ALIBABA CLOUD

阿里云

应用身份服务 IDaaS

最佳实践

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.账户同步

1.1. 通过SCIM协议从IDaaS同步企业数据到相关应用

本文为您介绍IDaaS如何通过SCIM协议将企业数据同步到相关应用中，保持企业信息化相关应用数据的实时统一性。

背景信息

现代企业的数字化管理，一般由多个应用互相配合来完成，而由不同团队或供应商开发的应用易成为一个个信息孤岛，所有应用的数据同步难题，正困扰着越来越多的企业管理者。

解决方案

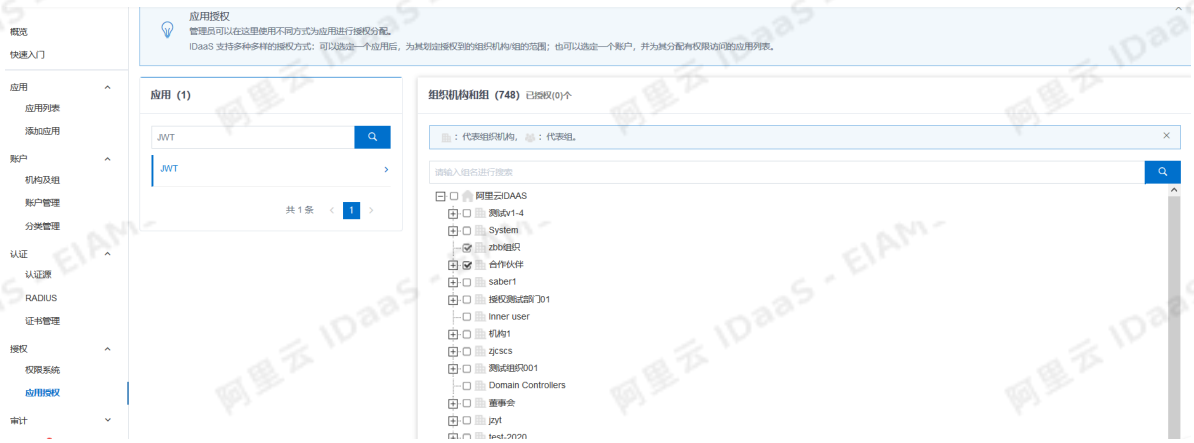
通过IDaaS应用身份服务的SCIM协议,将企业内部共享数据同步到IDaaS覆盖到的所有应用中去。

添加应用

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. 点击左侧导航栏**应用 > 添加应用**。
3. 选择 JWT 应用模板，点击添加应用。创建一个应用

4. 创建成功后，点击立即授权，给应用授权

> **说明**
>
> 您也可以在左侧导航栏点击 **授权 > 应用授权** ，给应用进行授权



配置SCIM同步

在应用列表中，选择应用，点击展开应用的详情

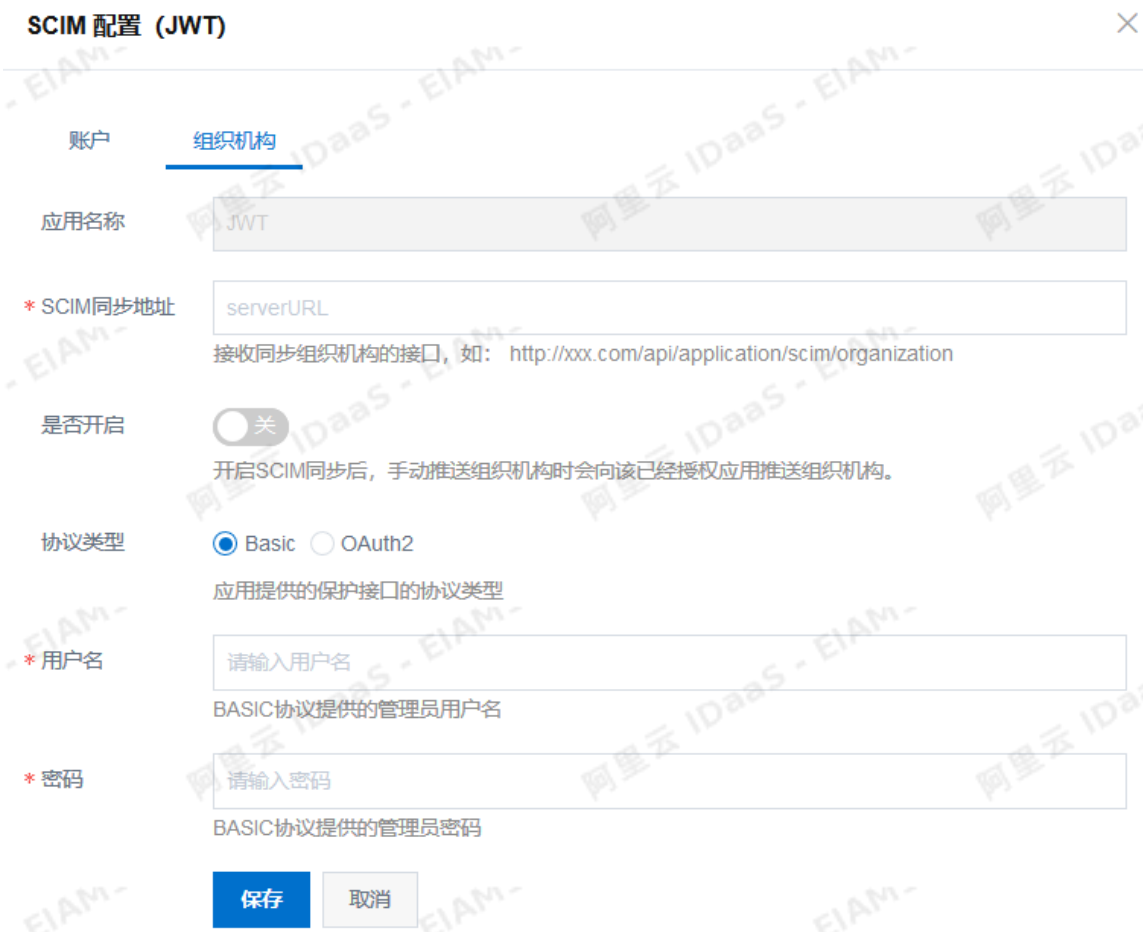
点击应用的SCIM配置

SCIM同步支持“Basic”和“OAuth2”两种协议类型。

- Basic

  Basic协议支持所有类型的SP应用，组织机构和账户的同步配置信息如下图：

- 配置组织机构同步信息


SCIM 配置（JWT）
账户
组织机构
应用名称
JWT
* SCIM同步地址
serverURL
接收同步组织机构的接口，如： http://xxx.com/api/application/scim/organization
是否开启
关
开启SCIM同步后，手动推送组织机构时会向该已经授权应用推送组织机构。
协议类型
Basic
OAuth2
应用提供的保护接口的协议类型
* 用户名
请输入用户名
BASIC协议提供的管理员用户名
* 密码
请输入密码
BASIC协议提供的管理员密码
保存
取消

- 配置账户同步信息

其中：

SCIM同步地址：在SP应用中获取，为业务系统接收组织机构/账户的接口地址。

用户名和密码：SP应用的登录账户和密码。

- OAuth2

SP应用支持Oauth2协议时才可选择组织机构和账户的同步配置信息如下图：

- 配置组织机构同步信息


SCIM 配置（JWT）
账户
组织机构
应用名称
JWT
* SCIM同步地址
serverURL
接收同步组织机构的接口，如： http://xxx.com/api/application/scim/organization
是否开启
开
开启SCIM同步后，手动推送组织机构时会向该已经授权应用推送组织机构。
协议类型
Basic
OAuth2
应用提供的保护接口的协议类型
* oauth url
http:// or https://
oauth url 必填
* client_id
client_id
client_id 必填
* client_secret
client_secret
client_secret 必填
保存
取消

- 配置账户的同步信息

其中：

SCIM同步地址：业务系统接收组织机构/账户的接口地址。

oauth_url：业务系统OAuth2鉴权的地址，通常是业务系统访问地址/oauth/token

client_id：OAuth2鉴权使用的client_id

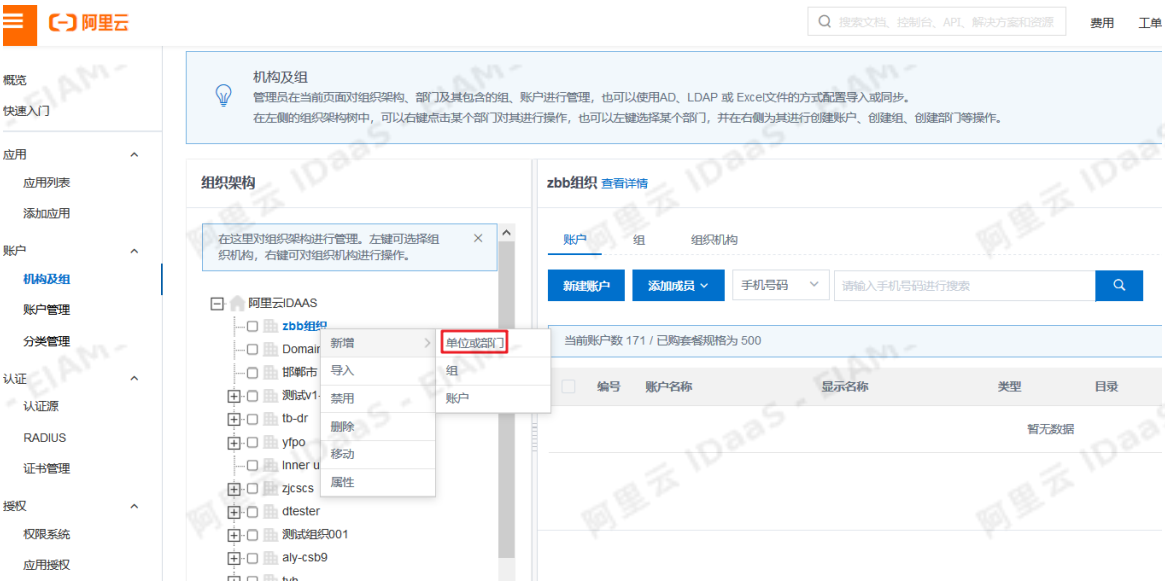
client_secret：OAuth2鉴权使用的 client_secret

> 说明
>
> IDaaS内置的应用模板，如钉钉、RAM、阿里邮箱等也支持 OAuth2 协议的数据同步。这些应用模板配置SCIM同步填写的参数的获取方式与上述描述的不太一致。如果您需要同步到这些系统，请根据具体的文档进行配置。

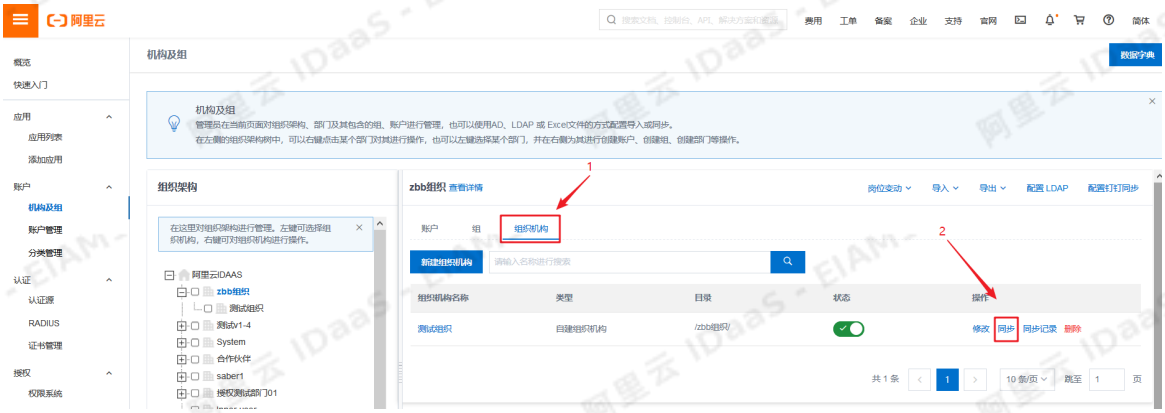
数据同步

- 组织机构同步到SP应用中

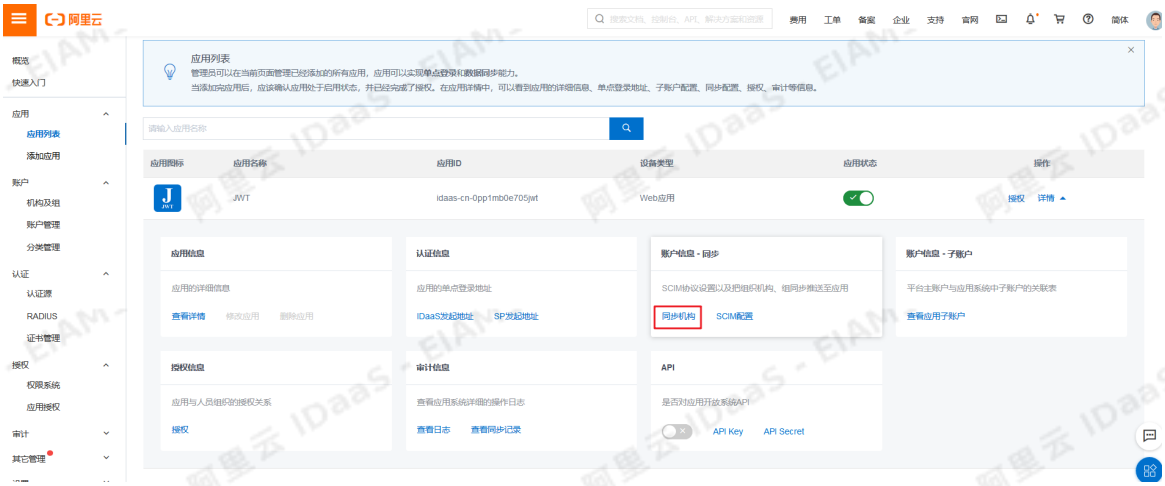
- 新增组织机构进行同步：在账户及组页面，右击组织机构选择新增组织机构



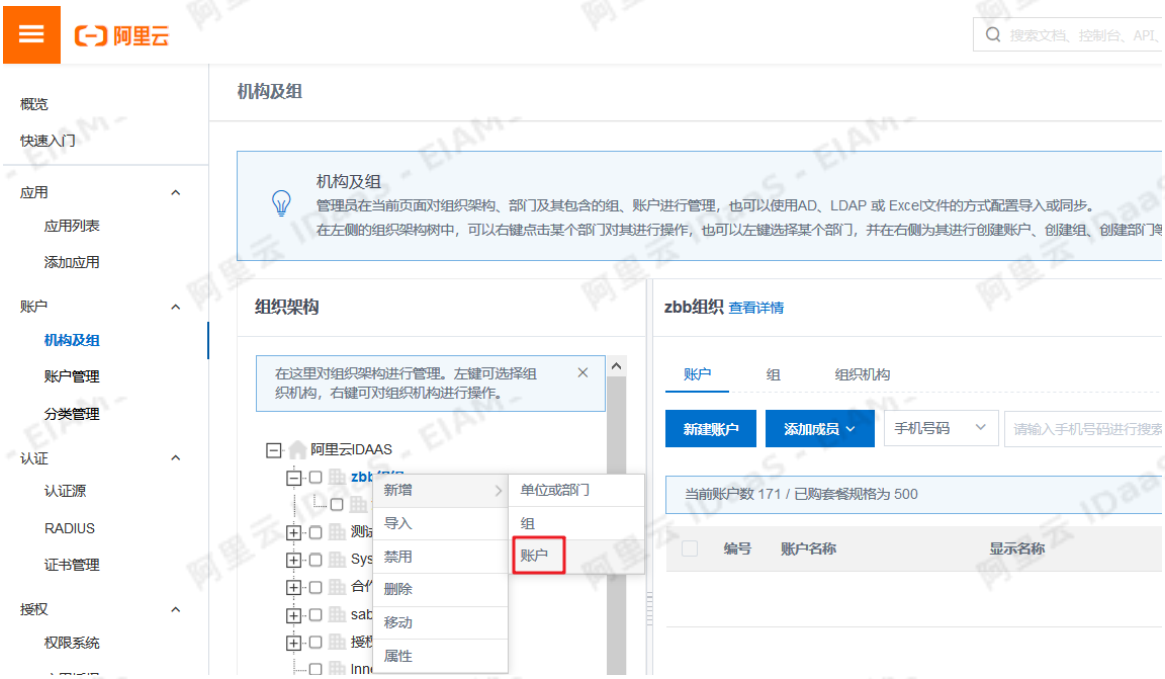
- 手动同步组织机构：在账户及组页面，右侧选择组织机构栏，点击组织机构操作中的同步



- 针对某个应用进行组织机构的同步：在应用列表中点开应用详情，在账户信息-同步标签下，点击同步机构进行同步

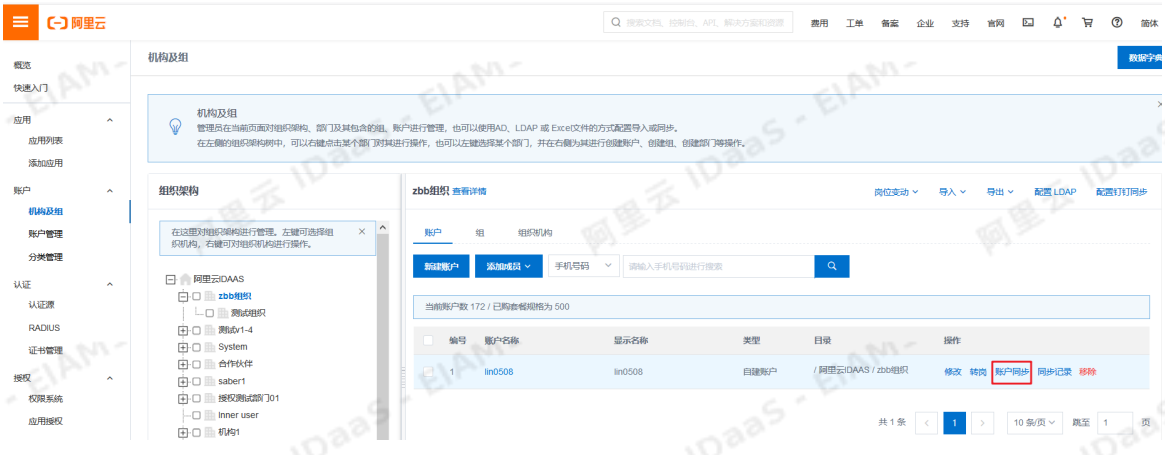


- 账户同步到SP应用中
  - 新增账户进行同步：在账户及组页面，右击组织机构选择新增账户


阿里云
概览
快速入门
应用
应用列表
添加应用
账户
机构及组
账户管理
分类管理
认证
认证源
RADIUS
证书管理
授权
权限系统
机构及组
机构及组
管理员在当前页面对组织架构、部门及其包含的组、账户进行管理，也可以使用AD、LDAP 或 Excel文件的方式配置导入或同步。
在左侧的组织架构树中，可以右键点击某个部门对其进行操作，也可以左键选择某个部门，并在右侧为其进行创建账户、创建组、创建部门
组织架构
在这里对组织架构进行管理。左键可选择组织机构，右键可对组织机构进行操作。
阿里云IDAAS
新增
导入
禁用
删除
移动
属性
单位或部门
组
账户
zbb组织 查看详情
账户
组
组织机构
新建账户
添加成员
手机号码
当前账户数 171 / 已购套餐规格为 500
编号
账户名称
显示名称


增量同步
LDAP同步
将数据同步至所有LDAP
应用授权
将自动继承父级的应用授权
3
SCIM同步
通过SCIM将数据同步至已授权应用
当前已授权并配置了可以同步的应用:
JWT
当前已授权但未配置同步的应用:
暂无
确认
取消

- 手动同步账户：在账户及组页面，右侧选择账户栏，点击账户操作中的账户同步。



- 批量同步机构下的账户：在手动同步机构时，可以勾选是否同步子级账号 选项，同步时会将机构下的账户批量同步到应用系统中。

1.2. IDaaS 同步中心使用说明

同步中心说明

同步中心功能通过connector进行实现，connector需要进行单独部署。

Connector只专属版进行提供，标准版不支持。

使用connector原因

1. IDaaS如果同步的数据量过大，会有网关超时的限制，如果把同步功能放到connector中，connector进行独立部署，不会引起网关超时；
2. 内网应用，如AD无法和公网直接通信，可以在内外网之间部署connector，实现内网AD经由connector同步数据到公网IDaaS的目的；
3. 通过定时自动从AD同步账户到IDaaS，以及阿里云控制台。

Connector和IDaaS结合实现的场景

1. IDaaS和AD之间的双向同步
2. IDaaS和钉钉之间的双向同步
3. IDaaS同步账户到RAM系统

1. 同步中心配置

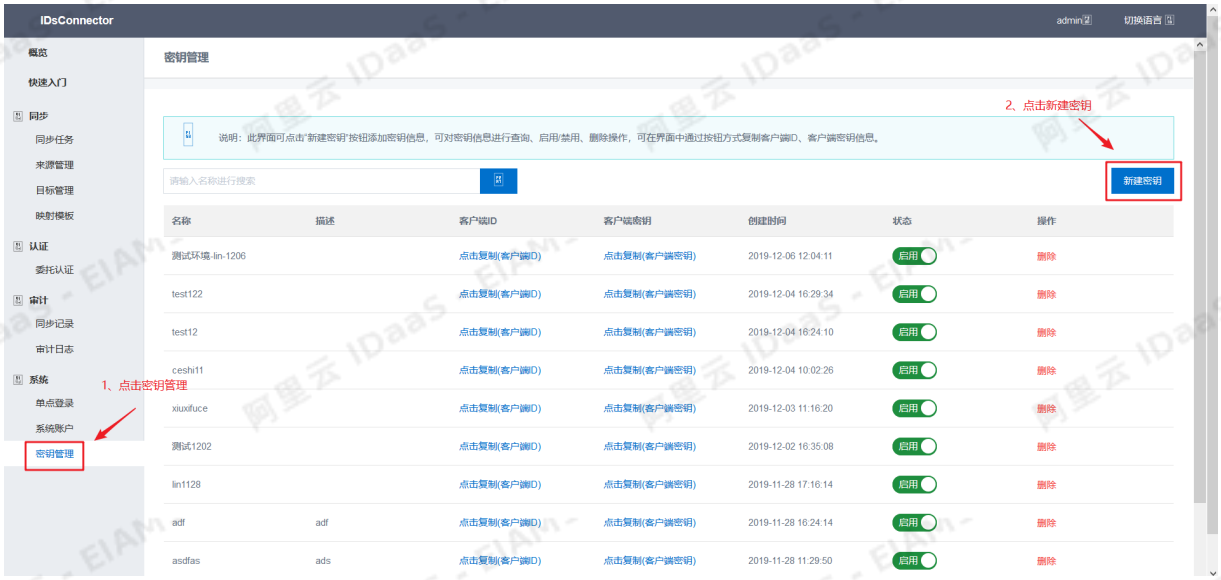
此处我们使用connector从AD同步数据到IDaaS，再同步账户到RAM进行配置说明

1.1. 前提

Connector 需要部署在阿里云的ECS服务器上，需要用户自行购买。服务器的配置推荐为4核8G，200G的存储空间。操作系统选择CentOS 7以上64bit的Linux系统

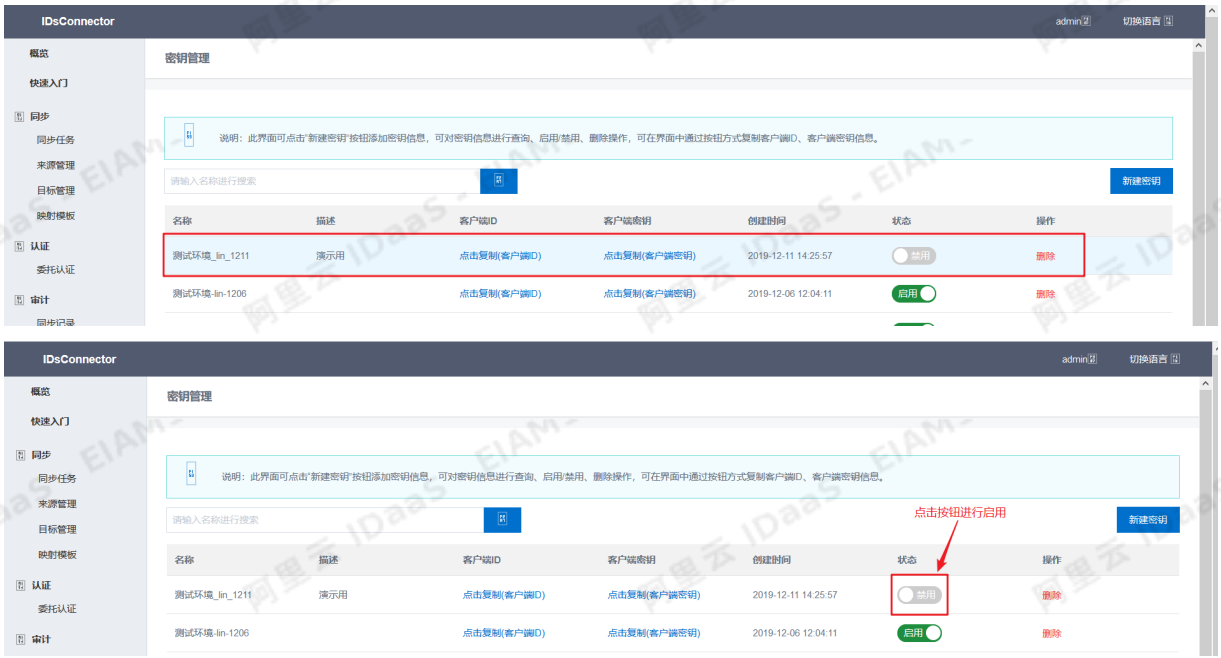
1.2. 添加建立连接使用的密钥对

部署好Connector组件之后，在浏览器输入服务器的IP进行访问。登录成功之后，点击左侧导航栏中的密钥管理，添加一对密钥。



在新建密钥界面输入密钥的名称即可。如果需要建立多个密钥，则需要保证名称的唯一性。

点击保存之后，界面上会展示一条新的密钥信息，点击按钮进行启用。



IDaaS同步中心创建Connector连接器时，需要填写Connector的客户端ID和客户端密钥，从此处直接点击复制即可。一个密钥对对应一个Connector连接器，如需创建多个Connector连接器，需要创建多个密钥对。

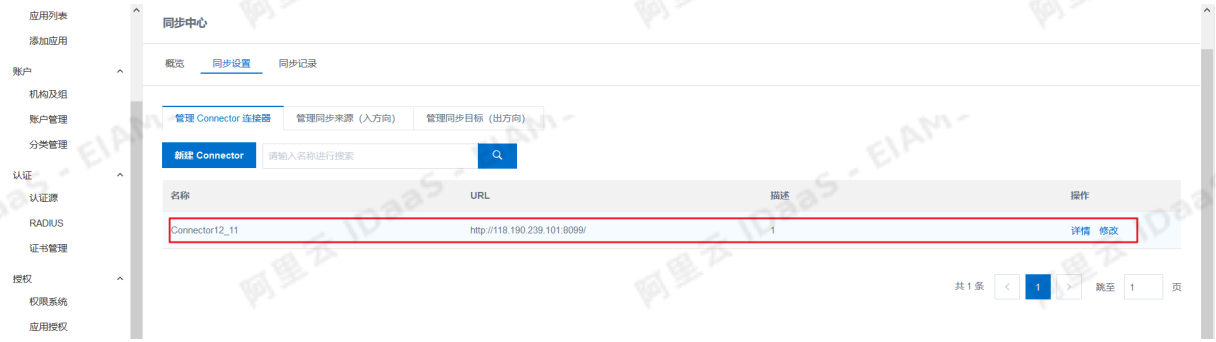
1.3. 新建Conntector连接

管理员登录后，在左侧导航栏中点击同步中心，切换到同步设置页面。在管理Connector连接器的标签下，点击新建Connector

必填项参数说明：

- 名称：connector连接器的名称
- 接口调用地址： connector的地址接口
- ClientId：上述步骤创建好密钥对后，获取的客户端ID接口
- ClientSecret：上述步骤创建好密钥对后，获取的客户端密钥

创建成功之后，会在管理Connector连接器中创建一条记录，如图：

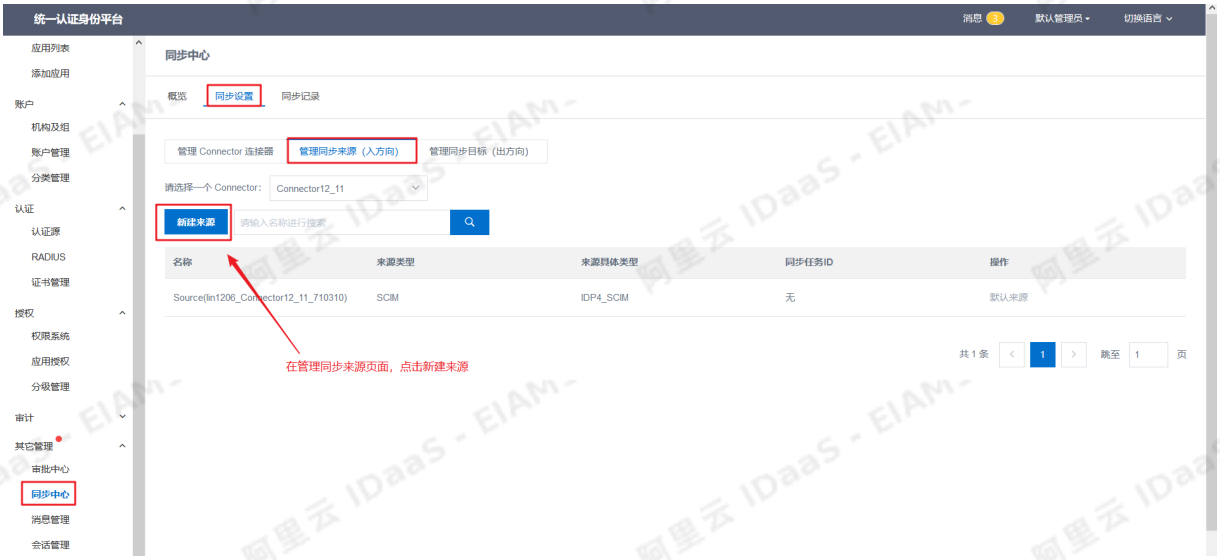


2. 拉取第三方应用/AD数据到IDaaS

本章节以LDAP作为数据源，介绍如何配置实现拉取LDAP数据到IDaaS。

2.1. 创建同步来源

在管理同步来源（入方向）的标签下，点击新建来源。




新建同步来源
同步来源指的是一个同步事件中的源头方，在这里配置的是相对于 IDaaS 而言同步进来的数据来源，一般是企业的现有用户目录、HR 系统等。
* 名称
测试LDAP
来源名称长度不能超过32个字符
* 来源类型
LDAP / OPEN_LDAP
同步来源类型
描述
请输入来源描述
同步来源描述
是否启用
是否启用
是否启用同步来源

参数说明：

- 名称：同步来源的名称，唯一
- 来源类型：同步来源使用的协议类型以及子类型，如LDAP/OPEN_LDAP指的是来源使用的是LDAP协议，类型是OPEN_LDAP
- LDAP服务器的连接信息
  - 服务器地址：LDAP服务器的地址
  - 端口号：LDAP服务器的端口号，默认为389
  - Base DN：LDAP同步来源的账户范围
  - 管理员DN：拥有LDAP管理员权限的账号

