应用身份管理服务

用户指南

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 使用前必读

OneAccess使用对象有企业管理员和普通用户两种。

- 企业管理员：主账号或拥有OneAccess管理权限的用户。企业管理员负责用户（组）、组织、应用、及API等实体的管理。如果您是企业管理员，请参考**企业管理员指南**使用OneAccess。
- 普通用户：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平台访问应用。如果您是普通用户，请参考**普通用户指南**使用OneAccess。

说明

OneAccess当前仅在华东-上海一Region支持，且需要申请开启白名单。

2 购买实例

在使用应用身份管理服务前，需要按照指引购买实例。

- **注册账号并实名认证**
- **为账户充值**
- **购买实例**

注册账号并实名认证

如果您已有一个账号，请直接**购买实例**。如果还没有华为账号，请参考以下步骤创建。

步骤1 打开**https://www.huaweicloud.com/intl/zh-cn/**，单击“注册”。

步骤2 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。

步骤3 完成**个人实名认证**，或**企业实名认证**。

----结束

为账户充值

购买应用身份管理服务实例，需要确保您的账户有足够金额。若您账号里有足够的余额，可略过此部分内容。

- 关于应用身份管理服务的计费标准，请参见购买页实际显示价格。
- 关于充值，请参见“**如何给华为云账户充值**”。

购买实例

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。

购买OneAccess实例，即可使用OneAccess。

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。
3. 在“用户数”中可拖动滚动条设置用户数。

   说明

   - 当实例规格为“基础版”时，用户数支持选择100或500。
   - 当实例规格为“专业版”时，可拖动滚动条设置用户数。用户数支持设置200或1000~10000之间，其中1000~10000之间用户数设置是以1000为步长步进式增长。如需购买用户数为10000以上的专业版实例时，请**提交工单**。
   - 当实例规格为“企业版”时，用户数固定为40,000，不支持设置。

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。

   说明

   当实例规格为“企业版”时，实例数为1，且不支持设置。

步骤3 输入管理员密码和确认密码。账号默认为开通租户的账号名。密码长度为8至18位，至少包含以下字符中的3种：数字、大写字母、小写字母和特殊字符-+~!@#$%^&*,:;<=>_?`./。

说明

实例规格为“企业版”时需要执行此步骤。

步骤4 单击“下一步：确认配置”。

步骤5 勾选“我已阅读并同意《OneAccess服务声明》”，单击“立即购买”。

说明

- 当实例规格为“基础版”或“专业版”时，购买完成，开始发放OneAccess实例，实例创建完成，会自动生成用户访问域名。
- 当实例规格为“企业版”时，购买完成后，需**提交工单**开通企业版实例。

----结束

3 实例管理

本文介绍华为云账号对购买的OneAccess实例的操作指导。华为云账号可使用OneAccess的功能，子账号或委托账号需要实例授权后才能使用OneAccess的功能。

新增授权

通过新增授权，您可以授权IAM用户访问OneAccess实例的管理门户进行管理。

说明

OneAccess“实例授权”可支持授权50个IAM用户访问OneAccess服务的权限。

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. 单击待操作的OneAccess实例。
4. 单击“实例授权”，进入实例授权页面。
5. 单击“新增授权”，在弹出框中选择IAM用户。
6. 单击“确定”，完成IAM用户授权操作。

说明

- IAM用户进入OneAccess管理门户后，无“安全 > 管理员权限”页签的查看权限。其他操作可参考**企业管理员指南**。
- 如需IAM用户拥有OneAccess服务的所有权限，请授予“OneAccess FullAccess”权限。

移除权限

如您需要解除某个IAM用户访问“实例名称”的权限，可以进行如下操作

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. 单击待操作的OneAccess实例。
4. 单击“实例授权”，进入实例授权页面。
5. 单击IAM用户名称操作列的“移除”。
6. 在弹出框中单击“确定”，则该IAM用户不再有访问该实例管理门户的权限。

自定义域名

可以按照企业用户的喜好自定义域名。

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. 单击待操作的OneAccess实例。
4. 单击“自定义域名”进入自定义域名页面。
5. 在“域名”输入框输入自定义域名，其中自定义域名必须为子域名。
6. 单击“下一步：域名验证”，在“验证域名”页面，单击“验证”完成TXT类型的记录验证。
7. 完成验证后，单击“下一步：上传证书”，将证书信息上传完成。
8. 单击“完成配置”则自定义域名配置完成。

变更规格

OneAccess管理控制台支持变更实例的规格，即可将基础版变更为专业版，也可变更实例的用户数，但用户数只能增加，不可减少。

说明

企业版不支持变更规格，也不支持将基础版或专业版变更为企业版。

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. 在待变更规格的OneAccess实例右侧“操作”列单击“变更规格”，进入变更规格页面。也可单击待操作的OneAccess实例进入实例详情页面，单击“变更规格”进入变更规格页面。
4. 选择合适的实例规格。

   说明

   - 变更规格操作只能增加用户数，不可减少用户数，且专业版也不可变更为基础版。
   - 若原实例规格为基础版且用户数为100时，支持变更为用户数为500的基础版，也可变更为专业版且可设置用户数。
   - 若原实例规格为基础版且用户数为500时，则只能变更为专业版且只能设置用户数为1000~10000之间。
5. 单击“下一步：确认配置”,确认变更后的规格信息。
6. 单击“立即变更”，完成规格变更。

续费与退订实例

- 购买OneAccess实例，只有包年/包月一种计费模式，当购买的OneAccess实例到期后，请在OneAccess华为云控制台单击“续费”进行续费操作，也可在管理控制台**续费管理**页面进行续费操作，详细操作请参考**续费管理**。
- 客户购买包年/包月资源后，如需停止使用，请在OneAccess控制台，单击“退订”执行退订操作。退订资源实例包括资源续费部分和当前正在使用的部分，退订后资源将无法使用。退订资源实例需收取手续费。可在OneAccess华为云控制台单击“退订”进行退订实例操作

4 企业管理员指南

4.1 登录 OneAccess 管理门户

本文介绍管理员如何在开通OneAccess服务后，登录到OneAccess的管理门户。

前提条件

- 请确保您已注册华为账号并实名认证。
- 请参考**购买实例**已购买实例。

操作步骤

进入OneAccess管理门户可以有如下两种方式：

- 管理员通过控制台进入OneAccess管理门户。
  a. 登录华为云控制台。
  b. 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。
  c. 在实例列表页面，单击待访问的OneAccess实例。
  d. 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，请参考**授权IAM用户访问OneAccess实例**。
- 管理员通过访问域名方式登录OneAccess管理门户。
  a. 登录华为云控制台。

b. 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。
c. 单击待访问的OneAccess实例。
d. 获取管理员访问域名。

图 4-1 获取管理员访问域名

说明

管理员访问域名即为账号在购买OneAccess实例时生成的“用户访问域名”。

e. 参考**管理管理员权限**添加管理员。
f. 管理员访问“管理员访问域名/admin”，如：https://example.com/admin，进入OneAccess管理门户登录页面。
g. 输入管理员用户名和密码，单击“登录”，进入OneAccess实例管理门户。

4.2 用户管理

4.2.1 管理用户

在OneAccess管理门户，您可以进行添加、编辑、修改、删除用户等操作。

如果需要添加大量用户，建议采用身份源同步、数据导入的方式批量添加。

- 身份源同步：从身份源同步用户数据到OneAccess，在高级配置中可以对同步的处理逻辑进行灵活配置，实现将上游身份源数据同步至OneAccess。具体可参考**身份源管理**。
- 数据导入：将用户信息按照模板进行整理，并将其导入OneAccess，即可批量导入用户。具体可参考**用户导入**。

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。

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4-1**填写用户基本信息。

表 4-1 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**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。
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 若需开启密码登录，则执行该步骤，单击  开启密码登录。当前密码登录有两种方式。

- 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 若想添加用户的工作信息，则在“添加用户”页面单击“填写更多信息”参考**表4-2**填写用户工作信息。

表 4-2 工作信息

工作信息属性	属性含义
工号	用户工号，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
直属上级	输入该用户的直属上级，可通过**修改用户属性**设置该属性是否为必填。
人员类型	可选择人员类型，包括正式、实习、劳务派遣、劳务外包。
入职时间	设置用户的入职时间，可通过**修改用户属性**设置该属性是否为必填及时间范围。
工作所在地	设置用户工作所在地，可通过**修改用户属性**设置该属性是否为必填及字符长度范围。

说明

用户信息包含基本信息属性和工作信息属性，所有属性均可以通过**用户属性定义**进行设置，具体可参考**用户属性定义**。

步骤7 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

查看用户详情

在用户列表中，单击用户名，可以查看用户详情。包括用户信息、所属用户组、已授权应用和审计日志。

- 用户信息

  包含用户基本属性和扩展属性信息。

- 所属用户组
  - 用户所属用户组信息，包括用户组名称、用户组授权应用、组织路径。
  - 单击用户组列表右上方的“加入组”，勾选需要加入的用户组，即可将用户加入用户组，您还可以通过**用户加入用户组**操作完成。如果应用开启了基于用户组的自动授权策略，将用户加入已授权的用户组，会同步至应用侧，具体可参考**应用账号授权策略**。
  - 单击操作列的“删除”，可将用户从该用户组中删除。

    如果应用开启了基于用户组的自动授权策略，将删除已授权用户组中的用户，会同步至应用侧，具体可参考**应用账号授权策略**。

- 已授权应用
  - 用户在已授权应用中的信息，包括应用图标、应用名称、应用账号等。
  - 单击已授权应用列表右上方的“应用授权”，勾选需要授权的应用，即可为用户进行应用授权，您还可以通过**为用户授予应用的使用权限**操作完成。
  - 如果应用开启了应用侧权限，单击操作列的“应用侧角色/权限”，可对该用户进行授权，在该处授权的操作方法与在应用账号处类似，可参考**应用侧角色/权限**。应用侧权限的配置可参考**管理应用侧权限**。
  - 单击操作列的“删除”，可取消对该用户的授权。

- 审计日志

  审计日志记录了企业管理员与用户的操作记录，包括管理员日志、用户日志。
  - 管理员日志

    通过管理员日志可以查看管理员对该用户的操作，如修改密码、应用授权等。同时，可根据条件过滤。
  - 用户日志

    通过用户日志可以查看用户访问用户门户和应用的操作，如SSO登录、登出等。同时，可根据条件过滤。

编辑用户信息

步骤1 在用户列表中，鼠标放置在用户名右侧状态栏下方单击，弹出“编辑用户”弹框。

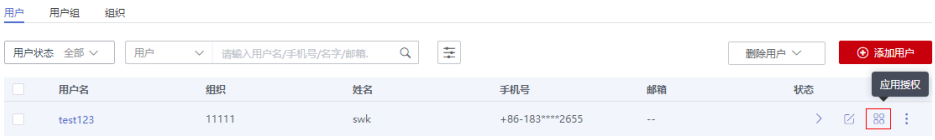
步骤2 修改用户的基本信息和更多信息，包括修改用户所属组织，如将多组织调整为单组织，或将单组织调整为多组织。

步骤3 单击“确定”。

----结束

为用户授予应用的使用权限

步骤1 在用户列表中，鼠标放置在用户名右侧状态栏下方，单击进入用户详情的“已授权应用”页签。如需添加应用，可参考**集成企业应用**。



步骤2 在用户详情的“已授权应用”页签，单击“应用授权”。

步骤3 在应用授权页面，勾选需要授权的应用，单击“确定”，完成用户授权。在已选应用列表中，可编辑应用账号，如需编辑应用账号的其他属性，单击应用名称，进入应用账号信息页面，即可编辑。系统默认用户名为应用账号名。如需在应用中对用户授权，请参考**授权管理**。

----结束

修改用户所属组织

通过调整组织：

- 可变更用户所属组织。
- 可将只属于一个组织的用户修改为属于多个组织。

- 可将属于多组织的用户修改为只属于一个组织。

步骤1 在用户列表中，鼠标放在待操作用户的状态栏，单击用户后的，选择“ 调整组织”。

步骤2 在调整组织弹框，选择您要调整的目标组织。可选择一个目标组织，也可同时选中几个组织。默认先选中的组织为主组织。当设置为多组织时，可通过单击目标组织后的“设为主组织”将其设置为主组织。

步骤3 单击“确定”，完成修改。

说明

如果应用开启了**用户自动授权功能**，修改用户所属组织会修改用户的应用访问权限。具体可参考**应用账号授权策略**。

----结束

用户加入用户组

步骤1 在用户列表中，单击某一用户后的，单击“用户组”进入用户详情的“所属用户组”页签。

步骤2 在用户详情页面，单击右侧的“加入组”。

步骤3 在选择用户组弹框，勾选需要加入的用户组，单击“确定”，即可将用户加入用户组。单击操作列的“删除”，可将用户从该用户组中删除。

----结束

用户密码管理

密码生成方式有“自定义”和“自动生成”两种方式，可通过这两种方式对用户密码进行修改、重置管理。其密码设置规范请参考**管理密码策略**。

- 自定义方式。
  a. 在用户列表中，单击某一用户后的，选择“密码管理”打开“密码管理”弹框。
  b. 选择密码生成方式，默认选择“自定义”，输入用户密码可自定义用户的登录密码。
     - 默认选中“首次登录时修改密码”，则该用户在使用新密码首次登录用户门户时，会强制要求用户修改密码。
     - 不选择“首次登录时修改密码”，则该用户在使用新密码首次登录用户门户时，不用修改密码。

  图 4-2 自定义

  c. 单击“确定”，用户密码管理完成。
- 自动生成方式。
  a. 在用户列表中，单击某一用户后的，单击“密码管理”打开“密码管理”弹框。
  b. 选择密码生成方式，选择“自动生成”。

图 4-3 自动生成

c. 选择“通知方式”和“发送语言”。根据您选择的通知方式，用户会收到重置密码的短信、邮件通知类消息，用户使用新密码可以登录用户门户。

说明

- 重置密码后，用户以密码方式首次登录用户门户时，会强制要求修改密码，其密码规范要求可参考**管理密码策略**。
- 如果您需要使用邮件方式通知用户，请配置邮件网关，具体方法请参考**邮件网关配置**。

d. 单击“确定”，用户密码管理完成。

删除用户

步骤1 在用户列表中，单击某一用户后的 ，单击“删除”。

步骤2 单击“确定”，删除用户。

说明

请谨慎删除用户，删除以后该用户无法访问用户门户，如有需要请再次添加，具体可参考**添加用户**。

----结束

禁用用户

说明

请谨慎禁用用户，禁用以后该用户将无法访问用户门户。

步骤1 在用户列表中，单击目标用户状态列的 。对于新创建的用户，用户状态默认为启用。

图 4-4 禁用用户

步骤2 在提示窗口中，单击“确定”，页面提示禁用成功。

----结束

启用用户

步骤1 在用户列表中，单击被禁用的目标用户状态列的 。

图 4-5 启用用户

步骤2 在提示窗口中，单击“确定”，页面提示启用成功。

----结束

4.2.2 管理组织

在OneAccess管理门户，您可以创建组织，并将用户加入到相应的组织中，实现用户批量管理和授权。同时，可以根据需要添加、修改、移动、删除组织。基于组织的授权请参考**应用机构授权策略**。

如果您需要添加大量的组织，建议采用身份源同步、数据导入的方式批量添加。

- 身份源导入：从身份源同步组织信息到OneAccess，在高级配置中可以对同步的处理逻辑进行灵活配置，实现将上游组织数据同步至OneAccess。具体可参考**管理身份源**。
- 数据导入：将组织信息按照模板进行整理，并将其导入OneAccess，即可批量导入组织。具体可参考**导入组织**。

添加组织

组织为树状结构，您可以添加顶层组织，也可以添加子组织。

步骤1 登录OneAccess管理门户。

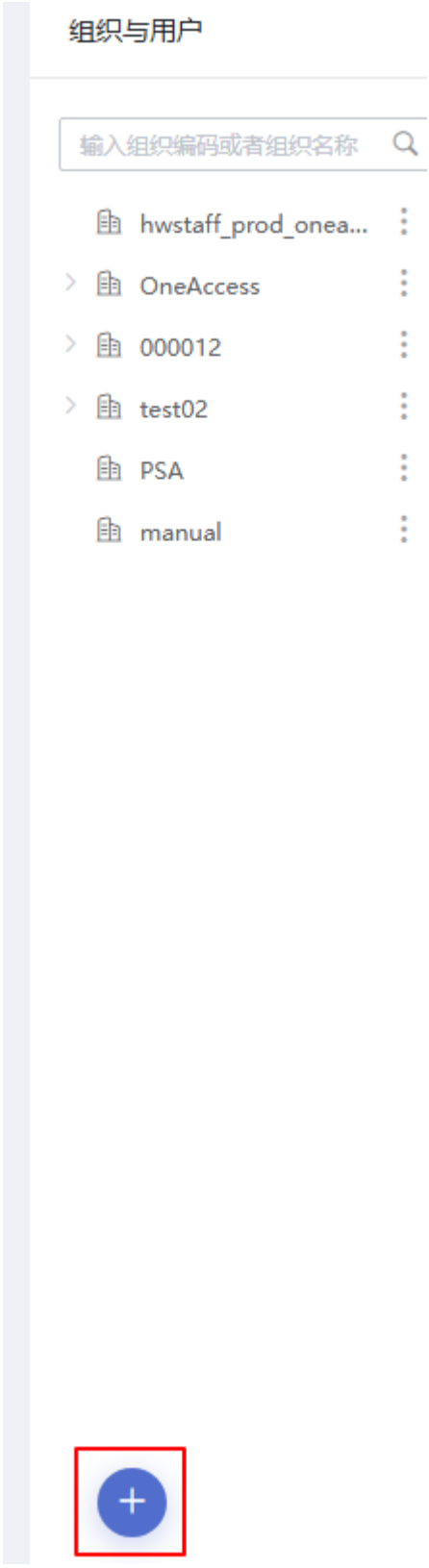
步骤2 在导航栏中，选择“用户 > 组织与用户”。

步骤3 在组织与用户页面，切换“组织”页签。

步骤4 在组织列表页面，单击“添加组织”。

说明

- 在组织与用户页面，可单击如下图标快速添加顶层组织。



- 在左侧组织树上，单击组织右侧的 ，选择“ 添加子组织”，如图4-6，可快速为其添加子组织，也可在左侧组织导航中，选择已添加的顶层组织，并单击“添加组织”为其添加子组织。

图 4-6 添加子组织

步骤5 在添加组织页面，输入组织信息。

表 4-3 组织信息

组织信息	说明
* 组织类型	可通过下拉框设置组织属于的类型，包括：部门、单位、公司和集团。
* 组织编码	组织的唯一标识，不可与其他组织重复。
* 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	组织在组织树中的显示位置，系统默认添加到本层次最后面，可修改。
上级组织	• 当添加顶层组织时，此参数置空。 • 当添加子组织时，默认为选择的上级组织。

步骤6 单击“确定”，添加组织完成。组织列表中显示已添加的组织。

----结束

查看组织详情

在组织列表中，单击需要查看的组织编码，可以查看组织的审计日志。通过审计日志可以查看管理员对该组织的操作，如创建、修改等。同时，可根据条件过滤。

编辑组织信息

在组织列表中，单击组织右侧的“编辑”，可以修改组织的编码、名称和显示顺序。不支持修改组织的上级组织，如果您需要调整组织的上级组织，可通过移动组织完成。具体可参考**移动组织**。

在左侧组织树上，单击组织右侧的 ，单击“ 编辑组织”，如图4-7，可快速编辑组织。

图 4-7 编辑组织

移动组织

您可以通过移动组织修改组织的上级组织。如果应用开启了用户自动授权功能，移动组织将同步修改组织中用户的应用访问权限。具体可参考应用账号授权策略。

步骤1 在组织列表中，单击待移动组织右侧操作列的“移动”，弹出“选择组织”弹框。您也可在左侧组织树上，单击组织右侧的 ，单击“ 移动组织”快速移动组织。

步骤2 在“选择组织”弹框，选择上级组织。

说明

- 若移动的组织为子组织，如需要将子组织设为顶层组织，单击“设为顶层组织”即可。
- 若移动的组织不是子组织，则在“选择组织”弹框只需选择上级组织进行移动。

步骤3 单击“确定”，在弹出框中单击“确定”完成组织移动。

----结束

删除组织

步骤1 在组织列表中，单击目标组织右侧的“删除”。

图 4-8 删除组织

步骤2 在确认弹框中单击“确定”删除组织完成。

说明

- 组织删除后，不可恢复，请谨慎操作。
- 当组织下存在用户、用户组或子组织时，会删除失败，需要将该组织下相关用户、用户组、子组织删除成功后，才可删除。

----结束

4.2.3 管理用户组

在OneAccess管理门户，可以建立用户组，并将用户加入到相应的用户组中，基于用户组对用户进行管理和授权。同时，可以根据需要添加、编辑、删除用户组等。基于用户组的授权请参考**应用账号授权策略**。

添加用户组

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”。

步骤3 在“组织与用户”页面，切换到“用户组”页签。

步骤4 在用户组列表页面，单击“添加用户组”。

步骤5 在“添加用户组”弹框，选择所属组织，输入用户组名称、描述，选择使用场景。

步骤6 单击“确定”，用户组添加完成，用户组列表中显示已添加的用户组。

----结束

查看用户组详情

在用户组列表中，单击用户组名称，可以查看用户组详情，包括管理成员、已授权应用和审计日志。若您想查看及操作动态用户组，请参考**管理动态用户组**。

- 管理成员，可查看用户组中用户的信息，如用户名、手机号、邮箱等。
  - 在用户组详情页面的“管理成员”页签，单击用户组成员列表右上方“添加成员”，勾选需要加入的用户，即可将用户加入用户组。您还可以通过**为用户组添加用户**操作完成。

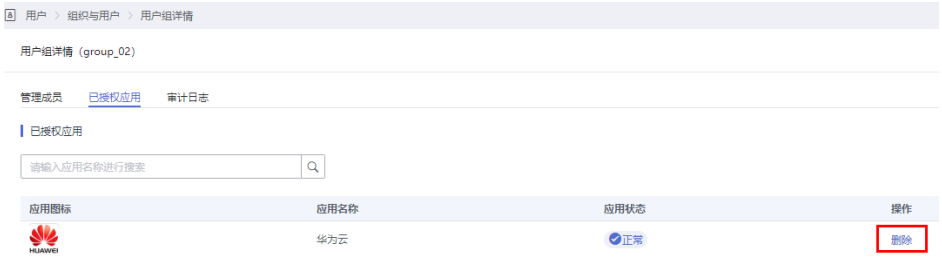
    图 4-9 添加成员

  - 在用户组详情页面的“管理成员”页签，单击操作列的“删除”，可将用户从该用户组中删除。您还可以通过**删除用户组**操作完成。
- 已授权应用，用户组在已授权应用中的信息，包括应用图标、应用名称等。

  单击应用操作列的“删除”后，应用中应用账号的授权策略会同步删除该用户组。对该用户组添加、删除成员操作将自动同步至应用中。

图 4-10 删除已授权应用



- 审计日志

  通过审计日志可以查看管理员对该用户组的操作，如创建、新增成员等。可根据时间、管理员用户名或姓名进行筛选。

编辑用户组信息

步骤1 在用户组列表中，单击用户组右侧的“编辑”。

步骤2 在“编辑用户组”弹框中可以修改用户组的名称和描述。不支持修改用户组所属的组织。

步骤3 单击“确定”。

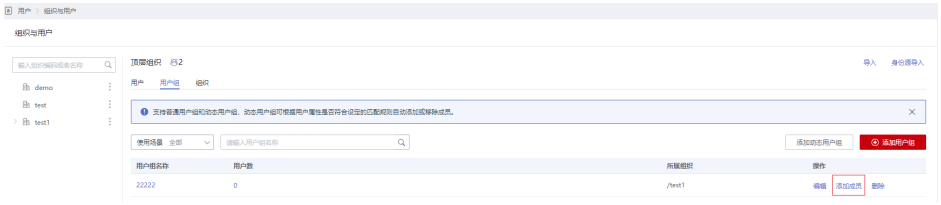
----结束

为用户组添加用户

通过为用户组添加用户，可以将不同组织的成员加入同一个用户组，方便您进行统一管理和授权。基于用户组的授权可参考**应用账号授权策略**。

步骤1 在用户组列表中，单击用户组右侧操作列的“添加成员”。

图 4-11 添加成员



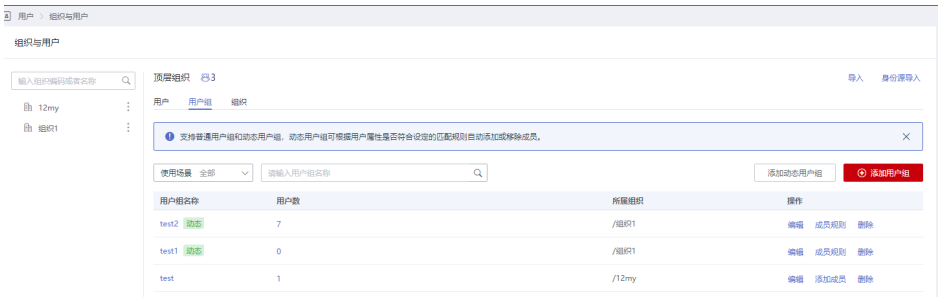
步骤2 在添加成员页面，先选择顶层组织，再勾选该组织下用户，单击“确定”。

----结束

删除用户组

在用户组列表中，单击用户组右侧的“删除”，单击“确定”，删除用户组。删除用户组不会删除用户，但会影响用户的应用权限，基于用户的授权请参考**应用账号授权策略**。

图 4-12 删除用户组



4.2.4 管理动态用户组

在OneAccess管理门户，可以建立动态用户组，可以按照成员规则（成员匹配范围，匹配规则，运算规则，黑白名单）自动添加用户到用户组中。同时，可以根据需要添加、编辑、删除动态用户组等。基于动态用户组的授权请参考**应用账号授权策略**。

添加动态用户组

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”。

步骤3 在“组织与用户”页面，切换到“用户组”页签。

步骤4 在用户组列表页面，单击“添加动态用户组”。

步骤5 在“添加动态用户组”弹框，选择所属组织，输入用户组名称、描述，选择使用场景。

步骤6 单击“下一步”，填写动态用户组成员规则。

1. 成员匹配范围。单击“选择”选择组织，通过选择“包含下级组织”、“不包含下级组织”和“包含下级组织但排除部分组织”限定成员匹配范围。

   说明

   - 如果选择“不包含下级组织”，系统只会在所选部门的直属成员中寻找符合过滤规则的成员。
   - 如果选择“包含下级组织但排除部分组织”则需设置排除的下级组织。

2. 匹配规则。选择属性，选择限制条件，输入属性值，对用户的属性进行大于、小于、等于、不等于、包含等条件限制。可单击“添加规则”添加多条匹配规则。
3. 运算规则，定义**步骤6.2**中添加的多条规则之间的关系，默认为AND关系，可根据需要进行调整。
4. 选择用户添加黑白名单。

步骤7 单击“确定”，动态用户组添加完成，用户组列表中显示已添加的动态用户组。

----结束

查看动态用户组详情

在用户组列表中，单击动态用户组名称，可以查看动态用户组详情，包括用户组信息、匹配成员、已授权应用和审计日志。

- 用户组信息，可查看动态用户组的基本信息（如名称、所属组织、描述、使用场景）和成员规则（如成员匹配范围、匹配规则、运算规则、黑白名单）。
- 匹配成员，可查看动态用户组中匹配到的用户的信息，如用户名、手机号、邮箱等。

  单击用户组成员列表右上方“成员计算”，可以将符合成员规则的用户自动添加到动态用户组中。
- 已授权应用，用户组在已授权应用中的信息，包括应用图标、应用名称等。

  单击应用操作列的“删除”后，应用中应用账号的授权策略会同步删除该用户组。对该用户组添加、删除成员操作将自动同步至应用中。
- 审计日志，通过审计日志可以查看管理员对该用户组的操作，如新增、计算等。可根据时间、管理员用户名或姓名进行筛选。

