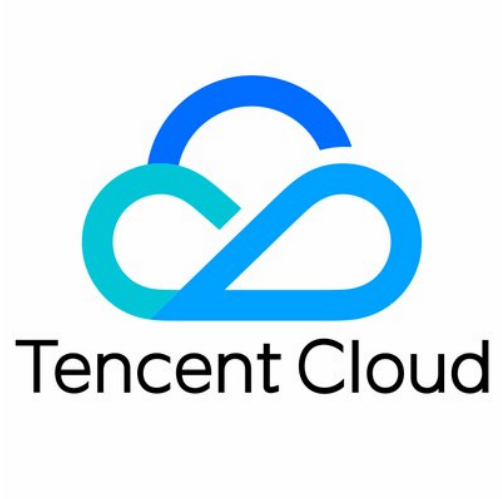
集团账号管理

操作指南

产品文档



文档目录

使用 TCCLI 登录
获取临时访问凭证

操作指南
控制台概述

最近更新时间：2024-03-06 18:40:46

集团账号管理控制台为集团提供账号管理功能。组织创建者能够建立组织关系，通过邀请或添加的方式管理组织成员，为成员设置财务管理策略、共享资源等。具体功能如下表：

名称	具体功能
集团组织设置	创建集团组织
	查看集团组织信息
	删除集团组织
	查看被邀请信息
	接受或拒绝邀请
	成员退出集团组织
部门管理	创建部门
	修改部门信息
	删除部门
	移动成员
成员账号管理	查看成员列表及成员基础信息
	移除组织成员
	邀请组织成员
	取消成员邀请
	授权访问成员账号
服务管控策略	服务管控策略概述
	开启服务管控策略
	创建自定义服务管控策略
	查看服务管控策略详情

	修改自定义服务管控策略
	删除自定义服务管控策略
	绑定自定义服务管控策略
	解绑自定义服务管控策略
	关闭服务管控策略
成员审计	审计成员日志

集团组织设置
使用限制说明

最近更新时间：2024-03-06 18:40:46

一、场景及限制说明

功能模块	管理账号操作场景	经销商子客	直销客户
账号管理	新建成员账号	新建的成员账号默认绑定管理账号同一经销商子客关系，且默认继承管理账号的企业实名	新建的成员账号实名主体与管理账号一致或者为已进行关联的其他主体
	邀请成员账号	待邀请账号必须是同一经销商的子客，且企业实名主体必须与管理账号一致，并且没有加入其他集团组织/没有其他集团账号的待处理邀请	待邀请账号必须是直销客户，且实名主体与管理账号一致或者为已进行关联的其他主体，并且没有加入其他集团组织/没有其他集团账号的待处理邀请
	退出集团账号	不支持成员退出集团组织	不支持成员退出组织
财务管理	查看财务概览	管理账号可以查看集团成员的代付账单概览	不支持
	代付费	成员账号的消费统一由管理账号支付	成员账号的消费统一由管理账号支付
	自付费	不支持	成员的消费自己支付（创建成员需要先选择代付，待绑卡开户后可转为自付）
	查看账单	管理账号可以查看成员的账单详情	管理账号可以查看成员的账单详情
	查看余额	不支持	管理账号可以查看成员账号的账户余额信息
	优惠继承	不支持	成员账号可以继承管理账号的折扣
	合并出账	不支持	管理账号将多个成员账号的费用合并下载
	开票	不支持	管理账号可以代成员账号开票

二、系统限制说明

模块	限制项	限制值
成员	创建成员的数量上限（实名账号数量的限制）	5
部门	部门层级的数量上限	5
	每个部门创建子部门的数量上限	20
成员登录	自定义登录权限上限	20
	自定义登录权限关联预设策略上限	30
	自定义登录权限关联自定义策略上限	1

创建集团组织

最近更新时间：2024-03-06 18:40:46

通过企业实名认证的用户，在未加入或未创建组织前，可通过集团账号管理创建组织。

操作步骤

登录集团账号管理控制台，选择左侧导航栏中的 **基本信息**，即可在页面中单击**创建**创建组织。

说明：

- 仅支持已通过企业实名认证的用户创建组织。企业实名认证详情请参见 企业实名认证指引 。
- 成功创建组织后，该账号不能加入其他的集团组织，直到此组织被删除。
- 仅支持腾讯云直接客户与经销商子客使用集团账号，且集团组织内账号类型必须一致。

查看集团组织信息

最近更新时间：2024-03-06 18:40:46

集团管理员或者成员，可在集团账号管理中查看组织中的部门信息。

操作步骤

登录集团账号管理控制台，单击左侧导航中的 **部门管理**，即可查看组织信息。组织信息包含了部门名称、部门 ID、成员名称、成员 ID、权限范围及付费模式等信息。

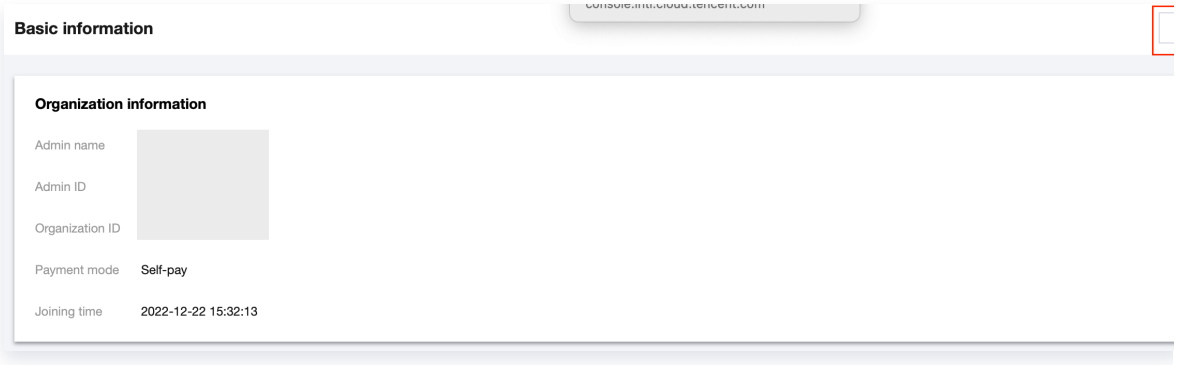
删除集团组织

最近更新时间：2024-03-06 18:40:46

集团组织创建者可以删除自己创建的集团组织。

操作步骤

1. 登录集团账号管理控制台，选择左侧导航栏中的**集团设置** > **基本信息** 。
2. 进入“基本信息”页面，并单击右上角的**删除组织**。如下图所示：



3. 在弹出的“删除集团组织”窗口中，单击**确定**即可删除组织。
   如存在以下场景，则无法直接删除组织：
   - 组织中仍有成员账号存在。
   - 组织资源共享中。

用户查看被邀请信息

最近更新时间：2024-03-06 18:40:46

用户可以通过集团账号管理控制台，查看被组织邀请信息。

操作步骤

登录集团账号管理控制台，选择左侧导航栏中的 **基本信息**，即可查看记录。

说明：

- 当您在未加入任何组织时，可以查看被邀请信息。
- 邀请列表仅展示近三个月的被邀请记录。
- 单条邀请记录最长15天内有效。

用户接受或拒绝邀请

最近更新时间：2024-03-06 18:40:46

用户可通过集团账号管理控制台，接受或拒绝集团组织邀请。

操作步骤

登录集团账号管理控制台，选择左侧导航栏中的 **基本信息**，即可“基本信息”页面中查看在有效期内的邀请记录，单击**接受**即可加入组织。
如需拒绝加入该集团组织，单击**拒绝**即可拒绝加入。

说明：

- 只有完成企业实名认证的用户才可加入集团组织。企业实名认证详情请参见 企业实名认证指引 。
- 成员的企业实名主体要与被邀请人一致，或成员的企业实名主体已成功添加至集团认证主体信息。
- 加入组织后，被邀请列表将会隐藏，直到退出组织。

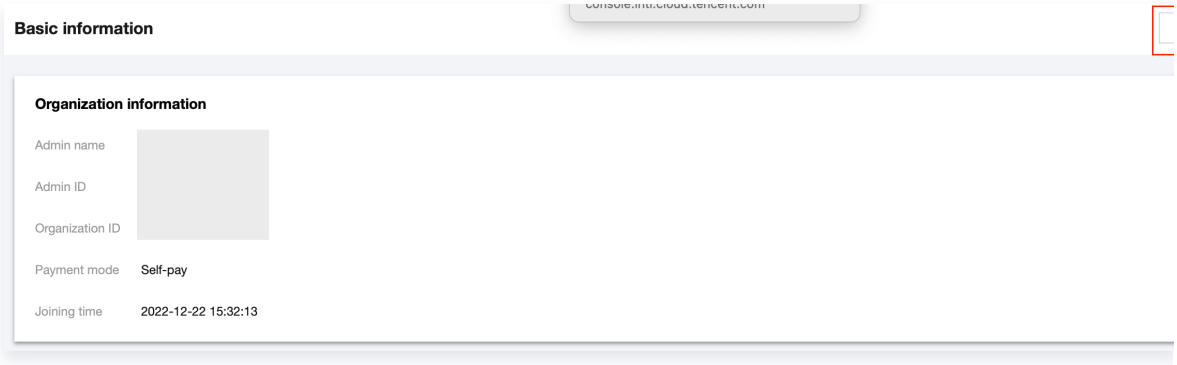
成员退出集团组织

最近更新时间：2024-03-06 18:40:46

组织成员可以退出自己所在的集团组织。

操作步骤

1. 登录集团账号管理控制台，选择左侧导航栏中的 **基本信息** 。
2. 进入“基本信息”页面，并单击**删除组织**。如下图所示：



3. 在弹出的“删除集团账号管理”确认窗口中，单击**确定**即可退出组织。
   如存在以下场景，则该成员无法直接退出：
   - 集团管理员设置该成员不允许退出。
   - 通过集团组织创建的成员。

部门管理
创建部门

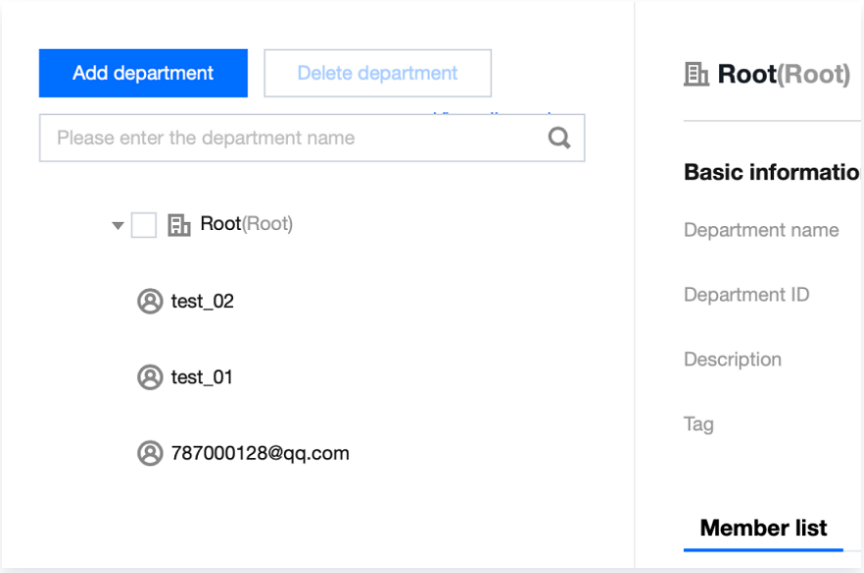
最近更新时间：2024-03-06 18:43:08

集团组织创建者可以对组织成员进行分部门管理，本文介绍如何通过集团账号管理控制台创建部门。

> **说明：**
> 部门关系最多支持5层。

操作步骤

1. 登录集团账号管理控制台，选择左侧导航中的 **部门管理** 。
2. 在“组织架构”页面中，单击**新增部门**。如下图所示：



3. 在弹出的“新建部门”窗口中，选择根单元名称、填写部门名称、输入描述、选择标签。
4. 单击**确定**即可在指定单元下创建子部门。

修改部门信息

最近更新时间：2024-03-06 18:43:08

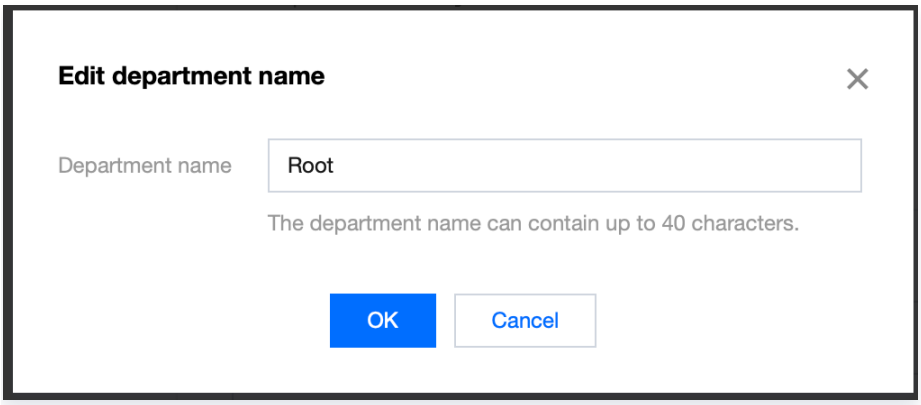
本文介绍如何通过集团账号管理控制台，修改部门信息。

操作步骤

登录集团账号管理控制台，选择左侧导航中的 **部门管理** 。按需修改组织单元相关信息。

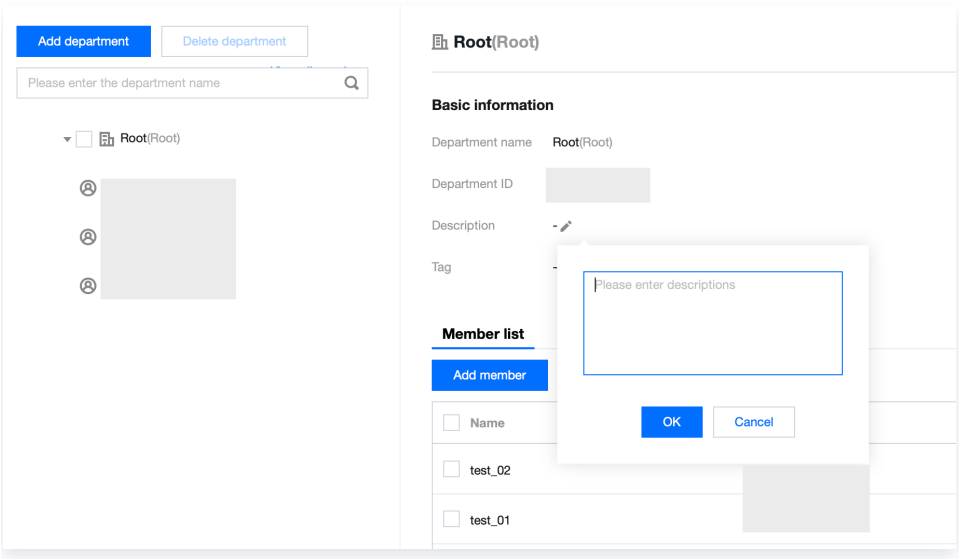
修改部门名称

单击部门名右侧的 ，在弹出的“编辑部门名称”窗口中输入新单元名称后，单击**确定**即可完成修改。如下图所示：



修改部门描述及标签

在组织架构右侧窗口中，选择描述或标签右侧的 ，在弹出的窗口中编辑后，单击**确定**即可完成修改。如下图所示：



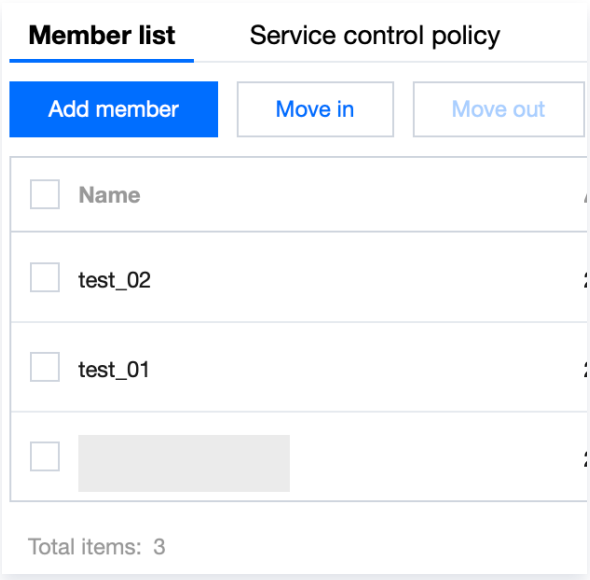
删除部门

最近更新时间：2024-03-06 18:43:08

当不再需要某个部门时，可通过集团账号管理控制台删除。

操作步骤

1. 登录集团账号管理控制台，选择左侧导航中的 **组织关系** 。
2. 在“组织架构”页面中，勾选需删除的部门，并单击上方的**删除部门**。如下图所示：



3. 在弹出的“删除部门”确认窗口中，单击**删除**即可。

移动成员

最近更新时间：2024-03-06 18:43:08

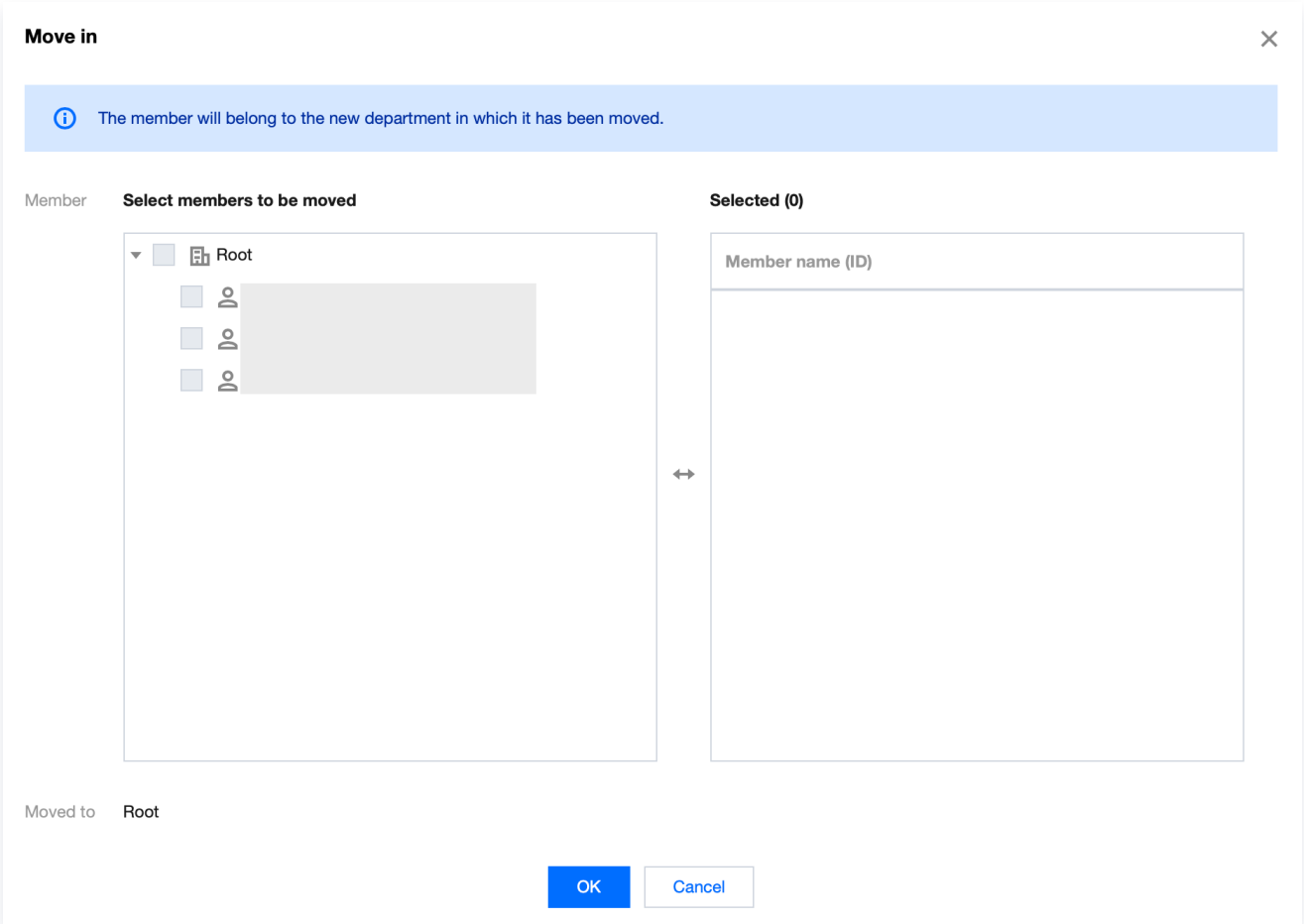
新成员默认在根单元目录下，集团组织创建者可以将成员移动到对应的部门中。

操作步骤

1. 登录集团账号管理控制台，选择左侧导航中的 **部门管理** 。
2. 在组织架构右侧窗口中，按需进行操作：

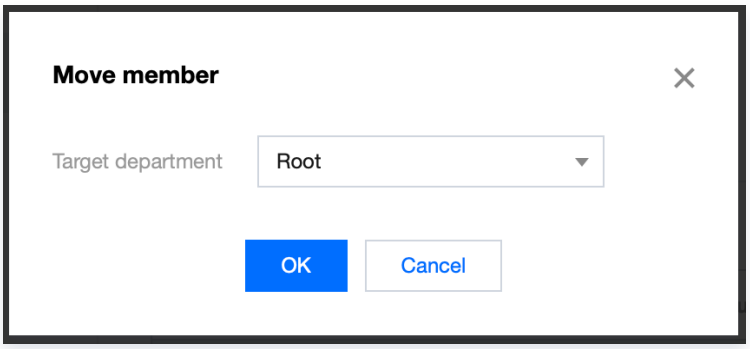
移入成员

1. 选择右侧“成员列表”中的**移入成员**。
2. 在弹出的“移入成员”窗口中，勾选需移入成员后单击**确定**即可。如下图所示：



移出成员

1. 选择右侧“成员列表”中的移出成员。
2. 在弹出的“移动成员”窗口中，选择目标部门，并单击确定即可。如下图所示：



成员账号管理
查看成员列表及成员基础信息

最近更新时间：2025-01-02 18:00:28

本文介绍如何通过集团账号管理控制台，查看成员列表及成员基础信息。

操作步骤

1. 登录集团账号管理控制台，选择左侧导航中的 成员账号管理，即可查看当前集团组织的成员信息。
   成员信息包含了成员名称、成员账号 ID、访问权限、财务权限、付费模式、所属部门、加入方式、是否允许退出等，其中名称、财务权限、付费模式、所属部门可修改。
2. 在“成员列表”页面中，选择需更改名称成员所在行的编辑按钮。在弹出的编辑框中输入新的成员名称，并单击确定即可保存修改。如下图所示：

3. 单击需更换所属部门成员所在行右侧的编辑，在弹出的“编辑成员”窗口中的“所属部门”下拉列表中，选择目标部门，并单击确定即可保存修改。如下图所示：

4. 单击需要更改财务权限或者付费模式的成员所在行右侧的编辑，在弹出的“编辑成员”窗口中的“财务权限”以及付费模式的模块进行更改，并单击确定即可保存修改。如下图所示：

移除组织成员

最近更新时间：2024-03-06 18:43:08

本文介绍如何通过集团账号管理控制台，移除组织成员。

> **注意：**
> - 移除组织成员后，将无法在成员列表中查看及编辑，在组织关系中显示及移动该成员。
> - 集团组织创建者账号无法移除。

操作步骤

1. 登录集团账号管理控制台，选择左侧导航栏中的 **成员账号管理** 。
2. 您可移除单个或批量成员：
   - **移除单个成员**：选择成员所在行右侧的**移除**，在弹出确认框中单击**确定**即可。
   - **批量移除成员**：勾选成员名称左侧的复选框，单击成员列表上方的**删除成员**即可。

添加组织成员

最近更新时间：2025-01-02 18:00:28

集团组织创建者可以为组织添加成员，支持邀请和创建两种方式。

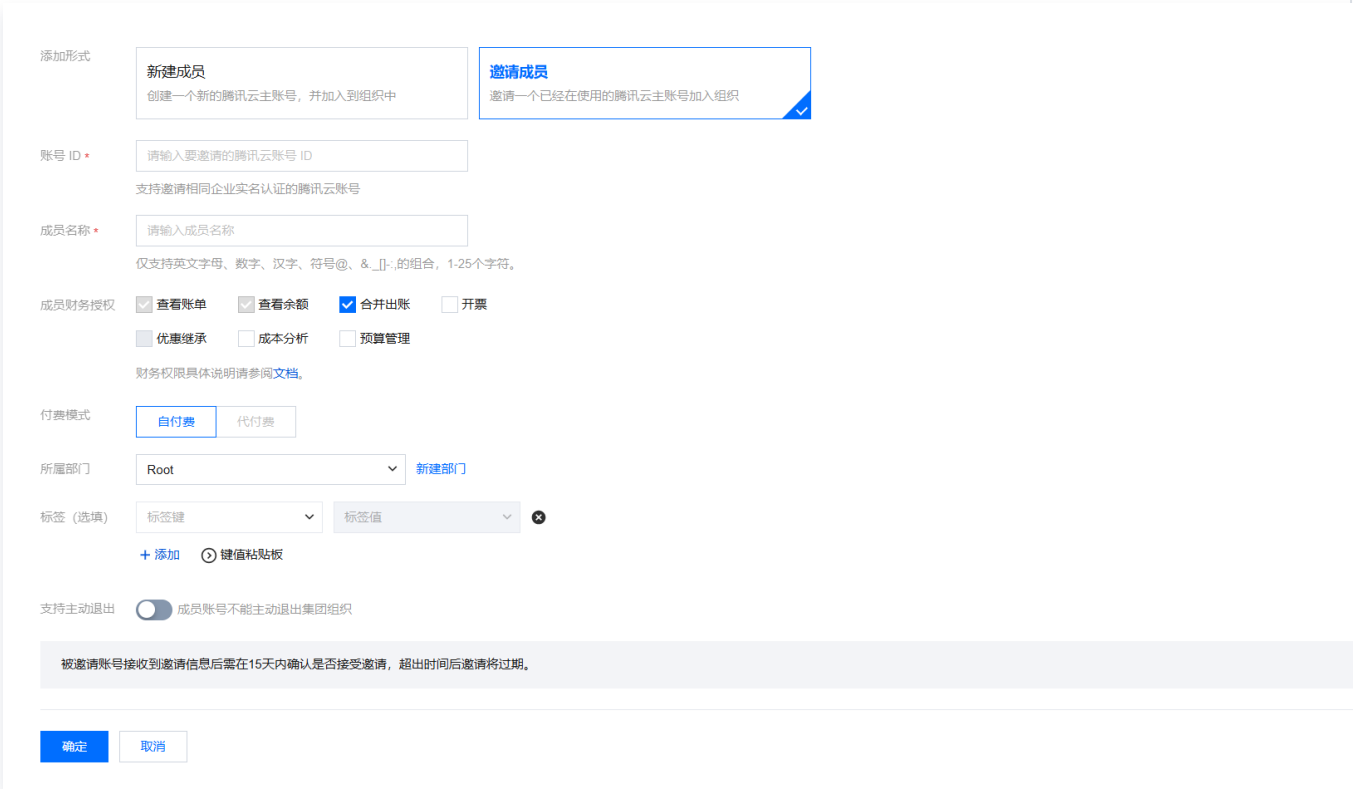
操作步骤

请您结合实际需求，按需选择添加成员方式：

邀请成员

一. 直客场景：

1. 登录集团账号管理控制台，选择左侧导航中的 成员账号管理 。
2. 在**成员账号管理**页面中，单击**添加成员**。
3. 在**添加成员**页面，选择**邀请成员**，如下图所示：



4. 依次按需填写账号 ID、成员名称、财务权限、付费模式、所属部门及是否支持主动退出。其中，账号 ID 可

前往 账号信息 页面获取。

5. 填写完成后，单击**确定**，需要进行被邀请成员信息验证。被邀请账号需要完成企业实名认证且未加入任何集团组织，另外认证主体需要和管理账号一致或者已完成主体关联认证。若未完成主体关联认证，需要联系商务同学进行主体关联才可以邀请成员。
6. 邀请成功后，邀请信息15天内有效。您可选择左侧导航中的 **组织变更记录**，选择**成员邀请记录**页签，查看邀请信息，如下图所示：

二. 经销商子客场景：

> **说明：**
> 在经销场景下：
> - 需保证集团下所有成员账号的经销关系统一，即成员账号与管理员账号同属于一个经销商；在邀请新账号加入集团时，需要满足被邀请账号和集团管理员为统一经销商的前提条件。
> - 成员账号付费模式仅支持代付费，暂不支持自付费模式。

1. 登录集团账号管理控制台，选择左侧导航中的 **成员账号管理**。
2. 在**成员账号管理**页面中，单击**添加成员**。
3. 在**添加成员**页面，选择**邀请成员**，
4. 依次按需填写账号 ID、成员名称、所属部门及是否支持主动退出。其中，账号 ID 可前往 账号信息 页面获取。

> **注意：**
> - 经销商子客场景下财务权限默认选择“查看账单”，付费模式暂时仅支持“代付费”。
> - 如需创建部门，则请参见 创建部门。

5. 填写完成后，单击**确定**，需要进行被邀请成员信息验证，校验内容如下：
   - 被邀请账号需要完成企业实名认证且未加入任何集团组织；
   - 企业实名认证主体需要和管理账号一致；
   - 需保证集团下所有成员账号的经销关系统一，即成员账号与管理员账号同属于一个经销商。

6. 邀请成功后，邀请信息15天内有效。您可选择左侧导航中的 **组织变更记录**，选择**成员邀请记录**页签，查看邀请信息，如下图所示：

新建成员

一. 直客场景：

> **说明：**
> 集团组织创建者可以为组织新建当前主体或其他主体的成员。其中当前主体为管理账号所属主体，如果新建成员的主体与管理账号主体不一致，则为其他主体。

