ALIBABA CLOUD

# 阿里云

## 应用身份服务
## 钉钉相关对接

文档版本：20210720

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<br>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<br>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<br>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<br>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`<br>*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.IDaaS与钉钉对接场景介绍

本文为应用身份服务IDaaS与钉钉在日常使用中的对接场景介绍，通过钉钉和IDaaS的集成，可以实现用户使用钉钉账户登录各个办公系统的目的。

## 背景

在公司中，员工需要每天反复的登录各个办公系统，并且需要记录多套账号密码，在频繁的登录过程中就为员工带来很多重复性工作。对于管理员也很难对用户登录各个办公系统的行为进行审计统计，并且如果每个办公系统都需要管理员单独维护员工账户生命周期，那么势必也会为管理员带来很多重复和耗时耗力的工作。

## 解决方案介绍

目前越来越多的公司使用钉钉作为办公软件，钉钉已成为员工工作中必不可少的一款使用工具。如果公司管理人员把钉钉和其它系统的数据进行打通，员工每天对各个办公应用的登录访问和钉钉进行协同，那么将会减少很多重复性的工作，给企业节约更多成本。

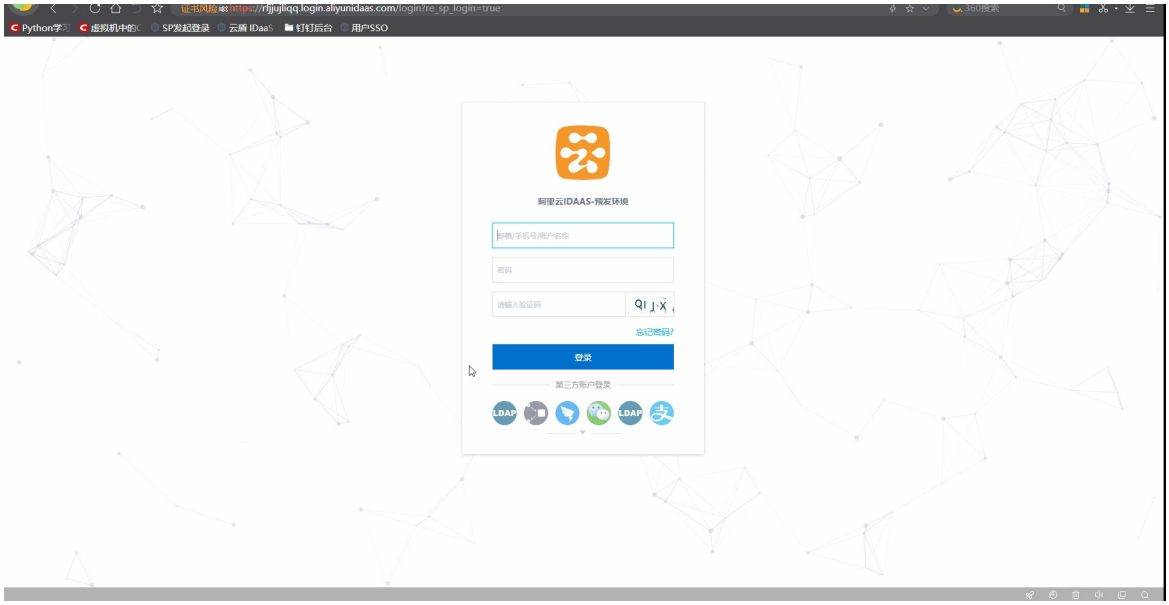
## 场景介绍

1. **通过钉钉OA工作台实现单点登录**


IDaaS提供各种标准协议模板，可以快速帮助客户对接不支持改造的应用，满足客户对各种办公系统单点登录的需求。 通过钉钉和IDaaS进行集成，用户访问钉钉OA工作台，点击应用的图标就可以单点登录到各个办公系统中（包括移动端和PC端），不需再记录各个登录地址和账户密码。


场景举例： 用户打开钉钉客户端访问OA工作台，点击公司办公系统的图标如JIRA，可以直接单点登录到JIRA进行使用。


2. **钉钉扫码登录IDaaS统一门户**




IDaaS支持统一的WEB门户，用户可以使用各种认证源登录IDaaS门户，在门户中点击各个应用图标实现单点登录。

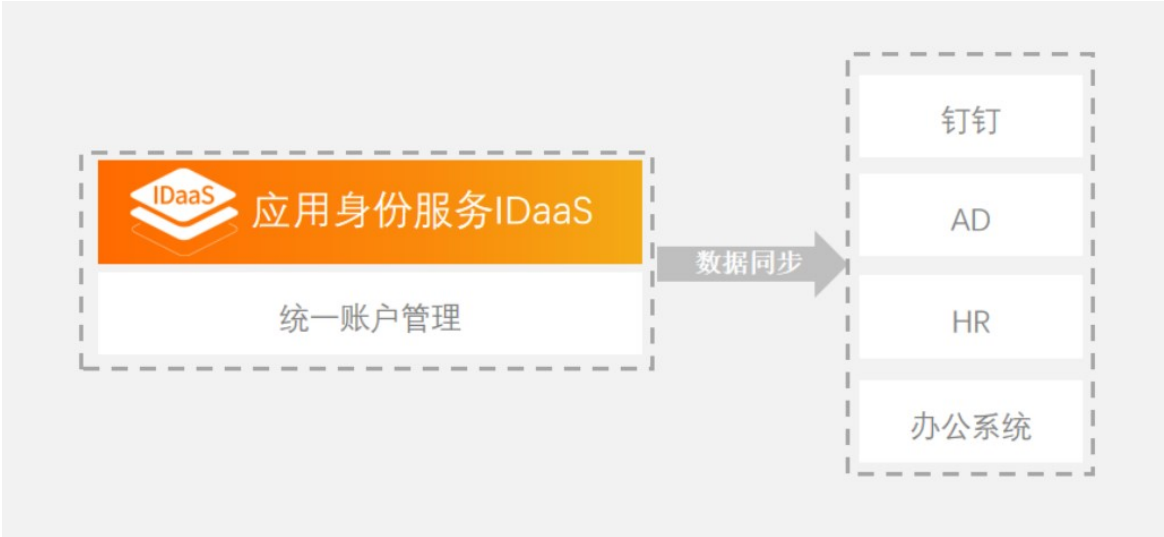
支持的认证源包括：钉钉扫码，微信扫码，AD账户等


使用钉钉扫码登录IDaaS见下图


3. **IDaaS同步数据到钉钉**

   IDaaS支持对账户生命周期的统一管理，IDaaS中的账户可以同步到任意系统中，包括钉钉、AD、HR系统以及各种第三方应用等。

   管理员只需在IDaaS中对用户进行统一管理，用户将会自动同步到各个应用中，不需要再手动维护每个系统中的账户体系。



# 2.钉钉同步数据到IDaaS（钉钉旧版页面）

本文介绍如何配置钉钉同步配置，实现将钉钉组织架构和账户数据拉取到IDaaS。将钉钉数据同步到 IDaaS，和钉钉进一步集成打通，为钉钉客户提供到 AD 或其他身份源的同步。

## 添加钉钉同步配置

1. 在钉钉开放平台添加一个钉钉微应用，可参考创建钉钉微应用。

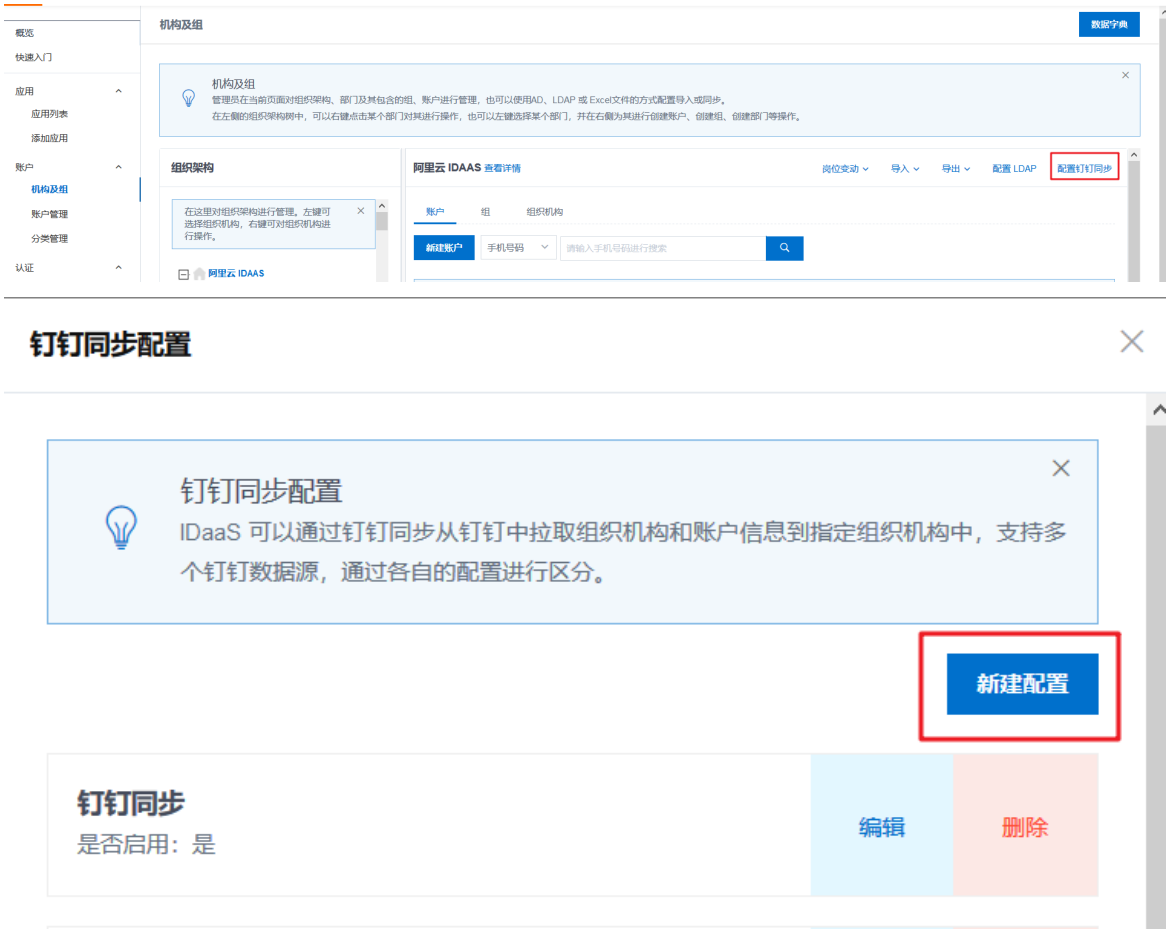

**注意** 请确认钉钉微应用配置的服务器出口IP为IDaaS服务器的出口IP，否则无法成功拉取到钉钉的账户/组织机构数据。

**说明** 如果已创建过钉钉微应用，可以直接使用现有的

**需要确认您使用的钉钉微应用的接口权限开启了通讯录权限和手机号码信息权限，否则有可能导致无法拉取钉钉账户**



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. 在机构及组页面，点击配置钉钉同步，新建一个钉钉同步配置。


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
机构及组
数据字典
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、创建部门等操作。
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
阿里云 IDAAS 查看详情
岗位变动
导入
导出
配置 LDAP
配置钉钉同步
账户
组
组织机构
新建账户
手机号码
请输入手机号码进行搜索


钉钉同步配置
钉钉同步配置
IDaaS 可以通过钉钉同步从钉钉中拉取组织机构和账户信息到指定组织机构中，支持多个钉钉数据源，通过各自的配置进行区分。
新建配置
钉钉同步
是否启用：是
编辑
删除