- 管理员密码：管理员账户对应的密码

2.2. 配置同步任务

创建同步来源后，需要配置同步任务。在管理同步来源（入方向）的标签下，选择同步来源，点击配置同步。

参数说明：

- 名称：同步任务的名称，需要唯一
- 目标根节点标识：IDaaS中目标机构的外部ID，获取方式如图
- 描述：同步任务的描述

配置完成之后，点击立刻执行同步，即可实现拉取LDAP数据到IDaaS平台。

2.3. 设置定时同步

Connector组件还支持定时同步功能，即定时拉取LDAP数据到IDaaS平台，配置步骤如下：

1、在Connector应用界面点击同步任务，选择对应的任务点击编辑

2、点击“下一步”，切换到“同步计划”标签页。然后开启定时同步，并进行配置。

3、配置定时同步任务

定时同步任务有两种执行方式，分别是周期执行和定时执行：

- 周期执行：每隔一段时间将LDAP数据拉取到IDaaS平台，时间间隔由管理员设定，最短1小时，最长23小时。
- 定时执行：到规定时间后自动执行同步任务，将LDAP数据拉取到IDaaS平台，时间可以由管理员设置，可以添加多个执行时间点。

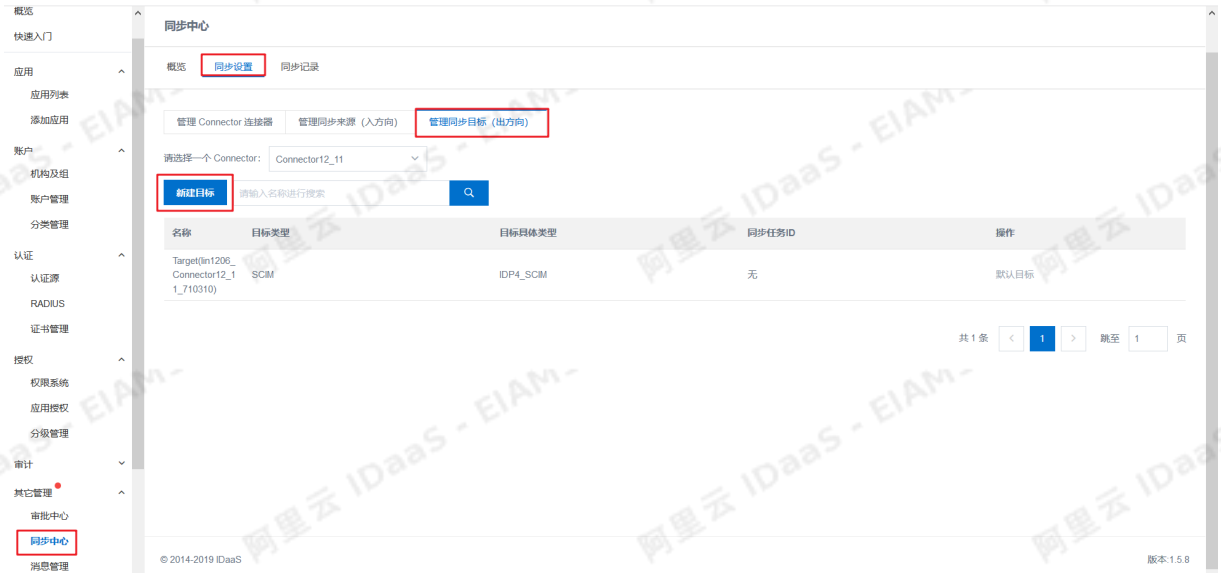
通过以上步骤即可实现定时执行同步任务。

3. 将IDaaS数据推送到第三方应用

本章节以阿里云RAM作为接收方，介绍如何配置实现将IDaaS数据推送到RAM。

3.1. 创建同步目标

在管理同步目标（出方向）的标签下，点击新建目标。



必填参数说明

- 目标名称：同步目标的名称，需唯一
- 目标类型：同步目标的应用类型或使用的协议类型及子类型
- 区域ID：固定值，为cn-hangzhouAccess Key ID：阿里云RAM中的
- AccessKey ID，获取方式如图Access Key Secret：阿里云RAM中的AccessKey Secret，获取方式如图
  API 版本：IDaaS 对外提供的 API 版本，固定为v1.2

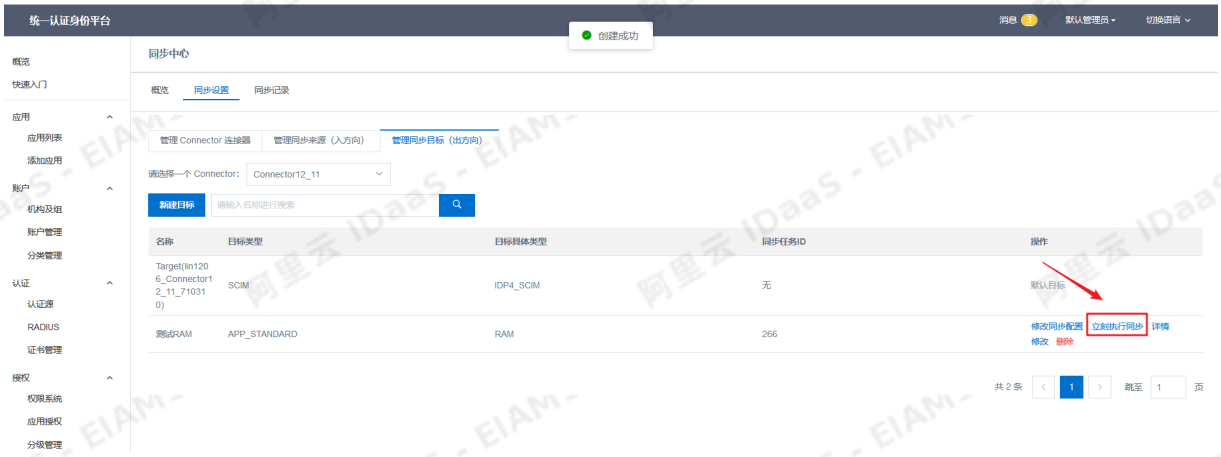
3.2. 配置同步任务

创建同步目标后，需要配置同步任务。在管理同步目标（出方向）的标签下，选择同步目标，点击配置同步。

参数说明：

- 名称：同步任务的名称，需要唯一
- 描述：同步任务的描述

配置完成之后，点击立刻执行同步，即可实现将IDaaS数据全量推送到阿里云RAM。



3.3. 自动同步及同步范围

3.3.1. 自动同步

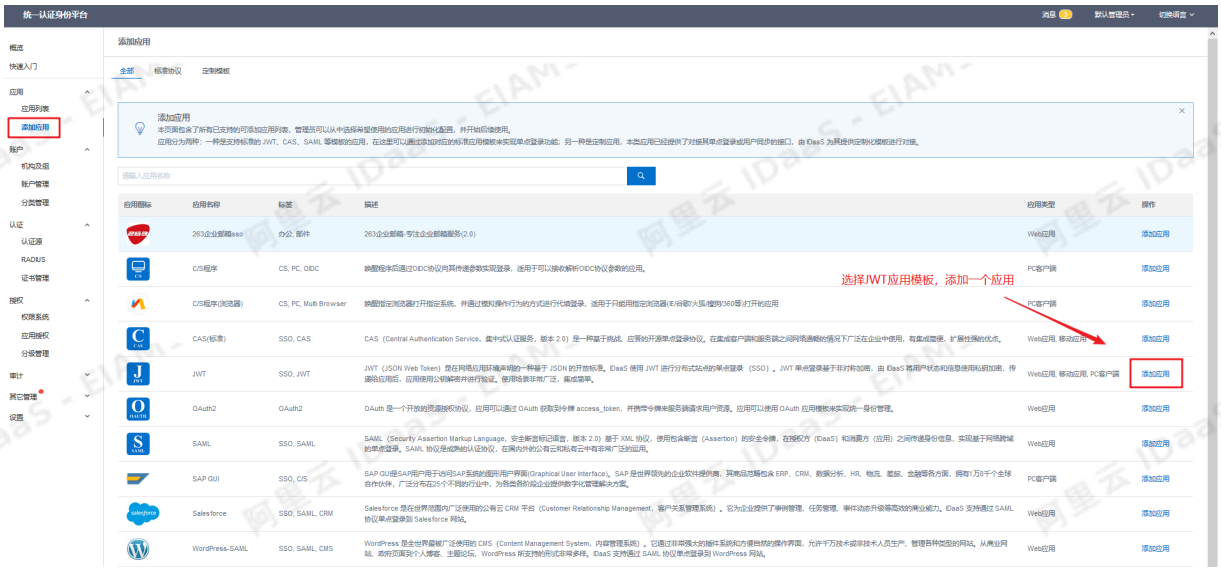
同步中心默认将同步来源同步到IDaaS的数据自动推送同步目标。即如果依照上述步骤同时配置了LDAP同步来源和RAM同步目标，管理员在同步中心手动点击LDAP来源的“立刻执行同步”按钮后。会拉取LDAP的数据到IDaaS，并且同时将拉取到的数据推送到RAM。

3.3.2. 设置自动同步的范围

管理员可以在管理同步目标（出方向）中，进行同步范围的配置。操作步骤如下：

1、创建应用

管理员在左侧导航栏中点击添加应用，进入添加应用界面。选择JWT应用模板，创建一个应用：

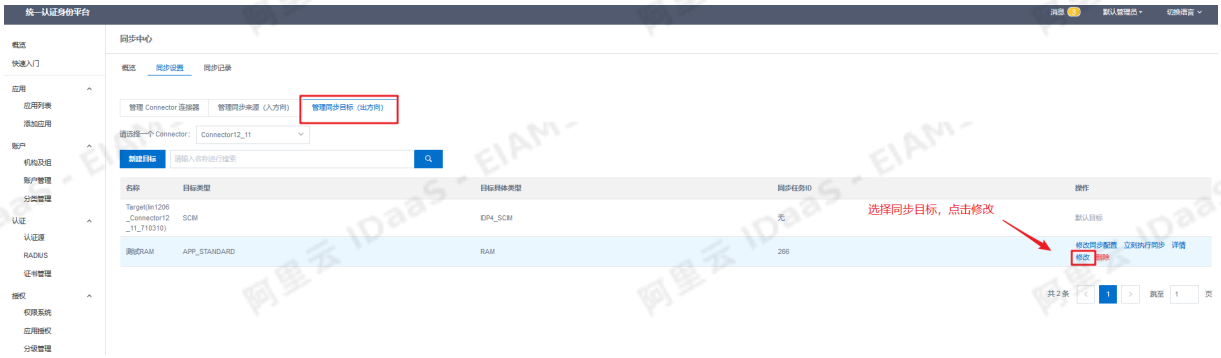


2、应用授权

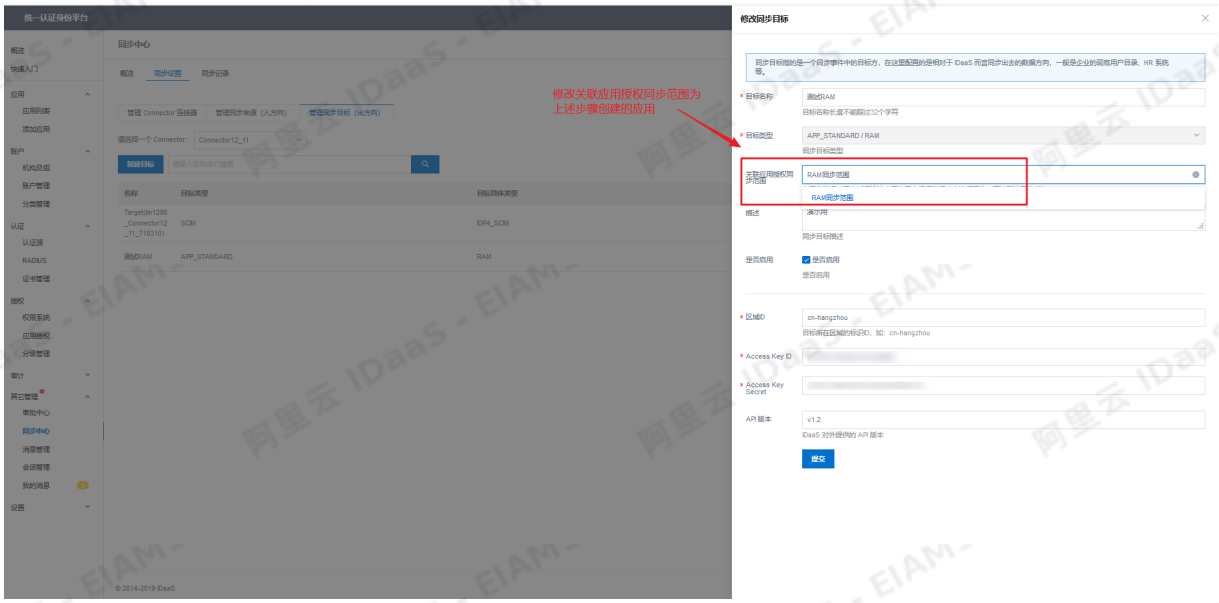
在左侧导航栏中点击应用授权，选择对应的应用改变授权范围。下图表示仅对机构1及其子级机构进行授权。

3、配置关联应用授权同步范围

在管理同步目标（出方向）标签下，选择同步目标，点击修改。



关联应用授权同步范围，输入应用的名称，点击保存。



通过以上步骤，实现自动同步到同步目标时，仅同步指定范围的账户和机构。

1.3. LDAP账户同步配置

IDaaS 可以通过 LDAP 配置从 AD 或 OpenLDAP 中拉取组织机构和账户信息。同时支持向 AD 或 OpenLDAP 的增量和全量同步。

新建LDAP配置

操作步骤

1. 以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考 登录。
2. 点击左侧导航栏**账户 -> 机构及组**。
3. 点击【配置LDAP】，新建LDAP配置，填入必填信息，开启从 IDaaS 同步至 LDAP。

服务器链接：

- 服务名称

- 服务器地址和端口
- Base DN
- 是否使用 SSL 连接方式
- 管理员账户和密码
- 类型选择（ Windows AD/OpenLDAP ）

> **说明**
>
> IDaaS目前只支持公网访问，AD/LDAP需要提供公网地址，并开启389端口，可以在安全组策略设置只有IDaaS的出口IP可以访问AD/LDAP, IDaaS出口IP请提工单咨询IDaaS同学获取。

上述参数为LDAP连接的基本参数，请根据 LDAP 服务器的信息进行填写

- 所属组织架构 OU 节点：填写后，可以将 LDAP 的数据导入 IDaaS 平台指定的组织机构下，不填则默认导入到 IDaaS 根目录下。
- LDAP 同步至本系统：启用后，可以手动从 LDAP 同步数据到 IDaaS 系统
- 本系统同步至 LDAP: 启用后，在 IDaaS 系统对组织机构和账户进行操作后，会自动同步到 LDAP，

配置好后可点击测试连接，测试AD/LDAP是否连接正常。

字段匹配规则：

> **说明**
>
> 字段匹配规则为 IDaaS 中字段与 AD/LDAP 中属性的对应匹配

- 账户名称：cn（如AD中的cn对应在IDaaS的账户名）

> **说明**
>
> 如果您 AD 中的账户的 CN 字段值为中文，无法拉取到IDaaS。建议您使用 sAMAccountName 字段。

- 外部id：Windows AD 填写 objectGUID, OpenLdap 填写 uid
- 密码字段：Windows AD 填写 unicodePwd, OpenLdap 填写 userPassword

- 用户唯一标识：Windows AD 填写 DistinguishedName, OpenLdap 填写 EntryDN
- 手机字段：telephoneNumber
- 邮箱字段：mail
- 默认密码：定时从AD/LDAP 同步账户到IDaaS系统时的默认密码
- 昵称：在IDaaS中账户的显示名称

从AD导入组织机构和账户

- **导入组织机构**

i. 在机构及组页面，点击导入-LDAP-组织机构。

ii. 选择添加的LDAP配置，点击导入。

iii. 页面会展示组织机构的临时数据。确认数据正确后，点击确定导入，即可将AD的组织机构全量导入到IDaaS。

- **导入账户**

  i. 在**机构及组**页面，点击**导入-LDAP-账户**。

  ii. 选择添加的LDAP配置，点击**导入**。

iii. 页面会展示组织机构的临时数据。确认数据正确后，点击确定导入，即可将AD的组织机构全量导入到IDaaS 。

导出组织机构或账户到AD

> 重要
>
> 导出组织机构及账户时，请确认已将父级组织机构导出到AD，否则会导出失败。

- **导出组织机构**

  i. 在机构及组页面，点击导出-LDAP-组织机构。

  ii. 勾选LDAP配置，再勾选需要导出的组织机构。

iii. 点击确定，成功导出后会显示如下提示。

- **导出账户**
  i. 在机构及组页面，点击导出-LDAP-账户。
  ii. 勾选LDAP配置，再勾选需要导出账户的组织机构，点击确定即可将机构下的账户导出到AD。
  iii. 切换到单个导出页签，也可以支持导出指定账户到AD。

通过上述步骤，即可将IDaaS组织机构和账户数据导出到AD。

FAQ

1. 是否可以使用ldap账户进行登录？

可以，请查看LDAP认证登录

可以，请查看LDAP认证登录

2. 是否可以实现定时自动从AD中同步账户到IDaaS？

支持。需要使用connector实现同步，只在专属版支持。

3. 是否可以只导入某个OU中的账户信息？

可以。需要新建ldap同步配置，不支持在原来配置上修改Base DN，在Base DN 中加上OU值。

4. 新建LDAP配置，点击测试连接失败。

请求连接后需要比较久才返回结果，请查看网络是否通，IDaaS目前只支持公网访问；

请求连接后很快返回连接失败，请检查配置的连接参数是否正确，以及检查密码，密码会转义特殊字符，如 <>，单引号，双引号等。

5. 从IDaaS导出组织机构到LDAP，提示：导出失败，请检查配置。

往LDAP中导出组织机构是有层级结构的，请确认IDaaS中组织机构的根节点是否已经导出到LDAP中，如下图所示。

6. 从LDAP导入账户到IDaaS， 提示：InvalidUserLicense。

请查看购买的license数是否足够， 比如购买了100个license，导入的账户数超出了这个限制。可以先指定base DN 到某个OU， 先导入部分账户测试，或者升级license数量。

7. 从IDaaS导出组织机构到LDAP成功，但是导出账户提示导出成功0个。

请查看LDAP配置中的字段匹配规格是否正确，请参考下图参数配置。

8. 本地内网AD是否可以支持数据同步？

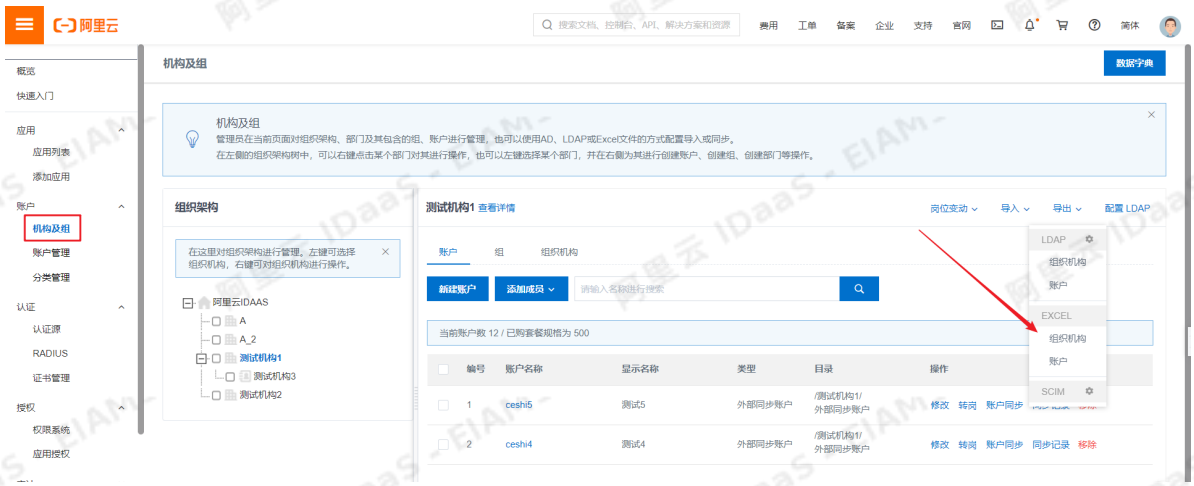
支持，需要使用connector实现，只在专属版支持，对接过程请查看同步中心使用说明。

1.4. IDaaS通过Excel导出和导入流程

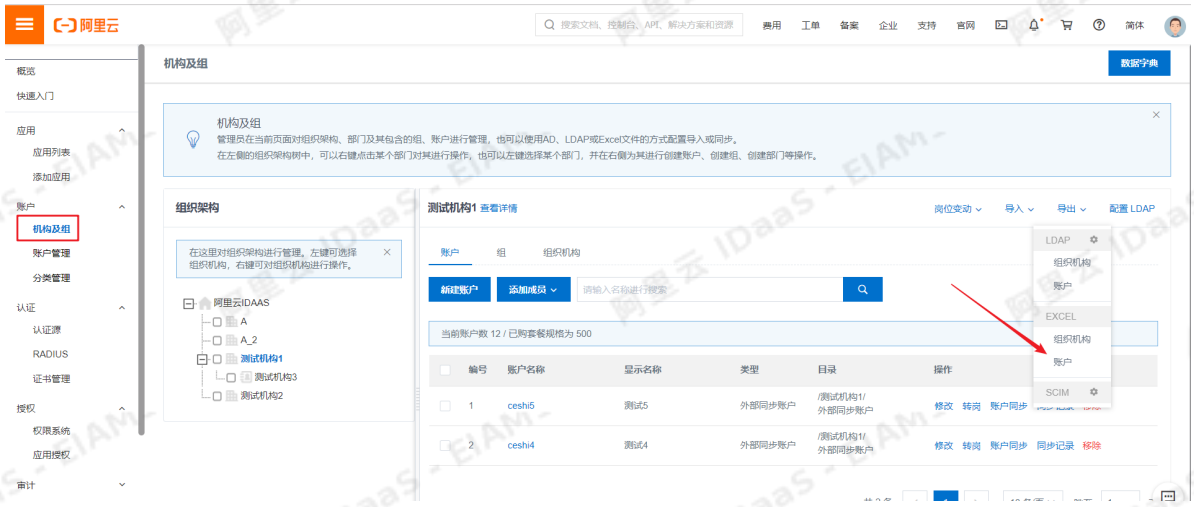
Excel导出组织机构和账户

操作步骤

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，点击账户 > 机构及组。
3. 选择需要导出的机构，点击导出-excel-组织机构，即可导出对应组织机构下的所有组织机构。



4. 选择需要导出的机构，点击导出-excel-账户，即可导出对应组织机构下的所有账户。

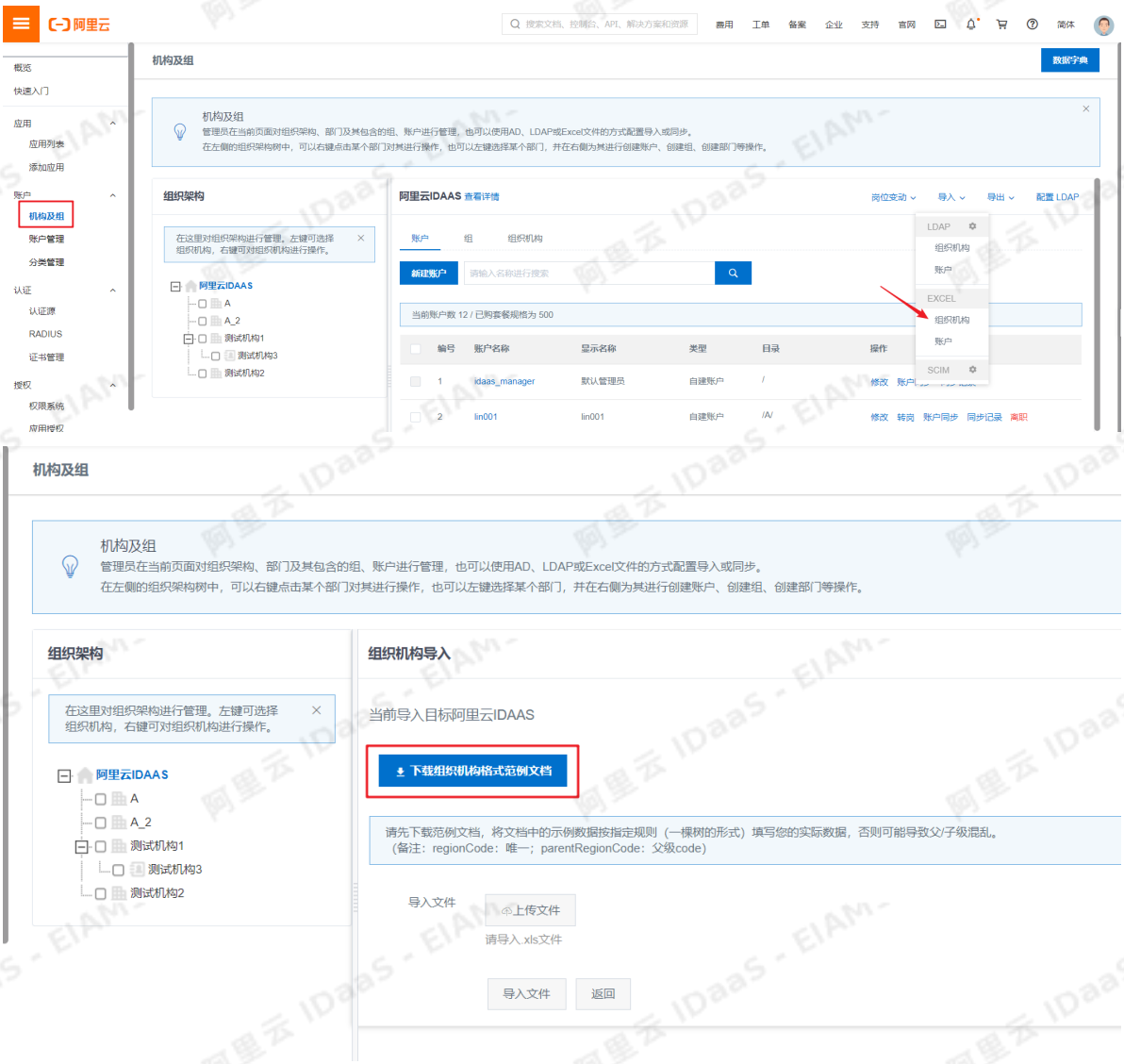


Excel导入组织机构和账户

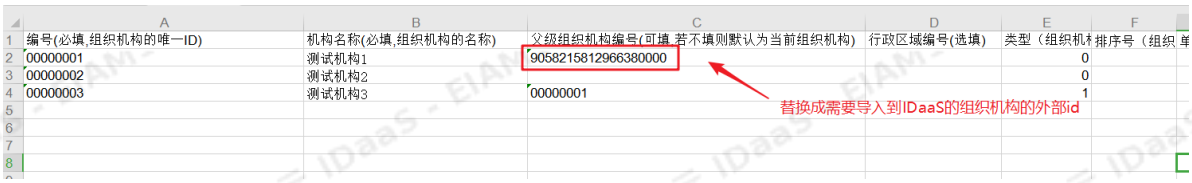
Excel导入组织机构

操作步骤

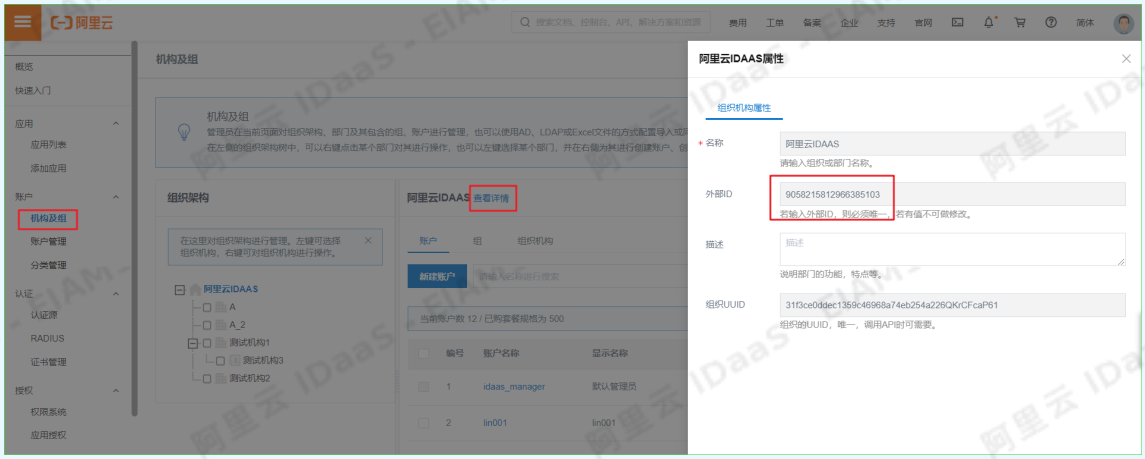
1. 以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考 IT管理员指南-登录。
2. 在左侧导航栏，点击账户 > 机构及组。
3. 点击导入-excel-组织机构，然后点击下载组织机构格式范例文档



4. 根据范例文档填写Excel表格



> 说明
>
> 组织机构的外部ID获取方式如图

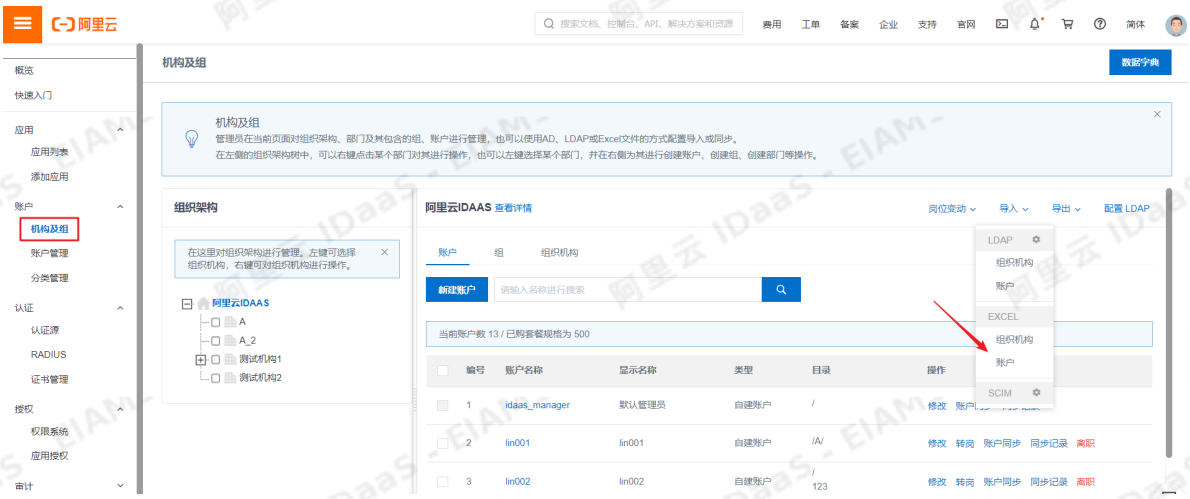


5. 点击上传文件，将填写好的excel上传到IDaaS平台，点击导入文件

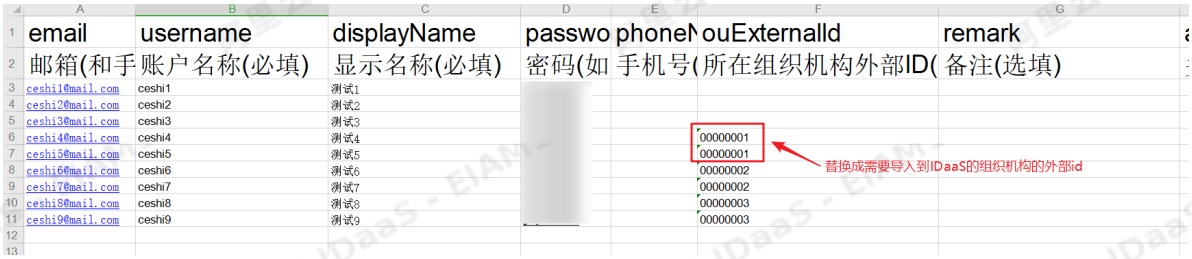
Excel导入账户

操作步骤

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，点击账户 > 机构及组。
3. 点击导入-excel-账户，然后点击下载账户格式范例文档。