新建当前主体成员

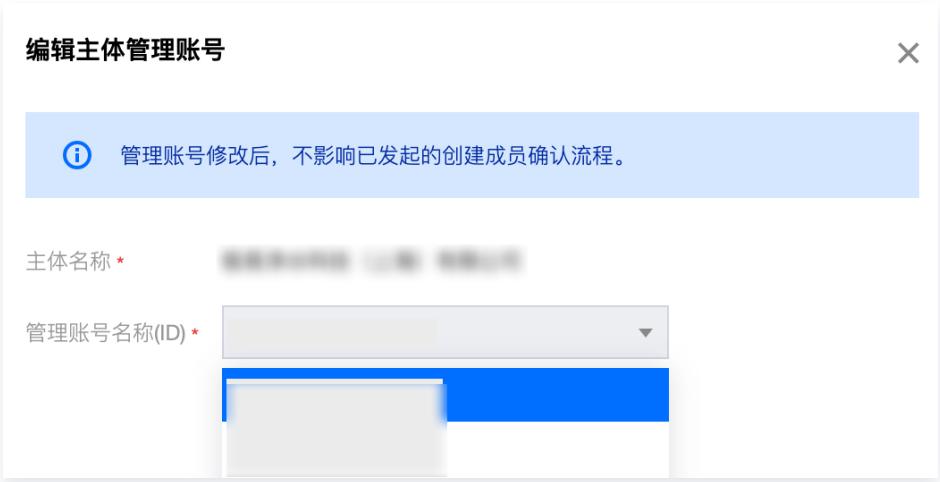
1. 登录集团账号管理控制台，选择左侧导航中的 成员账号管理 。
2. 在“成员列表”页面中，单击**添加成员**，如下图所示：

3. 依次按需填写名称、所属主体、财务权限及所属部门。
   - 其中所属主体选择“当前主体”。
   - 创建成员默认选择代付费。
   - 如需创建部门，则请参考 创建部门 。
4. 单击**确定**后，会自动创建成员账号。成员账号将继承创建者的企业实名信息。
   您可在左侧导航中的 **组织变更记录** ，选择**成员变更记录** > **成员新建记录**页签查看创建记录和结果，如下图所示：

新建其他主体成员

1. 联系商务申请关联其他主体。
2. 待商务申请关联其他主体成功后，登录 集团账号管理 控制台，选择左侧导航栏中的**认证主体管理**。在主体管理列表中，单击邀请成员，邀请对应主体的成员加入组织。详情请参见 添加组织成员 中的**邀请成员**页签。

3. 返回 认证主体管理，单击编辑主体管理账号，设置对应主体的管理员，如下图所示：



4. 在**认证主体管理**页面的“主体管理列表”或者 成员账号管理 页面的“成员列表”中，单击创建成员，默认选择“新建成员”。
5. 依次按需填写名称、所属主体、财务权限、付费模式及所属部门。其中所属主体选择“其他主体”，在下拉列表中选择对应的主体。

> **注意：**
> - 创建成员默认选择代付费。
> - 如需创建部门，则请参见 创建部门 。

6. 对应主体管理账号进行审核，审核通过后创建完成。成员账号将继承主体管理员的企业实名信息。 您可在左侧导航中的组织变更记录，选择**成员变更记录** > **成员新建记录**页签查看创建记录和结果，如下图所示：

二. 经销商子客场景：

1. 登录集团账号管理控制台，选择左侧导航中的 **成员账号管理** 。
2. 在“成员列表”页面中，单击**添加成员**。
3. 依次按需填写名称、所属部门。

> **注意：**
> - 经销商子客场景下财务权限默认选择“查看账单”，付费模式暂时仅支持“代付费”。

- 如需创建部门，则请参见 创建部门 。

4. 单击**确定**后，会自动创建成员账号。成员账号将继承创建者的企业实名信息。
   您可在左侧导航中的 **组织变更记录**，选择**成员变更记录** > **成员新建记录**页签查看创建记录和结果，如下图所示：

5. 创建的成员默认继承管理账号的企业实名认证主体，并绑定管理账号同一经销商的子客关系。

取消成员邀请

最近更新时间：2024-03-06 18:43:08

集团组织创建者可以在被邀请人接受邀请前，进行取消邀请的操作。

操作步骤

1. 登录集团账号管理控制台，选择左侧导航中的 **组织变更记录** 。
2. 在“组织变更记录”页面中，选择**成员变更记录** > **成员邀请记录**页签，并单击被邀请人所在行右侧的**取消邀请**。
3. 在弹出提示框中，单击**确定**即可完成操作。

为成员和部门绑定标签

最近更新时间：2024-09-24 16:43:40

集团账号管理支持为成员账号和部门绑定标签，方便您为账号添加更多信息，实现基于标签的成员分类管理。

操作场景

标签由一个键值对（Key:Value）组成，包含标签键（Key）、标签值（Value）。有关标签的详细信息，请参见 标签。

支持管理账号给以下内容绑定标签：

- 成员账号
- 组织的根（root）
- 组织部门

您可以在以下场景绑定标签：

- 添加成员时：新建成员和邀请成员加入组织时，为成员绑定标签。
- 已在组织内成员：在集团账号管理控制台的成员账号管理页面，编辑对应成员的标签信息。
- 新增部门时：新增部门时绑定标签。
- 已有部门：为已存在的部门编辑标签。

操作步骤

成员账号

添加成员时绑定标签

1. 登录 集团账号管理控制台。
2. 在左侧导航栏中：
   - 单击**部门管理**，进入部门管理页面；
   - 或者单击**成员账号管理**，进入成员账号管理页面。
3. 单击**添加成员**。
4. 在编辑标签的位置，在下拉列表里选择标签键值。若当前已有标签键值无法满足需求，请前往 标签控制台 创建新标签，详情请参见 创建标签并绑定资源。

说明：

以新建成员时绑定标签为例，邀请成员时操作相同。

编辑给成员绑定的标签

1. 登录 集团账号管理控制台 。
2. 在左侧导航栏中，单击**成员账号管理**，进入成员账号管理页面。
3. 单击对应**成员名称**，进入该成员详情页。

4. 在编辑标签的位置，单击右侧编辑图标，进入编辑标签。

5. 在**编辑标签**中，进行标签绑定和解绑等操作。为成员账号解绑标签，单击对应标签右侧的删除图标即可。

6. 单击**确定**完成修改。

部门

新增部门时添加标签

1. 登录 集团账号管理控制台 。
2. 在左侧导航栏，单击部门管理，进入**部门管理**页面。
3. 单击**新增部门**。
4. 在编辑标签的位置，添加标签键值。

5. 单击**确定**，完成创建部门并绑定标签。

编辑给部门绑定的标签

1. 在**部门管理**页面，单击对应部门节点。
2. 单击标签右侧的编辑图标，进入编辑标签。

3. 在编辑标签中，进行标签绑定和解绑等操作。

4. 单击**确定**保存。

> **说明：**
> - 集团账号管理已标准化接入标签，后续“原部门标签”将下架，请尽快将“原部门标签”复制到标准“标签”。
> - 方法：将原部门标签的“标签键:标签值”在 标签控制台 创建成新标签，再参考上述 编辑给部门绑定的标签，为部门绑定标签。

创建成员登录权限

最近更新时间：2024-10-30 10:55:18

操作场景

在集团账号管理中，集团管理员可通过创建**登录权限**来细化成员权限。被授予登录权限的子用户仅可在其拥有的权限范围内登录成员账号。本文介绍如何通过集团账号管理控制台创建成员登录权限。

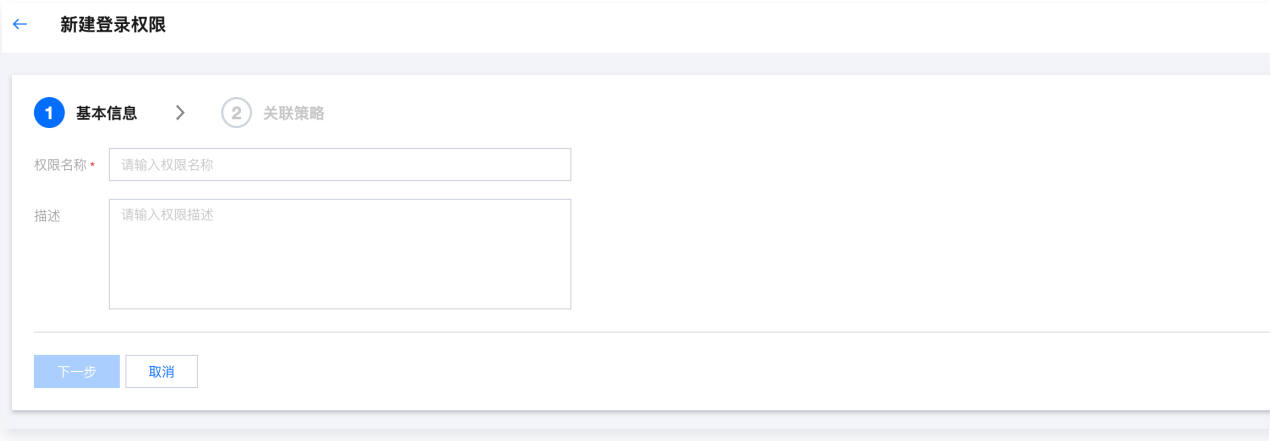
操作步骤

创建登录权限

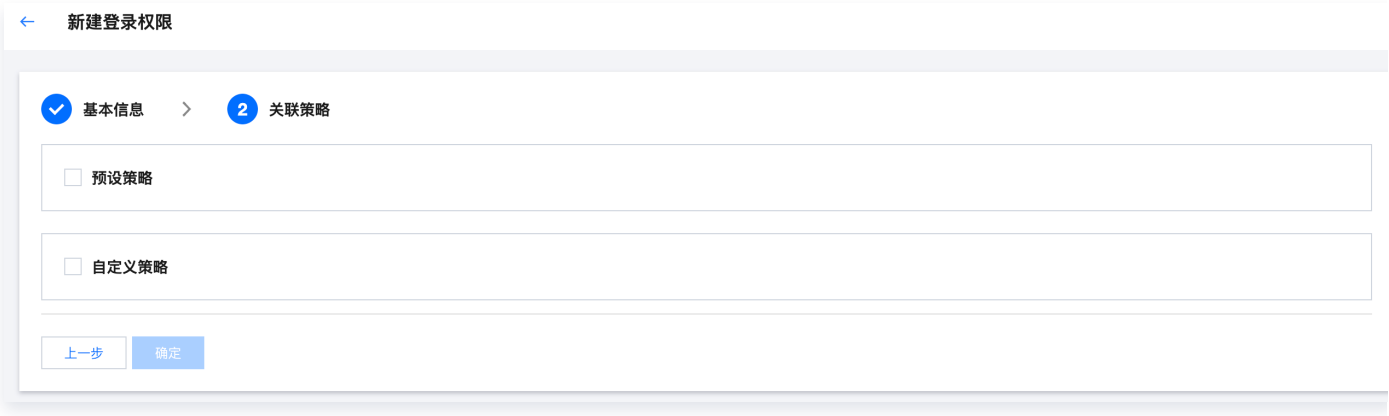
1. 登录**集团账号管理控制台**，选择左侧导航栏中的 成员登录权限设置 。
2. 单击**新建登录权限**。
3. 在弹出的**新建登录权限**窗口中，按需设置权限名称、描述、关联权限策略。

> **说明：**
> 您可前往 策略 页面，了解策略具体含义。

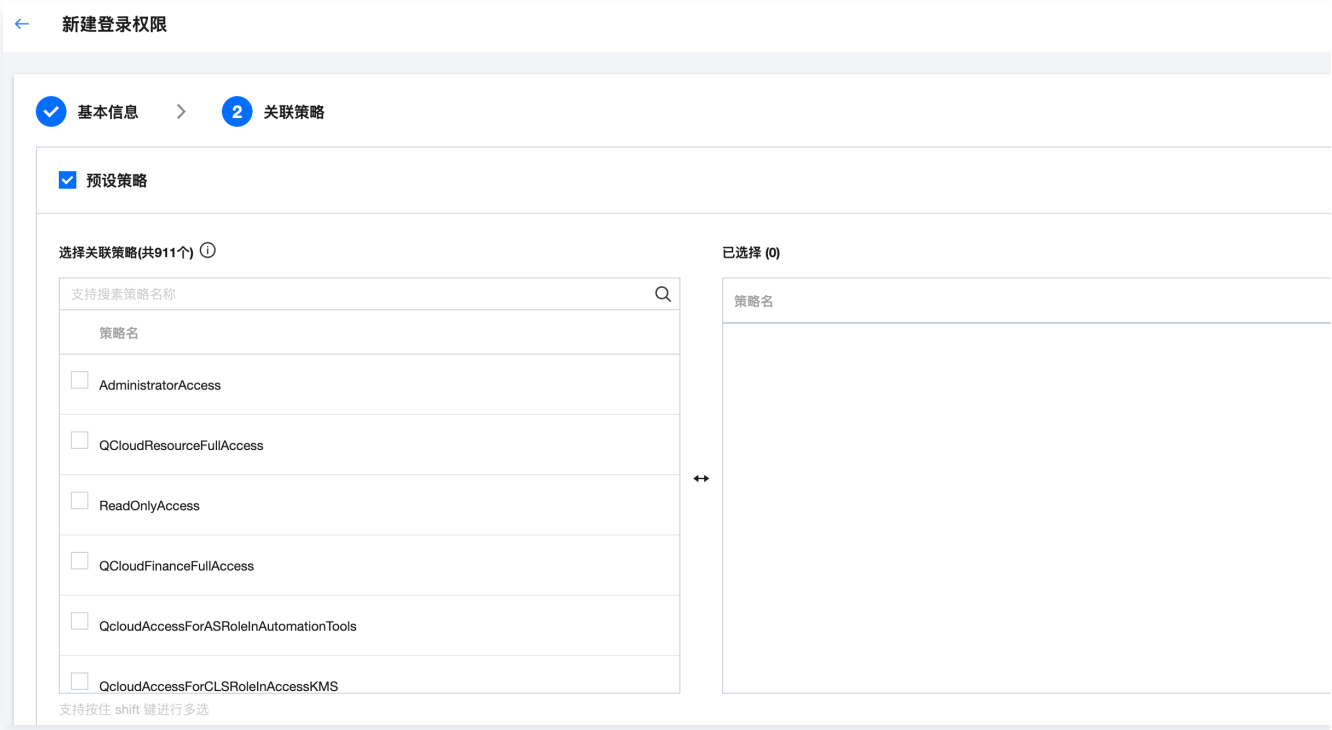
3.1 填写登录权限基本信息，包含权限名称和描述，其中权限名称为必填，描述为选填，输入基本信息后单击**下一**



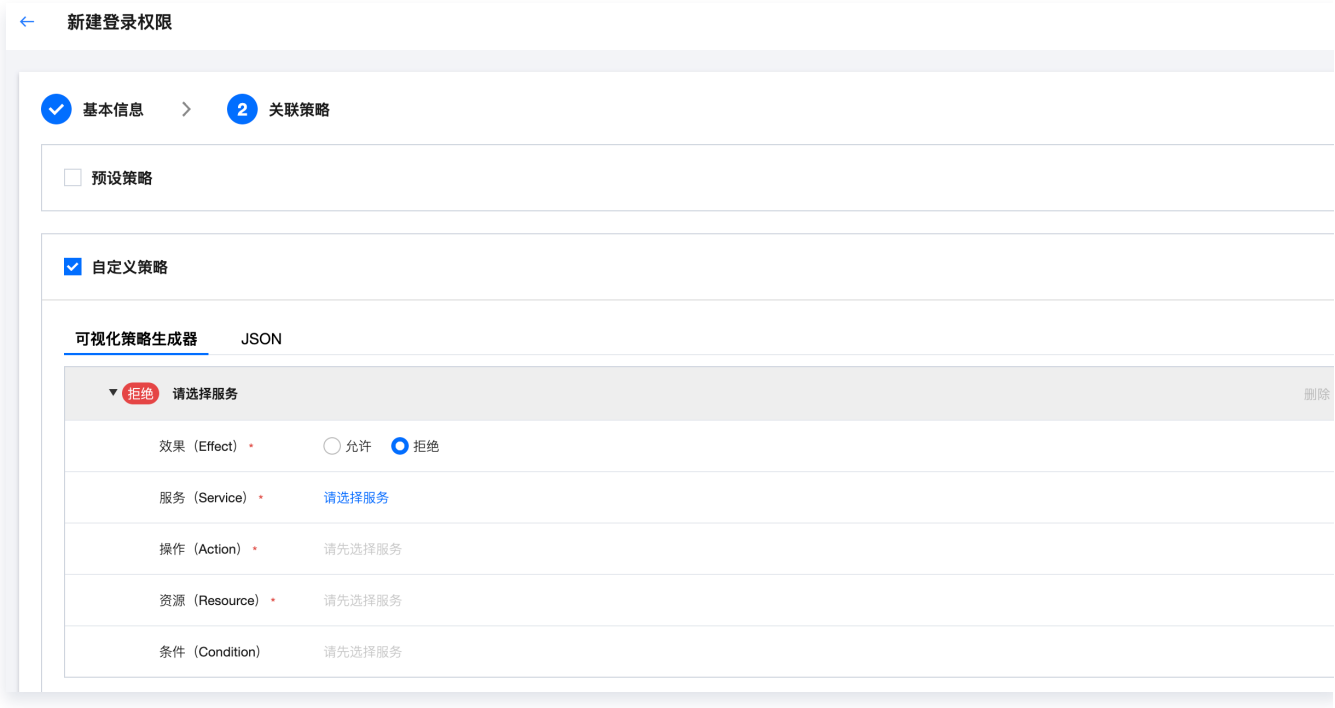
3.2 选择登录权限关联的策略，可以根据需求选择预设策略或自定义策略（可同时选择）。



- 选择预设策略，可在预设策略列表中进行勾选。



- 选择自定义策略，可使用可视化策略生成器或者JSON，根据需求自定义设置策略。



4. 单击**确定**即可成功创建登录权限。

> **注意：**
> - Admin 为默认权限，该权限可使成员账号具备管理员权限。
> - 集团管理员最多只能创建30个自定义权限。

为成员配置登录权限

最近更新时间：2024-09-12 18:27:57

操作场景

创建了登录权限后，您可以为成员配置登录权限，本文介绍如何通过集团账号管理控制台，为成员配置登录权限，以及删除成员登录权限。

操作步骤

配置成员登录权限

1. 登录**集团账号管理控制台**，选择左侧导航栏中的 多成员授权管理 。
2. 在成员列表中勾选需要配置权限的成员。
3. 单击**配置权限**。

3.1 选择权限

在权限列表中选择需要配置的权限。如下图所示：

3.2 预览确认

在预览页面确认成员账号和权限信息，如下图所示：

4. 单击**完成**即可成功为成员配置登录权限。

> **注意：**
> - 选择成员时，一次最多勾选10个成员。
> - 配置权限时，可选择的权限列表包含全部默认的登录权限和自定义创建的登录权限。
> - 对于功能上线前邀请的成员账号，暂不支持配置成员登录权限，需要联系商务开通相关功能。

删除登录权限

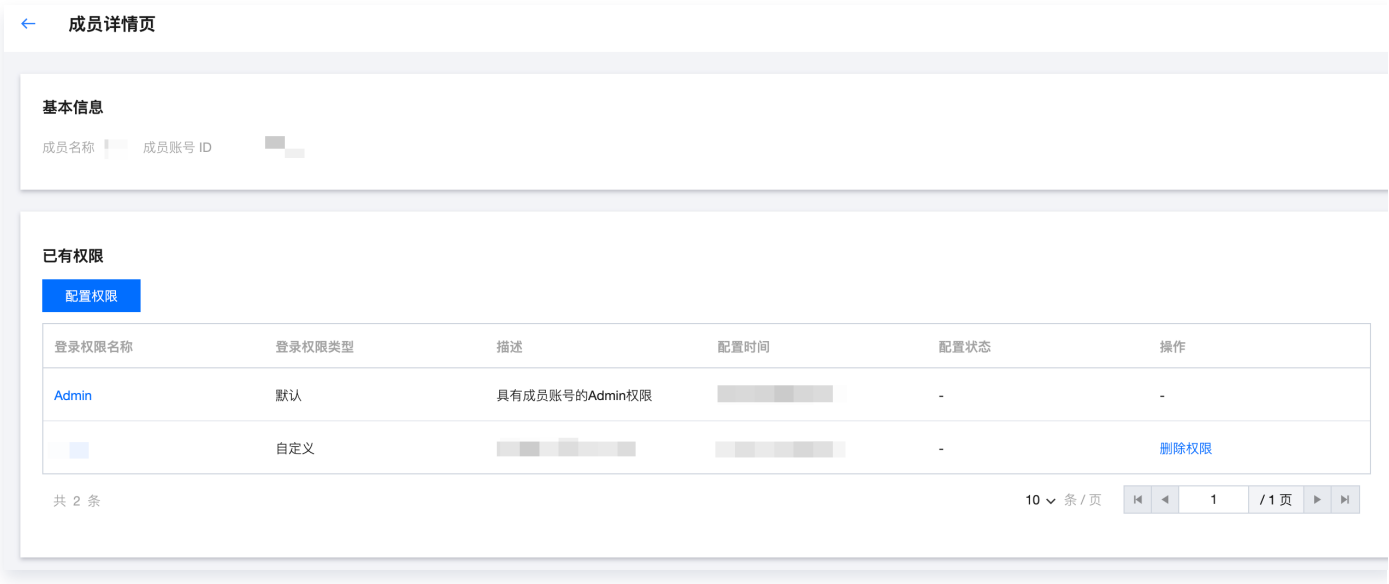
方式一：

1. 登录**集团账号管理控制台**，选择左侧导航栏中的 多成员授权管理 。
2. 选择对应的成员并单击其操作列的**删除权限**。
3. 在弹出的**删除登录权限**窗口中，选择需要删除的权限。

4. 单击**删除**即可成功删除登录权限。

方式二：

1. 登录**集团账号管理控制台**，选择左侧导航栏中的 多成员授权管理 。
2. 单击对应的成员名称进入**成员详情页**。
3. 在**成员详情页**中，选择需要删除的权限，并单击操作列的**删除权限**，如下图所示：



4. 在弹出的窗口中，单击**确定**即可成功删除登录权限。

授权登录成员账号

最近更新时间：2024-09-12 18:28:38

操作场景

集团管理账号可以通过创建集团管理策略，授权子用户登录并管理成员账号的权限。本文介绍如何通过为集团管理账号的子用户授予集团管理策略，使其可以登录集团组织的成员账号。

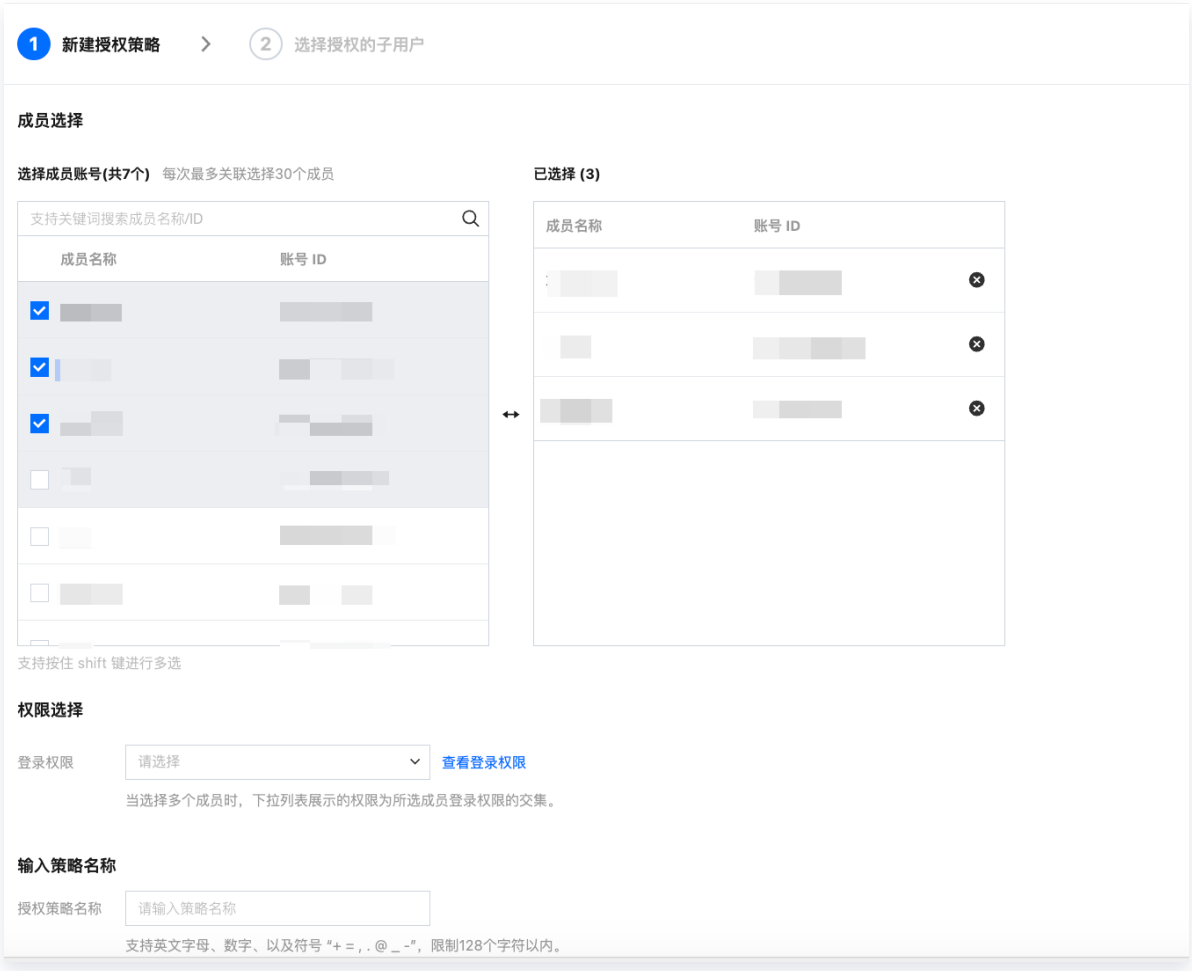
> **说明：**
> 若成员账号是新创建的，请15分钟后再进行登录操作，否则可能无法正常进入腾讯云控制台。

操作步骤

一、添加授权

1. 登录**集团账号管理控制台**，选择左侧导航栏中的 多成员授权管理 。
2. 单击**添加子用户授权**页签，单击**添加授权**。如下图所示：

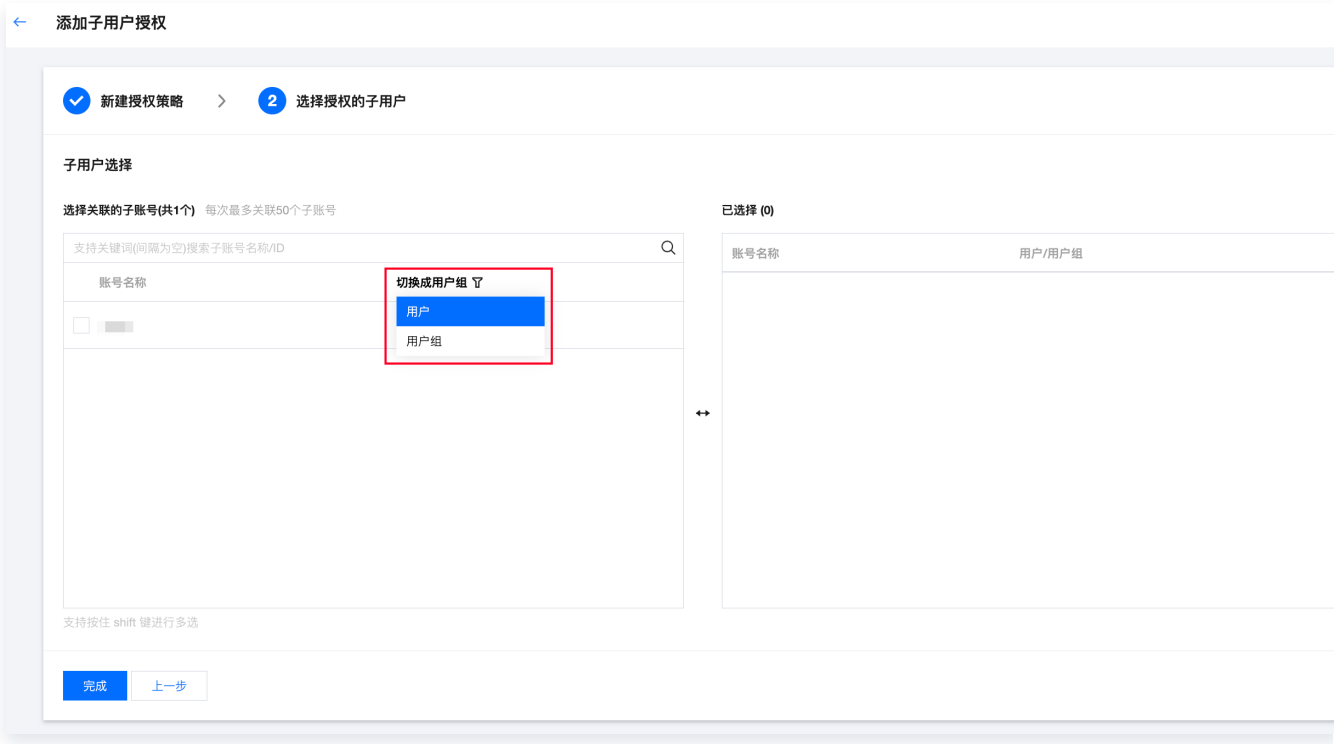
3. 在弹出的**添加授权**窗口中，依次选择成员、权限和输入授权策略名称。如下图所示：



