应用身份管理服务

产品介绍

文档版本 01

发布日期 2024-09-24

华为云计算技术有限公司

版权所有 © 华为云计算技术有限公司 2024。 保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

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。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 图解应用身份管理服务.....1
2 什么是应用身份管理服务.....2
3 基本概念.....5
4 产品规格差异.....7
5 权限管理.....9

 版权所有 © 华为云计算技术有限公司

1 图解应用身份管理服务

版权所有 © 华为云计算技术有限公司

2 什么是应用身份管理服务

应用身份管理服务（OneAccess）具备集中式的身份管理、认证和授权能力，保证企业用户根据权限访问受信任的云端和本地应用系统，并对异常访问行为进行有效防范。

图 2-1 什么是应用身份管理服务

产品功能

- **统一身份管理**

  提供统一的用户、组织机构、用户组、应用、账号和凭证管理及设置，同时提供数据同步、密码策略及用户自服务，方便企业和管理员对用户身份进行全生命周期管理。

- **统一权限管理**

  提供对应用内部权限、平台权限的管理和配置，使用多种授权方式结合权限规则的灵活策略来满足大部分的权限需求。

- **统一认证管理**

  提供集中统一的认证管理功能，包括：内置多种认证方式、认证策略灵活配置、访问控制、单点登录/登出等，帮助企业实现可信身份认证，提升信息安全。

- **智能访问控制**

版权所有 © 华为云计算技术有限公司

提供自适应的访问控制能力，基于访问上下文信息（访问时间/地点/设备等）和用户行为数据，使用设定的规则实时判断用户访问过程中的风险。如果发现风险，实时调度认证方式加强校验。

- **流程审计**

  提供认证日志、访问日志、操作日志、同步日志、系统日志等记录，将用户日志、管理员日志分别进行集中管理，可以通过内置报表引擎进行可视化展示，供企业管理员进行查询、跟踪和审计。

产品优势

- **提升企业管理效率**
  - 集中存储全生命周期的用户账号和数据信息，实现用户信息集中存储、用户各应用账号的集中管理。
  - 结合用户管理的不同场景，如入职、调岗、返聘、离职等，提供自动化创建、权限变更、账号禁用、账号删除等功能，实现用户身份全生命周期管理。
  - 支持客户本地身份中心、个人社交认证身份源、企业社交认证身份源的集成，实现组织、身份数据的一键同步，在保护存量数据资产的同时提供灵活的用户登录体验。
- **提升用户登录体验**
  - 支持用户“一站式”访问所有可信应用，无需维护多套账号、多个URL、多个入口，避免多次登录。
  - 与1000+第三方应用标准化预集成，用户一次登录，免密访问所有可信应用。
  - 支持CAS、SAML2.0、OAuth2.0、OIDC多种协议的认证集成，企业管理员轻松对接多种数据源。
  - 提供多种认证方式，如静态密码、短信验证码、动态口令、二维码等，企业可以自定义选择多种认证方式的组合。
- **保障资源信息安全**
  - 基于事先预设好的访问控制规则，自动分析用户接入时间、接入地点、接入设备等环境风险，对用户的访问行为进行严格判断。
  - 通过设计风险阻断机制，自动触发预设的条件访问控制策略，实时告知管理员及用户存在的潜在风险，同时主动阻断风险。
  - 用户可自定义条件访问控制策略，根据企业需求灵活组合时间、地点、设备等环境要素，对风险行为设置拦截、二次认证等多种应对措施。
- **降低应用运维成本**
  - 与1000+应用预集成，快速开通，明显减少应用系统重复建设投入，同时可降低信息安全事故的间接损失
  - 该服务支持多种规格，按需购买，减少资源浪费。