4. 根据范例文档填写excel表格



	email	username	displayName	passwo	phoneN	ouExternalId	remark
2	邮箱(和手	账户名称(必填)	显示名称(必填)	密码(如	手机号(	所在组织机构外部ID(	备注(选填)
3	ceshi1@mail.com	ceshi1	测试1				
4	ceshi2@mail.com	ceshi2	测试2				
5	ceshi3@mail.com	ceshi3	测试3				
6	ceshi4@mail.com	ceshi4	测试4			00000001	
7	ceshi5@mail.com	ceshi5	测试5			00000001	
8	ceshi6@mail.com	ceshi6	测试6			00000002	
9	ceshi7@mail.com	ceshi7	测试7			00000002	
10	ceshi8@mail.com	ceshi8	测试8			00000003	
11	ceshi9@mail.com	ceshi9	测试9			00000003	

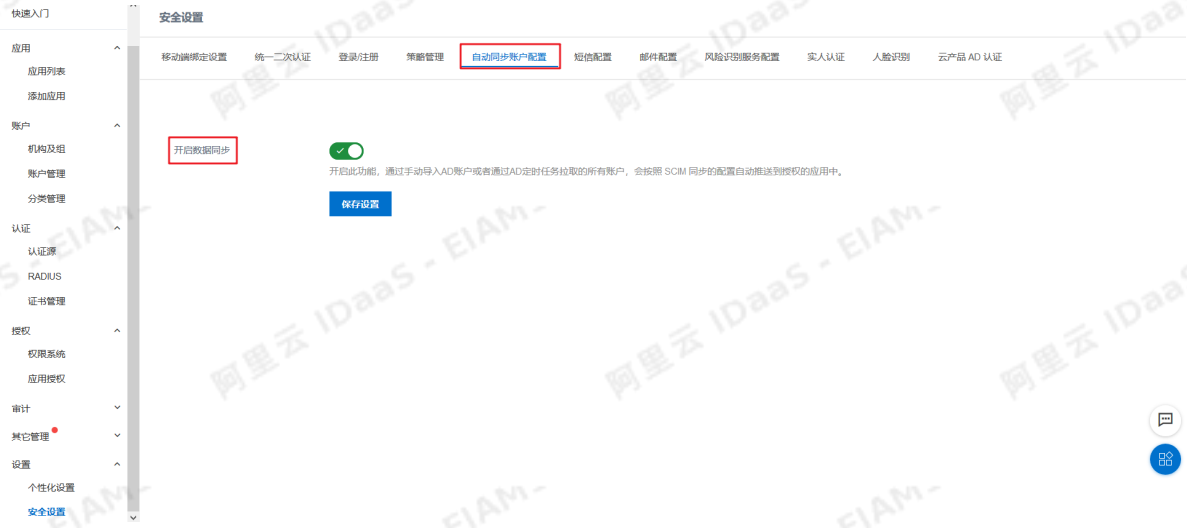
5. 点击上传文件，将填写好的excel上传到IDaaS平台，点击导入文件

1.5. 自动同步账户配置

IDaaS支持定时或手动拉取 AD/LDAP 数据时，自动将账户数据推送到配置了SCIM同步的应用系统中。

操作步骤

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，点击设置 > 安全设置。
3. 点击 **自动同步账户配置** 页签，然后开启数据同步开关，保存设置。



4. 配置应用的SCIM同步，可参考同步账户到应用配置。

完成上述步骤，从AD导入账户及组织机构时，会自动将账户数据推送到配置了SICM同步的应用系统。

2.应用管理

2.1. 添加应用子账户

本文为您介绍如何通过应用管理功能添加应用子账户。通过添加应用子账户，用户可以通过IDaaS单点登录到其他应用。

背景信息

传统应用的登录方式通过输入用户名和密码，随着日常办公软件数量的不断增加、用户需要记忆多套用户名和密码，给用户带来记忆负担；统一所有用户名和密码固然方便，却会令企业账户体系面临严重的安全隐患。

解决方案

IDaas的单点登录功能，只需完成用户的应用子账户的添加，即可实现一键登录后访问所有授权应用，应用之间进行切换时，用户无需再次输入用户名和密码，全面提升办公效率。

操作步骤

1. 管理员添加应用

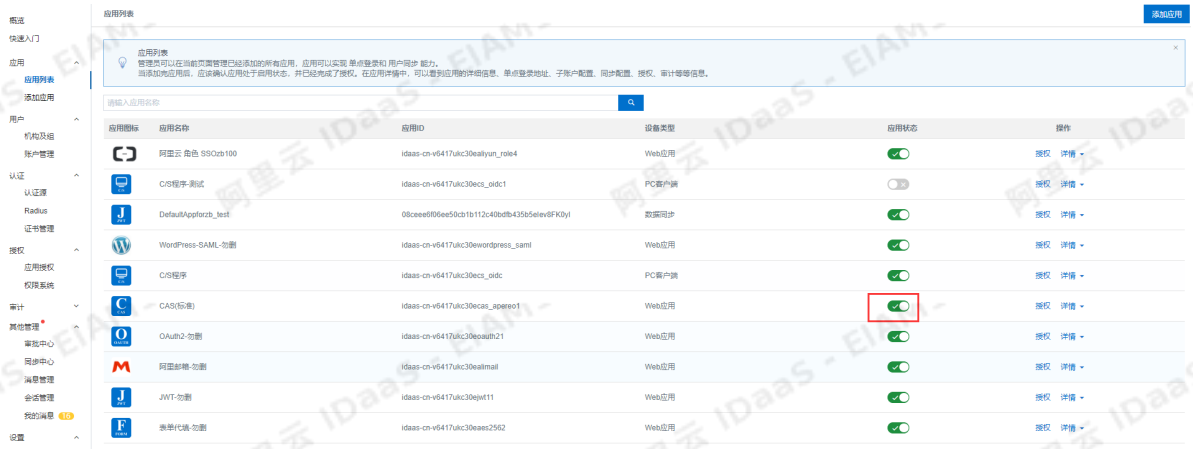
   管理员在添加应用的时候，可以选择账户关联的方式。

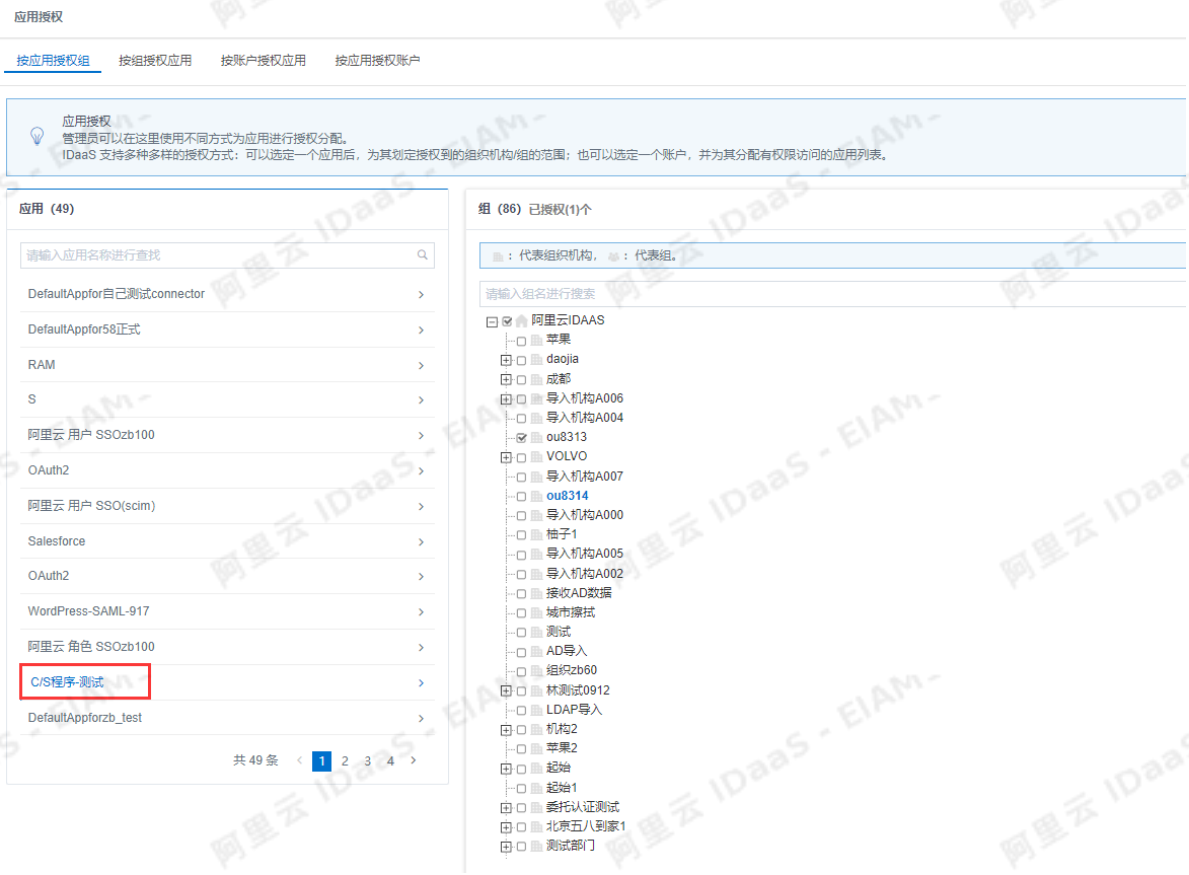
   账户关联方式分为两种：账户关联和账户映射。

   账户关联是系统按照子账户对应关系进行手动关联，适合用户已有应用账户的情况。

   账户映射是指系统自动将主账户名称作为应用的子账户，适合用户没有该应用的账户的情况。

2. 启用应用并将应用授权组织机构





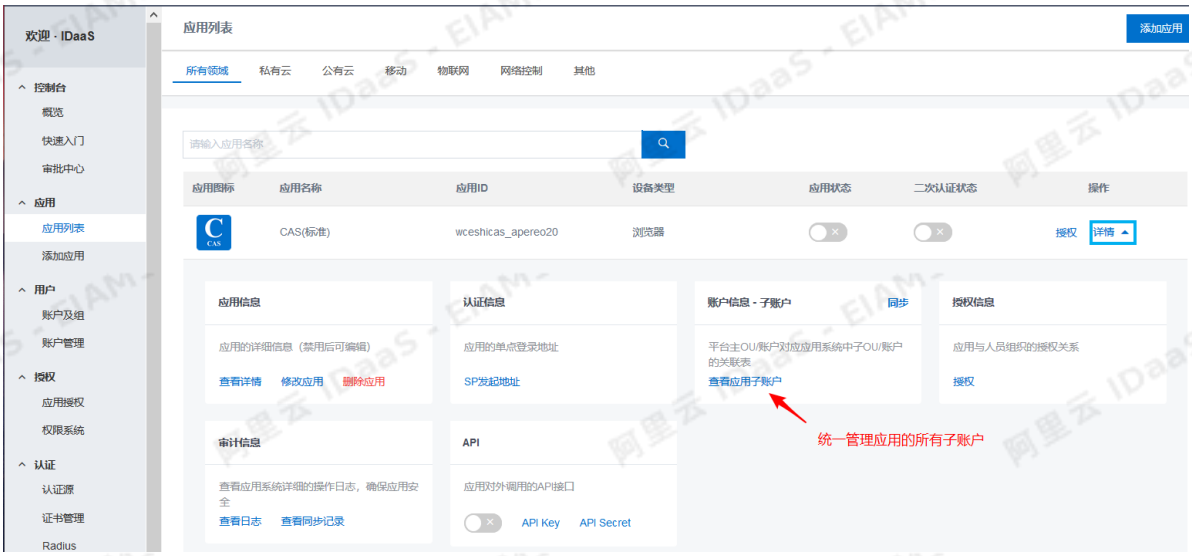
3. 手动添加子账户关联

   手动关联子账户可以分为两种方式：

   - 一是管理员为账户添加子账户关联。
   - 二是用户申请子账户关联，再由管理员对用户的申请进行审批。

管理员为账户添加子账户关联

1. 管理员点击应用的“详情”按钮，点击“查看应用子账户”即可对应用的所用子账户进管理，包括添加应用子账户操作。

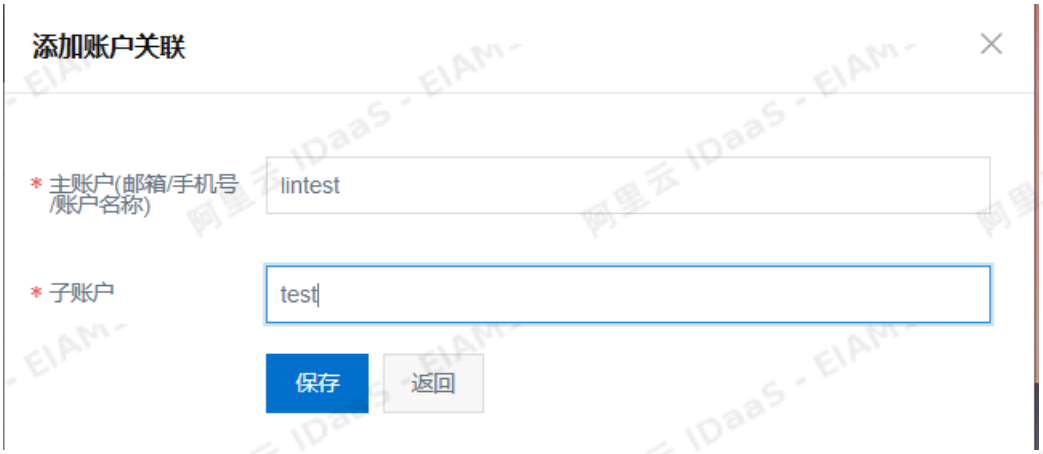


管理员在查看应用子账户界面有两种方式为应用添加账户关联：

- 点击“添加账户关联”

  管理员可以点击“添加账户关联”按钮手动为该应用添加一个关联子账户。

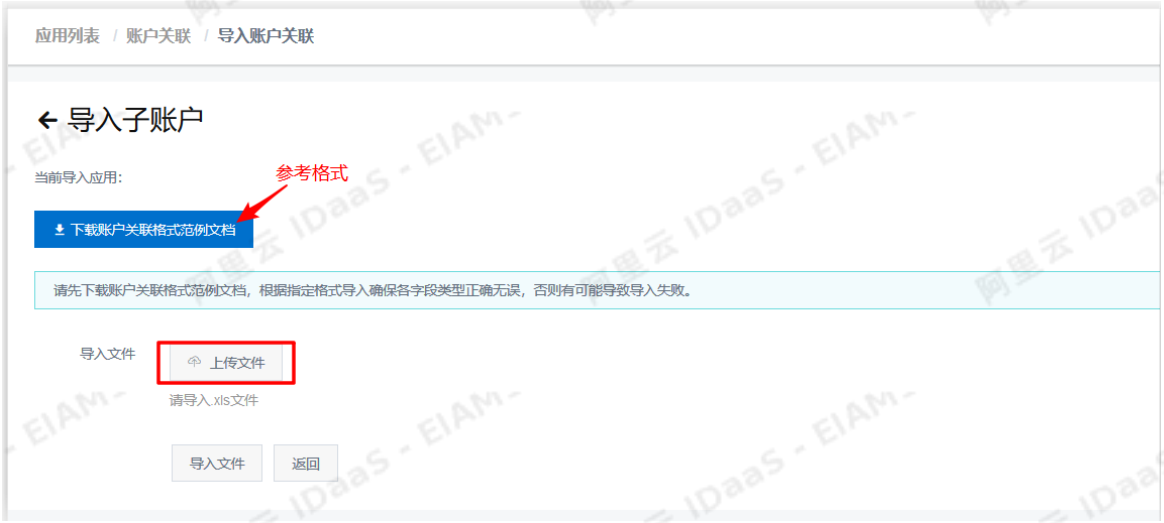
输入主账户的邮箱/手机号/账户名称以及子账户，点击保存按钮，即可成功添加一条账户关联。



- 点击“批量导入”

  管理员可以点击右上角“批量导入”按钮，从文件批量导入关联子账户。

点击“批量导入”按钮后，跳转到导入账户关联页面，点击上传文件，选择需要上传的文件。（上传文件的格式可以参考下载的“账户关联格式范例文档”）.



A列是主账户名称，B列是子账户名称，两个账户相互对应。

	A	B
1	主账户（IDP账户）	子账户（业务系统账户）
2	lintest	uploadtest

上传成功后，点击“导入文件”按钮。

系统会自动检测上传文件的内容，并返回每一条记录的检测结果。管理员可以查看检测结果，并根据结果修改文件，或移除某一条导入数据。确认无误之后，点击右上角“确定上传导入”即可实现批量添加应用子账户。

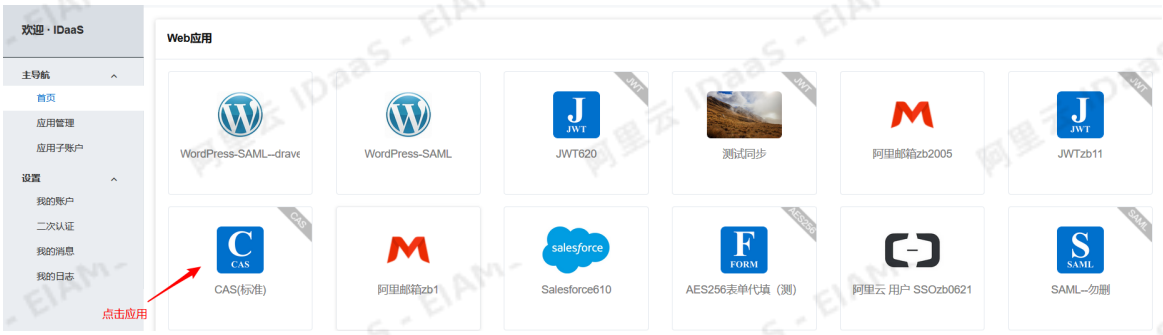
用户申请子账户关联

操作步骤：

1. 用户申请关联子账户

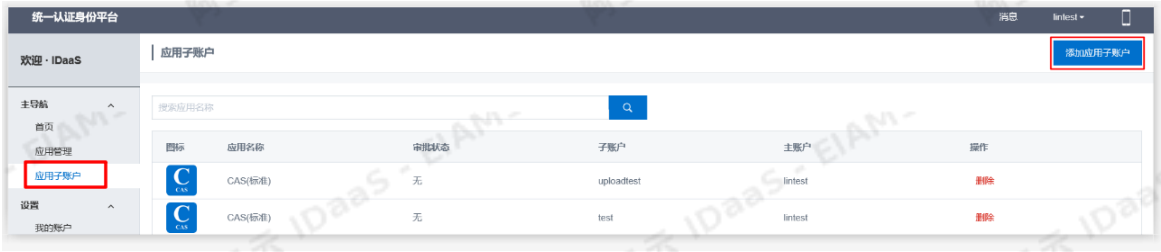
   普通用户有两种途径申请添加应用子账户。

   - 如果应用尚未绑定子账户，可以在首页的免登应用栏中直接点击应用。



   此时会提示用户进行子账户的添加，用户输入子账户，等待管理员审批通过后即可添加该应用的子账户。

   - 用户也可以在导航栏中选择应用子账户，点击右上角的“添加应用子账户”进行子账户的添加。



用户选择添加子账户的应用，输入子账户，点击保存按钮。等待管理员审批通过，即完成了添加子账户。

2. 管理员对用户的申请进行审批

用户发出添加子账户的申请之后，管理员会收到添加子账户的申请。管理员可以在审批中心下的子账户审批中对该用户添加子账户操作进行审批，同意申请后，用户即可成功添加应用子账户。

若以上步骤全部成功完成，即可实现添加应用子账户的功能。

3.其他

3.1. 管理员、普通用户、开发者的访问方式

背景信息

IDaaS 的EIAM实例登录访问区分角色，主要分为三种角色：管理员，普通用户，开发者。

管理员： 创建IDaaS实例后，默认生成管理员角色，可以通过阿里云账户或者RAM账户直接登录到IDaaS管理员页面，在IDaaS管理员页面，可以针对应用，人员，权限，审计等内容进行统一管理。

普通用户：IDaaS提供用于单点登录的门户，需要先在管理员页面创建普通用户，然后通过普通用户可以登录IDaaS门户，点击不同的应用图标实现单点登录。

开发者：如果需要通过接口对接STS令牌服务，需要给开发人员授权开发者角色，用于创建STS应用和查看具体对接参数；如果对接其它接口或功能，不需要授权开发者角色。

管理员登录

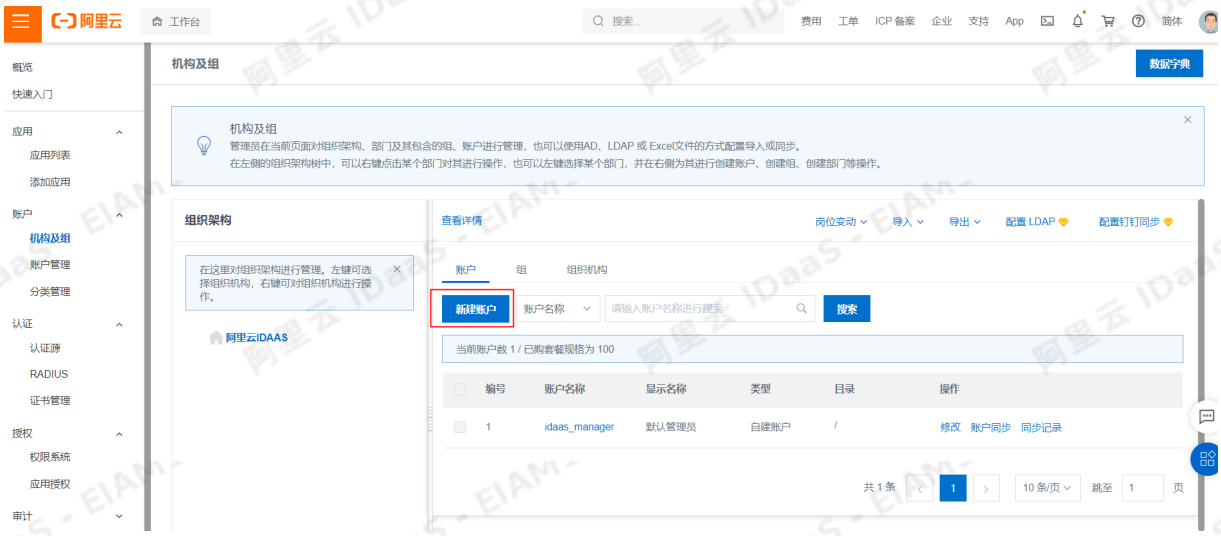
1. 管理员需要先开通IDaaS实例，然后进入云盾IDaaS管理控制台。
2. 在EIAM实例列表页，选择要访问的IDaaS实例，单击【**实例ID**】 或者操作下的【**管理**】。即可进入IDaaS 管理员界面。

3. IDaaS 管理员页面具体操作，请查看对接指引。

普通用户登录

1. 查看管理员登录，访问管理员页面。
2. 在管理员页面，选择左侧导航栏中的【机构及组】。

3. 点击【新建账户】。

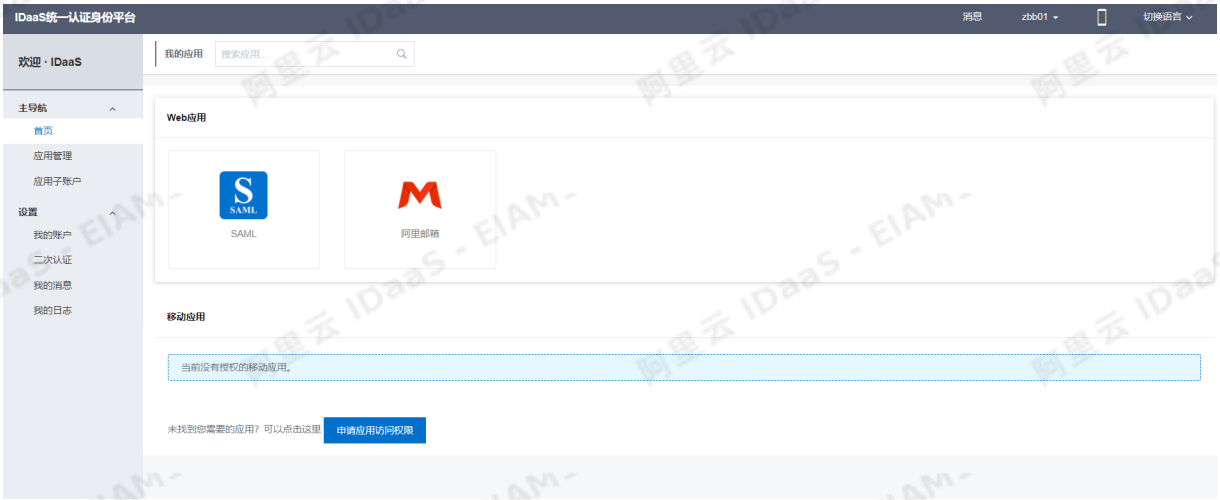


4. 根据页面提示，填写账户信息，点击提交创建账户。

5. 访问IDaaS EIAM实例列表页，点击【用户登录地址】，访问普通用户登录的门户。

6. 输入步骤4中创建的账户进行登录，也支持微信扫码，钉钉扫码，LDAP账户和密码登录，短信登录等方式。

7. 登录以后可以看到不同应用的图标，如下图的阿里邮箱图标，点击后会进行免密登录。



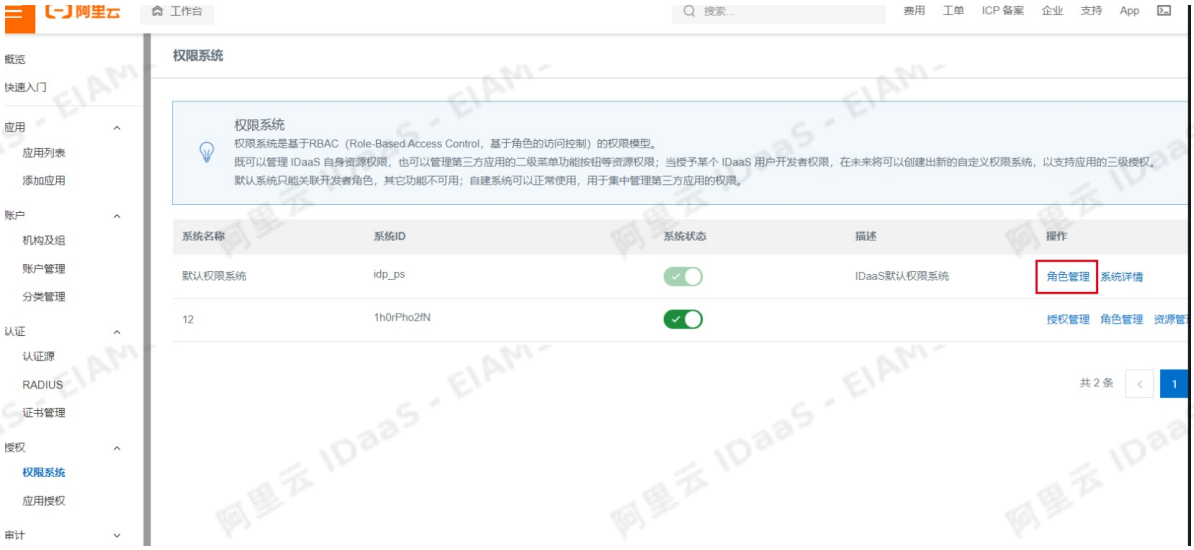
开发者角色授权

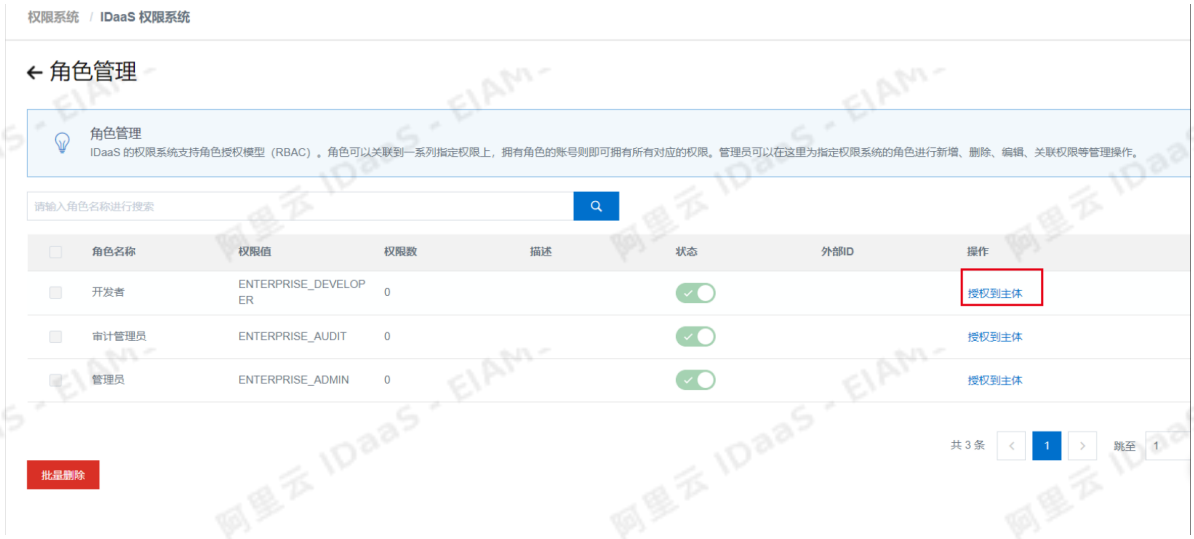
开发者登录方式与普通用户登录方式相同，但需要管理员**授予账户开发者角色**

操作步骤：

1. 以IT管理员账号登录云盾IDaaS管理平台。
2. 点击左侧导航栏【**权限系统**】。

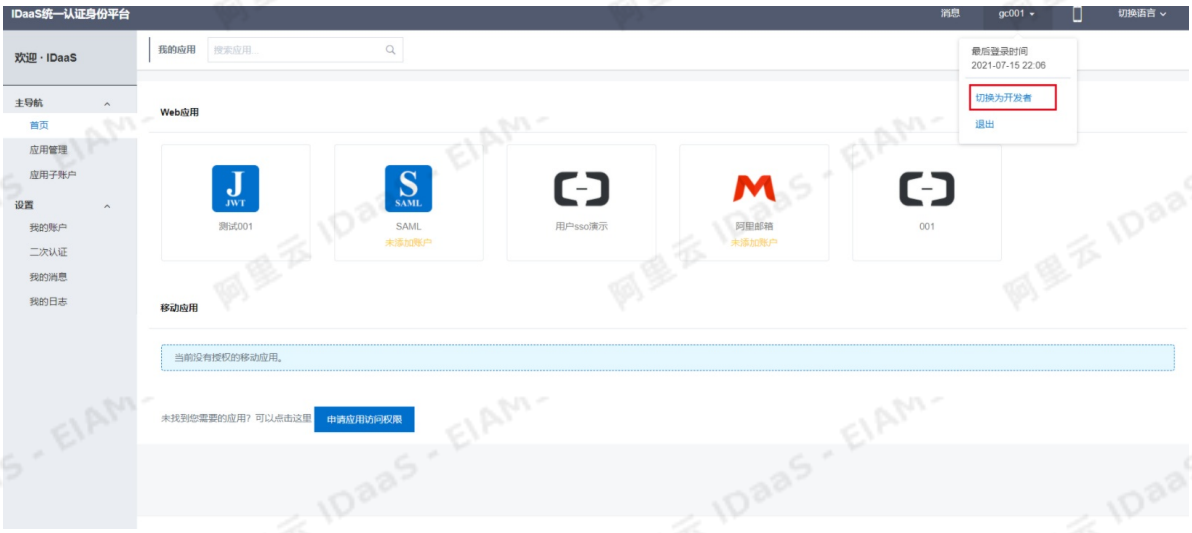
3. 点击【**角色管理**】进入角色管理页面。选择开发者角色，点击授权到主体。