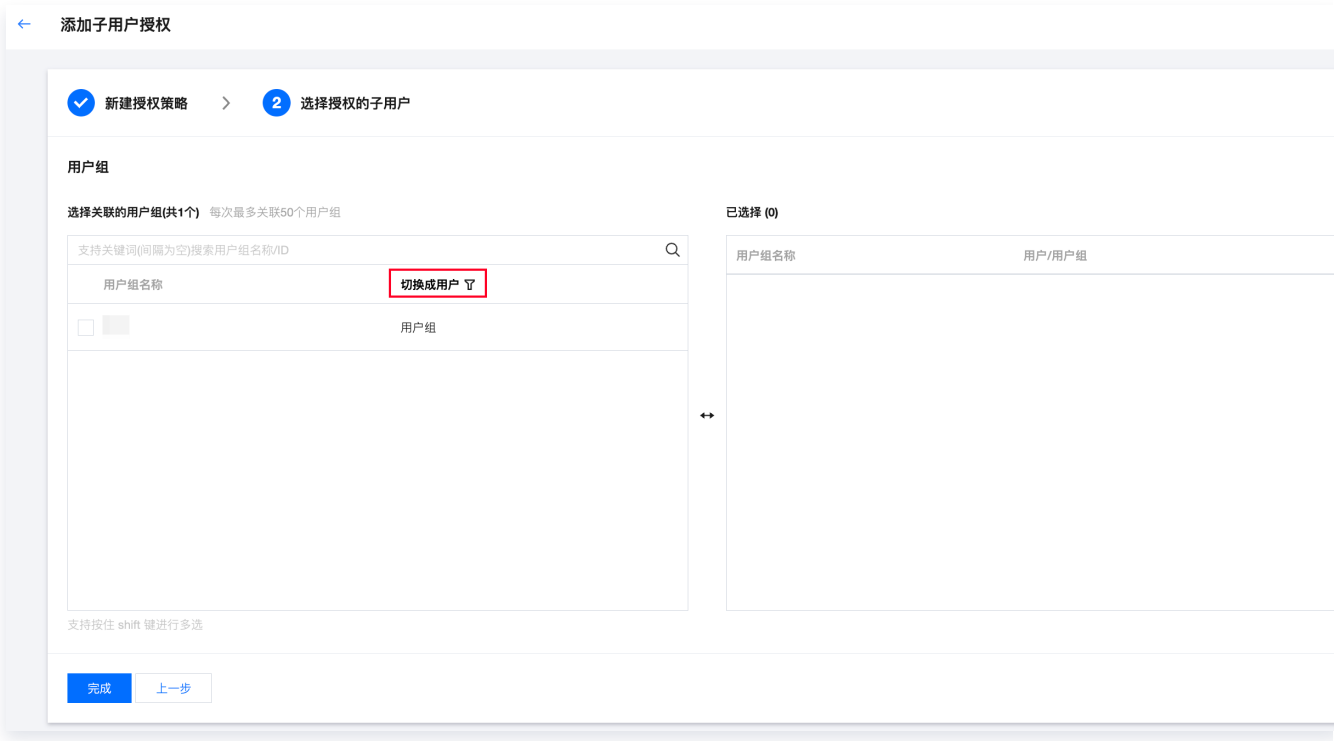
说明：

- 本步骤中新建的策略即为集团管理策略。
- 集团管理策略不允许在 CAM 修改或删除，若需要修改集团管理策略，请前往 授权策略管理 页面。
- 授权策略名称不允许重复。
- 对于功能上线前邀请的成员账号，暂不支持授权，需要联系商务开通相关功能。
- 当选择多个成员时，**登录权限下拉列表**展示的权限为所选成员登录权限的交集，并且只允许选择一个登录权限。

4. 单击**下一步**，按需选择关联的子账号，支持选择子用户或者用户组。
   - 默认选择子用户，若需要选择用户组，可以切换成用户组，如下图所示。



- 选择用户组后，也可切换成子用户，如下图所示。



5. 单击**完成**即可完成授权。

二、使用子账号登录成员控制台

完成授权后，您可使用对应的子账号登录成员控制台并进行管理操作。

1. 使用授权子账号登录**集团账号管理控制台**，选择左侧导航栏中的 成员登录 。
2. 在**成员登录**页面中，选择需要登录的成员账号，并单击操作列的**登录账号**，在弹出的**登录成员账号**窗口中选择登录权限进行登录。如下图所示：

> **注意：**
> - 每次只能选定一个权限进行登录。
> - 只能使用管理账号的子账号授权登录成员账号。

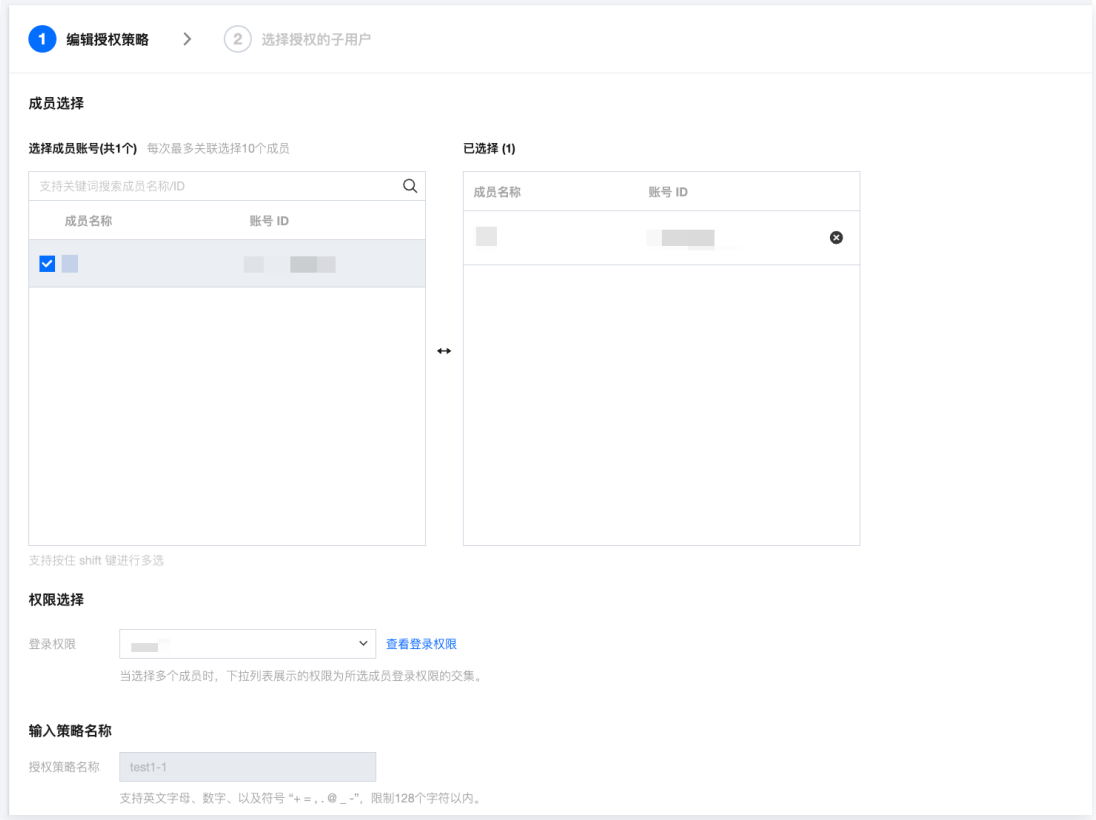
三、取消授权

1. 登录**集团账号管理控制台**，选择左侧导航栏中的 多成员授权管理 ，单击**添加子用户授权**页签。
2. 在**添加子用户授权**页面，单击操作列的**解绑**。

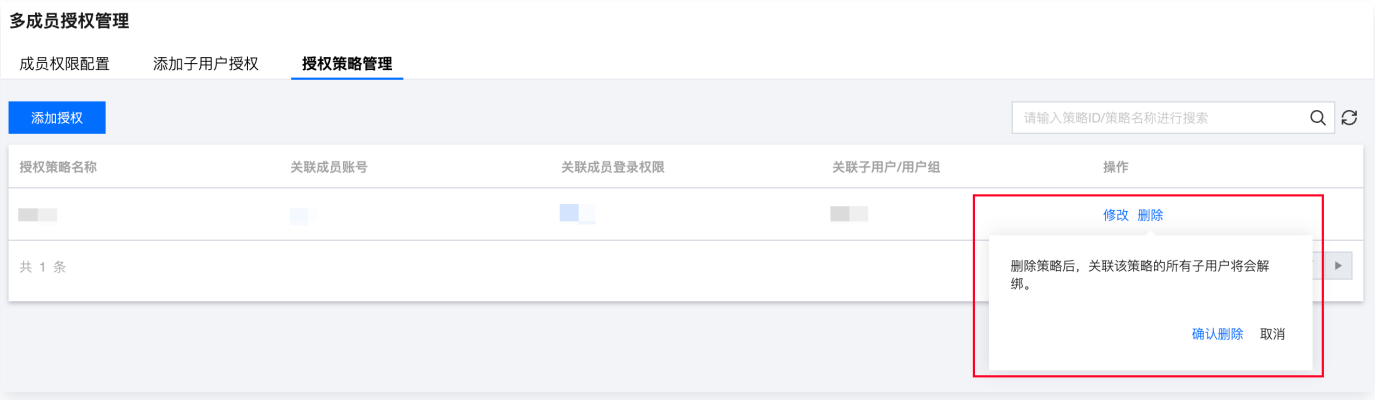
3. 单击确定即可取消授权。

四、修改或删除集团管理策略（授权策略）

1. 登录**集团账号管理控制台**，选择左侧导航栏中的 多成员授权管理 ，单击**授权策略管理**页签。
2. 在**授权策略管理**页签，单击操作列的**修改**，即可在对应页面修改策略内容，其中策略名称不支持修改。



3. 在**授权策略管理**页签，单击操作列的**删除**，在弹窗中单击**确认删除**，即可删除对应的授权策略。



五、管理子账号登录成员账号的权限

集团管理账号的**根账号（主账号）**可以查看所有子账号可登录成员账号的列表，并有权回收子账号的权限。

1. 登录**集团账号管理控制台**，选择左侧导航栏中的 成员登录 。
2. 在**成员登录列表**页面，选择对应成员，单击操作列的**回收权限**。

3. 或者选择左侧导航栏中的多成员授权管理，在添加子用户授权页面，单击操作列的解绑。

4. 单击**确定**即回收权限成功。

为创建的成员设置消息订阅

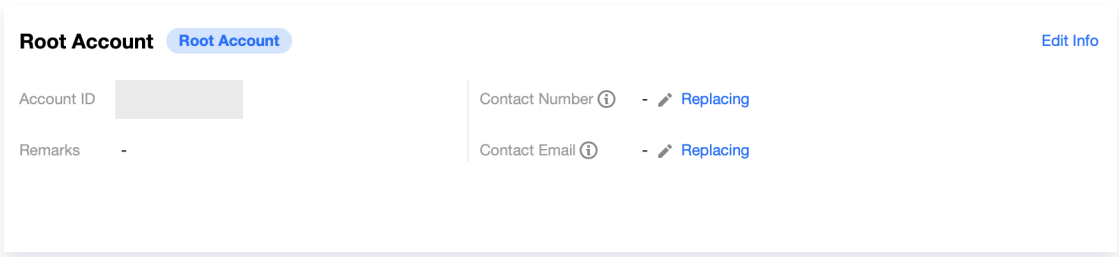
最近更新时间：2024-03-06 18:43:08

操作场景

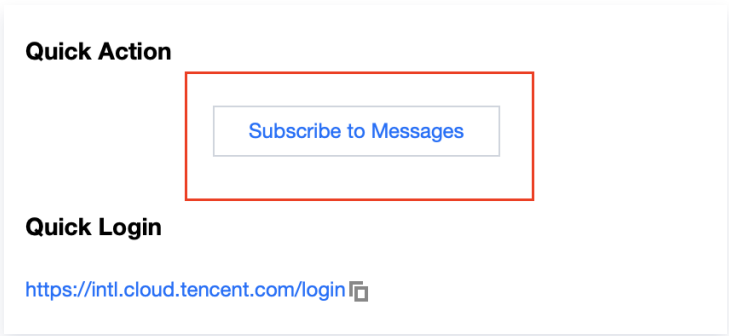
通过集团账号管理创建的成员默认没有配置联系方式，无法直接通过短信、邮箱等渠道接受消息通知。如需配置消息订阅，可参考本文进行配置。

操作步骤

1. 登录成员账号控制台，详情请参见 授权访问成员账号 。
2. 登录访问管理控制台，选择则侧导航栏中的**用户** > 用户列表 。
3. 在“用户列表”页面，单击用户名称进入用户详情页。
4. 单击联系方式后的 ，即可按照页面提示添加联系手机和邮箱。如下图所示：



5. 完成联系方式添加后，可单击右侧“快捷操作”中的**订阅消息**。如下图所示：



6. 在弹出的“订阅消息”窗口中，设置需接收的消息即可。

> **说明：**
> 您也可以在成员账号下创建子用户，参考上述操作通过子用户来接收消息。

为成员绑定安全信息

最近更新时间：2024-11-04 15:05:55

操作场景

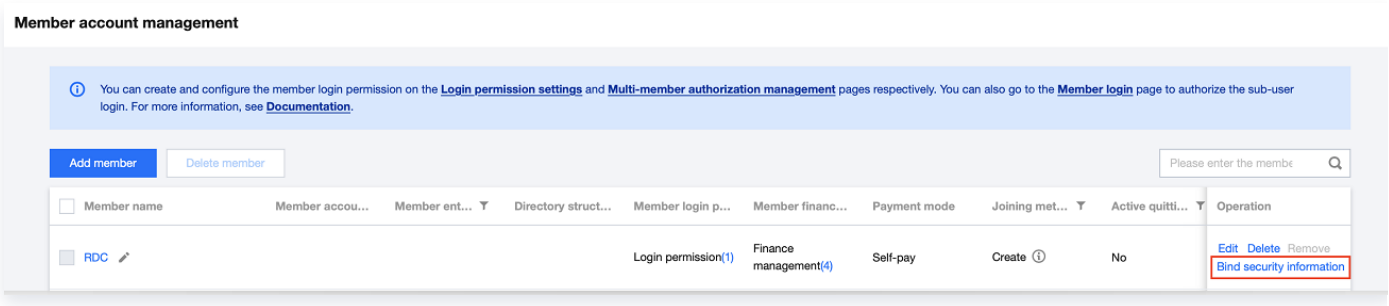
本文介绍如何通过集团账号管理控制台，为创建的成员账号绑定邮箱和安全手机信息。绑定成功后您可以使用该邮箱登录成员账号，也可根据实际情况将该成员移除出组织。

> **注意：**
> 通过邀请方式加入组织的成员账号，暂不支持绑定安全信息。

操作步骤

绑定安全信息

1. 登录集团账号管理控制台，选择左侧导航栏中的 成员账号管理 。
2. 在“成员账号管理”页面中，单击成员所在行右侧的**绑定安全信息**。如下图所示：



3. 在弹出的“配置安全信息”窗口中填写邮箱及手机号后，单击**提交**。

> **注意：**
> - 每个邮箱只能绑定一个成员账号。
> - 绑定的安全信息在激活前仅支持修改三次，请正确填写邮箱和手机号码。

4. 绑定信息提交成功后，系统将发送15天有效的激活链接到邮箱，请前往邮箱并单击激活链接。

重新发送激活链接

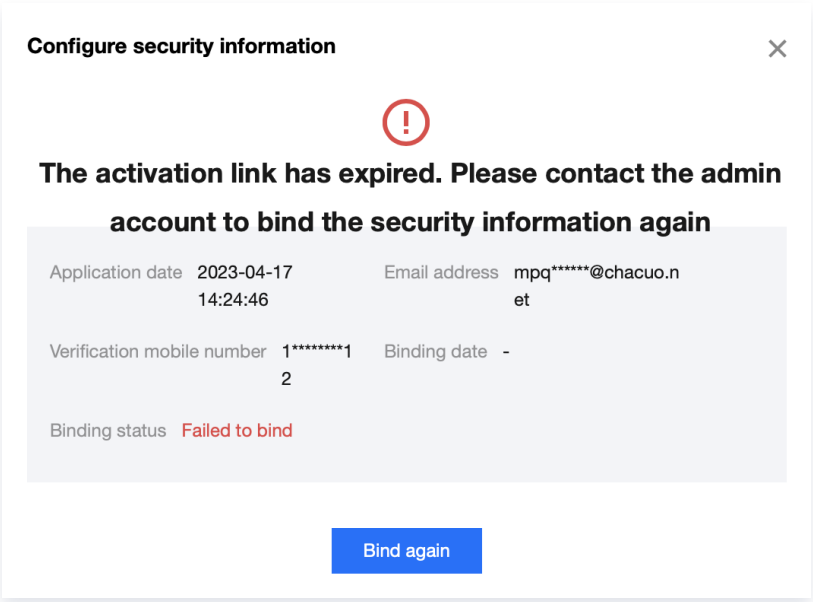
在激活链接的15天有效期内，您可通过控制台重新发送激活链接。

1. 在“成员账号管理”页面中，单击成员所在行右侧的 **绑定安全信息(激活)**。
2. 在弹出的“配置安全信息”窗口中，单击**重新发送**即可。

重新绑定信息

若您未在规定期限内单击激活链接，则绑定信息将激活失败。请通过控制台重新提交绑定信息，且需使用其他邮箱，激活失败的邮箱将不能再次绑定。

1. 在“成员账号管理”页面中，单击成员所在行右侧的 **绑定安全信息(失败)**。
2. 在弹出的“配置安全信息”窗口中，单击**重新绑定**。如下图所示：



3. 在弹出的“配置安全信息”窗口中填写邮箱及手机号后，单击**提交**。

后续操作

绑定信息激活成功后，您可进行以下操作：

- 使用该成员账号直接登录控制台。
- 根据实际情况移除账号，详情请参见 移除组织成员 。
- 在**成员账号管理**单击**成员名称**，可查看您为该成员绑定的登录邮箱。

删除在集团账号中创建的成员

最近更新时间：2024-12-09 15:16:11

您只能使用**管理账号下具有管理员权限的子用户**删除在集团账号中创建的成员。成员删除后，其下的所有资源及数据都会被删除，您无法再次登录和使用它。

> **警告：**
> 在集团账号中创建的成员账号一旦删除，即为在腾讯云中将该账号进行注销，不可找回，请您谨慎操作。

一、删除条件检查项

集团账号检查项

删除成员前，系统会自动检查集团账号的以下条件是否满足要求：

1. 成员删除许可检查

只有开启了成员删除许可，才能删除成员。具体操作，请参见 开启成员删除许可 。

2. 删除操作者检查

根据安全最佳实践，您只能使用管理账号下具有管理员权限的子用户删除成员，不能使用管理账号根用户删除成员。具体操作，请参见 新建子用户 。

3. 删除对象（成员）检查

- **不允许删除委派管理员账号。**
  您需要先解除委派管理员账号的身份，再删除成员。具体操作，请参见 移除委派管理员账号 。
- **不允许删除主体管理员账号。**
  您需要先解除主体管理员账号的身份，再删除成员。
- **不允许删除存在操作审批的账号**
  您需要先在成员列表中将操作审核与对应成员解绑，再删除成员。
- **不允许删除共享资源管理员账号**
  您需要先让该成员在资源共享中将共享给其他账号的资源删除，再删除成员。
- **不允许删除不满足代付准出条件的账号**
  代付准出的具体条件请参见 代付准入及准出条件
- **仅允许删除在集团账号中创建的成员。**
  对于通过邀请方式加入集团账号的腾讯云账号，您只能将其从集团账号中移除，但不能在集团账号中删除。如需删除，该类账号请遵照腾讯云账号注销流程进行删除。具体操作，请参见 账号注销 。

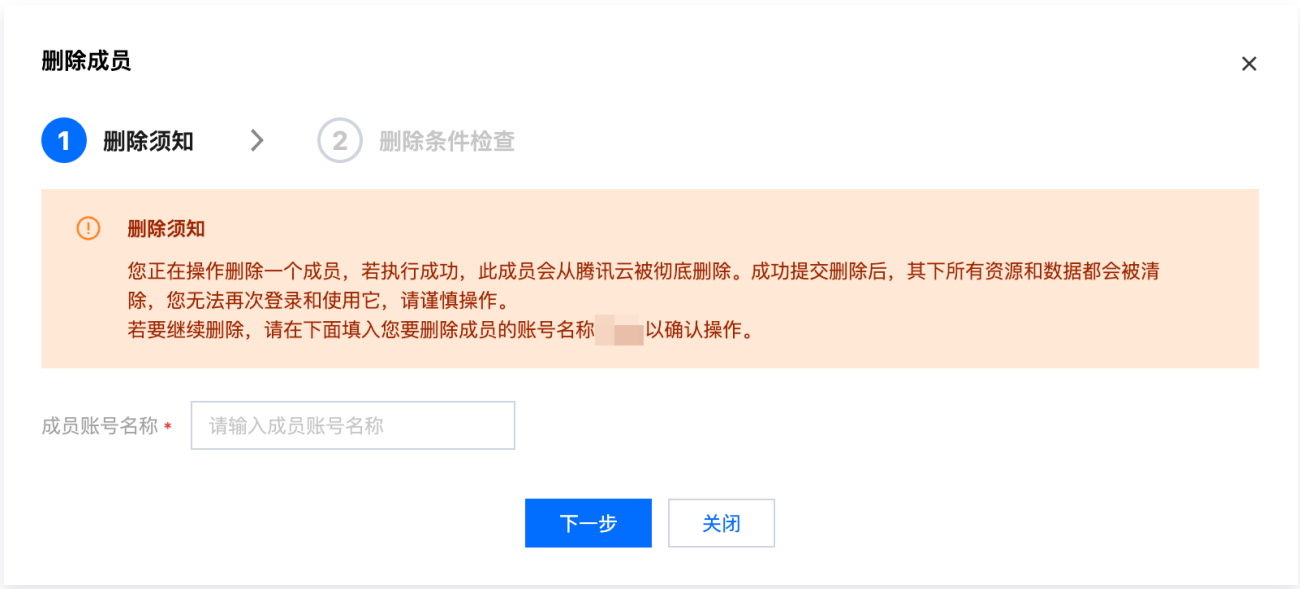
账号注销审核

删除成员前，系统会检查成员是否满足账号注销要求。对于不满足注销条件的成员，请参照页面提示和《账号注销》处理后，再重新删除成员。

二、操作步骤

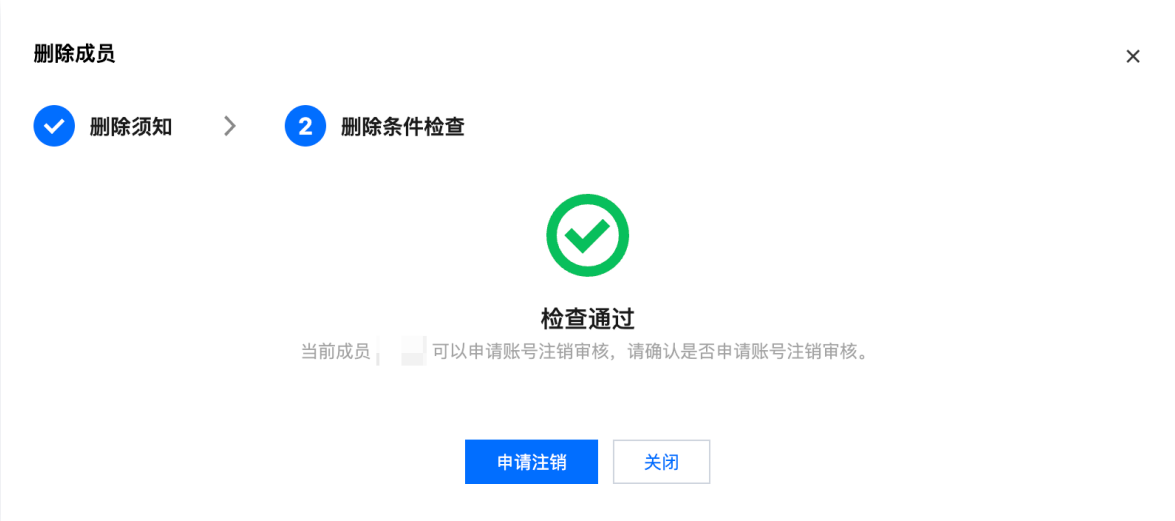
1. 登录 集团账号控制台 。
2. 在左侧导航栏，选择 成员账号管理 。
3. 在**成员账号管理**页面中，找到对应的成员，单击操作列的**删除**。

4. 在**删除成员**页面中，仔细阅读删除须知，并输入成员的账号名称，单击**下一步**。

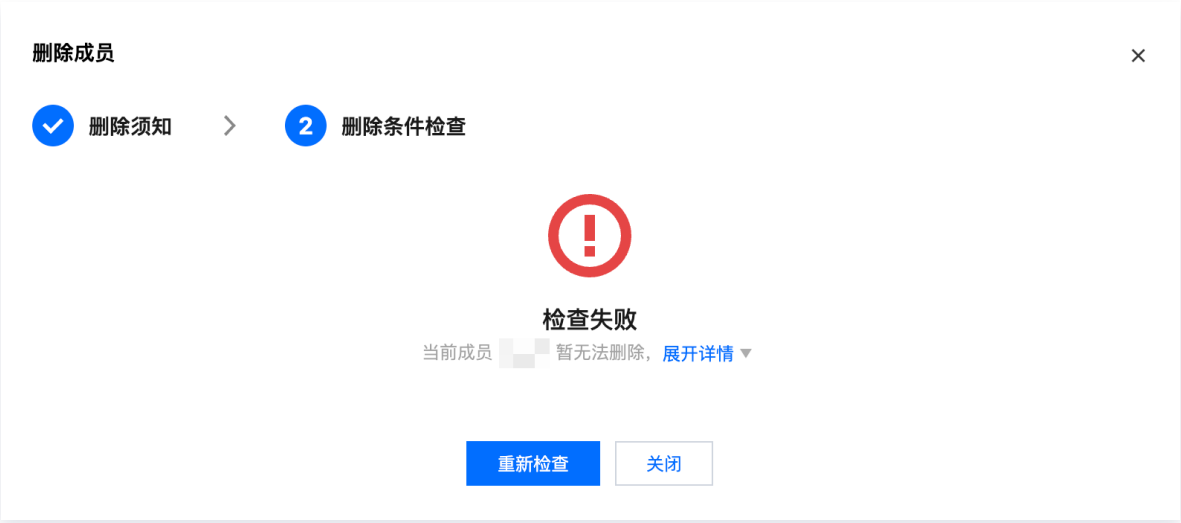


5. 等待集团账号删除条件检查结果出来后，依据检查结果，进行后续操作。
   - **检查通过：**

     单击**申请注销**，则进入账号注销审核；单击**关闭**，则终止删除成员的操作。



- **检查失败：**



  - 您可单击**展开详情**，查看具体的检查结果，并根据页面提示，手动处理不符合项。处理完成后再重新删除成员。

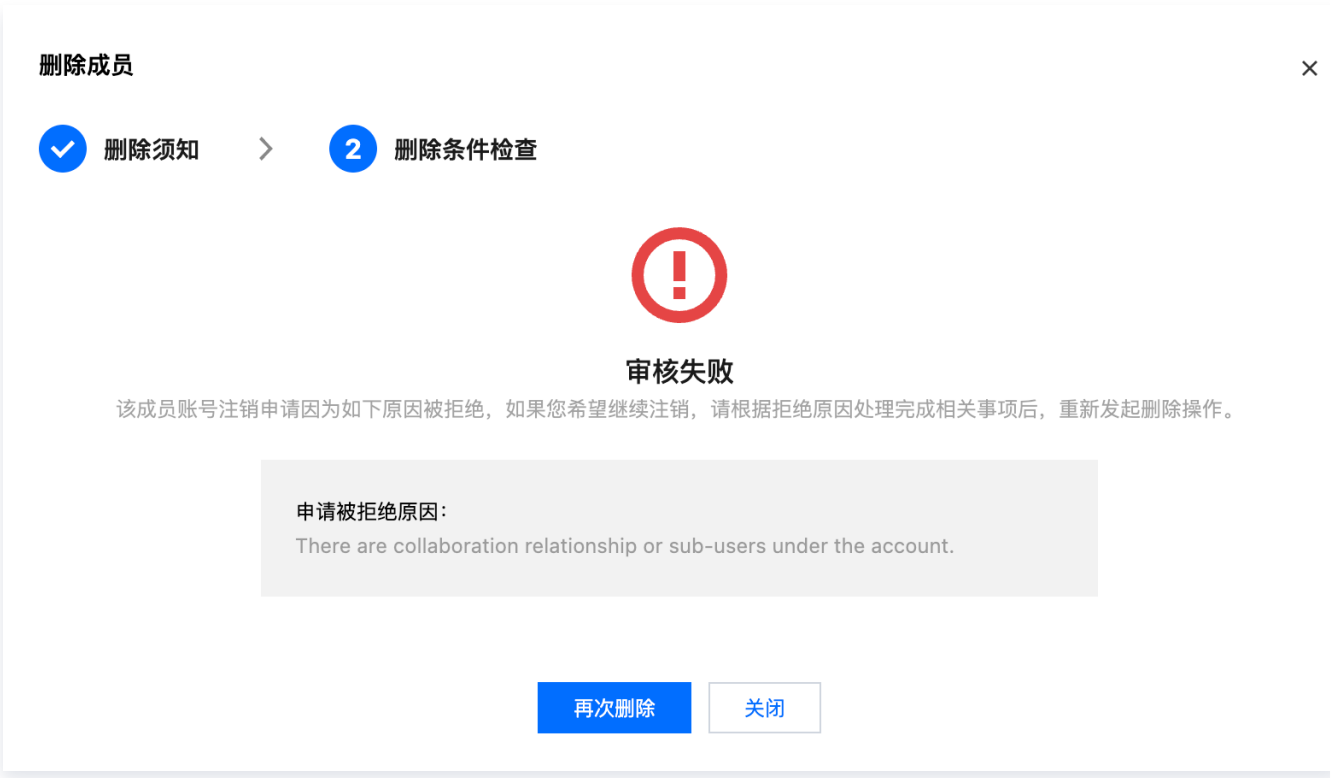
- 您也可以单击**重新检查**再次进行条件检查，检查通过后再进行删除成员。

6. 集团账号删除条件检查通过后，单击**申请注销**，进入账号注销审核。我们将在3个工作日内完成审核，期间成员删除状态为“审核中”。
   - 审核中

- 审核成功

  审核成功后该成员账号将会被直接删除且移除组织。
- 审核失败

  若不符合账号注销条件，将显示审核失败并告知您原因，待您处理完成后可以再次发起删除操作。



开启成员删除许可

最近更新时间：2024-12-09 15:16:11

当您开启成员删除许可后，才能删除资源账号类型的成员。您也可以随时关闭成员删除许可，禁止删除资源账号类型的成员。

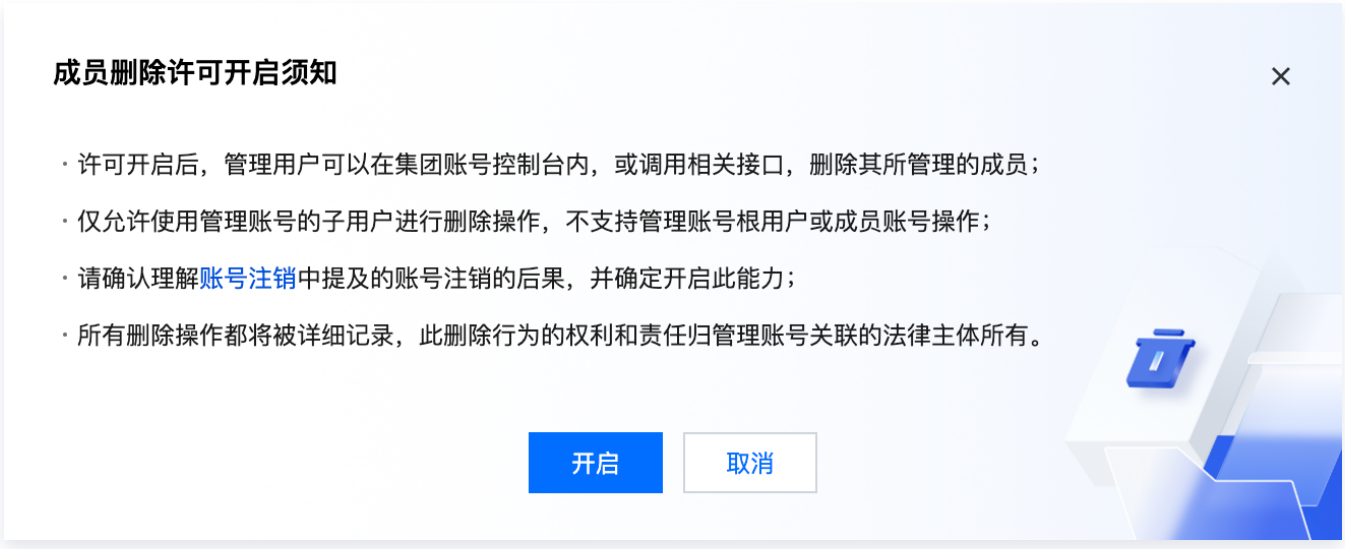
操作场景

您只能使用管理账号根用户或管理账号下具有管理员权限的子用户开启或关闭成员删除许可。

操作步骤

开启成员删除许可

1. 登录 集团账号控制台 。
2. 在左侧导航栏，选择 基本信息 。
3. 在**成员删除许可**区域，单击**开启成员删除许可**，并在弹出的窗口中仔细阅读提示信息，确认后单击**开启**即可。



