ALIBABA CLOUD

阿里云

应用身份服务 IDaaS

产品简介

文档版本：20230215

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
Courier字体	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

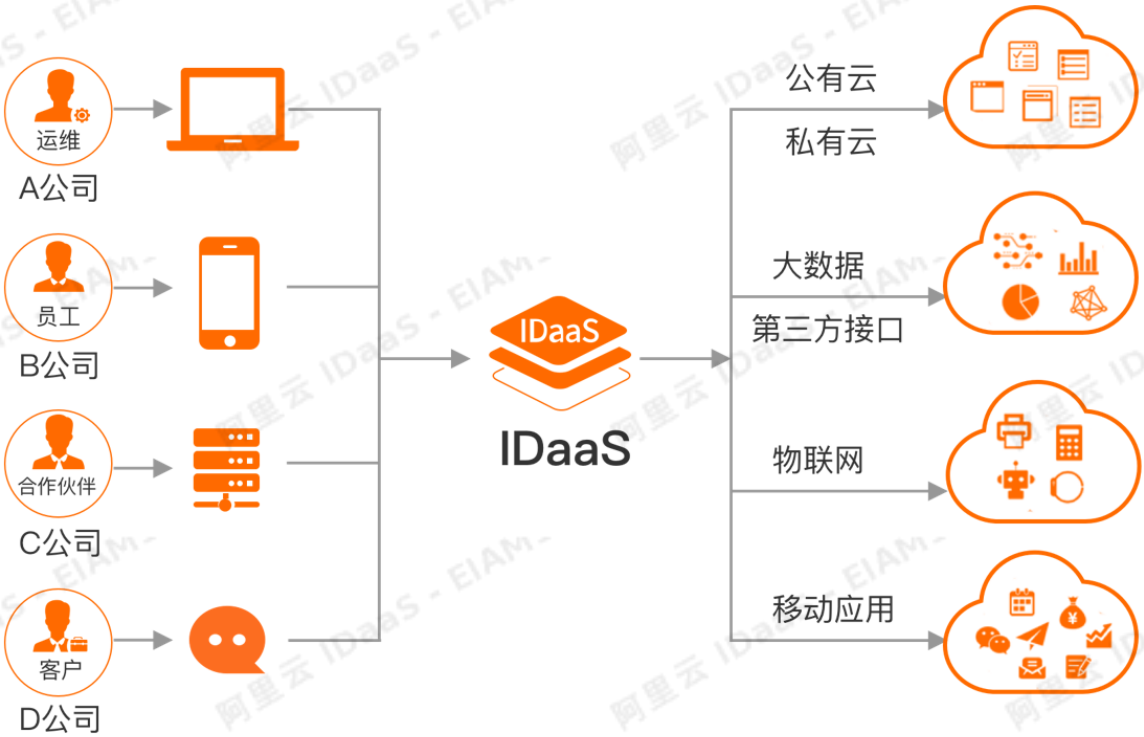
目录

1.什么是IDaaS

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，IDaaS支持多种产品，下面具体介绍产品信息。

EIAM

EIAM（Employee IAM）：针对内部员工、生态合作伙伴、分级线下店铺等企业内的身份管理，帮助整合部署在本地或云端的内部办公系统、业务系统及三方SaaS系统的所有身份，实现一个账号打通所有应用的服务。



用户可以使用一个账户，在不同终端上畅通所有办公应用。如可以在PC客户端，使用钉钉扫码方式登录OA，Jira, Gitlab 等不同应用。

更多支持场景，请查看应用场景。

具体对接操作，请查看IDaaS通用-对接指引。

CIAM

CIAM（Customer IAM）：针对外部消费者、会员、订阅服务者等终端用户进行的统一身份管理，实现跨平台的高性能、高安全的本土化会员身份使用和管理。

不管消费者是通过门店、App、Web页面、微信小程序等渠道进行访问，还是通过微信，微博，短信等方式进行登录，都可以快速识别用户，方便用户灵活选择适合登录方式，企业也可以对用户消费行为进行运营分析。

CIAM 具体介绍，请查看什么是 IDaaS CIAM。

安全认证

安全认证提供便捷，安全，全面的注册、登录和支付认证解决方案，支持多认证方式的一站式快速集成，支持手机号认证，生物识别（IFAA），短信，OTP令牌，社交账户登录等。

1. 手机号认证服务： 整合三大运营商特有的数据网关认证能力，升级短信验证码体验，应用于用户注册、登录、安全校验等场景，可实现用户无感知校验，操作更安全、便捷、低时延。

2. 生物识别（IFAA）：支持通过指纹和人脸识别进行认证，通过移动端硬件级加密，防Root及中间人攻击，保障认证的安全性。可实现用户便捷的登录和支付操作，提高安全性，并降低成本。

其它产品

IDaaS除了公有云上支持的EIAM，CIAM，安全认证产品以外，还支持智慧城市身份中台，零信任身份定义边界SDP等产品， 并支持私有化部署。

如果需要对IDaaS使用场景进一步沟通，欢迎联系我们。

2.应用场景

本文介绍IDaaS主要的应用场景，帮助您快速找到适合的解决方案。

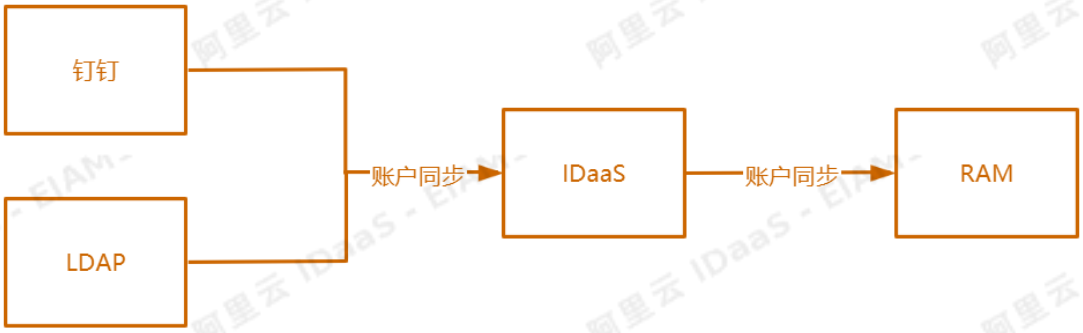
IDaaS主要支持以下应用场景：

- 企业账户统一管理和授权
- 一次性登录
- 支持多认证方式
- API令牌保护
- 不同账户之间数据同步
- 简化权限分配管理
- VPN网关双因子认证

企业账户统一管理

- **支持第三方应用账户自动同步**

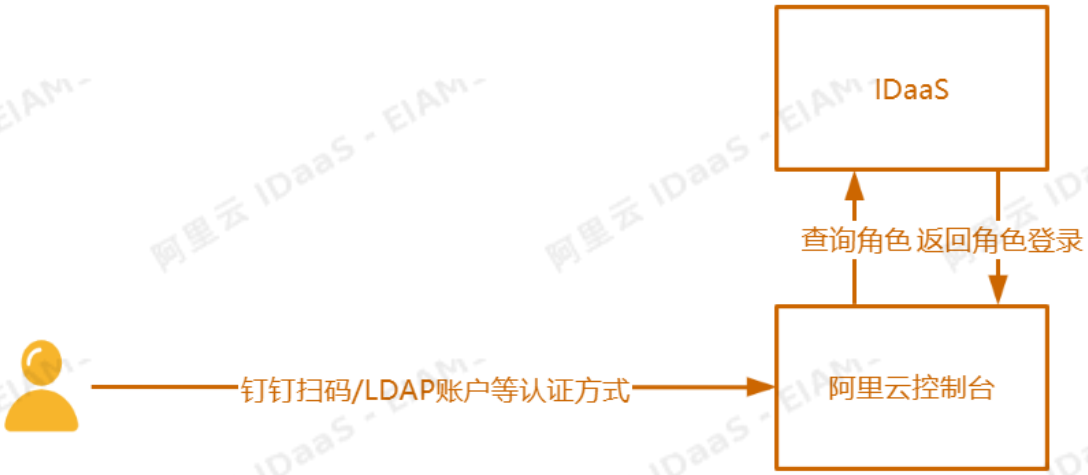
  如果使用钉钉、LDAP 等第三方应用管理账户，IDaaS可以同步这些账户信息到RAM，实现您只需要在钉钉或者LDAP中管理账户的需求。



