ALIBABA CLOUD

阿里云

应用身份服务

身份管理服务公共云合集

文档版本：20220707

阿里云

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。

1. 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。

2. 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。

3. 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。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 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，不是用户必须了解的内容。	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，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 list --instanceid` *Instance_ID*
[] 或者 [a|b]	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

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。

- **低门槛**：上手容易、免费开通、预算经济
- **云原生**：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。

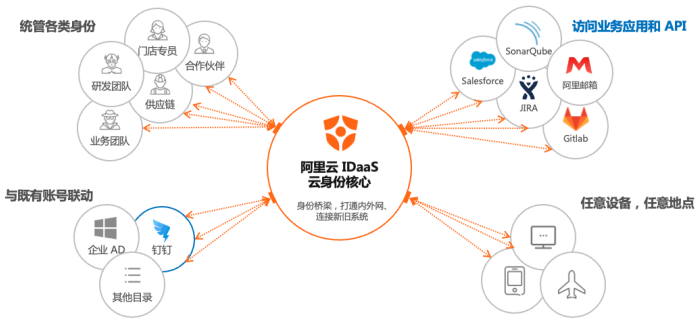
核心能力

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。

> 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。

CIAM 用户身份权限管理（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：安全认证整体介绍。

1.1.2. IDaaS 术语表

产品相关

IDaaS

Identity-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。

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

Identity 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

IdP-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（IdP）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 IdP 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。

OTP

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。

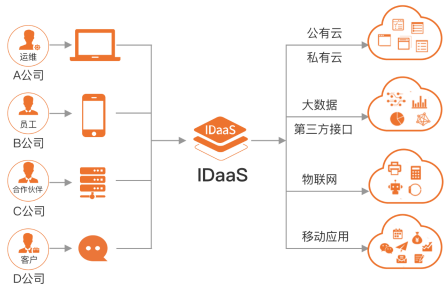
IDaaS 可以将研发、运维工作相关的应用尽数打通，实现一套账户登录、统一授权管理。安全价值高，配置简化，效率高。

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。

IDaaS 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

现阶段不计费。

IDaaS 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。

IDaaS 2.0 会提供如下版本：

- **免费版。**IDaaS 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，新版本是不兼容更新，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。

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。
应用	应用市场	积累应用模板	不支持	支持
		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
	应用管理	应用列表	支持	支持
		应用生命周期	支持	支持
		子账户管理	支持	支持
		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	账户管理	账户列表	支持	支持
		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
		单个账户同步	支持	开发中，暂不支持触发单个账户同步。
	组织架构	组织树形管理	支持	支持
		组织生命周期管理	支持	支持
		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
认证	登录方式/认证源	登录方式模板	支持	支持
		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
		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	应用授权	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
		按应用授权账户	支持	支持
		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
其他	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
	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。

“**默认安全**”的设计理念：在“**可用性**”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“**易用性**”。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“**开箱即安全**”。

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。

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。

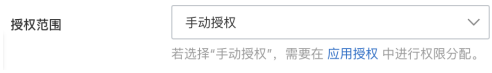
IDaaS 在如下操作中预置了风控埋点，覆盖了对访问、对开发、对数据最敏感的一些场景。

- 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

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。

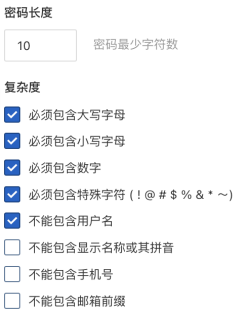


新创建出来的应用，在管理员明确其授权范围前，无人可以访问。以最小权限原则，避免应用访问权限的泛滥问题。

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。



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。

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。

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。

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

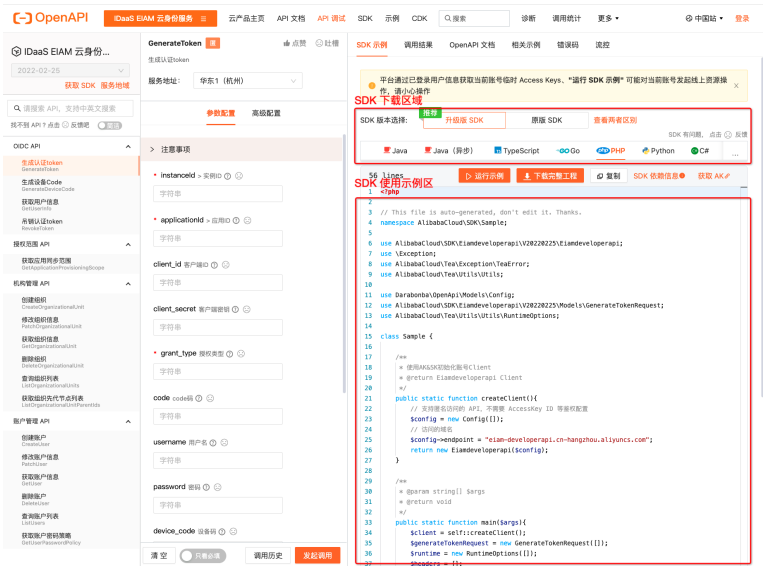
针对不同场景，IDaaS 提供管理说明文档、开发说明文档和 SDK 及样本代码，汇总如下：

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。

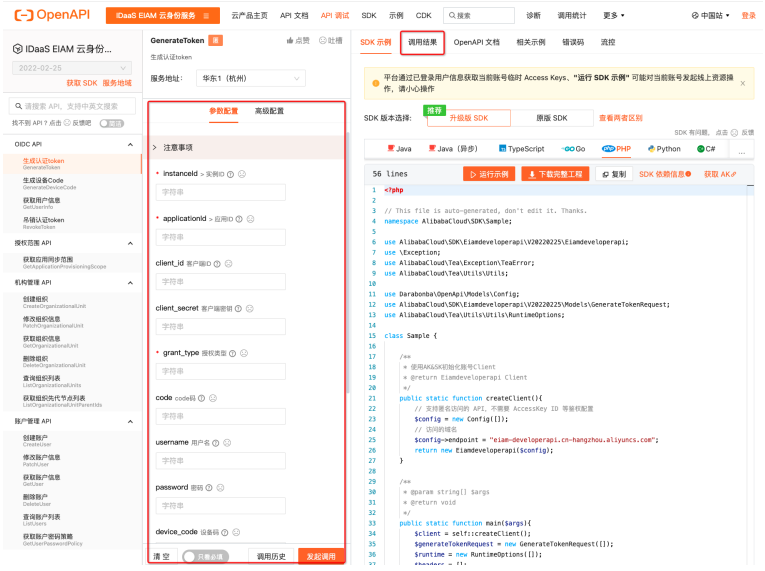
可以前往 阿里云 IDaaS API 开发者平台，在左侧可切换到不同接口，在右侧可选择对应语言【下载完整工程】，参照其中代码实现 SDK 安装、应用和调用。



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 阿里云 IDaaS API 开发者平台 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。

在实例列表页点击【免费创建实例】，勾选协议后直接创建即可。

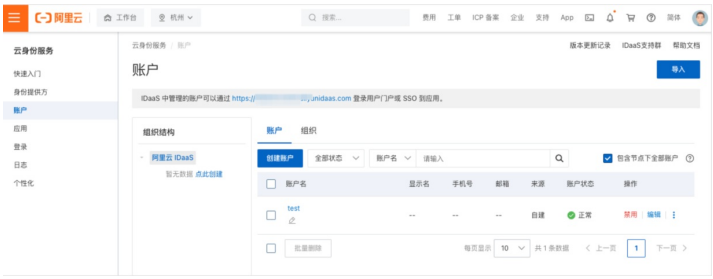
实例创建会瞬时完成。创建成功后，点击实例 ID 或【访问控制台】，前往 IDaaS 管理控制台。

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。



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。

> 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。

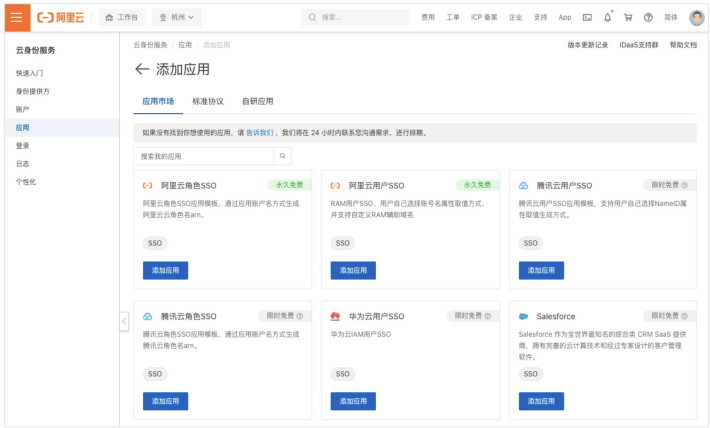
本文将以配置【阿里云用户 SSO】应用为例，实现 IDaaS 账户登录到阿里云控制台。

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。

> 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。

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。

> 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。

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：IDaaS 账户名。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：手动授权。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。

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。

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。

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	• 将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
三方应用方案（快速绑定钉钉）	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。 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。
一方应用方案（钉钉高级配置）	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： • 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。

第一步 选择场景

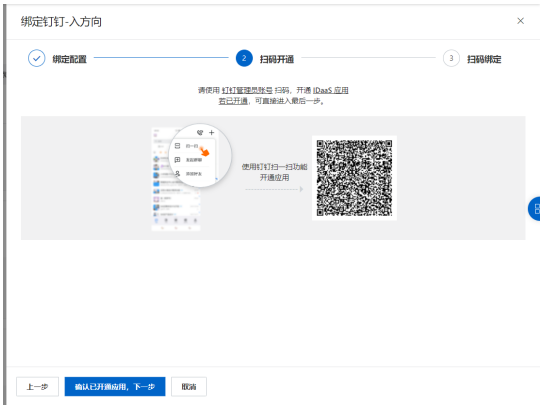
在第一步中，选择希望和钉钉实现的场景能力，若无偏好，可直接下一步。

能力说明

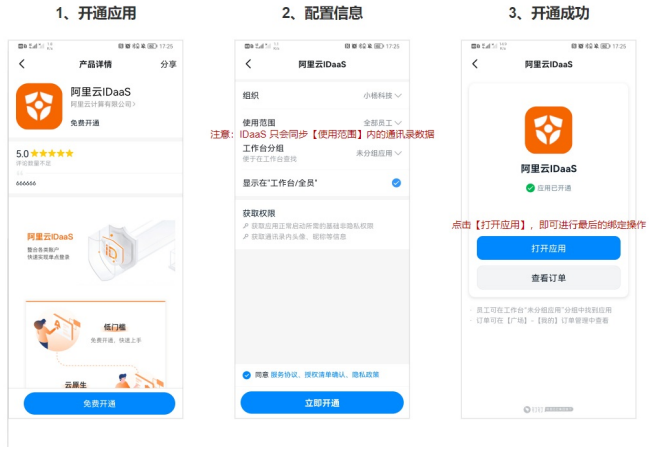
- **同步目标**：钉钉的通讯录数据将会导入到 IDaaS 的这个节点之下。
- **增量同步**：启用后，IDaaS 调用钉钉接口，监听钉钉通讯录事件。钉钉通讯录有变动，可实时将变动数据同步到 IDaaS 中。
  - 从钉钉导入的账户，IDaaS 会默认使用其钉钉 userId 与 IDaaS 账户进行匹配（可在字段映射中自定义规则），如果匹配成功，将覆盖更新，否则将创建账户。
  - 建议在增量同步前进行一次全量同步，否则部分数据可能会同步失败。
  - 单条记录无法导入，不影响其他数据导入。
  - 失败信息可在【同步日志】中查看。
- **钉钉扫码登录**：勾选后，会在【登录】菜单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



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。

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。

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。

查看导入状态

- **导入提示**：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。
- **手机号/邮箱缺失处理**：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

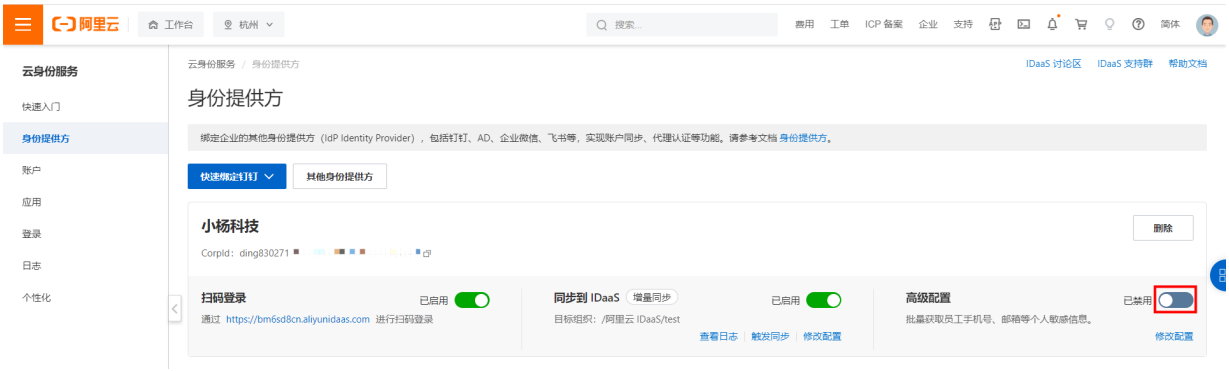
IDaaS 支持绑定多个钉钉通讯录，只需用不同的钉钉企业管理员，按照上述扫码开通流程即可完成。

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。

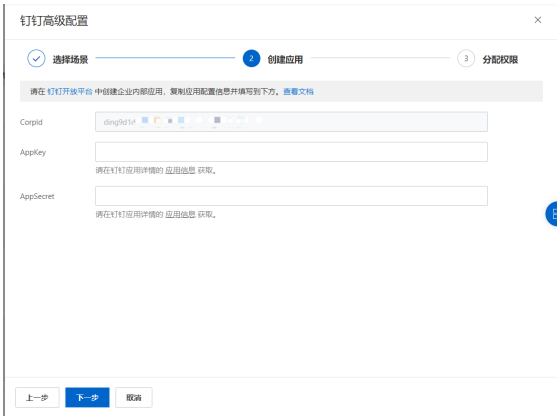


第一步 选择场景

在第一步中，目前暂不开放配置能力，可直接下一步。

第二步 创建应用

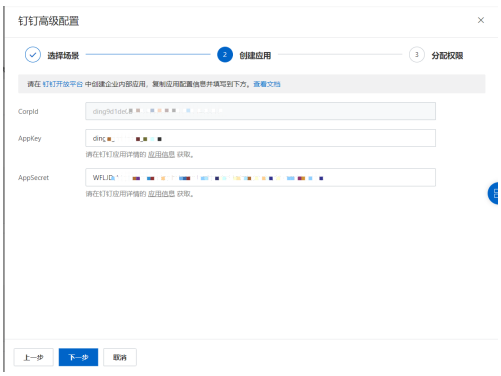
在第二步中需要将钉钉中的应用信息配置到 IDaaS 中。



登录 钉钉开放平台-企业内部开发，点击【创建应用】，填写企业内部应用的基本信息。

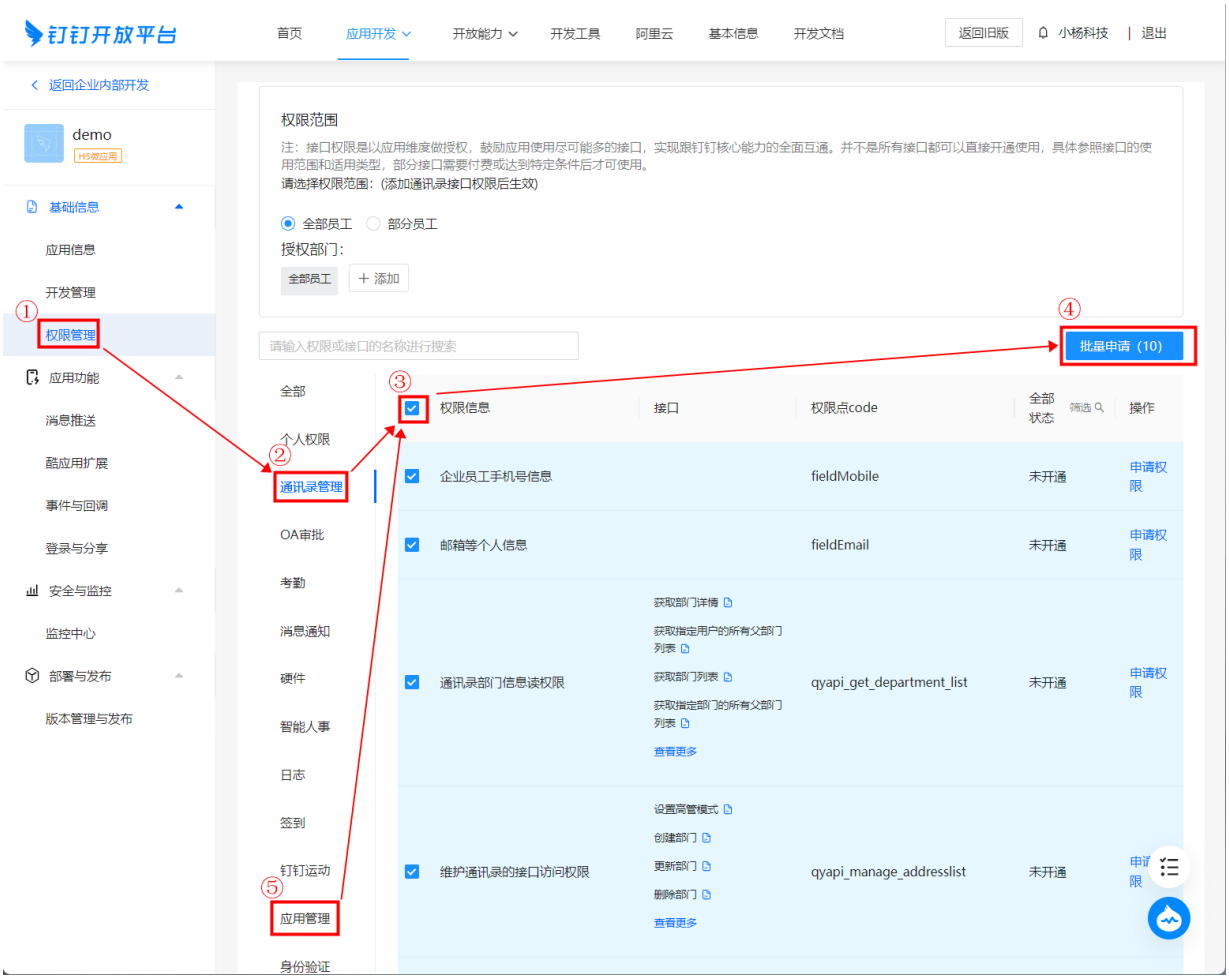
完成创建后，将自动跳转到钉钉的应用详情页。依次将 AppKey 和 AppSecret 复制粘贴到 IDaaS 中。

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。



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】。



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。

> 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

由于该应用主要用于同步数据而不用于员工日常使用，【应用首页地址】填写任意地址即可。

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 字段映射 中进行配置。

1.4.1.2. 绑定钉钉-出方向

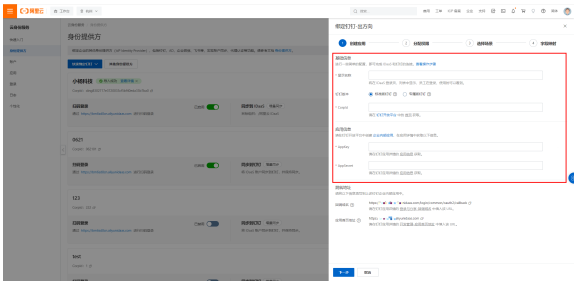
介绍绑定钉钉-出方向的操作步骤。

快速绑定钉钉

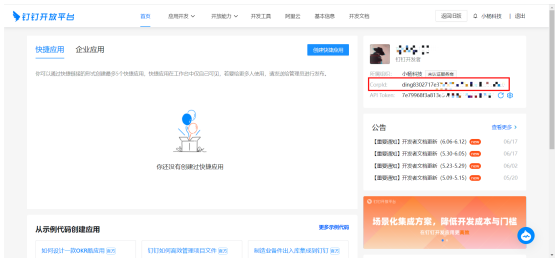
在【快速入门】或【身份提供方】菜单中，点击【快速绑定钉钉】，即可开始快速绑定钉钉-出方向流程。

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。
- CorpId：在 钉钉开放平台-首页 获取。

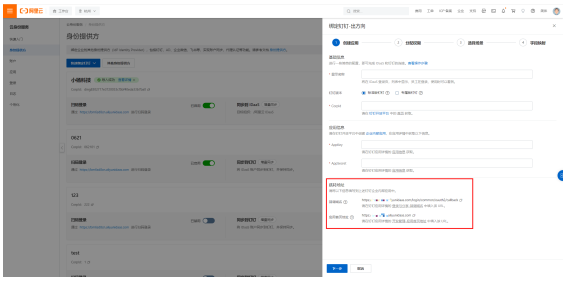


- AppKey/AppSecret。

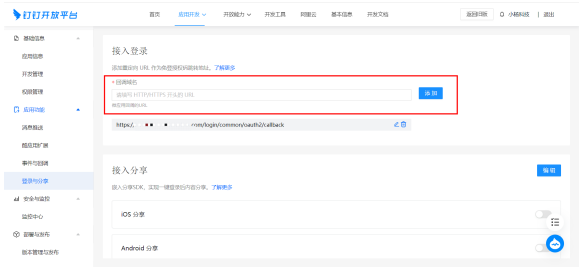
- 在 钉钉开放平台-企业内部开发 中创建应用。

- 在应用详情中获取 AppKey/AppSecret。

您还需要将以下信息填到到钉钉中：



- **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 IDaaS。

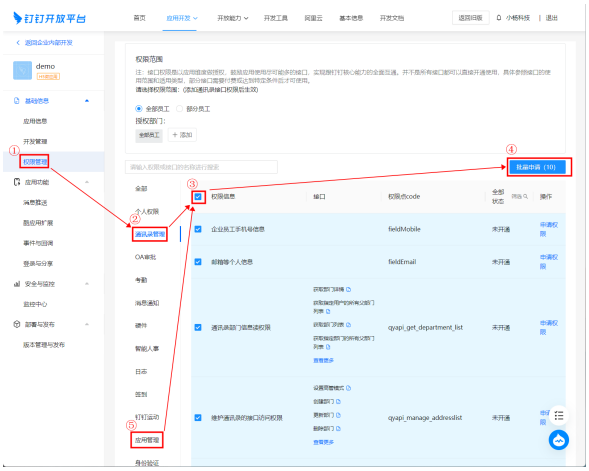


- **应用首页地址**：填写到应用详情中的 登录与分享-回调域名。配置该字段后，用户在钉钉控制台点击该应用时（在 版本管理与发布 中可以设置应用的可见范围），可以单点登录到 IDaaS 应用门户。

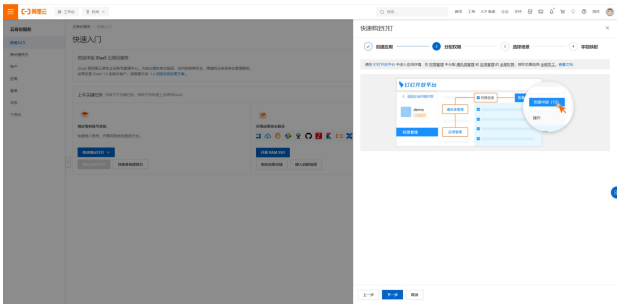
> 说明
>
> 如果您希望只有 IDaaS 可以请求该钉钉应用，请在该钉钉应用页面的【开发管理】中填写【服务器出口IP】：
>
> 112.124.239.96,112.124.239.101,112.124.239.100,112.124.239.99,112.124.239.98,112.124.239.97,112.124.239.105,112.124.239.104,112.124.239.103,112.124.239.10

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】。

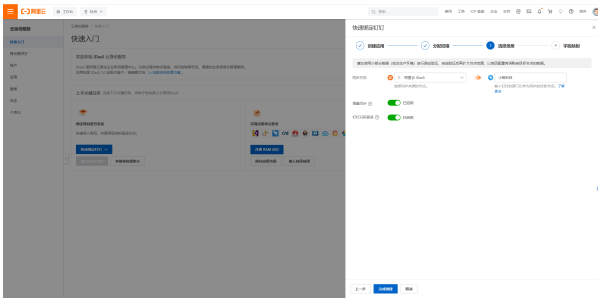


完成授权后，在 IDaaS 中点击【下一步】按钮，IDaaS 将检查该应用是否拥有钉钉通讯录管理权限，检查通过则完成了配置。



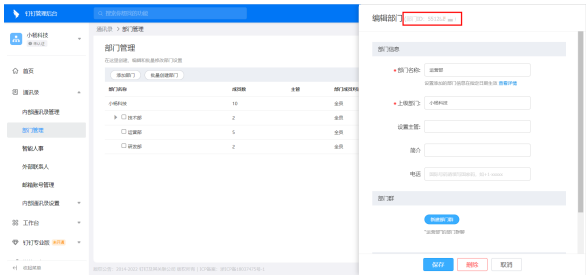
第三步 选择场景

在第三步中，选择希望和钉钉实现的场景能力。



能力说明

- **同步目标**：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。

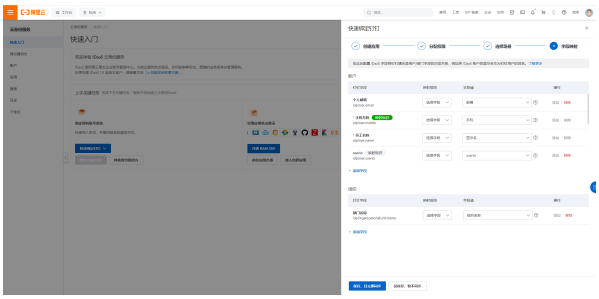


- **增量同步**：启用后，当 IDaaS 账户/组织数据有变动时，将实时将变动数据同步到钉钉通讯录中。导出到钉钉的账户，IDaaS 会根据第四步【字段映射】中的【映射标识】与钉钉用户进行匹配（可在字段映射中自定义规则），如果匹配成功，将覆盖更新，否则将创建账户。
- **钉钉扫码登录**：勾选后，会在【登录】菜单中创建【钉钉扫码登录】，并处于启用状态，用户可直接扫码登录。

> 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。

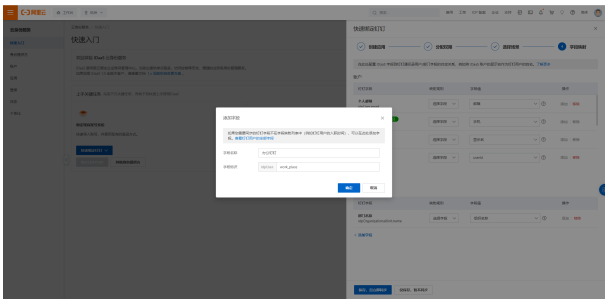
第四步 字段映射

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。



> 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】。



- **字段名称**：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：

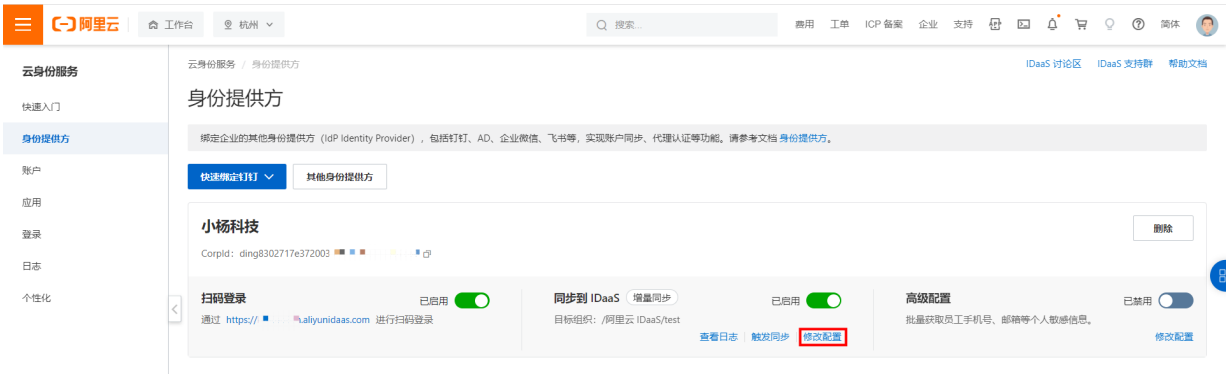
- **账户层面**：通过**账户绑定关系**将账户的**状态**保持一致。以导入钉钉通讯录为例，如果某个钉钉用户与 IDaaS 账户建立了绑定关系，在钉钉删除该用户时，在 IDaaS 中也会删除对应的账户。
- **字段层面**：在账户绑定关系的基础上，通过**字段映射关系**将账户的**信息**保持一致。以导入钉钉通讯录为例，如果将钉钉用户的企业邮箱作为 IDaaS 账户的显示名，当钉钉用户的企业邮箱修改时，IDaaS 账户的显示名也会修改。

> 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

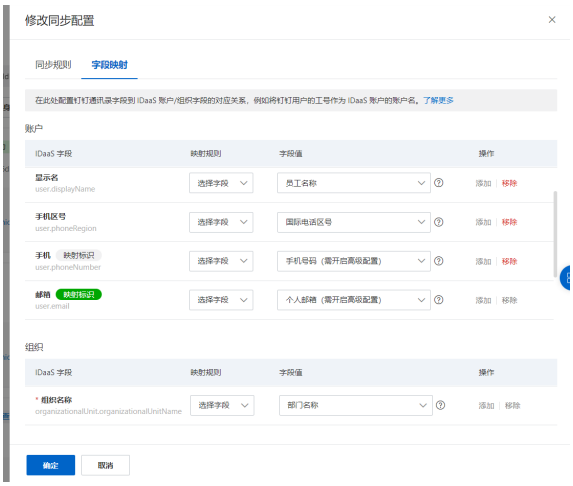
您可以通过两个入口配置字段映射：

- **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。



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。



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：SubstringBefore(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.userId。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

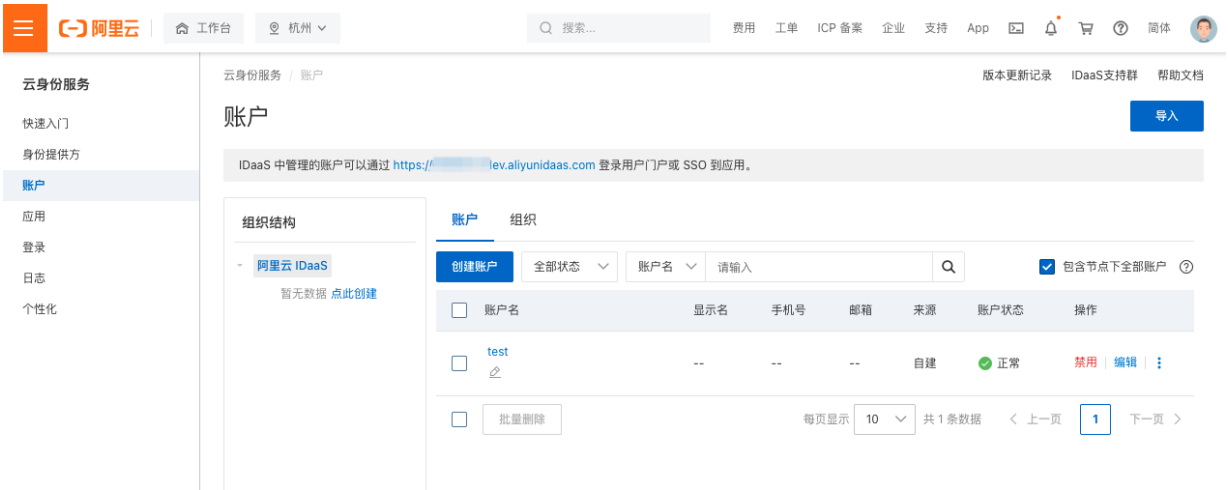
1.4.2.1. 创建账户/组织

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：绑定钉钉。 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：2. 创建账户。
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。

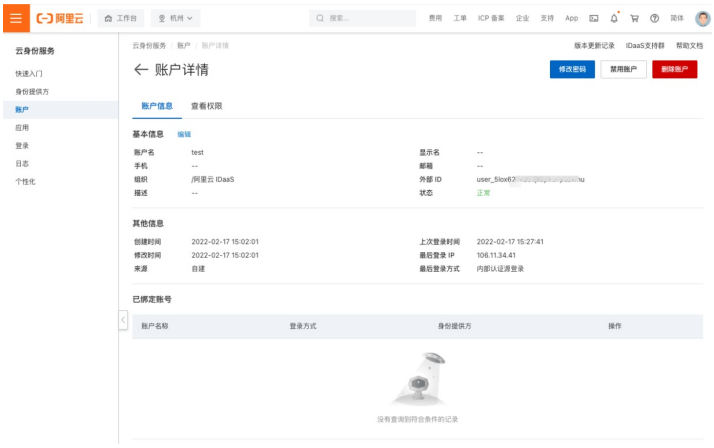


1.4.2.2. 账户详情

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。

> 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。



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 userId，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。

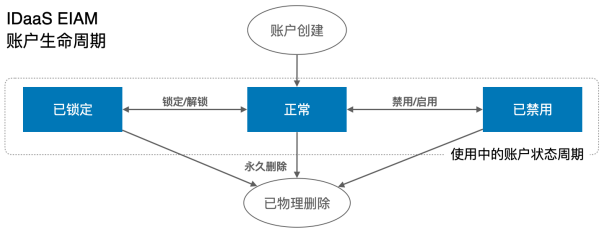
修改密码

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。

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. **查看**。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. **同步**。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。

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：

- **入方向**：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	IdP 身份提供方	当前支持钉钉。操作参考：绑定钉钉。 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：应用开发 API 说明。
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 IDaaS 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

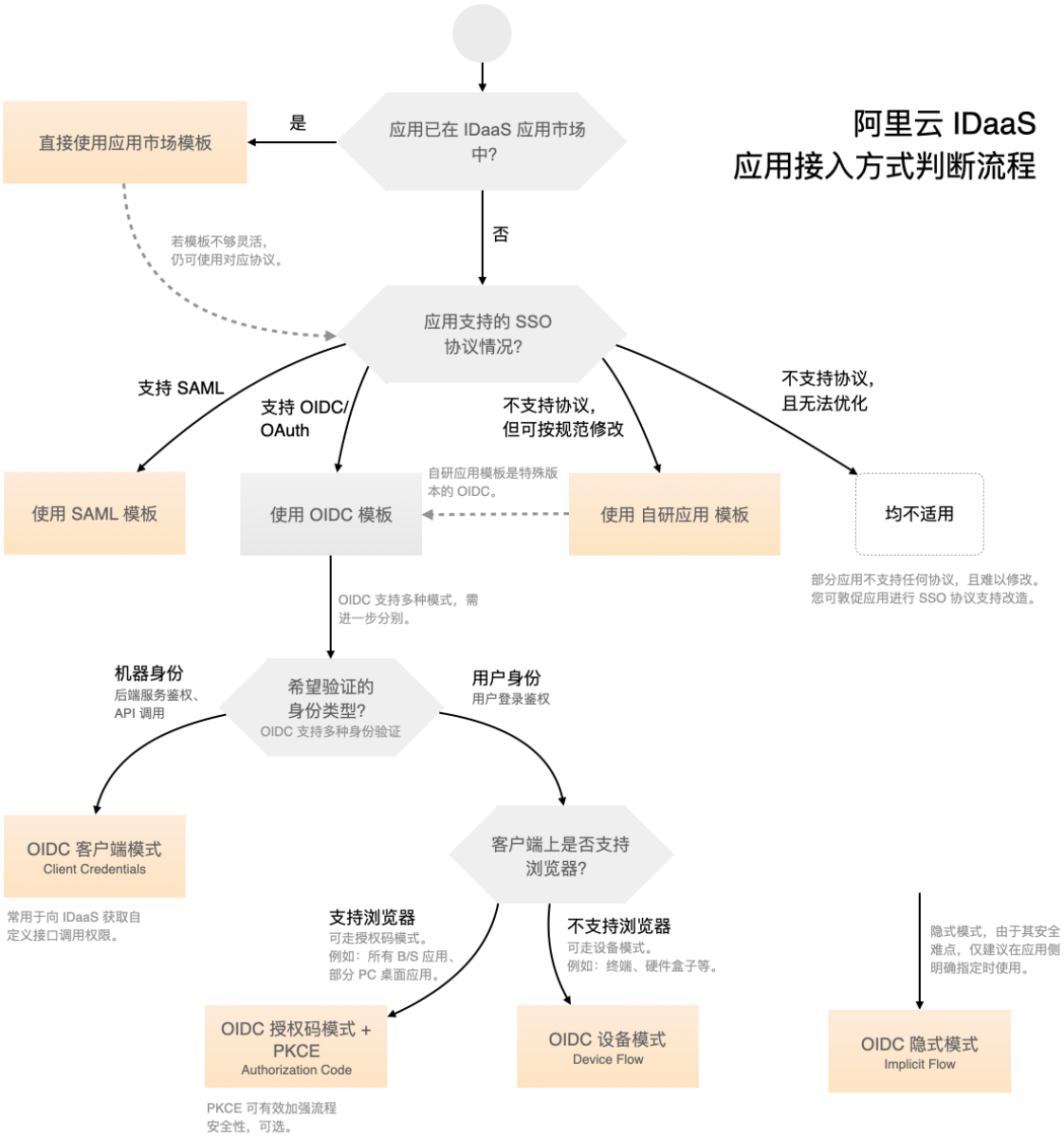
1.4.3.1. 应用开通说明

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。



1.4.3.2. 1. 应用市场

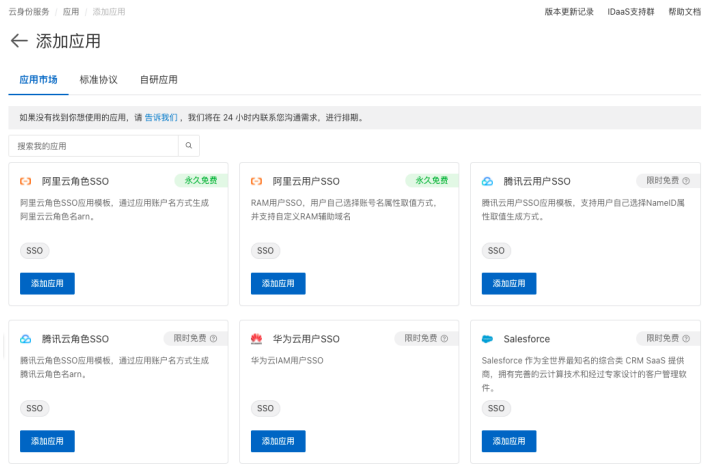
应用市场

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。



> 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 IdP（在我们的语境中，IdP 就是 IDaaS）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。

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。

CAS 未来版本	CAS （Central Authentication Service）3.0 发布于2013 年，CAS 由耶鲁大学制定维护，在诸多应用中均有支持。

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。

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：

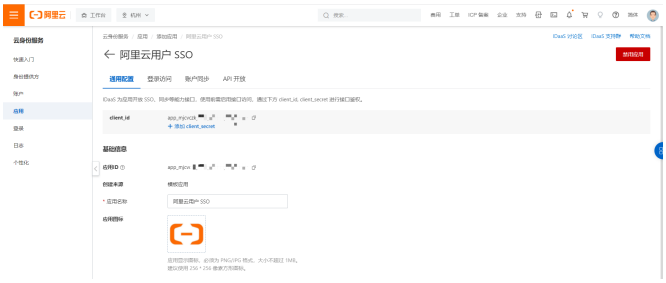
接入层次	说明	价值
第一层：登录统一	实现单点登录（SSO）。通过接入 OIDC 协议，配置应用账户和应用授权，允许 IDaaS 中的企业账户单点登录到应用中。 开发文档：自研应用接入单点登录。	员工一套账户，畅游所有应用。 统一授权、统一管理、统一行为审计。
第二层：账户统一	实现账户同步。通过对接 IDaaS 同步接口，打通身份孤岛。 开发文档：自研应用接入账户同步。	实现账户管理一处修改、处处生效，管理方便快捷，极大减少低效工作。
第三层：权限统一 （暂不支持）	实现权限托管。通过对接 IDaaS 标准灵活的 RBAC 模型，将应用内角色、菜单、功能等权限托管在 IDaaS 中，并统一授权管理。	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。



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。

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：

- **单点登录状态**
- **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

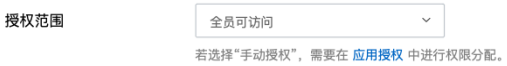
应用市场预集成模板	SAML 2.0	3. 创建应用
标准协议 - SAML	SAML 2.0	SAML 2.0 SSO 配置
标准协议 - OIDC	OIDC	OIDC SSO 配置
自研应用	OIDC	自研应用 SSO 配置

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。

> 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 metadata 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。

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
基本配置（必填）	单点登录地址 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*****4813/saml/SSO
	应用唯一标识 SP Entity ID	应用在 IDaaS 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*****4813/saml/SSO
	应用账户	SAML 协议中将应用账户称为 NameID。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
高级配置（选填）	**默认跳转地址** 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/manage
	NameID 格式 NameIDFormat	SAML Response 中指定账户标识 NameID 字段格式。很多应用不对 NameIDFormat 进行处理，所以一般无需修改。	选择：1.0 Unspecified
	Binding 格式 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
	是否对断言签名 Sign Assertion	IDaaS 会为所有 SAML 请求签名，暂不支持修改。	-
	签名算法 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
	账户字段 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。	-
	SSO发起方	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。

部分应用配置 SSO 时，支持 metadata 信息上传。可将 IDaaS 配置文件上传，或将 metadata 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
IDP 唯一标识 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://xxxxx.aliyunidaas.com.cn/saml/idp/saml1
单点退出地址 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。	-

公钥证书 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 CERTIFICATE----- MIIDEjCCAfqgAwIBAgIHAYnNmX60izANBgkqhkiG9w0BAQsFADApMRowGAYDVQQD.....

