组织成员账号

产品介绍

文档版本 03

发布日期 2024-03-29

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目 录

1 图解 OrgID

2 什么是 OrgID

组织成员账号OrgID是面向企业提供组织管理、企业成员账号管理以及SaaS应用授权管理能力的云服务。OrgID将Huawei ID账号体系延伸到企业用户，统一华为云面向生态SaaS服务的组织、账号，面向生态伙伴推出SaaS服务账号集成规范。

为什么选择 OrgID

OrgID通过将Huawei ID扩展到企业组织内部应用领域，解决：

- 企业应用账号统一：企业可以选择使用Huawei ID作为企业SaaS服务的账号，并与企业内部账号关联。
- 账号绑定统一：与企业使用的IDaaS集成，企业用户可以选择使用Huawei ID或企业内部账号登录。
- 单点登录：企业用户一次登录实现轻应用间或SaaS服务间统一登录。
- 企业的统一管理：支持企业管理员对企业的部门、部门用户、账号、应用、应用认证源进行统一管理。
- 企业用户登录成功后，可以免登录打开任意企业内的应用，包括移动端，PC端。
- 通过统一账号来实现企业多维度运营分析：包括租户维度、用户维度、应用维度。

产品功能

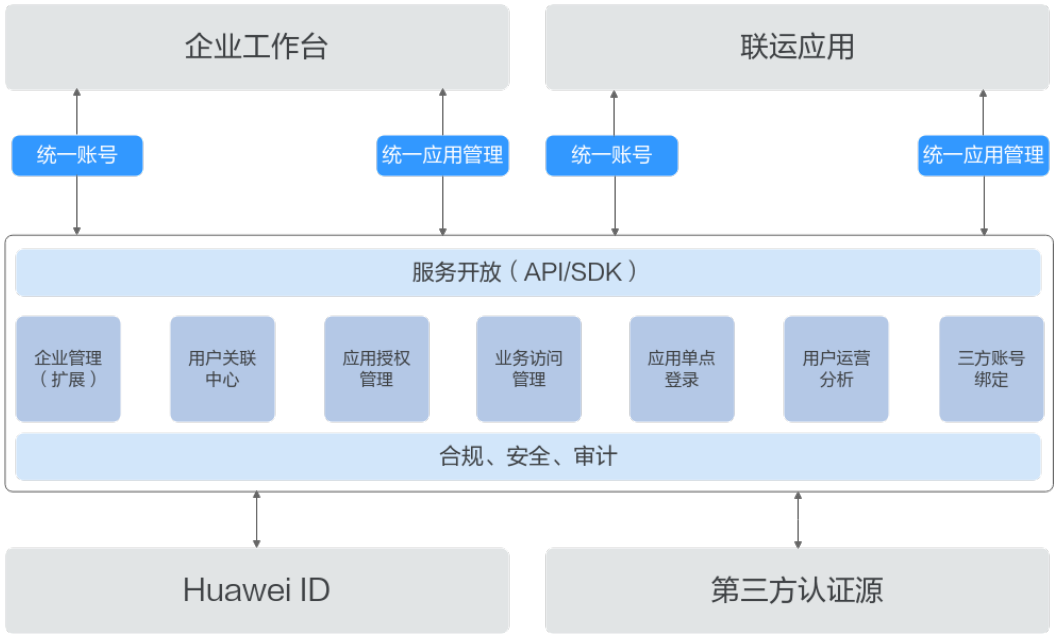
- 账号登录：提供组织成员（个人华为账号、管理式华为账号、第三方认证源账号）统一登录界面，实现企业内账号在华为云、业务应用的统一。
- 组织管理：通过个人华为账号或者管理式华为账号管理组织，包括组织部门管理、组织成员管理、组织信息管理，为企业内应用提供组织、部门、成员的统一管理。
- 应用注册：提供多种协议的应用注册管理，包括CAS、OAuth、OIDC、SAML。
- 用户关联中心：Huawei ID和第三方认证源的账号会关联生成用户标识，统一管理在OrgID的用户中心，通过用户中心控制组织下应用的访问。
- 应用授权管理：管理员授权用户可以访问的应用，包括自有应用和云商店联运KIT的SaaS应用。
- 业务访问控制：管理应用的访问策略，包括用户、设备、区域和认证源等。
- 应用单点登录：提供基于OrgID登录后应用间的免登录能力，提供基于App内部应用的免登录能力，提供其他应用的免登录能力。