- **RAM账号自动授权**

  使用RAM的角色SSO，只需要在RAM中创建不同的角色，给角色赋予不同的权限。

  员工通过IDaaS登录时使用对应的角色，就可以自动集成角色的权限，无需为每位员工单独创建RAM账户。

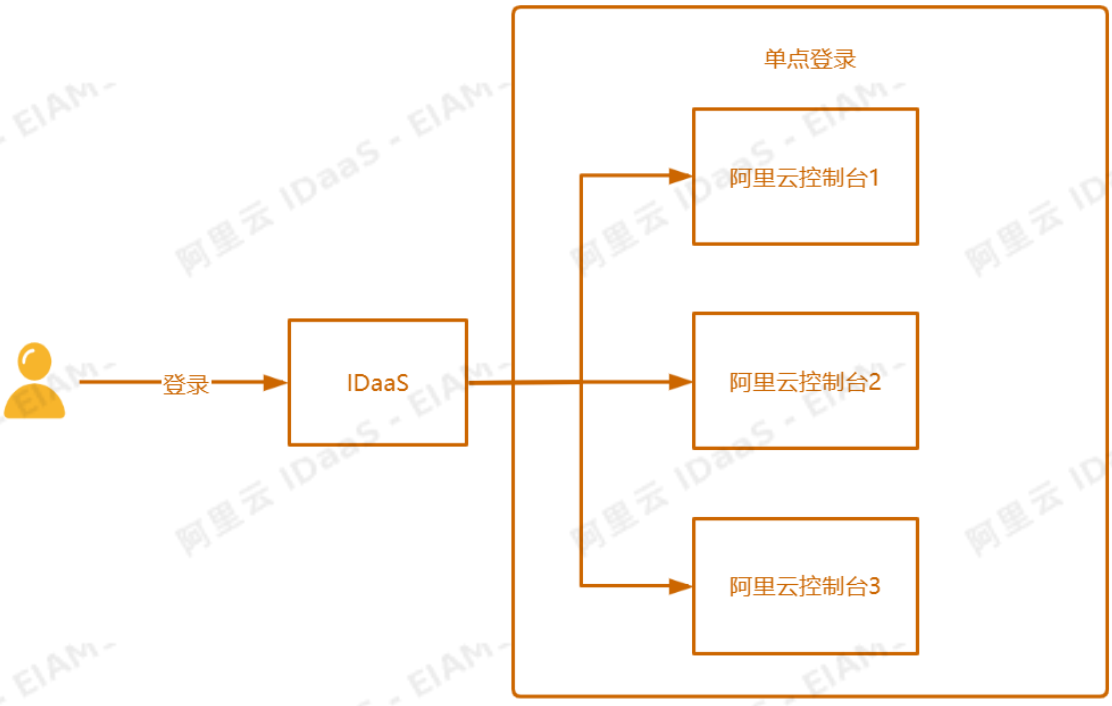


一次性登录到阿里云控制台和其他应用系统

- **单个账号实现单点登录多个阿里云控制台**

  企业可能会出于部门之间的相互独立、应用之间的强隔离、财资的独立结算、子公司法律主体的差异、单个阿里云账户使用云产品上存在的规格限制，或者需要区分正式、测试环境等需求，创建了多个阿里云账户。因此，需要频繁切换多个登录账号登录阿里云控制台，极大影响工作效率。

  IDaaS提供单点登录功能，实现只需登录一次IDaaS控制台，无需切换账号就可以畅通访问所有有权限访问的阿里云控制台。



- **登录后直接跳转到指定的阿里云应用管理系统**

  企业员工需要使用不同的办公应用，经常会在不同的应用系统间切换登录账号，影响工作效率。

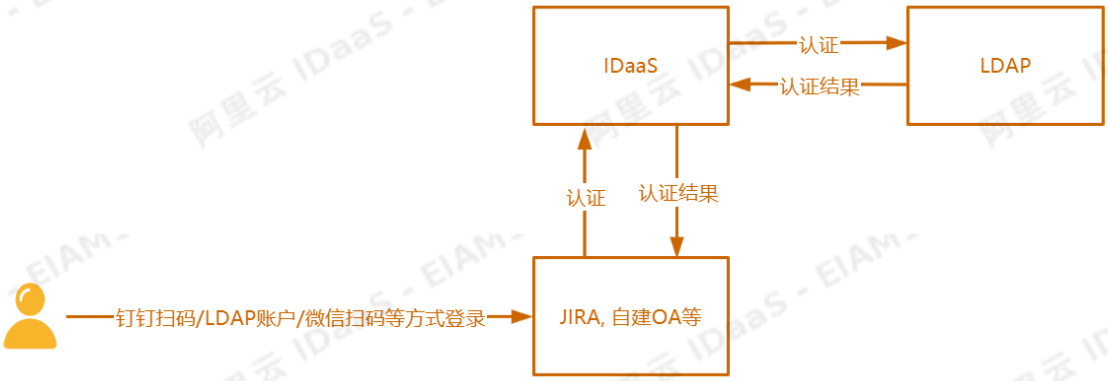
IDaaS提供多种应用模板，既支持标准的SaaS应用，满足单点登录要求，同时也支持自建系统的单点登录集成对接，为企业员工提供统一的登录门户。IDaaS帮助您通过一次单点登录，就可以直接访问其他所有已配置的应用，提高企业员工的工作效率。

如果您的服务器使用了云效、云桌面、DMS等应用， 登录IDaaS后可以直接跳转到指定应用的管理系统。

支持多认证方式

IDaaS提供的多种认证方式，只需简单的配置，员工就可以使用钉钉扫码等常用的登录方式，直接登录到应用系统中。

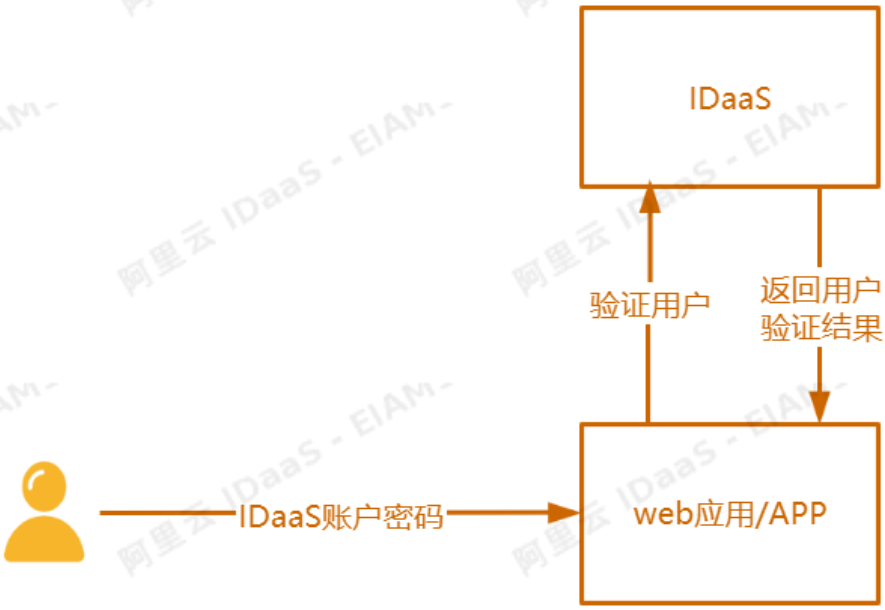
企业员工如果使用RAM子账号登录阿里云控制台，需要单独记录RAM账号及其密码。IDaaS可以实现通过钉钉扫码、LDAP账号密码、微信扫码等常用方式登录阿里云控制台。



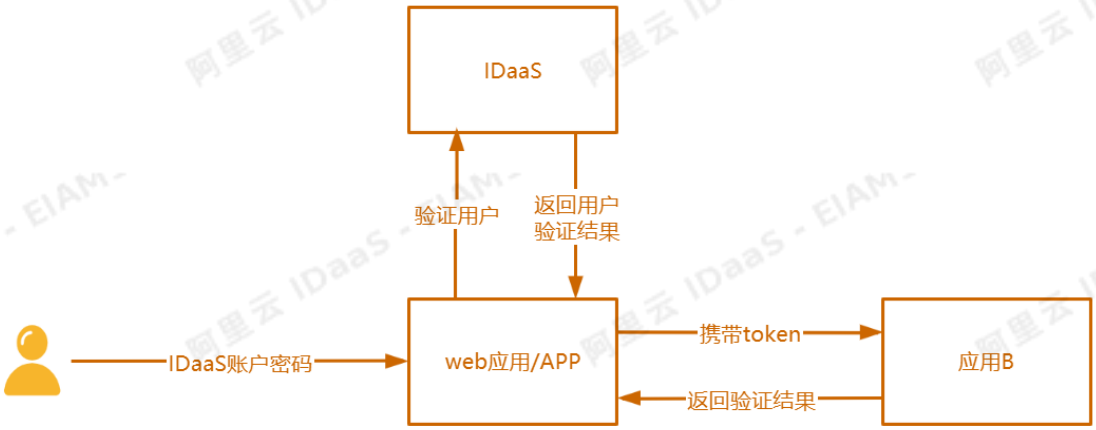
API令牌保护

客户应用在登录认证，或者系统之间交互时，希望仍然使用自己的登录页面。

- IDaaS提供登录认证接口，将API认证授权集成到IDaaS平台，使用户可以直接访问自己的登录页面。适用于Web应用和APP登录认证。



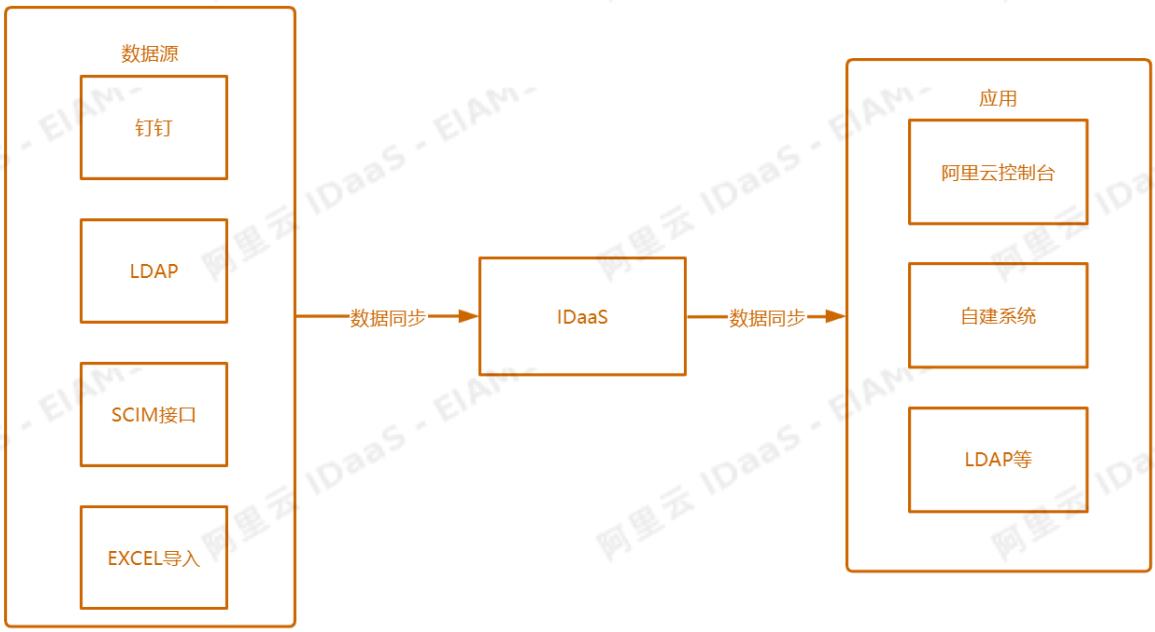
- IDaaS提供系统之间的API保护，如应用A使用IDaaS的登录接口认证通过，应用A需要访问应用B的资源时，可以携带IDaaS颁发的token访问应用B，应用B通过预集成的public key解析token，解析通过后应用A可访问应用B的资源。



