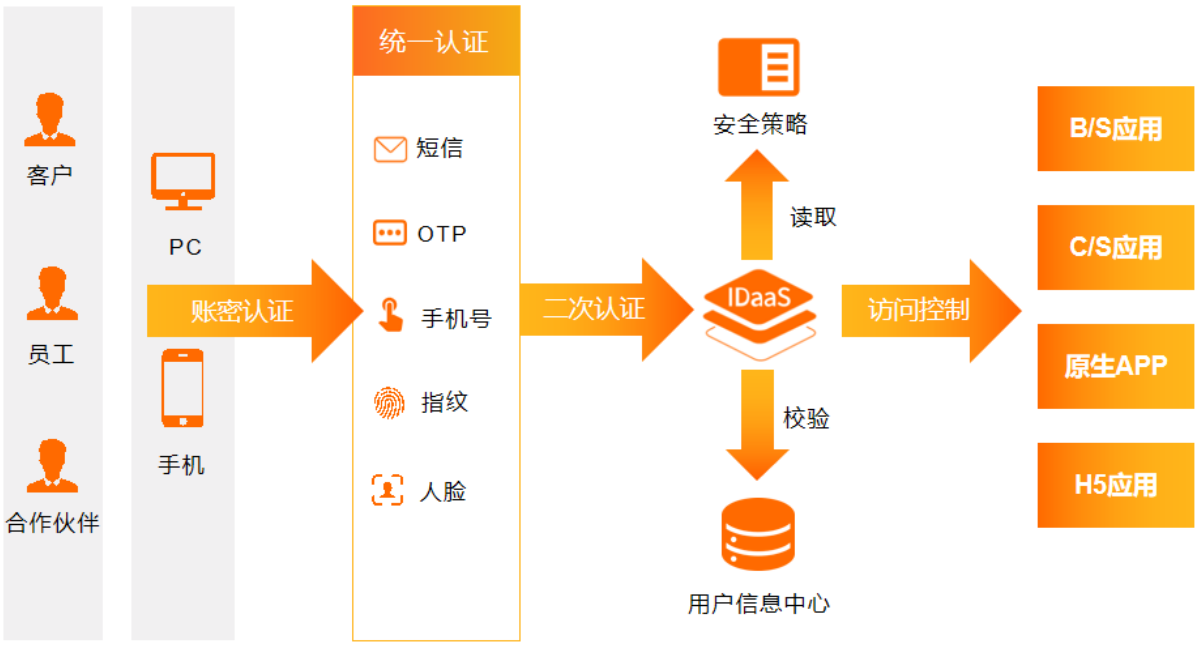
IDaaS-聚石塔对接文档-v1.8.5

1. IDaaS介绍

1.1 基本介绍

阿里云应用身份服务 IDaaS（英文名：Alibaba Cloud Identity as a Service，简称 IDaaS）是阿里云为企业用户提供的一套集中式身份、权限、应用管理服务。



针对聚石塔客户，使用 IDaaS 可以快速满足身份识别与访问管理能力，实现安全、高效、合规的账号防护。IDaaS 支持统一认证、自适应二次认证、弱密码监测、账号生命周期管理、异常账号锁定等众多账号防护能力，并预先对接了御城河所需的 IDaaS日志和二次认证日志。

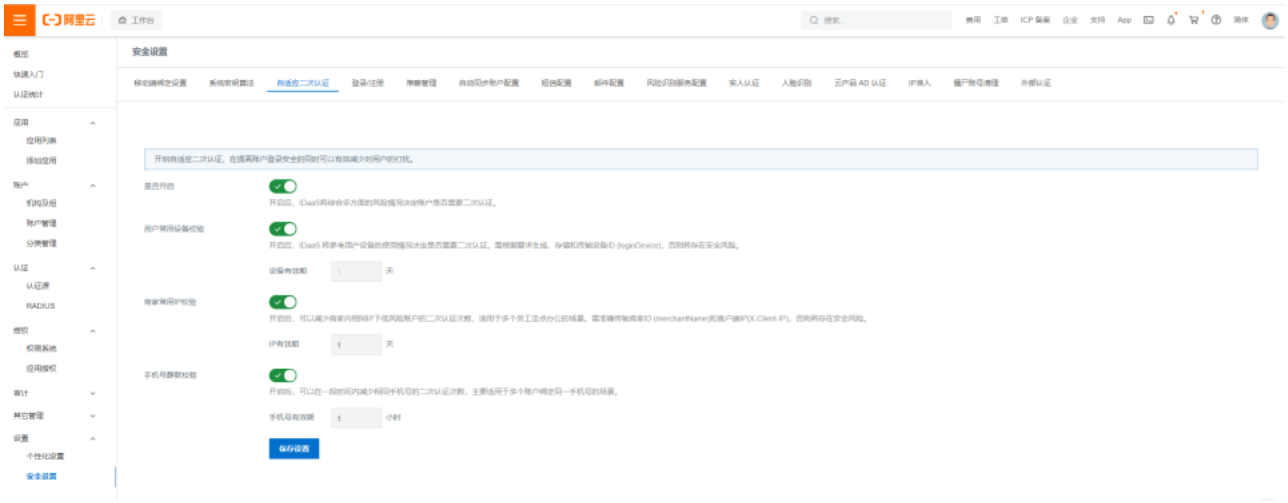
1.2 核心价值

1.2.1 全链路分级防护

IDaaS 支持全链路的分级防护能力，从秘钥、IP、账号三大层次，提供 IP 黑白名单防护、异常登录锁定、弱密码检测、图片验证码、僵尸账号管理等能力，**全面提高身份认证安全水位。**与此同时，IDaaS 还提供了可视化的图表界面，直观展示安全风险。

1.2.2 自适应二次认证

IDaaS 支持自适应二次认证，通过 IP、设备、手机号综合判断账号风险，智能判断用户是否需要二次认证。例如，通过智能识别可信的办公环境，同一个办公室/仓库内的员工可以大幅降低二次认证频率，**在大幅提高安全性的同时，有效降低对用户的打扰和短信费用的支出。**

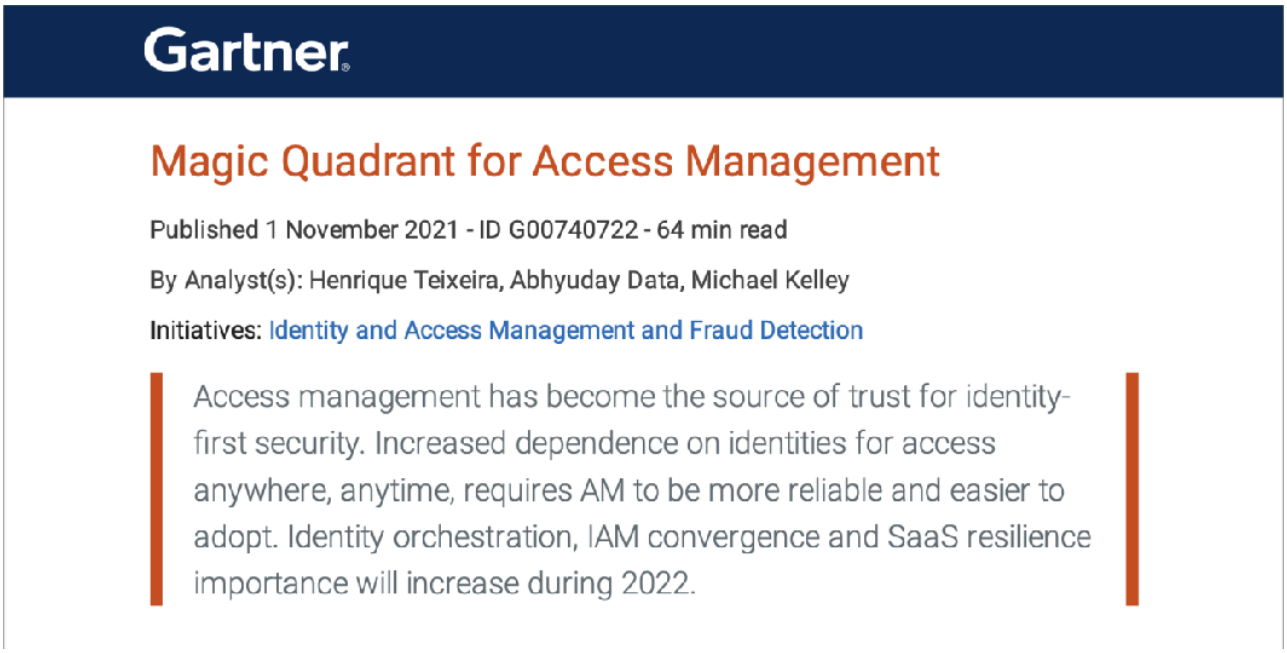


1.2.3 专业合规保障

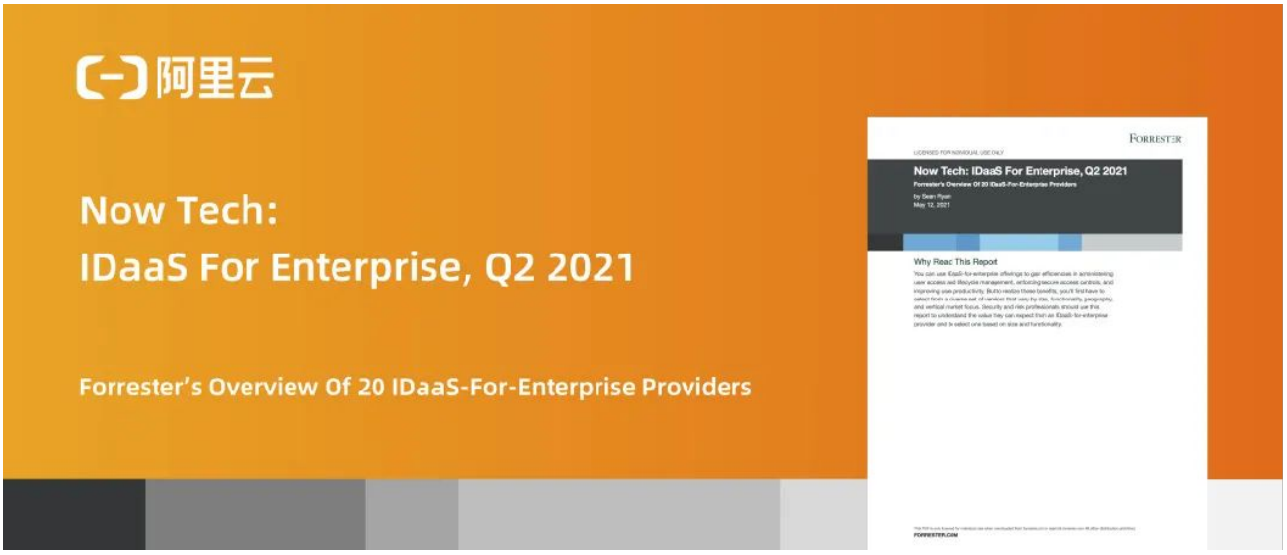
IDaaS 支持淘宝开放平台所需的身份识别与访问管理能力，**预先集成了御城河所需的 IDaaS日志和二次认证日志，自动实现上述日志的回流。**此外，IDaaS 还拥有 ISO、PCI、SOC、等保等一系列标准的合规资质，并确保安全合规能力的最及时、最完整的更新，对身份安全进行兜底保障，保障用户的身份安全无虞。

1.3 主要荣誉

阿里云 IDaaS 凭借强大的产品能力和丰富的实践案例，**是中国第一家也是唯一一家进入 Gartner AM 魔力象限报告的厂商**，打破了多年来国内无厂商入围的现状，实现零突破。



在国际知名研究机构Forrester发布的《Now Tech IDaaS For Enterprise, Q2 2021》报告中，阿里云 IDaaS 也凭借强大的产品能力和丰富的实践案例，成为**亚太地区唯一入围该报告的厂商。**



2. 购买说明

如果您在购买、对接、使用过程中遇到问题，**请使用钉钉搜索 33623553 加入支持群【备注 IDaaS】**，联系阿里云 IDaaS 团队进行支持。

2.1 新购流程

2.1.1 进入新购页面

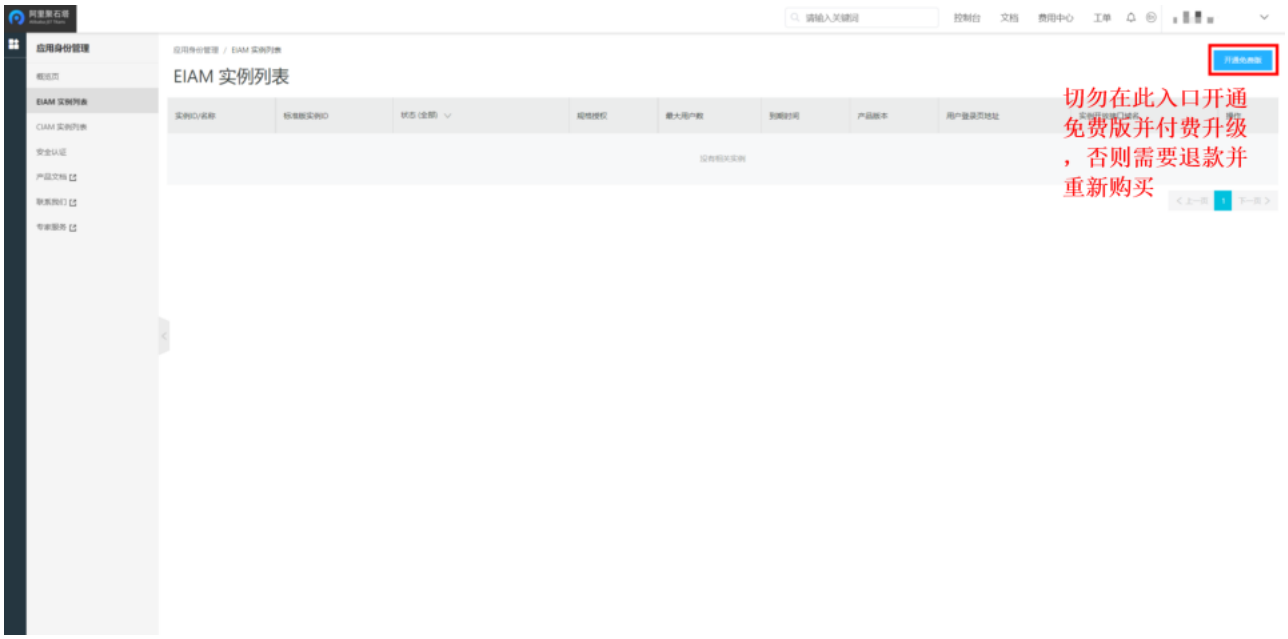
请通过如下方式进入购买页面：

1、登录聚石塔：https://console.cloud.tmall.com/home#/

2、点击 **资源视图–IDAAS**，进入 IDaaS 控制台

3、在浏览器输入购买链接：https://common-buy4service.aliyun.com/?commodityCode=idaas#/buy

请注意：IDaaS 暂不支持在阿里云购买，也不支持在聚石塔中开通免费版后升级购买（见下图）。如果您是通过免费版升级购买的实例，请尽快联系 IDaaS 团队进行退款，并通过上述方式购买。IDaaS 免费版及其升级版本的能力无法适用于聚石塔。