编辑动态用户组信息

步骤1 在用户组列表中，单击待编辑的动态用户组“操作”列的“编辑”。

步骤2 在“编辑用户组”弹框中可以修改用户组的名称、使用场景和描述。不支持修改用户组所属的组织。

步骤3 单击“确定”完成动态用户组编辑。

----结束

编辑成员规则

通过修改成员规则，可以将不同组织的符合成员规则的成员加入同一个用户组，方便您进行统一管理和授权。基于用户组的授权可参考**应用账号授权策略**。

步骤1 在用户组列表中，单击动态用户组右侧操作栏的“成员规则”。

步骤2 在编辑成员规则页面，选择成员匹配范围，填写匹配规则，选择黑白名单用户，单击“提交计算”，成员规则编辑完成。

----结束

删除动态用户组

在用户组列表中，单击动态用户组右侧的操作栏“删除”，单击“确定”，删除动态用户组。删除动态用户组不会删除用户，但会影响用户的应用权限，基于用户的授权请参考**应用账号授权策略**。

说明

已授权应用的动态用户组无法被删除。

4.2.5 管理身份源

OneAccess具有同步身份数据的功能，数据传递的关系模型可以理解为“上游 - 中游 - 下游”。其中，上游是企业管理的核心身份源，中游是OneAccess平台，下游是需要和上游保持同步的应用系统。通过该模型，OneAccess可将上游的身份数据实时同步到下游应用系统，确保人员的入离调转行为可以准确的传递到各个应用系统，实现用户的全生命周期管理，确保身份数据同步的准确和安全。

身份源相当于企业的核心身份管理系统，包含企业用户的详细信息。OneAccess提供了标准的上游身份源，例如企业微信、钉钉、AD和LDAP，通过简单的连接配置，即

可实现将这些身份源的组织、用户数据同步到OneAccess中。身份源同步可用于以下场景：

- 唯一身份源

  当企业配置唯一身份源后，可通过该身份源的管理系统维护企业的身份数据。

- 多个独立身份源

  当企业配置的身份源相互独立，且身份数据之间没有交集时，可分别通过身份源的管理系统维护对应的企业身份数据。例如，总公司的下属子公司A、子公司B，分别拥有独立的的身份管理系统，可对应OneAccess中的不同机构，通过各自独立的身份管理系统维护对应的身份数据。

- 多个相关身份源

  当企业配置的身份源存在关联时，即身份数据之间有交集，为避免同步时，可能出现的数据覆盖问题，建议身份数据的创建、更新通过唯一的源头控制。

OneAccess支持企业以多种身份源同步用户和组织信息，不同的身份源配置信息略有差异。具体可参考：

- 添加AD身份源请参考：**集成AD身份源**。
- 添加LDAP身份源请参考：**集成LDAP身份源**。

本章以AD身份源为例介绍添加身份源的操作步骤。

操作步骤

步骤1 在OneAccess中创建身份源。

1. 登录OneAccess管理门户。
2. 在导航栏中，选择“用户 > 身份源管理”。
3. 在身份源管理页面，单击AD身份源操作列的“添加身份源”，输入“身份源名称”，单击“确定”。

步骤2 设置导入配置。

1. 在AD身份源列表页面，单击目标身份源的“详情”。

   图 4-13 AD 身份源详情

2. 选择“导入配置”页签，填写导入配置参数并单击“确定”。
   - 基础配置：企业AD服务器的连接参数，实现OneAccess和企业AD的连接，请务必填写正确。

     表 4-4 基础配置

参数	说明
*主机	运行企业AD服务器的主机名称或 IP 地址。

参数	说明
*TCP端口	用于与企业AD服务器进行通信的服务器TCP/IP 端口号。默认为389。 **说明** OneAccess目前只支持公网访问，需要提供公网地址，并开启389端口。
SSL	系统默认true，即使用 SSL 连接到 企业AD服务器。
StartTLS	是否启用startTLS进行加密通信 ■ true：启用StartTLS，且SSL不能设置为true； ■ false：不启用StartTLS。
校验证书	是否校验证书。仅在SSL为true或者StartTLS为true时有效。true: 校验证书，false: 不校验证书。证书必须是公网认证的证书，自签名证书不可以。
协议版本	系统默认TLSv1.2，推荐使用TLSv1.3、TLSv1.2。
*主体	进行企业AD服务器验证时使用的标识名，即拥有AD域读取权限的账号名。传参带域名，如“admin@test.com ”或“TEST\admin”。
*密码	主体账号的密码。
*基本上下文	搜索企业AD树时将使用该树中的一个或多个节点作为起始点，需填写要同步AD用户所在AD中的树的根节点，如“OU=huaweitest,DC=test,DC=com”。
*UID 属性	映射到UID属性的AD属性的名称。
*账户对象类	在AD树中创建新用户对象时将使用的一个或多个对象类。如果输入多个对象类，每一项输入应独占一行；请不要使用逗号或分号来分隔多个对象类。有些对象类可能要求您指定类分层结构中的所有对象类。

- 可选配置：可默认配置，如需同步密码需配置密码的相关参数，包括启用密码同步和要同步的密码属性，如出现同步异常，可根据实际的使用情况进行参数调整，包括但不限于账户对象类、机构对象类等参数。

表 4-5 可选配置

参数	说明
域名	域名存在时，回收的用户名中将该域名排除掉（ 存在多个域名用","分隔，默认用户名会排除域名 ）
账户用户名属性	保存账户用户名的一个或多个属性。在进行验证时，将使用这些属性查找要验证的用户名的AD 条目。

参数	说明
机构对象类	在AD 树中创建新机构对象时将使用的一个或多个对象类。如果输入多个对象类，每一项输入应独占一行；请不要使用逗号或分号来分隔多个对象类。有些对象类可能要求您指定类分层结构中的所有对象类。
机构名属性	保存机构名的一个或多个属性。在进行验证时，将使用这些属性查找要验证的机构名的 AD 条目。
故障转移服务器	列出首选服务器发生故障时将用于故障转移的所有服务器。如果首选服务器发生故障，JNDI 将连接到列表中的下一个可用服务器。按照 "ldap://ldap.example.com:389/" 格式（符合RFC 2255中所述的标准AD v3 URL）列出所有服务器。只有 URL 的主机和端口部分在此设置中是相关的。
密码属性	用于保存密码的AD属性的名称。在更改用户的密码时，会为该属性设置新密码。
用于检索账户的AD过滤器	用于控制从AD资源返回的账户的可选AD过滤器。如果未指定任何过滤器，则只返回包含所有指定对象类的账户。
密码散列算法	指出Identity System对密码执行散列时应使用的算法。目前支持的值为SSHA、SHA、SMD5和MD5。空值表示系统不会对密码执行散列。除非LDAP服务器执行散列（Netscape Directory Server 和 iPlanet Directory Server执行散列），否则这将导致明文密码存储在AD中。
优先处理资源密码策略重置后更改	如果在登录模块中指定此资源（即，此资源是传递验证目标），并且将资源的密码策略配置为在重置后更改，则以管理方式重置了资源账户密码的用户需要在成功验证后更改该密码。
使用VLV控件	指定是否在标准AD控件上强制使用VLV控件。默认为“false”。
VLV 排序属性	指定用于资源上 VLV 索引的排序属性。

参数	说明
读取模式	如果为TRUE，连接器将从服务器中读取模式。如果为FALSE，连接器将根据配置中的对象类提供一个默认模式。要使用扩展对象类，该属性必须为TRUE。
要同步的基本上下文	AD树中用于确定是否应同步更改的一个或多个起始点。如果未设置此属性，则将使用基本上下文属性来同步更改。
要同步的对象类	要同步的对象类。更改日志针对所有对象；它会根据所列出的对象类来对更新进行过滤。除非您要将对象与任何超类值同步，否则不应列出对象类的超类。例如，如果仅应同步 "inetOrgPerson" 对象，但应过滤掉 "inetOrgPerson" 的超类（"person"、"organizationalperson" 和 "top"），则此处仅应列出 "inetOrgPerson"。AD中的所有对象都是 "top" 的派生子类。因此，绝不应列出 "top"，否则将无法过滤任何对象。
要同步的属性	要同步的属性的名称。设置此项后，如果更改日志中的更新没有对任何命名属性进行更新，则会忽略这些更新。例如，如果仅列出 "department"，则只处理影响 "department" 的更改。而忽略所有其他更新。如果将其留空（默认设置），则处理所有更改。
要同步的账户的 AD 过滤器	同步对象时使用的可选AD过滤器。由于更改日志适用于所有对象，因此此过滤器只更新符合指定过滤器条件的对象。如果指定了过滤器，则只有在对象符合过滤器条件并且包含已同步的对象类时，才会对其进行同步。
更改日志块大小	每个查询获取的更改日志条目数。
更改编号属性	更改编号属性
使用 OR 而不是 AND 进行过滤	通常，用于获取更改日志条目的过滤器是基于AND条件检索一段时间间隔内的更改条目。如果设置了此属性，则过滤器将改用OR条件配合所需的更改数量进行过滤。

参数	说明
从过滤器中删除日志条目对象类	如果设置了此属性（默认设置），用于获取更改日志条目的过滤器不会包含 "changeLogEntry" 对象类，因为更改日志中应该不包含其他对象类型的条目。
要同步的密码属性	在执行密码同步时要同步的密码属性的名称。
状态管理类	用于管理启用/禁用状态的类。 如果未指定类，则无法进行身份状态管理。
是否搜索密码	搜索时是否检索用户密码。 默认值为“否”。
DN属性	条目DN属性名称（默认：entryDN）
AD过滤器	一个可选的AD过滤器，用于控制从AD资源返回的组。 如果未指定过滤器，则仅返回包含所有指定对象类的组。
读超时	等待接收响应的时间。如果在指定的时间内没有响应，读取尝试将被中止。值为0或小于0表示没有限制。
连接超时	打开新服务器连接时的等待时间。值0表示将使用TCP网络超时，可能是几分钟。 值小于0表示没有限制。
账号DN前缀	默认值cn，也可以为uid等其它用于dn前缀的属性名。

- 高级配置：用于配置顶层组织、组织、用户映射策略。

表 4-6 高级配置

参数	说明
开启定时回收	可设置是否开启定时回收，若开启，每天定时执行回收任务。
定时频率	定时频率固定为1天。 **说明** 当开启了定时回收后，显示此参数。
选择回收开始时间	可在选择框中设置回收开始时间。 **说明** 当开启了定时回收后，才需设置此参数。

参数	说明
选择根组织	企业AD身份源组织同步至OneAccess后的父级组织。如果不填，将自动创建顶层组织。
组织匹配策略	企业AD组织与OneAccess组织的映射关系。当OneAccess同步企业AD中的组织时，根据该策略进行匹配。如属性名为**编码**、身份源属性名为**组织编码**，企业AD中的组织将以编码为匹配策略映射至OneAccess。
创建组织	开启后，如果同步组织时匹配失败，则OneAccess将自动创建对应组织。默认开启，为了您的数据完整，建议开启。
更新组织	开启后，如果同步组织时匹配成功，则OneAccess将自动更新该组织。默认开启，为保证您的数据正确，建议开启。
删除组织	当AD的组织数据成功同步至OneAccess后，如果删除AD中的组织，则OneAccess会和设置的删除阈值进行对比，删除组织数和上次同步数据总数的比值大于阈值则删除失败，删除组织数和上次同步数据总数的比值小于阈值则删除成功。
用户匹配策略	企业AD用户与OneAccess用户的映射关系。当OneAccess同步企业AD中的用户时，根据该策略进行匹配。如属性名为用户ID、身份源属性名为**员工唯一标识ID**，企业AD的用户将以编码为匹配策略映射至OneAccess。
创建用户	开启后，如果同步用户时匹配失败，则OneAccess将自动创建对应用户。默认开启，为了您的数据完整，建议开启。
更新用户	开启后，如果同步用户时匹配成功，则OneAccess将自动更新该用户。默认开启，为保证您的数据正确，建议开启。
删除用户	当AD的用户数据成功同步至OneAccess后，如果删除AD中的用户，则OneAccess会和设置的删除阈值进行对比，删除用户数和上次同步数据总数的比值大于阈值则删除失败，删除用户数和上次同步数据总数的比值小于阈值则删除成功。
禁用用户阈值调节	默认20%，该功能为平台提供的一种保护机制，支持自定义设置比例。当上游身份源应用禁用/删除超过设定的阈值数据，平台接到指令后，不会进行同步禁用/删除。

步骤3 （可选）设置对象模型。

在身份源详情页面，选择“对象模型”页签，修改、添加、删除用户和机构的属性、映射规则。

表 4-7 对象模型

参数		说明
用户对象	属性定义	AD身份源的用户属性。
	映射定义	AD与OneAccess用户数据同步时的映射规则，支持脚本转换。
机构对象	属性定义	AD身份源的组织属性。
	映射定义	AD与OneAccess组织数据同步时的映射规则，支持脚本转换。

- 添加属性。
  a. 在“属性定义”页签，单击“添加”，弹出“添加属性”弹框。

  b. 选择“身份源可选属性”，输入“显示标签”、描述。
  c. 选择“类型”。当“类型”选择为“文本”时，需要设置“格式”。
  d. 设置该属性是否为必填，单击“确定”，属性添加完成。
- 设置映射规则。
  在“映射定义”页签，单击“编辑”，通过设置转换方式、脚本表达方式、执行方式、系统用户设置映射规则。

----结束

4.2.6 管理用户属性定义

当企业需要配置更多的用户信息，并将其同步至下游应用系统时，可以通过用户属性定义添加用户属性，可通过基本信息、工作信息两个分组设置用户属性，您还可以根据需求自行添加自定义分组。

- 基本信息：用户的个人属性，如用户名、手机号等。已设置的基本属性不允许删除，只允许新增和修改。

- 工作信息：用户的工作属性，员工id、工作所在地等。已设置的工作信息不允许删除，只允许新增和修改。

添加用户基本信息属性

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“用户 > 用户属性定义”。

步骤3 在用户属性定义页面，在“基本信息”右侧选择“设置 > 添加字段”。

图 4-14 添加属性

步骤4 在添加字段页面，填写字段信息。

表 4-8 字段信息和字段内容

参数	说明
* 字段名称	用户属性的名称，不可重复。
* 属性代码	**属性名称**对应的代码，不可重复。
* 字段类型	显示类型可在下拉框选择，不同的显示类型可配置的**选项**不同。 **说明** • 当显示类型为字典时，需要关联字典，添加字典可参考**管理数据字典**。 • 当显示类型为敏感文本时，系统默认部分脱敏，您可以选择全部脱敏。
字段备注	属性值的填写描述。
字段校验规则	对属性是否必填，是否唯一，和字符长度做限制。

表 4-9 显示配置

参数	说明
控制台用户管理	若勾选查询条件显示，在用户列表页面，该属性可作为用户的查询选项。
管理员添加用户	添加用户时，是否允许显示、隐藏该属性。
管理员编辑用户	编辑用户信息时，是否允许管理员修改该属性。

参数	说明
注册信息采集	查看个人信息时，是否允许显示、隐藏该属性。
个人资料页	• 通过设置显示或隐藏来设置查看个人信息时，是否允许显示、隐藏该属性。 • 通过设置是否允许用户修改，来设置修改个人信息时，是否允许用户修改该属性。
导入/导出	导入/导出用户时，是否允许导入/导出该属性。

步骤5 单击“确定”，属性添加完成，列表中显示已添加的属性。

----结束

添加用户工作信息属性

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“用户 > 用户属性定义”。

步骤3 在用户属性定义页面，在“工作信息”右侧选择“设置 > 添加字段”。

图 4-15 添加属性

步骤4 在添加字段页面，填写字段信息。

表 4-10 字段信息和字段内容

参数	说明
* 字段名称	用户属性的名称，不可重复。
* 属性代码	**属性名称**对应的代码，不可重复。

参数	说明
* 字段类型	显示类型可在下拉框选择，不同的显示类型可配置的**选项**不同。 **说明** • 当显示类型为字典时，需要关联字典，添加字典可参考**管理数据字典**。 • 当显示类型为敏感文本时，系统默认部分脱敏，您可以选择全部脱敏。
字段备注	属性值的填写描述。
字段校验规则	对属性是否必填，是否唯一，和字符长度做限制。

表 4-11 显示配置

参数	说明
控制台用户管理	若勾选查询条件显示，在用户列表页面，该属性可作为用户的查询选项。
管理员添加用户	添加用户时，是否允许显示、隐藏该属性。
管理员编辑用户	编辑用户信息时，是否允许管理员修改该属性。
注册信息采集	查看个人信息时，是否允许显示、隐藏该属性。
个人资料页	• 通过设置显示或隐藏来设置查看个人信息时，是否允许显示、隐藏该属性。 • 通过设置是否允许用户修改，来设置修改个人信息时，是否允许用户修改该属性。
导入/导出	导入/导出用户时，是否允许导入/导出该属性。

步骤5 单击“确定”，属性添加完成，列表中显示已添加的属性。

----结束

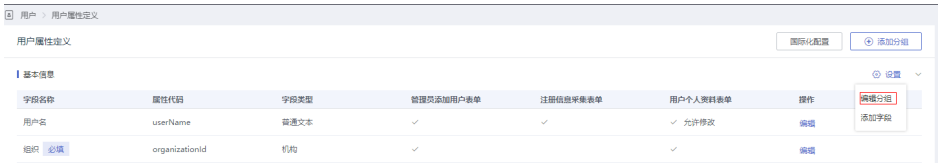
编辑分组

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“用户 > 用户属性定义”。

步骤3 在用户属性定义页面，在“基本信息”右侧选择“设置 > 编辑分组”。

图 4-16 编辑分组



说明

若您想编辑工作信息分组，则在用户属性定义页面，在“工作信息”右侧选择“设置 > 编辑分组”进行编辑。

步骤4 输入分组信息后，单击“确定”，分组信息编辑完成，管理员添加用户时，可根据分组添加字段信息。

----结束

添加自定义分组

如果基本信息和工作信息分组不能满足您的场景需求，可以参考如下步骤添加自定义分组。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“用户 > 用户属性定义”。

步骤3 在用户属性定义页面，单击“添加分组”。

步骤4 输入中、英文分组名称。

步骤5 单击“确定”，分组添加成功，分组列表显示已添加的分组。

----结束

删除自定义分组

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“用户 > 用户属性定义”。

步骤3 在用户属性定义页面，在待删除的自定义分组右侧选择“设置 > 删除分组”，单击“确定”可以删除该自定义分组。

----结束

国际化配置

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“用户 > 用户属性定义”。

步骤3 在用户属性定义页面，单击“国际化配置”。

步骤4 单击某一字段右侧操作列的“多语言设置”可配置基本信息、工作信息和自定义分组的属性的字段名称或字段备注的中英文。

步骤5 单击“保存”设置完成，或单击“保存并继续配置”配置其他中英文没有全部配置的属性。

----结束

删除自定义属性

说明

- 不支持删除用户的基本信息和工作信息中的属性。
- 自定义删除后不可恢复，请谨慎删除。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“用户 > 用户属性定义”。

步骤3 单击自定义属性“操作”列的“删除”。

步骤4 单击弹窗中的“确定”，删除自定义属性。

----结束

修改用户属性

说明

字段名称、属性代码、字段类型不支持修改。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“用户 > 用户属性定义”。

步骤3 单击基本信息、工作信息、自建分组列表“操作”列的“编辑”，可以修改用户的属性信息。

图 4-17 修改属性

步骤4 单击“确定”，用户属性修改完成。

----结束

4.2.7 管理授权

OneAccess可通过授权管理功能实现分级管理员在没有应用配置权限的情况下对自己权限范围内的应用和用户进行应用账号授权，支持按照组织批量授权用户，并且支持给已授权用户分配应用侧角色/权限，同时也可编辑、删除、启用/禁用已授权的应用账号（需要超级管理员授予该功能权限）。

授权应用账号

管理OneAccess用户与应用侧账号之间的绑定关系，即一个OneAccess用户可以对应多个不同应用系统的应用账号，实现一对多的映射关系。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“用户 > 授权管理”。

步骤3 在授权管理页面，单击要授权的应用下的“用户授权”进入用户授权页面。

说明

授权管理页面只显示分级管理员有权限的应用。

步骤4 单击右上角的“添加用户”，在“添加账号”页面，单击要授权的用户所在的组织名称，选中账号。

说明

在“用户授权”页面只显示分级管理员有权限的应用账号。

步骤5 单击“保存”，即可完成授权。

----结束

编辑应用账号

管理员可编辑用户授权页面的应用账号，对应用账号的信息进行修改。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“用户 > 授权管理”。

步骤3 在授权管理页面，单击某应用下的“用户授权”进入用户授权页面。

步骤4 单击待编辑的用户“操作”列的“编辑”，弹出“编辑用户授权信息”页面。

步骤5 输入要修改的信息，单击“保存”编辑应用账号完成。

----结束

禁用/启用应用账号

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“用户 > 授权管理”。

步骤3 在授权管理页面，单击某应用下的“用户授权”进入用户授权页面。

步骤4 单击待操作用户“状态”列的  可禁用账号。禁用账号后，该用户的用户门户不显示该应用，即被禁止访问该应用，单击  可启用账号，开启后，该用户的用户门户显示该应用，即允许访问该应用。

----结束

删除应用账号

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“用户 > 授权管理”。

步骤3 在授权管理页面，单击某应用下的“用户授权”进入用户授权页面。

步骤4 单击待删除的用户“操作”列的“删除”。

步骤5 在弹出提示框中单击“确定”，则可取消该用户对该应用访问权限。

----结束

添加应用侧角色/权限

使用应用侧角色/权限授权的前提是配置应用侧权限。具体可参考**管理应用侧权限**。

在“用户授权”页面可显示分级管理员拥有权限的应用账号，分级管理员可对这些应用账号添加角色/权限。对配置“基于角色的应用权限管理”的应用，只可进行角色添加，对配置“基于角色、权限、资源的应用权限管理”的应用，可添加角色，也可添加权限。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“用户 > 授权管理”。

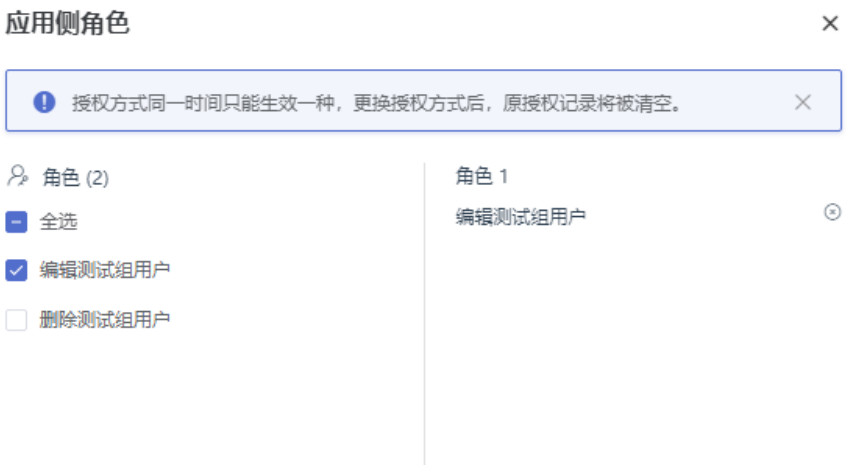
步骤3 在授权管理页面，单击某应用下的“用户授权”进入用户授权页面。

步骤4 单击待操作的用户“操作”列的“应用侧角色/权限”。

步骤5 按应用侧角色或权限授权。

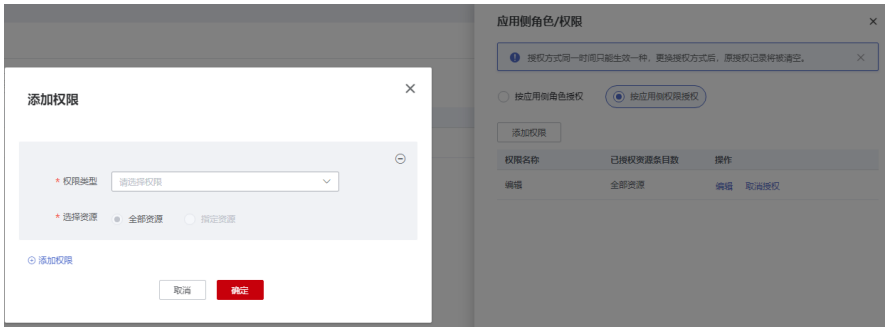
- 当应用的应用侧权限配置为“基于角色的应用权限管理”。

  在“应用侧角色”弹框中，选择角色名称，单击“确定”，则完成按应用侧角色给用户授权。



- 当应用的应用侧权限配置为“基于角色、权限、资源的应用权限管理”。
  - 在“应用侧角色/权限”弹框中，选择“按应用侧角色授权”，选择角色名称，单击“确定”，则完成按应用侧角色给用户授权。

- 在“应用侧角色/权限”弹框中，选择“按应用侧权限授权”，单击“添加权限”，在“添加权限”弹框中，选择“权限类型”并选择资源，单击“确定”，则完成按应用侧权限给用户授权。



----结束

应用账号的检索

在“用户授权”页面，管理员可对应用账号按照检索条件对应用账号进行筛选。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“用户 > 授权管理”。

步骤3 在授权管理页面，单击某应用下的“用户授权”进入用户授权页面。

步骤4 在“用户授权”页面可筛选符合条件的用户。

- 可按应用账号创建时间，在“开始时间”和“结束时间”框中选择开始和结束时间，单击“确定”可筛选出此时间段创建的应用账号。
- 可选择“账号”，在输入框输入账号名或姓名，筛选符合条件的应用账号。
- 可选择“系统用户”，在输入框中输入账号名或姓名，筛选符合条件的应用账号。

- 可选择“应用机构”，在输入框中输入机构名或组织编码，筛选符合条件的应用账号。
- 可按照状态，在“状态”选择框中通过选择“正常”或“禁用”两种状态筛选符合条件的应用账号。

----结束

4.3 资源管理

4.3.1 资源管理概述

OneAccess支持对资源进行统一管理，包括对应用、企业API的管理。本章旨在为您介绍在OneAccess中如何管理企业应用、企业API。

应用

应用可以理解为企业的下游系统，OneAccess支持基于SAML、OAuth2、OIDC、CAS协议的单点登录，同时，也支持插件代填和SDK/API。当配置完成后，用户登录OneAccess用户门户，单点已授权的应用，即可实现多个已授权应用的单点登录。具体可参考**登录OneAccess用户门户并进入应用**。同时，支持基于事件回调、SCIM 、LDAP方式的同步集成，配置完成后，可将OneAccess的数据同步至应用。

OneAccess已预集成1000+应用，您可以按需添加。

在**添加应用**、**应用管理**、**启用/禁用/删除应用**章节将为您详细介绍应用管理及其授权的相关操作。

企业 API

OneAccess提供企业API功能，包含系统API产品和自定义API产品。

- 系统API产品：OneAccess内置的API产品。
- 自定义API产品。

您可以根据需要将开放接口注册到OneAccess平台，方便企业应用调用。

企业API系统API产品是OneAccess内置的API产品和权限，自定义API产品是由用户自定义的API产品和权限。对于系统API产品，只支持查看和授权。

在**授权内置API产品**、**调用内置API产品**、**修改内置API产品**、**添加自定义API产品**、**配置自定义API产品**、**删除自定义API产品**章节将为您详细介绍系统API的授权与调用操作。

4.3.2 应用管理

4.3.2.1 添加应用

OneAccess提供自建应用和预集成应用的添加，您可以根据企业需要添加。

添加自建应用

自建应用指企业的自研应用、不在预集成应用列表中的SaaS类或商业应用等。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，单击“资源 > 应用”。

步骤3 在企业应用页面，单击自建应用下的“添加自建应用”。

步骤4 在添加应用页面，设置应用LOGO、输入应用名称，单击“保存”，应用添加完成，应用列表中显示已添加的应用。

步骤5 添加应用后，需要配置相关参数，才可正常使用，详情请参考**应用管理**。

----结束

添加预集成应用

预集成应用指OneAccess根据应用的开发接口、相应协议已提前集成的应用。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，单击“资源 > 应用”。

