11-10210			
	1101234	IIN1234	lin1234@a.com			
	newuer2	newuer2				
确定 点击取消关	取消 联,可删除账户和角色的	的关联关系				
	登 卫王 按角色接权					
☆ 授权 ★ ★ ★ ▲ ★ ▲ ★ ▲ ★ ▲ ★ ▲ ★ ▲ ★ ▲ ★ ▲ ★	管理 訳见是基于RBAC(Role-Based Access Control,	基于角色的访问控制)的权限模型。既可以答	理 IDaaS 自身系统权限,也可以管理第三方应	用的二三级授权(需要开发者角色)。		×
角色列表 (4)		关联到权限 攢	权到账号			
语编入角色进行	行搜索	Q。 请输入账户名称进行搜索		٩		添加关联 批量取消关联
角色2		> % 9	昵称	邮拍	描述	證作
角色3		> ceshi1	调6式1	ceshi1@mail.com	外部同步账户	取消关款
角色4		> ceshi2	测试2	ceshi2@mail.com	外部同步账户	取消关联
1 11 11 万进	_{共4条} <		_{調話} 6 6 的 关联 关 系	ceshi5@mail.com	外部间步账户	取消大禁 共3条 < 1 > 跳至 1 页
权限系统 / 测	LitoA系统					
	計理					
₩ 授权(角色振	管理 訳見基于RBAC(Role-Based Access Control,	,基于角色的访问控制)的权限模型。既可以管	5種 IDaaS 自身系统权限,也可以管理第三方的	立用的二三级授权(需要开发者角色)。		×
角色列表 (4)		关联到权限 援	权到账号			
请输入角色进行	行搜索	Q. 请输入账户名称进行搜索	e	Q		添加关联 批量取消失职
角色2		> 账号	昵称	66740	描述	操作
角色3		> ceshi1	测试1	ceshi1@mail.co	m 外部同步账户	取漏关联
角色4		> ceshi2	測试2	ceshi2@mail.co	n 外部同步账户	取湍关联
角色1		> Ceshi5	测试5	ceshi5@mail.co	n 外部同步账户	取消关联
	共4条 <	1 >				共3条 〈 1 〉 跳至 1 页

3.2.4. 权限系统API接口清单

1、概述

本文档为IDaaS对外提供的权限相关的API文档,开发者可根据该文档进行集成IDaaS权限功能,进而实现系统权限数据的管控。

接口文档分类三大类:第一类,角色和权限管理接口,开发者可将业务系统中的角色和权限资源等通过RestFul API定义到IDaaS当中,第二类,授权管理接口,开发者可通 过API对系统中的"人员","角色"之间进行授权的关联操作,第三类,开发者可通过API,在用户登录业务系统或操作业务系统中功能的时候对该"人员"进行一个鉴权 的操作。

2、接口清单

权限系统全局接口

- 1. 获取权限系统授权 access_token
- 2. 获取权限系统信息

角色管理接口

- 1. 获取权限系统的所有角色(分页)
- 2. 新增角色
- 3. 编辑角色
- 4. 删除角色
- 5. 新增权限
- 6. 编辑权限
- 7. 删除权限

授权管理接口

- 1. 获取指定角色的已关联权限(分页)
- 2. 把人授权到角色
- 3. 把权限关联到角色
- 4. 获取指定权限节点下,用户已授权的权限
- 5. 获取角色所有已授权用户(分页)
- 6. 获取权限系统指定用户的角色和权限

鉴权接口

- 1. 判断用户是否有角色
- 2. 根据权限uuid判断用户是否有权限
- 3. 根据权限值判断用户是否有权限

获取权限系统授权 access_token

接口地址

POST https://{{your-idaas-domain}}/oauth/token

接口说明

所有的权限系统相关的接口,都是受保护的资源。只有通过本接口获取到 access_token,才能继续调用后续接口。

access_token 的使用方式有两种:

1. 第一种

Header参数传递

头名称为 Authorization, 值为bearer {access_token}(请注意bearer和access_token之间的空格)

2. 第二种

Query参数传递

在请求URL的最后添加参数。如: http://your-idaas-domain/?access_token={access_token}

请求参数

参数	类型	必须	示例值	描述
client_id	string	是	78d8be99ef30197c31888f5d2d 1390a6pHn71sZEqvP	从权限系统详情中获取到的 AppKey
client_secret	string	是	96csUmei1g0tL629ufrVMZviFie7 NWBOnGYsJNLknQ	从权限系统详情中获取到 的AppSecret
grant_type	array	是	固定值: client_credentials	
Scope	string	是	固定值: read	

返回参数

参数	类型	示例值	描述
access_token	string	bd3a80ca-24c3-4da8-836f- 9efcb2c52c4b	外部ID
token_type	string	bearer	OU uuid
expires_in	string	43199	access_token 过期时间,单位为秒。7200 秒为 2 小时。
scope	string	read	固定值: read

示例

```
请求示例
```

http://{{your-idaas-domain}}/oauth/token? client_id=78d8be99ef30197c318885d2d1390a6 &client_secret=96csUmeilg0tL629ufrVMZv &grant_type=client_credentials&scope=read

正常返回示例

"access_token": "bd3a80ca-24c3-4da8-836f-9efcbb", "token_type": "bearer", "expires_in": 41177, "scope": "read"