4. 填写配置参数


名称：可以随意填写，支持中文、大小写字母、数字。

CorpID：登录钉钉开放平台首页展示的值。

appKey、appSecret：钉钉微应用-应用详情中展示的值。


**注册回调：开启注册回调后，在钉钉OA工作台对账户和组织机构的操作会自动同步到IDaaS。**

根节点：填写后，钉钉的组织机构和账户会导入到指定的组织机构下。如果不填写，则默认导入到IDaaS根目录下。

密码：钉钉账户同步到IDaaS后，为账户设置的用于登录IDaaS平台的默认密码。

> 注意　请确认导入的密码符合当前的密码策略，否则无法导入账户。

5. 点击测试连接，确认参数填写正确后，启用配置并点击保存

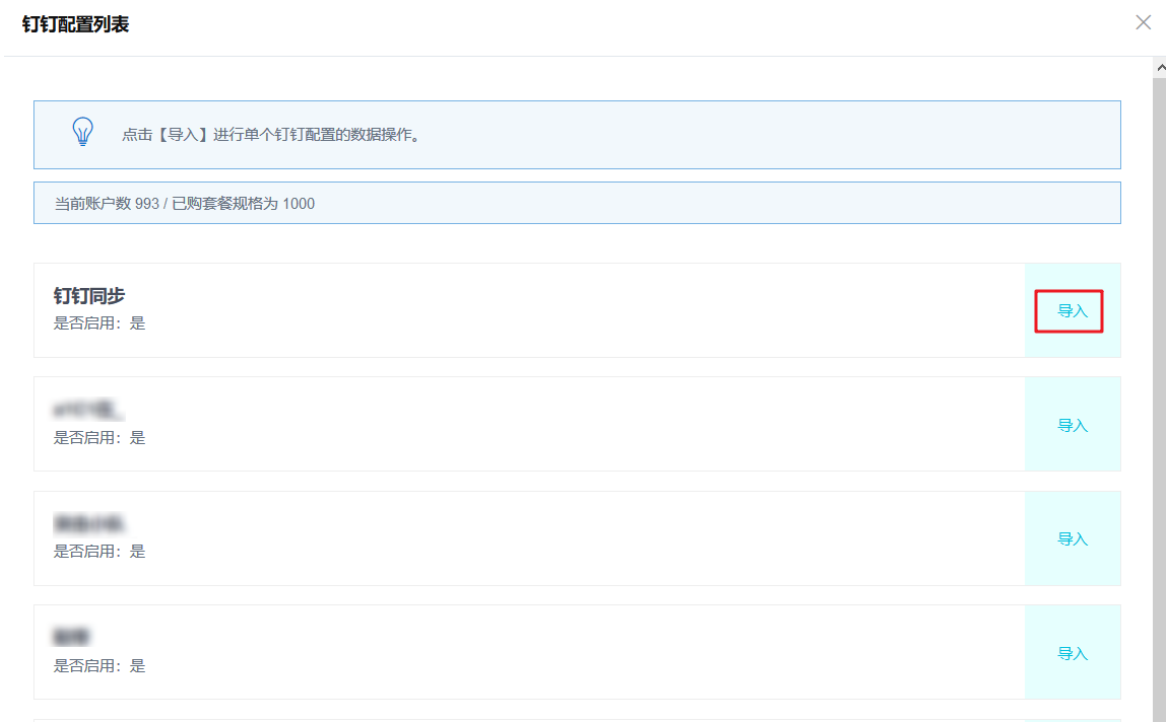
## 导入钉钉组织机构和账户数据

新建钉钉同步配置后，即可在机构及组页面全量导入钉钉的组织机构和账户数据。

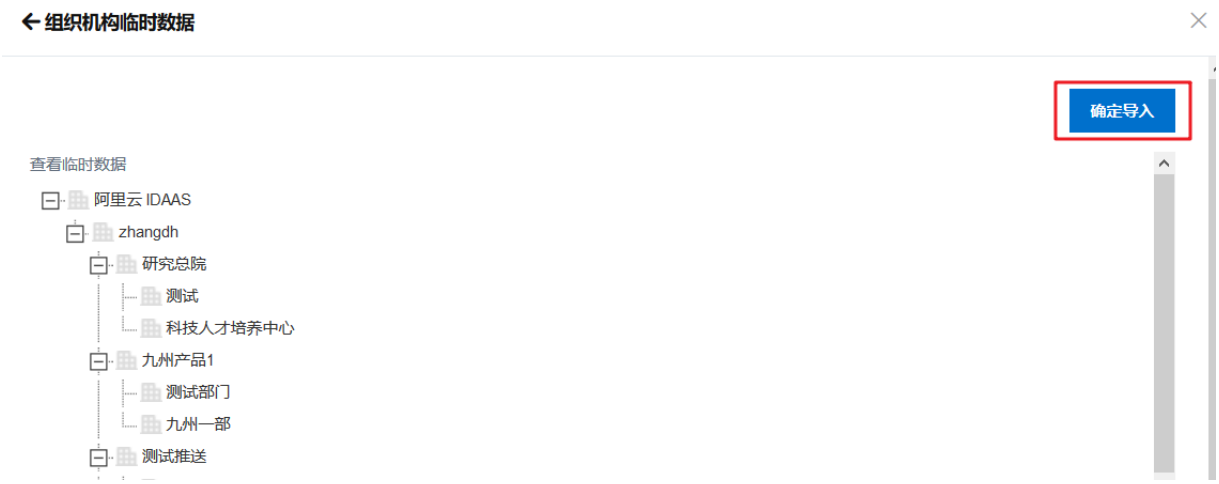
### 导入钉钉组织机构

1. 在机构及组页面，点击导入-钉钉同步-组织机构


2. 选择添加的钉钉同步配置，点击导入




3. 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，即可将钉钉的组织机构全量导入到IDaaS




**导入钉钉账户**

> **注意** 在导入钉钉账户前，请确认钉钉组织机构已导入成功，否则会导入失败。

1. 在机构及组页面，点击导入-钉钉同步-账户


2. 选择添加的钉钉同步配置，点击导入
3. 页面会展示将要导入的账户列表。


点击一键移除，将无法导入的数据移除，再点击确定导入即可将钉钉的账户数据导入到IDaaS。

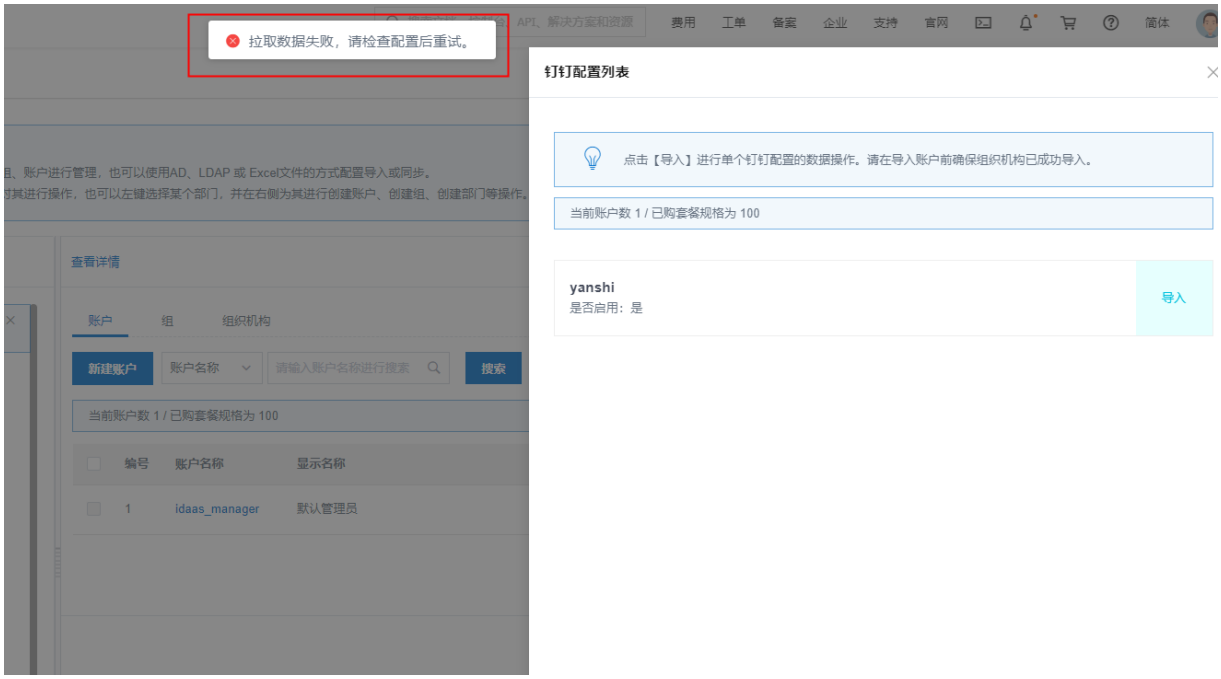
只有处理了不符合规范的数据才可以导入成功


## FAQ

**1. 拉取钉钉组织机构时，显示数据为空，看不到钉钉上的组织机构**


请查看钉钉开放平台上，添加的钉钉微应用是否填写了IDaaS的出口IP，如未填写请联系IDaaS同学获取出口IP。

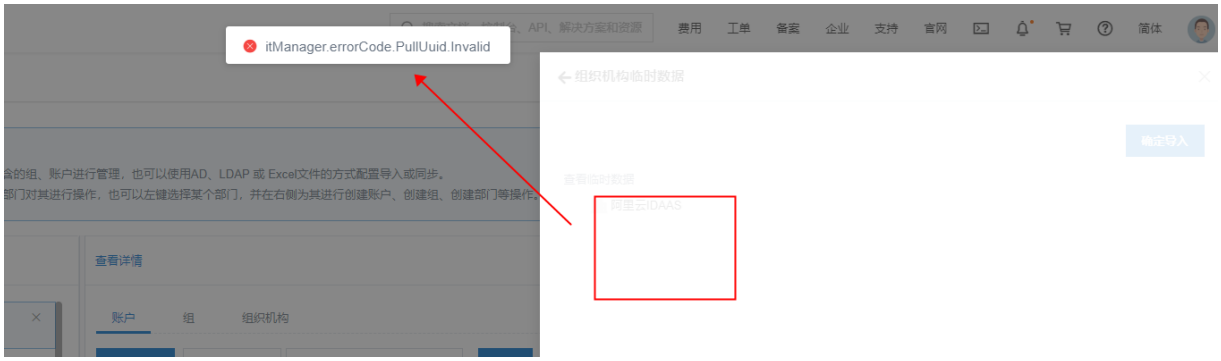
**2. 导入钉钉的账户提示：拉取数据失败，请检查配置后重试。**




2.1请检查钉钉开放平台上的接口权限是否配置正确。


2.2 请检查钉钉通讯录中是否有账户没有填写手机号


**3. 预导入组织机构页面没有显示组织机构，并且点击导入后报错：**
**itManager.errorCode.PullUuid.Invalid**




请修改授权范围是全部员工。

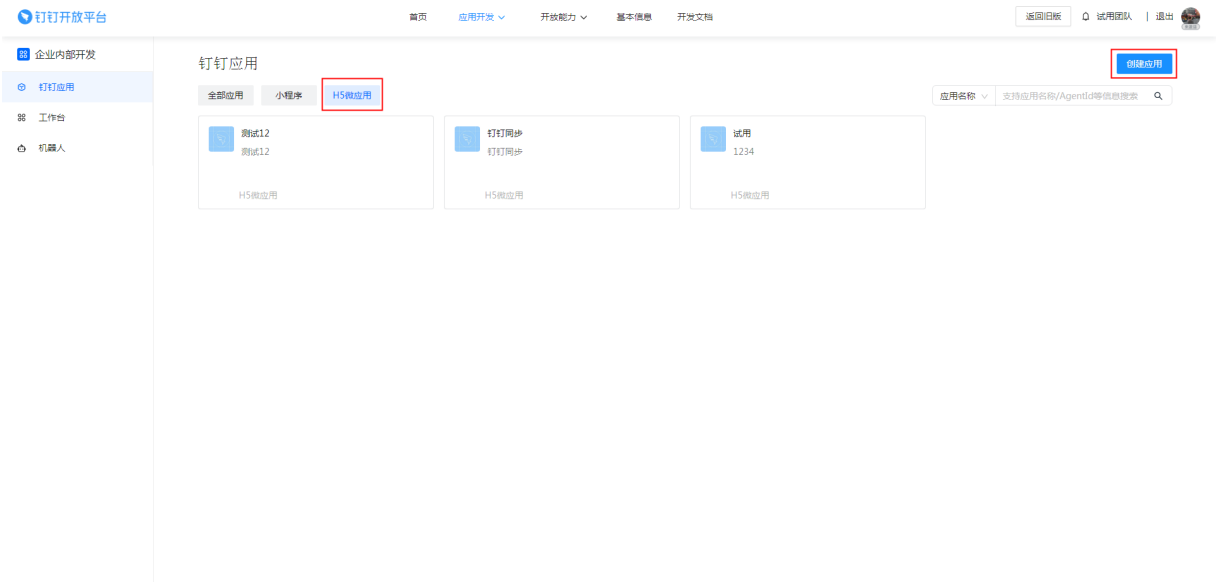

如果检查钉钉上配置没有问题， 请在钉钉上重新建一个应用，并输入IDaaS出口IP再次尝试导入。

# 3.钉钉同步数据到IDaaS（钉钉新版页面）

本文介绍如何配置钉钉同步配置，实现将钉钉组织架构数据拉取到IDaaS。将钉钉同步数据到 IDaaS，和钉钉进一步的集成打通，为钉钉客户提供到 AD 或其他身份源 的同步。

## 添加钉钉同步配置

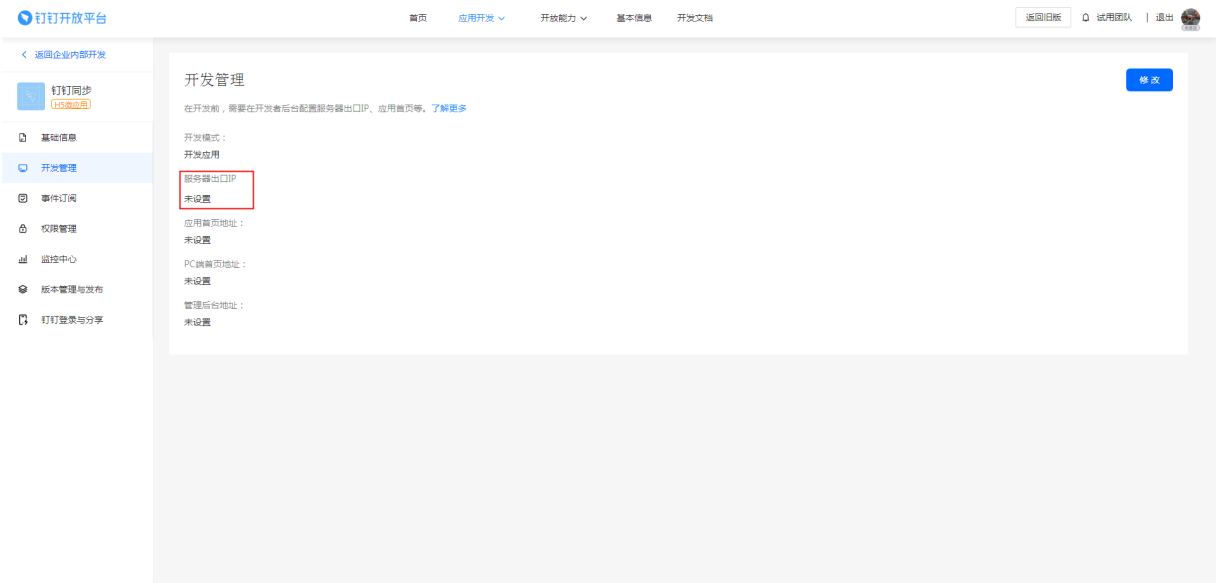
1. 在钉钉开放平台添加一个钉钉微应用，可参考创建钉钉微应用。




**注意** 请确认钉钉微应用配置的服务器出口IP为IDaaS服务器的出口IP，否则无法成功拉取到钉钉的账户/部门数据。

**说明** 如果已创建过钉钉微应用，可以直接使用现有的

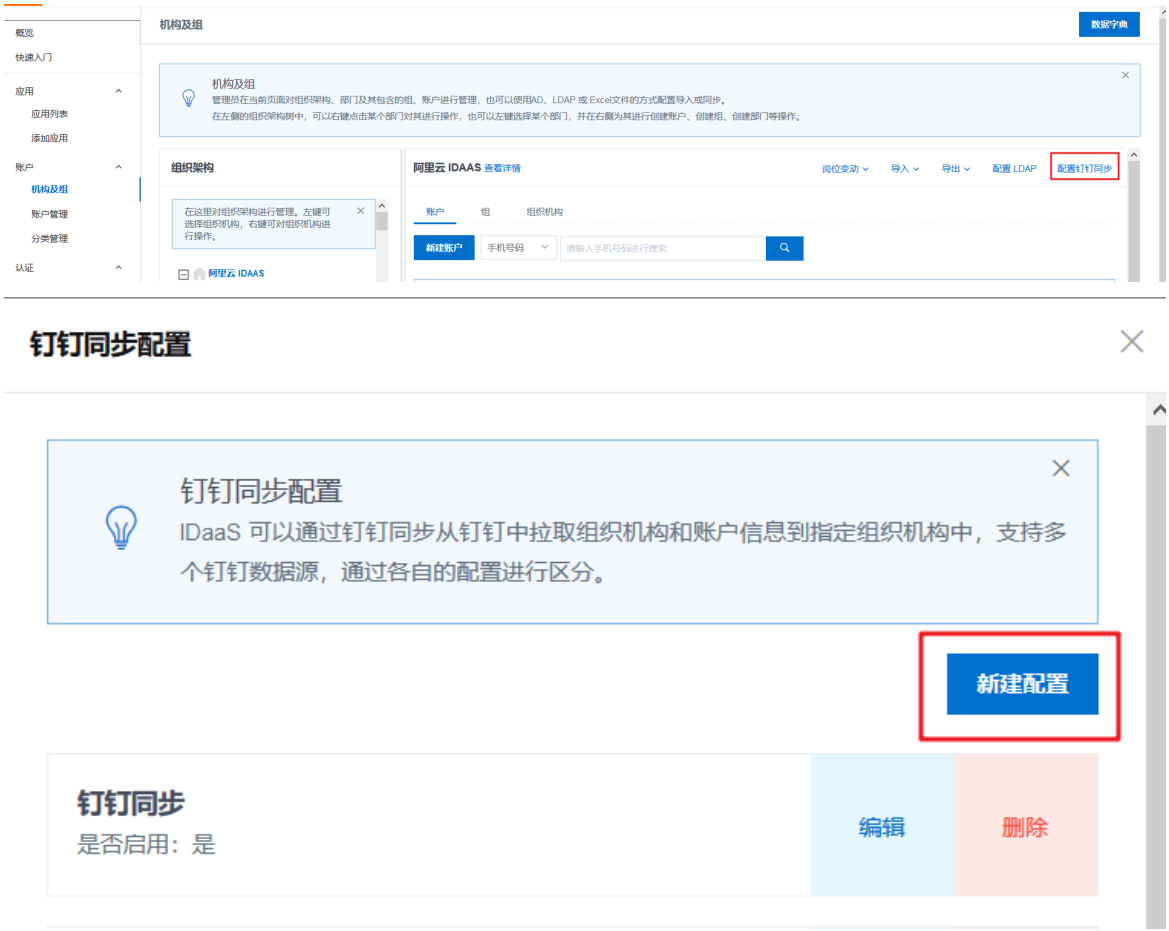
**需要确认您使用的钉钉微应用的接口权限开启了通讯录权限和手机号码信息权限，否则有可能导致无法拉取钉钉账户**



| | | | |
|---|---|---|---|
| 企业员工手机号信息 | | 已开通 | 移除权限 |
| 邮箱等个人信息 | | 已开通 | 移除权限 |
| 通讯录部门信息读权限 | 获取部门详情<br>获取指定用户的所有父部门列表<br>获取部门列表<br>获取指定部门的所有父部门列表<br>查看更多 | 已开通 | 移除权限 |
| 维护通讯录的接口访问权限 | 创建部门<br>更新部门<br>删除部门<br>更新用户信息<br>查看更多 | 已开通 | 移除权限 |
| 成员信息读权限 | 根据userid获取用户详情<br>获取部门用户userid列表<br>获取管理员列表<br>获取员工人数<br>查看更多 | 已开通 | 移除权限 |
| 根据手机号姓名获取成员信息的接口访问权限 | 根据手机号获取userid<br>根据手机号获取userid | 已开通 | 移除权限 |
| 通讯录部门成员读权限 | 获取部门用户详情<br>获取部门用户基础信息<br>获取部门用户详情<br>获取角色详情<br>查看更多 | 已开通 | 移除权限 |
| 企业外部联系人读取权限 | 获取企业外部联系人标签列表<br>获取企业外部联系人列表<br>获取企业外部联系人详情 | 已开通 | 移除权限 |
| 企业外部联系人维护权限 | 删除企业外部联系人<br>更新企业外部联系人<br>添加企业外部联系人 | 已开通 | 移除权限 |
| 调用企业API基础权限 | 更新工作通知状态栏<br>连接器事件发送<br>通过免登码获取用户信息(v2)<br>查询群消息已读人员列表<br>查看更多 | 已开通 | 默认开通 |

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. 在机构及组页面，点击配置钉钉同步，新建一个钉钉同步配置。

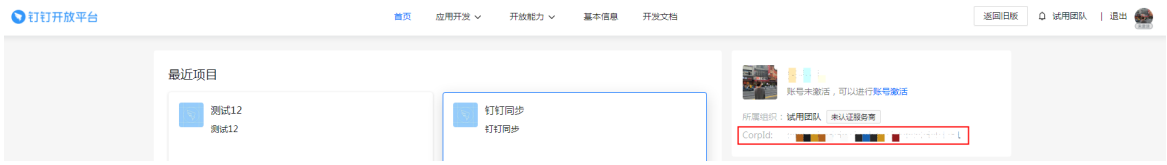




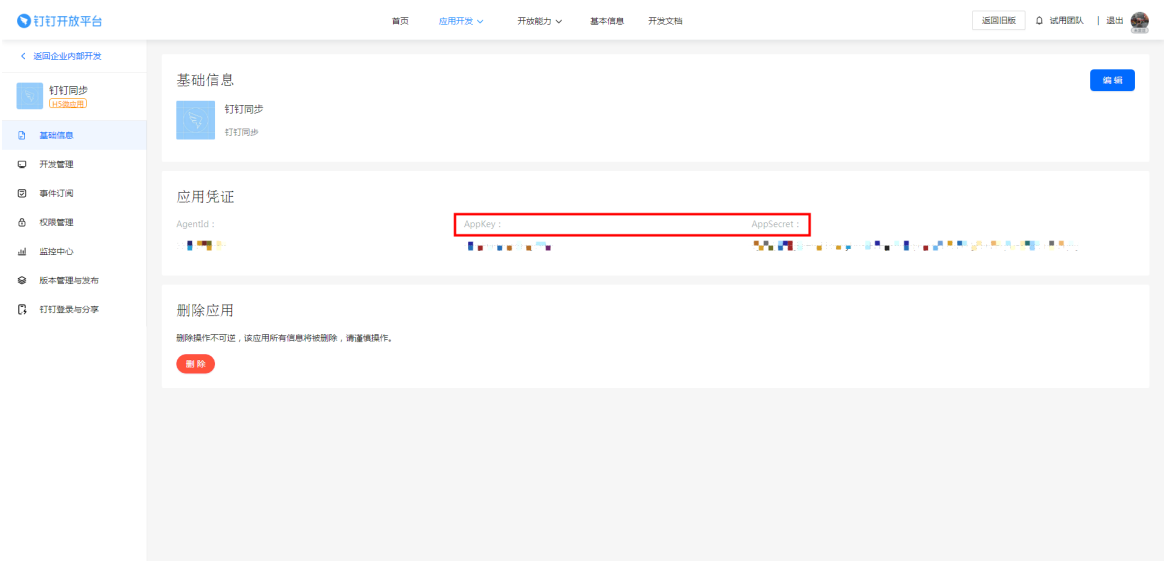


4. 填写配置参数


名称：可以随意填写，支持中文、大小写字母、数字。CorpID：登录钉钉开放平台首页展示的值。




appKey、appSecret：钉钉应用-应用详情中展示的值。




**注册回调：开启注册回调后，在钉钉OA工作台对账户和组织机构的操作会自动同步到IDaaS。**根节点：填写后，钉钉的组织机构和账户会导入到指定的组织机构下。如果不填写，则默认导入到IDaaS根目录下。密码：钉钉账户同步到IDaaS后，为账户设置的用于登录IDaaS平台的默认密码。**注意** 请确认导入的密码符合当前的密码策略，否则无法导入账户。