不同账户之间数据同步

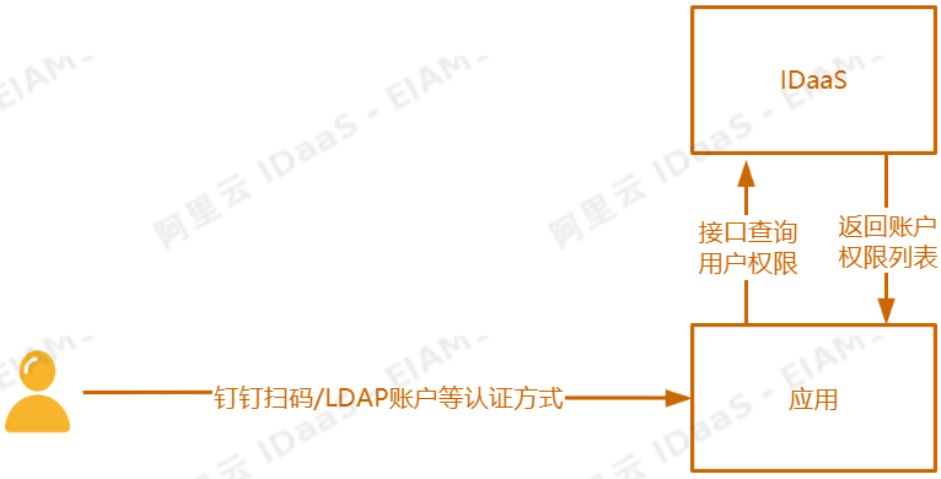
员工数据如果在每个应用中单独管理，不但费时费力，还很容易出现错误，如果只在统一的系统中管理用户，将极大减少维护数据的成本。

IDaaS提供多种数据同步方式，既支持LDAP协议、SCIM协议、EXCEL导入以及标准应用的接口同步，也支持自建应用同步的方式，实现各应用和IDaaS之间的数据同步。



简化权限分配管理

IDaaS提供基于RBAC、ABAC的权限控制，可以根据人员、组织、角色、账户属性等多维度的权限控制，极大地简化了权限分配的管理。实现对员工访问应用的权限进行细粒度的控制。校验用户是否有应用登录的权限，可以访问应用中的哪些菜单、按钮，对哪些数据有查看、编辑等权限。



VPN网关双因子认证

使用VPN网关，配置SSL服务端并开启双因子认证。客户端通过SSL-VPN接入云上VPC，不仅要完成证书认证，还需要完成双因子认证，认证通过后才可以访问云上资源，提高了VPN连接的安全性和可管理性。

双因子认证包含两种方式：使用IDaaS账户和密码做认证； 经由IDaaS使用LDAP或AD账户和密码做认证。


VPC
华东1(杭州)
192.168.1.0/24
ECS
VPN网关
SSL-VPN
证
+
证书密钥认证
双因子认证
Windows客户端

视频介绍

3.IDaaS通用-对接指引

本文是为阿里云客户提供的方案，实现和IDaaS的快速对接。聚石塔客户请查看聚石塔身份护航-对接指引。

单点登录

单点登录（SSO），英文全称为 Single Sign On。 SSO 是指在多个应用系统中，用户只需要登录一次，就可以访问所有相互信任的应用系统。

使用场景介绍

1. 单点登录到IDaaS门户

场景：企业内部有多个办公系统，员工访问IDaaS提供的门户，登录后可以看到有权限访问的应用，点击应用图标实现单点登录。

优势：只需要登录一次就可以访问所有应用。

说明：需要选择IDaaS提供的应用模板，进行单点登录的对接，点击下图中的图标，实现单点登录。

2. 访问IDaaS登录页面，直接登录到应用

场景：使用IDaaS提供的登录页面，登录后直接访问到应用中，如登录后直接访问到Jira。

优势：不用访问IDaaS的门户，直接访问应用。

说明：需要选择IDaaS提供的应用模板，进行单点登录对接，登录页面的logo，公司名称等信息可以自定义设置。

3. 访问应用提供的登录页面，IDaaS认证通过后直接访问到应用

场景：企业使用自己的登录页面，当输入IDaaS账户和密码进行登录时，通过接口向IDaaS发送验证请求，验证通过后用户登录到应用。

优势：企业可以使用自己的登录页面，展示风格和内容可以自己维护。

说明：不需要使用IDaaS的应用模板，直接调用IDaaS的登录认证接口进行身份验证。

请参考该文档 https://help.aliyun.com/document_detail/145016.html

应用模板和接口说明

IDaaS支持的应用模板，可以在管理员-添加应用页面看到。

如何选择应用模板

1. 如果是标准应用 Jira , Gitlab 等，可以直接使用应用支持的标准协议对接，如Jira选择SAML模板进行对接，更多应用对接请参考单点登录最佳实践 。阿里云控制台对接可以参考阿里云控制台单点登录。

1. 如果是标准应用 Jira , Gitlab 等，可以直接使用应用支持的标准协议对接，如Jira选择SAML模板进行对接，更多应用对接请参考单点登录最佳实践 。阿里云控制台对接可以参考阿里云控制台单点登录。

2. 如果是自建应用，应用不支持图片验证码的，可以使用表单代填验证是否支持，如果不支持的话，需要应用做少量代码改造，可以使用JWT 或者 OAuth2模板进行改造对接，对接 参考文档。

2. 如果是自建应用，应用不支持图片验证码的，可以使用表单代填验证是否支持，如果不支持的话，需要应用做少量代码改造，可以使用JWT 或者 OAuth2模板进行改造对接。

用户目录

UD（User Directory）用户目录，用于集中管理公司的组织机构，组及账户，管理员通过设置IDaaS中的组织单位、组及账户，实现用户的统一身份管理。一个用户，一套账户密码，对账户进行统一管理，可以在功能上替代传统的AD。

使用场景介绍

1. 应用中的组织/账户和IDaaS同步

场景： 如企业中使用OA管理用户数据，这些数据需要同步到IDaaS，以实现账户单点登录的权限控制，或者使用IDaaS统一管理用户数据。

具体接口请查看应用数据推送到IDaaS 和 IDaaS推送数据到应用。

2. LDAP中的组织/账户和IDaaS同步

场景：如企业中使用LDAP管理用户数据，这些数据需要同步到IDaaS，以实现通过LDAP账户和密码进行单点登录等需求。

具体配置文档请查看 LDAP组织/账户同步到IDaaS 和 使用LDAP账户密码进行单点登录。

3. 钉钉中的组织/账户和IDaaS同步

场景：企业使用钉钉维护用户数据，这些数据需要同步到IDaaS，以实现通过钉钉扫码/钉钉微应用进行单点登录等需求。

具体配置文档查看 钉钉数据同步到IDaaS、IDaaS数据同步到钉钉、使用钉钉扫码进行登录和使用钉钉微应用进行单点登录。

认证源

用户登录到IDaaS门户或者应用中，除了使用账户和密码登录方式以外，IDaaS还提供多种便捷登录方式以及二次认证功能。

1. 便捷认证方式

场景：用户可以使用钉钉扫码，微信扫码，支付宝扫码等方式进行登录。

具体配置方式请参考帮助文档。

具体配置方式请参考帮助文档。

2. 二次认证

场景：使用单一的认证方式不满足安全需求，增加双因子认证以保障安全性，如登录后还需要验证OTP，或者短信，加强对用户的身份校验。

具体配置方式请参考帮助文档。

权限系统

IDaaS支持基于角色的权限访问控制（RBAC），以及基于属性的权限访问控制（ABAC）。

1. IDaaS系统权限控制

场景：企业设置分级管理员，以区分不同人员的管理权限，如审计管理员只可以看到审计日志，不能对人员进行入职，离职等操作；北京分公司的管理员只能管理北京的员工的数据，看不到其它区域的员工数据等。

说明：IDaaS系统权限控制只在专属版支持，在标准版不支持该能力，如有需求，可以使用专属版。

2. 自建系统权限控制

场景：企业内部的OA，需要区分不同人员的管理权限，如人事专员可以访问OA，但是不能看到所有页面，只能看到添加员工的页面，并且只具有“入职员工”的权限。该场景可以使用IDaaS统一管理OA的权限，当用户登录时，向IDaaS发送请求，校验该用户的身份以及访问OA的具体的权限。