}

{

获取token所需的Key和secret,通过权限系统中的系统详情页面获取,见下图。



参数和header请求示例

身份管理服务公共云合集·IDaaS 旧版 文档

s 💿 8 hidden	Body Pre-request Script Tests • Settings •	
Y	VALUE	DESCRIPTION
ontent-Type	application/json	
ey	Value	Description
S Y	∞ 8 hidden ntent-Type	value Intert-Type application/json value value

获取权限系统信息

接口地址

POST /api/bff/v1.2/developer/ps/details

接口说明

获取权限系统的基本信息。

请求参数

参数	类型	必须	示例值	描述
access_token	string	是	bd3a80ca-24c3-4da8-836f- 9efcb2c52c4b	
psld	String	是	Fgh9sKSS	系统id,详情处可见

返回参数

参数	类型	示例值	描述
uuid	string	bd3a80ca-24c3-4da8-836f- 9efcb2c52c4b	外部ID
createTime	string	2019-09-14 13:54	权限系统创建时间
archived	Boolean	False	逻辑删除,false代表正常,true代表已删除
psld	sting	Fgh9sKSS	PS系统唯一id
name	string	接口测试系统	权限系统名称
host	string	http://your-dmain.com	PS业务系统主页地址
remark	string	这是一个针对 BPM 应用的权限系统。	权限系统说明
creator	string	admin	权限系统创建人
enabled	boolean	true	是否已启用

示例

请求示例

{{your-idaas-domain}}/api/bff/v1.2/developer/ps/details?access_token={{access_token}}

请求入参示例
{ "psId":"Fgh9sKSS" }

正常返回示例

```
{
    "success": true,
    "code": "200",
    "message": null,
    "requestId": "47B0A008-778F-4BB9-801E-5D7C18FFE0EE",
    "data": {
        "uuid": "6e10dd2b2a0c4b92c64b840ea869886b6pWWnalmjpZ",
        "createTime": "2020-03-31 10:44",
        "archived": false,
        "name": "接口测试系统",
        "psId": "fglb3KSS",
        "host": null,
        "remark": null,
        "creator": "admin",
        "enabled": true
    }
}
```

Postman请求示例



dy Coo	kies (1) Headers (11) Test Results	Status: 2
Pretty	Raw Preview Visualize JSON 🔻 🚍	
1 {		
2	"success": true,	
3	"code": "200",	
4	"message": null,	
5	"requestId": "B55ED760-4 L "LL	
6	"data": {	
7	"uuid": "d931496e?	
8	"createTime": "2020-12-10 16:01",	
9	"archived": false,	
10	"name": "test",	

获取权限系统的所有角色 (分页)

接口地址

GET /api/bff/v1.2/developer/ps/all_roles				
接口说明				
获取指定权限系统下的角色信息。				
请求参数				
参数>	类型			

参数>	类型	必须	示例值	描述
access_token	string	是	bd3a80ca-24c3-4da8-836f- 9efcb2c52c4b	
currentPage	int	否	1	查询第几页的数据,从1开始

身份管理服务公共云合集·IDaaS 旧版 文档

参数>	类型	必须	示例值	描述
pageSize	int	否	10	每页查询多少条目,不填写默 认10条
psld	String	是	hU2czV4pMR	PS系统id

返回参数

参数	类型	示例值	描述
List	Array		角色列表
uuid	string	4c9b9f14e82a5d4978d5ed229ec1ae4d69 12xmCXA1l	OU uuid
name	string	测试角色	角色名,同一个权限系统内,角色名是唯一 的,最长64字符,不能为空
permissionValue	string	test_role	角色的权限值
remark	string	admin	描述
enabled	boolean	true	是否已启用
currentPage	int	1	当前页数,从 1 开始
ps	string	hU2czV4pMR	PS系统id
totalSize	int	2	总角色数量
pageSize	int	10	一页包含的角色数量
perPageSize	int	10	当前请求时参数返回

示例

请求示例

{{your-idaas-domain}}api/bff/v1.2/developer/ps/all_roles?currentPage=1&access_token={{access_token}}&psId=hU2czV4pMR

正常返回示例

"success": true,							
"code": "200",							
"message": null,							
"requestId": "D537580C-A5A2-4557-AEDD-3294DFB8ECE6",							
"data": {							
"list": [
{							
"uuid": "4c9b9f14e82a5d4978d5ed229ec1ae4d6912xmCXA11",							
"name": "Michael 测试角色",							
"permissionValue": "michael_test_role",							
"remark": "",							
"enabled": false							
},							
{							
"uuid": "61a779e3b2ac948d8768bb03801f99d9gRSYuTIStRH",							
"name": "Michael 测试角色 2",							
"permissionValue": "michael_test2",							
"remark": "",							
"enabled": true							
}							
],							
"totalSize": 2,							
"currentPage": 1,							
"psId":"hU2czV4pMR"							
"pageSize": 10,							
"perPageSize": 10,							
}}							