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 NameID 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

您可以在如下四种规则中进行选择：

选项	说明
1. **IDaaS 账户**	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。 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）** • **IDaaS 邮箱（Email）**
2.应用账户	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。 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： • **应用账户**
3.优先应用账户	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。 可选子选项有两个： • **次选 IDaaS 账户名（Username）** • **次选 IDaaS 邮箱（Email）**
4.表达式	若应用账户具备特定规则，可以配置表达式。 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。 **可输入表达式规则。**

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。

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
变量	user.username	账户名
	user.displayName	显示名称
	user.phone	手机号
	user.email	邮箱
	user.status	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。

> 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
客户端模式 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。
授权码模式 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。

令牌刷新模式 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。
设备模式 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 讨论区 告诉我们。

IDaaS 侧配置

	字段	说明	举例
基本配置（必填）	**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
	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）	**用户信息范围 scopes**	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
	Code Challenge 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。	-
	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
	id_token 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。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。	-
	id_token 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
	SSO 发起方	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 IDaaS 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 IDaaS / 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
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
发现端点 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
令牌端点 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/oidc/token
验签公钥端点 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://xxxxx.aliyunidaas.com.cn/oidc1/jwks
用户信息端点 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
退出端点（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	user.username	账户名
	user.displayName	显示名称
	user.phone	手机号，不包含国际区号
	user.email	邮箱
	user.status	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）	用户信息范围 scopes	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
	id_token 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。	-
	SSO 发起方	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
发现端点 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
令牌端点 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

令牌吊销端点 Revocation	将已生效的特定令牌注销掉。	https://xxxxx.aliyunidaas.com.cn/oauth2/revoke
验签公钥端点 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
用户信息端点 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
退出端点 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 内置了表达式引擎，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。

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。

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. **函数**，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
userSourceType	来源类型，取值为： build_in、ding_talk、ad、ldap、idp_auto_build
userSourceId	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

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

IdP 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。
Coalesce	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。
IFF	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。
IsNull	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**
StringReplace	StringReplace("hello $VariableName", VariableName, ReplaceString)	普通字符串替换。
Trim	Trim(source)	去除源值字符串前后的空白字符。
ToLower ToUpper	ToLower(source) ToUpper(source)	字符串变为全大写或全小写。
Substring	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】。

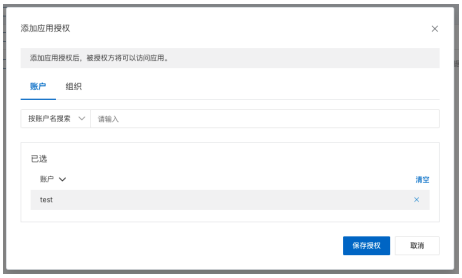
管理授权

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。

添加授权

点击【添加授权】，弹出表单。



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。

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。

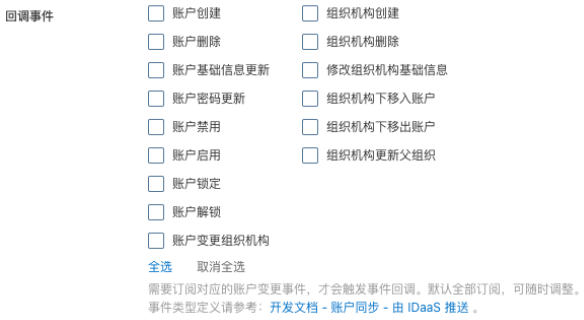
推送配置

请来到【同步到应用】标签。

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/provision
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。	2fdc67ca538cc9500bcad6518390feb937b58e9102b00bffb30a292112fdf626
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。



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。

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。

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。

接口权限

功能场景	权限名	权限值	对应接口
账户/组织	查询账户信息	urn:alibaba:idaas:scope:user:read_all	获取账户信息: GetUser 通过外部ID获取账户ID: GetUserIdByExternalId 查询账户列表: ListUsers 获取账户密码策略: GetUserPasswordPolicy
账户/组织	管理用户	urn: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:alibaba:idaas:scope:organizational_unit:read_all	获取组织信息: GetOrganizationalUnit 通过外部ID获取组织ID: GetOrganizationalUnitIdByExternalId 查询组织列表: 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。

【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。

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。

> 说明
> 为了保障您的使用安全性，二次认证能力默认开启。

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
OTP 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：

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。

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。

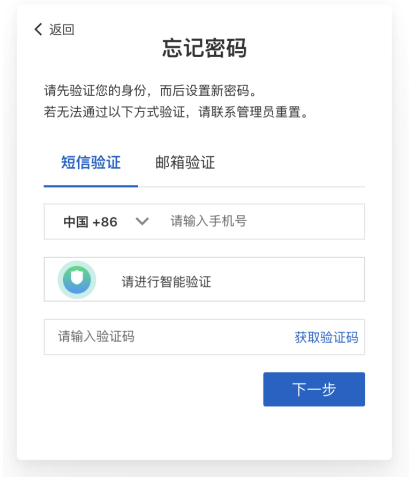
忘记密码

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。

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。

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。



而后即可设定新密码。

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

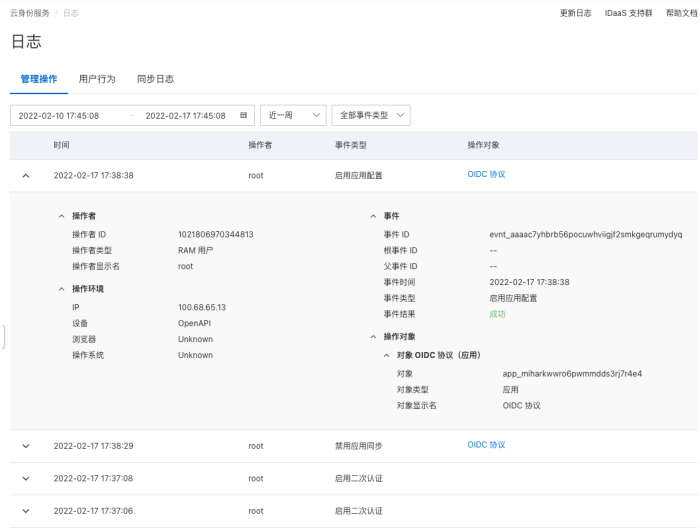
1.4.6.1. 管理/用户日志

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。

> **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。



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 推送给身份提供方（暂不支持）
不记录同步日志，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） • 懒加载 （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

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 IdP 批量导入（定时/手动） • 一次性全量同步到 IdP（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

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。

设定后，在组织根节点和登录页中，会有对应体现。

组织根节点

登录页

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。

> 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。

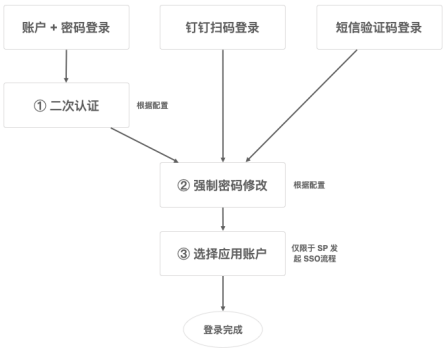
1.5. 用户指南

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。

> 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：二次认证。
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

> 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

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。

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）
短信/邮件 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。

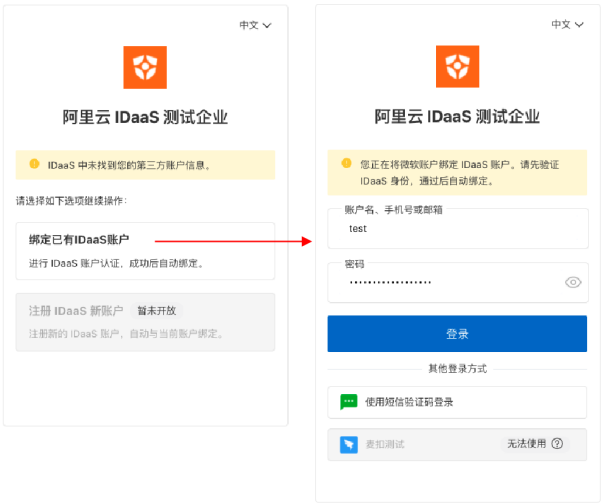
情况二、IDaaS 无法识别用户身份

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 **非钉钉扫码** 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。

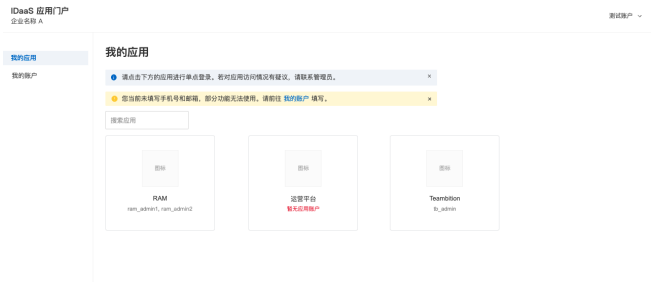
后续登录无需再次绑定。



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 IDaaS 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
情况一 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。
情况二 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。
情况三 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 登录方式。
超时不活跃	可配置。详情参考 登录方式。
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。
关闭浏览器	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：钉钉工作台访问门户。

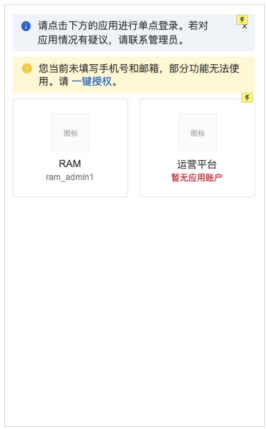
1.5.4. 钉钉工作台访问门户

IDaaS 中 绑定钉钉 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

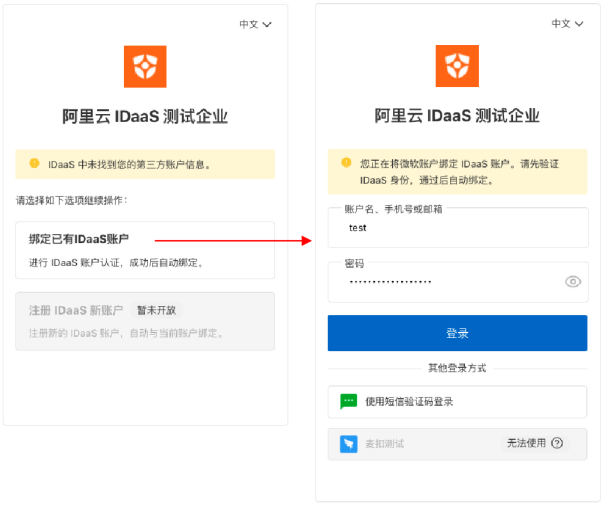
所有从钉钉导入 IDaaS 的账户，均无需绑定，可直接访问钉钉工作台中的 IDaaS 门户。

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 **非钉钉登录** 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**



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。

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。

> 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。
显示名	账户的显示昵称，通常为姓名。
手机	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。
密码	密码复杂度可由管理员配置。
三方登录绑定	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。

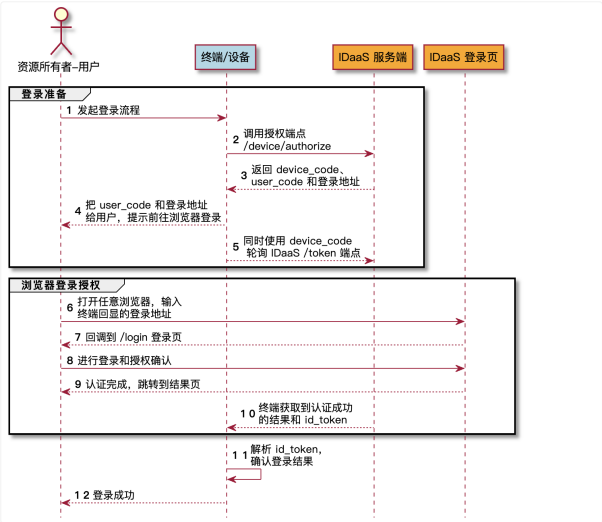
1.5.6. OIDC Device Flow 设备模式登录流程

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` 。

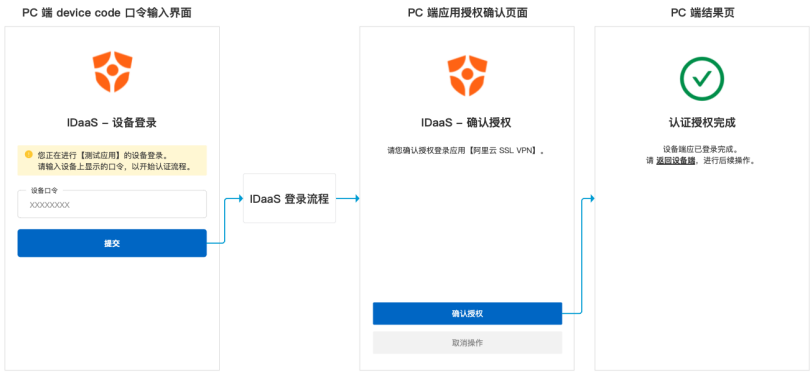
其中， **用户口令** 和 **登录地址** 需要展示给用户，并请用户在任意浏览器中打开 **登录地址** ，输入 **用户口令** ，进行登录流程。

> 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。



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

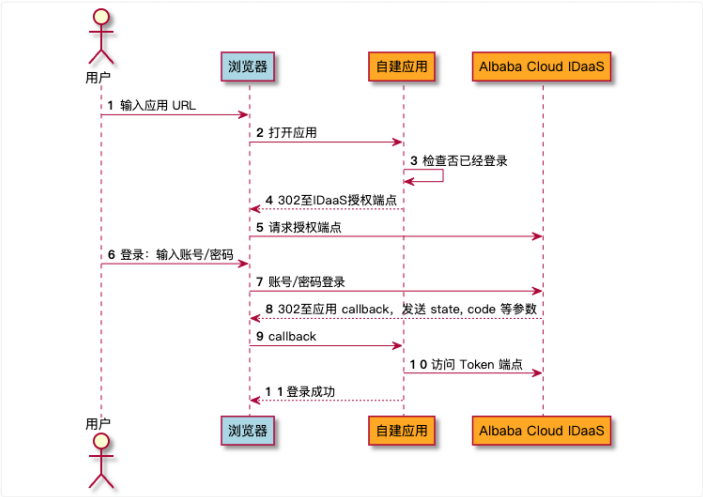
1.6.1.1. 自研应用接入 SSO

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。

> 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/aliyunidaas/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：

```
POST /token HTTP/1.0
Host: api.aliyunidaas.com
Authorization: Basic YXBwX21pY2hzN3I0ZndmY29zdDY2b3NoMzQ2cHllOkNTKioqKioq

grant_type=authorization_code
  &code=n0esc3NRze7LTCu7iYzS6a5acc3f0ogp4
  &client_id=s6******t3
  &client_secret=7F****************dmIw
  &redirect_uri=http%3A%2F%2Fwww.example.com%2Fsso%2Fcallback
```

字段	必填	示例	说明

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	CSAuycr3yWHNn8bEmdkoxBppbKJfXUWMPQ9avtqRozS1V1	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%2Fcallback	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": "ATM4SoVDqWgUJHLu3Bg6qF2hccE6cvjKXiKdiJ2Dc8RJZSbzpBDXPZK3gPhGxQs16s3s7MsZ46fEyiYTWG7EGFKi9uzGjRALaRLecPutBLzzQQRVUt6pbuarCbq5hFRje6bzsrW4jTehhCtZM5JneEfcSQ2ViSDVZGNNtMKAA6v7kTeubZrTaWNzosNMyzGXoD4rqPBwF9FsYqwACQ4aJrt9NnS3NpgDKoMtqEQs5TfDsCYMKYmp7Z73F2BJz89jzN1utEbnuj3HnvyRQPCismDiXjS8EPvoUZBrUBMhrnzYmMcT9KmzKoC12sQjDRQYqgPVxQyMKwQKwwHWXV7stEXnoSt524GW8HVrF3WRsM2N1Ykod1irCz7ZasSwk3ZS5mtn6fcSp8NH8",
  "expires_in": 1200,
  "expires_at": 1644843164,
  "id_token": "eyJraWQiOiJLRVkyVHkxcUw2dTIxTkdLbWNjdjNqd2ZkMm5kbWd0UVBuYWciLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJ1c2VyX3V5dmVmb3RqbjdrcGJlamZteG9vczNydG1tIiwianRpIjoiand0X2FhYWFjN3h5aGNsYWM2YXFrZ3RqYXhzdGh3NXlvdG41ZDc3cG1raSIsImlzcyI6Imh0dHBzOi8vcHJlLWVpYW0tYXBpLWNuLWhhbmd6aG91LmFsaXl1bi1pbmMuY29tL3YyL2lkYWFzX2JxZ2xkdnpwcGEyYWw2aTZhYzVxemphcWpxL2FwcF9taHlsZ28zaWFpcmpxamR4NWVvcDZ1YWYzNC9vaWRjIiwiaWF0IjoxNjQ0ODQxOTY1LCJuYmYiOjE2NDQ4NDE5NjUsImV4cCI6MTY0NDg0MjI2NSwiYXVkIjoiYXBwX2loeWxnbzNpYWlyanFqZHg1ZW9wNnVhZjM0IiwiYXRfaGFzaCI6IlhIRWFHcE1vb005enZRWGFNekNOREEifQ.abebHwoSzOi92-QOKO_E38jyfxjzVLpRIK858UsOehe_GzBoKOEl1zQOSljBB7CwZCdQJpqI1rUxqQopwjvHRSfA-O4_cc4sXDpZYXodeVRXUiv1kYB1b4gZ-hStcE1eh_5jJj1dpoGPBsjTTHjp43EgDx1-8M-8ePF3zXZAfqxCjjroGgB9qXtSreRAIUh5ODViyHYRSAis7CNdP7jKG1dU1UNSGwXWNyRcgVaCqL05gCh0LhHrutMXDy8pcKzdXHQMMBaHF-rGkkGdlp4q9KqwjkpzakcWieRmPa2UUXLdQgK1Pgzc5F7mE-fvsvVfMYfh_JgRIadj-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_mhylgo3iairjqjdx5eop6uaf34/oidc",
  "iat": 1644841965,
  "nbf": 1644841965,
  "exp": 1644842265,
  "aud": "app_mhylgo3iairjqjdx5eop6uaf34",
  "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 Token)令牌，使用签名方法创建也就是 JWS(JSON Web Signature)，对于JWT的解析可以参见https://jwt.io/libraries 找到合适的库，下面以 Java 库：org.bitbucket.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"
                + "      \"kty\": \"RSA\",\n"
                + "      \"e\": \"AQAB\",\n"
                + "      \"use\": \"sig\",\n"
                + "      \"kid\": \"KEY2H82C2at57itnW4onT3p1ySjwH4nirjCk\",\n"
                + "      \"n\": \"w7Jl3fAUJp_9GuxVXb9Jb_QsOA4lnXR5OD4kF4QbIeBiDiH8_MThrFi9k2MB6YMkSzf5JfIkpAS3JCqZ7k6Wooydp4pzaZNZAk3SGzdsa022RmAT"
                + "-Iayi4Yj6J9tSdTQCjwh2XkzzsIxA_Hla8rWiQ8Vhw1"
                +
                "-7QArgObfe67nSR7LxD55MFLxk9FU0NWLEjRRlGhrQGE_0LUuGWtCJG1r1e6aKquyswfxxAr3Rvj8QGIeJrG0R1Pv8m8d1_5OdULhB7149VqjM6D98WFjab0U2SNv0UlRE
ZXTcS4p-2QNm_1egYRRpJEY_00FZqNSYsmErMGepYhO_61KoGqd8cphWQ\"\n"
                + "    }\n"
                + "  ]\n"
                + "}";
        String jwt = "eyJraWQiOiJLRVkySDgyQzJhdDU3aXRuVzRvblQzcDF5U2p3SDRuaXJqQ2siLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJ1c2VyX2R0NmtqNnlmNjRjZjR3amFrbnBi
eGpjd3V1IiwianRpIjoiand0X2FhYWFkYWllYTc2eWg1cW0zcm11bnoyeGg0eHd5aTJzZHBoNjR6aSIsImlzcyI6Imh0dHBzOi8vZWlhbS1hcGktY24taGFuZ3pob3UuYWxpeXVuY3MuY29tL3Y
yL2lkYWFzX3BhZHlybHV4M21waHJsc2V4NHVvbnlxaHh1L2FwcF9taWY0ZHdscGVoNnM0cHhwemJhc3FtdS9vaWRjIiwiaWF0IjoxNjUzNjMwMDQxLCJuYmYiOjE2NTM2MzAwNDEsImV4cC
I6MTY1MzYzMDM0MSwiYXVkIjoiYXBwX21raWY0ZHdscGVoNmRuczRweHB6YmFzcW11IiwibmFtZSI6InRlc3QiLCJwcmVmZXJyZWRfdXNlcm5hbWUiOiJ0ZXN0IiwidXBkYXRlZF9hdCI6MTY1M
zYyODU5MH0.pAsUNB8OkdpIxJMZRfLJ7Pa31tsJyl44a1jVIlvdQxwOtPULAwrFxnB0X3eQx89hUGCdvYWl9FO9o-5kT7L-RER0wJYz9YNKqrVNBnaRwINRZyeYLRVurWMMzODQz-V0ULd9raM1
M_i2f_SoWFs1gPFtYh_ijUARHISi7Q3q93ZfAuY8Lq2Nq07QunmDbosvioUd5wJG7WCxW5XXZYDUQe9p5IEYd1MSvnWuTOLbg7rKn0Vm4dNYGWjz1WuoAyCsc_QxOCqpmQ_2czoqPeN-SvPJAQ2
CykLk7DSnGpABw1aNrjDidLS9Beqsga9VDCth86sk_0lyTZOaORtUrfVTtQ";

        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,
                nbf=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*******cHllOkNTKioqKioq

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：

```
<parent>
    <groupId>org.springframework.boot</groupId>
    <artifactId>spring-boot-starter-parent</artifactId>
    <version>2.4.1</version>
</parent>

<properties>
    <java.version>8</java.version>
</properties>

<dependencies>
    <dependency>
        <groupId>org.springframework.boot</groupId>
        <artifactId>spring-boot-starter-web</artifactId>
    </dependency>
    <dependency>
        <groupId>org.springframework.boot</groupId>
        <artifactId>spring-boot-starter-oauth2-client</artifactId>
    </dependency>
</dependencies>
```

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。

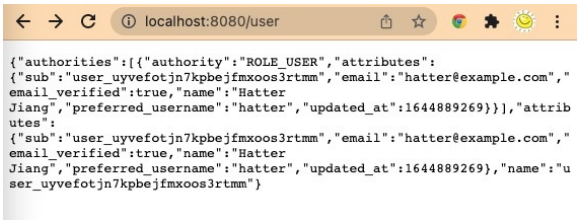
通过注入 `@AuthenticationPrincipal OAuth2User user` 即可获得最终的用户信息：

```
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：



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

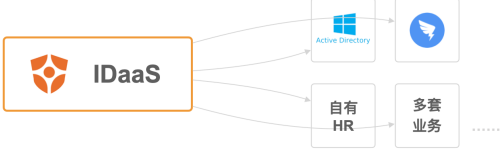
1.6.2.1. 账户同步接入概述

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 应用开发 API 说明。

应用同步配置请参考：账户同步 - IDaaS 同步到应用。本篇文档介绍应用按照 IDaaS 规范完成账户同步对接。



AD、钉钉、HR、自研同步

- **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。

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。

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":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKxwRJSMeKKF2QT4fwpMeJf36POk6yJV_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": "KEYH1zR7XLCGcHwlhzhkCqVjnuyaAJUf6yMR",
    "typ": "JWT",
    "alg": "RS256"
}
```

`payload` 举例：

```
{
  "iss":"urn:alibaba:idaas:app:event",
  "sub":"idaas-121313",
  "aud":"app_12131313",
  "exp":1640966400,
  "iat":1640966400,
  "jti": "cNetm9OD5bXqfVfdvqGMYw",
  "dataEncrypted":false,
  "cipherData":"",
  "plainData":{
    "aliUid":1231313,  //阿里云账号Uid
    "instanceId":"实例ID",  //实例id
    "eventVersion":"V1.0",  //版本号
    "eventData":[
      {
        "eventId":"",     //事件id
        "eventType":"",   //事件类型
        "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
	exp	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。

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。

```
{
    ...
    "cipher_data": "ZePq7ckODWnL54vqZc3kTw0vF7tjvIRZjqqy/gZm9oTEt71WMufD9swlmHzZkniSqyDGQpkmMRLCXz9gzRJ4BY2RroLUPQW8ZDPSfmJKEf2m2w6wY1twoRlnHLoFCVhravsvN0afBqmxd3eK5tHd05Ze6MLOXS3fqxqH61dGAm2mwecvAFPRrKVeg6JXBYUvA2Uu6dmCOP3y938kFdhodD13O05MBIqWghq569wYvVjKMFMcnsZqmGGKXN0vRFhg+SR16sr24b1X/gQDbNqyMDICB9k3QMe09dOodwNEwvgxbf1v4PbyCRX1P9UO74nDQaWROWZFplE7qP/JMy3pBr0pxW+hJS9u/Zpvj/hvLlhBTAZkmhAKDKxlrYztqrgJbr4VOUv8mlqxWjDK4I7VZugODJMSwi1HdjXL+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。

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 eventId 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 eventId 将触发重试。
-eventCode	String	错误码，IDaaS 将记录结果，便于排查问题。您可自定义 eventCode。
-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：

```
{
    "successEvents": [
        {
            "eventId": "事件ID",
            "eventCode": "SUCCESS",
            "eventMessage": "SUCCESS"
        }
    ],
    "skippedEvents": [
        {
            "eventId": "事件ID",
            "eventCode": "跳过code",
            "eventMessage": "跳过描述"
        }
    ],
    "failedEvents": [
        {
            "eventId": "事件ID",
            "eventCode": "错误code",
            "eventMessage": "错误描述"
        }
    ],
    "retriedEvents": [
        {
            "eventId": "事件ID",
            "eventCode": "错误code",
            "eventMessage": "错误描述"
        }
    ]
}
```

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
通讯录 增量事件	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
	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_unit
通讯录 全量事件	全量推送组织	urn:alibaba:idaas:app:event:ud:organizational_unit:push
	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：urn:alibaba:idaas:app:event:common:test

请求参数验签后 `payload` 示例：

```
{
  "iss": "urn:alibaba:idaas:app:event",
  "sub": "idaas_rhhoqmlnyu3cv7ow657gyvurky",
  "aud": "app_mjavzivahje6zxkbc4i2bierdu",
  "exp": 1648711369,
  "iat": 1648709570,
  "jti": "bNRrCYrqXjqe8B1xweq1Zw",
  "dataEncrypted": false,
  "cipherData": "",
  "plainData": {
    "instanceId": "idaas_rhhoqmlnyu3cv7ow657gyvurky",
    "aliUid": 1519714049632764,
    "eventVersion": "V1.0",
    "eventData": [
         {
          "eventId":"evnt_aaaac766x2somw2ptotoyk6ag6bmfkt5xpqprpq",
          "eventType":"urn:alibaba:idaas:app:event:common:test",
          "eventTime":"1648709509849",
          "bizId":"evnt_aaaac766x2somw2ptotoyk6ag6bmfkt5xpqprpq",
          "bizData":"{\"bizData\":\"req_xxxxxxxxxxsdfsdfsfd\"}"
         }
     ]
  }
}
```

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": [
    {
      "eventId": "evnt_aaaac766x2somw2ptotoyk6ag6bmfkt5xpqprpq",
      "eventCode": "SUCCESS",
      "eventMessage": "SUCCESS"
    }
  ],
  "skippedEvents": [
    {
      "eventId": "",
      "eventCode": "",
      "eventMessage": ""
    }
  ],
  "failedEvents": [
    {
      "eventId": "",
      "eventCode": "",
      "eventMessage": ""
    }
  ],
  "retriedEvents": [
    {
      "eventId": "",
      "eventCode": "",
      "eventMessage": ""
    }
  ]
}
```

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：

```
{
    "password": "ssGp96",
    "userId": "user_4alcbywzc7jyl23lu2srljsw7i",
    "username": "zhangsan",
    "displayName": "张三",
    "passwordSet": true,
    "phoneRegion": "",
   "phoneNumber": "155****5620",
    "phoneVerified": false,
    "email":"zh***@163.com",
    "emailVerified": false,
    "userExternalId": "user_4alcbywzc7jyl23lu2srljsw7i",
    "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
userId	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 userId 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userId。
userSourceType	String	来源类型，若为自建账户，则为 "build_id"。
userSourceId	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
accountExpireTime	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` 示例：同账户创建。

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
organizationalUnitSourceId	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。

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：

```
{
  "keys": [
    {
      "kty": "RSA",
      "e": "AQAB",
      "use": "sig",
      "kid": "KEY3PdQDx97WFk8G6pfzh83p8husNSC9AKMH",
      "n": "rLUnH5PNeGUZE-J4IUIJOvUGGIxyM5O7TDdaG4jUCjO2LzKD9mV1CjE8hVHBxXM96IcCCH_1xmUZEZRp_MBP6m2XeNWUXanCpeyuIAD2kxmaQAqituZdIlT4l3-q9gtccdY-khaE-OfH9qYZhlxFcYj0gVtOvKZFIkuGhME4IQJd_RAWS3OPXxtbGhO2fZYCiuuc8NWub5mcVQnqsy5aJPLwHbVwVUwYNOmaq97_m2TtPcIVWtw7AOzX8O78UrYnYt_QPrv7uVdJMbHleSOx2A1IXqrAkJWecwFfvTsBTCUOPPDeVRQEHzzwmf3zpz5KMgHZU1I5pyqi0KJ6BuMHWw"
    }
  ]
}
```

添加 Maven 依赖：

```
<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);
        }
    }

    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 (jsonWebKeySet == 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_xxxxxxxxxxxxxxxxxxxxxxxx95d1padSEABqIbcTKcnlTaET3WHaR"
            + "-3MvsooeZWluv94GQEp-U2jzM1adgTqBl_7KPjUk0dwrZbob_8pOLX5UQMF7Oo_nH5-H5EyL9-yGGhFA4oeuA"
            + "-b73qXShxP7eHs5xTT1kiYEu2NE3rBZdtrRwUiC_h1DvZMtyWFOPwm3dpLiwCcdlgcKvVuSEXyCBj6Gjevn3_G1guVQ2kHlNOVyNn6K y1iGQJzXctJCEJ5fnBRs4XZZbPNSc
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。

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"});
    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. **账户查询和管理接口**
3. **组织查询和管理接口**
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。

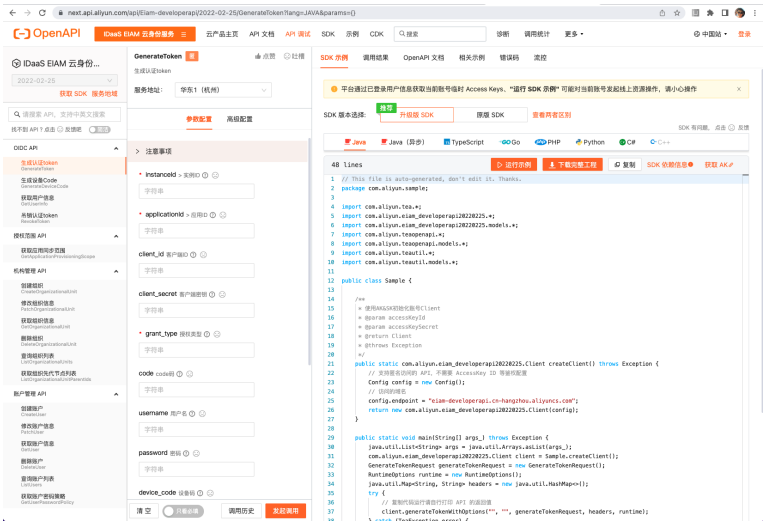
> 说明
>
> 注意：与阿里云 OpenAPI 不同，IDaaS 应用开放的 Developer API 依赖于 IDaaS 中应用的密钥，并在 IDaaS 应用管理中分配接口调用权限。Developer API 权限不依赖于 RAM。

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。

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】

令牌	获取令牌	• 获取令牌：GenerateToken	-
账户	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
	账户查询接口	• 获取账户信息：GetUser • 查询账户列表：ListUsers • 获取账户密码策略：GetUserPasswordPolicy	urn:alibaba:idaas:scope:user:read_all
组织	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:organizational_unit:manager_all
	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:organizational_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ID
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' \
  -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

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":"zhangsan1",
"displayName":"李四",
"description":"我的账号",
"primaryOrganizationalUnitId": "ou_001",
"userExternalId": "user_001",
"phoneRegion": "86",
"phoneNumber": "1560000****",
"phoneNumberVerified": true,
"email": "t****@example.com",
"emailVerified": true,
"password": "$sfdsf12AAfa_"
}
```

