ALIBABA CLOUD

阿里云

应用身份服务

统一认证

文档版本：20210802

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.第三方认证源接入

1.1. 微信扫码登录

本文为您介绍如何通过IDaaS认证源管控功能，帮您实现微信扫码登录功能。

背景信息

某些公司将微信作为团队日常办公工具，为了方便使用微信进行扫码登录，现采用微信开放平台扫码登录认证源来实现该功能。

操作步骤

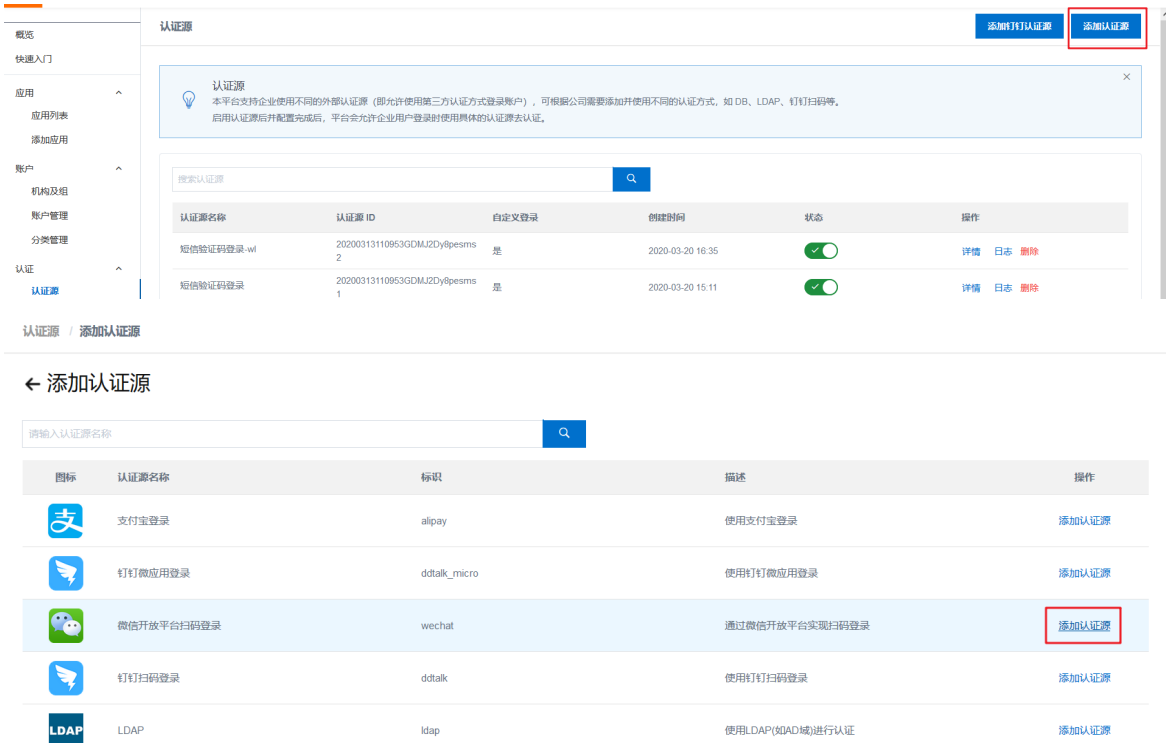
1. 登录微信开放平台
2. 点击“创建网站应用”按钮，进行网站应用创建时，授权回调域填写部署的IDaaS地址（需要外网域名），注意保留申请到的微信开放平台的App key和App Secret。

备注：(微信回调域默认使用80端口，需外网域名)

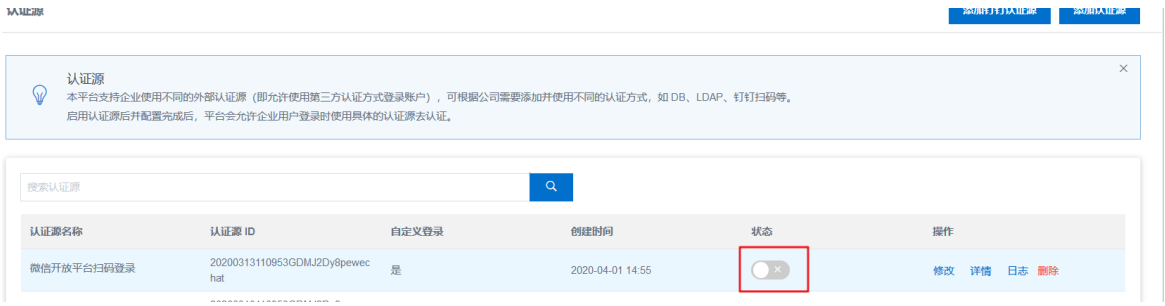
3. IT管理员登录后，依次进行认证、添加认证源、添加微信开放平台扫码登录等操作。

配置属性	配置说明
认证源名称	自定义认证源显示名称
AppId	用户在微信开放平台申请的AppId
AppSecret	用户在微信开放平台申请的AppSecret
授权回调域	由IDP生成，只读不可修改。（用户在微信开放平台设置的回调域必须完全按照该值填写）

4. 微信扫码登录配置确认保存之后，启用该认证源。


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
认证源
添加钉钉认证源
添加认证源
认证源
本平台支持企业使用不同的外部认证源（即允许使用第三方认证方式登录账户），可根据公司需要添加并使用不同的认证方式，如 DB、LDAP、钉钉扫码等。
启用认证源后并配置完成后，平台会允许企业用户登录时使用具体的认证源去认证。
搜索认证源
认证源名称
认证源 ID
自定义登录
创建时间
状态
操作
短信验证码登录-wl
20200313110953GDMJ2Dy8pesms2
是
2020-03-20 16:35
详情 日志 删除
短信验证码登录
20200313110953GDMJ2Dy8pesms1
是
2020-03-20 15:11
详情 日志 删除

