组织成员账号

用户指南

文档版本 12

发布日期 2025-02-10

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

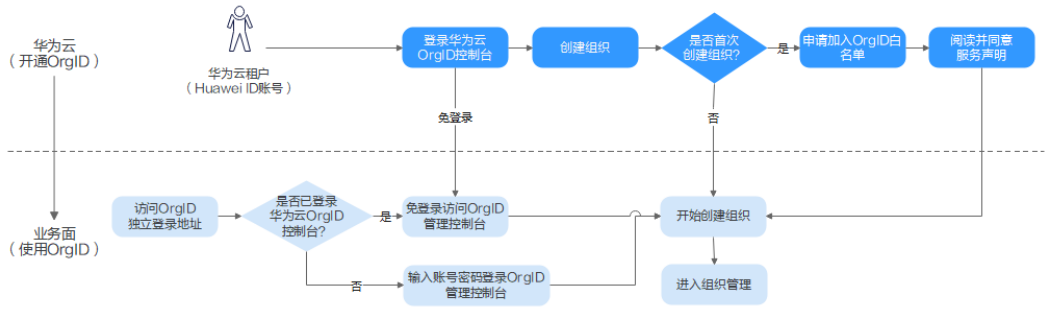
1 使用前必读

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通过将**Huawei ID**扩展到组织内部应用领域，实现对组织部门、用户、账号、应用、认证源的统一管理。

开通与使用流程

租户需要先在华为云开通OrgID服务，才能进一步登录并使用OrgID服务。OrgID的开通与使用流程如**图1-1**所示。

图 1-1 开通与使用流程



开通OrgID：

1. 登录华为云OrgID控制台：租户使用个人华为账号登录**华为云OrgID控制台**，如果没有个人华为账号请先注册**华为账号**并完成**实名认证**。
2. 创建组织：单击“创建组织”，系统会判断是否是首次创建组织。
   - 首次创建组织：需要申请加入OrgID白名单，加入白名单后阅读并同意服务声明，然后可以开始创建组织。
   - 非首次创建组织：进入OrgID业务面开始创建组织。

使用OrgID：

在华为云OrgID控制台开通OrgID后，才能开始使用OrgID。

- 个人华为账号直接访问**OrgID**管理控制台，可以**创建组织**，并进入组织的管理中心进行组织管理等操作，相关操作请参见**管理中心介绍**。

- 登录华为云后可以免登录访问OrgID管理控制台进行组织管理等操作，相关操作请参见**管理中心介绍**。

使用对象

OrgID使用对象分为超级管理员、组织管理员、部门管理员和普通用户四种，不同对象的操作权限请参见**常见操作与系统角色的关系**。

- **超级管理员**：是开通OrgID后拥有创建组织权限的用户。创建组织后，自动成为组织创建者，是组织内的超级管理员。
- **组织管理员**：是超级管理员创建组织后在组织管理中心的“权限管理”页面添加为组织管理员的用户。
- **部门管理员**：是超级管理员或组织管理员在组织管理中心的“权限管理”页面添加为部门管理员的用户。
- **普通用户**：指具体使用OrgID的用户，由管理员在管理中心添加或邀请的用户。添加的用户会自动开通管理式华为账号，可登录并访问OrgID用户中心，邀请的用户账号也可以登录并访问OrgID用户中心。

使用账号

OrgID使用账号分为个人华为账号、管理式华为账号和第三方认证源账号。

- **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。
- **第三方认证源账号**：是指登录认证由第三方认证源提供，鉴权认证通过后，将登录OrgID进行后续业务操作，具体支持的认证源及认证操作请参见**认证源管理**。

管理式华为账号归属于组织，个人华为账号归属于个人。这两种账号在使用中是有区分的，管理员可以为管理式账号重置密码，但无法为个人账号重置密码。

2 开通 OrgID

租户需要先在华为云开通OrgID服务，才能使用OrgID提供的组织管理、组织成员账号管理以及SaaS应用授权管理的能力。本章节主要介绍开通OrgID的具体操作，开通OrgID前需要先开通OrgID白名单。

前提条件

- 已**注册华为账号并开通华为云**。
- 已**实名认证华为账号**。
- 已开通OrgID白名单。
  - 开通方式：由其他已对接OrgID的服务自动发起，如开通工业数字模型驱动引擎（IDME），IDME服务开通时会主动开通OrgID的白名单（将租户加入OrgID白名单，不需要租户单独申请）。
  - 开通已对接OrgID的服务后，如果无法使用OrgID，请联系对应服务确认。

开通 OrgID

步骤1 加入OrgID白名单后，登录**华为云OrgID控制台**。

步骤2 单击“创建组织”。

步骤3 阅读《Huawei OrgID服务声明》并单击“同意”。

阅读并同意服务声明后表示已成功开通OrgID服务，开通OrgID后方可进行下一步。

步骤4 根据界面指引创建组织，具体请参见**创建组织**。

----结束

3 创建组织

个人华为账号登录OrgID后，可以创建组织，成为该组织的组织创建者及超级管理员，拥有该组织的所有管理权限，包括成员部门管理、应用管理、认证管理、日志审计、组织管理（包括移交组织和解散组织）和权限管理等。

前提条件

已**开通OrgID**。

约束与限制

一个账号最多可以创建5个组织，当您的账号下已有5个组织时，可以在“切换组织”页面单击“配额申请”，通过申请配额来提升创建组织的上限。

创建组织

步骤1 登录**OrgID管理控制台**。

步骤2 单击“创建组织”。

步骤3 在“创建组织”页面，输入组织名称。

名称由1~60个中文、英文、数字及合法字符组成。

步骤4 设置组织的域名。

域名是指网址 (如www.example.com) 中“www”之后的内容，以及电子邮件地址（如《用户名》@example.com）中“@”符号之后的内容。

- 没有域名，可以输入组织简称，使用2~30位字母、数字和.-或它们的组合，如abc，后缀名为固定的.orgid.top，如**图3-1**所示。

图 3-1 设置组织域名

- 已有域名，单击“使用自有域名”，输入自有域名，例如example.com，如图3-2所示。

图 3-2 使用自有域名

域名设置后管理员为组织创建成员时，成员的管理式华为账号默认带有域名后缀，如设置的组织域名为abc.orgid.top，创建的成员账号为xxx@abc.orgid.top，设置的组织域名为example.com，创建的成员账号为xxx@example.com。

步骤5 阅读并勾选相关服务协议，然后单击“创建”。

组织创建成功，您可以在**控制台**继续进行后续的组织管理操作。也可以在**华为云OrgID控制台**为组织**开通联邦认证**，开通联邦认证后，授权的用户可以通过联邦认证访问组织的华为云资源。

----结束

4 登录场景介绍

用户可以使用个人华为账号或管理式华为账号登录OrgID，用户可根据账号类型，选择不同的登录方式。另外，也支持个人华为账号、管理式华为账号或第三方认证源账号通过OrgID访问某个注册在OrgID的应用；或者登录OrgID后，在用户中心免登录访问应用列表中的应用或华为云服务。

表 4-1 OrgID 登录场景

登录场景	使用账号	操作步骤	操作说明
登录OrgID	个人华为账号	1. 访问**OrgID**。 2. 输入账号名和密码，账号名处也可以输入手机号码或者邮箱地址，单击“登录”。	• 首次登录后显示OrgID管理控制台，后续登录默认进入最近访问的OrgID组织用户中心。 • 登录后可以创建组织，具体请参见**创建组织**。创建完成后，该华为账号会自动成为该组织的超级管理员，拥有该组织的所有管理权限。可以访问该组织的用户中心，可切换至该组织的管理中心，并进行组织管理。

登录场景	使用账号	操作步骤	操作说明
	管理式华为账号	1. 访问**OrgID**。 2. 输入账号名和密码，仅支持输入账号名，单击“登录”。	成功登录后，根据账号的权限不同，界面的呈现和可执行的操作不同，具体如下： • 组织管理员：登录后显示用户中心，可切换至组织的管理中心，除不能进行创建组织和解散组织的操作外，其余权限与组织创建者一致。 • 部门管理员：登录后显示用户中心，可切换至组织的管理中心，拥有查看组织信息、管理成员部门、管理应用的操作权限。 • 普通用户：登录后只能访问组织的用户中心，支持的操作可参见**用户中心介绍**。
通过OrgID访问某个注册在OrgID的应用	• 个人华为账号 • 管理式华为账号	1. 通过管理员获取某个注册在OrgID的应用URL或者该应用的登录地址。 2. 访问该地址，页面显示OrgID登录页。 3. 输入账号名及密码，单击“登录”。 登录成功后，系统自动回调到应用首页，应用能够获取到用户授权的个人信息。	OrgID会给应用发放授权码，通过授权码，应用获取相关TOKEN，并根据TOKEN调用获取用户信息接口，获取的用户信息。
	第三方认证源账号	使用第三方认证源账号登录OrgID前，需组织创建者或组织管理员在OrgID中配置第三方认证源，具体请参见**认证源管理**。 1. 通过管理员获取某个注册在OrgID的应用URL或者该应用的登录地址。 2. 访问该地址，页面显示OrgID登录页。 3. 切换认证源，展示第三方认证源的登录页面。 4. 输入第三方认证源账号名和密码，单击“登录”。 成功登录后显示应用首页。	

登录场景	使用账号	操作步骤	操作说明
免登录访问用户中心界面的应用或华为云服务	• 个人华为账号 • 管理式华为账号 • 第三方认证源账号	1. 访问**OrgID**。 2. 输入账号名及密码，单击“登录”。 3. 成功登录后，进入用户中心首页。 4. 单击最近使用或者全部应用中的应用/华为云服务，免登录进入该应用/华为云服务系统。该应用/华为云服务会获取到用户授权的个人信息。	-

5 OrgID 管理控制台介绍

使用OrgID服务创建组织或进行组织管理前，您需要先使用个人华为账号**开通OrgID**，然后登录OrgID管理控制台。

登录 OrgID 管理控制台

步骤1 访问**OrgID**。

步骤2 输入账号名和密码。

账号名处也可以输入手机号码或者邮箱地址。

步骤3 单击“登录”，成功登录后显示OrgID管理控制台。

首次登录后显示OrgID管理控制台，后续登录默认进入最近访问的OrgID组织用户中心。如果进入用户中心，管理员可以在右上角账号名的下拉列表中切换组织，进入管理控制台。

----结束

OrgID 管理控制台功能介绍

OrgID管理控制台如**图5-1**所示，展示组织列表和创建组织的入口，未创建组织时组织列表为空。

图 5-1 OrgID 管理控制台

在OrgID管理控制台界面，您可以进行以下操作。

- 单击组织名称，进入该组织的用户中心首页，在账号的下拉菜单中选择管理中心。在管理中心您可以管理该组织，相关操作请参见**管理中心介绍**。
- 单击“创建组织”，您可以创建新的组织，具体操作请参见**创建组织**。

6 用户中心介绍

组织的普通成员使用个人华为账号或管理式华为账号登录OrgID后，可以访问组织的用户中心首页。

前提条件

使用个人账号登录OrgID需先完成以下操作：

- 已**注册华为账号并开通华为云**。
- 已**实名认证华为账号**。
- 账号已被管理员邀请为组织成员：具体请参见**邀请成员**。

登录用户中心

步骤1 访问**OrgID**。

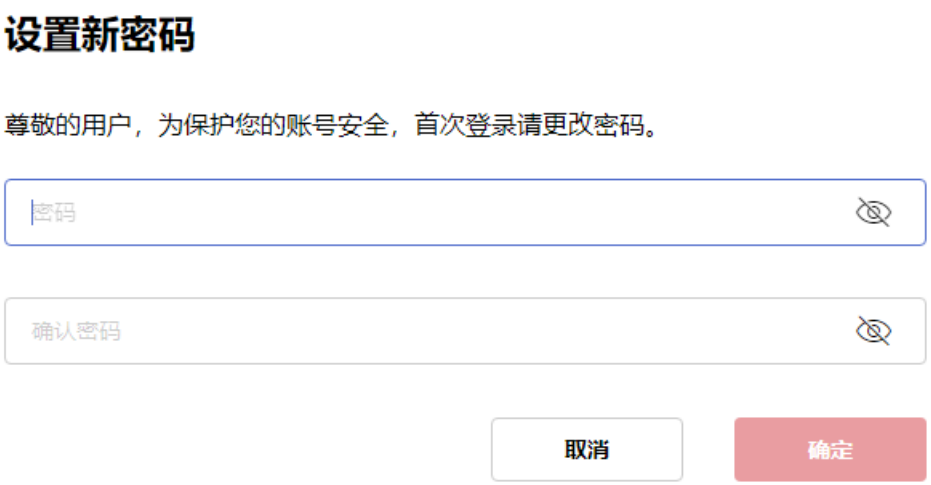
步骤2 输入账号名和密码，单击“登录”。

步骤3 通过管理员手动添加组织成员的方式创建的账号，首次登录需要设置新密码，如**图6-1**所示。设置密码后，下次才可使用账号名密码登录。如忘记密码，请单击登录页面的“忘记密码”，并根据界面提示找回密码。