2.1.2 选择配置

在配置选择上，地域和可用区请选择 **华北3（张家口）**，功能规格请选择 **聚石塔**，产品规格请选择 **聚石塔–独享版**。我们提供了不同的 **套餐规格** 和 **购买时长**，请根据业务需求选择。

IDaaS 只根据认证成功次数计费，单价约2分~5分/次（聚石塔客户可享受专属折扣），有效期1年。登录失败、恶意攻击、图片验证码、OTP 二次认证、弱密码检测等能力不会计费。请根据每年实际用量评估购买。

请注意：

（1）一个 IDaaS 实例支持对接一个聚石塔应用，如果您有多个应用，请购买多个 IDaaS 实例。

（2）每年计费周期结束时，实例的认证次数将清零。例如，您22年1月1日购买了3年300万次认证次数，那么23年1月2日后您的300万次认证次数将过期，并获得第二年的300万次认证次数，以此类推。

（3）如果无法看到 地域和可用区–华北3（张家口） 或 功能规格–聚石塔，或者遇到其他问题，**请使用钉钉搜索 33623553 加入支持群【备注 IDaaS】**，联系阿里云 IDaaS 团队进行支持。

2.1.3 完成支付

选择好配置后，您将可以看到作为聚石塔客户所享受的专属折扣。点击右下角 **立即购买** 按钮，再次确认参数配置，即可进入支付流程。

完成支付后，实例将会自动开始创建，此过程大概耗时10分钟，请您耐心等待。当实例完成创建后，您可以进入实例，并根据该文档开始对接、使用 IDaaS 的安全能力。

请注意：

（1）正常创建的实例的产品版本格式为 idaas–jst–*，如非该格式，是购买途径有误所致，请联系 IDaaS 团队退款并重新购买。**

（2）IDaaS 实例根据认证次数收费，不限制用户数，请忽略实例中的用户数限制。

2.2 续费流程

2.2.1 进入续费页面

登录聚石塔（https://console.cloud.tmall.com/home#/），点击 **资源视图–IDAAS**，进入EIAM实例列表页面。点击需要续费的实例右边的 **续费** 按钮，进入续费页面。

2.2.2 选择配置

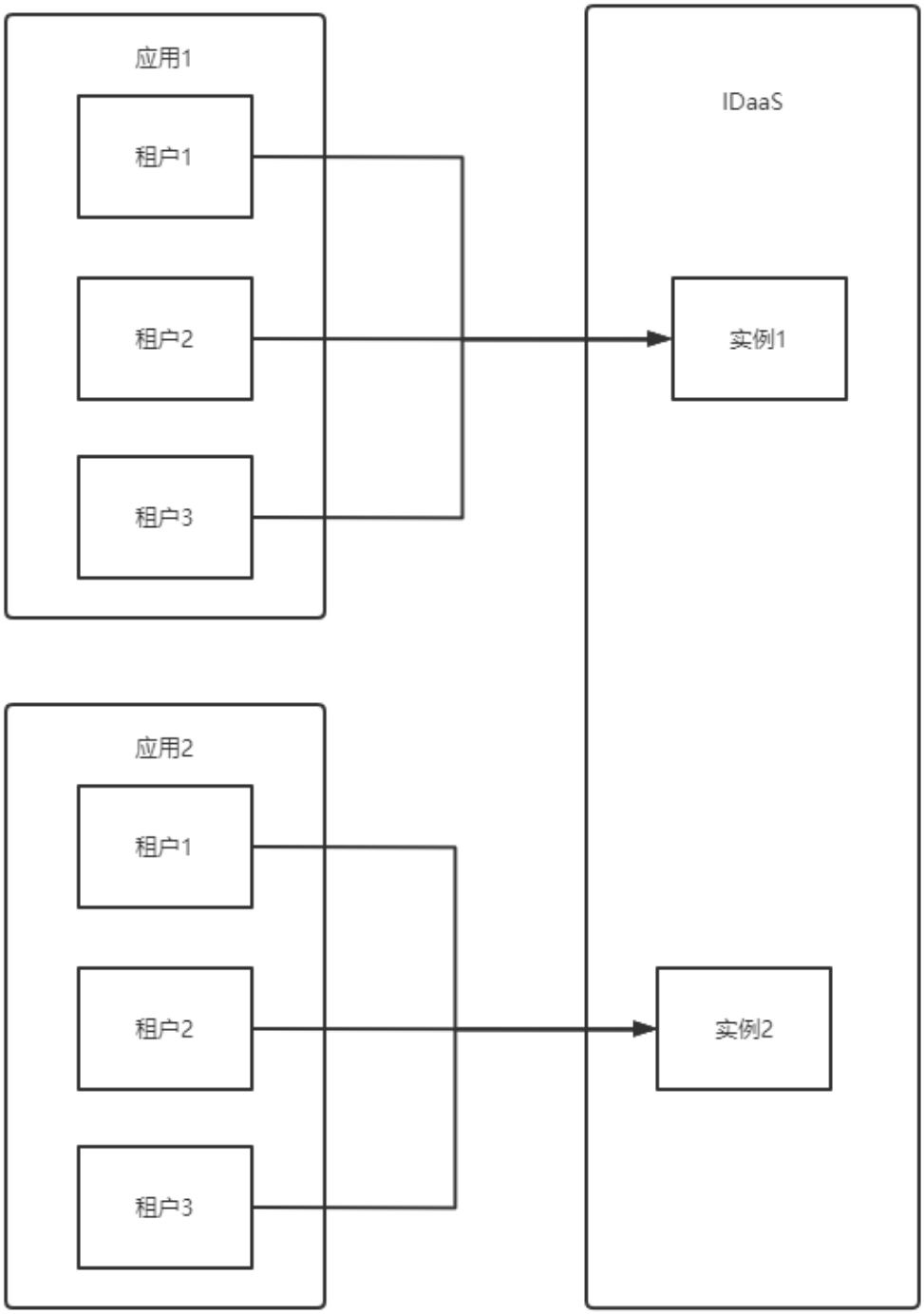
在续费页面，您只需选择续费的时长，完成支付后，该实例即可完成续费。

请注意：您需要在实例过期后7天内完成续费，否则实例将会被释放且数据无法恢复，从而对您的业务造成影响。

3. 对应关系

本章节介绍 IDaaS 与您的应用的对应关系，以便开发者了解 IDaaS 中的约束。IDaaS 支持多租户架构应用的对接，以下是 IDaaS 与应用的对应关系：

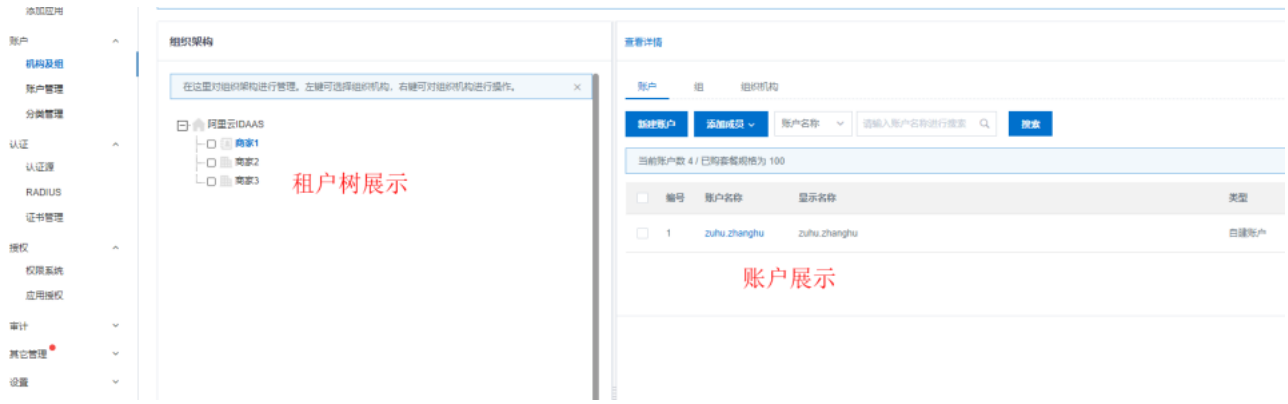
- 一个 IDaaS 实例，支持对接一个应用（如 ERP）
- 一个应用，支持对应多个租户（即淘宝商家，可以与 IDaaS 组织一一对应）
- 一个租户，支持对应多个账号（即应用中的账号，与 IDaaS 账户一一对应）



如果您的应用不存在一个账号对应多个租户的情况（比如账号 M 可以管理 A 商家和 B 商家），建议您创建一个租户后，调用 SCIM 同步接口，在 IDaaS 根节点下创建一个组织，对应租户的标识；在组织下面，您还可以增加子组织，可以对应租户在应用侧创建的组织机构。

如果您不希望将租户与账号的对应关系映射到 IDaaS 的组织中，也可以直接在 IDaaS 组织下创建账号。我们建议一个组织节点下的账号数小于 2000，以确保页面查询的高效。