5. 点击测试连接，确认参数填写正确后，启用配置并点击保存

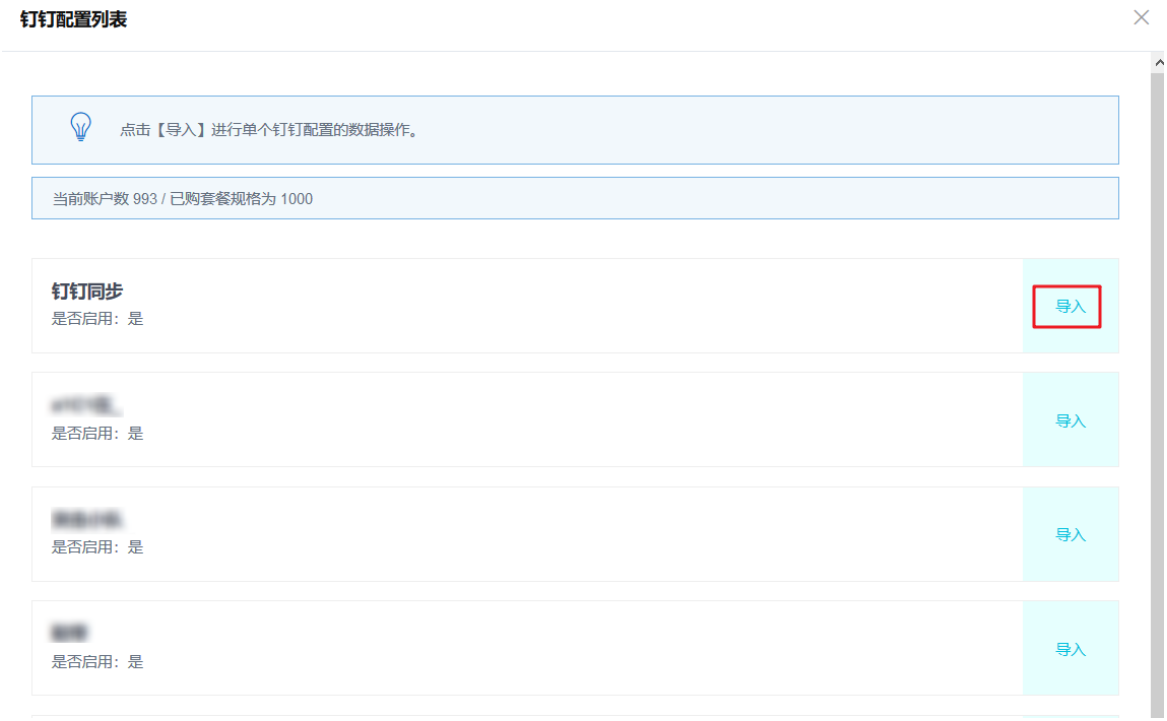
## 导入钉钉组织机构和账户数据

新建钉钉同步配置后，即可在机构及组页面全量导入钉钉的组织机构和账户数据。

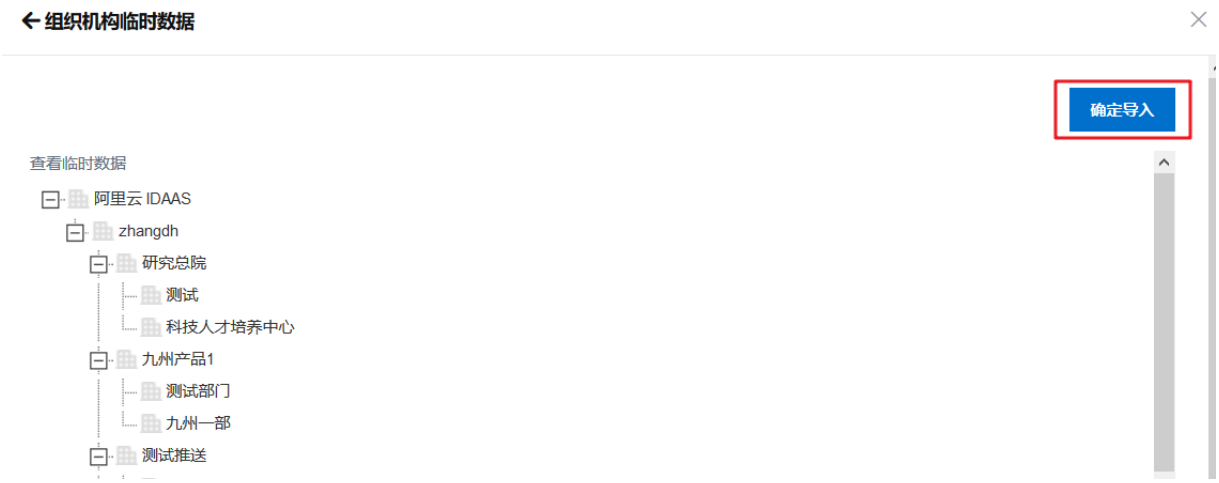
### 导入钉钉组织机构

1. 在机构及组页面，点击导入-钉钉同步-组织机构

2. 选择添加的钉钉同步配置，点击导入




3. 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，即可将钉钉的组织机构全量导入到IDaaS

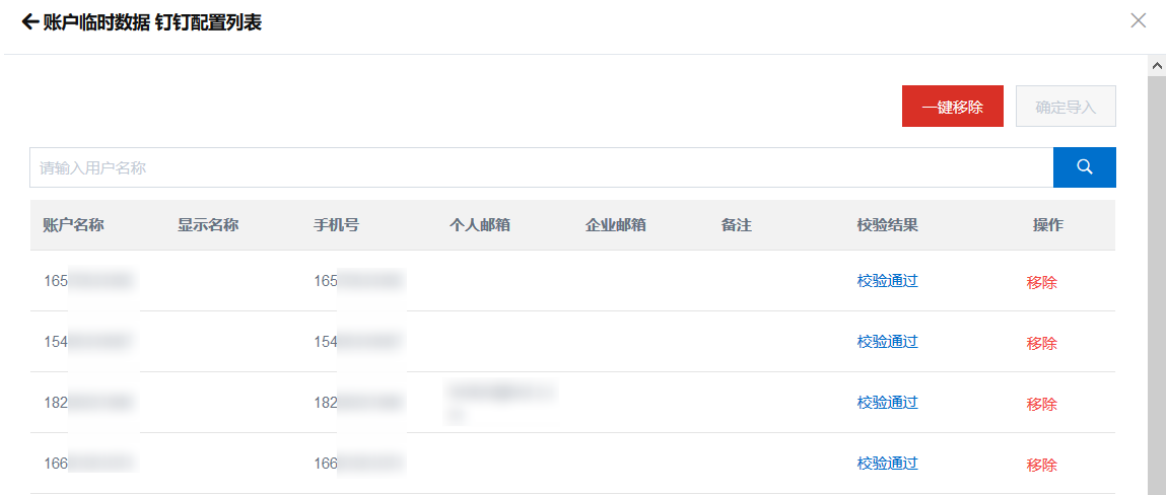



**导入钉钉账户**

**注意** 在导入钉钉账户前，请确认钉钉组织机构已导入成功，否则会导入失败。

1. 在机构及组页面，点击导入-钉钉同步-账户


2. 选择添加的钉钉同步配置，点击导入
3. 页面会展示将要导入的账户列表。



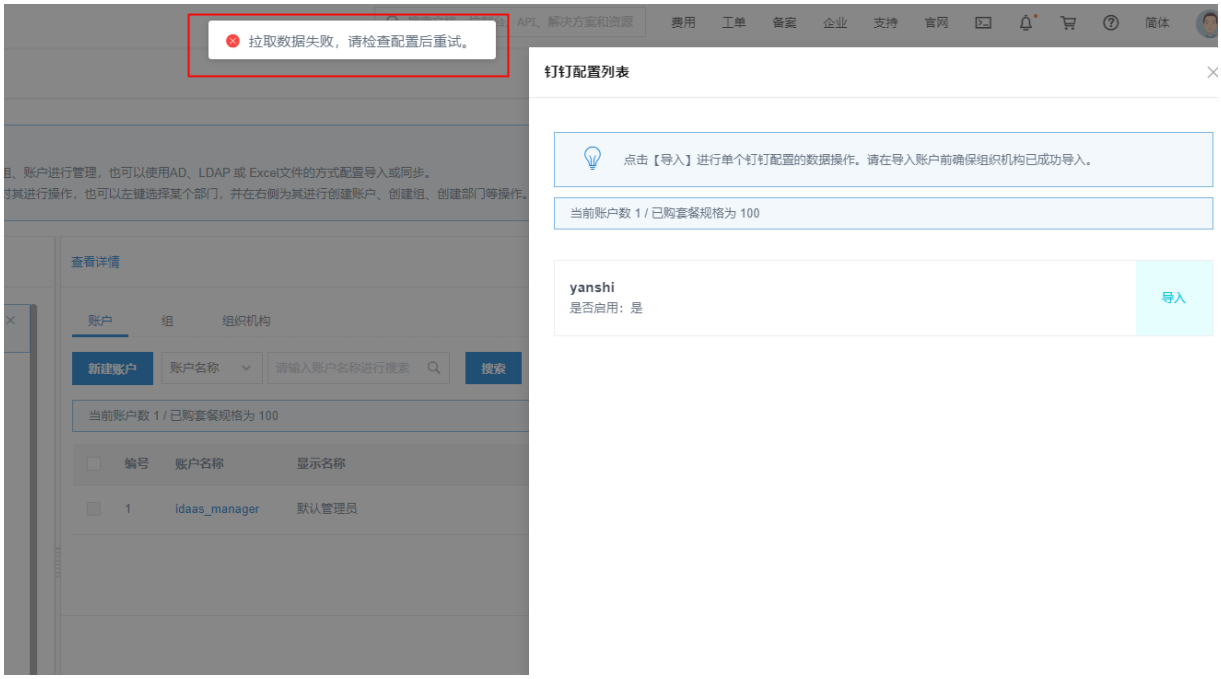

点击一键移除，将无法导入的数据移除，再点击确定导入即可将钉钉的账户数据导入到IDaaS。只有处理了不符合规范的数据才可以导入成功


## FAQ

**1. 拉取钉钉组织机构时，显示数据为空，看不到钉钉上的组织机构**


请查看钉钉开放平台上，添加的钉钉微应用是否填写了IDaaS的出口IP，如未填写请联系IDaaS同学获取出口IP。

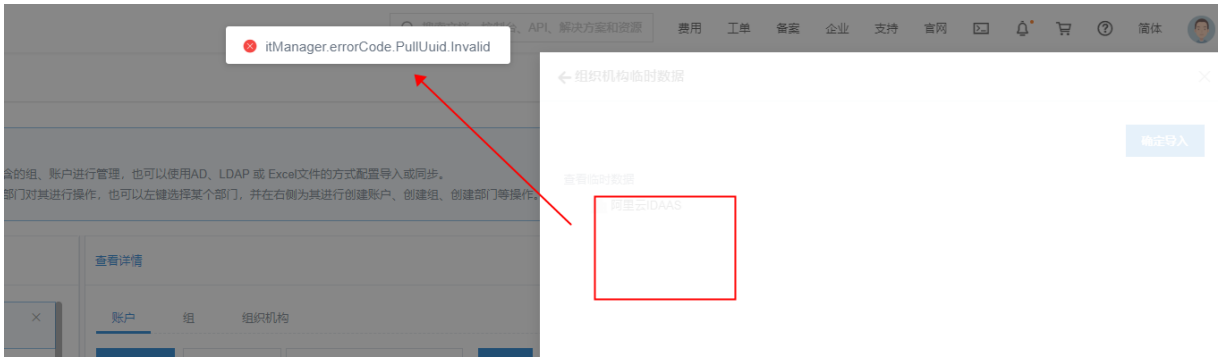
**2. 导入钉钉的账户提示：拉取数据失败，请检查配置后重试。**




2.1请检查钉钉开放平台上的接口权限是否配置正确。


2.2 请检查钉钉通讯录中是否有账户没有填写手机号


**3. 预导入组织机构页面没有显示组织机构，并且点击导入后报错：**
**itManager.errorCode.PullUuid.Invalid**




请修改授权范围是全部员工。


如果检查钉钉上配置没有问题， 请在钉钉上重新建一个应用，并输入IDaaS出口IP再次尝试导入。

# 4.IDaaS数据同步到钉钉（钉钉旧版页面）

本文介绍如何配置钉钉应用，实现将IDaaS的数据同步到钉钉。

配置钉钉同步的操作步骤主要可以分为两步：

1.在钉钉开发者平台创建一个微应用（可以使用已有的微应用）

2.在IDaaS添加钉钉应用并进行同步配置

## 在钉钉开发者平台创建微应用并获取参数

**操作步骤：**

1.登录钉钉开发平台，地址：https://open-dev.dingtalk.com

获取CorpId参数值


2.点击应用开发，选择H5微应用。点击创建应用，创建一个钉钉微应用。

> **说明** 如果已有钉钉微应用，可以使用已有的微应用，不需要进行创建。


3.选择应用，查看详情


获取应用的AppKey和AppSecret。

> **注意** 服务器出口IP可以先随意填写，后面需要替换成IDaaS服务器的出口IP，否则会同步失败。

4.点击接口权限，申请应用对通讯录的权限

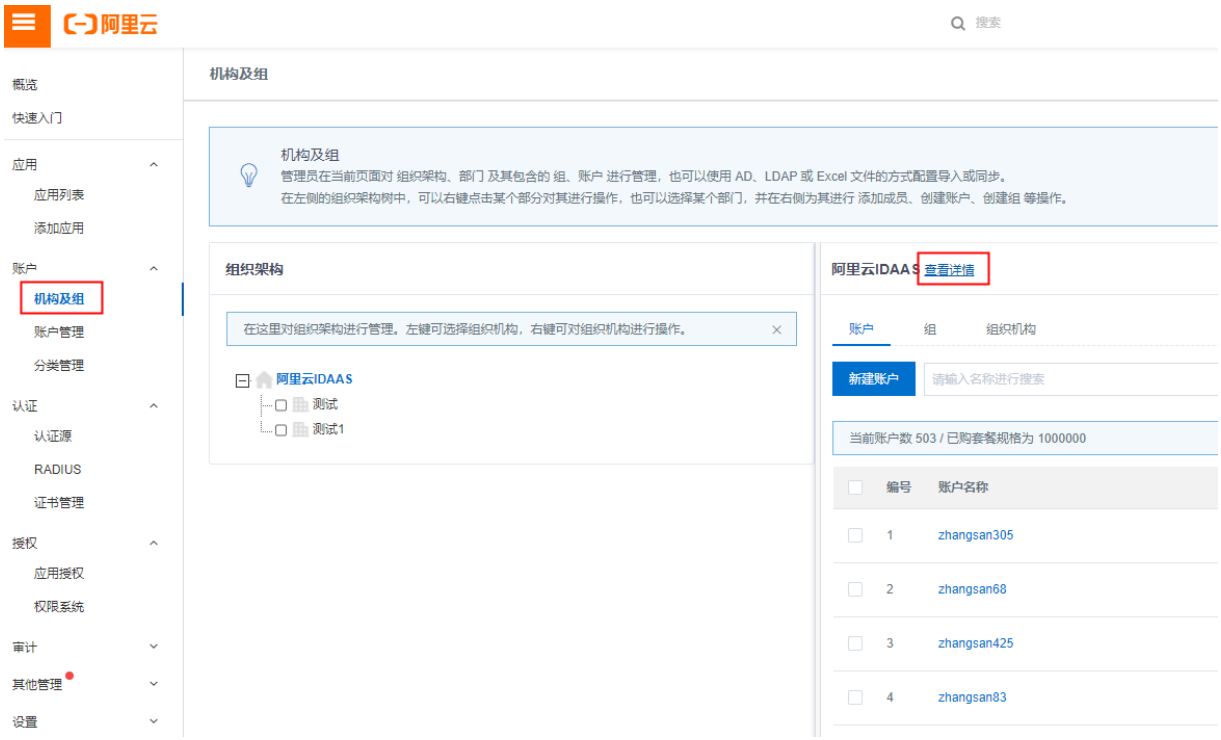

需要申请通讯录的权限后，同步才能成功。

## 在IDaaS添加钉钉应用并进行配置

### 操作步骤

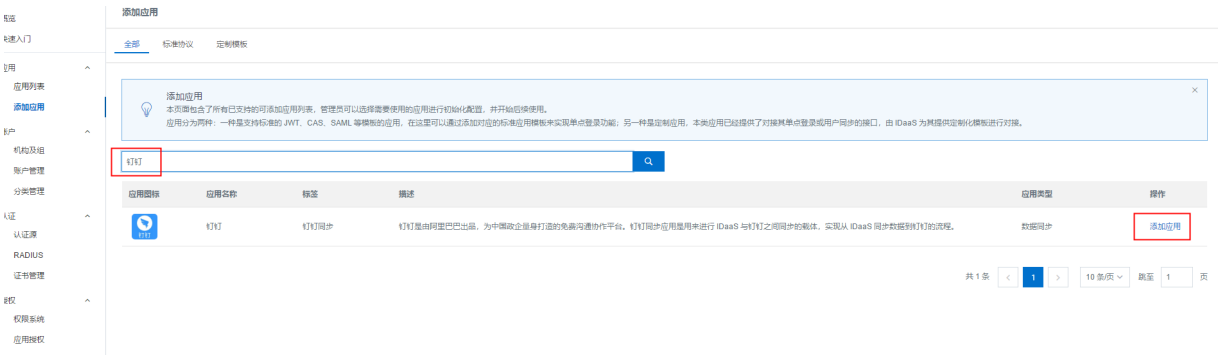
5.登录IDaaS管理员，点击机构及组。

> **说明** 添加钉钉应用前，需要先获取到 想要同步到钉钉的“根节点”机构 所对应的外部ID。




获取机构的外部ID参数


6.点击添加应用，选择钉钉



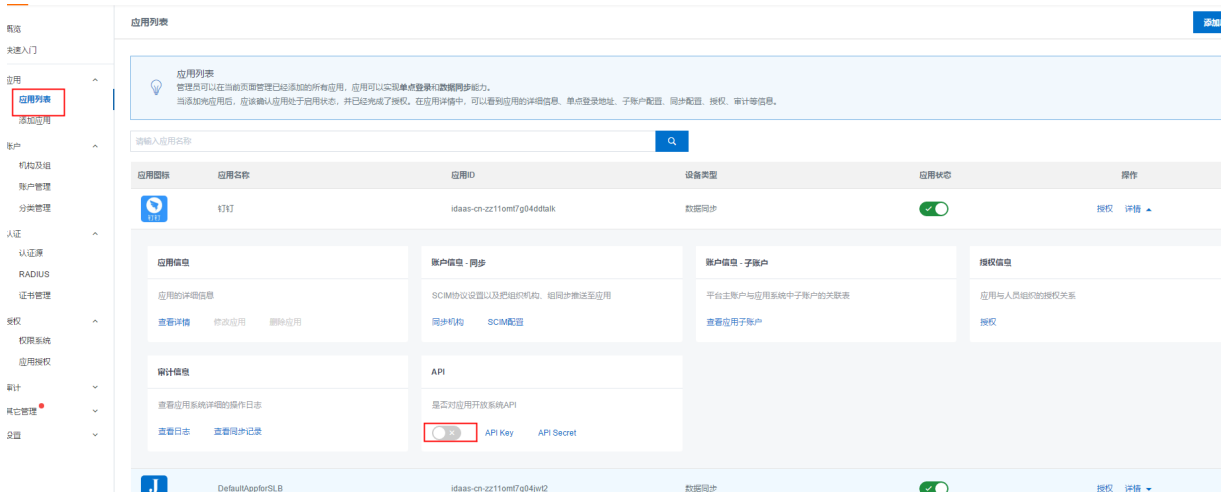