- 用户运营分析：提供成员行业分析，应用使用分析。
- 三方账号绑定：支持钉钉、企业微信、WeLink等外部认证源的账号登录。

产品架构

OrgID产品架构请参考**图2-1**。

图 2-1 OrgID 产品架构



访问方式

- 应用注册协议

  SaaS应用接入OrgID云服务，需要遵从联运KIT规范接入改造，主要是对接统一账号，详细请见**联营SaaS接入流程介绍**。
- 控制台方式

  如果用户已注册公有云，可直接登录管理控制台，从主页选择“组织成员账号OrgID”。如果未注册，请参见**注册华为云并实名认证**。
- 成员访问

  组织成员访问，通过**OrgID**访问。

3 产品优势

OrgID优势包括终端云积累的用户、华为云高质量的服务体验和政企市场的生态伙伴能力，利用行业aPaaS（基地模式）推广，协同开天aPaaS，来解决企业用户注册、登录体验和企业内应用账号不统一的痛点问题。

1. 基于终端云庞大的Huawei ID的基础，使用Huawei ID认证解决企业用户认证及注册体验的问题。
2. 解决企业存在多种认证源，如企业社交认证源、联邦认证源等。
3. 内部面向企业的云服务预集成OrgID，如企业工作台。实现Huawei ID与华为云账号的打通，便于企业与华为云市场的集成，实现企业内应用订购。

4 应用场景

应用场景一：个人华为账号登录 SaaS 应用

OrgID系统提供个人华为账号登录SaaS应用的功能，管理员邀请个人华为账号加入组织并授权访问某个应用后，个人华为账号就可以访问这个应用。

- 通过邀请将个人华为账号加入到组织内，并授权用户访问应用。
- 提供基于华为账号的统一登录、统一注册。
- 提供基于组织的成员管理（华为账号），并实现应用统一授权。

应用场景二：管理式华为账号登录 SaaS 应用

OrgID系统提供管理式华为账号登录SaaS应用的功能，管理员通过创建成员的方式为组织添加用户，用户被授权后，即可访问该应用。

- 管理员可为组织创建只归属于该组织的用户。
- 授权组织下用户访问SaaS应用。
- 提供统一登录框架支持个人华为账号和管理式华为账号登录。

应用场景三：SaaS 应用三方认证能力

OrgID系统提供SaaS应用三方认证的能力，管理员通过认证源配置，可以实现对应用认证源的管理，三方认证源的用户即可登录访问应用。

- 提供多种认证源管理能力：WeLink、OAuth、CAS、SMAL、OIDC、钉钉、企业微信。
- 提供应用与认证源绑定能力，实现三方认证源登录应用的功能。

应用场景四：用户中心多应用间的免登录

OrgID系统提供用户中心，用户登录用户中心后，可以看到所有已授权应用且免登录访问所有应用。

- 提供用户中心应用统一授权管理。
- 提供用户中心应用免登录功能。

5 计费说明

OrgID服务根据组织数、用户数来按需度量，当前免费。

6 安全

6.1 责任共担

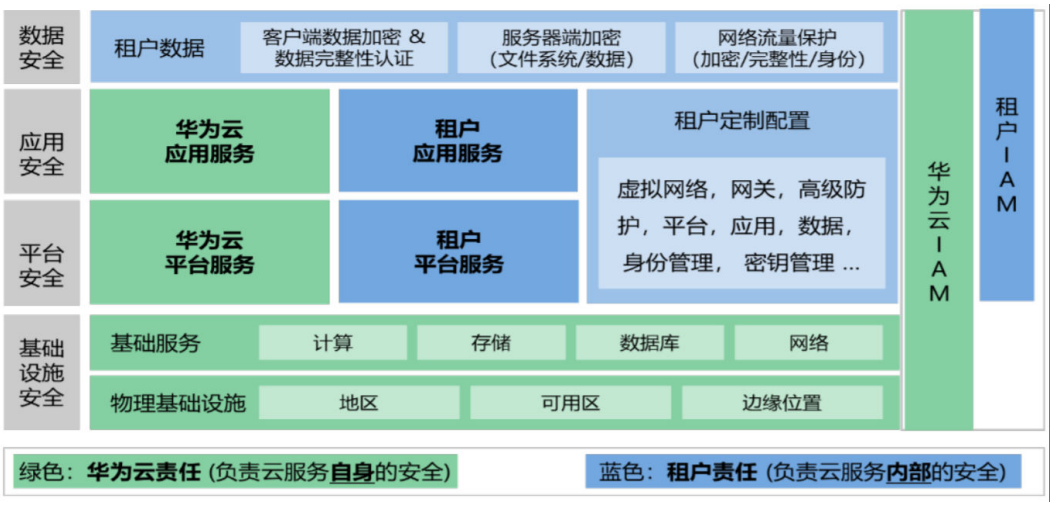
华为云秉承“将公司对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