请查看自建系统具体介绍 和 支持的接口清单。

案例

需求：使用AD账户管理阿里云控制台的RAM账户，实现用户只在AD中管理，不用手动维护RAM账户，用户登录阿里云控制台时可以使用AD账户和密码进行登录。

1. 配置RAM账户单点登录到阿里云控制台；

1. 配置RAM账户单点登录到阿里云控制台；

2. 配置LDAP认证并同步AD账户到IDaaS；

2. 配置LDAP认证并同步AD账户到IDaaS；

3. 配置IDaaS默认登录方式是AD账户认证，见下面自定义设置

4. 访问RAM子账户登录地址，自动跳转到IDaaS登录页面，认证通过后访问到阿里云控制台。

自定义设置

IDaaS除了以上功能，还支持自定义操作，以下是几个常用操作的介绍。

自定义域名

自定义登录页logo，公司名称等信息

配置阿里云-短信网关

自定义密码策略等内容

设置IDaaS登录页面默认登录方式，如设置钉钉扫码，或者AD账户和密码为默认登录方式

其它问题

主子账户关联和绑定

4.聚石塔身份护航-对接指引

背景介绍

此方案是为聚石塔客户提供的专项身份护航方案，聚石塔客户需要根据该方案进行对接，其它阿里云上客户，可以参考该访问对接，也可以查看IDaaS通用-对接指引。

对接方案介绍

应用侧需要根据IDaaS规范进行改造，购买IDaaS标准版进行对接，如有定制化需求，需要使用专属版进行定制开发，提供单独的报价。

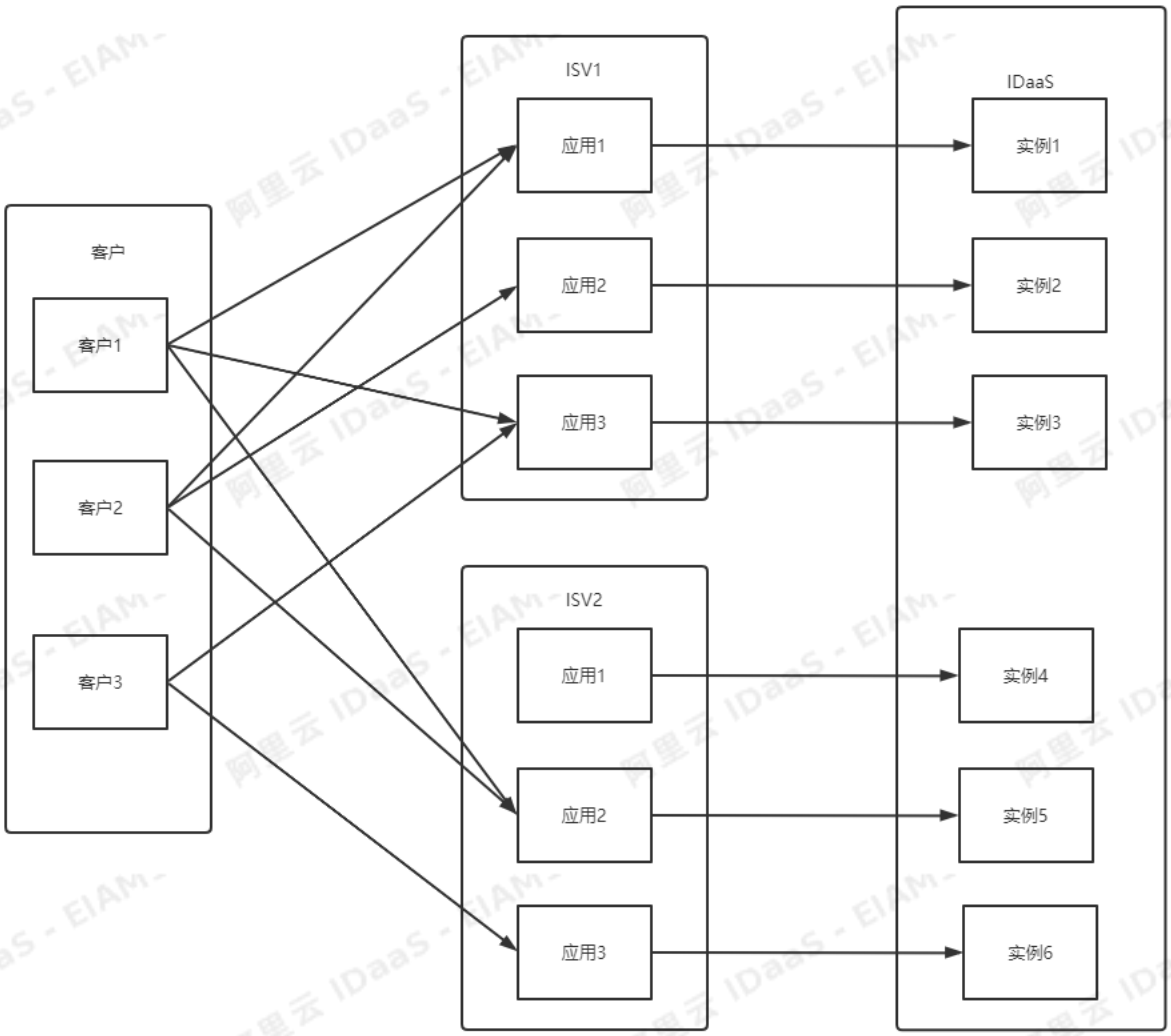
标准版对接方案介绍：

- 使用JWT应用模板进行单点登录对接，用户使用IDaaS提供的SP发起地址进行访问，IDaaS接管应用原来的登录入口。
- 当切换到IDaaS登录入口之前，需要应用把所有账户都同步到IDaaS中，当用户从IDaaS登录页面进行登录时，IDaaS需要校验用户的数据实现认证。用户数据仍然在应用页面进行维护，通过接口把账户信息以及明文密码同步到IDaaS中。

下面是对标准版对接方案的具体介绍

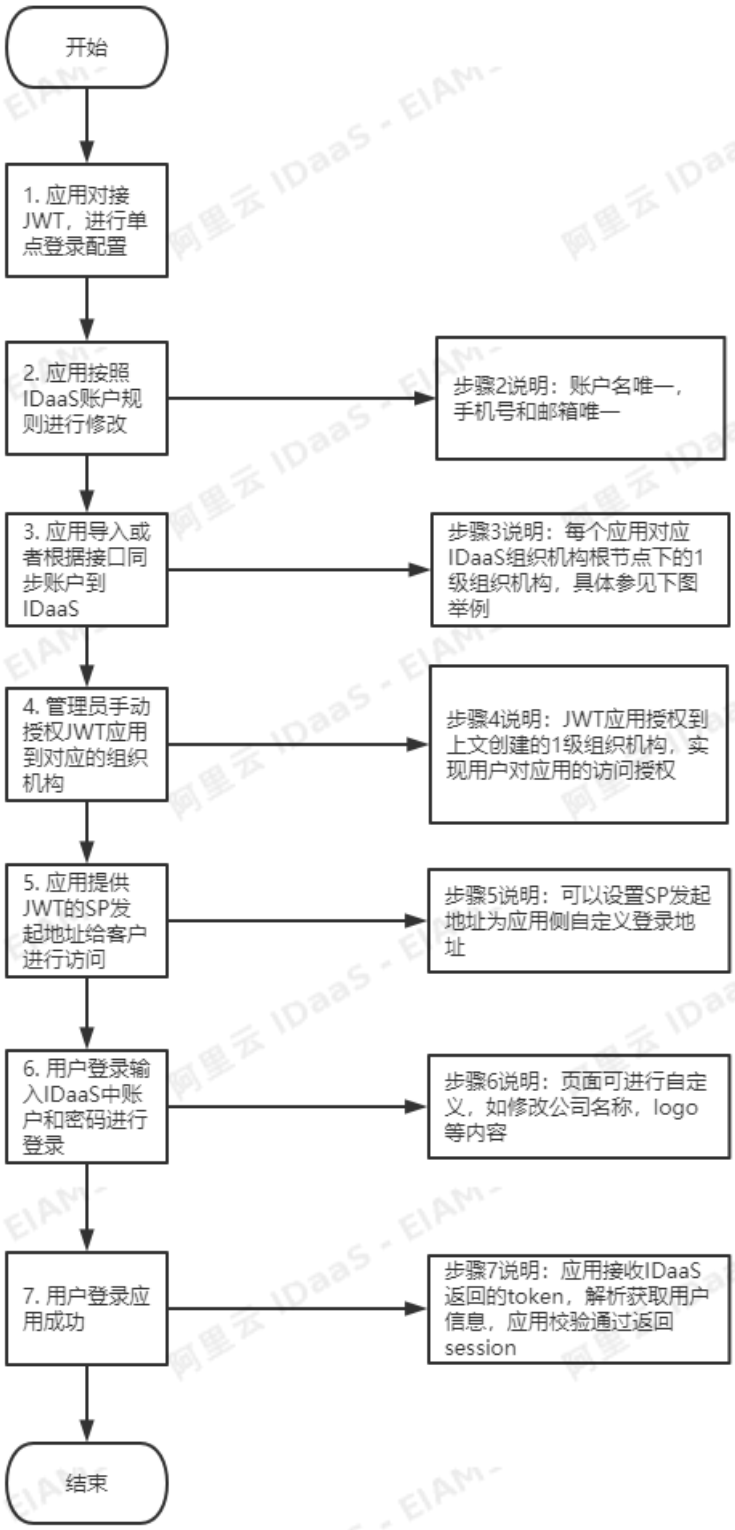
客户，ISV和IDaaS对应关系

淘宝商家，ISV 和 IDaaS直接对应关系。 一个淘宝客户可以购买多个应用，可以是同一个ISV提供的，也可以是不同ISV提供的； 一个应用对应1个IDaaS实例，实现不同应用数据之间实例的隔离。



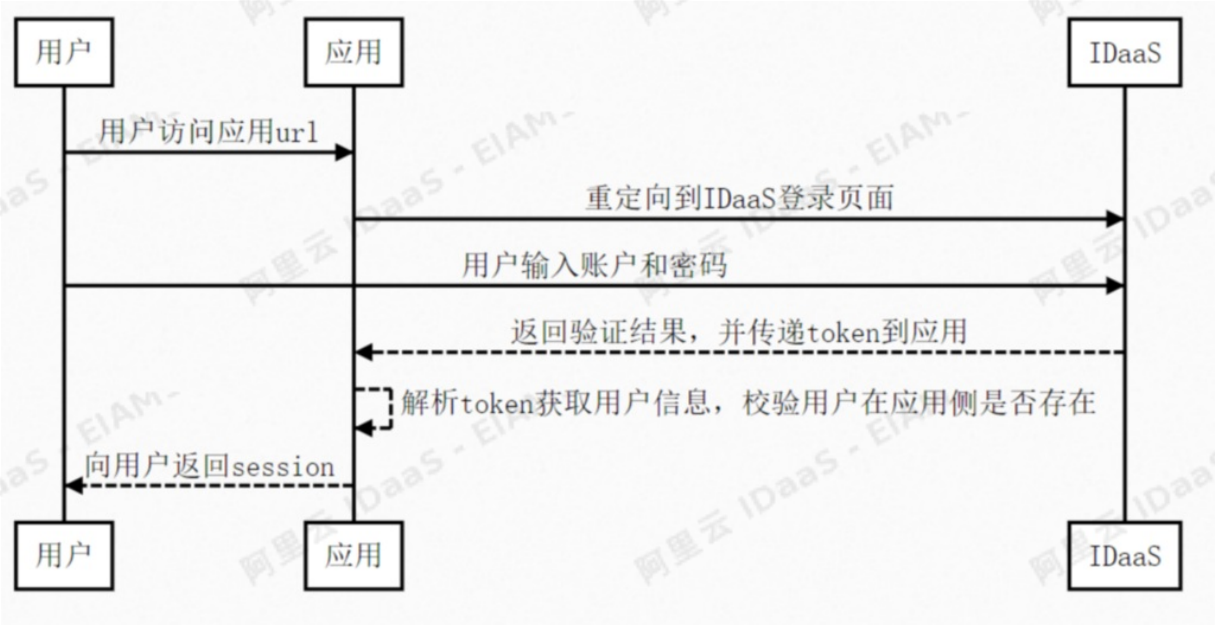
应用对接流程

应用侧的登录被IDaaS接管，通过集成IDaaS的JWT应用模板进行单点登录对接，用户访问IDaaS提供的登录页面进行登录，通过向应用传递token进行用户身份的验证。