新增角色

接口地址

POST /api/bff/v1.2/developer/ps/role/create?access_token={{access_token}}

接口说明

向当前的权限系统中新增一个角色。

请求参数

参数	类型	必须	示例值	描述
access_token	string	是	bd3a80ca-24c3-4da8-836f- 9efcb2c52c4b	
name	string	是	测试角色	角色名,同一个权限系统内,角色 名是唯一的,最长64字符,不能为 空
permissionValue	string	是	test_role	角色的权限值,统一个权限系统 内,角色的权限值是唯一的,最 长64字符,只能包含字母数字 和"-"或者"_",不能为空
enabled	boolean	是	true	是否启用角色
psld	String	是	hU2czV4pMR	PS系统id
remark	string	否	这是一个测试使用的角色	角色描述信息,最长255字符,可 以为空
clientToken	string	否	Kqji1upjakhjdihq3e	IDaaS 幂等机制字段,由调用方自 动随机生成,标识一次请求操作。

返回参数

参数	类型	示例值	描述
roleUuid	String	447fed833d8739ecb1caf6f38af14e65tth uiDBac88	新生成的角色 全局唯一标识

示例

请求示例

{{your-idaas-domain}}/api/bff/v1.2/developer/ps/role/create?access_token={{access_token}}

```
{
"name":"测试角色",
"permissionValue":"test_role",
"coabled":true,
、mutf体用的角色"
        "enabled":true,
"remark":"这是一个测试使用的角色",
"clientToken":"hycllbzqcjdra4fg",
```

- clientToken":"hycl1
 "psId":"hU2czV4pMR"
 }

正常返回示例

- {
 - "success":true,
 - "code":"200",
 - "message":null, "requestId":"51331044-A2FE-474A-BA0B-BF84599D8AEE",
- "roleUuid":"447fed833d8739ecb1caf6f38af14e65tthuiDBac88"
- }

编辑角色

接口地址

PUT /api/bff/v1.2/developer/ps/role/update?access_token={{access_token}}

接口说明

修改一个现有角色。

请求参数

参数	类型	必须	示例值	描述
access_token	string	是	bd3a80ca-24c3-4da8-836f- 9efcb2c52c4b	
uuid	String	是	447fed833d8739ecb1caf	待修改的角色全局唯一标识,角色 外部id,必填
name	string	是	测试角色	角色名,同一个权限系统内,角色 名是唯一的,最长64字符,如果为 空则代表不修改
permissionValue	string	是	test_role	角色的权限值,统一个权限系统 内,角色的权限值是唯一的,最 长64字符,只能包含字母数字 和"-"或者"_",如果为空则代 表不修改
enabled	boolean	是	true	是否启用角色
psld	String	是	hU2czV4pMR	PS系统id
remark	string	否	这是一个测试使用的角色	角色描述信息,最长255字符,可 以为空
clientToken	string	否	Kqji1 upjakhjdihq3e	IDaaS 幂等机制字段,由调用方自 动随机生成,标识一次请求操作。

返回参数

无。

示例

请求示例

{{your-idaas-domain}}/api/bff/v1.2/developer/ps/role/update?access_token={{access_token}}

请求入参示例

```
"name":"测试角色",
"uuid":"447fed833d8739ecb1caf6f38af14e65tthuiDBac88",
"permissionValue":"test_role",
"enabled":true,
"remark":"这是一个测试使用的角色",
   "clientToken":"hyc11bzqcjdra4fg",
   "psId":"hU2czV4pMR"
```

正常返回示例

}

```
{
   "success":true,
   "code":"200",
   "message":null,
    "requestId":"51331044-A2FE-474A-BA0B-BF84599D8AEE"
```

}

删除角色

接口地址

DELETE /api/bff/v1.2/developer/ps/role/delete/{uuid}?access_token={{access_token}}

接口说明

删除角色, 仅能删除禁用的角色

请求参数

参数	类型	必须	示例值	描述
access_token	string	是	bd3a80ca-24c3-4da8-8 36f-9efcb2c52c4b	
uuid	String	是	447fed833d8739ecb1caf 6f38af14e65tthuiDBac88	待删除的角色全局唯一标识,角色 外部id

返回参数

```
无。
```

示例

{

}

请求示例

{{your-idaas-domain}}/api/bff/v1.2/developer/ps/role/delete/{{roleUuid}}?access_token={{access_token}}

正常返回示例

```
"success":true,
"code":"200",
"message":null,
"requestId":"51331044-A2FE-474A-BA0B-BF84599D8AEE",
"data": null
```

新增权限

接口地址

POST /api/bff/v1.2/developer/ps/permission/create

```
接口说明
```

向当前的权限系统中新增一个权限。

IDaaS 权限系统可以维持一个属性接口,所以可以通过 parent Uuid 参数指定父级权限。

参数	类型	必须	示例值	描述
access_token	string	是	bd3a80ca-24c3-4d a8-836f-9efcb2c52c4b	
name	string	是	测试权限	权限名,最长64字符,不可为空

参数	类型	必须	示例值	描述
permissionValue	string	是	demo_permission	权限的权限值,同一个权限系统内 唯一,最长64个字符,不可为空
type	String	是	menu	menu 或者 button,代表菜单类 权限或按钮型权限,data 代表是 数据类型
psld	String	是	hU2czV4pMR	PS系统id
parentUuid	String	쥼	9b63a96ee5aa800641b5a4	父级权限全局唯一标识,资源外部 id,可以为null或者空字符 串,null或者空字符串代表顶级的 权限
remark	string	否	这是一个测试使用的权限	权限描述信息,可以为空,最 长255字符
clientToken	string	否	Kqji1 upjakhjdihq3e	IDaaS 幂等机制字段,由调用方自 动随机生成,标识一次请求操作。

