应用身份管理服务

快速入门

文档版本 01

发布日期 2024-12-26

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。

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

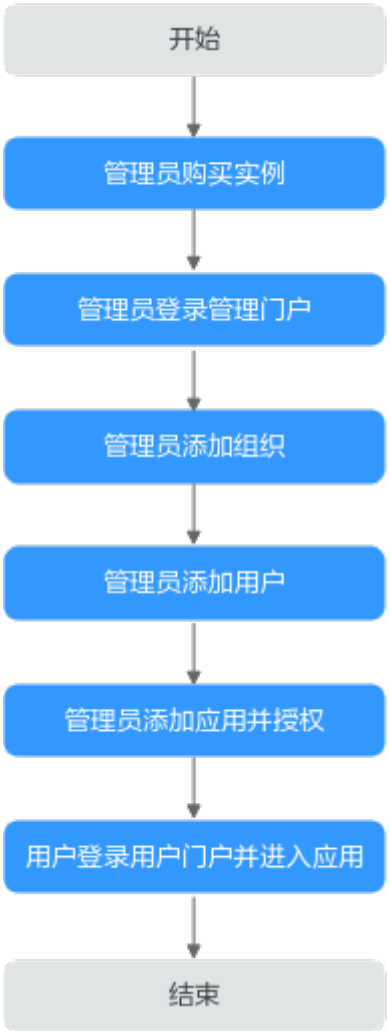
网址： https://www.huaweicloud.com/

目 录

1 普通用户登录用户门户并访问应用

图1-1为OneAccess基本的入门使用流程。本文旨在帮助您对OneAccess的入门操作有初步的认识，完成这些操作后，管理员可以在OneAccess管理门户对用户和应用进行详细配置和管理，用户可以在OneAccess用户门户单点登录访问已授权可信应用。

图 1-1 入门使用流程



1. 在使用应用身份管理服务前，管理员需要参考**购买实例**购买实例。
2. 管理员购买OneAccess实例后，参考**管理员登录管理门户**登录至OneAccess管理门户。
3. 参考**管理员添加组织**添加组织。
4. 管理员参考**管理员添加用户**在OneAccess管理门户添加用户。
5. OneAccess平台提供了1000+预集成应用，同时提供自建应用功能，参考**管理员添加应用并授权**添加应用并授权。
6. 登录OneAccess用户门户并直接进入应用，具体操作可参考**普通用户登录用户门户并进入应用**。

准备工作

1. 注册华为云并实名认证。

   如果您已有一个华为账户，请跳到下一个任务。如果您还没有华为账户，请参考以下步骤创建。

   a. 打开**华为云官网**，单击“注册”。

   b. 根据提示信息完成注册，详细操作请参见**如何注册华为云管理控制台的用户?** 。

   注册成功后，系统会自动跳转至您的个人信息界面。

   c. 参考**实名认证**完成个人或企业账号实名认证。

   说明

   仅在购买或使用位于中国大陆区域的资源时，需要实名认证。

2. 为账户充值。

   您需要确保账户有足够金额。

   - 关于OneAccess的价格，请参见购买页实际显示价格。
   - 关于充值，请参见**充值与还款**。

3. 为用户添加操作权限。

   用户在创建依赖资源和OneAccess前，需要具备相应的操作权限。具体权限请参考**权限管理**。

购买实例

步骤1 进入购买应用身份管理服务页面。

步骤2 在“购买应用身份管理服务”页面，配置实例参数。

1. 在“区域”下拉框中选择区域。
2. 在“规格选择”中选择实例规格，当前支持基础版、专业版和企业版三种，此处选择“基础版”。
3. 选择“用户数”，此处选择100。
4. 设置购买时长，默认勾选“自动续费”。
5. 设置实例数量，取值为1~100之间的整数，此处选择1。

步骤3 单击“下一步：确认配置”。

步骤4 勾选“我已阅读并同意《OneAccess服务声明》”，单击“立即购买”，开始发放实例，实例创建完成，会自动生成用户访问域名。

----结束

管理员登录管理门户

1. 登录华为云控制台。
2. 在服务列表中选择“管理与监管 > 应用身份管理服务 OneAccess”，进入应用身份管理服务控制台。
3. 单击待访问的OneAccess实例。
4. 单击要访问的“实例名称”，进入OneAccess实例管理门户。

如您没有访问“实例名称”的权限，需要通过IAM用户访问OneAccess管理门户，则需要给IAM用户授予访问OneAccess管理门户的权限，具体操作请参考**新增授权**。

管理员添加组织

组织用于对企业人员进行管理，一个公司或部门可对应一个组织，将其拥有的人员集中在该组织下。顶层组织作为根节点，可以在其下添加多个子组织与用户，同时，在子组织下可继续添加多层组织与用户。添加组织后便于管理员更高效的管理企业人员。