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}
userId	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":"zhangsan1",
"displayName":"李四",
"description":"我的账号",
"userExternalId": "user_001",
"phoneRegion": "86",
"phoneNumber": 1560000****",
"phoneNumberVerified": true,
"email": "t****@example.com",
"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/${userId}
- 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}

userId	String	path	是	账户ID

响应参数

参数名称	数据类型	参数位置	是否必填	描述
userId	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
userSourceType	String	body	是	来源类型
userSourceId	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

```
{
  "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			
• userId	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

• 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
• userSourceId	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

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,
        "containLowerCase": true,
        "containNumber": true,
        "containSpecialChar": true,
        "emailCheck": true,
        "usernameCheck": 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	否	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
instanceId	String	实例ID
organizationalUnitId	String	组织ID
organizationalUnitName	String	组织名称
parentId	String	上级组织Id
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ID
createTime	Long	创建时间
updateTime	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"
}
```

正确响应样例

```
{
    "instanceId": "idaas_h6pmuhzub3vbdp3exsyabvn33m",
    "organizationalUnitId": "ou_lloqvor2jbexeafkjwwx34vzha",
    "organizationalUnitName": "dsad1111sas1xc",
    "parentId": "ou_penjtomawyocl622uc63i6boea",
    "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/${instance_id}/${application_id}/organizationalUnits/${organizationalUnitId}
- 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_token}
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>	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。

> 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

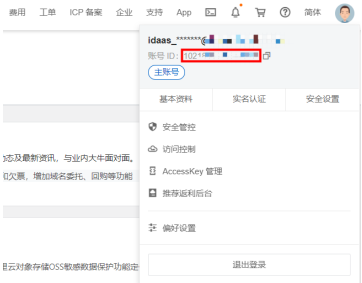
1. 登录 IDaaS管理控制台。
2. 前往 **应用-添加应用-应用市场**，搜索到阿里云用户 SSO 应用模板。点击 **添加应用**。

3. 确认应用名称，即可完成添加。

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。

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）。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。



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。

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。

四、在阿里云中配置子用户权限（可选）

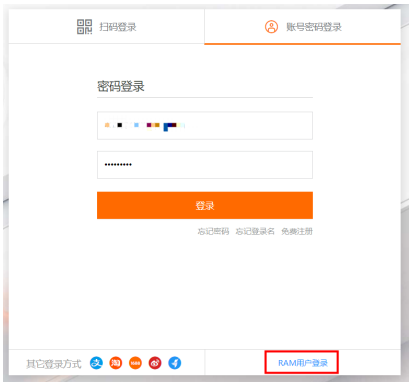
您可能拥有存量的阿里云子用户，或希望将 IDaaS 中账户同步至阿里云（详见文档：账户同步），此时请按需在左侧菜单栏的 **用户** 中为用户分配权限，以便用户拥有恰当的权限访问阿里云的资源。如果仅为了测试单点登录能力，请忽略此步骤。

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。

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。



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**。

3. 确认应用名称，即可完成添加。

二、配置应用单点登录

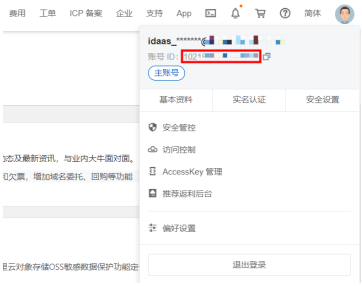
1. 添加应用后，将自动跳转到应用单点登录配置页，您将在此处进行配置。

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。



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。

4. 在 **单点登录-应用账户** 中，点击 **添加应用账户**。

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。

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。

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。

四、在阿里云中配置身份提供商权限

1. 在左侧导航栏中，单击 **身份管理-角色**。
2. 点击 **创建角色**，选择 **身份提供商**。

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。

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。

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。

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。

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。

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。

2. 输入腾讯云主账号 id（账号 id 可在腾讯云控制台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。

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。

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。

四、在腾讯云中配置子用户权限

1. 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。

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。

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**。

3. 确认应用名称，即可完成添加。

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。

2. 输入腾讯云主账号 id（账号 id 可在腾讯云控制台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。

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。

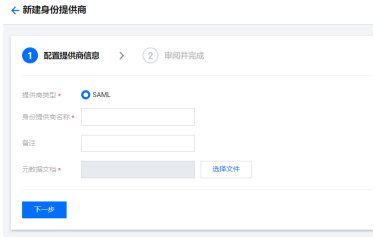
4. 在 **单点登录-应用账户** 中，点击 **添加应用账户**。

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。

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**。

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。

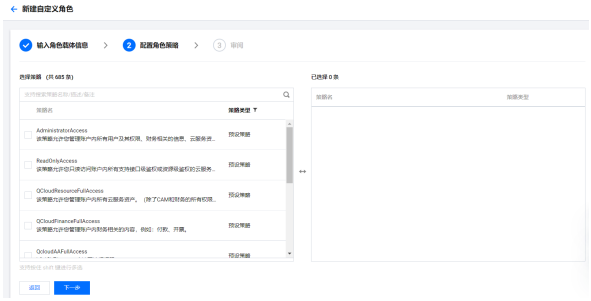


四、在腾讯云中配置身份提供商权限

1. 在左侧导航栏中，单击 **角色**。
2. 点击 **新建角色**，选择 **身份提供商**。

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。

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。



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。

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。

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。

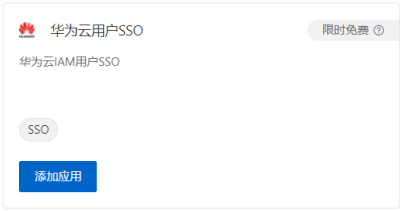
1.7.2.5. 华为云 SSO

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**。



1. 确认应用名称，即可完成添加。

二、配置应用单点登录

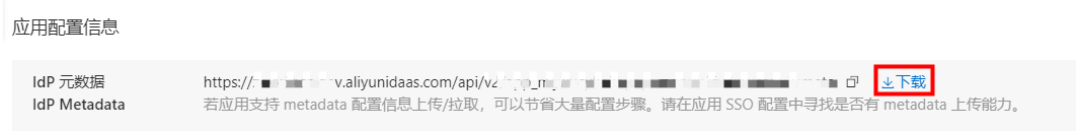
1. 添加应用后，将自动跳转到应用单点登录配置页，您将在此处进行配置。

2. 输入初始化登录地址（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。

3. 在 **应用配置信息** 中，下载 **IdP 元数据**，保存到电脑中。此文件用于建立华为云对 IDaaS 的信任关系。



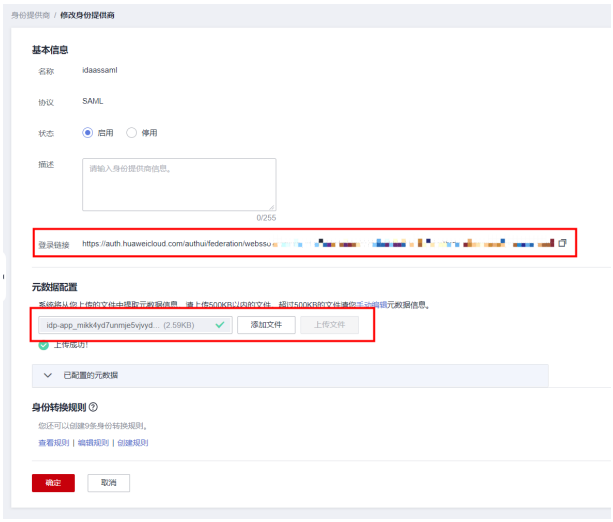
三、在华为云中配置用户 SSO

1. 登录华为云 IAM 控制台。
2. 在左侧导航栏中，单击 **身份提供商**。
3. 点击 **创建身份提供商**。

4. 填写名称，并点击确定。

5. 点击 **修改身份提供商**，或在 **身份提供商列表** 页面中点击 **修改**。

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。



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。

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**。

3. 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。

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

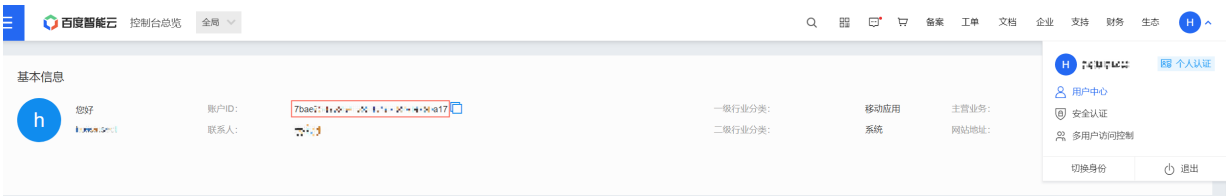
1. 登录 IDaaS管理控制台。
2. 前往 **应用-添加应用-应用市场**，搜索到 **百度智能云用户 SSO** 应用模板。点击 **添加应用**。

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

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



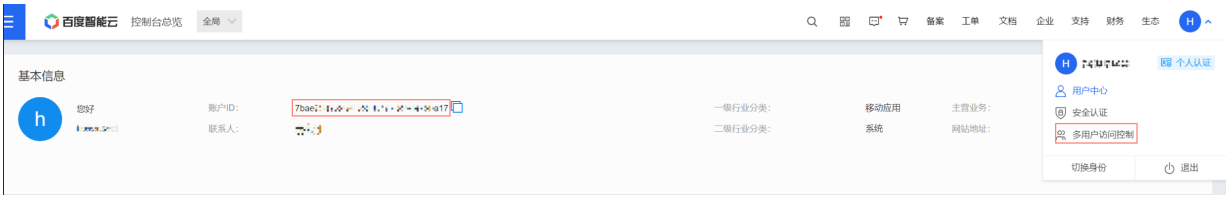
2. 其他选项保持默认，点击保存即可完成 IDaaS 侧的全部 SSO 配置。

> **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 IdP 元数据，保存至本地，在后续流程中将会使用。

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：



2. 在左侧导航栏栏中，选择【外部账号接入】【IAM用户联合】，打开如下图所示界面

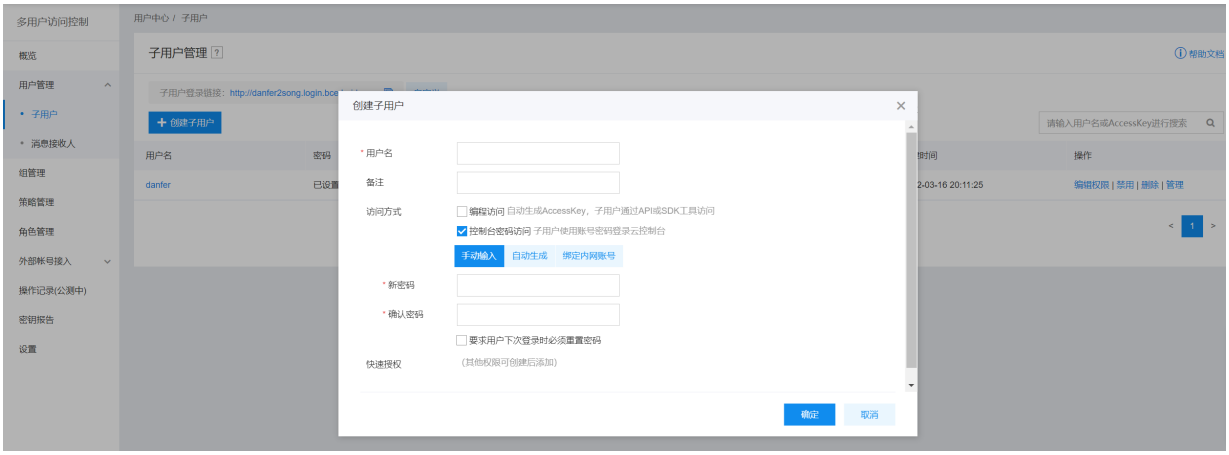
3. 将“功能状态”，修改为启用，同时上传之前下载的 IdP 元数据，如下图所示：

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



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 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。

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：

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 。

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 IDaaS 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

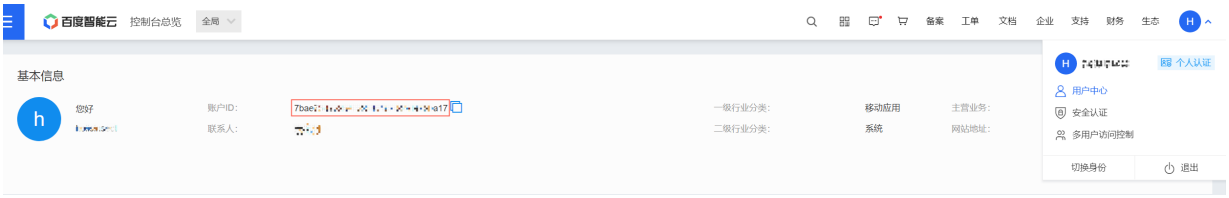
1. 登录 IDaaS管理控制台。
2. 前往 **应用-添加应用-应用市场**，搜索到 **百度智能云角色 SSO** 应用模板。点击 **添加应用**。

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

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



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

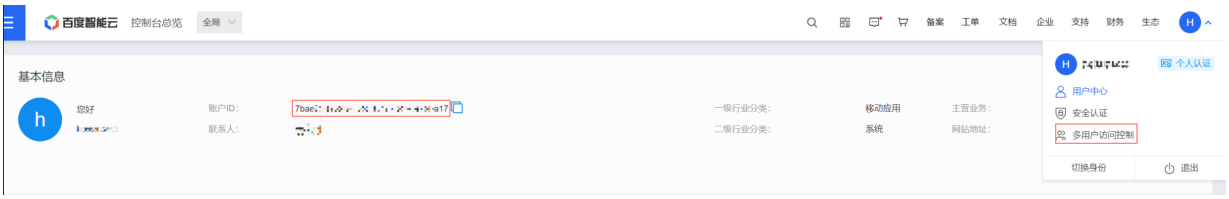
3. 其他选项保持默认，点击保存即可完成 IDaaS 侧 全部 SSO 配置。

> 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 IdP 元数据，保存至本地，在后续流程中将会使用。

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：



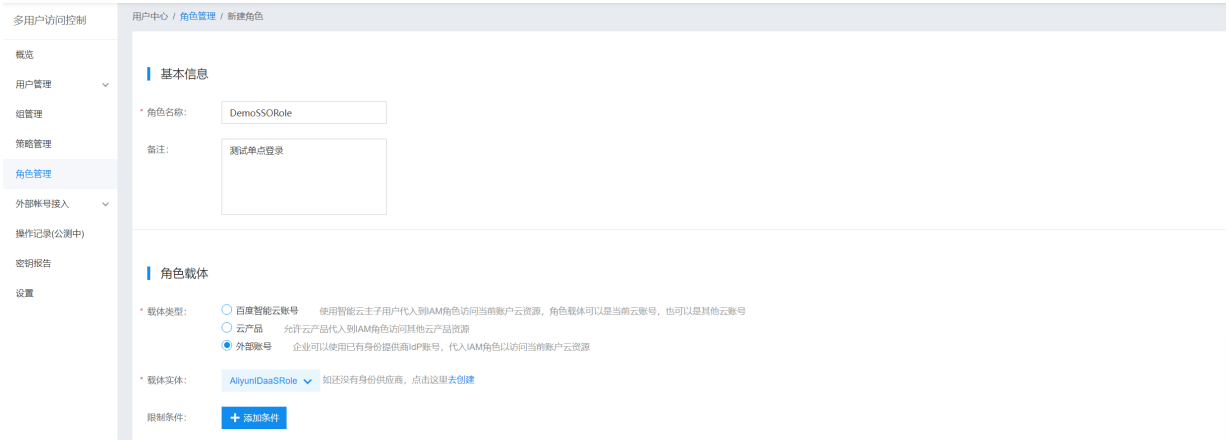
2. 在左侧导航栏栏中，选择【外部账号接入】【IAM角色联合】，打开如下图所示界面

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 IdP 元数据，进行上传。

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”。

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

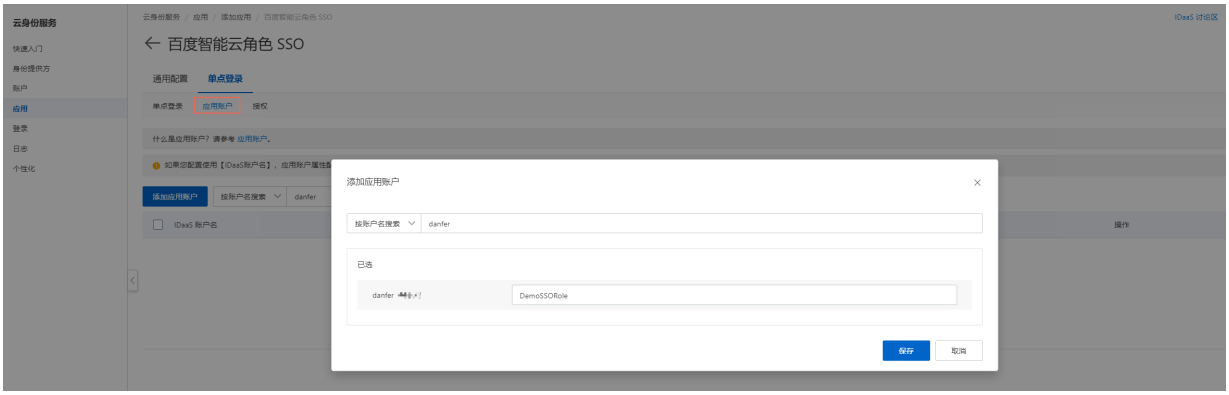


2. 输入角色名称，例如：DemoSSORole，角色载体-载体类型，选择外部账号，载体主体选择之前创建的身份服务提供者：AliyunIDaaSRole。您可以为该角色赋予一些权限

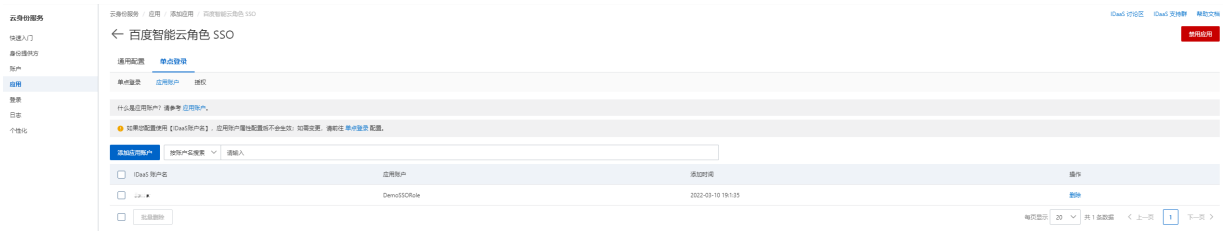
五、在 IDaaS 中为用户关联角色

返回 IDaaS 管理控制台

1. 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：



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。



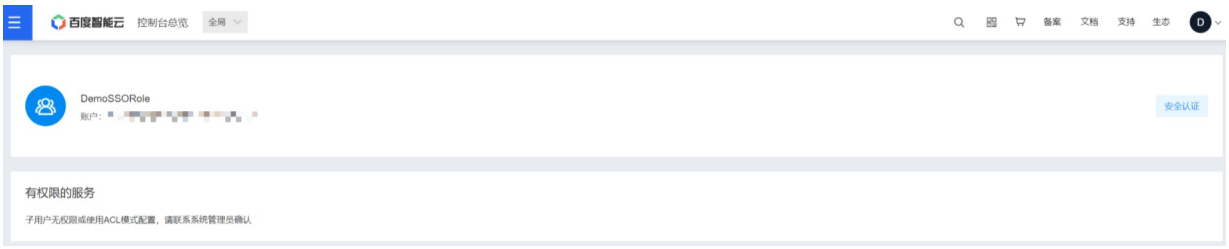
六、尝试SSO

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。

您将以“DemoSSORole”的身份，登录到百度智能云中，如下图所示：



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**。

3. 确认应用名称，即可完成添加。

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。

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。

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。

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 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IdP元数据，在 **应用配置信息** 中，下载 **IdP 元数据**，保存到电脑中。此文件用于建立金山云对 IDaaS 的信任关系。

1. 登录访问金山云管理控制台。
2. 选择左侧菜单**SSO管理** 。
3. 在**SSO管理**页面中单击**创建身份提供商**按钮。
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IdP的登录服务地址、用于验证签名的公钥及断言格式等信息

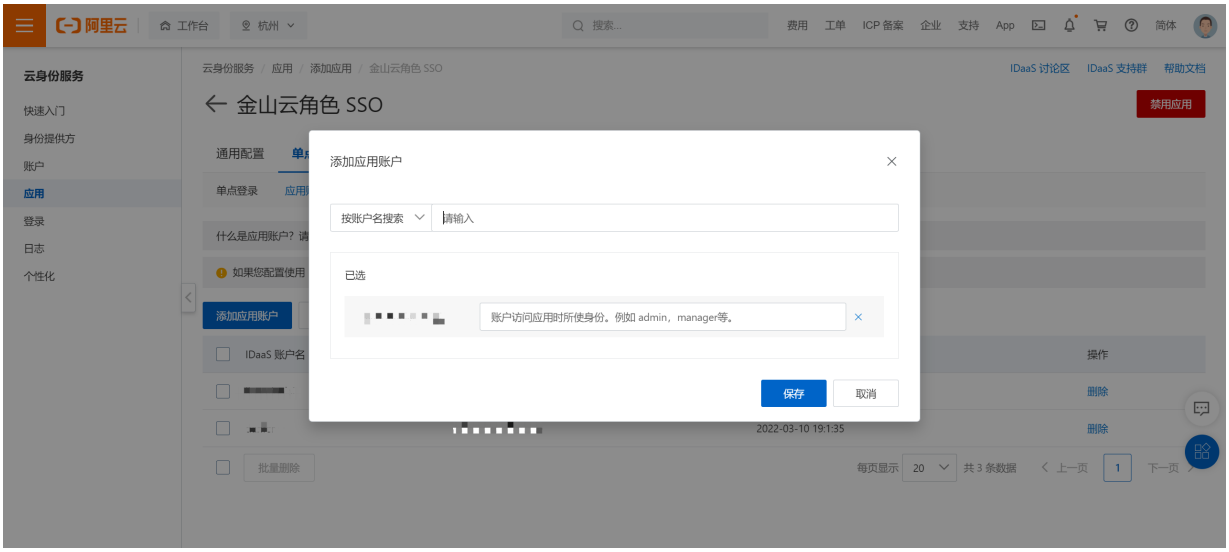
5. 单击提交，完成创建。

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**。
4. 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

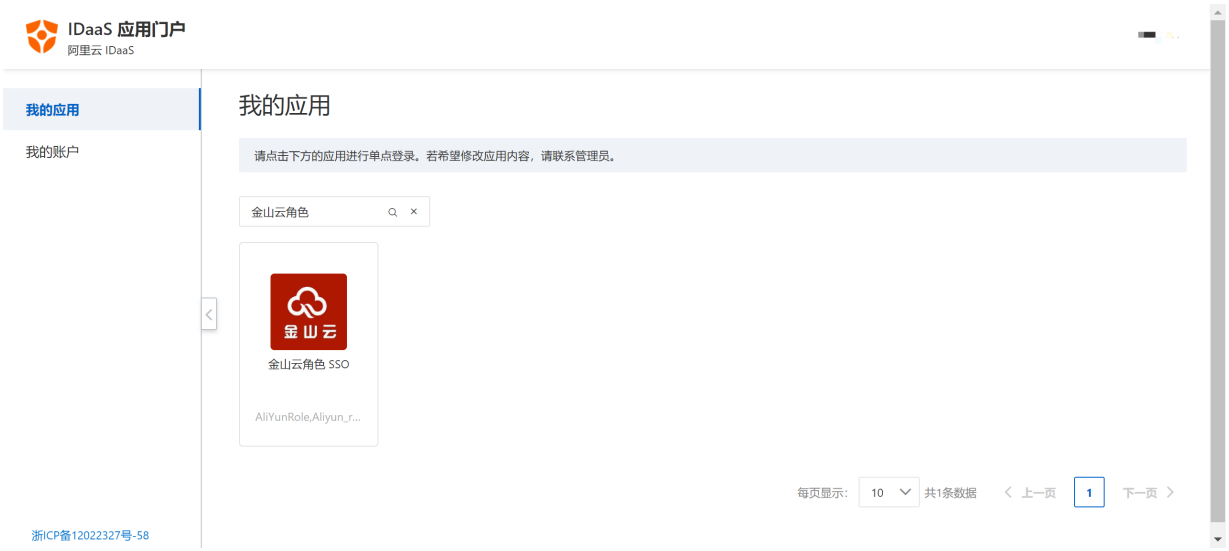
配置应用账户，选择需要使用金山云角色 SSO 的账户，为其添加应用账户。**应用账户名需要和金山云角色名称完全一致。**如果一个 IDaaS 账户对应多个金山云角色，可以创建多个应用账户。



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。



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。

1.7.2.9. Salesforce SSO

本文为您介绍如何在 IDaaS 中配置 Salesforce 单点登录。

应用简介

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 Salesforce 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 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。

