ALIBABA CLOUD

阿里云

应用身份服务
CIAM 进阶指南

文档版本：20220623

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}`

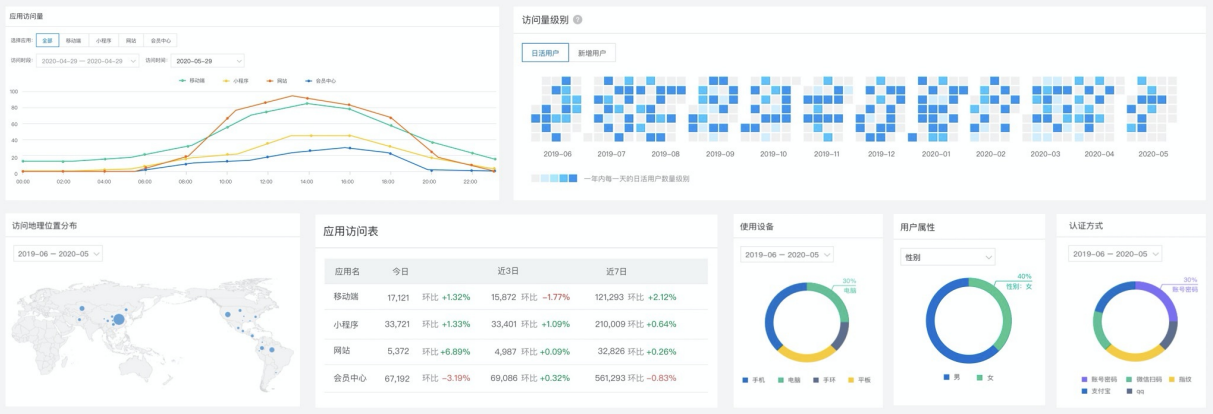
目录

1.统计与分析

统计与分析是 CIAM 的一个核心价值体现模块。当阿里云 IDaaS 完成了访客、消费者、会员的身份、权限统一管理后，所有的认证请求流量将通过 IDaaS 完成对应流程。在这一环节，我们可以将所有原始访问数据进行基本的分解和分析，并以报表和告警的方式来展示趋势或告知异常。

阿里云 IDaaS CIAM 为客户提供了三种类型的报表，包括用户访问数据分析报表组、应用访问数据分析报表组、用户画像分析报表组。通过这些报表，可以帮助企业的业务人员和管理人员理解当前身份模块的服务情况，并理解客户的使用习惯。

在积累了一定数据量后，阿里云 IDaaS 可以为专属客户提供由我们自研的高级安全模块：UEBA 用户实体行为分析。UEBA 可以在一定数据基础上，为每个客户进行特征定制，并为每位用户进行画像，以此来判断身份是否有效和安全，是一个兼容安全和便捷的最佳方案。



阿里云同样有对应的数据运营中台产品，已经与阿里云 IDaaS 完成对接集成，整体方案可以完成身份层面的整个闭环。详情请咨询阿里云 IDaaS 产品团队。

2.访问权限控制

访问控制和权限控制是任何 IAM 系统、乃至任何信息建设的核心咽喉，其掌控了不同类型的用户、管理员、财务审计等不同角色的定义，以及所有用户对任何内部、外部服务的访问权限。

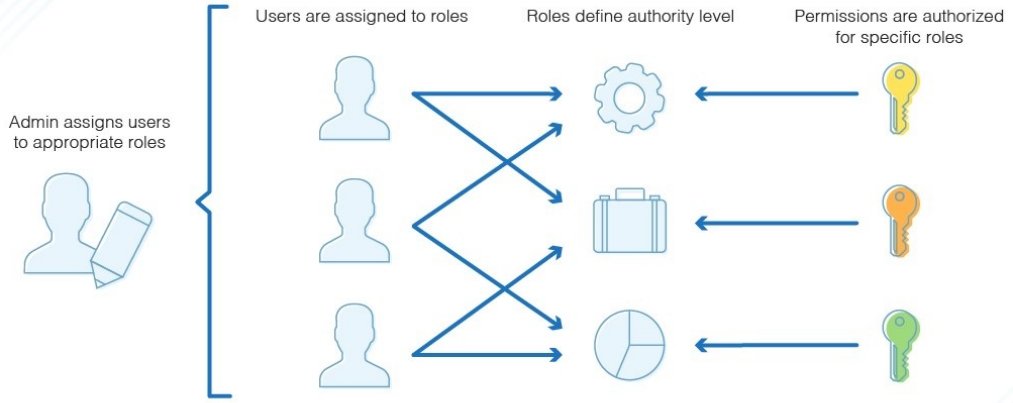
除了授权关系的管理外，权限管理同时包含了对权限变化的跟踪能力。在日常的商业活动中，员工可能会访问、修改或删除数据。若操作符合流程且遵循授权原则，该操作明显是合理合法的，但如果管理不当，则很容易出现权限过大、权限滥用的情况。权限管理系统的使用需要遵循权限最小化原则，同时不过度损害生产效率、不造成疑惑困扰，这些限制对权限管理系统的复杂度和灵活性都设置了非常高的起始基准。