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



5. 普通用户在登录页，点击微信开放平台认证源


扫码登录更便捷
阿里云
阿里云IDaaS服务
draven
请输入验证码
忘记密码
提交
注册
第三方认证登录
LDAP

使用移动端微信扫描二维码，并在移动端点击授权登录。

如果用户的微信之前没有绑定过IDaaS的账户，则会弹出一个账户绑定的页面，需要用户在页面上输入IDaaS的账号密码进行绑定。

绑定成功后，即可登录到IDaaS平台，之后使用微信开放平台扫码登录无需再次绑定。

如果用户希望解除微信与IDaaS的账户绑定关系。在用户登录后，点击 **我的账户 > 三方账户** ，选择认证源点击解除绑定即可。

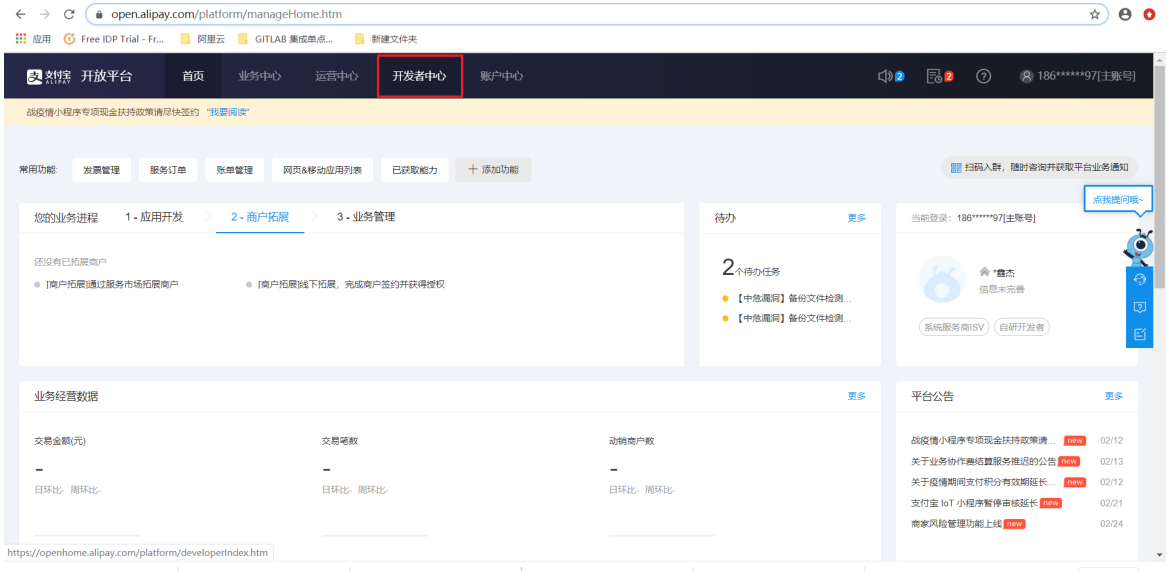
1.2. 支付宝扫码登录

本文为您介绍如何通过IDaaS认证源功能，帮您实现使用支付宝扫码登录IDaaS的功能。

一、支付宝开放平台创建应用

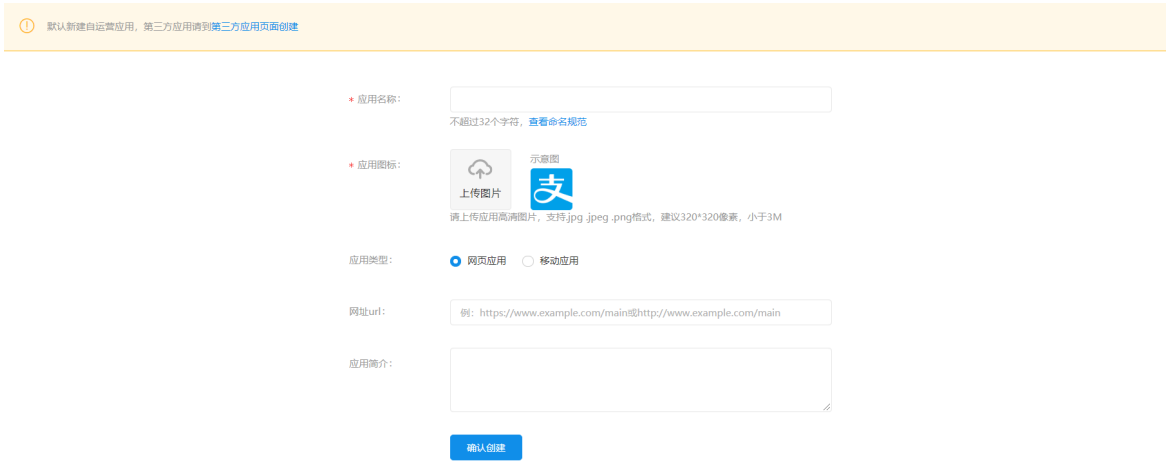
操作步骤

1. 登录支付宝开放平台
2. 点击进入开发者中心

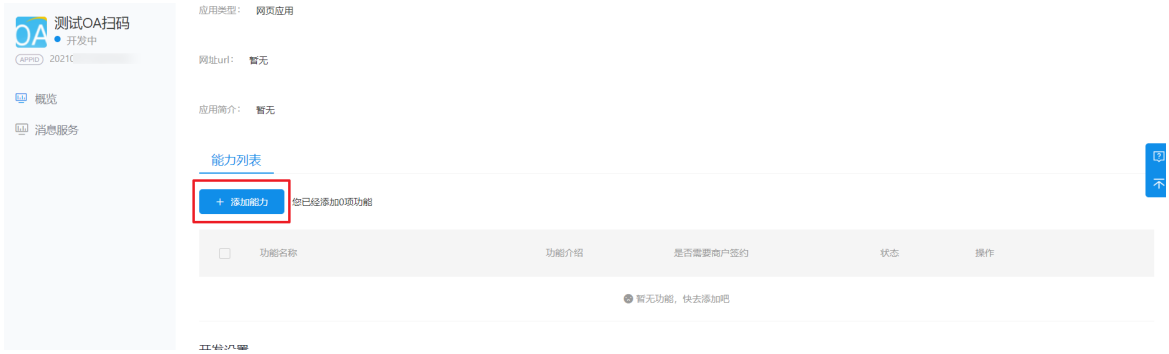


3. 点击创建应用，选择网页&移动应用标签下的自定义接入

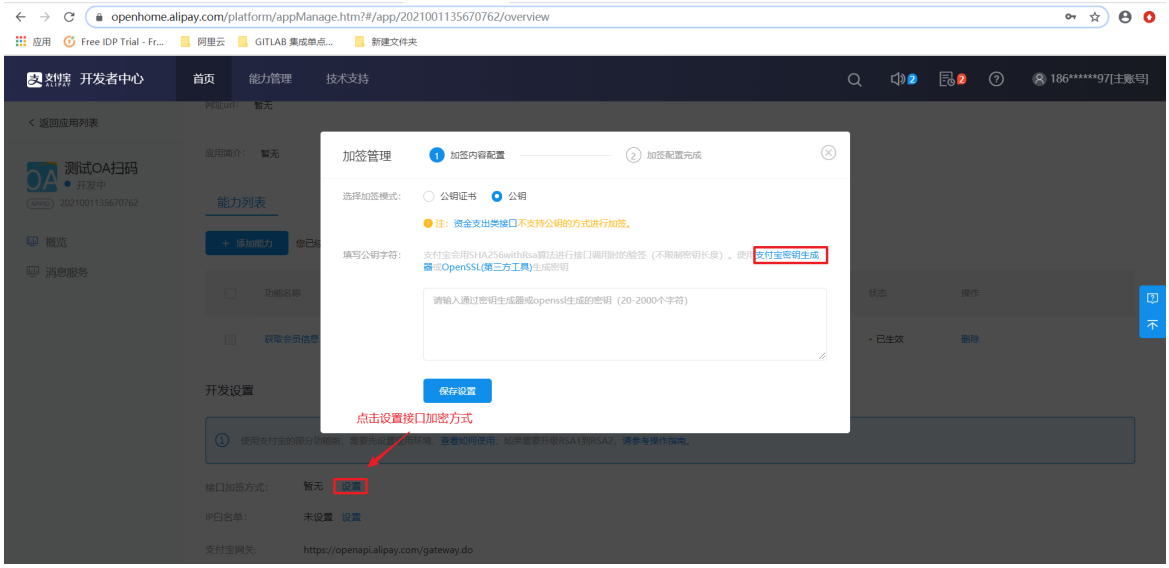
4. 配置应用的基本信息



5. 为应用添加 获取会员信息的能力



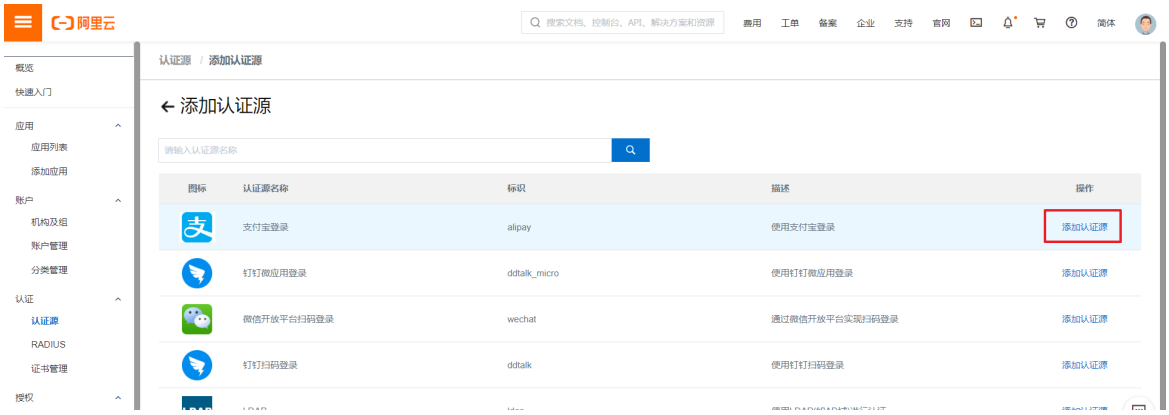
6. 设置接口加签方式



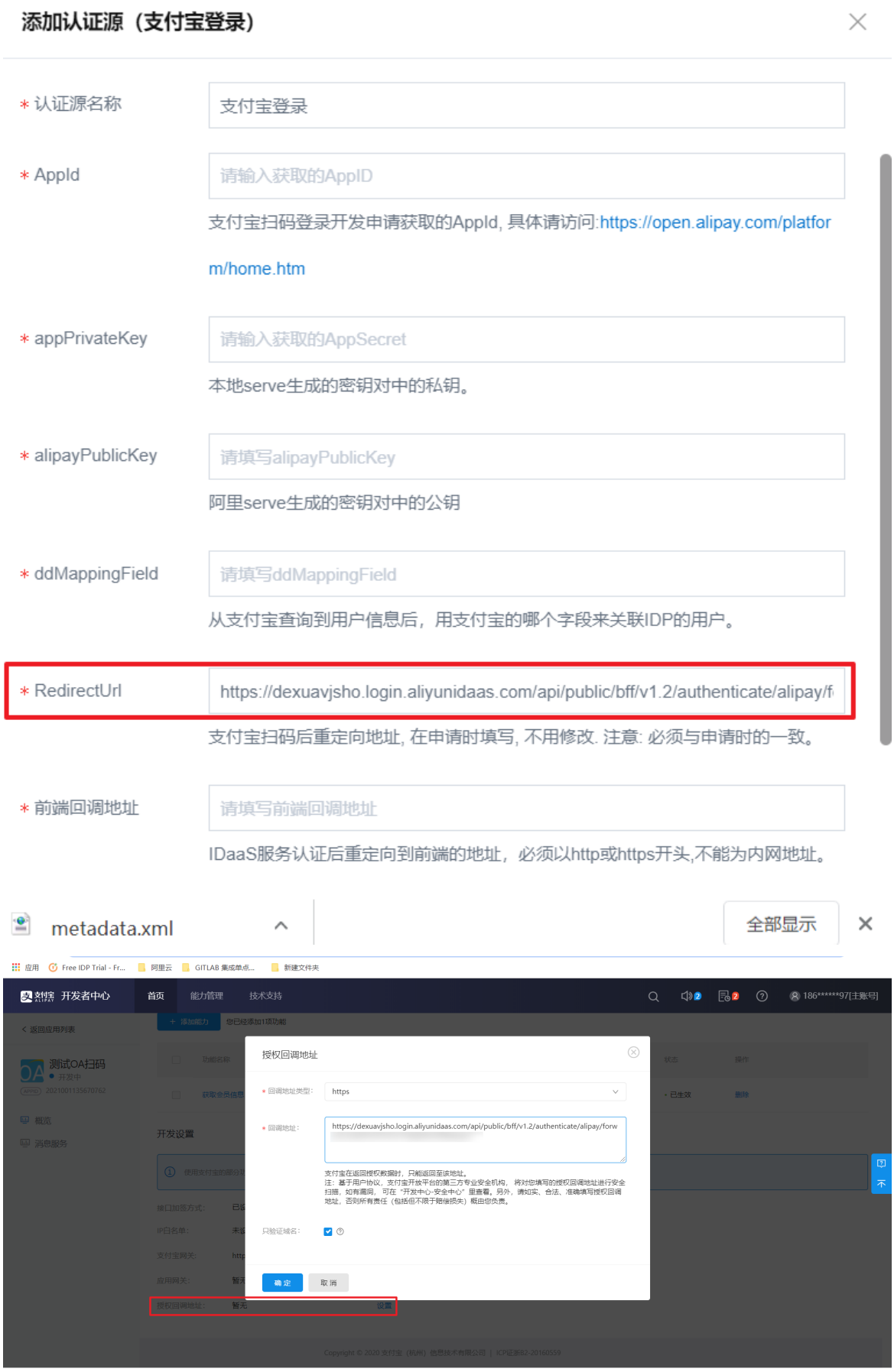
将工具生成的密钥对和支付宝生成的支付宝公钥保存在本地

二、创建支付宝认证源

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. 点击左侧导航 **认证 > 认证源**。
3. 点击右上角**添加认证源**，选择支付宝登录，点击**添加认证源**。



4. 将自动生成的Redirect Url填写到支付宝创建的应用的授权回调地址中


添加认证源（支付宝登录）
* 认证源名称
支付宝登录
* AppId
请输入获取的AppID
支付宝扫码登录开发申请获取的AppId，具体请访问:https://open.alipay.com/platform/home.htm
* appPrivateKey
请输入获取的AppSecret
本地serve生成的密钥对中的私钥。
* alipayPublicKey
请填写alipayPublicKey
阿里serve生成的密钥对中的公钥
* ddMappingField
请填写ddMappingField
从支付宝查询到用户信息后，用支付宝的哪个字段来关联IDP的用户。
* RedirectUrl
https://dexuavjsho.login.aliyunidaas.com/api/public/bff/v1.2/authenticate/alipay/f
支付宝扫码后重定向地址，在申请时填写，不用修改. 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。
metadata.xml
全部显示
开发者中心
首页
能力管理
技术支持
授权回调地址
https
https://dexuavjsho.login.aliyunidaas.com/api/public/bff/v1.2/authenticate/alipay/forw
确定
取消

5. 获取应用的APPID参数保存到本地，并提交审核

> **说明**
>
> 使用支付宝扫码登录功能，必须确保支付宝开放平台的应用已通过审核

6. 配置支付宝认证源参数

其中：

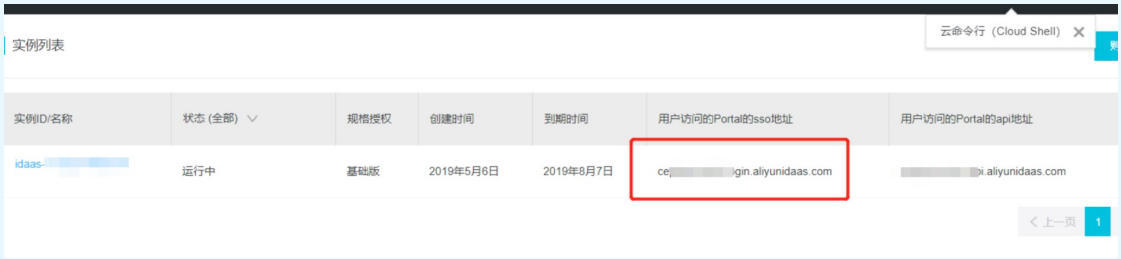
AppId、appPrivateKey、alipayPublicKey为上述过程中获取的支付宝应用参数

ddMappingField：nickName

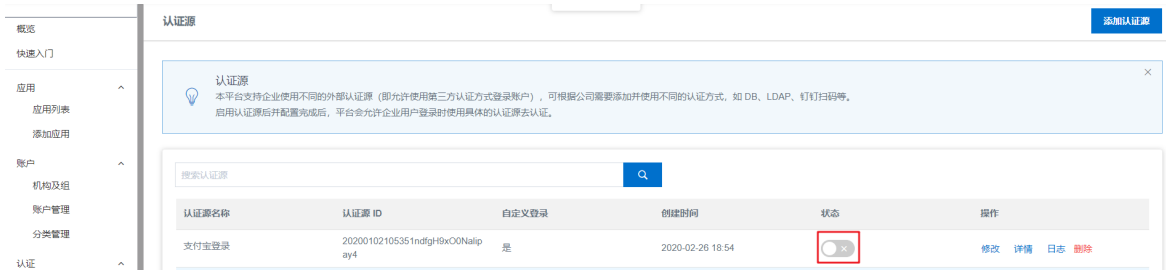
前端回调地址：IDaaS域名地址+/frontend/login#alipayCallback

是否显示：勾选之后，会在登录页面展示支付宝认证源

> 说明
>
> IDaaS域名地址可以在云盾IDaaS管理控制台获取。



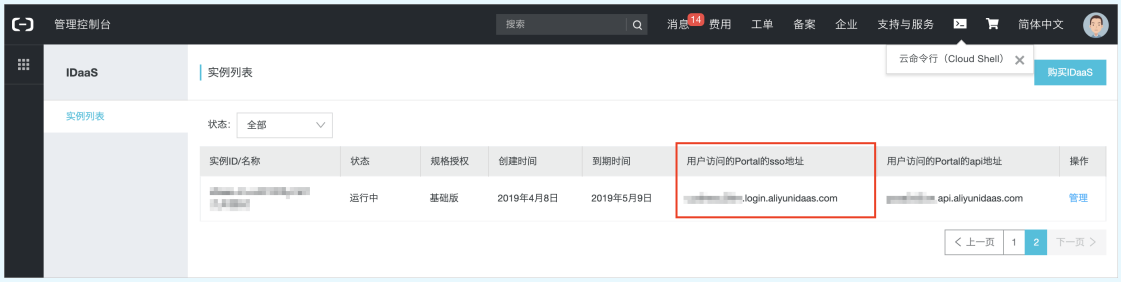
7. 认证源添加完成后，点击启用认证源



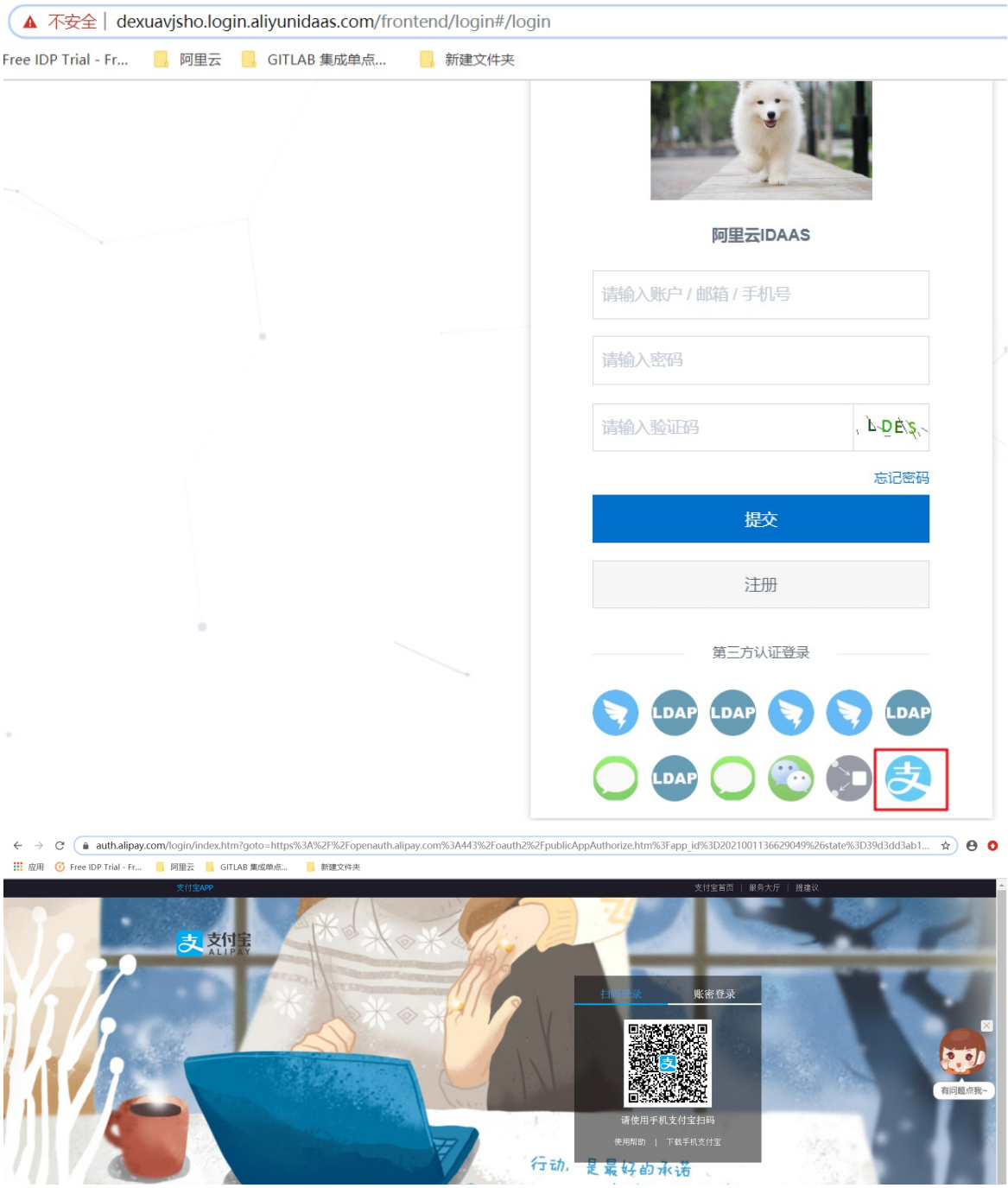
三、支付宝扫码登录IDaaS

1. 通过浏览器访问云盾IDaaS用户Portal地址。

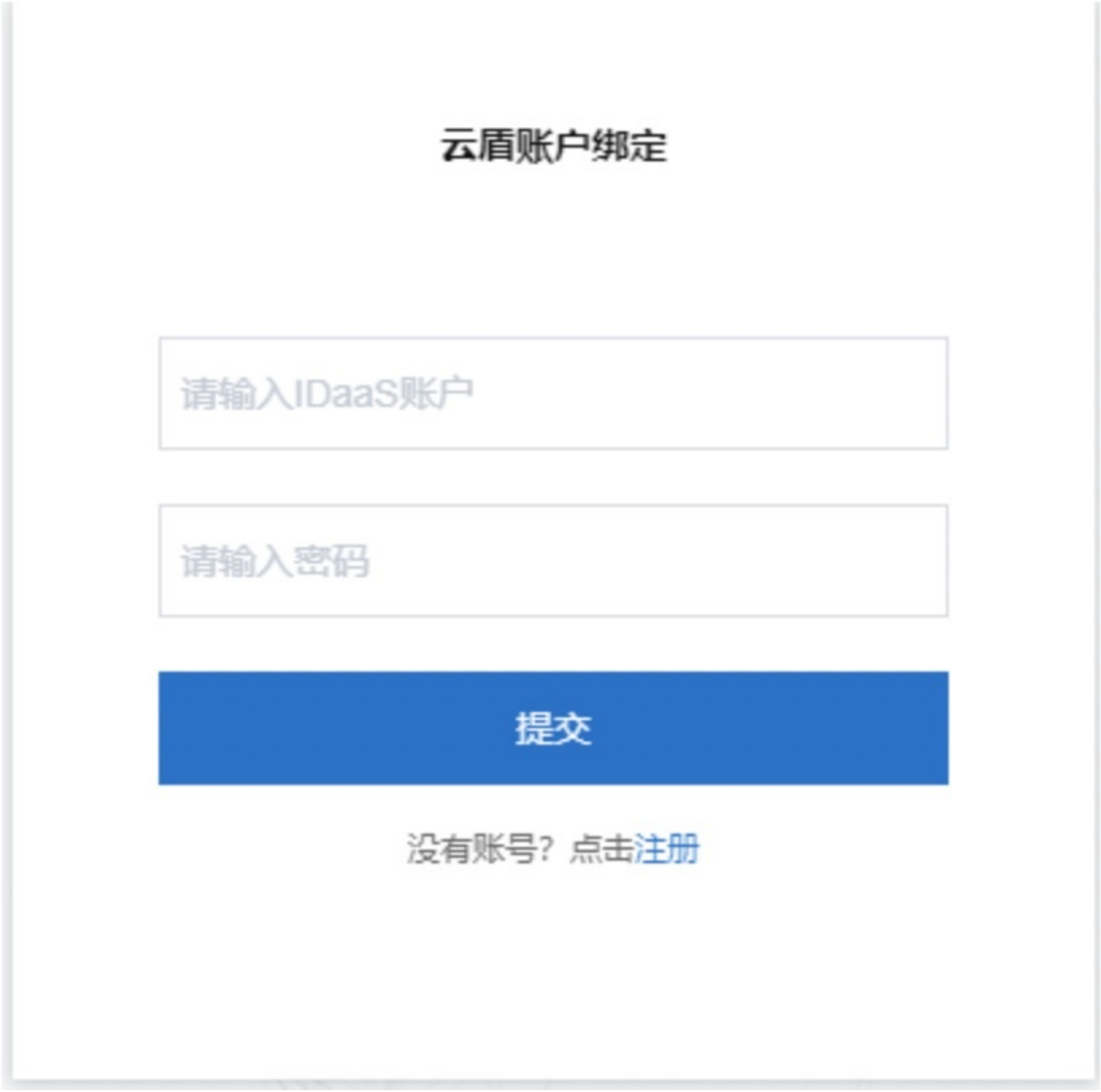
> 说明
>
> 该地址由IT管理员提供。IT管理员可以在云盾IDaaS实例列表中查看用户访问的Portal地址。