设置的密码需要满足以下规则：

- 至少8个字符。
- 至少包含字母和数字，不能包含空格。

图 6-1 设置密码



步骤4 阅读并同意“管理式华为账号服务协议”。

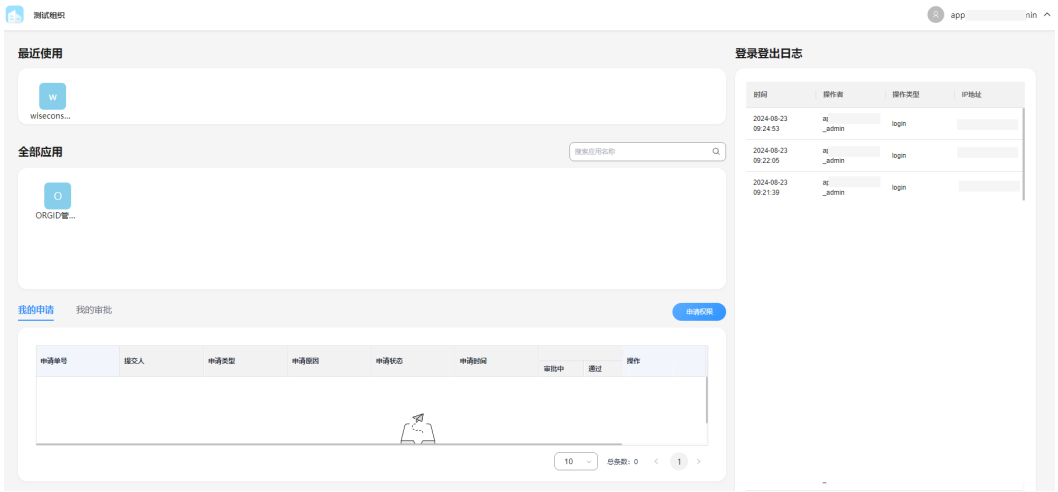
步骤5 登录后进入组织的用户中心首页。

----结束

用户中心首页介绍

在用户中心首页，您可以查看组织已有权限的全部应用及最近使用应用、查看我的申请和我的审批、查看登录登出日志或退出登录等操作。

图 6-2 用户中心首页



用户中心首页主要包含以下部分：

- 最近使用：展示您近期使用的应用，可单击应用直接免登录访问应用。
- 全部应用：展示组织的所有应用，可单击应用直接免登录访问应用。

- 我的申请：展示我的申请记录，可查看详情，也可在详情页撤回未审批的申请。
- 我的审批：展示需要审批的权限申请记录，可通过或驳回对应申请。
- 申请权限：可单击“申请权限”，进入权限管理页面申请其他权限。
- 登录登出日志：展示您的登录登出日志详情，包括时间、操作者、操作类型和IP地址。
- 账号的下拉菜单：可查看我的权限、账号信息，也支持退出登录。

7 管理中心介绍

组织创建者或组织创建者设置的拥有管理权限的组织用户（即组织管理员、部门管理员）可登录组织的管理中心对组织进行管理操作，包括成员部门管理、应用管理、认证管理、日志审计和组织管理（移交组织和解散组织仅支持组织创建者操作）等。

登录管理中心

步骤1 访问OrgID，进入用户中心首页。

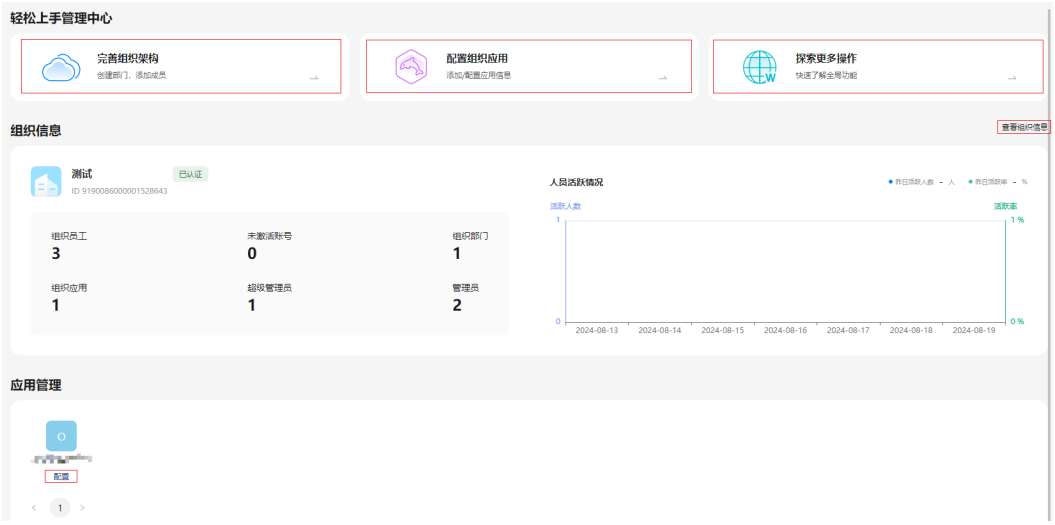
步骤2 单击右上角账号名，在下拉列表中选择“管理中心”，切换至管理中心。

----结束

管理中心首页功能介绍

管理中心首页不仅提供了完善组织架构、配置组织应用和探索更多操作的常用功能入口，还展示了组织的统计数据和应用管理的快捷入口，如图7-1所示。组织创建者或组织管理员可以通过管理中心快速访问所需功能，并了解组织的整体信息。

图 7-1 管理中心首页



具体快捷功能如下：

- 完善组织架构：可快速访问成员管理页面。
- 配置组织应用：可快速访问应用管理页面。
- 探索更多操作：可快速访问OrgID帮助文档。
- 查看组织信息：可快速访问组织信息界面。
- 配置：可快速访问对应应用的配置页面。

8 成员部门管理

8.1 部门管理

在部门管理页面，组织创建者或组织管理员可以通过添加部门、添加子部门、编辑部门、删除部门等操作完善组织架构。

添加部门

步骤1 登录管理中心。

步骤2 选择左侧导航栏的“成员部门管理 > 部门管理”。

步骤3 单击“添加部门”。

步骤4 输入部门名称、选择上级部门、设置部门CODE（可选），单击“确认”。

设置部门CODE后，可在部门管理界面通过部门CODE搜索部门。

----结束

更多操作

部门添加成功后，您还可以进行以下操作。

表 8-1 部门管理

操作名称	操作步骤
编辑部门	1. 单击待修改部门所在行“操作”列下的“编辑部门”。 组织创建成功后，会默认生成一个一级部门，该一级部门不支持编辑。 2. 修改部门信息，单击“更新”。
添加子部门	1. 单击待添加子部门的部门所在行“操作”列下的“添加子部门”。 2. 输入部门名称、设置部门CODE（可选），单击“确认”。

操作名称	操作步骤
删除部门	1. 单击待删除部门所在行“操作”列下的“删除”。 一级部门不支持删除。删除部门后，数据无法恢复，请谨慎操作。 2. 单击“确认”。

8.2 成员管理

在成员管理页面，管理员可以查看成员详情、创建/移除成员、变更成员部门、以及邀请已有个人华为账号的用户加入组织。

约束与限制

每个组织下默认最多可以创建和邀请共200个成员，如您有更大的使用需求，可以在组织信息页面**申请组织配额**。

创建成员

步骤1 **登录管理中心**。

步骤2 选择左侧导航栏的“成员部门管理 > 成员管理”。

步骤3 单击“创建成员”。

步骤4 填写成员信息，参数说明如**表8-2**所示。如果在**用户属性配置**中添加了自定义属性，还需根据属性要求填入相关信息。填写完成后，单击“保存”或“保存并继续”。

表 8-2 创建成员参数说明

参数名称	参数说明
成员姓名	成员的姓名。最多可输入20个字符。
成员账号	管理员为成员设置的账号。输入账号前半部分，并选择组织域名。 账号默认带组织域名后缀，如“zhangsan01@abc.orgid.top”。
手机号	成员的手机号码。非必填项，当邮箱地址未填写时手机号必须填写。
邮箱地址	成员的邮箱地址。非必填项，当手机号未填写时邮箱地址必须填写。
设置密码	管理员为成员设置的账号密码，支持选择“自动生成密码”或“手工输入密码”。 手工输入的密码长度必须超过8位，需要包含数字和英文字母，且不能出现三个连续相同的字符。 **成员首次登录需修改密码。**
部门	成员所属部门。
成员工号	成员的工号。

参数名称	参数说明
职位	成员所担任的职位。
用户组	选择成员所属的用户组。选择后在用户组列表下会展示该成员信息。
失效时间	设置成员账号的失效时间，到失效时间，系统将自动禁用账号。失效时间设置为空表示长期有效。 如果成员登录时账号到期失效，管理员可以为成员账号续期，具体请参见**账号续期**。

----结束

邀请成员

步骤1 **登录管理中心**。

步骤2 选择左侧导航栏的“成员部门管理 > 成员管理”。

步骤3 单击“邀请成员”。

步骤4 填写受邀的成员信息，成员信息参数说明如**表8-3**所示。如果在**用户属性配置**中添加了自定义属性，还需根据属性要求填入相关信息。填写完成后，单击“确认”。

表 8-3 邀请成员参数说明

参数名称	参数说明
姓名	成员的姓名。
手机号	成员的手机号码。非必填项，当邮箱地址未填写时手机号必须填写。
邮箱	成员的邮箱地址。非必填项，当手机号未填写时邮箱地址必须填写。
有效期	三天内有效，需要邀请的成员在三天内登录激活该账号。

----结束

批量导入成员

步骤1 **登录管理中心**。

步骤2 选择左侧导航栏的“成员部门管理 > 成员管理”。

步骤3 单击“批量导入成员”。

步骤4 单击“下载空白模板”下载CSV文件模板。

步骤5 完善成员信息并上传文件。

步骤6 单击“确定”，完成批量导入成员。

您可以单击“成员管理”页面的“导入历史”，查看导入成员的历史信息。

----结束

切换域名

仅支持为非“未激活”、“已冻结”状态的成员账号（管理式华为账号）切换域名。

步骤1 **登录管理中心**。

步骤2 选择左侧导航栏的“成员部门管理 > 成员管理”。

步骤3 在列表中勾选需要切换域名的成员，然后单击列表上方的“切换域名”。

步骤4 选择需要切换的域名，然后单击“确认”。

----结束

查看成员详情

步骤1 **登录管理中心**。

步骤2 选择左侧导航栏的“成员部门管理 > 成员管理”。

步骤3 选中成员所属部门。支持搜索部门名称，在搜索结果中选中部门名称。

步骤4 单击待查看成员所在行“操作”列的“查看详情”，进入“成员详情”页面查看成员具体信息。

在“成员详情”页面可以编辑该成员信息或者移除已冻结或未激活的成员。

----结束

重置密码

仅支持为通过**创建成员**加入组织的管理式华为账号重置密码。

步骤1 **登录管理中心**。

步骤2 选择左侧导航栏的“成员部门管理 > 成员管理”。

步骤3 选中成员所属部门。支持搜索部门名称，可搜索后选中部门名称。

步骤4 单击待重置密码成员所在行“操作”列的“重置密码”。

步骤5 在“重置密码”页面选择“自动生成密码”或“手工输入密码”。如果选择“手工输入密码”，需输入具体密码。密码设置完成后单击“确定”。

----结束

变更部门

步骤1 **登录管理中心**。

步骤2 选择左侧导航栏的“成员部门管理 > 成员管理”。

步骤3 选中成员所属部门。支持搜索部门名称，在搜索结果中选中部门名称。

步骤4 单击目标成员所在行“操作”列的“更多 > 变更部门”。

步骤5 选择目标部门，单击“确认”。

----结束

账号续期

步骤1 登录管理中心。

步骤2 选择左侧导航栏的“成员部门管理 > 成员管理”。

步骤3 选中成员所属部门。支持搜索部门名称，在搜索结果中选中部门名称。

步骤4 单击目标成员所在行“操作”列的“更多 > 续期”。

步骤5 选择账号失效时间，单击“确认”。

----结束

冻结、解冻成员

步骤1 登录管理中心。

步骤2 选择左侧导航栏的“成员部门管理 > 成员管理”。

步骤3 选中成员所属部门。支持搜索部门名称，在搜索结果中选中部门名称。

步骤4 单击目标成员所在行“操作”列的“更多 > 冻结”。

- 冻结后，账号将无法正常使用，请谨慎操作。
- 状态为“正常”的账号支持冻结。
- 冻结后，可单击“更多 > 解冻”解除账号的冻结状态。

----结束

移除成员

步骤1 登录管理中心。

步骤2 选择左侧导航栏的“成员部门管理 > 成员管理”。

步骤3 选中成员所属部门。支持搜索部门名称，在搜索结果中选中部门名称。

步骤4 单击目标成员所在行“操作”列的“更多 > 移除成员”。

- 移除后，该成员的账号将无法使用，请谨慎操作。
- 状态为“未激活”、“已冻结”的账号支持移除。

步骤5 单击“确认”。

----结束

8.3 用户组管理

在用户组管理页面，管理员可以对用户进行分组管理，完成新建用户组、查看用户组详情、添加成员、编辑或删除用户组的操作。

新建用户组

步骤1 登录管理中心。

步骤2 选择左侧导航栏的“成员部门管理 > 用户组管理”。

步骤3 单击“创建”，进入“新建用户组”页面。

步骤4 填写用户组信息，如图8-1所示，填写完成后单击“下一步：添加成员”。

图 8-1 新建用户组

步骤5 在“添加成员”页面勾选需要添加的成员后单击“确认”。

----结束

查看用户组详情

如果所属组织已开通联邦认证，用户组列表会默认显示与组织同名的用户组，组织创建者默认作为用户组成员和负责人。

步骤1 登录管理中心。

步骤2 选择左侧导航栏的“成员部门管理 > 用户组管理”。

步骤3 在用户组列表中单击待查看用户组名称。

步骤4 在用户组详情页面可以查看该用户组的基本信息、负责人信息及成员信息，并且可以在该详情页完成添加或移除用户组负责人、添加或移除用户组成员操作。

----结束

更多操作

用户组新建成功后，您还可以进行以下操作。

表 8-4 用户组管理

操作名称	操作步骤
编辑用户组	1. 单击待编辑用户组所在行“操作”列下的“编辑”。 仅限普通类型用户组可编辑，联邦认证的安全类型用户组不可编辑。 2. 修改用户组信息，单击“确认”。
添加成员	1. 单击待添加成员用户组所在行“操作”列下的“添加成员”。 2. 勾选需要添加的成员，单击“确认”。
删除用户组	1. 单击待删除用户组所在行“操作”列下的“删除”。 仅限普通类型用户组可删除，联邦认证的安全类型用户组不可删除。 2. 单击“确认”。