4. 按客体授权到主体页面，在列表中查找想要关联的用户，或直接在输入框中搜索用户的名称，勾选并点击确定，即可授予用户开发者角色

5. 当用户同时拥有普通用户和开发者两种角色时，可以在登录后点击右上角【**切换为开发者**】或 【切换为普通用户】进行角色的切换。



通过以上访问方式（管理员在实例列表点击管理进入、普通用户和开发者通过管理员提供的域名进入），区分管理员和用户的登录方式，避免越权操作。

3.2. 配置自定义域名访问IDaaS

本文介绍如何使用自定义域名访问IDaaS。

前提条件

需要购买SSL证书网站代理HTTPS服务，使用网站代理HTTPS可以申请免费证书，也可以使用付费证书。

查看网站代理HTTPS内容，请看帮助文档。

添加自定义域名

1. 登录阿里云SSL证书控制台。

2. 单击一键式HTTPS，访问域名管理页面。

3. 单击添加站点。

在添加站点页面，输入站点域名。在站点域名页签，阅读使用条款并勾选我已仔细阅读并同意该服务条款，然后输入企业自己的域名。

可以使用阿里云购买的域名，也可以是在其它网站购买的域名。

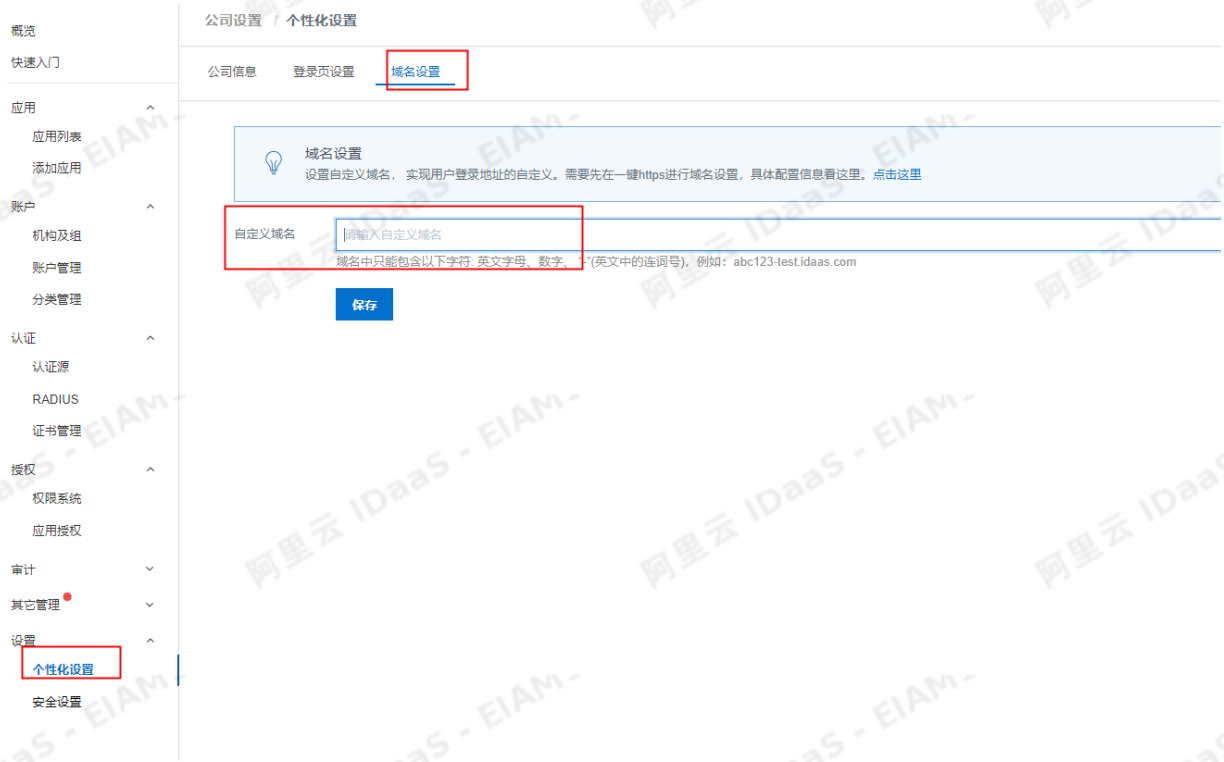
4. 单击右下角的下一步，在站点IP页，选择类型为域名，输入IDaaS的用户访问地址。

5. 单击下一步，配置证书并完成服务接入。

6. 修改DNS配置

在阿里云购买的域名，只需以上一键HTTPS页面配置，其它操作默认完成。如果是其它网站购买的域名，在完成一键HTTPS配置后，还需要在购买域名的账户下，使用DNS配置域名的CNAME解析，使用一键HTTPS生成的CNAME值。

7.切换到IDaaS管理员侧，个性化设置页面，填写自定义域名并进行保存。



8. 直接访问自定义域名测试效果。

修改自定义域名

可以删除原来的一键HTTPS配置，在域名管理下新增站点。

1. 去掉自定义域名的CNAME的解析， 一键HTTPS会自动验证自定义域名是否解除解析;

2. 验证通过后在域名管理页面，会显示删除按钮，可以删除原来的一键HTTPS配置;

3. 根据上文重新添加和配置自定义域名。

更新证书

1. 如果使用的是一键HTTPS购买的证书，在续费一键HTTPS时，会自动续费证书。

2. 续费单独购买的证书。

续费购买的证书必须在证书类型、证书品牌和申请企业信息方面与旧证书保持完全一致，否则会被识别为新购证书，从而导致无法补齐旧证书剩余的有效期时间。

2.1 登录阿里云SSL证书控制台，查看即将过期的证书。

2.2 证书续费

在即将过期的证书列表中，定位到待续费证书，单击到期时间栏的续费。

在证书购买页面选择您需要的证书类型和配置。

说明

a）完成续费后，您将获得一个新的证书订单，您需要提交证书申请后才能签发该证书。

b）到期续费签发的证书将和您上次购买证书时的品牌和型号完全一致。

说明 申请证书时，阿里云SSL证书服务会自动同步您上次提交的申请信息和资料。

单击提交审核，等待CA机构完成审核并签发。

DV证书最快5~10分钟完成签发；OV和EV证书最快2个工作日完成签发。

2.3 在一键HTTPS中更新证书

访问证书配置。

在下拉列表页，选择续费后新生成的证书，进行保存。

FAQ

1. 访问自定义域名报错

请确认CNAME是否生效，如果CNAM生效后，ping 自定义域名 与 ping idaas原来的地址应该是一个IP地址。

2. 是否需要在服务器配置证书

网站配置证书时，正常需要在tomcat 服务器上配置证书的私钥，完成浏览器访问域名的安全性。使用一键HTTPS进行域名解析，只需要添加新的域名，源站信息，以及选择证书就可以，其它操作都由一键HTTPS通过反向代理等操作实现，无需其它配置。

3.3. 管理员修改公司信息及用户自助修改个人信息

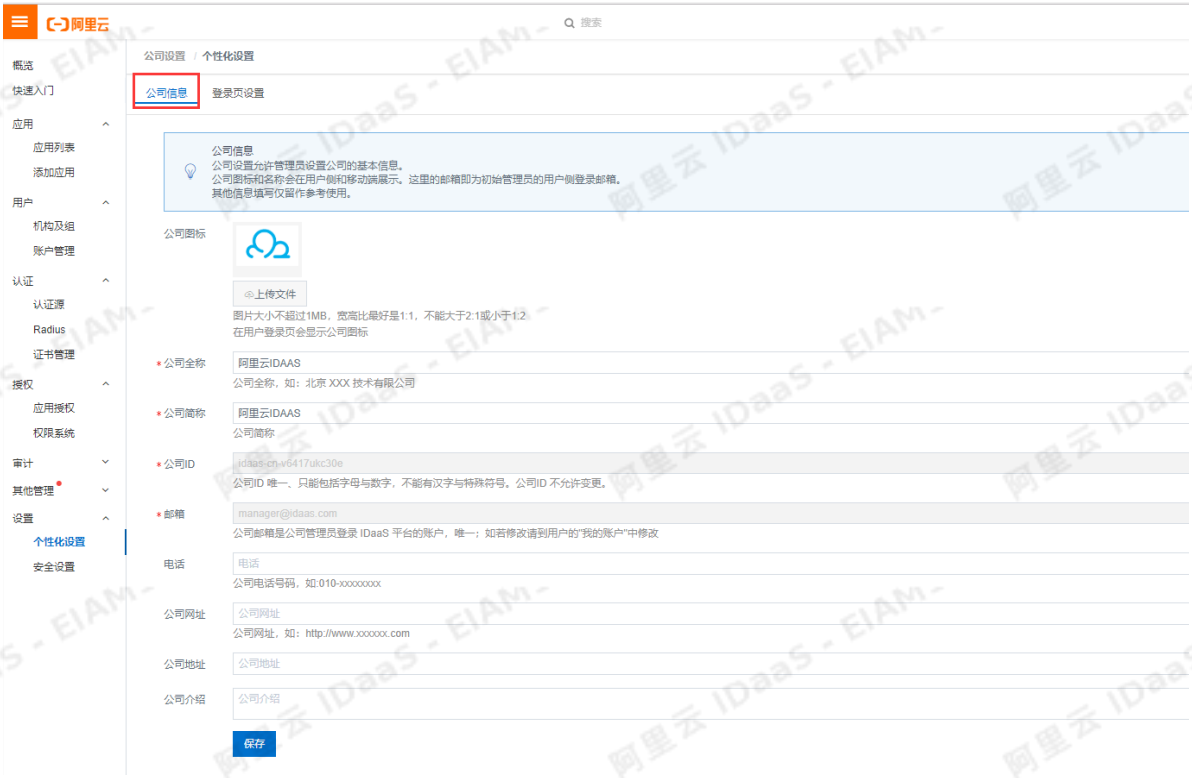
本篇文章为您介绍管理员如何修改公司的信息，以及用户如何修改自己的信息。

管理员修改公司信息

操作步骤

- 管理员进入IDaaS 管理员进入阿里云控制台，在实例列表中选择实例，点击“管理”按钮，即可进入IT管理员界面。

- 管理员修改公司信息：管理员点击右侧导航栏“设置-个性化设置-公司信息”，可以查看公司的信息，也可以修改公司图标和名称。修改之后点击保存，可以在普通用户的登录界面查看到修改后的信息。



- 访问用户登录的地址，如下图：公司图标对应的是登录界面的logo，公司全称对应的是登录界面显示的公司名称。

操作步骤

- 用户自助修改个人信息。

- 获取登录地址 。

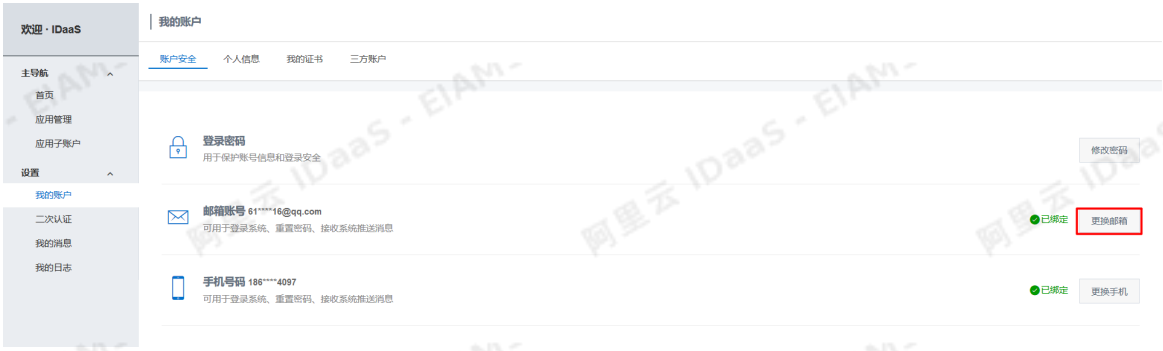
- 登录IDaaS。

- 修改个人信息：用户登录IDaaS之后，可以在“设置-我的账户”中修改用户的个人信息。

- 修改登录密码
点击修改密码按钮 。

在弹出的界面输入原密码和新密码，点击保存即可修改成功。

- 更换个人邮箱：用户可以在我的账户下的账户安全界面，点击“更换邮箱”，来修改用户的个人邮箱。



输入新的邮箱账号，以及登录密码（这里的登录密码指的是登录IDaaS所用的密码，而不是登录邮箱所用的密码），点击下一步。此时IDaaS会以邮件的形式给用户发送一封邮件，验证通过之后，即可成功更换邮箱账号。

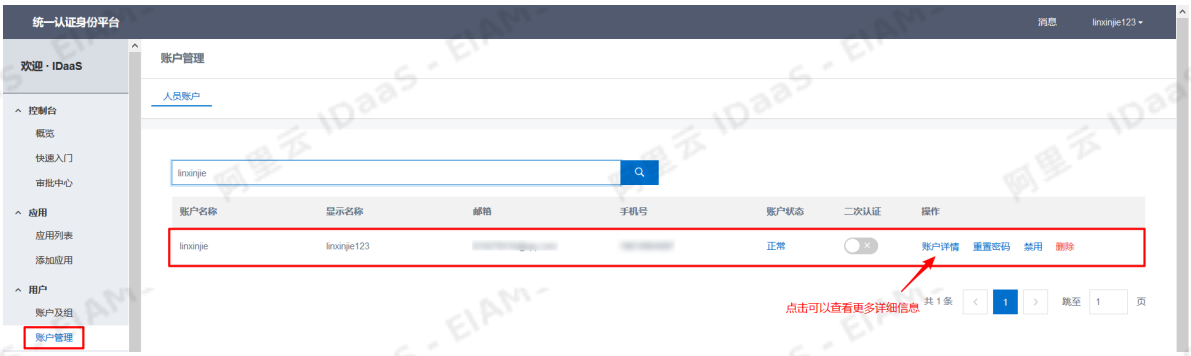
- 更换手机号码：用户可以在我的账户下的账户安全界面，点击“更换手机”，来修改用户的手机号码。

输入新的手机号码，以及登录IDaaS所用的登录密码，点击下一步。

此时IDaaS会以短信的形式给用户新的手机号发送一条验证码，验证通过之后，即可成功更换手机号码。

- 修改显示名称：用户可以点击我的账户下的“个人信息”，在此页面修改账号的显示名称，输入新的显示名称，点击保存即可修改成功。

- 查看修改结果：用户自助修改个人信息后，除了用户自己可以在“我的账户”界面直观的看到修改结果。管理员也可以在账户管理和账户及组查看到用户修改的结果。



通过以上步骤，即可实现管理员修改公司信息及用户自助修改个人信息的功能。

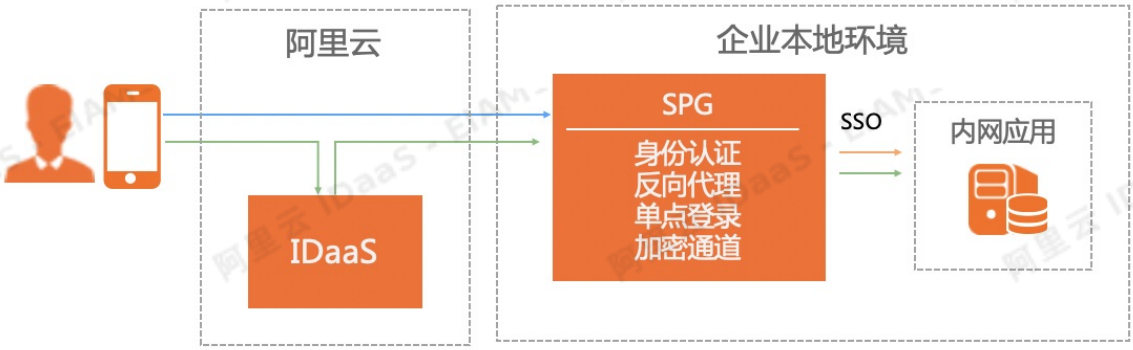
3.4. 基于IDaaS的远程办公解决方案

解决内网应用局限性，快速实现在家办公需求。

解决方案概述

架构说明：使用 IDaaS 提供身份认证以及权限管理，SPG(*)提供基于身份校验以及应用代理等能力，使员工在家也能安全连上内网应用。

> **说明**
>
> (*)SPG为阿里线下产品，支持部署在虚拟机或者物理机上，产品具体信息请联系阿里售前专员或钉钉搜索“idaasgc”。



优点：

- 本方案以身份为核心，采用多因子强认证方式建立可信通道，分组授权，最小化暴露面，解决远程办公过程中身份冒用和业务安全的问题。
- 无论客户业务部署在阿里云、友商云，还是IDC都适用。
- 可结合钉钉使用，实现从钉钉一键访问内网应用。

更多场景方案，请详询阿里售前专员或客服

一、环境准备

1. 购买 IDaaS 产品
2. 将您需要远程办公的人员导入 IDaaS，账户迁移支持LDAP账户同步配置和Excel导入
3. 部署 SPG，需要您提目标虚拟机或者物理机，目标机需要能被用户访问到同时可联通到内网应用，然后联系售前专员进行SPG产品部署。

二、在IDaaS中创建应用

操作步骤

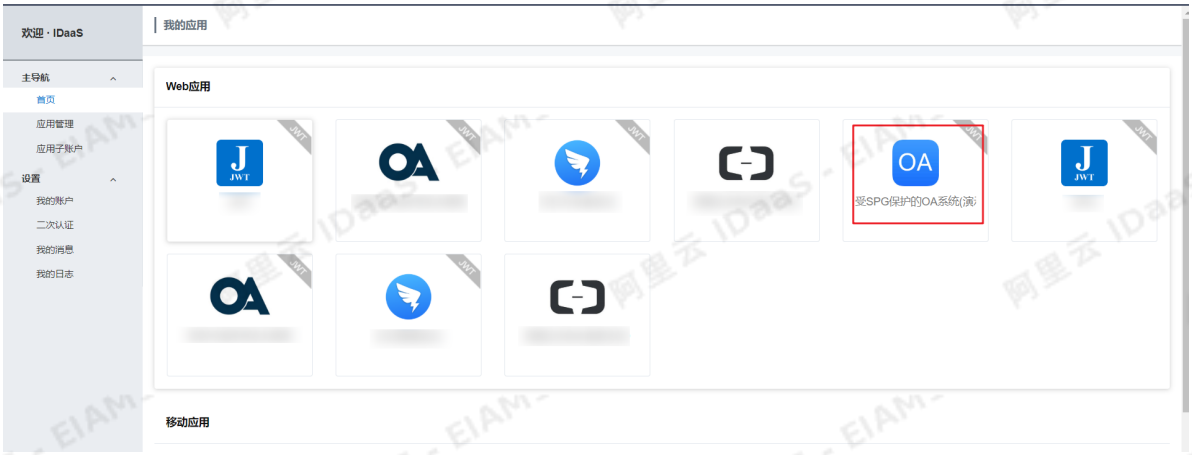
1. 以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考 IT管理员指南-登录。
2. 在左侧导航栏，点击**应用 > 添加应用**。选择JWT应用模板点击**添加应用**。

3. 根据页面提示，在添加应用配置对话框完成添加配置

> **说明**
>
> 应用系统可参考 单点登录配置 > JWT模版使用指南 中的内容进行内网应用的单点登集成，应用如果不进行改造也不影响整体方案，但是跳转到应用后用户还需要手动输入在应用里的账户密码。

> **说明**
>
> redirect_uri 为经过SPG反向代理后的内网应用的登录地址。操作步骤参考本章步骤三、SPG反向代理应用系统

4. 应用添加完成后，使用普通用户账号登录云盾IDaaS控制台，具体操作请参考普通用户指南-登录。
5. 在**主导航 > 首页**，点击应用图标，访问内网应用。



通过以上步骤即可实现用户通过 IDaaS 访问 SPG 反向代理后的内网 OA 系统。

> **说明**
>
> 用户内网OA系统的地址为http://xxx.xxx.com/jwtdemo， SPG反向代理后的地址为https://spg.idsmanager.com:8041/jwtdemo

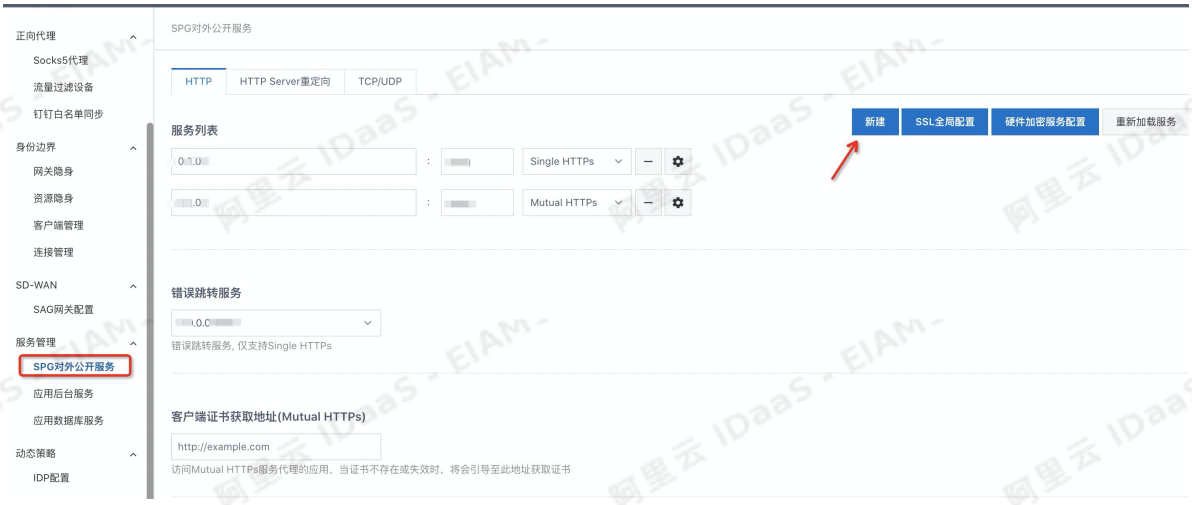
三、SPG反向代理应用系统

操作步骤

1. 管理员登录SPG，点击服务**管理 > 服务列表**

2. 点击**添加服务**，输入后端服务器的信息

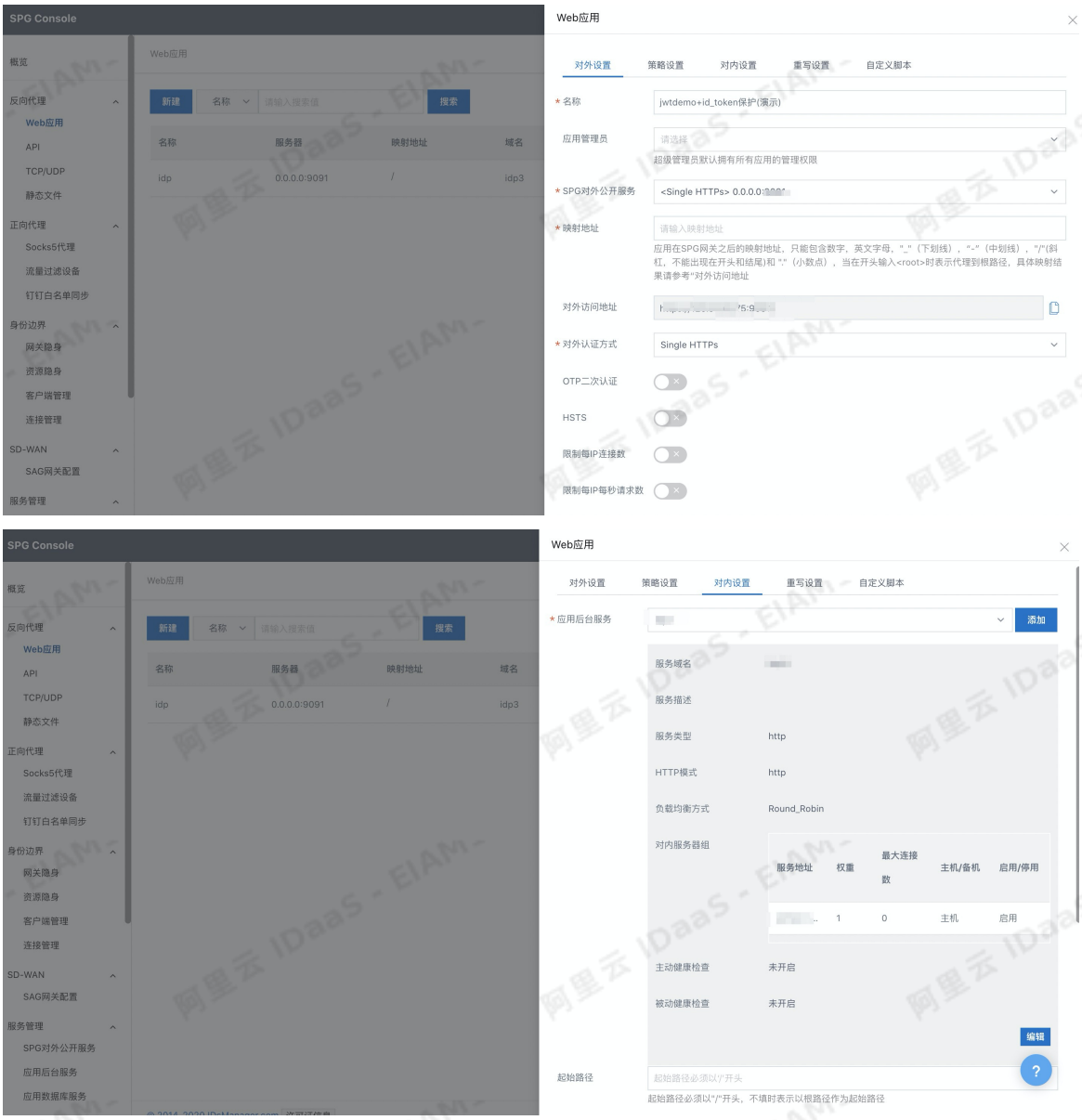
3. 点击**服务管理 > SPG对外公开服务**，添加服务器配置



4. 点击**应用管理 > 应用列表**，添加Web服务器的反向代理

i. 点击**添加应用**，选择**WEB代理**

ii. 配置代理信息,如图



iii. 点击确认提交，点击右上角**重新加载服务**

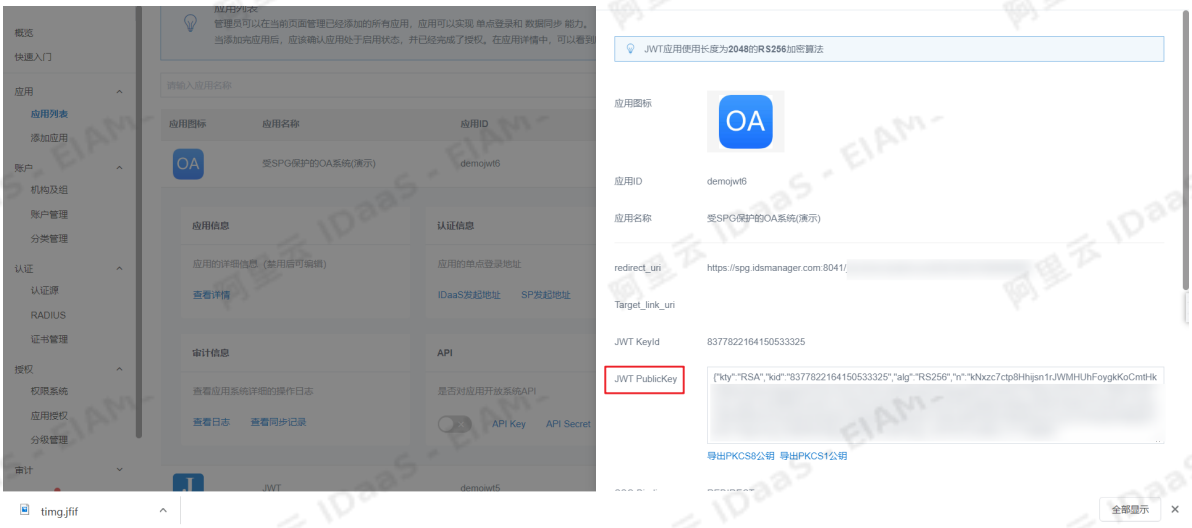
通过以上步骤即可实现将内网应用反向代理到外网

四、ID_Token保护代理后的内网应用

操作步骤

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，点击**应用 > 应用列表**。选择应用点击**详情**，获取应用的**SP发起地址**。

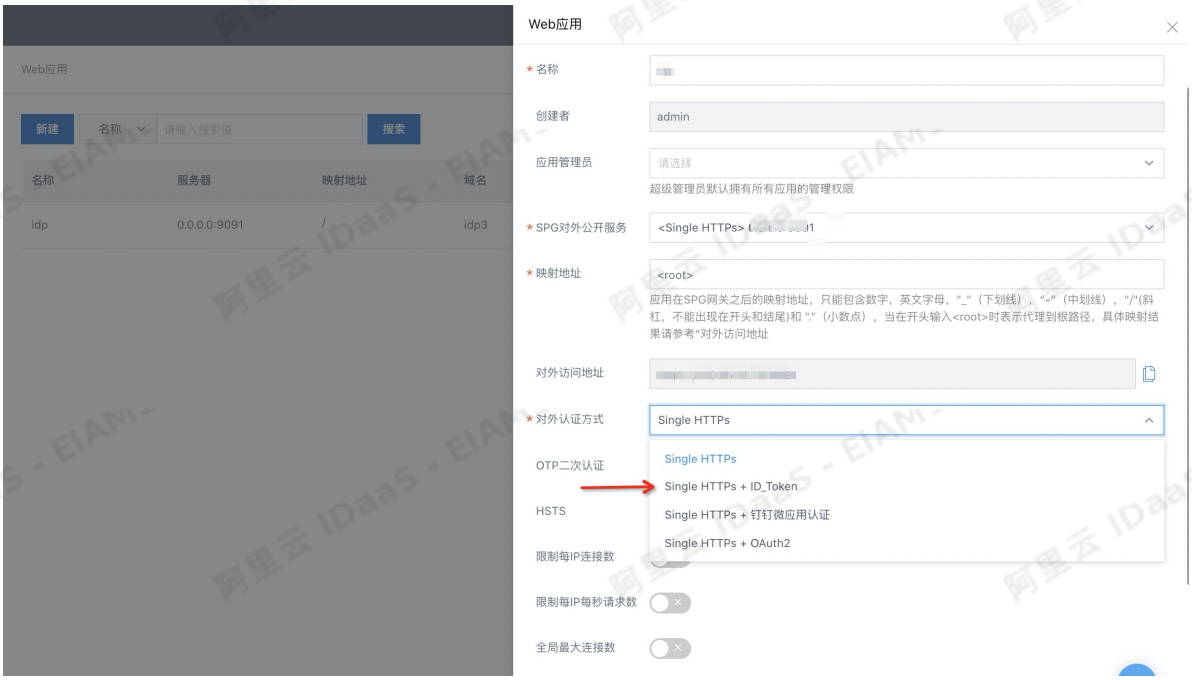
3. 点击**查看详情**，获取应用公钥



4. 管理员登录SPG，选择代理后的应用，点击**编辑**

5. 修改认证方式为Single HTTPS + ID_Token，并配置SP SSO URL和公钥配置

> **说明**
>
> SP SSO URL即为步骤2中获取的SP发起地址；公钥配置为步骤3中的JWT PublicKey。

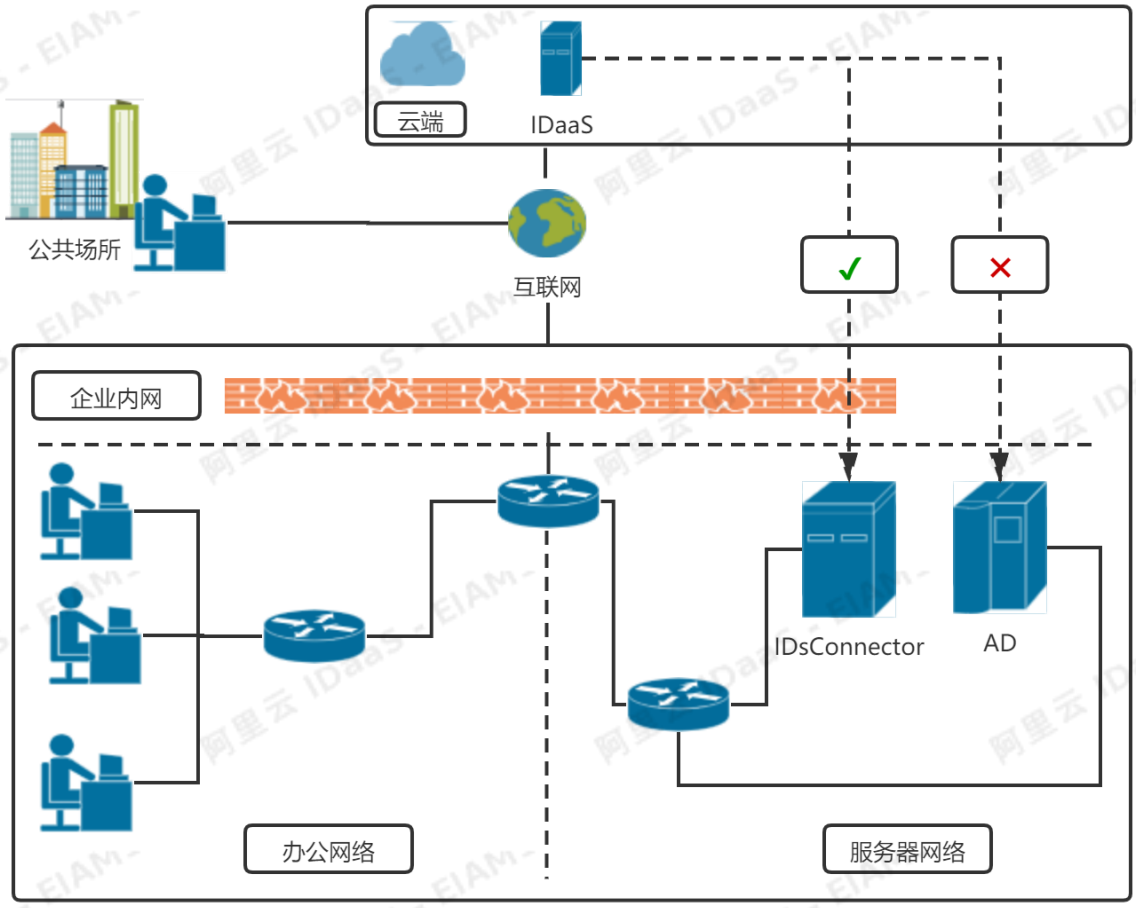


6. 点击确认，再次点击右上角**重新加载服务**

通过以上步骤，实现IDaaS与SPG联动。通过ID_Token保护代理后的内网应用，用户在访问代理后的内网应用时，需携带IDaaS签发的ID_Token才可以成功访问。否则，将会强制重定向到IDaaS进行身份认证。