2. 点击支付宝认证源图标，并使用移动端打开支付宝扫描页面二维码进行扫码登录



若用户首次使用支付宝扫码认证源，则需要绑定IDaaS账户，在绑定页面中输入IDaaS的用户名和密码



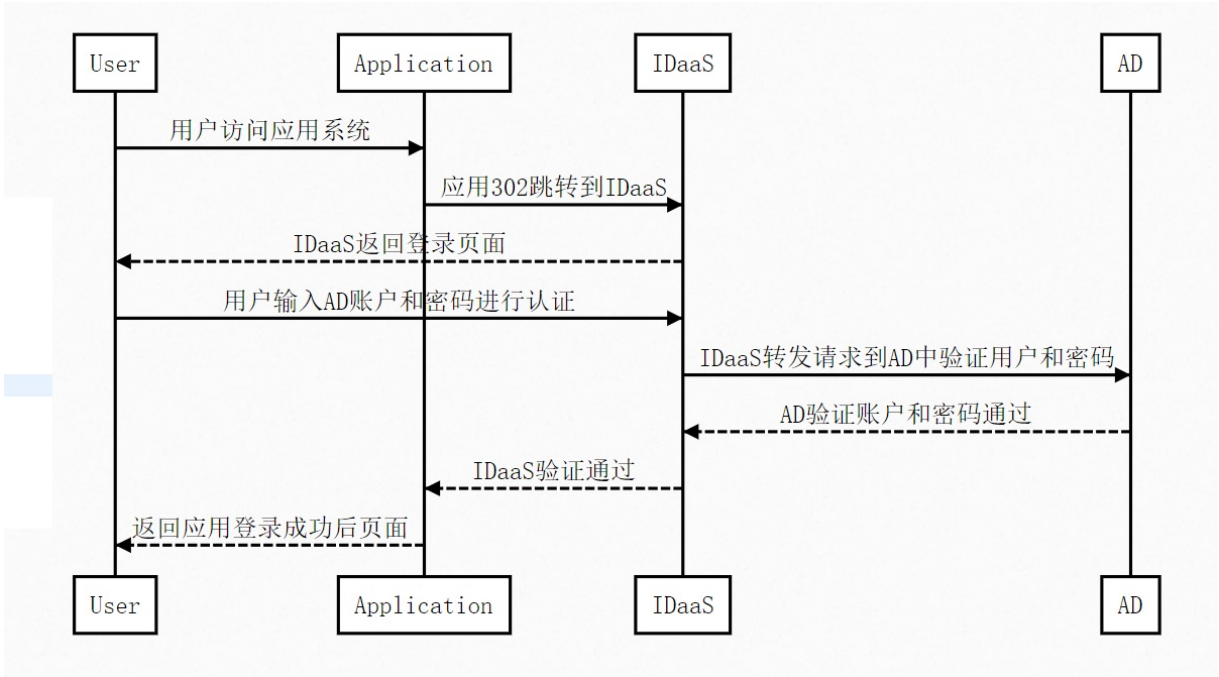
首次绑定后，后续使用都无需再绑定，如果用户想要解绑当前的支付宝账号，需要进入用户界面 **我的账户 > 三方账户**，进行解绑

1.3. LDAP认证登录

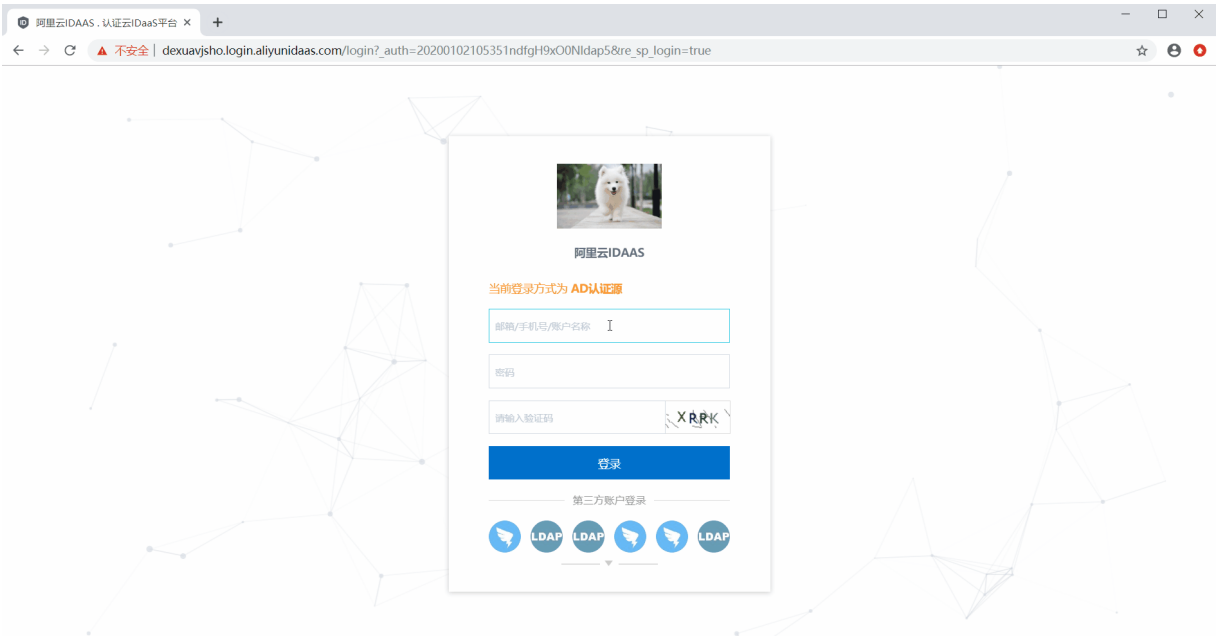
本文介绍如何通过LDAP认证源，使用AD域里面的用户登录IDaaS，或者直接登录到应用。

场景

如果客户不希望保存AD用户的密码到阿里，可以使用IDaaS的LDAP认证服务，实现使用AD账户和密码登录阿里控制台，或者其它应用的目的。



演示动图

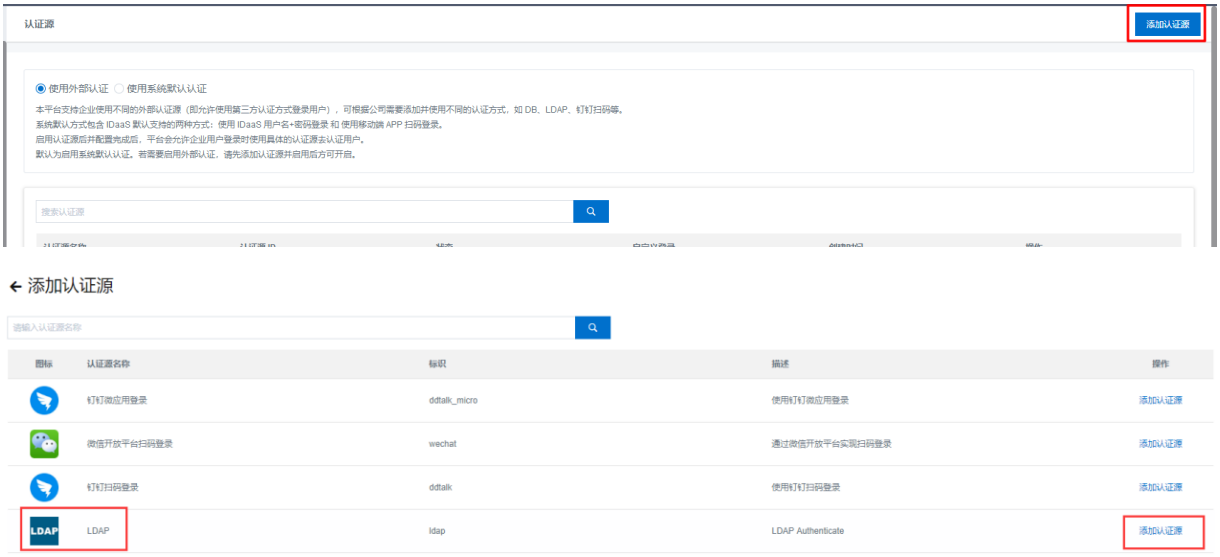


配置步骤

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- 登录。

2. 在左侧导航点击 **认证 ->认证源** 跳转到认证源界面。

3. 点击右上角**添加认证源**，选择**LDAP认证源**，点击【添加认证源】，即可在弹出的界面中配置LDAP认证源。



LDAP URL为AD域的IP加端口号；

LDAP Base、LDAP UserDn、LDAP密码为AD的值；

过滤条件填写为如 (UID=$username$) 。

> **说明**
>
> IDaaS目前只支持公网访问，AD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, IDaaS出口IP请提工单咨询IDaaS同学获取。

4. 在AD中创建账户。

> **说明**
>
> 若您的AD中已有账户数据，可以跳过该步骤。AD中账户必须同步IDaaS中，才能实现认证。

5. 在右侧导航中点击机构及组，在机构及组页面 新建LDAP配置，配置完成后，将AD中的账户数据拉取到IDaaS中。

6. AD中的账户需要同步IDaaS后，才能使用ldap认证源进行登录认证。 用户输入AD中的账户和密码时，会先检验登录的这个账户是否在IDaaS中存在，如果在IDaaS中存在， 再传递账户到LDAP中去认证， 如果IDaaS中不存在，不会进行下面的操作。

> **说明**
>
> 若已经在机构及组中存在LDAP认证源对应的LDAP配置，则不需要新建LDAP配置。

7. 在用户登录页面下侧的第三方认证登录中点击LDAP认证源，跳转到LDAP账户登录界面，使用AD域中的账户密码进行登录。

> **注意**
>
> 使用LDAP认证源进行登录时，需要使用AD域里面的密码进行登录，不能使用IDaaS里面的密码登录。

通过以上步骤，完成了添加配置LDAP认证源，用户可以直接使用AD中的账户和密码登录IDaaS。

FAQ

1. 是否使用LDAP认证源，一定要同步ldap的账户到IDaaS中。

是的。只需同步账户，不会同步LDAP中的密码到IDaaS中。

2. 添加了ldap认证源，但是在登录页面没有显示ldap图标。

请查看下图中的登录页显示，是否进行了勾选。

3. 是否可以更新LDAP中的密码到IDaaS中。

支持。参考下图设置同步ldap的密码到IDaaS中，当使用LDAP账户和密码登录一次后会自动更新IDaaS中的密码。

4. 通过ldap认证源进行登录，提示账户名和密码不正确。

请检查下面参数和格式是否正确。

5. 是否可以指定默认的登录方式是ldap认证源

支持。参考下图配置默认的登录方式是ldap认证源。

1.4. 钉钉扫码登录

本文为您介绍在 IDaaS 中如何配置钉钉扫码认证源，并使用钉钉扫码登录 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用户可以更加灵活、方便地登录到IDaaS。