7.填写参数，保存钉钉应用


CorpId、AppKey、AppSecret为在钉钉开发者平台中获取到的参数。

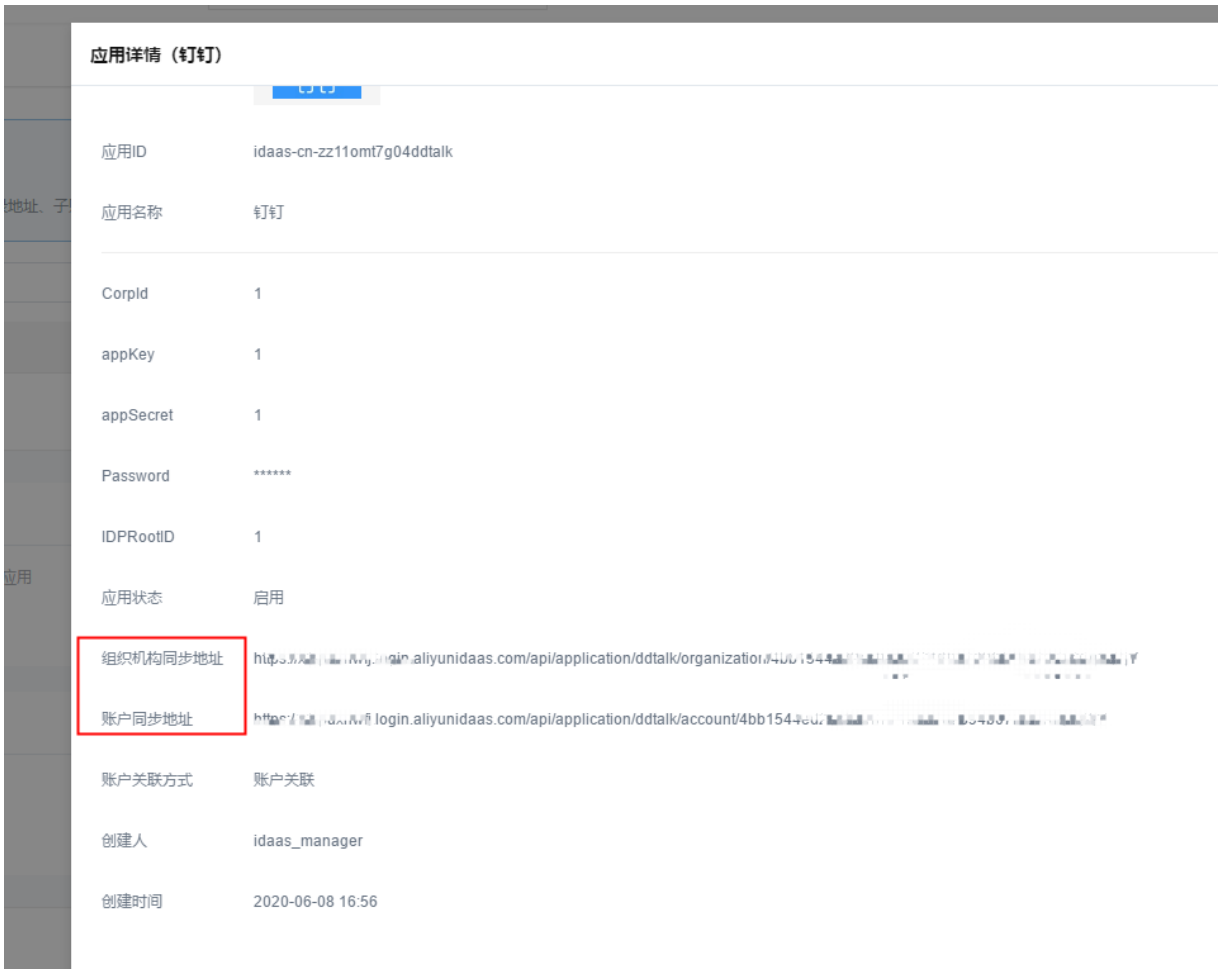
IDPRootID为上述步骤1中获取的 机构的外部ID参数的值。

账户关联方式选择账户关联。

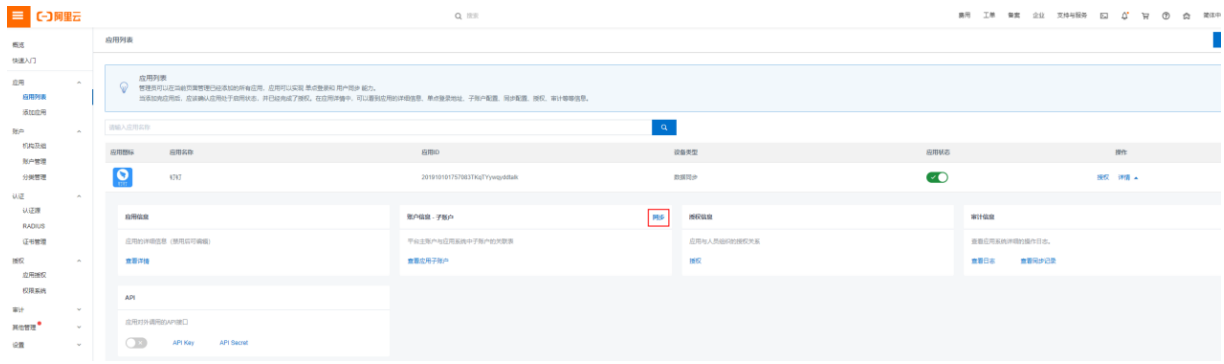
8.点击应用列表，点击详情，打开API开关，复制出APIKey和APISecret




9.点击查看详情，复制出组织机构和账户的同步地址




10.点击同步按钮



11.点击SCIM配置

12.配置SCIM


填写账户同步和组织机构同步地址，同步地址填写的是上述**步骤5**中获取的同步地址

协议类型选择OAuth2

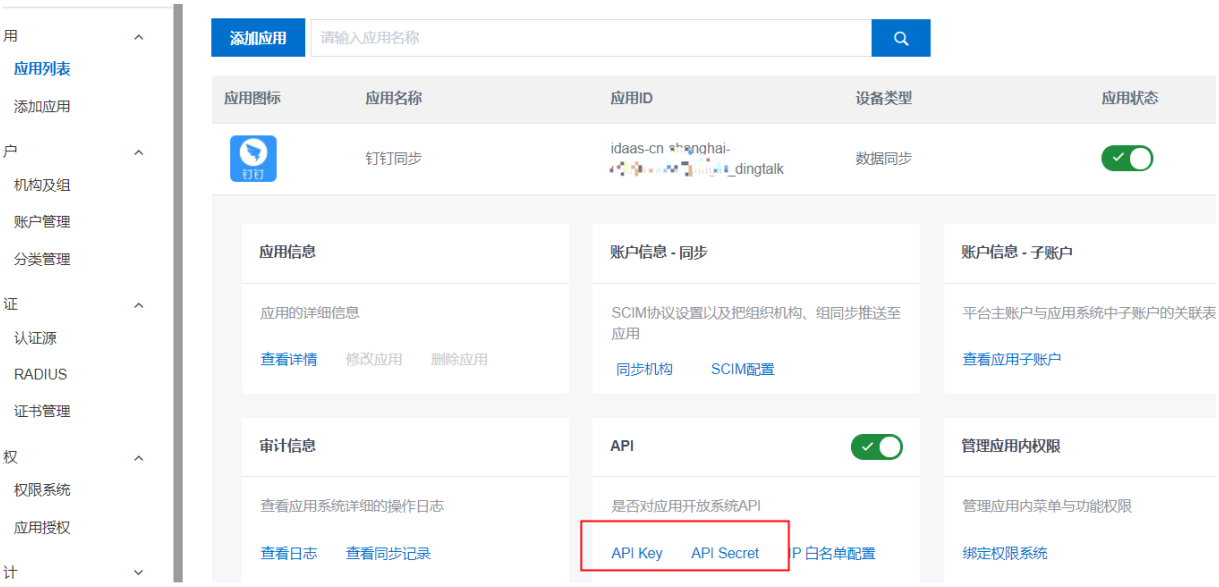
oauth url: IDaaS 用户侧的地址+/oauth/token

> **说明** IDaaS 用户侧的地址 请到云盾IDaaS控制台页面获取。如下图：则oauth url需要填写成：

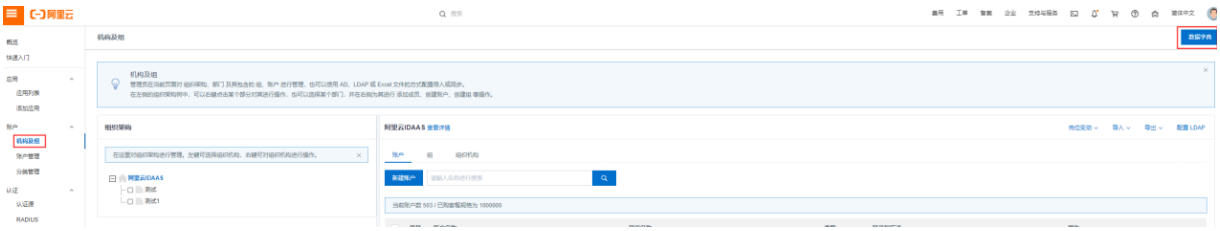

https://xxxx.login.aliyunidaas.com/oauth/token

Client_id: IDaaS应用的API Key，见下图

Client_secret： IDaaS应用的API Secret，见下图




13.点击机构及组，点击数据字典



14.添加数据字典


数据字典1：

字段名：钉钉部门ID

字段值：ddtalkId

所属分类：组织机构

字段类型：文本框

是否必填：否

是否唯一：是

数据字典2：

字段名：钉钉人员ID

字段值：ddAccountId

所属分类：账户

字段类型：文本框

是否必填：否

是否唯一：是

通过以上步骤，完成钉钉同步的配置。现在在IDaaS中新增修改删除组织机构和账户都会增量同步到钉钉应用。


备注：新增账户时，必须填写手机号才可同步成功。

## 常见问题

Q：配置完成后，同步机构或账户提示同步失败，同步结果显示如下：服务器返回错误码:60020错误信息:请参考FAQ：https://open-doc.dingtalk.com/microapp/faquestions/cvbtph。错误原因：访问ip不在白名单之中,request ip=xxx.xxx.xxx.xxx appKey(dingbkmqsdymhczxxmx8)，如何解决？

A：失败原因是钉钉会检查发送请求的IP是否在对应钉钉微应用的服务器出口IP中，需要把上述的请求IP地址加入到对应钉钉微应用的服务器出口IP配置中。

Q：配置完成后，同步机构或账户提示同步失败，同步结果显示如下：服务器返回错误码:40066错误信息:不合法的部门列表，如何解决？

A：请检查需要同步的机构是否在正确的机构下（即是否在创建钉钉应用所填写的IDPRootID对应的组织机构下）。 如果是同步过去一个机构后，在该机构下创建的机构和用户同步失败，请检查文档 **步骤14的数据字典是否添加。**

# 5.IDaaS数据同步到钉钉（钉钉新版页面）

本文介绍如何配置钉钉应用，实现将IDaaS的数据同步到钉钉。

配置钉钉同步的操作步骤主要可以分为两步：

1.在钉钉开发者平台创建一个微应用（可以使用已有的微应用）

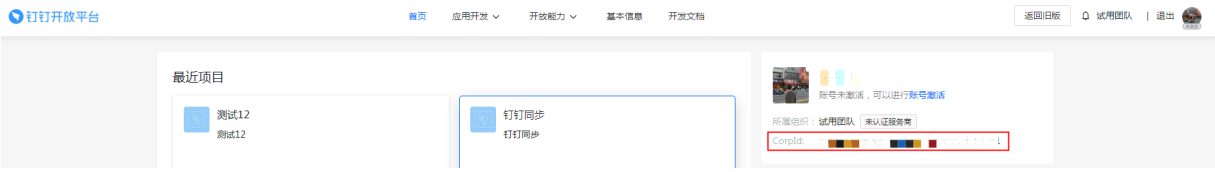
2.在IDaaS添加钉钉应用并进行同步配置

## 在钉钉开发者平台创建微应用并获取参数

**操作步骤：**

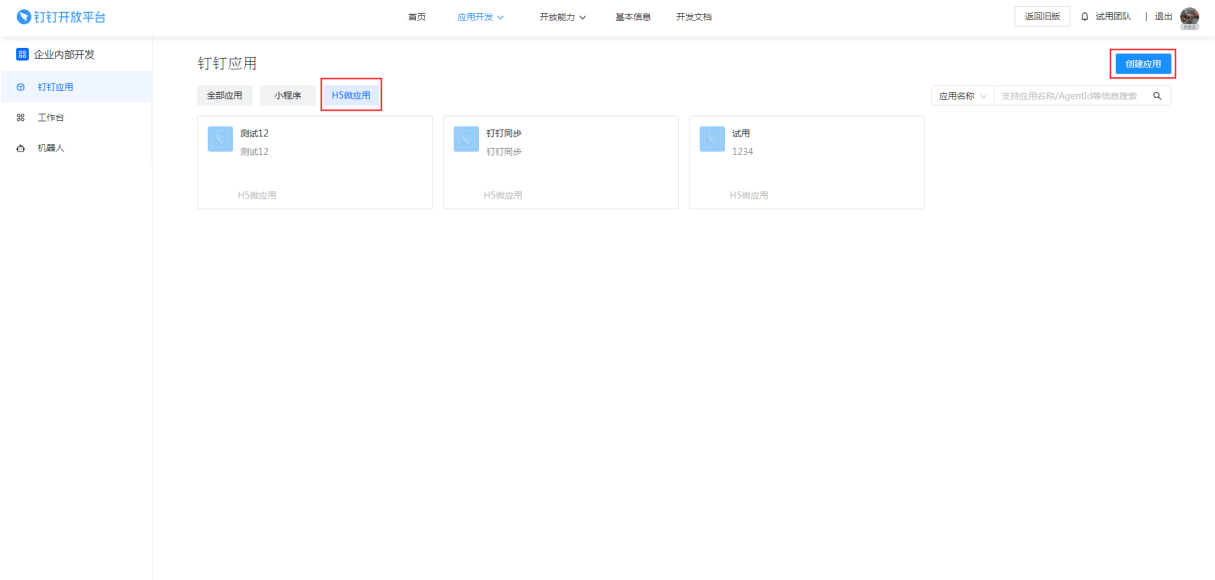
1.登录钉钉开发平台，地址：https://open-dev.dingtalk.com