参数	类型	示例值	描述
permissionUuid	string	7dabd9e92a175781072c265aeccfc0f6nm YAtFqciZ8	新生成的 全局唯一标识

示例

请求示例

{{your-idaas-domain}}/api/bff/v1.2/developer/ps/permission/create?access_token={{access_token}}

请求入参示例

```
{
    "type":"menu",
    "permissionValue":"demo_permission",
    "name":"测试权限",
    "remark":"这是一个测试使用的权限",
    "psId":"mkcwicd4pffhyd73"
```

正常返回示例

}

```
{
    "success":true,
    "code":"200",
    "message":null,
    "requestId":"51331044-A2FE-474A-BA0B-BF84599D8AEE",
        "data": {
            "permissionUuid": "7dabd9e92a175781072c265aeccfc0f6nmYAtFqciZ8"
        }
}
```

编辑权限

接口地址

PUT /api/bff/v1.2/developer/ps/permission/update?access_token={{access_token}}

接口说明

```
向当前的权限系统中编辑一个角色。
```

参数	类型	必须	示例值	描述
access_token	string	是	bd3a80ca-24c3-4da8-836f- 9efcb2c52c4b	

参数	类型	必须	示例值	描述
uuid	string	是	9b63a96ee5aa800641b5a4a	待编辑的权限全局唯一标识,资源 外部id
name	string	否	测试权限	权限名,最长64字符,为空代表不修 改
permissionValue	string	否	demo_permission	权限的权限值,同一个权限系统内 唯一,最长64个字符,为空代表不 修改
remark	string	否	这是一个测试使用的权限	权限描述信息
parent Uuid	string	否	9b63a96ee5aa800641b5a4a	父级权限全局唯一标识,资源外部 id,为 null 代表不修改,为空字符 传代表 修改为顶级节点
clientToken	string	否	Kqji1 upjakhjdihq3e	IDaaS 幂等机制字段,由调用方自 动随机生成,标识一次请求操作。

无。

示例

请求示例

{{your-idaas-domain}} /api/bff/v1.2/developer/ps/permission/update?access_token={{access_token}}

请求入参示例

```
{
   "type":"menu",
    "permissionValue":"demo_permission",
    -
"name":"测试权限",
    "remark":"这是一个测试使用的权限",
       "clientToken":"mkcwicd4pqfhyd73",
"psId":"hU2czV4pMR"
```

正常返回示例

}

```
{
   "success":true,
   "code":"200",
    "message":null,
   "requestId":"51331044-A2FE-474A-BA0B-BF84599D8AEE"
    "data": null
```

删除权限

接口地址

}

DELET E /api/bff/v1.2/developer/ps/permission/delete/{uuid}?access_token={{access_token}}

接口说明

请求参数

删除一个现有权限。注意,当拥有子权限时,不可直接删除。

参数	类型	必须	示例值	描述
access_token	string	是	bd3a80ca-24c3-4da8 -836f-9efcb2c52c4b	
uuid	String	是	447fed833d8739ecb1ca f6f38af14e65tthuiDBac88	待删除的角色全局唯一标识,资源 外部id

返回参数

无。

示例

}

{{your-idaas-domain}}/api/bff/v1.2/developer/ps/permission/delete/{{permissionUuid}}?access_token={{access_token}

正常返回示例

```
"success":true,
"code":"200",
"message":null,
"requestId":"51331044-A2FE-474A-BA0B-BF84599D8AEE"
"data": null
```

获取指定角色的已关联权限(分页)

接口地址

POST /api/bff/v1.2/developer/ps/role_permissions

接口说明

获取指定角色的所有已关联权限。

请求参数

参数	类型	必须	示例值	描述
access_token	string	是	bd3a80ca-24c3-4da8-836f- 9efcb2c52c4b	
roleUuid	String	ጽ	447fed833d8739ecb1c af6f38af14e65tthuiDBac88	指定角色 全局唯一标识,角色外部 id
currentPage	int	否	1	当前返回页数,从1开始
pageSize	int	否	10	每页数量
psld	Stirng	是	KSJDJSKkk	系统id,详情处可见

参数	类型	示例值	描述
List	Array		角色列表
uuid	string	4c9b9f14e82a5d4978d5ed22 9ec1ae4d6912xmCXA1l	权限 uuid
parentPermissionUuid	String	978d5ed229ec1ae4d6912xmC XA1l4c9b9f14e82a5d4	父级权限的 uui
name	string	测试权限	权限名,最长64字符,不可为空
permissionValue	string	test_permission	权限的权限值
relationUrl	string		暂无使用
remark	string	这是一个新的测试权限。	描述
type	boolean	menu	是否已启用
dataAccessRules	string		暂无使用
perPageSize	string	shanghonglin	创建人
currentPage	int	1	当前页数,从 1 开始

参数	类型	示例值	描述
totalSize	int	2	总角色数量
pageSize	int	10	一页包含的角色数量

示例

```
请求示例
```

{{your-idaas-domain}}}/api/bff/v1.2/developer/ps/role_permissions?access_token={{access_token}}