3.5. 内网AD认证

解决方案概述



背景信息：

当下大部分企业会选择将公司用户的数据存储在AD域中，将AD域作为用户数据中心进行维护。应用系统部署在内网时，应用系统可以访问 AD 进行账户的认证。随着企业信息化的转型，企业开始逐渐使用云产品和云服务。出于安全考虑，企业的AD往往不会开放到公网，这些云产品就很难与企业现有身份目录 AD 集成联动，造成云上身份孤岛问题，增加了企业维护成本和安全风险。用户也需要记录多套账号信息，容易出现账号记录混乱等问题；

解决方案：

通过 IDaaS 整合云产品，实现云产品的单点登录，并使用 Connector 服务组件实现内网 AD 和 IDaaS 的认证联动，达到使用内网 AD 账户认证登录到 IDaaS 以及其他在 IDaaS 中所有集成的应用系统。

收益：

1. 客户内网 AD 无需开放到公网，降低安全风险，同时用户只需使用AD中的账户密码，就可畅通访问所有集成了的应用系统，减少多套账户维护成本；
2. IDaaS提供对接文档，操作简单，对接快速，减少自我研发对接认证方式的成本；

一、环境准备

1、购买公有云 IDaaS 产品；

2、部署 Connector 服务组件，Connector 服务器需要保证可以访问到您内网的 AD，同时需要将 Connector 服务器的对应端口开放到公网；

3、将您 AD 中的账户通过 Connector 导入到 IDaaS，您可以参考 基于 IDaaS 的AD账号同步 中的步骤1-3；

二、支持的对象

AD 中的可用账户；

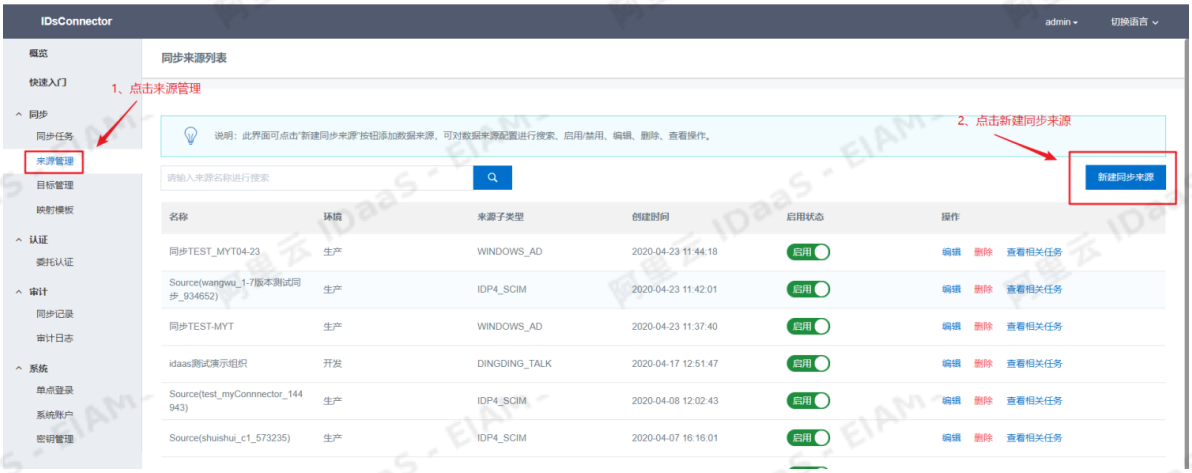
三、配置流程

在 Connector 中创建 AD 来源（如果使用 Connector 拉取 AD 数据到 IDaaS，可以使用同一个来源），并将其添加为委托认证的认证源，然后在 IDaaS 中添加并配置委托认证的认证源即可。

3.1 新建同步来源

1. 部署好 Connector 后，通过 *http://IP* 的方式进行访问，输入用户名和密码进行登录

2. 在左侧导航栏点击**同步 > 来源管理**，点击新建同步来源



3. 在**新建同步来源**页面，配置AD的信息内容，并点击**提交**

配置项	说明
来源主类型	LDAP
来源子类型	WINDOWS_AD
服务器地址	AD服务器的地址
端口号	默认为389
默认域	AD的域名，如test.com
查询基准DN	如果AD域是test.com，此处填写DC=test,DC=com；如果想只查询其中的一个OU下的账户（例如002组织），那么在前面增加ou=002。
管理员DN	参考格式CN=administrator,CN=Users,DC=test,DC=com，其中administrator是管理员账户名，Users值不需更改，test 和 com 是AD域信息。
管理员密码	填写上述填写的管理员账户的密码，即 administrator 账户的密码。

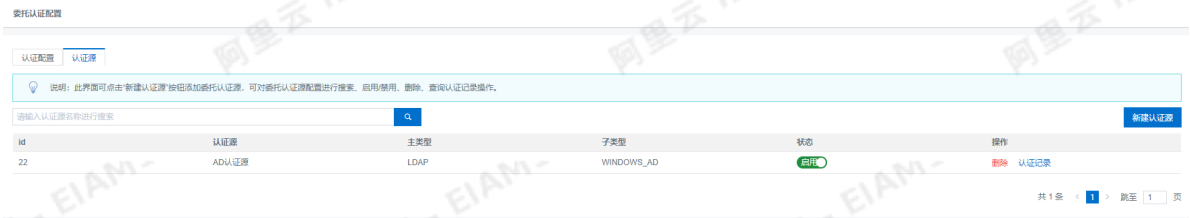
4. 点击**测试连接**，确保连接的参数配置正确。然后点击保存

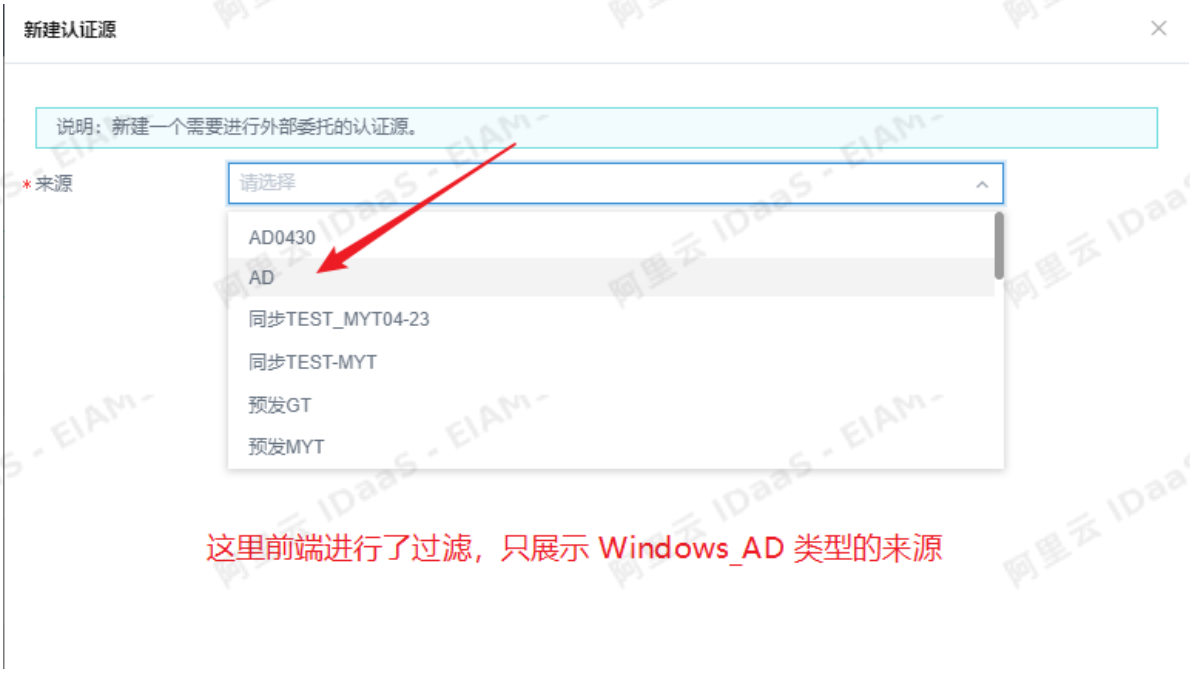
3.2 配置 Connector 委托认证

1. 在左侧导航栏中，点击**认证 > 委托认证**。在委托认证配置页面，点击开启委托认证功能

2. 获取数据加密公钥，在IDaaS 中创建委托认证源时会用到该参数

3. 在 **认证源** 页签，点击新建认证源，添加之前创建的AD来源

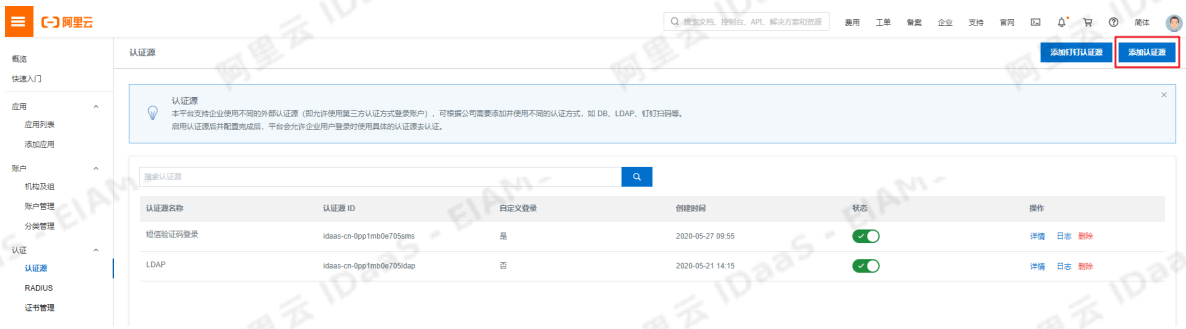




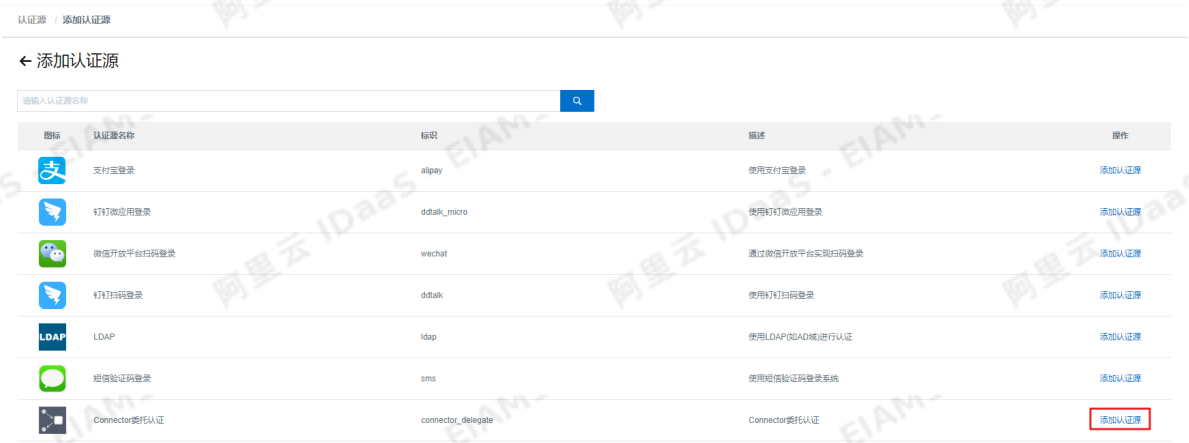
4. 添加完成后，会生成一个id，IDaaS 创建委托认证认证源时会用到

3.3 添加委托认证认证源

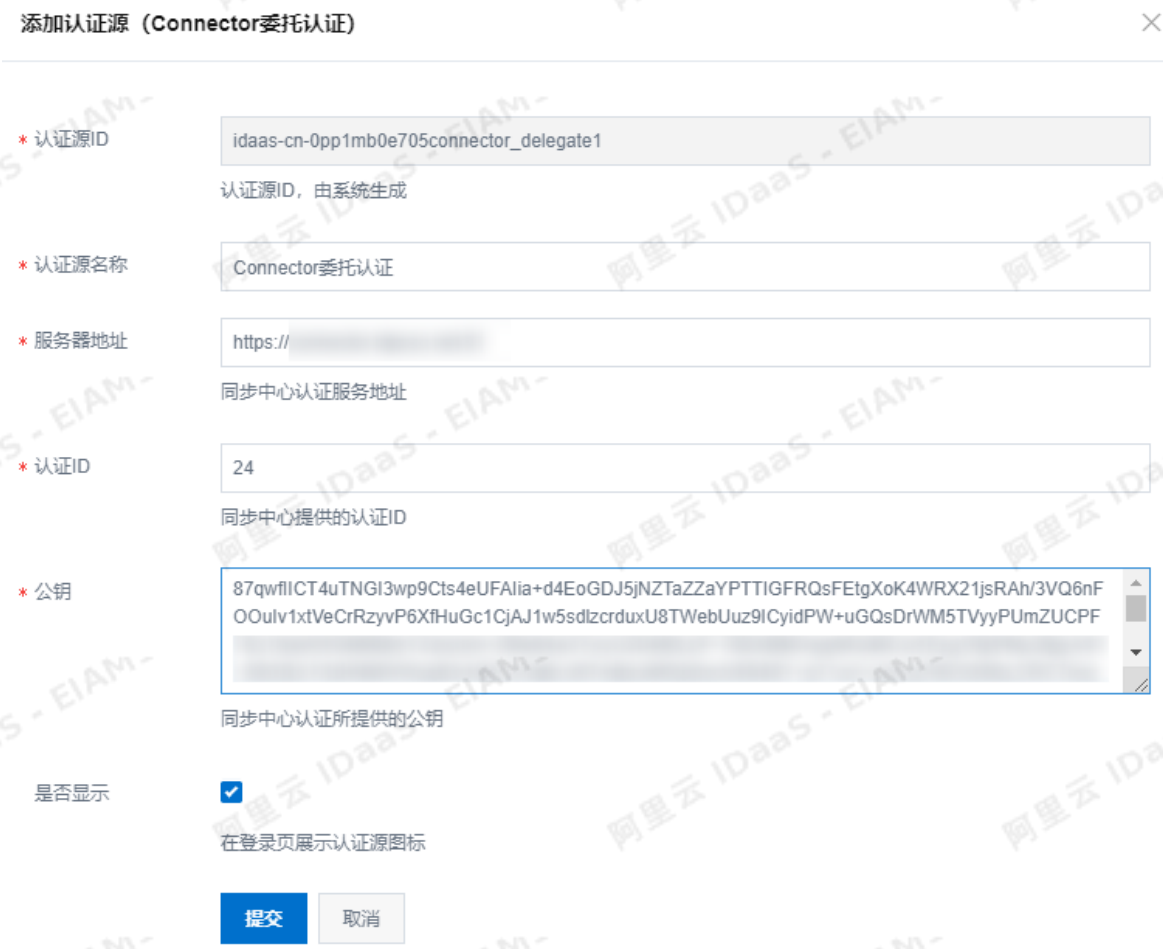
1. 登录 IDaaS，在左侧导航栏中点击 **认证 > 认证源**，点击**添加认证源**



2. 选择 Connector 委托认证，点击**添加认证源**


认证源 / 添加认证源
← 添加认证源
请输入认证源名称
图标
认证源名称
标识
描述
操作
支付宝登录
alipay
使用支付宝登录
添加认证源
钉钉微应用登录
ddtalk_micro
使用钉钉微应用登录
添加认证源
微信开放平台扫码登录
wechat
通过微信开放平台实现扫码登录
添加认证源
钉钉扫码登录
ddtalk
使用钉钉扫码登录
添加认证源
LDAP
ldap
使用LDAP(如AD域)进行认证
添加认证源
短信验证码登录
sms
使用短信验证码登录系统
添加认证源
Connector委托认证
connector_delegate
Connector委托认证
添加认证源

3. 配置认证源

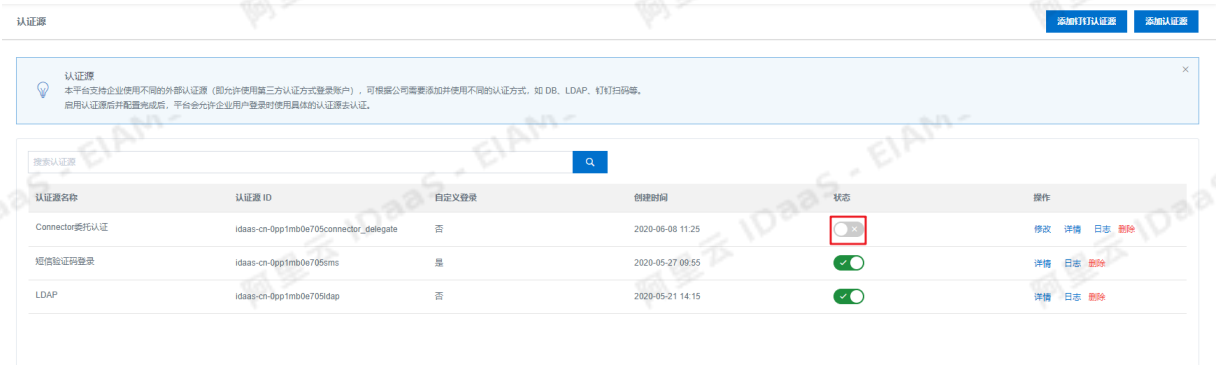


服务器地址：Connector访问地址

认证ID：Connector 认证源id， 3.2 步骤4中获取

公钥：Connector 委托认证数据加密公钥， 3.2 步骤2中获取

4. 创建成功后，启用它



完成上述步骤，用户在 IDaaS 登录页会看到对应的认证源图标

点击图标会进入 AD 认证源的登录页面，直接使用 AD 账户进行认证即可进入 IDaaS 中，并可单点登录到已集成并授权了的公网应用

3.6. Connector集群部署

3.7. 配置阿里云短信服务

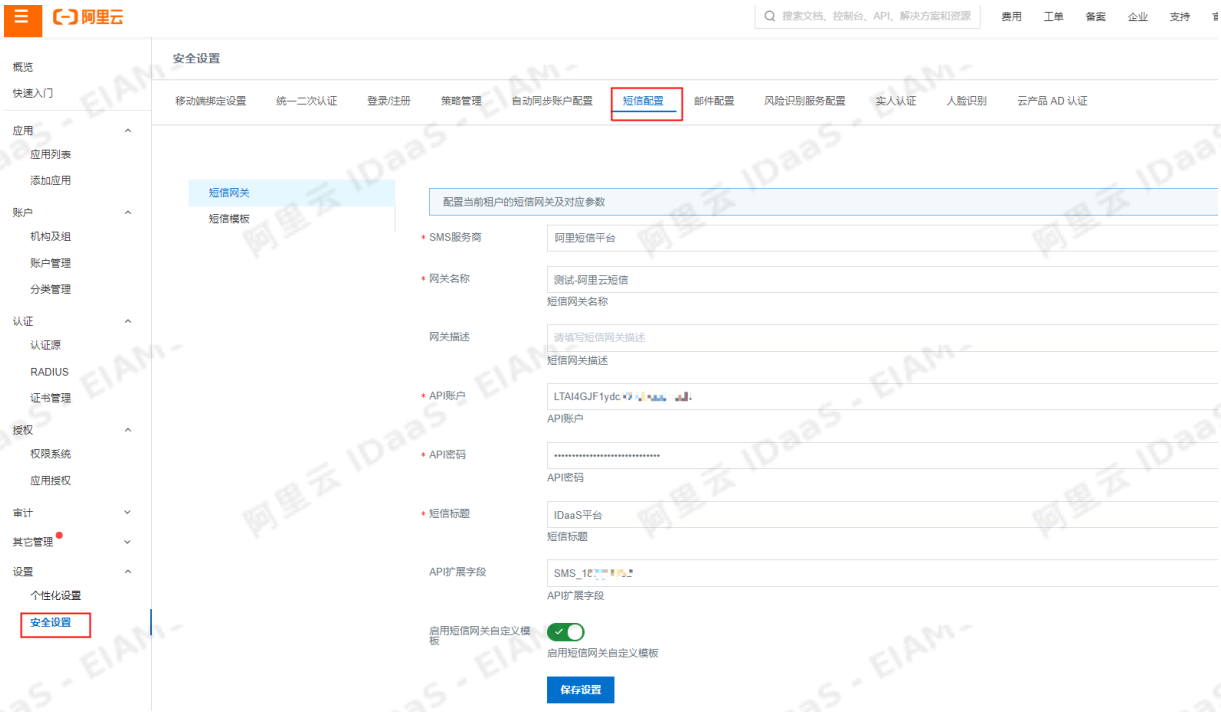
IDaaS默认提供短信服务，可以用于需要手机号验证的场景。但是默认的短信有条数限制，只能用于测试使用，或者偶尔使用短信找回密码等场景，如果经常使用短信功能，需要配置自定义短信网关，使用企业自己购买的短信服务。 本文以阿里云短信服务为例，介绍如何在IDaaS上配置自定义短信服务。

开通短信服务

开通阿里云短信服务，根据短信服务的帮助文档，配置好签名和模板。

IDaaS页面配置

1. 在安全设置中的短信配置页面，配置短信服务相关参数。



API 账户 ： 对应RAM用户的 Access ID

API 密码 : 对应RAM用户的 AccessKey Secret

短信标题：对应短信服务中的签名名称

API扩展字段：选择任意短信模板code，用于下面发送测试短信

> **说明**
>
> RAM用户需要在访问控制授权短信服务，使RAM用户有权限访问短信服务相关内容。

2. 获取RAM账户对应的 Access ID 和 AccessKey Secret

3. 发送测试短信，验证配置的短信服务可用。

4. 配置短信模板，不同场景发送短信的内容也不一样，需要配置对应的短信模板。扩展ID对应短信服务中的模板code。

5. IDaaS 中通过手机号找回密码、短信二次认证等场景都会用到短信服务，测试短信服务是否可用，可以在登录页“忘记密码“中用手机号找回，尝试是否能正常使用短信找回密码。

3.8. 聚石塔相关 API 列表

IDaaS提供一些数据同步的接口API（所有的API都是遵循SCIM协议），SP通过调用这些API，可以将数据同步到IDaaS。SP在调用IDaaS接口时，必须传递access_token。以下，我们将常用的API按照组织机构，账户，组进行分类。

前提条件

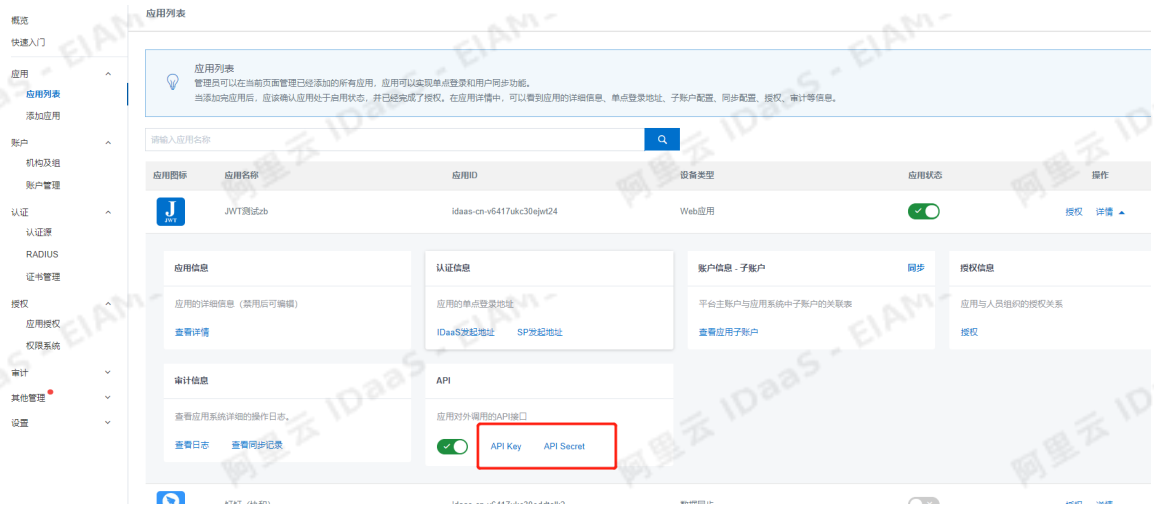
1. **获取IDaaS-Base-URL**

   文档中的“IDaaS-Base-URL”需要替换为当前访问地址的主域，文中接口地址前也都需要替换主域地址。主域为IDaaS控制台中的用户访问的Portal的sso地址。

2. **获取client-id和client-secret**

获取access_token时需要使用client-id和client-secret，我们可以在管理员控制台获取到。

在管理员控制台添加一个应用，在应用的详情中可以启动API,API的两个值对应client-id和client-secret。



接口列表

- 获取access_token

以下是关于组织机构操作的API，包括：

- 推送组织机构
- 修改或移动组织机构
- 删除组织机构
- 查询组织机构
- 获取组织机构列表
- 获取根节点组织机构信息
- 获取组织机构的直属子级

以下是关于账户操作的API，包括：

- 推送账户
- 修改或移动账户
- 删除账户
- 获取账户信息
- 查询账户列表

以下是关于组操作的API，包括：

- 推送账户组
- 更新账户组
- 删除账户组

其他：

- 获取应用已经授权的组织机构及账户列表

具体接口

获取access_token

调用以下API接口时，需要先获取access_token，调用接口时传入access_token有两种方式：

- URL值后：URL?access_token={access_token}
- Header里面：Authorization bearer {access_token}（注意 bearer与access_token之间的空格）

access_token获取方式：向下面的URL进行POST请求，请求将返回JSON包含access_token

```
{IDaaS-Base-URL}/oauth/token?client_id={client-id}&client_secret={client-secret}&scope=read&grant_type=client_credentials
```

> 说明
>
> client_id和client_secret即为创建应用中的API Key和API Secret

推送组织机构

在SP中添加一个组织机构，调用此接口，将新添加的组织机构的信息同步到IDaaS。

> 说明
>
> 同步时，请按照层级关系进行同步，先同步父级再同步子级

Request URI: /api/bff/v1.2/developer/scim/organization/create `POSTREST`

Content-Type: application/json

Request Body:

```
{
    "organizationName": "成都研发部",
    "externalId": "123456",
    "parentExternalId": "test3",
    "type": "DEPARTMENT",
    "sortNumber": "3",
    "enabled":true,
    "description": "负责产品研发",
    "extendFields":{
         "test1":"123"
    }
}
```

请求参数说明：

参数名	参数值	类型	备注
organizationName	{organizationName}	String	组织机构名称。必填

externalId	{externalId}	String	组织机构的唯一ID,该ID是SP同步过来的，所以在IDaaS中称为外部ID。如果不填IDP将随机生成一个外部ID。选填
parentExternalId	{parentExternalId}	String	所属的父级组织机构的唯一ID, 该ID是SP同步过来的, 所以在IDaaS中称为父级外部ID，通过在系统“机构及组”中在组织机构属性中查看参数“外部ID”即可。必填
type	{type}	String	自建组织单位： SELF_OU 自建部门： DEPARTMENT 外部同步组织机构：EXTERNAL_OU 默认为DEPARTMENT.选填
rootNode	{rootNode}	boolean	如果填true,将更新IDP中原本的根节点。选填
enabled	{enabled}	boolean	机构的状态。true：启用，false：禁用，默认为true。选填
sortNumber	{sortNumber}	int	用于展示排序。选填
description	{description}	String	用于说明当前OU，不超过500个字符。选填
extendFields	{extendFields}	Map<String,String>	自定义扩展的字段。在IDP数据字典中定义，如果自定义扩展的字段是必填选项，则该属性必填

Response Body:

```
{
"success": true,
"code": "200",
"message": null,
"requestId": "974CA7CA-1C98-4557-AC90-9425B2ED4719",
"data": {
    "externalId": "123456",
        "id": "123456"
        }
}
```

返回参数说明：

succes代表请求是否成功，code为错误码 ，message为错误信息为接口。

success为true时，代表请求成功，此时code为200，data返回数据。请求失败时，success为false，code为一串语义化的错误码，如：InvalidParameter.ParentOUUuid.NotExist

参数名	说明
externalId	组织机构的唯一ID,该ID是SP同步过来的，所以在IDaaS中称为外部ID。如果不填IDP将随机生成一个外部ID。
id	IDaaS平台机构的Uuid

错误码说明：

HttpCode（请求状态码）	code（错误码）	message（错误信息）	备注
200	200	null	请求成功
400	InvalidParameter	例如：父级机构123456不存在	请求参数错误
400	InvalidParameter.ExternalId.Exist	例如：外部ID重复，externalId：123456	外部ID重复
400	InvalidParameter.Name.Exist	例如：OU名称重复，OrganizationName：研发部	组织机构的名称已存在
403	Forbidden	没有权限操作该父OU	没有权限操作

修改或移动组织机构

在SP中修改一个组织机构，调用此接口，将修改的组织机构的信息同步到IDaaS。

Request URI: /api/bff/v1.2/developer/scim/organization/update `PUTREST`

Content-Type: application/json

Request Body:

```
{
    "description": "",
    "organizationName": "成都研发部",
    "externalId": "123456",
    "parentExternalId": "test3",
    "enabled":false,
    "type": null,
    "sortNumber": "5",
    "extendFields":{
       "test1":"1235123"
    }
}
```

请求参数说明：

参数名	参数值	类型	备注
externalId	{externalId}	String	组织机构的唯一ID,该ID是SP同步过来的,在IDaaS中称为外部ID。必填
organizationName	{organizationName}	String	组织机构名称。选填
parentExternalId	{parentExternalId}	String	所属的父级组织机构的唯一ID, 该ID是SP同步过来的, 所以在IDaaS中称为父级外部ID，通过在系统"机构及组"中在组织机构属性中查看参数“外部ID”即可。选填
type	{type}	String	自建组织单位： SELF_OU 自建部门： DEPARTMENT 外部同步组织机构：EXTERNAL_OU 默认为DEPARTMENT.选填

enabled	{enabled}	boolean	机构的状态。true：启用，false：禁用。选填，填写则代表更新该项信息。
sortNumber	{sortNumber}	int	用于展示排序。选填，填写则代表更新该项信息。
description	{description}	String	用于说明当前OU，不超过500个字符。选填，填写则代表更新该项信息。
extendFields	{extendFields}	Map<String,String>	在IDaaS数据字典中定义，如果自定义扩展的字段是必填选项，则该属性必填

