ALIBABA CLOUD

阿里云

应用身份服务 IDaaS

快速入门

文档版本：20230215

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

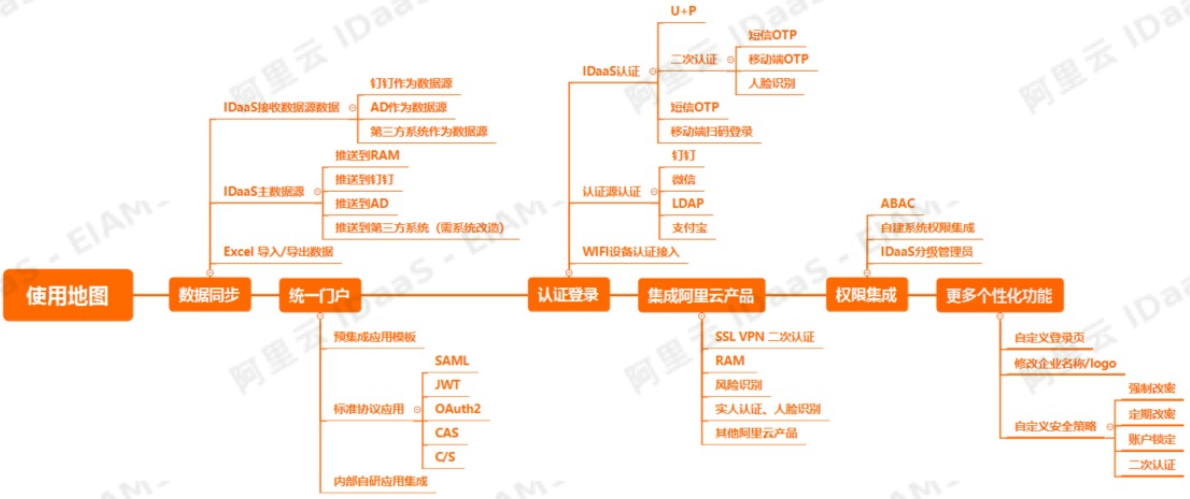
格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**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.快速入门 ---------- 05
2.单点登录集成流程指导 ---------- 08
3.数据同步集成流程指导 ---------- 11
4.快速入门 ---------- 14

1.快速入门

本文档梳理出目前云上用户使用的主要功能及帮助文档链接。帮助您在第一次接触IDaaS的时候快速定位自己的需求，并且可以快速找到需要的文档。



数据同步

IDaaS作为云上的用户目录，可以接收来自外部数据源（如钉钉、AD、第三方系统）的数据同步。同时也可以将数据推送至下游的业务系统。

完整的流程指导可以参考：数据同步集成流程指导。

如果您已明确了数据来源，可以参考如下帮助文档链接

- 钉钉同步数据到IDaaS
- LDAP数据同步到IDaaS
- 第三方系统数据同步到IDaaS
- Excel导入数据到IDaaS

如果您是想要 IDaaS 往下游系统推送数据，可参考如下帮助文档链接

- IDaaS 数据同步到RAM
- IDaaS 数据同步到钉钉
- IDaaS 数据同步到LDAP
- IDaaS 数据同步到第三方系统
- IDaaS 导出数据到Excel