请求入参示例

```
{
    "roleUuid":"447fed833d8739ecb1caf6f38af14e65tthuiDBac88",
    "pageSize":"2",
    "psId":"hU2czV4pMR",
        "currentPage":"1"
}
```

正常返回示例

```
{
    "success": true,
    "code": "200",
    "message": null,
    "requestId": "D537580C-A5A2-4557-AEDD-3294DFB8ECE6",
    "data": {
        "list": [
            {
                 "uuid": "65f9e06df1a1cb04133845fd47e35196WUjqj9nkA1P",
                 "parentPermissionUuid": null,
                 "name": "打印-户籍卡",
                  "permissionValue": "print_card",
                 "remark": null,
"type": "menu",
             },
             {
                 "uuid": "540cf6e8b05b09b3938f865b33ab30d1GsMhz5NkVTq",
"parentPermissionUuid": "65f9e06df1a1cb04133845fd47e35196WUjqj9nkA1P",
"name": "本地的",
                 "permissionValue": "local",
                 "remark": null,
                  "type": "menu",
            }
        ],
        "totalSize": 2,
        "currentPage": 1,
        "pageSize": 10,
                "perPageSize": 10,
    }
}
```

把人授权到角色

接口地址

POST /api/bff/v1.2/developer/ps/role/modify_users?access_token={{access_token}}

接口说明

新增或者取消人和角色之间的授权关系

参数	类型	必须	示例值	描述
access_token	string	是	bd3a80ca-24c3-4da8-836f- 9efcb2c52c4b	
roleUuid	String	是	447fed833d8739e cb1caf6f38af1	指定角色 全局唯一标识,角色外部 id
attachedUDAccount UuidCollection	Array	否	["09b00e257ede 0a38a5f54a94"]	想要增加授权到该角色的账号全局 唯一标识数组

参数	类型	必须	示例值	描述
detachedUDAccountUuidCollecti on	Array	否	["09b00e257ede0a38a5f54a94"]	想要取消授权该角色的账号 全局唯 一标识数组
attachedUsernameCollection	Array	否	["zhang_san"]	想要增加授权到该角色的账号识数 组
detachedUsernameCollection	Array	否	["li_si"]	想要取消授权该角色的账号 数组

无。

示例

请求示例

{{your-idaas-domain}} /api/bff/v1.2/developer/ps/role/modify_users?access_token={{access_token}}

请求入参示例

```
{
   "attachedUDAccountUuidCollection":["09b00e257ede0a38a5f54a94c4d64000EwQtyG8nUWw"],
   "detachedUDAccountUuidCollection":["90d99090309433adeaf4a94c4d64000EwQtyG8nUWw"],
   "attachedUsernameCollection":["zhang_san","li_si",
   "detachedUsernameCollection":["wang_wu","zhao_liu"],
   "roleUuid":"447fed833d8739ecblcaf6f38af14e65tthuiDBac88"
}
```

正常返回示例

{

}

```
"success": true,
"code": "200",
"message": null,
"requestId": "D537580C-A5A2-4557-AEDD-3294DFB8ECE6"
"data": null
```

把权限关联到角色

接口地址

POST api/bff/v1.2/developer/ps/role/modify_permissions?access_token={{access_token}}

接口说明

建立权限和角色之间的关联关系。

请求参数

参数	类型	必须	示例值	描述
access_token	string	是	bd3a80ca-24c3-4da8-836f- 9efcb2c52c4b	
roleUuid	String	是	447fed833d8739ecb1 caf6f38af1	指定角色 全局唯一标识,角色外部 id
attachedPermissionUuid Collection	Array	否	["tyG8nUWw"]	想要新増权限 全局唯一标识数组, 资源外部id
detachedPermissionUuid Collection	Array	ሸ	["tyG8nUWw"]	想要取消权限 全局唯一标识数组, 资源外部id

返回参数

无。

示例

请求示例

{{your-idaas-domain}} api/bff/v1.2/developer/ps/role/modify_permissions?access_token={{access_token}}

请求入参示例

}

{

}

"roleUuid":"447fed833d8739ecblcaf6f38af14e65tthuiDBac88", "attachedPermissionUuidCollection":["65f9e06df1a1cb04133845fd47e35196WUjqj9nkA1P","540cf6e8b05b09b3938f865b33ab30d1GsMhz5NkVTq"], "detachedPermissionUuidCollection":["12f9e06df1a1cb04166666fd47e35196WUjqj9nkAee","340cf6e8b05b09b397890qeb33ab30d1GsMhz5NkVar"] 正常返回示例 "success": true, "code": "200",

"message": null, "requestId": "D537580C-A5A2-4557-AEDD-3294DFB8ECE6" "data": null

获取指定权限节点下,用户已授权的权限

接口地址

POST /api/bff/v1.2/developer/ps/listSubLevelPermissions

接口说明

获取一个指定权限节点下,一个用户的所有已授权的权限。

请求参数

参数	类型	必须	示例值	描述
access_token	string	是	bd3a80ca-24c3-4da8-836f- 9efcb2c52c4b	
username	string	是	michael	指定用户的账户名
permissionValue	String	否	print_card	指定父级权限节点的权限值
psid	String	是	SAFKJkljL	系统详情处可见
type	String	否	ALL,button,menu	权限类型