在 IDaaS 中，允许不同的账号使用同一个手机号，以满足租户隔离时手机号重复的场景。账户名称需要唯一。

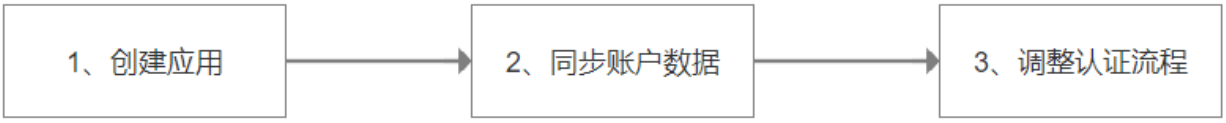


4. 对接说明

本章节介绍对接 IDaaS 的核心流程和操作步骤，以便您进行技术上的设计、评估和准备。

4.1 对接流程

您至少需要完成以下三步，才算完成了与 IDaaS 的对接。**以下改造不会在您的客户界面透传。**



1、在 IDaaS 创建一个应用，因为需要使用应用的 APP Key/Secret。

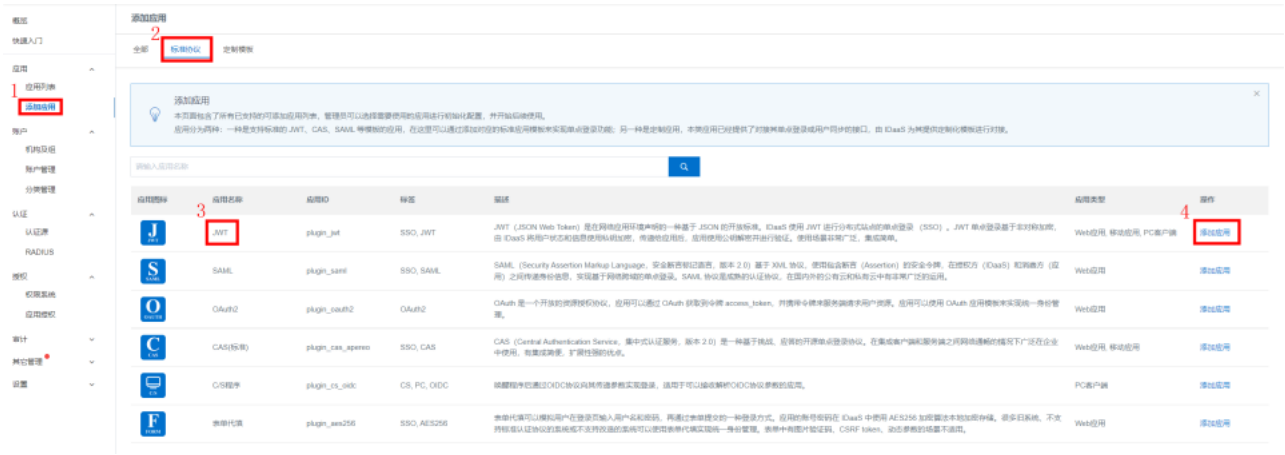
2、对接 IDaaS 同步相关接口，将您的应用的账户数据同步到 IDaaS。

3、对接 IDaaS 认证相关接口，将您的应用的认证请求切换到 IDaaS。

4.2 创建应用

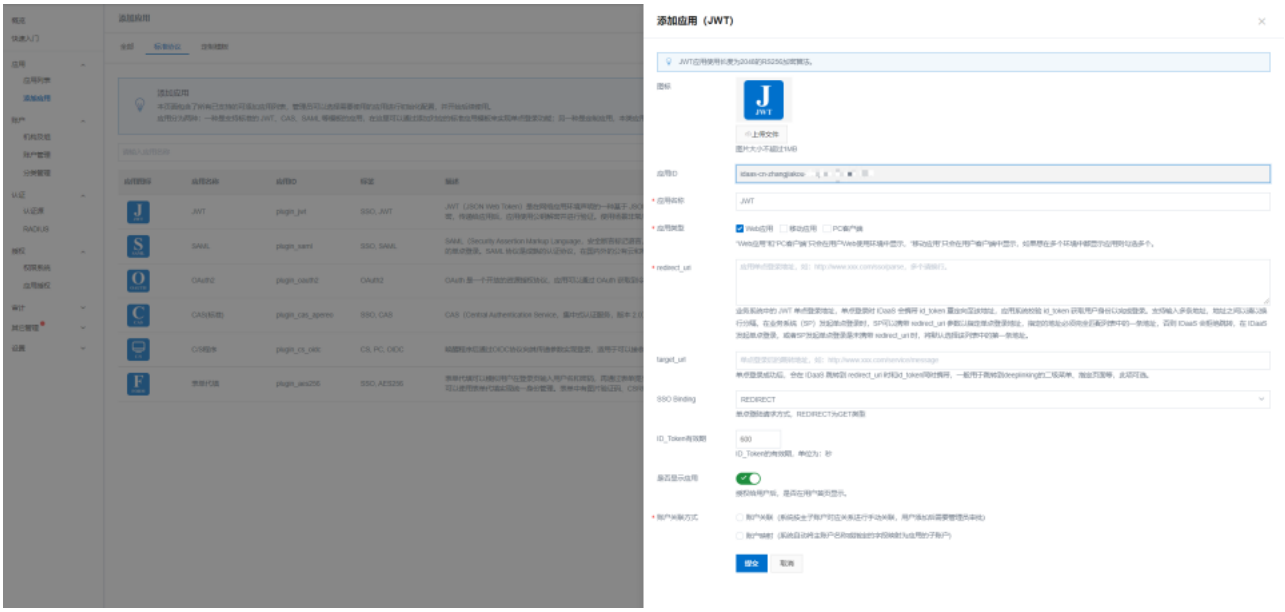
4.2.1 进入添加应用页

在 IDaaS 实例中，点击左侧的 **添加应用** 菜单，选择顶部的 **标准协议** 选项卡，找到 **JWT** 应用，点击右侧的 **添加应用** 按钮。



4.2.2 填写应用信息

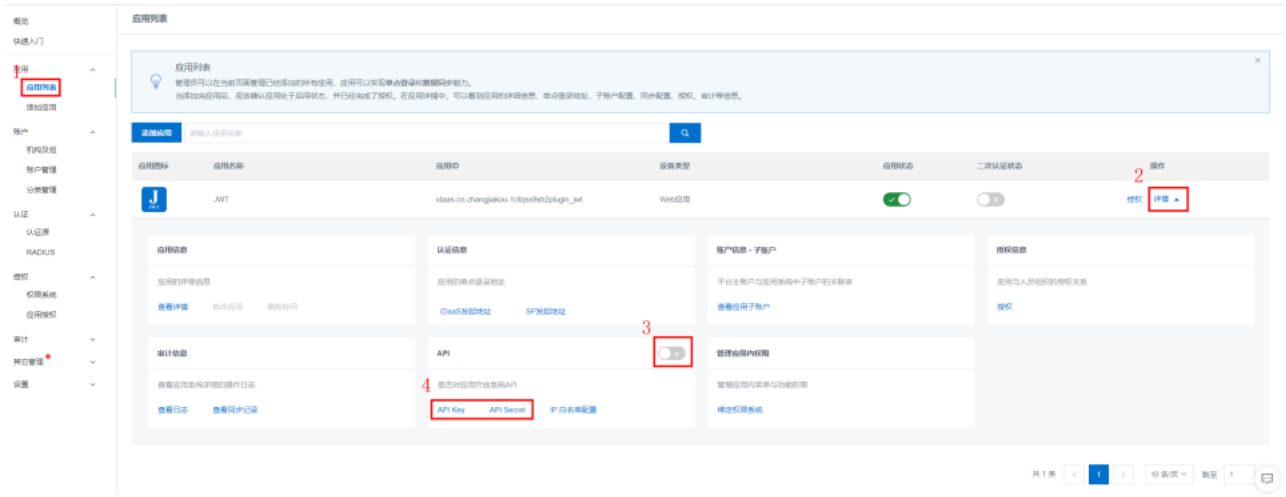
首先请准确填写应用名称；应用类型选择 **Web应用** 即可，当前暂不对应用类型作区分；redirect_uri 在聚石塔场景中暂无作用，填写符合字段规则的地址即可；账户关联方式选择 **账户映射**；其余非必填参数均不需要填写。完成填写后点击 **提交** 按钮，即可完成应用的创建。



4.2.3 获取 APP Key/Secret

完成应用的创建后，将自动跳转到 **应用列表** 页，此过程会弹窗提示您对应用进行授权，此时点击 **我知道了** 即可。

点击应用右侧的 **详情** 按钮，开启 **API** 开关后，依次复制 **API Key** 与 **API Secret** 并妥善保管。开启此开关时，意味着您对该应用进行了授权，应用将拥有权限调用该 IDaaS 实例中的 API，因此请您在妥善保管 API Key 与API 的同时，勿随意关闭 API 开关，否则应用将失去权限、无法正常使用 IDaaS 的能力。



4.3 同步账户数据

同步账户数据指的是您通过标准的同步接口将应用内的用户账号数据同步到 IDaaS，从而由 IDaaS 进行统一认证。IDaaS 会根据您的指令对账户进行增、删、改、查等操作。

IDaaS 准备了符合国际规范的、标准的 SCIM 同步接口，您只需对接 **本文档5.2章节** 中所提供的接口，即可完成同步相关能力的对接。

在 IDaaS 中，账户名称是唯一标识，且不可修改；手机号、邮箱可以重复。如果您的应用是多租户架构，建议您在同步账户数据时，在账户名称前拼接租户唯一标识，以防止账户名称重复导致同步失败。例如，test 租户内的账号 zhangsan，在 IDaaS 中账号名称可以为 test.zhangsan。

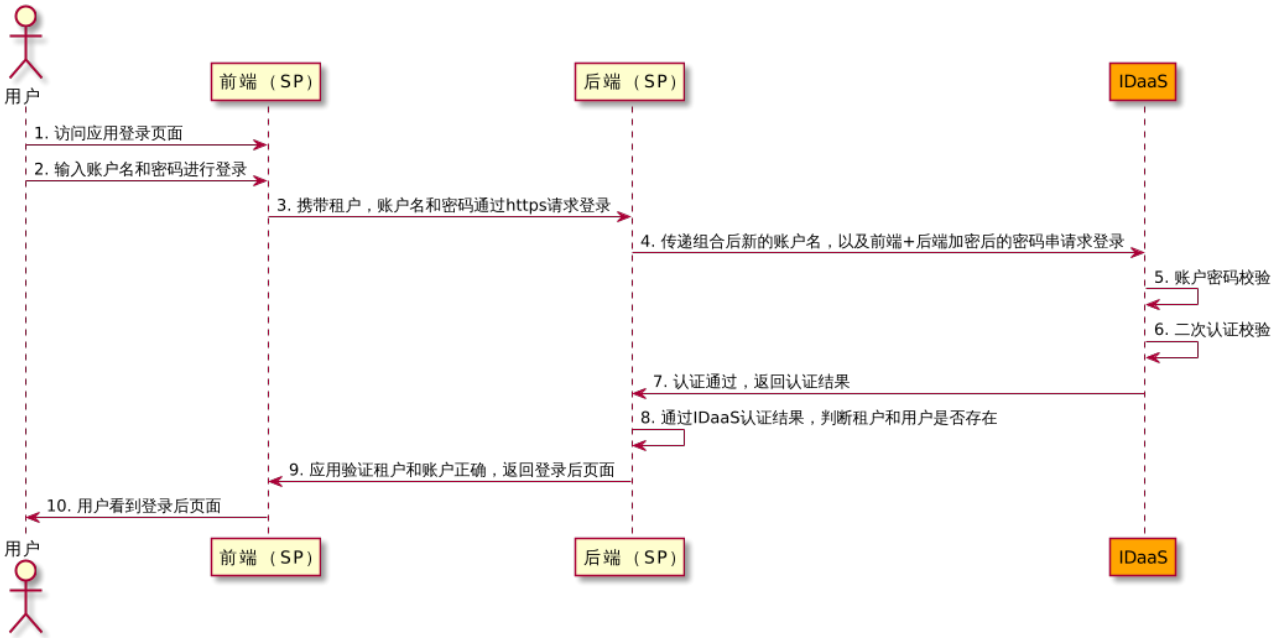
4.4 调整认证流程

除了同步能力的对接，您还需要对认证流程（即用户登录与二次认证流程）进行调整，本章节即是对认证流程进行深入的介绍，以便您进行设计和评估。改造后，将由 IDaaS 对您的用户进行统一的认证，为您的应用提供全链路的分级防护。

您需要对接 **本文档5.3章节** 中所提供的接口，进行登录流程调整；并根据业务需要对接 **本文档5.4~5.8章节** 中所提供的接口，进行二次认证流程的调整。

4.4.1 总认证流程

如下图所示，用户在登录时，由 IDaaS 进行统一的认证。



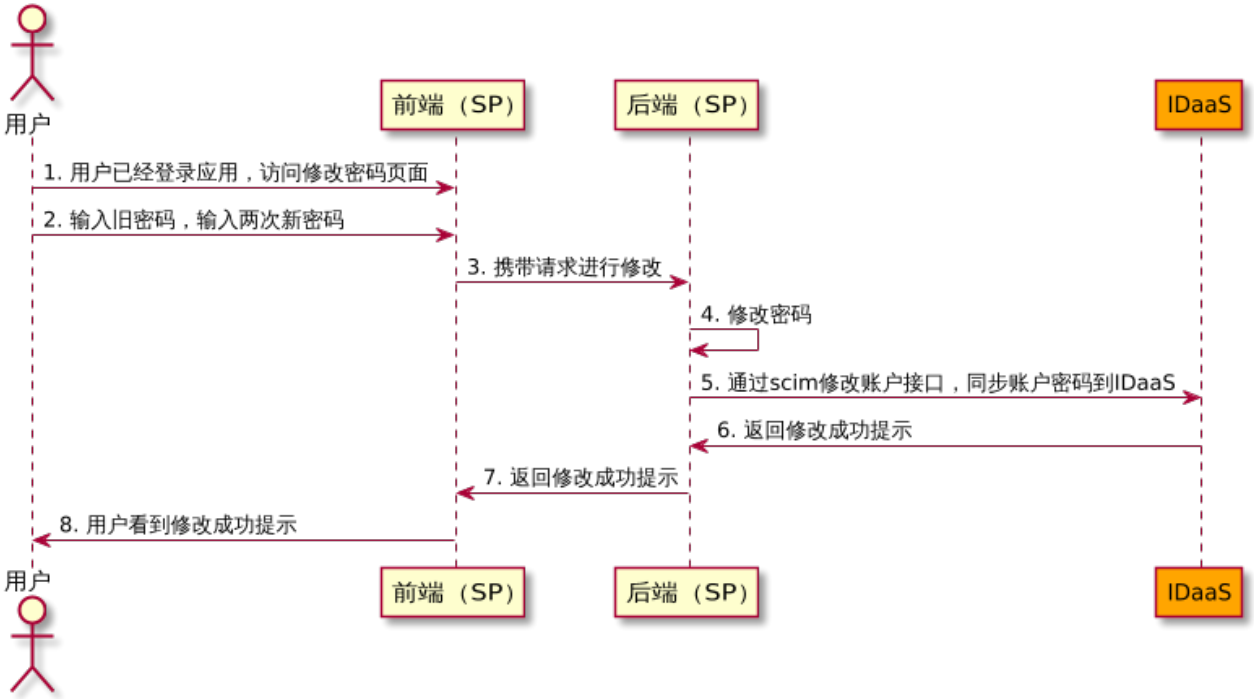
注意：

（1）步骤4 新的账户名，建议由租户和账户名组合生成，规则：租户名_账户名 或者 租户名.账户名。

（2）步骤4 应用通过 SICM 接口同步到 IDaaS 的是应用前端+后端加密后的密码（**切勿直接传输明文**），IDaaS 会根据 IDaaS 加密规则再次加密进行存储。用户登录时，IDaaS 使用加密后的密码和数据库中的密码做校验。

4.4.2 修改密码

当用户在应用侧修改密码时，请通过同步接口同步新密码，以保持应用侧密码与 IDaaS 侧密码的一致。



4.4.3 二次认证类型

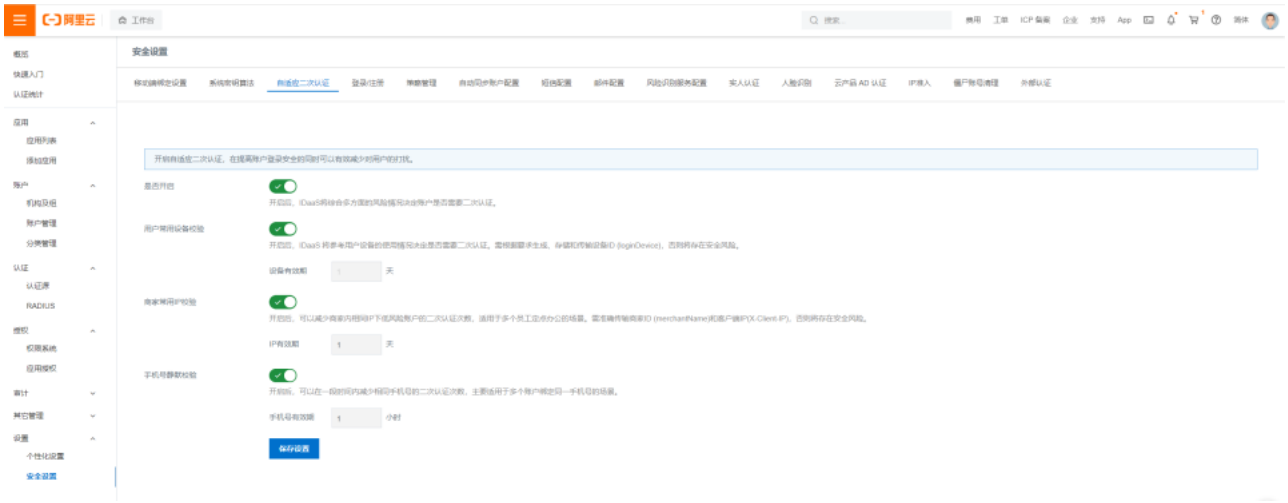
二次认证指的是账户在完成一次认证（如账户密码）后，再通过手机短信、OTP、设备等进行第二次认证，以提高账户登录的安全性。IDaaS 支持 **自适应** 和 **强制** 两种二次认证类型。