步骤1 管理员登录OneAccess管理门户。

步骤2 在导航栏中，选择“用户 > 组织与用户”，进入组织与用户页面。

步骤3 单击页面左下角的“  ”，弹出“添加组织”窗口。

步骤4 在“添加组织”弹窗中填写参数并单击“确定”，添加顶层组织。左侧组织导航中出现新添加的组织。

表 1-1 组织信息

组织信息	说明
组织类型	组织的类型，有部门、单位、公司、集团四种类型。
组织编码	组织的唯一标识，全局不可重复。
组织名称	组织的名称，同一层级的组织名称不允许重复。
显示顺序	组织在同层级组织中的显示顺序。

组织信息	说明
上级组织	创建组织的上级组织，创建顶层组织时则置空。

步骤5 单击“确定”，添加组织完成。

----结束

管理员添加用户

在OneAccess管理门户，可创建一人一组织，也可创建一人多组织的用户即一个用户可以属于多个组织。管理员在OneAccess管理门户添加用户，用户将拥有独立的OneAccess账号。

当创建的用户属于多组织时，如当用户属于组织A和B，且组织A有应用C的访问权限，组织B拥有应用D的访问权限，该用户同时拥有组织A和B的权限，则登录用户中心后，该用户便可以同时访问应用C和D。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“用户 > 组织与用户”进入组织与用户页面。

步骤3 在组织与用户页面，选择“用户”页签。

步骤4 单击“添加用户”，参考**表1-2**填写用户基本信息。

表 1-2 基本信息

基本信息属性	属性含义
用户名	可通过**修改用户属性**设置该属性是否为必填，缺省用户名时，系统会自动生成用户名。可在**修改用户属性**中设置该属性输入的字符及长度要求。新建用户绑定的用户名不可与其他用户重复。用户名不区分大小写。
组织	可选择添加的用户所属的组织。可选择一个组织，也可同时选择多个组织，默认先选择的组织为主组织。添加组织可参考**管理员添加组织**。 **说明** • 当先在左侧组织树选中组织，再单击“添加用户”时，则选中的组织默认为主组织。 • 用户最多只能拥有1个主组织和9个从组织。主从组织可以在用户名右侧单击，选择“调整组织”，在“调整组织”弹框进行调整。
姓名	可通过**修改用户属性**设置该属性是否为必填及设置该属性输入的字符长度要求。
手机号	可通过**修改用户属性**设置该属性是否为必填及设置该属性输入的字符长度要求。手机号是唯一的，不可同其他用户重复。
邮箱	可通过**修改用户属性**设置该属性是否为必填及该属性输入的字符长度要求。邮箱是唯一的，不可同其他用户重复。

基本信息属性	属性含义
国家或地区	选择用户所在国家或地区。可通过**修改用户属性**设置该属性是否为必填。
城市	输入用户所在城市。可通过**修改用户属性**设置该属性是否为必填及设置该属性输入的字符长度要求。

说明

- 用户可以使用此处设置的用户名、手机号或邮件地址任意一种方式登录用户门户。
- 当管理员管理用户密码时，可以通过此处绑定的邮件地址或手机号管理密码。
- 当用户忘记密码时，可以通过此处绑定的邮件地址或手机号自行重置密码。
- 建议设置“密码”，方便在未开启其他认证方式前，用户可以通过密码方式正常访问用户门户。

步骤5 单击 开启密码登录。当前密码登录有两种方式，此处选择“自定义”。

- 自定义，可自定义设置用户登录密码。
  - 勾选“首次登录时修改密码”时，则自定义设置的用户登录密码，在首次登录用户管理门户时，需要修改登录密码。
  - 不勾选“首次登录时修改密码”时，则自定义设置的用户登录密码，在首次登录用户管理门户时，不需要修改登录密码。
- 自动生成，系统根据密码初始化配置通知用户初始密码，用户需在有效期内完成登录。若还未开启初始化密码配置的，请参考**密码初始化设置**进行设置。