参数	类型	示例值	描述
permissions	Array		角色列表
uuid	string	4c9b9f14e82a5d4978d5ed229ec 1ae4d6912xmCXA1l	权限 uuid
parentPermissionUuid	String	978d5ed229ec1ae4d6912xmC XA1l4c9b9f14e82a5d4	父级权限的 uuid
name	string	测试权限	权限名,最长64字符,不可为空
permissionValue	string	test_permission	权限的权限值
remark	string	这是一个测试权限。	权限说明
type	string	button	权限类型,菜单/按钮
dat a Access Rules	string		暂无使用
relationUrl	stirng	http://your-domain.com	业务系统主页地址
displayOrder	long	0	资源排序号,整数,用于排序使用,数字越 小越靠前展示

身份管理服务公共云合集·IDaaS 旧版 文档

参数	类型	示例值	描述
children	Array	当前资源的子级资源	当前资源的直属子级资源列表

示例

请求示例

{{your-idaas-domain}}}/api/bff/v1.2/developer/ps/listSubLevelPermissions?access_token={{access_token}}

请求入参示例

```
{
"username":"michael",
"permissionValue":"print_card",
"psId":"hU2czV4pMR"
```

正常返回示例

}

```
{
    "success": true,
"code": "200",
"message": null,
     "requestId": "D537580C-A5A2-4557-AEDD-3294DFB8ECE6",
     "data": {
         "permissions": [
              {
                   "uuid": "65f9e06df1a1cb04133845fd47e35196WUjqj9nkA1P",
                   "parentPermissionUuid": null,
"name": "打印—户籍卡",
                    "permissionValue": "print_card",
                    "remark": null,
                    "type": "menu",
               },
               {
                    "uuid": "540cf6e8b05b09b3938f865b33ab30d1GsMhz5NkVTq",
"parentPermissionUuid": "65f9e06df1a1cb04133845fd47e35196WUjqj9nkAlP",
                    "name": "本地的",
                    "permissionValue": "local",
                    "remark": null,
"type": "menu",
              }
        ]
    }
}
```

获取角色所有已授权用户 (分页)

接口地址

POST /api/bff/v1.2/developer/ps/role_users 接口说明 获取角色所有已授权用户。

请求参数

参数	类型	必须	示例值	描述
access_token	string	是	bd3a80ca-24c3-4da8-836f- 9efcb2c52c4b	
roleUuid	String	否	447fed833d8739ecb1caf6f38af 14e65tthuiDBac88	指定角色 全局唯一标识,角色外部 id
currentPage	int	否	1	当前返回页数,从1开始
pageSize	int	否	10	每页数量
psld	String	是	SAFJASJk	系统id,详情处可见

应用身份服务

参数	类型	示例值	描述
list	Array		角色列表
udAccountUuid	String	978d5ed229ec1ae4d6912xmCX A1l4c9b9f14e82a5d4	IDaaS 系统内 UDAccount 的全局唯一标识
username	string	michael	用户名
displayName	string	Michael Dis	显示名称
perPageSize	int	10	每一页显示的用户数
totalSize	int	2	角色授权的用户数
psld	string	XuJNOLtDam	系统id,详情处可见
roleUuid	string	b661f136fbde1c895b44eda7111ab458s7 36vCvD8aB	IDaaS 系统内 角色的全局唯一标识
currentPage	int	1	查询第几页的数据,从1开始
pageSize	int	10	每一页显示的用户数

示例

请求示例

{{your-idaas-domain}}}/api/bff/v1.2/developer/ps/role_users?access_token={{access_token}}

请求入参示例

```
{
    "roleUuid":"447fed833d8739ecb1caf6f38af14e65tthuiDBac88",
    "psId":"SAFJASJk",
    "currentPage":"1",
    "pageSize":"10",
}
```

正常返回示例

```
{
    "success": true,
     "code": "200",
     "message": null,
     "requestId": "D537580C-A5A2-4557-AEDD-3294DFB8ECE6",
     "data": {
         "list": [
            {
    "udAccountUuid": "09b00e257ede0a38a5f54a94c4d64000EwQtyG8nUWw",
                 "username": "fufu033",
"displayName": "付付023",
             },
             {
                  "udAccountUuid": "dab27222a6cd330ff25dc4b6c4a21dcarH8a17zqk3z",
                  "username": "michael",
                  "displayName": "Michael_updated",
             }
         ],
                "psid":"XuJNOLtDam",
"roleUuid":"b661f136fbdelc895b44eda7111ab458s736vCvD8aB"
         "totalSize": 2,
         "currentPage": 1,
"perPageSize": 10,
"pageSize": 10
    }
}
```

获取权限系统指定用户的角色和权限

接口地址

POST /api/bff/v1.2/developer/ps/user_role_permissions

接口说明

获取用户已授权的角色和权限。

请求参数

参数	类型	必须	示例值	描述
access_token	string	是	bd3a80ca-24c3-4da8-836f- 9efcb2c52c4b	
username	String	是	Zhangsan	指定的用户名
psld	String	是	SAFJASJk	系统id,详情处可见