步骤3 在企业应用页面，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，单击需要的预置应用。

步骤5 在添加应用页面，编辑通用信息，设置应用名称，单击“下一步”。

步骤6 配置认证参数。不同应用的认证集成方式可能不同，需配置的认证参数也不同。

下面以SAML协议为例，说明认证集成参数的配置方法。OneAccess支持“上传文件”和“手动编辑”两种配置方法，选择其中一种即可。

- 上传元数据
  a. 单击认证参数配置页面的“导入SP应用元数据”。
  b. 单击“选择文件”，选择获取的应用SP的元数据文件。

     说明

     - 如果提示“请上传正确的文件类型”，需要您确认元数据文件的正确性后，重新上传或者通过手动编辑提取元数据。
     - 企业应用的元数据获取方法请参考企业应用的帮助文档。

  c. 待“选择文件”变为“√”时，即系统已提取元数据，单击“下一步”，应用添加完成。
- 手动编辑元数据
  a. 单击“手动输入配置数据”。
  b. 在手动编辑元数据页面，输入从SP元数据文件中获取的“Entity ID”、“Audience URI”等参数。

图 4-18 编辑元数据

表 4-12 认证参数

参数	说明
* SP Entity ID	SP唯一标识，对应SP元数据文件中的“Entity ID”的值。

参数	说明
* 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OneAccess认证成功后响应返回的地址
* Name ID	用户在应用系统中的账号名对应字段，可以选择用户的属性或者对应的账号属性,此字段的值将作为断言中的subject。
NameID Format	SP支持的用户名称标识格式。对应SP元数据文件中“NameIDFormat”的值。
Audience URI	允许使用SAML断言的资源，默认和SP Entity ID相同。
Single Logout URL	服务提供商提供会话注销功能，用户在OneAccess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。
Relay State	用户在OneAccess登录成功后默认跳转的URL。
Reponse签名	是否对SAML Response使用IDP的证书签名。
断言签名	是否对断言使用IDP的证书签名，对应SP元数据文件中“WantAssertionsSigned”值。
数字签名算法	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	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。
断言加密	是否对断言进行加密。
验证请求签名	是否对SAML Request签名进行验证，对应SP元数据文件中“AuthnRequestsSigned”值。
* 验证签名证书	SP公钥证书，用来验证SAML request的签名，对应SP元数据文件中use="signing"证书内容。

步骤7 配置同步参数。不同应用的同步集成方式可能不同，需配置的同步参数也不同。

下面以配置Coremail为例，说明同步集成参数的配置方法。

1. 配置认证参数后，单击“下一步”。
2. 在同步配置页面，填写参数，单击“测试”可测试配置的正确性，配置完成后，单击“下一步”，完成添加应用。如需配置其他菜单，请参考**应用管理**。

----结束

4.3.2.2 启用/禁用/删除应用

禁用/启用应用

- 如果需要暂时关闭该应用，可在应用信息页面禁用该应用。
  a. 登录OneAccess管理门户。
  b. 在导航栏中，选择“资源 > 应用”。
  c. 在应用页面，单击某应用进入应用信息页面。
  d. 单击页面右上角的，在弹框中单击“确定”该应用禁用成功。已禁用的应用会进入“已禁用应用”列表。
- 如果需要开启被禁用的应用，可在应用页面开启。
  a. 登录OneAccess管理门户。
  b. 在导航栏中，选择“资源 > 应用”。
  c. 在应用页面，单击“已禁用应用”。
  d. 单击需要启用的应用右上角的，选择“启用”。
  e. 在提示框中单击“确定”，启用成功。“已禁用列表”不再显示该应用。

说明

当应用已禁用，已授权用户登录以后不再显示该应用。

删除应用

须知

请谨慎删除应用，删除以后该应用的所有数据将被删除且不可恢复。

- 删除未禁用的应用。
  a. 在应用页面，单击需要删除的应用。
  b. 在应用信息页面，单击应用Logo或名称，进入通用信息页面。
  c. 单击下方的“删除应用”。
  d. 输入应用名称，单击“确定”。删除应用成功。
- 删除已禁用的应用。
  a. 登录OneAccess管理门户。
  b. 在导航栏中，选择“资源 > 应用”。
  c. 在应用页面，单击“已禁用应用”。
  d. 单击需要启用的应用右上角的，选择“删除应用”。
  e. 在提示框中单击“确定”，删除成功。应用页面不再显示该应用。

4.3.2.3 通用信息

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“资源 > 应用”。

步骤3 在应用页面，单击某应用进入应用信息页面。

步骤4 单击应用Logo或名称，进入通用信息页面。在通用信息页面可查看以下信息。

- 接口认证凭证
  - ClientId：接口认证凭证ID，注册应用后，由系统自动分配。
  - ClientSecret：接口认证凭证密钥，注册应用后，单击“启用”获取。

    说明

    如不慎丢失访问密钥，请单击“重置”获取新的访问密钥。
- 应用信息

  包含应用LOGO和应用名称，可单击“编辑”修改应用LOGO和应用名称，单击“保存”修改完成。
- 集成信息
  - 认证集成：企业应用与OneAccess认证集成的协议，一旦设置不可修改。
  - 同步集成：企业应用与OneAccess同步集成的方式，一旦设置不可修改。
- 其他信息

  可单击“编辑”修改应用显示的方式，应用显示指应用在用户门户首页的显示方式，包含自动显示、固定显示、不显示三种方式。
  - 自动显示：有该应用账号的用户在登录用户门户后，首页显示该应用。
  - 固定显示：所有用户在登录用户门户后，首页都显示该应用。

- 不显示：所有用户在登录用户门户后，首页都不显示该应用。

- 删除应用

  单击“删除应用”，在弹出框中输入待删除应用的名称，单击“确定”可删除该应用。

----结束

4.3.2.4 认证集成

认证集成配置包括“参数配置”和“映射配置”。当认证集成方式为“插件代填”时，其配置为“基本配置”和“账号配置”。

参数配置

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“资源 > 应用”。

步骤3 在应用页面，单击任一应用进入应用信息页面。

步骤4 在通用信息模块，单击“认证集成”后的  打开认证集成设置，选择适合的集成方式，单击“保存”。

步骤5 在通用信息模块，单击“认证集成”后的“配置”默认进入认证集成的“参数配置”页签，填写参数信息，单击“保存”。认证集成的方式不同，需配置的参数也不同，具体可参考：

- SAML协议的认证配置可参考**认证集成**。
- OAuth2协议的认证配置可参考**认证集成**。
- OIDC协议的认证配置可参考**认证集成**。
- CAS协议的认证配置可参考**认证集成**。
- 插件代填方式的认证配置可参考**认证集成**。

----结束

映射配置

映射配置，即认证成功后需要返回给应用的属性，以建立OneAccess与应用侧属性的映射关系。包括添加映射、编辑映射、删除映射。

- 添加映射

  以SAML协议为例，说明添加映射的方法。

  选择“映射配置”页签，单击“添加映射”，填写映射信息，单击“保存”映射添加完成。

图 4-19 添加映射

表 4-13 映射参数

参数	说明
* 应用系统属性名	企业应用的用户属性名称。即认证成功后，OneAccess返回给应用的用户属性。
* 映射类型	不同的映射类型决定不同的接口在认证成功后返回的属性值，可在下拉框选择。 • 用户属性：将OneAccess的用户属性返回给下游企业应用。 • 账号属性：将应用的账号属性返回给下游企业应用。 • 账号权限：将应用的账号权限返回给下游企业应用。当下游应用需要OneAccess用户携带权限信息返回时，可通过该配置实现。 • 社交属性：将OneAccess用户绑定的社交属性值返回给下游企业应用。 • 固定属性值：可配置固定值。 • 动态脚本：可通过脚本自定义返回给下游企业应用的属性值，可参考**如何开发映射脚本**。 • 会话属性：将会话的参数返回给下游企业应用。 • 授权应用：用户已授权的应用添加该映射。
* 用户属性名	OneAccess映射至应用的属性，可在下拉框选择。该属性的选项随映射类型变化。
* Friendly Name	与**应用系统属性名**一致。当认证协议为SAML时，可配置该参数。
* Attr Name Format	SAML协议返回的一种数据格式，可在下拉框选择。

- 编辑映射

  单击添加的映射右侧操作列的“编辑”，在“编辑映射”页面可修改映射，单击“保存”修改映射信息完成。

- 删除映射

单击添加的映射右侧操作列的“删除”，在提示框中单击“确定”可删除映射。如需再次添加，可参考**添加映射**。

4.3.2.5 同步集成

同步集成配置包括“参数配置”和“常规配置”。当同步集成方式为“事件回调”时，其操作还包括“全量同步”。

参数配置

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“资源 > 应用”。

步骤3 在应用页面，单击任一应用进入应用信息页面。

步骤4 在通用信息模块，单击“同步集成”后的  打开同步集成设置，选择适合的集成方式，单击“保存”。

步骤5 在通用信息模块，单击“同步集成”后的“配置”进入同步集成的参数配置页签，填写参数信息，单击“保存”。同步集成的方式不同，需配置的参数也不同，具体可参考：

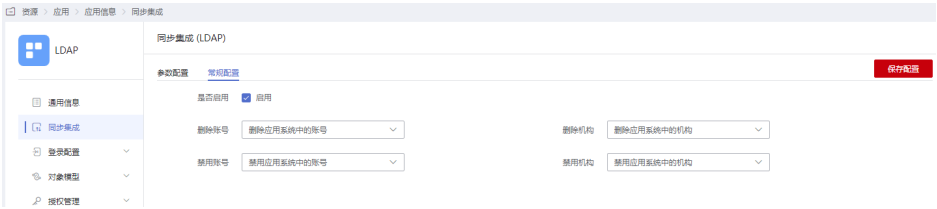
- 事件回调的同步集成参数配置可参考**事件回调配置**。
- SCIM协议的同步集成参数配置可参考**同步配置**。
- LDAP协议的同步集成参数配置可参考**同步配置**。

----结束

常规配置

常规配置，即同步时的映射关系。

在同步集成页面，选择“常规配置”页签，默认启用常规配置，其配置映射关系包括删除账号、删除机构、禁用账号、禁用机构。



- 删除账号

  当OneAccess删除应用账号后，下游应用系统根据该配置决定需执行的操作，可在下拉框选择，包括删除应用系统中的账号、禁用应用系统中的账号、不同步。

- 删除机构

  当OneAccess删除应用机构后，下游应用系统根据该配置决定需执行的操作，可在下拉框选择，包括删除应用系统中的机构、禁用应用系统中的机构、不同步。

- 禁用账号

  当OneAccess禁用应用账号后，下游应用系统根据该配置决定需执行的操作，可在下拉框选择，包括禁用应用系统中的账号、不同步。

- 禁用机构

  当OneAccess禁用机构后，下游应用系统根据该配置决定需执行的操作，可在下拉框选择，包括禁用应用系统中的机构、不同步。

全量同步

当同步集成方式为事件回调时，可实现全量同步，具体可参考**全量同步**。

4.3.2.6 登录配置

OneAccess支持对每个应用配置独立的登录认证方式，包括网站应用、移动应用、公众号。

网站应用

- 配置企业用户从PC端通过浏览器访问应用时的登录认证方式。开启认证方式的前提是添加相应认证源，具体可参考**集成认证源**。
- AD、LDAP认证会占用密码登录方式的输入框，故密码认证、AD认证、LDAP认证只允许同时开启一种。
- 配置ID、挂接URL由系统自动生成，可通过浏览器访问挂接URL登录应用，该URL可编辑。

移动应用

- 配置企业用户从移动端访问应用时的登录认证方式。开启认证方式的前提是添加相应认证源，具体可参考**集成认证源**。
- AD、LDAP认证会占用密码登录方式的输入框，故密码认证、AD认证、LDAP认证只允许同时开启一种。
- 配置ID、挂接URL由系统自动生成，可在移动端访问挂接URL登录应用，该URL可编辑。

公众号

- 配置企业用户通过微信公众号免密登录企业应用。添加配置的前提是添加微信公众号认证源。
- 在配置公众号页面，单击“添加配置”，进入添加微信公众号页面，选择认证源即可。添加完成后，系统自动生成配置ID、挂接URL，单击操作列的“查看URL”可查看该URL，如需删除，单击“删除”即可。

4.3.2.7 访问控制

访问控制是对已授权用户的行为进行风险管控，如果用户未授权访问应用的权限，则策略对该用户不生效。配置应用访问控制策略前，需开启访问控制策略，即配置默认策略。

以下介绍配置自定义策略的方法。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“资源 > 应用”。

步骤3 在应用页面，单击某应用进入应用信息页面。

步骤4 在通用信息模块，单击认证集成后的 选择认证集成方式，单击“保存”。

说明

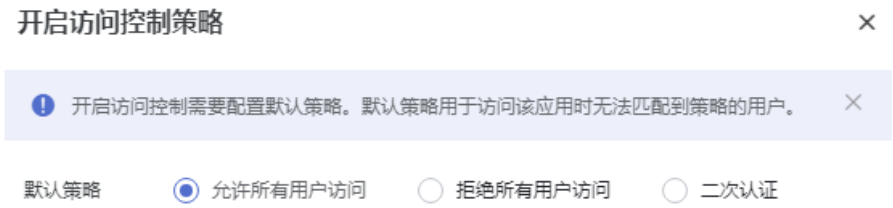
只有打开认证集成，才可以配置访问控制。

步骤5 在通用信息模块，单击“认证集成”后的“配置”默认进入“认证集成”页面。

步骤6 选择左侧导航栏的“访问控制”，进入访问控制页面，单击页面右上角 弹出“开启访问控制策略”页面配置默认策略。

说明

单击 关闭默认策略后，将清空所有策略且无法恢复，请谨慎操作。



步骤7 单击“保存”配置完成，添加的默认策略会显示在访问控制界面。若需修改默认策略，可单击默认策略后的弹出“修改访问控制策略”进行修改。

步骤8 在访问控制页面，单击“添加策略”配置访问控制参数，单击“保存”添加策略完成。

表 4-14 策略参数

参数	说明
* 策略名称	策略的名称。
描述	策略的描述信息。
用户条件	指定访问应用的用户范围，可在下拉框选择。
条件关系	用户条件（**用户属于组**、**用户属于组织**、**指定用户**、**自定义条件**）之间的关系。
用户属于组	用户条件之一，通过指定用户组控制用户的访问行为。用户组请参考**管理用户组**。
用户属于组织	用户条件之一，通过指定组织控制用户的访问行为。组织请参考**组织**。
指定用户	用户条件之一，通过指定用户控制用户的访问行为。用户请参考**管理用户**。
自定义条件	• 用户条件之一，通过指定用户的属性控制用户的访问行为。 用户属性请参考**管理用户属性定义**。 • 单击“继续添加自定义条件”可添加多条自定义条件。

参数	说明
访问时间	指定访问应用的时间范围，可在下拉框选择。
选择日期	指定访问应用的日期，可在下拉框选择。
选择时间段	指定访问应用的时间段，可在下拉框选择。
具体时间段	• 通过指定具体时间段控制用户的访问行为。 • 单击“ 继续添加时间段”可添加多条具体时间段。
设备类型	指定访问应用的介质，包含浏览器、桌面端、移动端。 • 浏览器：谷歌、火狐、IE、其他。 • 桌面端：Windows、Linux、MacOs、其他。 • 移动端：Android、IOS、其他。
区域范围	• 访问应用的区域，可在下拉框选择。 • 如需指定具体的区域，单击“配置区域范围”配置区域，具体方法请参考**管理区域**。
认证源类型	指定访问应用的认证源，可在下拉框选择。
THEN	是否允许访问应用。当选择“二次认证”时，需配置二次认证频率和二次认证方式。 • 二次认证频率：在访问凭证有效期内，指定访问应用的频率。 • 二次认证方式：指定认证方式。 • 当勾选OTP后，用户登录二次认证时可按照页面提示获取动态口令，可参考**配置动态口令**查看具体配置。 • 当二次认证方式勾选多个后，用户登录二次认证时，可选择二次认证方式。

----结束

配置多条应用访问控制策略后，可调整其优先级。当企业用户访问应用时，根据自定义策略的优先级进行匹配，如果匹配失败，将通过默认策略判断用户是否可以访问。

- 在访问控制页面，可通过拖拽调整策略优先级。
- 单击某策略右侧操作列的“编辑”，在“编辑策略”页面可编辑该策略的配置，单击“保存”编辑完成。
- 单击某策略右侧操作列的“详情”可查看该策略的配置信息。
- 单击某策略右侧操作列的“删除”，在弹框中单击“确定”可删除该条策略。

4.3.2.8 管理对象模型

对象模型是OneAccess的数据同步至下游应用的基础，包括应用账号模型和应用机构模型。

在开启同步配置后，OneAccess已定义了账号名、姓名、应用机构等常规的内置属性，如需同步更多的属性，可通过在对象模型处添加属性并配置映射实现。同步时，需保持添加的属性名与应用的属性名一致。除此之外，对象模型还有常规配置功能，可以设置删除或者禁用系统用户/组织后，应用账号/机构的状态。

应用账号模型

- 属性定义
  a. 登录OneAccess管理门户。
  b. 在导航栏中，选择“资源 > 应用”。
  c. 在应用页面，单击某应用进入应用信息页面。
  d. 单击应用图标，默认进入该应用的通用信息页面。
  e. 在左侧导航栏选择“对象模型 > 应用账号模型”，默认进入“属性定义”页签，单击“添加”，配置应用的账号属性，单击“保存”添加属性完成。

图 4-20 配置属性参数

表 4-15 属性参数

参数	说明
* 属性名	应用账号的属性名称。
* 显示标签	属性名称的标识，建议与**属性名**对应。
描述	**属性名**的说明。
* 属性类型	属性值的类型，可在下拉框选择。
格式	只有“属性类型”选择文本时才需要设置该参数，用来设置文本的格式。

参数	说明
是否必填	勾选后，同步用户数据至应用时，该属性必须有值，为空时，会提示“{显示标签}为必填属性”。
是否唯一	只有“属性类型”选择文本时才需要设置该参数，勾选后，同步用户数据至应用时，该属性的值具有唯一性，重复时，会提示“{显示标签}”已存在。
是否敏感	只有“属性类型”选择文本时才需要设置该参数，勾选后，同步用户数据至应用时，数据隐藏展示，单击可以看到数据内容。

f. 可单击属性右侧操作列的“更新”、“删除”可编辑、删除账号的属性，对于内置属性，不支持删除操作。

- 映射定义

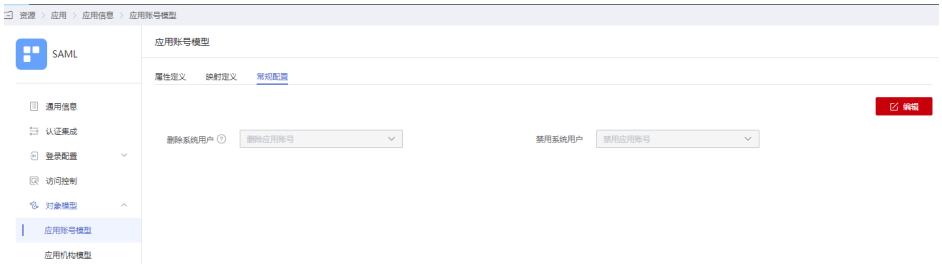
  选择“映射定义”页签，单击“编辑”，配置账号属性的映射关系。为了避免同步异常，建议添加的账号属性与需要映射的用户属性类型保持一致。

  表 4-16 映射参数

参数	说明
系统用户	映射至**应用账号**的用户属性，可在下拉框选择。
转换方式	**用户**与**应用账号**属性之间的映射方式，可在下拉框选择。
脚本表达式	填写映射脚本。具体可参考**如何开发映射脚本**。
执行方式	**应用账号**属性的同步方式，可在下拉框选择。
应用账号	应用账号属性的显示标签。

- 常规配置

  选择“常规配置”页签，“删除系统用户”默认配置为删除应用账号，“禁用系统用户”默认配置为禁用应用账号。单击“编辑”，可以修改配置，其中“删除系统用户”如果选择禁用或保留应用账号，由于用户已删除，账号会自动变更为孤儿账号；“禁用系统用户”可以改成保留应用账号。修改完成后，单击“保存”即可生效。



应用机构模型

配置应用机构模型前需开启应用机构，配置方法与应用账号模型类似，具体可参考**应用账号模型**。

为了避免同步异常，建议添加的机构属性与需要映射的组织属性类型保持一致。

- 属性定义
  a. 登录OneAccess管理门户。
  b. 在导航栏中，选择“资源 > 应用”。
  c. 在应用页面，单击某应用进入应用信息页面。
  d. 单击应用图标，默认进入该应用的通用信息页面。
  e. 在左侧导航栏选择“对象模型 > 应用机构模型”进入应用机构模型页面，单击  ，在弹出框单击“确定”开启应用机构。默认进入“属性定义”页签，单击“添加”，配置应用的机构属性，单击“保存”添加属性完成。

图 4-21 配置属性参数

表 4-17 属性参数

参数	说明
* 属性名	应用机构的属性名称。
* 显示标签	属性名称的标识，建议与**属性名**对应。
描述	**属性名**的说明。
* 属性类型	属性值的类型，可在下拉框选择。
格式	只有“属性类型”选择文本时才需要设置该参数，用来设置文本的格式。
是否必填	勾选后，同步机构数据至应用时，该属性必须有值，为空时，会提示“{显示标签}为必填属性”。
是否唯一	只有“属性类型”选择文本时才需要设置该参数，勾选后，同步机构数据至应用时，该属性的值具有唯一性，重复时，会提示“{显示标签}”已存在。

参数	说明
是否敏感	只有“属性类型”选择文本时才需要设置该参数，勾选后，同步机构数据至应用时，数据隐藏展示，单击可以看到数据内容。

可单击属性右侧操作列的“更新”、“删除”可编辑、删除机构的属性，对于内置属性，不支持删除操作。

- 映射定义

  选择“映射定义”页签，单击“编辑”，配置账号属性的映射关系。为了避免同步异常，建议添加的账号属性与需要映射的用户属性类型保持一致。

  表 4-18 映射参数

参数	说明
组织	映射至**应用机构**的组织属性，可在下拉框选择。
转换方式	**组织**与**应用机构**属性之间的映射方式，可在下拉框选择。
脚本表达式	填写映射脚本。具体可参考**如何开发映射脚本**。
执行方式	**应用机构**属性的同步方式，可在下拉框选择。
应用机构	应用机构属性的显示标签。

- 常规配置

  选择“常规配置”页签，“删除系统组织”默认配置为删除应用机构，“禁用系统组织”默认配置为禁用应用机构。单击“编辑”可以修改配置，其中“删除系统组织”可以配置为禁用应用机构或不影响；“禁用系统组织”可配置为不影响。修改完成后，单击“保存”即可生效。

4.3.2.9 授权管理

4.3.2.9.1 管理应用账号

管理OneAccess用户与应用侧账号之间的绑定关系，即一个OneAccess用户可以对应多个不同应用系统的应用账号，实现一对多的映射关系。

如果已配置同步参数，且同步正常时，添加、通过授权策略新增和删除、编辑、删除、启用、禁用应用账号会触发向下游应用的同步操作。具体可参考**通过事件回调方式同步数据至应用**。

应用账号包括新账号和存量账号。

- 新账号

  “新账号”可以理解为“开通”，表示通过手工添加或授权策略为企业用户授权访问应用的权限，即分配应用账号。

- 存量账号

  “存量账号”可以理解为“绑定”，表示应用系统原有的历史账号，您可以通过线下梳理OneAccess用户和存量账号的绑定关系后，批量导入应用账号中，也可

以批量导入存量账号到孤儿账号中，再通过绑定OneAccess用户关联这些存量账号。具体可参考**导入应用账号**。

添加账号

添加账号是手工授予用户应用权限的基本方式，如需自动授权，请参考**应用账号授权策略**。

如果应用机构开启机构自动授权，“添加账号”时，可选择的用户范围为已自动授权的机构。应用机构授权请参考**应用机构授权策略**。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“资源 > 应用”。

步骤3 在应用页面，单击某应用进入应用信息页面。

步骤4 单击应用图标，默认进入该应用的通用信息页面。

步骤5 在左侧导航栏选择“授权管理 > 应用账号”进入应用账号页面。

步骤6 单击“添加账号”，在添加账号页面，选择需要授予应用权限的用户，单击“保存”，完成用户授权。

----结束

用户机构计算

当开启应用机构的自动授权后，应用账号模型未配置应用机构的映射时，单击“用户机构计算”后，应用账号列表显示其归属的应用机构。应用机构的自动授权请参考**应用机构授权策略**，应用账号模型的配置请参考**应用账号模型**。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“资源 > 应用”。

步骤3 在应用页面，单击某应用进入应用信息页面。

步骤4 单击应用图标，默认进入该应用的通用信息页面。

步骤5 在左侧导航栏选择“授权管理 > 应用账号”进入应用账号页面。

步骤6 单击“用户机构计算”。

图 4-22 用户机构计算

----结束

清空账号

清空账号会初始化该应用的授权数据，即取消已授权用户访问该应用的权限，请谨慎操作。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“资源 > 应用”。

步骤3 在应用页面，单击某应用进入应用信息页面。

步骤4 单击应用图标，默认进入该应用的通用信息页面。

步骤5 在左侧导航栏选择“授权管理 > 应用账号”进入应用账号页面。

步骤6 单击“清空账号”。

说明

在弹窗中如勾选“同时删除孤儿账号和公共账号”，会同时清空孤儿账号和公共账号。清空公共账号后，该账号的责任人登录用户门户后，公共账号列表不显示该应用的公共账号，即同步该操作。

步骤7 单击“确定”。

----结束

应用账号授权策略

授权策略可自动授予、删除用户访问应用的权限，方便您对企业应用的用户权限进行统一管理和维护。

当开启用户自动授权后，对所授权的组织添加用户、删除用户、调整用户组织，对所授权的用户组添加、删除用户，可自动同步至应用中。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“资源 > 应用”。

步骤3 在应用页面，单击某应用进入应用信息页面。

步骤4 单击应用图标，默认进入该应用的通用信息页面。

步骤5 在左侧导航栏选择“授权管理 > 应用账号”进入应用账号页面。

步骤6 单击“授权策略”。

步骤7 在授权策略页面，单击 开启用户自动授权并选择用户，单击“保存”，保存当前策略，不立即授权用户。

说明

- 如果应用机构开启机构自动授权，当选择用户为“机构范围中所有用户”或“自定义”时，可选的“机构范围”为已自动授权的机构，即可授予已自动授权机构中的用户访问应用的权限，用户组范围不受已自动授权机构的限制。应用机构授权请参考**应用机构授权策略**。
- 已经禁用的用户再次启用后不会触发自动授权，需要手动授权。

- 当选择用户为“机构范围中所有用户”时，“机构范围”会显示全部机构，即授予所有用户访问应用的权限。
- 当选择用户为“自定义”时。
  - 当条件关系选择“AND”时，则机构范围和用户组范围可只选其中一个或两个同时选择，则会授予所选机构中的用户访问应用的权限或所选用户组中的用户访问应用的权限或所选机构、用户组的共有用户即二者的交集访问应用的权限。
  - 当条件关系选择“OR”时，则需同时选择“机构范围”和“用户组范围”，会授予所选机构和用户组中所有用户访问应用的权限。

步骤8 单击“执行新增”，完成用户授权，新增成功后，请单击，应用账号列表显示已选择的用户。

步骤9 如需批量删除基于机构、用户组的授权，在授权策略页面，取消勾选需要删除的机构、用户组，单击“保存”后，只保存当前策略，不立即取消用户授权。再单击“执行删除”，完成对用户的取消授权，删除成功后，请单击，应用账号列表不显示已取消授权的用户。