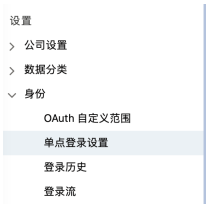
点击【下载证书 .cer 文件】进行下载，在后续步骤中上传到 Salesforce 中。

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。



> 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。

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
姓名	-	固定值：IDaaS，可随意填写。
API 名称	-	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。
实体 ID	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。
身份提供商证书	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。

身份供应商登录 URL（选填）	IdP Sign-in URL、SAML SSO URL 等	从 IDaaS SSO 配置页【应用配置信息】中获取 `IdP SSO 地址` 。 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：

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。

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。

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】。

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：用于 SSO 的身份标识，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【全员可访问】

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。

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。

添加后，会自动来到 SSO 配置页。

配置 SSO

您只需要将 JumpServer 根域名填写进来。

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。 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 IDaaS 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。

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 本链接 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。

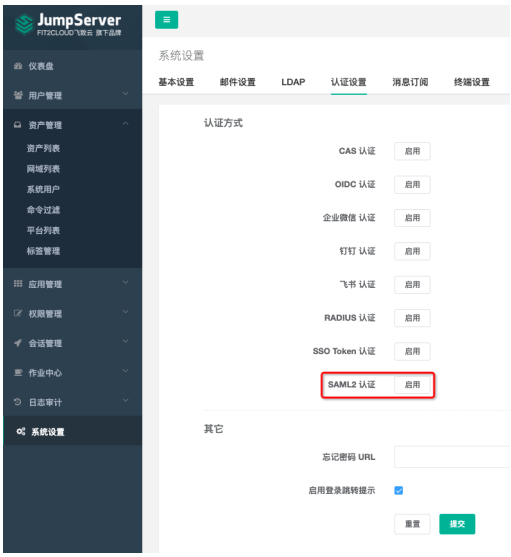
将私钥【Private Key】内容复制在本地，保存为 `.pem` 文件。将【X.509 cert】公钥保存为 `.cer` 文件。

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【SAML 2 认证】的【启用】按钮。



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
SP 密钥	即上一步生成的私钥 Private Key，文件上传 .pem。
SP 证书	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。
高级设置 `strict`	将 `strict` 的值改为 `false` 。 > *提示：将 `strict` 设定为 `false` 会存在安全风险。但由于 JumpServer 官网对 SAML 配置描述不清，只得如此配置过渡。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：

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。

> 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。

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 Atlassian 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。

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 JIRA 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。

开启单点登录。

> 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	IdP 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。
X.509 证书	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：

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。

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)`。

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 CI&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。

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。

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。

> 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【IdP 元数据】链接复制出来即可，后续步骤将在 Jenkins 中粘贴。

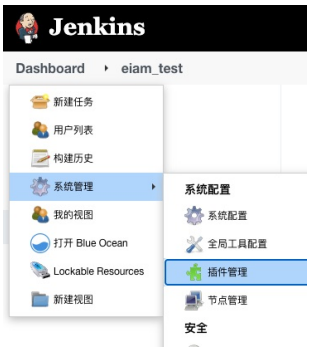
二、Jenkins 中配置 SSO

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。



切换到【可选插件】标签，搜索 【SAML】 插件。勾选后选择安装。

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】。

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。

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：**表单最上方的【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。

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

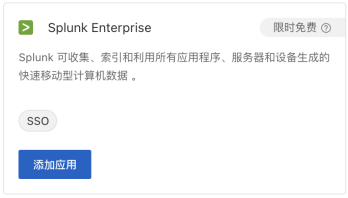
Splunk 可收集、索引和利用所有应用程序、服务器和设备生成的快速移动型计算机数据。

> 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。

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。

> 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。

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。

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。

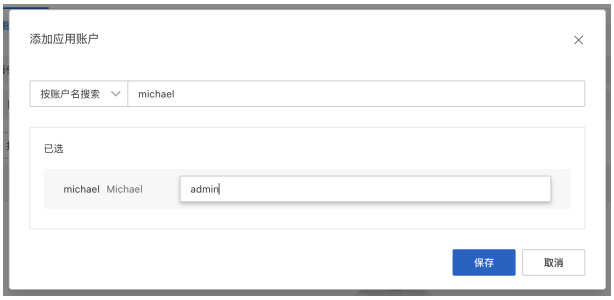
为了测试的目的，在新弹出的表单中，命名组名为 admin，并选择 `admin` 角色。真实情况下，请您按需分配角色。

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。

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。



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。

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

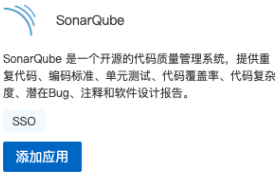
SonarQube 是一个开源的代码质量管理系统，支持超过 25 种语言，提供重复代码、编码标准、单元测试、代码覆盖率、代码复杂度、潜在Bug、注释和软件设计报告。

> 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。

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。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 SAML 应用账户配置 进行配置。 若希望指定可访问应用的 IDaaS 账户，请参考应用授权 进行配置。

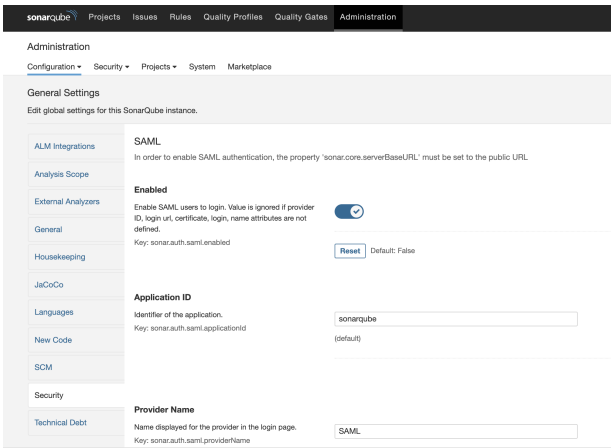
配置页面下方，包含了一系列 SonarQube 完成配置所需要的参数。

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。



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

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	IdP 唯一标识 IdP Entity ID	从 IDaaS SSO 配置页【应用配置信息】中获取。
SAML Login URL	IdP SSO 地址 IdP 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。

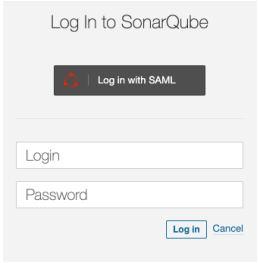
> 说明
>
> 注意：SonarQube 支持【自动创建账户】（Just-in-time Provisioning），单点登录时，若 SonarQube 中不存在指定应用账户，则会直接创建，不会拒绝访问。请在 IDaaS 中管理 SonarQube 访问权限。

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。

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。



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。

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】。

将【CorpID】填写到表单中。

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。

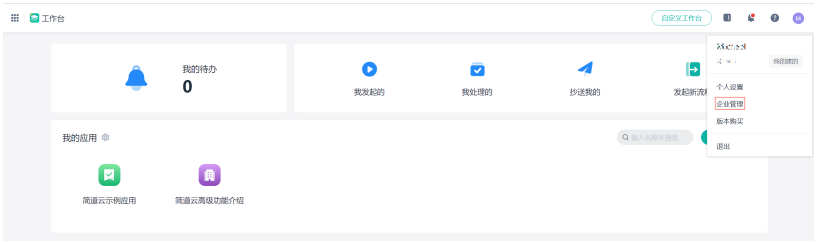
> 说明
>
> - 应用账户：默认使用 IDaaS 账户名作为应用登录标识。应用中用户名必须要和 IDaaS 账户名保持一致，才能完成 SSO。 若希望灵活配置，请参考 SAML 应用账户配置 进行配置。
> - 授权范围：若希望指定可访问应用的 IDaaS 账户，请参考 单点登录通用说明 进行配置。

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。

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。



导航前往【企业信息】【高级设置】【单点登录】选项。

开启单点登录。

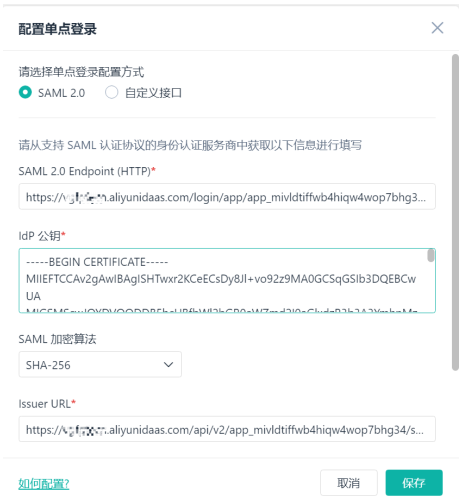
2. 进行 SAML 配置

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	IdP 唯一标识 IdP Entity ID	从 IDaaS SSO 配置页【应用配置信息】中获取。
SAML 加密算法	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：



点击保存后，展示出详细 SSO 信息。

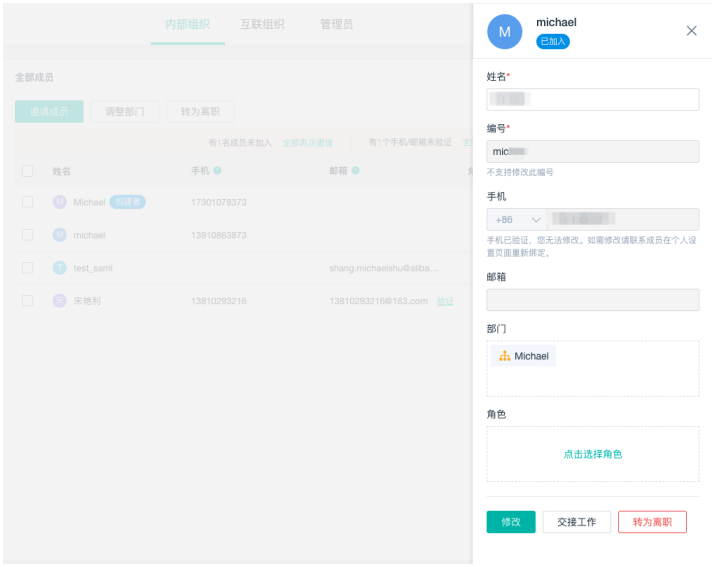
单点登录配置完成。

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。

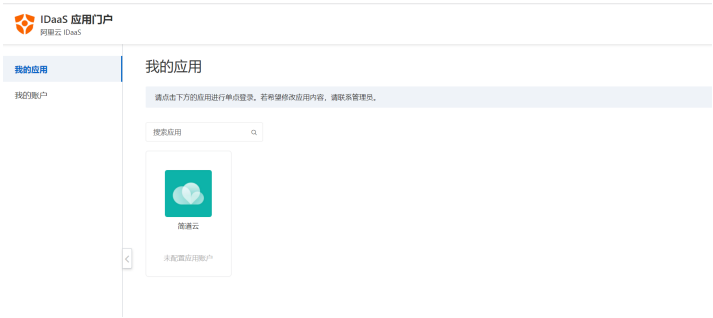


四、尝试 SSO

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.

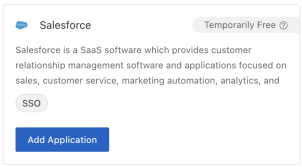
App Introduction

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

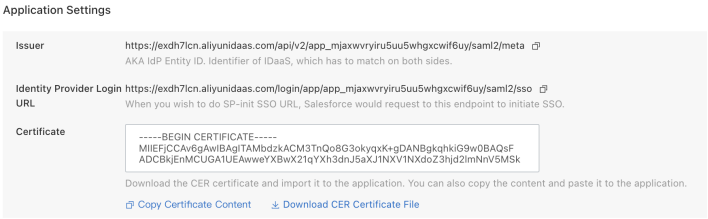
1. Create Application

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.

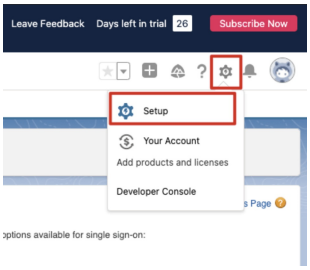


Download the certificate to be uploaded on Salesforce later.

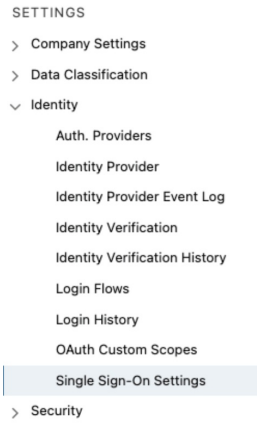
2. Configure Salesforce SSO

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.

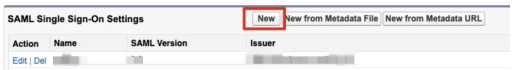


说明

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

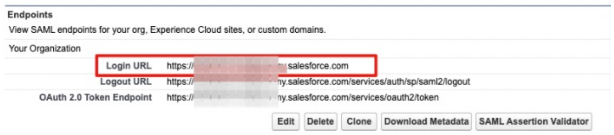
Click New.



There are quite a few things an the form, but we only need to pay attention to the following:

Attribute	Alias	Comments
Name	-	Fixed Value: IDaaS。You may enter as you wish.
API Name	-	Fixed Value: IDaaS。You may enter as you wish.
Issuer	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.



2.3. Enable SAML SSO

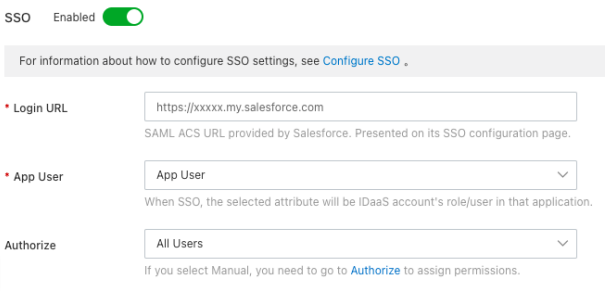
You need to go back into the Salesforce SSO configuration and enable this setting.

Click on Edit on the SSO main page, and enable SAML SSO.

3. Configure SSO in IDaaS

Go back to IDaaS page.

Paste the Login URL from Salesforce.



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

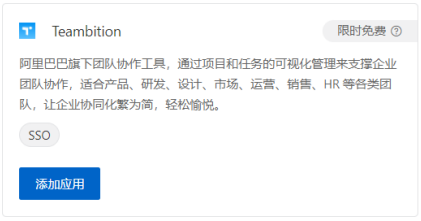
Teambition 是阿里巴巴旗下的团队协作工具，通过项目和任务的可视化管理来支撑企业团队协作，适合产品、研发、设计、市场、运营、销售、HR 等各类团队，让企业协同化繁为简，轻松愉悦。

> 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**。



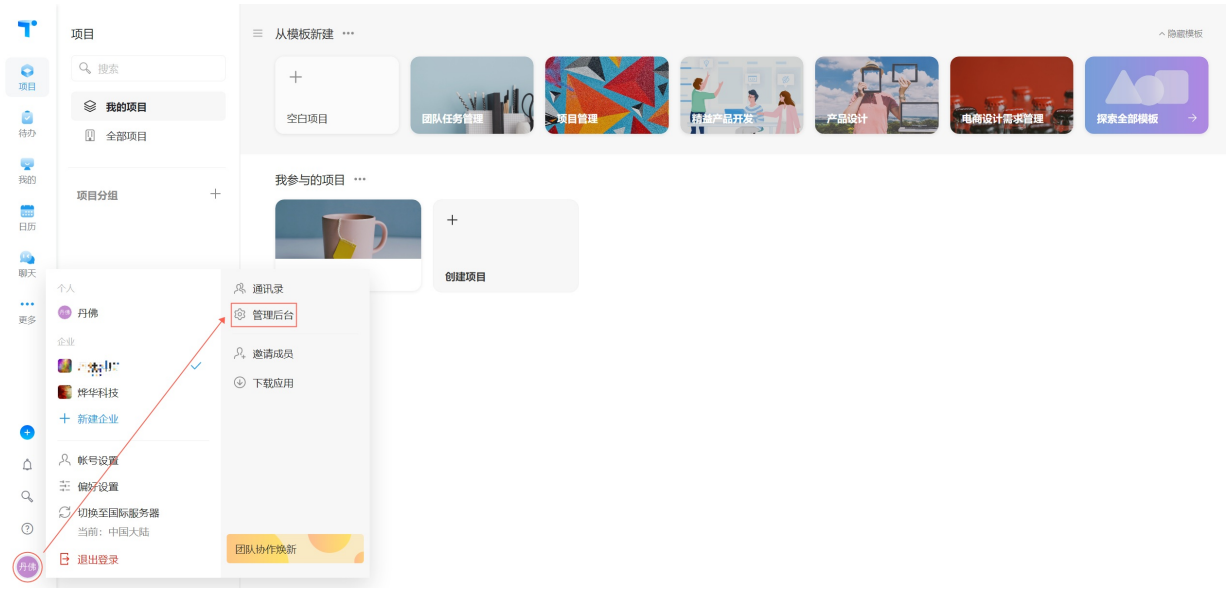
3. 确认应用名称，即可完成添加。

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。

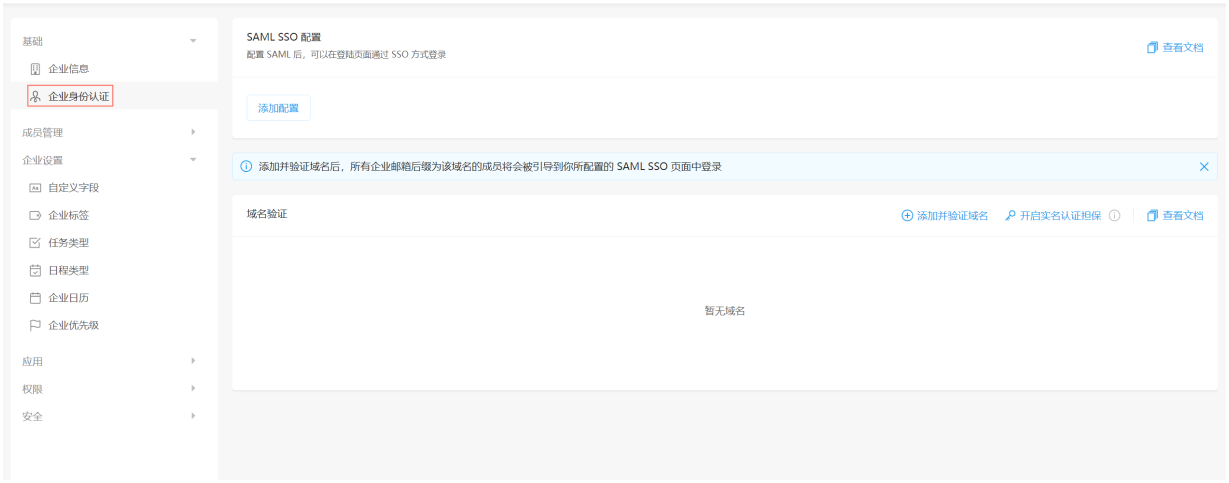
二、配置 Teambition

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SAML SSO 配置。



点击 **添加配置**，打开如下所示对话框。

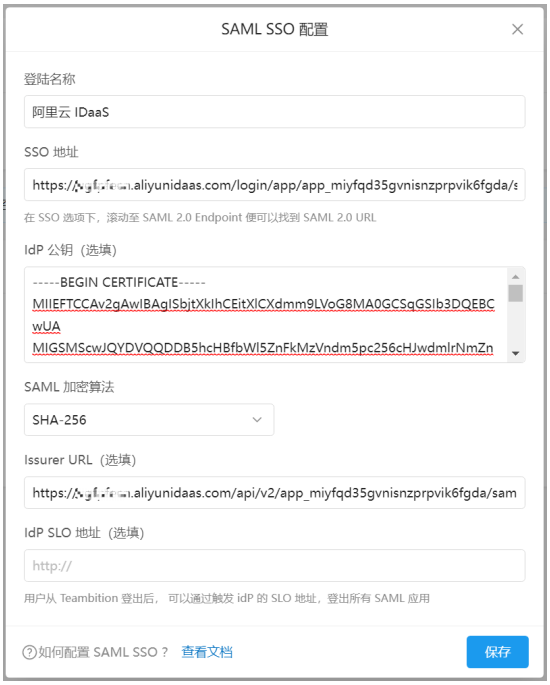
2. 进行 SAML 配置

点击 **配置** 按钮，弹出配置表单。

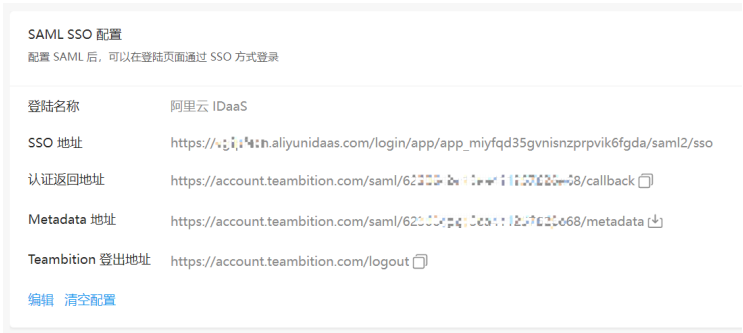
将 IDaaS **应用配置信息** 中的参数全部填写到配置表单中。

字段	别称	说明
登录名称		建议填写为：阿里云 IDaaS
SSO 地址	IdP SSO 地址 IdP 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	IdP 唯一标识 IdP 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：



点击保存后，展示出详细 SSO 信息。



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**。

其他选项保持默认，点击保存即可完成全部 SSO 配置。

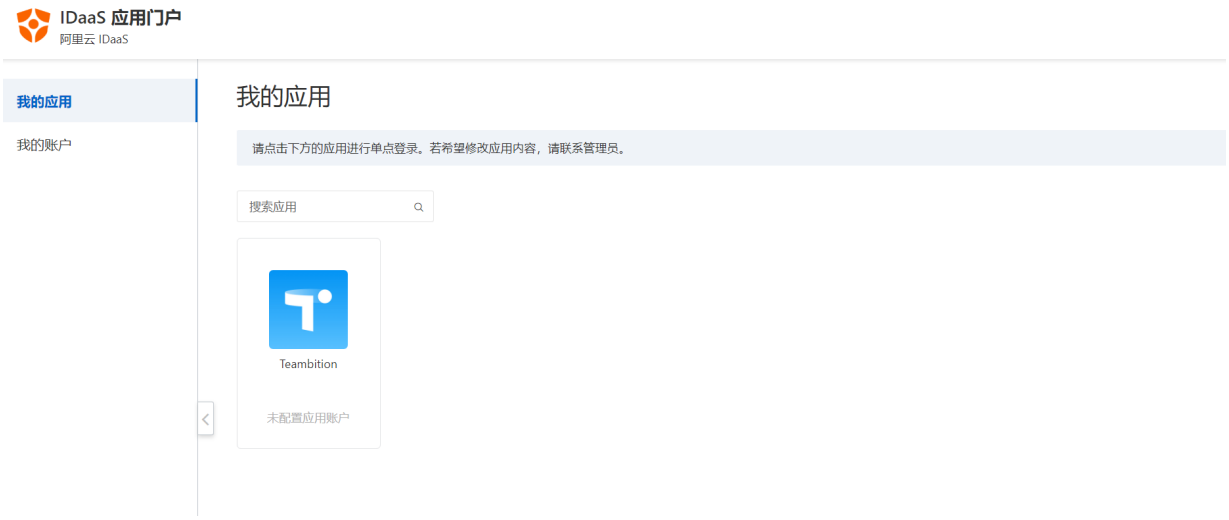
> **说明**
>
> 提示 应用账户：默认使用 IDaaS 账户名作为应用登录标识。应用中用户名必须要和 IDaaS 账户名保持一致，才能完成 SSO。 若希望灵活配置，请参考 单点配置通用说明 - 应用账户 进行配置。 授权范围：默认全员可用。若希望指定可访问应用的 IDaaS 账户，请参考 单点配置通用说明 - 应用账户 进行配置。

四、尝试 SSO

您已经可以尝试 Teambition SSO。

IDP 发起

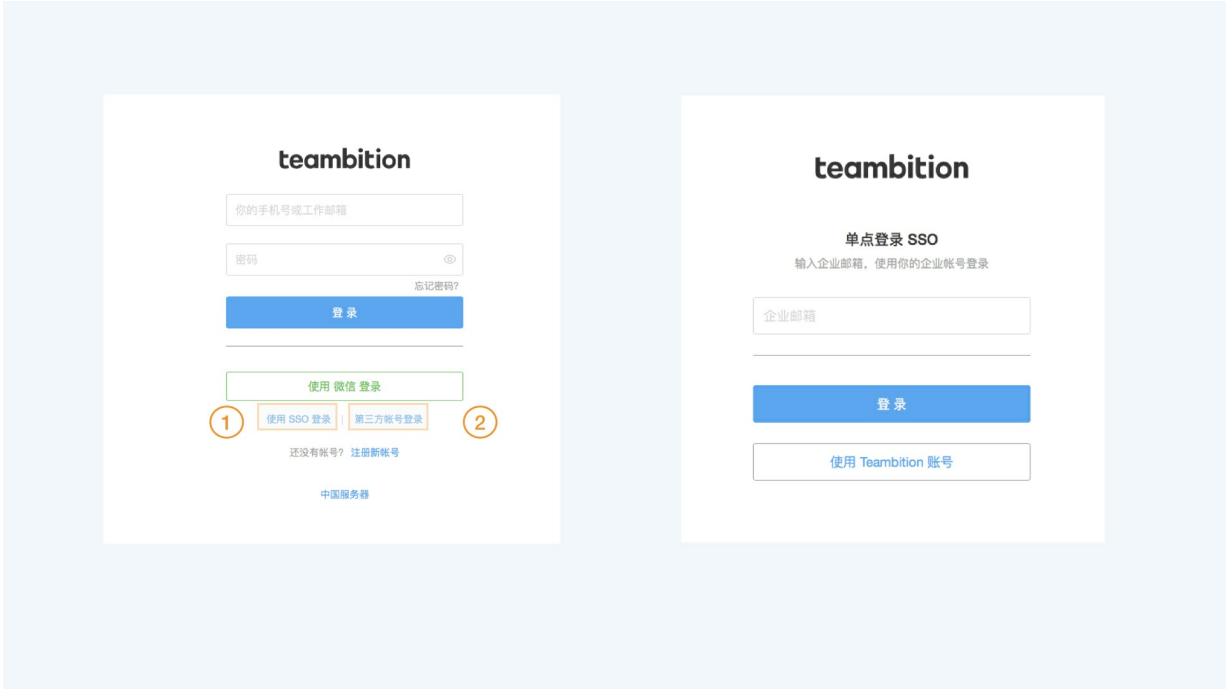
请用已授权使用 Teambition 的 IDaaS 账户，登录到 IDaaS 门户页，点击页面上 【Teambition 】图标，发起 SSO。



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。

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。



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。

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。

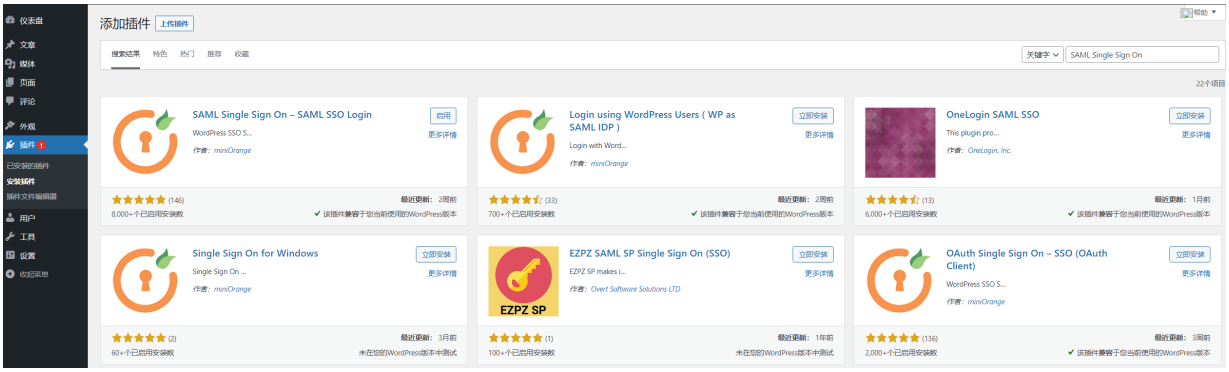
查看配置页下方的 **应用配置信息** 中，包含了 WordPress 完成配置所需要的参数。

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。

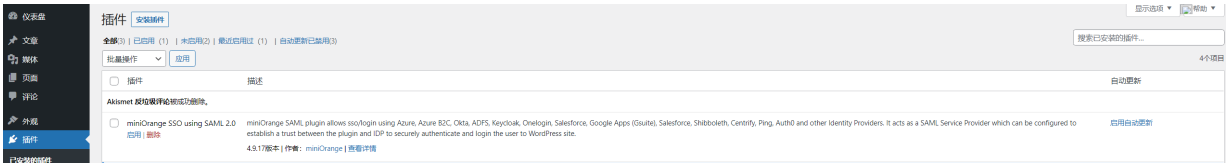
三、WordPress 中配置 SSO

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**。

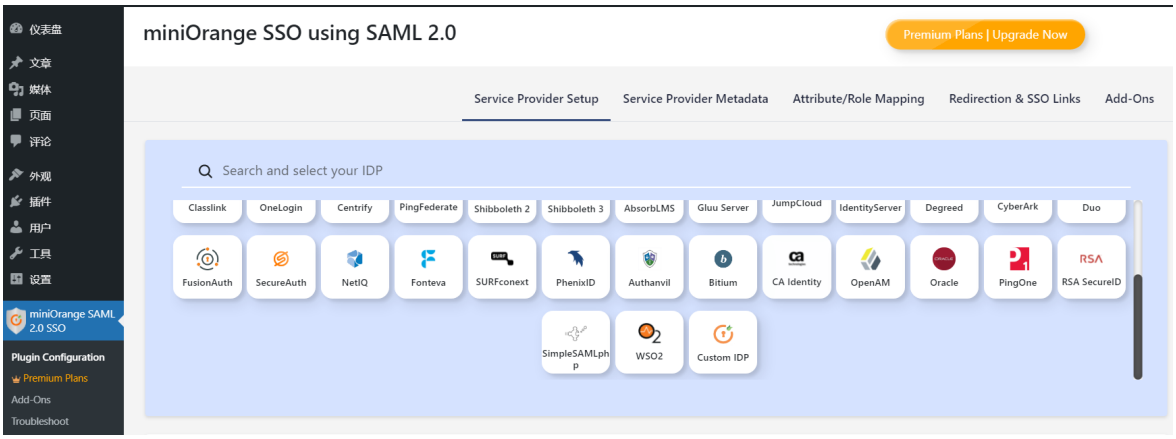


插件安装成功之后，在 **插件-安装插件** 列表中，找到 **miniOrange SSO using SAML 2.0** 插件，启用该插件。