JWT对接参考文档：https://help.aliyun.com/document_detail/167870.html

用户认证流程

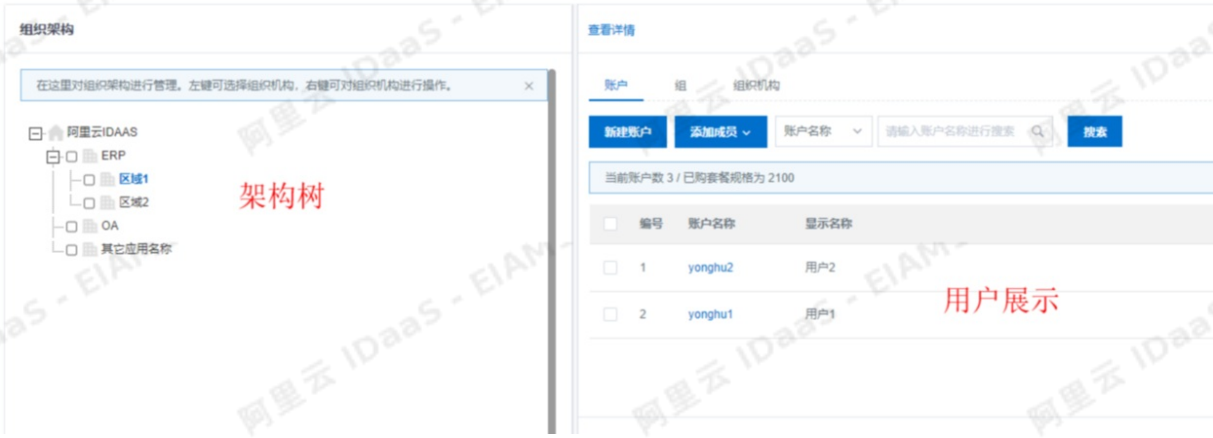


数据同步

以IDaaS的组织机构对应SaaS应用的数据。

- 当添加一个应用时，在IDaaS的根节点下创建一个和应用名称相同的组织机构；应用节点下也可以增加下级组织，如下图所示。
- 历史账户通过导入或者接口同步到IDaaS，新建账户通过接口直接同步到IDaaS指定组织机构节点下，修改和删除也可以通过接口同步到IDaaS。

从应用推送数据到IDaaS文档：https://help.aliyun.com/document_detail/143467.html



新建账户指定属于哪个架构树的节点，如属于上图ERP的区域1。

推送账户

SP中添加一个账户，调用此接口，将新添加的账户的信息同步到IDaaS中。

Request URI: /api/bff/v1.2/developer/scim/account/create `POST` `REST`

Content-Type: application/json

Request Body:

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

应用侧删除账户，直接调用删除接口进行删除。

删除账户

在SP中删除一个账户，通过调用此接口，删除IDaaS中该账户信息。

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

请求参数说明：

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

请求示例：

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

Response Body：

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

应用授权

在IDaaS中通过JWT模板创建的应用，按照组织节点进行授权，如ERP应用只授权ERP及其子节点。

主子账户关联

主账户：IDaaS中的账户为主账户

子账户：应用内的账户为子账户

当IDaaS向应用传递的token中，会包含账户的子账户信息，应用侧校验子账户是否属于应用内的账户，校验通过给用户返回session。

账户关联两种方式：

账户关联：系统按主子账户对应关系进行手动关联；

账户映射：系统自动将主账户名称或指定的字段映射为应用的子账户。

建议使用账户映射，IDaaS中创建主账户后，当用户访问应用时会自动生成和主账户同名的子账户，不需要手动维护主子账户关系。

注意：需要保证应用侧的账户名称（或者其它用于校验用户的唯一标识）和IDaaS中的账户名相同。

自定义设置

自定义域名：https://help.aliyun.com/document_detail/164042.html

自定义登录页，请参考下图

定制化场景

1. SaaS产品有多个子域名

如产品地址是oa.com, 每个租户的域名是a1.oa.com; a2.oa.com; a3.oa.com.

需要沟通解决方案，使用专属版进行定制开发，单独提供报价。

2. SaaS产品有多个租户

如用户可以1个产品开通多个租户，每个租户中记录的用户信息不同。

需要沟通解决方案，使用专属版进行定制开发，单独提供报价。

3. 密码加密同步

如果用户密码在应用侧前端和后端都进行了加密，那么传递给我们的是加密的密码，当用户登录时，是输入的明文密码，IDaaS无法做校验。

需要沟通解决方案，使用专属版进行定制开发，单独提供报价。

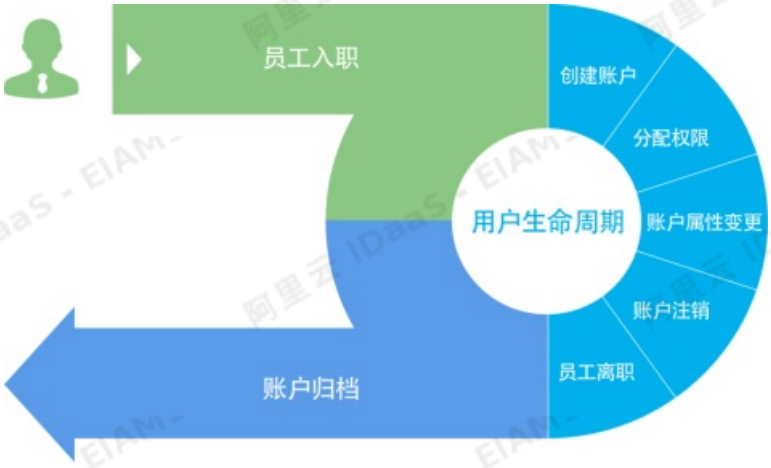
5.IDaaS 5A能力介绍

IDaaS 向您提供集统一账户管理（Account）、统一身份认证（Authentication）、统一授权管理（Authorization）、统一应用管理（Application）、统一审计管理（Audit）五项能力于一体的统一身份平台。

统一账号管理（Account）

随着企业业务的不断发展，众多应用系统不仅仅对员工开放，还要对合作伙伴甚至客户开放，面对繁多的应用系统，员工的入职、调岗、离职，不同身份的用户访问，账户管理和用户体验成为了企业 IT 面临的一大难题。

IDaaS 的统一用户管理，提供了统一集中的账号管理，支持管理所有的业务员工账号，支持矩阵式组织架构创建，提供横向、纵向灵活设计，实现被管理资源账号的创建、删除、启用/禁用及同步等流程的自动化管理，实现账号管理生命周期所包含的基本功能并可进行生存周期设定。



账户同步

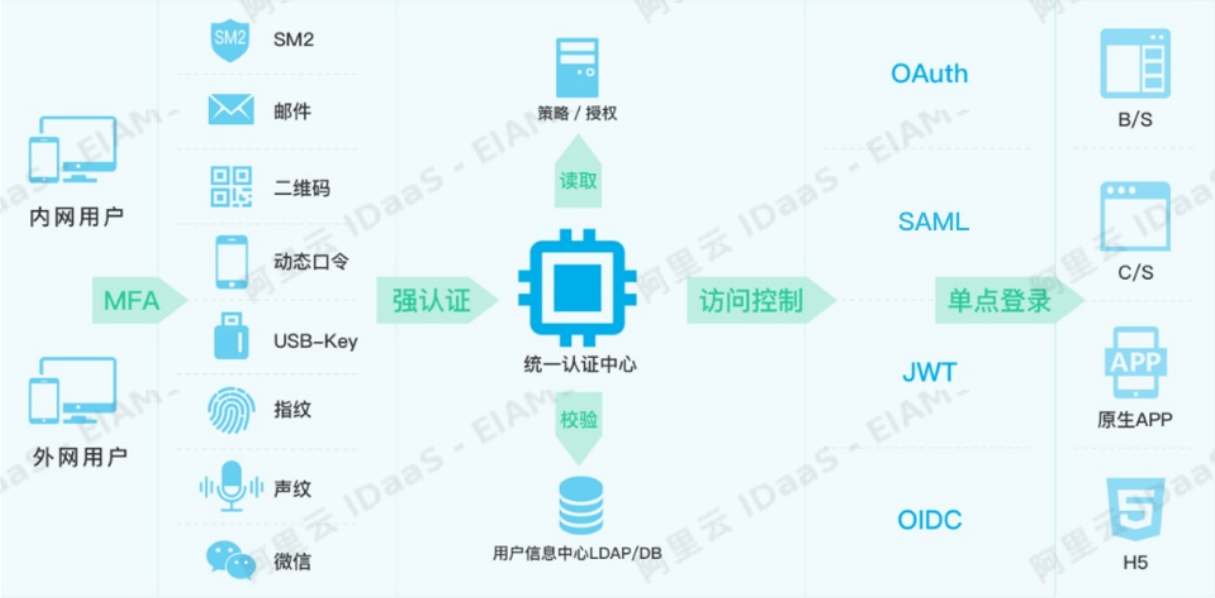
IDaaS 与应用系统之间以 SCIM / LDAP 方式建立通信。数据通过同步引擎、事务机制和 SCIM 与 LDAP 协议实现与应用系统之间的同步。同步的成功和失败都进行多维度记录，同步的成功信息以报告形式方便于管理人员查看，同步的失败信息通过定时器机制自动完成，直至同步成功。