8.4 三方认证用户

背景信息

OrgID支持基于OAuth2、CAS、SAML、OIDC和AD协议的身份认证，组织创建者或组织管理员可根据需要添加基于OAuth2、CAS、SAML、OIDC和AD协议的组织认证源，添加时通过设置绑定策略，可以设置该认证源下的用户为第三方认证用户，具体可参见**认证源管理**。已添加的第三方认证用户可以在“三方认证用户”页面查看用户详情。

查看三方认证用户

步骤1 **登录管理中心**。

步骤2 选择左侧导航栏的“成员部门管理 > 三方认证用户”。

步骤3 在“三方认证用户”页面查看三方认证用户。

也可以通过选择认证源或者搜索账号名/手机号/邮箱查看三方认证用户。

----结束

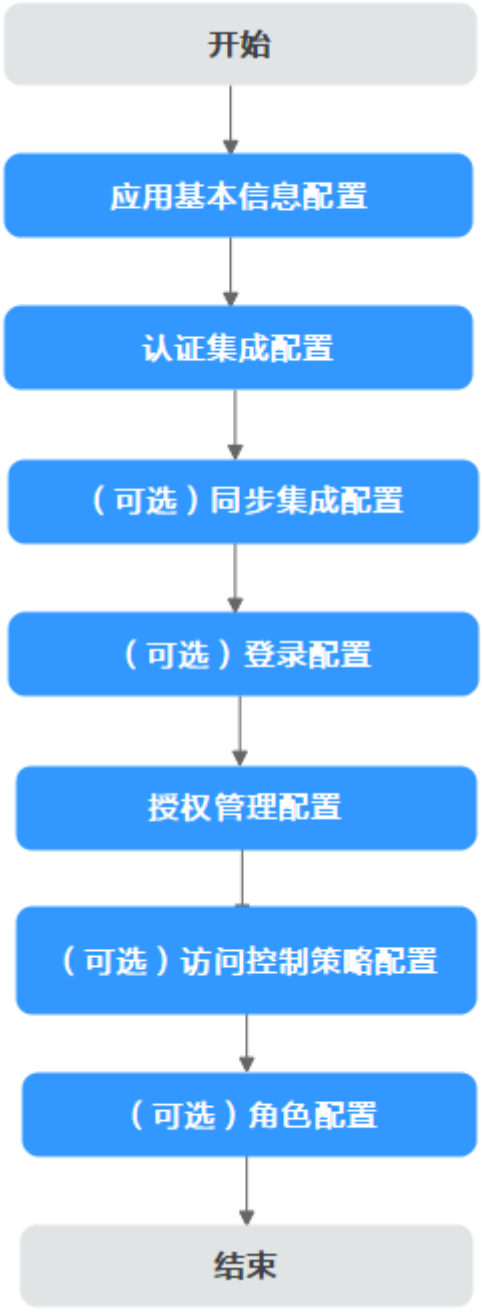
9 应用管理

9.1 创建自建应用

通过应用管理，组织创建者或组织管理员可根据业务场景创建或配置自建应用，OrgID用户中心首页会展示所有已创建的应用。用户可以在登录OrgID后，在用户中心首页实现免登录访问已成功创建并且有权限访问的所有应用，无需在访问不同应用时切换不同的登录账号，提升用户体验。

操作流程

图 9-1 创建自建应用流程图



应用基本信息配置

步骤1 登录管理中心。

步骤2 选择左侧导航栏的“应用管理”。

步骤3 单击“添加自建应用”。

步骤4 输入应用名称，如“App-test”。

步骤5 上传应用图标，图标要求必须为JPG或PNG格式，大小不超过20KB，尺寸240*240px。

步骤6 选择应用类型，当前仅支持选择“Web”。

步骤7 设置应用负责人，输入并选择成员姓名，将成员设置为应用负责人。

- 应用负责人即该应用的应用管理员，只有应用管理员才能更新该应用配置，其他管理员没有操作该应用的权限。
- 普通成员不能成为应用负责人，需先成为组织管理员、部门管理员才能被设置为应用负责人。

步骤8 单击“确认”，进入认证集成页面。

----结束

认证集成配置

步骤1 选择认证集成方式：OAuth2、OIDC、SAML、CAS3，选择后不支持修改。

步骤2 根据选择的认证集成方式不同，需要配置不同的参数，参数说明如表9-1所示。配置完成后，单击“保存”。

表 9-1 认证集成配置参数说明

认证集成方式	参数名称	参数说明
OAuth2	首页URL	应用首页的URL地址，例：https://xx.xx。 支持设置多个首页的URL地址，可单击“新建URL”，添加新的URL地址。
	管理员登录URL	可选项，管理员登录应用的URL地址。
	退出地址	可选项，应用的退出地址，请以http或https开头，例：https://xxx.xxx.xxx/logout。
	Refresh Token有效期（秒）	允许用户在多久时间内不用重新登录应用的时间。
	Access Token有效期（秒）	允许用户在多久时间内保持登录应用的时间。
OIDC	首页URL	应用首页的URL地址，例：https://xx.xx。
	管理员登录URL	可选项，管理员登录应用的URL地址。
	退出地址	可选项，应用的退出地址，请以http或https开头，例：https://xxx.xxx.xxx/logout。
	授权码模式	可选项，是否开启授权码模式。
	TOKEN签名算法	支持选择：RS256、RS384、RS512。

认证集成方式	参数名称	参数说明
	Access Token有效期（秒）	允许用户在多久时间内保持登录应用的时间。
	Refresh Token有效期（秒）	允许用户在多久时间内不用重新登录应用的时间。
SAML	SP Entity ID	SP唯一标识，对应SP元数据文件中的“Entity ID”的值。
	断言消费地址(ACS URL)	SP回调地址（断言消费服务地址），对应SP元数据文件中“AssertionConsumerService”的值，即当认证成功后响应返回的值。
	Name ID	用户在应用系统中的账号名对应字段，支持选择：邮箱、手机号、用户名、用户ID、账号名。
	NameID Format	可选项，SP支持的用户名称标识格式。对应SP元数据文件中“NameIDFormat”的值。支持选择： ● urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified ● urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress ● urn:oasis:names:tc:SAML:2.0:nameid-format:transient ● urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
	Audience URI	可选项，允许使用SAML断言的资源，默认和SP Entity ID相同。
	Single Logout URL	可选项，服务提供商提供会话注销功能，用户在OrgID注销会话后返回绑定的地址。对应SP元数据文件中“SingleLogoutService” 的值。“SingleLogoutService” 需要支持HTTP Redirect或HTTP POST方式。
	默认Relay State	可选项，使用在IdP发起的认证中，作为默认的一个值。
	支持ForceAuth	可选项，如果SP要求重新认证，则强制用户再次认证。
	Response签名	可选项，是否对SAML Response使用IdP的证书签名。
	断言签名	可选项，断言需使用IdP的证书签名，对应SP元数据文件中“WantAssertionsSigned”值。
	数字签名算法	可选项，SAML Response或者断言签名的算法。支持RSA_SHA256、RSA_SHA512、RSA_RIPEMD160，可在下拉框选择。

认证集成方式	参数名称	参数说明
	数字摘要算法	可选项，SAML Response或者断言的数字摘要算法。支持SHA256、SHA512、RIPEMD160，可在下拉框选择。
	验证请求签名	可选项，是否对SAML Request签名进行验证，对应SP元数据文件中“AuthnRequestsSigned”值。
CAS3	首页URL	应用首页的URL地址，例：https://xx.xx。
	管理员登录URL	可选项，管理员登录应用的URL地址。
	退出地址	可选项，应用的退出地址，请以http或https开头，例：https://xxx.xxx.xxx/logout。

步骤3 （可选）如果需要关联OrgID和自建应用的用户属性，可选择“映射配置”页签，单击“添加映射”，选择关联属性和映射属性，单击“确认”保存映射，单击“测试”，测试映射关系是否成立。

需要修改映射时，可单击操作列的“编辑”进行修改。

----结束

（可选）同步集成配置

步骤1 当需要同步应用的数据给第三方系统时，可开启同步集成开关，详细的同步数据请参见**联营Kit接口描述**联营Kit接口描述。

步骤2 配置相关参数，参数说明如**表9-2**所示。

表 9-2 同步集成配置参数说明

参数名称	参数说明
回调URL	用于同步该应用的数据给其他第三方系统的URL。
签名密钥	用于对回调消息体内容签名。
加密密钥	用于传输ClientSecret的加密公钥。
摘要算法	选择加密算法，如：SHA256或SHA1。 **SHA1安全强度不高，不建议使用。**

----结束

（可选）登录配置

步骤1 （可选）如果需要获取首页URL或管理员登录URL供其他用户使用，可单击获取。

管理员登录URL为空即表示在**步骤5**中未配置管理员登录地址。

步骤2 （可选）如果已进行**认证源管理**，可选择开启认证源。最多可以开启3个认证源，例如可以同时开启钉钉和2个OAuth认证源。根据开启的认证源类型不同，界面操作不同，具体如下。

- 开启组织社交认证源（钉钉、企业微信或Welink）：开启后，界面提示“保存成功”即成功开启。
- 开启组织认证源（OAuth、CAS、SAML、OIDC或AD）：开启后，需要选择关联的认证源，最多可关联3个，单击“保存”，界面提示“保存成功”即成功开启。

开启后，登录页会新增“其他方式登录”选项，可选择使用该认证源登录应用。

----结束

授权管理配置

步骤1 单击“授权设置”，在“授权设置”界面中选择被授权成员信息，单击“下一步”。

步骤2 选择可用成员范围，可勾选“全员可用”或“自定义人员范围”，勾选“自定义人员范围”后可以指定成员、部门或者用户组，然后单击“确认”。

设置后，应用授权范围中会显示授权部门、授权人员或授权用户组信息。同时，授权用户列表中也会展示授权账号的详细情况（包括姓名、账号名、应用侧角色、来源、更新时间和同步状态），支持按照时间或账号名进行过滤查询。

----结束

（可选）访问控制策略配置

步骤1 当需要控制用户在指定的时间或区域范围内访问应用时，可开启访问控制开关。

步骤2 配置默认策略。默认策略可选择“允许所有用户访问”或“拒绝所有用户访问”。

步骤3 单击“添加策略”，配置策略参数，参数说明如**表9-3**所示。

策略添加完成后，可单击“是否生效”列的  开启策略。开启后可单击“是否生效”列的  关闭策略。

表 9-3 添加策略参数说明

参数名称	参数说明
策略名称	应用访问策略的名称。
描述	可选项，应用访问策略的描述信息。
访问时间	可选择任意时间、指定星期范围内或指定日期范围内。
区域范围	可选择不限定或指定ip段。 选择指定ip段后，需先添加区域范围，包括设置区域名称、区域网段和描述信息。然后选择已添加的区域范围即可。

参数名称	参数说明
-	勾选访问策略。 • 允许访问：符合设置的访问时间或区域范围的用户允许访问该应用。 • 拒绝：符合设置的访问时间或区域范围的用户无法访问该应用。 • 二次验证：符合设置的访问时间或区域范围的用户可以使用手机验证码进行验证，验证通过后即可访问该应用。