注意：IDaaS 产品版本大于 v2.3.0 的实例，才可使用全部的二次认证能力。如果您的产品版本小于 v2.3.0，请联系 IDaaS 团队对您的实例进行升级。

4.4.3.1 自适应二次认证

自适应二次认证指的 IDaaS 根据设备、IP 等情况综合判断账户的登录是否需要二次认证。IDaaS 提供了配置界面，您可以在 **设置–安全设置–自适应二次认证** 中进行配置。

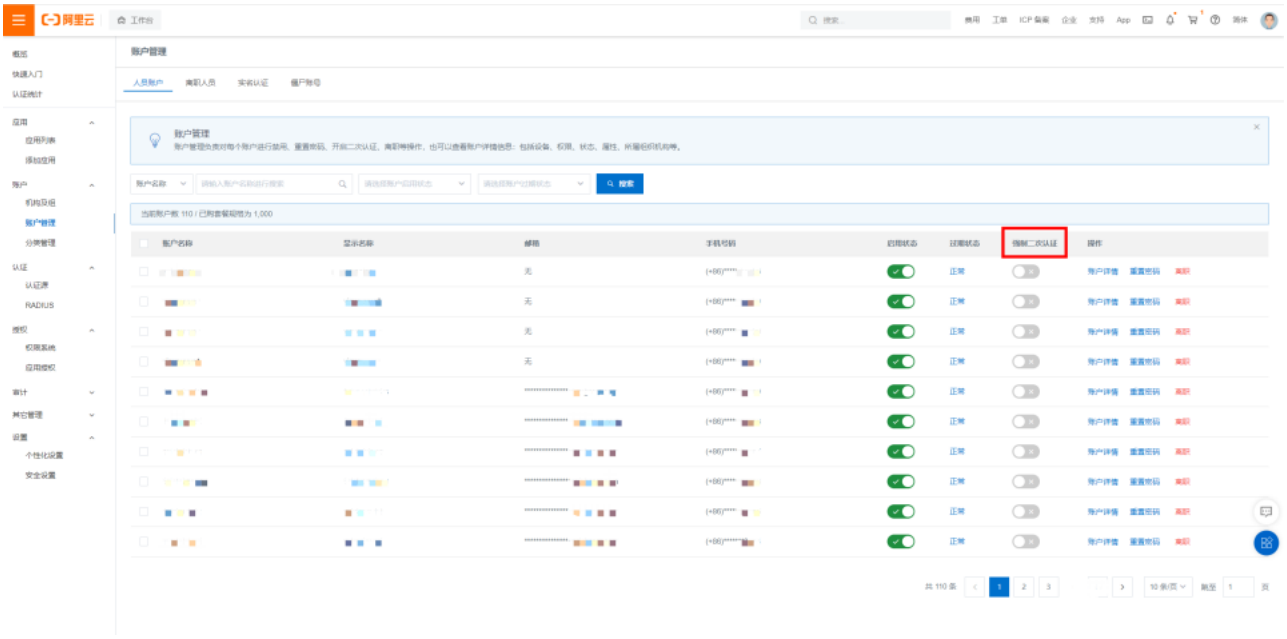
自适应二次认证可以有效减少认证短信的数量、降低对客户的打扰，但**需要准确传递设备 ID、商家 ID、客户端 IP 等参数，如传输有误可能导致二次认证风控失效。**



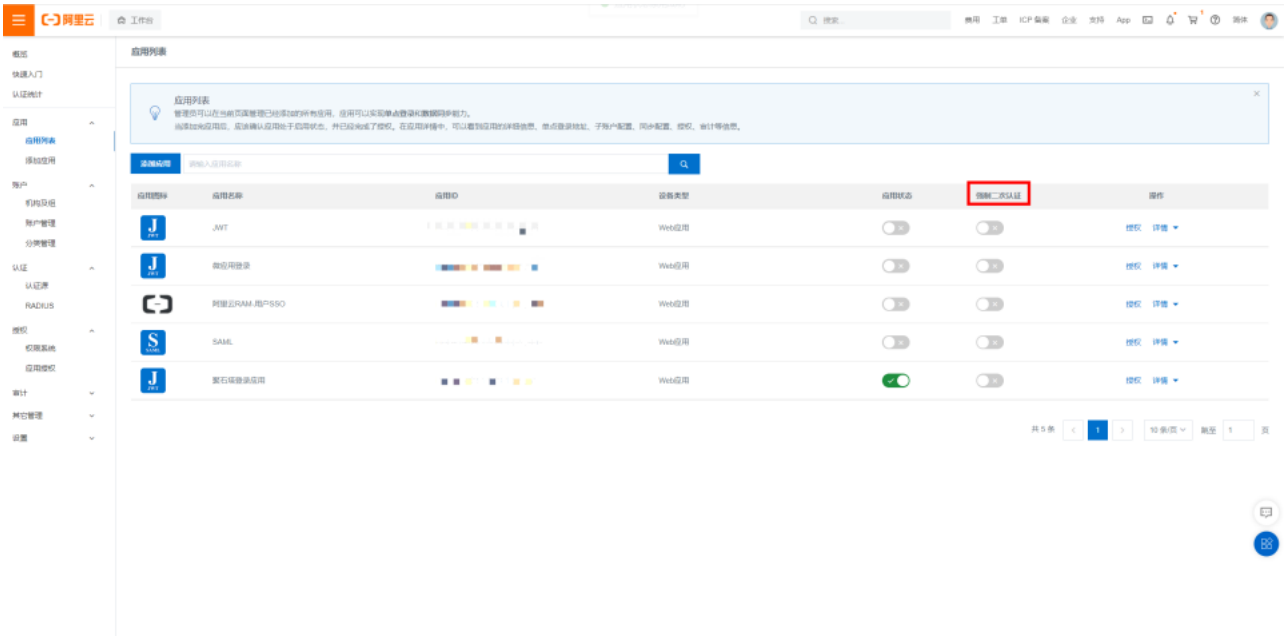
4.4.3.2 强制二次认证

强制二次认证指的是每次登录都需要二次认证，分为账户粒度和应用粒度。如果同时开启了强制二次认证和自适应二次认证，将优先执行强制二次认证。

账户粒度：在 **账户管理** 中可以针对账户开启强制二次认证，开启后账户每次登录均需要二次认证。



应用粒度：也可以在 **应用列表** 中针对应用开启强制二次认证，由于一个聚石塔实例只能对接一个应用，因此开启应用粒度的强制二次认证后，相当于实例下所有账户登录均需要二次认证。



4.4.4 二次认证流程

IDaaS 目前支持的二次认证方式包括：**短信认证** 和 **OTP 认证**。短信认证发时会产生短信费用，**IDaaS 暂时免费提供短信服务，以方便您快速接入。**OTP 认证不会产生额外费用。请您根据实际业务需要选择二次认证方式。

注意：IDaaS 产品版本大于 v2.3.0 的实例，才可使用全部的二次认证能力。如果您的产品版本小于 v2.3.0，请联系 IDaaS 团队对您的实例进行升级。

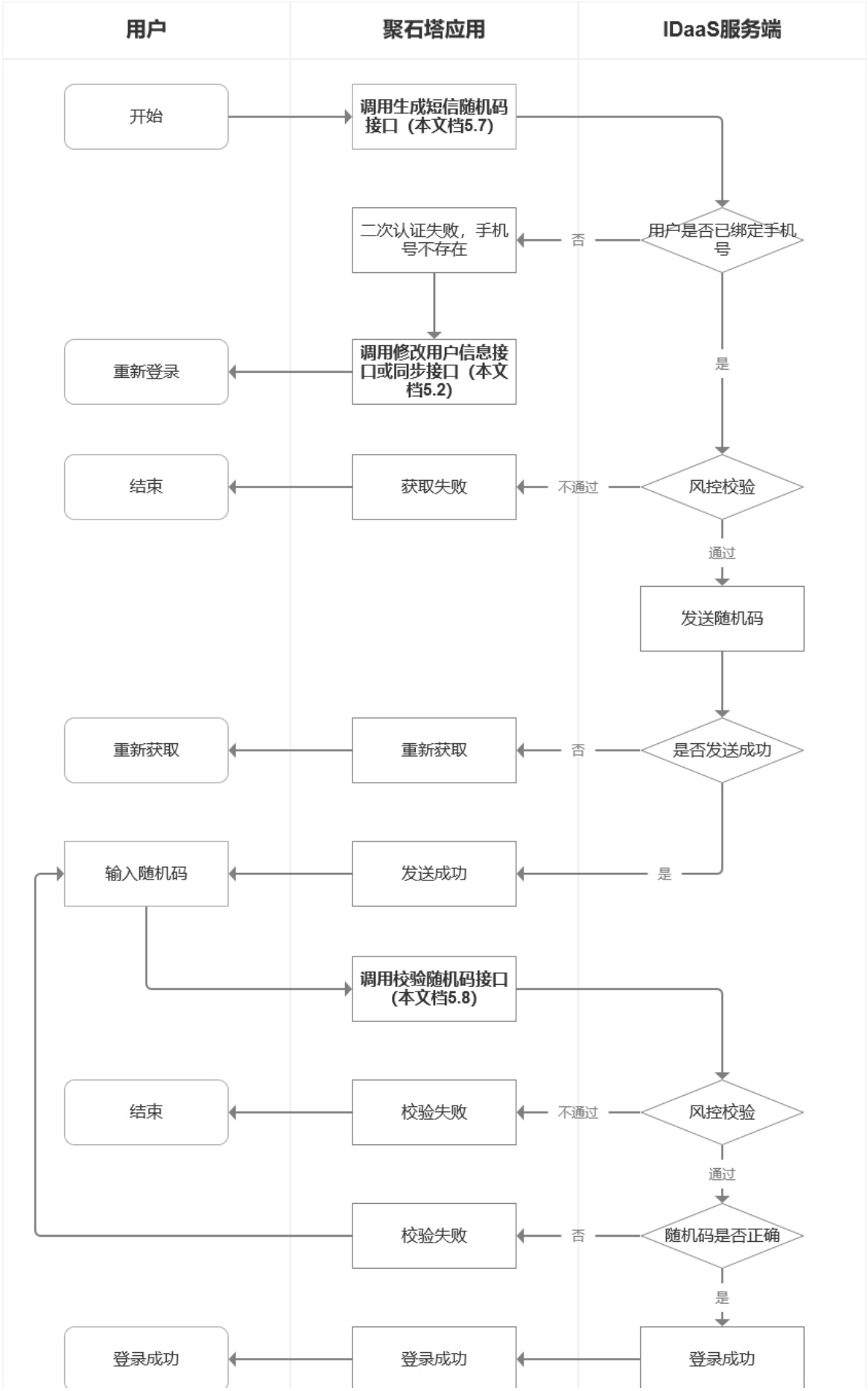
4.4.4.1 短信二次认证

下图是短信二次认证的业务流程图，以便您了解该流程中的关键环节和所需接口。

如需使用短信二次认证，建议提前将用户的手机号全量同步至 IDaaS，以保证用户体验。

当用户进行短信二次认证时，如果用户的手机号在 IDaaS 中不存在，本次登录将会失败，IDaaS 会将该结果返回至应用。如果您无法提前全量同步用户手机号，建议在获取到 IDaaS 认证接口的出参时，先引导用户绑定手机号并同步至 IDaaS，再调用二次认证相关接口。