通过 IDaaS 与各业务系统之间构建同步机制，只需在 IDaaS 一处管理（创建、修改、删除、移动）组织机构及用户信息即可根据平台配置策略同步到指定的业务系统中，业务系统运维人员无需再进行单独管理。

统一身份认证（Authentication）

IDaaS 实现用户在各个不同业务应用过程中的单点登录功能。支持不同域下业务应用统一认证集成，通过集中资源服务及授权管理系统提供的集中身份信息和权限信息，消除客户信息系统的业务孤岛和数据孤岛及对员工、合作伙伴、客户登录各个应用系统造成混淆和障碍。

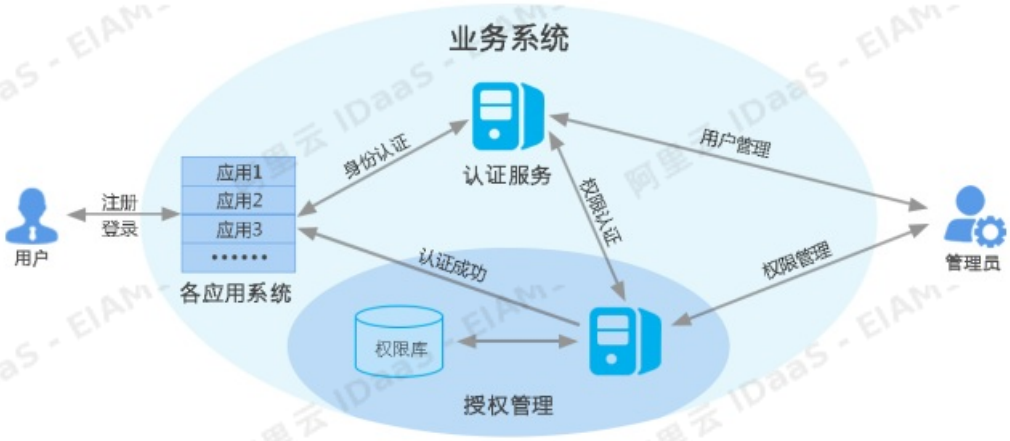
在用户认证之后，可以在不同业务系统中灵活切换角色和权限信息。从而确保用户只需要认证一次，便可以在访问权限的约束范围内访问不同的应用系统，从而达到“一次认证，安全漫游”的效果。



统一授权管理（Authorization）

IDaaS在对众多业务系统、运维管理设备有效管理的基础上，建立以人为主体、资源为客体的授权管理体系；并建立对应用权限申请、审批和授权的流程化管理；实现对网上用户统一的权限控制和管理。

通过统一授权管理，建立统一用户管理和权限视图，当用户职务、岗位等自然属性发生变化时，可以较快地响应变化，根据用户新的属性自动调整其能访问的应用客体对象，进一步降低管理成本，提高工作效率。通过平台创建安全组，将所有的系统用户以组的形式管理起来，通过应用授权给安全组或通过安全组指定应用两种授权机制，已达到管理用户的访问去向。用户访问控制总体框架如下图所示：



在此框架下，整个授权控制的工作流程如下：

1. 统一身份认证管理系统的初始化，添加并配置系统管理员；
2. 由系统管理员添加并配置下级管理员或用户；
3. 管理员添加受控访问资源，并设置每个用户的权限；
4. 用户访问各应用系统，首先由统一身份认证系统验证该用户的身份；
5. 认证通过后根据用户身份，对用户进行权限认证；
6. 如果用户通过权限认证，则说明该用户可以进入相应的应用系统，访问权限许可内的资源；否则，拒绝用户访问。

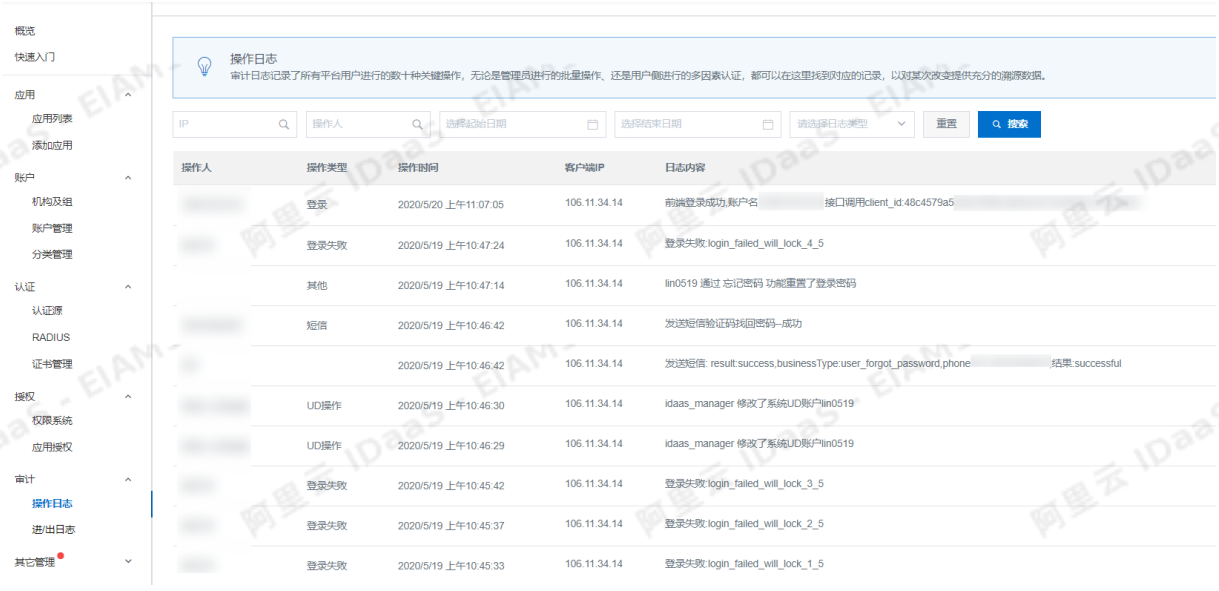
统一应用管理（Application）

为方便对业务应用的集中管控，IDaaS 的应用管理模块内预置了多种模板应用。所谓模板应用就是定义了一系列有规则的应用配置模板，根据企业用户现有业务系统架构、开发语言以及支持的认证协议不同与平台中已有的应用模板相匹配，只需要选择对应的模板应用，通过界面化最小配置便可完成单点登录的集成，从而到达安全快速管理所有业务应用的目的。

IDaaS 自身提供统一标准规范。平台自带开发者服务功能模块，此模块提供应用系统账户、应用的集成能力，并提供针对所有功能实现的标准规范，针对不同模块提供不同接口说明，满足企业现有业务系统便捷集成的同时可保证未来新业务系统实现统一规范化集成、管理，形成标准化流程操作。

统一审计管理（Audit）

透明审计管理主要记录系统范围内的安全和系统审计信息，有效地分析整个系统的日常操作与安全事件数据，通过归类、合并、关联、优化、直观呈现等方法，使管理员轻松识别应用系统环境中潜在的恶意威胁活动，可帮助企业/用户明显地降低受到来自外界和内部的恶意侵袭的风险。