----结束

（可选）角色配置

可以按照如下操作配置自建应用的角色并为角色关联权限或权限集，并配置数据范围，也支持**批量导入角色配置数据**，当角色配置后，支持**导出已配置的角色数据**。

步骤1 新建角色。

1. 在“角色管理”页签，单击“新建角色”。
2. 配置角色信息，具体参数请参见**表9-4**，配置完成后，单击“确定”。

表 9-4 角色信息参数说明

参数名称	参数说明
角色编码	自定义角色编码，最多可输出64个字符。
角色名称	自定义角色名称，最多可输出32个字符。
角色描述	填写角色描述，最多可输出256个字符。
最大可申请时间	可以设置该角色可申请的最大时间，即用户申请该角色权限时可申请的最长时间。 单位为天，如设置180天，用户申请该角色权限时，权限的有效期最多只能设置到180天后。如不设置，则默认用户申请后权限3年内有效。
审批人	需要设置用户申请该角色权限时的审批人。 – 按照角色审批：按照角色设置审批人，需要选择是否为OrgID应用角色，并选择对应角色。 – 按照用户审批：直接指定审批人。
OrgID应用角色	选择是否为OrgID应用角色。 – 是：选择OrgID应用角色，包括部门管理员、组织管理员、超级管理员。 – 否：选择已创建的应用角色。

步骤2 新增权限。

1. 在“权限管理”页签，单击“新增权限”。
2. 配置权限信息，具体参数请参见表9-5，配置完成后，单击“确定”。

表 9-5 权限信息参数说明

参数名称	参数说明
权限编码	自定义权限编码，最多可输出64个字符。
权限名称	自定义权限名称，最多可输出32个字符。
权限描述	填写权限描述，最多可输出256个字符。
权限类型	可以按照应用的API、菜单、按钮分别设置权限。
权限内容	设置具体的权限内容，使用英文逗号隔开。 其中API权限需要输入正确的API格式，包括接口方法和路径，如：POST /v1/xxx,GET /v1/xxx。

步骤3 （可选）新增权限集。

1. 在“权限集管理”页签，单击“新增权限集”。
2. 配置权限集信息，具体参数请参见表9-6，配置完成后，单击“确定”。

表 9-6 权限集信息参数说明

参数名称	参数说明
权限集编码	自定义权限集编码，最多可输出64个字符。
权限集名称	自定义权限集名称，最多可输出64个字符。
权限集描述	填写权限集描述，最多可输出256个字符。
权限	选择已新增的权限。

步骤4 为角色配置权限或权限集。

- 配置权限
  a. 在“角色管理”页签，角色列表中，单击已创建的角色所在行“操作”列的“权限配置”。
  b. 单击“添加权限”。
  c. 可以在不同页签分别勾选已创建的权限，然后单击“确定”。
  完成角色与权限的关联，当用户申请相应角色权限后，拥有该角色关联的权限。
- 配置权限集
  a. 在“角色管理”页签，角色列表中，单击已创建的角色所在行“操作”列的“权限集配置”。
  b. 单击“添加权限集”。
  c. 勾选已新增的权限集，然后单击“确定”。

完成角色与权限集的关联，当用户申请相应角色权限后，拥有该角色关联的权限集的全部权限。

步骤5 新增数据范围并指定具体的数据明细。

1. 在“数据范围”页签，单击“新增数据范围”。
2. 输入数据范围编码、数据范围名称、数据范围描述以及父数据范围，然后单击“确定”。

   新增后列表显示已新增的数据范围。
3. 在数据范围列表中，单击已新增的数据范围所在行“操作”列的“数据明细”。
4. 单击“新增”。
5. 输入明细编码、明细名称、明细描述，然后单击“确定”。

   如需批量导入数据明细，可单击“导入”，单击“下载空白模板”，在模板中编辑数据明细，然后上传文件，单击“提交”。

步骤6 为角色添加数据范围。

1. 在“角色管理”页签，角色列表中，单击已创建的角色所在行“操作”列的“数据范围”。
2. 单击“添加数据范围”。
3. 勾选已新增的数据范围，然后单击“确定”。

----结束

更多操作

创建自建应用后，您还可以进行以下操作。

表 9-7 应用的更多操作

操作名称	操作步骤
启用/禁用应用	开启：自建应用创建完成后，默认自动开启。 禁用：在“应用管理 > 全部应用”界面，在“应用状态”列，关闭  ，在弹出的提示框中，单击“确认”。 **禁用应用后，该应用无法使用，且用户中心不显示该应用，请谨慎操作。**
配置应用	具体请参见**配置自建应用**。
删除应用	1. 在“应用管理 > 全部应用”界面，在“应用状态”列，关闭  ，在弹出的提示框中，单击“确认”。 2. 单击操作列的“删除”，在弹出的提示框中，单击“确认”。 **删除后，该应用的数据将被删除且不可恢复，请谨慎操作。**

9.2 配置自建应用

9.2.1 通用配置

应用基本信息（应用名称、应用图标等）变更时，可通过通用配置界面进行修改。

修改通用配置

步骤1 登录管理中心。

步骤2 选择左侧导航栏的“应用管理”。

步骤3 在“全部应用”页签，单击待修改的应用操作列的“配置”。

步骤4 单击“通用配置”，进入“通用配置”页签。

步骤5 根据需要，修改应用图标、应用名称或应用负责人。

图标要求必须为JPG或PNG格式，大小不超过20KB，尺寸240*240px。

步骤6 单击“保存”。

----结束

9.2.2 认证集成配置

通过认证集成界面，可更改应用的认证集成参数，也可根据所需添加或修改映射。

配置认证集成方式

步骤1 登录管理中心。

步骤2 选择左侧导航栏的“应用管理”。

步骤3 在“全部应用”页签，单击待修改的应用操作列的“配置”。

步骤4 单击“认证集成”，进入“认证集成”页签。

步骤5 根据选择的认证集成方式不同，需要配置不同的参数，参数说明如表9-8所示。配置完成后，单击“保存”。

表 9-8 认证集成配置参数说明

认证集成方式	参数名称	参数说明
OAuth2	首页URL	应用首页的URL地址，例：https://xx.xx。 支持设置多个首页的URL地址，可单击“新建URL”，添加新的URL地址。
	管理员登录URL	可选项，管理员登录应用的URL地址。
	退出地址	可选项，应用的退出地址，请以http或https开头，例：https://xxx.xxx.xxx/logout。
	Refresh Token有效期（秒）	允许用户在多久时间内不用重新登录应用的时间。
	Access Token有效期（秒）	允许用户在多久时间内保持登录应用的时间。

认证集成方式	参数名称	参数说明
OIDC	首页URL	应用首页的URL地址，例：https://xx.xx。
	管理员登录URL	可选项，管理员登录应用的URL地址。
	退出地址	可选项，应用的退出地址，请以http或https开头，例：https://xxx.xxx.xxx/logout。
	授权码模式	可选项，是否开启授权码模式。
	TOKEN签名算法	支持选择：RS256、RS384、RS512。
	Access Token有效期（秒）	允许用户在多久时间内保持登录应用的时间。
	Refresh Token有效期（秒）	允许用户在多久时间内不用重新登录应用的时间。
SAML	SP Entity ID	SP唯一标识，对应SP元数据文件中的“Entity ID”的值。
	断言消费地址(ACS URL)	SP回调地址（断言消费服务地址），对应SP元数据文件中“AssertionConsumerService”的值，即当认证成功后响应返回的值。
	Name ID	用户在应用系统中的账号名对应字段，支持选择：邮箱、手机号、用户名、用户ID、账号名。
	NameID Format	可选项，SP支持的用户名称标识格式。对应SP元数据文件中“NameIDFormat”的值。支持选择: ● urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified ● urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress ● urn:oasis:names:tc:SAML:2.0:nameid-format:transient ● urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
	Audience URI	可选项，允许使用SAML断言的资源，默认和SP Entity ID相同。
	Single Logout URL	可选项，服务提供商提供会话注销功能，用户在OrgID注销会话后返回绑定的地址。对应SP元数据文件中“SingleLogoutService” 的值。“SingleLogoutService” 需要支持HTTP Redirect或HTTP POST方式。
	默认Relay State	可选项，使用在IdP发起的认证中，作为默认的一个值。

认证集成方式	参数名称	参数说明
	支持ForceAuth	可选项，如果SP要求重新认证，则强制用户再次认证。
	Response签名	可选项，是否对SAML Response使用IdP的证书签名。
	断言签名	可选项，断言需使用IdP的证书签名，对应SP元数据文件中“WantAssertionsSigned”值。
	数字签名算法	可选项，SAML Response或者断言签名的算法。支持RSA_SHA256、RSA_SHA512、RSA_RIPEMD160，可在下拉框选择。
	数字摘要算法	可选项，SAML Response或者断言的数字摘要算法。支持SHA256、SHA512、RIPEMD160，可在下拉框选择。
	验证请求签名	可选项，是否对SAML Request签名进行验证，对应SP元数据文件中“AuthnRequestsSigned”值。
CAS3	首页URL	应用首页的URL地址，例：https://xx.xx。
	管理员登录URL	可选项，管理员登录应用的URL地址。
	退出地址	可选项，应用的退出地址，请以http或https开头，例：https://xxx.xxx.xxx/logout。

步骤6 （可选）如果需要关联OrgID和自建应用的用户属性，可选择“映射配置”页签，单击“添加映射”，选择关联属性和映射属性，单击“确认”保存映射，单击“测试”，测试映射关系是否成立。

需要修改映射时，可单击操作列的“编辑”进行修改。

----结束

9.2.3 同步集成配置

通过同步集成配置，可以将该应用的数据同步给配置的第三方系统。详细的同步数据请参见**联营Kit接口描述**。

配置同步集成信息

步骤1 **登录管理中心**。

步骤2 选择左侧导航栏的“应用管理”。

步骤3 在“全部应用”页签，单击待修改的应用操作列的“配置”。

步骤4 单击“同步集成”，进入“同步集成”页签。

步骤5 配置相关参数，参数说明如**表9-9**所示。

表 9-9 同步集成配置参数说明

参数名称	参数说明
回调URL	用于同步该应用的数据给其他第三方系统的URL。
签名密钥	用于对回调消息体内容签名。
加密密钥	用于传输ClientSecret的加密公钥。
摘要算法	选择加密算法，如：SHA256或SHA1。 **SHA1安全强度不高，不建议使用。**

----结束

9.2.4 登录配置

在登录配置界面，可获取应用登录地址，包括首页URL和管理员登录URL。首页URL和管理员登录URL是在认证集成界面进行配置的，登录配置界面不支持修改。当已进行**认证源管理**，登录配置界面支持开启或关闭认证源。

开启/关闭认证源

步骤1 **登录管理中心**。

步骤2 选择左侧导航栏的“应用管理”。

步骤3 在“全部应用”页签，单击待修改的应用操作列的“配置”。

步骤4 单击“登录配置”，进入“登录配置”页签。

步骤5 在“认证方式”模块，开启/关闭指定认证源操作列的开关即可。最多可以开启3个认证源，例如可以同时开启钉钉和2个OAuth认证源。根据开启的认证源类型不同，界面操作不同，具体如下：

- 开启组织社交认证源（钉钉、企业微信或Welink）：开启后，界面提示“保存成功”即成功开启。
- 开启组织认证源（OAuth、CAS、SAML、OIDC或AD）：开启后，需要选择关联的认证源，最多可关联3个，单击“保存”，界面提示“保存成功”即成功开启。

开启后，登录页会新增“其他方式登录”选项，可选择使用该认证源登录应用。

----结束

9.2.5 授权管理配置

通过授权管理，可以配置应用的授权范围，并选择应用的可用成员范围。组织创建者或组织管理员可根据应用所需更改授权设置。

配置应用授权

步骤1 **登录管理中心**。

步骤2 选择左侧导航栏的“应用管理”。

步骤3 在“全部应用”页签，单击待修改的应用操作列的“配置”。

步骤4 单击“授权管理”，进入“授权管理”页签。

步骤5 单击“授权设置”，在“授权设置”界面中选择被授权成员信息，单击“下一步”。

步骤6 选择可用成员范围，可勾选“全员可用”或“自定义人员范围”，勾选“自定义人员范围”后可以指定成员、部门或者用户组，然后单击“确认”。

设置后，应用授权范围中会显示授权部门、授权人员或授权用户组信息。同时，授权用户列表中也会展示授权账号的详细情况（包括姓名、账号名、应用侧角色、来源、更新时间和同步状态），支持按照账号名进行过滤查询。