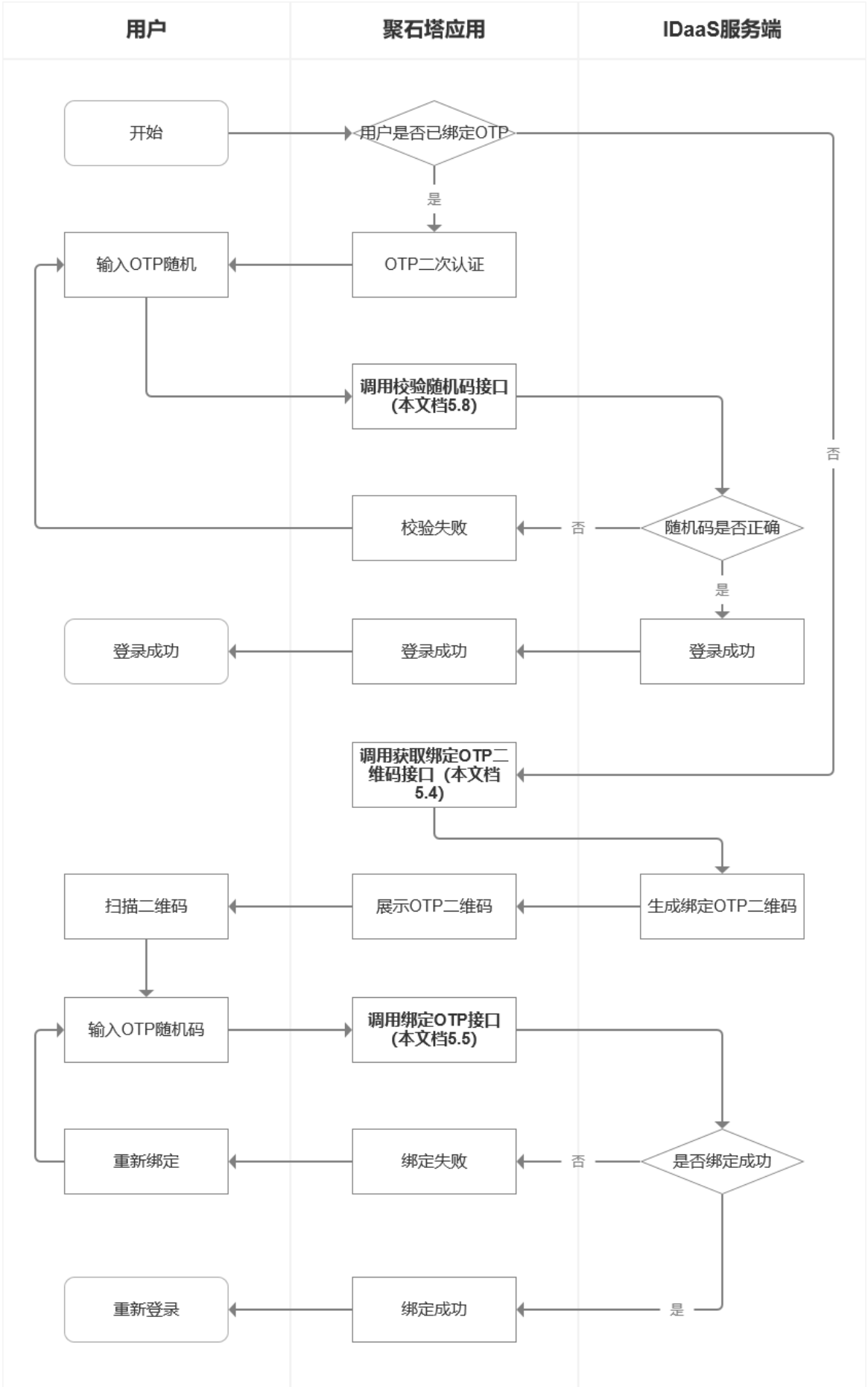
短信二次认证接口内置风控校验，包括错误次数过多失效、超时失效等，以防止暴力破解。


用户
聚石塔应用
IDaaS服务端
开始
调用生成短信随机码接口（本文档5.7）
用户是否已绑定手机号
否
二次认证失败，手机号不存在
是
调用修改用户信息接口或同步接口（本文档5.2）
重新登录
风控校验
不通过
获取失败
结束
通过
发送随机码
是否发送成功
否
重新获取
重新获取
是
发送成功
输入随机码
调用校验随机码接口(本文档5.8)
风控校验
不通过
校验失败
结束
通过
随机码是否正确
否
校验失败
是
登录成功
登录成功
登录成功

4.4.4.2 OTP 二次认证

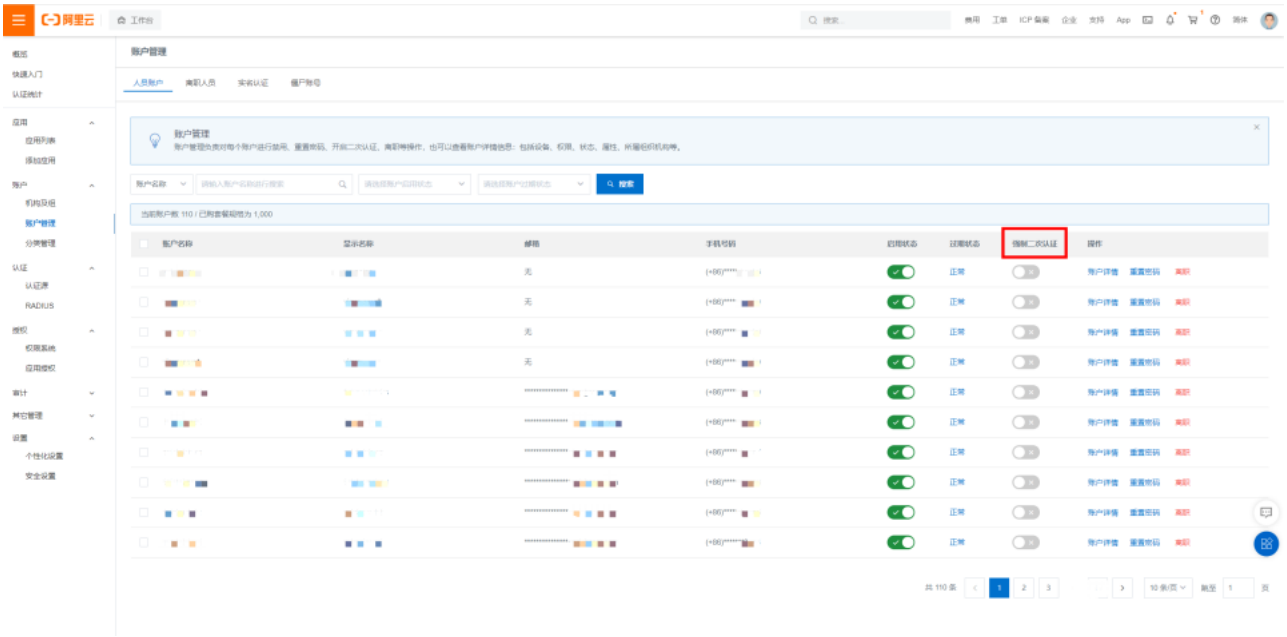
下图是 OTP 二次认证的业务流程图，以便您了解该流程中的关键环节和所需接口。

IDaaS 也支持 OTP 二次认证能力。如需使用该能力，用户需要安装 Google Authenticator APP 或 Microsoft Authenticator，Microsoft Authenticator 可在国内各大应用市场下载。


用户
聚石塔应用
IDaaS服务端
开始
用户是否已绑定OTP
是
否
输入OTP随机
OTP二次认证
调用校验随机码接口(本文档5.8)
校验失败
否
随机码是否正确
是
登录成功
登录成功
登录成功
调用获取绑定OTP二维码接口（本文档5.4)
扫描二维码
展示OTP二维码
生成绑定OTP二维码
输入OTP随机码
调用绑定OTP接口(本文档5.5)
重新绑定
绑定失败
否
是否绑定成功
重新登录
绑定成功
是

4.4.5 二次认证测试

初次对接二次认证功能，您需要有一个开发、测试过程。在开发、测试过程中，建议针对单个账户开启二次认证，此时其他用户均不受影响：



使用开启二次认证的用户调用【账号密码认证】接口，如果是首次执行 OTP 认证，此时会返回 code = InvalidParameter.NeedBoundOTPCode ，表示用户尚未绑定动态口令，此时客户需要调用【获取绑定OTP二维码】接口，将返回的 base64 图片二维码展示到用户界面，用户使用 OTP 认证器扫描二维码，此时用户可以得到动态口令，用户界面需要给与提示，

当您完成开发和测试后，可开启自适应二次认证或应用粒度的强制二次认证，以保证账户安全。

5. 接口列表

IDaaS 提供了一系列丰富的、稳定的接口，以满足您的不同业务场景。随着 IDaaS 的不断优化以及与各方合作的不断深入，该接口列表会持续丰富，开放更多安全防护能力。

如果您初次对接 IDaaS，**请您重点关注本章节中的 5.1、5.2、5.3，这些是对接 IDaaS 时必须使用的接口；**另外，请您关注本章节中的二次认证相关的接口，**使用短信二次认证时请关注本章节中的 5.7、5.8，使用 OTP 二次认证时请关注本章节中的 5.4、5.5、5.8。**

接口中提到的 **your-idaas-domain** 可以在实例列表页中获取，使用下图中的 **用户登录页地址** 或 **实例开放接口域名** 均可，建议选择后者。

如果您在购买、对接、使用过程中遇到问题，**请使用钉钉搜索 33623553 加入支持群【备注 IDaaS】**，联系阿里云 IDaaS 团队进行支持。

5.1 获取 access_token

5.1.1 使用说明

IDaaS 所有的接口，都是受保护的资源。只有通过本接口获取到 access_token，应用才能调用接口。access_token 的传递方式有两种：

1. 第一种：Header参数传递

头名称为 Authorization，值为bearer {access_token} （请注意bearer和access_token之间的空格）

2. 第二种：Query参数传递

在请求URL的最后添加参数。如：http://your-idaas-domain/?access_token={access_token}

5.1.2 接口地址

POST https://{{your-idaas-domain}}/oauth/token

5.1.3 请求参数

参数	类型	是否必须	示例值	描述
client_id	string	是	78d8be99ef30197c31888f5d2d1390a6pHn71sZEqvP	从应用中获取到的AppKey
client_secret	string	是	96csUmei1g0tL629ufrVMZviFie7NWBOnGYsJNLknQ	从应用中获取到的AppSecret
grant_type	array	是	固定值：client_credentials	

Scope	string	是	固定值：read	

5.1.4 返回参数

参数	类型	示例值	描述
access_token	string	bd3a80ca-24c3-4da8-836f-9efcb2c52c4b	外部ID
token_type	string	bearer	OU uuid
expires_in	string	43199	access_token 过期时间，单位为秒。7200 秒为 2 小时。
scope	string	read	固定值：read

5.1.5 示例

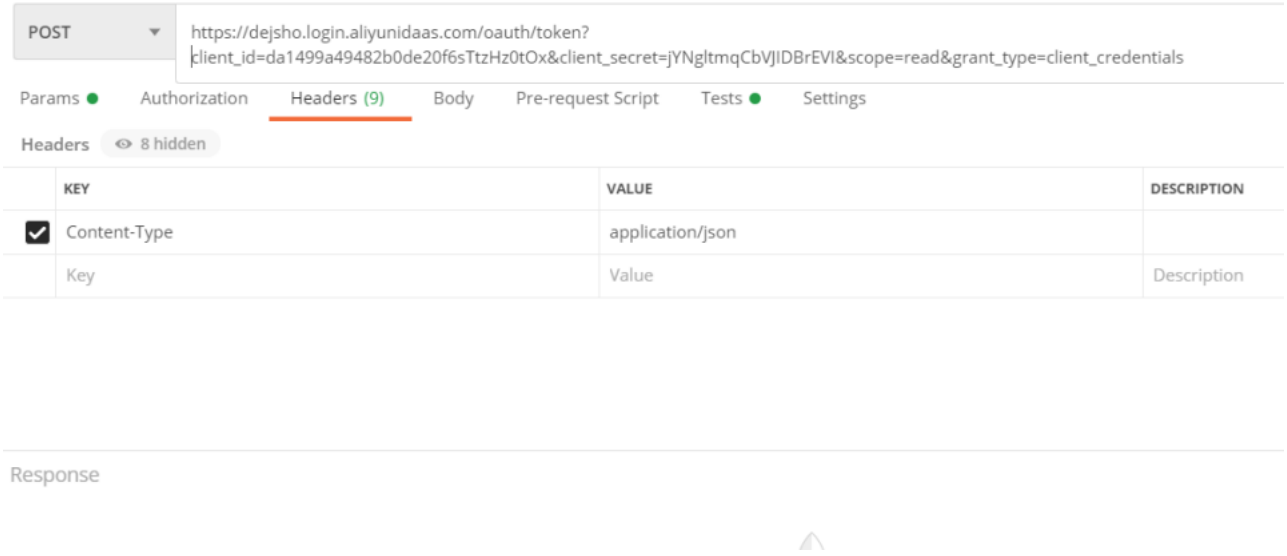
请求示例

```
http://{{your-idaas-domain}}/oauth/token?
client_id=78d8be99ef30197c318885d2d1390a6pHn71sZEqvP
&client_secret=96csUmei1g0tL629ufrVMZviFie7NWBOnGYsJNLknQ
&grant_type=client_credentials&scope=read
```

正常返回示例

```
{
    ”access_token”: ”bd3a80ca-24c3-4da8-836f-9efcb2c52c4b”,
    ”token_type”: ”bearer”,
    ”expires_in”: 41177,
    ”scope”: ”read”
}
```

参数和header请求示例



5.2 组织账户同步

使用 IDaaS 的同步能力，您主要需要使用以下四个接口：

- **推送组织机构**：/api/bff/v1.2/developer/scim/organization/create
- **推送账户**：/api/bff/v1.2/developer/scim/account/create
- **修改账户**：/api/bff/v1.2/developer/scim/account/update
- **删除账户**：/api/bff/v1.2/developer/scim/account/delete

更多同步相关接口信息，请在此文档中了解：https://help.aliyun.com/document_detail/143467.html

5.3 账户密码认证

5.3.1 接口说明

用户账号密码认证接口。

5.3.2 接口地址

POST /api/public/bff/v1.2/developer/mobile/pwd_logon_by_auth_source

请求示例：

```
POST https://<your-idaasdomain>/api/public/bff/v1.2/developer/mobile/pwd_logon_by_auth_source?
appKey=397438f8155906251eb5581b0de0180a1wySiYJCALm&timestamp=1580975586256&nonce
=00889977&signature=3b0ea0c627494361fcac0dfc3210b2a875bd70da
```