----结束

编辑账号

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“资源 > 应用”。

步骤3 在应用页面，单击某应用进入应用信息页面。

步骤4 单击应用图标，默认进入该应用的通用信息页面。

步骤5 在左侧导航栏选择“授权管理 > 应用账号”进入应用账号页面。

步骤6 单击待编辑的应用账号操作列的“编辑”，可修改用户授权信息，该页面显示的账号属性可通过应用账号的属性定义来配置。具体可参考**应用账号模型**。

步骤7 单击“保存”。

----结束

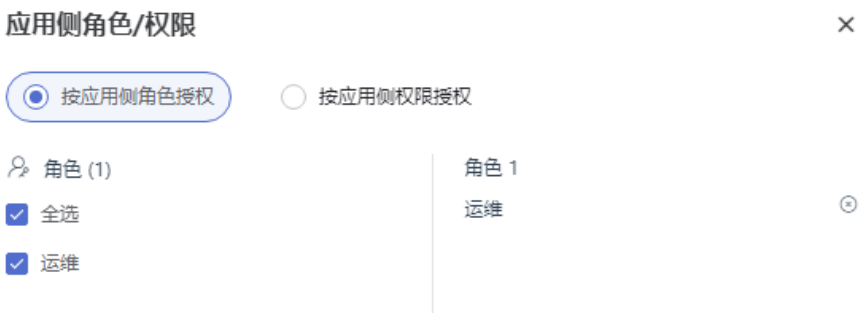
应用侧角色/权限

使用应用侧角色/权限授权的前提是配置应用侧权限。具体可参考**管理应用侧权限**。

在应用账号页面，在应用账号操作列选择“更多 > 应用侧角色/权限”。

- 当应用侧权限配置为基于角色的应用权限管理时，只可按应用侧角色授权，选择需要授予角色的账号，单击“确定”，完成基于角色的授权。基于角色的应用权限管理请参考**基于角色的应用权限管理**。

图 4-23 按应用侧角色授权



- 当应用侧权限配置为基于角色、权限、资源的应用权限管理时，可选择按应用侧角色授权、按应用侧权限授权两种方式，每个账号只能选择一种授权方式。
  - 按应用侧权限授权时，单击“添加权限”，在添加权限页面，选择权限类型，选择资源可选全部资源也可指定资源，当选择指定资源时，勾选所需资源条目，单击“确定”，完成基于应用侧权限的授权，其中，资源条目与其子条目之间权限独立，按单独授权。

    图 4-24 按应用侧角色授权

    当对账号按应用侧权限授权后，可在“应用侧权限 > 权限集合”中在相应资源的已授权账号中查看。

  - 按应用侧角色授权请参考**按应用侧角色授权**。

转孤儿账号

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“资源 > 应用”。

步骤3 在应用页面，单击某应用进入应用信息页面。

步骤4 单击应用图标，默认进入该应用的通用信息页面。

步骤5 在左侧导航栏选择“授权管理 > 应用账号”进入应用账号页面。

步骤6 在待操作应用账号操作栏选择“更多 > 转孤儿账号 ”。

步骤7 单击“确定”，转孤儿账号成功，会在“授权管理 > 孤儿账号”中看到被转的账号。

----结束

删除账号

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“资源 > 应用”。

步骤3 在应用页面，单击某应用进入应用信息页面。

步骤4 单击应用图标，默认进入该应用的通用信息页面。

步骤5 在左侧导航栏选择“授权管理 > 应用账号”进入应用账号页面。

步骤6 在待删除应用账号操作栏选择“更多 > 删除 ”。

步骤7 单击弹窗中的“确定”，可删除账号。删除账号后，该用户将无访问应用的权限，请谨慎删除。如需批量删除请参考**应用账号授权策略**。

----结束

启用/禁用账号

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“资源 > 应用”。

步骤3 在应用页面，单击某应用进入应用信息页面。

步骤4 单击应用图标，默认进入该应用的通用信息页面。

步骤5 在左侧导航栏选择“授权管理 > 应用账号”进入应用账号页面。

步骤6 单击待禁用应用账号状态列的在应用账号页面，单击应用账号状态列的  可禁用账号。禁用账号后，该用户的用户门户不显示该应用。

步骤7 单击待开启应用账号状态列的  可开启账号，该用户的用户门户显示该应用，即允许访问该应用。用户访问应用请参考**登录OneAccess用户门户并进入应用**。

----结束

4.3.2.9.2 管理应用机构

应用机构主要管理应用侧与OneAccess机构的关系，可覆盖以下场景：

- 应用侧的机构与OneAccess保持一致，随OneAccess同步变更。
- 应用侧的机构只是OneAccess的一部分，随OneAccess同步变更。

- 应用侧的机构是OneAccess的全部或部分，同时，拥有自身独立的应用机构，即虚拟机构。

使用应用机构前，需开启应用机构，具体可参考**应用机构模型**。

如果已配置同步参数，且同步正常时，通过授权策略新增和删除应用机构、添加虚拟机构、编辑虚拟机构、移动虚拟机构、删除虚拟机构会触发向下游应用的同步操作。具体可参考**通过事件回调方式同步数据至应用**。

应用机构中操作包括清空机构、授权策略、添加虚拟机构、编辑虚拟机构、移动虚拟机构、删除虚拟机构。

清空机构

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“资源 > 应用”。

步骤3 在应用页面，单击某应用进入应用信息页面。

步骤4 单击应用图标，默认进入该应用的通用信息页面。

步骤5 在左侧导航栏选择“授权管理 > 应用机构”进入应用机构页面。

步骤6 单击“清空机构”在弹框中单击“确定”将删除本应用的授权机构数据，即清空OneAccess平台组织（不同步到下游应用系统），请谨慎操作。

说明

- 清空机构后，通过“添加账号”、“授权策略”授权用户访问应用的权限时，可选择的机构范围不受已授权机构的限制，即可以选择OneAccess的所有机构。
- 当归属于已授权机构的应用账号、孤儿账号、公共账号未被清空，且应用账号的列表显示其归属的机构时，“清空机构”会提示“机构中存在应用账号/孤儿账号/公共账号”，需优先清空应用账号、孤儿账号、公共账号。

----结束

应用机构授权策略

如果已配置同步参数，且同步正常时，对通过授权策略新增的应用机构执行添加子组织、编辑、移动、删除会触发向下游应用的同步操作。具体请参考**管理组织**。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“资源 > 应用”。

步骤3 在应用页面，单击某应用进入应用信息页面。

步骤4 单击应用图标，默认进入该应用的通用信息页面。

步骤5 在左侧导航栏选择“授权管理 > 应用机构”进入应用机构页面。

步骤6 单击“授权策略”。

步骤7 在授权策略页面，单击  开启机构自动授权并选择机构，单击“保存”，保存当前策略，不立即授权机构。

- 当“请选择机构”为“全部机构”时，会授权OneAccess的所有机构。

- 当“请选择机构”为“自定义”时，需至少选择一个机构。选择需要授权的机构。若不启用“同步上级机构”，只会授权所选机构；若启用“同步上级机构”，会同时授权所选机构的上级。

步骤8 单击“执行新增”，完成机构授权，新增成功后，请单击，应用机构列表显示已选择的机构。

步骤9 如需批量删除授权的机构，在授权策略页面，取消勾选需要删除的机构，单击“保存”后，只保存当前策略，不立即取消机构授权。再单击“执行删除”，完成对机构的取消授权，删除成功后，请单击，应用机构列表不显示已取消授权的机构。

----结束

添加虚拟机构

虚拟机构归属企业应用，满足了企业应用拥有自身独立机构的场景。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“资源 > 应用”。

步骤3 在应用页面，单击某应用进入应用信息页面。

步骤4 单击应用图标，默认进入该应用的通用信息页面。

步骤5 在左侧导航栏选择“授权管理 > 应用机构”进入应用机构页面。

步骤6 单击，打开“添加虚拟机构”页面，输入机构名称、机构编码，选择父组织。

步骤7 单击“保存”，完成虚拟机构的添加。当选择父组织时，添加的虚拟机构为其子机构，当父组织为空时，添加的虚拟机构为顶层机构。

----结束

编辑虚拟机构

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“资源 > 应用”。

步骤3 在应用页面，单击某应用进入应用信息页面。

步骤4 单击应用图标，默认进入该应用的通用信息页面。

步骤5 在左侧导航栏选择“授权管理 > 应用机构”进入应用机构页面。

步骤6 单击待编辑虚拟机构操作栏的“编辑”，可修改虚拟机构的信息。

----结束

移动虚拟机构

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“资源 > 应用”。

步骤3 在应用页面，单击某应用进入应用信息页面。

步骤4 单击应用图标，默认进入该应用的通用信息页面。

步骤5 在左侧导航栏选择“授权管理 > 应用机构”进入应用机构页面。

步骤6 单击待移动的虚拟机构操作栏的“移动”，可修改虚拟机构的上级机构。

----结束

删除虚拟机构

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“资源 > 应用”。

步骤3 在应用页面，单击某应用进入应用信息页面。

步骤4 单击应用图标，默认进入该应用的通用信息页面。

步骤5 在左侧导航栏选择“授权管理 > 应用机构”进入应用机构页面。

步骤6 单击待删除的虚拟机构操作栏的“删除”。

步骤7 单击弹窗中的“确定”，可删除虚拟机构。如需再次添加可参考**添加虚拟机构**。

----结束

4.3.2.9.3 管理同步事件

当OneAccess向下游企业应用同步数据时，同步事件会记录同步的所有操作，方便您进行查看。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“资源 > 应用”。

步骤3 在应用页面，单击某应用进入应用信息页面。

步骤4 单击应用图标，默认进入该应用的通用信息页面。

步骤5 在左侧导航栏选择“授权管理 > 同步事件”进入同步事件页面。可根据时间、操作类型、对象类型以及同步状态进行筛选查看同步记录。

说明

对于同步失败的事件的处理：

- 可以查看响应信息并在解决问题后，单击操作列的“重试”再次同步。
- 可以通过“一键重试”快速执行同步。当父机构的同步事件重试成功后，会同时触发执行其下的子机构和账号的同步事件。

----结束

4.3.2.9.4 管理孤儿账号

孤儿账号指与OneAccess用户无绑定关系的账号。

如果已配置同步参数，且同步正常时，添加、编辑、删除孤儿账号会触发向下游应用的同步操作。具体可参考**通过事件回调方式同步数据至应用**。

添加账号

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“资源 > 应用”。

步骤3 在应用页面，单击某应用进入应用信息页面。

步骤4 单击应用图标，默认进入该应用的通用信息页面。

步骤5 在左侧导航栏选择“授权管理 > 孤儿账号”进入孤儿账号页面。

步骤6 在孤儿账号页面，单击“添加账号”，填写账号信息。

步骤7 单击“保存”，完成孤儿账号的添加。孤儿账号列表显示已添加的孤儿账号。该页面显示的账号属性可通过应用账号的属性定义来配置。具体可参考**应用账号模型**。

----结束

启用/禁用账号

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“资源 > 应用”。

步骤3 在应用页面，单击某应用进入应用信息页面。

步骤4 单击应用图标，默认进入该应用的通用信息页面。

步骤5 在左侧导航栏选择“授权管理 > 孤儿账号”进入孤儿账号页面。

步骤6 单击待禁用的孤儿账号状态列的在孤儿账号页面，单击孤儿账号状态列的  可禁用账号，单击  可开启账号。

----结束

编辑账号

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“资源 > 应用”。

步骤3 在应用页面，单击某应用进入应用信息页面。

步骤4 单击应用图标，默认进入该应用的通用信息页面。

步骤5 在左侧导航栏选择“授权管理 > 孤儿账号”进入孤儿账号页面。

步骤6 单击待编辑孤儿账号操作列的“编辑”，可修改孤儿账号的信息，该页面显示的账号属性可通过应用账号的属性定义来配置。具体可参考**应用账号模型**。

----结束

绑定用户

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“资源 > 应用”。

步骤3 在应用页面，单击某应用进入应用信息页面。

步骤4 单击应用图标，默认进入该应用的通用信息页面。

步骤5 在左侧导航栏选择“授权管理 > 孤儿账号”进入孤儿账号页面。

步骤6 在待操作孤儿账号操作列选择“更多 > 绑定用户 ”，在绑定用户的弹窗中输入存在的用户名。

步骤7 单击“确定”，可建立孤儿账号与用户之间的绑定关系。如输入的用户不存在，会提示“绑定的用户不存在”。

绑定用户后，该账号会自动移动至应用账号，可在应用账号中查看。

----结束

转公共账号

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“资源 > 应用”。

步骤3 在应用页面，单击某应用进入应用信息页面。

步骤4 单击应用图标，默认进入该应用的通用信息页面。

步骤5 在左侧导航栏选择“授权管理 > 孤儿账号”进入孤儿账号页面。

步骤6 在待操作孤儿账号操作列选择“更多 > 转公共账号”。

步骤7 单击“确定”，可将该账号转换为公共账号。

转公共账号后，该账号会自动移动至公共账号，可在公共账号中查看。

----结束

删除账号

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“资源 > 应用”。

步骤3 在应用页面，单击某应用进入应用信息页面。

步骤4 单击应用图标，默认进入该应用的通用信息页面。

步骤5 在左侧导航栏选择“授权管理 > 孤儿账号”进入孤儿账号页面。

步骤6 在待删除的孤儿账号操作列选择“更多 > 删除”。

步骤7 单击“确定”，可删除账号。

----结束

4.3.2.9.5 管理公共账号

公共账号是面向“多人使用一个账号的”场景，当企业应用需要配置一个公共账号供多人使用时，可以通过“责任人”授权“使用者”对该账号进行管理。其中，责任人对公共账号的管理可参考**公共账号**。

如果已配置同步参数，且同步正常时，添加、编辑、删除公共账号会触发向下游应用的同步操作。具体可参考**通过事件回调方式同步数据至应用**。

添加账号

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“资源 > 应用”。

步骤3 在应用页面，单击某应用进入应用信息页面。

步骤4 单击应用图标，默认进入该应用的通用信息页面。

步骤5 在左侧导航栏选择“授权管理 > 公共账号”进入公共账号页面。

步骤6 单击“添加账号”，填写账号信息。

步骤7 单击“下一步”，进入添加责任人页面，单击“保存”，完成公共账号的添加，公共账号列表显示已添加的公共账号。

- 如果在添加责任人页面，输入的用户名存在，单击“保存”后，该公共账号的责任人显示为已输入的用户名。
- 如果输入的用户名不存在，单击“保存”后，该公共账号的责任人显示为空。

说明

- 当公共账号的责任人显示为空时，可通过修改责任人来添加，具体可参考**责任人**。
- 添加公共账号页面显示的账号属性可通过应用账号的属性定义来配置。具体可参考**应用账号模型**。

----结束

启用/禁用账号

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“资源 > 应用”。

步骤3 在应用页面，单击某应用进入应用信息页面。

步骤4 单击应用图标，默认进入该应用的通用信息页面。

步骤5 在左侧导航栏选择“授权管理 > 公共账号”进入公共账号页面。

步骤6 单击公共账号状态列  可禁用账号，单击  可开启账号。

- 如果用户只有公共账号的使用权限，即是公共账号的使用者，禁用账号后，该用户的用户门户不显示该应用，即被禁止访问该应用，开启后，该用户的用户门户显示该应用，即允许访问该应用。用户访问应用请参考**登录OneAccess用户门户并进入应用**。
- 如果用户是公共账号的使用者，同时，该用户拥有应用账号，禁用公共账号后，该用户的用户门户依然显示该应用，访问应用时，使用的是应用账号的信息，开启公共账号后，访问应用时，由用户选择访问应用的账号。用户访问应用请参考**登录OneAccess用户门户并进入应用**。

----结束

编辑账号

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“资源 > 应用”。

步骤3 在应用页面，单击某应用进入应用信息页面。

步骤4 单击应用图标，默认进入该应用的通用信息页面。

步骤5 在左侧导航栏选择“授权管理 > 公共账号”进入公共账号页面。

步骤6 单击待编辑公共账号操作列的“编辑”，可修改公共账号的信息，该页面显示的账号属性可通过应用账号的属性定义来配置。具体可参考**应用账号模型**。

----结束

添加责任人

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“资源 > 应用”。

步骤3 在应用页面，单击某应用进入应用信息页面。

步骤4 单击应用图标，默认进入该应用的通用信息页面。

步骤5 在左侧导航栏选择“授权管理 > 公共账号”进入公共账号页面。

步骤6 在待操作的公共账号操作列选择“更多 > 责任人 ”，在修改责任人的弹窗中输入存在的用户名。

步骤7 单击“确定”，完成责任人的添加。该用户在用户门户的公共账号处，可管理使用者。具体可参考**公共账号**。

----结束

添加使用者

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“资源 > 应用”。

步骤3 在应用页面，单击某应用进入应用信息页面。

步骤4 单击应用图标，默认进入该应用的通用信息页面。

步骤5 在左侧导航栏选择“授权管理 > 公共账号”进入公共账号页面。

步骤6 在待操作的公共账号操作列选择“更多 > 使用者 ”，在选择使用者的页面勾选需要授权的用户。

步骤7 单击“保存”，完成使用者的添加。同时，责任人登录用户门户后，可在公共账号处管理授权的用户，具体可参考**公共账号**。

----结束

删除账号

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“资源 > 应用”。

步骤3 在应用页面，单击某应用进入应用信息页面。

步骤4 单击应用图标，默认进入该应用的通用信息页面。

步骤5 在左侧导航栏选择“授权管理 > 公共账号”进入公共账号页面。

步骤6 在待删除的公共账号操作列选择“更多 > 删除 ”。

步骤7 单击“确定”，可删除账号。

----结束

4.3.2.10 管理 API 权限

API权限支持管理员在OneAccess管理门户中，授权需要调用API产品的应用，具体操作请参考**授权内置API产品**。

授权API后，可以调用API实现相关接口功能，具体操作请参考**调用内置API产品**。

4.3.2.11 管理应用侧权限

如果需要OneAccess用户根据相应的权限访问企业应用，可以通过应用侧权限实现。授予用户权限后，如需用户携带权限信息返回给应用系统，需配置映射，具体可参考**映射配置**。

应用侧权限根据授权的精细程度分为基于角色和基于角色、权限、资源的权限管理。

基于角色的应用权限管理

根据用户的工作职能定义权限的一种粗粒度授权机制。该机制以用户的职能为粒度，将用户划分到相应的角色， 角色与其对应的权限由企业应用维护。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“资源 > 应用”。

步骤3 在应用页面，单击某应用进入应用信息页面。

步骤4 在应用侧权限模块，单击“配置”进入应用侧权限页面。

步骤5 单击“基于角色的应用权限管理”，填写角色信息，可单击“继续添加”一次添加多个角色，单击“保存”，添加完成后，在应用侧权限下会生成一个应用侧角色菜单，会显示已添加的角色列表，即可开启基于角色的应用权限管理。

----结束

基于角色的应用权限管理包括：添加角色、编辑、添加成员、删除。

- 在应用侧角色页面，单击“添加角色”，输入“角色名称”和“角色代码”，单击“确定”完成角色添加。
- 单击角色操作列的“编辑”，可修改角色名称。
- 单击角色操作列的“添加成员”，选择需要授予角色权限的账号，单击“确定”，完成角色授权。如需对一个账号授予多个角色权限时，通过单击 开启支持一人多角色即可实现，该功能开启后不可关闭。
- 单击角色操作列的“删除”，单击弹窗中的“确定”，可删除角色。当应用角色存在被引用的账号时，不可删除。

基于角色、权限、资源的应用权限管理

可以精确到应用的具体角色、权限、资源的一种细粒度授权机制。该机制能够满足企业对权限最小化的安全管控要求。例如，对于应用的数据资源，可以控制部分用户对其进行指定的操作。

当对角色授予树形结构的资源权限时，资源的父级与子级不存在父子关系，可独立授权。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“资源 > 应用”。

步骤3 在应用页面，单击某应用进入应用信息页面。

步骤4 在应用侧权限模块，单击“配置”进入应用侧权限页面。

步骤5 在应用侧权限页面，单击“基于角色、权限、资源的应用权限管理”，输入“资源名称”、“资源代码”，选择“数据结构”。可单击“继续添加”添加多个资源。也可单击“使用应用机构”直接调用应用机构信息。

步骤6 单击“下一步，输入“权限名称”、“权限代码”，选择“使用资源”和“权限类型”，可单击“继续添加”可以一次添加多个相应的权限。

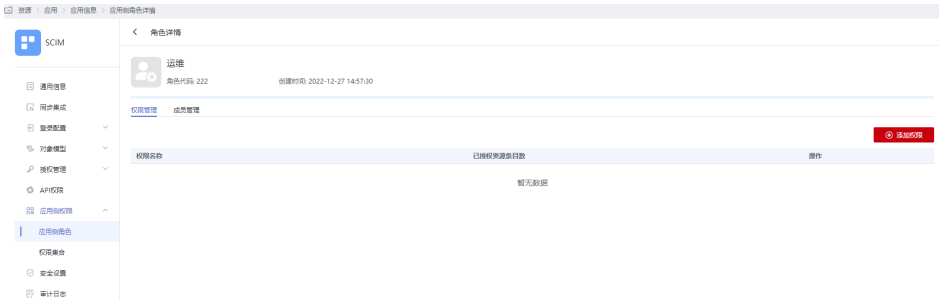
步骤7 单击“下一步”输入“角色名称”和“角色代码”，可单击“继续添加”可以一次添加多个相应的角色，单击“完成”即可开启基于角色、权限、资源的应用权限管理。在应用侧权限下会生成应用侧角色、权限集合菜单，在相应菜单的右侧会显示已添加的角色、权限列表。

----结束

应用侧角色包括添加角色、编辑角色、添加权限、添加成员、删除角色、权限管理、成员管理。

- 在应用侧角色页面，单击“添加角色”，输入“角色名称”和“角色代码”，单击“确定”完成角色添加。
- 单击角色操作列的“编辑”，可修改角色名称。
- 单击角色操作列的“添加权限”，选择权限名称和资源，资源可选全部资源，也可指定资源，单击“确定”完成权限添加。
- 单击角色操作列的“添加成员”，选择需要授予角色权限的账号，单击“确定”，添加成功后，可在相应资源的已授权角色列表中查看，如需对一个账号授予多个角色权限时，通过单击  开启支持一人多角色即可实现，该功能开启后不可关闭。
- 单击角色操作列的“删除”，单击弹窗中的“确定”，可删除角色。当应用角色存在被引用的账号时，不可删除。
- 单击角色名称，进入角色详情的“权限管理”页签，单击“添加权限”，可对角色进行授权。

图 4-25 添加权限



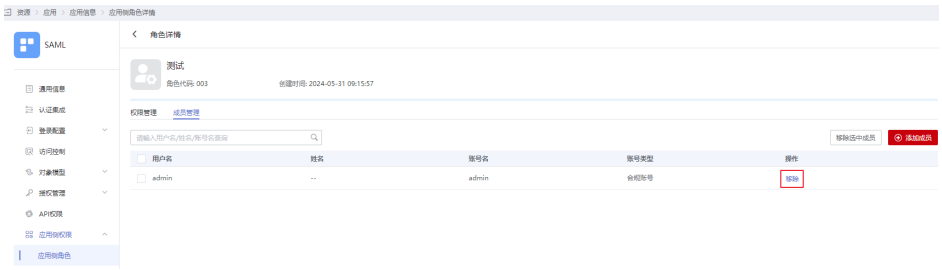
- 在“权限管理”页签，单击权限列表操作列的“编辑”，可编辑权限。
- 在“权限管理”页签，单击权限列表操作列的“取消授权”，可对角色取消授权该权限。

- 单击角色名称，进入角色详情的“权限管理”页签，切换至“成员管理”页签。
  - 单击“添加成员”，可对角色添加成员。

图 4-26 添加成员

- 在成员管理页面，勾选需要移除的成员，单击“移除选中成员”，可一次移除多个成员，也可单击成员列表操作列的“移除”，可移除对应成员。

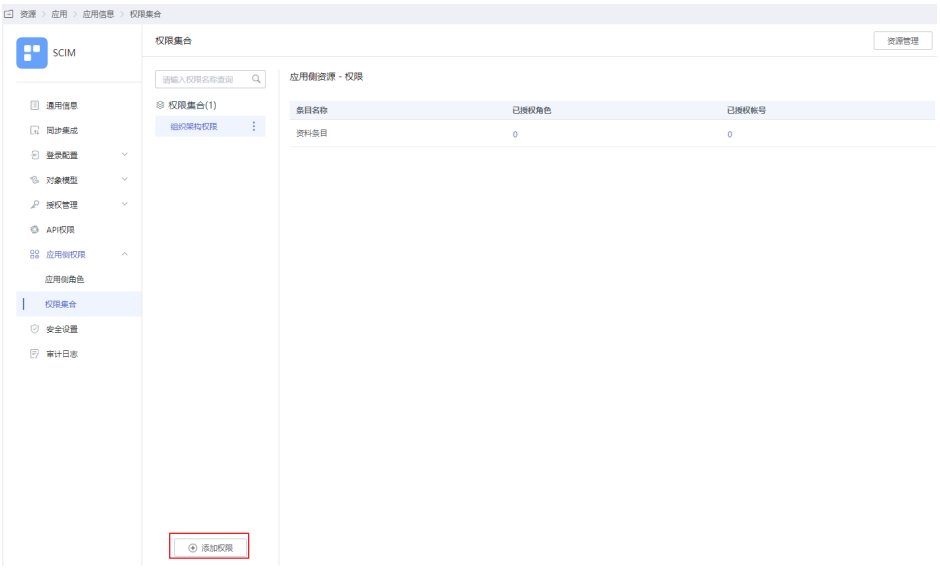
图 4-27 移除成员



权限集合包括权限管理和资源管理。

- 权限管理
  - 在权限集合页面，单击“添加权限”，可添加权限，权限代码唯一。

图 4-28 添加权限



- 单击权限名称右侧的，选择“详情”可查看权限详情，包括权限的名称、代码以及使用资源等。

图 4-29 查看权限详情

- 单击权限名称右侧的，选择“编辑”可编辑权限的名称、类型。
- 单击权限名称右侧的，选择“删除”可删除权限。

- 资源管理

  在应用侧资源中，可以将应用机构作为一种资源，对应用机构的维护可参考**管理应用机构**。如需使用应用机构，需开启应用机构模型，具体可参考**应用机构模型**。资源的数据结构包含树形和列表方式，其中，树形结构的资源支持多层级结构，可按需创建。应用机构的数据结构默认为树形。

  条目是资源的子集，对资源的各项操作，包括新增、编辑、删除同样适用于条目，操作方法类似。以下以资源为例进行介绍。

  a. 在权限集合页面，单击“资源管理”，进入应用侧资源页面。
  b. 单击“新增资源”，填写资源名称、资源代码，选择数据结构。
  c. 填写完成后，单击“确定”，资源添加成功，应用侧资源列表显示已添加的资源。

  资源管理的操作有：添加条目、编辑资源、删除资源。

- 单击资源操作列的“添加条目”，可对资源添加条目。当资源的数据结构为树形时，可对条目继续添加子条目。归属于同一个资源的条目代码唯一。
- 单击资源操作列的“编辑”，可修改资源。如需修改条目，单击相应条目操作列的“编辑”即可。单击应用机构的“编辑”后，会进入应用机构的页面，对应用机构的维护可参考**管理应用机构**。
- 单击资源操作列的“删除”，可删除资源。如需删除条目，单击相应条目操作列的“删除”即可。

4.3.2.12 安全设置

在安全设置中，可以配置调用开放API接口的服务器出口IP，不配置时可正常调用。支持最后一位为*号通配的IP格式。如需输入多个以英文逗号分隔，最多允许10个IP， 例如（192.168.0.*,192.168.1.1）。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“资源 > 应用”。