获取CorpId参数值

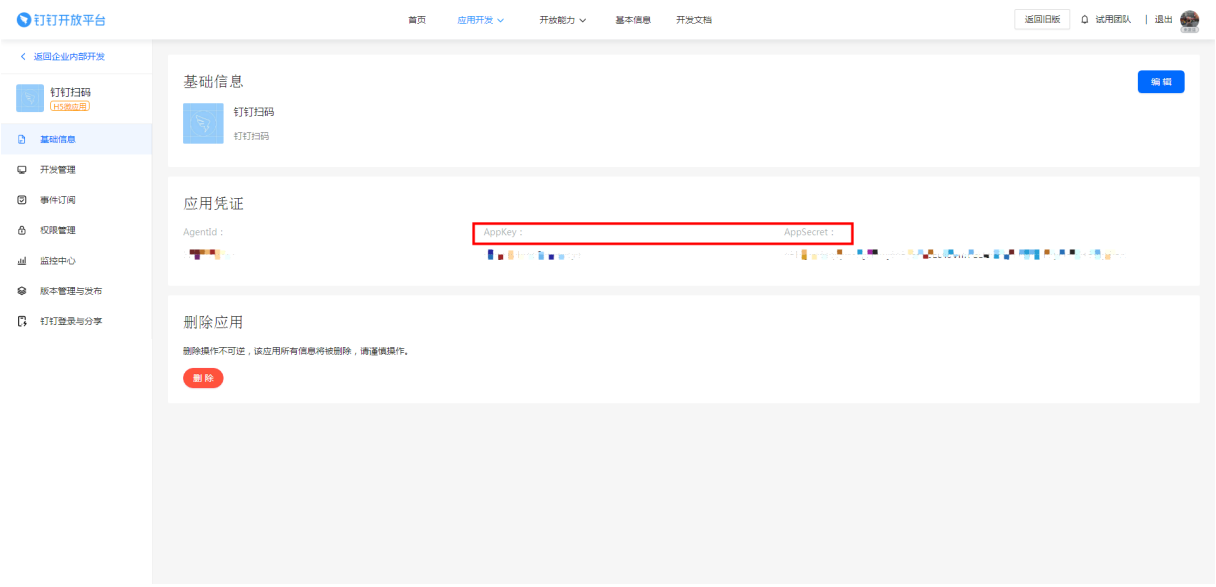



2.点击应用开发，选择H5微应用。点击创建应用，创建一个钉钉微应用。

**说明** 如果已有钉钉微应用，可以使用已有的微应用，不需要进行创建。




3.选择应用，查看详情




获取应用的AppKey和AppSecret。

**注意** 服务器出口IP可以先随意填写，后面需要替换成IDaaS服务器的出口IP，否则会同步失败。

4.点击权限管理，申请应用对通讯录的权限

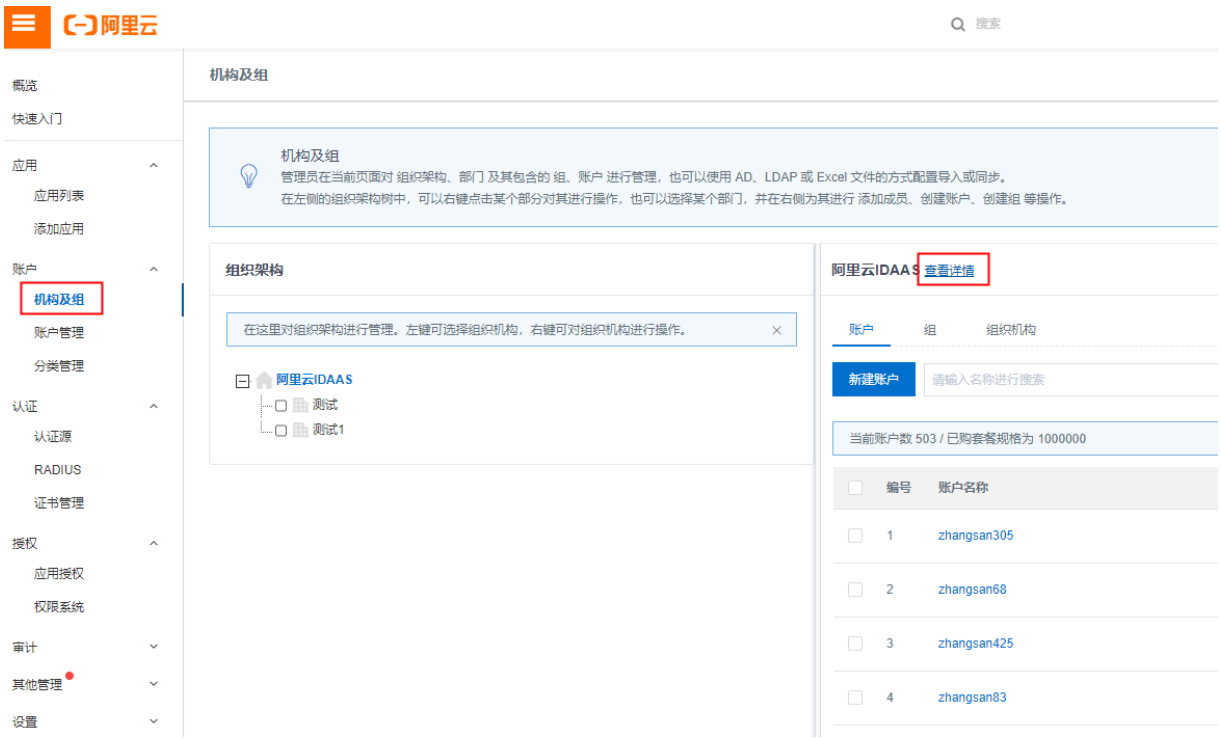
| | | | |
|---|---|---|---|
| 通讯录部门信息读权限 | 获取部门详情<br>获取指定用户的所有父部门列表<br>获取部门列表<br>获取指定部门的所有父部门列表<br>查看更多 | 已开通 | 移除权限 |
| 维护通讯录的接口访问权限 | 创建部门<br>更新部门<br>删除部门<br>更新用户信息<br>查看更多 | 已开通 | 移除权限 |
| 成员信息读权限 | 根据userid获取用户详情<br>获取部门用户userid列表<br>获取管理员列表<br>获取员工人数<br>查看更多 | 已开通 | 移除权限 |
| 通讯录部门成员读权限 | 获取部门用户详情<br>获取部门用户基础信息<br>获取部门用户详情<br>获取角色详情<br>查看更多 | 已开通 | 移除权限 |
| 企业外部联系人读取权限 | 获取企业外部联系人标签列表<br>获取企业外部联系人列表<br>获取企业外部联系人详情 | 已开通 | 移除权限 |
| 企业外部联系人维护权限 | 删除企业外部联系人<br>更新企业外部联系人<br>添加企业外部联系人 | 已开通 | 移除权限 |
| 通讯录基本数据读权限 | 获取企业最新钉钉指数信息<br>获取企业邀请信息 | 已开通 | 移除权限 |
| 调用企业API基础权限 | 更新工作通知状态栏<br>连接器事件发送<br>通过免登码获取用户信息(v2)<br>查询群消息已读人员列表<br>查看更多 | 已开通 | 默认开通 |

需要申请通讯录的权限后，同步才能成功。

## 在IDaaS添加钉钉应用并进行配置

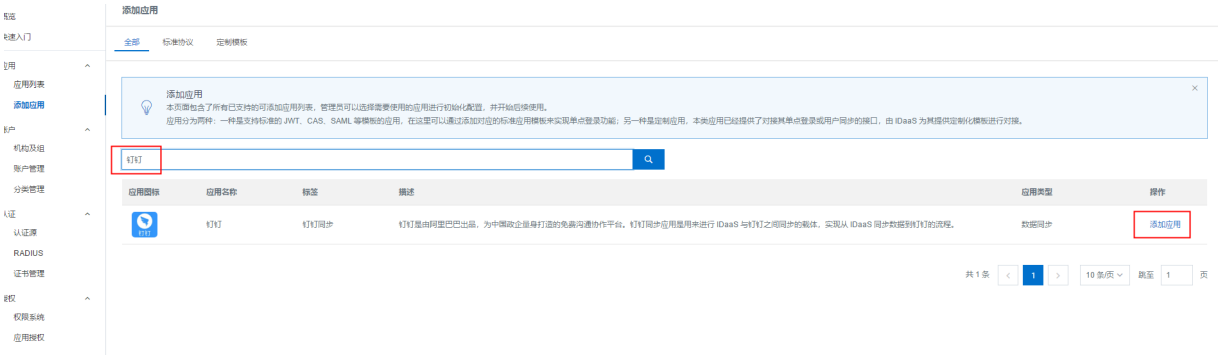
5.登录IDaaS管理员，点击机构及组。

**说明** 添加钉钉应用前，需要先获取到 需要同步到钉钉的“根节点”机构 所对应的外部ID。

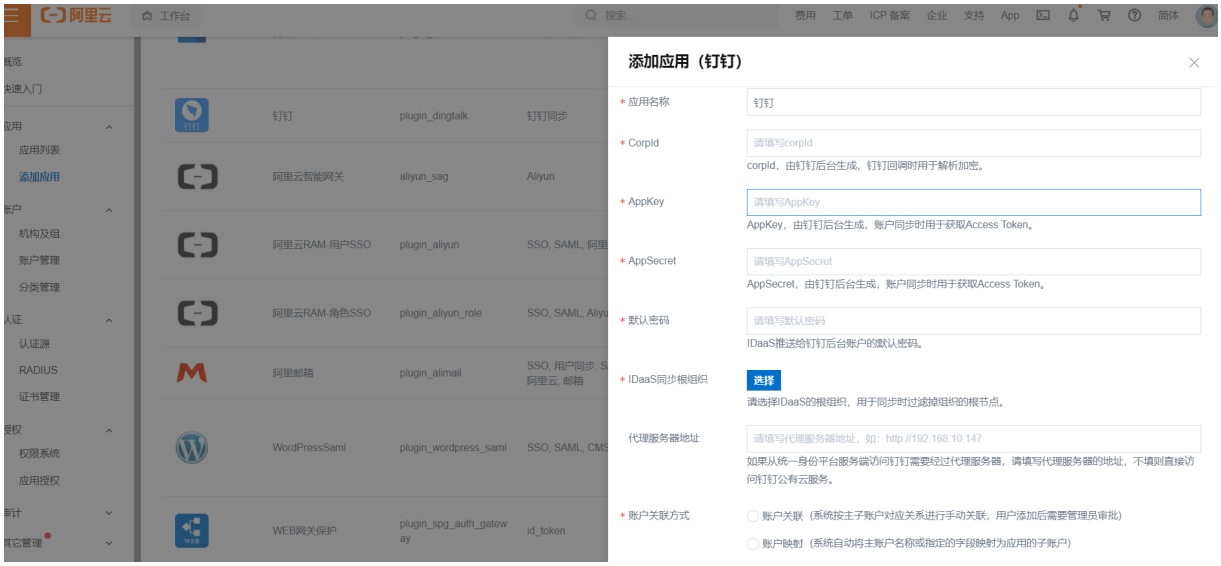



获取机构的外部ID参数


6.点击添加应用，选择钉钉




7.填写参数，保存钉钉应用

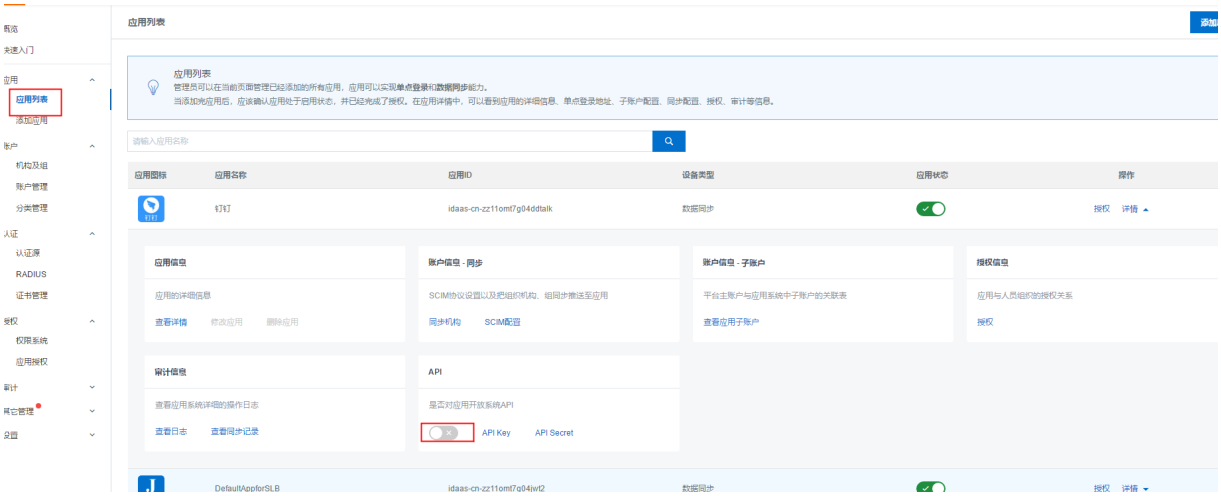



CorpId、AppKey、AppSecret为在钉钉开发者平台中获取到的参数。

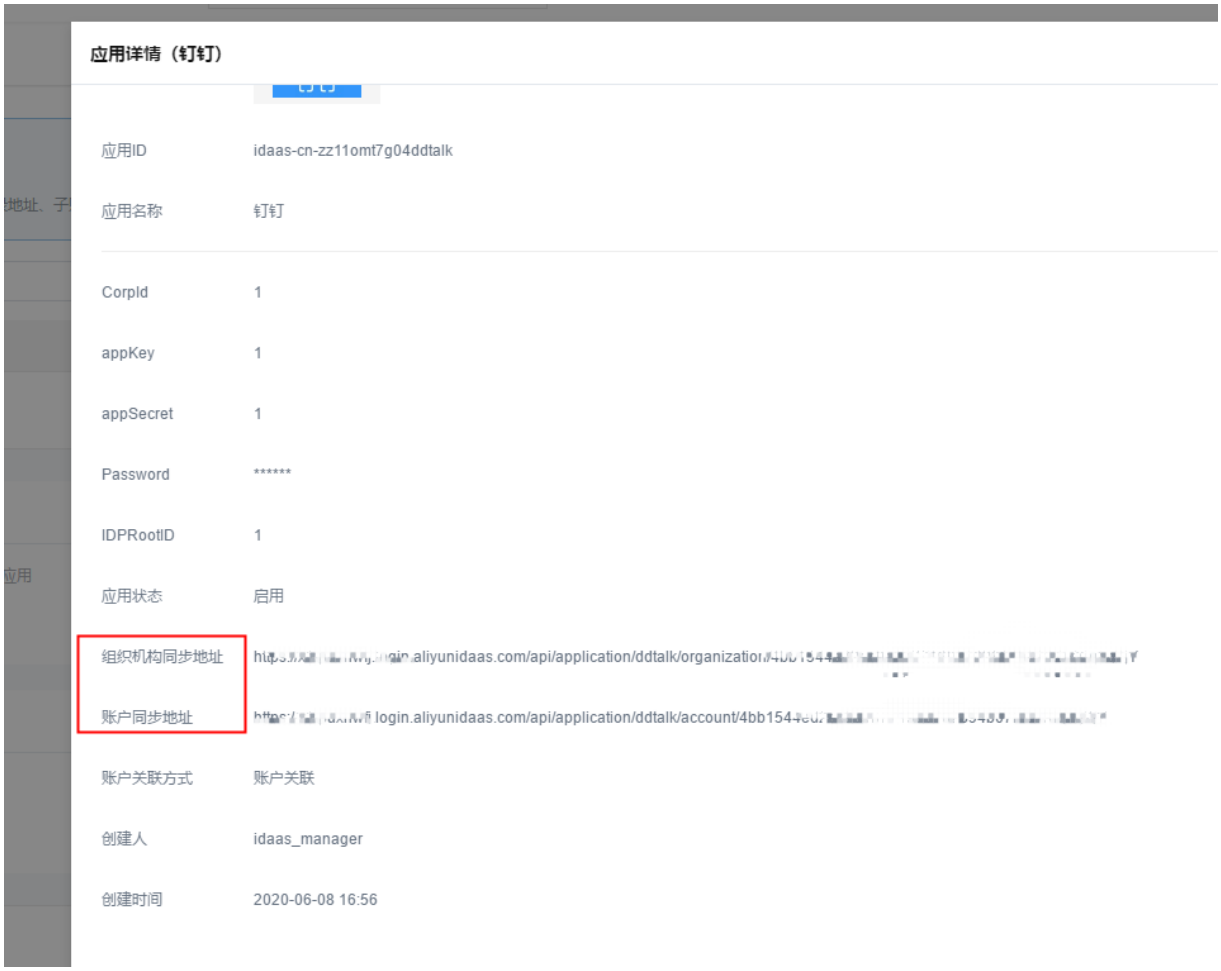
IDaaS同步根组织选择将钉钉数据同步至IDaaS的节点，请查看步骤5。

账户关联方式选择账户关联。

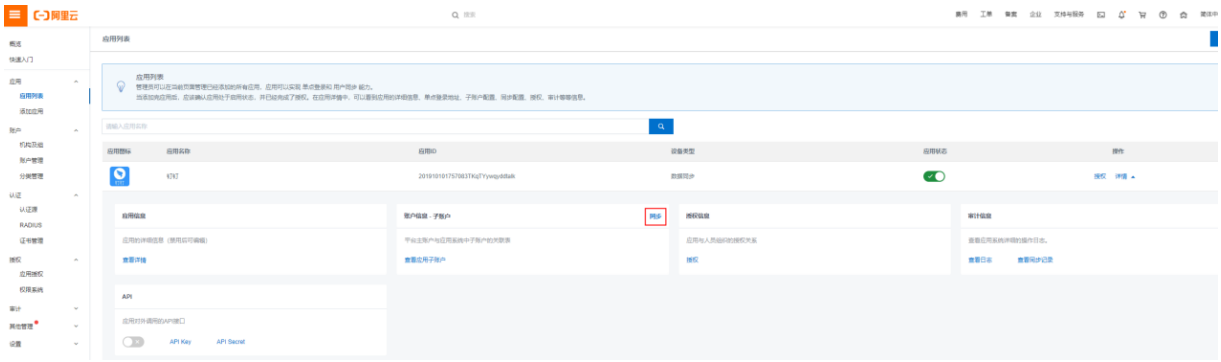
8.点击应用列表，点击详情，打开API开关，复制出APIKey和APISecret