访问方式

您可以通过以下两种方式访问OneAccess。

- 管理控制台

  您可以通过基于浏览器的可视化界面，即控制台访问OneAccess。
- REST API

 版权所有 © 华为云计算技术有限公司

您可以使用OneAccess提供的REST API接口以编程方式访问OneAccess。

 版权所有 © 华为云计算技术有限公司

3 基本概念

企业管理员

企业管理员包括主账号或拥有OneAccess管理权限的用户。企业管理员在OneAccess管理门户负责用户（组）、组织、应用及API等实体的管理。

超级管理员

超级管理员是主账号在OneAccess管理门户创建的管理员，拥有对企业所有组织结构、用户、应用及管理门户菜单的管理权限。超级管理员属于超级管理组，超级管理组拥有OneAccess管理门户的最高权限。

分级管理员

分级管理员由主账号或超级管理员在OneAccess管理门户创建，拥有对企业部分组织结构、用户、应用及管理门户菜单的管理权限。分级管理员不属于超级管理组，可以属于超级管理组下的分级管理组，也可以不属于任何管理组。

系统管理员

系统管理员由华为云主账号在统一身份认证服务中创建，拥有对企业所有组织结构、用户、应用及除创建管理员以外其他管理门户菜单的管理权限。系统管理员不属于任何管理组。

普通用户

普通用户是企业应用使用者，包含企业员工、合作伙伴、客户等。普通用户可以登录OneAccess用户门户访问和操作应用。

应用

应用是指在OneAccess上进行统一管理和授权的第三方系统。OneAccess的应用根据是否需要用户自集成分为预集成应用和自建应用。

- 预集成应用：OneAccess根据应用的开发接口或者相应协议提前进行预集成的应用，企业只需购买并完成基础配置即可使用。
- 自建应用：企业的自研应用或者不在预集成应用列表中的软件类或商业应用，企业还需要选择应用支持的认证协议、同步方式创建应用实例，进行应用集成开发。

 版权所有 © 华为云计算技术有限公司

身份源

OneAccess支持企业从多种系统导入用户和机构信息，实现将多个系统汇聚为一个完整的用户目录，便于在OneAccess中统一管理，这些系统就称为身份源。目前OneAccess支持的身份源有企业微信、钉钉、AD、LDAP、飞书、薪人薪事、北森HR、名才HR、SAP SuccessFactors和泛微OA_E9等。

认证源

OneAccess支持用户使用第三方系统的账号、密码等进行登录。企业可以根据需要添加并使用认证源，如微信、微博等个人社交认证，钉钉、企业微信等企业社交认证，也可以使用支持CAS、SAML2.0、OAuth2.0、OIDC协议的本地身份认证系统进行认证。

单点登录

单点登录（Single Sign-On，简称SSO）是指用户在OneAccess用户门户登录后，选择需要访问的可信应用，无需再次验证就可以使用应用。如：管理员在OneAccess管理门户添加华为云并授权给用户后，用户登录至OneAccess用户门户选择华为云，无需输入账号和密码即可跳转访问华为云。

外部应用接口

外部应用接口（Open API Platform，简称OAP）是OneAccess开放给第三方开发者使用的API接口，第三方开发者可以通过这些接口实现功能的定制，如：组织管理、用户管理、应用管理等。

版权所有 © 华为云计算技术有限公司

4 产品规格差异

应用身份管理服务OneAccess提供了基础版、专业版和企业版三种规格。各规格支持的功能如表4-1。

- **基础版**提供部分功能，暂不支持条件访问控制等专业功能，支持的用户数为100或500，适用于小型企业，支持包年/包月计费方式。
- **专业版**提供更多访问控制、权限管理、扩容等专业功能，支持按需调整用户数量，支持用户数量为200或1,000~10,000之间，能够满足政府、中大型企业对云上业务高性价比、高可靠性的需求。支持包年/包月计费方式。
- **企业版**支持资源独立部署，提供更多访问控制、权限管理等功能，支持的最大用户数量为40,000，能够满足大型企业和政府的业务需求。支持包年/包月计费方式。