步骤3 在应用页面，单击某应用进入应用信息页面。

步骤4 单击应用图标，进入应用“通用信息”页面。

步骤5 选择“安全设置”。

步骤6 在输入框输入有效的IP后，单击“保存”。

----结束

4.3.2.13 审计日志

在审计日志中可以查看管理员对该应用的操作记录，同时，可以通过开始及结束时间和管理员名称进行搜索相应操作记录。

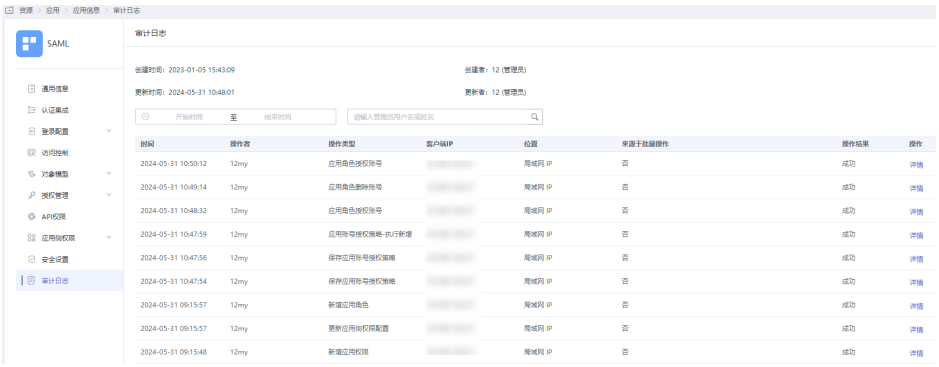
步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“资源 > 应用”。

步骤3 在应用页面，单击某应用进入应用信息页面。

步骤4 单击应用图标，进入应用“通用信息”页面。

步骤5 选择“审计日志”可查看管理员对该应用的操作记录。



----结束

4.3.3 企业 API 管理

4.3.3.1 授权内置 API 产品

管理员在OneAccess管理门户中，授权需要调用API产品的应用。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“资源 > 企业API”。

步骤3 在企业API页面，选择“系统API产品 > 内置API”，进入“修改API产品”页面，切换“应用授权”页签，单击目标应用操作列的“授权”，即可授权使用API产品的应用。

步骤4 在应用中，授权具体的API。添加应用请参考**集成企业应用**。

说明

如果企业应用只需要调用**auth_api**（自定义绑定、注册、绑定并注册场景）的权限接口，需设置该应用的认证集成方式为**OPEN_API**，如果不需要调**用auth_api**的权限接口，则按需设置认证集成方式。

1. 在导航栏中，选择“资源 > 应用”。
2. 单击**步骤3**中授权的应用名称。
3. 单击应用图标，进入通用信息页面。
4. 选择“API权限 > 内置API”，在API权限页面，单击某一权限代码右侧操作列的“授权”则授权成功。其中权限与接口对应关系如下表。

表 4-19 权限与接口对应表

权限代码	权限描述	对应接口描述	对应接口URL	备注
user_all	用户管理接口的读写权限	创建用户	POST /api/v2/tenant/users	-
		修改用户	PUT /api/v2/tenant/users/{user_id}	-
		删除用户	DELETE /api/v2/tenant/users/{user_id}	-

权限代码	权限描述	对应接口描述	对应接口URL	备注
		禁用用户	PUT /v2/tenant/users/{user_id}/disable	-
		启用用户	PUT /v2/tenant/users/{user_id}/enable	-
		修改密码	PUT /api/v2/tenant/users/{user_id}/change-password	-
		校验原密码修改用户密码	PUT /api/v2/tenant/users/{user_id}/change-password-verify	-
		用户授权应用账号	POST /api/v2/tenant/users/{user_id}/applications/{application_id}/accounts	-
		根据用户id查询用户详情	GET /api/v2/tenant/users/{user_id}	user_read权限
		获取用户所有授权的应用账号	GET /api/v2/tenant/users/{user_id}/accounts	user_read权限
		查询用户列表	GET /api/v2/tenant/users	user_read权限
org_all	组织管理接口的读写权限	创建组织	POST /api/v2/tenant/organizations	-
		修改组织	PUT /api/v2/tenant/organizations/{org_id}	-
		删除组织	DELETE /api/v2/tenant/organizations/{org_id}	-
		查询组织详情	GET /v2/tenant/organizations/{org_id}	org_read权限
		查询组织列表	GET /api/v2/tenant/organizations	org_read权限
account_all	账户管理接口的读写权限	创建应用账号	POST /api/v2/tenant/applications/{application_id}/accounts/basic-account	-
		更新应用账号	PUT /api/v2/tenant/applications/{application_id}/accounts/{account_id}	-

权限代码	权限描述	对应接口描述	对应接口URL	备注
		删除应用账号	DELETE /api/v2/tenant/applications/{application_id}/accounts/{account_id}	-
		获取应用账号列表	GET /v2/tenant/applications/{application_id}/accounts	account_read权限
		获取应用账号详情	GET /api/v2/tenant/applications/{application_id}/accounts/{account_id}	account_read权限
		禁用应用账号	PUT /api/v2/tenant/applications/{application_id}/accounts/{account_id}/disable	-
		启用应用账号	PUT /api/v2/tenant/applications/{application_id}/accounts/{account_id}/enable	-
app_org_all	应用机构管理接口的读写权限	获取应用已授权应用机构列表	GET /api/v2/tenant/applications/{application_id}/organizations	app_org_read权限
		查询应用机构详情	GET /api/v2/tenant/applications/{application_id}/organizations/{org_id}	app_org_read权限
		新增应用机构	POST /api/v2/tenant/applications/{application_id}/organizations	-
		修改应用机构	PUT /api/v2/tenant/applications/{application_id}/organizations/{org_id}	-
		删除应用机构	DELETE /api/v2/tenant/applications/{application_id}/organizations/{org_id}	-
app_role_all	应用侧角色接口的读写权限	新增应用侧角色	POST /api/v2/tenant/applications/{application_id}/role	-
		修改应用侧角色信息	PUT /api/v2/tenant/applications/{application_id}/role/{role_id}	-
		删除应用侧角色	DELETE /api/v2/tenant/applications/{application_id}/role/{role_id}	-

权限代码	权限描述	对应接口描述	对应接口URL	备注
		新增应用侧角色成员	POST /api/v2/tenant/applications/{application_id}/role-member	-
		删除应用侧角色成员	DELETE /api/v2/tenant/applications/{application_id}/role-member	-
		查询应用侧角色列表	GET /api/v2/tenant/applications/{application_id}/role-list	app_role_read
		查询应用侧角色详情	GET /api/v2/tenant/applications/{application_id}/role/{role_id}	app_role_read
		查询应用侧角色成员列表	GET /api/v2/tenant/applications/{application_id}/role-member-list/{role_id}	app_role_read
all	OAP全部接口读写权限	包含以上所有接口	-	-

----结束

4.3.3.2 调用内置 API 产品

授权API后，可以调用API实现相关接口功能。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“资源 > 企业API”，单击待调用的API产品。

步骤3 在“应用授权”页签，单击操作列的“授权”，授予指定应用调用该内置API的权限。

步骤4 在导航栏中，选择“资源 > 应用”，单击应用名称，进入“应用信息”页面。

步骤5 在“应用信息”页面，获取应用的client_id与client_secret。

步骤6 单击“应用信息”页的应用名称，进入该应用的“通用信息”页面。

步骤7 选择“API权限”，进入API权限页面，参考**步骤4**授予应用所需API权限。

步骤8 根据**6**获取到的client_id与client_secret，获取access_token，详见**获取访问凭据**。

步骤9 携带已授权的access_token请求OneAccess的内置接口。

----结束

4.3.3.3 修改内置 API 产品

在OneAccess管理门户可以修改内置API，其通用信息不支持修改。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“资源 > 企业API”。

步骤3 在企业API页面，选择“系统API产品 > 内置API”，进入企业API详情页面。

步骤4 切换到“应用授权”页签，修改应用授权。单击应用名称操作列的“授权”或“取消授权”可以按需授权/取消授权调用内置API的企业应用。添加应用请参考**集成企业应用**。

步骤5 切换到“权限信息”页签修改权限信息。单击目标权限操作列的“修改”，可修改权限描述，并勾选设置默认权限。

表 4-20 权限参数

参数	说明
* 权限代码	权限code，支持英文和下划线。
权限描述	描述信息。
设置默认权限	默认不勾选。 • 若勾选，该API产品权限授权应用后，不需要在应用中再次授权，即应用默认拥有该权限。 • 若需要在应用中取消授权的默认权限，则需要修改为非默认权限后取消授权。

步骤6 切换到“审计日志”页签查看审计日志。可以查看API产品的操作记录。

----结束

4.3.3.4 添加自定义 API 产品

OneAccess管理员在OneAccess管理门户中添加企业需要的自定义API产品。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“资源 > 企业API”。

步骤3 在企业API页面，单击自定义API产品下的“添加自定义API产品”。

步骤4 在“添加企业API”页面，上传产品LOGO，填写产品名称和描述，单击“确定”，自定义API产品添加完成，自定义API产品列表中显示已添加的API产品。

----结束

4.3.3.5 配置自定义 API 产品

添加API产品后，需要添加企业的开放接口并进行授权。（自定义API可选择性添加内置API的权限代码，从而达到目标应用授权API权限的便利，同时自定义API也可添加外部API权限。）授权后，相应的应用才可以正常使用。

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 > 企业API”。

步骤3 在企业API页面，单击指定自定义API产品，进入“修改API产品”页面。

步骤4 在“通用信息”页签，修改产品Logo、产品名称、产品描述。

步骤5 切换到“应用授权”页签，修改应用调用该API的权限。如需添加应用请参考**添加应用**。

说明

授权应用后，需在应用中，授权具体的API，可参考**步骤4**。

步骤6 切换到“权限信息”页签，单击“添加”，添加权限代码（权限代码可选择于内置API中的权限代码，或是外部的API的权限代码）。

步骤7 切换到“审计日志”页签，查看审计日志。可以查看API产品的操作记录。

----结束

4.3.3.6 删除自定义 API 产品

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 > 企业API”。

步骤3 在企业API页面，选择“自定义API产品”，单击目标API产品右上角的，单击“删除”，在提示框中单击“确定”删除自定义API产品成功。

说明

请谨慎删除API产品。删除企业API后拥有该API权限的应用将无法正常使用该API。

----结束

4.4 认证管理

4.4.1 认证源管理

OneAccess支持配置多种第三方认证源，包括个人社交认证、企业社交认证、企业认证源，为企业用户登录OneAccess提供便利。管理员可以根据企业需要添加、修改和删除认证源。

说明

OneAccess同时支持本地认证和第三方认证机制，客户在配置认证方式时，建议选择安全的认证方式。

下面以Welink为例说明个人社交认证的配置方法。如需了解认证源配置方法，请参考**集成认证源**。

添加认证源

说明

- 请确保管理员已拥有WeLink开放平台账号管理员权限。
- 请确保管理员已在WeLink开放平台创建了应用。具体可以参考**WeLink对接文档**。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“认证 > 认证源管理”。

步骤3 在认证源管理页面，选择“企业社交认证 > WeLink”。

步骤4 在“添加WeLink认证源”页面，填写应用参数。

表 4-21 配置参数

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。
AppSecret	WeLink开放平台创建应用获取的 client_secret。
关联源属性	WeLink开放平台创建应用时配置的用户属性，支持mobileNumber、userNameCn、userNameEn、userEmail、corpUserId。
关联用户属性	WeLink对接OneAccess的映射属性。可在手机号、用户ID、用户名、邮箱中任选一个。
未关联用户时	当用户使用WeLink扫码登录时，可根据该设置继续操作。可在绑定、绑定或注册、自动创建用户、失败中任选一个。

步骤5 单击“保存”，成功添加认证源。

----结束

修改认证源

管理员可以根据需要修改认证源。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“认证 > 认证源管理”。

步骤3 在认证源管理页面，选择“企业社交认证 > WeLink”。

步骤4 在“添加WeLink认证源”页面，修改应用参数。

步骤5 单击“保存”，成功修改认证源。

----结束

删除认证源

说明

- 请谨慎删除认证源 ，删除以后该认证源的所有数据将被删除且不可恢复。
- 企业社交认证源不支持删除，您可以在应用中禁用此认证方式。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“认证 > 认证源管理”。

步骤3 在认证源管理页面，单击需要删除的认证源。

步骤4 在该认证源界面，单击认证源操作列的“删除”。

步骤5 在弹窗中确认并单击“确定”，删除认证源成功。

----结束

4.4.2 管理区域

您可以添加区域规则，方便您在访问控制中进行配置。

添加区域

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“认证 > 区域范围”。

步骤3 在区域范围页面，单击“添加区域”。

步骤4 在添加区域页面，填写区域信息。

表 4-22 区域信息

参数	说明
* 区域名称	企业部门的分布区域命名，如开发区域。支持自定义。
* 区域网段	企业部门所在的具体IP范围，仅支持CIDR格式。不可重复。
描述	区域的描述，支持自定义。

步骤5 单击“保存”，完成区域添加。

----结束

编辑区域

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“认证 > 区域范围”。

步骤3 在区域列表中，单击目标区域右侧的操作栏的“编辑”，可以修改表4-22。

步骤4 单击“保存”。

----结束

删除区域

说明

请谨慎删除区域，删除以后不可恢复。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“认证 > 区域范围”。

步骤3 在区域列表中，单击目标区域右侧的操作栏的“删除”。

步骤4 在确认提示框中单击“确定”，删除区域。

----结束

4.4.3 管理认证策略

OneAccess对用户的访问进行统一管理，其管理方式就是添加认证策略，通过认证策略给选定的用户设置访问时间、设备类型、区域范围等权限，满足设置的访问条件的用户可以设定登录时的验证方式如二次认证、拒绝、允许访问三种情况。

添加认证策略

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“认证 > 认证策略”。

步骤3 在认证策略页面，单击“添加策略”。

步骤4 在添加策略页面进行认证策略的相关配置。

表 4-23 策略信息

参数	说明
*策略名称	为添加的认证策略进行命名便于管理。
描述	为添加的认证策略添加描述信息。
用户条件	选择用户范围，可在下拉菜单选择：所有用户、满足条件的用户和不满足条件的用户。
访问时间	用户访问的时间，可在下拉菜单选择：任意时间、在该时间范围内和不在该时间范围内。
设备类型	用户访问的设备，可在下拉菜单选择：浏览器、桌面端和移动端。
区域范围	用户区域范围设置IP地址范围，可在下拉菜单选择：不限定、中国区、非中国区、属于下列范围和不属于下列范围。
认证源类型	选择认证源访问的用户，可在下拉菜单选择：不限定、指定认证源和非指定认证源。
风险行为	选择触发某个风险事件的用户，可在下拉菜单选择可以多选，同风险行为管理中的风险事件一致。
访问控制	设置满足条件的用户登录时的验证方式，分别是：允许访问、拒绝和二次认证。 **说明** 当选择二次认证时，有五种认证方式：OTP、短信、邮件、FIDO2和指纹认证。

步骤5 单击“保存”，完成认证策略添加。

----结束

编辑认证策略

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“认证 > 认证策略”。

步骤3 在认证策略页面，单击待操作的策略“操作”列的“编辑”进入编辑策略页面，可修改认证策略配置信息。

步骤4 单击“保存”编辑完成。

----结束

删除认证策略

如果不再需要认证策略，可以删除指定策略。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“认证 > 认证策略”。

步骤3 在待删除的策略右侧“操作”列，单击“删除”。

步骤4 在弹出框中单击“确定”删除该策略。

----结束

禁用认证策略

如需要在某个时间段不使用认证策略，可通过更改认证策略的状态来实现，即可禁用认证策略。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“认证 > 认证策略”。

步骤3 在待操作的行为的“状态”列，单击  。

步骤4 在弹出框中单击“确定”禁用该策略。

----结束

启用认证策略

如已禁用的认证策略，需要再次使用该认证策略时可重新启用该认证策略。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“认证 > 认证策略”。

步骤3 在待操作的策略的“状态”列，单击  。

步骤4 在弹出框中单击“确定”启用该策略。

----结束

调整策略优先级

最多可添加10条认证策略，添加的认证策略存在优先级，可通过在认证策略列表中拖拽某认证策略改变其优先级。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“认证 > 认证策略”。

步骤3 向上或向下拖动待调优先级的策略，放置到合适的顺序。

----结束

4.5 安全管理

4.5.1 管理管理员权限

OneAccess支持对管理门户的权限进行管理，您可以根据需要添加管理员、管理组，并配置相应的使用权限。

管理员分为超级管理员、分级管理员、系统管理员：

- 超级管理员：拥有管理门户所有组织架构、应用、菜单的管理权限。
- 分级管理员：拥有管理门户所授权的组织架构、应用、菜单（首页菜单除外）的管理权限。
- 系统管理员：是由管理面租户子账号登录管理门户生成的分级管理员账号，拥有管理门户所有组织架构、应用的管理权限，及除管理员权限功能外所有菜单的管理权限。

说明

系统管理员默认在系统管理组，该管理组在管理门户中不可见。

添加超级管理员

租户主账号登录管理门户，在管理门户添加管理员，并给管理员加入超级管理组，获得管理门户所有管理权限。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“安全 > 管理员权限”。

步骤3 在权限管理页面，进入“管理员”页签，单击“添加管理员”。

步骤4 在添加管理员页面，输入管理员信息。

表 4-24 管理员信息

管理员信息	说明
用户名	管理员的用户名。支持由字母开头的字符，不支持汉字。
姓名	管理员的姓名。支持汉字。
手机号	管理员的手机号。不可与其他管理员重复。

管理员信息	说明
邮箱	管理员的邮箱。不可与其他管理员重复。
密码	管理员的密码。
确认密码	与**密码**一致。
管理员权限	分为“管理组”和“自定义”，此处默认选中“管理组”。
管理组	选择已有管理组，获得该管理组拥有的权限，此处默认“超级管理组”。

步骤5 单击 “保存”，超级管理员添加完成，超级管理员列表中显示已添加的超级管理员。

----结束

添加分级管理员

拥有管理员权限的管理员登录管理门户，在管理门户添加管理员，并给管理员赋予最大不超过自身权限范围的权限，若添加的管理员不属于超级管理员，即为分级管理员。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“安全 > 管理员权限”。

步骤3 在权限管理页面，进入“管理员”页签，单击“ 添加管理员”。

步骤4 在添加管理员页面，输入管理员信息。

表 4-25 管理员信息

管理员信息	说明
用户名	管理员的用户名。支持由字母开头的字符，不支持汉字。
姓名	管理员的姓名。支持汉字。
手机号	管理员的手机号。不可与其他管理员重复。
邮箱	管理员的邮箱。不可与其他管理员重复。
密码	管理员的密码。
确认密码	与**密码**一致。

步骤5 选择管理员权限。

- 管理组：默认选中“管理组”，在“管理组”下拉框中选择管理员所属管理组，拥有管理组配置的管理权限，此处不选择默认的“超级管理组”，可自定义管理组所拥有的权限，添加管理组请参考**添加管理组**。
- 自定义：选中“自定义”，分级管理员不属于任何管理组，为分级管理员自定义组织架构、应用、菜单的管理权限，可默认选择全部部门、全部应用及全部菜单，也可指定部门、应用及菜单（首页菜单除外）。

步骤6 单击“保存”，分级管理员添加完成，分级管理员列表中显示已添加的分级管理员。

----结束

修改管理员信息

在管理员页面，单击需要修改信息的管理员姓名，查看管理员详情，单击管理员详情页面的“修改”，可以修改管理员的信息、所属管理组。

说明

- 如果需要修改企业创建人的信息，请参考**设置租户类型**。
- 修改超级管理员的管理组为非超级管理组或自定义权限范围后，该超级管理员转为分级管理员。

修改管理员密码

在管理员页面，单击需要修改信息的管理员姓名，查看管理员详情，单击管理员详情页面的“修改密码”，在修改密码页面，输入新密码并单击“保存”，完成密码修改。

说明

超级管理员中的创建人，以及系统管理员，无法修改密码。

删除管理员

在管理员页面，单击需要修改信息的管理员姓名，查看管理员详情，单击管理员详情页面的“删除”，在弹窗中确认并单击“确定”，删除成功。

说明

请谨慎删除管理员，删除后该管理员无法访问管理门户，如有需要请再次添加，具体方法请参考**添加超级管理员**或**添加分级管理员**。

添加管理组

管理员可以创建管理组，并给管理组授予权限，然后修改管理员所属管理组 ，使得管理组中的管理员获得相应的权限。

说明

给子管理组授权菜单权限的时候，没有首页菜单选项。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“安全 > 管理员权限”。

步骤3 在左侧的权限管理页面，切换到“管理组”页签。

步骤4 在左侧的管理组页面，单击需要添加子节点的管理组名称，在右侧管理组详情页面，单击“添加子管理组”。

步骤5 在添加管理组页面，输入管理组名称，配置需要的组织架构、应用以及菜单权限，单击 “保存”，管理组添加完成，管理组列表中显示已添加的管理员。

----结束

修改管理组信息

说明

当管理组的权限发生变化时，属于该管理组的管理员权限随之变化。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“安全 > 管理员权限”。

步骤3 在左侧的权限管理页面，切换到“管理组”页签。

步骤4 在管理组页面，单击需要修改的管理组。

步骤5 在右侧管理组详情页面，单击“修改”。可以修改管理组的名称和权限。

步骤6 单击“保存”。

----结束

删除管理组

删除管理组前，请确保该管理组无成员。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“安全 > 管理员权限”。

步骤3 在左侧的权限管理页面，切换到“管理组”页签。

步骤4 在管理组页面，单击需要删除的管理组。

步骤5 在右侧管理组详情页面，单击“删除”。

步骤6 在弹出确认框单击“确定”，删除成功。

----结束

4.5.2 管理密码策略

OneAccess为企业提供安全的密码策略，企业管理员可以通过密码强度设置、登录安全设置、高级设置、密码初始化设置保障企业用户的账号安全。

说明

- 建议设置密码策略，保证用户密码都是满足密码策略的安全密码。
- 密码策略对OneAccess实例中所有用户生效。

密码强度设置

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“安全 > 密码策略”，进入密码策略页面。

步骤3 单击“密码强度设置”区域可进入修改页面。可设置密码长度、密码复杂度、字符校验、是否开启密码包含用户信息检查和弱密码字典库。

- 密码长度。

  设置密码的长度范围。最小长度默认为8个字符，最大长度默认为18个字符。最小长度和最大长度可以在8~50个字符之间设置。

- 密码复杂度。

  设置密码需要包含的字符种类和种类数量。例如：至少包含数字、大写字母、小写和特殊字符中的3种。

  说明

  用户密码支持的特殊字符有~!#$%&+-,*:;<=>@_?^、`./ 。

- 字符校验。

  设置密码可以包含重复字符的个数。默认“不可包含重复字符”，如需修改，可以设置相同字符出现的最大次数为1~10之间。设置为1，表示密码中不允许出现相同字符。

- 密码包含用户信息检查。

  设置是否检查密码包含用户信息。默认关闭。开启后，在用户设置密码时，不允许包含用户名、手机号、邮箱前缀、姓名拼音。

- 开启弱密码字典库。

  设置是否开启弱密码检查。开启后，在用户设置密码时，不允许包含弱密码库中的密码。

步骤4 修改完成后，单击“保存”，密码强度设置完成。

----结束

登录安全设置

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“安全 > 密码策略”，进入密码策略页面。

步骤3 单击“登录安全设置”区域可进入修改页面。可设置账号锁定条件和账号解锁时间。

- 账号锁定。

  用户连续登录失败次数达到设定值时，账号会自动锁定。默认10次，可以在1~10次之间进行设置。

  说明

  登录失败次数超过阈值后，将开启滑动验证码，自动计算的阈值为账号锁定次数的三分之一。

- 账号解锁时间。

  用户账号被锁定后，到达设定时长自动解锁。默认3分钟，可以在1~1440分钟之间进行设置。

步骤4 修改完成后，单击“保存”，登录安全设置完成。

----结束

高级设置

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“安全 > 密码策略”，进入密码策略页面。

步骤3 单击“高级设置”区域可进入修改页面。可设置是否开启密码倒写、历史密码和密码过期检查。

- 密码倒写

  设置密码是否可以使用用户名倒写。默认关闭。开启后，用户设置密码时，不允许使用用户名的倒写。

- 历史密码

  设置密码是否可以使用历史密码。默认关闭。开启后，用户设置新密码不能与最近几次的历史密码相同。默认为5次，可以在1~10次之间进行设置。例如设置为3，表示不能使用最近3次的历史密码，在用户设置密码时，如果新密码与历史密码相同，OneAccess将会提示“与历史密码一致，需要重新设置密码”。

- 密码过期

  设置密码有效期和提醒时间。默认关闭。开启后，OneAccess会根据设置的到期时间提示用户修改密码，如选择“跳过”，在密码失效后访问用户门户，会强制要求用户修改密码。默认密码失效时长为120天，必须大于或等于1。默认密码过期提示为5天，必须大于或等于1，但小于或等于密码失效时长。

  说明

  密码过期设置可以强制用户修改密码，提高账号安全性。

步骤4 修改完成后，单击“保存”，高级设置完成。

----结束

密码初始化设置

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“安全 > 密码策略”，进入密码策略页面。

步骤3 单击“密码初始化设置”区域可进入修改页面。可设置是否开启初始化密码和开启初始化密码的通知方式和有效期。

- 开启初始化密码。

  启用初始化密码需添加用户有效联系方式，否则无法通知到用户。已开启初始化密码设置时可选择系统自动生成密码。

- 通知方式。

  通知方式有邮件和短信两种，若使用邮箱通知方式，需先参考**邮件网关配置**；若同时选择邮箱和短信，系统将优先通过邮箱发送用户。

- 初始化密码有效期。

  最长可设置7天有效期。

步骤4 修改完成后，单击“保存”，密码初始化设置完成。

----结束

4.5.3 管理风险行为

OneAccess为企业提供账号异常行为检测功能，在设置的行为状态开启后，系统将按照设定的行为规则进行用户异常行为检测，当触发风险后，系统将实时发送风险告警提示。

异常行为分为四种类型：

- IP异常：账号登录IP地址和常用IP不一致会触发风险。
- 位置异常：账号登录位置和常用位置不一致会触发风险。
- 设备异常：账号登录设备（浏览器，终端设备等）和常用设备不一致会触发风险。
- 账号锁定：用户密码输入错误次数超过密码策略设置阈值，账号会被锁定并且触发风险。

当设置的行为触发风险后，系统按照选择的通知方式实时发送风险告警通知，有三种通知方式：邮件、短信和钉钉。

添加行为

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“安全 > 风险行为管理”。

步骤3 在风险行为管理界面，单击“添加行为”，并设置相关参数。

表 4-26 添加行为

配置	说明
* 行为名称	风险行为的名称。
* 风险类型	风险事件类型。可设置的风险类型有：异常位置、异常设备、异常IP和账号锁定。

配置	说明
位置类型	位置异常范围，根据位置类型选择的位置范围定义位置异常事件。 **说明** 仅当“风险类型”选择为“异常位置”时，才有该参数。
* 次数配置	之前登录常用的IP、设备和位置按次数设为默认值，不是默认值则为异常事件，会在风险事件和风险大盘展示和统计。 **说明** 当风险类型选择为“账号锁定”时，不存在该参数配置，账号锁定功能依靠密码策略，用户错误密码输入次数超过密码策略的阈值，账号则被锁定并标记为风险事件，会在风险事件和风险大盘展示和统计。
描述	对于添加的行为进行说明。

步骤4 单击“确定”，添加行为成功，风险行为管理列表中显示已添加的风险行为，可在“风险类型”进行筛选查询，便于后期对于已添加的行为进行管理。

----结束

编辑行为

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“安全 > 风险行为管理”。

步骤3 在待编辑的行为右侧“操作”列，单击“编辑”可重新设置该行为的配置。

步骤4 单击“确定”修改完成。

----结束

删除行为

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“安全 > 风险行为管理”。

步骤3 在待删除的行为右侧“操作”列，单击“删除”。

步骤4 在弹出框中单击“确定”删除该行为。

----结束

禁用风险行为

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“安全 > 风险行为管理”。

步骤3 在待操作的行为的“状态”列，单击  。

步骤4 在弹出框中单击“确定”禁用该行为。

----结束

启用风险行为

设置的行为状态开启后，系统将按照设定的行为规则进行用户异常行为检测，当触发风险后，系统将实时发送风险告警提示。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“安全 > 风险行为管理”。