关闭成员删除许可

1. 登录 集团账号控制台 。
2. 在左侧导航栏，选择 基本信息 。

3. 在**成员删除许可**区域，单击**关闭成员删除许可**，在弹出的窗口中单击**确定**即可。

成员财务管理
集团财务概览

最近更新时间：2025-08-06 15:06:23

集团财务概览支持管理账号按照成员、产品等维度查看和管理企业消费管理账号。企业管理账号可以统一查看和管理企业内所有账号的消耗，提升企业财务的管理效率。

说明：

1. 集团财务概览暂时仅支持经销商子客使用，且仅支持展示代付费的费用趋势以及账单详情。
2. 集团财务概览每天上午定时同步当月账单数据，若成员在当月1号之后加入，则无法看到该成员当月的财务数据（管理账号除外）。
3. 集团账单概览无法看到集团组织创建前的费用趋势以及账单详情。
4. 集团账号仅支持管理账号查看组织内的财务概览情况，若需要查看完整的账单详情请前往 费用中心 。

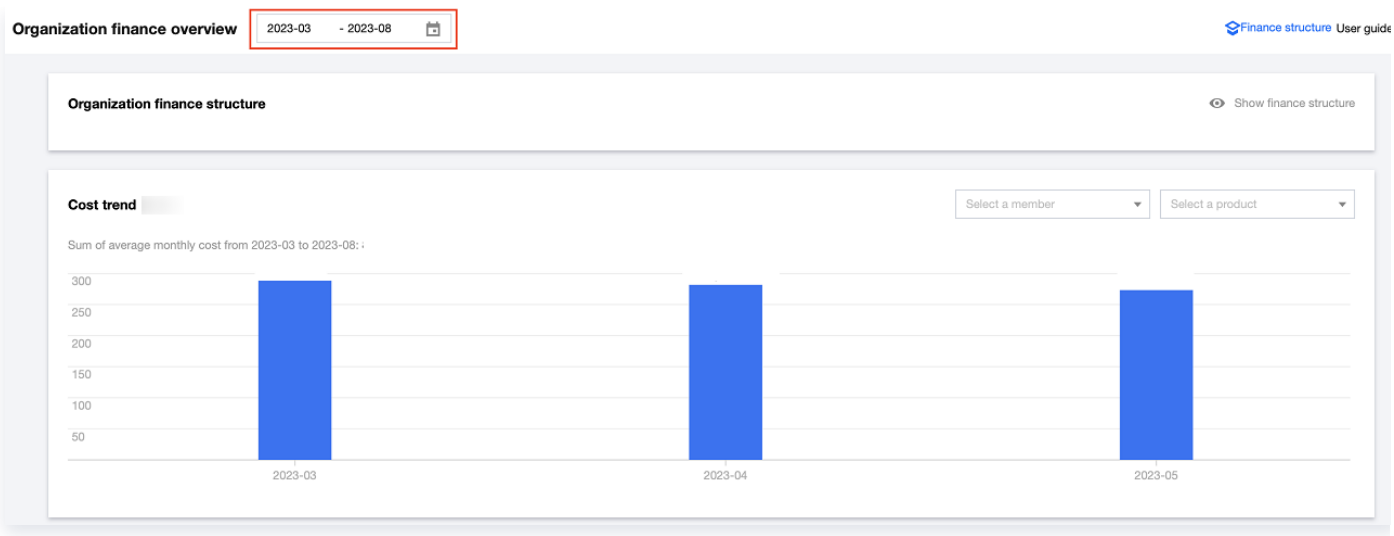
操作步骤

查看费用趋势及账单详情

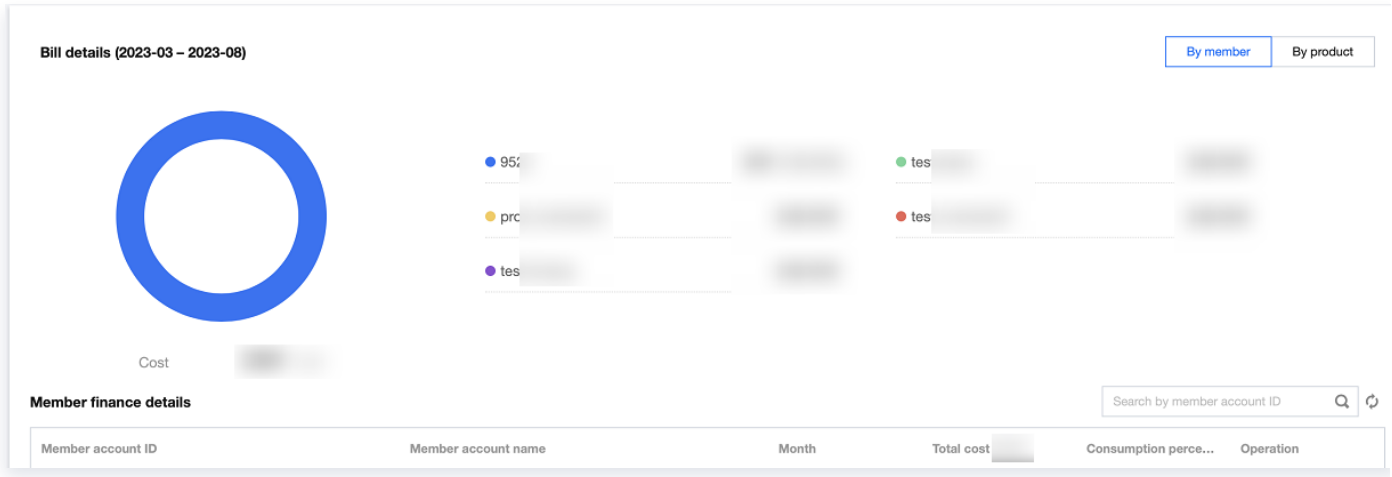
1. 登录 集团账号管理控制台，选择左侧导航中的**集团财务概览**。
2. 在**集团财务概览**页面最上方选择相应的时间，在**费用趋势**模块选择成员以及产品，则会对应显示出费用趋势和账单详情。

注意：

- 进入**集团财务概览**页后，默认展示全部成员和产品近半年的财务概览详情。
- 最多支持选择时间间隔范围为6个月的费用信息，若超过则不支持展示。



3. 在**费用趋势**模块可以查看所选成员在所选时间内，对所选产品的费用趋势图以及每个月具体的消费金额和月均总费用。
4. 在**账单详情**模块可以查看所选成员在所选时间内，对所选产品的费用详情。在右上角可以按需选择**按成员**或者**按产品**展示。



（1）**若选择“按成员”：**

- 在上方展示消费总金额 top5 的成员账号的饼状图，右侧展示具体的成员账号名称和对应的金额以及所占比例。
- 在下方展示所选成员的财务列表，包含成员账号 ID、成员账号名称、时间、总费用、消费占比、详情。单击消费详情则会显示某成员在所选时间内的产品消耗分布图。

（2）**若选择“按产品”：**

- 在上方展示消耗总金额 top5 的产品的饼状图，右侧展示具体的产品名称和对应的金额以及所占比例。
- 在下方展示所选产品的财务列表，包含产品名称、时间、总费用、消费占比、详情。单击详情则会显

示某产品在所选时间内的成员消费分布图。

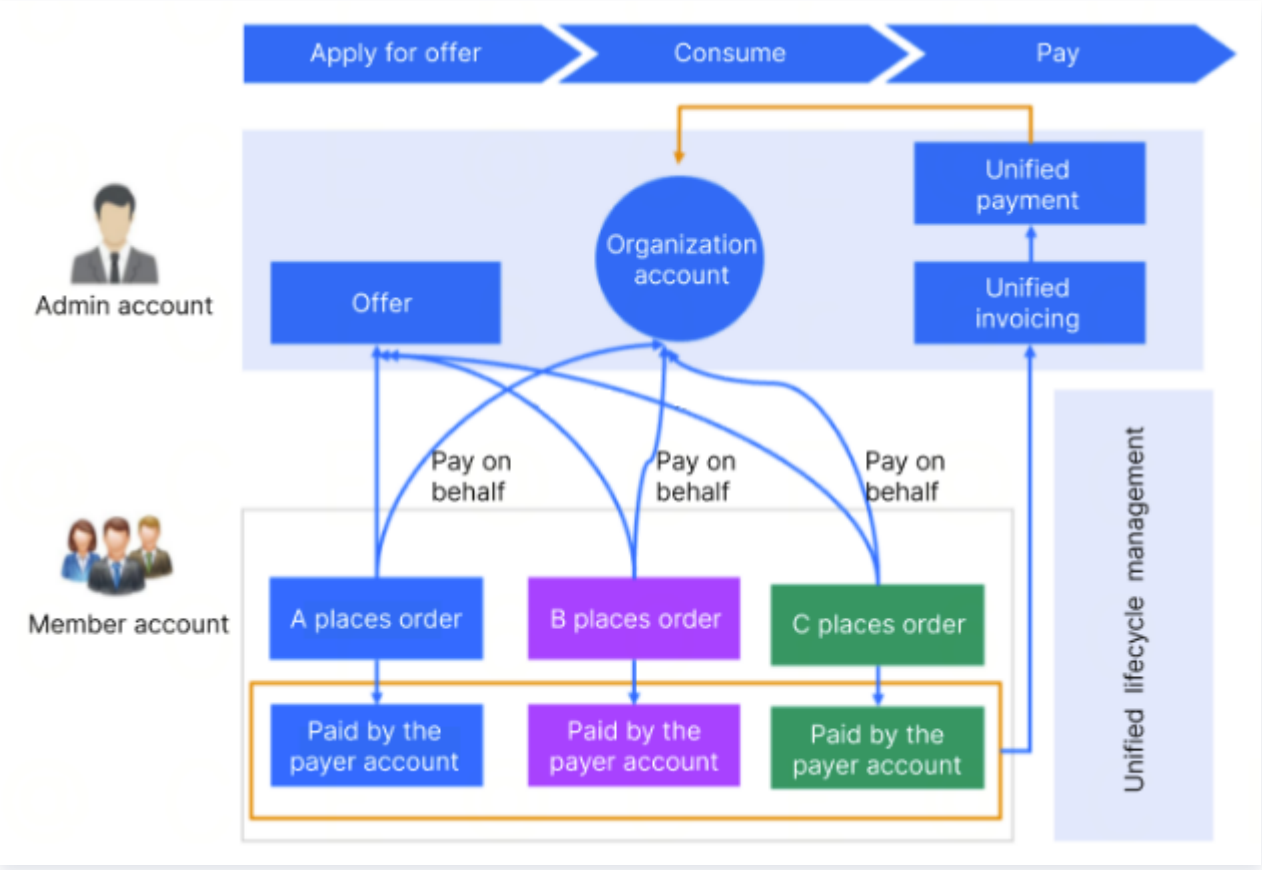
财务管理模式

最近更新时间：2024-03-06 18:45:06

集团账号管理结合集团用户的财务管理方式，提供**集团统一支付模式**和**成员自付模式**，用户可以结合自身的财务现状进行对应的选择。

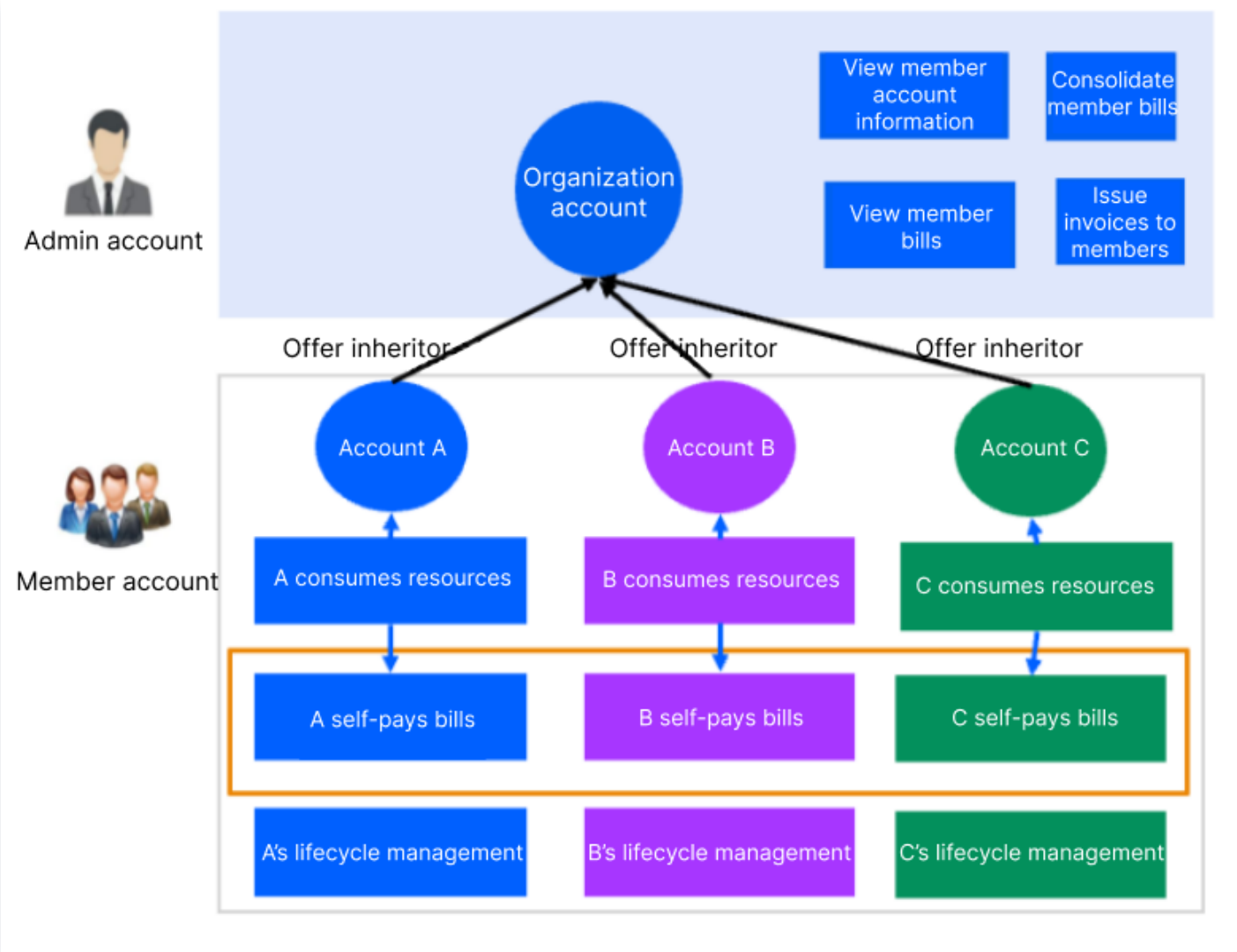
集团统一支付模式

由集团账号统一回款到集团账户，每个成员账号的消费自动从集团进行代付，不需要资金划拨。该模式下，针对同一个主体的用户，可以设置管理员为代付账号，自动代付名下成员的消费。如下图所示：



成员自付模式

该模式下，集团管理账号可查看名下成员账号的账户信息、账单信息、为成员开票、合并出账。同实名认证主体的成员账号可以快速继承管理账号的合同价优惠。成员账号自己的消耗由自己支付。如下图所示：



集团统一支付模式（代付费）
代付准入及准出条件

最近更新时间：2024-03-06 18:45:06

- 代付准入条件：成员账号加入组织，申请代付模式时，必须满足如下条件。

对象	条件
成员账号	账号方面的校验： 1. 成员账号必须和集团账号是同一个企业实名认证的主体，均为国际站。 2. 代理商或代客不可以选择财务代付模式。 3. 经销子客仅支持代付模式。 **经销模式下需额外校验：** 1. 校验管理员和成员需属于同一个经销商。 2. 校验子客账户是否存在子客代金券，若存在子客代金券，需要先将代金券消耗完毕或失效。
	账户方面的校验： 1. 外部账号或内部469账号：成员账号可用额度>=0。 2. 内部非469账号：不校验。
	订单方面的校验： 成员账号不可以有待支付、到期待续费、退款未完成的订单。 对应订单状态：待支付、处理中。
集团账号	目前只放开了集团账号成为代付账号； 代理商或代客不可以成为代付账号； 经销商或子客不可以成为代付账号； 1. 外部账号或内部469：代付账号**没有欠费或者可用额度 >= 0**。 2. **内部非469账号：不校验**。

- 代付准出条件：成员账号退出组织，取消代付模式时，必须满足如下条件。

对象	条件
成员账号	账户方面的校验： 1. 外部账号或内部469账号：成员账号可用额度 >= 0。 2. 内部非469账号：不校验。
	订单方面的校验： 成员账号不可以有待支付、到期待续费、退款未完成的订单。 对应订单状态：待支付、处理中。

	绑卡方面的校验： 没有商务跟进的中长尾成员账号，需要已绑卡信用卡。

支持能力及规则说明

最近更新时间：2024-11-05 17:46:38

集团统一支付模式是一种财务代付的模式，包含如下能力：

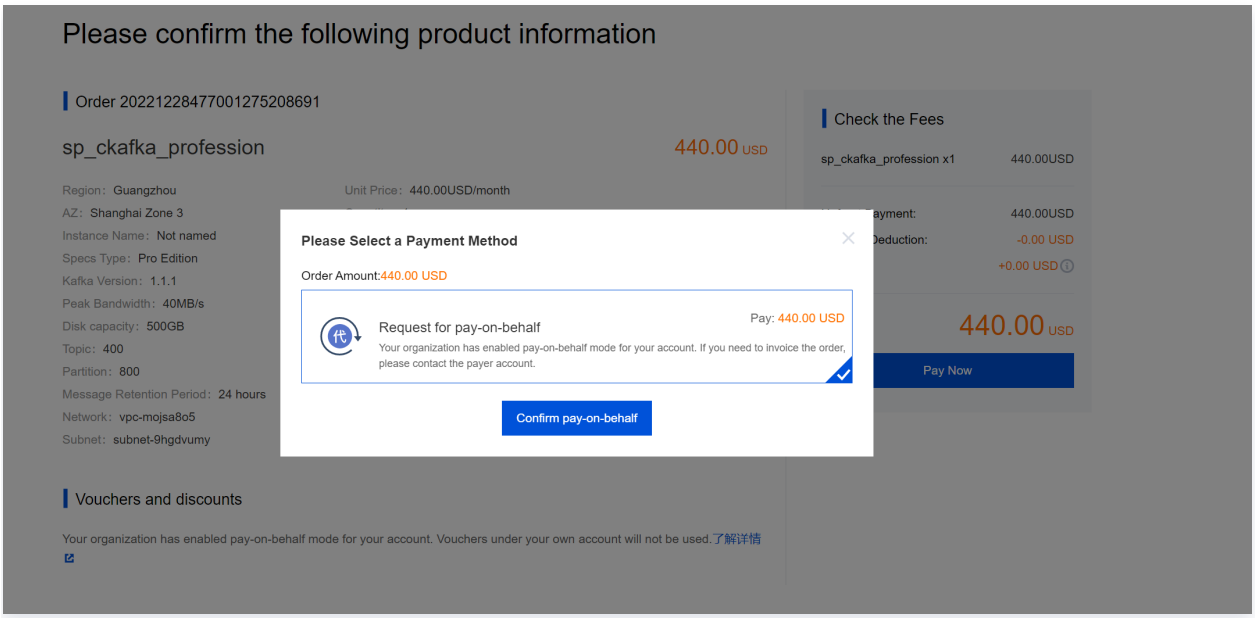
能力	说明
预后订单	成员账号包年包月的订单，按量付费的结算，自动由代付账号进行支付。
优惠	可选项。成员账号如果有“优惠继承”财务管理权限，则遵循优惠继承规则；如果没有“优惠继承”财务管理权限，则成员账号使用自己的优惠。
代金券	自动使用管理员账号的代金券。
账单	成员账号的账单自动结算至代付账号，由代付账号统一管理。
发票	成员账号的可开票金额自动结算至代付账号，由代付账号统一开具。
收支明细	成员账号的收支明细自动结算至代付账号，由代付账号统一查看。
生命周期	成员账号名下的资源欠费、停服、冲正统一参考代付账号的余额。
成本分析	成员账号的成本分析数据自动结算至代付账号，由代付账号统一管理。
预算管理	成员账号的预算管理自动结算至代付账号，由代付账号统一管理。

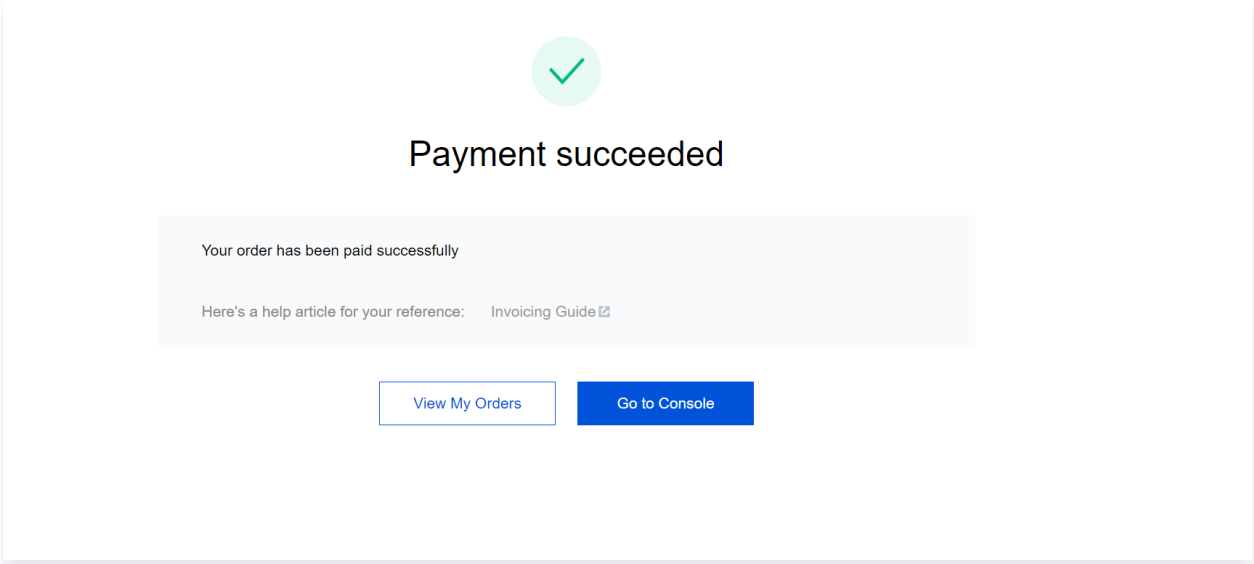
相关规则及说明如下：

预后订单

预付费新购/升配

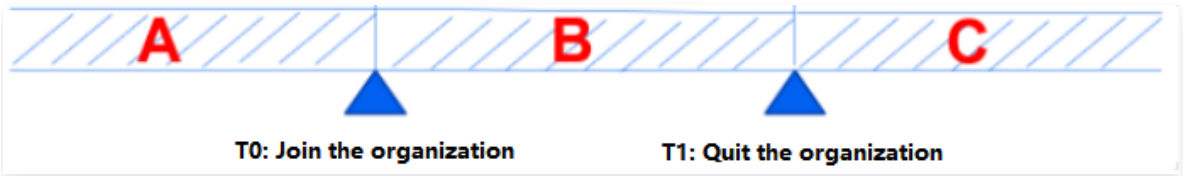
成员账号进行预付费新购/升配时，只能选择申请代付者账号支付，不需要余额支付或在线支付。选择申请代付者账号支付后，不需要代付账号人工操作，系统会参考代付账号的余额、信用额度情况，进行自动代付并展示代付结果。成员账号提交订单后，选择申请代付者账号支付后单击确认申请代付即可。如下图所示：





预付费降配/退订

成员账号进行预付费降配或退订时，按订单的支付者账户 UIN 和比例退回支付者账户。
您可参考以下示例场景了解规则：
成员账号情况如下图所示：

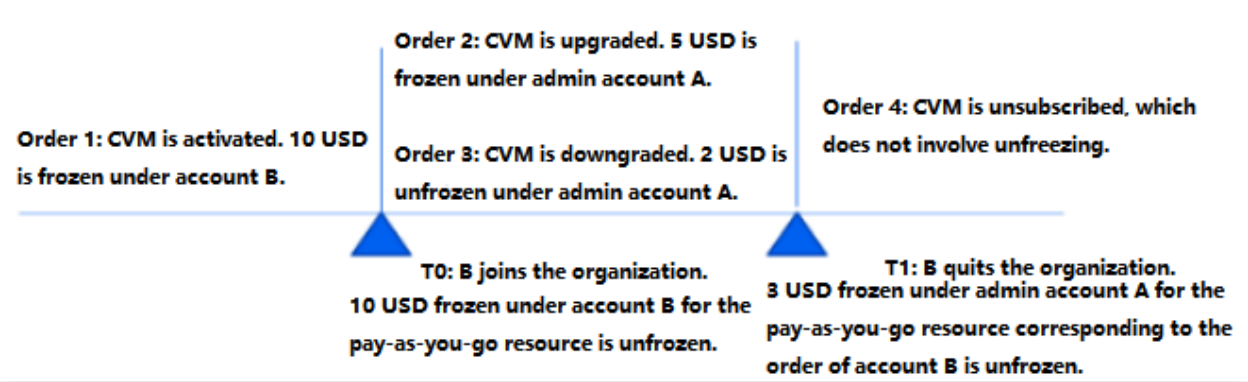


订单	是否有代付	退款到的账户
在A区域下单，在B区域退订	没有	按 payer uin 原路退回 成员账号的账户

	有 （可能在B区域升配）	按 payer uin 原路退回成员、集团的账户
在B区域下单	有	按 payer uin 原路退回 管理账号的账户
在A区域下单，在C区域退订	没有	按 payer uin 原路退回 成员账号的账户
	有（可能在B区域升配）	按 payer uin 原路退回成员、集团的账户