其中，IDaaS 与第三方系统的数据同步都需要系统进行一定的开发改造。

企业统一门户

IDaaS的单点登录（Single Sign On，SSO）能力，可以为企业提供统一的门户。用户只需要认证登录一次，就可以访问所有集成了的应用系统。

完整的流程指导可以参考：单点登录集成流程指导。

IDaaS内置了一些SaaS应用模板，您可以使用这些模板快速集成单点登录。如

- 阿里云 RAM 控制台
- 阿里邮箱
- Gitlab对接（SAML）
- SAP GUI
- JIRA或Confluence

如果第三方系统支持标准的协议，可参考如下帮助文档链接

- JWT 协议配置单点登录
- SAML协议配置单点登录
- OAuth2.0模板使用指南
- C/S应用配置单点登录
- 表单代填实现单点登录

企业内部自研系统建议使用 JWT 协议接入，您也可以使用CAS协议或者其他标准协议进行接入。

登录认证方式

IDaaS支持使用多种第三方认证源进行认证登录，同时本身也具备多种认证方式。

第三方认证源集成可以参考如下帮助文档链接

- 钉钉扫码登录
- 支付宝扫码登录
- 微信扫码登录
- LDAP认证登录
- 短信OTP认证登录

IDaaS也支持使用移动端云盾IDaaS APP 进行移动端扫码登录。

使用账户/密码登录时，支持使用二次认证功能保证账户的安全性，认证方式有：

- 短信OTP二次认证
- 移动端APP OTP二次认证

IDaaS还可以通过使用 RADIUS 实现对防火墙、堡垒机、Wi-Fi 等设备的统一认证。操作步骤可参考添加Radius配置。

集成阿里云产品

- IDaaS支持对接阿里云访问控制RAM系统的单点登录和数据同步。RAM相关的对接可参考IDaaS与访问控制RAM系统对接场景。
- 如果您想要接入其他使用RAM账户体系的阿里云产品，如图形工作站、云效的单点登录，也可以参考单点登录阿里云控制台进行配置。

权限集成

IDaaS可以从单个账户、账户组、组织单位等不同的维度集中管理所有接入的业务系统授权，可参考 应用授权。同时也支持基于属性的授权管理，可参考 分类管理。

同时业务系统内的角色和资源的权限，也可以接入到IDaaS进行集中管理。可参考自建权限系统进行权限接入。

> **说明**
>
> 业务系统内的菜单、按钮、某些特定数据的访问权限，都属于一种资源（Resource）。

> **重要**
>
> 云上的IDaaS暂时不支持分级管理的操作。如果您有相关的需求，可以联系我们咨询线下交付实施相关的方案。

2.单点登录集成流程指导

IDaaS： 应用身份服务

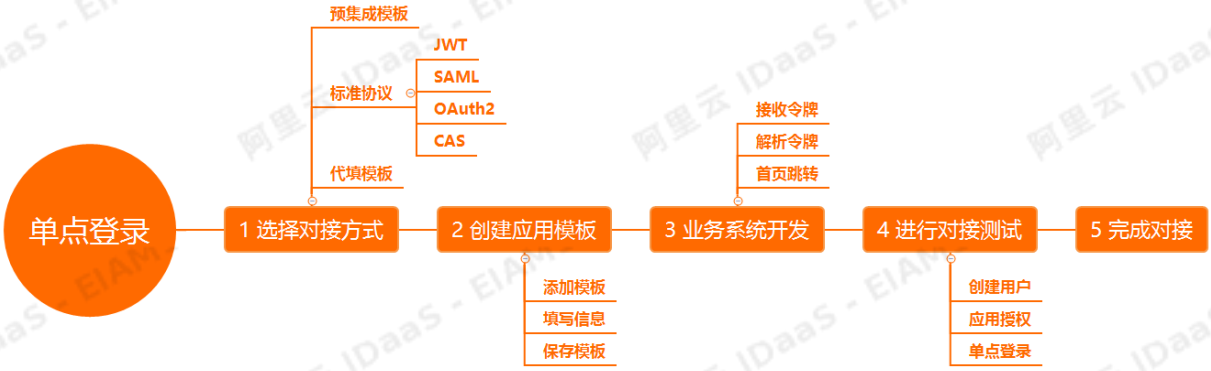
SP： 服务提供者，指第三方业务系统

指导说明

本文为二级引导文章，主要帮助用户理解 IDaaS 实现单点登录的全流程。常用的操作文档参考如下：

- SAML 模板使用指南
- OAuth2.0模板使用指南
- JWT 模板使用指南
- CAS 模板使用指南
- C/S（程序）模板使用指南
- 表单代填模板使用指南