Response Body:

```
{
    "success": true,
    "code": "200",
    "message": null,
    "requestId": "C98418A3-63B5-49CA-9C85-A820A65D3247",
        "data": {
            "externalId": "123456",
            "id": "123456"
        }
}
```

返回参数说明:

succes代表请求是否成功，code为错误码 ，message为错误信息为接口。

success为true时，代表请求成功，此时code为200，data返回数据。请求失败时，success为false，code为一串语义化的错误码，如：InvalidParameter.ParentOUUuid.NotExist

返回参数说明:

succes代表请求是否成功，code为错误码 ，message为错误信息为接口。

success为true时，代表请求成功，此时code为200，data返回数据。请求失败时，success为false，code为一串语义化的错误码，如：InvalidParameter.ParentOUUuid.NotExist

参数名	说明
externalId	组织机构的唯一ID,该ID是SP同步过来的，所以在IDaaS中称为外部ID。如果不填IDP将随机生成一个外部ID。

id	IDaaS平台机构的Uuid

错误码说明：

HttpCode（请求状态码）	code（错误码）	message（错误信息）	备注
200	200	null	请求成功
400	InvalidParameter	例如：描述信息不能超过500个字符	请求参数错误
400	EntityNotFound	组织机构不存在	未查找到要更新的OU
400	InvalidParameter.Name.Exist	例如：OU名称重复，OrganizationName：研发部	组织机构的名称已存在
400	OperationDenied	OU不能移动到自己子级下	不被允许的操作
403	Forbidden	没有权限操作该父OU	没有权限操作

删除组织机构

在SP中删除一个组织机构，调用此接口，在IDaaS中也删除这个组织机构

Request URI: /api/bff/v1.2/developer/scim/organization/delete `DELETEREST`

Content-Type: application/json

请求示例：

```
/api/bff/v1.2/developer/scim/organization/delete?externalId=1694618271068407094
```

请求参数说明：

参数名	参数值	备注
externalId	{externalId}	IDaaS系统中组织机构的外部ID。

Response Body:

```
{
    "success": true,
    "code": "200",
    "message": null,
    "requestId": "30A38CA4-D640-4CBA-B85F-A0234D0181F1"
}
```

返回参数说明：

succes代表请求是否成功，code为错误码 ，message为错误信息为接口。

success为true时，代表请求成功，此时code为200，data返回数据。请求失败时，success为false，code为一串语义化的错误码，如：InvalidParameter.ParentOUUuid.NotExist

错误码说明：

HttpCode（请求状态码）	code（错误码）	message（错误信息）	备注
200	200	null	请求成功
400	InvalidParameter	例如：外部id(externalId)不能为空	请求参数错误
400	EntityNotFound	组织机构不存在	未查找到要更新的OU
400	OperationDenied.OUContainsChildren	该OU存在关联关系，不能删除	机构下存在子级机构或账户，不允许删除
403	Forbidden	没有权限操作该OU	没有权限操作

查询组织机构

查询单个组织机构

Request URI: /api/bff/v1.2/developer/scim/organization/detail `GETREST`

请求示例：

/api/bff/v1.2/developer/scim/organization/detail?externalId=1694618271068407094

请求参数说明：

参数名	参数值	备注
externalId	{externalId}	IDaaS系统中组织机构的外部ID。

Response Body:

```
{
    "success": true,
    "code": "200",
    "message": null,
    "requestId": "B5D4A6D1-9C51-4AC3-A413-4A27EE1C1474",
    "data": {
        "organizationName": "ceshi导入0009",
        "externalId": "9999",
        "parentExternalId": "764712910283009725",
        "type": "SELF_OU",
        "rootNode": false,
        "sortNumber": 0,
        "enabled": true,
        "description": null,
        "extendFields": {
            "4": "asd"
        }
    }
}
```

返回参数说明：

succes代表请求是否成功，code为错误码 ， message为错误信息为接口。

success为true时，代表请求成功，此时code为200，data返回数据。请求失败时，success为false，code为一串语义化的错误码，如：InvalidParameter.ParentOUUuid.NotExist

参数名	说明
externalId	组织机构的外部ID
organizationName	组织机构名称
parentExternalId	父组织机构外部ID
type	类型
enabled	组织机构的状态
description	描述
extendFields	扩展字段
sortNumber	机构的排序号

rootNode	标识该机构是否为根节点

错误码说明：

HttpCode（请求状态码）	code（错误码）	message（错误信息）	备注
200	200	null	请求成功
400	InvalidParameter	例如：外部id(externalId)不能为空	请求参数错误
400	EntityNotFound	组织机构不存在	未查找到要更新的OU
403	Forbidden	没有权限操作该父OU	没有权限操作

获取组织机构列表

SP通过调用此接口，可以查看所有的OU或者某OU及其所有子OU的组织机构列表。

Request URI: /api/bff/v1.2/developer/scim/organization/list `GET`

请求示例：

获取该公司的所有组织机构：/api/bff/v1.2/developer/scim/organization/list

获取某个OU下所有组织机构的信息：/api/bff/v1.2/developer/scim/organization/list?id=5986176890912195413

请求参数说明：

参数名	参数值	类型	备注
externalId	{externalId}	String	IDaaS系统中组织机构的外部ID。选填

> **说明**
>
> 如果不传值则返回该公司的所有组织机构。如果ID不为空：则返回对应OU下的组织机构的信息

Response Body:

```
{
            "success": true,
            "code": "200",
            "message": null,
            "requestId": "3CCA4939-170C-46AA-BE11-F3DE924FC0E9",
            "data": {"organizations": [
```

```
                {
                    "organizationName": "成都研发部",
                    "externalId": "2858068028015036528",
                    "parentExternalId": "129733886490329012",
                    "type": "DEPARTMENT",
                    "rootNode": false,
                    "sortNumber": 0,
                    "enabled": true,
                    "description": "",
                    "extendFields": {}
                },
                {
                    "organizationName": "成都分公司",
                    "externalId": "129733886490329012",
                    "parentExternalId": "6721629573848908864",
                    "type": "SELF_OU",
                    "rootNode": false,
                    "sortNumber": 0,
                    "enabled": true,
                    "description": "",
                    "extendFields": {}
                },
                {
                    "organizationName": "测试研发部3-3",
                    "externalId": "test3-3",
                    "parentExternalId": "test3",
                    "type": "DEPARTMENT",
                    "rootNode": false,
                    "sortNumber": 3,
                    "enabled": true,
                    "description": "通过SCIM同步组织机构",
                    "extendFields": {
                        "test1": "1235123"
                    }
                },
                {
                    "organizationName": "研发部3-4",
                    "externalId": "test3-4",
                    "parentExternalId": "test3",
                    "type": "DEPARTMENT",
                    "rootNode": false,
                    "sortNumber": 3,
                    "enabled": true,
                    "description": "研发分部",
                    "extendFields": {
                        "test1": "123"
                    }
                }
                ]
            }
        }
```


返回参数说明：

succes代表请求是否成功，code为错误码 ， message为错误信息为接口。

success为true时，代表请求成功，此时code为200，data返回数据。请求失败时，success为false，code为一串语义化的错误码，如：InvalidParameter.ParentOUUuid.NotExist

参数名	说明
organizations	返回的组织机构信息
├ externalId	组织机构的外部ID
├ organizationName	组织机构名称
├ parentExternalId	父组织机构外部ID
├ type	类型
├ rootNode	标识该机构是否为根节点
├ sortNumber	机构的排序号
├ enabled	组织机构的状态
├ description	描述
└ extendFields	扩展字段

错误码说明：

HttpCode（请求状态码）	code（错误码）	message（错误信息）	备注
200	200	null	请求成功
400	EntityNotFound	例如：组织机构123456不存在	未查找到externalId对应的OU
403	Forbidden	没有权限操作该父OU	没有权限操作

获取根节点组织机构信息

获取当前租户的根节点组织机构信息

Request URI: /api/bff/v1.2/developer/scim/organization/root `GETREST`

请求示例：

```
/api/bff/v1.2/developer/scim/organization/root
```

Response Body:

```
{
        "success": true,
        "code": "200",
        "message": null,
        "requestId": "C757F8D6-E96A-4399-823C-E55AED4D59C3",
        "data": {
            "organizationName": "XXX技术有限公司",
            "externalId": "67216295738489088 64",
            "parentExternalId": null,
            "type": "SELF_OU",
            "rootNode": true,
            "sortNumber": 0,
            "enabled": true,
            "description": "",
            "extendFields": {}
        }
}
```

返回参数说明：

succes代表请求是否成功，code为错误码 ，message为错误信息为接口。

success为true时，代表请求成功，此时code为200，data返回数据。请求失败时，success为false，code为一串语义化的错误码，如：InvalidParameter.ParentOUUuid.NotExist

参数名	说明
externalId	组织机构的外部ID
organizationName	组织机构名称
parentExternalId	父组织机构外部ID
type	类型
enabled	组织机构的状态
description	描述

extendFields	扩展字段
sortNumber	机构的排序号
rootNode	标识该机构是否为根节点

错误码说明：

HttpCode（请求状态码）	code（错误码）	message（错误信息）	备注
200	200	null	请求成功
400	InvalidParameter	cannot get current enterpriseUuid（获取不到当前租户信息）	请求参数错误
400	EntityNotFound	cannot get rootOU	未查找根OU
403	Forbidden	没有权限操作该父OU	没有权限操作

获取组织机构的直属子级

SP通过调用此接口，可以查看指定OU的所有直属子OU。

Request URI: /api/bff/v1.2/developer/scim/organization/children `GET`

请求参数说明：

参数名	参数值	类型	备注
externalId	{externalId}	String	IDaaS系统中组织机构的外部ID。必填

> **说明**
>
> 如果不传值则返回该公司的所有组织机构；如果ID不为空：则返回对应OU下的组织机构的信息

请求示例：

/api/bff/v1.2/developer/scim/organization/children?externalId=1

Response Body:

```
{
"success": true,
"code": "200",
"message": null,
"requestId": "26AD790D-FB7D-4ED9-B07E-82448C929F88",
"data": {
    "organizations": [
        {
            "organizationName": "销售部",
            "externalId": "130015784",
            "parentExternalId": "1",
            "type": "DEPARTMENT",
            "rootNode": false,
            "sortNumber": 130015784,
            "enabled": true,
            "description": null,
            "extendFields": {
            }
        },
        {
            "organizationName": "研发部",
            "externalId": "129387071",
            "parentExternalId": "1",
            "type": "DEPARTMENT",
            "rootNode": false,
            "sortNumber": 129387071,
            "enabled": true,
            "description": null,
            "extendFields": {
            }
        },
        {
            "organizationName": "测试部",
            "externalId": "129083981",
            "parentExternalId": "1",
            "type": "DEPARTMENT",
            "rootNode": false,
            "sortNumber": 129083981,
            "enabled": true,
            "description": null,
            "extendFields": {
            }
        }
    ]
}
}
```


返回参数说明：

succes代表请求是否成功，code为错误码 ，message为错误信息为接口。

success为true时，代表请求成功，此时code为200，data返回数据。请求失败时，success为false，code为一串语义化的错误码，如：InvalidParameter.ParentOUUuid.NotExist

参数名	说明
organizations	返回的组织机构信息
├ externalId	组织机构的外部ID
├ organizationName	组织机构名称
├ parentExternalId	父组织机构外部ID
├ type	类型
├ rootNode	标识该机构是否为根节点
├ sortNumber	机构的排序号
├ enabled	组织机构的状态
└ description	描述
└ extendFields	扩展字段

错误码说明：

HttpCode（请求状态码）	code（错误码）	message（错误信息）	备注
200	200	null	请求成功
400	InvalidParameter	例如：外部id(externalId)不能为空	请求参数错误
400	EntityNotFound	组织机构不存在	未查找到externalId对应的OU
403	Forbidden	没有权限操作该父OU	没有权限操作

推送账户

SP中添加一个账户，调用此接口，将新添加的账户的信息同步到IDaaS中。

Request URI: /api/bff/v1.2/developer/scim/account/create POSTREST

Content-Type: application/json

Request Body:

```
{
    "externalId": "123456",
    "userName": "developer2",
    "displayName": "开发人员3",
    "password": "Jdev@12345",
    "email": "test2@****.com",
    "phoneNumber": "",
    "description": "",
    "belongs": [
        "test1","test2"
        ],
    "extendFields": {
        "test":"123456",
        "test1":"woman"
    }
}
```

请求参数说明：

参数名	参数值	类型	备注	是否必填
userName	{userName}	String	云IDaaS平台主账户	必填
password	{password}	String	云IDaaS平台主账户密码	非必填，若为空，则将使用系统随机密码。
displayName	{displayName}	String	用户的显示名称	必填
externalId	{externalId}	String	账户的唯一ID	选填。如果不填，将随机生成一个，并在结果中返回
email	{email}	String	邮箱	选填。
phoneNumber	{phoneNumber}	String	手机号，只能一个且唯一	选填。

phoneRegion	{phoneRegion}	String	手机区号，不填则默认为86	选填
belongs	{belongs}	Array	所属ou的外部ID的集合	必填，具体看请求参数示例
locked	{locked}	boolean	账户是否锁定，true：锁定账户，false：不锁定账户。锁定账户后将不能登录 IDaaS	选填。填写则代表更新该项信息。
enabled	{enabled}	boolean	用户启用状态，true启用,false禁用。禁用账户将不能登录 IDaaS	非必填，不填默认启用账户
description	{description}	String	描述信息	选填
expireTime	{expireTime}	String	过期时间。格式：yyyy-MM-dd,例如：2020-01-12	选填
extendFields	{extendFields}	Map<String,String>	自定义扩展的字段，在IDP数据字典中定义。	选填，填写则代表更新该项信息。更新时，如果自定义扩展的字段是必填选项，则该属性必填

Response Body:

失败示例：

```
{
        "success": false,
        "code": "InvalidParameter",
        "message": "密码不符合密码策略 / 邮箱（email）： test@****.com 已经存在 / 所属组织机构(belongs):123456不存在",
        "requestId": "7BA02087-4789-4FA6-A414-45BAC671945E",
        "data": null
}
```

成功示例：

```
{
        "success": true,
        "code": "200",
        "message": null,
        "requestId": "BF66FA08-E57B-4387-90C0-A72E41307239",
        "data": {
            "externalId": "123456"
        "id":"e717a0cd5b1059bda8a6dd35cfce8e48DxlBg123456"
        }
}
```

返回参数说明：

succes代表请求是否成功，code为错误码 ，message为错误信息为接口。

success为true时，代表请求成功，此时code为200，data返回数据。请求失败时，success为false，code为一串语义化的错误码，如：InvalidParameter.ParentOUUuid.NotExist

参数名	说明
externalId	账户的唯一ID,该ID是SP同步过来的，所以在IDaaS中称为外部ID。如果不填IDP将随机生成一个外部ID。
id	IDaaS平台账户的Uuid

错误码说明：

HttpCode（请求状态码）	code（错误码）	message（错误信息）	备注
200	200	null	请求成功
400	InvalidParameter	例如：账户名称不能为空	请求参数错误
400	InvalidParameter.ExternalId.Exist	externalId外部ID重复	外部ID重复
400	InvalidParameter.Name.Exist	账户名（username）已经存在	账户名称已经存在
400	InvalidParameter.DisplayName.Exist	显示名已经存在	显示名已经存在
400	InvalidParameter.Email.Exist	邮箱（email）已被其他账户绑定	邮箱（email）已被其他账户绑定

400	InvalidParameter.PhoneNumber.Exist	手机号（phoneNumber）已被其他账户绑定	手机号（phoneNumber）已被其他账户绑定
400	EntityNotFound	例如：所属组织机构（belongs）：123456不存在	未查找到externalId对应的OU

修改或移动账户

SP中修改一个账户，调用此接口，将修改的账户的信息同步到IDaaS中。

Request URI: /api/bff/v1.2/developer/scim/account/update `PUTREST`

Content-Type:application/json

Request Body:

```
{
    "externalId": "test-2",
    "userName": "test-2",
    "displayName": "test-3",
     "password": "Jzyt@123456",
     "email": "test2@****.com",
    "phoneNumber": "188****0900",
     "expireTime": "2117-01-01",
     "description": "123ttt",
     "locked":false,
    "belongs": [
        "test2"
        ],
    "extendFields": {
        "test":"t",
        "test1":"woman123"
    }
}
```

请求参数说明：

参数名	参数值	类型	备注	是否必填
userName	{userName}	String	云IDaaS平台主账户	选填，userName和externalId选填一个。

password	{password}	String	云IDaaS平台主账户密码	选填。填写则代表更新该项信息。
displayName	{displayName}	String	用户的显示名称	选填。填写则代表更新该项信息。
externalId	{externalId}	String	账户的唯一ID	选填，userName和externalId选填一个。
email	{email}	String	邮箱	选填。填写则代表更新该项信息。
phoneNumber	{phoneNumber}	String	手机号，只能一个且唯一	选填。填写则代表更新该项信息。
belongs	{belongs}	String	所属OU外部ID的集合，必须存在	选填。填写则代表更新该项信息。具体看请求参数示例
locked	{locked}	boolean	账户是否锁定，true：锁定账户，false：不锁定账户。锁定账户后将不能登录 IDaaS	选填。填写则代表更新该项信息。
enabled	{enabled}	boolean	用户启用状态，true启用,false禁用。禁用账户将不能登录 IDaaS	选填，不填默认启用账户
description	{description}	String	描述信息	选填。填写则代表更新该项信息。
expireTime	{expireTime}	String	过期时间。格式：yyyy-MM-dd,例如：2020-01-12	选填。填写则代表更新该项信息。

extendFields	{extendFields}	Map<String,String>	自定义扩展的字段，在IDP数据字典中定义。	选填，填写则代表更新该项信息。更新时，如果自定义扩展的字段是必填选项，则该属性必填

Response Body:

失败示例:

```
{
        "success": false,
        "code": "InvalidParameter",
        "message": "密码不符合密码策略 / 邮箱（email）： test@****.com 已经存在 / 所属组织机构(belongs):123456不存在",
        "requestId": "7BA02087-4789-4FA6-A414-45BAC671945E",
        "data": null
}
```

成功示例:

```
{
        "success": true,
        "code": "200",
        "message": null,
        "requestId": "BF66FA08-E57B-4387-90C0-A72E41307239",
        "data": {
        "externalId": "123456"
        "id":"e717a0cd5b1059bda8a6dd35cfce8e48DxlBg123456"
    }
}
```

返回参数说明:

succes代表请求是否成功，code为错误码 ，message为错误信息为接口。

success为true时，代表请求成功，此时code为200，data返回数据。请求失败时，success为false，code为一串语义化的错误码，如：InvalidParameter.ParentOUUuid.NotExist

返回参数说明:

succes代表请求是否成功，code为错误码 ，message为错误信息为接口。

success为true时，代表请求成功，此时code为200，data返回数据。请求失败时，success为false，code为一串语义化的错误码，如：InvalidParameter.ParentOUUuid.NotExist

参数名	说明

externalId	组织机构的唯一ID,该ID是SP同步过来的，所以在IDaaS中称为外部ID。如果不填IDP将随机生成一个外部ID。
id	IDaaS平台机构的Uuid

错误码说明：

HttpCode（请求状态码）	code（错误码）	message（错误信息）	备注
200	200	null	请求成功
400	InvalidParameter	例如：账户名称不能为空	请求参数错误
400	InvalidParameter.ExternalId.Exist	externalId外部ID重复	外部ID重复
400	InvalidParameter.Name.Exist	账户名（username）已经存在	账户名称已经存在
400	InvalidParameter.DisplayName.Exist	显示名已经存在	显示名已经存在
400	InvalidParameter.Email.Exist	邮箱（email）已被其他账户绑定	邮箱（email）已被其他账户绑定
400	InvalidParameter.PhoneNumber.Exist	手机号（phoneNumber）已被其他账户绑定	手机号（phoneNumber）已被其他账户绑定
400	InvalidParameter.ExternalId.NotExist	通过externalId查询不到账户	未查找到externalId对应的账户
400	EntityNotFound	例如：所属组织机构（belongs）：123456不存在	未查找到externalId对应的OU

删除账户

在SP中删除一个账户，通过调用此接口，删除IDaaS中该账户信息。

Request URI: /api/bff/v1.2/developer/scim/account/delete `DELETEREST`

请求参数说明：

参数名	参数值	备注
externalId	{externalId}	IDaaS系统中账户的外部ID。

请求示例：

```
/api/bff/v1.2/developer/scim/account/delete?externalId=4544581305390943066
```

Response Body：

```
{
    "success": true,
    "code": "200",
    "message": null,
    "requestId": "BF66FA08-E57B-4387-90C0-A72E41307239",
    "data": null
}
```

返回参数说明：

succes代表请求是否成功，code为错误码 ，message为错误信息为接口。

success为true时，代表请求成功，此时code为200，data返回数据。请求失败时，success为false，code为一串语义化的错误码，如：InvalidParameter.ParentOUUuid.NotExist

错误码说明：

HttpCode（请求状态码）	code（错误码）	message（错误信息）	备注
200	200	null	请求成功
400	InvalidParameter	例如：外部id(externalId)不能为空	请求参数错误
400	EntityNotFound	账户不存在	未查找到要删除的账户
403	OperationDenied	例如：管理员 admin 不能删除	删除操作不被允许

获取账户信息

在SP中通过调用此接口，获取IDaaS中账户信息。

Request URI:/api/bff/v1.2/developer/scim/account/detail `GETREST`

Content-Type:application/json

请求参数说明：

参数名	参数值	备注
externalId	{externalId}	IDaaS系统中账户的外部ID。必填

请求示例：

```
/api/bff/v1.2/developer/scim/account/detail?externalId=123456&access_token=bcab-ae1.2123456461626-590-496789-73082615978
```

Response Body：

```
{
    "success": true,
    "code": "200",
    "message": null,
    "requestId": "278D7B88-6C26-4C7F-90A7-F126CF52F3E1",
    "data": {
        "externalId": "123456",
        "username": "test-2",
        "displayName": "test-3",
        "phoneNumber": "188****0900",
        "email": "test2@****.com",
        "enabled": true,
        "locked": false,
        "description": "123ttt",
        "extendFields": {
            "test": "t",
            "test1": "woman123"
        },
        "belongs": [
            "test2"
        ]
    }
}
```

返回参数说明：

succes代表请求是否成功，code为错误码 ，message为错误信息为接口。

success为true时，代表请求成功，此时code为200，data返回数据。请求失败时，success为false，code为一串语义化的错误码，如：InvalidParameter.ParentOUUuid.NotExist

参数名	参数值	备注
externalId	{externalId}	IDaaS系统中账户的外部ID

username	{username}	用户名
displayName	{displayName}	显示名
phoneNumber	{phoneNumber}	手机号
email	{email}	邮箱
locked	{locked}	账号是否锁定,true为锁定,false为未锁定
enabled	{enabled}	账号是否可用,true为启用,false禁用
belongs	{belongs}	账户所属组织机构列表
extendFields	{extendFields}	扩展字段，用于账户保存的自定义字段

错误码说明：

HttpCode（请求状态码）	code（错误码）	message（错误信息）	备注
200	200	null	请求成功
400	InvalidParameter	例如：外部id(externalId)不能为空	请求参数错误
400	InvalidParameter.ExternalId.NotExist	externalId不存在	未查找到该账户

查询账户列表

在SP中通过调用此接口，获取IDaaS中账户列表信息。

Request URI: /api/bff/v1.2/developer/scim/account/list `GETREST`

Content-Type:application/json

请求参数说明：

参数名	参数值	备注

ouExternalId	{ouExternalId}	指定具体组织机构的ID，可选
createStartDate	{createStartDate}	指定账户创建开始日期，格式：yyyy-MM-dd，如：2018-01-01，可选
createEndDate	{createEndDate}	指定账户创建结束日期，格式：yyyy-MM-dd，如：2018-01-30，可选
start	{start}	可选，分页开始位置，默认0
limit	{limit}	可选，分页数据条件限制，默认10，最大100

请求示例：

```
/api/bff/v1.2/developer/scim/account/list?ouExternalId=test&access_token=bcab-ae1.22461626-590-496789-73082615978
```

Response Body：

```
{
    "success": true,
    "code": "200",
    "message": null,
    "requestId": "5709C39A-D53A-4D74-8765-7D763907877B",
    "data": {
        "total": 3,
        "accounts": [
            {
                "externalId": "3543180585310896590",
                "username": "developer2",
                "displayName": "开发人员3",
                "phoneNumber": "",
                "email": "test2@****.com",
                "enabled": true,
                "locked": false,
                "description": "来自应用{test-developer}的同步",
                "extendFields": {
                    "test": "123456",
                    "test1": "woman"
                },
                "belongs": [
                    "test2",
                    "test1"
                ]
            },
            {
                "externalId": "test-2",
                "username": "test-2",
```

```
                "displayName": "test-3",
                "phoneNumber": "188****0900",
                "email": "test2@****.com",
                "enabled": false,
                "locked": false,
                "description": "123ttt",
                "extendFields": {
                    "test": "t",
                    "test1": "woman123"
                },
                "belongs": [
                    "test2"
                ]
            },
            {
                "externalId": "test-1",
                "username": "test-1",
                "displayName": "test-1",
                "phoneNumber": "",
                "email": "tangyuehan@idsmanager.com",
                "enabled": false,
                "locked": false,
                "description": "来自应用{test-developer}的同步",
                "extendFields": {},
                "belongs": [
                    "test2",
                    "test1"
                ]
            }
        ]
    }
}
```


返回参数说明：

succes代表请求是否成功，code为错误码 ，message为错误信息为接口。

success为true时，代表请求成功，此时code为200，data返回数据。请求失败时，success为false，code为一串语义化的错误码，如：InvalidParameter.ParentOUUuid.NotExist

参数名	参数值	备注
externalId	{externalId}	IDaaS系统中账户的外部ID
username	{username}	用户名
phoneNumber	{phoneNumber}	手机号
email	{email}	邮箱

locked	{locked}	账号是否锁定,true为锁定,false为未锁定
enabled	{enabled}	账号是否可用,true为启用,false禁用
belongs	{belongs}	账户所属组织机构列表
extendFields	{extendFields}	扩展字段，用于账户保存的自定义字段

错误码说明：

HttpCode（请求状态码）	code（错误码）	message（错误信息）	备注
200	200	null	请求成功
400	InvalidParameter	例如：Invalid createStartDate	请求参数错误

推送账户组

在SP中添加一个组，通过调用此接口，将组的信息推送到IDaaS中。

Request URI: /api/bff/v1.2/developer/scim/group/create `POSTREST`

Content-Type: application/json

Request Body:

```
{
    "externalId": "121-11",
    "displayName": "测试同步组11",
    "ouExternalId": "605016592710192945",
    "members": [
        {
            "accountExternalId":"",
            "username":"test1"
        }
    ],
    "extendFields": {
        "test":"123456"
    }
}
```

请求参数说明：

参数名	参数值	类型	备注
externalId	{externalId}	String	IDaaS系统中账户组的外部ID，唯一。选填，不填时，系统会随机生成一个，并在结果中返回
displayName	{displayName}	String	组显示名称。必填
ouExternalId	{ouExternalId}	String	所属组织单位（OU）的外部ID，必填
description	{description}	String	描述信息，选填
members	{members}	String	组成员，已经存在的账户外部ID和账户名，accountExternalId是账户外部ID，username是账户名
extendFields	{extendFields}	Map	自定义扩展字段，选填

Response Body:

```
{"success": true,
        "code": "200",
        "message": null,
        "requestId": "BF66FA08-E57B-4387-90C0-A72E41307239",
        "data": {
        "externalId":"123456"
        }
}
```

success代表请求是否成功，code为错误码 ， message为错误信息为接口。

success为true时，代表请求成功，此时code为200，data返回数据。请求失败时，success为false，code为一串语义化的错误码，如：InvalidParameter.ParentOUUuid.NotExist

错误码说明:

HttpCode（请求状态码）	code（错误码）	message（错误信息）	备注
200	200	null	请求成功

400	InvalidParameter	例如：组名称不能为空	请求参数错误
400	InvalidParameter.DisplayName.Exist	当前OU下，组名已经存在	显示名已经存在
400	InvalidParameter.ExternalId.Exist	externalId已存在	externalId已存在
400	EntityNotFound	OU不存在	组隶属的OU不存在
403	Forbidden	没有权限操作该组	没有权限操作该组

更新账户组

在SP中更新一个组，通过调用此接口，将组的信息推送到IDaaS中。

Request URI: /api/bff/v1.2/developer/scim/group/update `PUTREST`

Content-Type: application/json

Request Body:

```
{
    "externalId": "121",
    "description": "tttt测试",
    "displayName": "测试t121",
    "extendFields": {
        "test":"ttt测试"
    }
}
```

请求参数说明：

参数名	参数值	类型	备注
externalId	{externalId}	String	IDaaS系统中账户组的外部ID,唯一。必填
displayName	{displayName}	String	组显示名称。选填，填写则代表更新该项信息。
description	{description}	String	描述信息，选填。填写则代表更新该项信息。

extendFields	{extendFields}	Map	自定义扩展字段，选填，填写时代表更新。

Response Body:

```
{
    "success": true,
    "code": "200",
    "message": null,
    "requestId": "BF66FA08-E57B-4387-90C0-A72E41307239",
    "data": null
}
```

返回参数说明：

succes代表请求是否成功，code为错误码 ，message为错误信息为接口。

success为true时，代表请求成功，此时code为200，data返回数据。请求失败时，success为false，code为一串语义化的错误码，如：InvalidParameter.ParentOUUuid.NotExist

错误码说明：

HttpCode（请求状态码）	code（错误码）	message（错误信息）	备注
200	200	null	请求成功
400	InvalidParameter	例如：组的externalId参数不能为空	请求参数错误
400	InvalidParameter.DisplayName.Exist	当前OU下，组名已经存在	显示名已经存在
400	InvalidParameter.ExternalId.NotExist	externalId不存在	externalId不存在
403	Forbidden	没有权限操作该组	没有权限操作该组

删除账户组

在SP中删除一个组，通过调用此接口，将IDaaS中的组删除。

Request URI: /api/bff/v1.2/developer/scim/group/delete `DELETEREST`

Content-Type:application/json

请求参数说明：

参数名	参数值	备注
externalId	{externalId}	IDaaS系统中账户组的外部ID。

Response Body:

```
{
    "success": true,
    "code": "200",
    "message": null,
    "requestId": "BF66FA08-E57B-4387-90C0-A72E41307239",
    "data": null
}
```

返回参数说明:

succes代表请求是否成功，code为错误码 ，message为错误信息为接口。

success为true时，代表请求成功，此时code为200，data返回数据。请求失败时，success为false，code为一串语义化的错误码，如：InvalidParameter.ParentOUUuid.NotExist

错误码说明:

HttpCode（请求状态码）	code（错误码）	message（错误信息）	备注
200	200	null	请求成功
400	InvalidParameter	例如：组的externalId参数不能为空	请求参数错误
400	EntityNotFound	例如：查询不到组信息	未查询到组信息
400	OperationDenied.GroupContainsChildren	例如：组有关联成员（如有子成员），不能删除	组有关联成员（如有子成员），不能删除
403	Forbidden	没有权限操作该组	没有权限操作该组

获取应用已经授权的组织机构及账户列表

根据应用的uuid获取直接授权的组织机构及账户的外部ID。

Request URI: /api/bff/v1.2/developer/scim/application/authorized/list `GETREST`

请求示例:

```
/api/bff/v1.2/developer/scim/application/authorized/list?applicationUuid=1694618271068407094
```