9.点击查看详情，复制出组织机构和账户的同步地址




10.点击同步按钮



11.点击SCIM配置

12.配置SCIM


填写账户同步和组织机构同步地址，同步地址填写的是上述步骤9中获取的同步地址

协议类型选择OAuth2

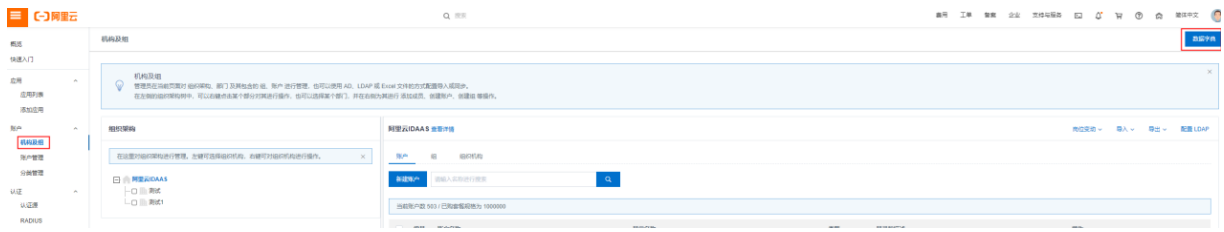
oauth url: IDaaS 用户侧的地址+/oauth/token

**说明** IDaaS 用户侧的地址 请到云盾IDaaS控制台页面获取。如下图：则oauth url需要填写成：https://xxxx.login.aliyunidaas.com/oauth/token


Client_id: IDaaS应用的API Key，见步骤8

Client_secret：IDaaS应用的API Secret，见步骤8

13.点击机构及组，点击数据字典



14.添加数据字典


数据字典1：

字段名：钉钉部门ID

字段值：ddtalkId

所属分类：组织机构

字段类型：文本框

是否必填：否

是否唯一：是

数据字典2：

字段名：钉钉人员ID

字段值：ddAccountId

所属分类：账户

字段类型：文本框

是否必填：否

是否唯一：是

通过以上步骤，完成钉钉同步的配置，在IDaaS中新增/修改/删除组织机构和账户都会增量同步到钉钉应用。


备注：新增账户时，必须填写手机号才可同步成功。

## 常见问题

Q：配置完成后，同步机构或账户提示同步失败，同步结果显示如下：服务器返回错误码:60020错误信息:请参考FAQ：https://open-doc.dingtalk.com/microapp/faquestions/cvbtph。

错误原因：访问ip不在白名单之中,request ip=xxx.xxx.xxx.xxx appKey(dingbkmqsdymhczxxmx8)，解决方案如下：

A：失败原因是钉钉会检查发送请求的IP是否在对应钉钉微应用的服务器出口IP中，需要把上述的请求IP地址加入到对应钉钉微应用的服务器出口IP配置中。

Q：配置完成后，同步机构或账户提示同步失败，同步结果显示如下：服务器返回错误码:40066错误信息:不合法的部门列表，如何解决？

A：请检查需要同步的机构是否在正确的机构下（即是否在创建钉钉应用所填写的IDPRootID对应的组织机构下）。 如果是同步过去一个机构后，在该机构下创建的机构和用户同步失败，请检查文档 步骤14的数据字典是否添加。

# 6.钉钉扫码登录

本文为您介绍如何配置钉钉扫码认证源。配置完成后，您可以通过钉钉扫码的方式，直接登录IDaaS平台。

## 背景信息

云盾IDaaS平台支持公司成员使用多种外部认证源登录。IT管理员可以根据公司需要，添加并启用不同的认证方式，例如DB、LDAP、钉钉扫码、OTP验证码登录等。钉钉作为常用的办公软件，以钉钉作为外部认证源，通过钉钉扫码的方式可以更加灵活、方便地登录到IDaaS。

配置钉钉扫码认证源的操作步骤主要分为两步：

1. 在钉钉开发者平台添加微应用并配置扫码登录
2. 在IDaaS平台创建钉钉扫码认证源

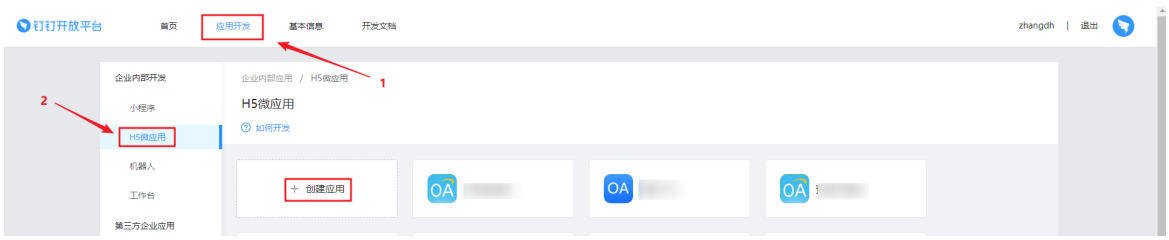
完成以上两步，即可实现使用钉钉扫码登录到IDaaS

## 在钉钉开发者平台添加微应用并配置扫码登录

1. 登录钉钉开发平台，地址：https://open-dev.dingtalk.com
2. 登录成功后，在首页获取CorpId参数


3. 点击应用开发，在左侧导航栏中选择H5微应用，创建一个钉钉微应用

> 说明 如果已创建过H5微应用，可以直接使用现有的。

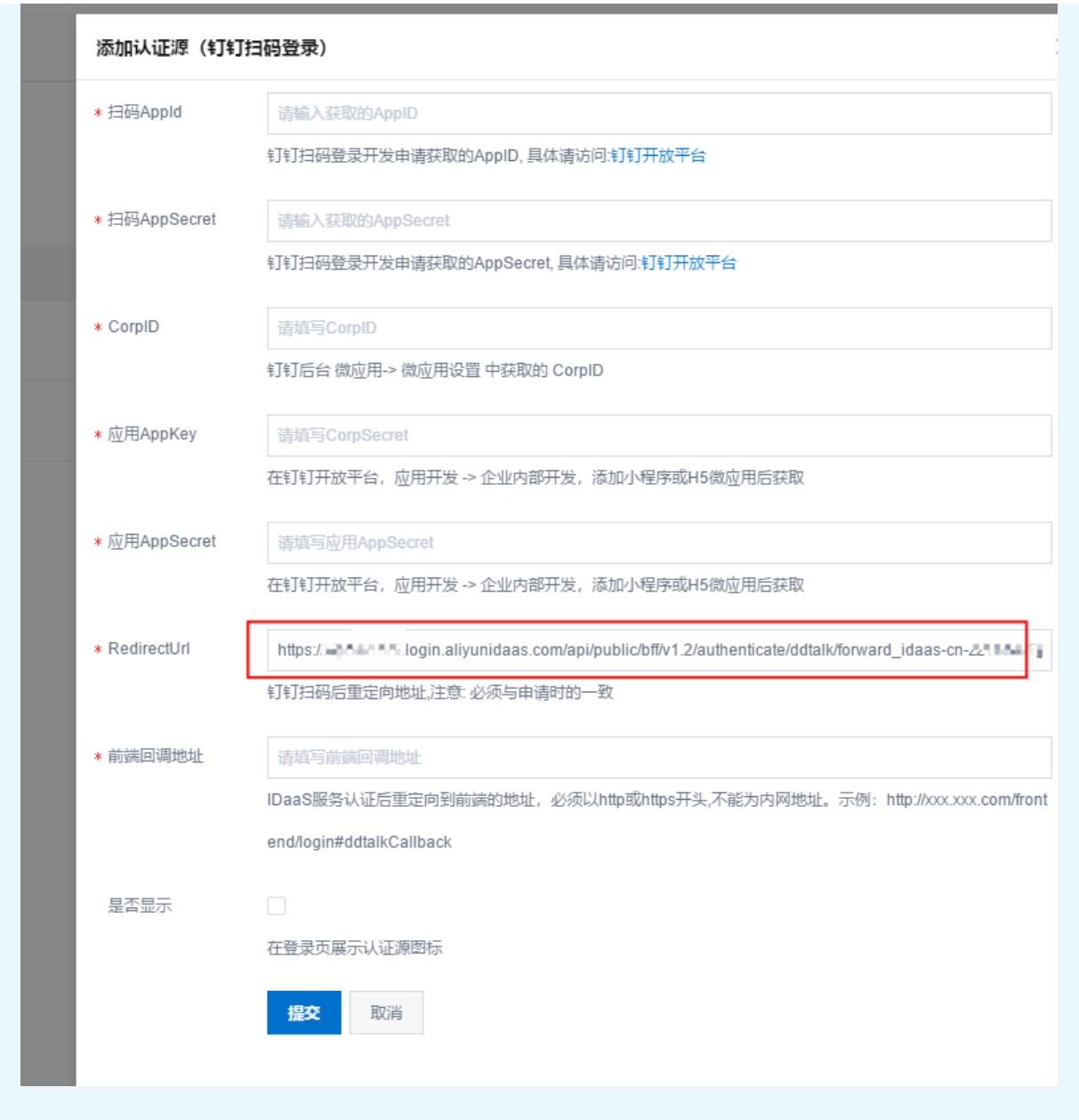



4. 创建完成后，点击应用图标。查看应用详情，获取AppKey和AppSecret参数。


5. 在左侧导航栏中点击移动应用接入-登录，然后点击创建扫码登录应用授权

6. 创建扫码登录应用授权的必填参数中，名称、描述可以随便填写，授权logo地址和回调域名需要填写IDaaS里面的RedirectUrl的地址。

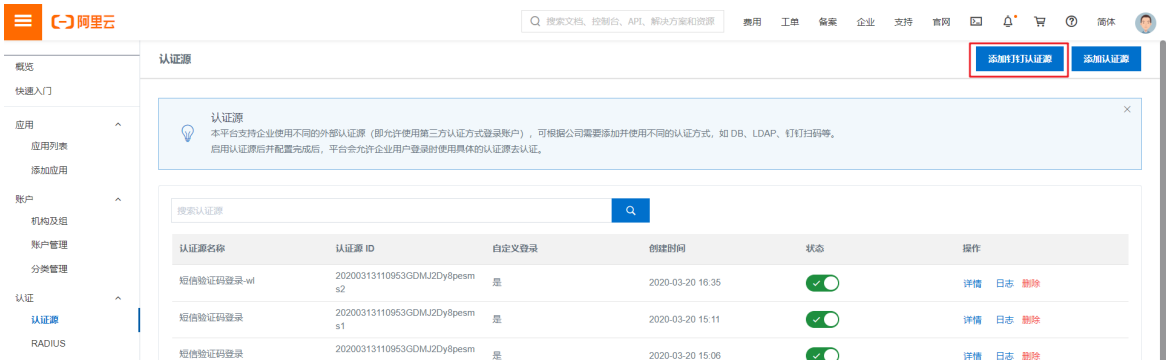
> **说明** 管理员在IDaaS平台新建钉钉扫码认证源时，会自动生成并展示RedirectUrl参数。直接将页面展示的RedirectUrl参数复制粘贴到对应位置即可。


添加认证源（钉钉扫码登录）
* 扫码AppId
请输入获取的AppID
钉钉扫码登录开发申请获取的AppID, 具体请访问:钉钉开放平台
* 扫码AppSecret
请输入获取的AppSecret
钉钉扫码登录开发申请获取的AppSecret, 具体请访问:钉钉开放平台
* CorpID
请填写CorpID
钉钉后台 微应用-> 微应用设置 中获取的 CorpID
* 应用AppKey
请填写CorpSecret
在钉钉开放平台，应用开发 -> 企业内部开发，添加小程序或H5微应用后获取
* 应用AppSecret
请填写应用AppSecret
在钉钉开放平台，应用开发 -> 企业内部开发，添加小程序或H5微应用后获取
* RedirectUrl
https:/ login.aliyunidaas.com/api/public/bff/v1.2/authenticate/ddtalk/forward_idaas-cn-
钉钉扫码后重定向地址,注意: 必须与申请时的一致
* 前端回调地址
请填写前端回调地址
IDaaS服务认证后重定向到前端的地址，必须以http或https开头,不能为内网地址。示例：http://xxx.xxx.com/front
end/login#ddtalkCallback
是否显示
在登录页展示认证源图标
提交
取消

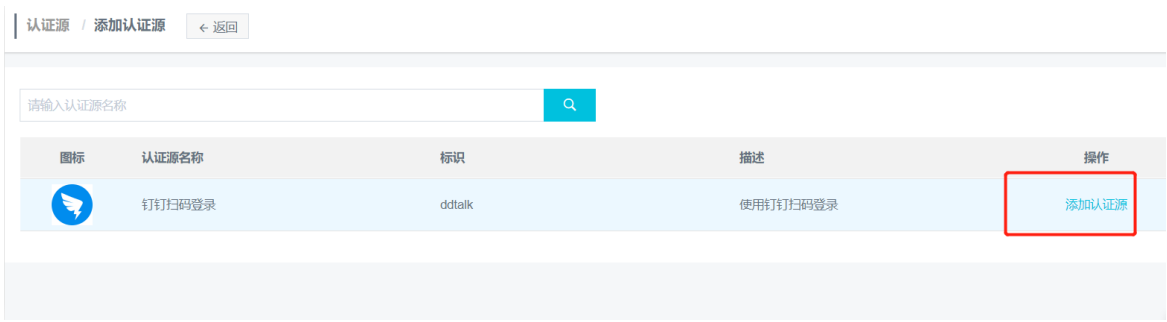

7. 添加成功以后，获取扫码登录页面所展示得appId、appSecret参数。


## 在IDaaS平台创建钉钉扫码认证源

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**认证 > 认证源**，在认证源页面点击右上角的添加钉钉认证源。




3. 在认证源中选择钉钉扫码登录，点击右侧的添加认证源。




4. 配置钉钉扫码认证源


扫码AppId和扫码AppSecret：上述在钉钉开发者平台配置步骤7所获取的appId、appSecret参数。

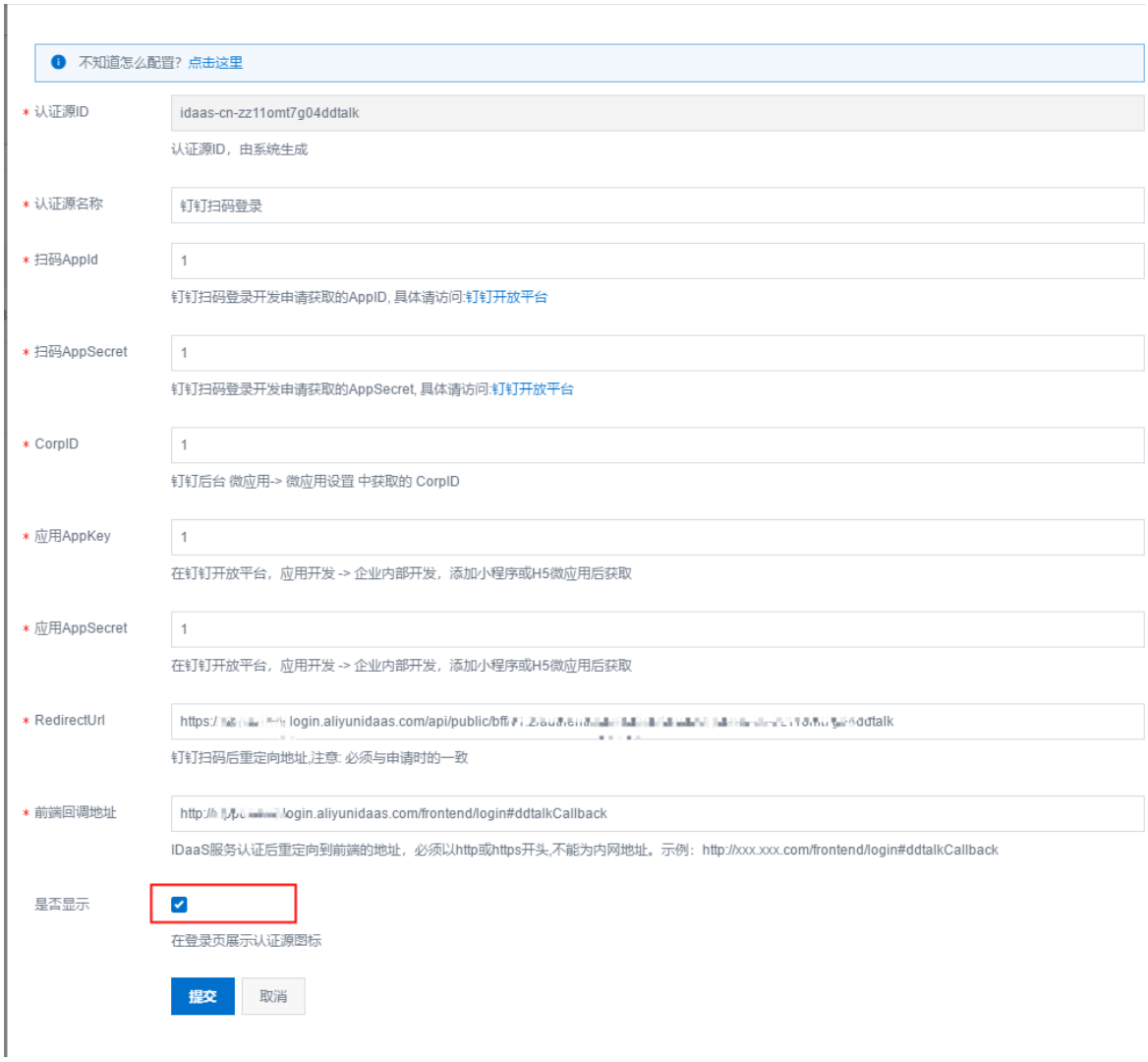
CorpID：上述在钉钉开发者平台配置步骤2所获取的CorpId参数。

应用AppKey和应用AppSecret：上述在钉钉开发者平台配置步骤4所获取的H5微应用的AppKey和AppSecret参数。

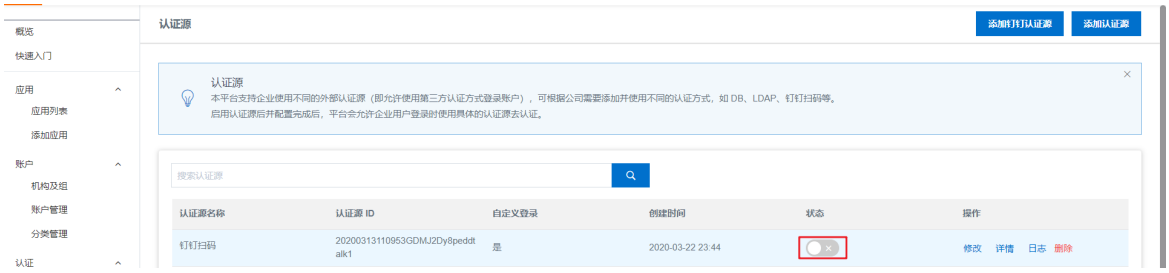
前端回调地址: IDaaS 用户侧的地址+/frontend/login#ddtalkCallback