步骤3 在待操作的行为的“状态”列，单击  。

步骤4 在弹出框中单击“确定”启用该行为。

----结束

通知设置

当设置的行为触发风险后，系统按照选择的通知方式实时发送风险告警通知。

步骤1 在风险行为管理界面，单击“通知设置”。

步骤2 在“通知设置”弹窗中设置通知方式和对象。

表 4-27 通知设置

配置	说明
* 通知方式	触发风险行为时，系统发送通知的方式。 当前提供邮件、短信、钉钉三种通知方式。如果选择邮件、钉钉通知，请先配置对应网关，详情请参考**邮件网关配置**、**钉钉网关配置**。
* 发送对象	触发风险行为时，系统发送通知的对象。默认发送所有用户，您也可以排除指定用户发送。

步骤3 单击“确定”，完成设置。

----结束

4.6 审计

OneAccess提供的审计功能，可以查看用户、管理员操作日志、风险事件、风险大盘，用于支撑安全分析、审计、资源跟踪和问题定位等常见应用场景。

查看用户操作

查看所有用户在用户中心进行的操作，包括时间、姓名、用户名、操作类型、结果等。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“审计 > 用户操作”，进入用户操作页面。

步骤3 单击用户操作列表操作栏的“查看”，可以查看用户操作详情。

步骤4 单击用户操作页面的“导出”即可导出所有用户操作日志。

----结束

如果您需要查看超过两年的日志，在用户操作页面，单击右上方的“日志归档”，进入用户日志归档页面，单击目标日志操作列的下载即可。解压并打开以后，会详细展示用户的操作时间、姓名、结果、操作类型等信息。

查看管理员操作

查看所有管理员在管理门户进行的操作，包括时间、操作者、操作对象、操作类型等。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“审计 > 管理员操作”，进入管理员操作页面，即可查看管理员操作日志。

步骤3 单击管理员操作页面的“导出”即可导出所有管理员操作日志。

----结束

如果您需要查看超过两年的日志，在管理员操作页面，单击右上方的“日志归档”，进入管理员日志归档页面，单击目标日志操作列的下载即可。解压并打开以后，会详细展示管理员的操作时间、操作对象、操作类型、位置等信息。

风险事件

查看所有用户或管理员已触发的风险事件，包括触发时间、风险类型、登录方式、姓名、用户名等。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“审计 > 风险事件”，进入风险事件页面。

步骤3 可按照起始时间、风险类型、姓名或用户名筛选条件，筛选出符合条件的风险事件。

步骤4 单击风险事件列表操作列的“查看”，可以查看风险事件详情。

----结束

风险大盘

风险大盘从全局角度查看实例下的所有风险操作。OneAccess为了更好的统计和查看风险事件提供了风险大盘模块，风险大盘顶部统一时间筛选条件， 分为今天，近7天，近30天，自定义时间段。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“审计 > 风险大盘”，进入风险大盘页面查看已触发的异常风险行为。

表 4-28 风险大盘

模块	说明
当日风险数	当天触发风险事件的数量。所选时间范围不影响该数量。

模块	说明
风险事件总数	所选时间条件内的风险事件日志总数。
风险用户总数	所选时间条件内触发风险事件用户数量。
当日风险用户数	当天触发风险事件的用户数量。所选时间范围不影响该数量。
触发的风险类型	所选时间范围内，各种异常类型风险事件的数量。
风险用户列表	触发近期风险事件用户列表。单击“更多”跳转到“审计 > 风险事件”页面。
风险事件列表	近期风险事件列表。单击“更多”跳转到“审计 > 风险事件”页面。
登录风险次数	所选时间范围内，各节点新增风险事件的数量。各时间条件下，记录风险事件的节点不同： ● 今日：按小时进行统计，横坐标显示00:00-23:00。 如00:15的风险事件将统计在00:00时间中，9:30的风险事件将会统计在09:00时间中，23:45的风险事件将会显示在23:00时间中。 ● 近7天：按天进行统计，横坐标显示近7天的日期（包含今天）。 ● 近30天： 按天进行统计，横坐标显示近30天的日期。 如今天12月28号，则显示11-29 到 12-28每天的风险事件数。 ● 自定义时间段：按天进行统计，横坐标显示自定义的起止日期。
近10个被检测的异常设备	所选时间范围内，触发风险事件数量TOP10的设备，以设备类型+浏览器为维度划分设备。
被检测的异常IP排行TOP10	所选时间范围内，触发风险事件数量TOP10的位置IP。

----结束

4.7 设置

4.7.1 修改企业信息

在OneAccess管理门户，管理员可以对企业所属行业类型、人员规模、联系人、联系电话、企业地址信息等进行设置。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“设置 > 企业信息”。

步骤3 在企业信息页面，单击“修改”，可以修改基本信息和联系信息，例如，企业全称、联系人信息等，单击“保存”，企业信息修改成功。

----结束

4.7.2 企业配置

4.7.2.1 概述

为了满足企业内部对安全的要求，OneAccess提供了多种认证方式。

管理员可以在通用配置设置用户名规则、管理门户双因子认证、管理门户Welink认证。为了防止用户在“登录认证”、“注册”、“忘记密码”、“VPN双因素”等环节中出现冒名或身份盗用情况发生，管理员可以进行用户协议配置、短信网关配置、语音网关配置、邮件网关配置、钉钉网关配置，通过短信、语音、邮件等对用户的身份进行确认。

4.7.2.2 通用配置

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“设置 > 企业配置”。

步骤3 在左侧导航栏选择“通用配置”，在“通用配置”页面可进行如下配置。

- 用户名规则

  管理员创建用户或导入身份源数据时，用户姓名的拼音会自动填充至用户名，例如，添加用户时，输入姓名为“张三”，添加成功后，该用户的用户名自动显示为“zhangsan”，实现此功能需满足以下条件：

  a. 勾选“启用用户名规则”。

  b. 用户名字段设置为非必填，即选择“用户 > 用户属性定义”，单击“用户名”字段名称操作列的“编辑”，在编辑字段弹框中的“字段校验规则”的“是否必填”不勾选。

  c. 用户名为空，即参考**添加用户**添加用户时，用户名为空。

- 管理门户双因子认证

  勾选“启用双因子认证”后，在登录管理门户时，需要输入密码和手机验证码才可以登录。

- 管理门户WeLink认证

  勾选“启用WeLink认证”并配置参数后，可使用WeLink登录管理门户。

表 4-29 参数

参数	说明
Client Id	WeLink开发平台创建应用获取的 client_id。
Client Secret	WeLink开发平台创建应用获取的 client_secret。
回调地址	平台自动生成且只读，例如，https://xxx.huaweibccastle.com/api/ecb/welink/login。

说明

如需开通管理门户WeLink认证，请确保您已在WeLink开发平台创建了应用。

- "验证码"类信息发送方式配置
  - 当勾选“短信”时，用户登录、注册、忘记密码等场景都会收到短信验证码。
  - 当勾选“钉钉”时，用户登录、忘记密码、二次验证、重置密码场景会优先使用钉钉发送验证码，前提是已参考**钉钉网关配置**配置钉钉网关。
- 国际区号配置

  在下拉框中选择“支持国际区号”和“首选国际区号”。

  配置支持国际区号后需配置首选国际区号，支持国际区号用于用户输入手机号场景选择国家地区，此场景默认选中首选国际区号；未配置首选国际区号时用户输入手机号场景不需要选择国际区号；第一次配置首选国际区号时会将现有用户中手机号未带有国际区号的手机号更新为带有首选国际区号的手机号。

步骤4 单击“保存”。

----结束

4.7.2.3 用户协议配置

管理员在OneAccess控制台配置用户需要遵守的协议和隐私声明，方便用户在首次登录OneAccess用户门户或在用户门户注册用户时，可以清楚的了解自己的权益及约束。

开启及配置用户协议

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“设置 > 企业配置”。

步骤3 在企业配置页面，选择“用户协议配置”。

步骤4 【可选】单击  打开用户协议配置。

说明

用户协议配置默认为关闭状态。开启后，用户在登录/注册时需要勾选所配置的服务条款和隐私条款等内容。

步骤5 单击“编辑”，可以根据界面语言分别设置不同的协议内容。

1. 分别单击界面语言为中文和英文对应的“插入协议”，在“插入协议”弹框，输入协议名称和协议内容。
2. 单击“确定”，配置的协议名称便显示在输入框，如：我已阅读并同意{*协议名称*}。您可单击输入框中的协议名称，查看协议详情。

说明

可同时插入10条协议。

步骤6 单击“保存”，完成用户协议配置。

----结束

编辑协议

说明

已开启用户协议配置。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“设置 > 企业配置”。

步骤3 在企业配置页面，选择“用户协议配置”。

步骤4 单击“编辑”。

步骤5 单击输入框中的协议名称，在“编辑协议”弹框，可修改协议名称和协议内容。

步骤6 单击“确定”，修改后的协议名称便显示在输入框。

----结束

查看协议签订用户和历史版本

说明

已配置过用户协议。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“设置 > 企业配置”。

步骤3 在企业配置页面，选择“用户协议配置”。

步骤4 单击协议名称，可查看签订用户和协议的历史版本。

- 在“签订用户”页签，可看到签订了此协议的用户信息，包括签订时间、用户名、姓名、版本号、签订位置和签订结果。
- 在“历史版本”页签，可看到此协议的历史版本信息，包括版本号、签订用户数、生效日期和失效日期。可单击“操作”列的“查看”，查看历史协议内容。

----结束

关闭用户协议配置

说明

已开启用户协议配置。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“设置 > 企业配置”。

步骤3 在企业配置页面，选择“用户协议配置”。

步骤4 单击  关闭用户协议配置。关闭后，用户在登录/注册时不需要勾选服务条款和隐私条款等内容。

----结束

4.7.2.4 短信网关配置

短信网关是OneAccess提供给用户的一种通过手机获取信息或验证码的方式，包括内置网关、自定义网关两种方式。

在您购买创建OneAccess时会自动配置短信次数，默认每月发送1000次短信免费，超过此次数就无法发送短信了，当超过后若还需短信服务，请参考下文配置短信网关或联系技术人员添加发送短信次数。

- 内置网关
  - 内置网关”是OneAccess提供给用户的一种获取短信或验证码的方式。当您选择“内置网关”后，可以在短信网关配置页面查看短信的总量和已使用量。
  - 场景和模板预置：在短信网关配置页面，管理员可以查看获取短信的场景和模板，OneAccess对场景和模板已经进行了预置和注册审核。用户在使用相应场景时，会收到预置的短信或验证码信息。
  - 场景测试：如果管理员需要对设置的场景和短信模板进行测试，单击模板操作列的“测试”，在弹窗中选择用户并单击“测试”即可测试短信模板是否有效。
- 自定义网关

  当您选择“自定义网关”后，您需要提前在网关的SMS服务商处申请注册账号，并将网关参数配置到OneAccess中，同时，因“国家短信管理要求”，短信模板需要在SMS服务商平台注册并审核通过，您才可以将其ID/CODE应用到具体的场景中。

  自定义网关的SMS服务商可以选择华为云、阿里云和鸿源云道。以华为云为例。

  a. 登录OneAccess管理门户。
  b. 在导航栏中，选择“设置 > 企业配置”。
  c. 在企业配置页面，选择“短信网关配置”，网关类型选择“自定义网关”，配置基本参数。

  表 4-30 基本配置

参数	是否必填	说明
SMS服务商	是	选择短信服务商，例如“华为云”。
AccessKey ID	是	SMS服务商平台创建短信应用时生成的APP_Key。
AccessKey Secret	是	SMS服务商平台创建短信应用时生成的APP_Secret。
签名名称	是	SMS服务商平台申请短信签名时的签名名称。
验证码签名通道号	是	SMS服务商平台申请验证码短信签名时生成的签名通道号。
通知类签名通道号	否	SMS服务商平台申请通知类短信签名时生成的签名通道号。

参数	是否必填	说明
APP接入地址	是	SMS服务商平台创建短信应用时生成的APP接入地址。

d. 在“发送场景”模块，选择语言，如中文或English，配置模板ID/CODE，单击“保存”，完成华为云自定义网关配置。

说明

模板ID/CODE 对应SMS服务商平台申请短信模板时生成的模板ID。

e. （可选）单击目标场景操作列的“测试”，在弹窗中输入用户名，可以测试短信配置是否成功。

4.7.2.5 语音网关配置

语音网关是OneAccess提供的“语音验证码”功能，当用户的手机无法收到短信验证码时，可以通过配置语音网关发送语音验证码，确保业务的连续性。包括内置网关、自定义网关两种方式。

- 内置网关
  - 使用情况：选择“内置网关”后，可以在语音网关配置页面查看语音的总量和已使用量。
  - 发送场景：在语音网关配置页面，可以查看语音验证码的场景和模板，OneAccess对场景和模板已经进行了预置和注册审核。用户在使用相应场景时，会收到预置的语音验证码信息。
  - 场景测试：如果需要对设置的场景和语音模板进行测试，单击模板操作列的“测试”，在弹窗中选择用户并单击“测试”即可测试语音模板是否有效。
- 自定义网关

  自定义网关需要提前在网关的语音服务商处申请注册账号，并将网关参数配置到OneAccess中，同时，因“国家短信管理要求”，语音模板需要在语音服务商平台注册并审核通过，您才可以将其ID/CODE应用到具体的场景中。自定义网关的语音服务商支持华为云和阿里云。

本章节以语音服务商为华为云为例介绍配置语音网关操作，

前提条件

已购买语音服务。

在 OneAccess 中配置语音网关

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“设置 > 企业配置”。

步骤3 在企业配置页面，选择左侧的“语音网关配置”，单击 开启语音网关，网关类型选择“自定义网关”，配置基本参数。

表 4-31 基本配置

参数	说明
* 语音服务商	选择语音服务商，例如“华为云”。
* AccessKey ID	语音服务商平台添加应用获取的APP_Key。
* AccessKey Secret	语音服务商平台添加应用获取的APP_Secret。
* APP接入地址	语音服务商平台添加应用后获取。
* 主叫号码	语音服务商平台处获取。

步骤4 在“发送场景”模块，选择发送语言，如中文或English，配置模板ID/CODE，单击“保存”，完成华为云自定义网关配置。

步骤5 （可选）单击目标场景操作列的“测试”，在弹窗中输入用户名，可以测试语音网关配置是否成功。

----结束

4.7.2.6 邮件网关配置

邮件网关是OneAccess针对重置用户密码场景，提供给用户的一种通过邮箱获取信息的方式。开启邮件网关后，管理员重置用户密码时，可以选择由OneAccess产生随机密码，并通过邮件的方式发送给用户，该用户将收到邮件密码，登录成功后可以进行密码重置。

本文主要介绍OneAccess配置邮件网关的方法。

前提条件

开启邮箱POP3/SMTP服务，请进入邮箱账号管理页面，根据页面提示，开启POP3/SMTP服务，并保存授权码。

说明

请妥善保管已获取的授权码，如果不慎丢失，可在设置账号页面，根据提示再次生成授权码。

在 OneAccess 中配置邮箱网关

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“设置 > 企业配置”。

步骤3 在企业配置页面，选择左侧的“邮件网关配置”，单击  开启邮件网关，配置基本参数。

表 4-32 基本配置

参数	是否必填	说明
SMTP HOST	是	提供SMTP服务的主机地址。可在提供邮件网关服务平台的帮助文档中获取。
SMTP 端口	是	默认465，指提供SMTP服务的端口。
邮箱地址	是	企业邮箱地址。即系统邮件的发件地址。
发送者名称	是	邮件发件人的名称，支持自定义。
邮箱授权码	是	前提条件中获取的授权码。
安全类型	是	邮件的加密方式，与提供邮件网关服务的平台设置保持一致，可在提供邮件网关服务平台的帮助文档中获取。默认为TLS，选择无或SSL存在安全风险。

步骤4 （可选）单击“模板设置”，可自定义发送模板，按需配置邮件模板。

----结束

4.7.2.7 钉钉网关配置

当“短信验证码”和“语音验证码”都无法满足需求时，可以使用钉钉网关发送验证码，在登录用户门户、忘记密码、二次验证、重置密码、风险预警场景，OneAccess同时支持钉钉发送验证码，您只需要通过配置钉钉网关即可实现。

本文主要介绍OneAccess配置钉钉网关的方法。

前提条件

- 请确保您已拥有钉钉开放平台账号管理员权限。具体可参考钉钉开放平台的帮助文档。
- 请确保您已拥有OneAccess管理门户的访问权限。

在 OneAccess 中配置钉钉认证

在OneAccess中配置钉钉认证源，并建立OneAccess用户与钉钉的绑定关系，确保用户可以正常接收钉钉发送的验证码。

在钉钉开放平台创建小程序

在钉钉开放平台上创建小程序，并授权接口权限，可以建立小程序与钉钉认证源之间的关联关系。

步骤1 登录钉钉开放平台。

步骤2 在钉钉开放平台，选择“应用开发 > 企业内部开发 > 小程序”，设置应用参数，单击“确定创建”后，会自动生成AgentId、AppKey和AppSecret。具体可参考钉钉开放平台的帮助文档。

步骤3 在权限管理处，添加接口权限“通讯录只读权限”。

----结束

在 OneAccess 中配置钉钉网关

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“设置 > 企业配置”。

步骤3 在企业配置页面，选择左侧的“钉钉网关配置”，单击 开启钉钉网关，配置基本参数。

表 4-33 基本配置

参数	说明
* AgentId	钉钉开放平台创建小程序获取的 AgentId。
* AppKey	钉钉开放平台创建小程序获取的 AppKey
* AppSecret	钉钉开放平台创建小程序获取的 AppSecret。

步骤4 （可选）单击目标场景操作列的“测试”，在弹窗中输入用户名，可以测试钉钉网关配置是否成功。

说明

当提示“验证码发送失败：用户未绑定钉钉账号！”，请参考**在OneAccess中配置钉钉认证**绑定钉钉账号。

----结束

4.7.3 管理数据字典

通过配置“数据字典”，管理员可以方便有效地管理和维护企业中与业务相关的一些信息。例如，手机号、省市编码、供应商的区域划分等。数据字典支持列表和树形两种方式。

新增字典

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“设置 > 数据字典”。

步骤3 在数据字典页面，单击页面下方的  。

步骤4 在新增字典页面，填写字典信息，单击“保存”，字典添加完成，字典列表显示已添加的字典。

表 4-34 新增字典

参数	说明
* 字典类型编码	字典的类型编码，不可重复。为了方便维护管理，建议您设置一定的编码规则。
* 字典类型名称	字典的类型名称，不可重复。
是否树形展示	控制字典的显示方式：列表或树形。
备注	描述字典的用途、使用场景等。

步骤5 在左侧字典列表页面，单击目标字典。

说明

- 新增字典项的前提是存在字典，字典项属于字典的子集。
- 只有配置了字典项的字典，才可以在添加用户扩展属性时发挥其作用。

步骤6 在右侧字典页面，单击“新增字典项”，在新增字典项页面，填写字典项信息。

表 4-35 新增字典项

参数	说明
* 字典名称	字典项的父节点。系统默认，不可修改。
* 字典项编码	字典项的唯一标识，不可重复。为了方便维护管理，建议您设置一定的编码规则。
* 字典项名称	字典项的名称，可以重复。
备注	描述字典项的用途、使用场景等。

步骤7 单击“保存”，字典项添加完成，字典项列表显示已添加的字典项。

----结束

修改字典

当与字典关联的用户属性有变化时，可以通过修改字典来完成适配。

- 修改字典属性

  说明

  字典的字典类型编码、是否树形展示不可修改。

  a. 登录OneAccess管理门户。
  b. 在导航栏中，选择“设置 > 数据字典”。
  c. 在待修改的数据字典右侧 中选择“编辑”，打开“编辑字典”弹窗。
  d. 修改字典类型名称和备注，单击“保存”。

  说明

  字典的字典类型编码、是否树形展示不可修改。

- 修改字典项

  a. 登录OneAccess管理门户。
  b. 在导航栏中，选择“设置 > 数据字典”。
  c. 单击待修改的数据字典，在右侧字典项列表中，单击待修改的字典项操作栏的“编辑”。
  d. 修改字典项名称和备注，单击“保存”。

删除字典

说明

如需删除字典，请确保该字典已经解除了与用户属性的关联关系。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“设置 > 数据字典”。

步骤3 在待删除的数据字典右侧 中选择“删除”。

步骤4 在弹窗中确认并单击“确定”，删除成功。

----结束

4.7.4 导入/导出数据

4.7.4.1 导入数据

OneAccess支持以数据导入的方式快速创建批量用户、组织和应用账号。

说明

进行数据导入时，需确保您上传的Excel文件与模板格式一致且为.xlsx，且一次导入的数据不超过1万条。

用户导入

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“设置 > 导入/导出”，默认进入“用户导入”页面。

说明

导入用户的前提是用户所属的组织已存在。如需添加少量组织，请参考**添加组织**。如需批量添加组织，请参考**导入应用机构**。

步骤3 单击“下载导入模板”。

步骤4 打开下载的Excel文档，编辑需要上传的用户信息并保存。

说明

当导入的用户为一人多组织用户时，则组织编码输入多个组织，以英文逗号“,”隔开，默认第一个为主组织。

步骤5 在用户导入页面，单击“选择文件”，选择**步骤4**保存的文件并单击“打开”，获取用户信息 。

步骤6 单击“导入”导入用户数据。

----结束

导入组织

1. 登录OneAccess管理门户。
2. 在导航栏中，选择“设置 > 导入/导出”，默认进入“用户导入”页面。
3. 在页面左侧选择“组织导入”，进入“组织导入”页面。
4. 单击“下载导入模板”。
5. 打开下载的Excel文档，根据文档说明编辑需要上传的组织信息并保存。
6. 在组织导入页面，单击“选择文件”，选择**5**保存的文件并单击“打开”，获取组织信息 。
7. 单击“导入”导入组织数据。

导入应用账号

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“设置 > 导入/导出”，默认进入“用户导入”页面。

步骤3 在页面左侧选择“应用账号导入”，进入“应用账号导入”页面。

说明

导入应用账号的前提是应用已存在。如需添加应用，请参考**添加应用**。

步骤4 单击“下载导入模板”。

步骤5 打开下载的Excel文档，根据文档说明编辑需要上传的账号信息并保存。

步骤6 在应用账号导入页面，单击“选择文件”，选择**步骤5**保存的文件并单击“打开”，获取应用账号信息 。

步骤7 单击“导入”导入应用账号数据。

----结束

导入公共账号

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“设置 > 导入/导出”，默认进入“用户导入”页面。

步骤3 在页面左侧选择“公共账号导入”，进入“公共账号导入”页面。

说明

导入公共账号的前提是应用已存在。如需添加应用，请参考**添加应用**。

步骤4 单击“下载导入模板”。

步骤5 打开下载的Excel文档，根据文档说明编辑需要上传的账号信息并保存。

步骤6 在公共账号导入页面，单击“选择文件”，选择**步骤5**保存的文件并单击“打开”，获取公共账号信息 。

步骤7 单击“导入”导入公共账号数据。

----结束

导入应用机构

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“设置 > 导入/导出”，默认进入“用户导入”页面。

步骤3 在页面左侧选择“应用机构导入”，进入“应用机构导入”页面。

说明

导入应用机构的前提是应用已存在，如需添加应用，请参考**添加应用**。

步骤4 单击“下载导入模板”。

步骤5 打开下载的Excel文档，根据文档说明编辑需要上传的应用机构信息并保存。

步骤6 在应用机构导入页面，单击“选择文件”，选择**5**保存的文件并单击“打开”，获取应用机构信息 。

步骤7 单击“导入”导入应用机构数据。

----结束

导入应用侧资源条目

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“设置 > 导入/导出”，默认进入“用户导入”页面。

步骤3 在页面左侧选择“应用侧资源条目导入”，进入“应用侧资源条目导入”页面。

步骤4 单击“下载导入模板”。

步骤5 打开下载的Excel文档，根据文档说明编辑需要上传的应用侧资源条目信息并保存。

步骤6 在应用侧资源条目导入页面，单击“选择文件”，选择5保存的文件并单击“打开”，获取应用侧资源条目信息 。

步骤7 单击“导入”导入应用侧资源条目。

----结束

4.7.4.2 导出数据

导出用户

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“设置 > 导入/导出”，默认进入“用户导入”页面。

步骤3 在页面左侧选择“数据导出 > 用户导出”进入“用户导出”页面。

步骤4 单击“导出”，在弹出页面，可选择导出用户范围（全部/指定范围）。

步骤5 单击“确定”，弹出“安全验证”框，单击“获取验证码”获取验证码并输入后单击“确定”，用户数据导出成功。

----结束

导出组织

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“设置 > 导入/导出”，默认进入“用户导入”页面。

步骤3 在页面左侧选择“数据导出 > 组织导出”进入“组织导出”页面。

步骤4 单击“导出”，在弹出页面，可选择导出组织范围（全部/指定范围）。

步骤5 单击“确定”，弹出“安全验证”框，单击“获取验证码”获取验证码并输入后单击“确定”，组织数据导出成功。

----结束

4.7.5 界面配置

OneAccess提供了界面定制功能，管理员可以根据需要自定义用户门户的登录界面、注册界面和找回密码界面。管理员可以选择OneAccess提供的内置模板，也可以自定义模板。在自定义模板中，您可以修改顶部区域、表单区域和底部区域的透明度、主题色、内容颜色等，也可以修改底图，以及认证窗体的左中右布局位置等参数。

设置全局参数

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“设置 > 界面配置”，进入界面配置页面。

步骤3 单击右侧的“全局参数配置”，在全局参数配置页面单击右上角“编辑”，可以配置全局参数。

表 4-36 全局参数配置

全局参数		说明
基本配置	PC 端企业Logo	PC 端登录页面的Logo。 支持png/jpg/gif格式，大小不超过50K，建议尺寸42*180px。
	移动端企业Logo	移动端登录页面的Logo。 支持png/jpg/gif格式，大小不超过50K，建议尺寸140*140px。
	网站图标Favicon	网站的标志。 支持ico格式，大小不超过5K，建议尺寸32*32px。
用户门户登录配置	人机校验	登录页面的一种二次校验方式，默认滑动验证码，不可修改。
	开启找回密码	默认开启，当用户忘记密码时，可在用户门户进行忘记密码操作。
	开启注册	默认关闭，开启后，如果用户无用户门户账号，可在登录页面进行注册操作。 **须知** 当开启后，外部用户也可以注册新账号，新注册的账号所属组织默认为根组织。请谨慎操作。
	Logo右侧文字中文	该文字显示在登录注册页企业Logo右侧，中文字体。
	Logo右侧文字英文	该文字显示在登录注册页企业Logo右侧，英文字体。
用户门户首页配置	顶部背景色	正常登录用户门户，用户首页顶部的显示颜色。
	顶部文字颜色	正常登录用户门户，用户首页顶部的显示文字颜色。
	Logo右侧文字中文	该文字显示在用户门户首页浏览器窗口和页面顶部，中文字体。
	Logo右侧文字英文	该文字显示在用户门户首页浏览器窗口和页面顶部，英文字体。
国际化	可选语言	用户门户的语言配置，可以选择中文、英文。
	默认语言	用户门户的默认语言，可以在配置的可选语言中任选一种。
验证码配置	验证码长度	用户门户进行手机验证时，验证码的长度，可在4位、6位中任选一个。
	过期时间	用户门户进行手机验证时，验证码的过期时间，默认，可在3~15min之间设置。