单点登录对接流程图



什么是应用模板？

在 IDaaS 中，我们会通过应用模板方式来集中管理第三方业务系统的配置。主要包括：单点登录配置、数据同步配置、主子账号管理、授权管理、应用状态管理、审计信息等。

更多详细的应用管理操作说明请阅读： IDaaS 应用管理（连接补充）

第 1 步选择对接方式

首先我们需要选择合适的 SSO 单点登录对接协议，也就是在 IDaaS 中挑选应用模板。那么我们该如何去判断该使用哪种应用模板呢？可以从以下 4 个方面考虑：

1）IDaaS 预集成

在 IDaaS 里，我们预先集成了一些常用的 SaaS 应用，比如：钉钉、阿里云 RAM 、阿里邮箱等

在 **添加应用** 的搜索栏中输入应用名称，即可看到查询结果。填写基本信息后即可开始使用，快速配置，无需开发，5分钟搞定。

如果您在使用模板填写配置信息时遇到问题，请使用右上角的搜索栏，查找对应的模板使用手册，按使用手册步骤进行配置即可。

如果您未找到想要的应用模板，并且希望增加在 IDaaS 预集成应用模板中，请 联系我们。

2）B/S or C/S ?

通常业务系统的网络结构模式主要有两种：B/S 结构（浏览器/服务器模式）C/S 结构（客户端/服务器模式）

B/S 结构：我们通常推荐使用：SAML、OAuth2.0、JWT 、CAS 应用模板对接

- SAML 模板使用指南
- OAuth2.0模板使用指南
- JWT 模板使用指南
- CAS 模板使用指南

C/S 结构：我们通常使用 C/S（程序）应用模板进行对接

- C/S（程序）模板使用指南

3）IDaaS 标准协议

IDaaS目前主要提供四种 SSO 协议：SAML、JWT 、OAuth2.0、CAS

如果您的业务系统支持上述其中的某个协议，仅需在应用模板中进行配置，然后业务系统进行少量的开发工作，即可实现 SSO 单点登录。

如果以上协议都不支持，在这里，我们将主推 JWT 模式，开发简单，容易实现。

- JWT 模板使用指南

4）代填模板

由于某些特殊情况下，业务系统不支持 IDaaS 提供的 4 种协议，同时又面临改造困难的问题。比如：系统建设时间长，联系供应商困难，或者供应商收费高昂无法进行适配改造等。

针对这种情况，可以使用表单代填来实现业务系统的单点登录，都是通过模拟用户输入账号密码方式实现。

- 表单代填模板使用指南

通过下表，您可以进一步选择模板

对接协议（应用模板）	B/S	C/S	SP是否需要开发	开发/对接难度
JWT	✔	×	✔	简单
SAML	✔	×	✔	中等

OAuth	✔	×	✔	中等
CAS	✔	×	✔	简单
C/S（程序）	×	✔	✔	简单
C/S（浏览器）（指令代填）	✔	✔	×	简单
表单代填	✔	×	×	简单

第 2 步创建应用模板

选定好对接协议后，我们就要开始在IDaaS创建模板。

1）搜索模板

- 预集成应用模板创建：在 **添加应用** 中搜索应用名称，如：阿里邮箱，填写信息进行应用创建。
- 标准协议模板创建：在 **添加应用** 中搜索协议名称，如：JWT，填写信息进行应用创建。

2）填写信息

详细请参考应用模板使用文档。

3）保存模板

第 3 步业务系统研发

当我们创建好应用后，业务系统获取到一些相关信息，比如：JWT PublicKey，就可以开始研发工作了。主要研发的内容大致为：获取 token 参数，进行解析，跳转首页。目的就是拿到 IDaaS 已完成认证的账户信息，然后业务系统直接放行跳转至用户首页。详细过程可见上述应用模板使用文档