参数	类型	示例值	描述
username	string	Zhangsan	指定的用户名
rolePermissions	Array		用户拥有的角色及权限集合
uuid	string		IDaaS系统内角色的全局唯一标识
name	string		IDaaS系统内角色的
permissionValue	string		IDaaS系统内角色的权限值
remark	string		IDaaS系统内角色的描述
enabled	boolean		IDaaS系统内角色的状态,true为启用,
permissions	Array		角色拥有的权限列表
uuid	string	978d5ed229ec1ae4d6912xmCX A1l4c9b9f14e82a5d4	IDaaS 系统内 权限的全局唯一标识
name	string	Add用户	权限relationUrl
remark	string	Add user test	备注
permissionValue	string	ADD	权限值
type	string	Menu	类型, menu, button等
dataAccessRules	string		暂无使用
permission	Array		账户拥有的所有权限列表
uuid	string	978d5ed229ec1ae4d6912xmCX A1l4c9b9f14e82a5d4	IDaaS 系统内 权限的全局唯一标识
name	string	Add用户	权限名称
relationUrl	string		暂无使用
remark	string	Add user test	备注
permissionValue	string	ADD	权限值

参数	类型	示例值	描述
type	string	Menu	类型, menu, button等
dataAccessRules	string		暂无使用
roles	Array		角色列表,暂时不返回参数

示例

```
请求示例
```

{{your-idaas-domain}}}/api/bff/v1.2/developer/ps/user_role_permissions?access_token={{access_token}}

请求入参示例

```
{
"psId":"SAFJASJk",
"username":"michael"
}
```

正常返回示例

```
{
    "success": true,
    "code": "200",
    "message": null,
    "requestId": "BC8EF781-56CA-4EA4-95FB-BE19A9832A84",
    "data": {
        "username": "test007",
        "rolePermissions": [
            {
                 "uuid": "58e146dd8def3b9052411ba408bf8a5bDnUgQB07md2",
                 "name": "审计管理员",
"permissionValue": "audit_admin",
                 -
"remark": "权限接口创建的角色",
                 "enabled": true,
                 "permissions": [
                     {
                         "uuid": "67af927c55941dd4742a3019ff3a9641hqRqvIdzuIG",
                          "parentPermissionUuid": null,
                         "name": "审计",
                         "permissionValue": "audit",
"relationUrl": null,
"remark": "通过接口创建权限资源",
"type": "menu",
                          "dataAccessRules": []
                     }
               ]
         1
         "permissions": [
                    {
                         "uuid": "67af927c55941dd4742a3019ff3a9641hqRqvIdzuIG",
                          "parentPermissionUuid": null,
                          "name": "审计",
                         "permissionValue": "audit",
"relationUrl": null,
                          "remark": "通过接口创建权限资源",
                          "type": "menu",
                          "dataAccessRules": []
                     }
               ]
        "roles": [
       1
   }
}
```

判断用户是否有角色

接口地址 POST /api/bff/v1.2/developer/ps/has_role 接口说明 判断用户是否拥有某角色。

参数	类型	必须	示例值	描述
access_token	string	是	bd3a80ca-24c3-4da8-836f- 9efcb2c52c4b	
roleUuid	String	是	540cf6e8b05b09b393 8f865b33ab30d1	指定角色全局唯一标识,角色外部 id
username	String	是	michael	指定账号的账户名
psld	String	是	SAFJASJk	系统id,详情处可见

```
无
```

```
示例
```

请求示例

{{your-idaas-domain}}}/api/bff/v1.2/developer/ps/has_role?access_token={{access_token}}

请求入参示例

```
{
   "roleUuid": "540cf6e8b05b09b3938f865b33ab30d1GsMhz5NkVTq",
     "psId":"SAFJASJk",
     "username": "michael"
```

}

正常返回示例

```
{
    "success": true,
    "code": "200",
    "message": null,
    "requestId": "76C29BF5-3236-4C17-9C0D-92834AC12B73",
"data": false
```

根据权限uuid判断用户是否有权限

接口地址

}

POST /api/bff/v1.2/developer/ps/has_permission

接口说明

判断用户是否拥有某权限。

请求参数

参数	类型	必须	示例值	描述
access_token	string	是	bd3a80ca-24c3-4da8-836f- 9efcb2c52c4b	
permissionUuid	String	是	447fed833d8739ecb1caf6f38af 14e65tthuiDBac88	指定权限全局唯一标识,资源外部 id
username	String	是	michael	指定账号的账户名
psld	String	是	ASFjasds	系统id,系统详情处可见

返回参数

参数	类型	必须	示例值	描述
hasPermission	Boolean	是	false	是否已有授权关系

根据权限值判断用户是否有权限

接口地址

POST /api/bff/v1.2/developer/ps/isUserHasPermission

接口说明

通过权限值来判断用户是否拥有某权限/角色。

请求参数

参数	类型	必须	示例值	描述
access_token	string	是	bd3a80ca-24c3-4da8-836f- 9efcb2c52c4b	
permissionValue	String	是	test_permission	指定权限的权限值
username	String	是	09b00e257ede0a38a5f54a94c4 d 64000EwQtyG8nUWw	指定账号的用户名
psld	String	是	KDJDJSSKK	系统id,详情处可见