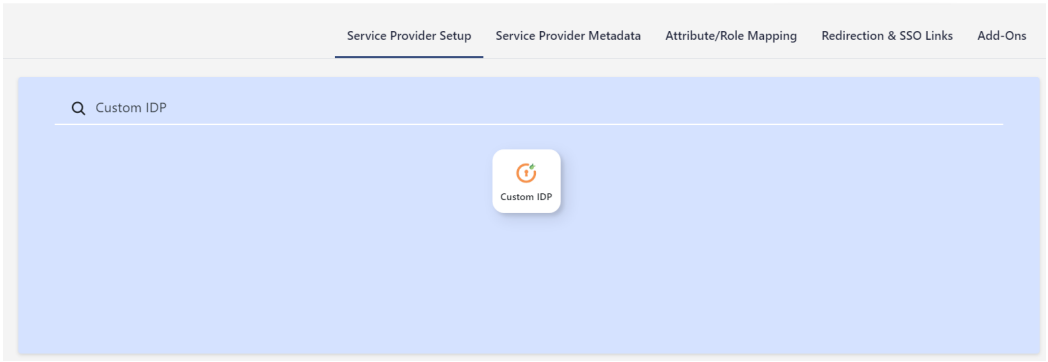


2. 配置 SSO

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：



在 **Service Provider Setup** 标签内，搜索 **Custom IDP**，如下图所示：



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。

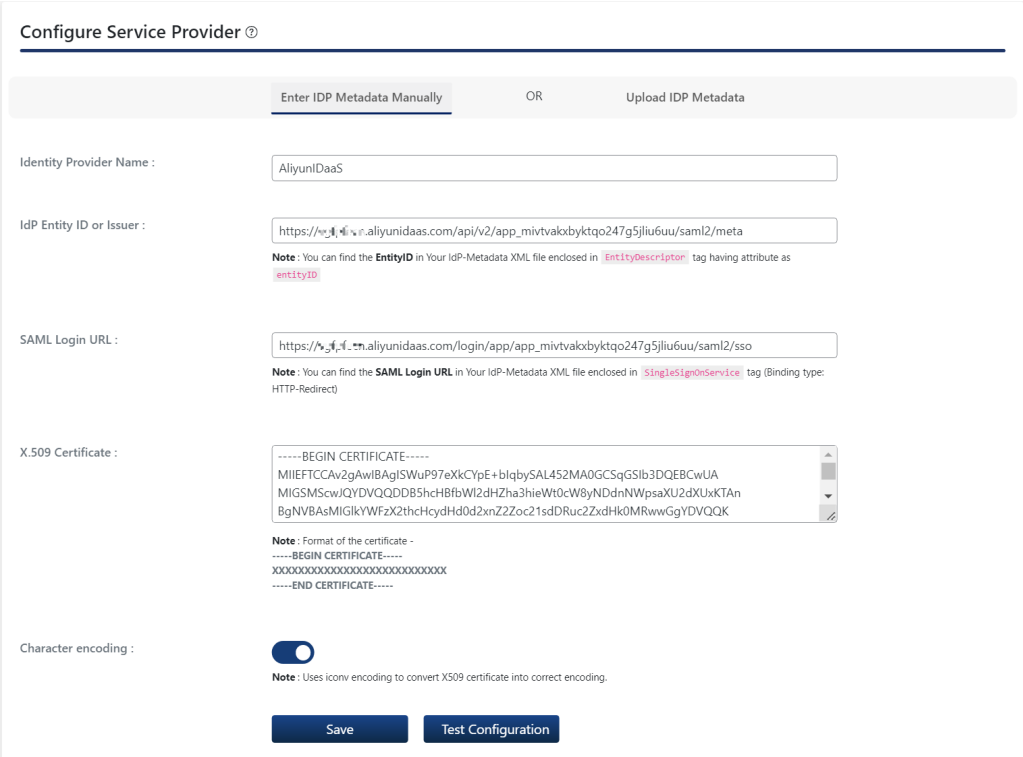
- **上传IDP元数据**

选择 **Upload IDP Metadata** 页签

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。
Upload Metadata	IdP 元数据 IdP 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。
Enter metadata URL		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：

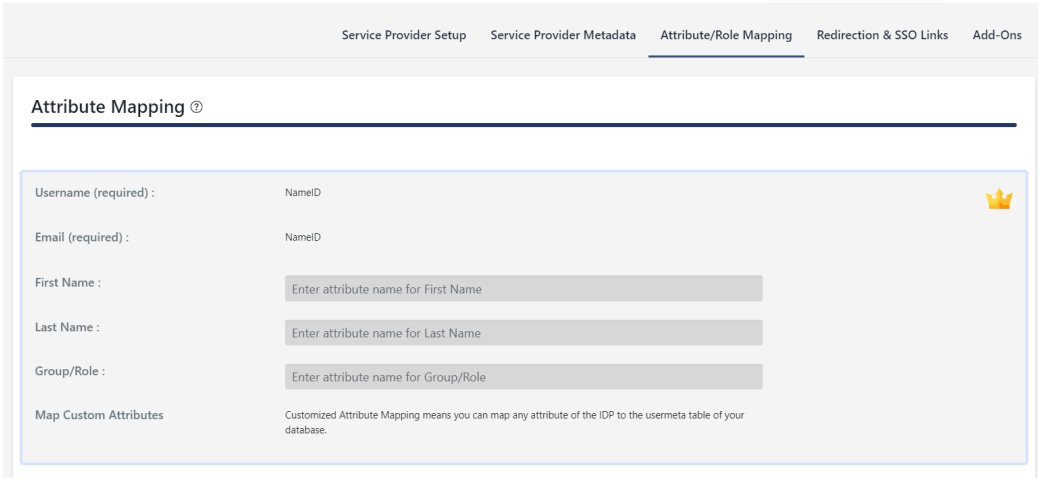


字段	IDaaS 中字段名称	说明
Identity Provider Name		输入一个名字，例如： `AliyunIDaaS` ，这个名字将在 WordPress 登录页中显示。
IdP entity ID or Issuer	IdP 唯一标识 IdP Entity ID	从 IDaaS SSO 配置页 **应用配置信息** 中获取，对应 “ IdP 唯一标识”

SAML Login URL	IdP 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”
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：

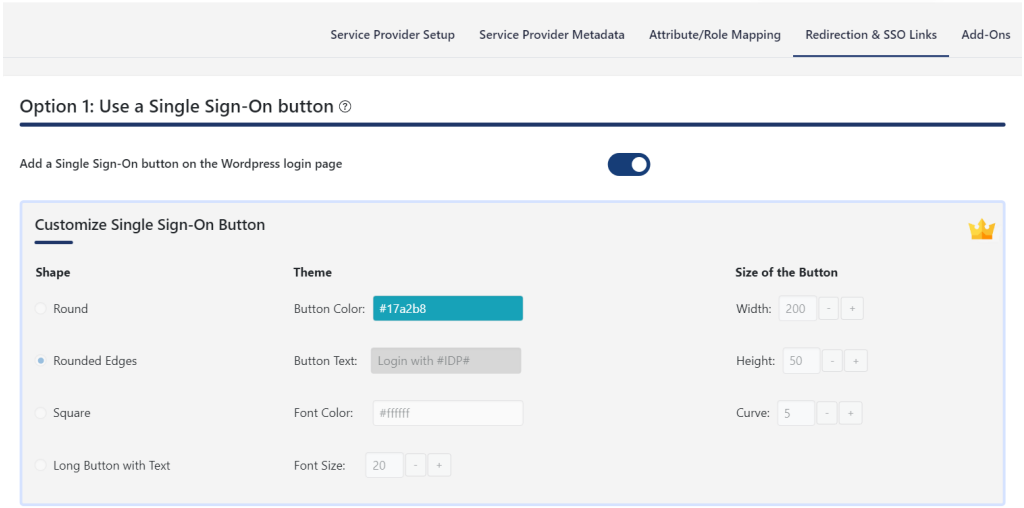


目前支持的属性映射：

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。



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。

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 。

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 Bitbucket miniOrange saml单点登录。

应用简介

Bitbucket

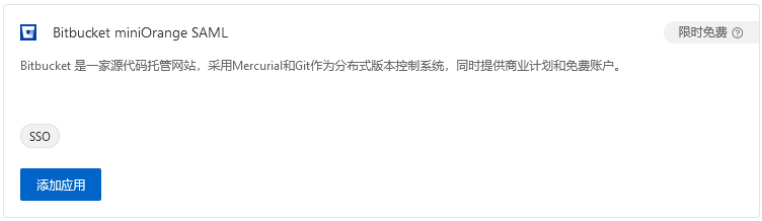
注意：Bitbucket 需要额外插件才能实现 SSO，例如：SAML Single Sign On - SAML SSO Login

本篇文档中 Bitbucket 版本为 6.0.3。 在 Bitbucket 中通过 配置请参考文档：https://miniorange.com/atlassian/setup-saml-single-sign-on-sso-for-bitbucket#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 **Bitbucket miniOrange SAML** 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 Bitbucket 服务地址填写进来，注意结尾不要以“/”结尾。

1. 填写 SSO 配置

其他选项保持默认，点击 **保存** 即可完成全部 SSO 配置。

- 应用账户：默认使用 IDaaS 账户名作为应用登录标识。Bitbucket 支持 **自动创建账户**，单点登录时，若 Bitbucket 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 Bitbucket 配置信息

配置页下方的 **应用配置信息** 中，包含了 Bitbucket 完成配置所需要的参数。

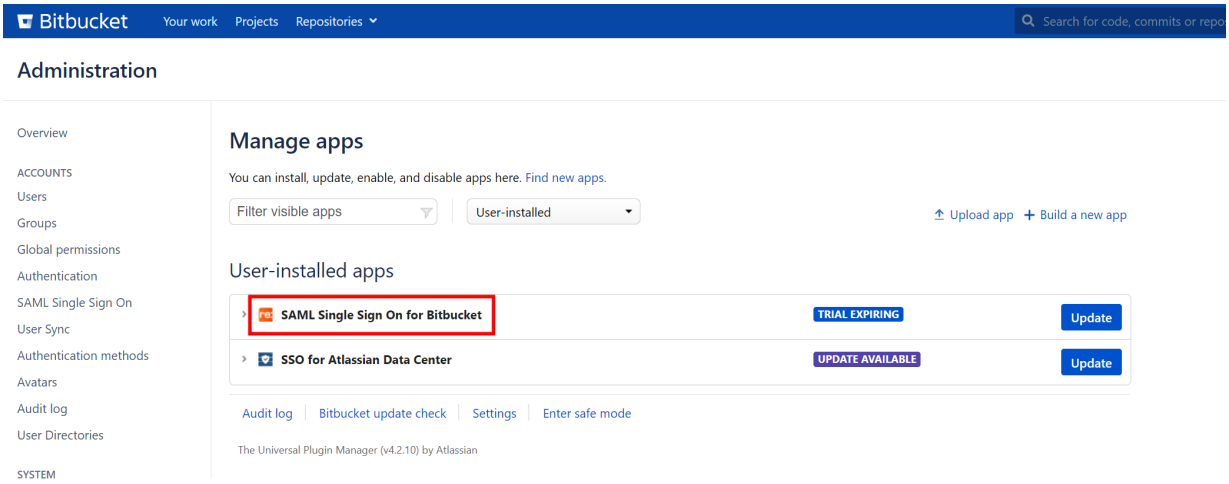
从中您需要获取 IdP 元数据，IdP 唯一标识IdP， 发起 SSO 地址和公钥证书四个参数。

三、Bitbucket 中配置 SSO

1. 安装插件

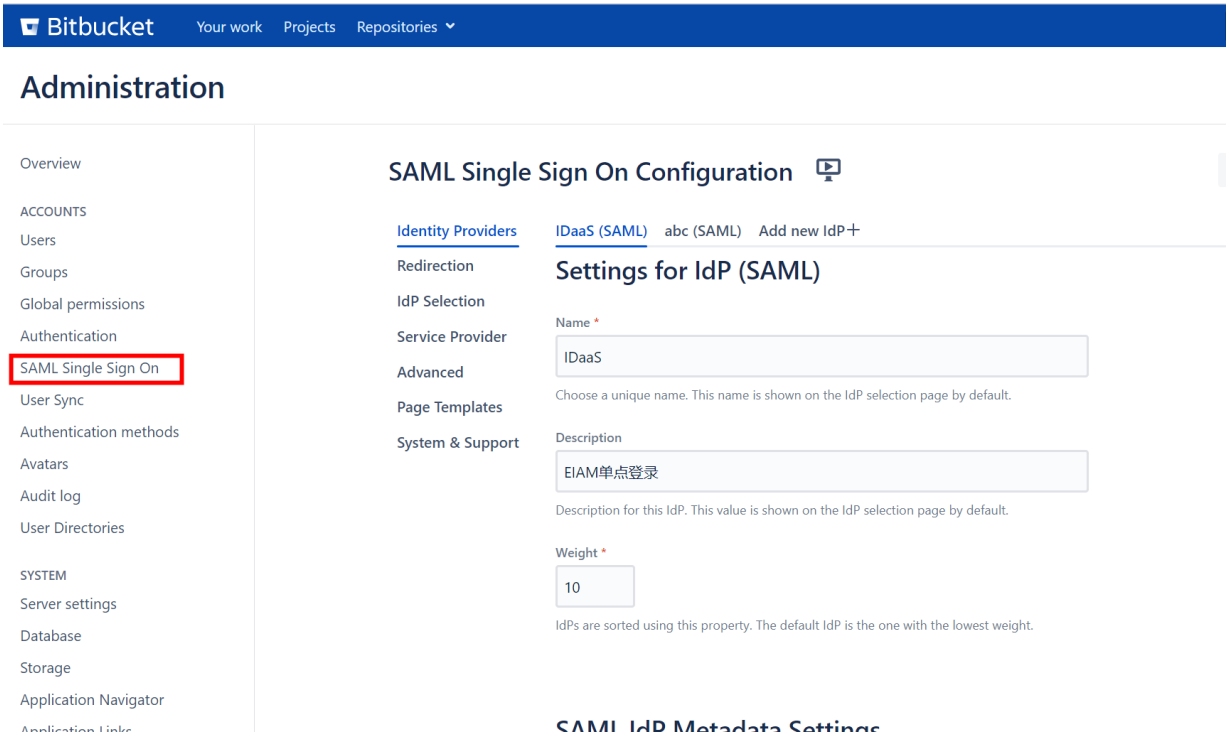
Bitbucket 插件市场中有多款用于实现单点登录的插件，点击 **设置按钮-Manage apps**，搜索“SAML Single Sign On”，在搜索列表中，选择“SAML Single Sign On - SAML SSO Login”插件（该插件由 miniOrange 提供），点击“立即安装”。

插件安装成功之后，在 **User-installed apps** 中可找到 **SAML Single Sign On for Bitbucket**。

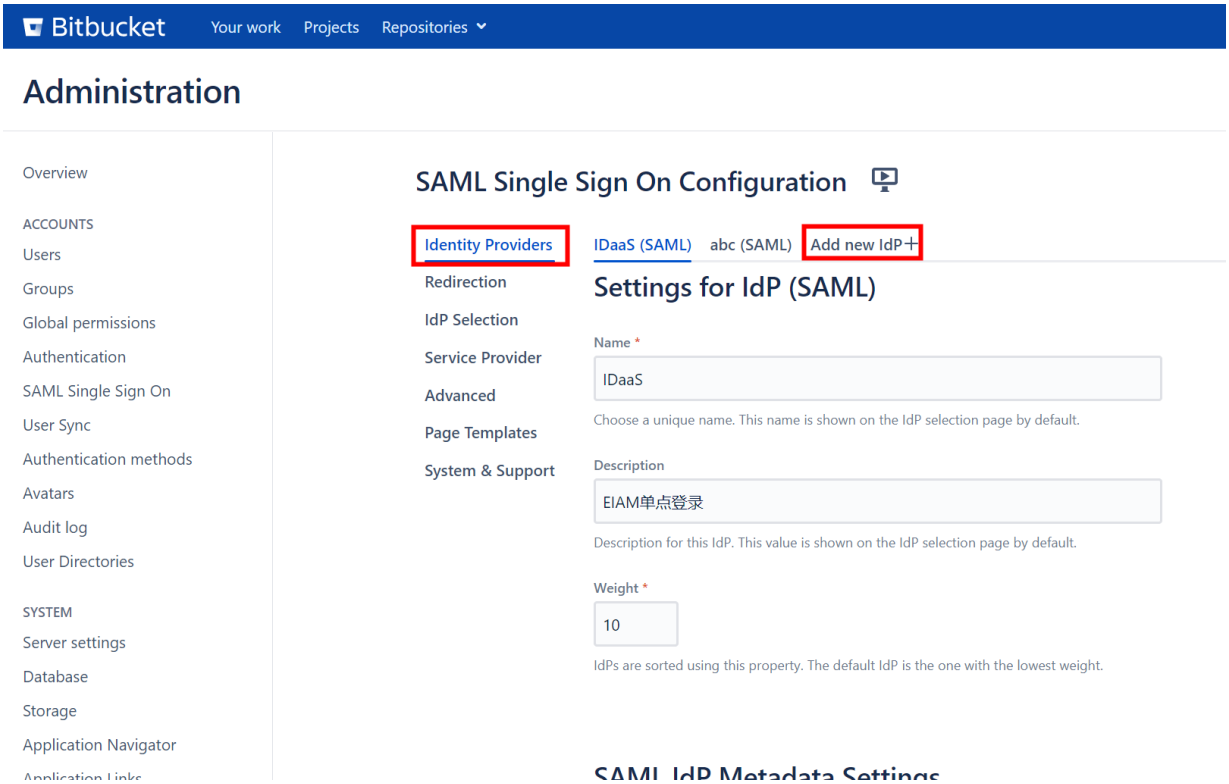


2. 配置 SSO

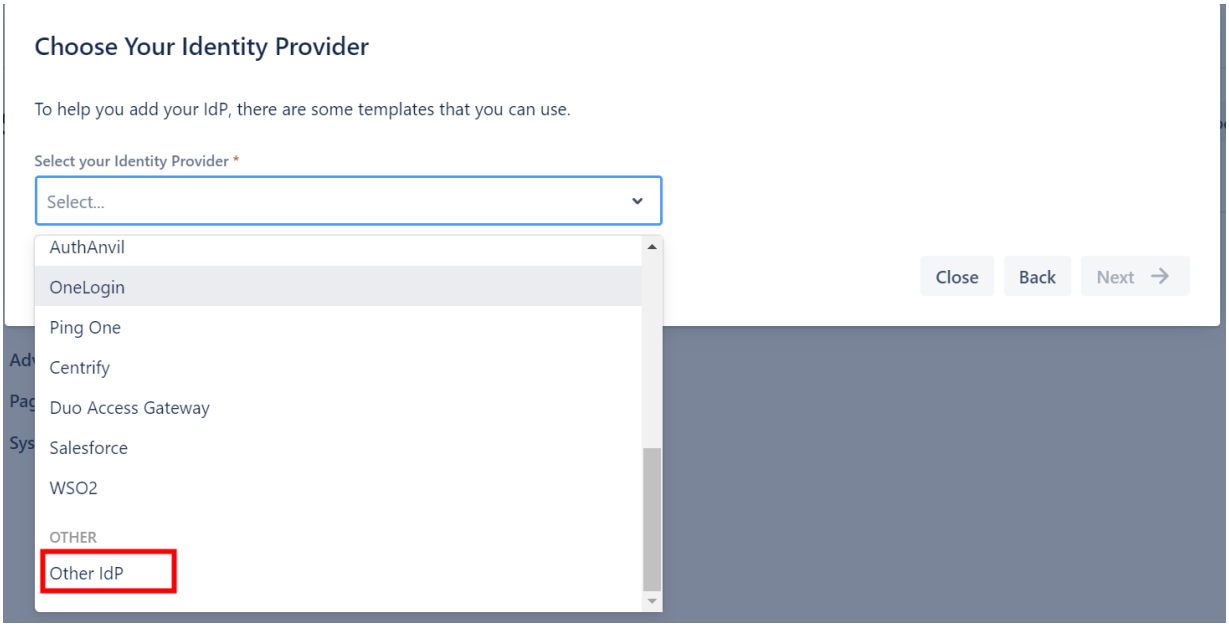
启用插件之后，Bitbucket 将在左侧导航栏中增加菜单 **SAML Single Sign On**，点击该菜单，即可进入编辑页面，如下图所示：



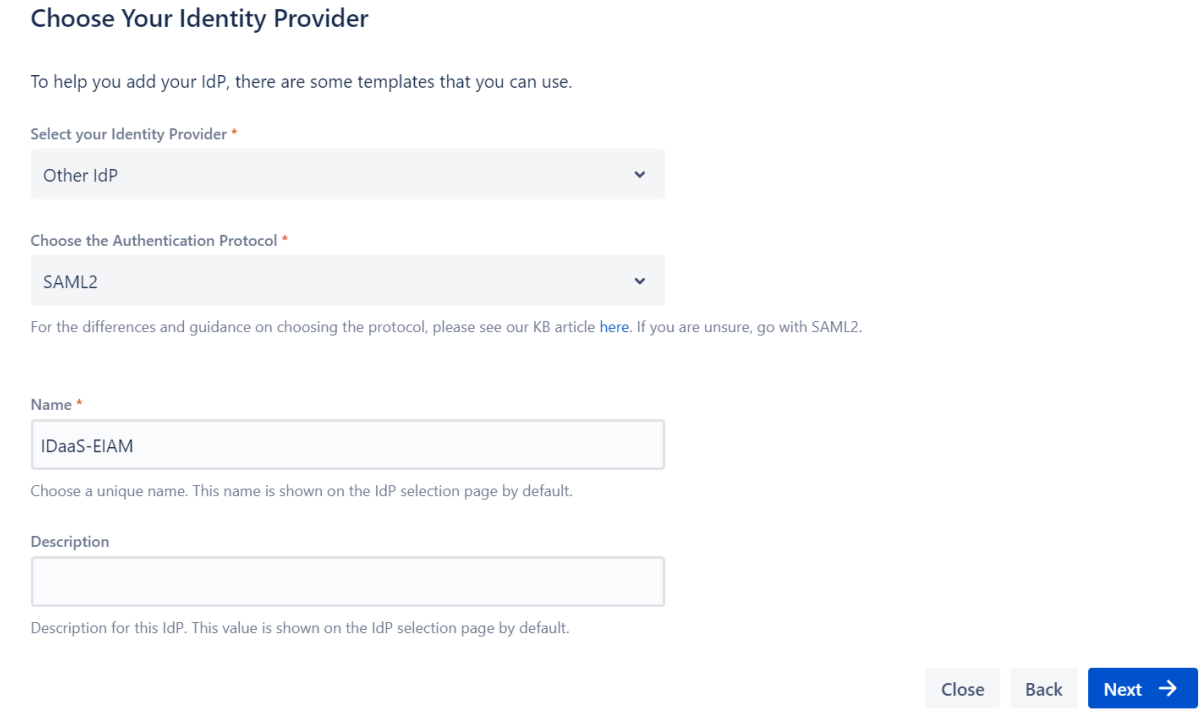
在 **Identity Providers** 标签内，点击 **Add new Idp**，如下图所示：



点击 **Add new Idp** 图标后，弹框，选择您的身份提供方 **Other Idp**。



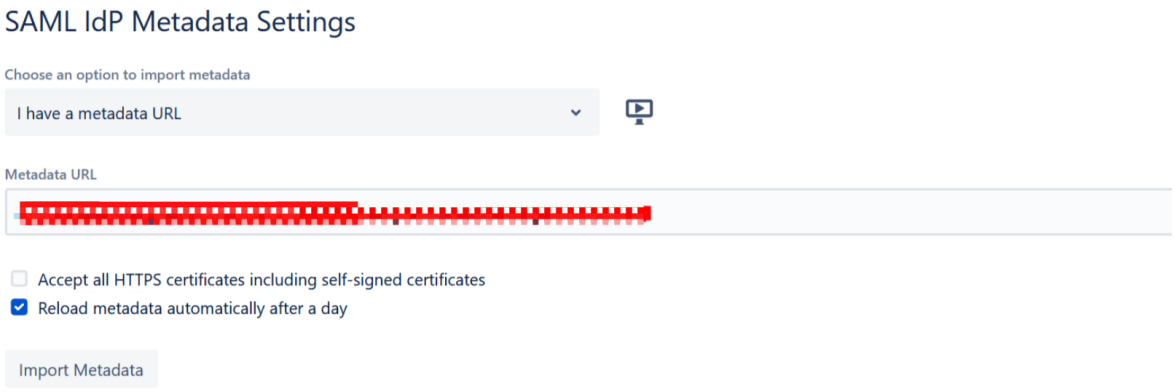
选择完身份提供方后，填写Name，如下图，然后点击 **Next** 。



找到界面中的“SAML Idp 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IdP信息。

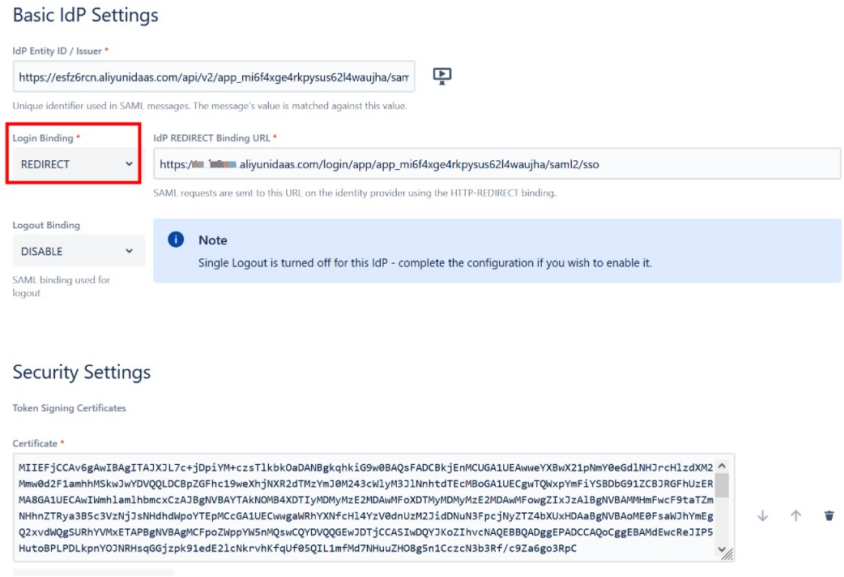
- **上传IDP元数据**

下载列表，选择 **I have ametadata URL** 页签，“Metadata URL”填写 **Idp元数据** 地址。



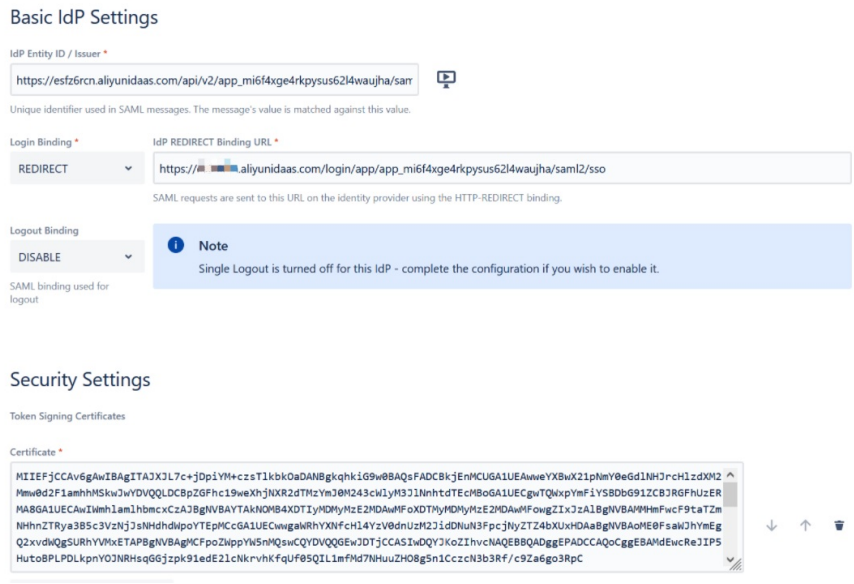
字段	IDaaS 中字段名称	说明
Name		输入一个名字，例如： AliyunIDaaS
Metadata URL	IdP 元数据 IdP Metadata	从 IDaaS 单点登录配置页 **应用配置信息** 中获取，对应 “IdP 元数据”，您可以将元数据下载到本地之后，然后在当前页面进行上传。

导入完成后可看到如下图，修改Login Binding 方式为 **REDIRECT** 。



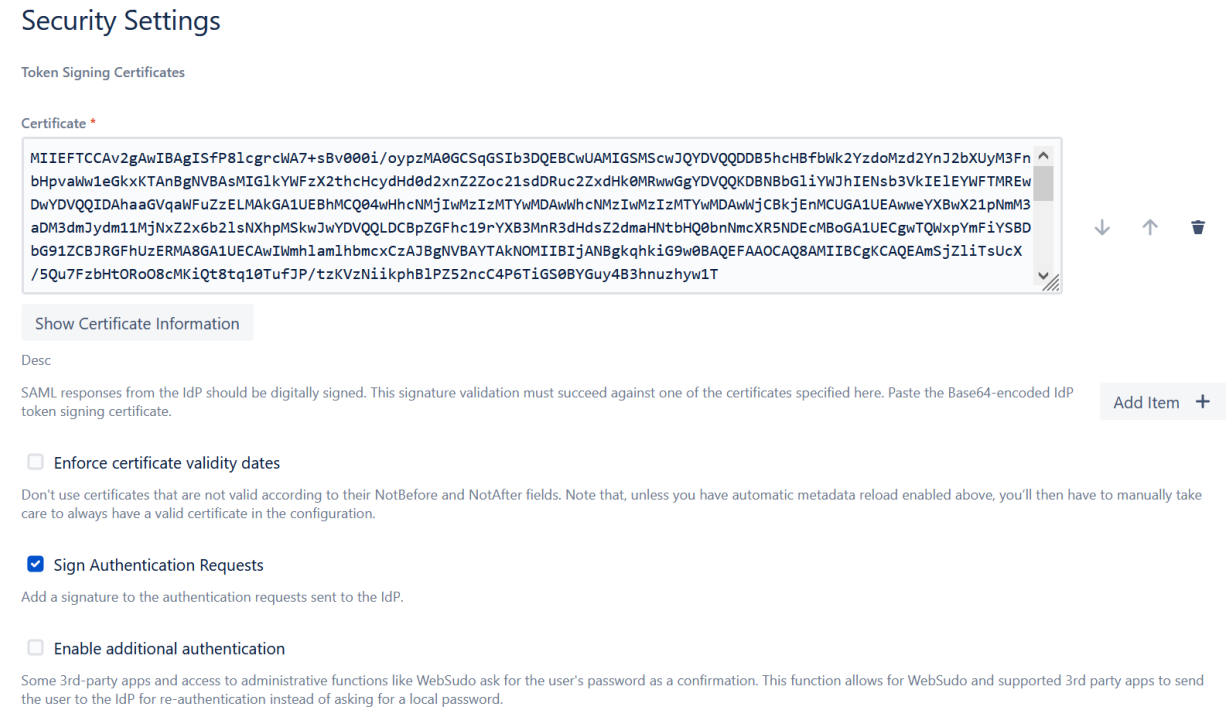
- **手动填写IDP元数据**

将 IDaaS 中获取到的信息填写进入表格中。参数对照如下：

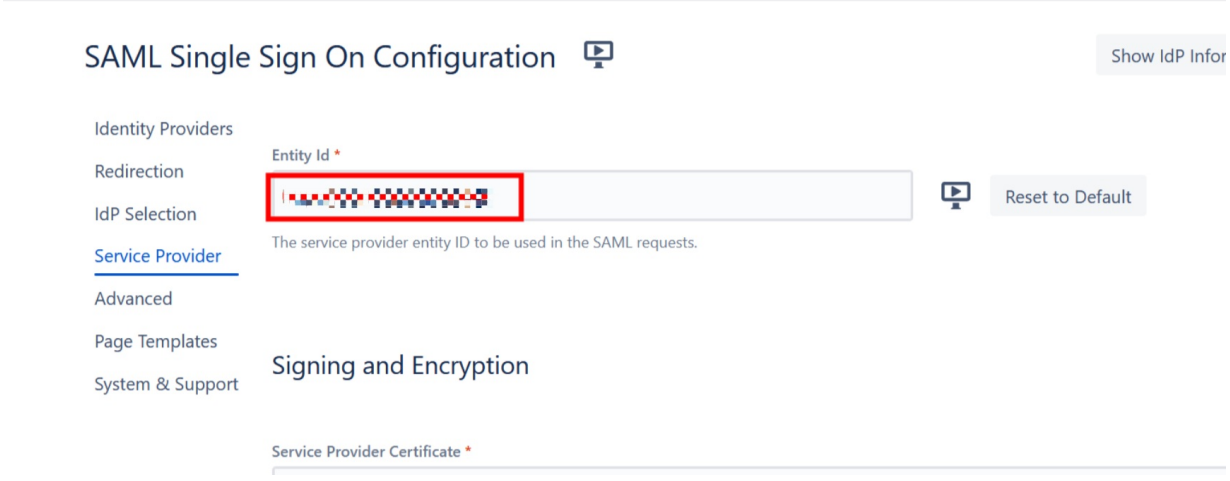


字段	IDaaS 中字段名称	说明
Identity Provider Name		输入一个名字，例如： AliyunIDaaS，这个名字将在 WordPress 登录页中显示。
IdP Entity ID / Issuer	IdP 唯一标识 IdP Entity ID	从 IDaaS SSO 配置页 **应用配置信息** 中获取，对应 “ IdP 唯一标识”
Login Binding	SP发起请求方式	**固定值：REDIRECT**
Idp REDIRECT Binding URL	IdP SSO 地址 IdP Sign-in URL	从 IDaaS SSO 配置页 **应用配置信息** 中获取，对应 “ IdP SSO 地址”
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”

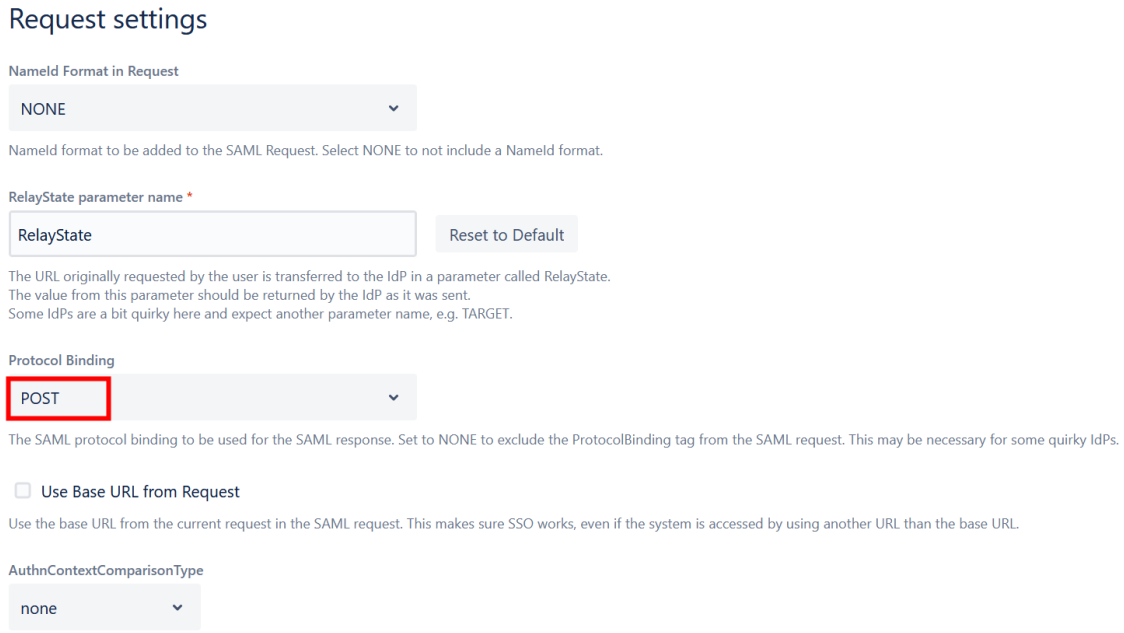
同时关闭 “Sign Authentication Requests”



选中 **Service Provider**，修改Entity Id为Bitbucket的域名

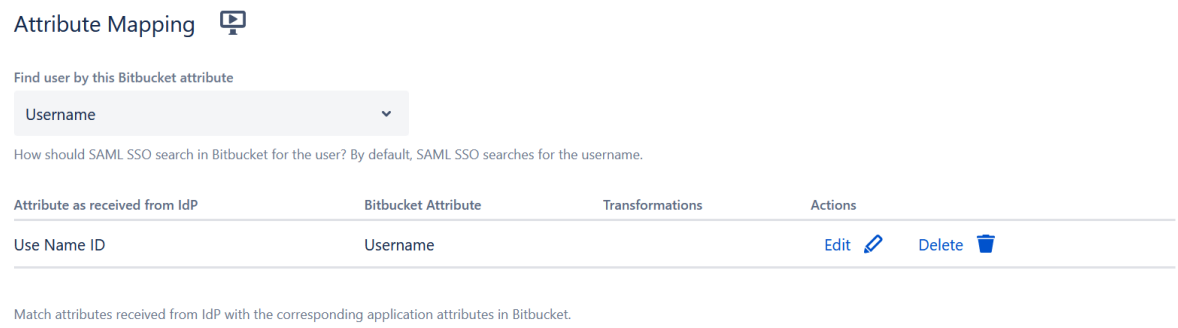


修改Protocal Binding方式为 **POST** 。



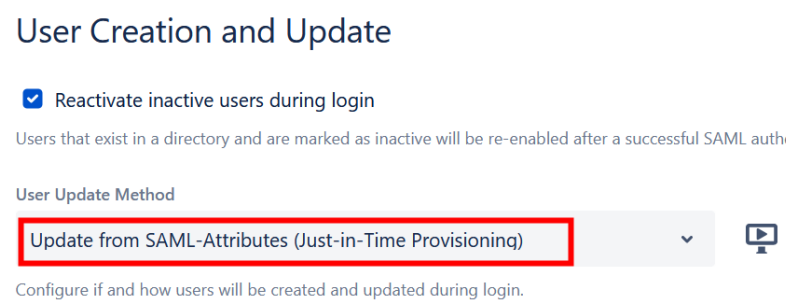
3. 配置属性映射

若只进行单点登录，则在 **Find user by Bitbucket attribute**，选择对应的映射规则即可。



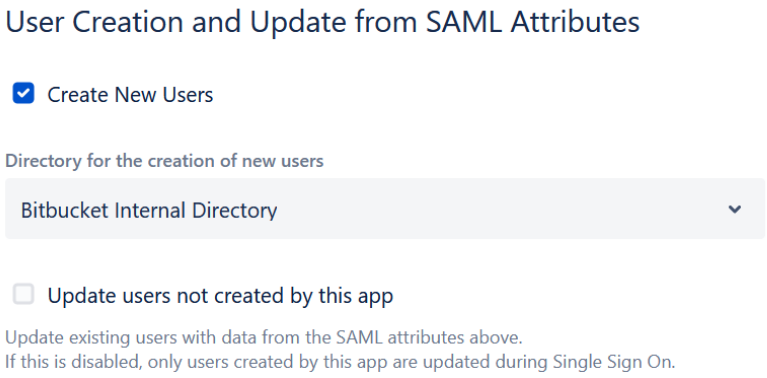
4. 单点登录时同步配置（可选）

选择 User Update Method 为 **Update from SAML-Attribute(Just-in-Time Provisioning)**，如下图：

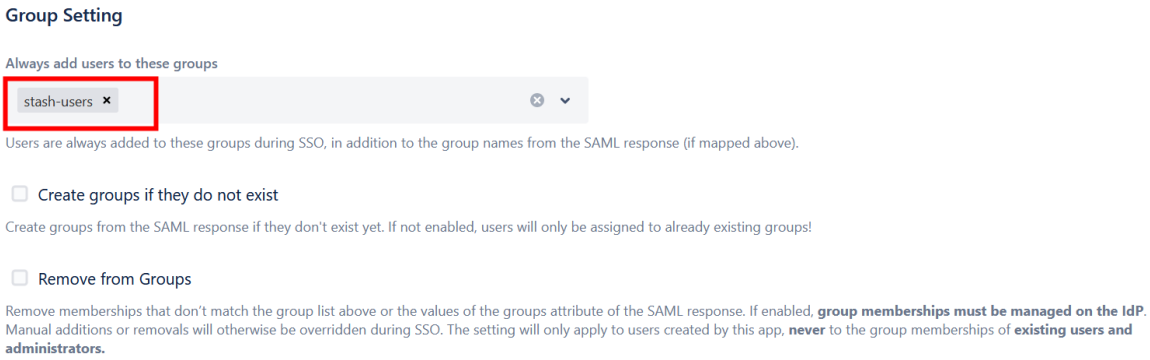


开启“Create New Users”

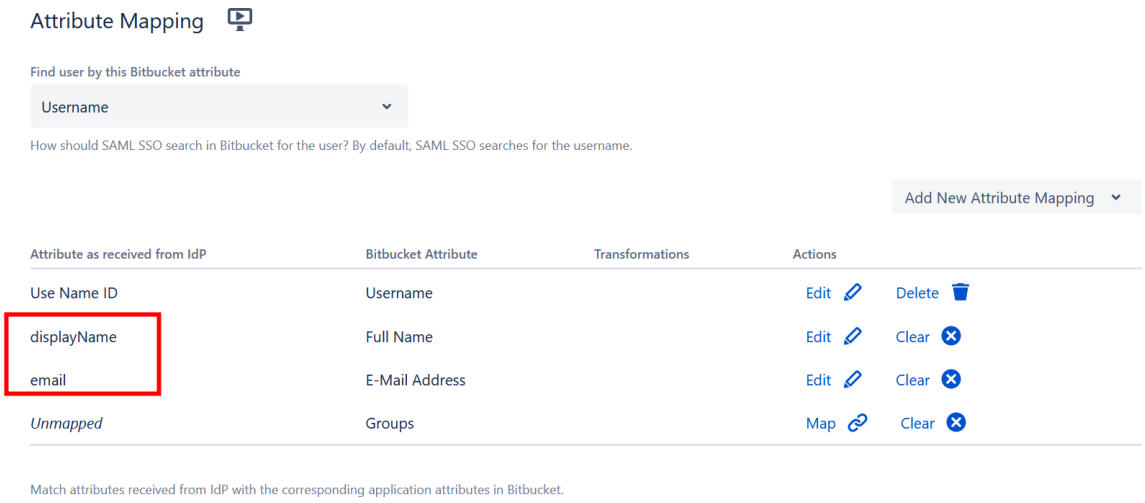
建议关闭 **Update users not created by this app**(关闭后，同步时修改只修改单点登录同步过来的用户)



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



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：



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

Full Name	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 Bitbucket。
E-Mail Address	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 Bitbucket。

四、尝试 SSO

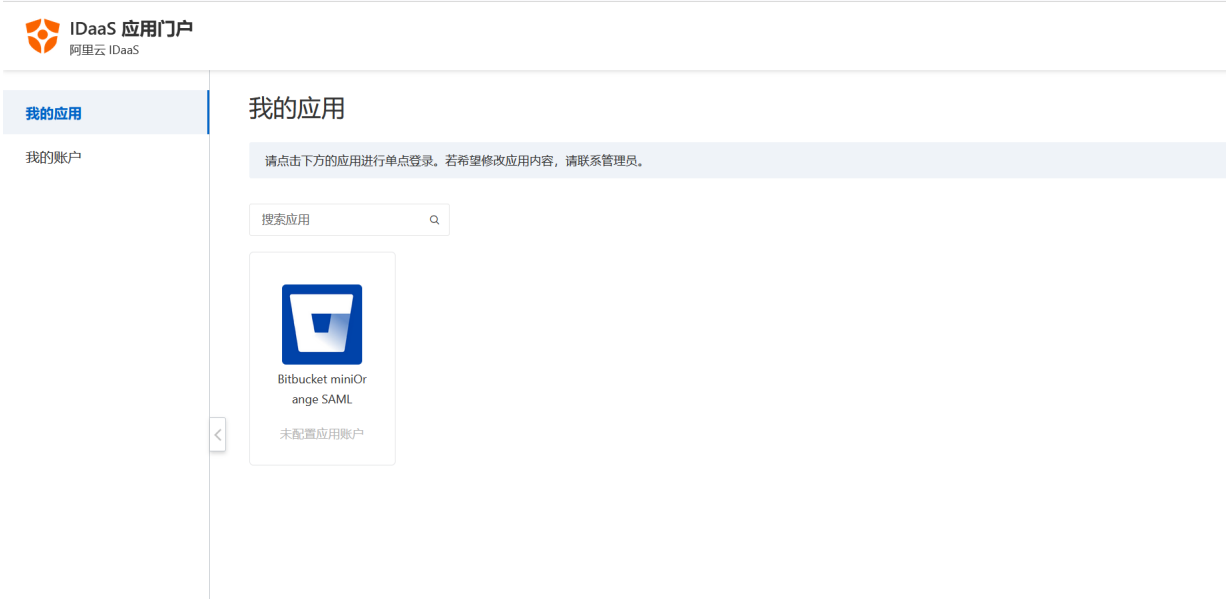
您已经可以尝试 Bitbucket SSO。

Bitbucket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。

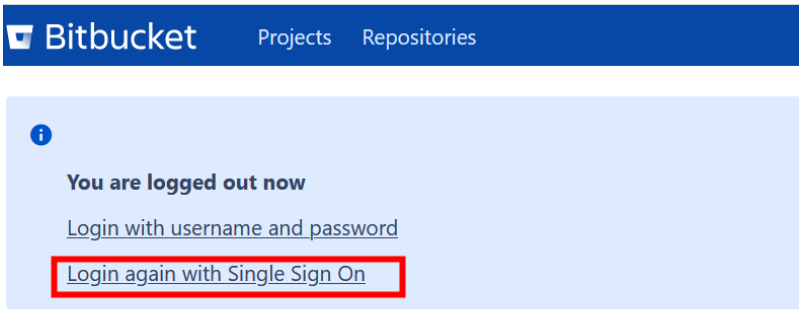
IDP 发起

请用已授权使用 Bitbucket 的 IDaaS 账户，登录到 IDaaS 门户页，点击页面上 Bitbucket 图标，发起 SSO。



SP 发起

请在匿名浏览器中，打开 Bitbucket 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 Bitbucket 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。

> 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/documentation/current/en/manual/web_interface/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。

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。

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。

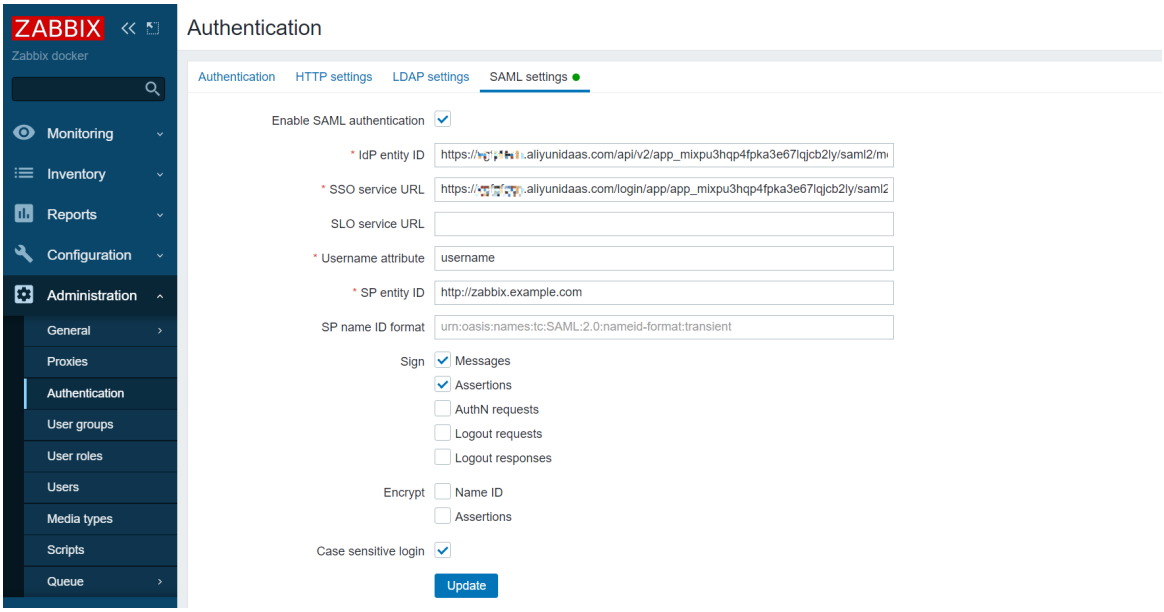
从中您需要获取 `IdP 唯一标识` `IdP SSO 地址` 和 `公钥证书` 三个参数。其中 `公钥证书` 需要您下载到本地。

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。



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。
IdP entity ID	IdP 唯一标识 IdP Entity ID	从 IDaaS SSO 配置页【应用配置信息】中获取。
SSO service URL	IdP SSO 地址 IdP Sign-in URL	从 IDaaS SSO 配置页【应用配置信息】中获取。
Username attribute		填写 `username` 即可。
SP entity ID	-	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 `$SSO['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. **文件改名**。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. **文件上传**。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。

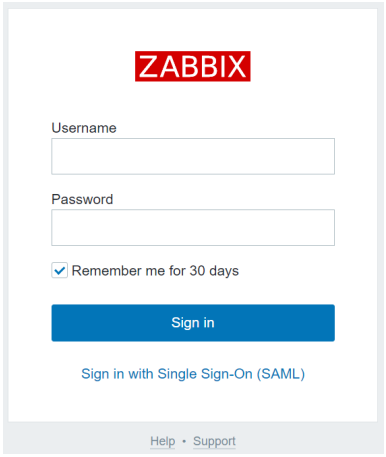
注意：Zabbix 支持【自动创建账户】（Just-in-time Provisioning），单点登录时，若 Zabbix 中不存在指定应用账户，则会直接创建，不会拒绝访问。请在 IDaaS 中管理 Zabbix 访问权限。

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。

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 。



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 Gitlab 单点登录。

应用简介

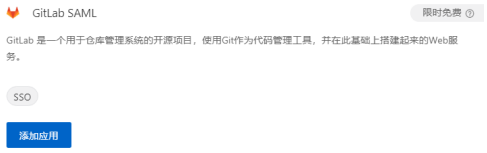
GitLab 是一个用于仓库管理系统的开源项目，使用Git作为代码管理工具，并在此基础上搭建起来的Web服务。

> 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。



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 GitLab 的服务地址填写进来，注意服务地址不要以“/”结尾

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 GitLab 完成配置所需要的参数。

二、配置 Gitlab

根据 Gitlab 官网文档 ，您需要在部署环境中编辑 gitlab 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',
      issuer:'http://gitlab.example.com/users/auth/saml',
      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_mivpoqqmz7zrslxcmlyxa25me4/saml2/sso',
      name_identifier_format:'urn:oasis:names:tc:SAML:2.0:nameid-format:persistent',
      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

args.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
args.idp_sso_target_url	IdP SSO 地址，从 IDaaS 获得	https://example.aliyunidaas.com/login/app/app_mivpoqqmz7zrslxcmlyxa25me4/saml2/sso
args.idp_cert_fingerprint	Idp 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 Gitlab 登录页下方，应出现【使用阿里云 IDaaS 账户登录】按钮。

配置完成。

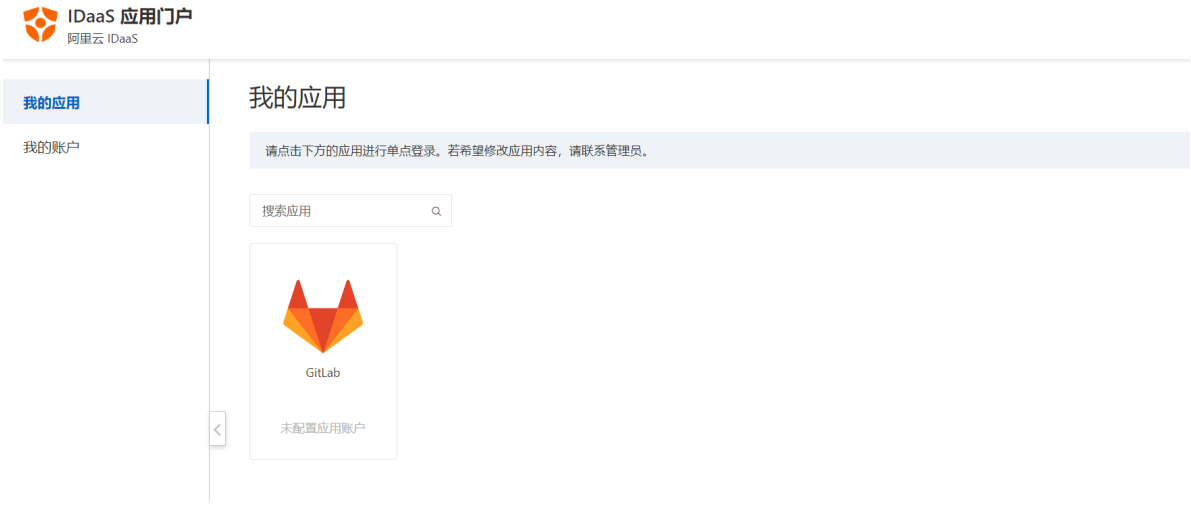
三、尝试 SSO

您已经可以尝试 GitLab SSO。

本文中 GitLab 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 GitLab 发起） SSO 流程。

IdP 发起

请用已授权使用 GitLab 的 IDaaS 账户，登录到 IDaaS 门户页，点击页面上 GitLab 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 。

IDaaS 验证用户身份通过后，将直接登录到 GitLab 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。

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。

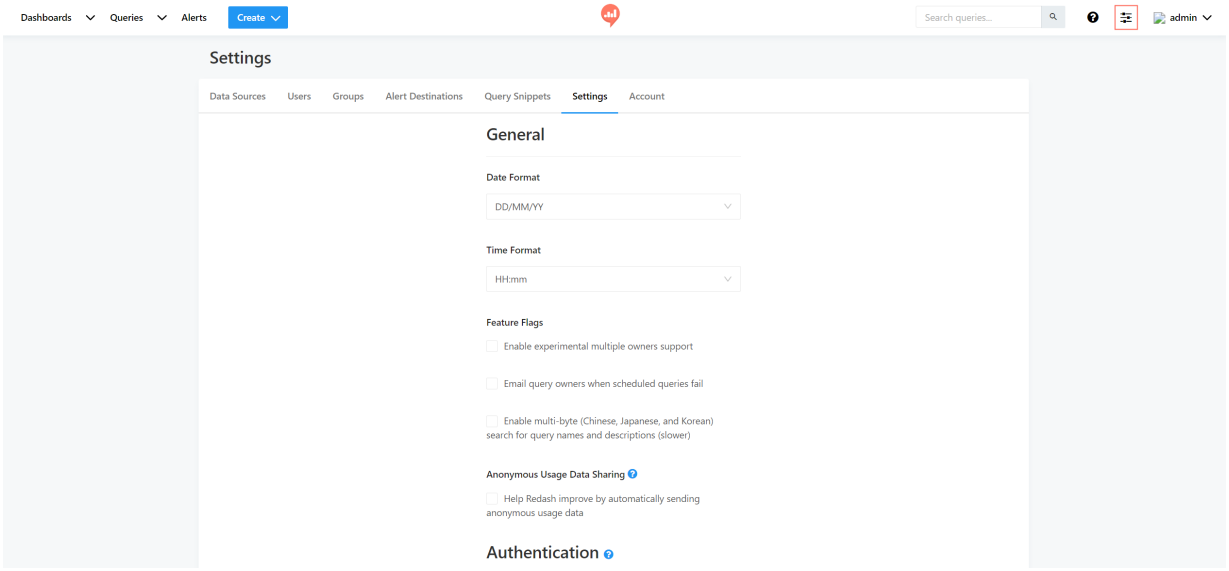
> 说明
> 提示 应用账户：默认使用 IDaaS 账户名作为应用登录标识。应用中配置IDaaS邮箱作为账户标识，才能完成 SSO。 若希望灵活配置，请参考 单点配置通用说明 - 应用账户 进行配置。 授权范围：若希望指定可访问应用的 IDaaS 账户，请参考 单点配置通用说明 - 应用账户 进行配置。

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。

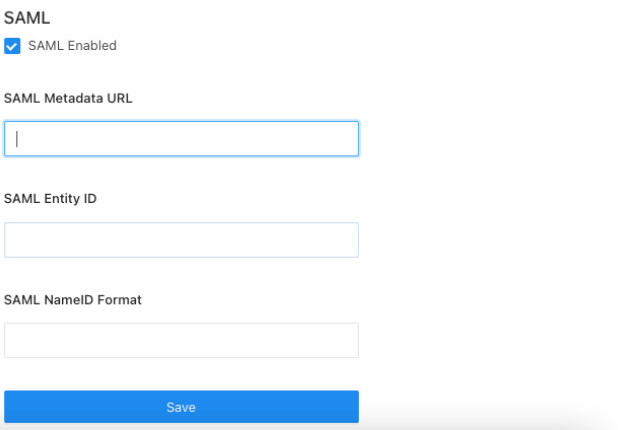
三、配置 Redash

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：



在 Authentication 区域，勾选【SAML Enabled】，将展开如下配置界面：



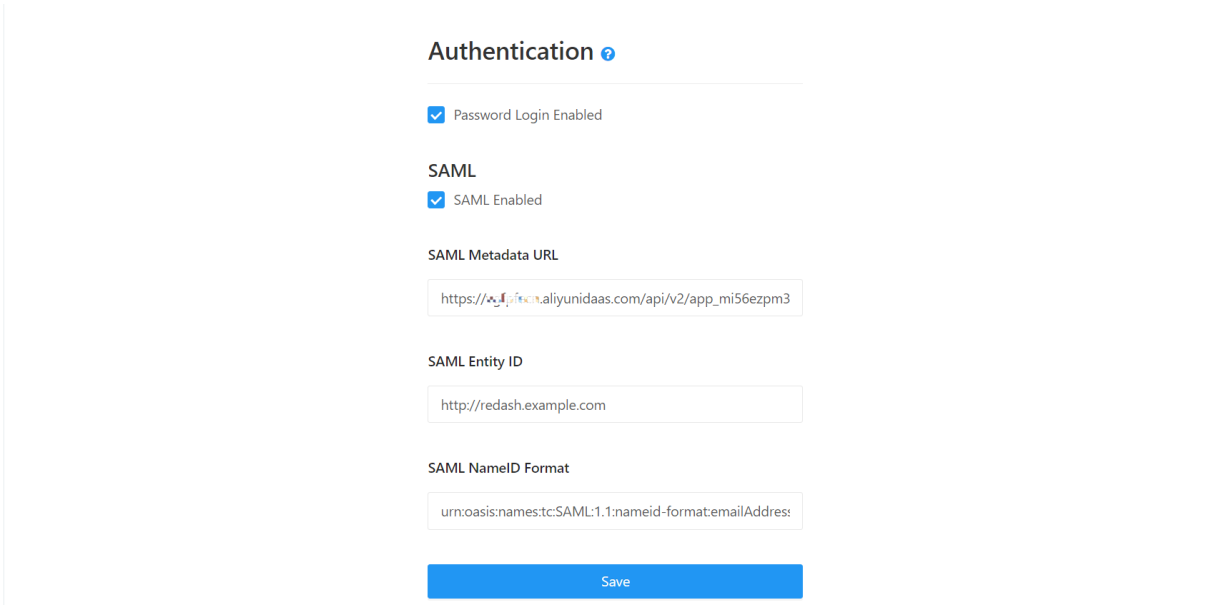
2. 进行 SAML 配置。

将 IDaaS 【应用配置信息】中的参数全部填写到配置表单中。

字段	别称	说明

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：



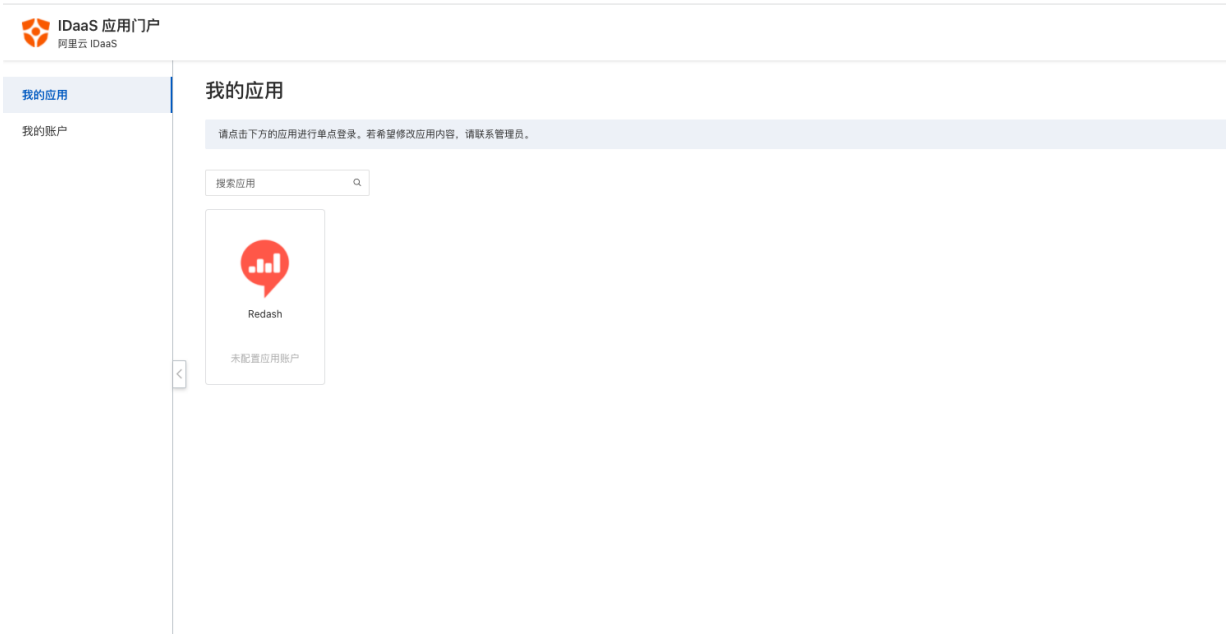
点击保存后，单点登录配置完成。

四、尝试 SSO

您已经可以尝试 Redash SSO。

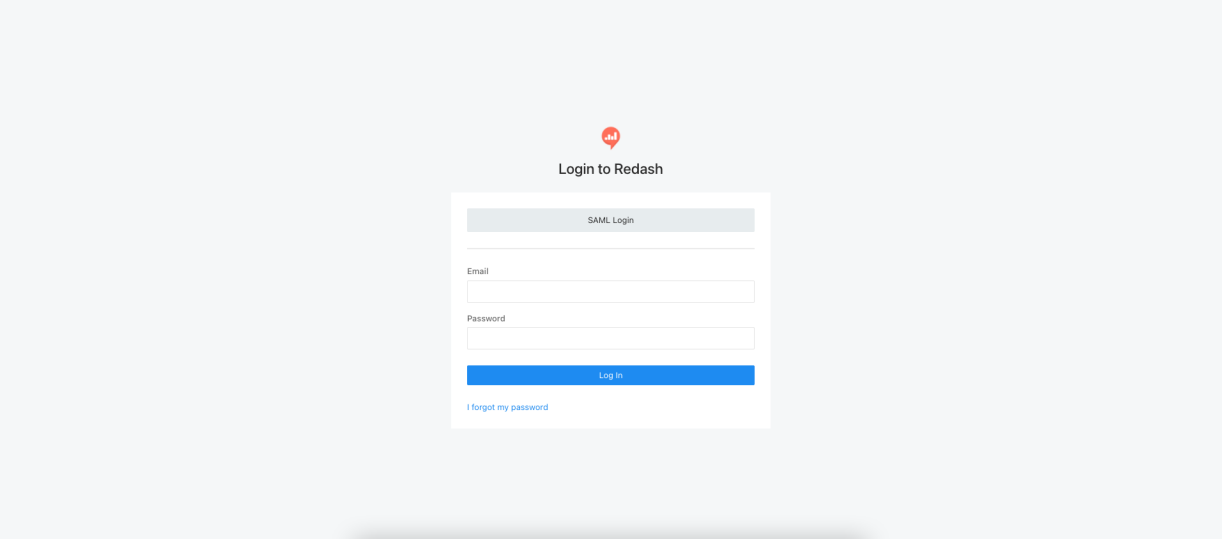
IDP 发起

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。



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 。



IDaaS 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。

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

复制Argo CD服务访问地址，例如：【https://argocd.example.com】。

将【https://argocd.example.com】填写到表单中。

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。

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。
ssoIssuer	IdP 唯一标识 IdP 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,
# 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: argocd
  name: argocd-cm
  namespace: argocd
  resourceVersion: "124561"
  uid: 9e161ab5-807e-449a-8488-7e764b4ed349
```