请求参数说明：

参数名	参数值	备注
applicationUuid	{applicationUuid}	IDaas中应用的唯一标识

Response Body：

```
{
"success": true,
"code": "200",
"message": null,
"requestId": "2230CE9E-4674-407C-A006-D29ACD9DADDB",
"data": {
    "ouExternalIds": [
        "1",
        "129387071",
        "4122068885249961546"
    ],
    "accountExternalIds": [
        "4484474128951618300",
        "5812895747601718104"
    ]
}
}}
```

返回参数说明：

succes代表请求是否成功，code为错误码 ，message为错误信息为接口。

success为true时，代表请求成功，此时code为200，data返回数据。请求失败时，success为false，code为一串语义化的错误码，如：InvalidParameter.ParentOUUuid.NotExist

参数名	说明
ouExternalIds	已授权的组织机构外部ID列表
accountExternalIds	已授权的账户外部ID列表

错误码说明：

HttpCode（请求状态码）	code（错误码）	message（错误信息）	备注
200	200	null	请求成功

400	InvalidParameter	例如：applicationUuid不能为空	请求参数错误
400	EntityNotFound	例如：无效的applicationUuid	通过applicationUuid未找到对应的应用
403	Forbidden	例如：没有权限操作该父OU	没有权限操作

4.聚石塔对接

简介

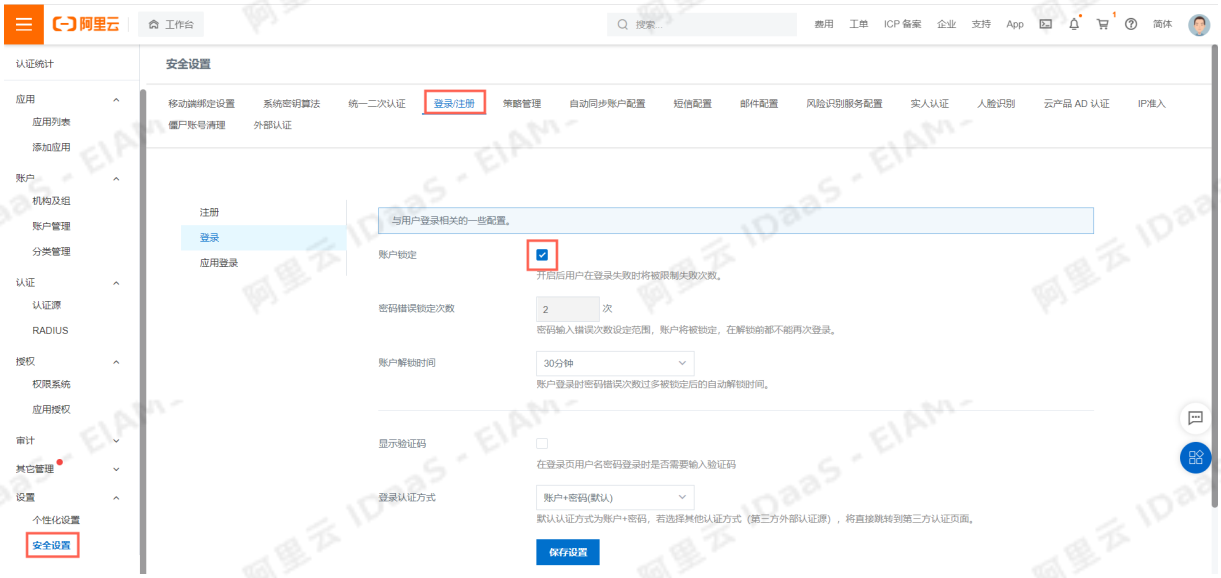
IDaaS 聚石塔版本旨在为客户提高身份认证安全水位、加强安全防护能力，从服务端、IP、账户三个层次，消除暴力破解、弱密码、僵尸账户等问题带来的安全风险。

本文针对聚石塔客户介绍 IDaaS 聚石塔版本**部分**安全能力的最佳实践，非聚石塔客户请查看其他最佳实践。

账户密码错误拦截

管理员可以在 **安全设置-登录/注册-登录** 中配置账户锁定规则，当用户尝试登录时如果密码错误超过一定次数，账户将被锁定一段时间，以防止暴力破解。

建议至少设置为：密码错误超过6次后，锁定30分钟。



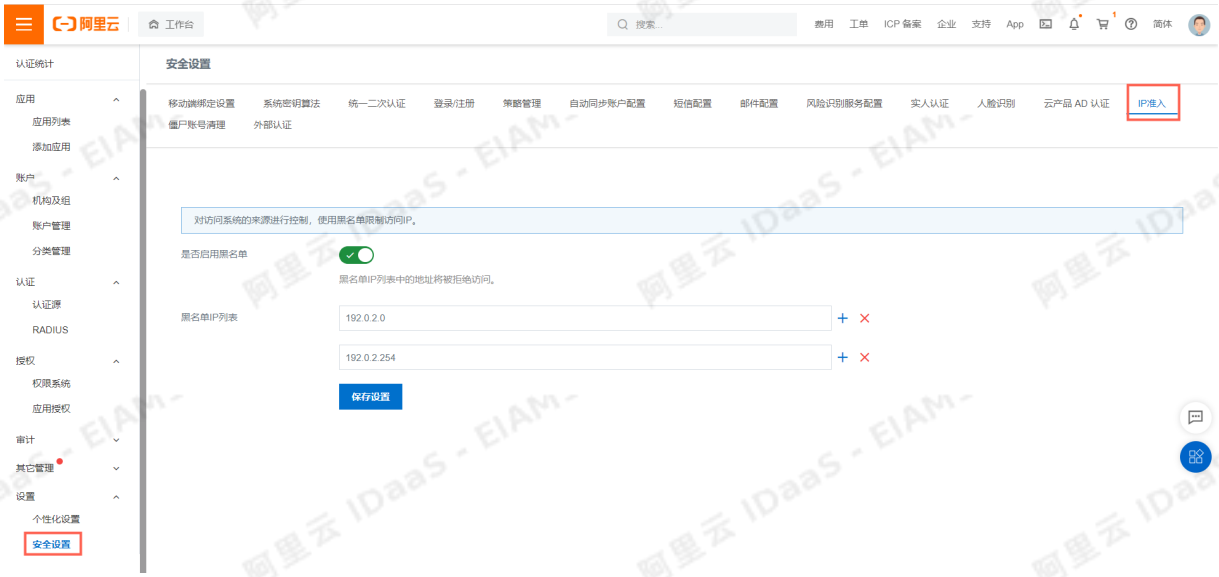
传输客户端 IP 地址

IDaaS 会识别异常的客户端 IP，并自动拦截在黑名单内的 IP。**请确保已根据《聚石塔接口对接文档》中账户密码认证接口的要求传输请求参数** `X-Client-IP` ，以实现 IP 层面的防护。

请使用钉钉搜索 33824749 加入 IDaaS 客户群，联系阿里云 IDaaS 产品团队获取《聚石塔接口对接文档》。

IP 黑名单拦截

管理员可以在 **安全设置-IP准入** 中配置客户端 IP 黑名单，黑名单内 IP 的访问将被拦截，以实现对异常客户端 IP 进行控制。



IP 白名单拦截

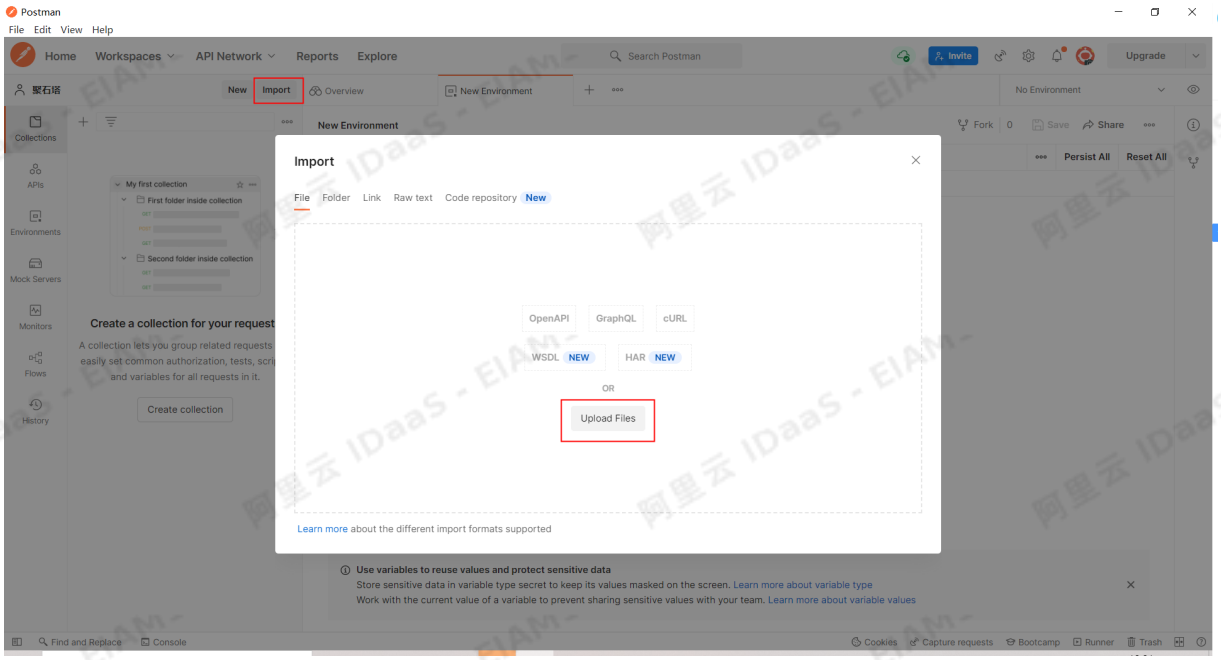
管理员可以在 **应用-应用列表-详情-IP白名单配置** 中配置服务端 IP 白名单，对调用 IDaaS 接口的 IP 进行限制，不在白名单内的 IP 的接口请求不会被执行，以提高服务端的安全性。**建议所有应用都配置 IP 白名单。**

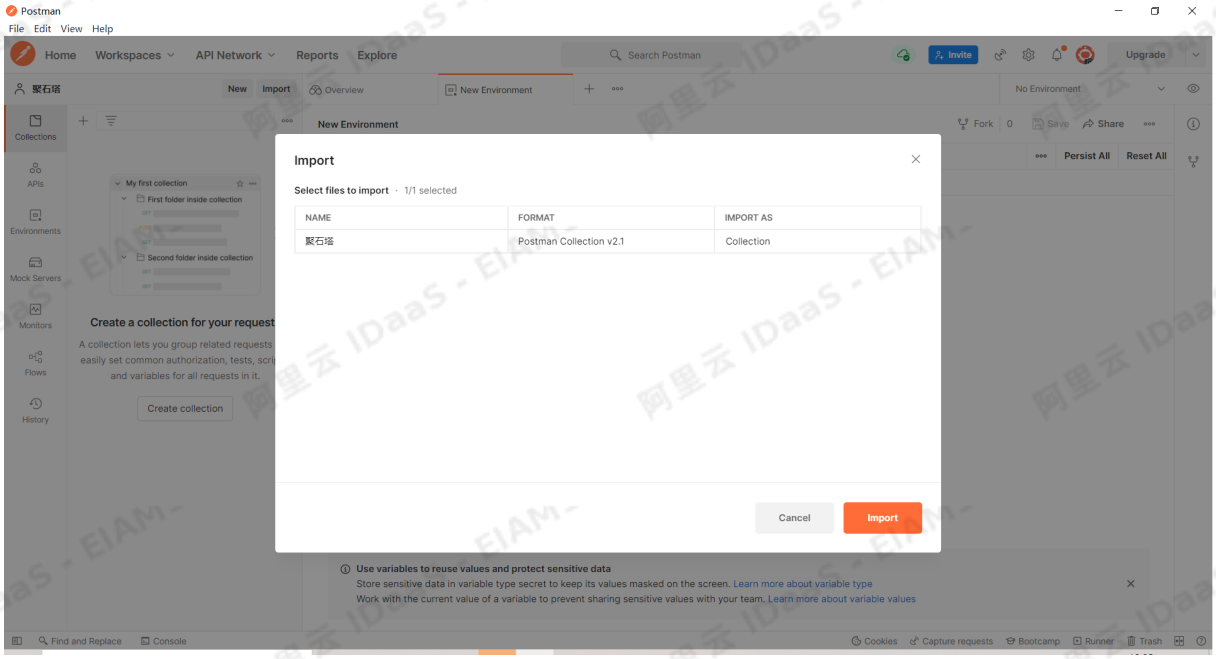
5.聚石塔 Postman 接口使用指南

本文旨在提供一套能够跑通聚石塔接口的 Postman Schema，帮助客户快速完成对接。如果在对接中发现问题，客户可根据 Postman 中接口的实现逻辑进行核对修正。在使用本文档时，可配合 IDaaS-聚石塔对接文档-v1.8.4.pdf 一同使用，能够更佳清晰地了解业务逻辑。

导入 Schema

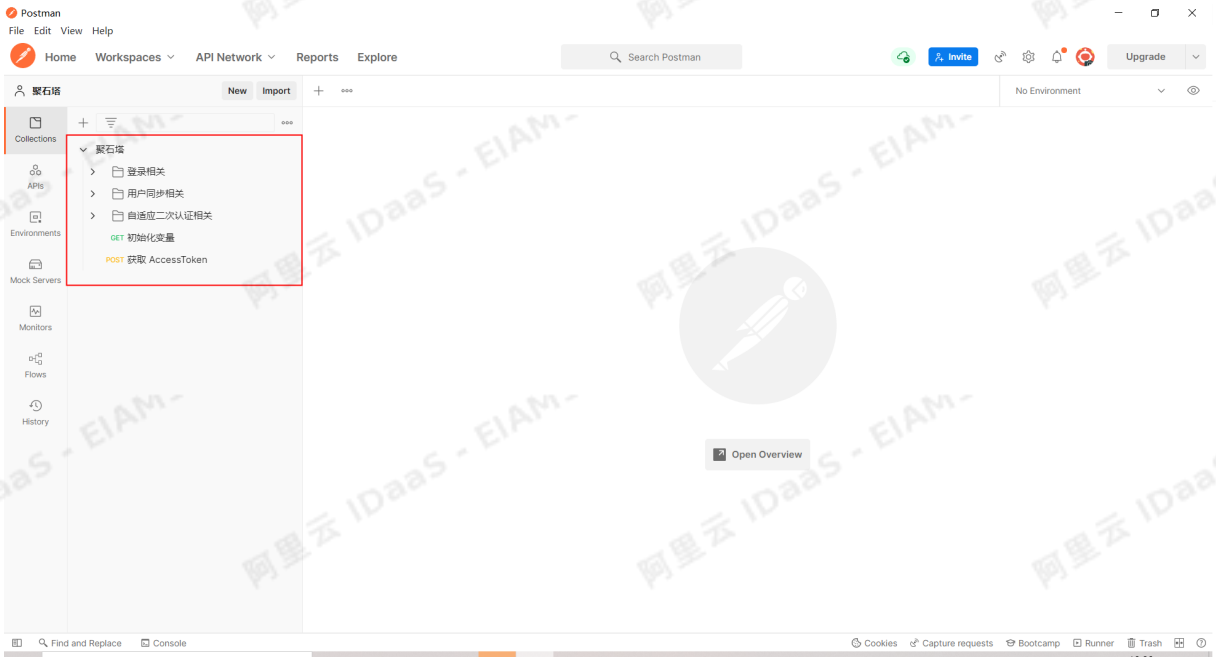
下载 聚石塔.postman_collection.json，导入到 Postman 中：



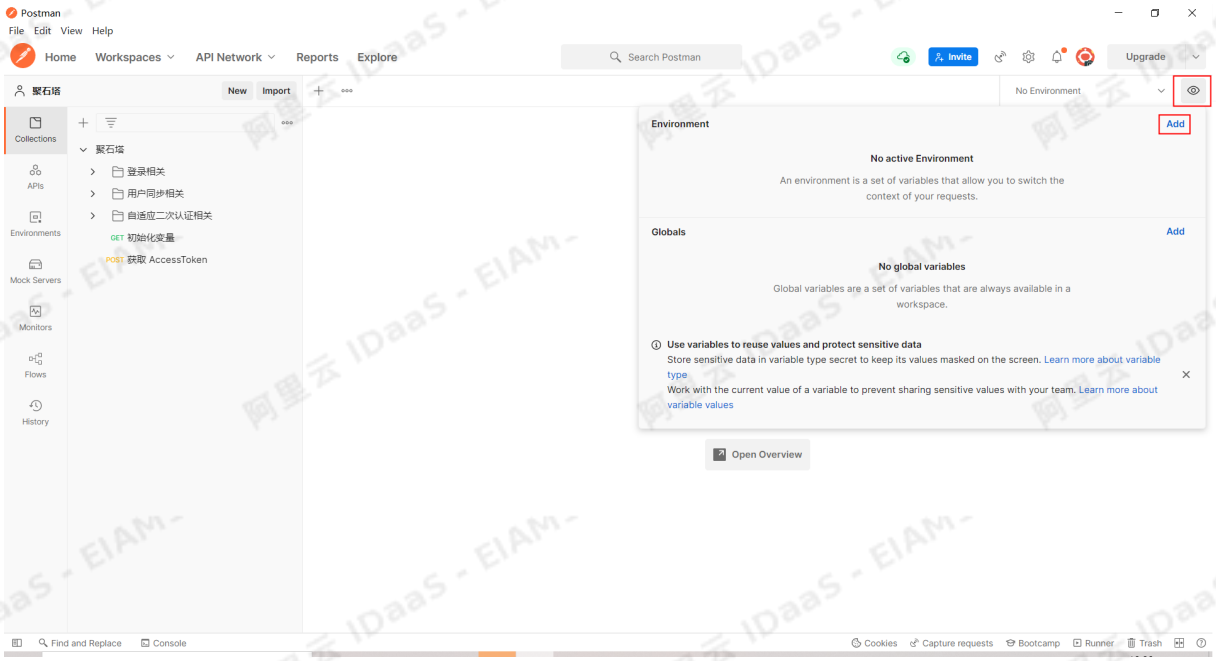


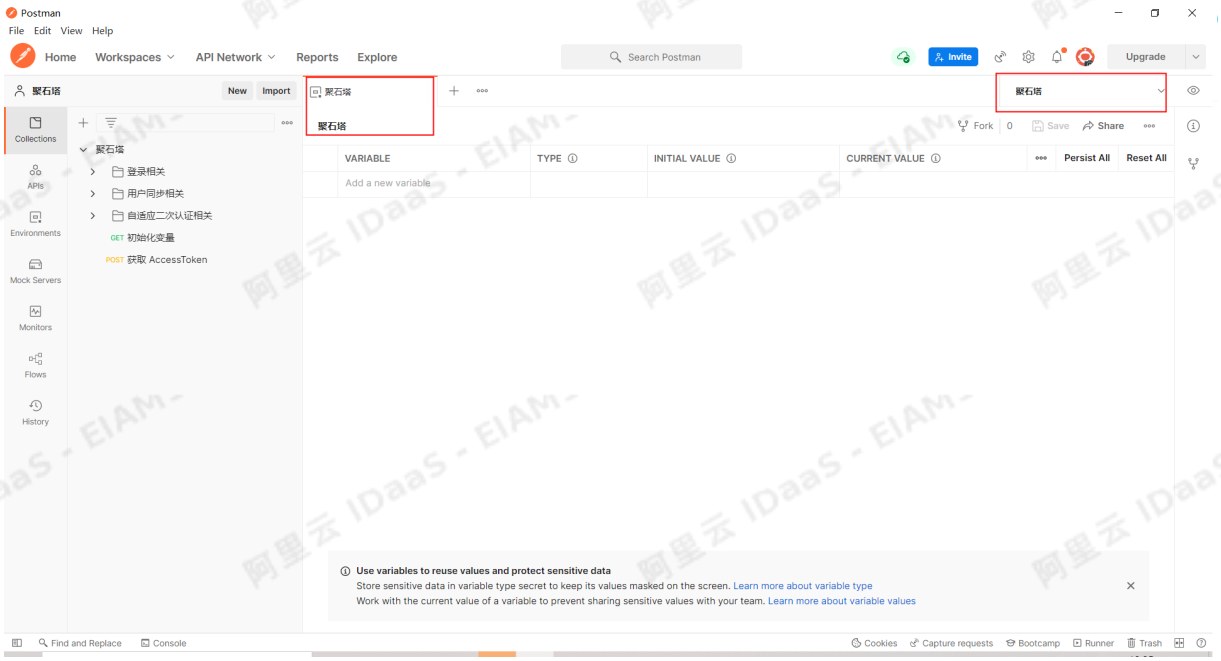
以上截图基于 Postman v9.15.4，版本不同界面展示可能存在差异。

导入完成后，目录结构如下：



添加一个环境，然后切换到该环境：

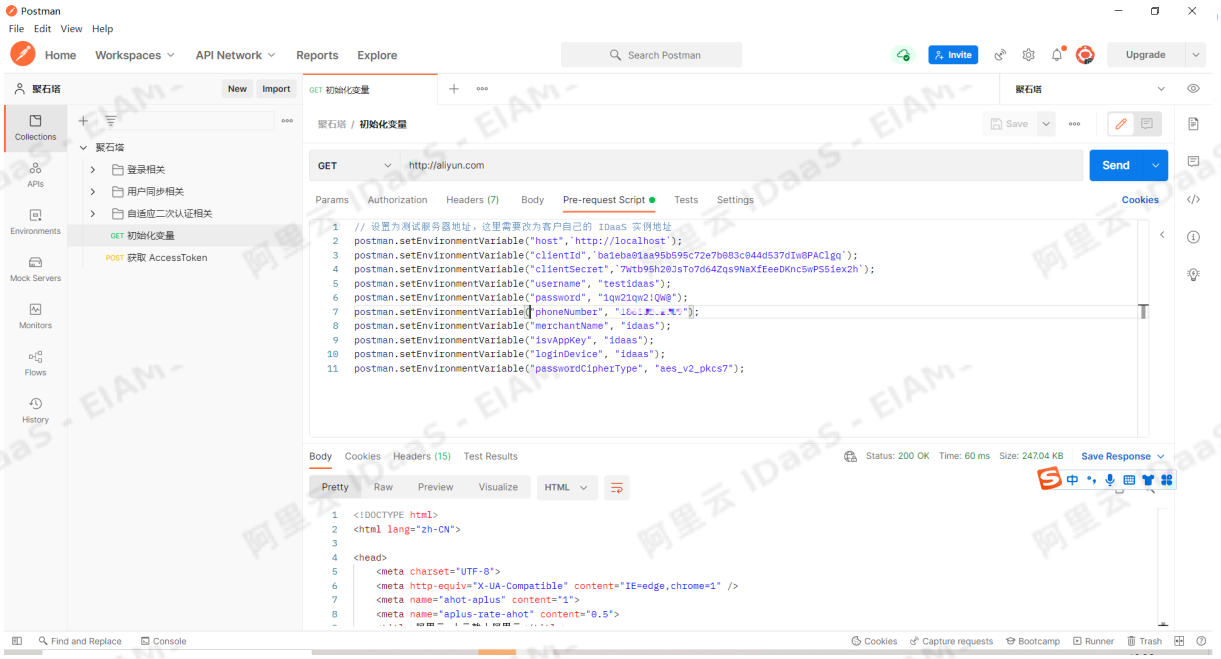




至此，准备工作已经完成，接下来开始调试接口。请按顺序执行接口，接口之间存在依赖关系，先执行的接口为后执行的接口提供环境变量。

初始化变量

首先，需要执行【初始化变量】：



url 可以任意填写，目的是为了能够执行脚本。

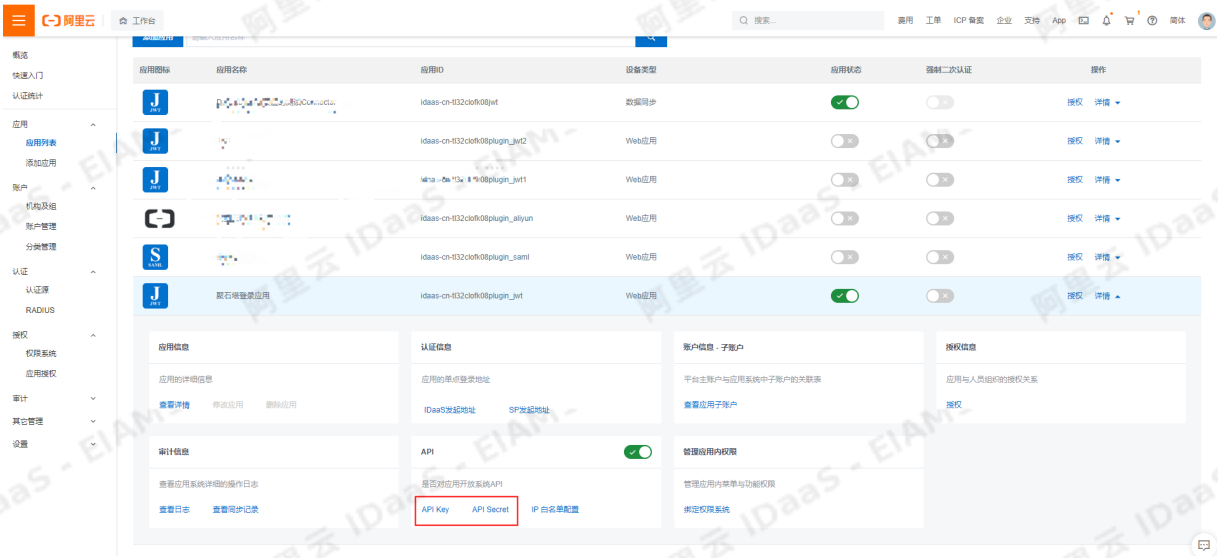
如果客户尚未购买实例，需要先对接，IDaaS 可以提供测试服务器供客户提前对接。

接下来介绍如何获取以上变量值。

host

host 即上图中 “实例开放接口域名”，特别注意聚石塔的版本为 idaas-jst-xxx，如果不是请立即联系 IDaaS。

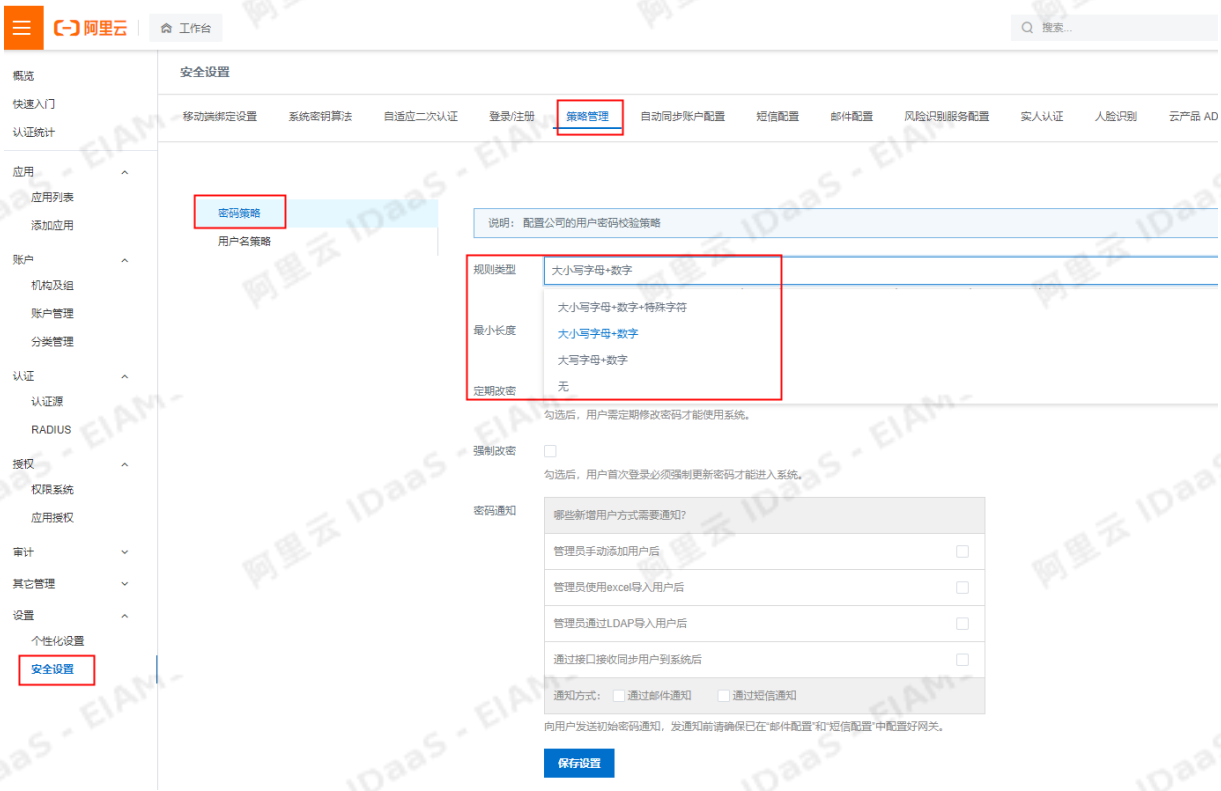
clientId 和 clientSecret



API Key为 clientId， API Secret为 clientSecret。

username、password、phoneNumber

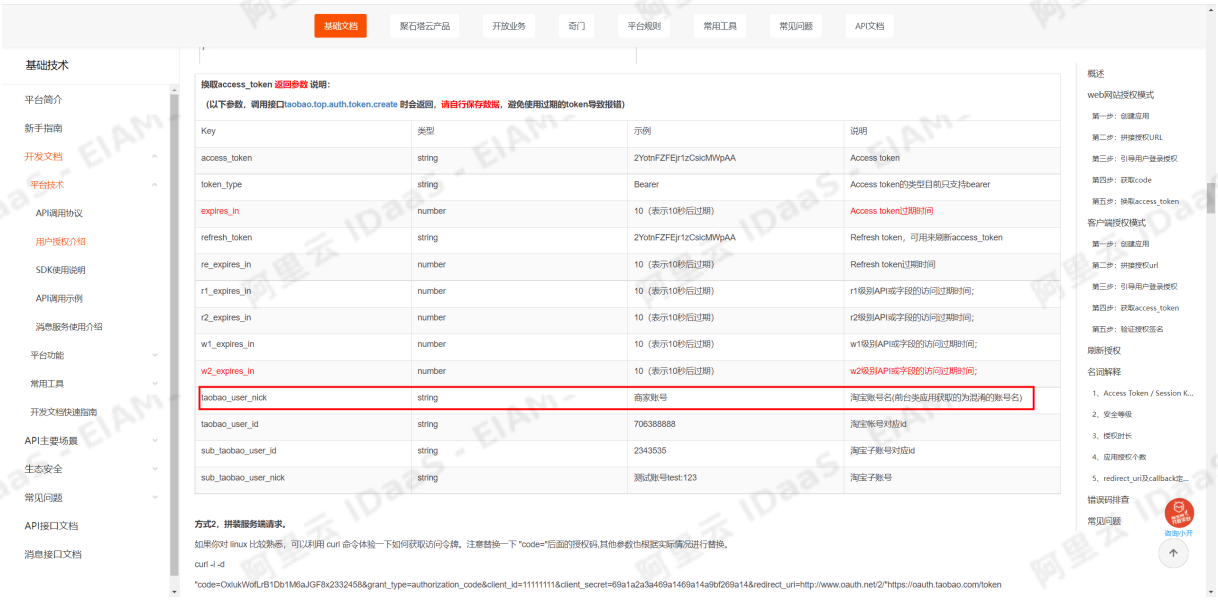
接下来会使用这里的用户信息调用接口创建账号。用户信息可以自行修改，但需要满足约束条件。如果提示不满足密码策略，可以在 IDaaS 控制台调整：