6.开通和试用流程

本文介绍了用户如何在注册阿里云账户后开通 IDaaS EIAM 免费版并进行使用。

IDaaS EIAM 开通说明

IDaaS EIAM 免费版是开通即用，只需要注册阿里云账户就可以进行开通IDaaS EIAM 免费版。

如果需要试用付费版功能，可以申请免费试用一个月进行升级。

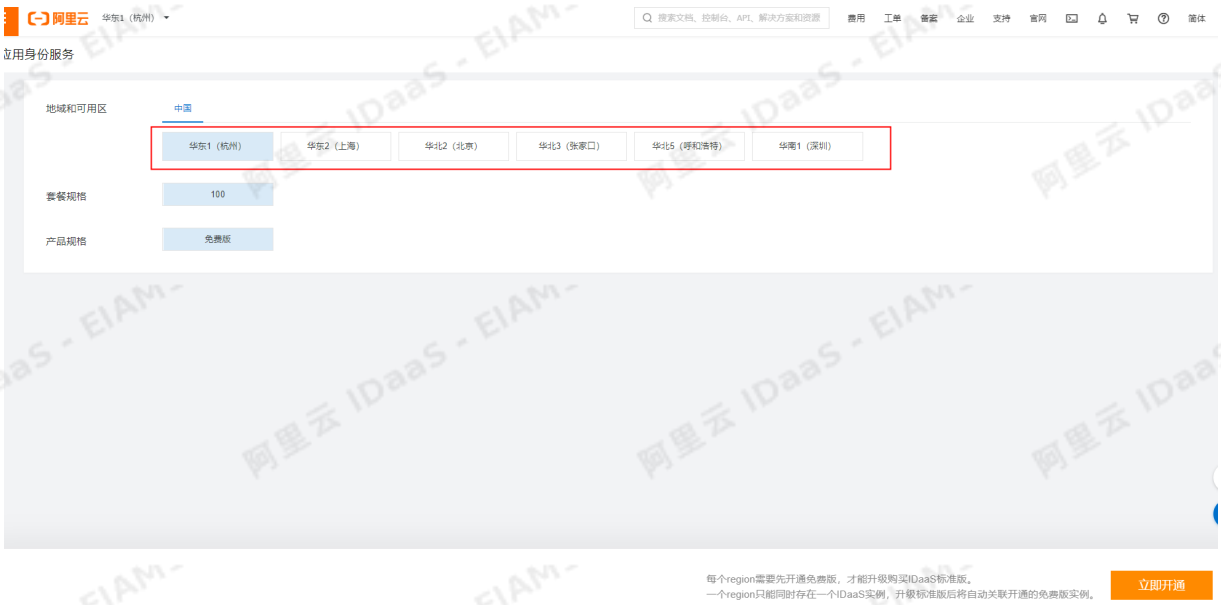
1. 访问 IDaaS产品详情页

点击免费开通EIAM。

2. 在IDaaS控制台，选择 EIAM 实例列表，点击右上角开通免费版

3. 选择region进行开通。

IDaaS控制台，默认显示杭州region，如果为了访问方便，可以优先选择杭州。



4. 开通后返回控制台查看

- 此处以开通北京region为例，默认显示杭州region没有开通。
- 通过左上角切换到北京region。

5. 点击实例名称，访问IDaaS管理员页面

6. 免费版开放单点登录，账户全生命周期管理等功能

如果需要试用标准版功能，可以点击升级。

7. 选择暂不升级，试用标准版一个月

跳转到调查问卷页面，填写完调查问卷，进行提交。

8. 调查问卷提交后，返回IDaaS管理员侧，点击立即升级

9. 可以免费升级标准版一个月

- 选择实例对应的region
- 选择100用户数规格

10. 重新返回IDaaS管理员侧，查看升级标准版成功

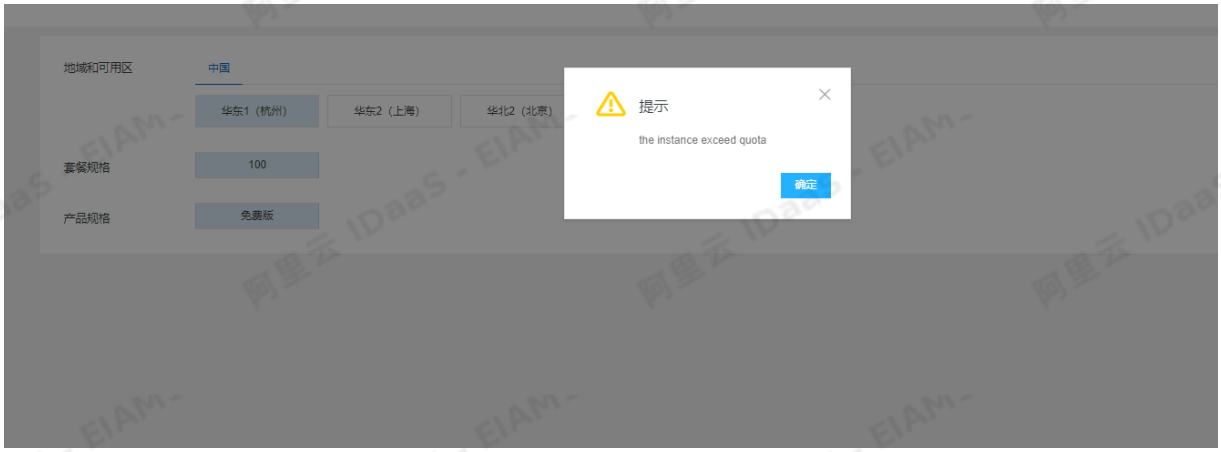
可以正常使用标准版功能

FAQ

填写完试用问卷后，但是新购仍然显示需要支持费用

请改用主账号登录，重新提交试用申请，然后点击升级。

开通IDaaS提示下面错误



在该region已经开通了IDaaS，不用重复开通，切换EIAM实例列表页左上角的region，查看对应region中的实例

IDaaS支持哪些region

目前支持：杭州，上海，北京，深圳，张家口

7.各版本功能和服务介绍

一、 各版本介绍

1.1 免费版

IDaaS免费版是开箱即用，客户无需支付任何费用就可以了解和试用IDaaS基础功能，为客户带来极大的便利，只需简单开通，主要用于开发测试联调，不提供SLA保障，客户服务是工单。

适用客户：适合前期调研了解IDaaS，不可用于生产环境，有释放期限。

1.2 标准版

收费版本，按照用户数量每月计费。标准版使用共享集群，客户会共享同一套集群中所有资源，不支持定制化开发功能，发版周期平均2-3个月更新一次，客户服务是工单+5x8钉钉群。

适用客户：适合中小型公司，使用IDaaS提供的标准能力，把IDaaS作为身份认证中心，没有定制需求。

1.3 专属版

收费版本，基础功能和标准版本大体一致。满足客户对稳定性的高要求，进行独立环境部署。支持专属版1000用户数及以上规格的功能定制服务（单独定价），支持方案咨询以及定制化方案、支持协助对接单点登录和数据同步等服务，发版周期短，可满足快速上线需求，客户服务是工单+7x24专属售后经理支持。

适用客户：适合中大型公司，有定制化需求，需要独立环境维护和更好的售后支持保障。

1.4 专家服务

可以申请IDaaS专家提供技术，提供解决方案及其它人工支持，IDaaS根据服务内容提供单独报价。

二、 各版本服务区别

	支持内容	免费版	标准版	专属版
	可购买用户数	100用户	100，300用户	1000及以上
	单点登录应用模板	支持1个	支持10个	无限制
	组织机构/组/账户增删改查操作	支持	支持	支持
	应用授权方式	支持账户授权	支持按组织/按账户/按分类授权	支持按组织/按账户/按分类授权
	登录方式	账户+密码	账户+密码，微信/钉钉/短信登录/AD等	账户+密码，微信/钉钉/短信登录/AD等
	二次认证	不支持	支持OTP，短信验证码	支持OTP，短信验证码

主要功能				
	钉钉相关	不支持	支持钉钉扫码，钉钉微应用，钉钉数据同步	支持钉钉扫码，钉钉微应用，钉钉数据同步
	LDAP导入/excel导入/SCIM同步	不支持	支持	支持
	自建系统对接权限系统	不支持	支持	支持
	日志审计	不支持	支持	支持
	Radius认证	不支持	支持	支持
	证书管理	不支持	支持	支持
	同步中心（connector同步）	不支持	不支持	支持connector
	登录页面个性化配置	不支持	支持	支持
	会话管理	不支持	支持	支持
	安全设置	不支持	支持	支持
	VPN二次认证	不支持	支持	支持
	实例释放	3个月释放（暂定）	降级到免费版（暂定）	到期后7天释放
	SLA	不保障。	99.9%	99.9%

服务可用	**高可用性**	不保障。	双节点高可用集群。	可定制高可用集群，可以在同一 region 下支持多节点多可用区部署，保障高可用性。
	部署环境	共享集群。	共享集群。	独享集群，独享计算资源、独享数据库实例、独享缓存。
	默认短信网关（会带阿里云签名，仅建议测试使用）	限额100条/月	限额1000条/月	赠送短信服务，具体短信赠送条数根据实际下单规格沟通决定
	使用购买的短信网关（可自定义短信签名，需要定制）	不支持	支持	支持
	测试联调环境	无。	无。	包含单独一套基本的测试联调环境，满足快速功能验证和上线联调需求。上线 1 个月后释放。若要申请延期，请联系 IDaaS 团队。
	安全运维	不保障。	基础安全运维，免费处理安全补丁。	当系统出现安全漏洞，最优先处理安全补丁。
	事件处理	不保障。	关键事件：45分钟内响应 大影响事件：2小时内响应 中影响事件：8小时内响应 小影响事件：1天内响应 事件咨询：3天内响应	关键事件：15分钟内响应 大影响事件：40分钟内响应 中影响事件：4小时内响应 小影响事件：8小时内响应 事件咨询：1天内响应

	关键事件护航	不支持。	不支持。	支持 7*24 小时的关键事件护航服务，确保 IDaaS 平稳支持关键活动。需要和 IDaaS 团队沟通事件情况、周期和对应费用，如双11服务保障等。
帮助咨询	**帮助文档**	访问 IDaaS帮助文档	访问 IDaaS帮助文档	访问 IDaaS帮助文档，支持沟通答疑。
	咨询支持	工单	工单 24 小时内反馈。5x8小时钉钉群支持	工单 24 小时内反馈。7x24 小时即时售后支持：电话、工单，专属服务群支持。
	对接工作支持（SSO，数据同步等）	不支持。	工单支持。支持购买专家服务进行人工支持。	包含人工对接支持服务，包含问题排查和必要的远程协助，确保对接使用顺利。
	专属技术服务经理	无。	无。	专属技术服务经理沟通最佳方案，输出最佳实践。
定制能力	**定制化、个性化功能**	不支持。	不支持。	支持为客户单独定制解决方案，支持产品能力定制。
	性能专属优化	不支持	不支持。	支持针对场景方案的性能调优，支持服务器弹性扩容，需单独沟通服务费用。

下面给出事件的基本定义和例子

- **关键事件**：系统高频操作行为（例如登录），在持续一段时间内（5分钟）内，至少有 50% 的请求失败，且业务影响范围极大（例如导致数万用户登录失败）

- **大影响事件**

  ：系统高频操作行为（例如登录），在持续一段时间内（15分钟）内，至少有 20% 的请求失败，且业务影响范围大（例如数百员工无法访问系统）

- **中影响事件**

  ：系统高频/关键操作行为（例如同步账户），在持续一段时间内（15分钟）内，至少有 20% 的请求失败，且业务影响明显（可能导致需要管理员手动进行频繁操作才能消泯影响）

- **小影响事件**：系统一般操作行为（例如新用户授权），在持续一段时间内（1小时）内连续失败，且业务影响可控较小

- **事件咨询**：针对可能发生的事件的咨询和沟通

8.功能特性

云盾IDaaS向您提供集统一账户（Account）、统一认证（Authentication）、集中授权（Authorization）、应用管理（Application）、透明审计（Audit）五项能力于一体的身份即服务平台（简称5A平台），本文介绍了具体的功能模块。