安全性是华为云与您的共同责任，如**图6-1**所示。

- 华为云：负责云服务自身的安全，提供安全的云。华为云的安全责任在于保障其所提供的IaaS、PaaS和SaaS各类各项云服务自身的安全，涵盖华为云数据中心的物理环境设施和运行其上的基础服务、平台服务、应用服务等。这不仅包括华为云基础设施和各项云服务技术的安全功能和性能本身，也包括运维运营安全，以及更广义的安全合规遵从。
- 租户：负责云服务内部的安全，安全地使用云。 华为云租户的安全责任在于对使用的IaaS、PaaS和SaaS类各项云服务内部的安全以及对租户定制配置进行安全有效的管理，包括但不限于虚拟网络、虚拟主机和访客虚拟机的操作系统，虚拟防火墙、API网关和高级安全服务，各项云服务，租户数据，以及身份账号和密钥管理等方面的安全配置。

《华为云安全白皮书》详细介绍华为云安全性的构建思路与措施，包括云安全战略、责任共担模型、合规与隐私、安全组织与人员、基础设施安全、租户服务与租户安全、工程安全、运维运营安全、生态安全。

图 6-1 华为云安全责任共担模型



6.2 身份认证与访问控制

- 身份认证

  OrgID提供的身份认证可以分为控制台和云服务两个层面。

  - 控制台层面：OrgID与IAM打通，企业租户可以使用华为云用户名与密码登录，实现租户的认证与鉴权，未授权的不能访问。
  - 数据业务面：租户管理员添加成员后，成员可以直接登录OrgID数据业务面，使用Huawei ID账号认证，业务鉴权由OrgID提供。

- 访问控制
  - Token认证：通过Token认证通用请求。关于Token的详细介绍及获取方式，请参见**获取IAM用户Token（使用密码）**。
  - AK（Access Key ID）/SK（Secret Access Key）认证：通过AK/SK加密调用请求。推荐使用AK/SK认证，其安全性比Token认证要高。关于访问密钥的详细介绍及获取方式，请参见**访问密钥（AK/SK）**。

6.3 数据保护技术

通过数据保护手段，保障租户数据可靠性。

表 6-1 数据保护手段

数据保护手段	简要说明
传输加密（HTTPS）	外部接口支持HTTPS传输协议，保障数据传输的安全性。
服务端加密	涉及个人数据处理，包括：姓名、手机号码、邮箱等。这些数据在企业工作台内加密存储，避免个人数据的泄露。

数据保护手段	简要说明
数据容灾保护	租户内的数据，包括RDS（Relational Database Service）、DCS（Distributed Cache Service），启用了定时备份机制，定时全量备份（默认每天）与增量备份（默认5分钟）。 同时，RDS、DCS启用了双AZ（Availability Zone）容灾，当一个AZ异常后，可以无缝切换到另一个AZ上继续使用。

7 权限管理

OrgID系统提供权限管理，主要分为四种角色：超级管理员、组织管理员、部门管理员、普通用户。而OrgID云服务开通的相关权限受华为云IAM控制， IAM是华为云提供权限管理的基础服务，无需付费即可使用，您只需要为您账号中的资源进行付费。关于IAM的详细介绍，请参见**《IAM产品介绍》**。

表1列出了OrgID常用操作与系统角色的关系，您可以通过该表了解系统角色的操作权限。

表 7-1 常用操作与系统角色的关系

操作	超级管理员	组织管理员	部门管理员	普通用户
创建组织	√	×	×	×
查看组织	√	√	√	×
修改组织信息	√	√	×	×
申请配额	√	√	×	×
添加域名	√	√	×	×
验证域名	√	√	×	×
移交组织	√	×	×	×
解散组织	√	×	×	×
创建部门	√	√	√	×
编辑部门	√	√	√	×
删除部门	√	√	√	×
查看部门	√	√	√	×
创建成员	√	√	√	×
邀请成员	√	√	√	×
批量导入成员	√	√	√	×