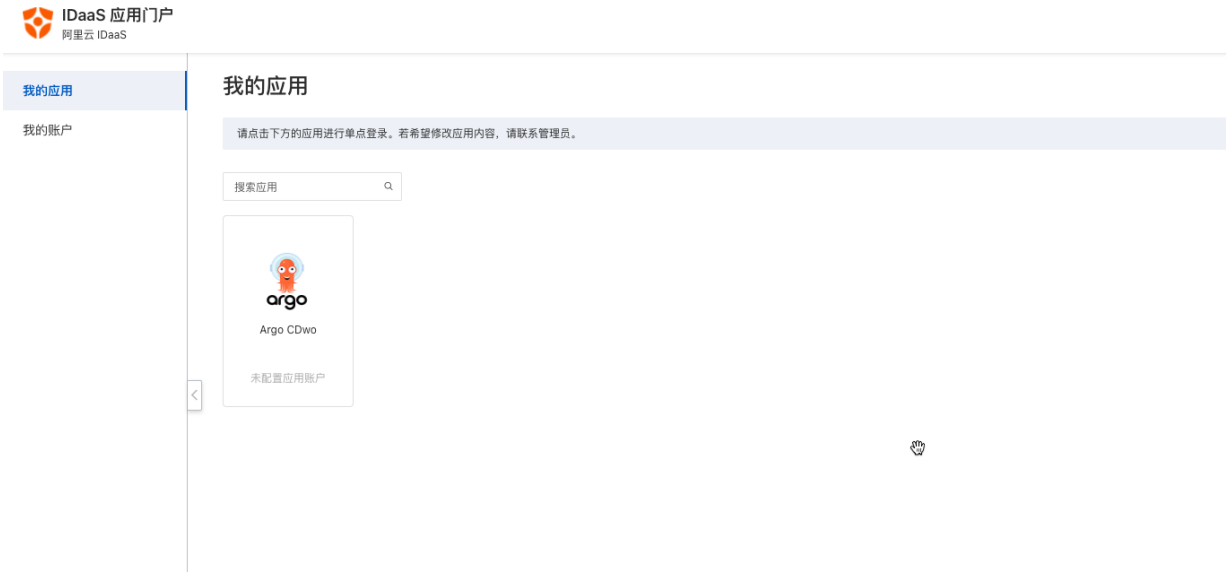
保存配置，重启服务吗，开启单点登录。

四、尝试 SSO

您已经可以尝试 Argo CD SSO。

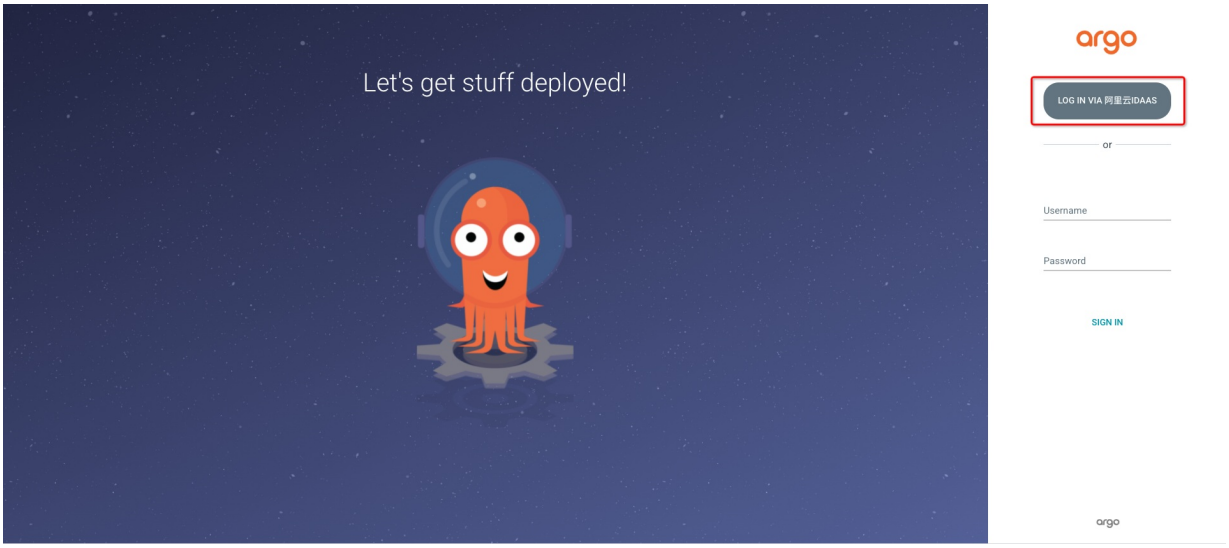
IDP 发起

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。



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
- 阿里云应用相关FAQ
- 钉钉相关FAQ
- 单点登录概述

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IP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。

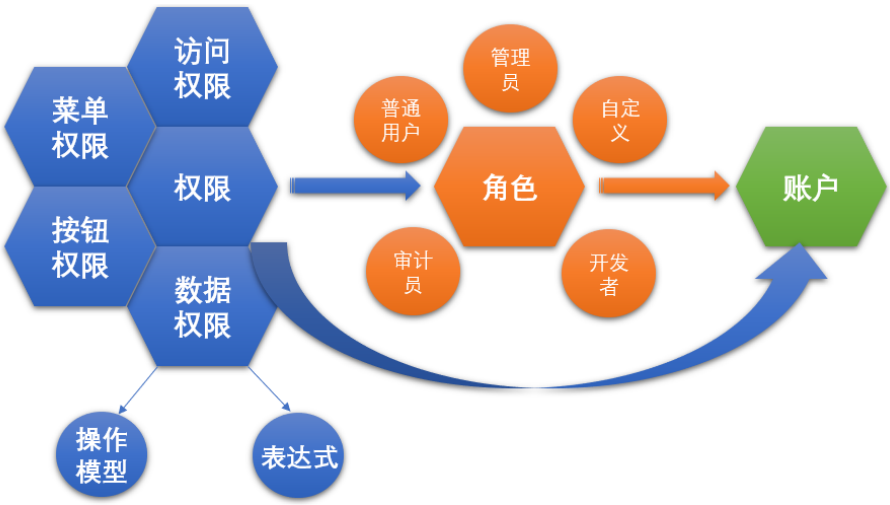
- 优点：便于角色划分，更灵活的授权管理；最小颗粒度授权

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。



2. 三级权限

我们将整体授权类型划分为三级

（1）一级权限：访问权限

（2）二级权限：菜单、按钮权限

（3）三级权限：数据权限

依据不同等级的授权，来控制授权的最小的颗粒度。

3. 权限系统

IDaaS权限系统，不仅支持IDaaS本身的一系列授权活动，还支持第三方接入，做到真正意义上的集中授权。我们提供丰富的API接口，方便业务系统能够更好对接。

三、主要功能

权限系统主要包括以下功能：

（1）默认权限系统（IDaaS平台）

1、角色管理

1）可以授予用户开发者角色

2、授权管理

1）授权->角色：支持授权到角色

2）授权->个人：支持授权到个人

3、查看系统详情

1）默认权限系统的权限详情查看

（2）第三方接入（外部系统接入）

1、新增系统

1）系统新建，管理

2、角色管理

1）用户可以按需定义角色

2）支持批量导入

3、授权管理

1）授权->角色：支持授权到角色

2）授权->个人：支持授权到个人

3）表格导入

4、资源管理

1）资源新增

2）资源导入、导出

5、查看系统详情

1）第三方接入系统的权限信息详情查看

5、权限系统API接口清单

1）权限系统全局接口

2）角色管理接口

3）授权管理接口

4）鉴权接口

最佳第三方接入实践，详见第三方业务系统接入权限系统

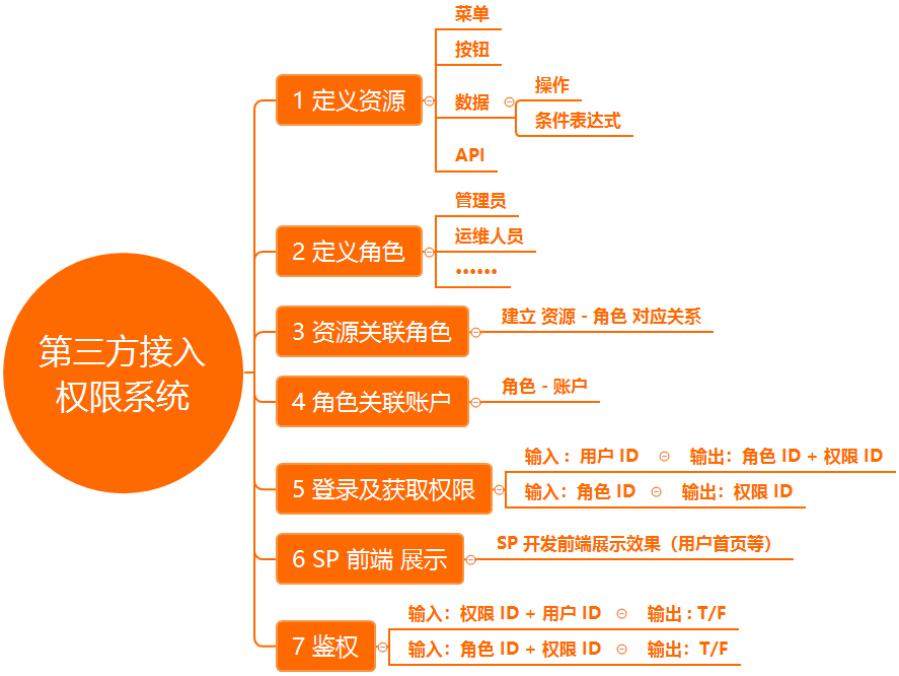
3.2.2. 最佳实践

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

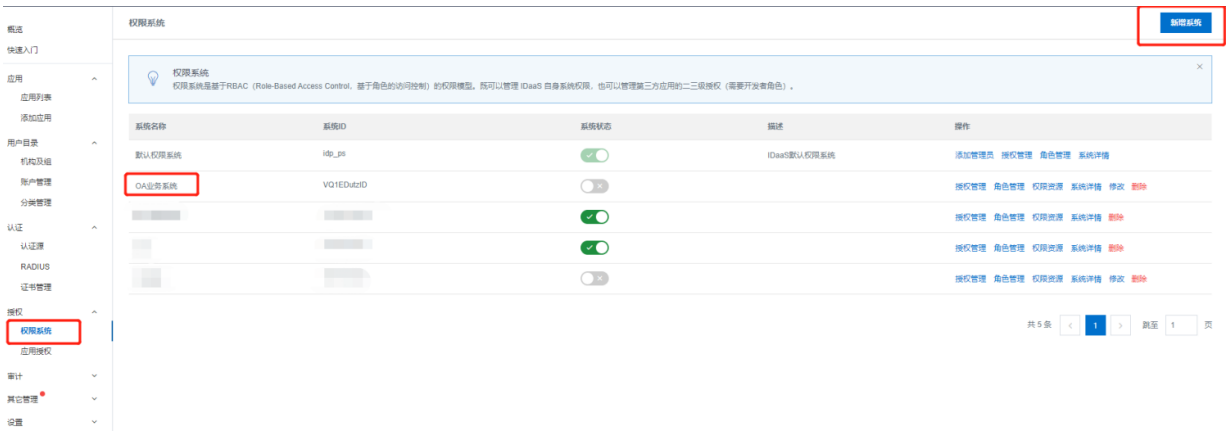
我们简单构建一个与 IDaaS 对接的第三方业务系统 （OA 工作平台），其 OA 系统菜单如下所示。

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。



1、定义资源

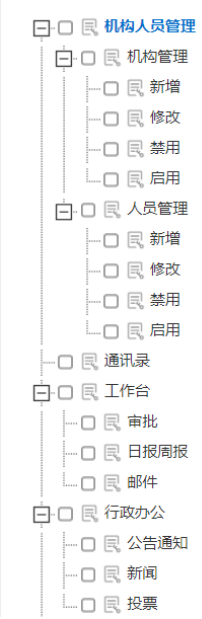
无论是某个功能、菜单、按钮的查看权、使用权，还是某些特定数据的访问权限，都属于一种资源（Resource）。资源支持嵌套树形结构。管理员在这里可以新增、导入、删除、编辑资源，也可以为某资源关联到角色使用。

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，权限系统API接口清单

创建好的权限树如下图所示



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，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

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

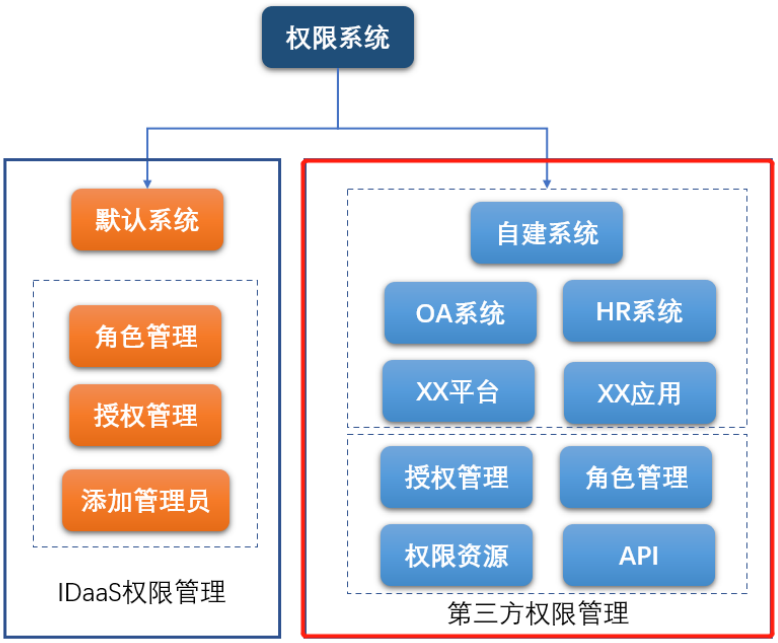
如果您想了解更多 IDaaS 权限系统内容，请联系我们

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

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

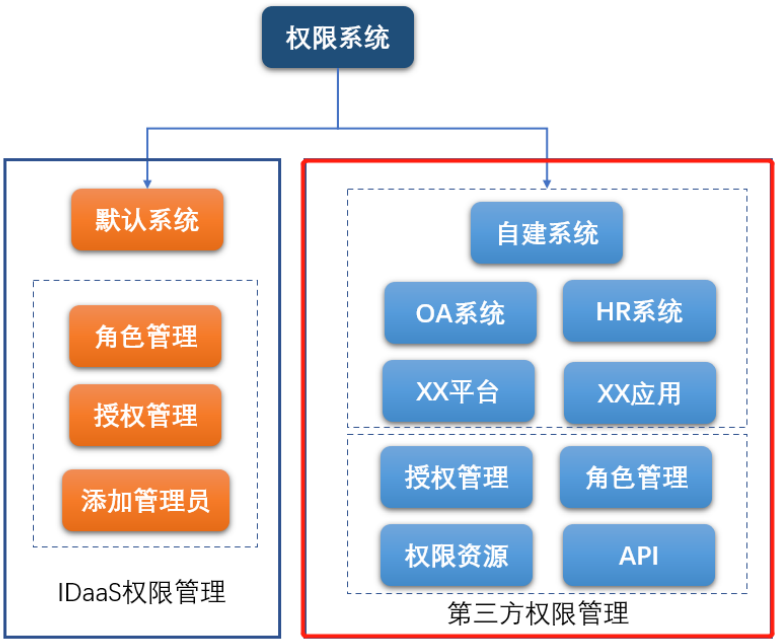
详细第三方接入流程请参考最佳实践： 第三方业务系统接入权限系统

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

3.2.3.2. 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**。

4. 在**新增系统**侧边页，填写系统名称点击**确定**。

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**。

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**。

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。

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。

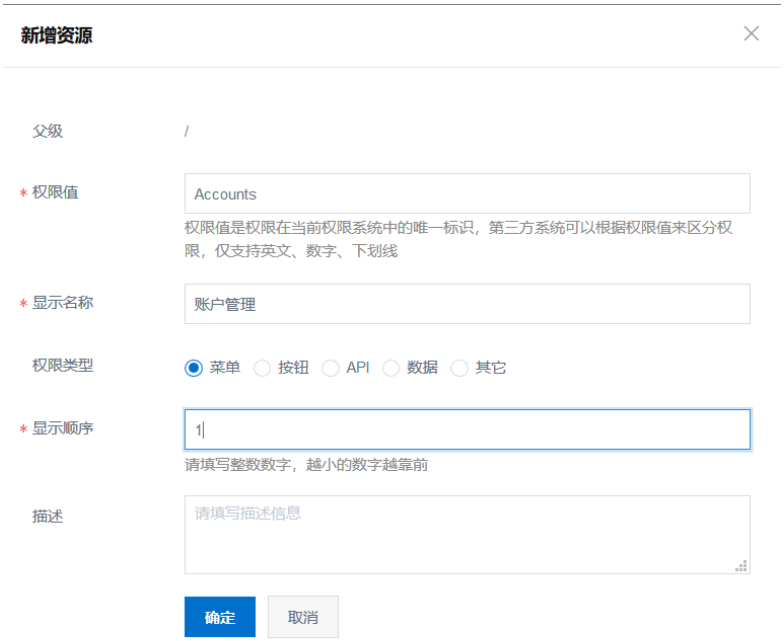
1. 以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考 IT管理员指南-登录。
2. 在左侧导航栏，单击**授权 > 权限系统**。
3. 新建一个权限系统，参考 使用新增系统。
4. 选择新增的权限系统，点击资源管理。
5. 根据需要，执行以下功能。
   - 新增权限资源
   - 新增子级权限资源
   - 导入权限资源
   - 编辑权限资源
   - 删除权限资源