表 4-1 产品规格功能说明

支持内容	基础版	专业版	企业版
增加用户容量	支持	支持	不支持
条件访问控制	不支持	支持	支持
自定义API访问控制	不支持	支持	支持
细粒度权限	不支持	支持	支持
身份同步	不支持	支持	支持
云桥Agent	不支持	支持	支持
组织与用户	支持	支持	支持
自定义用户属性	支持	支持	支持
认证集成（OAuth2、SAML、OIDC、CAS、插件代填、OPEN_API）	不支持插件代填和OPEN_API。	支持	支持

版权所有 © 华为云计算技术有限公司

支持内容	基础版	专业版	企业版
身份源（企业微信、钉钉、飞书、AD、LDAP、薪人薪事、北森HR、名才HR、SAP SuccessFactors、泛微OA_E9）	支持	支持	支持
应用授权（手动、自动）	支持	支持	支持
企业API（内置API、自定义API产品）	不支持自定义API产品。	支持	支持
认证源	支持认证源有：微信、微博、QQ、支付宝、钉钉、Welink、企业微信、云之家、飞书、泛微eteams、AD、LDAP。	支持的认证源有：微信、微博、qq、支付宝、钉钉、Welink、企业微信、云之家、飞书、泛微eteams、SAML、OIDC、OAuth、CAS、AD、LDAP 、Kerberos、FIDO2	支持的认证源有：微信、微博、qq、支付宝、钉钉、Welink、企业微信、云之家、飞书、泛微eteams、SAML、OIDC、OAuth、CAS、AD、LDAP 、Kerberos、FIDO2
区域范围	不支持	支持	支持
管理员权限	支持	支持	支持
密码策略	支持	支持	支持
审计	支持	支持	支持
企业信息	支持	支持	支持
短信网关	支持	支持	支持
邮件网关	支持	支持	支持
钉钉网关	支持	支持	支持
语音网关	支持	支持	支持
数据字典	支持	支持	支持
数据导入	支持	支持	支持
全局参数设置	支持	支持	支持
界面配置（内置模板、自定义）	支持	支持	支持
服务配置	支持	支持	支持

版权所有 © 华为云计算技术有限公司

5 权限管理

如果您需要对OneAccess管理门户上的应用及OneAccess的管理门户访问权限进行管理，如为企业中的员工设置OneAccess部分应用访问权限或管理门户部分功能的查看和编辑权限，可以在OneAccess上创建用户或管理员，并为其授予相应的权限，其操作请参考**管理员登录管理门户**~**用户登录用户门户并进入应用**。

如果您需要对华为云上购买的OneAccess实例进行编辑权限管理，如针对OneAccess为企业中的员工设置不同的权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制云服务资源的访问。IAM的权限管理是在华为云上进行的，主要针对OneAccess实例的编辑权限进行管理。

通过IAM，您可以在华为云账号中给员工创建IAM用户，并授权控制其对云服务资源的访问范围。例如对于负责企业信息管理的员工，您希望员工拥有查看OneAccess实例信息的权限，但是不希望员工拥有修改证书的权限，那么您可以使用IAM为其创建用户，通过授予仅能查看OneAccess实例信息，但是不允许修改证书的权限，控制用户对OneAccess资源的使用范围。

如果账号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用OneAccess服务的其它功能。

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**。

OneAccess 控制台权限

默认情况下，管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

OneAccess部署时不区分物理区域，为全局级服务。授权时，在全局级服务中设置权限，访问OneAccess时，不需要切换区域。

权限根据授权精细程度分为角色和策略。

- 角色：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于华为云各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。

 版权所有 © 华为云计算技术有限公司

- 策略：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。多数细粒度策略以API接口为粒度进行权限拆分，权限的最小粒度为API授权项（action），OneAccess支持的API授权项请参见**OneAccess授权项**。