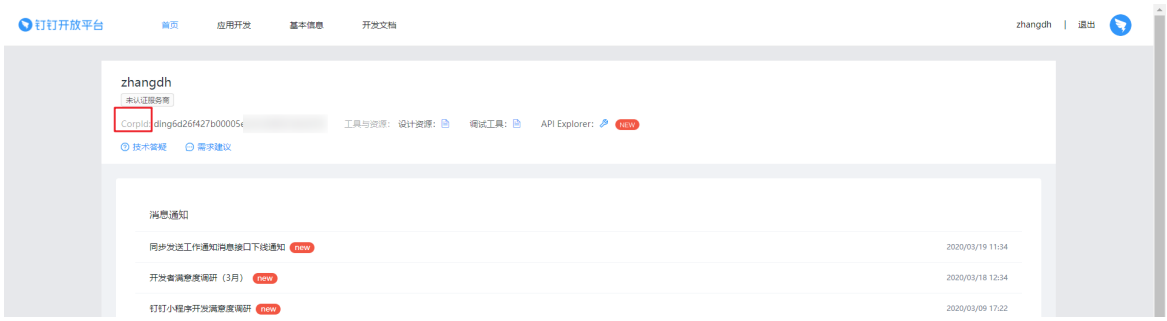
配置钉钉扫码认证源的操作步骤主要分为两步：

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

完成以上两步，即可实现使用钉钉扫码登录到IDaaS

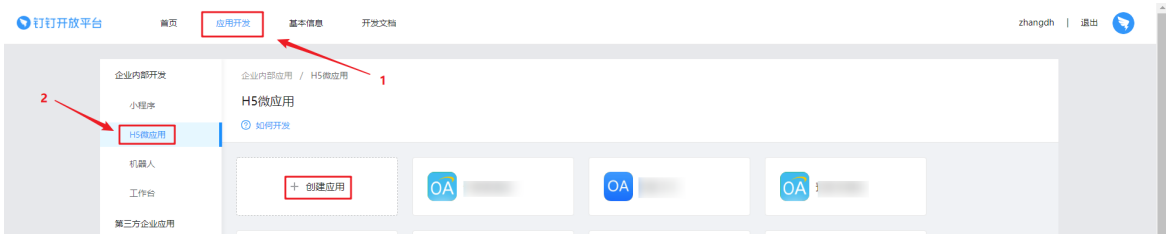
在钉钉开发者平台添加微应用并配置扫码登录

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

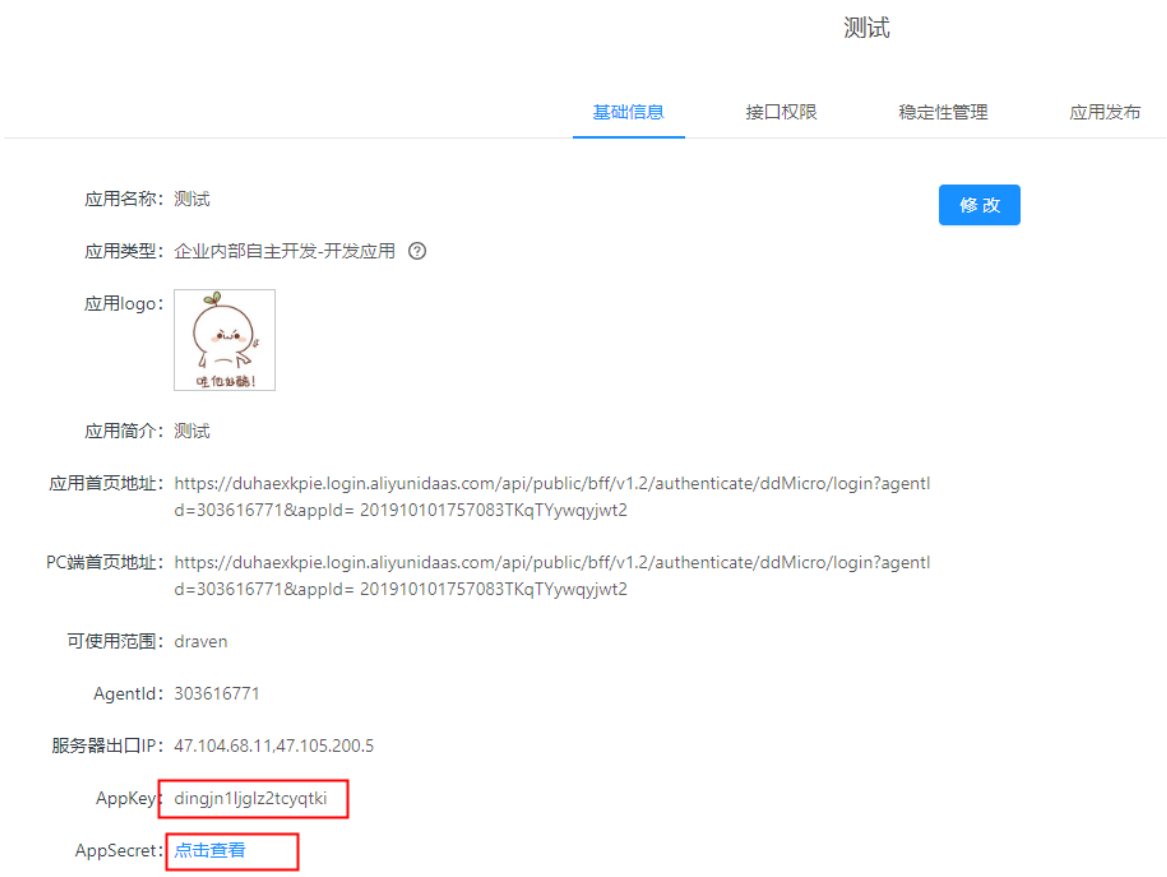


3. 点击应用开发，在左侧导航栏中选择H5微应用，创建一个钉钉微应用

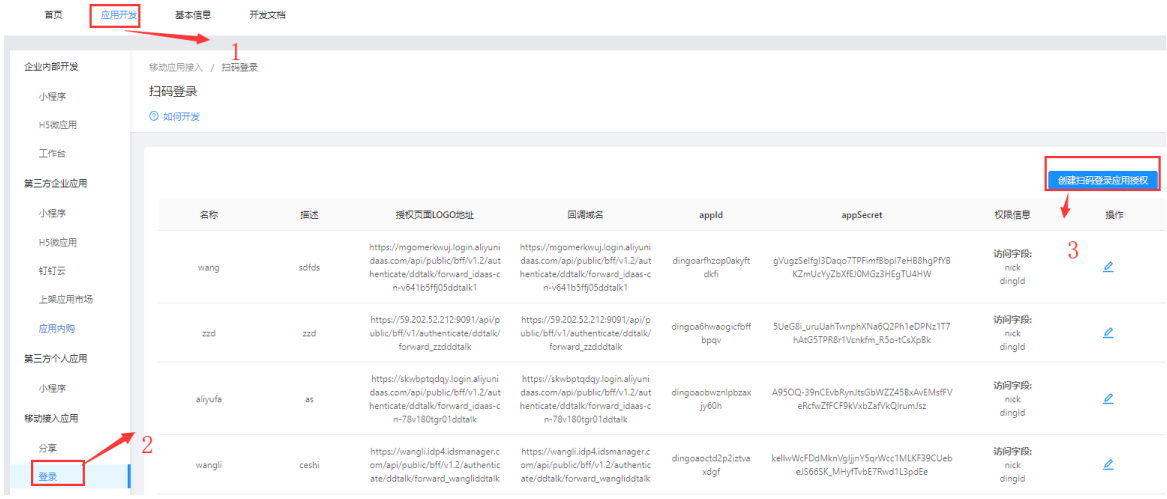
> **说明**
>
> 如果已创建过H5微应用，可以直接使用现有的。



4. 创建完成后，点击应用图标查看应用详情，获取应用的 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**

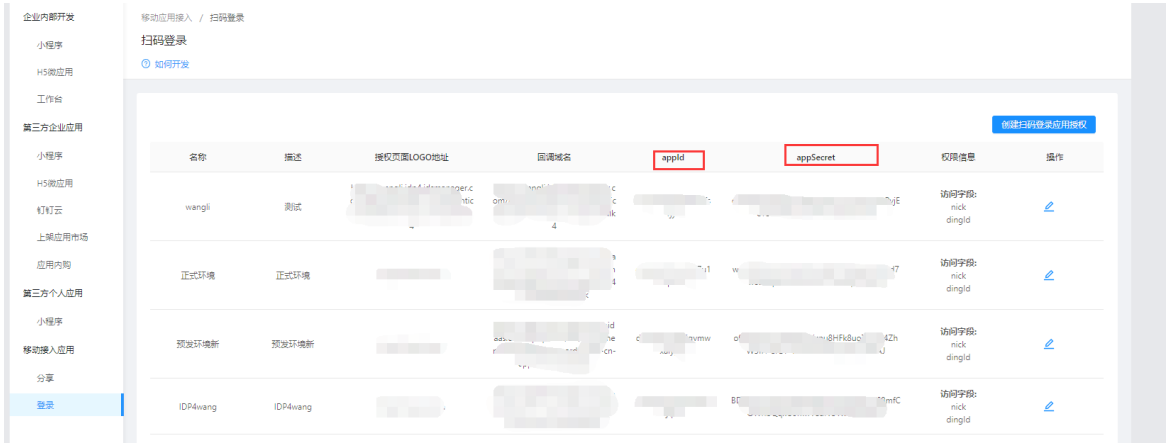


6. 创建扫码登录应用授权的必填参数中，名称、描述可以随便填写，授权 logo 地址和回调域名需要填写 IDaaS 里添加钉钉扫码认证源时系统生成的 **RedirectUrl** 的地址。

> **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。

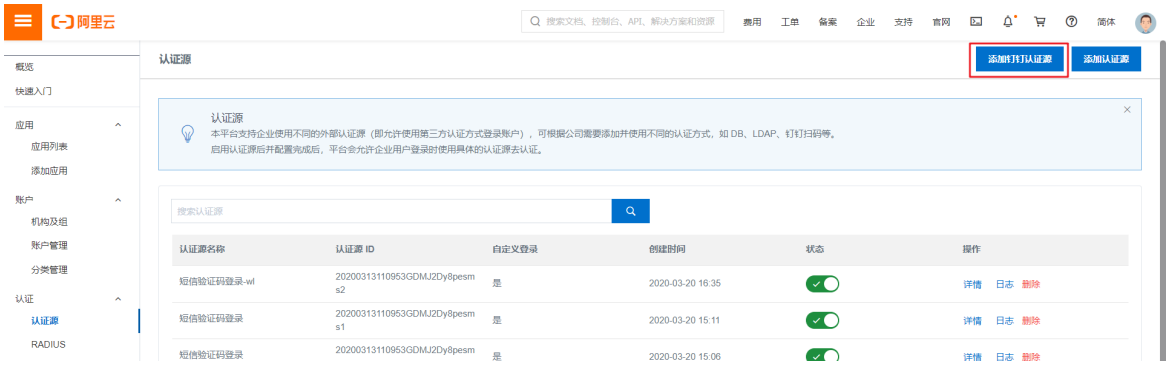

添加认证源（钉钉扫码登录）
认证源ID，由系统生成
* 认证源名称
钉钉扫码登录
* 扫码AppId
请输入获取的AppID
钉钉扫码登录开发申请获取的AppID, 具体请访问:钉钉开放平台
* 扫码AppSecret
请输入获取的AppSecret
钉钉扫码登录开发申请获取的AppSecret, 具体请访问:钉钉开放平台
* CorpID
请填写CorpID
钉钉后台 微应用-> 微应用设置 中获取的 CorpID
* 应用AppKey
请填写CorpSecret
在钉钉开放平台，应用开发 -> 企业内部开发，添加小程序或H5微应用后获取
* 应用AppSecret
请填写应用AppSecret
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://sbaucspfro.login.aliyunidaas.com/api/public/bff/v1.2/authenticate/ddtalk/f
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。

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

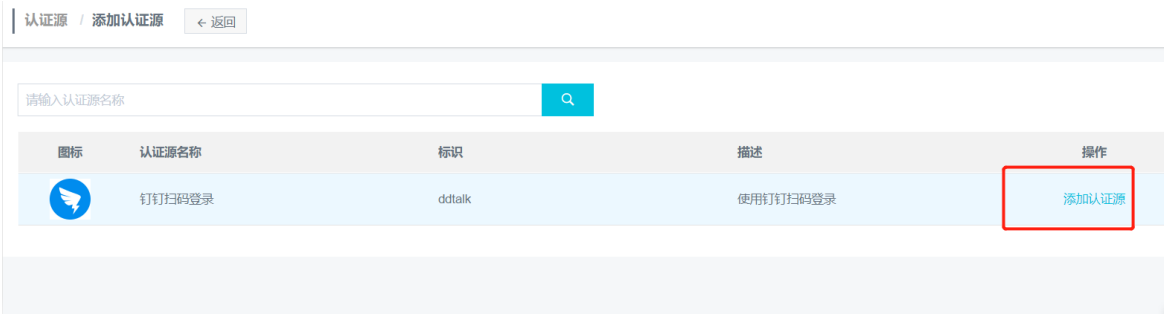


在IDaaS平台创建钉钉扫码认证源

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：/frontend/login/#/ddtalkCallback（固定值，添加时系统会默认生成）

> 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，在认证源列表中启用它

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。

首次绑定后，后续使用都无需再绑定，如果用户想要解绑当前的钉钉账号，需要进入用户界面 **我的账户** > **三方账户**，进行解绑

1.5. 钉钉微应用单点登录

通过 IDaaS 微应用认证源能力与钉钉微应用集成，实现在钉钉工作台中单点登录进入应用的效果。

操作流程

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**


首页
应用开发
基本信息
开发文档
企业内部开发
小程序
H5微应用
工作台
第三方企业应用
企业内部应用 / H5微应用
H5微应用
如何开发
创建应用

3. **点击创建应用**


创建应用
1 填写基本信息
2 配置开发信息
* 应用名称:
测试
名称可以由中文、数字及英文组成，长度在2-10个字符，可修改。点击了解更多《基本信息规范》
* 应用Logo:
点击上传
图片格式必须为：png、jpeg、jpg，建议大小为200PX*200PX，可修改
* 应用简介:
测试
请简要描述应用提供的产品或服务，最多32个字，可修改
* 开发方式:
企业内部自主开发 企业内部开发人员为企业开发应用
授权给服务商开发 企业内无开发团队，授权给定制服务商为企业开发应用
下一步