5.3.3 请求参数

参数名	必 须	位置	内容说明
Content-Type	是	header	application/json
X-Client-IP	是	header	客户端IP。**如传输有误可能导致二次认证风控失效，请准确传输。**
username	是	body	用户名
password	是	body	AES加密密码（apiSecret做为密钥） Java加密工具类如下： V1版本- AESUtils.java 不建议 V2版本-AESUtilsV2ForPKCS5.java 推荐 V2版本- AESUtilsV2ForPKCS.java 特殊场景使用
passwordCipherType	是	body	V1版本固定值：”aes”， 不推荐 V2版本PKCS5固定值：”aes_v2_pkcs5” 推荐 V2版本PKCS7固定值：”aes_v2_pkcs7” 特殊场景使用 如果不加密则输入”none” 如果不是 java 语言，可以参考以下链接：http://tool.chacuo.net/cryptaes，和它的逻辑保持一致即可
_enterprise_id	否	body	租户ID，即 IDaaS 实例 ID，可不传
appKey	是	body	ISV售卖应用的appkey，从淘宝市场获取，不从IDaaS中获取。**在请求body中传递**
loginDevice	是	body	登录设备机器码，用于标识用户的设备。需要通过密码学安全的随机数生成，长度不小于32字节。建议存储在客户端本地，以防标识被清除或过期导致频繁需要二次认证。 **如已对接御城河，请传递 ati 值**，请参考：孔明锁； **如果没有对接御城河，请自行实现**，推荐使用 UUID，Java 开发者可直接调用 *UUID.randomUUID()*。 **如传输有误可能导致二次认证风控失效，请准确传输。**
merchantName	是	body	客户主体名称，标识该账户属于哪个商家，对应淘系商家主账号昵称，**即掌柜名称（不是店铺名称）。** **如传输有误可能导致二次认证风控失效，请准确传输。**

			支持传递多个，以英文逗号隔开即可，当前版本默认使用首个名称进行自适应二次认证校验，后续将使用全部名称进行校验。
captchaText	否	body	用户输入的验证码值，只有当接口调用者的IP受限制后（认证接口返回错误码 InvalidParameter.Captcha.IsNull）代表必填
captchaCode	否	body	验证码code，只有当接口调用者的IP受限制后（认证接口返回错误码 InvalidParameter.Captcha.IsNull）代表必填
phoneRegion	否	body	如果username是手机号，则phoneRegion建议填写，如果 不填写，默认86
needToken	否	body	是否需要返回token，默认为false；（目前聚石塔没有场景需要token）
appKey	是	query	此处是appKey是在IDaaS中获取，**请在url中传递**
timestamp	是	query	时间戳，精确到毫秒。后台会校验时间戳声明的时间与服务器时间差，如果超过5分钟，则返回错误
nonce	是	query	随机数，推荐长度至少8位，用于对签名加盐
signature	是	query	Hex编码的字符串，使用SHA1算法对如下： timestamp + nonce + appSecret 进行Hash,然后对结果进 行16进制编码（Java工具类：DeveloperSignatureUtil.java）

请求Body：

```
{
”username”:”zuhu.test”,
”password”:”vMmQ7UB44yo2ORvyMtWJgw==”,
”passwordCipherType”:”aes”,
”_enterprise_id”:”jzyt”,
”captchaText”:”892K”,
”captchaCode”:”sfwf2w233fsfdsddf”,
”appKey”:”jst1”,
”loginDevice”:”87SD2W7ER1FFWR”,
”needToken”:false,
”merchantName”:”客户主体”
}
```

5.3.4 返回参数

字段名	类型	示例	**内容说明**
accessToken	string		用户access_token（请求body中，needToken为false，不返回token）

expiresIn	long	7200	token过期时间，单位：秒
enterpriseUuid	string	9afca4184	用户所属租户UUID
enterpriseId	string	jzyt	用户所属租户ID
username	string	R2019090	用户账号
needSecondFactor	boolean	true	是否需要二次认证
fid	string	1s2s23f1g3sdg34	流程id，用于下一个流程（一般为二次认证相关接口）使用。 **fid 有效期 5 分钟，每次请求需要使用上一个接口返回的 fid。**比如：登录时会返回 fid，发送短信验证码会返回 fid，验证短信验证码时，要传【发送短信验证码时所返回的fid】
bindOTPCode	boolean	false	用户是否已经绑定OTP
displayName	string	R2019090	显示名称
phoneNumber	string		用户手机号
phoneRegion	sring	86	用户手机国家号

错误码：

错误码	描述
200	成功
500	服务端异常，内部错误
InvalidParameter	参数错误，具体信息可以参考 message。 如账户被禁用或锁定， 请求不在白名单， 请求属于黑名单等， code都是invalidparameter
InvalidParameter.Captcha.IsNull	必须输入图形验证码（默认不需要输入，当系统检查 一个IP发送短信频率过高时，会要求输入图形验证 码）
InvalidParameter.Captcha.Invalid	图形验证码验证失败
InvalidParameter.User.Locked	用户存在并且已经被锁定（密码登录连续失败次数过 多导致锁定）或者禁用（管理员后台将用户禁用）
InvalidParameter.Password.Invalid	密码错误

InvalidParameter.NeedBoundOTPCode	用户未绑定动态口令
InvalidParameter.EndUser.NeedSecondFactor	需要二次认证
InvalidParameter.UserName.NotExist	指定的用户名或者手机号，系统中不存在

响应Body：

```
{
  ”success”: true,
  ”code”: ”200”,
  ”message”: null,
    ”data”: {
      ”accessToken”: ”27d74ece-88b2-44cd-a50e-9de335004c13”,//needToken为false不返回
      ”expiresIn”: 7200,
      ”username”:”138****3216”,
      ”displayName”:”显示名称”,
      ”enterpriseUuid”: ”9afca4184065cf7d58084826143”,
      ”enterpriseId”: ”jzyt”,
      ”phoneNumber”: ”138xxxxx10”,
      ”phoneRegion”:”86”,
      ”needSecondFactor”:true,
      ”fid”:”1s21fasdfsgjkll2342i34”,
      ”bindOTPCode”:false
    }
}
```

5.4 获取绑定OTP二维码

5.4.1 接口说明

用于用户使用google Authenticator APP 和 Microsoft Authenticator 来绑定OTP动态口令。

5.4.2 接口地址

POST /api/public/bff/v1.2/developer/mobile/secondFactor/generate/otp_code

请求示例：

```
POST https://<your-idaasdomain>/api/public/bff/v1.2/developer/mobile/secondFactor/generate/otp_code?
appKey=397438f8155906251eb5581b0de0180a1wySiYJCALm&timestamp=1580975586256&nonce
=00889977&signature=3b0ea0c627494361fcac0dfc3210b2a875bd70da
```

5.4.3 请求参数

参数名	必 须	位置	内容说明
Content-Type	是	header	application/json
X-Client-IP	是	header	客户端IP
username	是	body	用户名
fid	是	body	流程id，可使用账号+密码认证接口返回的fid，有效期5分钟。 fid 有效期 5 分钟，每次请求需要使用上一个接口返回的fid。比如：登录时会返回 fid，发送短信验证码会返回fid，验证短信验证码时，要传【发送短信验证码时所返回的fid】
appKey	是	query	此处是appKey是在IDaaS中获取，在url中传递该参数
timestamp	是	query	时间戳，精确到毫秒。后台会校验时间戳声明的时间与服务 器时间差，如果超过5分钟，则返回错误
nonce	是	query	随机数，推荐长度至少8位，用于对签名加盐
signature	是	query	Hex编码的字符串，使用SHA1算法对如下： timestamp + nonce + appSecret 进行Hash,然后对结果进 行16进制编码（Java工具类：DeveloperSignatureUtil.java）

请求Body：

```
{
    ”fid”:”30096a2fbcb325439d28b5d53dcb79f6pnlRwMsYOfM”,
    ”username”:”zhangsan”
}
```

5.4.4 返回参数

字段名	类型	示例	内容说明
success	boolean	true	成功返回true
code	string	200	成功返回200
message	string	用户不存在	错误信息

requestId	string		请求id，用户链路追踪，日志排查
fid	string	1231-234f	流程id，用于二次认证绑定验证码和OTP二次认证使用。（过期时间5分钟，且仅能使用一次）
base64QRCode	string	oAAAANSUhEUgAAAMgAAADIAQAAAACFI5MzAAACGUlEQVR42tWYS46DQAxEjVj0	base64格式的二维码图片

响应Body：


```
{
    ”success”: true,
    ”code”: ”200”,
    ”message”: null,
    ”requestId”: ”1635934154286$03fced0d-5cc3-1c90-dfdd-4a815d6fef9c”,
    ”data”: {
        ”fid”: ”6a836deeae47dc01e2843fba2bc57350rOqNsXi10KI”,
        ”base64QRCode”:
”iVBORw0KGgoAAAANSUhEUgAAAMgAAADIAQAAAACFI5MzAAACGUlEQVR42tWYS46DQAxEjVj0kiP0TZKLIYGUi4Wb9BF
```


5.5 绑定OTP

5.5.1 接口说明

用户扫码完成后需要输入一次OTP进行确定绑定OTP操作。

5.5.2 接口地址

POST /api/public/bff/v1.2/developer/mobile/secondFactor/otp_code/bind

请求示例：

```
POST https://<your-idaasdomain>/api/public/bff/v1.2/developer/mobile/secondFactor/otp_code/bind?
appKey=397438f8155906251eb5581b0de0180a1wySiYJCALm&timestamp=1580975586256&nonce
=00889977&signature=3b0ea0c627494361fcac0dfc3210b2a875bd70da
```

5.5.3 请求参数

参数名	必 须	位置	内容说明
Content-Type	是	header	application/json
X-Client-IP	是	header	客户端IP
username	是	body	用户名
fid	是	body	流程id，可使用账号+密码认证接口返回的fid，有效期5分钟。 **fid 有效期 5 分钟，每次请求需要使用上一个接口返回的fid。**比如：登录时会返回 fid，发送短信验证码会返回fid，验证短信验证码时，要传【发送短信验证码时所返回的fid】
code	是	body	动态口令
appKey	是	query	此处是appKey是在IDaaS中获取，在url中传递该参数
timestamp	是	query	时间戳，精确到毫秒。后台会校验时间戳声明的时间与服务 器时间差，如果超过5分钟，则返回错误
nonce	是	query	随机数，推荐长度至少8位，用于对签名加盐
signature	是	query	Hex编码的字符串，使用SHA1算法对如下： timestamp + nonce + appSecret 进行Hash,然后对结果进 行16进制编码（Java工具类：DeveloperSignatureUtil.java）

请求Body：

```
{
    ”fid”:”30096a2fbcb325439d28b5d53dcb79f6pnlRwMsYOfM”,
    ”username”:”zhangsan”,
    ”code”:”123456”
}
```

5.5.4 返回参数

字段名	类型	示例	内容说明
success	boolean	true	成功返回true
code	string	200	成功返回200
message	string	用户不存在	错误信息
requestId	string		请求id，用户链路追踪，日志排查

响应Body：

```
{
    ”success”: true,
    ”code”: ”200”,
    ”message”: null,
    ”requestId”: ”1636114647152$16e6e85a-14fe-0ff8-5e61-8986edc14c31”,
    ”data”: null
}
```

5.6 清除OTP绑定状态

5.6.1 接口说明

用户绑定OTP后，设备丢失或者更新设备，需要管理员先清除绑定状态更换密钥，再进行绑定（清除OTP绑定状态后，原APP生成的OTP也会失效）。

5.6.2 接口地址

POST /api/public/bff/v1.2/developer/mobile/secondFactor/clear/otp_code

请求示例：

```
POST https://<your-idaasdomain>/api/public/bff/v1.2/developer/mobile/secondFactor/clear/otp_code?
appKey=397438f8155906251eb5581b0de0180a1wySiYJCALm&timestamp=1580975586256&nonce
=00889977&signature=3b0ea0c627494361fcac0dfc3210b2a875bd70da
```

5.6.3 请求参数

参数名	必 须	位置	内容说明
Content-Type	是	header	application/json
X-Client-IP	是	header	客户端IP
username	是	body	用户名
appKey	是	query	此处是appKey是在IDaaS中获取，在url中传递该参数
timestamp	是	query	时间戳，精确到毫秒。后台会校验时间戳声明的时间与服务 器时间差，如果超过5分钟，则返回错误
nonce	是	query	随机数，推荐长度至少8位，用于对签名加盐
signature	是	query	Hex编码的字符串，使用SHA1算法对如下： timestamp + nonce + appSecret 进行Hash,然后对结果进 行16进制编码（Java工具类：DeveloperSignatureUtil.java）

请求Body：

```
{
    "username":"zhangsan"
}
```

5.6.4 返回参数

字段名	类型	示例	内容说明
success	boolean	true	成功返回true
code	string	200	成功返回200
message	string	用户不存在	错误信息
requestId	string		请求id，用户链路追踪，日志排查

响应Body：

```
{
    "success": true,
    "code": "200",
    "message": null,
    "requestId": "1635934962844$e1ec1d81-fc23-a541-1473-81a7736dde53",
    "data": null
}
```

5.7 生成短信随机码

5.7.1 接口说明

主要用于发送短信验证码。

5.7.2 接口地址

POST /api/public/bff/v1.2/developer/mobile/secondFactor/prepare

请求示例：

```
POST https://<your-idaasdomain>/api/public/bff/v1.2/developer/mobile/secondFactor/prepare?
appKey=397438f8155906251eb5581b0de0180a1wySiYJCALm&timestamp=1580975586256&nonce
=00889977&signature=3b0ea0c627494361fcac0dfc3210b2a875bd70da
```

5.7.3 请求参数

参数名	必 须	位置	内容说明
Content-Type	是	header	application/json
username	是	body	用户名
fid	是	body	流程id，需使用账号+密码认证接口返回的fid。 **fid 有效期 5 分钟，每次请求需要使用上一个接口返回的fid。**比如：登录时会返回 fid，发送短信验证码会返回fid，验证短信验证码时，要传【发送短信验证码时所返回的fid】
secondFactor	是	body	二次认证类型：短信固定值”SMS”.
_enterprise_id	否	body	租户ID
appKey	是	query	此处是appKey是在IDaaS中获取，在url中传递该参数
timestamp	是	query	时间戳，精确到毫秒。后台会校验时间戳声明的时间与服务 器时间差，如果超过5分钟，则返回错误
nonce	是	query	随机数，推荐长度至少8位，用于对签名加盐
signature	是	query	

			Hex编码的字符串，使用SHA1算法对如下： timestamp + nonce + appSecret 进行Hash,然后对结果进 行16进制编码（Java工具类：DeveloperSignatureUtil.java）