后付费开通冻结

加入组织时，解冻成员账号的后付费冻结金额。
退出组织时，解冻成员账号的订单，对应管理员账号的后付费冻结金额。
示例说明如下图所示：

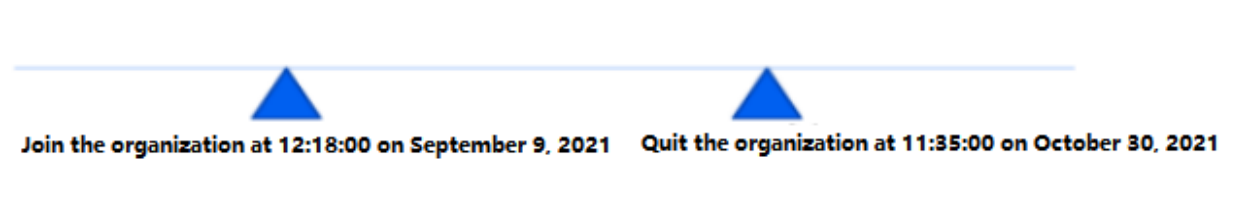


后付费结算

当前周期或下一个周期费用，从代付账号扣除。
最后周期费用，从成员账号扣除。

> **注意：**
> 后付费推量延迟带来的延迟结算也参考该规则进行计算。

代金券：可以使用代付账号的代金券。
资源包：新购、升降配、退订和包年包月产品规则保持一致。后付费结算时不支持代付，统一使用归属自己的资源包进行抵扣。
示例说明如下图所示：



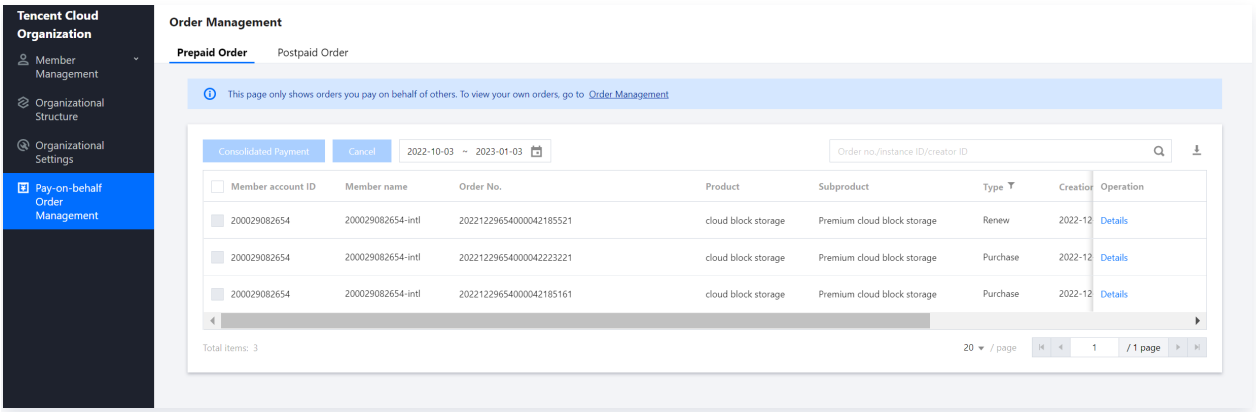
结算周期	样例	结算规则	资源包抵扣
按小时结算	2021-09-09 12：00：00-13：00：00	扣除代付账号的账户、代金券	不代付，扣除归属自己的资源包
	2021-10-30 11：00：00-12：00：00	扣除成员账号的账户、代金券、	不代付，扣除归属自己的资源包
按天结算	2021-09-09	扣除代付账号的账户、代金券	不代付，扣除归属自己的资源包
	2021-10-30	扣除成员账号的账户、代金券、	不代付，扣除归属自己的资源包
按月结算	2021-09	扣除代付账号的账户、代金券	不代付，扣除归属自己的资源包
	2021-10	扣除成员账号的账户、代金券	不代付，扣除归属自己的资源包

查看代付订单

当完成代付后，您可登录 集团账号管理控制台，选择左侧导航栏中的**代付订单管理**，根据实际角色类型，查看代付订单并进行相关操作。

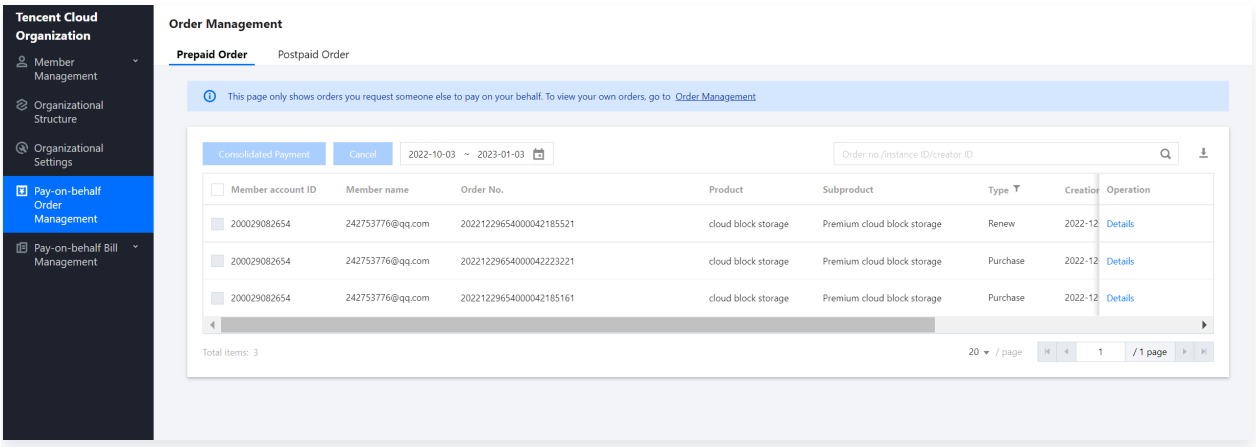
管理员账号

管理账号可以查看成员账号的代付订单，针对待支付订单可以**代付**或**取消**。如下图所示：



成员账号

成员账号可查看“被代付”的所有订单，还可在页面中进行**申请代付**操作。如下图所示：



优惠

集团账号财务代付模式下，管理员可选择代付成员是否开通优惠继承权限。成员账号如果有“优惠继承”财务管理权限，则遵循优惠继承规则；如果没有“优惠继承”财务管理权限，则成员账号使用自己的优惠。

注意：

- 优惠继承有黑名单，在黑名单的产品不参与优惠继承，维持使用成员账号自身的优惠。优惠继承的产品黑名单可以进一步咨询您的商务或提交工单咨询。
- 满返不参与优惠继承；如果代付账号有满返，成员账号不参与享受此优惠。
- 管理账号可为被代付成员设置是否开通优惠继承权限，若选择开通将校验账号现有优惠继承关系。例如成员账号A 选择B 作为代付者，如果B 已经继承了C的优惠，或者A继承了D的优惠，均无法新建继承关系。
  若需取消原优惠继承关系、新建成员与代付账号的优惠继承，需联系您的商务经理确认代付账号已正确申请合同价优惠 和 协助取消原继承关系，您也可 提交工单 咨询。

代金券

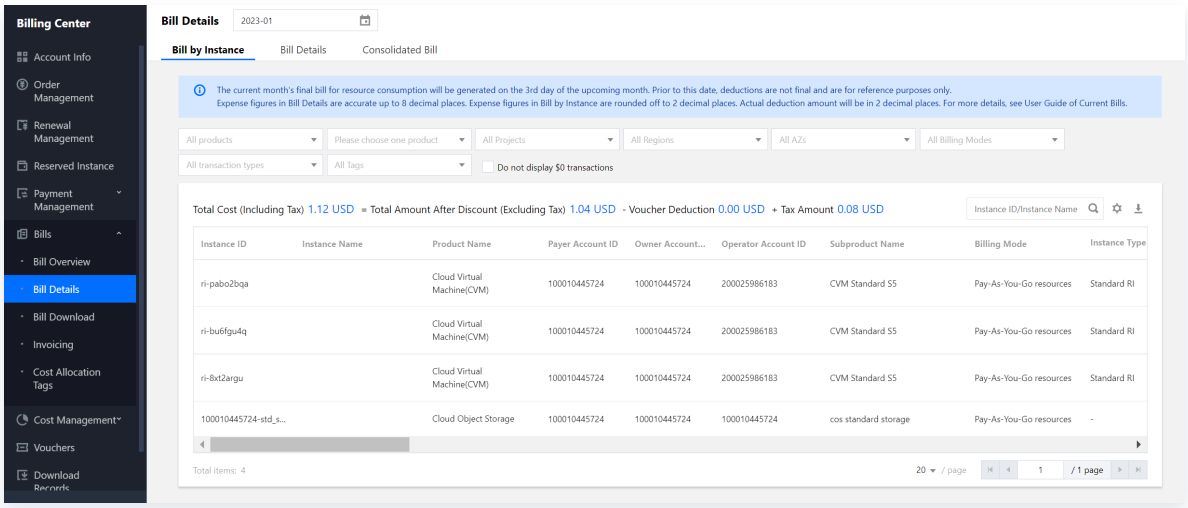
不可以使用成员账号的代金券，可以自动使用管理员的代金券。

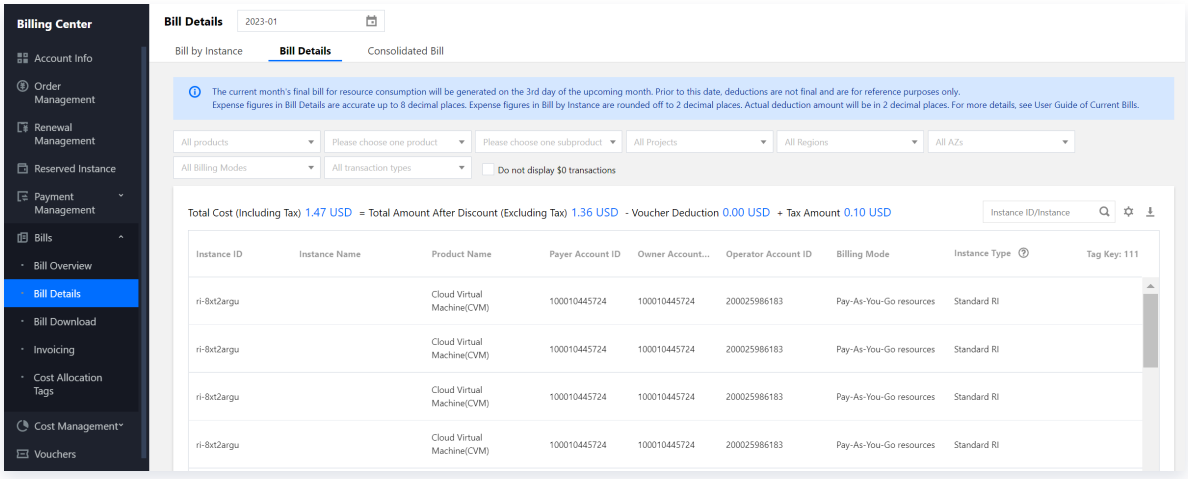
账单

成员账号的账单自动结算至代付账号，由代付账号统一管理。代付账号可以查看名下所有成员账号的账单。被代付的成员账号可查看自身相关的代付账单，不可查看其他成员账单。
集团账号管理 与 费用中心 均可查看账单。集团账号管理展示代付费相关账单，费用中心展示自付费相关账单，请注意区别。字段参考 账单字段说明 。
以下为管理员账号与成员账号视角供参考：

管理员账号查看代付账单

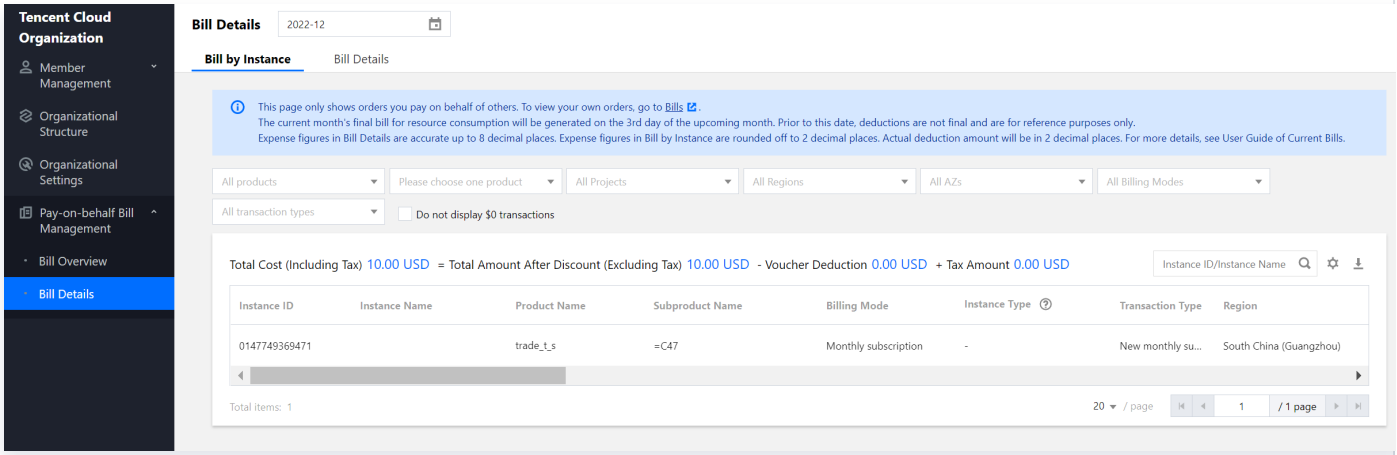
管理员账号登录控制台后，前往 费用中心–费用账单 查看。





成员账号查看代付账单

成员账单登录控制台后，前往 集团账号管理–代付账单管理 查看。



发票

代付账号和成员账号是同一个企业实名认证的用户，发票统一由代付账号进行开票。

收支明细

成员账号的收支明细自动结算至代付账号，由代付账号统一查看。

生命周期

代付账号有义务保障余额充足，保障成员账号的资源可以正常使用。对于需手动续费的资源，代付账号有义务保障及时续费。关于欠费消息、停服、销毁等事件，规则说明如下：

欠费消息事件

- 预付费消息（资源即将到期、已经到期、停服消息、销毁消息、冲正消息），将统一发送给代付账号。
- 后付费消息，暂时发送给成员账号。

执行事件

- 成员账号的停服、销毁事件处理，参考代付账号的余额。代付账号欠费时，会广播式对名下所有成员账号进行停服处理。
- 代付账号充值冲正后，会广播式对名下所有成员账号进行冲正处理。

临界处理

- 成员账号加入组织后，会触发参考代付账号的余额、信用账户或特权，判断冲正或停服处理。
- 成员账号退出组织后，会触发参考自身的余额、信用账户或特权，判断冲正或停服处理。

成本分析

成员账号的成本分析数据自动结算至代付账号，由代付账号统一管理。

预算管理

成员账号的预算管理自动结算至代付账号，由代付账号统一管理。

其他说明事项

如您和腾讯云有合同签署的私有云业务，付费规则以合同约束为准。

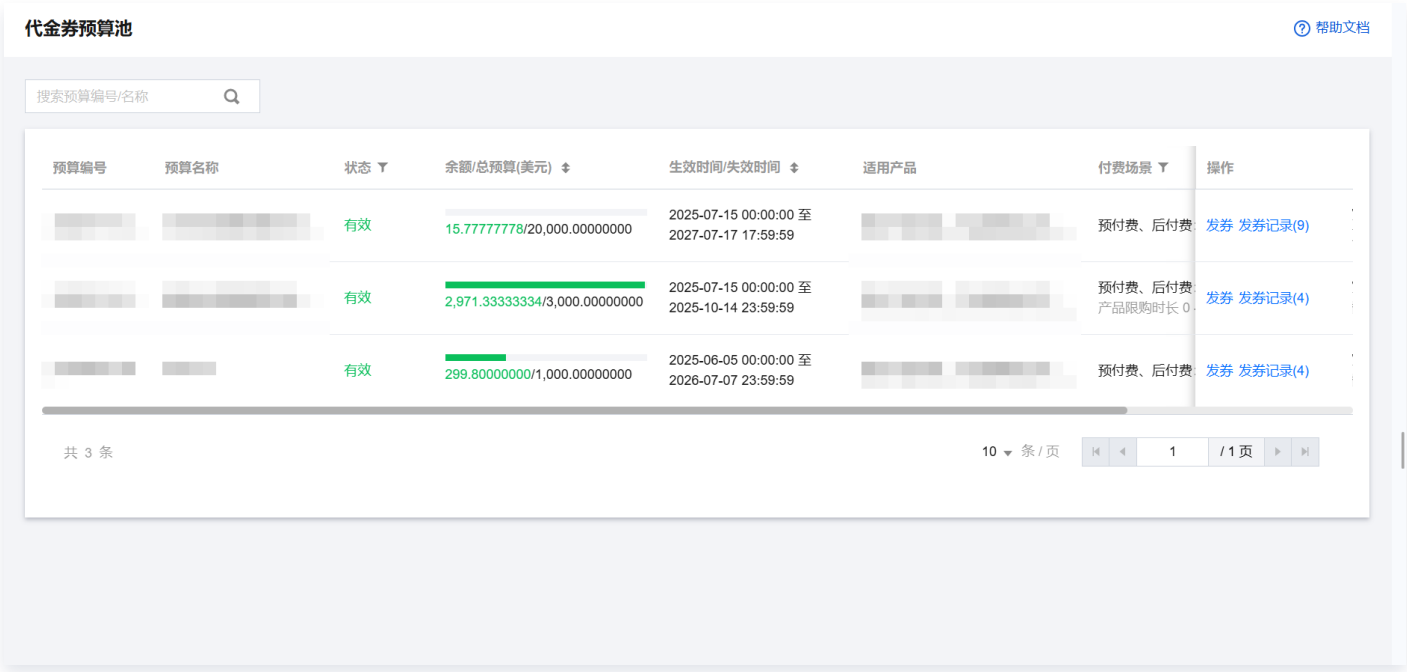
代金券预算池

最近更新时间：2025-09-03 15:42:42

代金券预算池 是经特殊申请，发放给集团管理账号的代金券预算。集团管理账号可以按预算池约定的代金券属性（适用产品、有效期、使用门槛等）给成员账号发放代金券。

说明：

- 代金券预算池无法直接抵扣费用，需发放为代金券才能抵扣费用。
- 通过预算池发放的代金券，与通过活动领取、商务发放等的使用规则一致，详情请参见 代金券 。



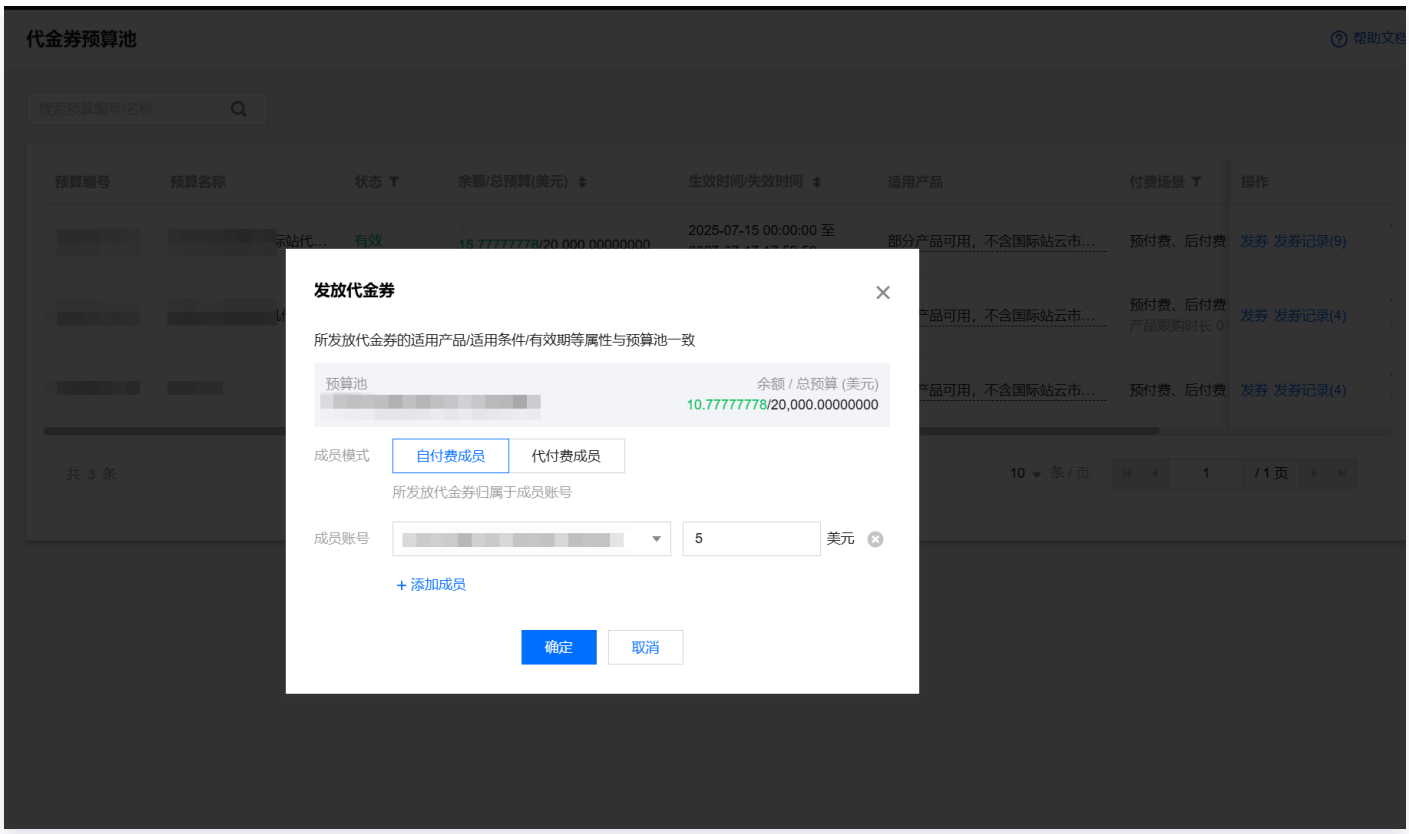
前提条件

成员账号需开通**发放代金券**权限。若成员账号没有该权限，请参见 成员权限配置 为成员账号开通发放代金券权限。

给成员账号发放代金券

代金券预算池有额度和有效期管控，预算池过期或额度用完后会失效，失效预算池不能再恢复，请合理安排尽快使用，避免过期。

给“自付费成员”发券

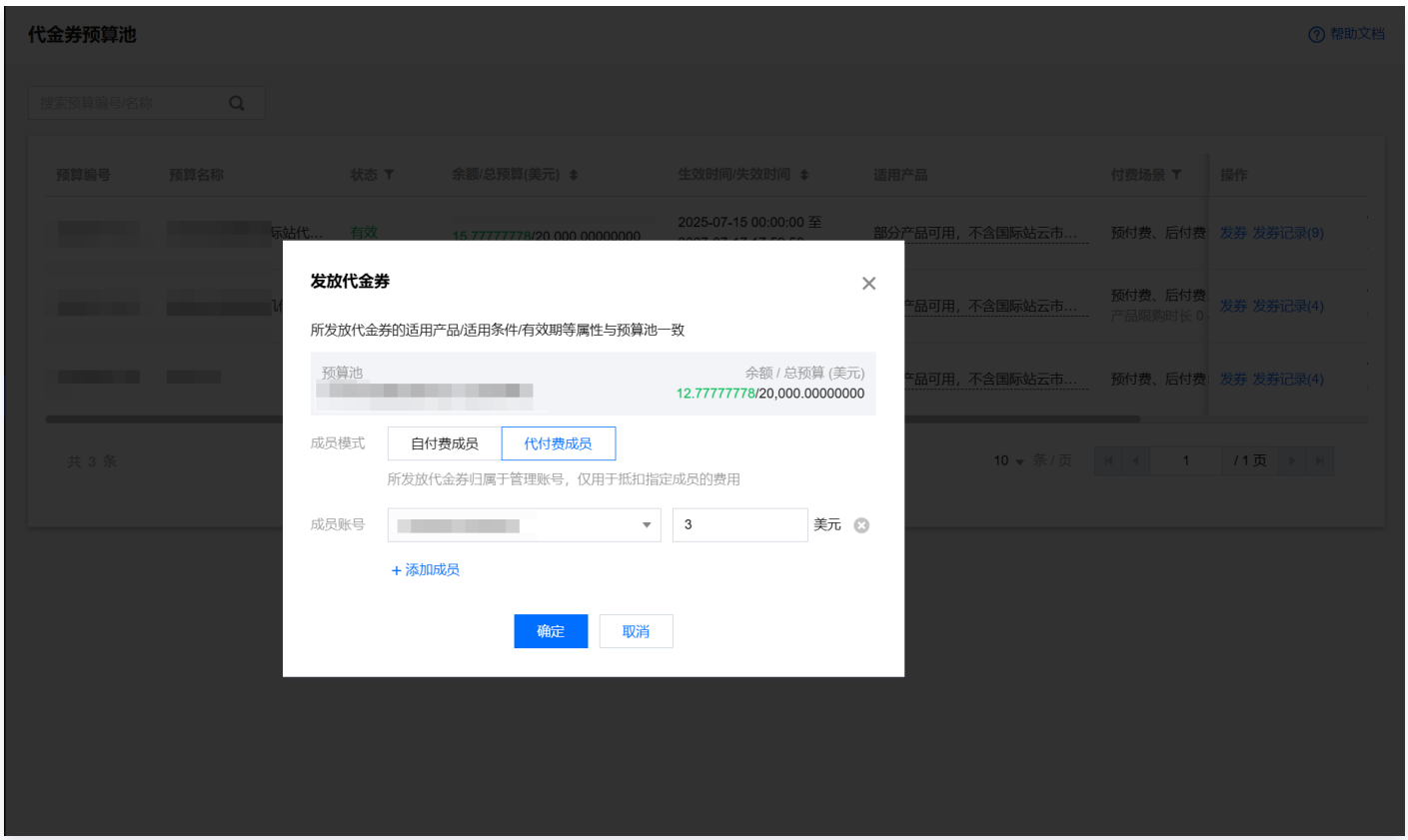


选择**预算池**，单击**发券**，在**发放代金券**页面中，选择**自付费成员**模式，下拉选择成员，输入代金券面额，单击**确定**即可。

- 自付费成员模式，代金券发放至成员账号中，成员能通过“代金券”列表查看。
- 每次最多可选10位成员发券。
- 发券金额不能超过单张券最大面额。

给“代付费成员”发券

> **注意：**
> 该操作与“自付费成员”模式的差异是代金券发放至集团管理账号中，同时指定需要代付的成员账号，这张券只能抵扣指定成员的费用，集团管理账号可通过“代金券”列表查看此券，成员账号无法查看此券。



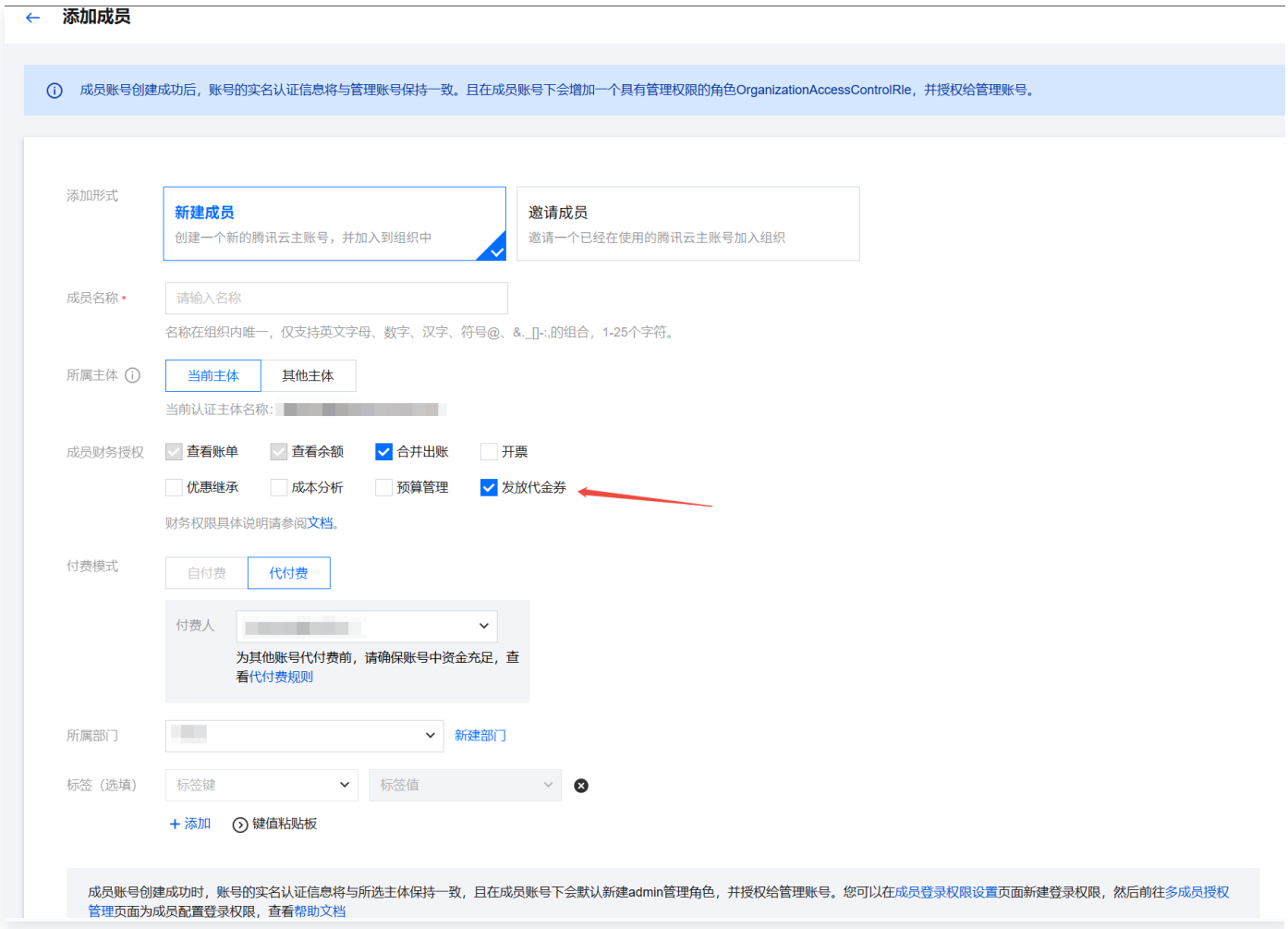
选择**预算池**，单击**发券**，在**发放代金券**页面中，选择**代付费成员**模式，下拉选择成员，输入代金券面额，单击**确定**即可。