----结束

9.2.6 访问控制策略配置

可以通过添加访问控制策略，允许/拒绝用户在指定的时间或区域范围内访问应用。组织创建者或组织管理员可修改或删除已添加的访问控制策略，也支持添加多个访问控制策略。

配置访问控制策略

步骤1 登录管理中心。

步骤2 选择左侧导航栏的“应用管理”。

步骤3 在“全部应用”页签，单击待修改的应用操作列的“配置”。

步骤4 单击“访问控制”，进入“访问控制”页签。

步骤5 开启/关闭访问控制开关：在“基础设置”中开启/关闭访问控制开关即可。

开启后需配置默认策略，请参见步骤6。

步骤6 配置默认策略。默认策略可选择“允许所有用户访问”或“拒绝所有用户访问”。

步骤7 根据所需，修改、新增或删除策略。

- 修改策略：单击指定策略操作列的“编辑”，修改策略参数，参数说明如表9-10所示。
- 新增策略：单击“添加策略”，配置策略参数，参数说明如表9-10所示。

表 9-10 添加策略参数说明

参数名称	参数说明
策略名称	应用访问策略的名称。
描述	可选项，应用访问策略的描述信息。
访问时间	可选择任意时间、指定星期范围内或指定日期范围内。
区域范围	可选择不限定或指定ip段。 选择指定ip段后，需先添加区域范围，包括设置区域名称、区域网段和描述信息。然后选择已添加的区域范围即可。

参数名称	参数说明
-	勾选访问策略。 – 允许访问：符合设置的访问时间或区域范围的用户允许访问该应用。 – 拒绝：符合设置的访问时间或区域范围的用户无法访问该应用。 – 二次验证：符合设置的访问时间或区域范围的用户可以使用手机验证码进行验证，验证通过后即可访问该应用。

- 删除策略：单击指定策略操作列的“删除”，单击“确认”。

  删除后，该策略的数据将被删除且不可恢复，请谨慎操作。

----结束

9.2.7 角色配置

可以配置自建应用的角色并为角色关联权限或权限集，并配置数据范围，也支持**批量导入角色配置数据**，当角色配置后，支持**导出已配置的角色数据**。

配置应用角色

步骤1 **登录管理中心**。

步骤2 选择左侧导航栏的“应用管理”。

步骤3 在“全部应用”页签，单击待修改的应用操作列的“配置”。

步骤4 单击“角色配置”，进入“角色配置”页签，默认显示“角色管理”。

步骤5 新建角色。

1. 在“角色管理”页签，单击“新建角色”。
2. 配置角色信息，具体参数请参见**表9-11**，配置完成后，单击“确定”。

表 9-11 角色信息参数说明

参数名称	参数说明
角色编码	自定义角色编码，最多可输出64个字符。
角色名称	自定义角色名称，最多可输出32个字符。
角色描述	填写角色描述，最多可输出256个字符。
最大可申请时间	可以设置该角色可申请的最大时间，即用户申请该角色权限时可申请的最长时间。 单位为天，如设置180天，用户申请该角色权限时，权限的有效期最多只能设置到180天后。如不设置，则默认用户申请后权限3年内有效。

参数名称	参数说明
审批人	需要设置用户申请该角色权限时的审批人。 – 按照角色审批：按照角色设置审批人，需要选择是否为OrgID应用角色，并选择对应角色。 – 按照用户审批：直接指定审批人。
OrgID应用角色	选择是否为OrgID应用角色。 – 是：选择OrgID应用角色，包括部门管理员、组织管理员、超级管理员。 – 否：选择已创建的应用角色。

步骤6 新增权限。

1. 在“权限管理”页签，单击“新增权限”。
2. 配置权限信息，具体参数请参见**表9-12**，配置完成后，单击“确定”。

表 9-12 权限信息参数说明

参数名称	参数说明
权限编码	自定义权限编码，最多可输出64个字符。
权限名称	自定义权限名称，最多可输出32个字符。
权限描述	填写权限描述，最多可输出256个字符。
权限类型	可以按照应用的API、菜单、按钮分别设置权限。
权限内容	设置具体的权限内容，使用英文逗号隔开。 其中API权限需要输入正确的API格式，包括接口方法和路径，如：POST /v1/xxx,GET /v1/xxx。

步骤7 （可选）新增权限集。

1. 在“权限集管理”页签，单击“新增权限集”。
2. 配置权限集信息，具体参数请参见**表9-13**，配置完成后，单击“确定”。

表 9-13 权限集信息参数说明

参数名称	参数说明
权限集编码	自定义权限集编码，最多可输出64个字符。
权限集名称	自定义权限集名称，最多可输出64个字符。
权限集描述	填写权限集描述，最多可输出256个字符。
权限	选择已新增的权限。

步骤8 为角色配置权限或权限集。

- 配置权限
  a. 在“角色管理”页签，角色列表中，单击已创建的角色所在行“操作”列的“权限配置”。
  b. 单击“添加权限”。
  c. 可以在不同页签分别勾选已创建的权限，然后单击“确定”。
     完成角色与权限的关联，当用户申请相应角色权限后，拥有该角色关联的权限。
- 配置权限集
  a. 在“角色管理”页签，角色列表中，单击已创建的角色所在行“操作”列的“权限集配置”。
  b. 单击“添加权限集”。
  c. 勾选已新增的权限集，然后单击“确定”。
     完成角色与权限集的关联，当用户申请相应角色权限后，拥有该角色关联的权限集的全部权限。

步骤9 新增数据范围并指定具体的数据明细。

1. 在“数据范围”页签，单击“新增数据范围”。
2. 输入数据范围编码、数据范围名称、数据范围描述以及父数据范围，然后单击“确定”。
   新增后列表显示已新增的数据范围。
3. 在数据范围列表中，单击已新增的数据范围所在行“操作”列的“数据明细”。
4. 单击“新增”。
5. 输入明细编码、明细名称、明细描述，然后单击“确定”。
   如需批量导入数据明细，可单击“导入”，单击“下载空白模板”，在模板中编辑数据明细，然后上传文件，单击“提交”。

步骤10 为角色添加数据范围。

1. 在“角色管理”页签，角色列表中，单击已创建的角色所在行“操作”列的“数据范围”。
2. 单击“添加数据范围”。
3. 勾选已新增的数据范围，然后单击“确定”。

----结束

批量导入角色配置数据

步骤1 登录管理中心。

步骤2 选择左侧导航栏的“应用管理”。

步骤3 在“全部应用”页签，单击待修改的应用操作列的“配置”。

步骤4 单击“角色配置”，进入“角色配置”页签。

步骤5 单击“导入”。

步骤6 在“角色配置导入”页面，单击“下载空白模板”，在模板中编辑角色配置数据，完善配置文件。

步骤7 上传配置文件，单击“提交”。

提交后，可以在“我的导入”页面查看导入结果。

----结束

导出已配置的角色数据

步骤1 **登录管理中心**。

步骤2 选择左侧导航栏的“应用管理”。

步骤3 在“全部应用”页签，单击待修改的应用操作列的“配置”。

步骤4 单击“角色配置”，进入“角色配置”页签。

步骤5 单击“导出”。

可以在“我的导出”页面查看导出结果、下载导出文件。

----结束

10 认证管理

10.1 认证源管理

10.1.1 配置组织社交认证源

OrgID支持配置多种第三方认证源，包括组织社交认证源和组织认证源，为组织用户登录OrgID提供便利。组织创建者或组织管理员可以根据组织需要添加、修改和删除认证源。组织社交认证源包括钉钉、企业微信、Welink，下面以Welink为例说明组织社交认证源的配置方法。应用绑定组织已添加的社交认证源后，组织用户可以通过三方认证源登录应用。

- 请确保组织创建者或组织管理员已拥有WeLink开放平台账号管理员权限。
- 请确保组织创建者或组织管理员已在WeLink开放平台创建了应用。具体可以参考**WeLink对接文档**。
- 第三方认证源账号认证后，会在OrgID中生成新的成员用户或者匹配到已存在的用户。
- 第三方账号默认为来宾身份，不可更改其角色。

配置组织社交认证源

步骤1 **登录管理中心**。

步骤2 选择左侧导航栏的“认证管理 > 认证源管理”。

步骤3 在组织社交认证源中，单击welink右侧的“配置”。

步骤4 进入“新增welink认证源”界面，配置相关参数，参数说明如**表10-1**所示。

表 10-1 组织社交认证源参数说明

参数名称	参数说明
显示名称	认证源名称，支持自定义。
AppKey	WeLink开放平台创建应用获取的client_id。

参数名称	参数说明
AppSecret	WeLink开放平台创建应用获取的client_secret。
关联属性	WeLink对接OrgID的映射属性。支持选择：用户账户名、邮箱、手机号。
绑定属性	WeLink开放平台提供的用户属性字段，用于和OrgID的用户属性进行关联。
绑定策略	通过设置绑定策略，设置认证源下的用户是否关联系统用户还是新增用户作为第三方认证用户。支持选择：新增或绑定、绑定、新增。 当选择新增或绑定时，先关联系统用户，如果未关联到系统用户，则新增为第三方认证用户。

步骤5 单击“确认”，成功添加认证源。

----结束

10.1.2 添加组织认证源

OrgID支持基于OAuth2、CAS3、SAML、OIDC和AD协议的身份认证，组织创建者或组织管理员可根据需要添加基于OAuth2、CAS3、SAML、OIDC和AD协议的组织认证源，添加成功后还需配置应用信息，确保用户可以通过OAuth2、CAS3、SAML、OIDC和AD登录OrgID用户中心。

添加 OAuth2 认证源

OAuth（开放授权）是一个开放标准，允许用户授权第三方应用访问其存储在资源服务器上的信息，而不需要将用户名和密码提供给第三方应用。当前OrgID支持添加2.0版本的OAuth认证源。

步骤1 登录管理中心。

步骤2 选择左侧导航栏的“认证管理 > 认证源管理”。

步骤3 在组织认证源中，选择“OAuth2”页签，单击“新增认证源”。

步骤4 进入“OAuth2认证源绑定”界面，配置相关参数，参数说明如表10-2所示。

表 10-2 OAuth2 认证源参数说明

参数名称	参数说明
显示名称	认证源的显示名称。如OAuth认证。
认证源图标	显示的认证源图标。必须为JPG、PNG格式，大小不超过20KB，尺寸240*240px。
授权地址	应用的认证授权地址，从待绑定的认证源应用处获取。
Token地址	获取token的地址，从待绑定的认证源应用处获取。
授权范围	授权范围，多值以“,”分隔。

参数名称	参数说明
Client ID	应用的接口认证凭证ID，从待绑定的认证源应用处获取。
Client Secret	应用的接口认证凭证密钥，从待绑定的认证源应用处获取。
授权方式	OAuth2支持通过如下方式授权，可根据需要进行选择。 ● Authorization Code：授权码方式，指第三方应用先申请一个授权码，然后再用该码获取令牌。是OAuth最常用的授权方式，适用于有后端的Web应用。 ● Implicit：隐藏式授权，有些Web应用是纯前端应用，没有后端，这时就不能用Authorization Code方式，必须将令牌储存在前端，允许直接向前端颁发令牌。 ● Resource Owner Password Credential：密码式授权，用户把用户名和密码直接告诉该应用，该应用就使用用户的密码申请令牌，适用于其他授权方式都无法采用的情况，而且必须是用户高度信任的应用。 ● Client Credential：客户端凭证授权，适用于没有前端的命令行应用，即在命令行下请求令牌。这种方式给出的令牌，是针对第三方应用的，而不是针对用户的，即有可能多个用户共享同一个令牌。
关联属性	OAuth2认证源对接OrgID的映射属性。支持选择：用户账户名、邮箱、手机号。
绑定属性	待绑定的认证源应用提供的用户属性字段，用于和OrgID的用户属性进行关联。
用户信息地址	获取用户信息的地址，从待绑定的认证源应用处获取。
绑定策略	通过设置绑定策略，设置认证源下的用户是否关联系统用户还是新增用户作为第三方认证用户。支持选择：新增或绑定、绑定、新增。 当选择新增或绑定时，先关联系统用户，如果未关联到系统用户，则新增为第三方认证用户。

参数名称	参数说明
认证方式	OAuth2支持通过如下方式进行认证，默认选择client_secret_post。 • basic：客户端使用HTTP Basic发送其客户端密钥。 • client_secret_basic：是将clientId和clientSecret通过“:”拼接，并使用Base64进行编码得到一个字符串。将此编码字符串放到请求头（Authorization）去发送请求。 • post：客户端使用表单参数发送客户端密钥。 • client_secret_post：是将clientId和clientSecret放到请求体（表单）去发送请求。 • client_secret_jwt：利用JWT进行认证，请求方和授权服务器都知道客户端的clientSecret，通过相同的HMAC算法（对称签名算法）去加签和验签JWT 。 • private_key_jwt：利用JWT进行认证，请求方拥有自己的公私钥（密钥对），使用私钥对JWT加签，并将公钥暴露给授权服务器，授权服务器通过请求方的公钥验证JWT。 • none：客户端不在令牌端点上进行身份认证，可能是因为客户端不使用令牌端点，或者使用令牌端点但它是公开客户端。
属性映射	可选项，用于关联OrgID和待绑定的认证源应用的用户属性。单击“添加映射”，在下拉框中选择固定属性或自定义属性。 • 固定属性：将第三方用户属性与系统用户属性做关联，需选择关联属性和映射属性。 • 自定义属性：自定义属性的固定值，需输入属性值和固定值。