第 4 步对接测试

业务系统完成开发工作后，就可以开始进行单点登录的测试工作了。在测试的时候需要注意要记得给账户授权，否则，用户将看不到应用的 Logo 图标。详细过程可见上述应用模板使用文档

第 5 步完成对接

测试通过后，我们就完成 SSO 单点登录对接啦，用户就可以开始在 IDaaS 中使用体验单点登录带来的便捷。

3.数据同步集成流程指导

IDaaS：应用身份服务

SP：服务提供者，指第三方业务系统

指导说明

本文为二级引导文章，主要帮助用户指导 IDaaS 数据初始化，和下游业务系统数据同步的全流程。

目的是让客户更清晰的做出数据同步的规划，和正确的找到对应的操作文档。

常用的操作文档如下：

SP 同步至 IDaaS

- 钉钉同步数据到IDaaS
- LDAP 数据同步到IDaaS
- IDaaS 数据同步API 标准
- Excel 表格导入到IDaaS

IDaaS 同步至 SP

- IDaaS 数据同步到RAM
- IDaaS 数据同步到钉钉
- IDaaS 数据同步到LDAP
- 数据同步 SCIM 标准
- IDaaS Excel 表格导出

IDaaS 同步的数据有哪些？

IDaaS 的数据同步主要有 3 类，组织机构信息、人员账户信息和用户组信息：

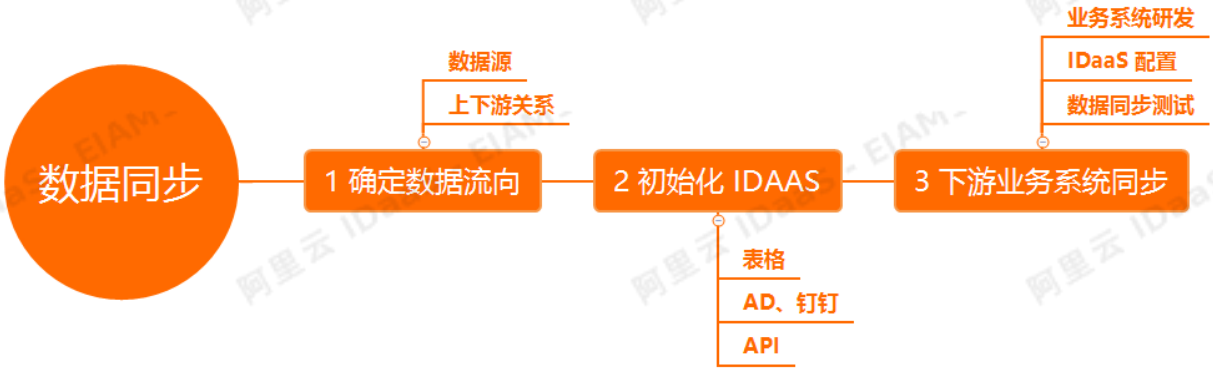
1）**组织机构**：包括机构名称，机构编码，父级机构编码等

2）**人员账户**：包括账户名称，显示名称，手机号，邮箱，外部 ID（唯一标志）

3）**用户组**：包括组名称，组编码，父级机构编码，组成员等

更多详细的同步数据请参阅 IDaaS 数据同步 API 标准

数据同步三大环节



环节一：确定数据流向

在开始数据同步之前，我们首先需要规划整体的数据同步流向。

- 谁是数据源，数据产生者（上游是谁）？
- 下游该同步给哪些业务系统（下游是谁）？

作为数据源，我们要确保唯一，做到一处修改，处处生效，这不仅有利于公司的整体身份中台建设规划，解决身份信息孤岛问题，同时也为后续更多新上线的业务系统，打下身份数据的基础。