- 代付费成员模式，代金券发放至管理账号中，管理账号通过“代金券”列表查看。
- 每次最多可选10位成员发券。
- 发券金额不能超过单张券最大面额。

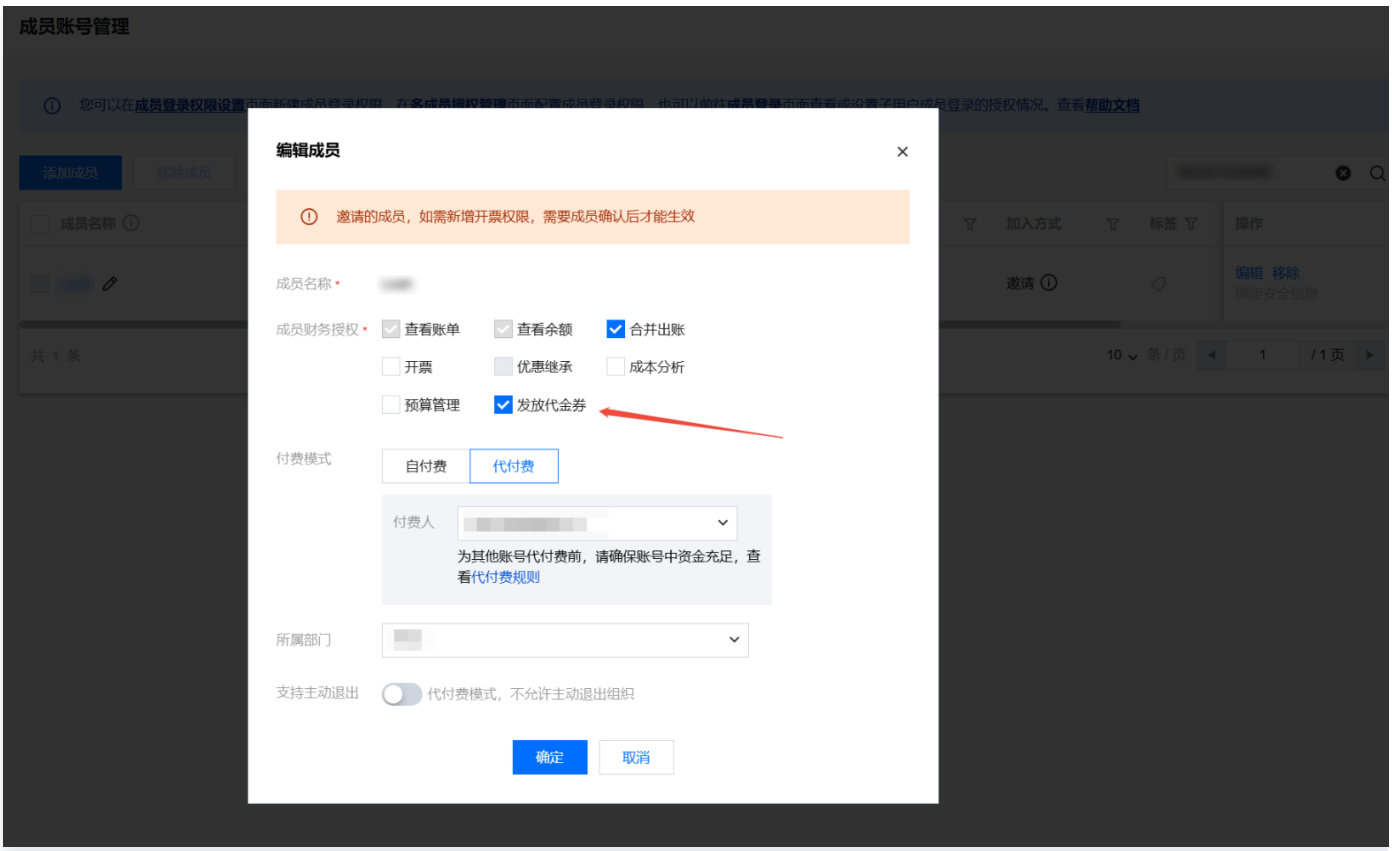
成员权限配置

给成员发放或回收代金券，需提前给成员开通**发放代金券**权限。开通方式有以下三种：

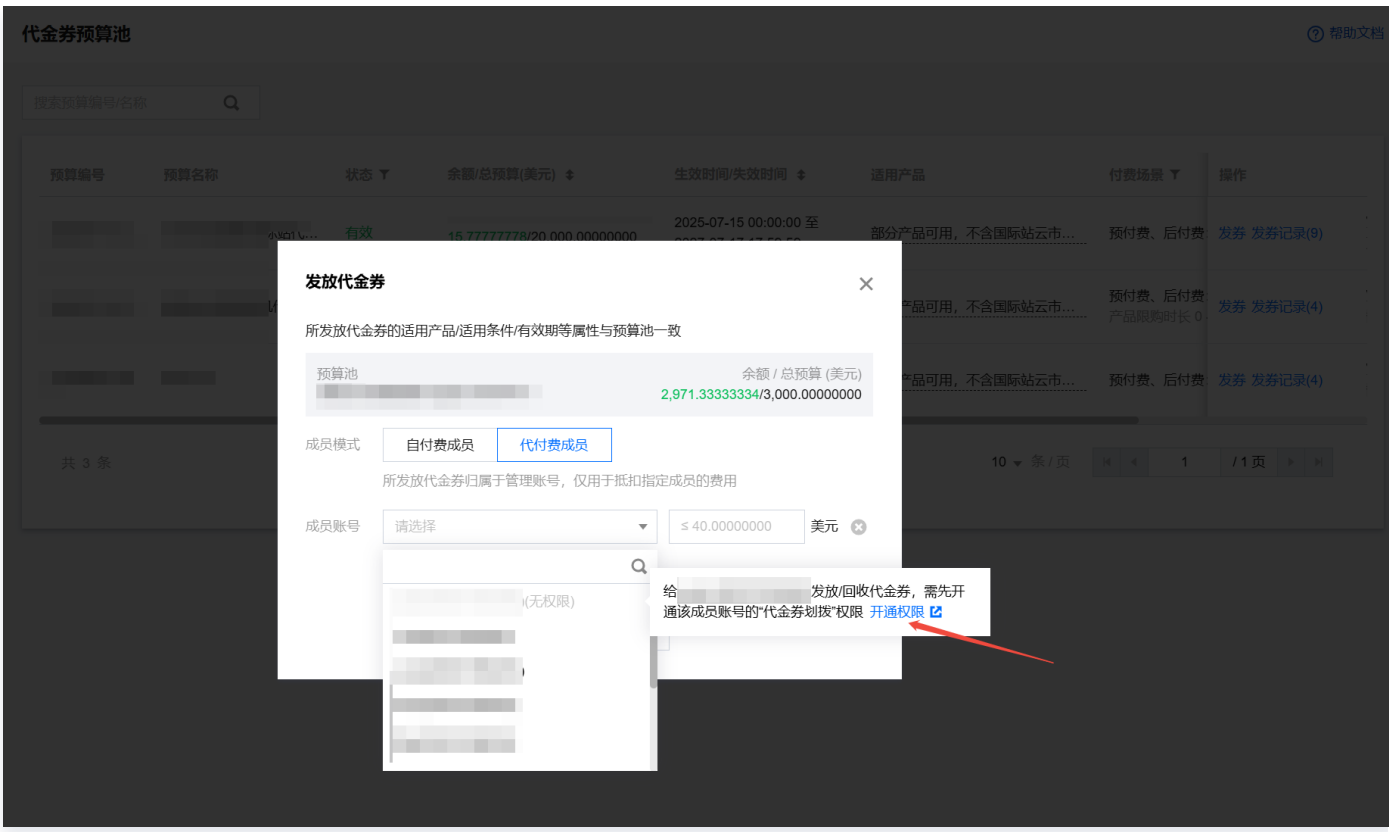
- 创建或邀请新成员时，为成员选择**发放代金券**权限。详情请参见 添加组织成员 。



- 在**集团账号管理控制台** > 成员账号管理 中，选择目标成员，单击**编辑**，在**编辑成员**页面，为成员选择**发放代金券**权限。



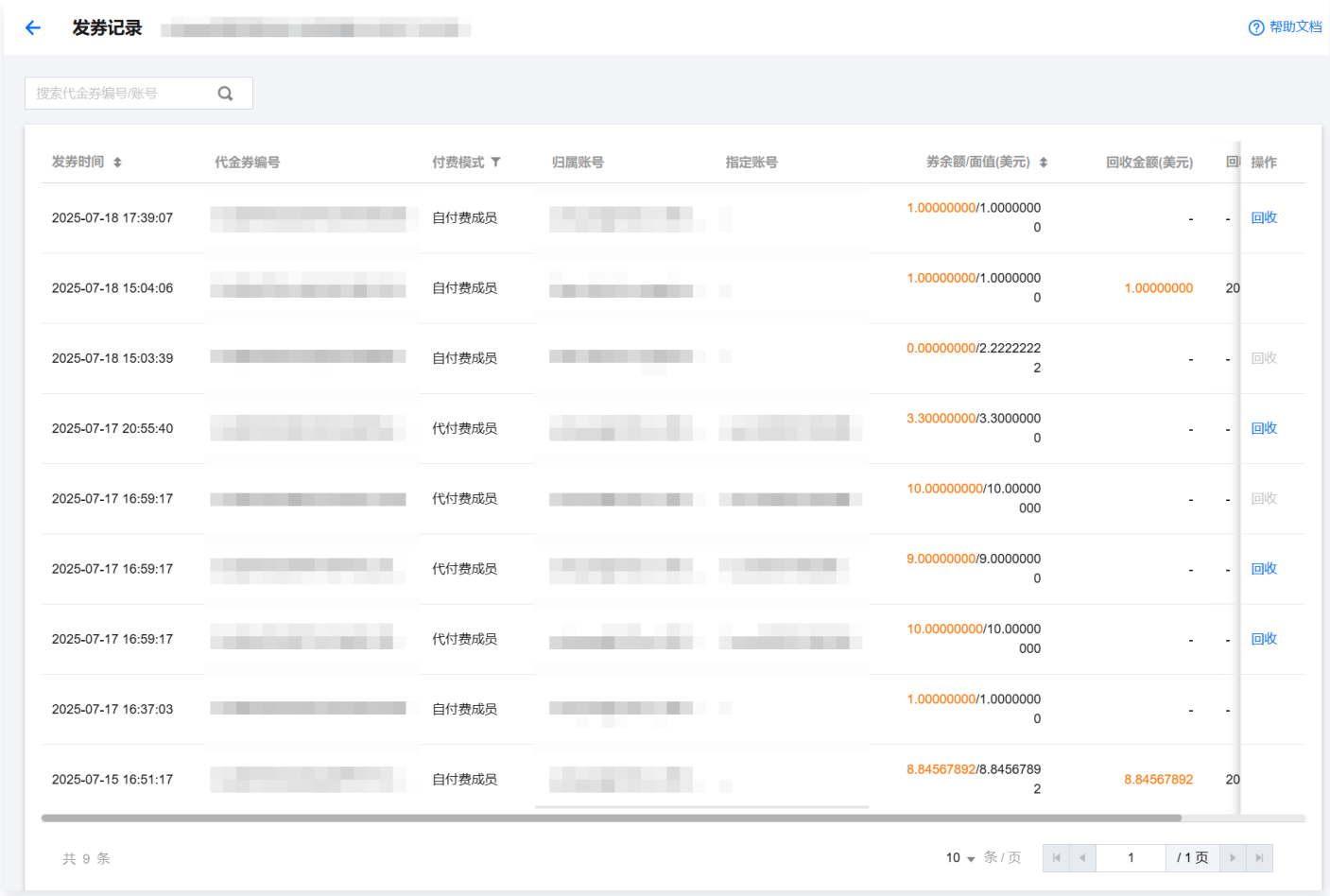
- 在**发放代金券**页面选择成员时，若提醒无权限，可单击**开通权限**，直接跳转到成员列表并为成员选择**发放代金券**权限。



其他相关操作

查询发券记录

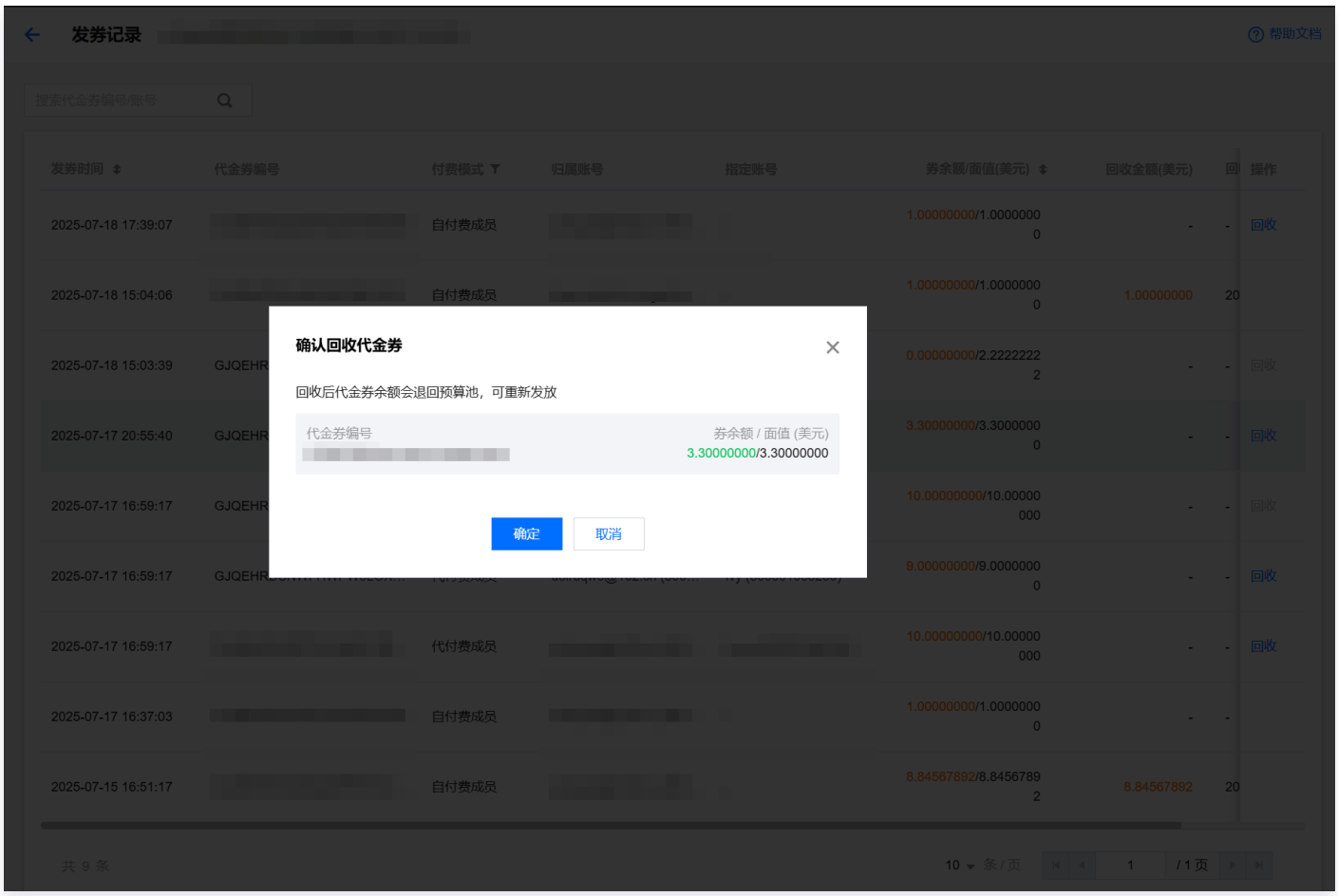
单击各预算池中的**发券记录**，可以查看预算池的发放和回收记录。



回收代金券

在**发券记录**中，单击**回收**，在弹出的窗口中，单击**确定**，则作废回收此代金券，代金券余额退回到预算池，可进行二次发放。以下情况不能回收：

- 代金券已使用，无剩余金额。
- 代金券已过期。
- 代金券已回收、已作废。


发券记录
帮助文档
搜索代金券编号/账号
发券时间
代金券编号
付费模式
归属账号
指定账号
券余额/面值(美元)
回收金额(美元)
操作
2025-07-18 17:39:07
自付费成员
1.00000000/1.00000000
回收
2025-07-18 15:04:06
自付费成员
1.00000000/1.00000000
1.00000000
2025-07-18 15:03:39
GJQEHR
0.00000000/2.22222222
回收
2025-07-17 20:55:40
GJQEHR
3.30000000/3.30000000
回收
2025-07-17 16:59:17
GJQEHR
10.00000000/10.00000000
回收
2025-07-17 16:59:17
GJQEHR
9.00000000/9.00000000
回收
2025-07-17 16:59:17
代付费成员
10.00000000/10.00000000
回收
2025-07-17 16:37:03
自付费成员
1.00000000/1.00000000
2025-07-15 16:51:17
自付费成员
8.84567892/8.84567892
8.84567892
共 9 条
10 条/页
1
/ 1 页
确认回收代金券
回收后代金券余额会退回预算池，可重新发放
代金券编号
券余额 / 面值 (美元)
3.30000000/3.30000000
确定
取消

成员自付费模式

最近更新时间：2025-01-02 18:00:28

成员自付模式包含如下功能：

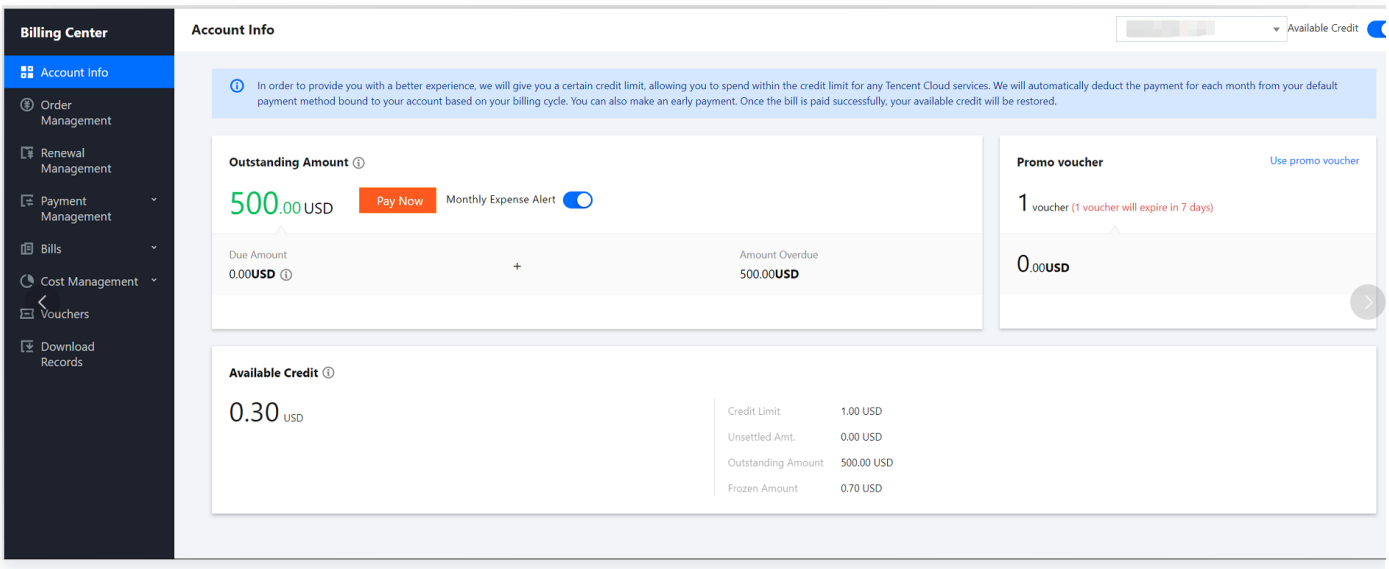
财务权限	说明
查看成员账户信息	管理账号查看成员账号的账户余额信息。
查看成员账单	管理账户查看成员账号的账单消耗信息。
为成员账号开票	管理账号给成员账号开具发票。
合并出账	管理账号将多个成员账号的费用合并下载。
优惠继承	成员账号继承管理账号的合同价优惠。
成本分析	管理账号可筛选、查看、分类、聚合和分析成员账号成本。
预算管理	管理账号支持为成员账号配置预算。

查看成员账户余额信息

介绍管理账号如何查看成员账号的账户余额信息。

操作步骤

1. 管理账号登录费用中心控制台，选择左侧导航栏中的 账户信息 。
2. 通过右上方的下拉列表，选择对应的成员账号，查看成员账号的账户余额信息。

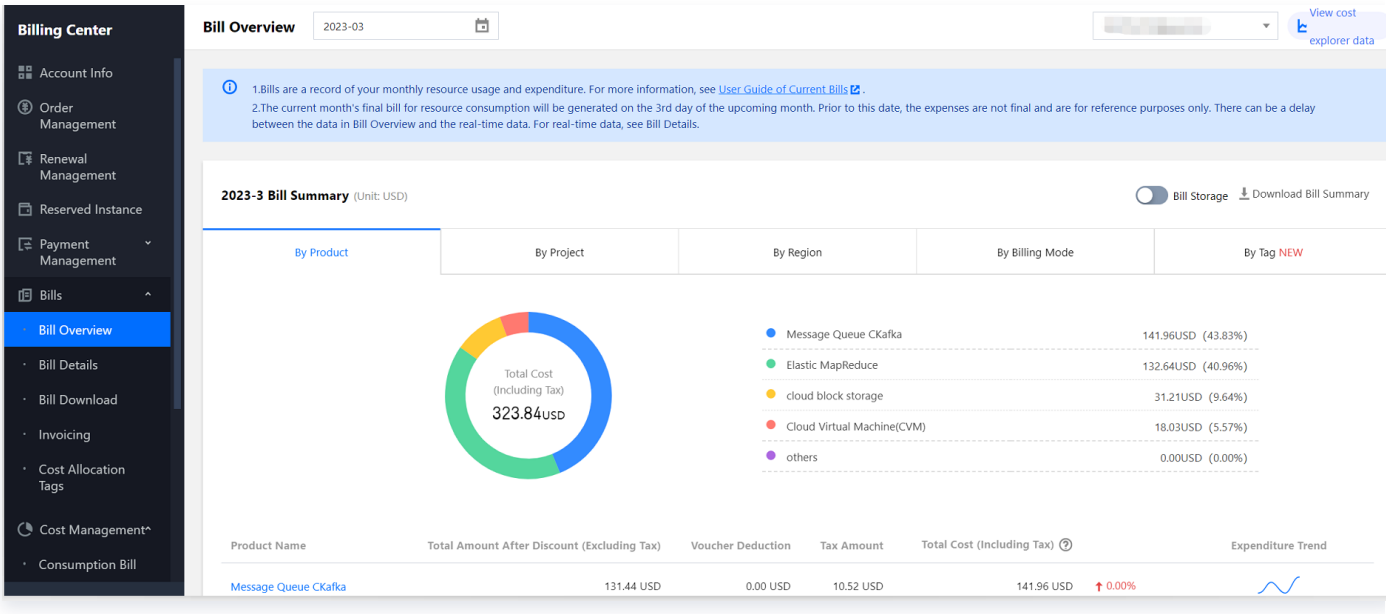


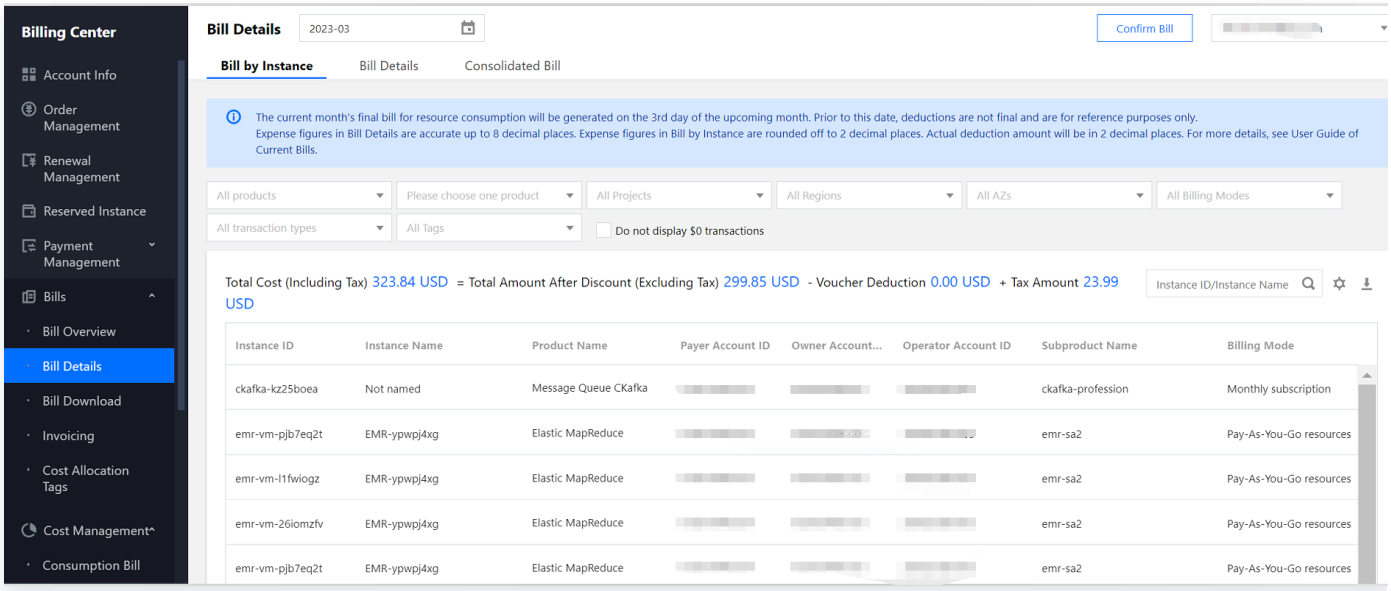
查看成员账号的账单

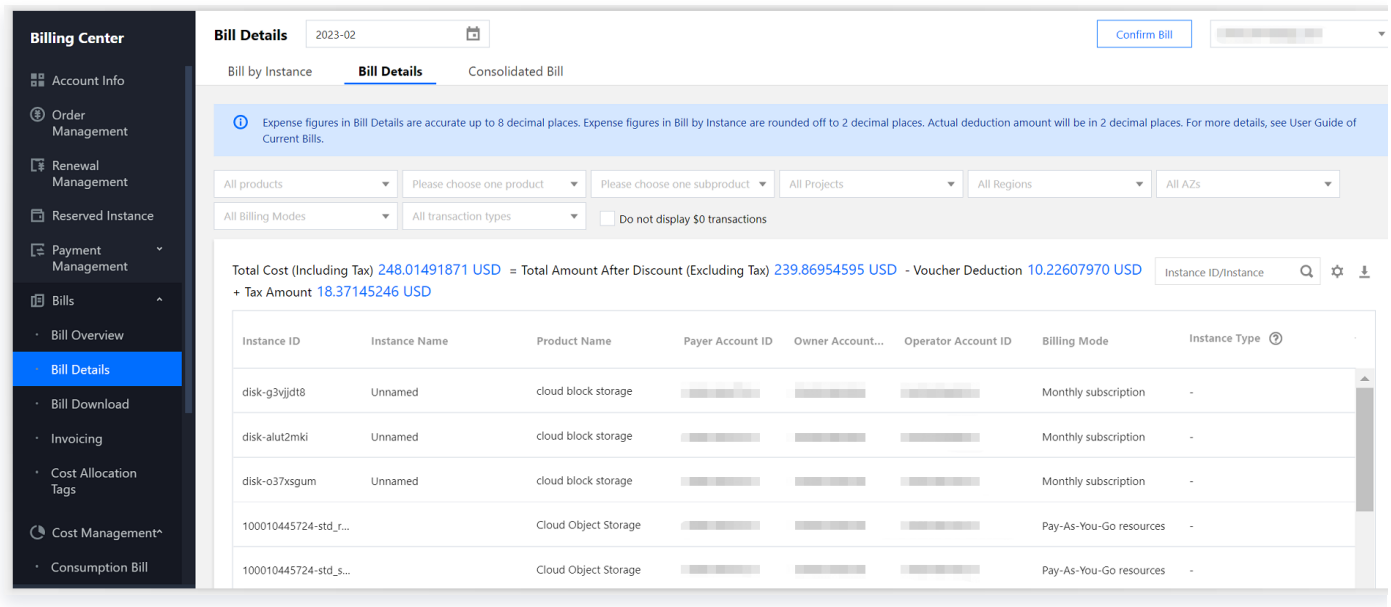
介绍管理账号如何查看成员账号的账单消费信息。

操作步骤

1. 管理账号登录费用中心控制台，选择左侧导航栏中的 费用账单 。
2. 通过右上方的下拉列表，选择对应的成员账号，查看成员账号的账单概览。
3. 通过右上方的下拉列表，选择对应的成员账号，查看成员账号的账单详情。在账单详情页面，也可以通过“账单确认”按钮，为成员账号确认对应月份的账单。