> **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

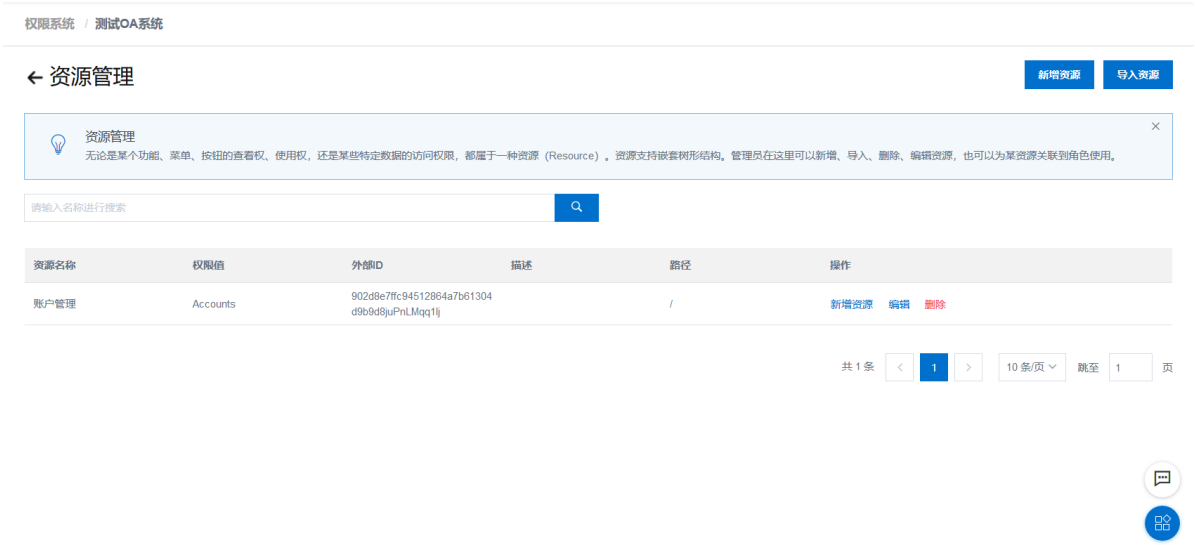
1. 在权限资源页面，点击新增资源

2. 在新增资源侧边页，完成新增资源参数的配置



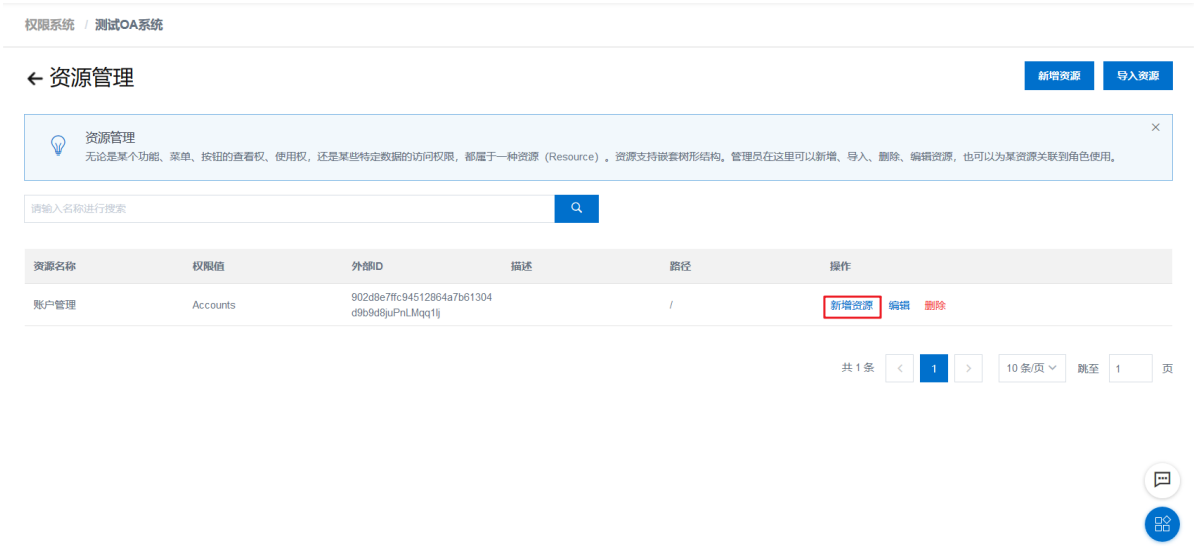
3. 点击确定

创建成功后，会在资源管理页面展示创建的权限资源



新增子级权限资源

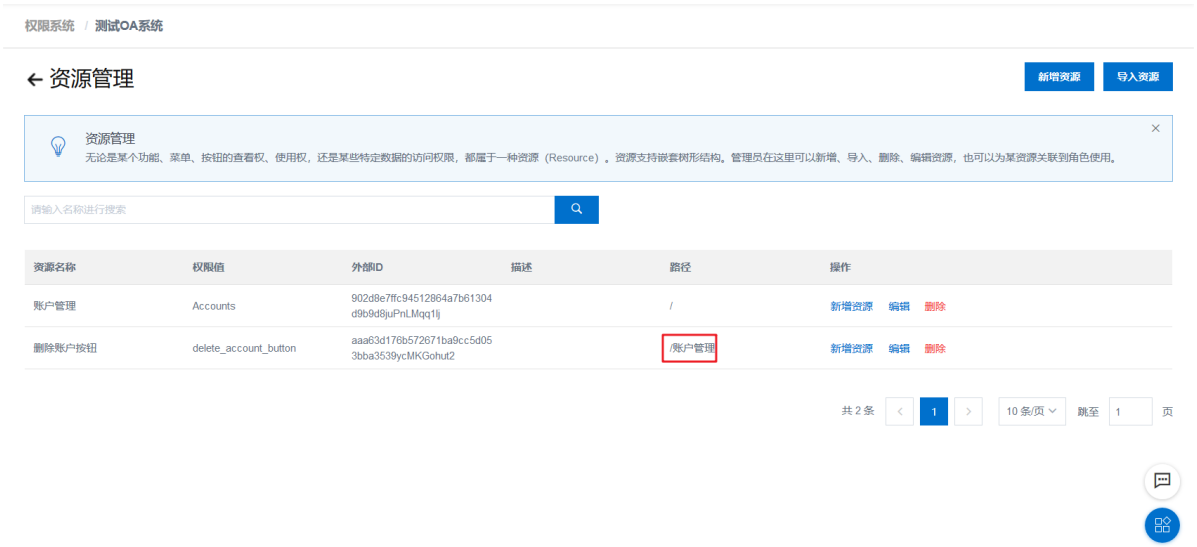
1. 选择需要创建子级资源的资源，点击操作栏中的 新增资源



2. 在新增资源侧边页，完成新增资源参数的配置

3. 点击确定

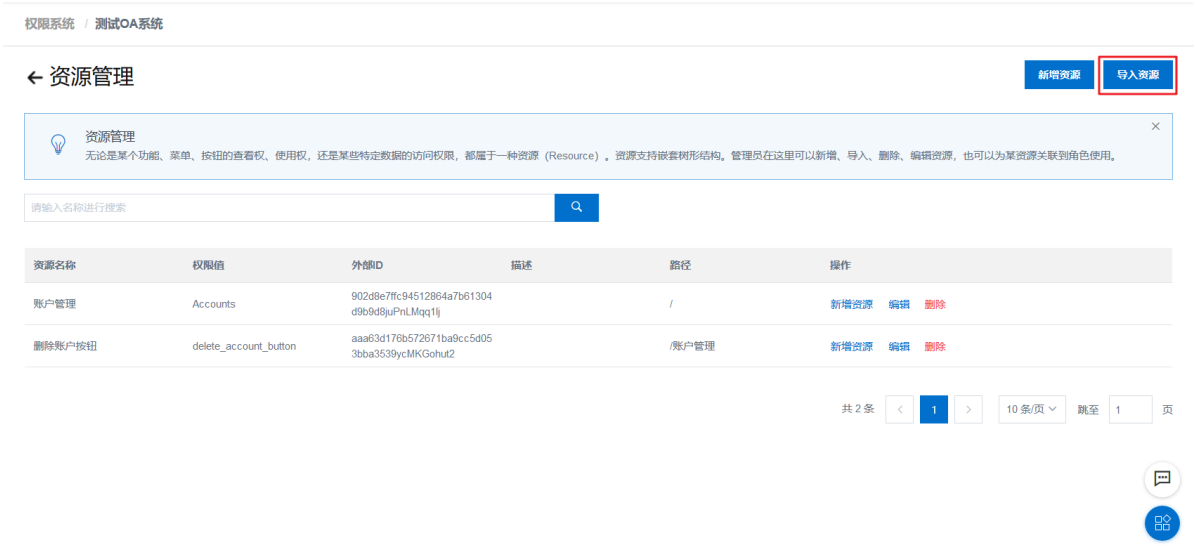
创建成功后，会在资源管理页面展示创建的权限资源，并且路径为之前选择的父级资源



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

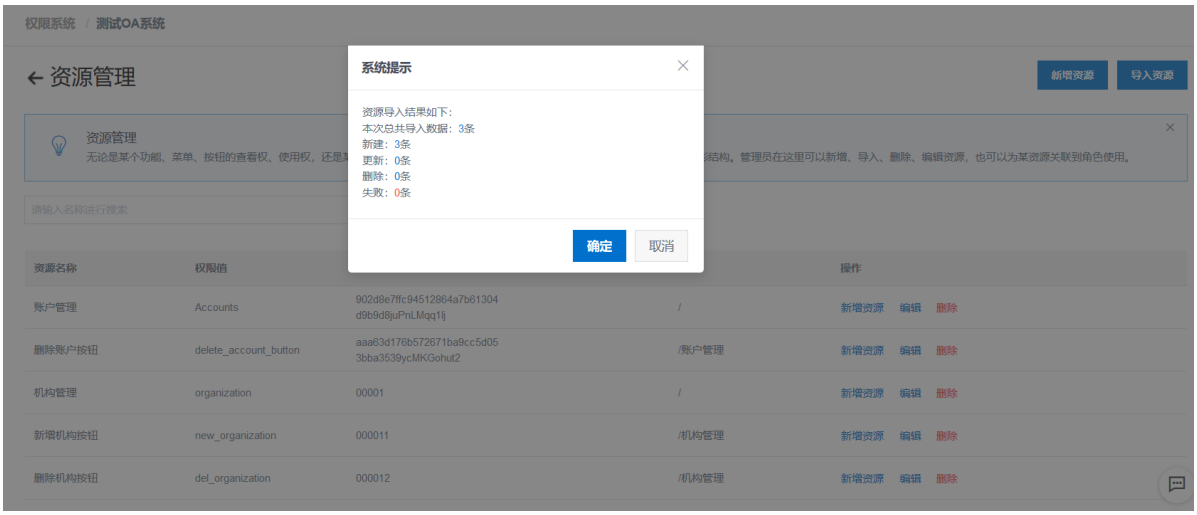


2. 下载 导入格式范例文档，并根据文档填写系统的所有权限资源的信息

3. 点击上传文件，选择填写好的文件

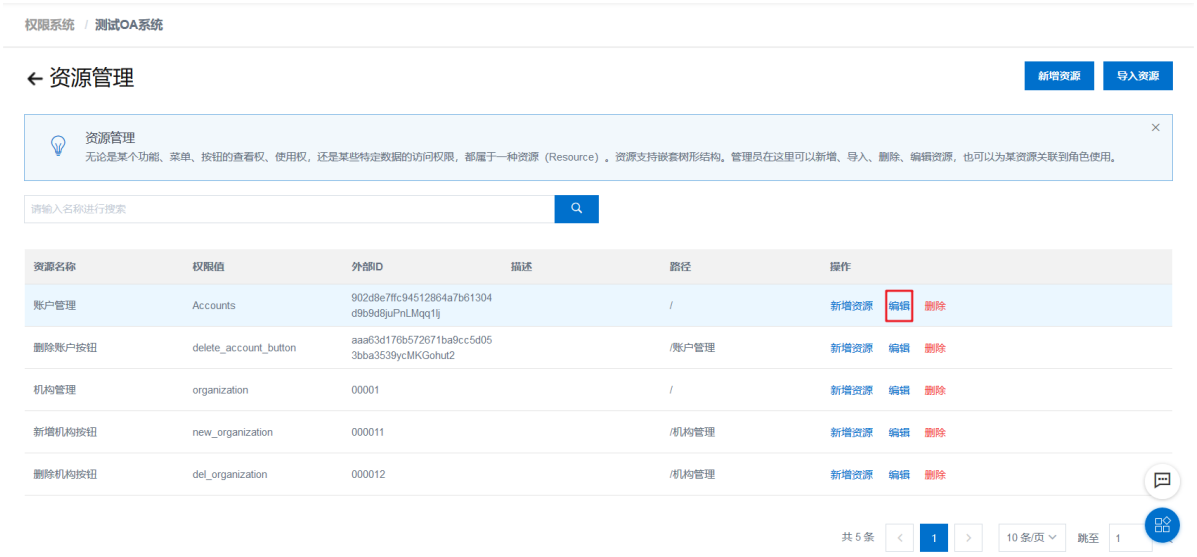
4. 点击导入文件

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



编辑权限资源

1. 选择需要更新的权限资源，点击编辑

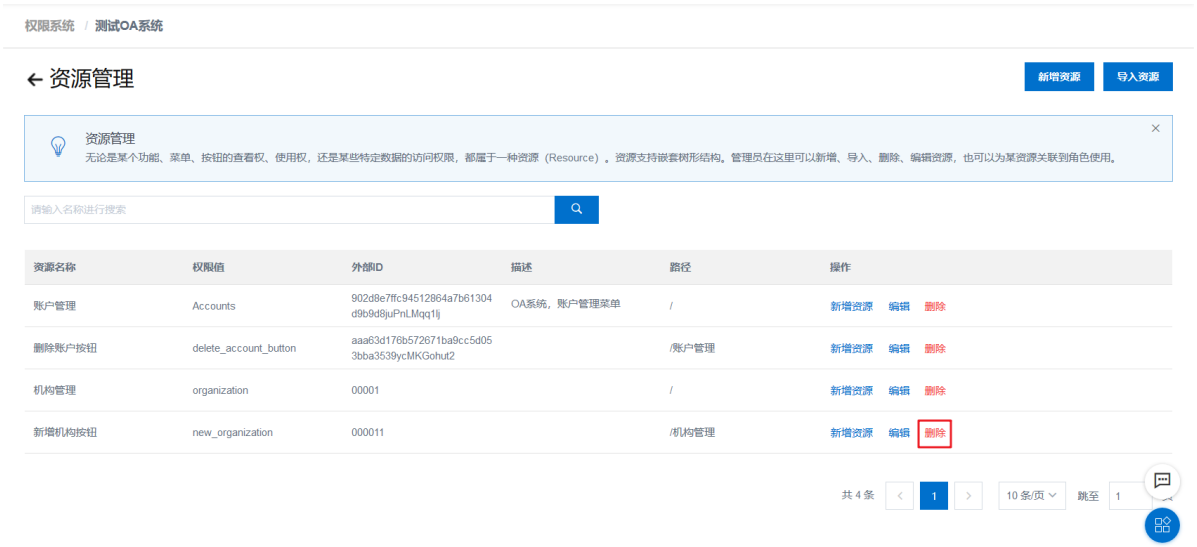


2. 在输入框中更新想要更新的内容，点击确定

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



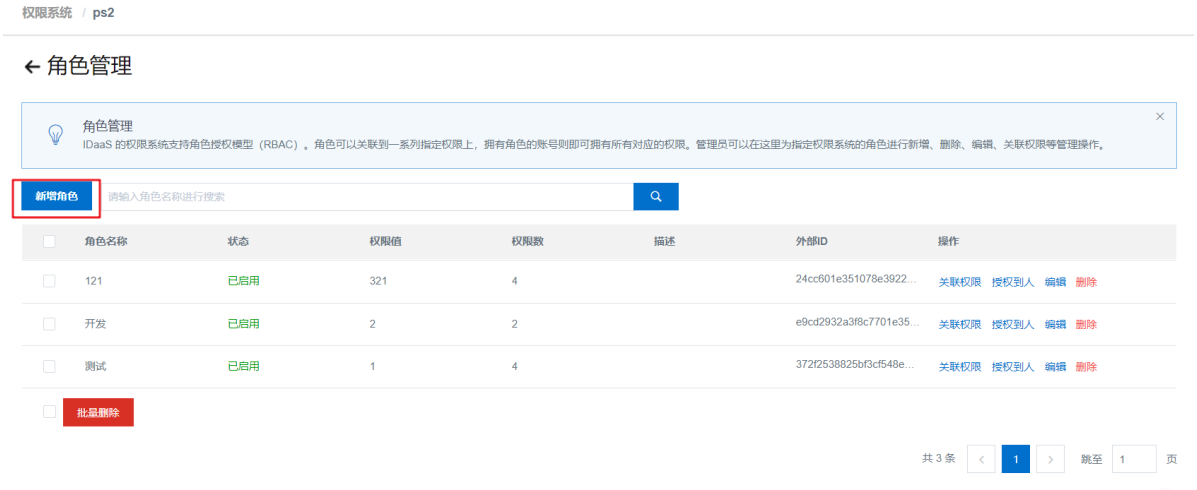
2. 在弹出的对话框中，点击确定

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**

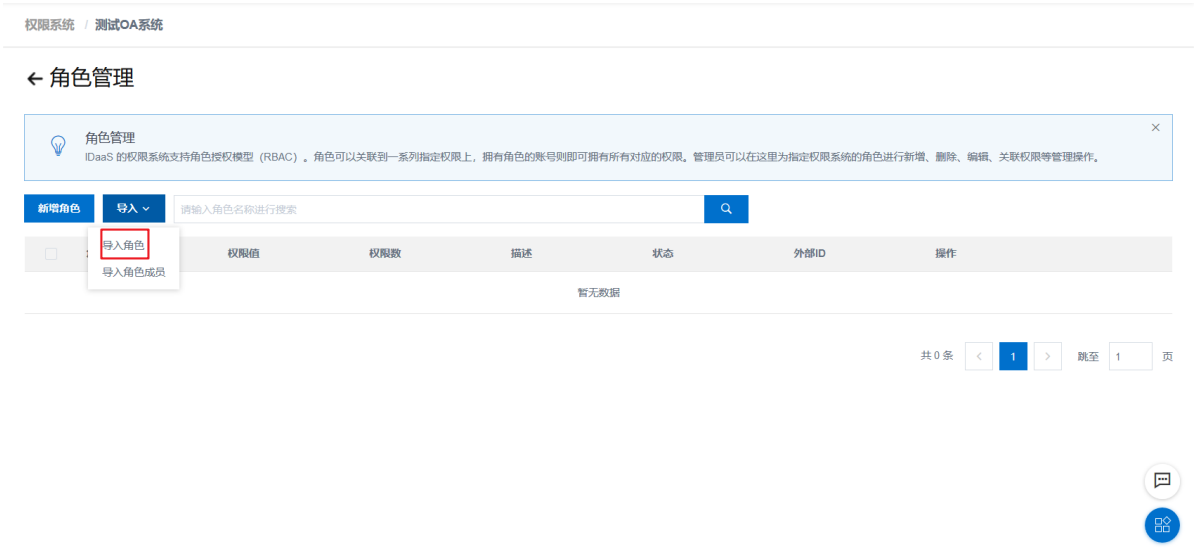


2. 在**新增角色**侧边页，完成以下配置。
   i. **名称**：为角色命名。角色名称应唯一。
   ii. **权限值**：设置角色的权限值。
   iii. **状态**：是否启用角色。
   iv. **描述**：添加角色备注信息。

3. 完成配置后，单击**提交**。

导入角色

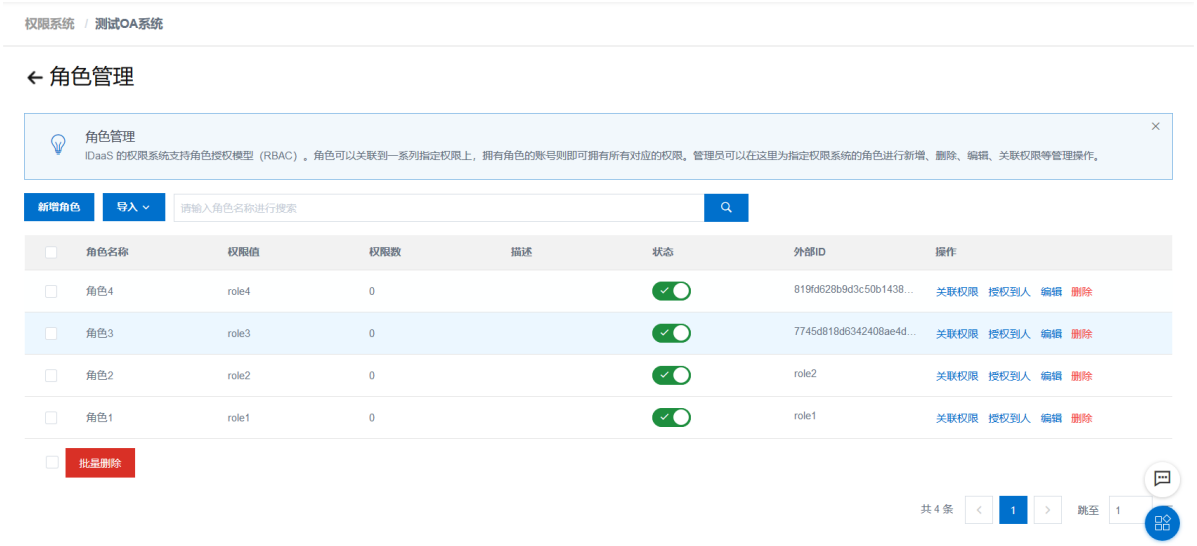
1. 在角色管理页面，点击 导入-导入角色



2. 下载 角色格式范例文档，并根据文档填写角色基本信息

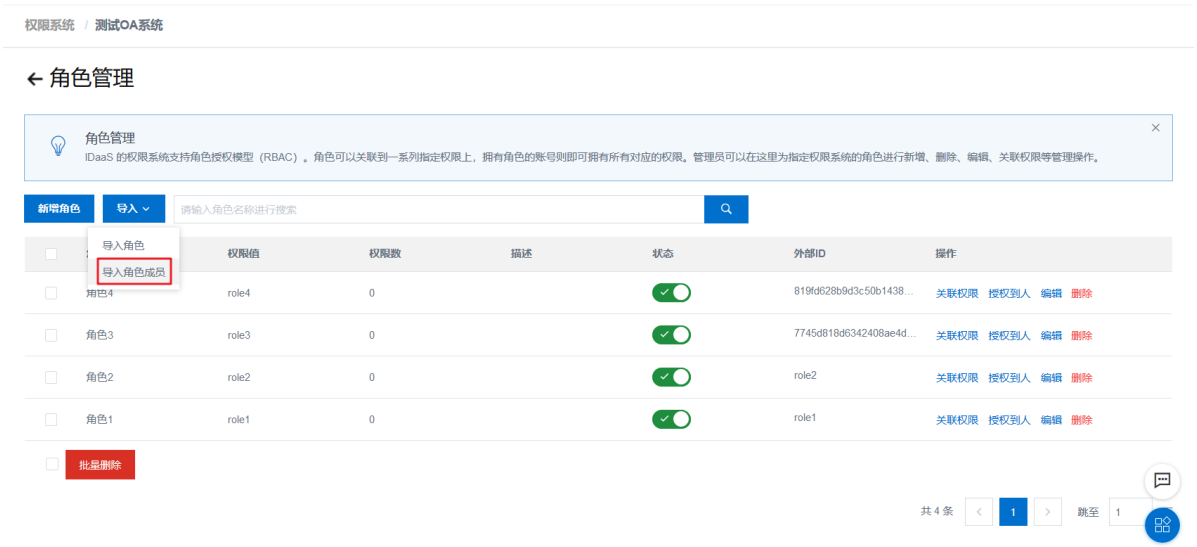
3. 点击上传文件，选择填写好的文件
4. 点击导入文件
5. 在导入角色侧边页，确认导入数据是否正确，确认无误后点击 确定上传导入

导入成功后，会在角色管理页面展示导入的角色

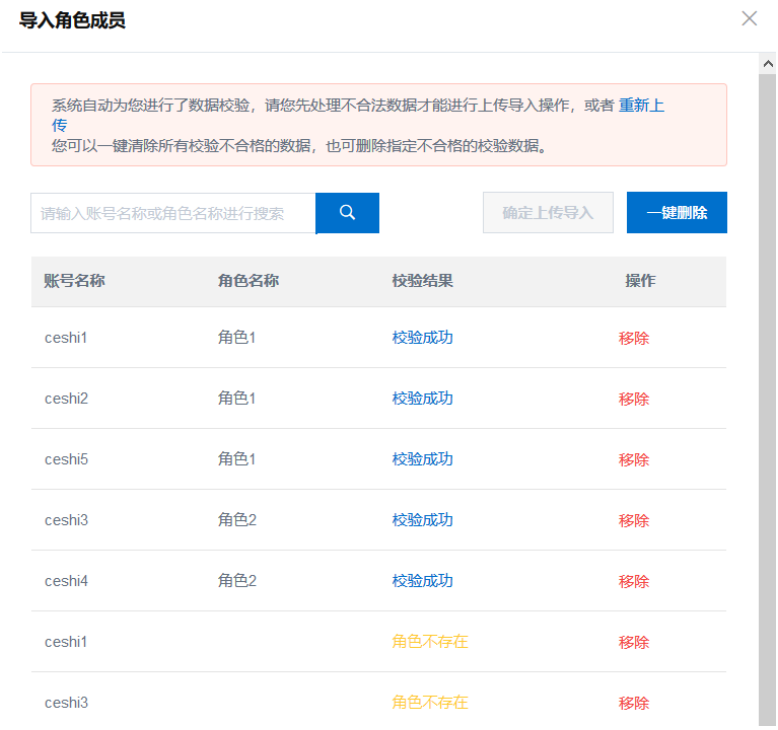


导入角色成员

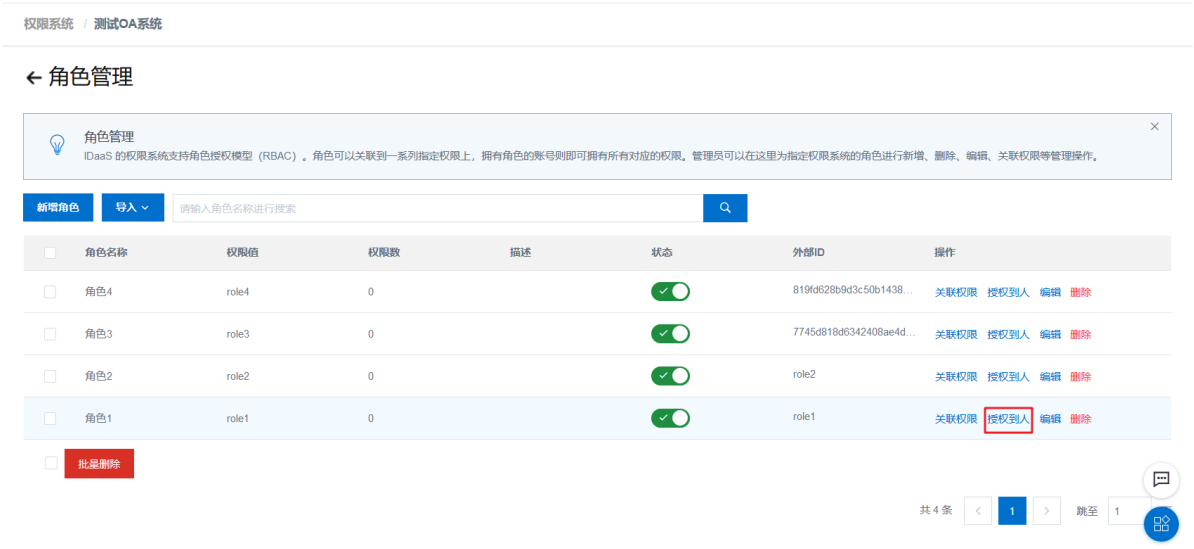
1. 在角色管理页面，点击 导入-导入角色成员



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



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

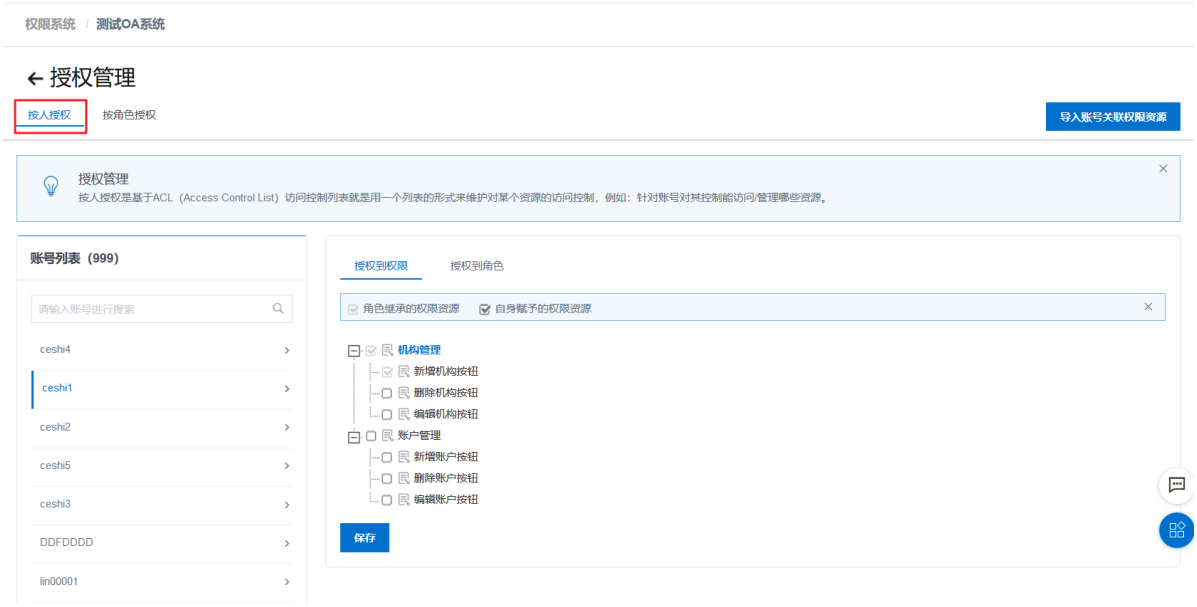
1. 在角色管理页面，勾选要操作的角色，单击页面下面的**批量删除**。
2. 在**提示**对话框中，单击**确定**。

3.2.3.5. 授权管理

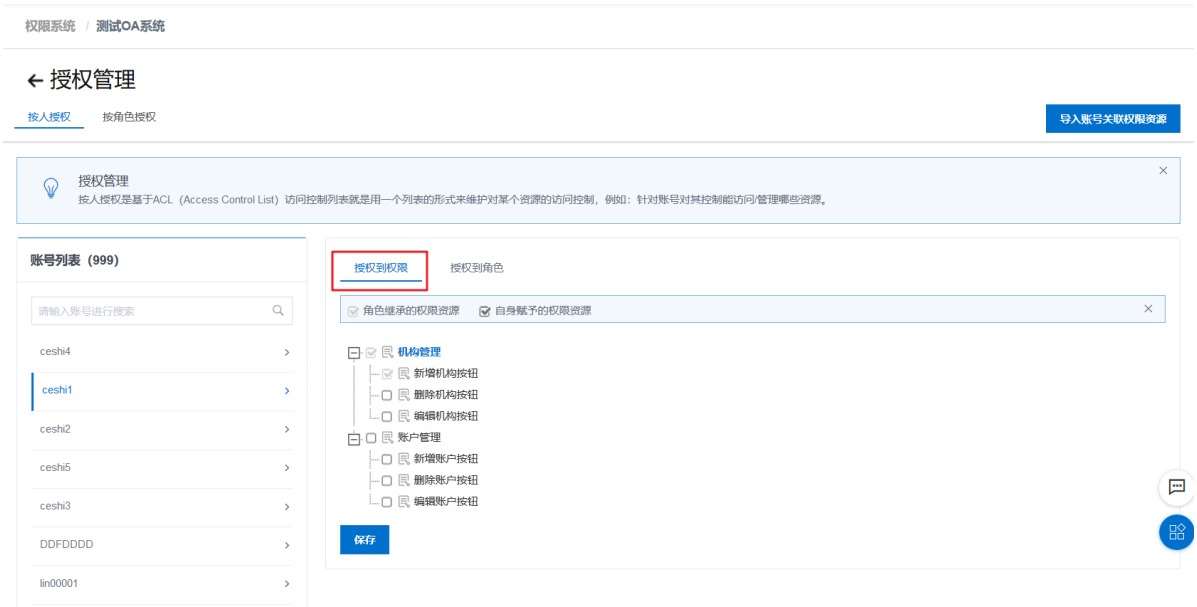
1. 以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考 IT管理员指南-登录。
2. 在左侧导航栏，单击**授权 > 权限系统**。
3. 新建一个权限系统，参考 使用新增系统。
4. 选择新增的权限系统，点击授权管理
5. 根据需要，执行以下功能
   - 按账户授权权限资源
   - 导入账户关联的权限资源
   - 按账户授权角色
   - 按角色授权权限资源
   - 按角色授权账户

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

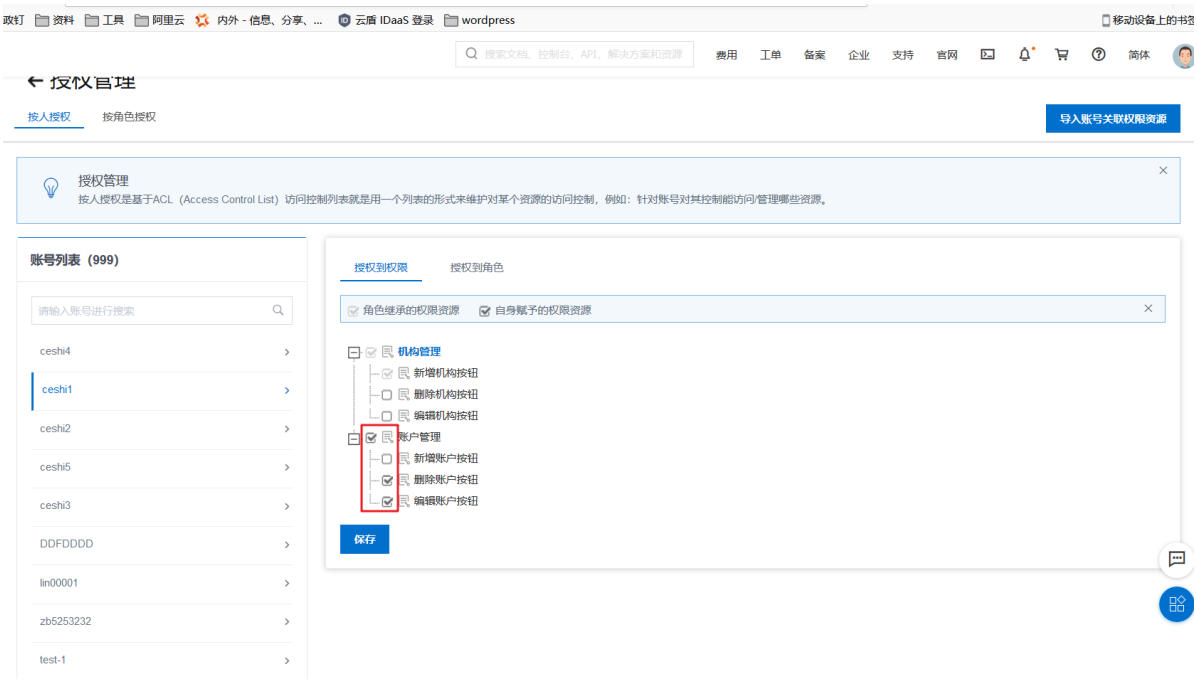


2. 在左侧账号列表中选择账户，点击授权到权限



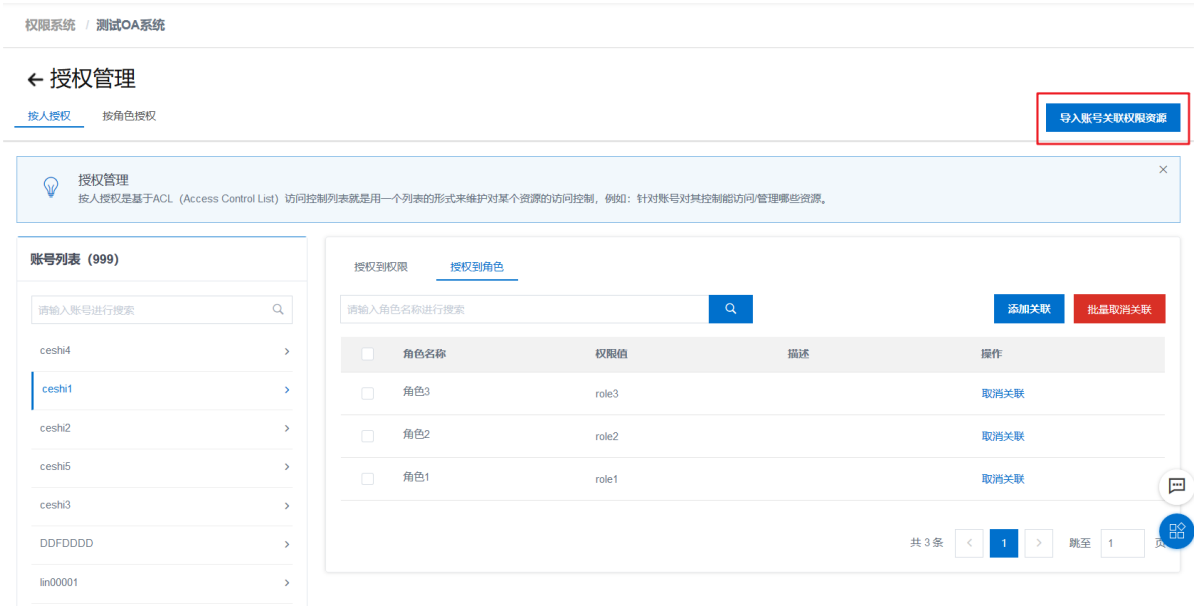
3. 勾选想要授权给账户的权限资源，点击保存，即可授予账户权限资源

> **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。



导入账户关联的权限资源

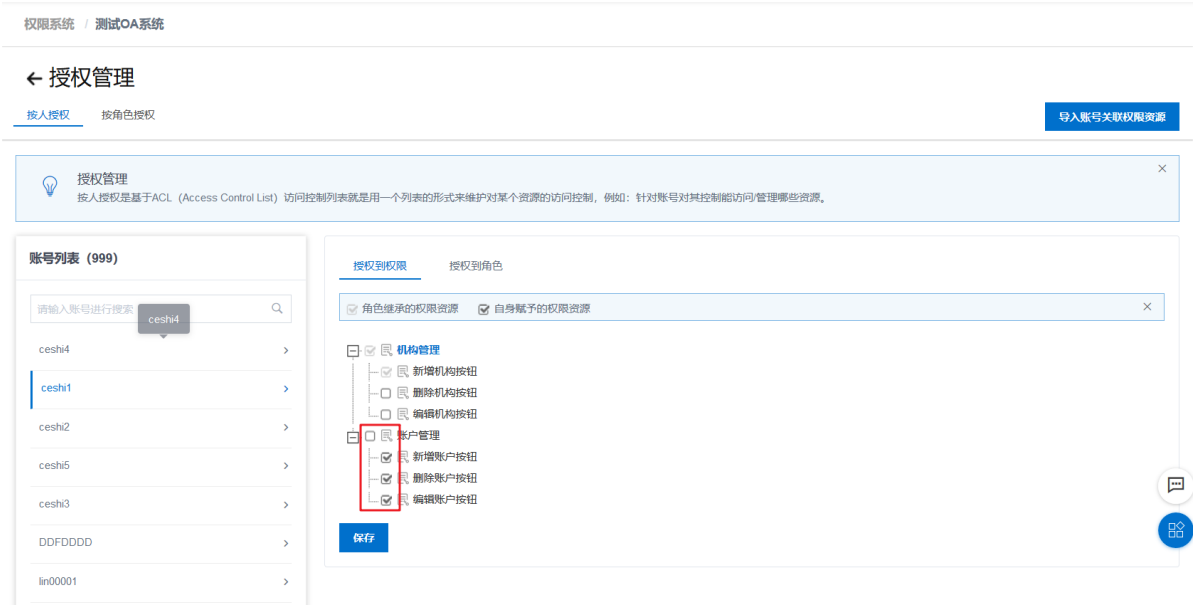
1. 在授权管理页面，点击页面右上角的 导入账号关联权限资源



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

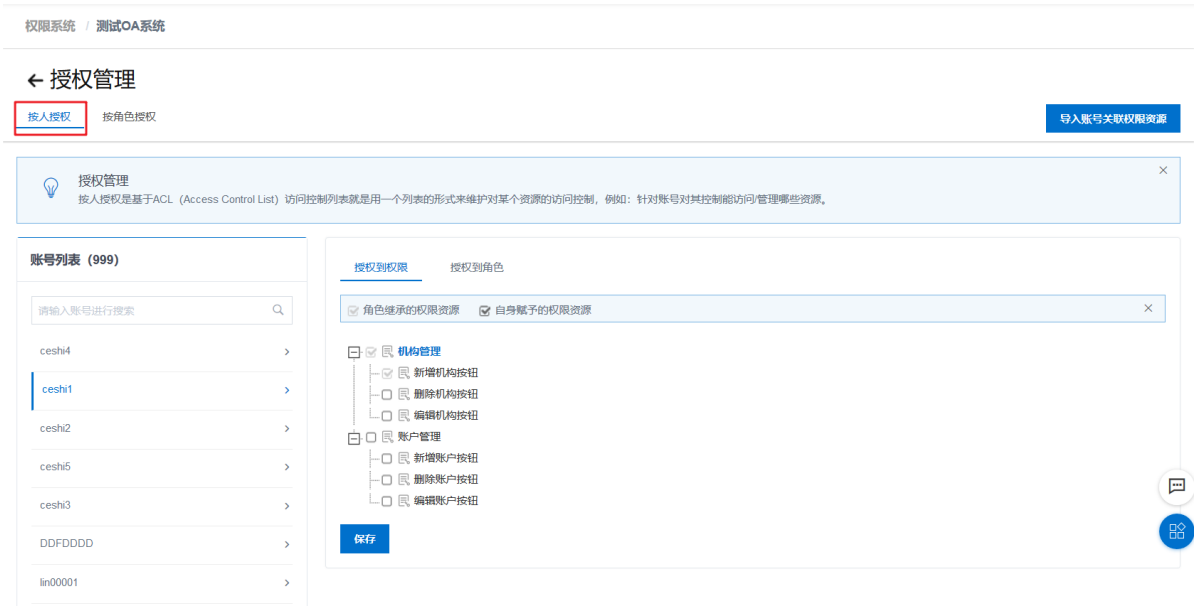
3. 点击上传文件，选择填写好的文件
4. 点击导入文件
5. 在导入角色侧边页，确认导入数据是否正确，确认无误后点击 确定上传导入