> **说明** IDaaS 用户侧的地址 请到云盾IDaaS控制台页面获取。如下图：

点击勾选最下方的是否显示




5. 创建成功后，在认证源页面启用钉钉扫码认证源




## 使用钉钉扫码登录到IDaaS

1.在云盾IDaaS控制台复制用户的登录地址进行访问。


2.在用户登录页面可以看到钉钉扫码认证源。


3.点击认证源显示扫码页面。


4.使用钉钉第一次扫码登录时需要绑定IDaaS账户，绑定完成后IDaaS账户会与钉钉账户关联起来，之后登录无需再次绑定，直接使用钉钉扫码即可登录IDaaS。


完成以上步骤，即可实现钉钉扫码登录的功能。

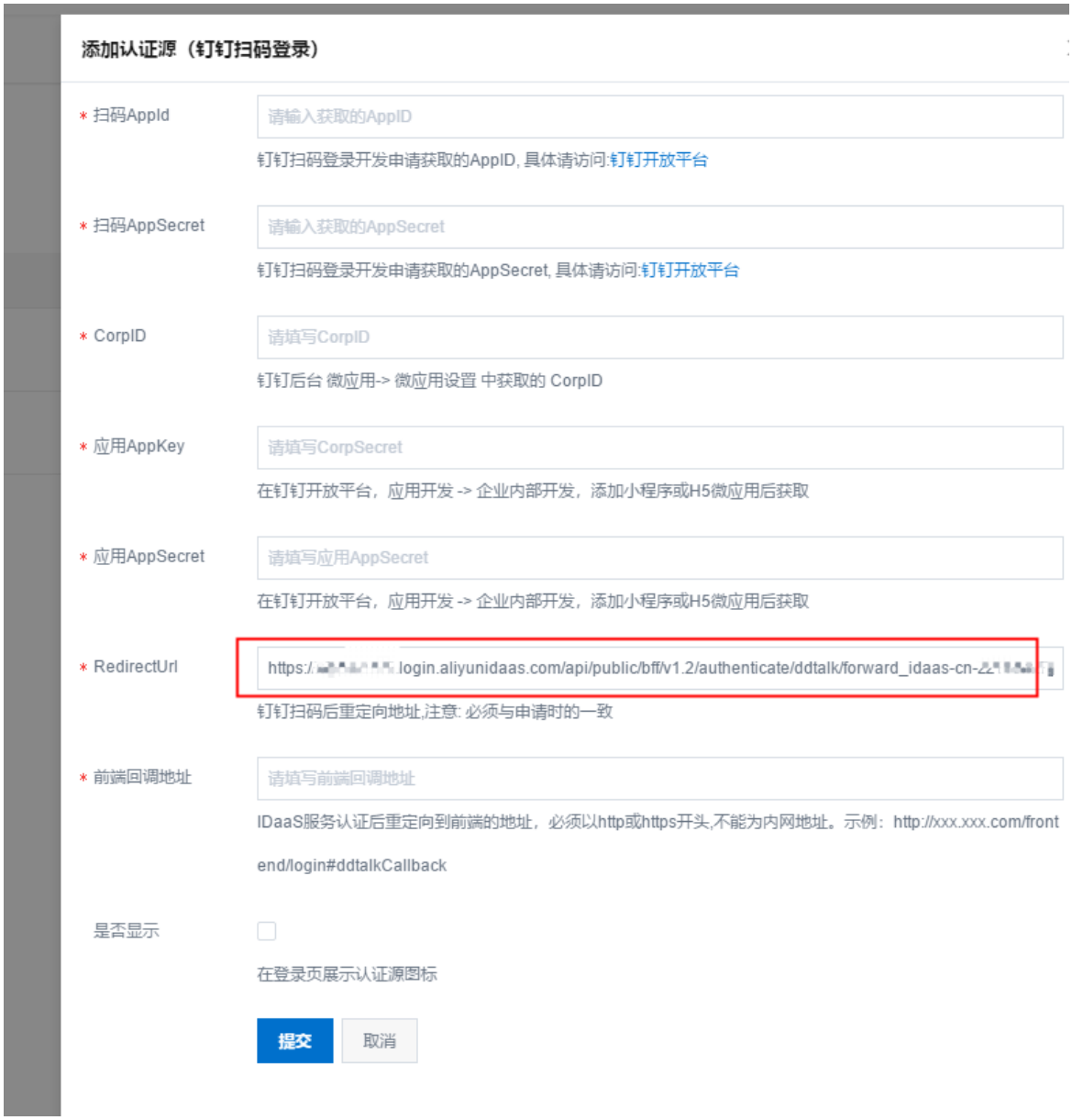
## 常见问题

1. **钉钉扫码配置完成之后，一直在loading是什么情况？**

   有可能是您复制钉钉参数粘贴到IDaaS时，参数多了空格。请检查您钉钉扫码配置中的各个参数值，是否多了空格。


2. **手机扫码提示无权查看该页面，如下图**


这个因为您第6步的RedirectUrl参数值没有填写到钉钉开发平台扫码登录的授权logo地址和回调域名。
需要把IDaaS钉钉扫码认证源的RedirectUrl参数值填写到对应位置。


添加认证源（钉钉扫码登录）
* 扫码AppId
请输入获取的AppID
钉钉扫码登录开发申请获取的AppID, 具体请访问:钉钉开放平台
* 扫码AppSecret
请输入获取的AppSecret
钉钉扫码登录开发申请获取的AppSecret, 具体请访问:钉钉开放平台
* CorpID
请填写CorpID
钉钉后台 微应用-> 微应用设置 中获取的 CorpID
* 应用AppKey
请填写CorpSecret
在钉钉开放平台，应用开发 -> 企业内部开发，添加小程序或H5微应用后获取
* 应用AppSecret
请填写应用AppSecret
在钉钉开放平台，应用开发 -> 企业内部开发，添加小程序或H5微应用后获取
* RedirectUrl
https:/ login.aliyunidaas.com/api/public/bff/v1.2/authenticate/ddtalk/forward_idaas-cn-
钉钉扫码后重定向地址,注意: 必须与申请时的一致
* 前端回调地址
请填写前端回调地址
IDaaS服务认证后重定向到前端的地址，必须以http或https开头,不能为内网地址。示例：http://xxx.xxx.com/front
end/login#ddtalkCallback
是否显示
在登录页展示认证源图标
提交
取消


创建扫码登录应用授权
* 名称:
授权微应用的名称，必填，最多不超过20个字符
* 描述:
扫码登录用于，主要是说明，使用的场景，必填，最多不超过20个字符
* 授权LOGO地址:
这个会显示在授权页面的中间页中，以http或https开头，必填，最多不超过500个字符
* 回调域名:
微应用回调的URL，以http或https开头，必填，最多不超过500个字符
取消
确定

# 7.使用钉钉微应用进行单点登录

使用钉钉微应用进行单点登录


## 准备工作

1. 在IDaaS管理员控制台的应用列表中添加想要单点登录的应用。
2. 申请注册钉钉组织。如果已有钉钉组织，可跳过该步骤。

## 创建钉钉微应用

操作步骤

1. **登录钉钉开发者平台**


2. **点击应用开发，选择H5微应用**


3. **点击创建应用**


开发方式：选择企业内部自主研发

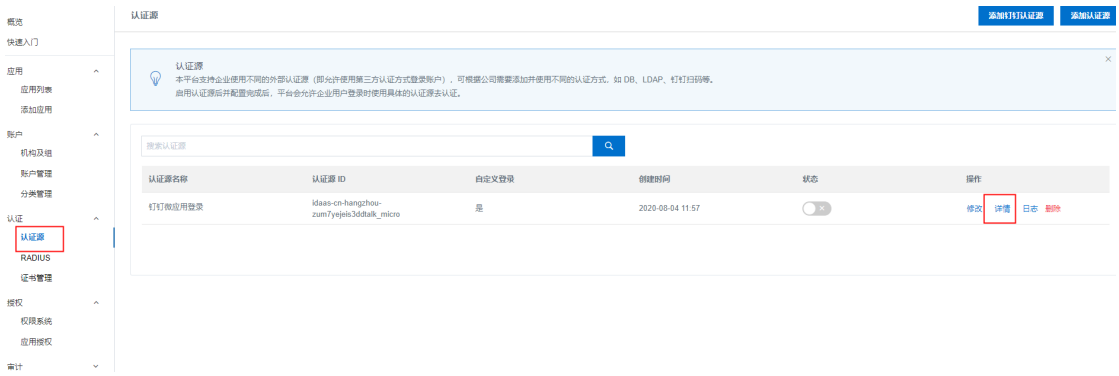
应用首页链接：在IDaaS上获取，获取方式参考下面步骤4（**应用首页链接参数的获取方式**）

PC端首页地址：和应用首页链接一致即可

服务器出口IP：IDaaS服务器的出口IP（请联系IDaaS同学获取出口IP）

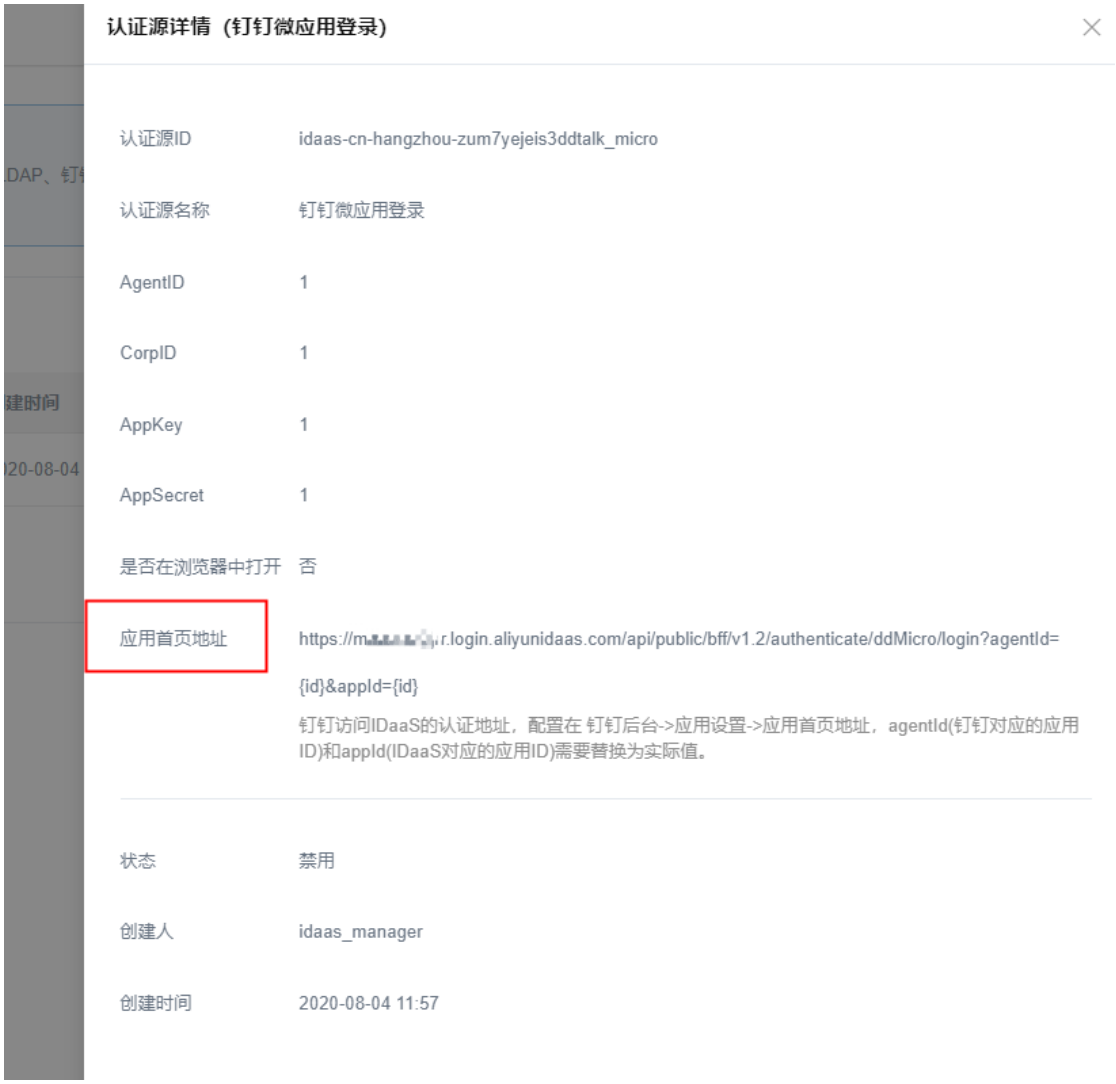
4. **应用首页链接参数的获取方式**

   i. 在IDaaS管理员页面，点击认证源 - 点击钉钉微应用登录的详情。




ii. 找到应用首页字段值：

https://xxx.login.aliyunidaas.com/api/public/bff/v1.2/authenticate/ddMicro/login?agentId=&appId=



iii. 点击应用列表，选择需要单点的应用


该应用ID是上面url中的appId参数，拼接成url值为：

https://xxx.login.aliyunidaas.com/api/public/bff/v1.2/authenticate/ddMicro/login?agentId=&appId= 201910101757083TKqTYywqyjwt2