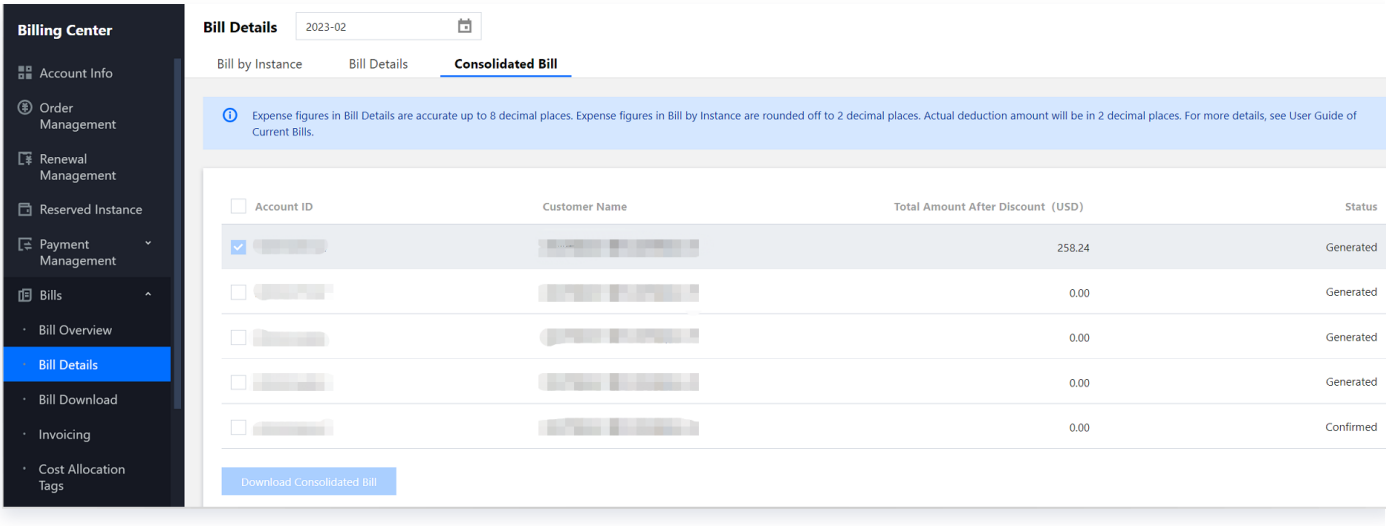
选择成员账号合并账单

介绍管理账号如何将多个成员账号的账单进行合并。

操作步骤

1. 管理账号登录费用中心控制台，选择左侧导航栏中的 账单详情 。

2. 选择“合并账单”页签，勾选需合并出账的成员账号，单击**下载合并账单**即可。如下图所示： 您也可在 下载记录 页面中，单击合并账单所在行右侧的**下载**，下载合并账单。

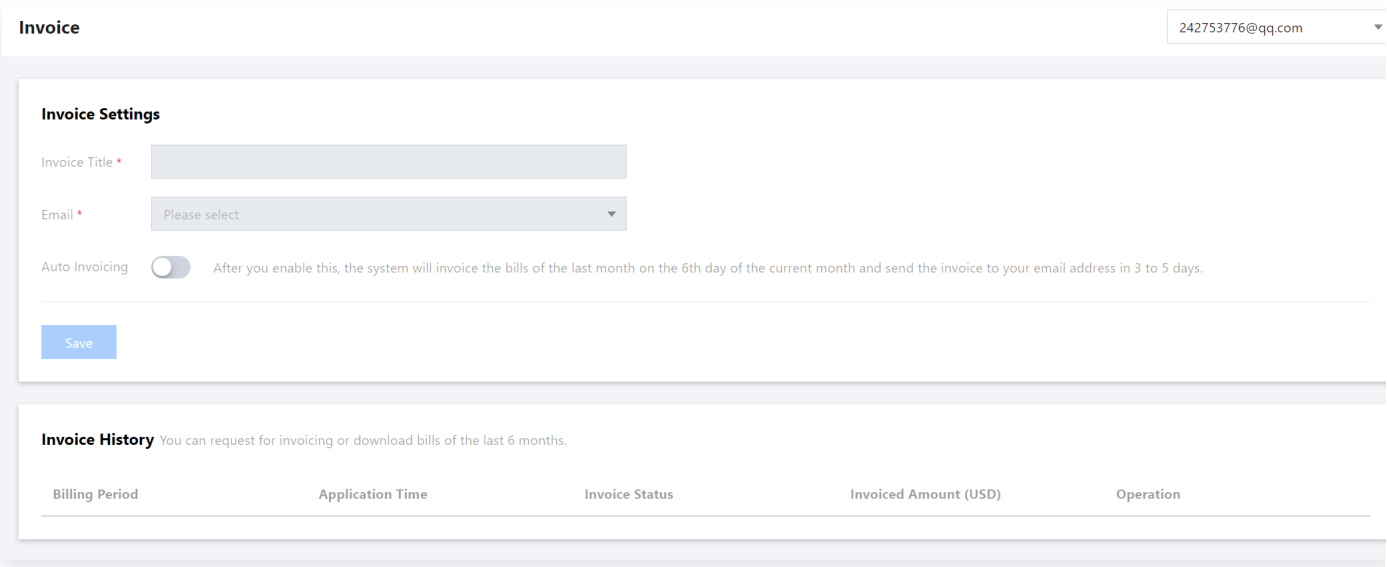


为成员账号开票

介绍管理账号如何为成员账号开具发票。

操作步骤

1. 管理账号登录费用中心控制台，选择左侧导航栏中的 发票 。
2. 通过右上方的下拉列表，选择对应的成员账号，为对应的成员账号开票。开具的发票归属于成员账号。



优惠继承

介绍成员账号如何继承管理账号的合同价优惠。

优惠继承范围

可继承商务给客户申请的合同价优惠，但不包含官网折扣和运营活动折扣。
合同价优惠的类型包含**计费级优惠**、**财务级优惠**及**满返**。不同场景下可继承关系如下表所示：

合同价优惠的类型	计费级优惠	账务级优惠	满返
优惠形式	基于单个预付费订单/单条后付费推量的优惠模式，实时生效	基于单个账号 ID 或多个账号 ID 合并整月消耗规模来设置的优惠，次月1日执行	参考本月已出账单金额，按比例返送代金券/赠送金的优惠模式， 次月3日执行
折扣	✔	×	×
合同价（线性、阶梯、一口价）	✔	×	×
保底（按月固定、按月浮动）	×	×	×

说明：
✔ 代表可继承，× 代表不可继承。

注意：
- 请务必确保管理员账号已申请的优惠包含了所有成员账号要享受的优惠。优惠继承后，成员账号将完全采用管理员账号的优惠，成员账号单独申请的优惠将不再生效。
- 优惠继承的产品范围不包含全量黑名单、指定产品黑名单。
- 成员账号UIN使用产品的计量方式（如日结/月结）需与主UIN一致才能继承，例如直播、点播、文本短信产品等，可通过CPQ报价器调整成员账号UIN的计量模式。
- 满返和账务级优惠不支持继承。

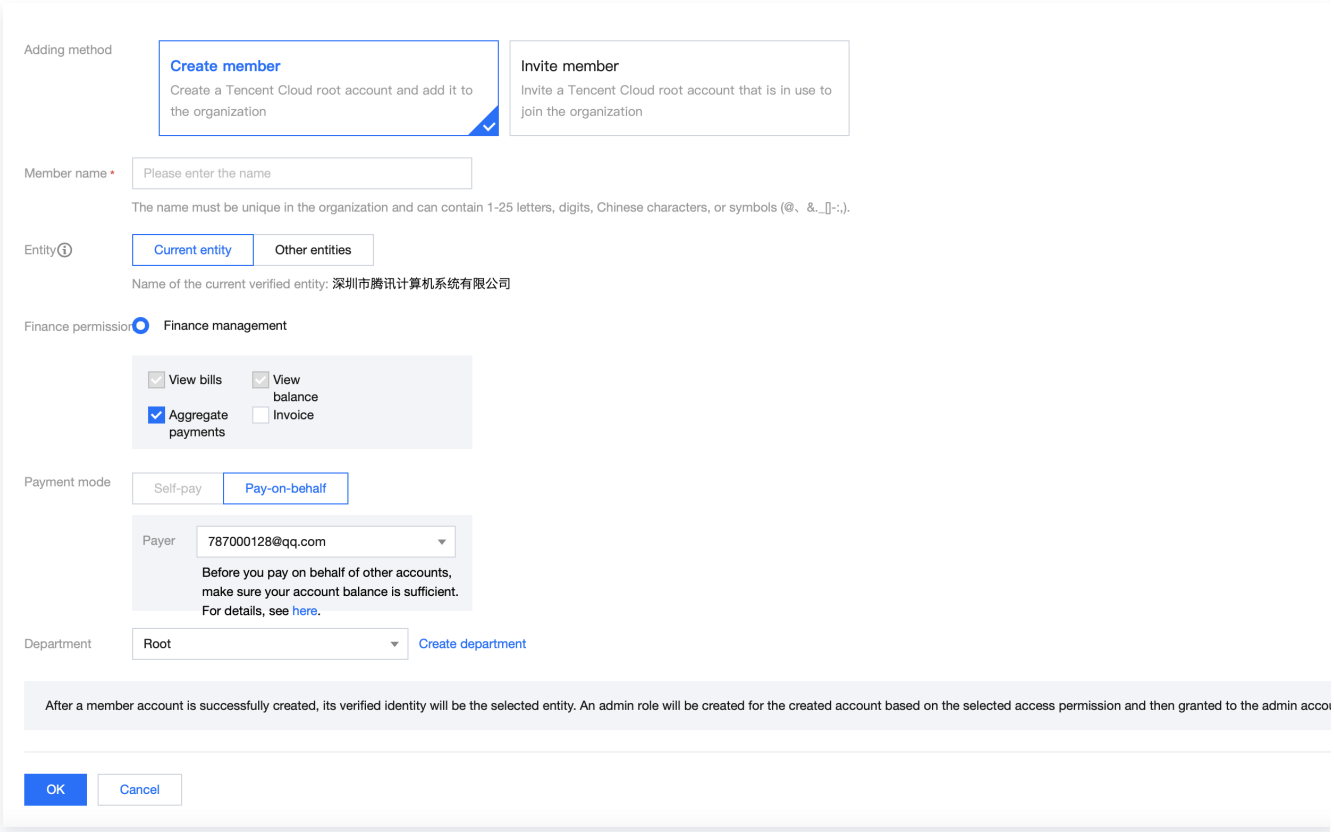
您可以通过集团账号管理为**同主体的账号**设置优惠继承，**不同主体的账号**可以联系商务进行申请。无论哪一种方式，在优惠继承建立后您都可以看到成员账号的优惠继承情况。

集团资金划拨模式（自付费）下，管理员删除集团组织、移除组织成员和成员主动退出集团组织时，已有的优惠继承不会自动取消，如需取消请联系您的商务经理进行处理。

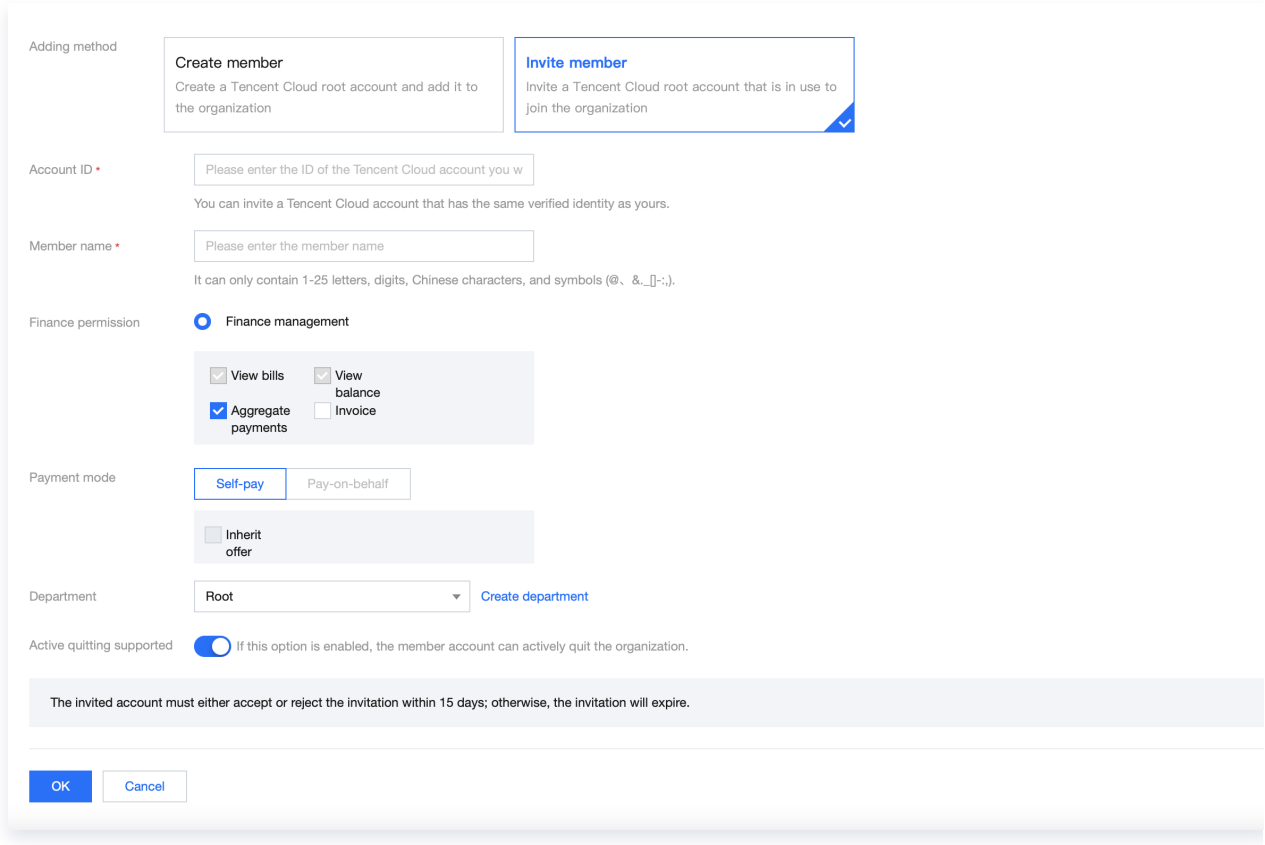
操作步骤

设置优惠继承

1. 您可在添加成员时，设置成员账号优惠继承，步骤如下：
2. 登录集团账号管理控制台，选择左侧导航栏中的 成员账号管理 。
3. 在“成员账号管理”页面中，单击添加成员。
4. 在“添加成员”页面中，根据添加成员方式，设置优惠继承：
   - 新建成员：新建成员时，成员账号默认和管理员账号使用同一个企业实名认证名称，在“付费模式”中勾选“自付费”后，可以再次勾选“优惠继承”，创建成员即可。如下图所示：



   - 邀请成员：
     - 若成员账号和管理员账号使用同一个企业认证主体，在“付费模式”中勾选“自付费”后，可以再次勾选“优惠继承”，邀请成员即可。如下图所示：



- 若成员账号和管理者账号企业认证主体不同时，在“付费模式”中勾选“自付费”后，如需设置“优惠继承”，请联系商务经理进行处理。

取消优惠继承

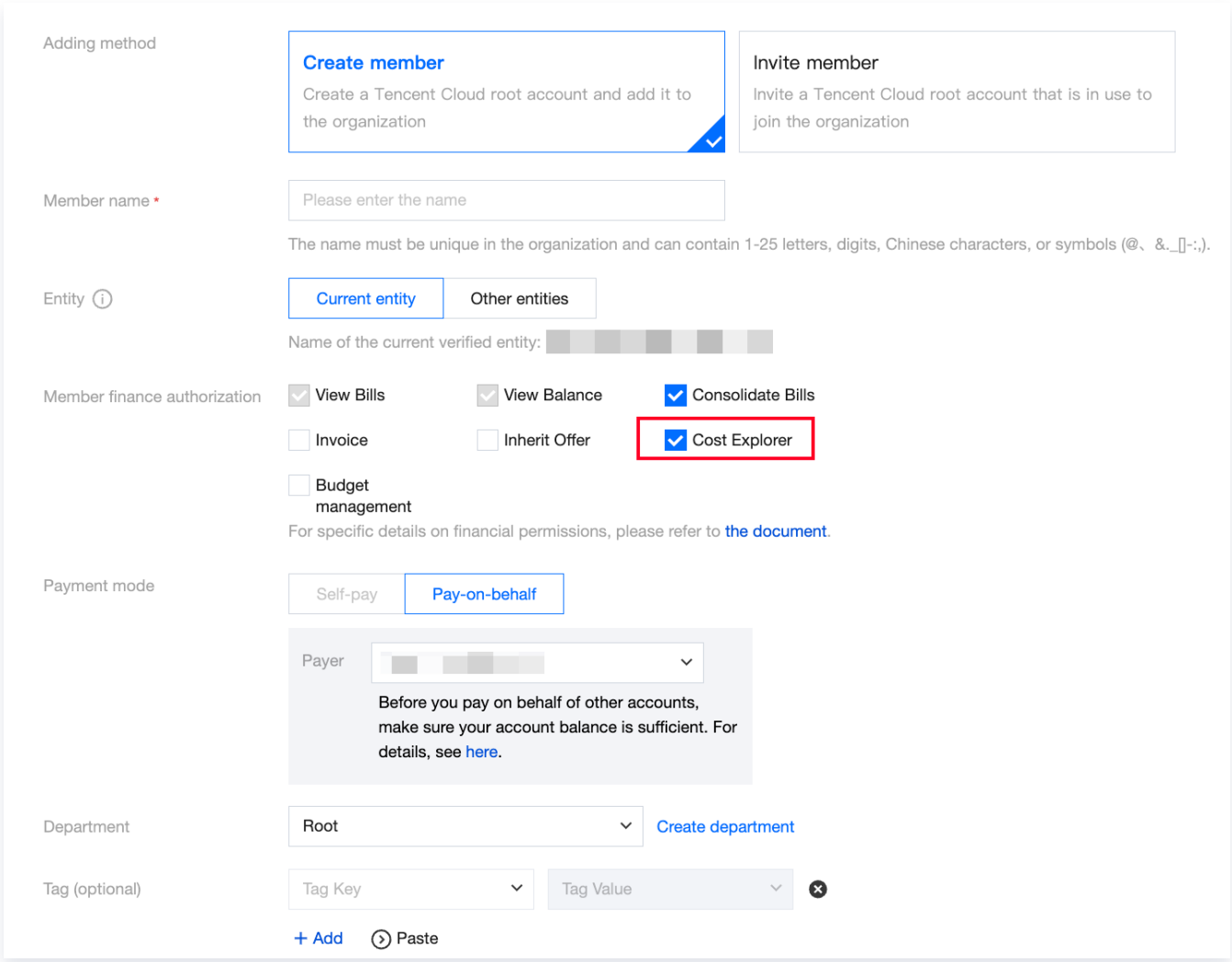
如需取消成员账号的优惠继承，请联系您的商务经理进行处理。

成本分析

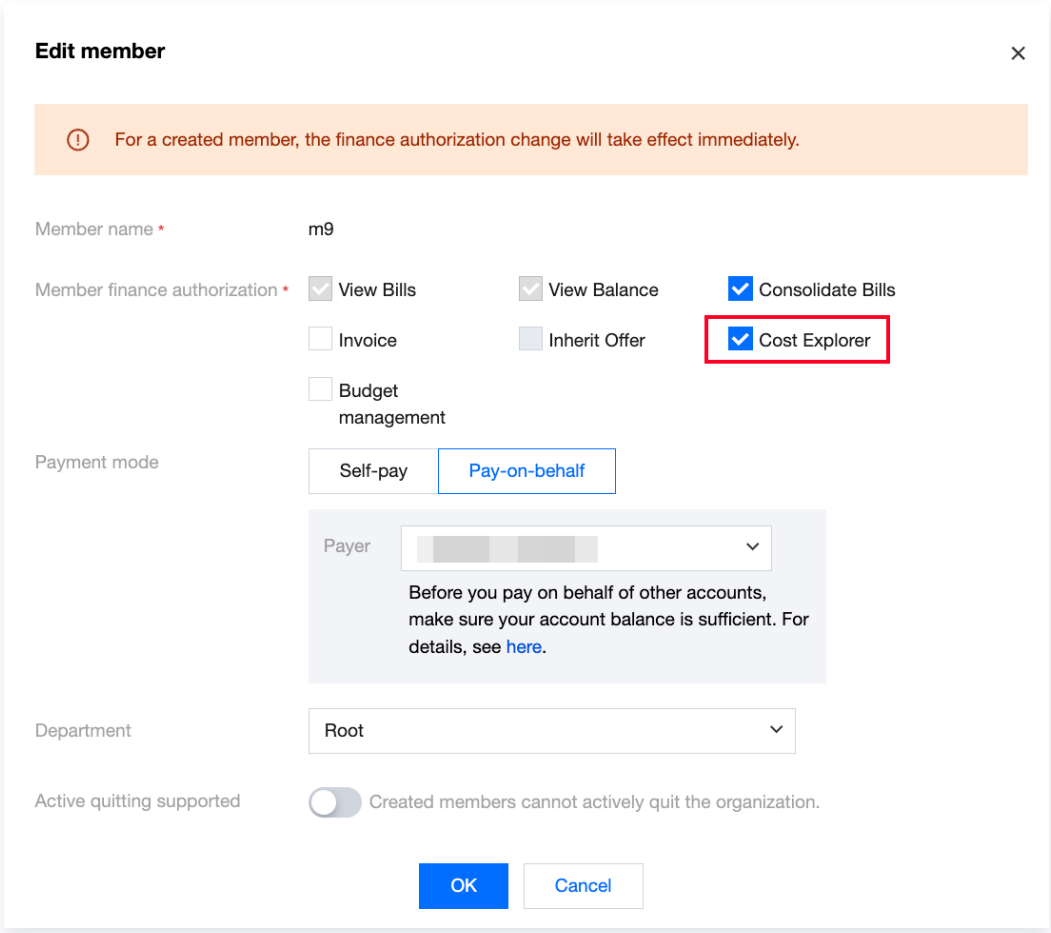
分配成本分析权限

您可在添加成员时，设置成本分析权限，具体操作步骤如下：

1. 登录集团账号管理控制台，选择左侧导航栏中的 成员账号管理 。
2. 在**成员账号管理**页面中，单击添加成员。
3. 在**添加成员**页面中，选择**新建成员**，勾选**成本分析**，单击**确定**。如下图所示：

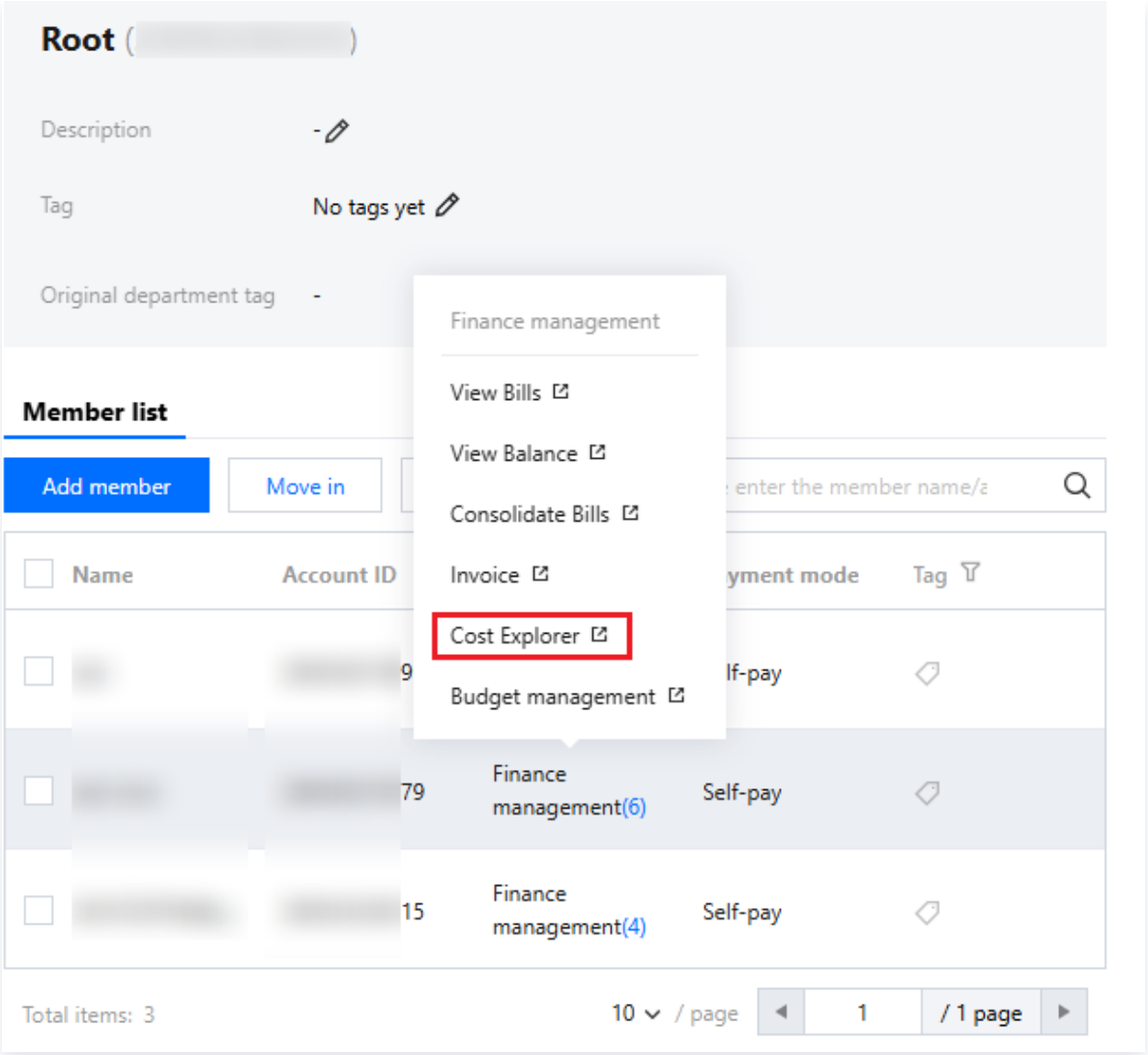


4. 已添加的成员，可在 成员账号管理 页面，找到成员账号，单击**操作**栏的**编辑**。
5. 在编辑成员页面，勾选**成本分析**后，单击**确定**。更多介绍请参见 成本分析 。



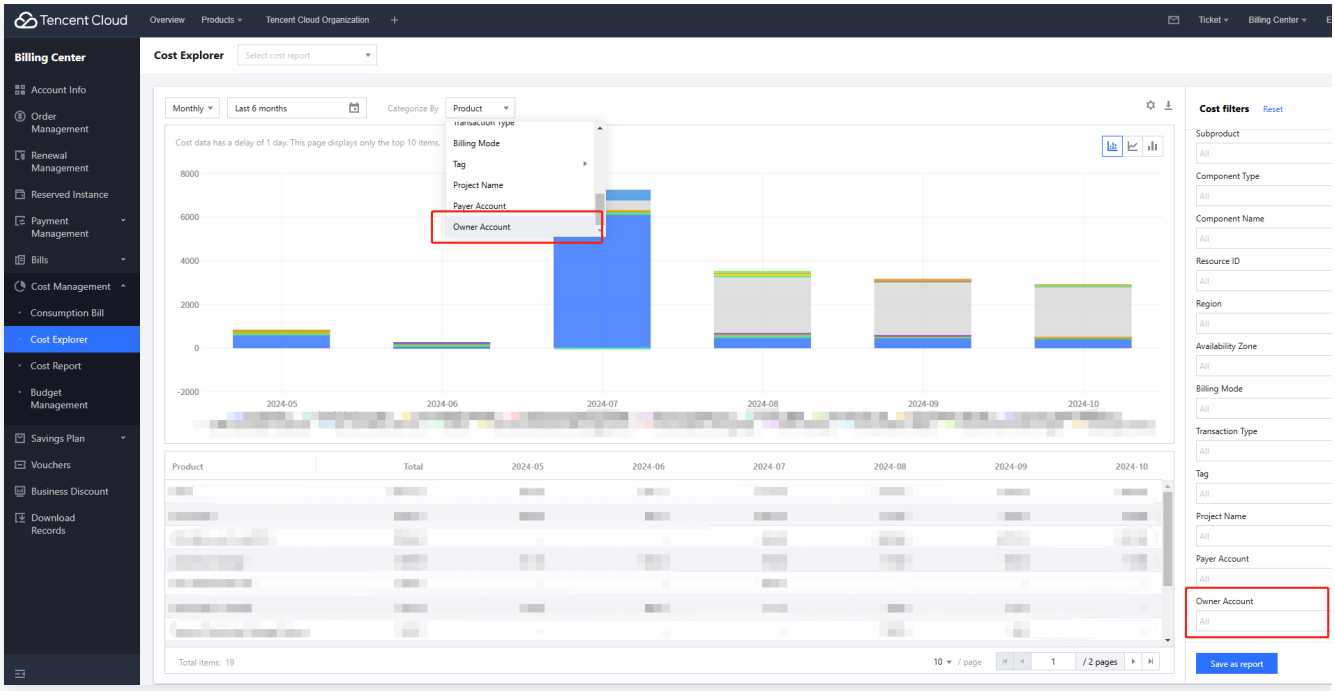
查看成本分析

1. 登录集团账号管理控制台，选择左侧导航栏中的 部门管理 。
2. 在组织架构页面，单击部门名称，查看成员列表及其权限。
3. 单击目标成员中的**财务管理** > **成本分析**。



> ⚠ 注意：
> 只有设置了成本分析权限的成员，才能查看成本分析。设置成本分析权限请参见 分配成本分析权限 。

4. 在成本分析页面：
   - 可通过分类维度筛选**使用者账号**后查看成员的成本分析数据；
   - 也可通过右侧筛选框**使用者账号**筛选成员账号并查看成员账号成本分析数据，如下图所示：