功能模块	描述
统一账户（Account）	一个账号对接多个子系统，同一用户在各种不同类型应用系统之间的账号相互打通。 各子系统的账户关联到主账户中，实现账号体系的统一，方便员工的生命周期管理。具体功能点包括： • 用户目录 • 身份信息同步 • 身份信息全生命周期管理
统一认证（Authentication）	采集多种认证因子，通过发行加密身份凭证到不同应用的服务端进行认证，实现统一认证和单点登录。 • 支持外部认证源，例如，LDAP、微信、钉钉等认证源。 • 提供多因素认证，支持主流的认证方式，例如，账号/密码、 账号/SM2加密密码、短信验证码、OTP码、声纹、指纹、面部人脸识别、证书认证等。
集中授权（Authorization）	集中管理应用系统的业务角色和功能资源，例如菜单、按钮、后台使用资源等，从单个账户、组织单位、组等不同维度与角色进行绑定，同时将角色与权限范围内的功能资源进行绑定，达到从不同粒度集中分配权限的目的，防止越权操作。
应用管理（Application）	集中管理企业私有云和公共云应用、移动应用、IoT设备的访问权限和账户体系。
透明审计（Audit）	通过审计报告追溯用户的访问行为，了解公司数字资产的使用效率。

9.产品优势

云盾IDaaS向您提供一个涵盖5A、多级授权等功能/服务的综合解决方案，本文介绍了其功能优势。

- 兼容业界常用的SaaS服务，只需设置开通即可，无需过多配置即能实现对接。
- IDaaS以SaaS方式提供服务，无需您自己运维，降低您的运维成本。
- 客户可根据实际使用量，购买或升级到适合的IDaaS规格，避免不必要的浪费
- 集中管理权限，避免信息泄露。当一名员工离职后，企业管理员可以快速取消该员工账户的所有应用权限。

10.应用场景

本文介绍云盾IDaaS的应用场景。

云盾IDaaS适用于以下场景：

- 使用IDaaS统一管理三方应用系统

  IDaaS本质上是一种“云连接器”，帮助您将公司及员工使用的大量软件应用整合在一起，以便让员工更便捷地使用统一、安全的账号，登录他们工作中需要使用的各种网络服务，包括供应商、承包商、合作伙伴和客户所使用的网络服务。

- 使用IDaaS整合及开发公司内部办公系统（简称OA系统）

  IDaaS提供一个完整的账号、认证、授权系统，您可以使用IDaaS完成以下任务：

  - 为新入职员工开通账号，分配应用访问权限；在员工转岗离职时变更管理权限。
  - 通过单点登录打通多个内部应用系统（这些系统原本使用不同的账号体系），实现员工登录某一系统后，即可免登录访问其他系统。
  - 开发新的应用系统。

- 使用IDaaS开发您提供给客户的业务系统

  IDaaS可以帮助您提供用户池的功能。您可以新创建一个用户池，然后在应用程序中通过IDaaS的API接口来调用新用户的注册、登录、注销等流程，以此您可以专注在业务系统流程本身，减少4A方面的工作。

11.客户服务矩阵

1. 介绍

阿里云公有云可以为大客户提供全方面的强力支持，以保障客户可以顺利、放心地开始使用云上的各类服务。保障的类型分为4部分：

- 阿里云 整体支持计划
- 阿里云产品通用服务协议
- 阿里云 IDaaS 产品 SLA
- 阿里云 IDaaS 专家保障服务

2. 支持类型

2.1 阿里云 IDaaS 产品保障服务

阿里云平台的专家保障服务包括了上云前 、上云中、上云后与云上优化多个阶段中的多个咨询点，包括咨询与设计、迁移与部署、运维与管理、优化与提升等主题，是为了企业客户整体性的解决方案。

类型	支持目录	免费版	标准版	专属版
服务可用	SLA	不保障。	99.9%	99.9%
	高可用性	不保障。	双节点高可用集群。	可定制高可用集群，可以在同一 region 下支持多节点多可用区部署，保障高可用性。
	部署环境	共享集群。	共享集群。	独享集群，不与其他客户共享实例。独享计算资源、独享数据库实例、独享缓存。
	测试联调环境	无。	无。	包含单独一套基本的测试联调环境，满足快速功能验证和上线联调需求。半年后或上线 1 个月后释放。若要申请延期，请联系 IDaaS 团队。
	安全运维	不保障。	基础安全运维，免费处理安全补丁。	当系统出现安全漏洞，最优先处理安全补丁。
	事件处理	不保障。	关键事件：45分钟内响应 大影响事件：2小时内响应 中影响事件：8小时内响应 小影响事件：1天内响应 事件咨询：3天内响应	关键事件：15分钟内响应 大影响事件：40分钟内响应 中影响事件：4小时内响应 小影响事件：8小时内响应 事件咨询：1天内响应

	关键事件护航	不支持。	不支持。	支持 7*24 小时的关键事件护航服务，确保 IDaaS 平稳支持关键活动。需要和 IDaaS 团队沟通事件情况、周期和对应费用，如双11服务保障等。
帮助咨询	帮助文档	访问 IDaaS帮助文档	访问 IDaaS帮助文档	访问 IDaaS帮助文档，支持沟通答疑。
	咨询支持	工单	工单 24 小时内反馈。	工单 24 小时内反馈。5x8 小时即时售后支持：电话、工单，专属服务群支持。
	对接工作支持（SSO，数据同步等）	不支持。	工单支持。支持购买专家服务直接与 IDaaS 团队取得支持。	包含人工对接支持服务，包含问题排查和必要的远程协助，确保对接使用顺利。
	专属技术服务经理	无。	无。	专属技术服务经理沟通最佳方案，输出最佳实践。
定制能力	定制化、个性化功能	不支持。	不支持。	支持为客户单独定制解决方案，支持产品能力定制。
	性能专属优化	不支持	不支持。	支持针对场景方案的性能调优，支持服务器弹性扩容。

下面给出事件的基本定义和示例

- **关键事件**：系统高频操作行为（例如登录），在持续一段时间内（5分钟）内，至少有 50% 的请求失败，且业务影响范围极大（例如导致数万用户抢票失败）
- **大影响事件**：系统高频操作行为（例如登录），在持续一段时间内（15分钟）内，至少有 20% 的请求失败，且业务影响范围大（例如数百员工无法访问系统）
- **中影响事件**：系统高频/关键操作行为（例如同步账户），在持续一段时间内（15分钟）内，至少有 20% 的请求失败，且业务影响明显（可能导致需要管理员手动进行频繁操作才能消泯影响）
- **小影响事件**：系统一般操作行为（例如新用户授权授权），在持续一段时间内（1小时）内连续失败，且业务影响可控较小
- **事件咨询**：针对可能发生的事件的咨询和沟通

2.1.1 对接支持工作

由于作为身份权限管理核心，牵扯到应用按照单点登录、身份同步等多种专业协议的集成和对接，IDaaS 为企业提供了以人天为单位的专家服务，在提供充分文档，鼓励客户自主实现的情况下，专家服务可以有效加速对接进度，消除客户的隐忧。服务内容包含但不限于：

- AD/LDAP 对接支持服务
- 跨云身份同步和统一认证支持服务

- 跨内外网身份同步和统一认证支持服务
- 标准协议应用对接单点登录支持服务
- 定制化应用对接单点登录支持服务
- 身份数据源对接身份同步支持服务
- 特殊认证协议咨询支持服务
- 权限统一管理咨询支持服务
- 技术专家现场支持服务

2.2 阿里云支持计划体系 TAM Technical Account Manager

阿里云支持计划体系是阿里云客户获取阿里云技术专家支持的通道。阿里云配备经验丰富的技术支持工程师，服务内容涵盖阿里云技术、产品、解决方案及架构，支持方式包括工单、专属企业群、电话等，全年全天候为客户提供支持。阿里云客户支持体系适合不同规模和技术能力的客户，帮助客户基于阿里云提供的产品和功能进行产品使用、方案设计、应用开发及数据管理等。阿里云提供全面但灵活可选的客户支持内容，客户可以根据实际需要有选择地采纳不同级别的阿里云客户支持计划。

支持计划体系不特指 IDaaS 产品，其支持范围囊括了所有云上产品服务。是综合性、全方面的支持保障体系。

支持计划体系具体包含的内容请参考支持计划，报价请参考支持计划计费标准。

注：IDaaS 当前还没有和 TAM 体系集成/赋能，TAM 自动包含的支持内容应该还不包括 IDaaS。这里仅为了说明阿里云有 TAM 体系去支持大客户。如果有 IDaaS 问题，TAM 肯定解决不了，还是要咱们自行解决。

2.3 阿里云产品通用服务协议

阿里云通用服务协议适用于所有产品，主要对阿里云产品服务，义务，知识产权，保密条款等内容进行介绍，具体内容请查看阿里云产品服务协议（通用）。

2.4 阿里云 IDaaS SLA 应用服务协议

阿里云 IDaaS公共云为所有客户统一提供高水准的 SLA 服务保障，为账号的认证、权限管理、账号生命周期管理等关键操作提供了99.9% 可用性保障。

详情请参考应用身份服务等级协议。

12.产品相关FAQ

IDaaS 是否支持自定义域名访问

可以支持。

IDaaS 是否支持私网访问

IDaaS 目前不支持私网访问，通过公网访问。

是否需要配置短信和邮件网关

IDaaS默认配置了短信和邮件网关，可以直接使用，默认短信限制数量。

如果您需要自定义短信和邮件的模板，或者使用短信量比较大，可以在安全设置中配置自己的短信和邮件网关，并自定义短信和邮件的模板内容。

发送邮件进行测试，提示“发送失败，请检查配置”

a）请检查配置参数是否正确，如账户和密码是否正确，选择的安全类型是否正确。

b）请确认邮件网关白名单中是否添加了IDaaS出口的IP。

IDaaS是否可以阿里云私网访问

目前不支持私网访问，IDaaS提供公网访问地址。

如果您有其他问题和需求，欢迎钉钉搜索“33328593”联系我们。

13.和云服务的关系