iv. 将上述生成的url值复制粘贴到应用首页链接和PC端首页地址的输入框中，点击保存应用。

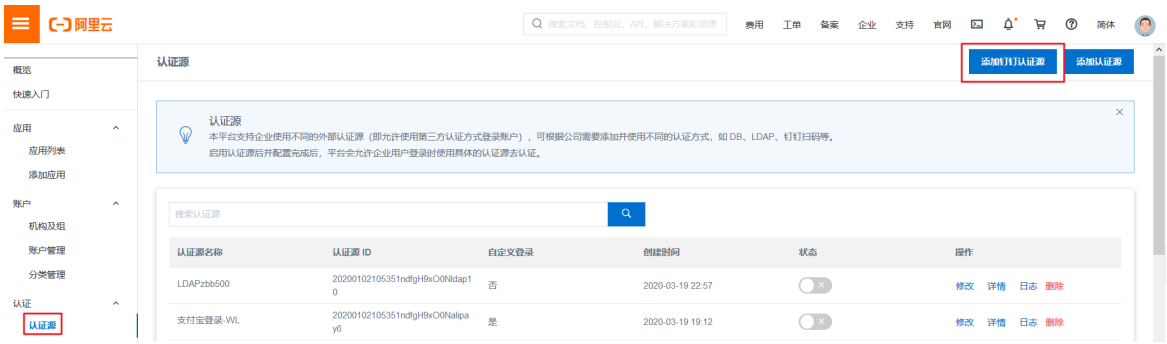
v. 查看应用的详情，获取应用的AgentId参数


vi. 修改应用，把应用详情中的AgentId的值添加到url的AgentId后

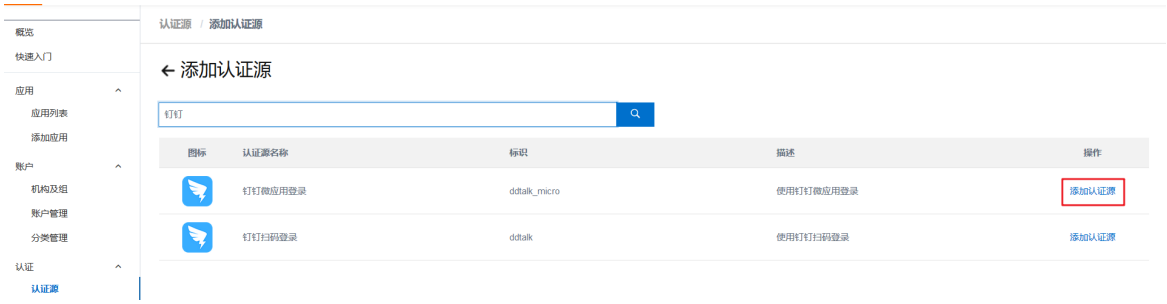

# 创建钉钉微应用认证源

操作步骤

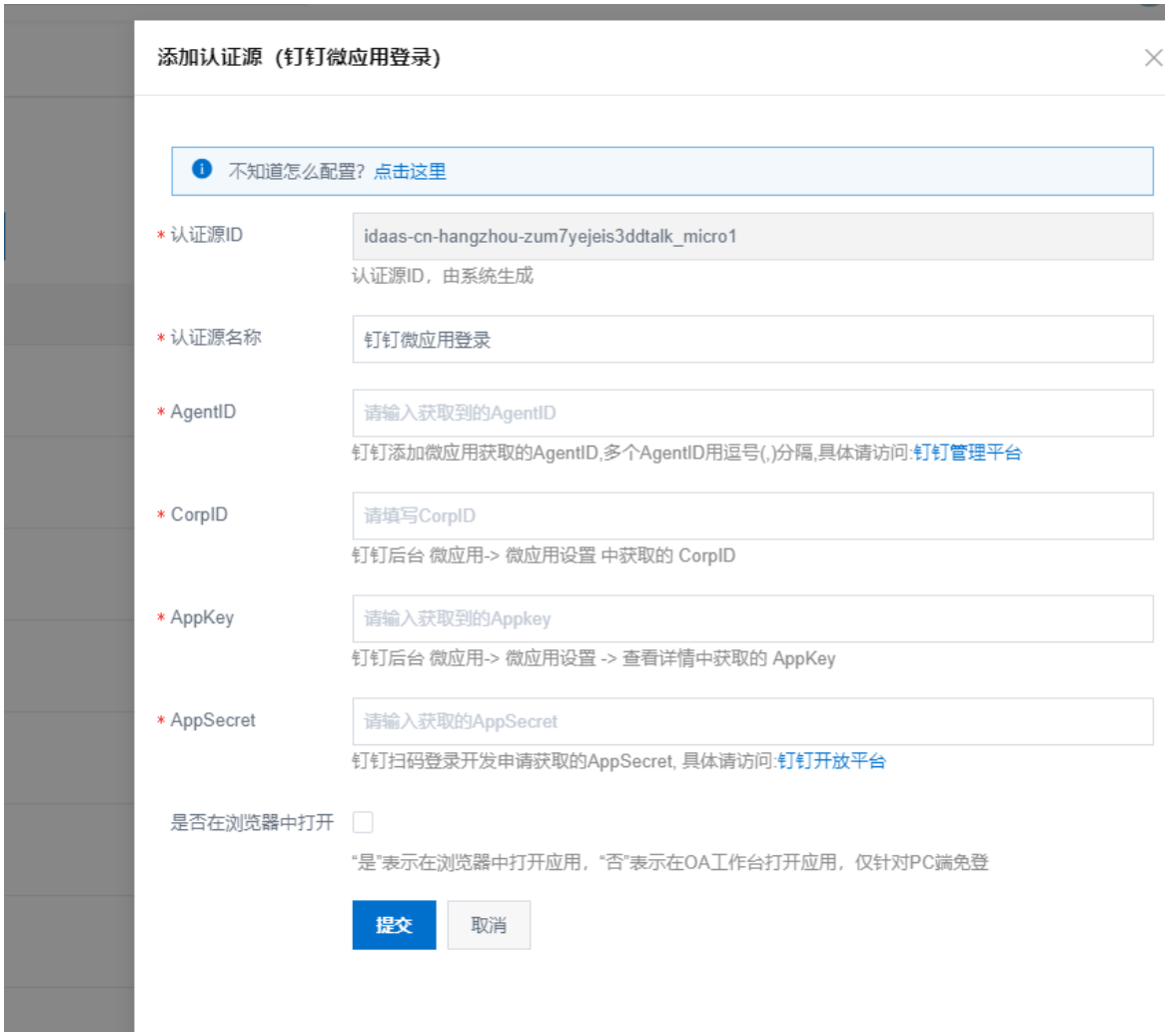
1. 在IDaaS管理员页面，点击认证源-点击添加钉钉认证源




2. 选择钉钉微应用登录-点击添加认证源




3. 配置钉钉微应用认证源参数

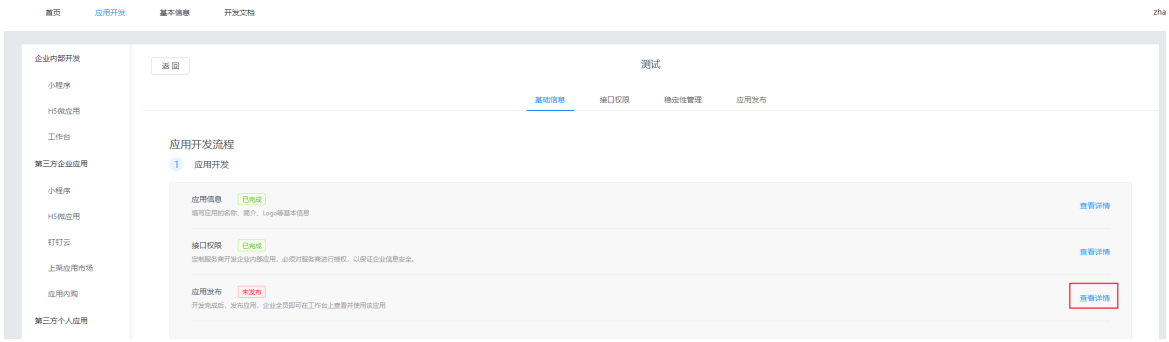



CorpID：登录钉钉开放平台首页展示的值


AgentID、AppKey、AppSecret：钉钉微应用-应用详情中展示的值


4. 点击启用钉钉微应用认证源


5. 在钉钉开放平台中发布应用




6. **打开钉钉，打开工作台，找到应用即可单点成功**

> 说明　第一次点击应用进行登录的时候，需要绑定IDaaS的账户。

备注：若提示IP不在白名单内，则需要在钉钉开放平台对应微应用的服务器出口IP中把提示的IP加上。


## FAQ

**1. 钉钉微应用单点登录提示无权限。**


请确认钉钉微应用上填写的应用首页地址是否正确，中间是否有空格等。

# 8.钉钉相关FAQ

## 钉钉微应用的出口IP怎么填

每一个 region 的出口 IP 不一样，您提交工单向我们咨询服务器出口 IP 。

## 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？

首先您需要确认您已经将 IDaaS 的服务器出口 IP 添加到对应钉钉微应用的服务器出口IP中。不同region的服务器出口IP不同，需要时您可以通过工单或者钉钉 联系我们进行获取。

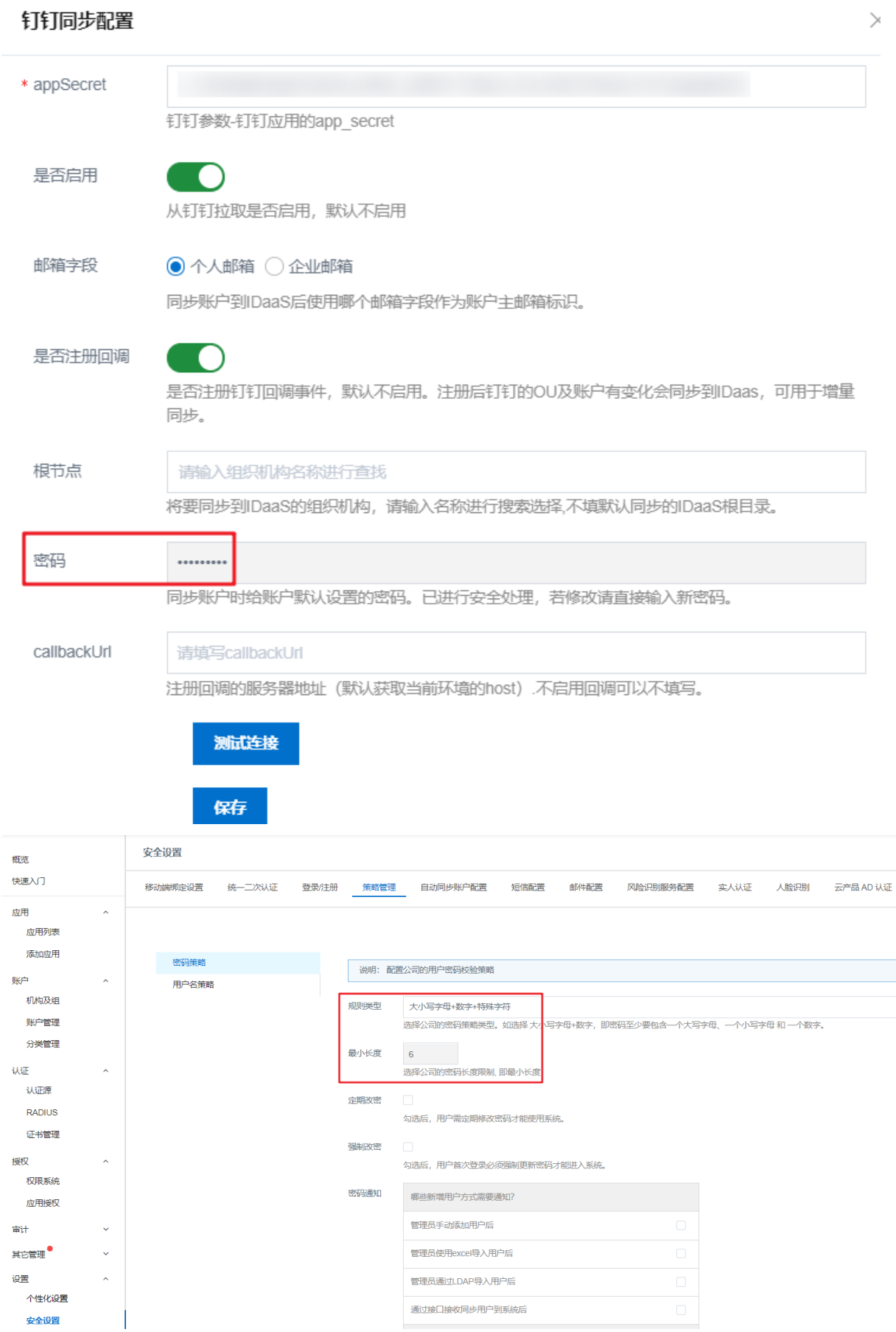
其次，您需要确认您钉钉微应用的接口权限，授权部门需要选择全部员工。


## 为什么可以拉取到钉钉的部门，但是拉取不到员工账户

如果您可以拉取到机构，但是拉取不到员工账户。请您检查下是否开启了必须的高级权限。如通讯录只读权限、通讯录编辑权限、手机号码信息。


## 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

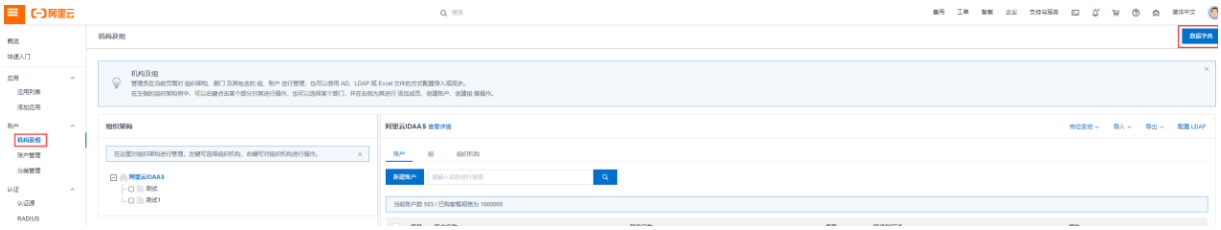
请检查钉钉同步配置中设置的密码，管理员设置的密码需要符合 IDaaS 的密码策略


钉钉同步配置
* appSecret
钉钉参数-钉钉应用的app_secret
是否启用
从钉钉拉取是否启用，默认不启用
邮箱字段
个人邮箱
企业邮箱
同步账户到IDaaS后使用哪个邮箱字段作为账户主邮箱标识。
是否注册回调
是否注册钉钉回调事件，默认不启用。注册后钉钉的OU及账户有变化会同步到IDaas，可用于增量同步。
根节点
请输入组织机构名称进行查找
将要同步到IDaaS的组织机构，请输入名称进行搜索选择,不填默认同步的IDaaS根目录。
密码
同步账户时给账户默认设置的密码。已进行安全处理，若修改请直接输入新密码。
callbackUrl
请填写callbackUrl
注册回调的服务器地址（默认获取当前环境的host）.不启用回调可以不填写。
测试连接
保存
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
应用授权
审计
其它管理
设置
个性化设置
安全设置
安全设置
移动端绑定设置
统一二次认证
登录/注册
策略管理
自动同步账户配置
短信配置
邮件配置
风险识别服务配置
实人认证
人脸识别
云产品 AD 认证
密码策略
用户名策略
说明：配置公司的用户密码校验策略
规则类型
大小写字母+数字+特殊字符
选择公司的密码策略类型。如选择 大小写字母+数字，即密码至少要包含一个大写字母、一个小写字母 和 一个数字。
最小长度
6
选择公司的密码长度限制, 即最小长度
定期改密
勾选后，用户需定期修改密码才能使用系统。
强制改密
勾选后，用户首次登录必须强制更新密码才能进入系统。
密码通知
哪些新增用户方式需要通知?
管理员手动添加用户后
管理员使用excel导入用户后
管理员通过LDAP导入用户后
通过接口接收同步用户到系统后

## 配置完成后，同步机构或账户提示同步失败，提示“不合法的部门列表”

请检查需要同步的机构是否在正确的机构下（即是否在创建钉钉应用所填写的IDPRootID对应的组织机构下）。

如果成功向钉钉同步一个机构后，在该机构下创建的机构和用户同步失败，请在 IDaaS 的数据字典中添加如下扩展字段



| 字段名 | 字段值 | 所属分类 | 字段类型 | 是否必填 | 是否唯一 |
| --- | --- | --- | --- | --- | --- |
| 钉钉部门ID | ddtalkId | 组织机构 | 文本框 | 否 | 是 |
| 钉钉人员ID | ddAccountId | 账户 | 文本框 | 否 | 是 |

## 配置完成后，同步机构或账户提示同步失败，提示“访问ip不在白名单之中”

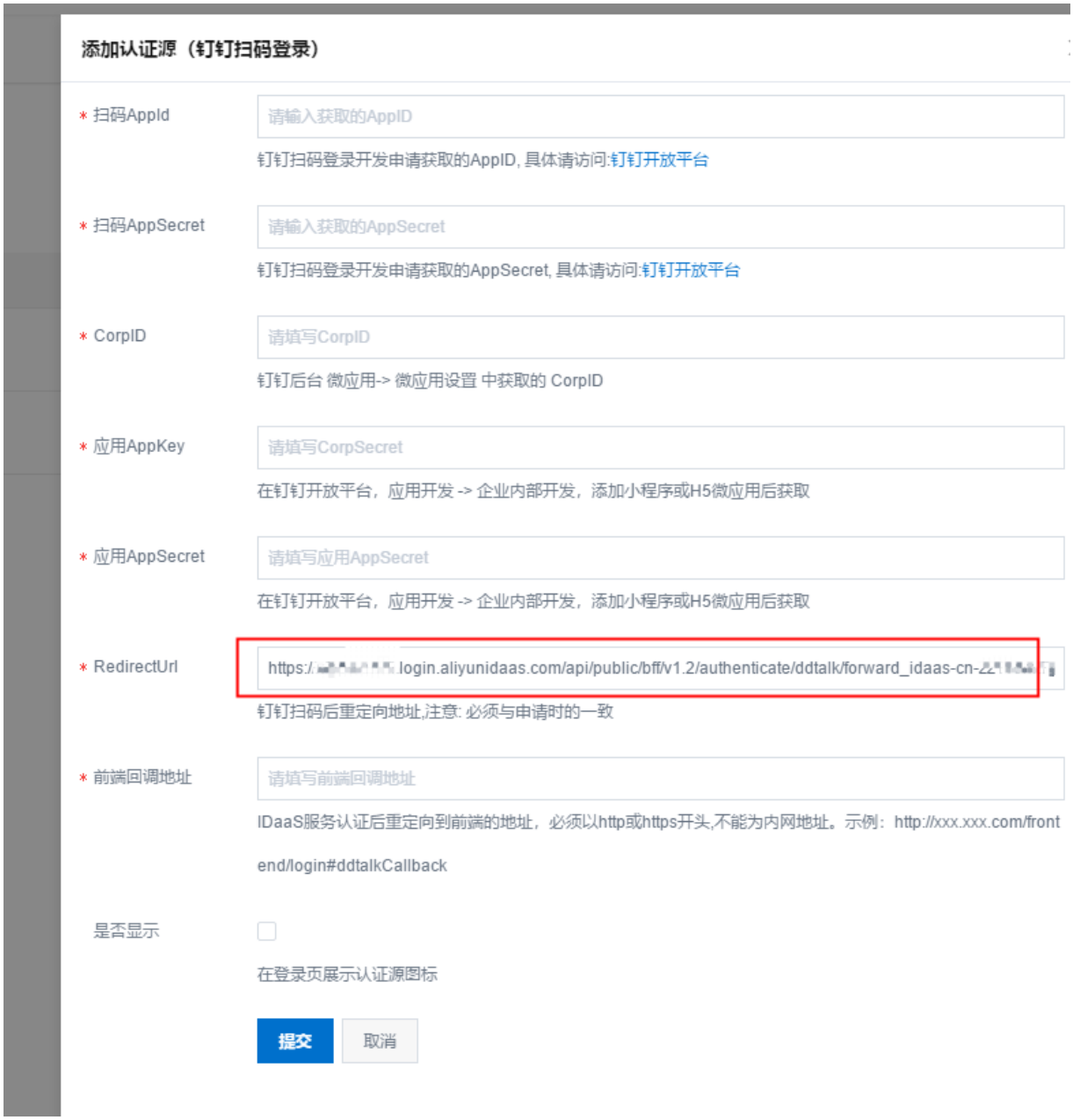
失败原因是钉钉会检查发送请求的IP是否在对应钉钉微应用的服务器出口IP中，需要把上述的请求IP地址加入到对应钉钉微应用的服务器出口IP配置中。

## 钉钉扫码登录，移动端确认后，页面一直在loading

有可能是您复制钉钉参数粘贴到IDaaS时，参数多了空格。请检查您钉钉扫码配置中的各个参数值，是否多了空格。


**手机扫码提示无权查看该页面**


这个因为您的RedirectUrl参数值没有填写到钉钉开发平台扫码登录的授权logo地址和回调域名。需要把IDaaS钉钉扫码认证源的RedirectUrl参数值填写到对应位置。


添加认证源（钉钉扫码登录）
* 扫码AppId
请输入获取的AppID
钉钉扫码登录开发申请获取的AppID, 具体请访问:钉钉开放平台
* 扫码AppSecret
请输入获取的AppSecret
钉钉扫码登录开发申请获取的AppSecret, 具体请访问:钉钉开放平台
* CorpID
请填写CorpID
钉钉后台 微应用-> 微应用设置 中获取的 CorpID
* 应用AppKey
请填写CorpSecret
在钉钉开放平台，应用开发 -> 企业内部开发，添加小程序或H5微应用后获取
* 应用AppSecret
请填写应用AppSecret
在钉钉开放平台，应用开发 -> 企业内部开发，添加小程序或H5微应用后获取
* RedirectUrl
https:/ login.aliyunidaas.com/api/public/bff/v1.2/authenticate/ddtalk/forward_idaas-cn-
钉钉扫码后重定向地址,注意: 必须与申请时的一致
* 前端回调地址
请填写前端回调地址
IDaaS服务认证后重定向到前端的地址，必须以http或https开头,不能为内网地址。示例：http://xxx.xxx.com/front
end/login#ddtalkCallback
是否显示
在登录页展示认证源图标
提交
取消


创建扫码登录应用授权
* 名称:
授权微应用的名称，必填，最多不超过20个字符
* 描述:
扫码登录用于，主要是说明，使用的场景，必填，最多不超过20个字符
* 授权LOGO地址:
这个会显示在授权页面的中间页中，以http或https开头，必填，最多不超过500个字符
* 回调域名:
微应用回调的URL，以http或https开头，必填，最多不超过500个字符
取消
确定