merchantName

商户名称是上图中的【掌柜】，务必传对，否则无法计分。

更准确地是从接口中获取，参考 接口文档：



两者值若不同，以接口为准。

ivsAppKey

参考 接口文档：

示例中的 client_id 和 redirect_uri 需要替换成您创建应用的实际数据。

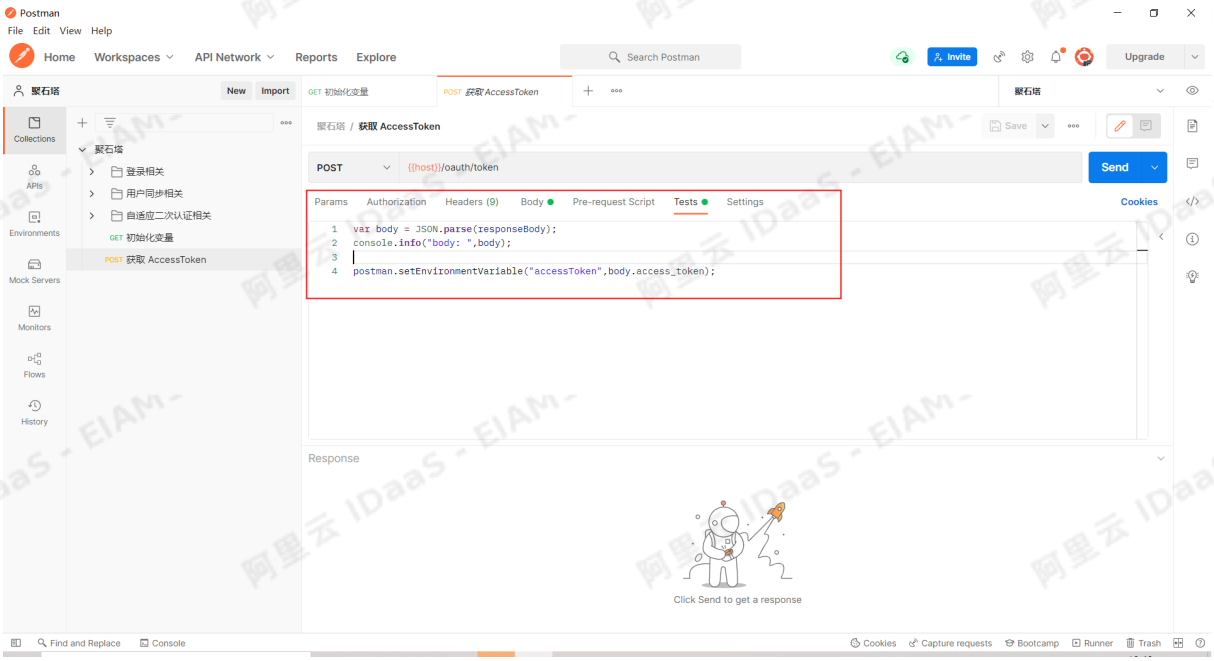
client_id 传入appkey，查找路径：【控制台】-【应用管理】-【管理】-【概览】-【APP证书】-【AppKey】，AppSecret 也在此处；

redirect_uri 传入回调地址，查找路径：【控制台】-【应用管理】-【管理】-【应用设置】-【基本信息】-【回调URL】。如下所示。

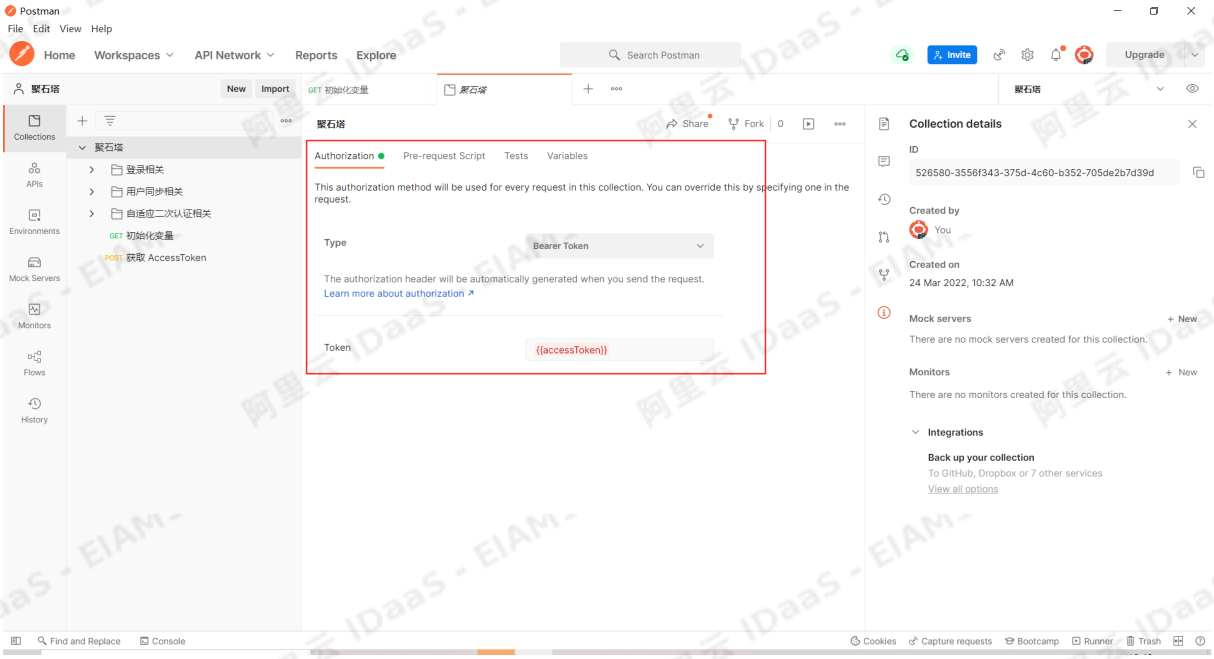
ivsAppKey 为上图中的 App Key，务必传对，否则无法计分。

创建用户流程

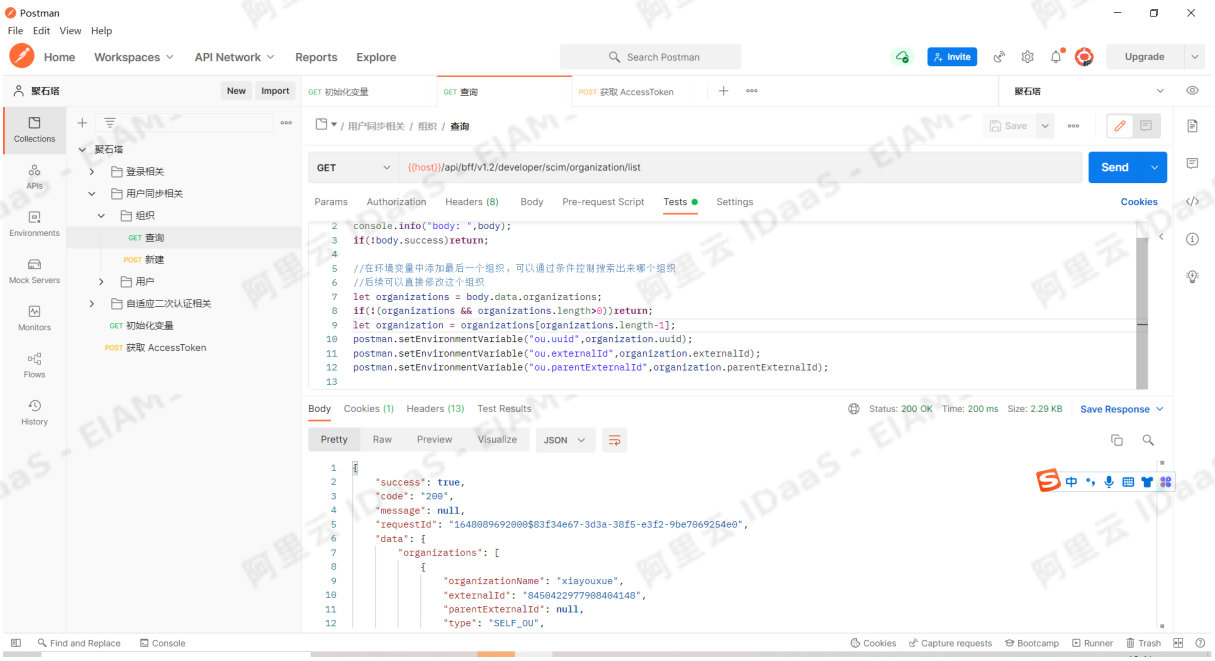
获取 AccessToken



获取 AccessToken，为后续接口提供认证需要的 token:

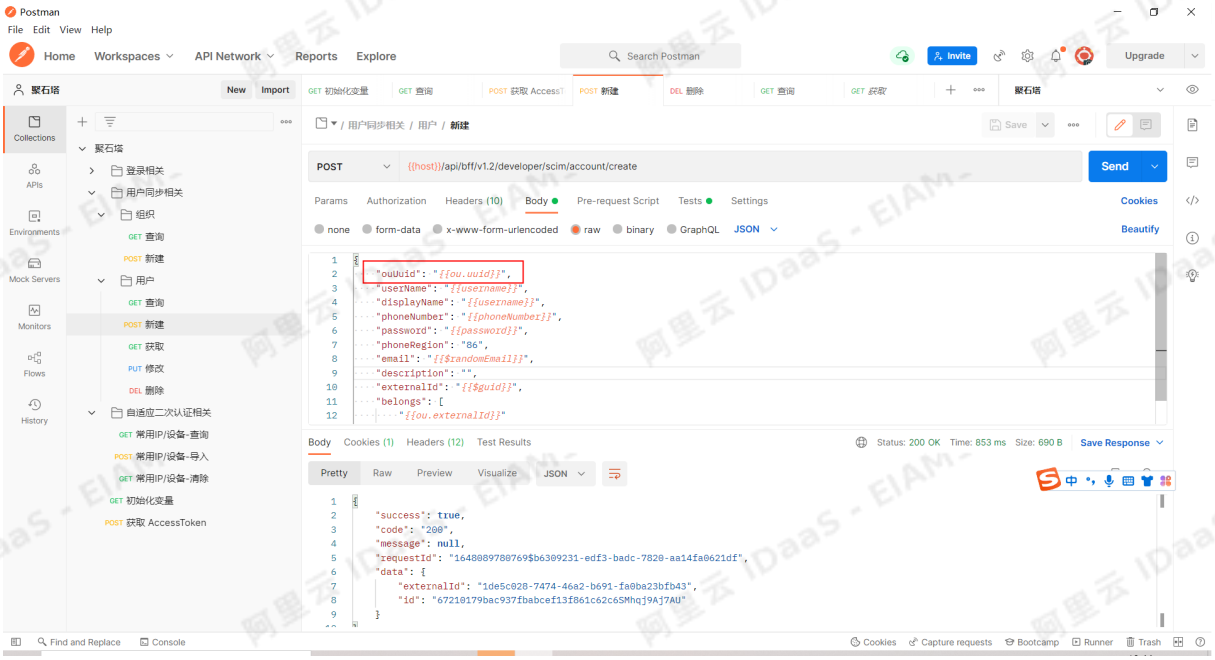


组织 / 查询



查询组织，将最后一个组织添加到环境变量，创建用户时需要设置所属的组织。

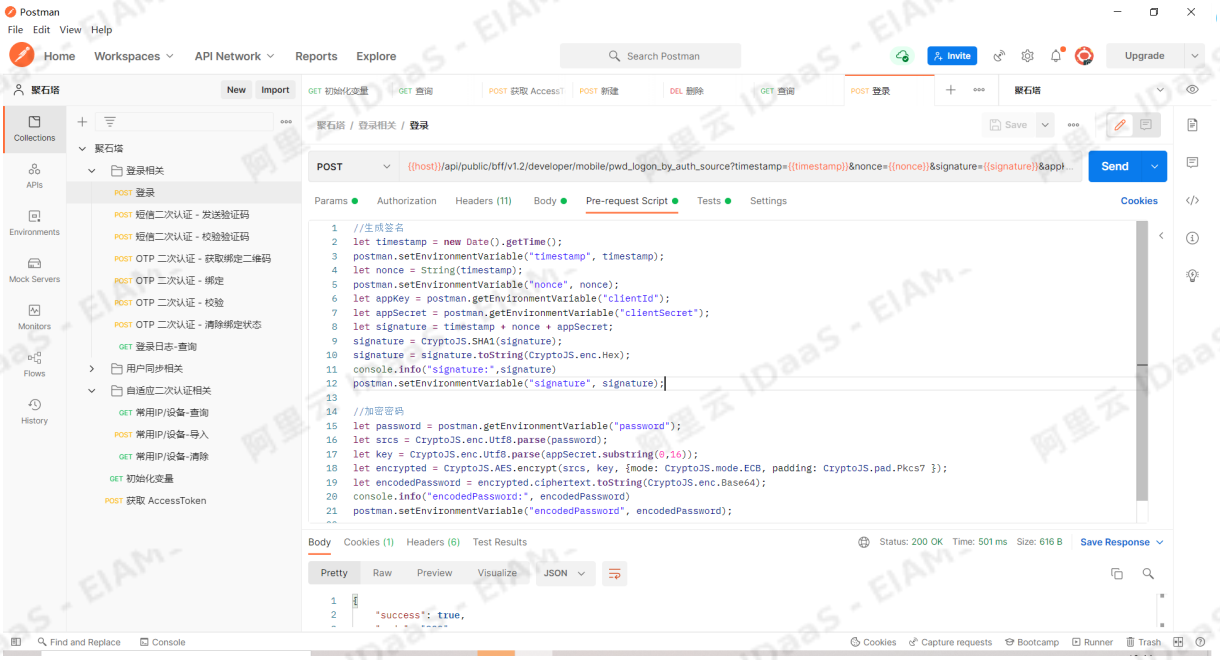
用户 / 新建



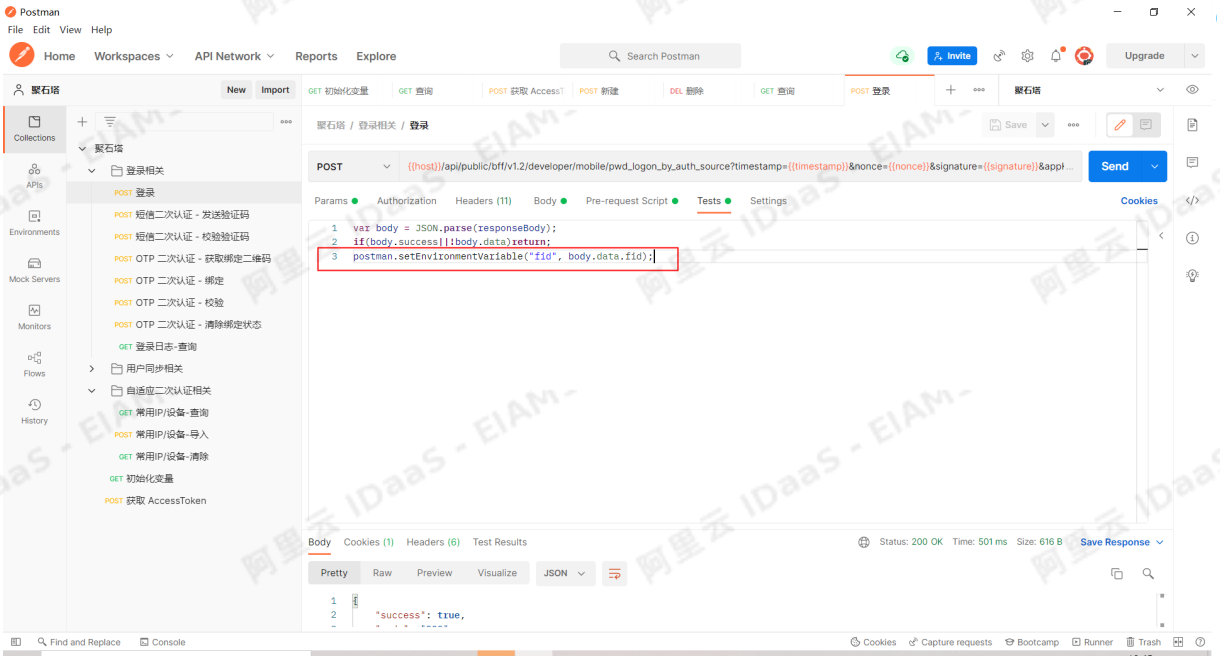
新建用户时，会使用上一步查询出来的组织。创建用户后，从 IDaaS 控制台开启用户二次认证：

短信二次认证流程

登录

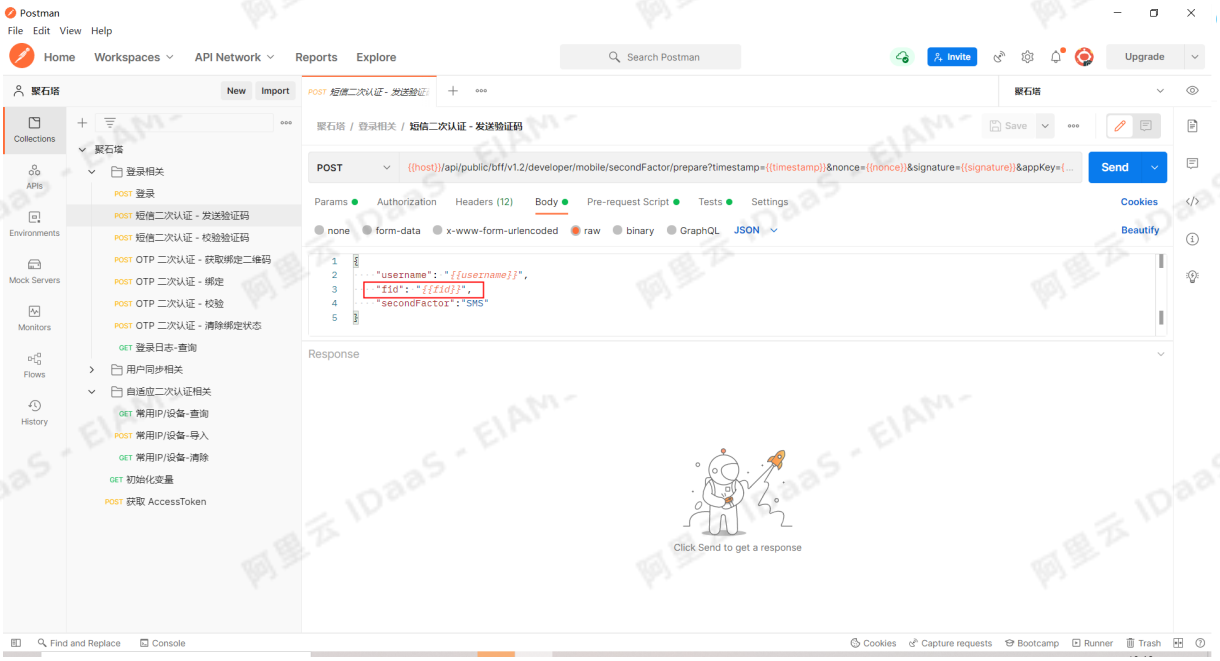


登录时，会自动计算签名并加密密码。



登录完成后，如果开启了二次认证，会自动添加 fid 环境变量。

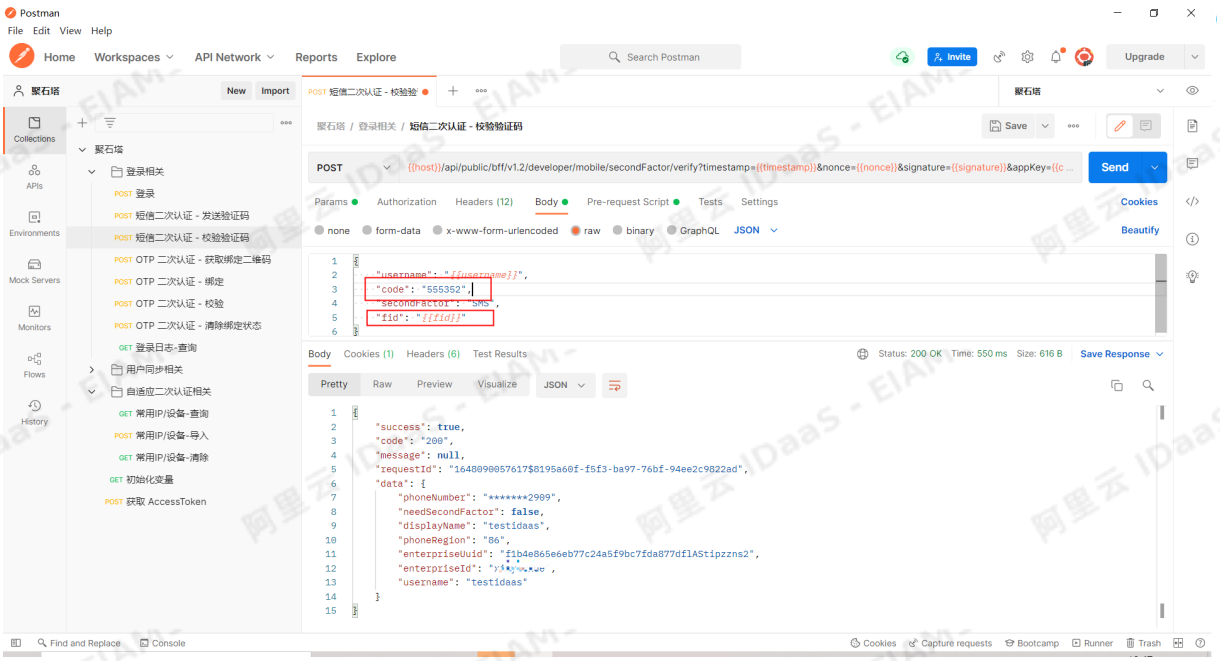
短信二次认证 - 发送验证码



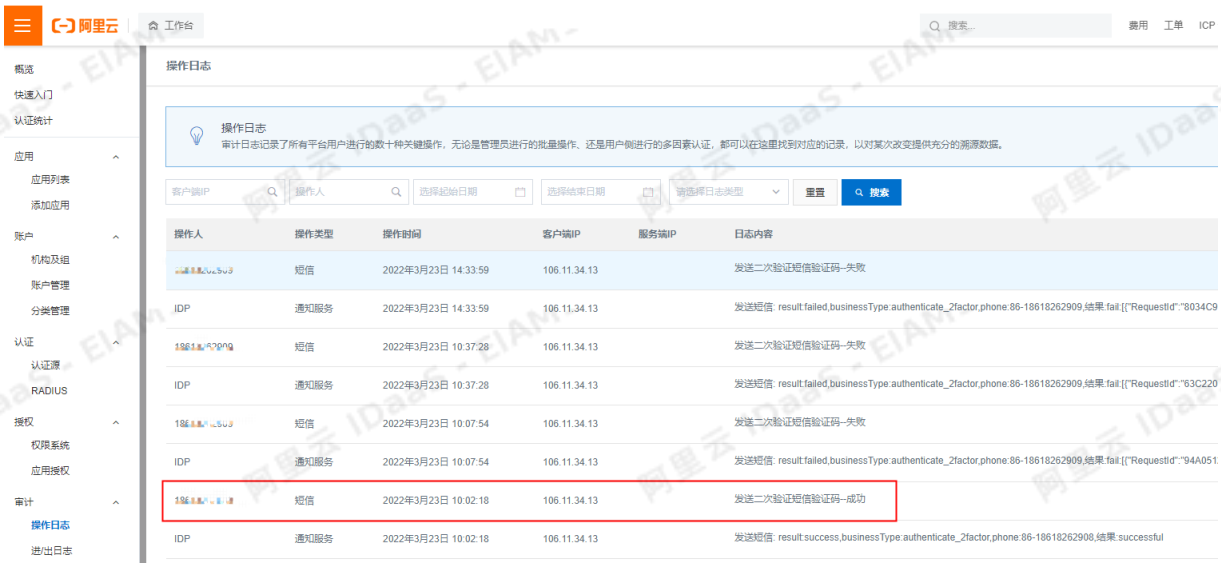
使用登录返回的 fid，发送短信二次认证验证码。

发送二次认证验证码成功后，更新 fid。

短信二次认证 - 校验验证码



使用上一步返回的 fid，校验短信二次认证验证码。code 传入手机上收到的验证码，如果没有收到验证码，请在 IDaaS 控制台通过日志核实是否发送成功：

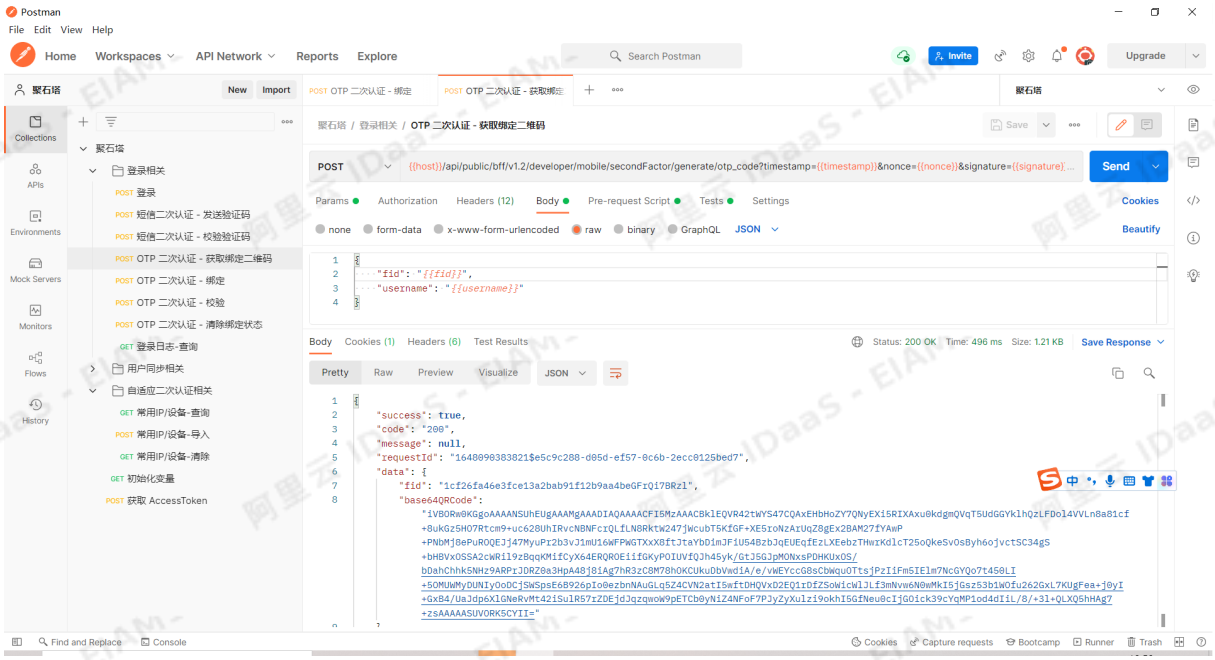


OTP 绑定流程

登录

同上。

OTP - 获取绑定二维码

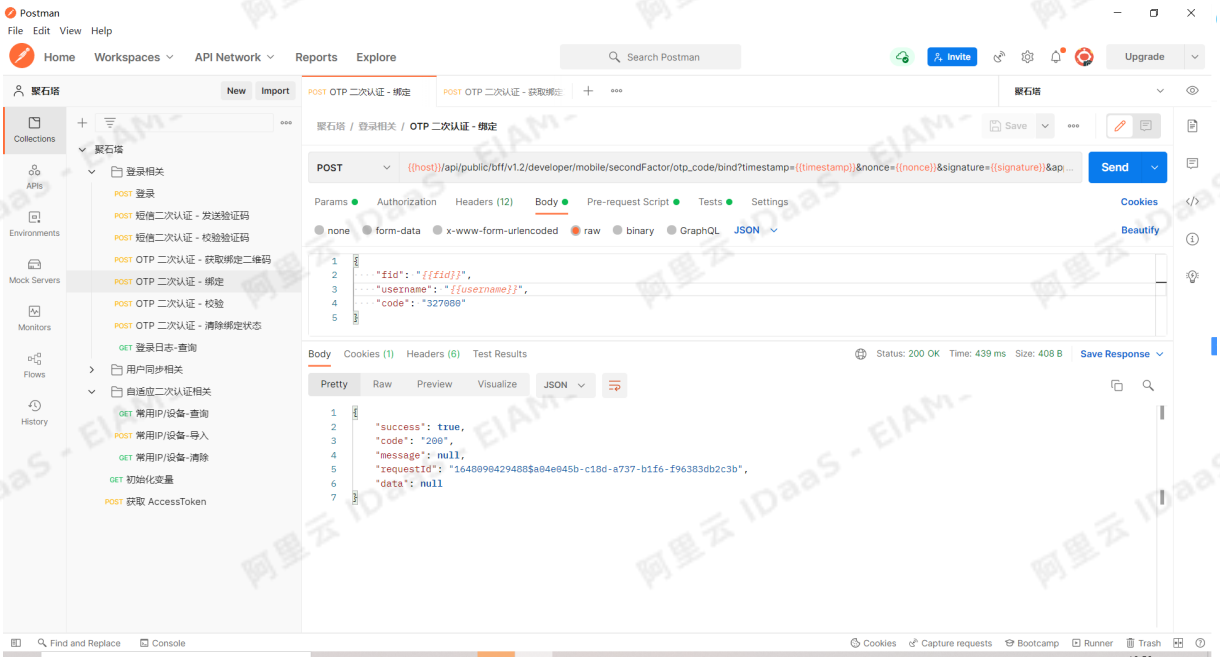


获取成功自动设置 fid 环境变量。

使用 Base64 图片转换网站 https://tool.chinaz.com/tools/imgtobase/ 展示 OTP 绑定二维码，拷贝 base64QRCode的值，添加前缀 **：

使用 Google 身份认证器（或其他认证器），扫描二维码，获取 OTP Code：

OTP - 绑定



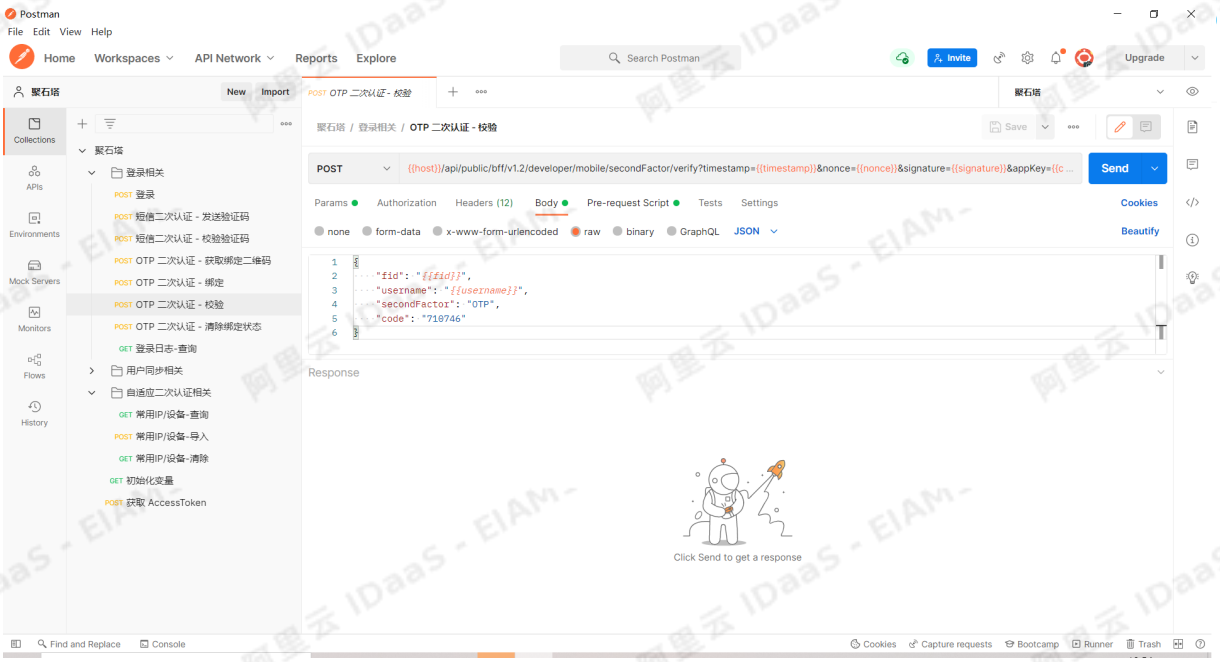
输入上一步中获取的 OTP Code。如果上一步操作时间过长，会导致 fid 失效，需要重新登录。登录后调用【OTP - 获取绑定二维码】，因为之前已经绑定过了，现在直接从认证器获取 OTP Code 调用【OTP - 绑定】。

OTP 二次认证流程

登录

同上。

OTP - 校验



输入从认证器中获取的 OTP Code。