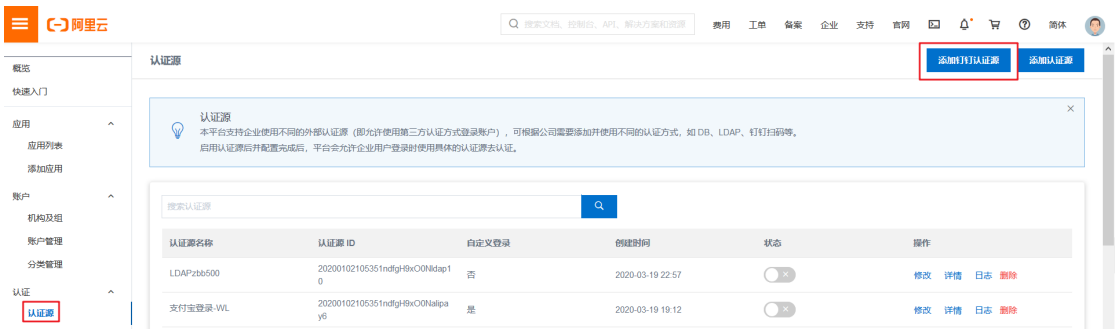
应用首页链接：在IDaaS上获取，获取方式参考下面步骤4

PC端首页地址：和应用首页链接一致即可

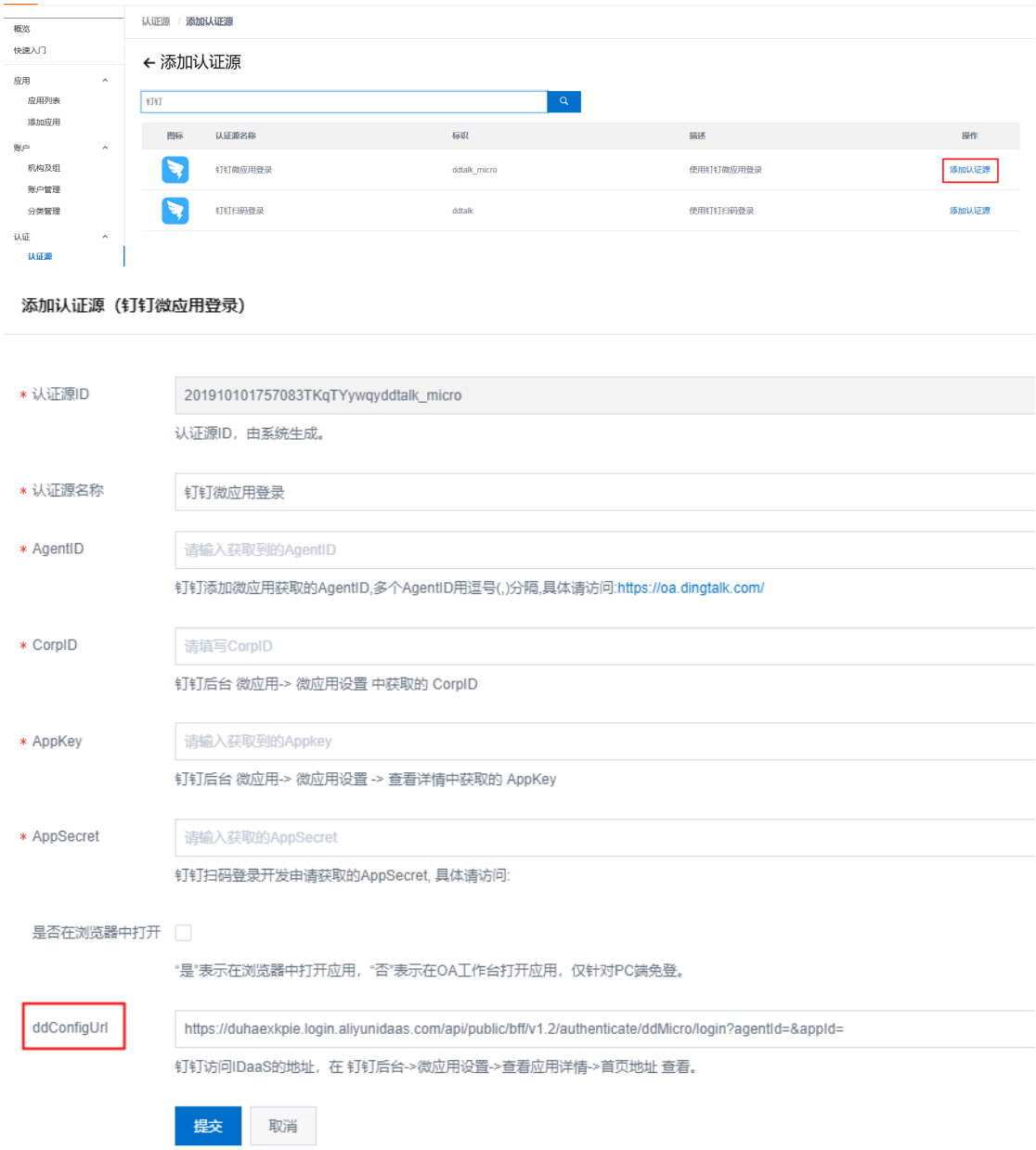
服务器出口IP：IDaaS服务器的出口IP

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-点击添加钉钉认证源



ii. 选择钉钉微应用登录-点击添加认证源



iii. 找到ddConfigUrl字段值：

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

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

v. 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。

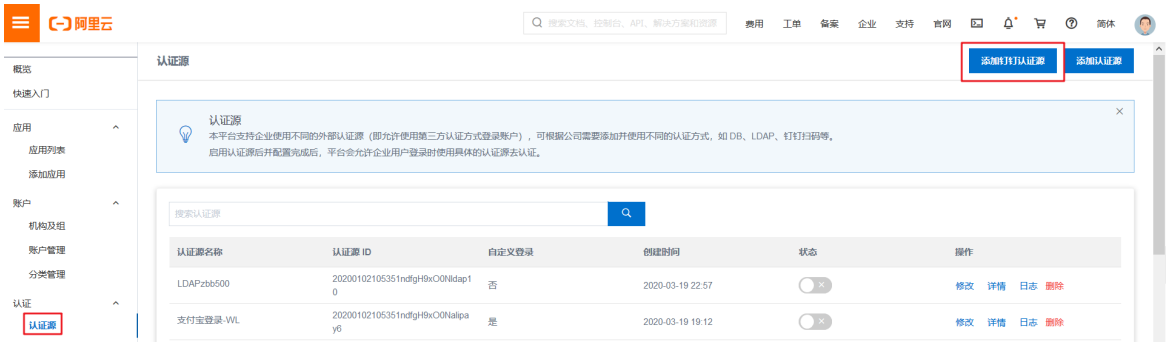
vi. 查看应用的详情，获取应用的AgentId参数

vii. 修改应用，把应用详情中的 AgentId 的值添加到 url 的 agentId 参数后面

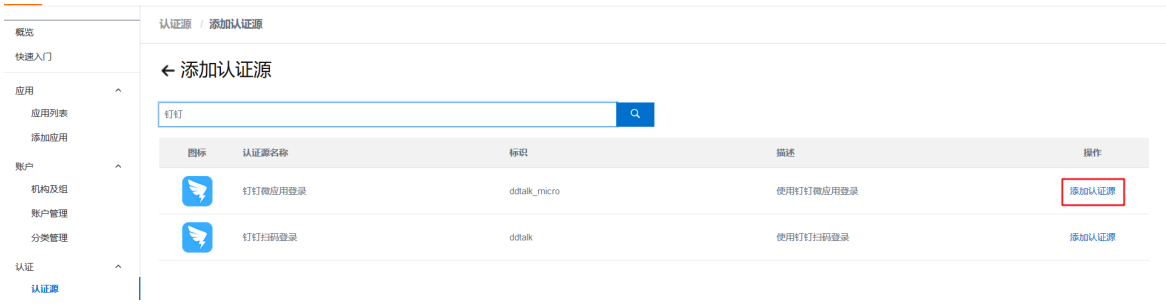
创建钉钉微应用认证源

操作步骤

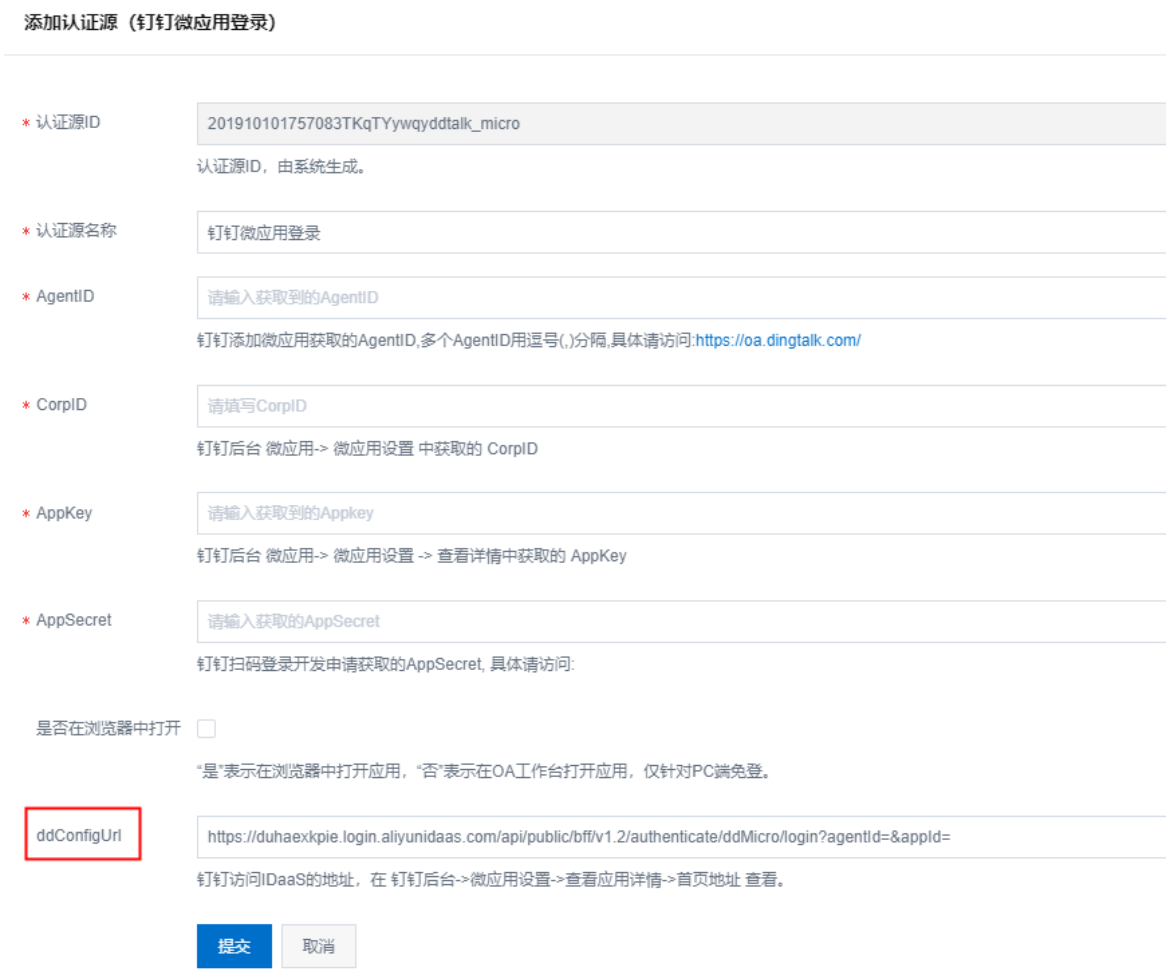
1. 在IDaaS管理员页面，点击认证源-点击添加钉钉认证源



2. 选择钉钉微应用登录-点击添加认证源

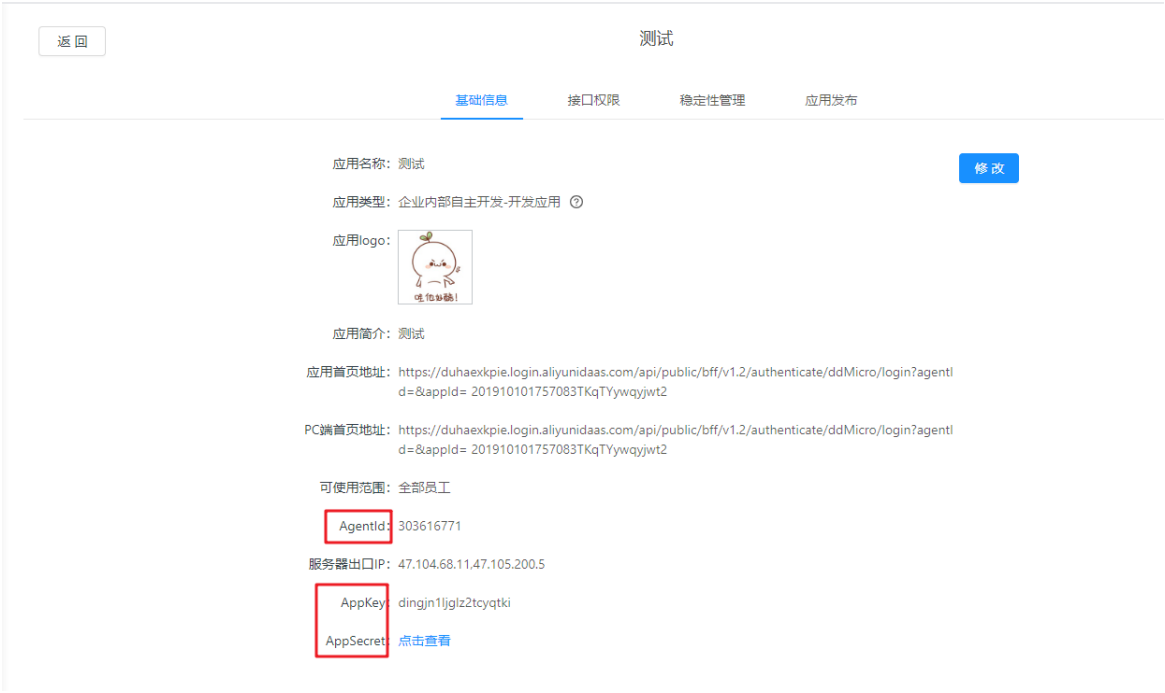


3. 配置钉钉微应用认证源参数



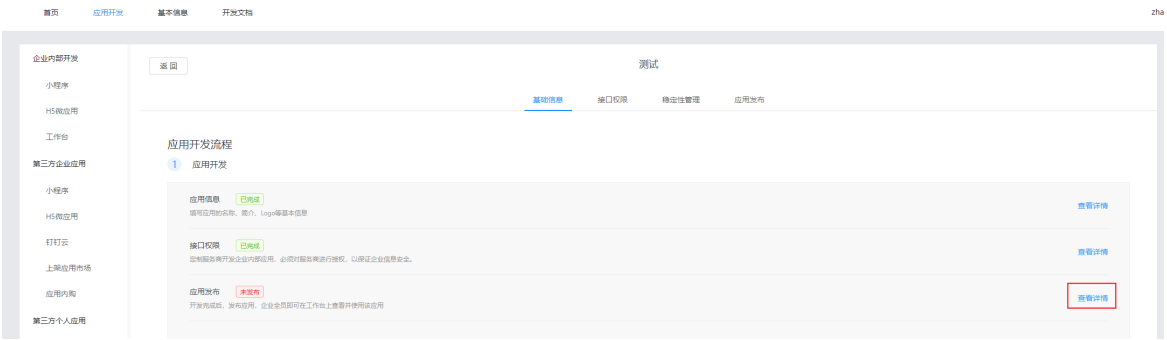
CorpID：登录钉钉开放平台首页展示的值

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上对应应用 **开发管理 > 服务器出口IP** 中添加上对应的IP地址。

1.6. 短信OTP认证登录

通过 IDaaS 认证源能力，配置使用短信接收OTP码进行认证登录 IDaaS 平台。

前提条件

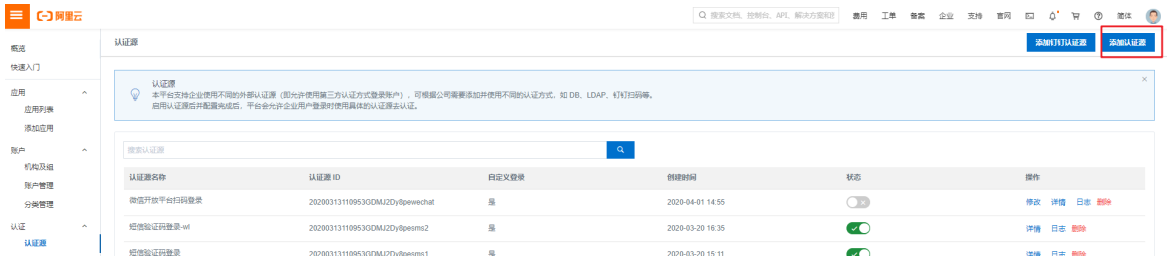
1、使用短信验证码登录的账户必须在IDaaS平台填写了手机号

2、管理员开启了短信网关 （配置阿里云短信服务）

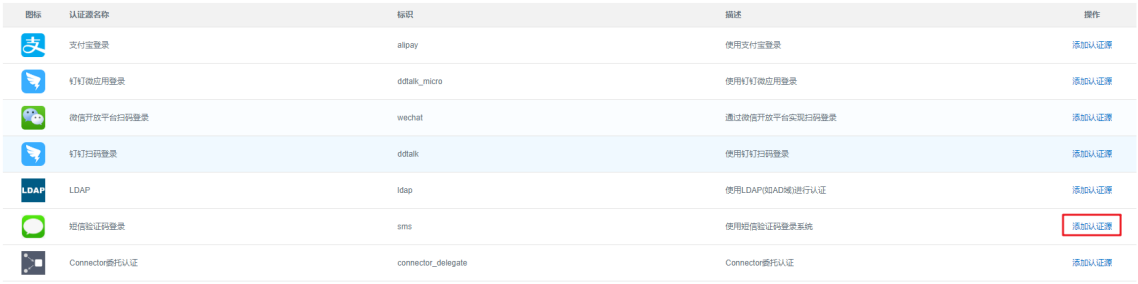
> **说明**
>
> 云上 IDaaS 内置了阿里云短信网关，可跳过该步骤。如果您希望使用第三方短信服务提供商的短信网关。也可以在 安全设置-短信配置中进行配置。

添加短信验证码认证源

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. 在左侧导航栏中，点击认证 > 认证源。在认证源页面，点击右上角的添加认证源按钮。