----结束

添加 CAS3 认证源

CAS是一个基于HTTP2、HTTP3的协议，要求每个组件都可以通过特定的URL访问应用 。当前OrgID支持添加3.0版本的CAS认证源。通过CAS协议将OrgID作为服务提供商，使第三方应用的用户账号可以通过CAS3协议访问OrgID。

步骤1 登录管理中心。

步骤2 选择左侧导航栏的“认证管理 > 认证源管理”。

步骤3 在组织认证源中，选择“CAS3”页签，单击“新增认证源”。

步骤4 进入“CAS3认证源绑定”界面，配置相关参数，参数说明如表10-3所示。

表 10-3 CAS3 认证源参数说明

参数名称	参数说明
显示名称	认证源的显示名称。如CAS3认证。
认证源图标	显示的认证源图标。必须为JPG、PNG格式，大小不超过20KB，尺寸240*240px。

参数名称	参数说明
登录URL	应用登录完成后的跳转地址，从待绑定的认证源应用处获取。
登出URL	应用退出登录的调用地址，从待绑定的认证源应用处获取。
校验Ticket地址	应用的验证地址，CAS3.0对应的验证地址为：https://xxx.xxx.xxx/p3/serviceValidate。
关联属性	CAS3认证源对接OrgID的映射属性。支持选择：用户账户名、邮箱、手机号。
绑定属性	待绑定的认证源应用提供的用户属性字段，用于和OrgID的用户属性进行关联。
请求类型	http请求发起的方式，支持GET和POST方式。
绑定策略	通过设置绑定策略，设置认证源下的用户是否关联系统用户还是新增用户作为第三方认证用户。支持选择：新增或绑定、绑定、新增。 当选择新增或绑定时，先关联系统用户，如果未关联到系统用户，则新增为第三方认证用户。
属性映射	可选项，用于关联OrgID和待绑定的认证源应用的用户属性。单击“添加映射”，在下拉框中选择固定属性或自定义属性。 • 固定属性：将第三方用户属性与系统用户属性做关联，需选择关联属性和映射属性。 • 自定义属性：自定义属性的固定值，需输入属性值和固定值。

----结束

添加 SAML 认证源

SAML，安全断言标记语言（Security Assertion Markup Language，缩写为SAML）是一个由一组协议组成，用来传输安全声明的XML框架。SAML是由标准化组织OASIS制定的标准，是很多身份提供商（Identity Provider，简称IdP）使用的一种开放标准。OrgID支持基于SAML协议的身份认证，如果您已经有自己的身份认证系统，您可以使用OrgID提供的SAML认证源功能，实现使用身份提供商账号登录OrgID用户中心。

步骤1 登录管理中心。

步骤2 选择左侧导航栏的“认证管理 > 认证源管理”。

步骤3 在组织认证源中，选择“SAML”页签，单击“新增认证源”。

步骤4 进入“SAML认证源绑定”界面，配置相关参数，参数说明如表10-4所示。

表 10-4 SAML 认证源参数说明

参数名称	参数说明
显示名称	认证源的显示名称。如SAML认证。

参数名称	参数说明
认证源图标	显示的认证源图标。必须为JPG、PNG格式，大小不超过20KB，尺寸240*240px。
entityId	对应IdP元数据文件中“entityID”的值。
issuerId	IdP的entityId，可从其IdP metedata文件中获取。
验签证书	IdP的签名证书，可从IdP的元数据文件中获取。 签名证书是一份包含公钥用于验证签名的证书。OrgID通过元数据文件中的签名证书来确认用户身份认证过程中断言消息的可信性、完整性。
请求协议绑定	对应IdP元数据文件中“SingleSignOnService”地址支持的绑定类型。 用户登录过程中发送SAML请求的方式。元数据文件中的“SingleSignOnService”需要支持HTTP Redirect或HTTP POST方式。
登录URL	应用登录完成后的跳转地址，从待绑定的认证源应用处获取。
登出URL	应用退出登录的调用地址，从待绑定的认证源应用处获取。
SAML请求签名	可选项，是否开启SAML请求签名，默认开启。
请求签名算法	请求签名算法，当前仅支持选择RSA-SHA256。
请求摘要算法	请求摘要算法，当前仅支持选择SHA256。
绑定属性	待绑定的认证源应用提供的用户属性字段，用于和OrgID的用户属性进行关联。
绑定策略	通过设置绑定策略，设置认证源下的用户是否关联系统用户还是新增用户作为第三方认证用户。支持选择：新增或绑定、绑定、新增。 当选择新增或绑定时，先关联系统用户，如果未关联到系统用户，则新增为第三方认证用户。
关联属性	SAML认证源对接OrgID的映射属性。支持选择：用户账户名、邮箱、手机号。
属性映射	可选项，用于关联OrgID和待绑定的认证源应用的用户属性。单击“添加映射”，在下拉框中选择固定属性或自定义属性。 ● 固定属性：将第三方用户属性与系统用户属性做关联，需选择关联属性和映射属性。 ● 自定义属性：自定义属性的固定值，需输入属性值和固定值。

----结束

添加 OIDC 认证源

OIDC是OpenID Connect的简称，是一个基于OAuth 2.0协议的身份认证标准协议。

步骤1 登录管理中心。

步骤2 选择左侧导航栏的“认证管理 > 认证源管理”。

步骤3 在组织认证源中，选择“OIDC”页签，单击“新增认证源”。

步骤4 进入“OIDC认证源绑定”界面，配置相关参数，参数说明如表10-5所示。

表 10-5 OIDC 认证源参数说明

参数名称	参数说明
显示名称	认证源的显示名称。如OIDC认证。
认证源图标	显示的认证源图标。必须为JPG、PNG格式，大小不超过20KB，尺寸240*240px。
授权地址	应用的认证授权地址，从待绑定的认证源应用处获取。
Token地址	获取token的地址，从待绑定的认证源应用处获取。
授权范围	授权范围，多值以“,”分隔。
Client ID	应用的接口认证凭证ID，从待绑定的认证源应用处获取。
Client Secret	应用的接口认证凭证密钥，从待绑定的认证源应用处获取。
授权方式	支持通过如下方式授权，可根据需要进行选择。 • Authorization Code：授权码方式，指第三方应用先申请一个授权码，然后再用该码获取令牌，适用于有后端的Web应用。 • Implicit：隐藏式授权，有些Web应用是纯前端应用，没有后端，这时就不能用Authorization Code方式，必须将令牌储存在前端，允许直接向前端颁发令牌。 • Resource Owner Password Credential：密码式授权，用户把用户名和密码直接告诉该应用，该应用就使用用户的密码申请令牌，适用于其他授权方式都无法采用的情况，而且必须是用户高度信任的应用。 • Client Credential：客户端凭证授权，适用于没有前端的命令行应用，即在命令行下请求令牌。这种方式给出的令牌，是针对第三方应用的，而不是针对用户的，即有可能多个用户共享同一个令牌。
关联属性	OIDC认证源对接OrgID的映射属性。支持选择：用户账户名、邮箱、手机号。
绑定属性	待绑定的认证源应用提供的用户属性字段，用于和OrgID的用户属性进行关联。
绑定策略	通过设置绑定策略，设置认证源下的用户是否关联系统用户还是新增用户作为第三方认证用户。支持选择：新增或绑定、绑定、新增。 当选择新增或绑定时，先关联系统用户，如果未关联到系统用户，则新增为第三方认证用户。
Issuer地址	Issuer地址，从待绑定的认证源应用处获取。

参数名称	参数说明
JWK Set地址	用于验证token的地址，从待绑定的认证源应用处获取。
用户信息地址	获取用户信息的地址，从待绑定的认证源应用处获取。
应用的全局退出地址	应用的全局退出地址，从待绑定的认证源应用处获取。
属性映射	可选项，用于关联OrgID和待绑定的认证源应用的用户属性。单击“添加映射”，在下拉框中选择固定属性或自定义属性。 • 固定属性：将第三方用户属性与系统用户属性做关联，需选择关联属性和映射属性。 • 自定义属性：自定义属性的固定值，需输入属性值和固定值。

----结束

添加 AD 认证源

AD是Active Directory的简称，即活动目录。您可以将AD简单理解成一个数据库，其存储有关网络对象的信息，方便管理员和用户查找所需信息。为方便企业用户的认证登录，OrgID通过LDAP协议把认证指向AD域，AD通过认证后，根据AD返回的用户属性与OrgID用户关联属性做匹配校验，验证通过即可登录OrgID。

步骤1 登录管理中心。

步骤2 选择左侧导航栏的“认证管理 > 认证源管理”。

步骤3 在组织认证源中，选择“AD”页签，单击“新增认证源”。

步骤4 进入“AD认证源绑定”界面，配置相关参数，参数说明如表10-6所示。

表 10-6 AD 认证源参数说明

参数名称	参数说明
显示名称	认证源的显示名称。如AD认证。
认证源图标	显示的认证源图标。必须为JPG、PNG格式，大小不超过20KB，尺寸240*240px。
服务器地址	指定AD服务器的地址。格式为ldap://*hostname*:*port*或ldaps://*hostname*:*port*。
管理员账号	输入具有管理员权限的AD账号。
管理员密码	输入管理员账号的密码。
Base DN	AD中的节点，会到该节点下认证用户。
用户ObjectClass	输入用户对象的对象类别名称，类似于user、person。

参数名称	参数说明
用户登录标识	标记登录的用户，登录标识的值与用户登录时的账号部分匹配。 如果以UPN（例如 "abc@examp.com"）为账号进行身份验证，则此字段通常必须设置为 userPrincipalName。否则，对于旧的NetBIOS风格的账号（例如 "abc"），则通常设为sAMAccountName。
关联属性	AD认证源对接OrgID的映射属性。支持选择：用户账户名、邮箱、手机号。
绑定属性	待绑定的认证源应用提供的用户属性字段，用于和OrgID的用户属性进行关联。
绑定策略	通过设置绑定策略，设置认证源下的用户是否关联系统用户还是新增用户作为第三方认证用户。支持选择：新增或绑定、绑定、新增。 当选择新增或绑定时，先关联系统用户，如果未关联到系统用户，则新增为第三方认证用户。
属性映射	可选项，用于关联OrgID和待绑定的认证源应用的用户属性。单击“添加映射”，在下拉框中选择固定属性或自定义属性。 • 固定属性：将第三方用户属性与系统用户属性做关联，需选择关联属性和映射属性。 • 自定义属性：自定义属性的固定值，需输入属性值和固定值。

----结束

更多操作

组织认证源添加成功后，您还可以进行以下操作。

表 10-7 组织认证源的更多操作

操作名称	操作步骤
启用/禁用组织认证源	开启：组织认证源添加成功后，默认自动开启。 禁用：在“认证管理 > 认证源管理”界面，在组织认证源模块指定认证源的“状态”列，关闭  ，在弹出的提示框中，单击“确认”。
更新组织认证源	在“认证管理 > 认证源管理”界面，单击操作列的“更新”，进入更新界面，根据所需修改组织认证源参数。
查看组织认证源详情	在“认证管理 > 认证源管理”界面，单击操作列的“查看详情”，进入查看详情界面，查看组织认证源详情。
删除组织认证源	在“认证管理 > 认证源管理”界面，单击操作列的“删除”，在弹出的提示框中，单击“确认”。 **删除后，该组织认证源的数据将被删除且不可恢复，请谨慎操作。**

10.2 区域范围管理

组织创建者或组织管理员可以添加区域范围，方便对OrgID进行访问控制。

添加区域范围

步骤1 登录管理中心。

步骤2 选择左侧导航栏的“认证管理 > 区域范围管理”。

步骤3 在区域范围管理页面，单击“添加区域”。

步骤4 在添加区域页面，输入区域信息，参数说明如表10-8所示，单击“保存”。

表 10-8 区域信息

参数名称	参数说明
区域名称	组织部门的分布区域命名，如开发区域。支持自定义。
区域网段	组织部门所在的具体IP范围，仅支持CIDR格式。不可重复。如0.0.0.0/0。
描述	区域的描述，支持自定义。