步骤6 单击“确定”，用户添加完成，用户列表中显示已添加的用户。

----结束

管理员添加应用并授权

管理员在OneAccess添加需要统一管理的应用。该操作步骤以添加SAML协议的应用为例，添加其他协议的应用请参考**集成企业应用**。

步骤1 管理员登录OneAccess管理门户。

步骤2 在导航栏中，选择“资源 > 应用”。

步骤3 单击预集成应用下的“新增预集成应用”。

步骤4 在新增预集成应用页面，搜索并选择需要添加的应用。

步骤5 在添加应用页面，编辑通用信息。

表 1-3 通用信息

参数	说明
应用LOGO	上传图片文件大小不超过50K。
应用名称	必填，支持自定义。

参数	说明
认证集成方式	应用的认证集成方式按照应用配置预集成，不可修改。
同步集成方式	应用的同步集成方式按照应用配置预集成，不可修改。

步骤6 单击“下一步”，在认证参数配置页面，导入预集成应用的元数据。

说明

- 认证参数配置可以采用导入和手动输入两种方式。为了避免输入错误，建议使用导入方式。
- 元数据需从企业应用处获取。

步骤7 配置完成后，单击“下一步”，应用添加完成。

步骤8 单击“进入应用”，进入应用信息页面。

步骤9 在应用信息页面，在“对象模型 ”区域，单击“应用机构”后的 ，在弹出框中单击“确定”打开应用机构配置。

步骤10 在应用信息页面，单击“授权管理 > 应用机构”后的“授权”，进入应用机构页面。

步骤11 单击“授权策略”，打开授权策略弹窗。

步骤12 单击 开启机构自动授权，并勾选自定义选择机构。

步骤13 选择需要授权的机构，依次单击“保存”和“执行新增”，应用机构新增成功。

步骤14 单击左侧导航的“授权管理 > 应用账号”，进入应用账号页面。

步骤15 单击“添加账号”。

步骤16 勾选**管理员添加用户**中添加的用户，授予该用户应用访问权限，单击“保存”，应用账号新增成功。

说明

为用户授权将自动为用户创建应用账号。

----结束

普通用户登录用户门户并进入应用

用户从管理员处获取用户访问域名，并登录OneAccess用户门户。

步骤1 用户从管理员处获取“用户访问域名”。

说明

“用户访问域名”由管理员在购买OneAccess实例时配置，在OneAccess管理控制台获取。如：example.huaweioneaccess.com。

步骤2 用户访问“用户访问域名”，进入用户门户登录页面。

步骤3 输入用户名和密码，单击“登录”，进入用户门户首页。

步骤4 单击**管理员添加应用并授权**中添加的应用，进入应用系统。

----结束

2 入门实践

当您购买了应用身份管理服务实例后，可根据业务需要使用OneAccess提供的一些实践操作。

实践		描述
集成身份源	集成AD身份源	本实践将为您介绍如何在OneAccess中配置AD身份源，通过身份源导入用户和组织信息，实现OneAccess实时同步身份源中用户和组织信息。
	集成LDAP身份源	本实践将为您介绍如何在OneAccess中配置LDAP身份源，通过身份源导入用户和组织信息，实现OneAccess实时同步身份源中用户和组织信息。
集成企业应用	使用OneAcceess用户门户登录华为云	华为云支持基于SAML、OIDC协议的单点登录，企业管理员在华为云和OneAccess进行配置后，普通用户登录OneAccess用户门户，即可免密进入华为云Console系统或者是某个具体的华为云应用。
	通过SAML协议单点登录至应用	本实践介绍在OneAccess中如何以SAML协议集成应用。
	通过OAuth2.0协议单点登录至应用	本实践介绍在OneAccess中如何以OAuth协议集成应用。
	通过OIDC协议单点登录至应用	本实践介绍在OneAccess中如何以OIDC协议集成应用。

实践		描述
	通过CAS协议单点登录至应用	本实践介绍在OneAccess中如何以CAS协议集成应用。
	以插件代填的方式集成应用	本实践介绍在OneAccess中如何以插件代填的方式集成应用。
同步企业数据	通过SCIM协议同步数据至Atlassian	本实践介绍在OneAccess中如何以SCIM协议同步用户至Atlassian的方法。
	通过LDAP协议同步数据	本实践介绍在OneAccess中如何以LDAP协议同步组织和用户数据至OpenLDAP的方法。
集成认证源	内置认证源	本实践为您介绍通过FIDO2认证源（人脸、指纹等生物认证）来登录OneAccess平台集成的应用系统。
	SAML认证登录	本实践为您介绍在OneAccess平台如何配置SAML认证源、如何配置配置SAML认证登录各应用系统。
	OIDC认证登录	本实践为您介绍在OneAccess平台如何配置OIDC认证源、如何配置OIDC认证登录各应用系统。
	CAS认证登录	本实践为您介绍在OneAccess平台如何配置CAS认证源、如何配置CAS认证登录各应用系统。
	OAuth认证登录	本实践为您介绍在OneAccess平台如何配置OAuth认证源、如何配置OAuth认证登录各应用系统。
	Kerberos认证登录	本实践为您介绍在OneAccess平台如何配置Kerberos认证源、如何配置Kerberos认证登录各应用系统。

实践		描述
	AD认证登录	本实践为您介绍在OneAccess平台如何配置AD认证源、如何配置AD认证登录各应用系统。
	LDAP认证登录	本实践为您介绍在OneAccess平台如何配置LDAP认证源、如何配置LDAP认证登录各应用系统。