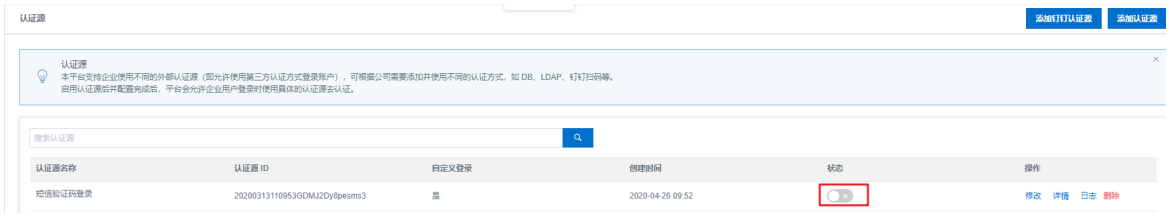


3. 选择短信验证码登录认证源，点击添加认证源



4. 配置短信认证源参数，并点击保存

5. 添加完成后，在认证源列表中启用它

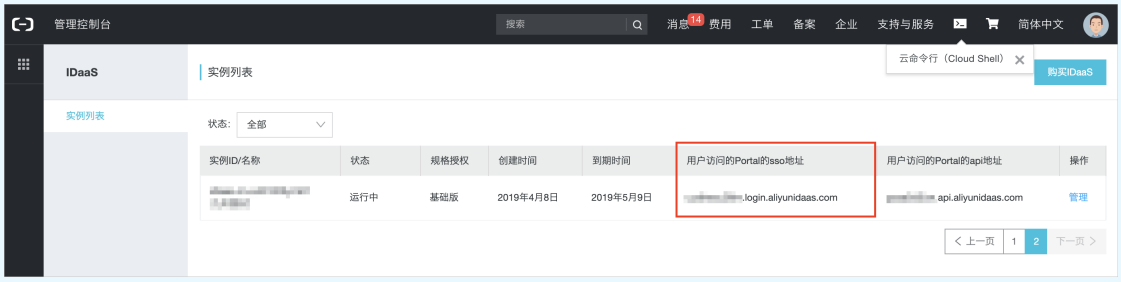


短信OTP码认证登录

成功添加短信认证源后，在用户登录页会出现短信认证源图标，用户即可使用短信验证码认证登录IDaaS。

1. 通过浏览器访问云盾 IDaaS 用户 Portal 地址（线下产品直接访问登录页）。

> **说明**
>
> 该地址由IT管理员提供。IT管理员可以在云盾IDaaS实例列表中查看用户访问的Portal地址。



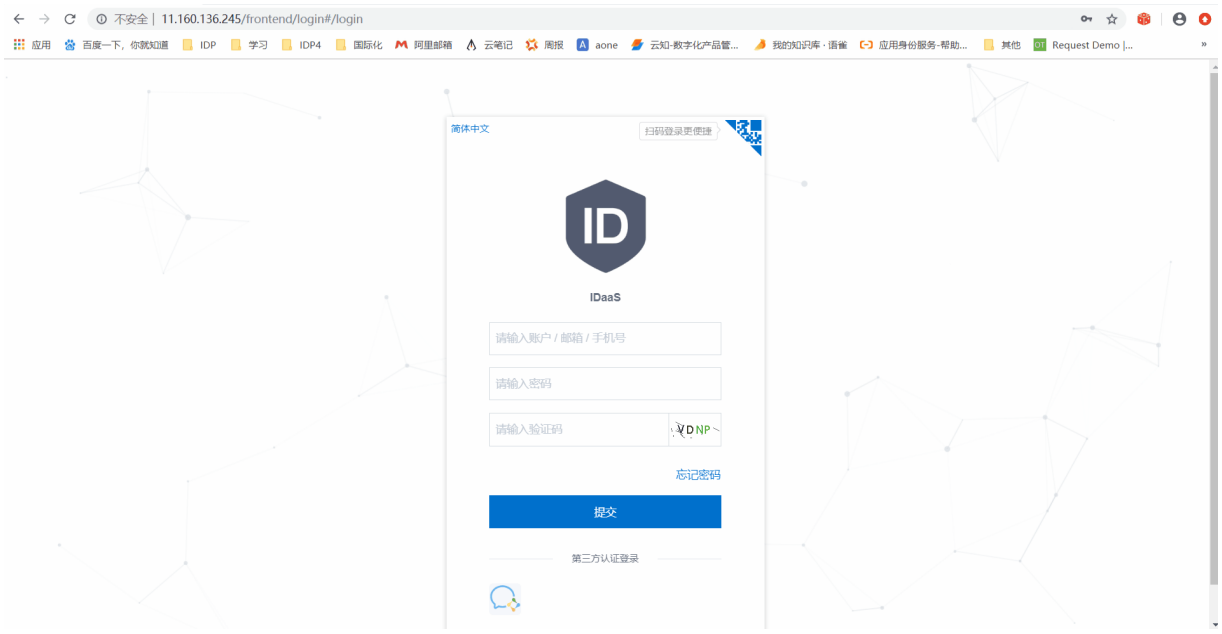
2. 点击短信认证源图标

3. 输入手机号和图片验证码获取短信验证码，再输入获取到的短信验证码即可登录IDaaS平台。

1.7. 企业微信扫码登录

本文为您介绍如何在 IDaaS 中添加企业微信认证源，实现企业微信扫码登录 IDaaS。

实现效果



使用流程

1）打开 IDaaS 用户登录页

2）点击选择左下角的【企业微信扫码登录】，界面显示登录二维码

3）手机移动端打开企业微信，通常和微信一样，默认已登录状态；如未登录，请先登录进入企业微信

4）使用扫一扫功能，对准屏幕二维码进行扫码登录

5）电脑浏览器显示扫描成功，手机移动端企业微信提示登录信息，点击【确认登录】

6）登录成功，浏览器显示 IDaaS 用户首页

配置流程

实现企业微信扫码登录 IDaaS 功能，主要有以下 3 个步骤

1）准备工作

2）IDaaS 认证源配置

3）企业微信应用配置

准备工作

1.1、IDaaS 标准版或专属版

备注说明：免费版不支持该功能，请升级标准版或按需升级至专属版 。

1.2、企业微信自建或第三方应用

备注说明：如之前未使用企业微信微应用，则创建新应用即可，具体操作步骤见本文最后 如何创建企业微信微应用。

1.3、登录 IDaaS IT管理员界面

登录地址：https://yundun.console.aliyun.com 或参考 管理员登录帮助文档

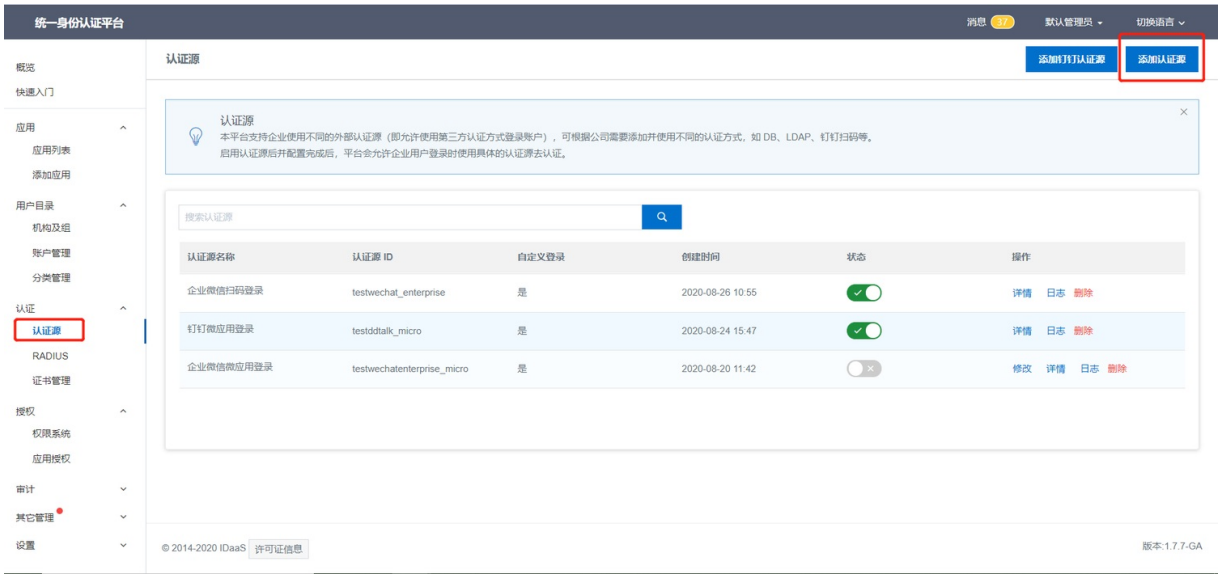
1.4、登录企业微信管理后台

登录地址：https://work.weixin.qq.com/wework_admin/loginpage_wx 可使用微信扫码登录。

IDaaS 认证源配置

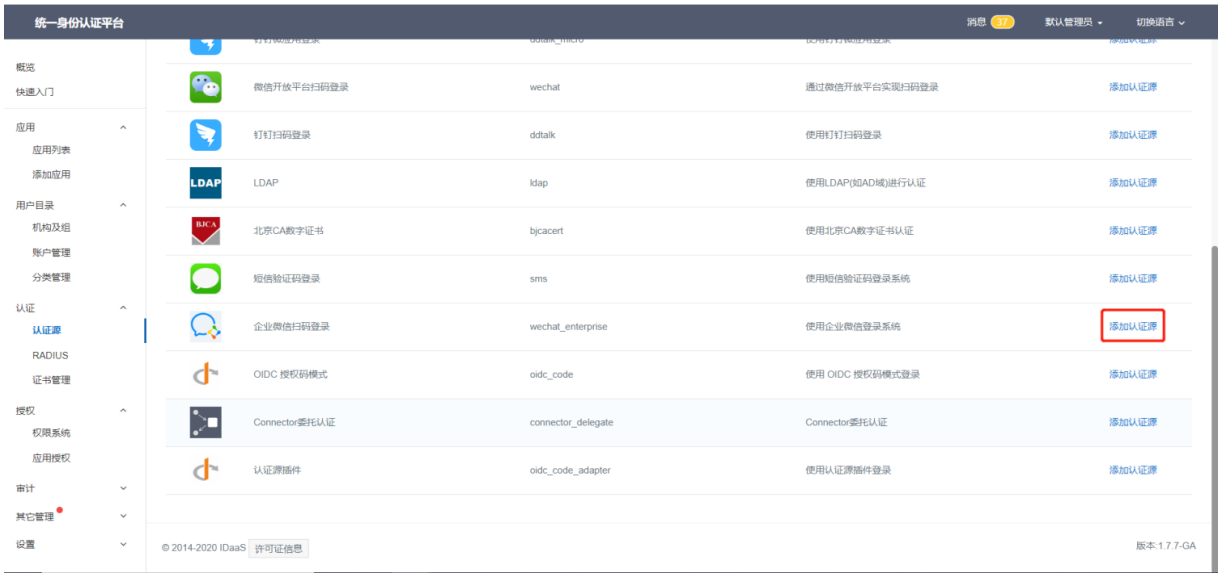
2.1、添加认证源

点击导航菜单【认证源】，点击右上角【添加认证源】

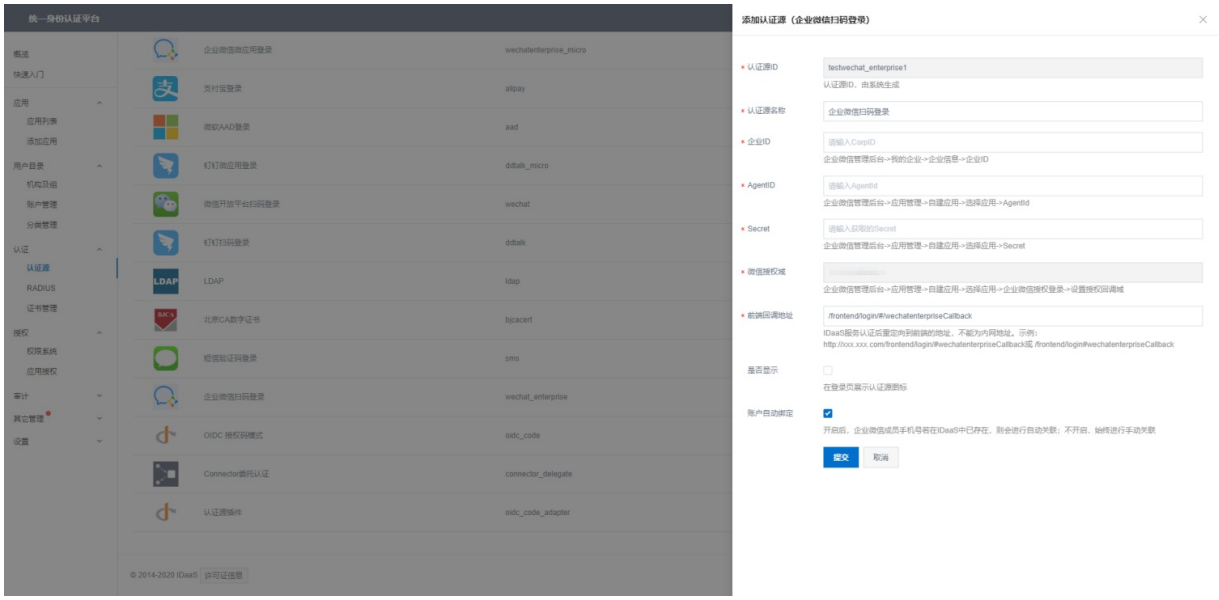


2.2、添加企业微信扫码登录

找到 企业微信扫码登录 认证源，点击【添加认证源】



2.3、填写认证源信息



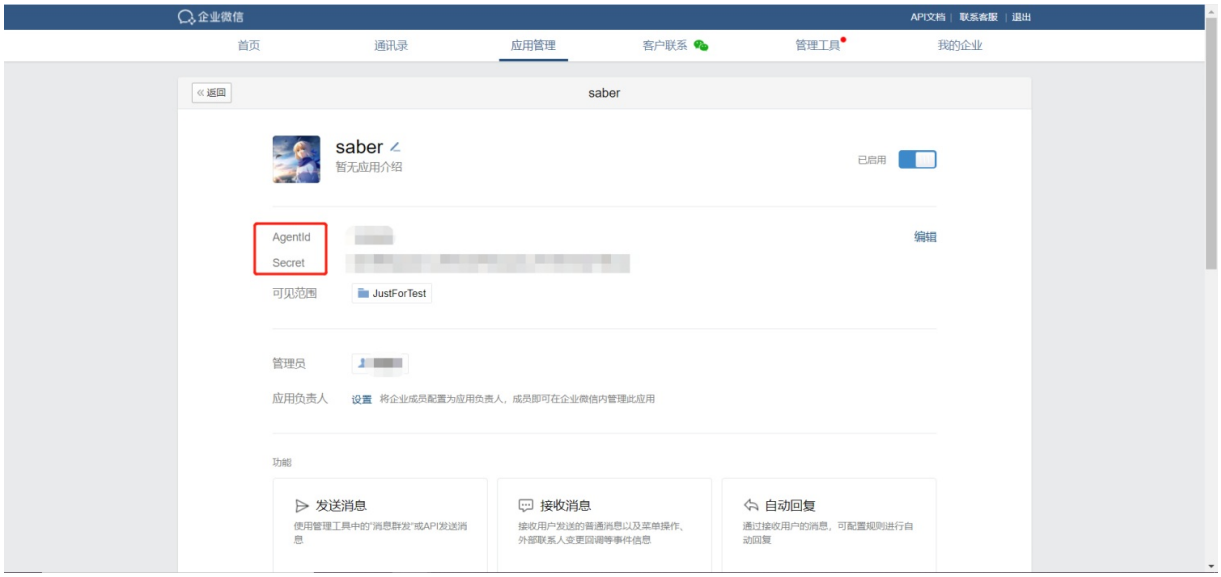
字段说明：

1.认证源 ID：系统默认生产，不可修改

2.认证源名称：通常填写为，企业微信扫码登录，也可自定义

3.企业ID：企业微信管理后台 【我的企业】最下方获取 企业ID

4.AgentID：企业微信管理后台 【应用管理】，点击准备好的应用进入，即可看到 AgentID 信息



5.Secret：企业微信管理后台 【应用管理】，点击准备好的应用进入，即可看到 Secret 信息，如上图所示

6.微信授权域：系统默认生成，后续在配置企业微信应用时使用

7.前端回调地址：系统默认生成，无特殊情况，请勿修改

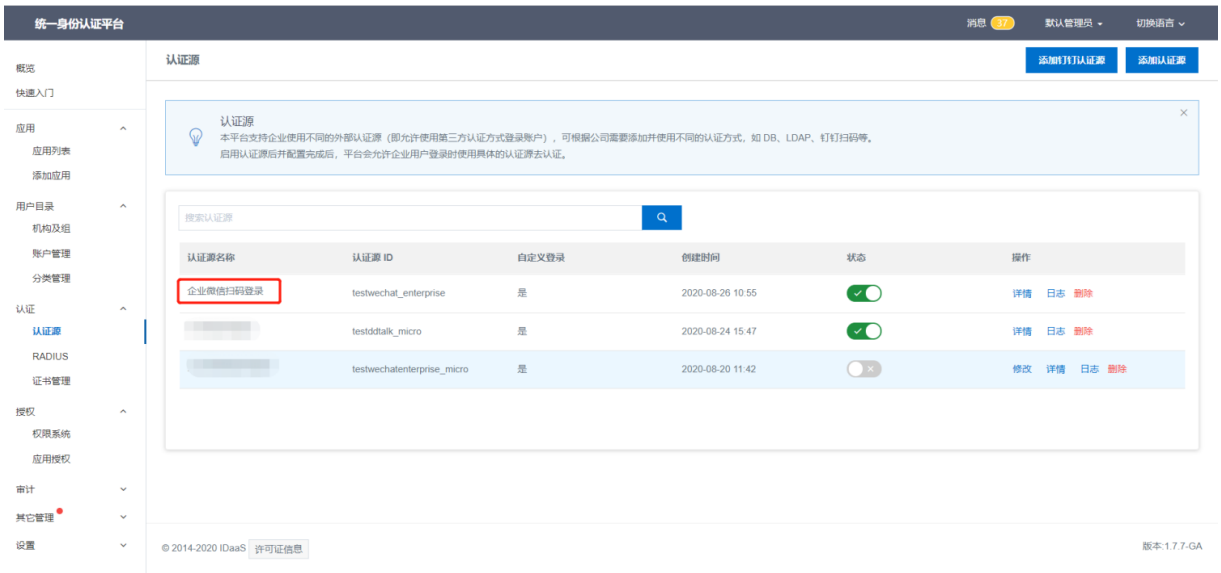
8.是否显示：勾选后会在用户登录页显示 企业微信扫码登录 LOGO图标，通常勾选