   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

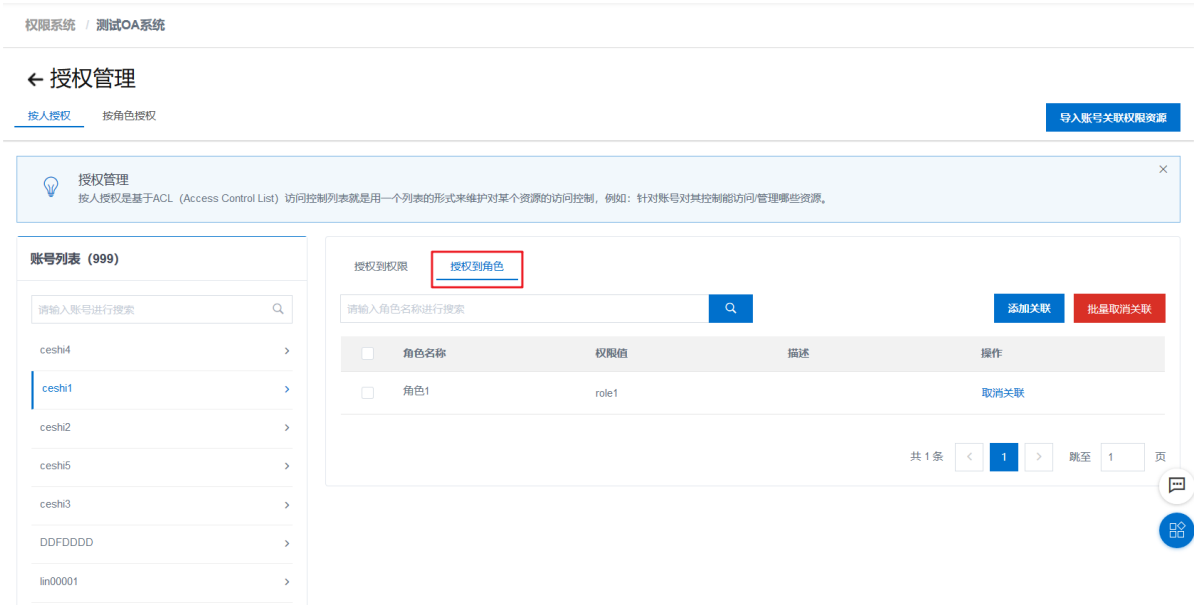


按账户授权角色

1. 在授权管理页面，点击按人授权页签

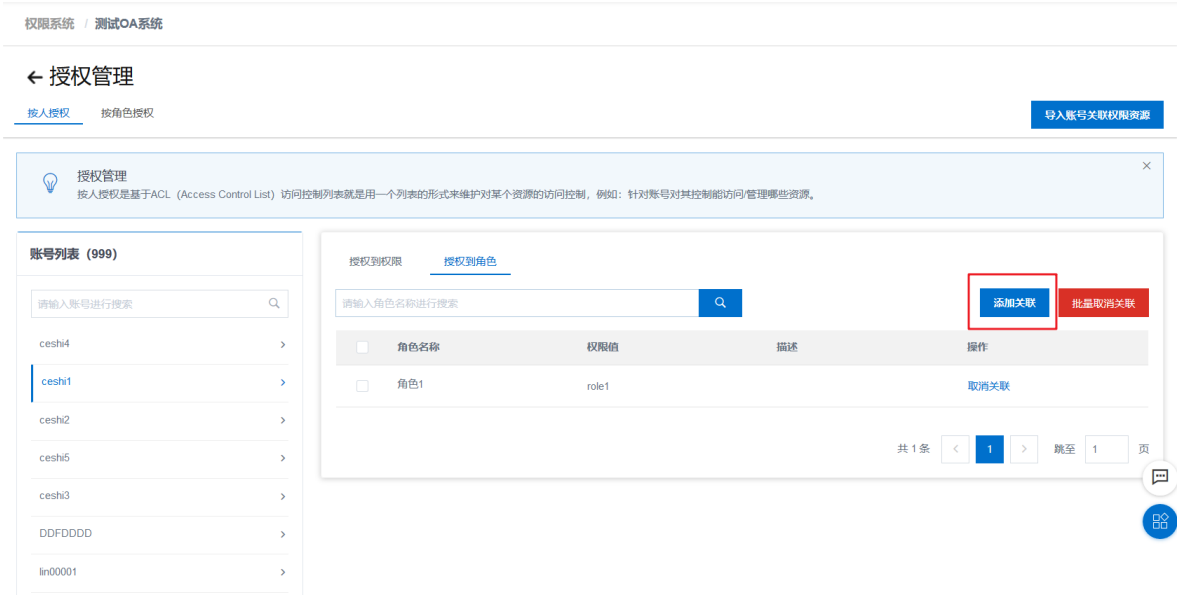


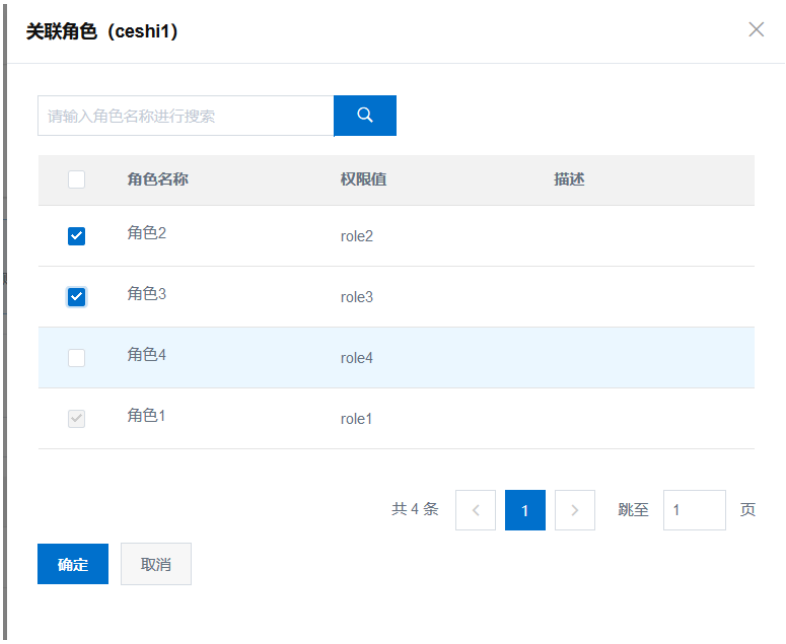
2. 在左侧账号列表中选择账户，点击授权到角色



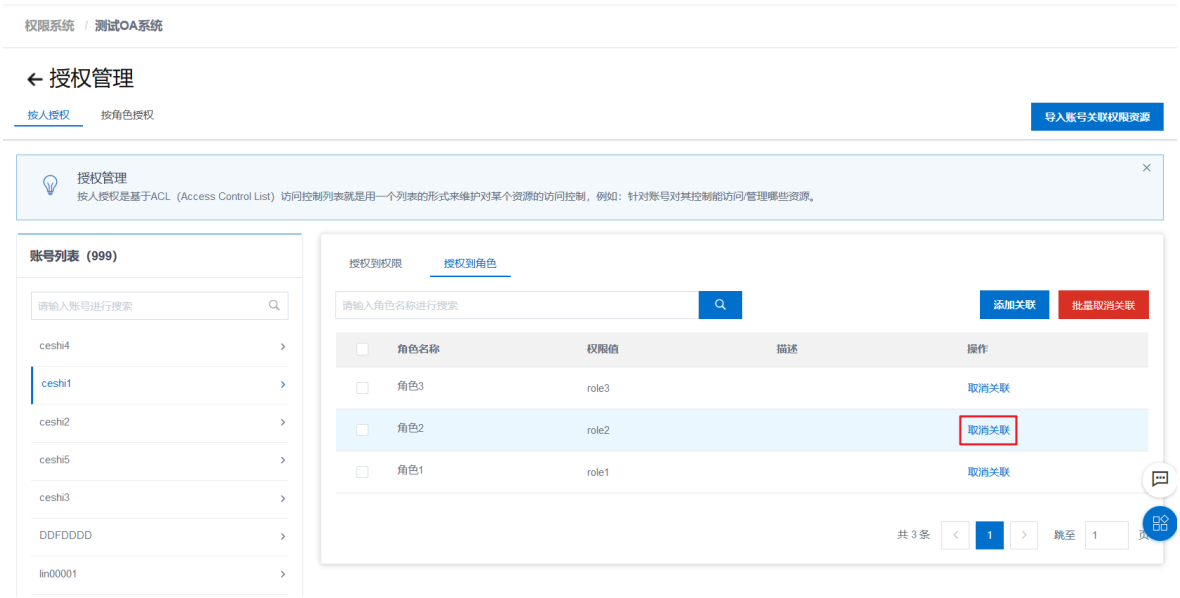
- 点击添加关联，可选择角色，添加账户和角色的关联关系。

> **说明** 添加关联关系后，账户会自动继承角色的权限资源。

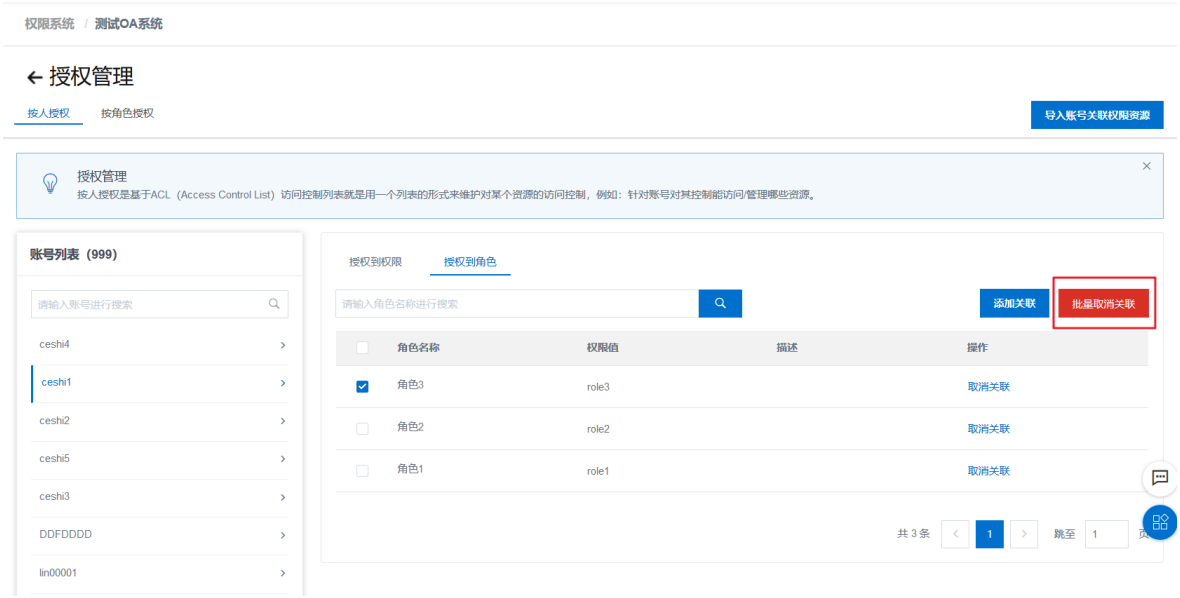




- 点击取消关联，可删除账户和角色的关联关系

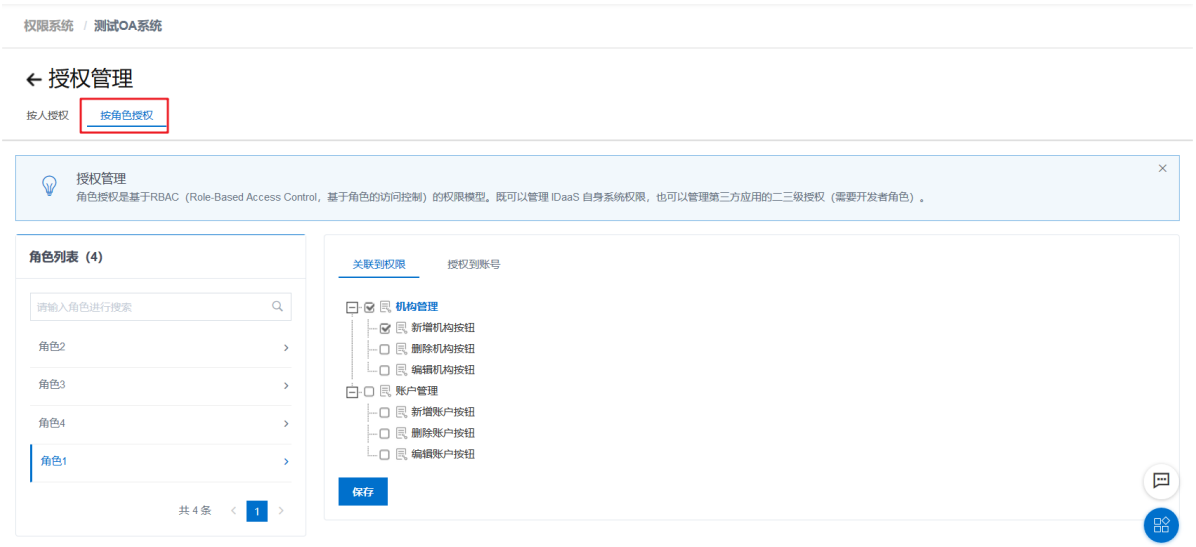


- 也可以勾选角色后，点击批量取消关联，批量删除账户和角色的关联关系

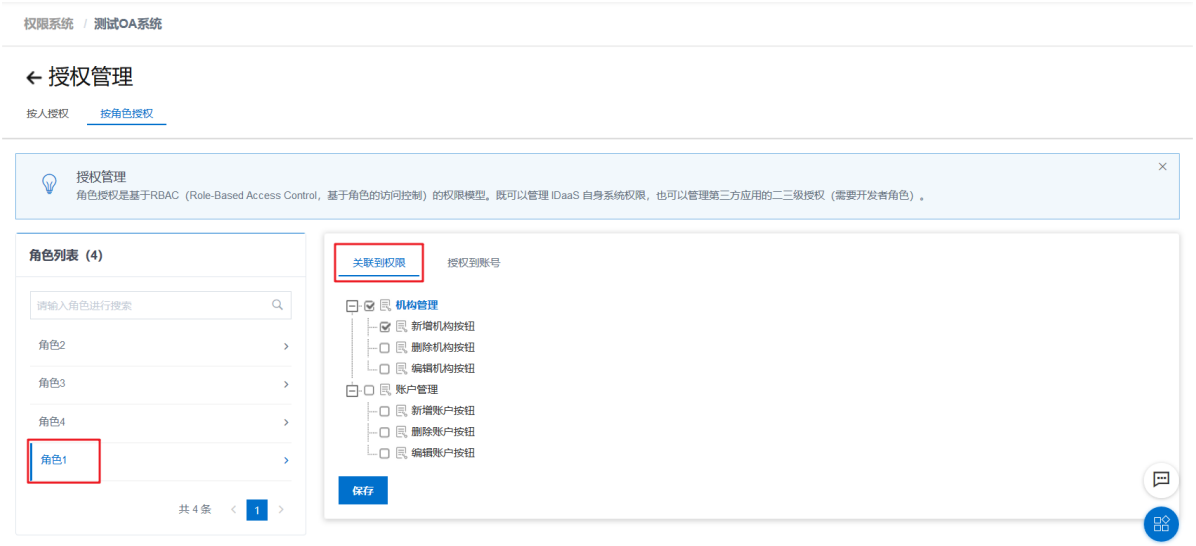


按角色授权权限资源

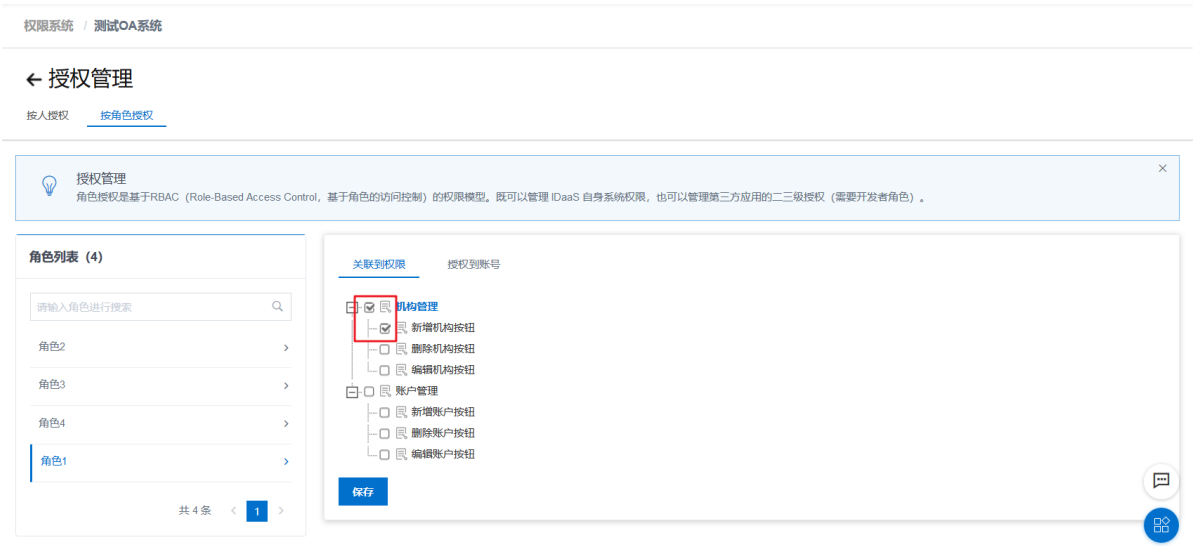
1. 在授权管理页面，点击按角色授权页签



2. 在左侧角色列表中选择角色，点击关联到权限

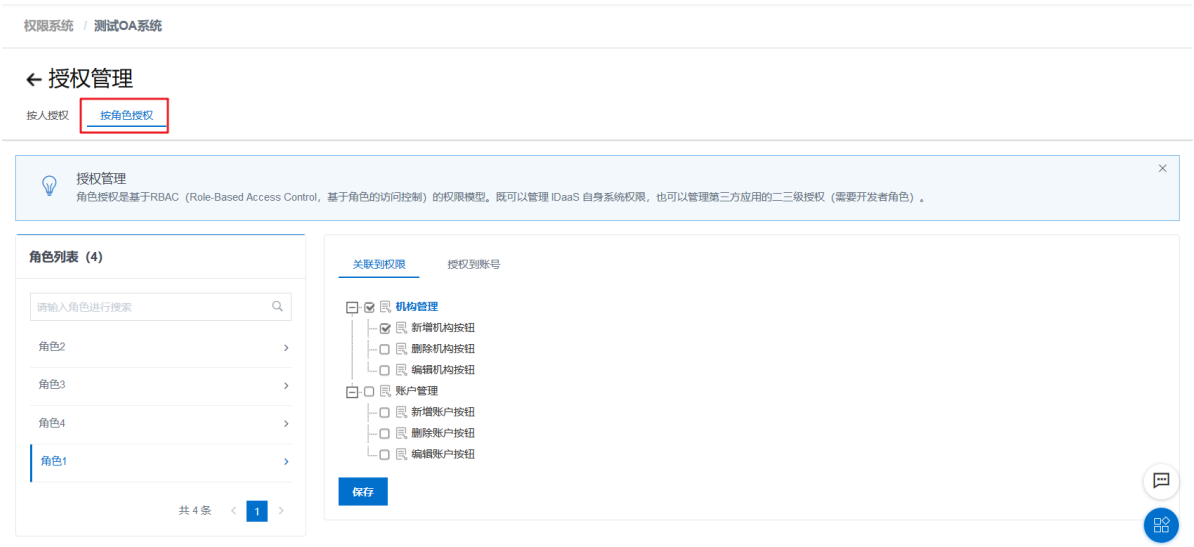


3. 勾选想要授权给角色的权限资源，点击保存，即可授予角色权限资源

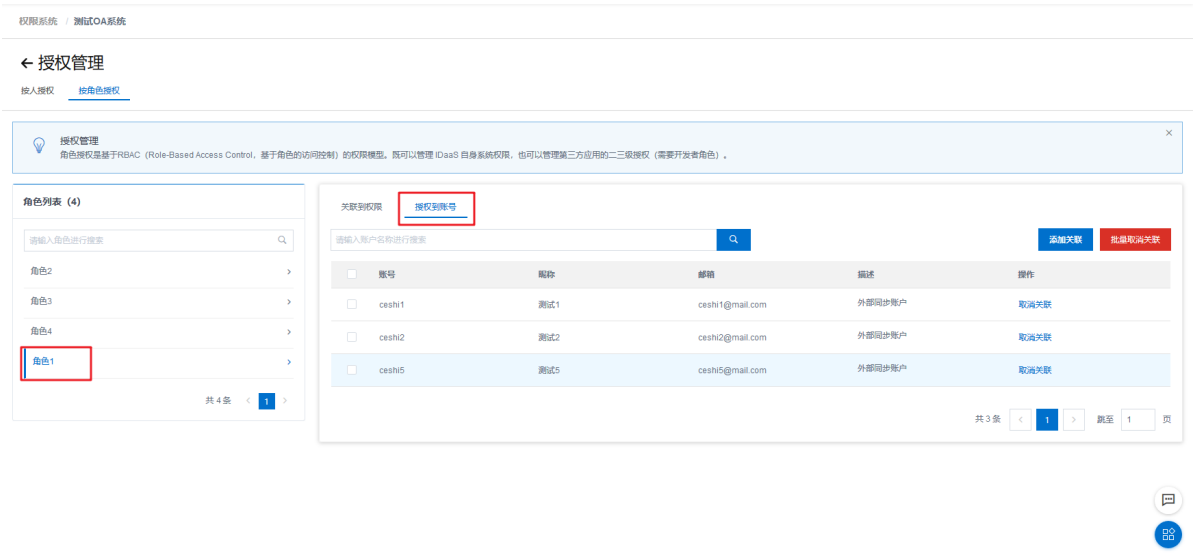


按角色授权账户

1. 在授权管理页面，点击按角色授权页签

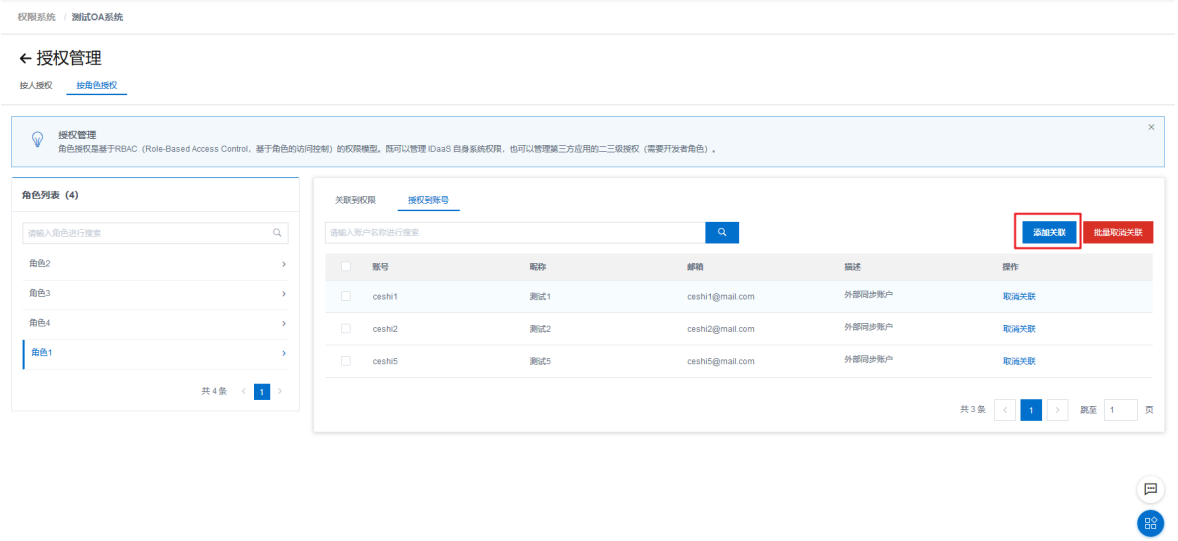


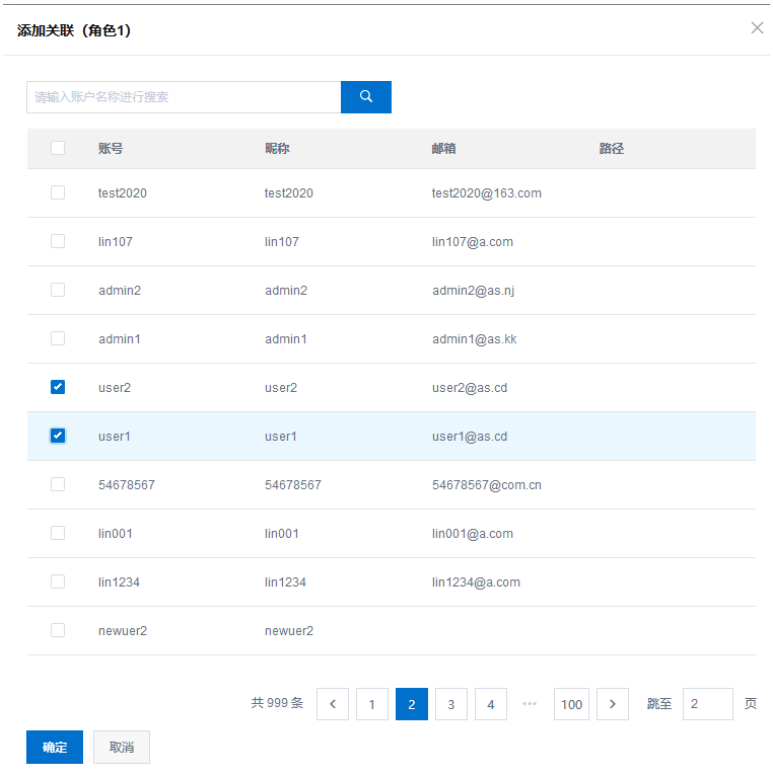
2. 在左侧角色列表中选择角色，点击授权到账号



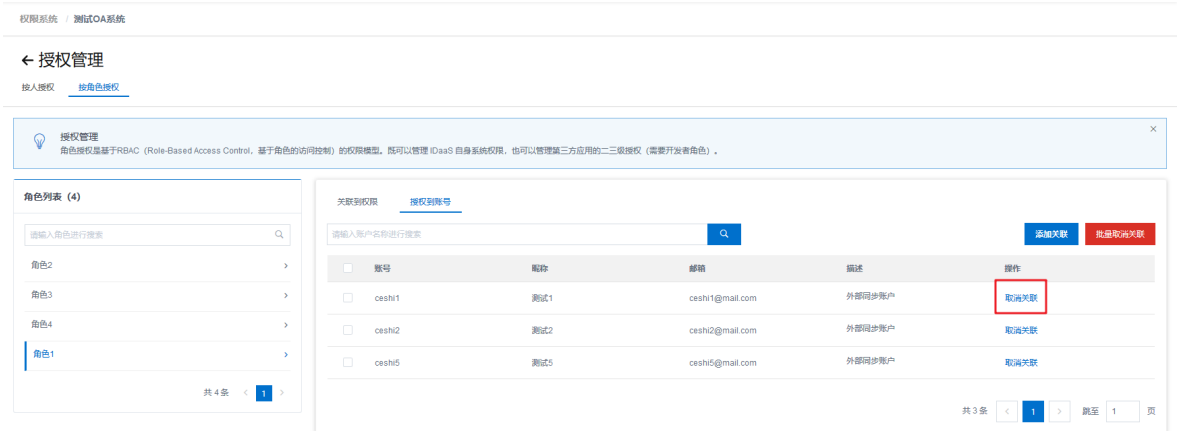
- 点击添加关联，可选择账户，添加账户和角色的关联关系。

> **说明** 添加关联关系后，账户会自动继承角色的权限资源。

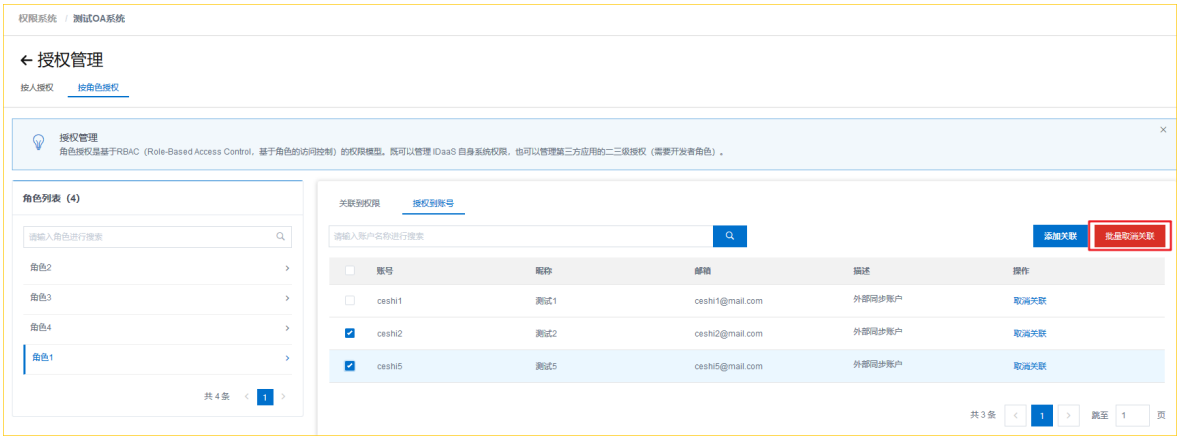




- 点击取消关联，可删除账户和角色的关联关系



- 也可以勾选账户后，点击批量取消关联，批量删除账户和角色的关联关系



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	78d8be99ef30197c31888f5d2d1390a6pHn71sZEqvP	从权限系统详情中获取到的AppKey
client_secret	string	是	96csUmei1g0tL629ufrVMZviFie7NWBOnGYsJNLknQ	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

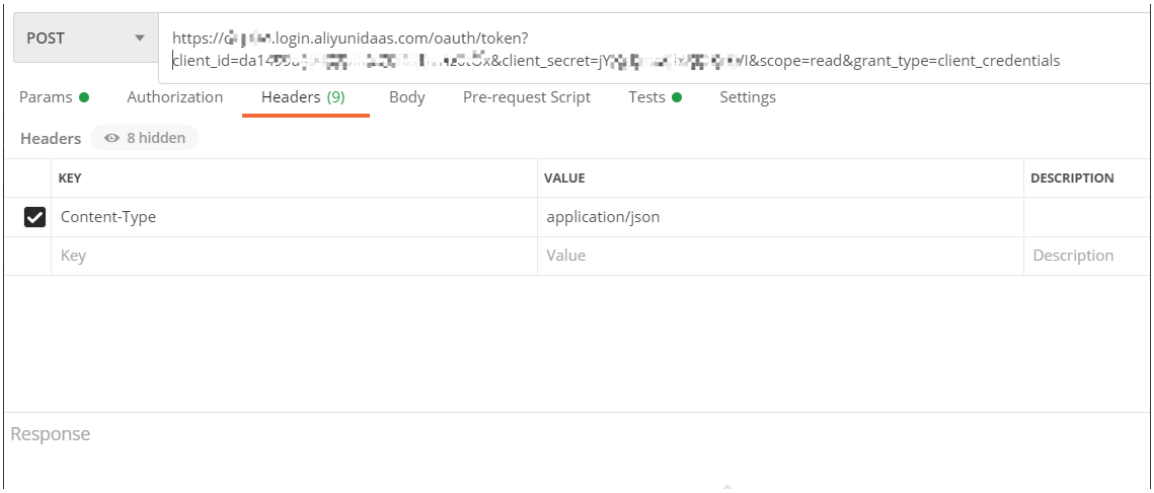
```
http://{{your-idaas-domain}}/oauth/token?
client_id=78d8be99ef30197c318885d2d1390a6
&client_secret=96csUmei1g0tL629ufrVMZv
&grant_type=client_credentials&scope=read
```

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



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	
psId	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
psId	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}}
```

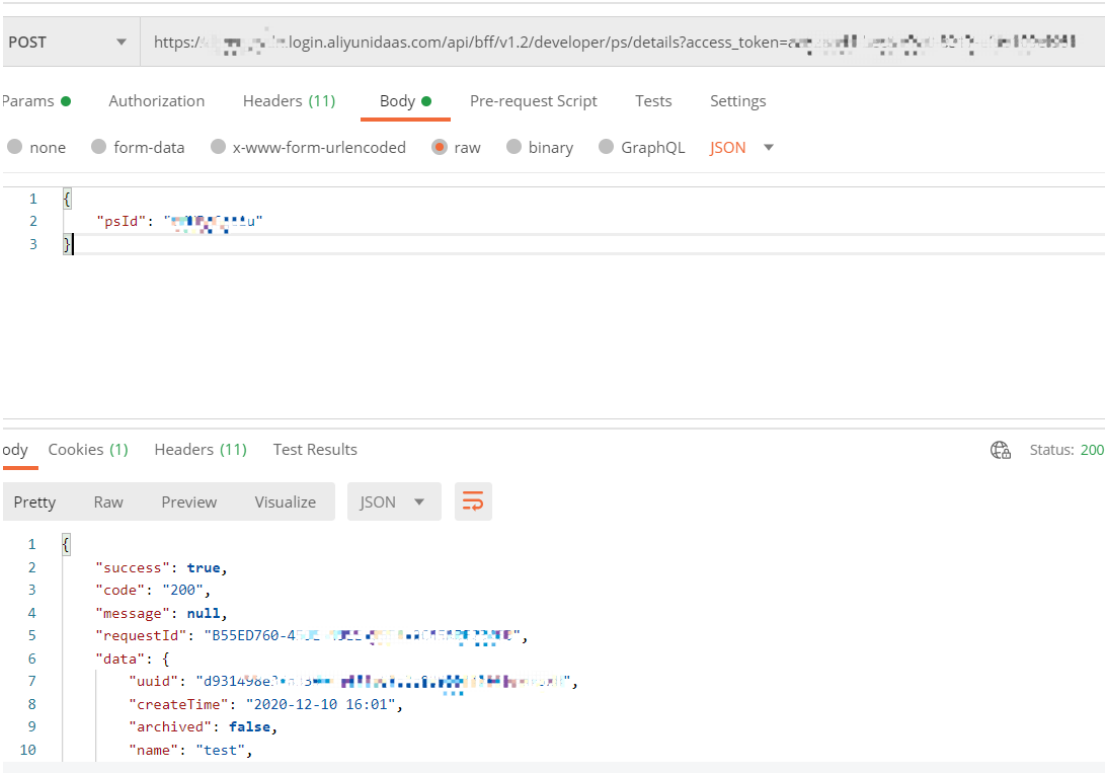
请求入参示例

```
{
  "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": "Fgh9sKSS",
        "host": null,
        "remark": null,
        "creator": "admin",
        "enabled": true
    }
}
```

Postman请求示例



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	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

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
psId	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	4c9b9f14e82a5d4978d5ed229ec1ae4d6912xmCXA1l	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
psId	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	447fed833d8739ecb1caf6f38af14e65tthuiDBac88	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}}
```

请求入参示例

```
{
    "name":"测试角色",
    "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",
    "data":{
        "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
psId	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

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-24c3-4da8-836f-9efcb2c52c4b	
uuid	String	是	447fed833d8739ecb1caf6f38af14e65tthuiDBac88	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 parentUuid 参数指定父级权限。

请求参数

参数	类型	必须	示例值	描述
access_token	string	是	bd3a80ca-24c3-4da8-836f-9efcb2c52c4b	
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
psId	String	是	hU2czV4pMR	PS系统id
parentUuid	String	否	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	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
permissionUuid	string	7dabd9e92a175781072c265aeccfc0f6nmYAtFqciZ8	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":"mkcwicd4pqfhyd73"
}
```

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。

请求参数

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
parentUuid	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	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

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

DELETE /api/bff/v1.2/developer/ps/permission/delete/{uuid}?access_token={{access_token}}

接口说明

删除一个现有权限。注意，当拥有子权限时，不可直接删除。

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	447fed833d8739ecb1caf6f38af14e65tthuiDBac88	待删除的角色全局唯一标识，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/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	否	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
psId	Stirng	是	KSJDJSKkk	系统id,详情处可见

返回参数

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

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

参数	类型	必须	示例值	描述
detachedUDAccountUuidCollection	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

返回参数

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":"447fed833d8739ecb1caf6f38af14e65tthuiDBac88"
}
```

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	447fed833d8739ecb1caf6f38af1	指定角色 全局唯一标识，角色外部id
attachedPermissionUuidCollection	Array	否	["tyG8nUWw"]	想要新增权限 全局唯一标识数组，资源外部id
detachedPermissionUuidCollection	Array	否	["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":"447fed833d8739ecb1caf6f38af14e65tthuiDBac88",
    "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

返回参数

参数	类型	示例值	描述
permissions	Array		角色列表
uuid	string	4c9b9f14e82a5d4978d5ed229ec1ae4d6912xmCXA1l	权限 uuid
parentPermissionUuid	String	978d5ed229ec1ae4d6912xmCXA1l4c9b9f14e82a5d4	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
dataAccessRules	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

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": "65f9e06df1a1cb04133845fd47e35196WUjqj9nkA1P",
                "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	447fed833d8739ecb1caf6f38af14e65tthuiDBac88	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
psId	String	是	SAFJASJk	系统id,详情处可见

返回参数

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
psId	string	XuJNOLtDam	系统id,详情处可见
roleUuid	string	b661f136fbde1c895b44eda7111ab458s736vCvD8aB	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":"b661f136fbde1c895b44eda7111ab458s736vCvD8aB"
        "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
psId	String	是	SAFJASJk	系统id,详情处可见

返回参数

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	978d5ed229ec1ae4d6912xmCXA1l4c9b9f14e82a5d4	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	978d5ed229ec1ae4d6912xmCXA1l4c9b9f14e82a5d4	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": "58e146dd8def3b9052411ba408bf8a5bDnUgQBO7md2",
                "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": []
                    }
                ]
         }]
        "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": [
        ]
    }
}
```

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。

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	540cf6e8b05b09b3938f865b33ab30d1	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
psId	String	是	SAFJASJk	系统id，详情处可见

返回参数

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	447fed833d8739ecb1caf6f38af14e65tthuiDBac88	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
psId	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	09b00e257ede0a38a5f54a94c4d 64000EwQtyG8nUWw	指定账号的用户名
psId	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

```
{
    "success": true,
    "code": "200",
    "message": null,
    "requestId": "76C29BF5-3236-4C17-9C0D-92834AC12B73",
    "data": {
        "hasPermission":false
    }
}
```

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}}

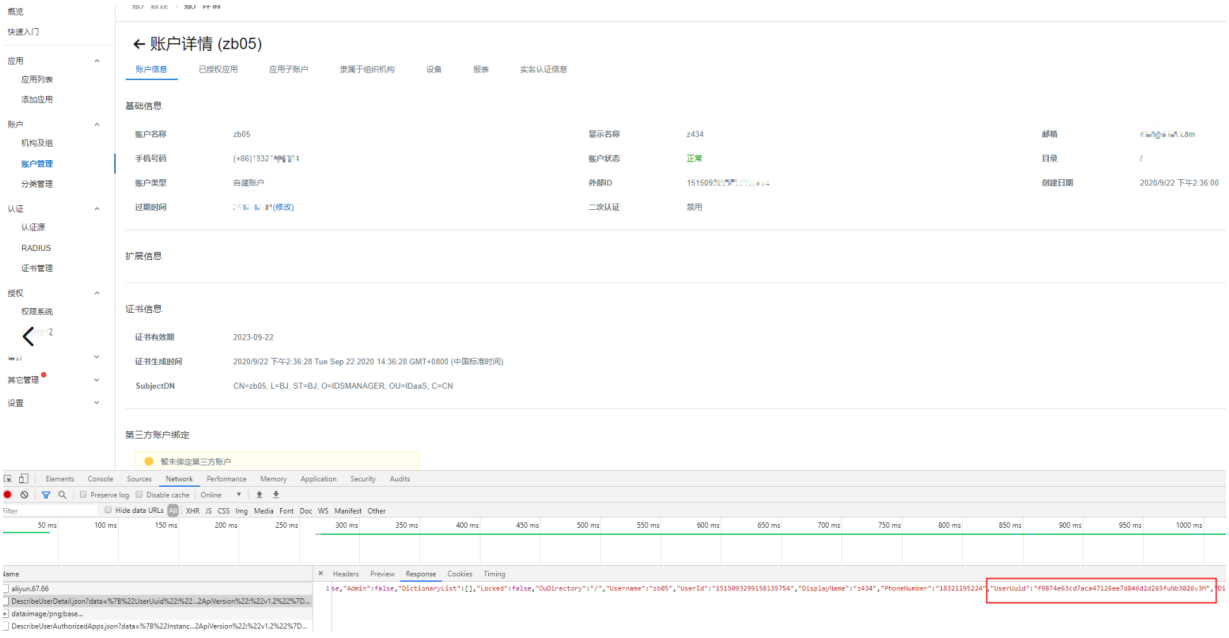
接口说明

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	447fed833d8739ecb1caf6f38af1	指定角色 全局唯一标识，角色外部id
attachedUDAccountUuidCollection	Array	否	["09b00e257ede0a38a5f54a94"]	想要增加授权到该角色的账号全局唯一标识数组
detachedUDAccountUuidCollection	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

按F12打开控制台，访问账户的详情，查看uuid



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	447fed833d8739ecb1caf6f38af1	指定角色 全局唯一标识，角色外部id
attachedUDAccountUuidCollection	Array	否	["09b00e257ede0a38a5f54a94"]	想要增加授权到该角色的账号全局唯一标识数组
detachedUDAccountUuidCollection	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

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

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，可以联系我们进行咨询。线下交付独立部署的IDaaS是可以支持分级管理的。