----结束

11 审计日志

11.1 管理操作日志

管理操作日志主要用于记录组织创建者或组织管理员的操作记录（如添加应用、添加部门等），便于日后的查询、审计和回溯。

查看管理操作日志

步骤1 登录管理中心。

步骤2 选择左侧导航栏的“审计日志 > 管理操作日志”。

步骤3 （可选）设置过滤条件。支持通过时间段和管理员用户名进行过滤。

步骤4 查看管理操作日志列表。每页最多显示50条日志。

----结束

11.2 登录登出日志

登录登出日志用于记录组织所有成员登录和登出OrgID的操作，可以了解组织的活跃度，便于日后回溯。

查看登录登出日志

步骤1 登录管理中心。

步骤2 选择左侧导航栏的“审计日志 > 登录登出日志”。

步骤3 （可选）设置过滤条件。支持通过时间段和操作员进行过滤。

步骤4 查看登录登出日志列表。每页最多显示50条日志。

----结束

12 组织管理

12.1 组织信息管理

12.1.1 修改组织信息

当组织信息（如组织logo、组织联系信息等）变更时，组织创建者或组织管理员可以在组织信息页面更新相关信息。

修改组织信息

步骤1 登录管理中心。

步骤2 选择左侧导航栏的“组织管理 > 组织信息”，即可查看组织信息。

步骤3 单击“更新”。

步骤4 修改组织基本信息和联系信息，单击“保存”。

----结束

12.1.2 申请组织成员配额

单个组织默认可以有200个成员，组织创建者或组织管理员可以通过配额申请扩大成员规模，每次申请增加100个成员配额，最大成员数不超过5000。

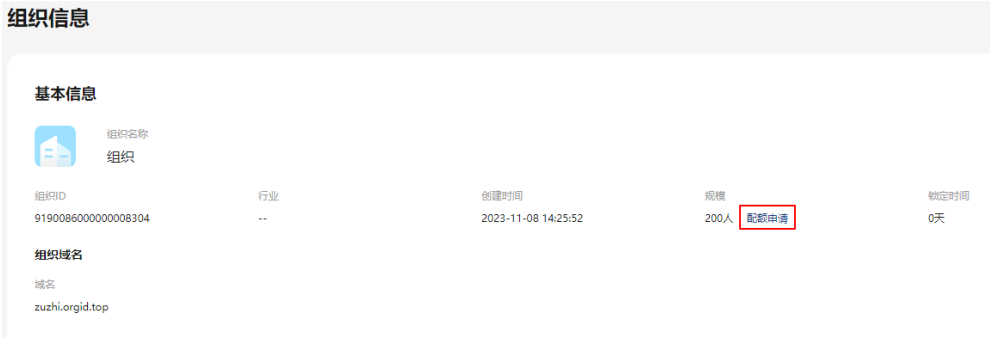
申请组织成员配额

步骤1 登录管理中心。

步骤2 选择左侧导航栏的“组织管理 > 组织信息”。

步骤3 单击基本信息模块中规模后的“配额申请”，如图12-1所示。

图 12-1 配额申请



步骤4 单击“确定”。

待OrgID人员审批通过后即可增加配额。

----结束

12.1.3 移交组织

组织创建者可以将组织移交给其他成员管理。移交组织后接受者将继承当前组织的所有权限，移交者将无法管理该组织，请谨慎操作。

移交组织

步骤1 登录管理中心。

步骤2 选择左侧导航栏的“组织管理 > 组织信息”。

步骤3 单击移交组织模块中的“移交”。

步骤4 在提示页面单击“确认”。

步骤5 在“移交组织”页面，填写接收者的姓名并选择验证方式，支持手机号验证和邮箱验证，选择后需要填写手机号或者邮箱，并选择是否需要自动退出组织。

步骤6 单击“确认”。

根据选择的验证方式给接收者发送验证短信或验证邮件，三天内有效，等待接收者验证后，组织移交成功。

如果选择自动退出组织，在组织移交成功后，移交者自动退出该组织。

----结束

12.1.4 解散组织

仅组织创建者可以解散组织，解散组织后该组织的所有数据会被删除，且该操作不可撤销，请谨慎操作。

解散组织

步骤1 登录管理中心。

步骤2 选择左侧导航栏的“组织管理 > 组织信息”。

步骤3 单击解散组织模块中的“解散”。

步骤4 单击“确认”。

----结束

12.2 数据报表

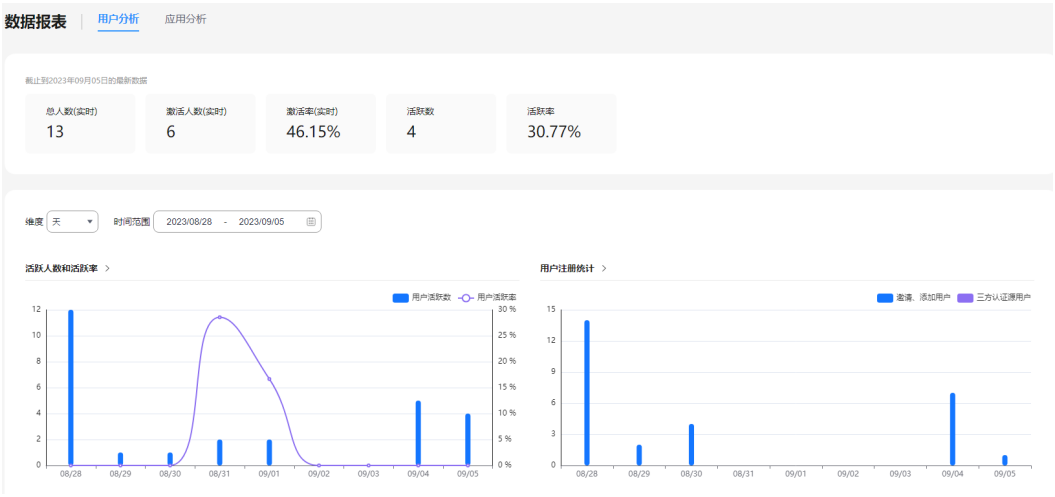
OrgID提供对用户、应用的数据分析能力，可视化显示分析数据，方便管理员了解用户和应用的实时数据，以及所选时间范围的分析数据。

查看用户分析报表

步骤1 登录管理中心。

步骤2 选择左侧导航栏的“组织管理 > 数据报表”，默认进入“用户分析”页签。在“用户分析”页签查看用户分析报表，如图12-2所示。

图 12-2 用户分析



具体展示内容如下：

- 最新的用户数据及激活、活跃数据统计，数据如表12-1所示。

表 12-1 用户分析数据

数据名称	数据说明
总人数(实时)	组织下实时的用户总人数。
激活人数(实时)	组织下实时的用户激活人数，加入组织的用户完成首次登录即状态已激活，统计激活人数。
激活率(实时)	组织下实时的用户激活人数与总人数的比值。

数据名称	数据说明
活跃数	截止时间内用户的活跃数，用户登录即表示用户活跃，统计活跃数。
活跃率	截止时间内用户的活跃数与截止时间内用户总人数的比值。

- 所选维度与时间范围内，活跃人数和活跃率、用户注册统计、用户删除统计的统计图。默认显示近9天内的统计数据。
  - 维度：可选天、周、月。
  - 时间范围：当维度为天时，时间范围最多可选9天；当维度为周时，时间范围最多可选8周；当维度为月时，时间范围最多可选6个月。
  - 统计图表：展示活跃人数和活跃率、用户注册统计、用户删除统计的统计图。

步骤3 单击图表名称进入图表详情页面，查看该统计图和所选维度、时间范围内的数据列表。

可以重新选择维度与时间范围，也可以单击页面右上角“导出”，导出该报表。

----结束

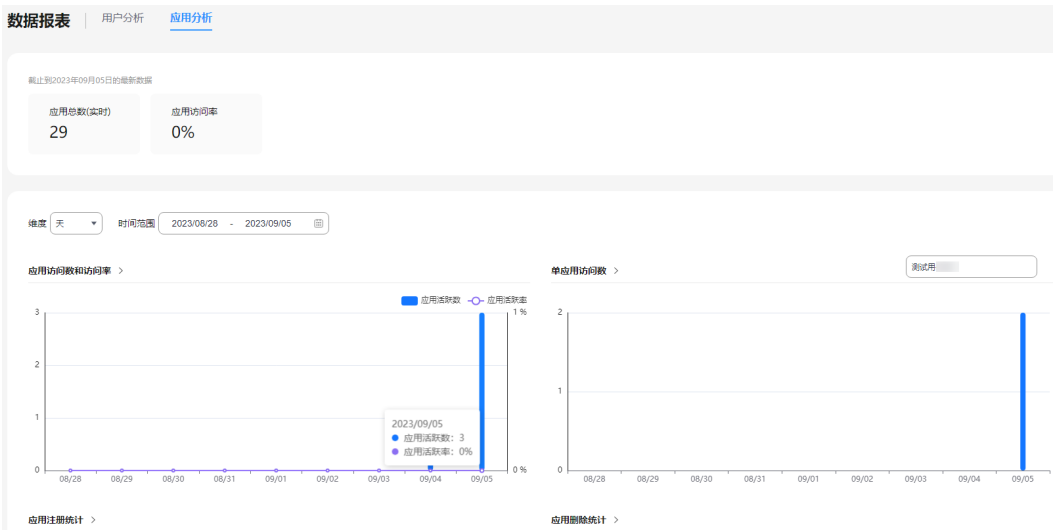
查看应用分析报表

步骤1 登录管理中心。

步骤2 选择左侧导航栏的“组织管理 > 数据报表”，默认进入“用户分析”页签。

步骤3 单击“应用分析”，在“应用分析”页签查看应用分析报表，如图12-3所示。

图 12-3 应用分析



具体展示内容如下：

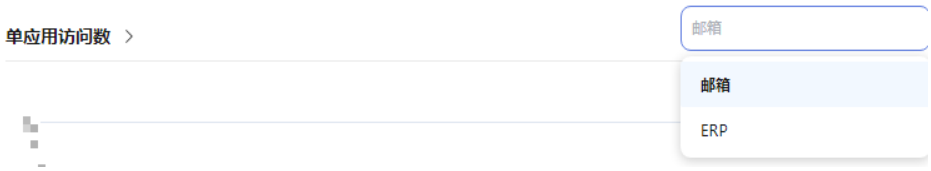
- 最新的应用数据统计，数据如表12-2所示。

表 12-2 应用分析数据

数据名称	数据说明
应用总数(实时)	组织下实时的应用总数。
应用访问率	截止时间内被访问应用数与截止时间内应用总数的比值。

- 所选维度与时间范围内，应用访问数和访问率、单应用访问数、应用注册统计、应用删除统计的统计图。默认显示近9天内的统计数据。
  - 维度：可选天、周、月。
  - 时间范围：当维度为天时，时间范围最多可选9天；当维度为周时，时间范围最多可选8周；当维度为月时，时间范围最多可选6个月。
  - 统计图表：展示应用访问数和访问率、单应用访问数、应用注册统计、应用删除统计的统计图。其中单应用访问数需选择具体应用，如图12-4所示，默认显示最新创建的应用的访问数。

    图 12-4 选择应用

步骤4 单击图表名称进入图表详情页面，查看该统计图和所选维度、时间范围内的数据列表。

可以重新选择维度与时间范围，也可以单击页面右上角“导出”，导出该报表。

----结束

12.3 域名管理

OrgID支持多域名管理，组织创建者或组织管理员可以为组织添加自有域名并验证，添加后可以用作管理员为成员创建管理式华为账号的后缀。

约束限制

- 每个组织最多支持管理3个域名，即除创建组织时设置的域名，最多可以添加2个域名。
- 域名添加后不支持修改和删除。
- 域名添加后，需要在试用期（180天）内完成域名验证。若在试用期内未完成域名验证，域名会被冻结，冻结后将无法使用该域名作为管理式华为账号的后缀。

添加域名

步骤1 登录管理中心。

步骤2 选择左侧导航栏的“组织管理 > 域名管理”。

步骤3 单击页面右上角“添加域名”。

步骤4 输入组织域名，单击“确定”。

添加完成后该域名会展示在域名列表中。

----结束

验证域名

步骤1 **登录管理中心**。

步骤2 选择左侧导航栏的“组织管理 > 域名管理”。

步骤3 在域名列表中单击已添加的域名所在行后的“验证”，进入“域名验证”页面，根据指引完成验证。

1. 设置域名，默认为已选择的待验证域名，单击“下一步”。
2. 按照界面步骤添加MX记录，如**图12-5**所示，添加完成后单击“下一步”。

图 12-5 域名验证

3. 检查设置，检查通过后即完成域名验证。

----结束

13 权限与审批

13.1 我的审批

成员获取到OrgID的SaaS应用的首页URL后，可以提供SaaS应用的登录入口给其他用户。用户登录后系统自动识别用户权限，根据用户访问权限的不同，可分为以下三种情况。

- 用户已加入本组织，且应用已授权给该用户。
- 用户已加入本组织，但应用并未授权给该用户。
- 用户未加入本组织。

已加入本组织，且应用已授权

如果该用户已加入本组织，访问应用URL后可直接输入华为账号及密码登录并访问应用。

已加入本组织，但应用未授权

如果该用户已加入本组织，但是没有权限访问该应用时，请参见以下步骤：

步骤1 输入华为账号及密码登录应用首页，页面提示用户应用授权申请已发送，请耐心等待管理员审批。

步骤2 管理员在管理中心接收到应用授权申请，可在“权限与审批 > 我的审批”中查看并通过或驳回该申请。还可单击申请单号进入查看并审批单。

步骤3 若申请通过，用户可重新登录后访问该应用；若申请驳回，用户可登录后单击“重新申请”再次发起申请。

----结束

未加入本组织

如果该用户尚未加入本组织，请参见以下步骤：

步骤1 输入华为账号及密码登录应用首页，页面提示用户加入组织申请已发送，请耐心等待管理员审批。

步骤2 管理员在管理中心会接收到加入组织及应用授权两个申请，可在“权限与审批 > 我的审批”中查看并通过或驳回该申请。

管理员需先审批用户加入组织的申请，才能审批应用授权的申请。

步骤3 若申请通过，用户可重新登录后访问该应用；若申请驳回，用户可登录后单击“重新申请”再次发起申请。

----结束

13.2 岗位管理

OrgID支持对组织成员进行岗位管理，创建并定义岗位的角色范围，并为岗位添加成员，指定岗位成员可操作的应用及权限范围。

创建岗位

步骤1 登录管理中心。

步骤2 选择左侧导航栏的“权限与审批 > 岗位管理”。

步骤3 单击“创建岗位”，参数说明如表13-1所示，然后单击“确定”。

表 13-1 创建岗位参数说明

参数名称	参数说明
岗位编码	自定义岗位编码，最多可输出64个字符。
岗位名称	自定义岗位名称，最多可输出32个字符。
岗位描述	填写岗位描述，最多可输出256个字符。
角色范围	勾选岗位需要添加的角色，可使用应用名称或角色名称进行搜索。