9.账号自动绑定：勾选后，会将企业微信成员的手机号与 IDaaS 成员的手机号自动关联，不开启则需要手动绑定，建议勾选

2.4、提交保存

完成企业微信扫码登录认证源的信息填写后，点击【提交按钮】，进行保存。

保存成功后，可在界面看见新添加的 企业微信扫码登录认证源



企业微信应用配置

3.1、打开微应用

登录企业微信管理后台，点击【应用管理】，点击之前准备好的应用，进入应用管理界面。

3.2、进入企业微信授权登录

在界面的最下方，开发者接口一栏中，点击中间的企业微信授权登录的【设置按钮】

3.3、设置回调域

点击第一个 Web 页面的【设置授权回调域按钮】

填写内容为：在添加 IDaaS 认证源配置时生成的“网页授权可信域“字段，填写完成后点击保存

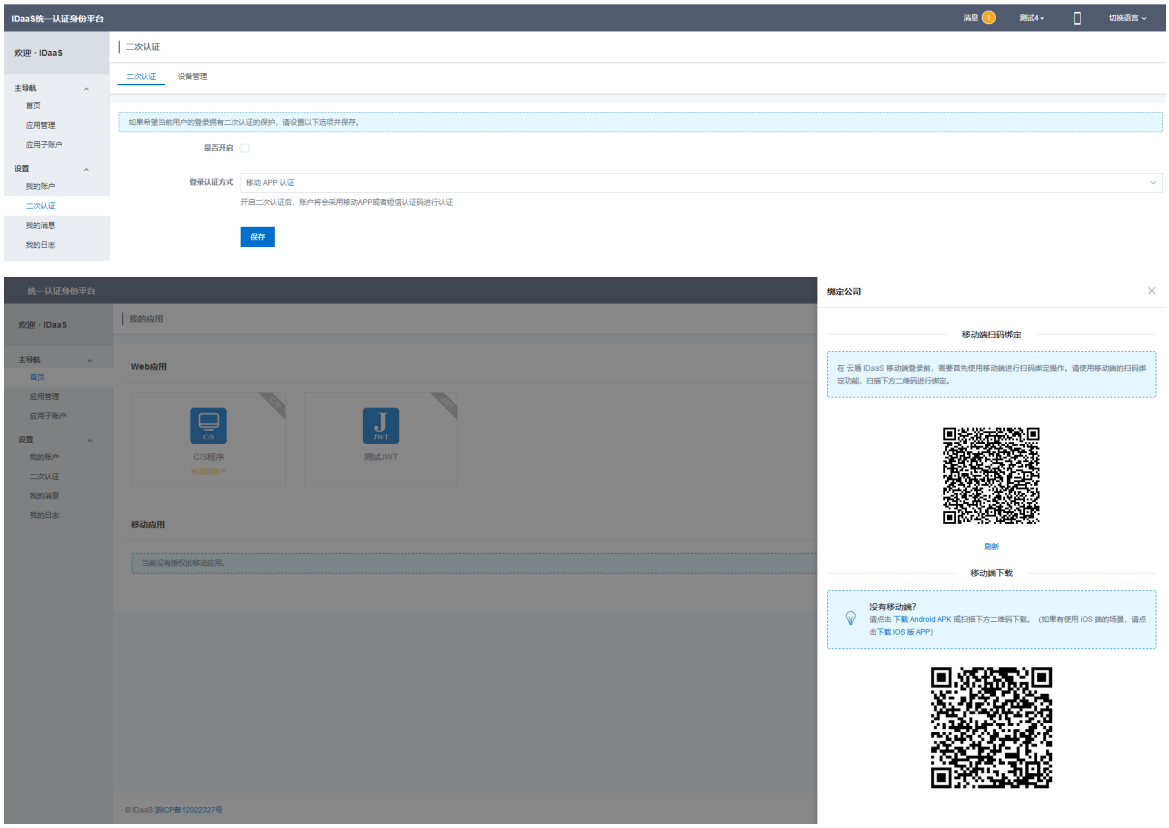
配置完成后，在 IDaaS 使用效果参考文档开头的“实现效果“。

2.移动端扫码登录IDaaS平台

本文为您介绍如何获取并绑定IDaaS的移动端应用-云盾IDaaS，并介绍如何通过移动端扫码登录IDaaS平台。

操作步骤

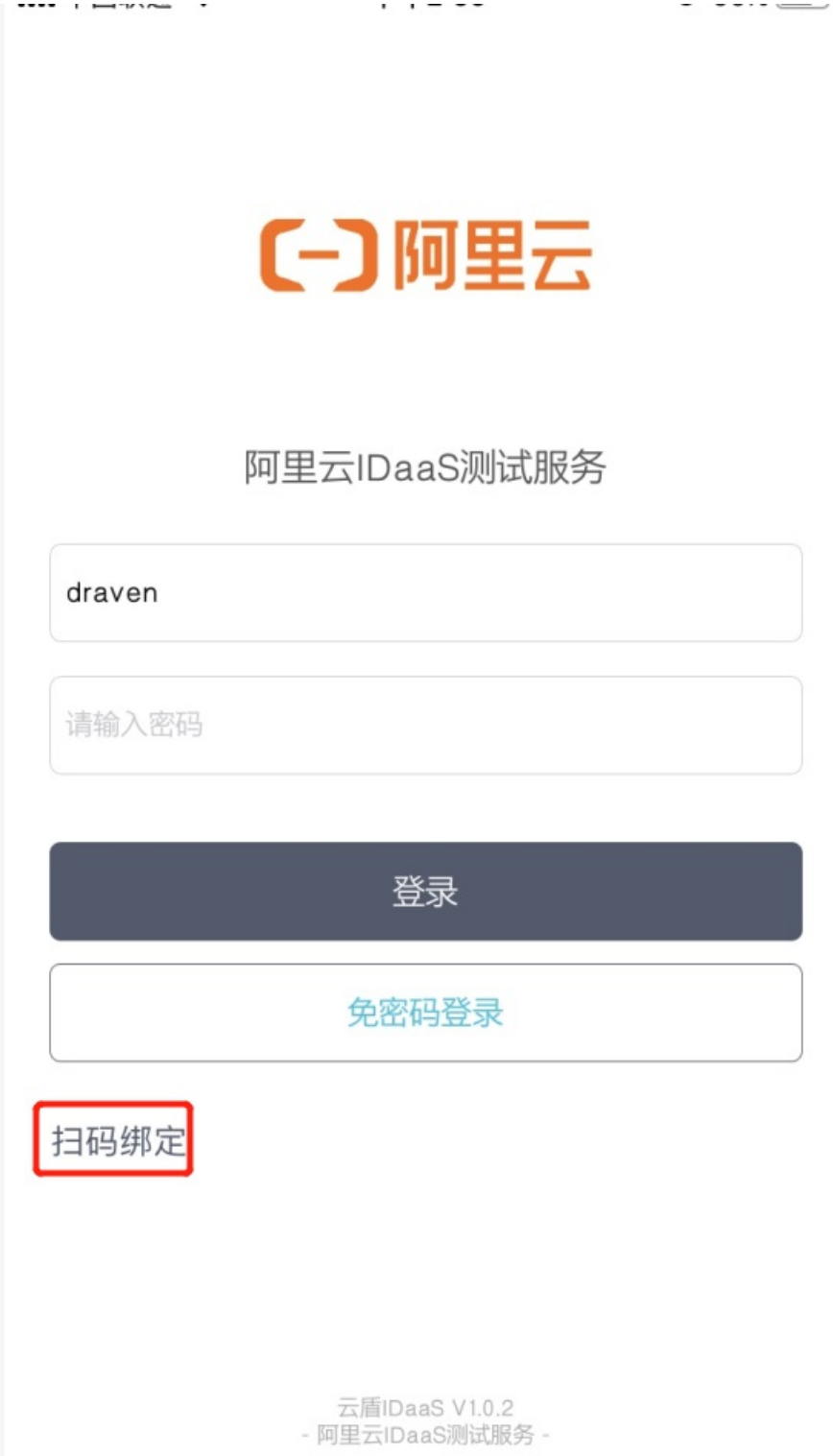
1. 使用普通用户账号登录云盾IDaaS控制台。具体操作请参考普通用户指南-登录。
2. 点击右上角的手机图标。使用微信或者其他APP在弹出的界面中，扫描第二个二维码进行下载。



3. APP扫码绑定公司

   在用户登录之前，需要扫描绑定登录的公司。之前若没有绑定过公司，应用界面如下图所示，点击“扫码绑定”扫描公司的二维码来绑定公司。

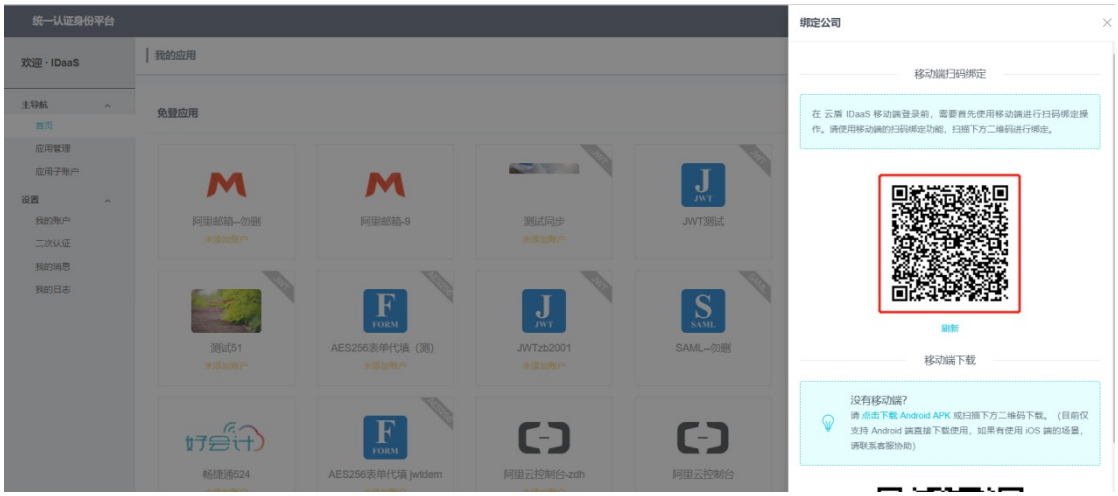
如果之前已经绑定过一个公司，想要登录到另一个公司的用户。可以在登录界面，点击“免密码登录”左下角的“扫描绑定”来重新绑定公司。



二维码获取来源：

i. 普通用户点击右上角的手机按钮，扫描弹出的第一个二维码进行扫码绑定。

ii. 企业管理员可以在安全设置的“移动端绑定设置”中获取公司的二维码。



4. 打开移动端APP，绑定完公司之后，输入用户的账户名和密码并点击登录，成功进入APP表示登录成功。

成功的登录一次之后，APP会自动把该账户的证书下载到本地，下次登录则可使用免密码登录，直接点击“免密码登录”即可登录成功。

5. PC端扫码登录功能

打开普通用户登录地址并在登录界面点击右上角二维码切换为扫码登录。打开云盾IDaaS应用，使用扫码功能扫描登录界面的二维码即可登录成功。

完成以上操作，即可实现移动端扫码登录功能。

3.二次认证

本文为您介绍IDaaS的二次认证功能。开启IDaaS的二次认证功能，能够在校验账号密码的同时校验app上的动态口令或者短信验证码，从而确保用户账号的安全性。

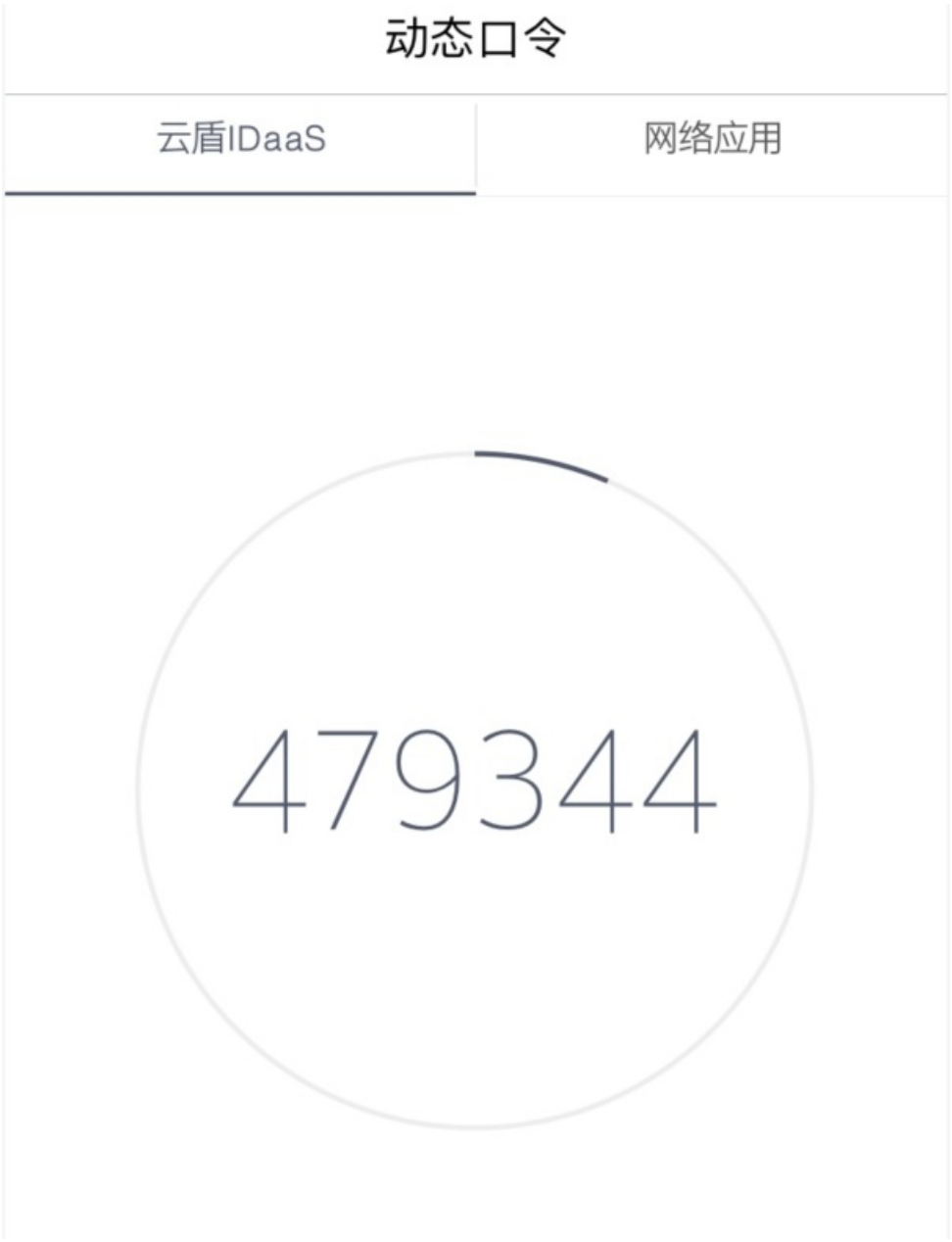
用户开启APP二次认证

登录普通用户开启APP二次认证功能（账户需要登录 云盾IDaaS APP）。

- 功能介绍：用户开启二次认证后，后续登录则需要进行二次认证，可使用APP上的动态口令进行二次验证登录，或摇一摇手机进行登录，或在APP上进行授权登录。
- 操作步骤：
  i. 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。
  ii. 在用户界面点击左侧导航栏设置中的二次认证。点选开启二次认证，并且认证方式选择移动app认证。

用户在开启二次认证之后的登录界面如下图，用户可以通过手机摇一摇或者在APP上进行授权登录。

用户也可以在输入框中输入APP中的动态口令进行登录。



用户开启短信二次认证

登录普通用户开启短信二次认证（该账户必须绑定手机号）。

- 功能介绍：用户开启短信二次认证后，使用短信验证码作为二次认证的凭据进行登录。
- 操作步骤：
  i. 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。
  ii. 在用户界面点击左侧导航栏设置中的二次认证。点选开启二次认证，并且认证方式选择短信认证码认证。