一个用户，可能只能访问应用 A 但不能访问小程序 B。一位电话客服，可能只能对账户进行查看和有限的编辑操作，例如修改手机号、重置密码、解锁等，但不能创建或删除账号。一位区域管理员，可能只能针对华北地区的注册账号进行管理，而对其他地域的账号不可见。

每一个账号的职能、状态变化，都需要通过人工或流水线自动的方式，即时反馈在他所拥有的权限中，才能避免权限和用户级别、状态的错位。

有鉴于完善灵活的权限系统的复杂性，企业普遍希望将权限管理交由成熟的产品服务、有经验的团队来支撑。

阿里云 IDaaS 提供了完善的权限管理方式，IDaaS 将多种授权模式、授权关系构建成为一个非常灵活、强大的授权矩阵，支持按角色授权、按组授权，按属性授权等多种方式，支持多种授权方向，且可以为专属客户提供更加完善、复杂的授权场景。



权限控制是合规最关注的一个重点，阿里云 IDaaS 经过了等保三级、ISO 系列等权威测评，可以确保信息系统建设过程中的法律合规性。

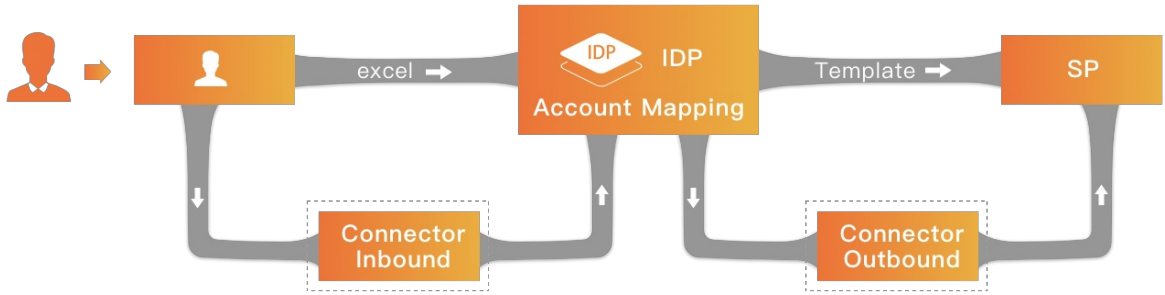
与此同时，在授权能力复杂化后，阿里云 IDaaS 有充分的经验为客户确保批量授权、高频鉴权的性能表现，取得易用性和灵活性之间的完美折中。详细方案请咨询 IDaaS 产品团队。

3.身份同步与分享

尽管我们希望企业的身份建设可以只有一个统一的身份核心，但往往处于兼容性问题、行业特殊考虑、企业组织方式等原因，无法或不应只维持单点身份可信（Single Source of Truth），而需要一个由多点构成的可信身份体系。身份数据往往还需要长期存在于其他系统中，且这些数据需要维持同步，以确保服务提供方的数据有效且可用。

作为身份平台，IDaaS 既可以通过各种常见方式将数据导入/同步进来，也可以将 IDaaS 的身份信息同步给常见的下游业务应用、数据画像产品、营销平台等，以便形成统一有效的身份体系。

同步机制复杂多样，根据不同的业务场景，同步的机制、限制、要求也会各有不同，需要明确具体需求后进行设计。我们推荐使用 SCIM 跨域身份管理协议来进行身份的同步，但也可以支持针对现有的协议、方式进行适配性兼容调整。