----结束

添加成员

步骤1 在“岗位管理”页面，单击已创建的岗位所在行“操作”列的“添加成员”。

步骤2 在“添加成员”页面，勾选需要授权的成员，单击“下一步”。

步骤3 选择角色的有效期，自建应用的角色还需要选择角色数据范围，然后单击“完成”。

----结束

更多操作

您还可以进行以下操作。

表 13-2 更多操作

操作名称	操作步骤
编辑岗位	1. 在“岗位管理”页面，单击岗位所在行“操作”列的“编辑”。 2. 编辑岗位信息，可以修改岗位名称、岗位描述和角色范围，然后单击“确定”。
查看岗位详情	在“岗位管理”页面，单击岗位所在行“操作”列的“查看详情”，可以在详情页面查看该岗位的成员和该岗位拥有的角色。
修改成员角色的有效期和数据范围	1. 在“岗位管理”页面，单击岗位所在行“操作”列的“查看详情” 2. 在成员列表，单击待修改的成员所在行“操作”列的“查看”。 3. 单击“查看成员角色”页面下方的“修改”。 4. 修改成员已拥有的角色的有效期和应用角色的数据范围，然后单击“确定”。
移除成员	1. 在“岗位管理”页面，单击岗位所在行“操作”列的“查看详情”。 2. 在成员列表，单击待移除的成员所在行“操作”列的“移除”。 3. 单击“确认”。
添加岗位角色	1. 在“岗位管理”页面，单击岗位所在行“操作”列的“查看详情”。 2. 单击“角色范围”，切换至“角色范围”页签。 3. 单击“添加角色”。 4. 勾选需要添加的角色，然后单击“确定”。
删除岗位角色	1. 在“岗位管理”页面，单击岗位所在行“操作”列的“查看详情”。 2. 单击“角色范围”，切换至“角色范围”页签。 3. 在角色列表，单击待删除的角色所在行“操作”列的“删除”。 4. 单击“确认”。
删除岗位	1. 在“岗位管理”页面，单击岗位所在行“操作”列的“删除”。 2. 单击“确认”。

13.3 角色授权

管理员可以为OrgID应用角色及自建应用新增的角色添加成员。OrgID应用角色指当前组织的OrgID管理中心的角色，包括组织管理员和部门管理员。添加成员后，成员拥有对应应用及角色的权限。

为角色添加成员

步骤1 登录管理中心。

步骤2 选择左侧导航栏的“权限与审批 > 角色授权”。

角色列表中展示OrgID管理中心角色，和自建应用已新增的角色。

步骤3 在角色列表中，单击需授权角色所在行“操作”列的“添加成员”。

步骤4 在“添加成员”页面，勾选需要授权的成员，单击“下一步”。

步骤5 选择角色的有效期，自建应用的角色还需要选择角色数据范围，然后单击“完成”。

----结束

更多操作

您还可以进行以下操作。

表 13-3 更多操作

操作名称	操作步骤
修改成员角色的有效期和数据范围	1. 在“角色授权”页面，单击角色所在行“操作”列的“查看详情”。 2. 在成员列表，单击待修改的成员所在行“操作”列的“查看”。 3. 单击“查看成员角色”页面下方的“修改”。 4. 修改成员已拥有的角色的有效期和自建应用角色的数据范围。 5. 单击“保存”。
移除成员	1. 在“角色授权”页面，单击角色所在行“操作”列的“查看详情”。 2. 在成员列表，单击待移除的成员所在行“操作”列的“移除”。 3. 单击“确认”。

14 系统管理

14.1 用户属性配置

成员详情界面可以通过自定义创建用户属性来灵活拓展成员信息。

添加用户属性

步骤1 登录管理中心。

步骤2 选择左侧导航栏的“系统管理 > 用户属性配置”。

步骤3 单击“添加属性”，参数说明如下表14-1所示。

只有属性展示名支持修改，其他参数不支持修改，请谨慎填写。

表 14-1 添加属性参数说明

参数名称	参数说明
属性展示名	在成员扩展属性中显示的名称。
属性名称	设置属性名称，关联OrgID和第三方系统成员模型之间属性的对应关系。
属性类型	可选择文本框、下拉框-单选、下拉框-多选、日期。
是否必填	选择该属性是否属于必填项。
是否敏感数据	仅当属性类型为文本框时，需选择输入后的数据是否需要密文展示。
下拉框候选值	仅当属性类型为下拉框-单选、下拉框-多选时，需要填写该项。候选值之间使用|隔开，例如：选项A|选项B。

步骤4 单击“确定”后保存，添加的所有属性展示在成员属性配置列表下，如图14-1所示。可在“状态”列设置该属性是否在成员详情页面展示。

图 14-1 成员属性配置

----结束

14.2 获取组织凭证

组织创建者或组织管理员可以获取组织凭证，用于调用OrgID服务已订阅的开放API接口。

获取组织凭证

步骤1 登录管理中心。

步骤2 选择左侧导航栏的“系统管理 > 凭证管理”，进入“凭证管理”页面。

步骤3 单击Client ID后的“查看”，可以获取Client ID。

步骤4 单击Client Secret后的“复制”，可以获取Client Secret。

Client Secret仅支持复制一次，复制后请妥善保管，如遗忘，可以单击“重置”，重置Client Secret后再重新复制。

----结束

15 任务中心

15.1 我的导入

管理员可以使用模板批量配置自建应用的角色，导入模板文件的任务执行状态可以在“我的导入”页面查看。支持查看任务详情或者下载原始导入文件。

查看导入任务

步骤1 登录管理中心。

步骤2 选择左侧导航栏的“任务中心 > 我的导入”。

在导入任务列表中，查看导入任务状态及结果。

步骤3 （可选）可以设置任务的开始日期和结束日期范围，或者任务状态筛选需查看的任务。

步骤4 （可选）可单击  刷新任务状态。

步骤5 在导入任务列表中，单击任务单号或者任务所在行的“查看详情”。

可以在“任务详情”页面查看任务信息及执行结果，如果任务执行失败可以在该页面查看失败原因。

----结束

下载原始文件

步骤1 登录管理中心。

步骤2 选择左侧导航栏的“任务中心 > 我的导入”。

步骤3 在导入任务列表中，单击任务所在行的“文件下载 > 原始文件”。

即可下载该任务导入时使用的原始文件。

----结束

15.2 我的导出

管理员可以全量导出自建应用的角色配置信息，导出文件的任务执行状态可以在“我的导出”页面查看，已完成的导出任务可以下载导出的文件。

查看导出任务

步骤1 **登录管理中心**。

步骤2 选择左侧导航栏的“任务中心 > 我的导出”。

在导出任务列表中，查看导出任务状态及结果。

步骤3 （可选）可以设置任务的开始日期和结束日期范围，或者任务状态筛选需查看的任务。

步骤4 （可选）可单击  刷新任务状态。

----结束

下载导出文件

步骤1 **登录管理中心**。

步骤2 选择左侧导航栏的“任务中心 > 我的导出”。

步骤3 在导出任务列表中，单击任务所在行的“文件下载”。

即可下载该任务导出的文件。

----结束

16 权限管理

OrgID支持权限管理，可以进行权限申请、变更、和取消的操作。

申请权限

步骤1 访问**OrgID**，进入用户中心首页。

步骤2 在OrgID右上角账号名下拉列表中选择“我的权限”，进入“权限管理”页面，默认显示“我的权限”页签。

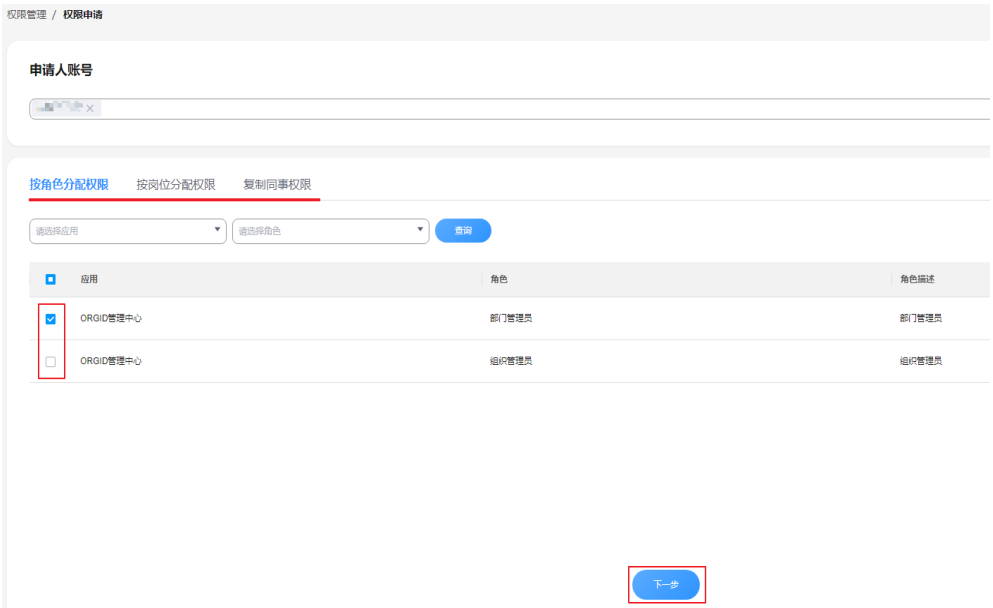
步骤3 单击“申请权限”。

步骤4 确认申请人账号，显示当前账号的姓名。

支持为其他成员申请权限，可在输入框中输入成员姓名并勾选该成员。

步骤5 勾选需要申请的权限，然后单击“下一步”。

图 16-1 申请权限



支持按照以下方式进行选择：

- 按角色分配权限：申请应用对应的角色权限，可申请OrgID管理中心的部门管理员、组织管理员和自建应用配置的角色。
- 按岗位分配权限：申请岗位权限，可申请岗位下全部应用角色权限，也可申请部分应用角色权限。
- 复制同事权限：输入同事姓名进行搜索，复制同事已有权限。

步骤6 设置权限有效期，自建应用配置的角色还需要设置数据范围，填写申请原因，然后单击“提交”。

提交后，会进入用户中心，在“我的申请”中显示已提交的申请，可单击操作列“查看详情”，查看申请详情，也可以撤销该申请。

----结束

变更权限

步骤1 访问**OrgID**，进入用户中心首页。

步骤2 在右上角账号名下拉列表中选择“我的权限”，进入“权限管理”页面，默认显示“我的权限”页签。

步骤3 在我的权限列表，勾选需要变更有效期或者数据范围的权限，然后单击列表上方的“变更权限”。

步骤4 设置权限有效期，自建应用配置的角色还可以修改数据范围，填写申请原因，然后单击“提交”。

提交后，会进入用户中心，在“我的申请”中显示已提交的申请，可单击操作列“查看详情”，查看申请详情，也可以撤销该申请。

----结束

取消权限

步骤1 访问**OrgID**，进入用户中心首页。

步骤2 在右上角账号名下拉列表中选择“我的权限”，进入“权限管理”页面，默认显示“我的权限”页签。

步骤3 在我的权限列表，勾选需要取消的权限，然后单击列表上方的“取消权限”。

步骤4 单击“确定”。

----结束

查看权限变更记录

步骤1 访问**OrgID**，进入用户中心首页。

步骤2 在右上角账号名下拉列表中选择“我的权限”，进入“权限管理”页面，默认显示“我的权限”页签。

步骤3 单击“权限变更记录”，切换至“权限变更记录”页签。

在列表中查看权限变更记录，也可以设置变更的开始日期和结束日期进行查询。

----结束

17 开通联邦认证

个人华为账号无法直接访问组织已开通或购买的华为云资源时，组织创建者可以为组织开通联邦认证，开通联邦认证后授权用户，让用户可以通过联邦认证访问组织的华为云资源。

前提条件

已**创建组织**。

开通联邦认证

步骤1 登录**华为云OrgID控制台**。

步骤2 将鼠标放置在待开通联邦认证的组织上，单击“开通联邦认证”。

开通成功后，系统会自动创建一个与该组织同名的联邦认证用户组和已经授权该用户组访问的华为云联邦应用，用户组成员可通过应用访问华为云资源。

----结束