用户在登录IDaaS时，IDaaS会发送短信认证码到用户的手机中，用户在输入框中输入短信认证码，完成二次认证，即可登录。

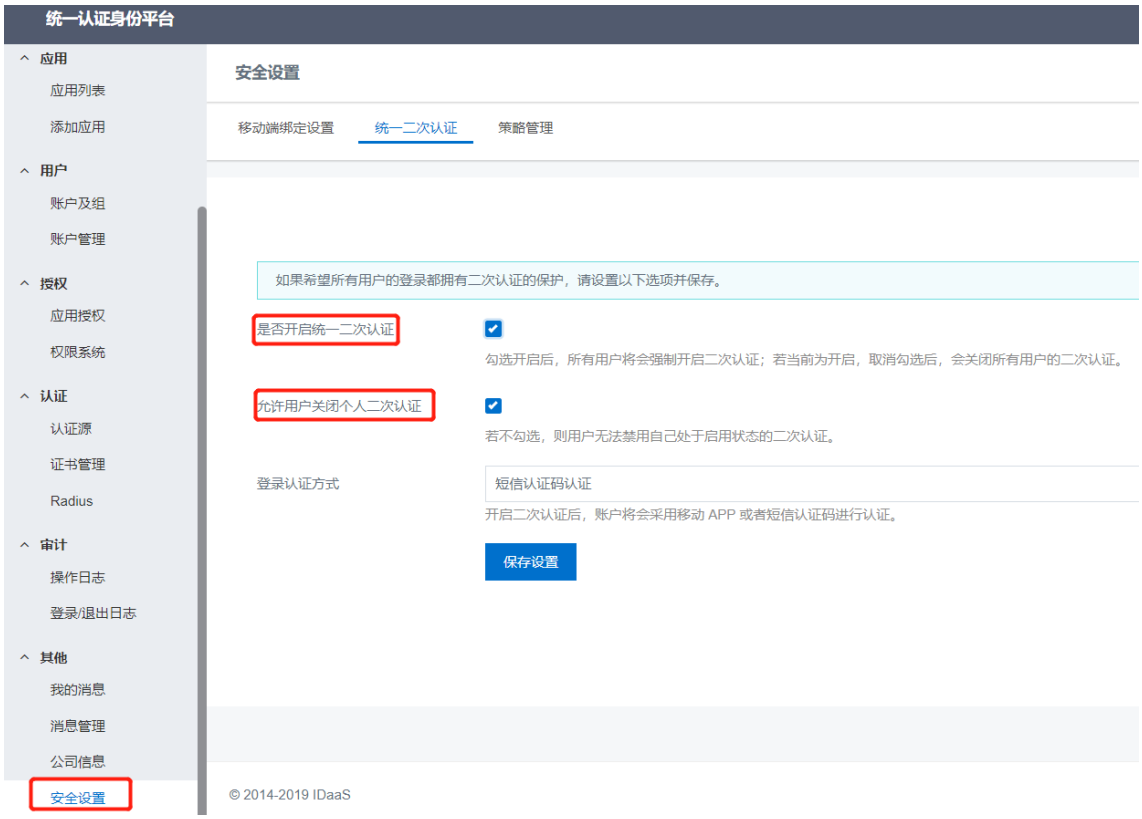
统一二次认证功能

管理员开启或关闭统一二次认证。

- 功能介绍：
  i. 若管理员开启统一二次认证，则所有的用户登录均需要进行二次认证（APP二次认证或短信二次认证）。若关闭统一二次认证，则所有的用户登录都不需要二次认证。

ii. 若管理员开启允许用户关闭个人二次认证功能，则用户登录后，可关闭二次认证。若管理员未开启允许用户关闭个人二次认证功能，则用户登录后，不能关闭二次认证。

- 操作步骤：
  i. 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。
  ii. 管理员在左侧导航栏中点击安全设置，点击统一二次认证。然后通过勾选来开启或关闭统一二次认证功能和允许用户关闭个人二次认证功能。



如果管理员开启了统一二次认证功能，并且关闭了“允许用户取消个人二次认证”功能，则用户取消二次认证会失败，并且提示“公司不允许用户关闭二次认证”。

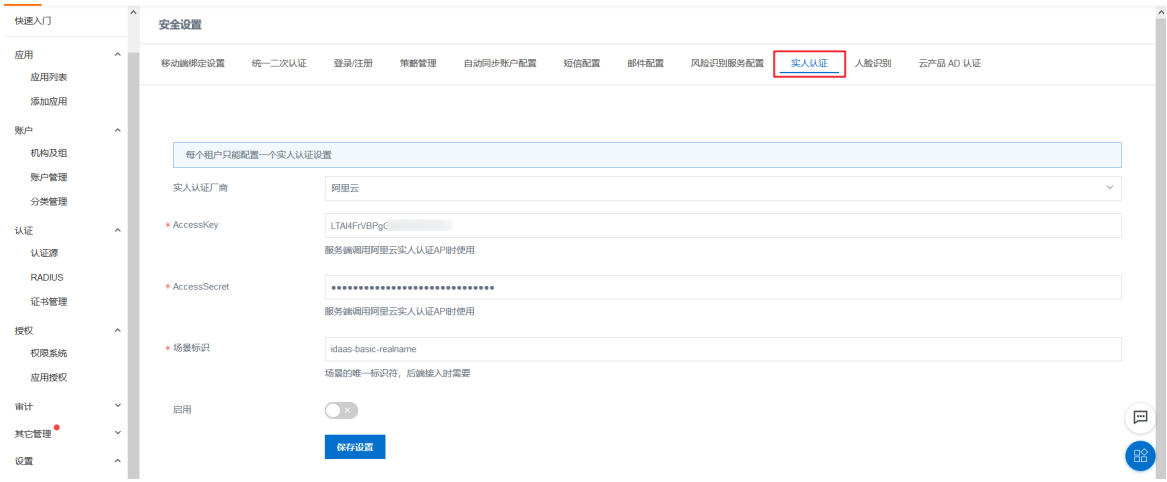
通过上述步骤，实现了用户登录二次认证功能。

4.实人认证

IDaaS支持接入阿里云实人认证功能，进一步为客户提供平台价值，提高身份验证的安全与便捷。

开启实人认证

1. 参考实人认证接入流程-准备工作开通实人认证服务，并配置**实人认证场景**。
2. 在阿里云AK管理平台获取用户的Access Key ID与Access KeySecret。
3. 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。
4. 在左侧导航栏，点击**设置 > 安全设置**。
5. 点击 **实人认证** 页签，在页面上进行实人认证的配置。



i. 实人认证产商选择阿里云

ii. 将获取的用户Access Key ID与Access KeySecret填写到对应位置

iii. 填写场景标识

> **说明** 场景标识为用户在实人认证控制台，新增实人认证场景时填写的场景标识

iv. 启用功能并点击保存设置。

完成上述步骤，即可开启实人认证功能

用户进行实人认证

前提条件

管理员开启并配置了实人认证功能

操作步骤

1. 用户登录移动端云盾APP。具体操作请参考用户指南-移动端登录。
2. 在我的设置页面，点击安全中心

3. 点击实名认证，并根据页面提示信息进行实名认证 。

4. 实名认证成功后，可在管理员页面查看对应账户的实名认证信息。


账户管理 / 账户详情
← 账户详情 ( )
账户信息
已授权应用
应用子账户
隶属于组织机构
设备
报表
实名认证信息
实名认证信息
姓名
林
性别
男
民族
汉
身份证号
3501811
地址
签发机构
证件有效开始时间
20151225
证件有效结束时间
20251225

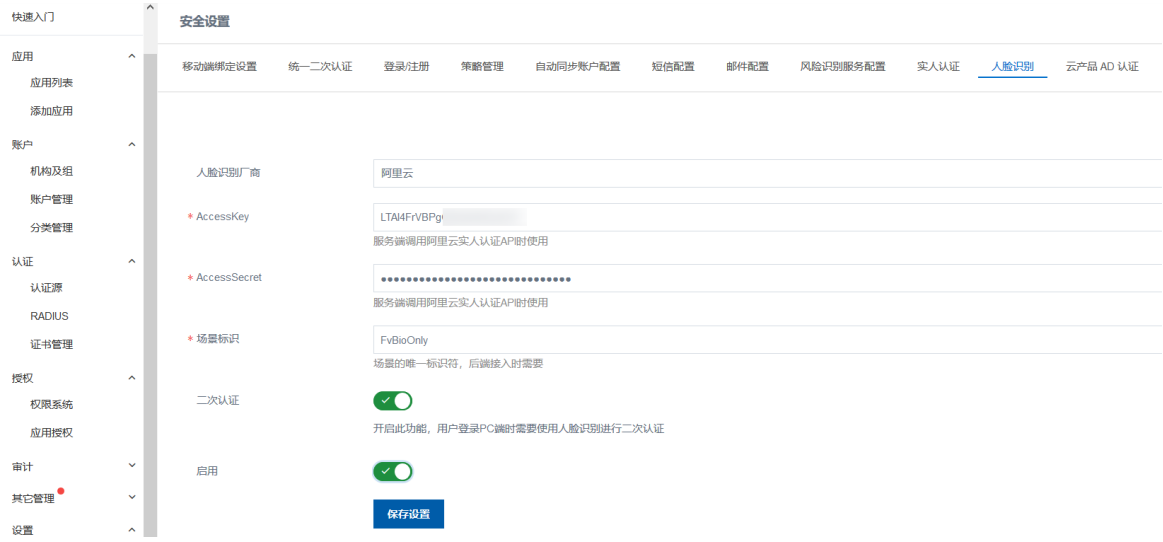
5.人脸识别

IDaaS支持接入阿里云实人认证服务的活体人脸验证功能，进一步为客户提供平台价值，提高身份验证的安全与便捷。用户通过实人认证后，可以扫脸免密登录到移动端，也可以使用扫脸完成PC端登录的二次认证。

启用人脸识别

操作步骤

1. 根据文档，开启并进行实人认证。
2. 参考活体人脸验证接入流程-准备工作，配置**活体人脸验证场景**。
3. 在阿里云AK管理平台获取用户的Access Key ID与Access KeySecret。
4. 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。
5. 在左侧导航栏，点击**设置 > 安全设置**。
6. 点击 人脸识别 页签，在页面进行人脸识别的配置



i. 人脸识别厂商选择阿里云

ii. 将获取的用户Access Key ID与Access KeySecret填写到对应位置

iii. 填写场景标识

iv. 根据需求开启或关闭二次认证

> **说明** 开启人脸识别-二次认证功能后。如果用户开启了APP二次认证，在登录PC端时需要进行扫脸

v. 启用功能并点击保存设置

通过人脸识别免密登录到移动端

操作步骤

1. 用户登录移动端云盾APP。具体操作请参考用户指南-移动端登录。
2. 使用移动端进行实人认证，操作步骤可参考用户进行实人认证。如果已完成实人认证，可以跳过该步骤。
3. 在安全中心开启证书免密登录。

> **说明** 用户账户首次登录移动端时会自动下载移动端证书，并开启证书免密登录功能。如果没有下载成功，可以在PC端管理员页面 认证 > 证书管理 页面重置账号证书，然后手动在安全中心开启证书免密登录。

4. 点击人脸识别，开启人脸识别功能

完成上述步骤后，用户可以在app登录页点击免密码登录，使用人脸识别免密登录到移动端。


阿里云 IDAAS
请输入邮箱/手机号/账户名称
请输入密码
登录
免密码登录
扫码绑定
云盾IDaaS V1.6.2
- 阿里云 IDAAS -

使用人脸识别进行二次认证

操作步骤

1. 用户登录移动端云盾APP。具体操作请参考用户指南-移动端登录。
2. 使用移动端进行实人认证，操作步骤可参考用户进行实人认证。如果已完成实人认证，可以跳过该步骤。
3. 在移动端开启人脸识别功能。
4. 开启用户开启APP二次认证，可以参考APP二次认证。

完成上述步骤后，用户登录pc端登录进行二次认证时，需要在移动端进行人脸识别的安全验证。验证通过后，才可以登录PC端。

6.添加Radius配置

本文介绍IT管理员如何在云盾IDaaS控制台添加Radius配置。

背景信息

RADIUS（Remote Authentication Dial In User Service，远程用户拨号认证系统）是一种用于在需要认证其链接的网络访问服务器（NAS）和共享认证服务器之间进行认证、授权和记帐信息的文档协议。

RADIUS 服务器负责接收用户的连接请求、认证用户，然后返回客户机所有必要的配置信息以将服务发送到用户。

IT管理员可以在云盾IDaaS中添加Radius，实现OTP登录VPN、连接WI-FI等。

操作步骤

1. 以IT管理员账号登录云盾IDaaS控制台。
2. 在左侧导航栏，单击**认证 > Radius**。
3. 在Radius页面，单击**新建 Radius**。
4. 在添加Radius页面，完成以下配置：

> **说明** 配置好Radius各属性值，下载Radius config配置文件，并将其与Radius服务器 一起使用，可实现OTP登录VPN，连接Wi-Fi等。

配置	描述
Radius名称	为Radius命名，该名称必须保持唯一。
Radius认证端口	Radius认证端口，默认为1812。
Radius计费端口	Radius的计费端口，默认为1813。
Radius SharedSecret	Raduis的共享密钥，10位及以上字符串组合。
Radius连接超时时间	Radius连接超时时间，单位为毫秒（ms）。默认值为10,000，即10秒。

配置	描述
Radius认证方式	Radius 服务器 在当前系统进行认证的方式，可选值： ○ 账号 OTP ○ 账号 密码 ○ 账号 （密码 OTP） ○ 账号 密码（LDAP或其它数据库）。 **说明** 若选择该方式，需要在IDaaS中添加对应的认证源并开启。 其他配置： ○ 启用Radius计费功能：是否启用Radius计费功能。Radius 服务器默认作为认证服务器使用，不启用Radius计费功能。 ○ 授权公司所有账户：是否授权公司所有账户登录该Radius。若不授权，可通过分配组来进行细粒度授权。 ○ 支持账户硬件OTP：若勾选，如果账户有硬件OTP，则允许其使用。
硬件 OTP 允许误差	支持硬件OTP时，配置硬件OTP的时间误差周期。取值范围：0-10。默认是2，即前后两周期范围内OTP码都允许。
IDaaS平台服务器地址	公司所在的 IDaaS 平台服务器地址。
Radius Vendor	选择Radius供应商，可选值： ○ 未知 ○ 华为 ○ 思科 ○ WISPr
备注	备注信息。

5. 单击**新建RADIUS**，填写radius名称，点击确定即可。

6. linux服务器上**部署RADIUS Server**。

- 在IDaaS页面下载 RADIUS Server 安装包
- 安装包中有安全部署文档说明，直接使用/run.sh 命令启动， 不需要编译

FAQ

1. 使用radius认证提示 Invalid username

请排查 sharedsecret 参数是否添加正确。

2.显示下图报错内容

```
java.lang.IllegalStateException: aesDecrypt error
        at com.idsmanager.oidc.OIDCUtils.aesDecrypt(OIDCUtils.java:156)
        at com.idsmanager.oidc.OIDCUtils.aesDecrypt(OIDCUtils.java:129)
        at com.idsmanager.oidc.OIDCUtils.aesDecrypt(OIDCUtils.java:168)
        at com.idsmanager.radius.infrastructure.IDPOTPCodeRetriever.parseToResult(IDPOTPCodeRetriever.java:118)
        at com.idsmanager.radius.infrastructure.IDPOTPCodeRetriever.lambda$retrieve$0(IDPOTPCodeRetriever.java:90)
        at com.idsmanager.commons.utils.httpclient.HttpClientExecutor.executeWithException(HttpClientExecutor.java:11
7)
        at com.idsmanager.radius.infrastructure.IDPOTPCodeRetriever.retrieve(IDPOTPCodeRetriever.java:86)
        at com.idsmanager.radius.IDaaSRadiusServer.accessRequestReceived(IDaaSRadiusServer.java:109)
        at org.tinyradius.util.RadiusServer.handlePacket(RadiusServer.java:477)
        at org.tinyradius.util.RadiusServer.processRequest(RadiusServer.java:432)
        at org.tinyradius.util.RadiusServer.listen(RadiusServer.java:377)
        at org.tinyradius.util.RadiusServer.listenAuth(RadiusServer.java:334)
        at org.tinyradius.util.RadiusServer$1.run(RadiusServer.java:137)
Caused by: org.jose4j.lang.InvalidAlgorithmException: A256KW is an unknown, unsupported or unavailable alg algorithm
(not one of [RSA1_5, RSA-OAEP, RSA-OAEP-256, dir, A128KW, ECDH-ES, ECDH-ES+A128KW, PBES2-HS256+A128KW, A128GCMKW]).
        at org.jose4j.jwa.AlgorithmFactory.getAlgorithm(AlgorithmFactory.java:52)
        at org.jose4j.jwe.JsonWebEncryption.getKeyManagementModeAlgorithm(JsonWebEncryption.java:151)
        at org.jose4j.jwe.JsonWebEncryption.decrypt(JsonWebEncryption.java:181)
        at org.jose4j.jwe.JsonWebEncryption.getPlaintextBytes(JsonWebEncryption.java:79)
        at org.jose4j.jwe.JsonWebEncryption.getPlaintextString(JsonWebEncryption.java:72)
        at org.jose4j.jwe.JsonWebEncryption.getPayload(JsonWebEncryption.java:87)
        at com.idsmanager.oidc.OIDCUtils.aesDecrypt(OIDCUtils.java:154)
        ... 12 more
```

是因为使用的算法 Java不支持，需要更新JDK或 JRE下的jce 配置。

3. Radius 服务器部署在内网，但是可以访问到公网的IDaaS，是否可以这样部署。

可以。 Radius通过调用IDaaS API实现认证。