操作	超级管理员	组织管理员	部门管理员	普通用户
重置成员密码	√	√	√	×
冻结、解冻成员	√	√	√	×
移除成员	√	√	√	×
创建用户组	√	√	×	×
编辑用户组	√	√	×	×
删除用户组	√	√	×	×
查看三方认证用户	√	√	×	×
创建应用	√	√	√	×
配置应用	√	√	√	×
删除应用	√	√	√	×
查看应用	√	√	√	×
新增认证源	√	√	×	×
更新认证源	√	√	×	×
删除认证源	√	√	×	×
查看认证源	√	√	×	×
添加区域范围	√	√	×	×
编辑区域范围	√	√	×	×
删除区域范围	√	√	×	×
查看区域范围	√	√	×	×
查看登录登出日志	√	√	√（只能查看自己的登录登出日志）	√（只能查看自己的登录登出日志）
查看管理操作日志	√	√	×	×
查看数据报表	√	√	×	×
导出数据报表	√	√	×	×
修改审批状态	√	√	×	×
查看角色	√	√	×	×
创建角色	√	√	×	×
添加角色成员	√	√	×	×

操作	超级管理员	组织管理员	部门管理员	普通用户
添加用户属性配置	√	√	×	×
修改用户属性配置	√	√	×	×

8 约束与限制

OrgID系统存在如下约束：

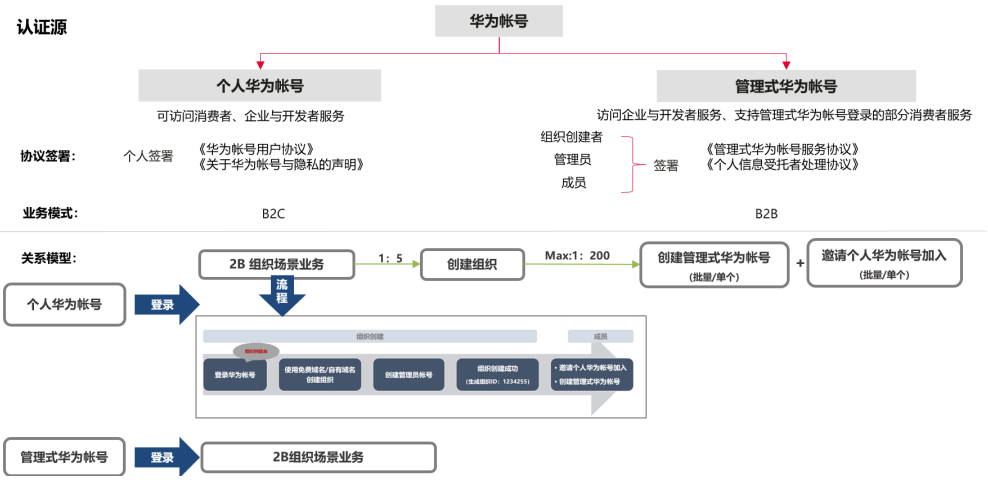
- OrgID默认认证源是华为账号，其账号分为个人账号和管理式账号。管理式账号由管理员创建，只能归属于本组织，登录时只能使用账号名登录，不能使用手机号或者邮箱地址登录。
- 华为账号最多可以创建5个组织，可以申请组织配额，每次申请增加一个组织配额。
- 每个组织支持管理3个域名。
- 单个组织默认可以有200个成员，可以**申请组织成员配额**，每次申请增加100个成员配额，最大成员数不超过5000。
- 部门最大层级不超过5级，一个组织最多可以有999个部门。
- OrgID当前只支持公有云，不支持HCS，伙伴云。
- 负责业务应用系统的统一认证，但应用的会话（与客户端的会话Session保持）不在OrgID管理范围。

9 基本概念

账号分类

- 个人华为账号：是由个人在华为集团账号系统申请获得，包括使用终端设备、华为云渠道、消费者应用等获取。该类账号归属于个人，可以通过邀请方式加入组织，也可以自己开通OrgID并创建组织。
- 管理式华为账号：是由组织的管理员创建生成，该类账号只归属于本组织所有，不可以加入其他组织。

图 9-1 华为账号



三方认证源

三方认证源是指登录认证由第三方认证源提供，鉴权认证通过后，用户将跳转至应用系统，继续后续业务操作。

Huawei ID

Huawei ID是外部用户使用华为所有产品和服务的统一身份标识(不包括华为IT账号)，外部用户包括企业客户、伙伴、供应商、消费者和华为云客户等。