步骤4 单击“保存”全局参数设置完成。

----结束

定制用户门户 Web 端页面

管理员可以定制用户门户Web端的访问页面，即用户通过浏览器访问的页面风格。

- 定制用户门户登录界面。
  a. 登录OneAccess管理门户。
  b. 在导航栏中，选择“设置 > 界面配置”，进入界面配置页面。
  c. 选择“用户门户Web端页面 > 定制用户门户登录界面”，可通过内置模板或自定义模板定制用户门户登录界面。
     - 在“内置模板”区域，鼠标放置在某一模板上，在处，单击“激活”，则该模板便为定制的用户门户登录界面。
     - 在“自定义模板”区域，单击“添加自定义模板”，参考表4-37配置参数信息。单击“保存并激活”，则该模板便为定制的用户门户登录界面。也可将鼠标放置自定义的某一模板上，在处选择“编辑”或“删除”编辑或删除自定义模板。

表 4-37 自定义方案参数

界面区域	参数	说明
页面布局	布局模板	可选择布局模板。
	页面背景图	用户门户的页面背景。推荐图片尺寸1920*1080。可在页面背景图参考中任选一个，也可以上传需要的背景图片。
	页面背景图参考	页面背景图选择的范围。上传的图片也会展示在这里。
	页面背景色	页面背景的颜色，支持自定义。 **说明** 页面背景图会覆盖页面背景色。
顶部区域	显示设置	控制用户门户顶部区域是否显示，可在显示、隐藏中任选一个。
	背景颜色	用户门户顶部区域的背景颜色。只有当显示设置为“显示”时，才需要设置该参数。
	内容颜色	用户门户顶部区域的文字颜色。只有当显示设置为“显示”时，才需要设置该参数。
表单区域	表单位置	控制用户门户表单区域登录表单的位置，可在居左、居中、居右中任选一个。

界面区域	参数	说明
	区域颜色	可设置： • 背景色：用户门户表单区域表单的背景颜色。 • 内容颜色：Tab标签栏默认文字、表单域标签文本、其他提示文本。 • 主色系：表单中按钮颜色、Tab标签选中/悬停颜色、链接文字颜色。
	输入框	可选择输入框样式，选择完输入框样式后，可设置用户门户表单区域表单输入框的边框和背景颜色。
	输入内容	可设置： • 内容颜色：用户门户表单区域表单文本的颜色。 • 提示内容颜色：用户门户登录表单的提示文字色。
	第三方登录	可设置： 按钮边框颜色、按钮背景颜色、内容颜色。
底部区域	显示设置	控制用户门户底部区域是否显示，可在显示、隐藏中任选一个。
	底部背景颜色	用户门户底部区域的背景颜色。 该参数只在Web端的登录、注册界面配置。
	底部内容颜色	用户门户底部区域的文字颜色。

- 定制用户门户注册界面。
  a. 登录OneAccess管理门户。
  b. 在导航栏中，选择“设置 > 界面配置”，进入界面配置页面。
  c. 选择“用户门户Web端页面 > 定制用户门户注册界面”，可通过内置模板或自定义模板定制用户门户注册界面。
     - 在“内置模板”区域，鼠标放置在某一模板上，在处，单击“激活”，则该模板便为定制的用户门户注册界面。
     - 在“自定义模板”区域，单击“添加自定义模板”，参考表4-38配置参数信息。单击“保存并激活”，则该模板便为定制的用户门户注册界面。也可将鼠标放置自定义的某一模板上，在处选择“编辑”或“删除”编辑或删除自定义模板。

表 4-38 自定义方案参数

界面区域	参数	说明
页面布局	布局模板	可选择布局模板。
	页面背景图	用户门户的页面背景。推荐图片尺寸1920*1080。可在页面背景图参考中任选一个，也可以上传需要的背景图片。
	页面背景图参考	页面背景图选择的范围。上传的图片也会展示在这里。
	页面背景色	页面背景的颜色，支持自定义。 **说明** 页面背景图会覆盖页面背景色。
顶部区域	显示设置	控制用户门户顶部区域是否显示，可在显示、隐藏中任选一个。
	背景颜色	用户门户顶部区域的背景颜色。只有当显示设置为“显示”时，才需要设置该参数。
	内容颜色	用户门户顶部区域的文字颜色。只有当显示设置为“显示”时，才需要设置该参数。
表单区域	表单位置	控制用户门户表单区域登录表单的位置，可在居左、居中、居右中任选一个。 该参数只在Web端的登录、注册界面配置。
	区域颜色	可设置： ● 背景色：用户门户表单区域表单的背景颜色。 ● 内容颜色：Tab标签栏默认文字、表单域标签文本、其他提示文本。 ● 主色系：表单中按钮颜色、Tab标签选中/悬停颜色、链接文字颜色。
	输入框	可选择输入框样式，选择完输入框样式后，可设置用户门户表单区域表单输入框的边框和背景颜色。
	输入内容	可设置： ● 内容颜色：用户门户表单区域表单文本的颜色。 ● 提示内容颜色：用户门户登录表单的提示文字色。
底部区域	显示设置	控制用户门户底部区域是否显示，可在显示、隐藏中任选一个。

界面区域	参数	说明
	底部背景颜色	用户门户底部区域的背景颜色。
	底部内容颜色	用户门户底部区域的文字颜色。

- 定制用户门户找回密码界面。
  a. 登录OneAccess管理门户。
  b. 在导航栏中，选择“设置 > 界面配置”，进入界面配置页面。
  c. 选择“用户门户Web端页面 > 定制用户门户找回密码界面”，可通过内置模板或自定义模板定制用户门户找回密码界面。
     - 在“内置模板”区域，鼠标放置在某一模板上，在处，单击“激活”，则该模板便为定制的用户门户找回密码界面。
     - 在“自定义模板”区域，单击“添加自定义模板”，参考表4-39配置参数信息。单击“保存并激活”，则该模板便为定制的用户门户找回密码界面。也可将鼠标放置自定义的某一模板上，在处选择“编辑”或“删除”编辑或删除自定义模板。

表 4-39 自定义方案参数

界面区域	参数	说明
页面布局	布局模板	可选择布局模板。
	页面背景图	用户门户的页面背景。推荐图片尺寸1920*1080。可在页面背景图参考中任选一个，也可以上传需要的背景图片。
	页面背景图参考	页面背景图选择的范围。上传的图片也会展示在这里。
	页面背景色	页面背景的颜色，支持自定义。 **说明** 页面背景图会覆盖页面背景色。
顶部区域	显示设置	控制用户门户顶部区域是否显示，可在显示、隐藏中任选一个。
	背景颜色	用户门户顶部区域的背景颜色。只有当显示设置为“显示”时，才需要设置该参数。
	内容颜色	用户门户顶部区域的文字颜色。只有当显示设置为“显示”时，才需要设置该参数。
表单区域	表单位置	控制用户门户表单区域登录表单的位置，可在居左、居中、居右中任选一个。

界面区域	参数	说明
	区域颜色	可设置： • 背景色：用户门户表单区域表单的背景颜色。 • 内容颜色：Tab标签栏默认文字、表单域标签文本、其他提示文本。 • 主色系：表单中按钮颜色、Tab标签选中/悬停颜色、链接文字颜色。
	输入框	可选择输入框样式，选择完输入框样式后，可设置用户门户表单区域表单输入框的边框和背景颜色。
	输入内容	可设置： • 内容颜色：用户门户表单区域表单文本的颜色。 • 提示内容颜色：用户门户登录表单的提示文字色。
底部区域	显示设置	控制用户门户底部区域是否显示，可在显示、隐藏中任选一个。
	底部背景颜色	用户门户底部区域的背景颜色。
	底部内容颜色	用户门户底部区域的文字颜色。

定制用户门户移动端页面

管理员可以定制用户门户移动端的访问页面，即用户通过手机、平板等移动设备访问的页面风格。

- 定制用户门户登录界面。
  a. 登录OneAccess管理门户。
  b. 在导航栏中，选择“设置 > 界面配置”，进入界面配置页面。
  c. 选择“用户门户移动端页面 > 定制用户门户登录界面”，可通过内置模板或自定义模板定制用户门户登录界面。
     - 在“内置模板”区域，鼠标放置在某一模板上，在处，单击“激活”，则该模板便为定制的用户门户登录界面。
     - 在“自定义模板”区域，单击“添加自定义模板”，参考表4-40配置参数信息。单击“保存并激活”，则该模板便为定制的用户门户登录界面。也可将鼠标放置自定义的某一模板上，在处选择“编辑”或“删除”编辑或删除自定义模板。

表 4-40 自定义方案参数

界面区域	参数	说明
页面布局	布局模板	-
	页面背景图	用户门户的页面背景。推荐图片尺寸1920*1080。可在页面背景图参考中任选一个，也可以上传需要的背景图片。
	页面背景图参考	页面背景图选择的范围。上传的图片也会展示在这里。
	页面背景色	页面背景的颜色，支持自定义。 **说明** 页面背景图会覆盖页面背景色。
顶部区域	显示设置	控制用户门户顶部区域是否显示，可在显示、隐藏中任选一个。
	背景颜色	用户门户顶部区域的背景颜色。只有当显示设置为“显示”时，才需要设置该参数。
	内容颜色	用户门户顶部区域的文字颜色。只有当显示设置为“显示”时，才需要设置该参数。
	图标	控制用户门户顶部区域图标是否显示，可在显示、隐藏中任选一个。
表单区域	区域颜色	可设置： ● 背景色：用户门户表单区域表单的背景颜色。 ● 内容颜色：Tab标签栏默认文字、表单域标签文本、其他提示文本。 ● 主色系：表单中按钮颜色、Tab标签选中/悬停颜色、链接文字颜色。
	输入框	可设置用户门户表单区域表单输入框的边框颜色。
	输入内容	可设置： ● 内容颜色：用户门户表单区域表单文本的颜色。 ● 提示内容颜色：用户门户登录表单的提示文字色。
底部区域	显示设置	用户门户底部区域的文字颜色。
	底部文字	用户门户底部区域的文字。

- 定制用户门户注册界面
  a. 登录OneAccess管理门户。

b. 在导航栏中，选择“设置 > 界面配置”，进入界面配置页面。

c. 选择“用户门户移动端页面 > 定制用户门户注册界面”，可通过内置模板或自定义模板定制用户门户注册界面。

- 在“内置模板”区域，鼠标放置在某一模板上，在 处，单击“激活”，则该模板便为定制的用户门户注册界面。
- 在“自定义模板”区域，单击“添加自定义模板”，参考表4-41配置参数信息。单击“保存并激活”，则该模板便为定制的用户门户注册界面。也可将鼠标放置自定义的某一模板上，在 处选择“编辑”或“删除”编辑或删除自定义模板。

表 4-41 自定义方案参数

界面区域	参数	说明
页面布局	布局模板	可选择布局模板。
	页面背景图	用户门户的页面背景。推荐图片尺寸1920*1080。可在页面背景图参考中任选一个，也可以上传需要的背景图片。
	页面背景图参考	页面背景图选择的范围。上传的图片也会展示在这里。
	页面背景色	页面背景的颜色，支持自定义。 **说明** 页面背景图会覆盖页面背景色。
顶部区域	背景颜色	用户门户顶部区域的背景颜色。只有当顶部banner条设置为“显示”时，才需要设置该参数。
	内容颜色	用户门户顶部区域的文字颜色。只有当顶部banner条设置为“显示”时，才需要设置该参数。
表单区域	区域颜色	主色系：可设置表单中按钮颜色、Tab标签选中/悬停颜色、链接文字颜色。
	输入框	设置用户门户表单区域表单输入框的边框颜色。
	输入内容	可设置： • 内容颜色：用户门户表单区域表单文本的颜色。 • 提示内容：用户门户登录表单的提示文字色。

4.7.6 服务配置

OneAccess支持基于OAuth2、SAML、OIDC、CAS协议的应用对接，同时，提供动态口令服务。当进行应用对接时，可通过服务配置页面查看相应的参数信息。

配置动态口令

动态口令是遵循基于时间的一次性密码（TOTP），通过虚拟Multi-Factor Authentication (MFA) 设备产生。MFA设备可以基于硬件也可以基于软件，OneAccess目前仅支持基于软件的虚拟MFA，虚拟MFA应用程序可以在移动硬件设备（包括智能手机）上运行，非常方便，虚拟MFA是多因素认证方式中的一种。

OneAccess支持动态口令配置，您可以将动态口令参数配置到虚拟MFA设备上，配置方法请参见MFA设备的帮助文档。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“设置 > 服务配置”。

步骤3 在“服务配置”页面，单击“动态口令配置”，在弹出框中配置如下参数。

表 4-42 参数设置

参数	说明
加密算法	系统默认为HMACSHA1，支持修改。
口令生成位数	系统默认为6位，不支持修改。
口令生成的周期（秒）	系统默认为30秒，不支持修改。
校验时间前后偏移量	系统默认为0，支持修改。
口令生成基准时间	系统默认为GMT标准时间，不支持修改。
是否联合密码启用双因素	默认关闭，当开启后，用户以动态口令方式登录时，需同时输入用户名、密码和动态口令。

步骤4 单击“保存”，动态口令配置完成。

----结束

说明

使用动态口令的前提是在应用的登录配置中开启网站或移动应用的动态口令验证码。

配置 IDP

当您需要与企业应用建立基于SAML协议的信任关系时，您需要将IDP侧的元数据上传到企业SP服务器上，上传方法请参见SP服务商的帮助文档。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“设置 > 服务配置”。

步骤3 在“服务配置”页面，单击“IDP配置”，在弹出框中配置如下参数。

表 4-43 IDP 服务参数

参数	说明
IDP EntityId	IDP的唯一标识。
SSO URL	单点登录的URL。
IDP 登出URL	全局退出的URL。
IDP 证书	签名证书是一份包含公钥用于验证签名的证书。企业应用通过元数据文件中的签名证书来确认用户访问应用认证过程中断言消息的可信性、完整性。
请求断言时间窗口	默认2分钟。可在下拉框中选择设置时间，范围为1分钟~5分钟。
Session有效期	默认30分钟。取值范围为1~480。
启用请求签名	默认开启。
启用断言签名	默认开启。
启用断言加密	默认开启。

步骤4 单击右上角的“下载IDP元数据”，数据会自动保存，将其上传到企业SP服务器上即可。

步骤5 单击“保存”，配置更新完成。

----结束

配置 OIDC

当您需要与企业应用建立基于OIDC、OAUTH2协议的信任关系时，您需要通过“OIDC配置”获取集成需要的端口信息。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“设置 > 服务配置”。

步骤3 在“服务配置”页面，单击“OIDC”，在弹出框中获取如下参数。

参数	说明
认证授权	用户获取应用认证授权的接口，系统默认。
获取Token	获取用户Token的接口，系统默认。
UserInfo	系统默认。
刷新Token	刷新用户Token的接口，系统默认。

步骤4 单击右上角的“OIDC设置”，可以下载OIDC数据。

----结束

配置 CAS

当您需要与企业应用建立基于CAS协议的信任关系时，您需要通过“CAS配置”查看CAS的服务信息。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“设置 > 服务配置”。

步骤3 在“服务配置”页面，单击“CAS配置”，在弹出框中查看和编辑如下参数。

表 4-44 配置参数

参数	说明
Server Prefix	系统自动生成，不可编辑。CAS服务地址的前缀。
Login URL	系统自动生成，不可编辑。CAS服务的请求授权地址。
Validate URL V3	系统自动生成，不可编辑。验证票据，推荐使用V3的地址。
Logout URL	系统自动生成，不可编辑。CAS服务的登出地址。
ST有效期	请求授权返回票据的有效期，建议设置为3~15分钟。

步骤4 单击“保存”，配置完成。

----结束

配置 API 认证

当企业需要将开放接口注册到OneAccess平台时，可以查看API配置信息，并与企业应用进行交互。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“设置 > 服务配置”。

步骤3 在“服务配置”页面，单击“API认证配置”，在弹出框查看如下参数。

参数	说明
签名算法	签名使用的算法，系统默认。
签名公钥	验证签名使用的密钥，系统默认。
加密算法	加密使用的算法，系统默认。
算法密钥	加密算法使用的密钥，单击“重置”可进行设置。
过期时间	access_token、id_token的过期时间，默认为30分钟，支持自定义，最长43200分钟（30天）。

----结束

4.7.7 云桥配置

云桥Agent作为一座“桥梁”，在企业内部服务和云上OneAccess之间建立了一条网络安全隧道，可以避免企业的内部服务直接暴露在公网上，从而有效的保护网络实体免受窃听和重复攻击等。

目前，云桥Agent支持AD身份源、AD及LDAP认证源，本节主要介绍AD和LDAP通过云桥Agent连接OneAccess的方法。

前提条件

请确保您已拥有部署云桥Agent的能力。

获取云桥软件部署包

表 4-45 云桥软件部署包

软件包名称	获取途径
cloudAgent-*.zip	• 云桥身份源包：**https://oneaccess-cn-east-3-obs.obs.cn-east-3.myhuaweicloud.com/cloudbridge/cloudAgent-identitySource-24.5.1.1.zip** • 云桥身份源包校验文件：**https://oneaccess-cn-east-3-obs.obs.cn-east-3.myhuaweicloud.com/cloudbridge/cloudAgent-identitySource-24.5.1.1.zip.sha256** • 云桥认证源包：**https://oneaccess-cn-east-3-obs.obs.cn-east-3.myhuaweicloud.com/cloudbridge/cloudAgent-authSource-24.5.1.1.zip** • 云桥认证源包校验文件：**https://oneaccess-cn-east-3-obs.obs.cn-east-3.myhuaweicloud.com/cloudbridge/cloudAgent-authSource-24.5.1.1.zip.sha256**

说明

云桥包下载地址是不带sha256后缀结尾的链接，带sha256后缀结尾的下载链接为对应软件包的校验文件。

云桥部署包更新日志

下表为云桥部署包更新日志。

版本号	更新内容
V24.5.1.1	升级JDK版本到17。
V23.12.1.1	优化了一些已知问题。

版本号	更新内容
V23.6.1.0	支持使用更安全的安全随机数。
V23.2.1.0	支持LDAP认证源及启动日志优化。
V22.11.1.0	新增功能：增加签名校验及优化日志打印。
V22.6.1.0	新增功能：管理员通过管理门户查看云桥客户端运行日志的能力。
V22.3.1.0	针对AD身份源Agent功能进行优化。
V21.9.2.0	新增看门狗机制。
V21.9.1.0	1. 云桥重连机制优化。 2. 优化了一些已知问题。

校验云桥 Agent 软件包完整性

说明

文中软件包版本号为示例，请以实际为准。

步骤1 使用PuTTY/FTP等工具连接待部署服务器，以root用户登录待部署服务器，使用SFTP工具将云桥Agent软件包和对应的SHA256文件上传到待部署服务器，执行**ll**查看已上传的软件包和校验文件。

```
[root@cluster-test-eq9ku xxx]# ll
total 75724
-rw-r--r-- 1 root root 32696037 Dec  1 16:12 cloudAgent-authSource-24.5.1.1.zip
-rw-r--r-- 1 root root      101 Dec  1 16:11 cloudAgent-authSource-24.5.1.1.zip.sha256
-rw-r--r-- 1 root root 44832098 Dec  1 16:12 cloudAgent-identitySource-24.5.1.1.zip
-rw-r--r-- 1 root root      105 Dec  1 16:11 cloudAgent-identitySource-24.5.1.1.zip.sha256
```

步骤2 执行以下命令校验网关软件包完整性，当回显信息显示OK，表明完整性校验成功。

sha256sum -c cloudAgent-identitySource-24.5.1.1.zip.sha256

```
[root@cluster-test-eq9ku xxx]#  sha256sum -c cloudAgent-identitySource-24.5.1.1.zip.sha256
cloudAgent-identitySource-24.5.1.1.zip: OK
```

sha256sum -c cloudAgent-authSource-24.5.1.1.zip.sha256

```
[root@cluster-test-eq9ku xxx]# sha256sum -c cloudAgent-authSource-24.5.1.1.zip.sha256
cloudAgent-authSource-24.5.1.1.zip: OK
```

说明

如果完整性校验不通过，则软件包可能在下载过程中损坏，请重新下载或联系技术支持人员解决。

----结束

操作步骤

步骤1 部署AD服务并创建域账号，建立企业自己的管理系统。具体可参考**搭建AD服务器**和**创建域账号**。

步骤2 添加云桥Agent。

1. 登录OneAccess管理门户。
2. 在导航栏中，选择“设置 > 云桥配置 ”。
3. 在云桥配置页面，单击“添加云桥Agent”，设置名称并选择云桥Agent类型，单击“确定”。至此，云桥Agent添加完成。云桥Agent类型支持认证源类型和身份源类型，请按需选择。

说明

- 云桥Agent添加完成后，系统会自动生成ClientID和ClientSecret，请妥善保管。
- 如不慎忘记ClientSecret，单击目标Agent的“重置密钥”即可重新生成。重置后，原密钥将会失效，请谨慎操作。
- 单击“配置IP”，配置云桥Agent所在服务器IP，不配置时不启用IP访问控制，只支持配置一个IP，不支持*号通配的IP格式（例如：10.10.10.*），仅允许该IP上搭建的云桥Agent连接。
- 单击“查看日志”，可以查看连接日志。
- 单击“删除”，可删除目标Agent，请谨慎删除。

步骤3 部署云桥Agent，部署成功以后，在管理门户的云桥配置中查看云桥Agent状态，会显示“在线”状态。

图 4-30 查看云桥 Agent 状态

以下分别介绍部署云桥Agent身份源、认证源的方法。

说明

- 服务器需要安装JDK17版本（云桥24.5.1.1之前的版本需要安装JRE1.8版本）。
  1. 请至官网下载源码JDK压缩包。
  2. 执行以下命令，提取JRE到指定目录，配置JRE环境变量。

     tar -zxvf jdk-17_linux-x64_bin.tar.gz -C /usr/local/

     chmod 755 /usr/local/jdk-17.0.12

     echo "export PATH" >> /etc/profile

     echo "export PATH=$PATH:/usr/local/jdk-17.0.12/bin" >> /etc/profile

     source /etc/profile

     java -version
- 如需使用看门狗功能，服务器需要安装curl、netstat工具。
- 建议使用非root用户运行云桥客户端。

  若已有非root用户，则无需再次创建。若想使用新的非root用户，则需要先以root用户执行以下命令进行创建：

  groupadd {用户组}

  useradd -d /home/用户名 -s /bin/bash -g 用户组 -m 用户名

  unzip -od {文件解压后的存放地址} cloudAgent.zip

  chown -R {用户名}:{用户组} {文件解压后的存放地址}

  chmod 700 -R {文件解压后的存放地址}

  su - {用户名}

- 以CentOS Linux release 8.2.2004 部署云桥Agent身份源为例。

  a. 请按照实例所在区域，下载Agent身份源的部署包。

  b. 将其上传至目标服务器。

  c. 执行**unzip -od {文件解压后的存放地址} cloudAgent.zip**解压部署包。存放地址必须唯一，否则会导致安装出错。部署包的具体信息可参考**表4-46**。

  表 4-46 目录结构

名称	说明
agent.sh	开机自启动Agent的文件。
cloudAgent-identitySource.jar	Agent的部署包。
cloudBridge.sh	手动启动Agent的文件。
config	Agent配置文件（application.yml）的存放目录。
connector	LDAP连接器的部署包，暂不关注。
encrypt.sh	加密文件，用来加密AD主体账号的密码。
log	Agent日志（agent.log）的存放目录。

  d. 进入文件解压后的存放地址，配置“config”目录下的“application.yml”文件。**每个属性值前面需要加1个空格**。部分参数可参考**在OneAccess中添加AD身份源**中的配置参数。

如需对agentSecret、credentials进行加密，请按照如下步骤进行操作：

i. 生成根密钥和工作密钥，在云桥安装包解压目录下执行**./encrypt.sh setKey**命令，提示“please enter the encryption key：”，输入自定义密钥后回车，提示“the encryption key setting succeeds”，代表密钥设置成功。

ii. 执行**./encrypt.sh encrypt**命令，提示“please enter what you want to encrypt content：”，输入agentSecret的值后回车，即可获取加密后的agentSecret，如“{AES_GCM}0000xxxxxx111111”。

iii. 执行**./encrypt.sh encrypt**命令，提示“please enter what you want to encrypt content：”，输入credentials的值后回车，即可获取加密后的credentials，如“{AES_GCM}0000xxxxxx222222”。

iv. 将加密后的值拷贝至“application.yml”文件中对应位置即可，注意需要前后添加英文双引号。

表 4-47 配置参数

参数	说明
* address	云桥服务启动监听地址，默认127.0.0.1。
* port	云桥服务启动的监听端口，可修改，当启动多个云桥时，需要修改为不同的端口号，默认9081
* serverAddress	wss://{需要使用云桥Agent的租户域名}/api/v1/ws。
* agentId	添加Agent后，系统自动生成。请参考**步骤2**。
* agentSecret	添加Agent后，系统自动生成。请参考**步骤2**。
* host	运行企业AD服务器的主机 IP 地址。
* port	与企业AD服务器进行通信的TCP/IP 端口号。
* ssl	默认为true，表示连接AD server使用SSL，否则配置为false。
* principal	进行企业AD服务器验证时使用的标识名。
* credentials	**principal**的密码。
* baseContexts	要同步的账号所在AD中的树的根节点，如“OU=huaweitest,DC=test,DC=com”。

说明

如果执行**./encrypt.sh setKey**命令输入Key后无响应，则需要安装rng-tools工具提高系统熵池的补充速率。

1. 执行以下命令进行安装rng-tools：

   yum install rng-tools

   cat /etc/sysconfig/rngd

   如果没有该文件，请执行以下命令新增该文件：

   echo "OPTIONS=\"-r /dev/urandom\"" > /etc/sysconfig/rngd

2. 执行以下命令启动rng服务以及查询rng服务状态。

   service rngd start 启动rng服务

   service rngd status 查看rng服务状态

   状态为enabled表示启动。

e. 配置完成后，执行**./cloudBridge.sh start**进行启动，提示“Starting Agent Success.”代表启动成功。

说明

- 请确保当前部署用户拥有部署安装包的相关权限。
- 如提示“Starting Agent Fail. ”代表启动失败，请排查配置文件。
- 如需开机自启动，请使用root用户执行**./agent.sh install**，安装过程中会对系统基础环境检查，保证满足服务安装要求。安装过程中会提示输入启动用户，如果为空则使用当前用户运行脚本。提示“The Agent service installed successfully, need to reboot will take effect.”代表安装成功。
- 如需卸载Agent，执行**./agent.sh uninstall**，提示“uninstall Agent Success.”代表卸载成功。
- 如果执行**./cloudBridge.sh start**无响应，参考上一章节执行**./encrypt.sh setKey**无响应进行安装rng-tools操作。

f. 可以通过目录中的“log/agent.log”文件获取日志信息。

- 以CentOS Linux release 8.0.1905部署云桥Agent认证源为例。

  a. 请按照实例所在区域，下载Agent认证源的部署包。

  b. 将其上传至目标服务器。

  c. 执行**unzip -od {文件解压后的存放地址} cloudAgent.zip**解压部署包。存放地址必须唯一，否则会导致安装出错。部署包的具体信息可参考**表4**。