经典数据同步场景

1）IDaaS 作为数据源（ IDaaS -> SP）

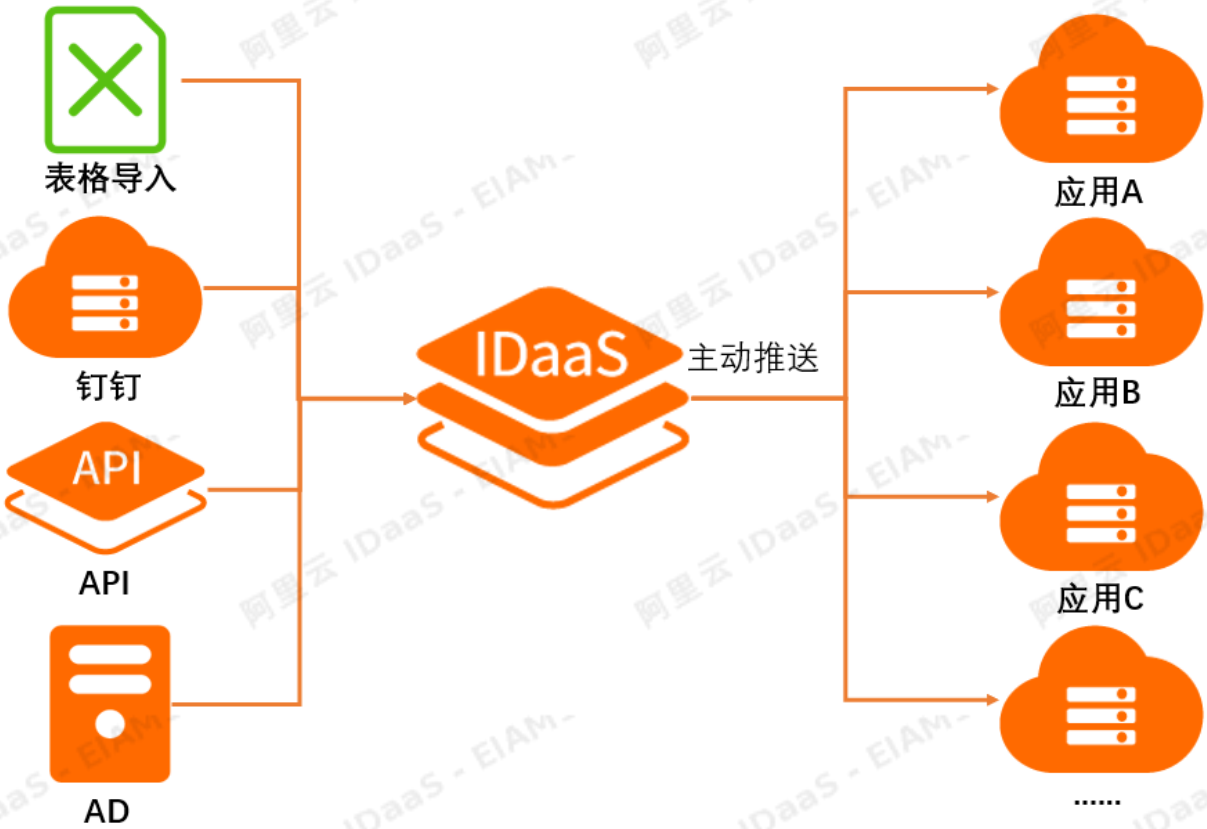
IDaaS 作为数据源是，当进行数据的增、删、改等操作都会实时同步至业务系统。通常情况下，为保障数据的一致性，避免数据混乱，业务系统和 IDaaS 只做单项同步对接。

2）第三方业务系统作为主数据源 （SP -> IDaaS -> SP）

IDaaS 同时也支持钉钉、AD、OA、HR 等业务系统作为数据源进行数据同步。通过和 IDaaS 的打通，集中收集数据，然后再推送给业务系统。做到一处修改，处处生效。