请求Body：

```
{
    ”username”:”138****3216”,
    ”fid”:”A011111”,
    ”secondFactor”:”SMS”,
    ”_enterprise_id”:”jzyt”
}
```

5.7.4 返回参数

字段名	类型	示例	**内容说明**
fid	string		流程id，校验接口需要传入

错误码：

错误码	描述
200	成功
500	服务端异常，内部错误
InvalidParameter	参数错误，具体信息可以参考 message。 如fid已失效、fid所关联用户不存在等等
InvalidParameter.Phone.NotExist	该用户目前还没有手机号，需要先绑定手机号
InvalidParameter.TooFrequency.SendSms	发送短信过于频繁,请5分钟后再试。5分钟内只能发送5次。

响应Body：

```
{
    ”success”: true,
    ”code”: ”200”,
    ”message”: null,
    ”data”: {
        ”fid”:”A011111”
     }
}
```

5.8 校验随机码

5.8.1 接口说明

用于校验用户的随机码，实现用户二次认证。对于短信而言是短信验证码，对于OTP而言是OTP动态口令。

5.8.2 接口地址

POST /api/public/bff/v1.2/developer/mobile/secondFactor/verify

请求示例：

```
POST https://<your-idaasdomain>/api/public/bff/v1.2/developer/mobile/secondFactor/verify?
appKey=397438f8155906251eb5581b0de0180a1wySiYJCALm&timestamp=1580975586256&nonce
=00889977&signature=3b0ea0c627494361fcac0dfc3210b2a875bd70da
```

5.8.3 请求参数

参数名	必 须	位置	内容说明
Content-Type	是	header	application/json
X-Client-IP	是	header	客户端IP
username	是	body	用户名
fid	是	body	流程id，需使用生成短信随机码接口返回的fid。 **fid 有效期 5 分钟，每次请求需要使用上一个接口返回的fid。**比如：登录时会返回 fid，发送短信验证码会返回fid，验证短信验证码时，要传【发送短信验证码时所返回的fid】
secondFactor	是	body	二次认证类型：OTP固定值”OTP”，短信固定值”SMS”.
code	是	body	随机码
appKey	是	query	此处是appKey是在IDaaS中获取，在url中传递该参数
timestamp	是	query	时间戳，精确到毫秒。后台会校验时间戳声明的时间与服务 器时间差，如果超过5分钟，则返回错误
nonce	是	query	随机数，推荐长度至少8位，用于对签名加盐

signature	是	query	Hex编码的字符串，使用SHA1算法对如下： timestamp + nonce + appSecret 进行Hash,然后对结果进 行16进制编码（Java工具类：DeveloperSignatureUtil.java）

请求Body：

```
{
    ”username”:”xiaolaohu”,
    ”fid”:”ea9e71caa1982c858af1d4501ae7d320J365dbham11”,
    ”secondFactor”:”OTP”,
    ”code”:”769015”
}
```

5.8.4 返回参数

字段名	类型	示例	内容说明
accessToken	string		用户access_token（请求body中，needToken为false，不返回token）
expiresIn	long	7200	token过期时间，单位：秒
enterpriseUuid	string	9afca4184	用户所属租户UUID
enterpriseId	string	jzyt	用户所属租户ID
username	string	R2019090	用户账号
displayName	string	R2019090	显示名称
phoneNumber	string		用户手机号
phoneRegion	sring	86	用户手机国家号

响应Body：

```
{
    ”success”: true,
    ”code”: ”200”,
    ”message”: null,
    ”requestId”: ”1635935652553$9682b862-50ca-5153-88f4-944b58f43928”,
    ”data”: {
        ”expiresIn”: 43199,
        ”phoneNumber”: ”*******5799”,
        ”displayName”: ”xiaolaohu”,
        ”phoneRegion”: ”86”,
        ”enterpriseUuid”: ”74a2c17b06fdbf84104d312e11781af9UW3kM34AF4I”,
```

```
        "enterpriseId": "idaas-cn-tl32erzp405",
        "accessToken": "ff74673f-fdcc-4901-8135-f5e82eb04746",
        "username": "xiaolaohu"
    }
}
```


5.9 导入常用设备和常用IP

5.9.1 接口说明

如果您目前已经积累了一些用户常用设备和商家常用IP，希望能够提前导入到系统中以降低对存量客户的打扰，则可以对接该接口。**需要确保数据的准确性，否则可能导致二次认证风控失效，并对用户登录造成影响。**

5.9.2 地址

POST /api/enduser/mfa_protection/preference_behavior/import

请求示例：

```
POST https://<your-idaasdomain>/api/enduser/mfa_protection/preference_behavior/import
```

5.9.3 请求参数

参数名	必 须	位置	内容说明
Content-Type	是	header	application/json
Authorization	是	header	Bearer 61fd3d0f-b272-4825-bebb-b70846ee06f1

请求Body：

```
[
    {
        "username": "1",
        "deviceIds": [
            "1",
            "2",
            "3"
        ]
    },
    {
        "merchantName": "1",
        "clientIps": [
            "1",
```

```
        "2",
        "3"
      ]
   }
]
```

注意：

（1）导入用户常用设备，需要传入参数 username 和 deviceIds。

（2）导入商户常用IP，需要传入参数 merchantName 和 clientIps。

（3）单次导入最多 1000 条记录。

5.9.4 返回参数

字段名	类型	示例	**内容说明**
success	boolean	true	成功返回true
code	string	200	成功返回200
message	string		错误信息
requestId	string		请求id，用户链路追踪，日志排查

响应Body：

```
{
    "success": true,
    "code": "200",
    "message": null,
    "requestId": "1641264643296$2d917618-8e64-7005-10f4-b3f6ca834e6a",
    "data": null
}
```

5.10 图片验证码接口

5.10.1 接口地址

Request URI: GET /api/public/bff/v1.2/developer/mobile/one_time_login/captcha

Content-Type: application/json

5.10.2 请求参数

参数名	必须	位置	内容说明
timestamp	否	query	时间值，可随机生成，保证请求无缓存

请求示例：

```
GET https://<your-idaasdomain>/api/public/bff/v1.2/developer/mobile/one_time_login/captcha?
timestamp=1565839531
```

5.10.3 返回参数

字段名	类型	示例	内容说明
code	string	sfwf2w233fsfdsddf	验证码code

响应Body：

```
{
”success”: true,
”code”: ”200”,
”message”: null,
”data”: {
”code”: ”sfwf2w233fsfdsddf”,
”captcha”: ”...”
}
}
```

注意：

（1）code是为了验证用户输入的图片验证码是否正常，在下面认证接口中使用； captcha返回的是图片验证码的64位加密，解密后展示图片验证码给客户。

（2）需要使用IDaaS提供的图片验证码，当账户+密码接口登录失败两次后，会要求输入图片验证码。

5.11 暴力破解锁定后解锁接口（解锁账户接口）

5.11.1 接口地址

Request URI: PUT /api/bff/v1.2/developer/scim/account/unlock

Content-Type: application/json

5.11.2 请求参数

参数名	必 须	位置	内容说明
Content-Type	是	header	application/json
Authorization	是	header	（格式：Bearer空格APIToken）
username	是	body	用户名

5.11.3 返回参数

字段名	类型	示例	内容说明
success	string	true	成功返回true
code	string	200	成功返回200
message	string	用户不存在	错误信息
requestId	string		请求id，用户链路追踪，日志排查

5.11.4 错误码

错误码	描述
200	成功
500	服务端异常，内部错误
InvalidParameter	参数错误，具体信息可以参考 message

5.12 僵尸账户启用接口（启用禁用用户接口）

5.12.1 接口地址

Request URl: PUT api/bff/v1.2/developer/scim/account/enable

Content-Type: application/json

5.12.2 请求参数

参数名	必 须	位置	内容说明
Content-Type	是	header	application/json
Authorization	是	header	（格式：Bearer空格APIToken）
username	是	body	用户名

5.12.3 返回参数

字段名	类型	示例	内容说明
success	string	true	成功返回true
code	string	200	成功返回200
message	string	用户不存在	错误信息
requestId	string		请求id，用户链路追踪，日志排查

5.12.4 错误码

错误码	描述
200	成功
500	服务端异常，内部错误
InvalidParameter	参数错误，具体信息可以参考 message

5.13 账户禁用

5.13.1 接口地址

Request URI: PUT api/bff/v1.2/developer/scim/account/disable

Content-Type: application/json

5.13.2 请求参数

参数名	必 须	位置	内容说明
Content-Type	是	header	application/json
Authorization	是	header	（格式：Bearer空格APIToken）
username	是	body	用户名

5.13.3 返回参数

字段名	类型	示例	内容说明
success	string	true	成功返回true
code	string	200	成功返回200
message	string	用户不存在	错误信息
requestId	string		请求id，用户链路追踪，日志排查

5.13.4 错误码

错误码	描述
200	成功

500	服务端异常，内部错误
InvalidParameter	参数错误，具体信息可以参考 message

注意：

（1）IDaaS有重置密码功能，但因为密码是应用推送给 IDaaS 的，如果在 IDaaS 中修改了密码，并不会反向同步到应用。

5.14 接口安全性问题

（1）调用token接口的时候，怎么保证appkey appsecret的安全?

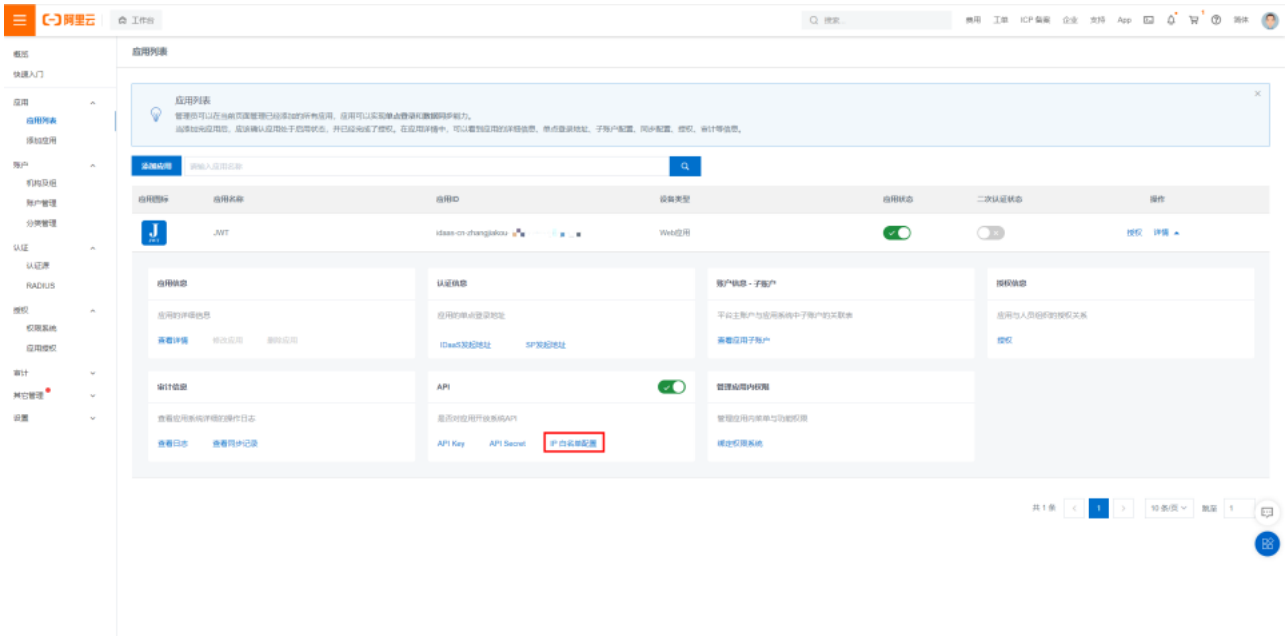
- 用于数据同步的scim接口： 请求报文https加密请求；appkey， appsecret 在业务系统进行使用时，业务系统进行加密存储；
- 用户认证接口：请求时传输appkey，以及SHA加密（appsecret+时间戳+盐）参数。

（2）获取token后如何保障token安全、防止token被劫持?