表 4-48 目录结构

名称	说明
agent.sh	开机自启动云桥Agent的文件。

名称	说明
cloudAgent-authSource.jar	Agent的部署包。
cloudBridge.sh	手动启动Agent的文件。
config	Agent配置文件（application.yml）的存放目录。
log	Agent日志（agent.log）的存放目录。

d. 进入文件解压后的存放地址，配置“config”目录下的application.yml文件。**每个属性值前面需要加1个空格**。

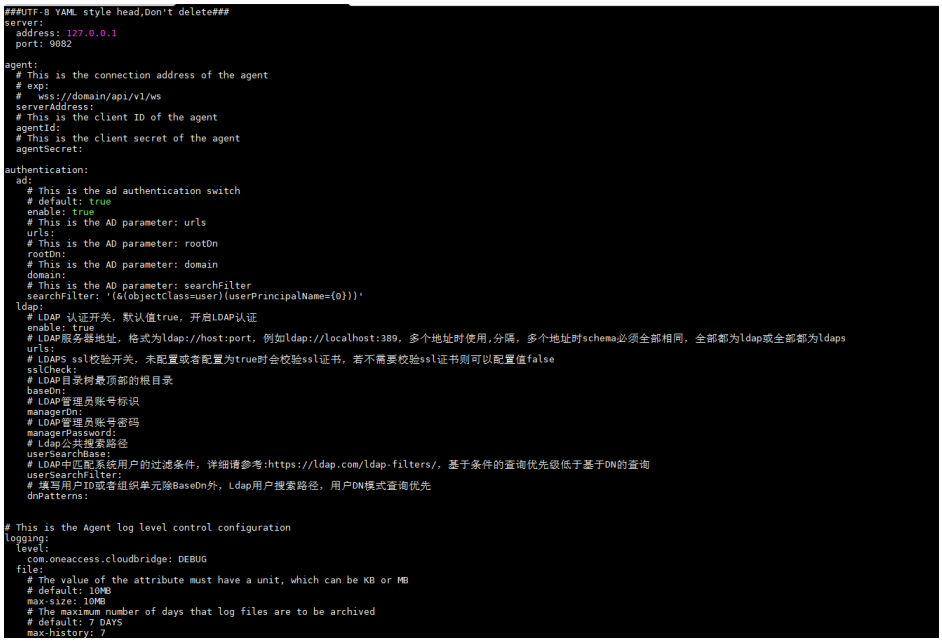


表 4-49 配置参数

参数	说明
* address	云桥服务启动监听地址，默认127.0.0.1。
* port	云桥服务启动的监听端口，可修改，当启动多个云桥时，需要修改为不同的端口号，默认9082
* serverAddress	wss://{需要使用云桥Agent的租户域名}/api/v1/ws。
* agentId	添加云桥Agent后，系统自动生成。请参考**步骤2**。
* agentSecret	添加云桥Agent后，系统自动生成。请参考**步骤2**。
* urls	AD地址。可参考**在OneAccess中添加AD认证源**中的配置参数。
* rootDn	AD中的节点，会到该节点下认证用户。可参考**在OneAccess中添加AD认证源**中的配置参数。

参数	说明
* domain	若租户域名包含AD域名，则该参数填写AD域名；若不包含，则为空。
* searchFilter	查询条件。可参考**在OneAccess中添加AD认证源**中的配置参数。
* urls	LDAP地址。可参考**在OneAccess中添加LDAP认证源**中的配置参数。
sslCheck	LDAPS ssl校验开关，未配置或配置为true时会校验ssl证书，若不需要校验ssl证书则可以配置值false。
* baseDn	用户的baseDN，可参考在OneAccess中添加LDAP认证源中的配置参数。
managerDn	管理员的标识名，默认cn=Directory Manager。
managerPassword	LDAP管理员账号标识。
userSearchBase	Ldap公共搜索路径。可参考**在OneAccess中添加LDAP认证源**中的配置参数。
userSearchFilter	LDAP中匹配系统用户的过滤条件，系统默认“(&(objectClass=user)(uid={0}))”，详细请参考**LDAP过滤器**。基于条件的查询优先级低于基于DN的查询。
dnPatterns	LDAP用户的搜索路径，系统默认“uid={0},ou=people”。用户DN模式查询优先。

说明

如需对agentSecret进行加密，可参考**步骤3.d**进行操作。

e. 配置完成后，执行 **./cloudBridge.sh start**进行启动，提示“Starting Agent Success.”代表启动成功。

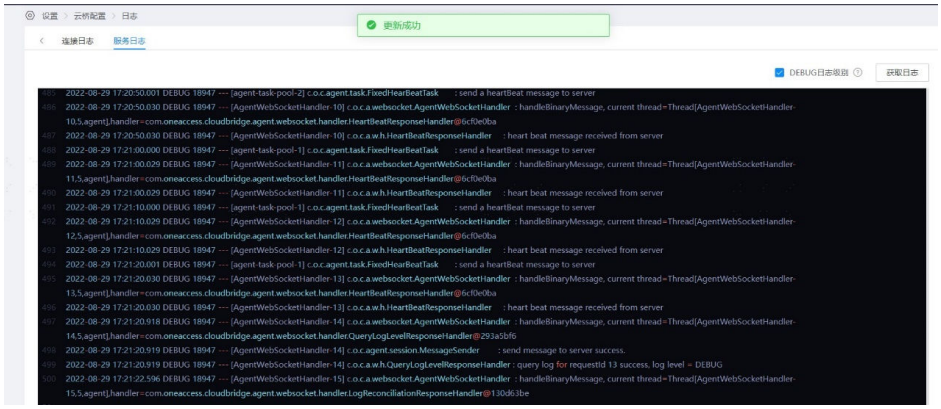
说明

- 请确保当前部署用户拥有部署安装包的相关权限。
- 如提示“Starting Agent Fail.”代表启动失败，请排查配置文件。
- 如需开机自启动，请使用root用户执行**./agent.sh install**，安装过程中会对系统基础环境检查，保证满足服务安装要求。安装过程中会提示输入启动用户，如果为空则使用当前用户运行脚本。提示“The Agent service installed successfully, need to reboot will take effect.”代表安装成功。
- 如需卸载Agent，执行**./agent.sh uninstall**，提示“uninstall Agent Success.”代表卸载成功。

f. 可以通过目录中的“log/agent.log”文件获取日志信息。

步骤4 单击“查看日志”，默认进入“连接日志”页签，可查看云桥上/下线的时间点。

步骤5 单击“服务日志”，可在当前页面实时查看云桥启动日志。



步骤6 添加AD身份源、AD认证源和LDAP认证源。

1. 添加AD身份源
   a. 登录OneAccess管理门户。
   b. 在导航栏中，选择“用户 > 身份源管理 ”。
   c. 在身份源管理页面，单击AD身份源操作列的“添加身份源”，输入“身份源名称”，单击“确定”。

d. 在AD身份源列表页面，单击目标身份源的“详情”，设置导入配置，选择“通过云桥Agent连接”并勾选已添加的云桥Agent即可。可勾选的云桥Agent最多不超过5个。高级配置、对象模型等的配置请参考**在OneAccess中添加AD身份源**。

图 4-31 AD 身份源详情

图 4-32 设置导入配置

e. 执行同步请参考**验证OneAccess同步企业AD数据**。

2. 添加AD认证源。
   a. 登录OneAccess管理门户。
   b. 在导航栏中，选择“认证 > 认证源管理 > AD”。
   c. 在AD认证源页面，单击右上方“添加认证源”，配置参数。

图 4-33 添加 AD 认证源

表 4-50 配置参数

参数	说明
* 显示名称	认证源的显示名称，支持自定义。如AD认证。
* 连接方式	选择通过云桥Agent连接。
* 选择云桥Agent	勾选**步骤2**中已添加的云桥。最多可勾选5个云桥Agent。
* 关联源属性	AD用户的属性，如sAMAccountName。
* 关联用户属性	AD在系统中映射的用户唯一文本属性，如用户名。

参数	说明
* 未关联用户时	登录成功后，如未关联到系统用户，可以根据该配置操作。
* 更新已存在属性	AD登录时若关联到了用户，可以通过该选项来确定是否更新已存在的用户属性值。

如果您需要同时映射其他属性，如name，可以设置“未关联用户时”为“自动创建用户”，通过“添加映射”完成。可参考表4-51。

表 4-51 映射参数

参数	说明
用户属性名	AD对接OneAccess的映射属性，可在下拉框选择，如邮箱。
映射类型	OneAccess与AD之间用户属性的映射方式，可在下拉框选择，如认证源属性。
认证源属性名	AD用户的属性名称。

d. 可输入“测试账号”和“测试密码”，单击“测试”进行验证连通性。

如果在添加AD认证源中，**选择云桥Agent**勾选了多个，最多不超过5个，单击“测试”后，系统会逐一进行连通性验证。如果验证失败，会进行提示。

e. 开启AD认证。具体可参考**在OneAccess中开启AD认证**。

f. 验证AD认证登录。具体可参考**验证AD认证登录OneAccess用户门户**。

3. 添加LDAP认证源。

a. 登录OneAccess管理门户。

b. 在导航栏中，选择“认证 > 认证源管理 > LDAP”。

c. 在LDAP认证源页面，单击右上方“添加认证源”，配置参数。

表 4-52 配置参数

参数	说明
* 显示名称	认证源的显示名称，支持自定义。如LDAP认证。
* 连接方式	选择通过云桥Agent连接。
* 选择云桥Agent	勾选**步骤2**中已添加的云桥。最多可勾选5个云桥Agent。
* 关联源属性	LDAP用户的属性，如sAMAccountName。
* 关联用户属性	LDAP在系统中映射的用户唯一文本属性，如用户名。
* 未关联用户时	登录成功后，如未关联到系统用户，可以根据该配置操作。
* 更新已存在属性	LDAP登录时若关联到了用户，可以通过该选项来确定是否更新已存在的用户属性值。

如果您需要同时映射其他属性，如name，可以设置“未关联用户时”为“自动创建用户”，通过“添加映射”完成。可参考**表4-53**。

表 4-53 映射参数

参数	说明
用户属性名	LDAP对接OneAccess的映射属性，可在下拉框选择，如邮箱。
映射类型	OneAccess与LDAP之间用户属性的映射方式，可在下拉框选择，如认证源属性。
认证源属性名	LDAP用户的属性名称。

d. 可输入“测试账号”和“测试密码”，单击“测试”进行验证连通性。

如果在添加LDAP认证源中，**选择云桥Agent**勾选了多个，最多不超过5个，单击“测试”后，系统会逐一进行连通性验证。如果验证失败，会进行提示。

e. 开启LDAP认证。具体可参考**在OneAccess中开启LDAP认证**。

f. 验证LDAP认证登录。具体可参考**验证LDAP认证登录OneAccess用户门户**。

----结束

5 普通用户指南

5.1 注册账号

可使用**添加用户**登录用户门户网站，若没有账号，可参考本章节注册账号。

前提条件

管理员已在界面配置中配置了“开启注册”功能，操作请参见**设置全局参数**。

操作步骤

步骤1 进入用户门户登录页面。

说明

请联系企业管理员获取用户访问域名，如https://example.huaweioneaccess.com。

步骤2 用户在登录页面单击“立即注册”。

步骤3 在注册页面，输入手机号。

步骤4 单击“发送验证码”，将收到的验证码输入在验证码输入框。

步骤5 单击“下一步”，输入密码、确认新密码和用户名。

说明

具体需要输入哪些用户信息是由管理员在**管理用户属性定义**中将用户的哪些字段的“注册信息采集”属性设置为“显示”决定的。

步骤6 【可选】勾选**开启及配置用户协议**中设置的用户协议。

说明

当开启了用户协议配置，具体操作请参考**开启及配置用户协议**，注册账号必须勾选配置的协议。

步骤7 单击“保存”账号注册成功并进入用户门户网站。

说明

新注册的账号所属组织默认为根组织。若您在注册账号时想自定义选择账号所属组织，可联系管理员将“组织”字段的“注册信息采集”属性设置为“显示”，具体操作请参见**修改用户属性**。

----结束

5.2 找回密码

若用户忘记密码，可通过用户门户登录页面的“忘记密码”功能找回密码。

前提条件

管理员已在界面配置中配置了“开启找回密码”功能，操作请参见**设置全局参数**。

操作步骤

步骤1 用户进入用户门户登录页面。

说明

请联系企业管理员获取用户访问域名，如https://example.huaweioneaccess.com。

步骤2 用户在登录页面单击“忘记密码”进入“找回密码”页面。默认是“通过手机号找回”。

步骤3 输入用户信息找回密码。

- 选择“通过手机号找回”。
  a. 输入手机号，单击“发送验证码”。
  b. 输入收到的验证码。
  c. 输入新密码，确认新密码。
  d. 单击“确认”密码找回成功，使用新密码登录用户门户。
- 选择“通过邮箱找回”。
  a. 输入邮箱，单击“发送验证码”。
  b. 输入收到的验证码。
  c. 输入新密码，确认新密码。
  d. 单击“确认”密码找回成功，使用新密码登录用户门户。

----结束

5.3 登录 OneAccess 用户门户并进入应用

5.3.1 短信登录

前提条件

- 已拥有用户门户账号，若您还没有用户门户账号，您可以联系您的企业管理员为您创建或可参考**注册账号**在用户门户网站注册账号。
- 管理员已在用户门户应用登录配置中开启短信认证，具体操作请参见**登录配置**。
- 管理员已完成短信网关配置，具体操作请参见**短信网关配置**。

操作步骤

步骤1 用户进入用户门户登录页面。

说明

请联系企业管理员获取用户访问域名，如https://example.huaweioneaccess.com。

步骤2 用户在登录页面选择“短信”页签，输入手机号。

步骤3 单击“发送验证码”，输入框中输入收到的验证码，如选择“记住手机号”则下次登录时，不用再输入手机号。

说明

若未收到短信，可单击“试试语音验证码”，收到语言验证码，此功能需要管理员已完成语音网关配置，具体操作请参见**语音网关配置**。

步骤4 单击“登录”。

步骤5 【可选】勾选**开启及配置用户协议**中设置的用户协议，单击“同意并登录”。

说明

- 当管理员开启了用户协议配置，具体操作请参考**开启及配置用户协议**，用户首次登录用户门户时必须勾选配置的协议。
- 当管理员修改了用户协议，具体参照请参考**编辑协议**，用户再次登录时必须勾选配置的协议。

步骤6 在用户门户首页单击需要访问的应用LOGO即可进入应用。

----结束

5.3.2 动态口令登录

前提条件

- 已拥有用户门户账号，若您还没有用户门户账号，您可以联系您的企业管理员为您创建或可参考**注册账号**在用户门户网站注册账号。
- 管理员已在用户门户应用登录配置中开启动态口令认证，具体操作请参见**登录配置**。
- 管理员已完成动态口令配置，具体操作请参见**配置动态口令**。
- 用户已在用户门户网站激活了动态口令，具体操作请参见**账号安全设置**。

操作步骤

步骤1 用户进入用户门户登录页面。

说明

请联系企业管理员获取用户访问域名，如https://example.huaweioneaccess.com。

步骤2 用户在登录页面选择“动态口令”登录。

- 默认为“用户名/邮箱”登录，输入用户名/邮箱和收到的动态口令。
- 选择“手机号登录”，输入手机号和动态口令验证码。

步骤3 可选中“记住登录名”，单击“登录”。

步骤4 【可选】勾选**开启及配置用户协议**中设置的用户协议，单击“同意并登录”。

说明

- 当管理员开启了用户协议配置，具体操作请参考**开启及配置用户协议**，用户首次登录用户门户时必须勾选配置的协议。
- 当管理员修改了用户协议，具体参照请参考**编辑协议**，用户再次登录时必须勾选配置的协议。

步骤5 在用户门户首页单击需要访问的应用LOGO即可进入应用。

----结束

5.3.3 密码登录

前提条件

- 已拥有用户门户账号，若您还没有用户门户账号，您可以联系您的企业管理员为您创建或可参考**注册账号**在用户门户网站注册账号。
- 管理员已在用户门户应用登录配置中开启密码认证，具体操作请参见**登录配置**。

操作步骤

步骤1 用户进入用户门户登录页面。

说明

请联系企业管理员获取用户访问域名，如https://example.huaweioneaccess.com。

步骤2 用户在登录页面选择“密码”登录。

- 默认为“用户名/邮箱”登录，输入用户名/邮箱和密码。

- 选择“手机号登录”，输入手机号和密码。

步骤3 可选中“记住登录名”，单击“登录”。

步骤4 【可选】勾选**开启及配置用户协议**中设置的用户协议，单击“同意并登录”。

说明

- 当管理员开启了用户协议配置，具体操作请参考**开启及配置用户协议**，用户首次登录用户门户时必须勾选配置的协议。
- 当管理员修改了用户协议，具体参照请参考**编辑协议**，用户再次登录时必须勾选配置的协议。

步骤5 在用户门户首页单击需要访问的应用LOGO即可进入应用。

----结束

5.3.4 认证源登录

用户门户网站支持认证源方式登录，具体操作可参见**认证源登录**。

说明

- 当管理员开启了用户协议配置，具体操作请参考**开启及配置用户协议**，使用认证源首次登录用户门户时必须勾选配置的协议。
- 当管理员修改了用户协议，具体参照请参考**编辑协议**，再次使用认证源登录时必须勾选配置的协议。

5.4 账号委托

概述

账号委托是将自己账号某个应用的跳转权限临时委托给被委托账号即被委托账号可以访问委托账号的某一应用，完全满足临时委托、委托时效性、用户自主性的需求，委托结束后临时授权结束，被委托人无法再访问该应用，大大提升账号安全性、便利性。

前提条件

- 委托用户：存在可跳转的应用，可登录OneAccess的用户门户。
- 被委托用户：可登录OneAccess的用户门户。

用户门户创建委托

步骤1 登录OneAccess用户门户。

步骤2 单击“账号委托”。

步骤3 在“创建委托”弹框，选择“委托应用”、输入“被委托人”、输入“委托说明”、选择“生效时间段”。

步骤4 单击“确定”委托完成。

----结束

访问委托账号的应用

步骤1 被委托账号登录OneAccess用户门户。

步骤2 在用户门户首页单击被委托的应用图标便可访问该应用。

说明

若被委托账号本身就有该应用的访问权限，则访问该应用时，需要选择自有账号或委托账号。

----结束

5.5 设置

用户在用户门户可以查看或修改个人资料、进行账号安全设置等。本文为您介绍用户如何进行账号设置。

查看或修改个人资料

在用户门户页面，单击右上角的用户图像，选择“账号设置”进入“个人资料”页面，在该页面可以查看、修改个人的基本信息。

说明

企业管理员在OneAccess管理门户配置用户基本信息是否支持查看、修改。如需更改，请联系企业管理员。

风险事件

在用户门户页面，单击右上角的用户图像，选择“账号设置”默认进入“个人资料”页面，在页面左侧选择“风险事件”进入“风险事件”页面，通过设置起始时间和风险类型，可查看风险事件详细信息。

账号安全设置

在用户门户页面，单击右上角的用户名，选择“账号设置”默认进入“个人资料”页面，在页面左侧选择“账号安全”进入“账号安全”页面，可以修改登录密码、绑定手机号、激活动态口令。

- 修改登录密码：用户可以修改账号的登录密码。
- 修改绑定手机号：用户可以修改账号绑定的手机号。
- 激活动态口令：动态口令是遵循基于时间的一次性密码（TOTP）。
  a. 绑定账号。
     打开微信小程序搜索OTP，比如进入“竹云城堡”小程序，单击“扫一扫”扫描二维码即可。

b. 验证动态码，输入OTP小程序中产生的动态码。

c. 单击“确定”完成动态命令激活。

说明

若无法扫描二维码，则打开OTP小程序，选择“手动输入”，在账号名、密钥输入框中分别输入界面上信息。

公共账号

如果在应用中添加了公共账号，并设置了当前登录账号为责任人，可以通过“公共账号”统一管理公共账号的使用人。

如需添加公共账号，请参考**授权管理**。

查看个人偏好

在用户门户页面，单击右上角的用户名，选择“账号设置”默认进入“个人资料”页面，在页面左侧选择“个人偏好”进入“个人偏好”页面，可以查看自己的常用应用、常用位置、认证时段分布、常用认证方式、认证失败原因、常用设备。

查看操作记录

在用户门户页面，单击右上角的用户名，选择“账号设置”默认进入“个人资料”页面，在页面左侧选择“操作记录”进入“操作记录”页面，可以查看自己的操作记录，可以根据时间、操作类型 、客体类型及结果进行查询。

6 云审计服务支持的关键动作

6.1 云审计服务支持的 OneAccess 操作列表

云审计服务（Cloud Trace Service，以下简称CTS），是华为云安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、审计、资源跟踪和问题定位等常见应用场景。

为了方便查看OneAccess控制台的关键操作事件，例如更新证书等，需要先**开通云审计服务**。

在OneAccess控制台进行操作，例如更新证书等，CTS将会记录这些操作。CTS支持记录OneAccess相关的操作事件，如**表1**所示。

表 6-1 CTS 支持的 OneAccess 操作列表

操作名称	资源类型	事件名称
订购实例	instance	orderInstance
更新证书	certificate	updateCertificate
创建自定义域名	domainName	createDomainName
删除自定义域名	domainName	deleteDomainName
删除实例	instance	deleteInstance

6.2 在 CTS 事件列表查看云审计事件

操作场景

用户进入云审计服务创建管理类追踪器后，系统开始记录云服务资源的操作。在创建数据类追踪器后，系统开始记录用户对OBS桶中数据的操作。云审计服务管理控制台会保存最近7天的操作记录。

说明

云审计控制台对用户的操作事件日志保留7天，过期自动删除，不支持人工删除。

本节介绍如何在云审计服务管理控制台查看或导出最近7天的操作记录。

- **在新版事件列表查看审计事件**
- **在旧版事件列表查看审计事件**

使用限制

- 单账号跟踪的事件可以通过云审计控制台查询。多账号的事件只能在账号自己的事件列表页面去查看，或者到组织追踪器配置的OBS桶中查看，也可以到组织追踪器配置的CTS/system日志流下面去查看。
- 用户通过云审计控制台只能查询最近7天的操作记录。如果需要查询超过7天的操作记录，您必须配置转储到对象存储服务(OBS)或云日志服务(LTS)，才可在OBS桶或LTS日志组里面查看历史事件信息。否则，您将无法追溯7天以前的操作记录。
- 云上操作后，1分钟内可以通过云审计控制台查询管理类事件操作记录，5分钟后才可通过云审计控制台查询数据类事件操作记录。
- CTS新版事件列表不显示数据类审计事件，您需要在旧版事件列表查看数据类审计事件。

在新版事件列表查看审计事件

1. 登录管理控制台。
2. 单击左上角 ☰ ，选择“管理与监管 > 云审计服务 CTS”，进入云审计服务页面。
3. 单击左侧导航树的“事件列表”，进入事件列表信息页面。
4. 事件列表支持通过高级搜索来查询对应的操作事件，您可以在筛选器组合一个或多个筛选条件：
   - 事件名称：输入事件的名称。
   - 事件ID：输入事件ID。
   - 资源名称：输入资源的名称，当该事件所涉及的云资源无资源名称或对应的API接口操作不涉及资源名称参数时，该字段为空。
   - 资源ID：输入资源ID，当该资源类型无资源ID或资源创建失败时，该字段为空。
   - 云服务：在下拉框中选择对应的云服务名称。
   - 资源类型：在下拉框中选择对应的资源类型。
   - 操作用户：在下拉框中选择一个或多个具体的操作用户。
   - 事件级别：可选项为“normal”、“warning”、“incident”，只可选择其中一项。
     - normal：表示操作成功。
     - warning：表示操作失败。
     - incident：表示比操作失败更严重的情况，例如引起其他故障等。

- 企业项目ID：输入企业项目ID。
- 访问密钥ID：输入访问密钥ID（包含临时访问凭证和永久访问密钥）。
- 时间范围：可选择查询最近1小时、最近1天、最近1周的操作事件，也可以自定义最近7天内任意时间段的操作事件。

说明

您可以参考**云审计服务应用示例**，来学习如何查询具体的事件。

5. 在事件列表页面，您还可以导出操作记录文件、刷新列表、设置列表展示信息等。
   - 在搜索框中输入任意关键字，按下Enter键，可以在事件列表搜索符合条件的数据。
   - 单击“导出”按钮，云审计服务会将查询结果以.xlsx格式的表格文件导出，该.xlsx文件包含了本次查询结果的所有事件，且最多导出5000条信息。
   - 单击按钮，可以获取到事件操作记录的最新信息。
   - 单击按钮，可以自定义事件列表的展示信息。启用表格内容折行开关，可让表格内容自动折行，禁用此功能将会截断文本，默认停用此开关。
6. 关于事件结构的关键字段详解，请参见**事件结构**和**事件样例**。
7. （可选）在新版事件列表页面，单击右上方的“返回旧版”按钮，可切换至旧版事件列表页面。

在旧版事件列表查看审计事件

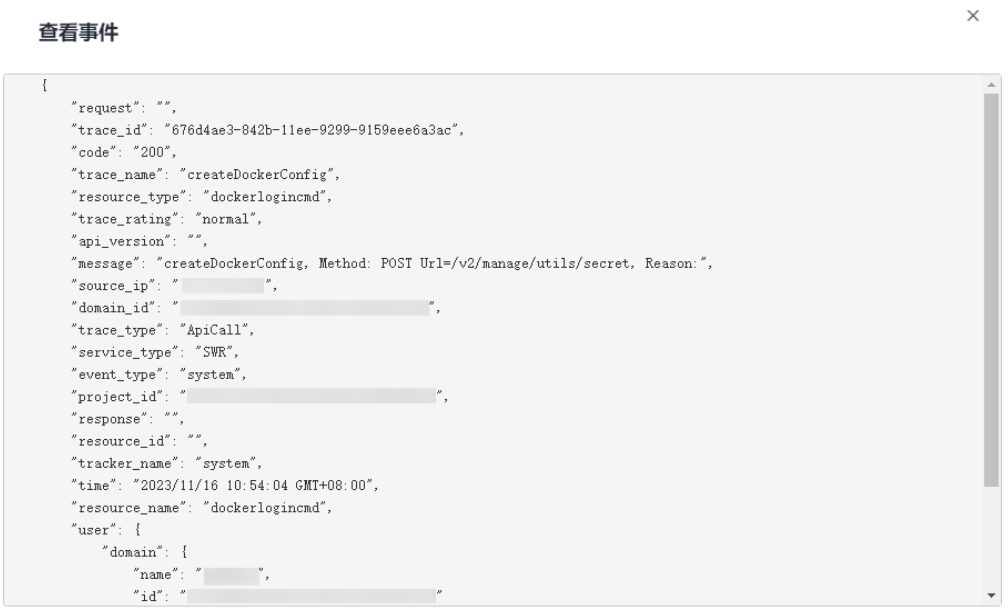
1. 登录管理控制台。
2. 单击左上角，选择“管理与监管 > 云审计服务 CTS”，进入云审计服务页面。
3. 单击左侧导航树的“事件列表”，进入事件列表信息页面。
4. 用户每次登录云审计控制台时，控制台默认显示新版事件列表，单击页面右上方的“返回旧版”按钮，切换至旧版事件列表页面。
5. 事件列表支持通过筛选来查询对应的操作事件。当前事件列表支持四个维度的组合查询，详细信息如下：
   - 事件类型、事件来源、资源类型和筛选类型，在下拉框中选择查询条件。
     - 筛选类型按资源ID筛选时，还需手动输入某个具体的资源ID。
     - 筛选类型按事件名称筛选时，还需选择某个具体的事件名称。
     - 筛选类型按资源名称筛选时，还需选择或手动输入某个具体的资源名称。
   - 操作用户：在下拉框中选择某一具体的操作用户，此操作用户指用户级别，而非租户级别。
   - 事件级别：可选项为“所有事件级别”、“Normal”、“Warning”、“Incident”，只可选择其中一项。
   - 时间范围：可选择查询最近1小时、最近1天、最近1周的操作事件，也可以自定义最近7天内任意时间段的操作事件。

说明

您可以参考**云审计服务应用示例**，来学习如何查询具体的事件。

6. 选择完查询条件后，单击“查询”。
7. 在事件列表页面，您还可以导出操作记录文件和刷新列表。
   - 单击“导出”按钮，云审计服务会将查询结果以CSV格式的表格文件导出，该CSV文件包含了本次查询结果的所有事件，且最多导出5000条信息。
   - 单击按钮，可以获取到事件操作记录的最新信息。
8. 在需要查看的事件左侧，单击 展开该记录的详细信息。

9. 在需要查看的记录右侧，单击“查看事件”，会弹出一个窗口显示该操作事件结构的详细信息。



10. 关于事件结构的关键字段详解，请参见《云审计服务用户指南》中的**事件结构**和**事件样例**。
11. （可选）在旧版事件列表页面，单击右上方的“体验新版”按钮，可切换至新版事件列表页面。