4. 日志审计

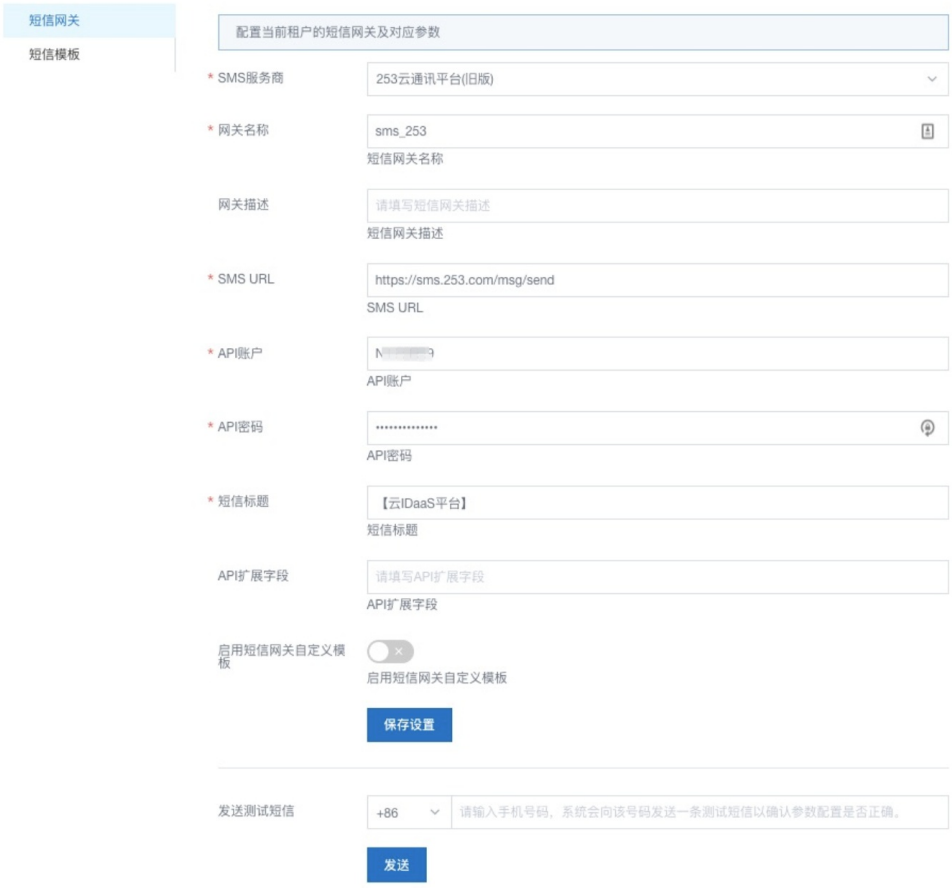
身份体系往往是企业信息化建设的最基本构件之一，在这个组件中发生的事情，轻则影响到调用服务的状态或表现，重则对企业服务可用和品牌都会造成严重打击。

阿里云 IDaaS CIAM 记录了用户侧和管理员侧的关键操作，可以做到事件发生前、中、后的全方面溯源，做到操作有迹可循。

5.配置使用短信网关

在身份管理的过程中，短信登录、短信二次认证、短信找回密码等功能都是常见能力，IDaaS 内置了发送短信的能力，但短信仅限于测试场景使用，且使用限额较低。在生产环境中，客户需要切换到自己的短信网关，或购买阿里云通信短信包后在 IDaaS 界面上配置使用。IDaaS 的产品使用费用不包含短信费用。

针对拥有定制化短信网关、自研短信网关或使用其他短信服务商的场景，阿里云 IDaaS 专属版也可以为大客户进行短信网关适配集成。



6.开发对接

使用阿里云 IDaaS CIAM 意味着将应用的认证逻辑「托管」给 IDaaS，无论是单端登录、注册、登录还是找回密码、身份安全管理等操作，全部交由 IDaaS 的接口或界面进行处理。这个托管流程和我们日常体验到的微信扫码登录有一定类似，但远不局限于此。

阿里云 IDaaS CIAM 是一个功能非常开放的平台。我们提供一整套完整的标准接口，为集成方提供用户自服务和管理功能。

我们提供了数十个接口为移动端、小程序、网站、广告落地页、抖音推广页等对客服务终端的身份安全验证保驾护航，并可以根据场景提供上百个接口，赋能企业的管理控制台，集中一点融合所有工作，并为高级安全能力，例如扫码、OTP 生成、国密算法安全键盘、id_token 验签等复杂功能或插件进行封装，统一提供各端的 SDK 集成。

如有需求进行对接，或希望查看详细的接口文档，请咨询 IDaaS 产品团队获取文档。