- 增加应用侧请求IDaaS接口的IP白名单机制，在每次请求token，以及接口携带token向IDaaS请求时，IDaaS会校验应用服务器的出口IP，只要白名单中的IP才能进行请求；
- 应用侧调用IDaaS接口时，需要根据正常流程校验https的证书，校验证书有效性。

（3）所有接口校验IP白名单，只有白名单中的IP才能获取token，进行数据推送

- 白名单校验的是应用服务器的出口IP。



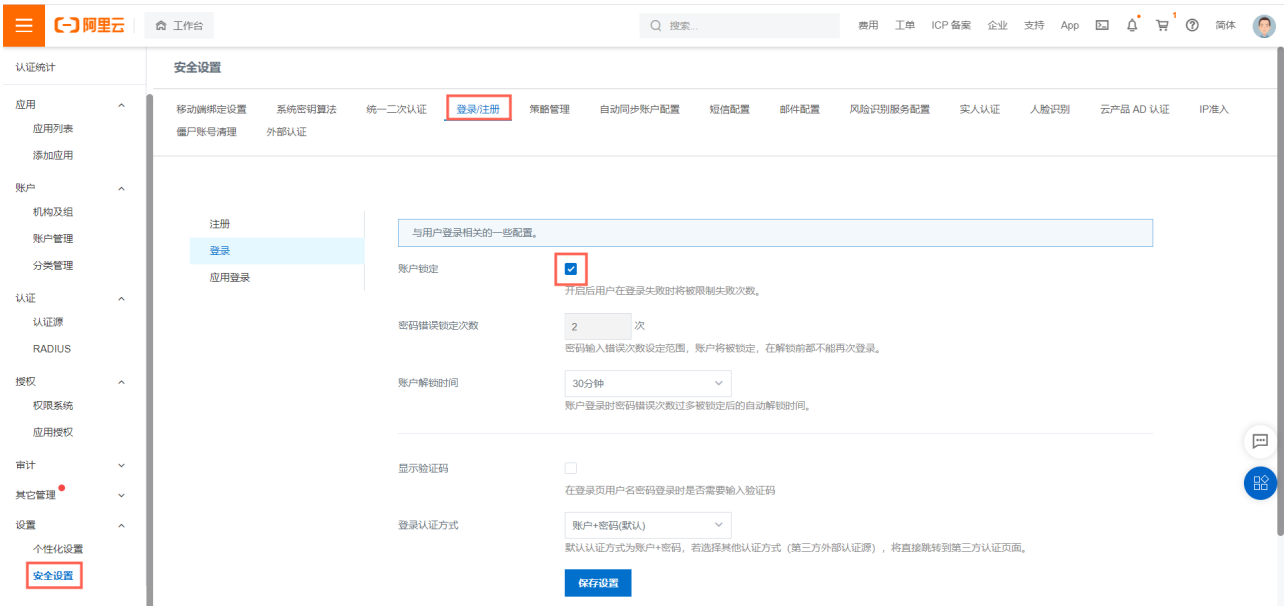
6. 安全实践

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。

6.1 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。

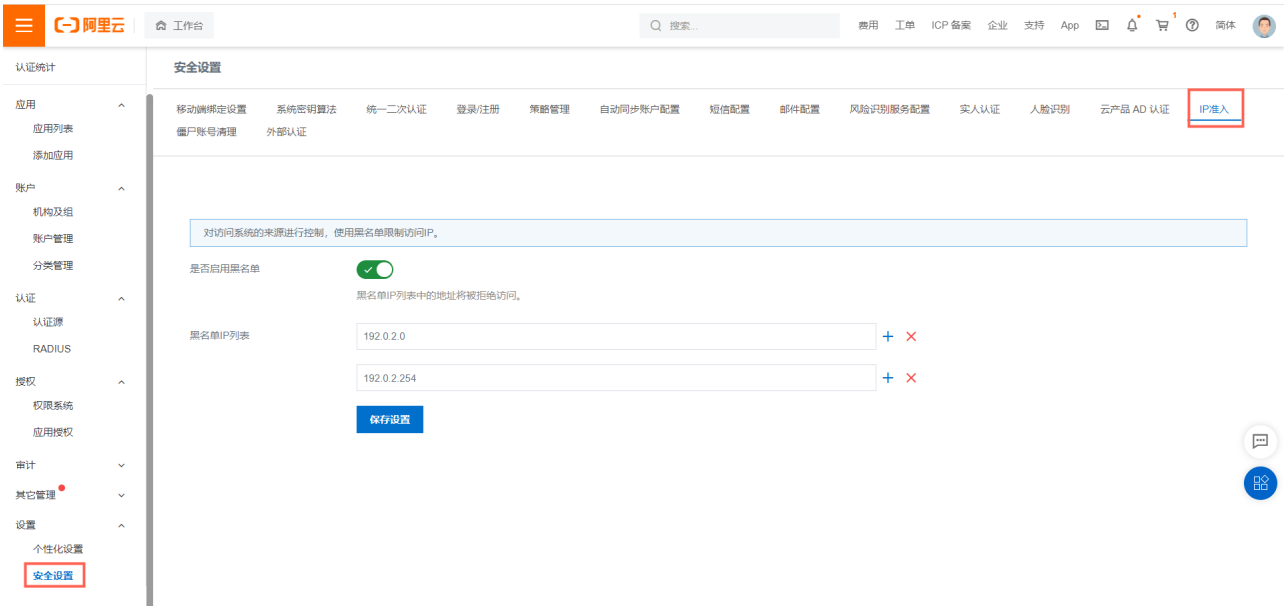


6.2 传输客户端 IP 地址

IDaaS 会识别异常的客户端 IP，并自动拦截在黑名单内的 IP。请确保已根据本文档中 **5.3** 章节中的要求传输请求参数 **X–Client–IP**，以实现 IP 层面的防护。

6.3 IP 黑名单拦截

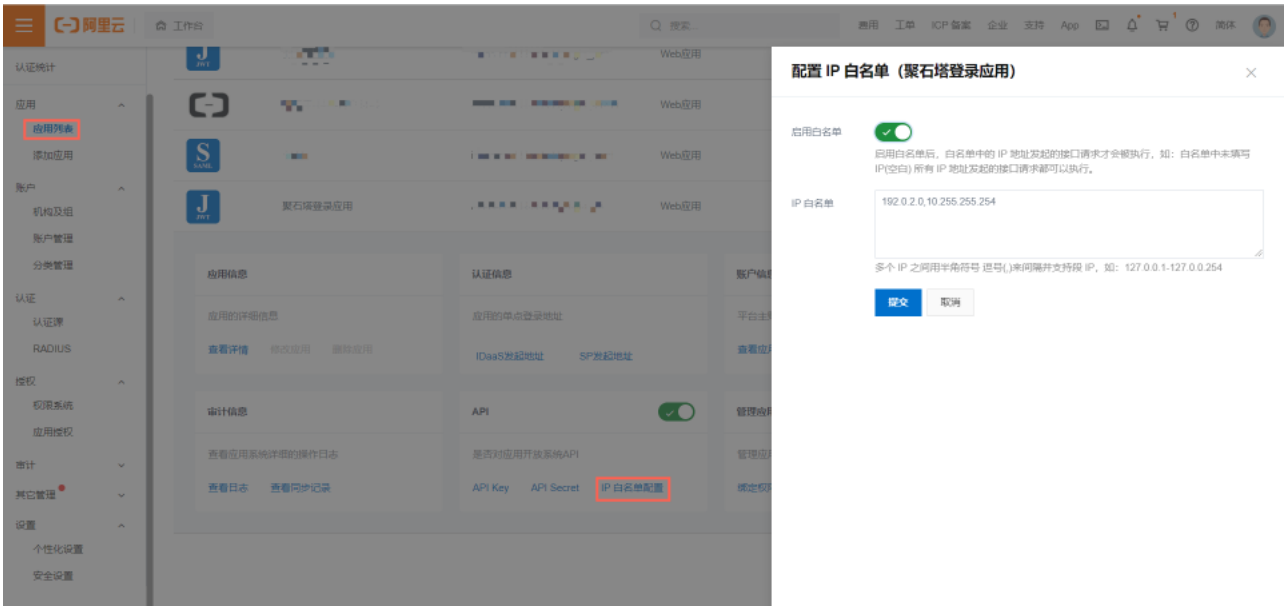
管理员可以在 **安全设置–IP准入** 中配置客户端 IP 黑名单，黑名单内 IP 的访问将被拦截，以实现对异常客户端 IP 进行控制。



6.4 IP 白名单拦截

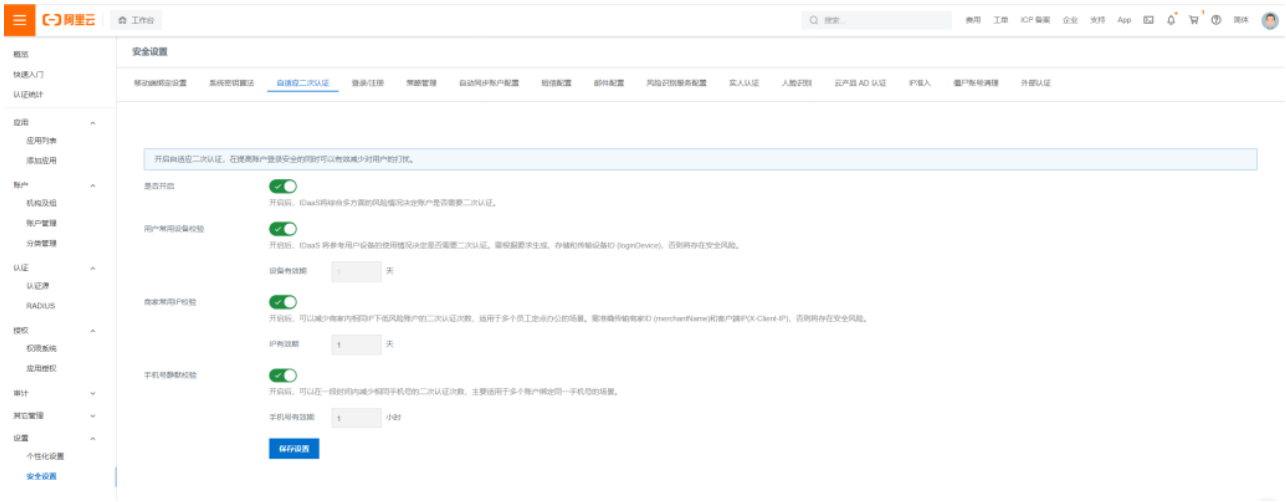
管理员可以在 **应用–应用列表–详情–IP白名单配置** 中配置服务端 IP 白名单，对调用 IDaaS 接口的 IP 进行限制，不在白名单内的 IP 的接口请求不会被执行，以提高服务端的安全性。

建议尽早开启 IP 白名单拦截，以提高服务端请求的安全性。



6.5 自适应二次认证

请在本文档 4.4 章节中，了解二次认证的概念和流程。如果开启自适应二次认证，我们建议适当缩短常用设备、常用 IP、静默校验等配置的有效期，以提高回流日志的覆盖率。



6.6 新注册用户不需二次认证

如果您希望一些场景下新注册的用户在首次登录时不需要二次认证（需确保注册时已经验证过用户，否则存在安全风险），可以使用本文档中 5.9 章节中的接口，在某个节点提前导入常用设备，并开启自适应二次认证中的用户常用设备校验。需要注意的是，如果用户长时间没有进行二次认证，可能会导致二次认证日志的覆盖率降低，请根据业务需要评估使用。

7. 常见问题

7.1 在淘宝开放平台中，是否所有应用都需要接入 IDaaS?

目前需要安全认证的、自建账号体系的应用才需要接入 IDaaS、具备IDaaS能力，淘系账号不需要。淘系账号的特点是：使用淘宝账号在淘宝登录页登录。

安全能力评估—安全分具体评分规则

分类	环节	评分项	评分标准
基础能力（门槛）	基础要求环节	数据处理	是否完成平台加密改造方案、历史数据清理、明文落库？
		数据使用	前端系统明文导出功能？
		渗透测试	近3个月内渗透测试报告
		等保测试	近1年内等保测试报告
		运维信息	企业、资产、人员信息补充完整
		内容安全	内容安全管控节点凭证
防护能力【1.75】	安全要求节点	账号风控（淘系账号/idaas）	系统具备账号风控能力，淘系账号体系默认享有平台提供的账号风控能力，自建账号体系接入idaas
		Web应用防护（waf）	系统具备waf防护能力，并具备反爬能力
		云防火墙	C/S应用需具备互联网边界防火墙防护能力
		安全访问服务边缘（sase）	内网安全防护能力，并开启二次认证功能
		云安全中心	不做安全分计算
运营能力【2.65】		解密日志	调用平台oaid解密接口日志回传平台
		订单日志	用户明文敏感信息相关订单操作日志回传平台
		登录日志	淘系用户登录日志回传平台
运维能力【0.6】		弱口令、账密加密存储 系统脆弱性监测 服务器的accesskey白名单限制 高危、敏感端口不得开放公网 网络安全组访问控制策略 抗DDOS能力	运营监控环节以御城河漏洞形式将问题下发
特殊加减分项	安全活动	参与组织安全活动、主动上报潜在风险隐患或情报信息、平台官方渠道公示的其他加分项	
	安全事件	重大风险事件、应用安全违规产生≥3分违规扣分事件、平台官方渠道公示的其他减分项	

7.2 接入 IDaaS 后，是否还需要对接御城河账号风控?

不需要。按要求对接 IDaaS 并开启二次认证即可。**IDaaS具有更强的账号风控能力**，已经接入御城河风控的应用，需尽快切换至 IDaaS。**后续接御城河账号风控是不得分的。**

7.3 接入 IDaaS 后，是否还需要对接御城河的日志?

IDaaS 会自动完成御城河所需的 **IDaaS日志** 和 **二次认证日志** 回流，您不需要单独对接。但目前御城河要求所有进行安全认证的应用，都需要对接御城河三个基础日志（登录日志、解密日志。订单日志）进行数据回流。

7.4 根据要求接入 IDaaS 后，账号风控模块依然被扣分?

存在三种可能性，可按顺序逐个排查：

（1）没有完成御城河第一节点的审核。

（2）没有正确对接 IDaaS 并开启二次认证，例如X-Client-IP、appKey、merchantName 等参数传输有误。需要注意，merchantName 指的是淘宝商家主账号名称（即掌柜名），而非店铺名。

（3）对接后在 IDaaS 中登录和二次认证的次数过少，导致一段时间内日志覆盖率不足。

7.5 如果认证次数提前用完了怎么处理?

实例的认证次数接近用完时请及时购买认证加油包（加油包无法享受聚石塔专属折扣），以免影响您的业务。一个加油包可以加到一个实例上。如有需要，请联系 IDaaS 团队获取加油包的购买链接。

7.6 二次认证所需的短信如何收费?

二次认证的短信费用暂时免费，以方便您快速接入。预计2022年2月份开始，IDaaS 将逐步提供短信包服务，供您进行购买和使用。

7.7 实例是否可以升降配?

目前支持续费变配，即在下一个计费周期续费为不同规格的实例。例如您购买了100万次规格的实例，可以续费变配为300万次规格，当100万次规格的实例到期时自动变配为300万次规格。如需进行该操作，请联系 IDaaS 团队获取续费变配链接。

需要注意的是，由于专属版和共享版（即针对小微 ISV 的试用版本）实例的部署架构不同，两者不能互相升降级。例如，如果您使用的是共享版实例，则需要重新新购、对接才能使用专属版。

8. 联系方式

如果您在购买、对接、使用过程中遇到问题，**请使用钉钉搜索 33623553 加入支持群【备注 IDaaS】**，联系阿里云 IDaaS 团队进行支持。