返回参数

参数	类型	必须	示例值	描述
hasPermission	Boolean	是	false	是否已有授权关系

示例

请求示例

{{your-idaas-domain}}}/api/bff/v1.2/developer/ps/isUserHasPermission?access_token={{access_token}}

请求入参示例

```
{
    "permissionValue": "print_card",
    "psId":"KDJDJSSKK",
    "username": "michael"
```

}

{

正常返回示例

FAQ

}

1. 下图中的Account uuid如何获取

把人授权到角色

接口地址

POST /api/bff/v1.2/developer/ps/role/modify_users?access_token={{access_token}} 接口说明 新增或者取消人和角色之间的授权关系

请求参数

参数	类型	必须	示例值	描述
access_token	string	是	bd3a80ca-24c3- 4da8-836f- 9efcb2c52c4b	
roleUuid	String	是	447fed833d8739e cb1caf6f38af1	指定角色 全局唯一 标识,角色外部id
attachedUDAccount UuidCollection	Array	否	["09b00e257ede 0a38a5f54a94"]	想要增加授权到该角 色的账号全局唯一标 识数组
detachedUDAccoun tUuidCollection	Array	否	["09b00e257ede0a3 8a5f54a94"]	想要取消授权该角色 的账号 全局唯一标 识数组
attachedUsernameC ollection	Array	否	["zhang_san"]	想要增加授权到该角 色的账号识数组
detachedUsername Collection	Array	否	["li_si"]	想要取消授权该角色 的账号 数组

按F12打开控制台,访问账户的详情,查看uuid

概范 30.0 HEAL / 30.0 HEAL 快速入门 ← 账户详情 (zb05) 应用 账户信息 已授权应用 应用子账户 隶属于组织机构 设备 报表 实名认证信息 应用列表 添加应用 基础信息 账户 机构及组 账户名称 zb05 显示名称 邮箱 z434 Ciange iun.com (+86)18321 手机号码 账户状态 正常 日录 账户管理 分类管理 账户类型 白建账户 外部ID 15150932055 创建日期 2020/9/22 下午2:36:00 过期时间 21版-1230(修改) 二次认证 禁用 认证 认证源 RADIUS 扩展信息 证书管理 授权 权限系统 证书信息 < 2 2023-09-22 2020/922 下午2-36-28 Tue Sep 22 2020 14-36-28 GMT+0800 (中国标准时间) 证书有效期 14151 证书生成时间 其它管理 SubjectDN CN=zb05, L=BJ, ST=BJ, O=IDSMANAGER, OU=IDaaS, C=CN 设置 第三方账户绑定 400 ms 450 ms 500 ms 550 ms 600 ms 650 ms 700 ms 750 ms 800 ms 850 ms 900 ms 950 ms K Headers Proview Response Cookies Timing
 Ise, "Admin":felse, "DictioneryList":[], "Locked":felse, "DuDire "+66" "licentd"-"1515003200158135754" "DicnlayNeme"-"+634" "DhoneN Detail.json?data=%78%22UserUuid%221%22...2ApiVersion%221%22v1.2%22%7D... ata=%78%22lortanc_2&ni//e on%22:%22v1.2%22%7D

建议使用username字段,直接对应账户名称。

接口地址

POST /api/bff/v1.2/developer/ps/role/modify_users?access_token={{access_token}} 接口说明 新增或者取消人和角色之间的授权关系

请求参数

参数	类型	必须	示例值	描述
access_token	string	是	bd3a80ca-24c3- 4da8-836f- 9efcb2c52c4b	
roleUuid	String	是	447fed833d8739e cb1caf6f38af1	指定角色 全局唯一 标识,角色外部id
attachedUDAccount UuidCollection	Array	否	["09b00e257ede 0a38a5f54a94"]	想要增加授权到该角 色的账号全局唯一标 识数组
detachedUDAccoun tUuidCollection	Array	否	["09b00e257ede0a3 8a5f54a94"]	想要取消授权该角色 的账号 全局唯一标 识数组
attachedUsernameC ollection	Array	否	["zhang_san"]	想要增加授权到该角 色的账号识数组
detachedUsername Collection	Array	否	["li_si"]	想要取消授权该角色 的账号 数组

←账户详情 (zb05)

- ////		/							
账户信息	已授权应用	应用子账户	隶属于组织机构	设备	报表	实名认证信息			
基础信息									
账户名称	zb05						显示名称	Zź	
手机号码	(+86)	8					账户状态	П	
账户类型	自建账	户					外部ID	1!	
过期时间	2116-1	2-31(修改)					二次认证	寿	
扩展信息									
证书信息									
证书有效期	2023-0	19-22							
证书生成时间	Mi 2020/9/22 下午2:36:28 Tue Sep 22 2020 14:36:28 GMT+0800 (中国标准时间)								

3.2.5. 权限系统相关FAQ

权限系统角色关联授权规则

- 1. 默认系统,开发者角色可以关联所有用户,其它角色只能关联管理员
- 2. 自建系统,所以角色可以关联所有用户

是否支持分级管理

CubicotDM

目前公有云的 IDaaS 暂时不支持分级管理。如果您近期有相关的需求,可以<mark>联系我们</mark>进行咨询。线下交付独立部署的IDaaS是可以支持分级管理的。