环节二：初始化IDaaS

当我们已经梳理好数据流程和明确数据源后，我们就需要开始初始化 IDaaS 了。当前我们支持 4 种初始化方式，具体流程如下



1）IDaaS 作为数据源：我们推荐使用表格导入的方式进行数据初始化。

详细操作文档，请参考：Excel 表格导入到 IDaaS

2）钉钉作为数据源：在 IDaaS 中我们已经预集成了钉钉的数据同步，只需要配置，即可将钉钉的部门数据，账户数据拉取到 IDaaS 中。

详细操作文档，请参考： 钉钉同步到 IDaaS

3）**AD 作为数据源**：在 IDaaS 中我们已经预集成了基于 LDAP 的数据同步，只需要配置，即可将AD、或 openLDAP 的部门数据，账户数据拉取到 IDaaS 中。

详细操作文档，请参考：LDAP 同步到 IDaaS

4）**第三方业务系统作为数据源**：为方便集成第三方业务系统的数据，IDaaS 已经整理好一系列 API 接口供 SP 调用。开发前可以使用 postman 等接口调用工具进行测试体验。

详细接口标准及调用方法，请参考：IDaaS 数据同步 API 标准

环节三：下游业务系统同步

IDaaS 的初始化工作完成之后，我们就开始进入第三个环节，给下游业务系统的数据同步工作了 。

具体流程如下图

1）IDaaS 同步至钉钉：在 IDaaS 中，我们已经预集成了与钉钉的数据同步功能。仅需要一些简单的配置工作就能实现数据同步。我们建议先使用测试钉钉组织进行数据同步测试，然后在切换至正式环境配置。

详细操作文档，请参考：IDaaS 同步到钉钉

2）IDaaS 同步至RAM：在 IDaaS 中我们已经预集成了RAM的数据同步，首先我们需要创建 RAM 模板，然后进行同步的配置后，即可将 RAM 同步数据。我们建议先使用测试 RAM 进行数据同步测试，然后在切换至正式环境配置。

详细操作文档，请参考： IDaaS 同步到 RAM

3）IDaaS 同步至 AD/LDAP：在 IDaaS 中我们已经预集成了基于 LDAP 的数据同步，只需要配置，即可向 AD 或openLDAP 同步部门数据，账户数据。我们建议先使用测试 RAM 进行数据同步测试，然后在切换至正式环境配置。

详细操作文档，请参考：IDaaS 同步到 LDAP

4）IDaaS 同步至 SP：IDaaS 给业务系统同步数据，主要使用 SCIM 协议。在这里，业务系统需要基于 SCIM 协议进行数据接收及数据存储逻辑研发。目的就是接收 IDaaS 推送的数据并且正确的存储到各自的数据库表中。业务系统提供同步的 API 接口，配置在 IDaaS 中，我们建议先使用测试环境进行数据同步测试，然后在切换至正式环境配置。