如**表5-1**所示，包括了OneAccess控制台的所有系统权限。

表 5-1 OneAccess 控制台权限

系统角色/策略名称	描述	类别
Tenant Administrator	除统一身份认证服务外，拥有其他所有服务的管理员权限包括应用身份管理服务所有权限。	系统角色
Tenant Guest	除统一身份认证服务外，拥有其他所有服务的只读权限。拥有该权限的IAM用户仅能查看应用身份管理服务，不具备服务配置权限。	系统角色
IAM ReadOnlyAccess	统一身份认证服务的只读权限。	系统策略
OneAccess FullAccess	应用身份管理服务所有权限。	系统策略
OneAccess ReadOnlyAccess	应用身份管理服务只读权限，拥有该权限的用户仅能查看应用身份管理服务，不具备服务配置权限。	系统策略

说明

华为云账号和被授权的子账号、委托账号可以购买应用身份管理服务实例，子账户和委托账号需要实例授权后才能使用应用身份管理服务。

表5-2列出了OneAccess常用操作与系统权限的授权关系，您可以参照该表选择合适的系统权限。

表 5-2 常用操作与系统权限的关系

操作	Tenant Administrator	Tenant Guest	OneAccess FullAccess	OneAccess ReadOnlyAccess
查询产品实例列表	√	√	√	√
查询域名证书详情	√	√	√	√

版权所有 © 华为云计算技术有限公司

操作	Tenant Administrator	Tenant Guest	OneAccess FullAccess	OneAccess ReadOnlyAccess
订购实例	√ **说明** 子账户或委托账号需同时具有IAM ReadOnlyAccess权限。	×	√ **说明** 子账户或委托账号需同时具有IAM ReadOnlyAccess权限。	×
自定义域名	√	×	√	×
解绑自定义域名	√	×	√	×
修改域名证书	√	×	√	×
删除实例	√	×	√	×

OneAccess 授权项

策略包含系统策略和自定义策略，如果系统策略不满足授权要求，管理员可以创建自定义策略，并通过给用户组授予自定义策略来进行精细的访问控制。策略支持的操作与API相对应，授权项列表说明如下：

- 权限：允许或拒绝某项操作。
- 授权项：自定义策略中支持的Action，在自定义策略中的Action中写入授权项，可以实现授权项对应的权限功能。
- IAM项目(Project)/企业项目(Enterprise Project)：自定义策略的授权范围，包括IAM项目与企业项目。授权范围如果同时支持IAM项目和企业项目，表示此授权项对应的自定义策略，可以在IAM和企业管理两个服务中给用户组授权并生效。如果仅支持IAM项目，不支持企业项目，表示仅能在IAM中给用户组授权并生效，如果在企业管理中授权，则该自定义策略不生效。关于IAM项目与企业项目的区别，详情请参见：**IAM项目与企业项目的区别**。

权限	授权项	IAM项目 (Project)	企业项目 (Enterprise Project)
开通产品实例	oneaccess:instances:create	√	×
查询产品实例列表	oneaccess:instances:get	√	×
自定义域名	oneaccess:domains:create	√	×
解绑自定义域名	oneaccess:domains:delete	√	×
查询域名证书详情	oneaccess:certificates:get	√	×
修改域名证书	oneaccess:certificates:update	√	×

版权所有 © 华为云计算技术有限公司

权限	授权项	IAM项目 (Project)	企业项目 (Enterprise Project)
变更规格	oneaccess:instances:update	√	×
授权用户实例访问权限	oneaccess:permissions:grantRoleToUser	√	×
移除用户实例访问权限	oneaccess:permissions:revokeRoleFromUser	√	×
查询权限角色	oneaccess:permissions:listRoles	√	×
查询权授权用户的权限角色	oneaccess:permissions:listRolesForUser	√	×
查询实例的授权用户列表	oneaccess:permissions:listUsersOnInstance	√	×

版权所有 © 华为云计算技术有限公司