详细数据同步 SCIM 接口标准及对接过程，请参考：数据同步 SCIM 标准

4.快速入门

本文将帮助您在开通IDaaS服务后，快速配置并通过IDaaS平台实现企业组织机构中用户指定应用的单点登录。

步骤1：添加应用-阿里邮箱

参考以下步骤，在IDaaS管理平台中添加阿里邮箱应用：

> **说明** 您必须已开通阿里邮箱企业版并拥有管理员账号权限。

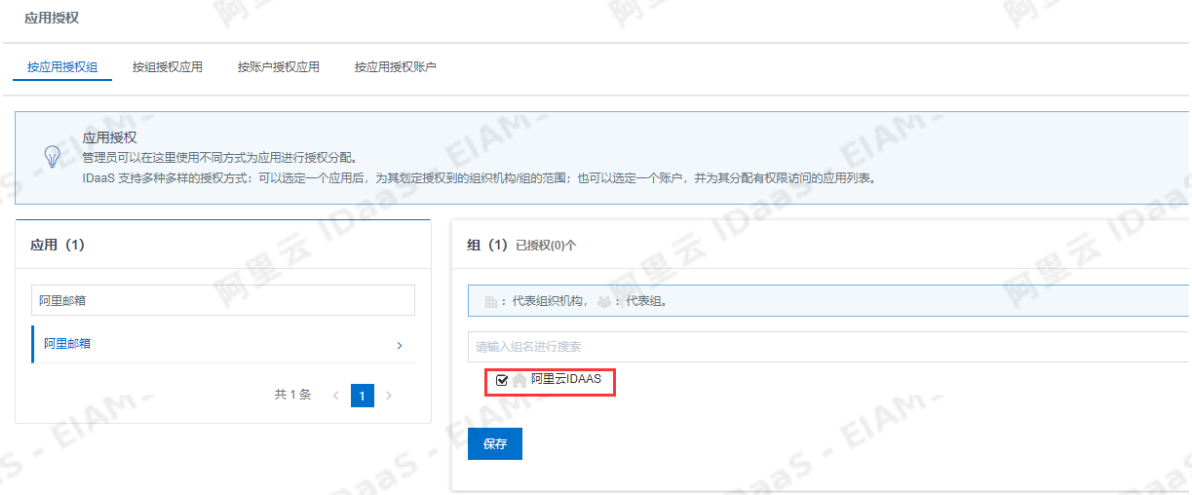
1. 以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考 IT管理员指南-登录。
2. 定位到**应用 > 添加应用**页面，在应用模版列表中选择阿里邮箱，单击其右侧的**添加应用**。

3. 在**添加应用**对话框中，根据您已开通的阿里邮箱产品的信息填写相关内容，单击**保存提交**。

> **说明** 其中，用于单点登录的 appCode和 appSecret信息，请咨询阿里邮箱的售后人员获取。

4. 定位到**应用 > 应用列表**页面，选择已添加的阿里邮箱应用，单击**授权**前往**应用授权**页面。

5. 在右侧账户组区域，勾选组织架构的根节点，单击**保存**。



6. 返回**应用列表**页面，将该阿里邮箱应用的状态设置为启用。

步骤2：在授权的组织机构中添加账户-用于单点登录

参考以下步骤，在IDaaS管理平台中为您的企业组织机构添用户账户：

1. 定位到**用户 > 机构及组**页面，单击**新建账户**。

2. 在**新建账户**对话框中，填写员工的基本信息并设置初始密码，单击**添加**。

> **说明** 您也可以从Excel或者LDAP服务器批量导入您企业组织机构的用户账号

> **重要** 邮箱和手机号必须至少填写一项。一般情况下，系统将以此作为该用户的唯一标识参数

步骤3：为上文新建的账户添加子账户-把IDaaS中的账户和应用中的账户进行绑定

参考以下步骤，将用户账户添加为阿里邮箱应用的子账户：

> **说明** 该用户账户必须在您的阿里邮箱企业版中已有相应的邮箱账号。

1. 定位到**应用 > 应用列表**页面，选择已添加的阿里邮箱应用，单击**详情**。
1. 在**账户信息 - 子账户**框中，单击**查看应用子账号**。

2. 在**应用列表 / 子账户**页面，单击**添加账户关联**。
3. 在**添加账户关联**对话框中，在**主账号**栏填写已在IDaaS平台中添加的用户账号，并在**子账号**栏填写该员工在阿里邮箱应用中的邮箱账户，单击**保存**即可为应用添加账户关联关系。

> **说明** 您也可以从Excel批量导入账户关联关系，或者采用由用户自助提出关联申请、管理员审批的形式添加账户关联关系。

步骤4：使用新添加的账户单点登录应用

参考以下步骤，使用用户账户登录IDaaS管理平台实现单点登录阿里邮箱应用：

1. 使用所添加的用户账户登录IDaaS管理平台。具体操作请参见 普通用户指南-登录。
2. 定位到**主导航 > 首页**页面，单击所添加的阿里邮箱应用。

浏览器在新标签页中自动打开阿里邮箱应用，并展示该用户邮箱账户的邮件列表页面，即用户单点登录成功。