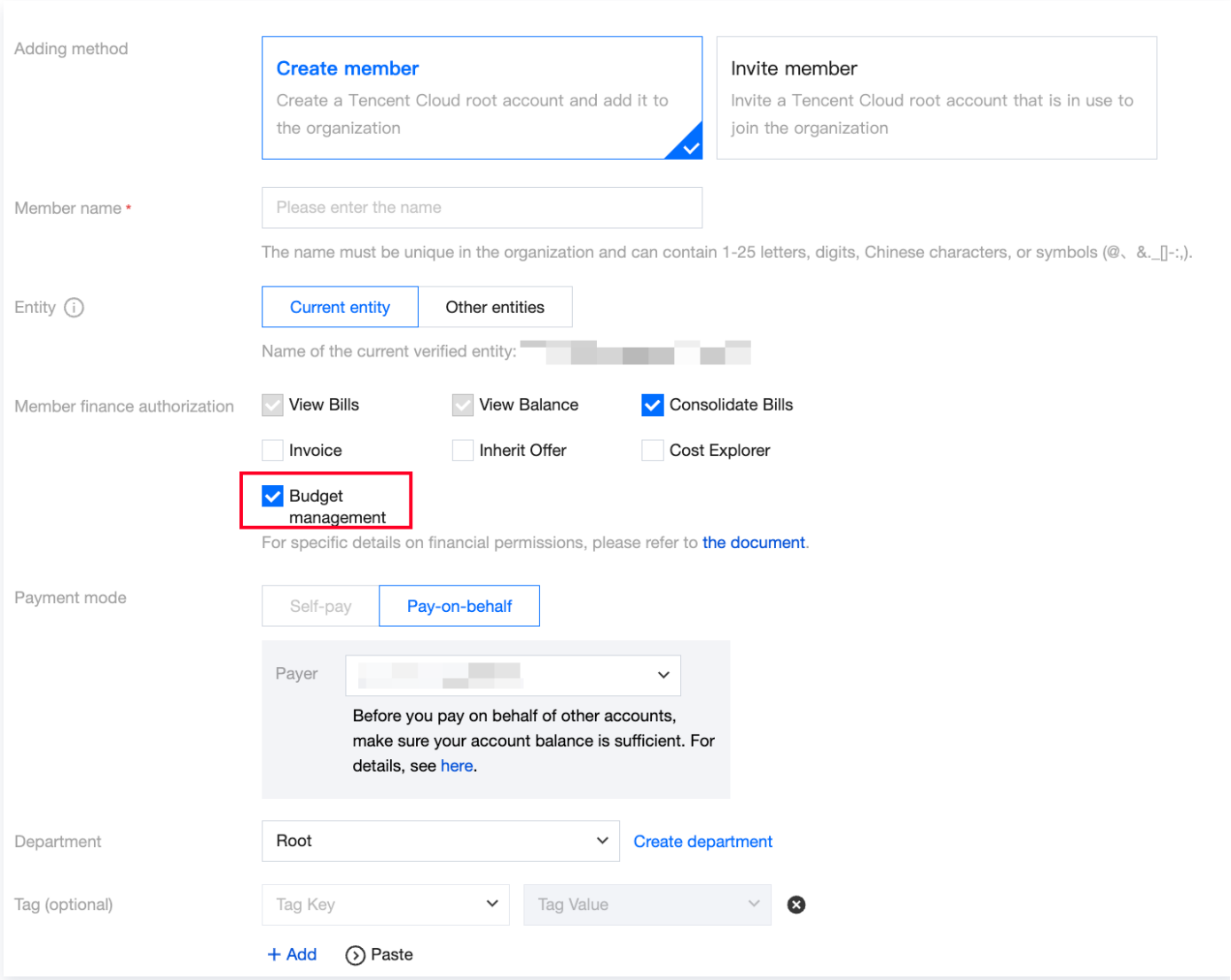


预算管理

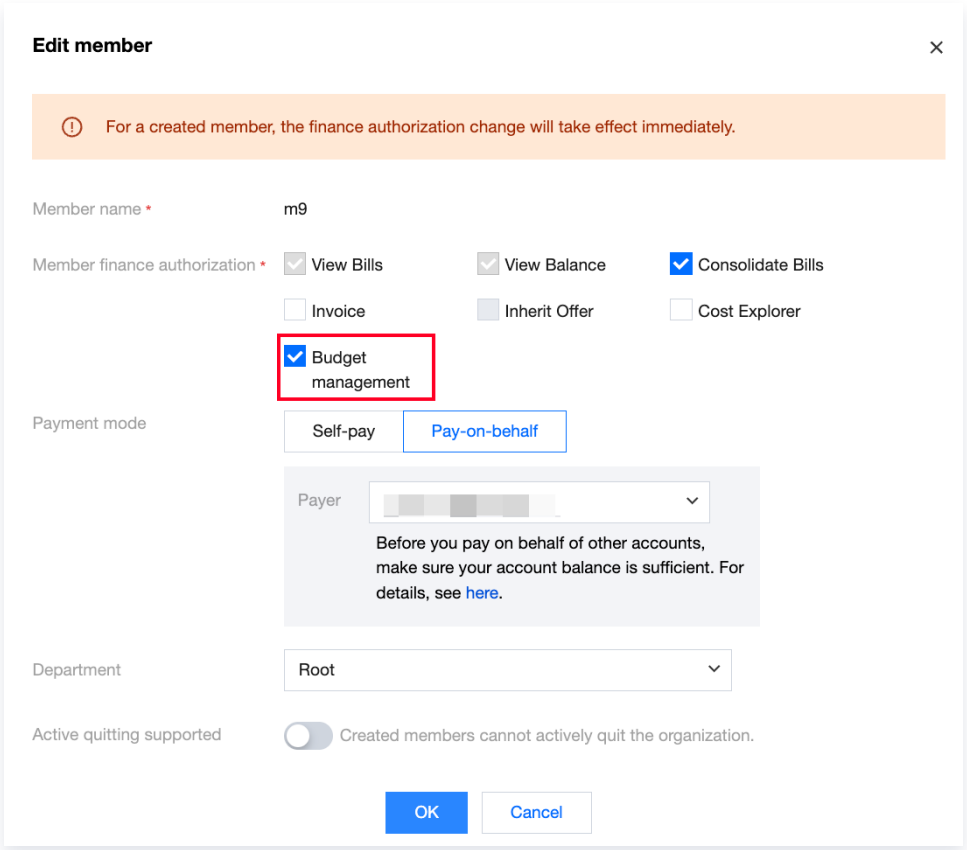
分配预算管理权限

您可在添加成员时，设置**预算管理**权限，具体操作步骤如下：

1. 登录**集团账号管理**控制台，选择左侧导航栏中的 成员账号管理 。
2. 在**成员账号管理**页面中，单击**添加成员**。
3. 在**添加成员**页面中，选择**新建成员**，勾选**预算管理**，单击**确定**。如下图所示：

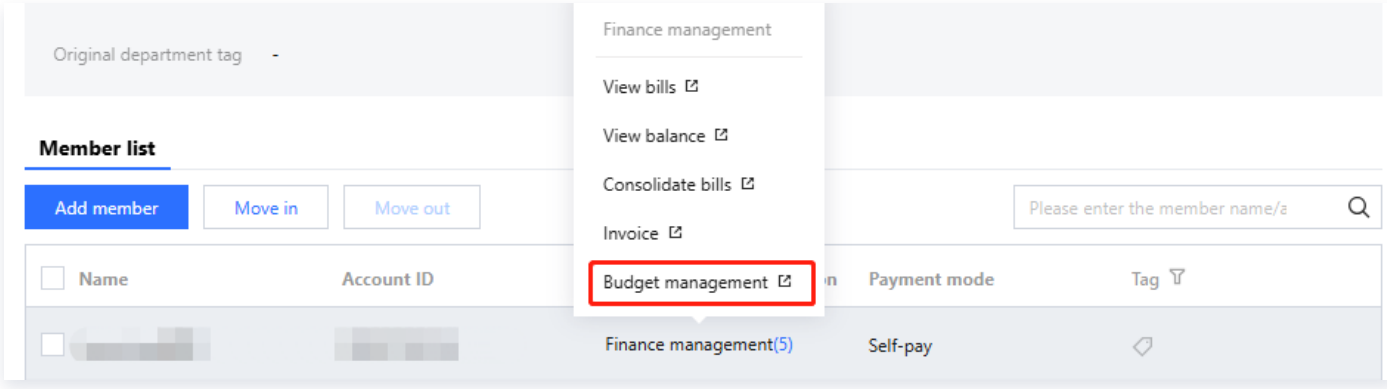


4. 已添加的成员，可在 **成员账号管理** 页面，找到成员账号，单击操作栏的**编辑**。
5. 在**编辑成员**页面，勾选**预算管理**后单击确定。更多介绍请参见 预算管理 。

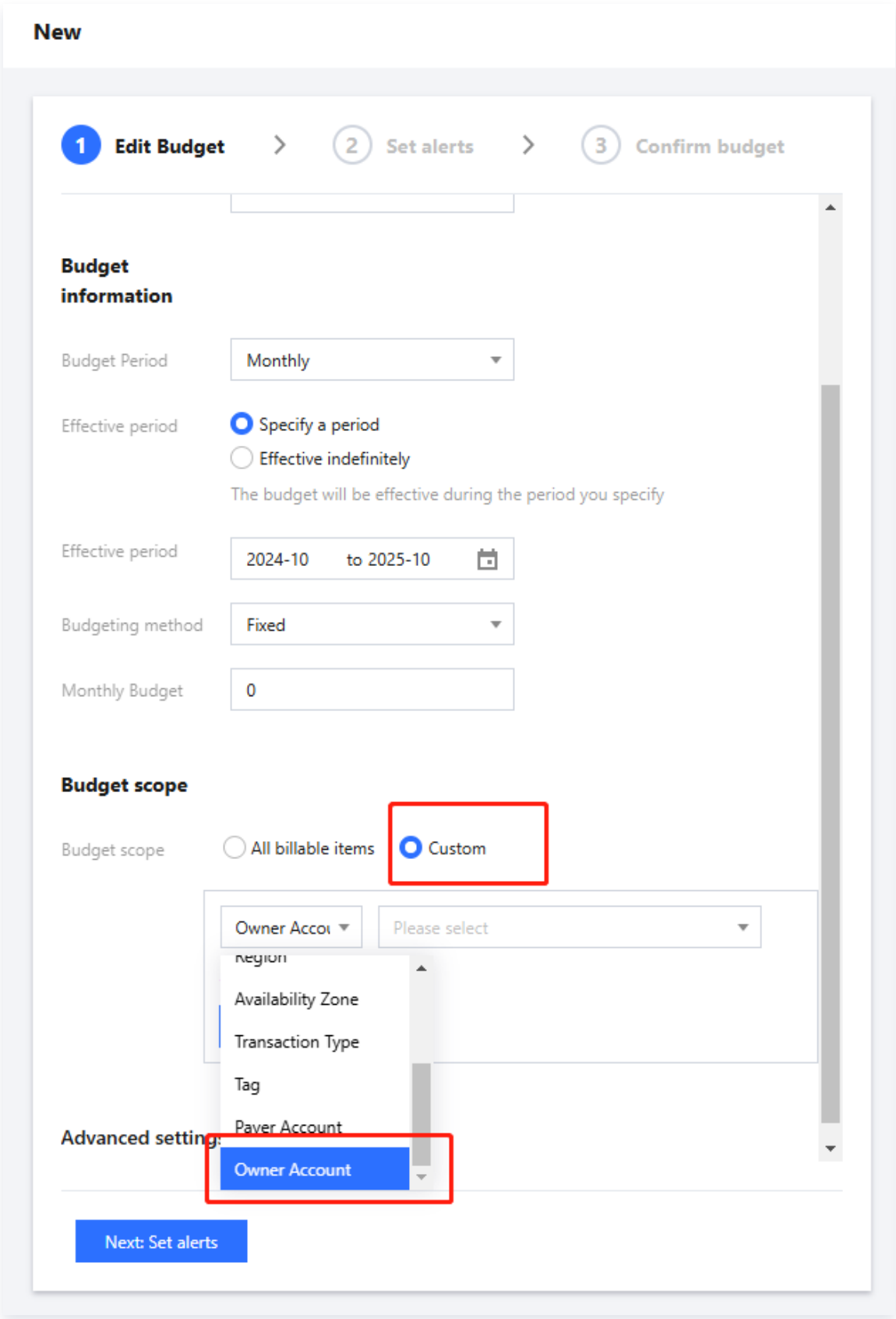


查看预算管理

1. 登录**集团账号管理**控制台，选择左侧导航栏中的 部门管理 。
2. 在组织架构页面，单击部门名称，查看成员列表及其权限。
3. 单击目标成员中的**财务管理** > **预算管理**。



4. 在**预算管理**页，单击**新建预算**，按页面提示填写相应信息，**费用范围** > **自定义费用范围** > **使用者账号**，筛选成员账号，为成员账号配置预算。



成员访问管理
服务管控策略
服务管控策略概述

最近更新时间：2024-03-06 18:52:29

集团账号服务管控策略是一种基于层级结构（部门或成员）的访问控制策略，可以统一管理集团账号各层级内资源访问的权限边界，建立企业整体访问控制原则或局部专用原则。服务管控策略只定义权限边界，并不真正授予权限，您还需要在某个成员中使用访问控制（CAM）设置权限后，相应身份才具备对资源的访问权限。

应用场景

当企业创建了一个集团账号，并为每个部门创建了成员后，如果对各成员的行为不加以管控，就会破坏运维规则，带来安全风险和成本浪费。集团账号提供服务管控策略功能，企业可以通过管理账号集中制定管理规则，并将这些管理规则应用于集团账号的各层级结构（部门、成员）上，管控各成员内资源的访问规则，确保安全合规和成本可控。例如：禁止成员申请域名、禁止成员删除日志记录等。

服务管控策略类型

- 系统服务管控策略

系统自带的服务管控策略。您只能查看，不能创建、修改和删除系统服务管控策略。开启服务管控策略功能后，集团账号内所有的部门和成员默认绑定了系统策略FullQcloudAccess，该策略允许对您在腾讯云上的所有资源进行任何操作。

- 自定义管控策略

用户自定义的服务管控策略。您可以创建、修改和删除自定义服务管控策略。自定义服务管控策略创建成功后，您需要将自定义服务管控策略绑定到部门或成员上，才能生效。不需要时，也可以随时解绑。

服务管控策略工作原理

1、使用管理账号开启服务管控策略功能。更多信息，请参见 开启管控策略功能 。
2、开启服务管控策略功能后，系统策略 FullQcloudAccess 将默认绑定到集团账号内的所有部门及成员，此策略允许所有操作，以防止管控策略的不当配置造成意料之外的访问失败。
3、使用管理账号创建服务管控策略。更多信息，请参见 创建自定义管控策略 。
4、使用管理账号将服务管控策略绑定到集团账号节点（部门、成员）。更多信息，请参见 绑定自定义管控策略 。
5、服务管控策略允许绑定到集团中的部门或成员。服务管控策略具备向下继承的特点，例如：为父部门设置管控策略A，为子部门设置管控策略B，则管控策略A和管控策略B都会在子部门及其下的成员中生效。

> ⚠ **注意：**
> **请先进行局部小范围测试，确保策略的有效性与预期一致，然后再绑定到全部目标节点（部门、成员）。**

6、当成员中的CAM用户或CAM角色访问腾讯云服务时，腾讯云将会先进行服务管控策略检查，再进行账号内的CAM权限检查。具体如下：

（1）服务管控策略鉴权从被访问资源所在账号开始，沿着集团账号层级逐级向上进行。

（2）在任一层级进行服务管控策略鉴权时，命中拒绝（Deny）策略时都可以直接判定结果为拒绝（Explicit Deny），结束整个服务管控策略鉴权流程，并且不再进行账号内基于CAM权限策略的鉴权，直接拒绝请求。

（3）在任一层级进行服务管控策略鉴权时，如果既未命中拒绝（Deny）策略，也未命中允许（Allow）策略，同样直接判定结果为拒绝（Explicit Deny），不再进入下一个层级鉴权，结束整个服务管控策略鉴权流程，并且不再进行账号内基于CAM限策略的鉴权，直接拒绝请求。

（4）在某一层级鉴权中，如果未命中拒绝（Deny）策略，而命中了允许（Allow）策略，则本层级鉴权通过，继续在父节点上进行管控策略鉴权，直至Root部门为止。如果Root部门鉴权结果也为通过，则整个管控策略鉴权通过，接下来进入账号内基于CAM权限策略的鉴权。

（5）服务管控策略对服务关联角色不生效。

（6）腾讯云将会评估被访问的账号自身及其所在的每一层级上绑定的服务管控策略，从而确保绑定在较高层级上的服务管控策略可以在其下的所有账号上生效。

开启服务管控策略

最近更新时间：2024-03-06 18:52:29

管控策略功能默认关闭，您需要开启后才能使用。

背景信息

开启管控策略功能后，集团账号的变化如下：
集团账号内的部门和成员会默认绑定系统策略 FullQcloudAccess ，该策略允许对您在腾讯云上的所有资源进行任何操作。
当创建部门或成员时，系统会自动为其绑定系统策略 FullQcloudAccess。
当邀请的腾讯云账号加入集团账号后，系统会自动为其绑定系统策略 FullQcloudAccess。
当移除成员时，该成员绑定的所有管控策略将会自动解绑。

操作步骤

1. 登录 集团账号控制台 。
2. 在左侧导航栏，选择 **集团账号** > **服务管控策略**。
3. 单击开启**服务管控策略**。

后续步骤

您可以创建自定义管控策略（例如：禁止对某资源的某个操作），然后绑定到集团账号的部门或成员，限制成员对资源的操作权限。操作方法请参见：

- 创建自定义管控策略
- 绑定自定义管控策略

创建自定义服务管控策略

最近更新时间：2024-03-06 18:52:29

您可以创建自定义服务管控策略，限制对某些资源执行某些操作，为集团账号内的部门和成员定义权限边界。

创建方式

1.通过可视化编辑模式创建自定义管控策略
系统提供所见即所得的可视化编辑界面，您只需选择效果、云服务、操作、资源和条件，就可以生成自定义管控策略。同时，提供的智能校验功能，帮助您提高管控策略的正确性和有效性。该方式操作简单，易于上手。
2.通过脚本编辑模式创建自定义管控策略
系统提供JSON脚本编辑界面，您需要按照服务管控策略语法和结构编写自定义管控策略。该方式使用灵活，适用于对服务管控策略语法比较熟悉的用户。

通过可视化编辑模式创建自定义服务管控策略

1. 登录 集团账号控制台 。
2. 在左侧导航栏，选择**集团账号** > **服务管控策略**。
3. 在策略列表页签，单击**新建策略**。
4. 在新建策略页面，单击**可视化策略生成器页签**。
5. 配置服务管控策略，然后单击下一步：**编辑基本信息**。
   - 在效果区域，选择允许或拒绝。
   - 在服务区域，选择云服务。

     > **注意：**
     > 支持可视化编辑模式的云服务以控制台界面显示为准。

   - 在**操作区域**，选择**全部操作或自定义操作** 。

     系统会根据您上一步选择的云服务，自动筛选出可以配置的操作。如果您选择了自定义操作，您需要继续选择具体的操作。
   - 在**资源区域**，选择 **全部资源或特定资源**。

     系统会根据您上一步选择的操作，自动筛选出可以配置的资源类型。如果您选择了 **特定资源**，您需要继续单击**添加自定义资源六段式**，配置具体的资源 ARN。您可以使用**匹配全部**功能，快速选择对应配置项的全部资源。
   - **可选：**在**条件**区域，单击**来源IP**，配置条件。

     您可以手动输入 **IP值（段）**，也可以点击添加其它条件包括腾讯云通用条件和服务级条件，系统会根据您前面配置的云服务和操作，自动筛选出可以配置的条件列表。您只需要选择对应条件键配置具体内容。
6. **编辑基本信息，** 输入服务管控策略的名称和描述，单击**完成**。

通过 JSON 模式创建自定义服务管控策略

1. 登录 集团账号控制台 。
2. 在左侧导航栏，选择**集团账号 > 服务管控策略**。
3. 在**策略列表**页签，单击**新建策略**。
4. 在**新建策略**页面，单击 JSON 页签。
5. 输入服务管控策略内容，然后单击 **下一步：编辑基本信息**。
6. 输入服务管控策略**名称**和**描述**。

后续步骤

自定义服务管控策略创建成功后，需要绑定到部门或成员才能生效。具体操作，请参见 绑定自定义管控策略 。

查看服务管控策略详情

最近更新时间：2024-03-06 18:52:29

您可以查看管控策略名称、策略类型、策略内容和绑定目标等。

操作步骤

1. 登录 集团账号控制台 。
2. 在左侧导航栏，选择**集团账号 > 服务管控策略**。
3. 在**策略列表**页签，单击**策略名称**。
   - 在**基本信息**区域，查看**策略名称**、**策略类型**、**策略描述**。
   - 在**策略语法**页签，查看策略内容。
   - 在**绑定管理**页签，查看策略绑定的部门或成员。

修改自定义服务管控策略

最近更新时间：2024-03-06 18:52:29

您可以根据需要修改自定义服务管控策略的名称、描述和内容。如果您修改了管控策略内容，则会在绑定了该管控策略的部门和成员上立即生效。

背景信息

系统管控策略不支持修改。

操作步骤

1. 登录 集团账号控制台 。
2. 在左侧导航栏，选择**集团账号 > 服务管控策略**。
3. 在**策略列表**页签，单击目标管控策略名称。
4. 在**策略详情**页面的右上角，单击**编辑策略**。

   通过可视化策略生成器或 JSON 编辑模式修改服务管控策略内容，然后单击 **下一步：编辑基本信息**。

   具体操作，请参见 创建自定义管控策略 。
5. 修改**名称**和**备注** ，然后单击 **确定**。

删除自定义服务管控策略

最近更新时间：2024-03-06 18:52:29

对于未绑定任何部门或成员的自定义管控策略，您可以随时删除。

背景信息

- 系统服务管控策略不支持删除。
- 对于已绑定了部门或成员的自定义服务管控策略，需要先解绑，然后才能删除。具体操作，请参见 解绑自定义管控策略 。

操作步骤

1. 登录 集团账号控制台 。
2. 在左侧导航栏，选择**集团账号 > 服务管控策略**。
3. 在**策略列表**页签，单击目标管控策略**操作**列的**删除**。
4. 单击**确定**。

绑定自定义服务管控策略

最近更新时间：2024-03-06 18:52:29

您可以为部门或成员绑定自定义管控策略。绑定成功后，部门或成员将会立即受到服务管控策略的管控。请务必确定绑定操作的结果是符合预期的，以免影响您的业务正常运行。

背景信息

1、系统会默认为资源夹和成员绑定系统策略 FullQcloudAccess 。
2、服务管控策略在绑定节点下整体生效，即父部门绑定的管控策略，会在其子部门及其成员上生效。

操作步骤

1. 登录 集团账号控制台 。
2. 在左侧导航栏，选择**集团账号 > 服务管控策略**。
3. 单击策略名称进入策略详情页签，选择**绑定管理**。
4. 单击**绑定**，在策略绑定对话框，选择需要绑定的部门或者成员。
5. 单击**确定**。

解绑自定义服务管控策略

最近更新时间：2024-03-06 18:52:29

您可以随时解绑自定义服务管控策略，解绑成功后，原绑定的部门或成员将会立即失去服务管控策略的管控。请务必确定解绑操作的结果是符合预期的，以免影响您的业务正常运行。

背景信息

系统策略和自定义服务管控策略都可以解绑，但部门或成员上绑定的最后一条服务管控策略不允许解绑。

操作步骤

1. 登录 集团账号控制台 。
2. 在左侧导航栏，选择 **集团账号 > 服务管控策略**。
3. 单击策略名称进入策略详情页签，选择**绑定管理**。
4. 在列表中单击目标部门或成员后，单击**解绑**。
5. 单击**确定**。

关闭服务管控策略

最近更新时间：2024-03-06 18:52:29

如果您不想限制集团账号内部门和成员的权限，则可以关闭服务管控策略功能。

背景信息

关闭服务管控策略功能后，您绑定到部门和成员上的管控策略会全部自动解绑。但管控策略本身不会被删除，只是不能再绑定到任何目标对象上。

> **注意：**
> 关闭服务管控策略将会影响整个集团账号内部门和成员的权限，请谨慎操作。

操作步骤

1. 登录 集团账号控制台 。
2. 在左侧导航栏，选择 **集团账号 > 管控策略**。
3. 在服务**管控策略**页面上方的标题区域，单击**关闭服务**。
4. 单击**确定**，当状态显示**管控策略已关闭**时，表示管控策略功能已关闭。

> **注意：**
> 您也可以单击**开启服务管控**，重新开启管控策略功能。开启成功后，默认系统管控策略 FullQcloudAccess 会自动绑定到部门和成员上，但其他自定义服务管控策略需要您重新绑定。

资源管理
资源共享
资源共享概述

最近更新时间：2024-12-09 15:15:13

资源共享是指多账号间通过共享的方式将一个腾讯云账号下的指定资源共享给其他腾讯云账号使用。

> **说明：**
> 目前仅 SP **节省计划**支持通过白名单的方式进行资源共享，若您需要使用该功能，可以联系我们。

资源共享方式

资源共享方式	说明	相关文档
允许共享给任意账号	1. 集团组织外共享 ○ 未加入集团账号的腾讯云账号，可以将资源共享给单个腾讯云账号。 ○ 集团账号的管理账号或成员，可以将资源共享给集团账号外的单个腾讯云账号。 2. 集团组织内共享 集团账号的管理账号或成员，可以将资源共享给本集团账号内的其他成员账号。 **注意：** • **组织外仅支持同主体共享：**组织外共享仅支持共享给与共享者企业实名相同的其他腾讯云账号。 • **不支持跨集团组织共享：**若共享者为集团组织内的管理账号或成员，被共享者不允许加入其他集团组织。 • 不支持经销商及经销商子客在集团账号控制台使用资源共享的功能。	将资源共享给任意账号
仅允许集团组织内共享	集团账号的管理账号或成员，可以将资源共享给本集团账号内的其他成员账号。	仅在集团账号内共享资源

共享者管理共享资源
将资源共享给任意账号

最近更新时间：2024-12-09 15:15:13

共享者可以将资源共享给任意的被共享者，共享者和被共享者不区分是否已加入集团账号。

应用场景

将资源共享给任意账号，主要存在以下几个场景：

1. **集团组织外共享**
   - 未加入集团账号的腾讯云账号，可以将资源共享给单个腾讯云账号。
   - 集团账号的管理账号或成员，可以将资源共享给集团账号外的单个腾讯云账号。
2. **集团组织内共享**

   集团账号的管理账号或成员，可以将资源共享给本集团账号内的其他成员账号。

> **注意：**
> - **组织外仅支持同主体共享：**组织外共享仅支持共享给与共享者**企业实名相同**的其他腾讯云账号。
> - **不支持跨集团组织共享：**若共享者为集团组织内的管理账号或成员，被共享者不允许加入其他集团组织。
> - 不支持经销商及经销商子客在集团账号控制台使用资源共享的功能。

操作步骤

创建共享单元

1. 登录集团账号管理控制台，选择左侧导航栏中的**资源共享** > 由我共享 。
2. 选择**共享单元**页签，在页面上方选择需共享审批流模板所在地域后，单击**创建共享单元**。
3. **配置基础信息：**包括共享单元名称、地域、描述。
4. **选择共享资源：**选择资源类型后，在共享资源列表中勾选需要共享的资源。

> **说明：**
> - 目前最多支持共享10个资源。
> - 列表中为当前账号所选地域下的审批流模板信息。

5. **选择共享账号：**

> **说明：**

- 单次最多添加10个共享账号。
- 一个共享单元最多支持添加20个共享账号。

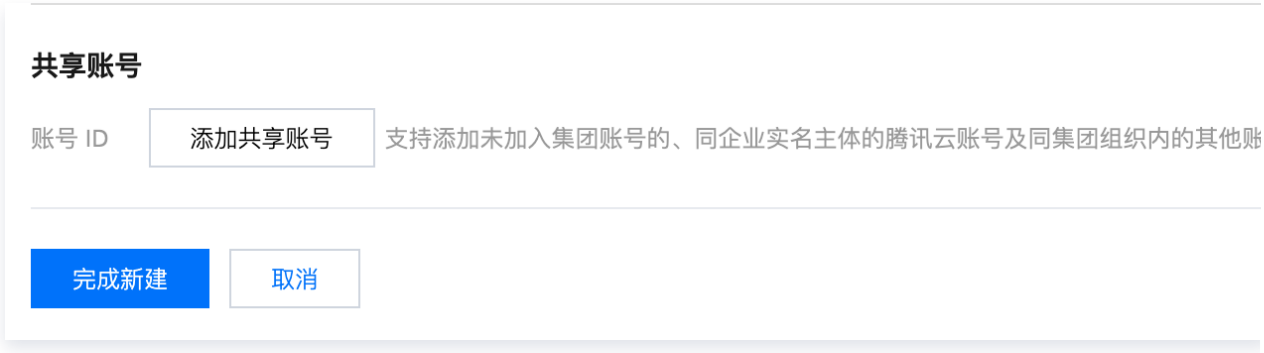
5.1 **未加入集团账号的腾讯云账号进行共享：**

- 单击**添加共享账号**

- 在弹出的**添加共享账号**窗口，选择**允许共享给任意账号**，勾选**手动添加**，单击**添加**，手动输入被共享的腾讯云账号 ID，单击**保存**。

5.2 **集团账号的管理账号或成员进行共享：**

- 单击**添加共享账号**



- 在弹出的**添加共享账号**窗口，选择**允许共享给任意账号**，添加方式按需勾选通过集团组织添加或者手动添加，在列表中选择或者手动输入被共享的腾讯云账号 ID，单击**保存**。

> **注意：**
> 管理账号和委派管理员支持通过集团组织添加，其他成员账号仅支持手动添加。

6. 单击**完成新建**即可完成创建共享单元。

仅在集团账号内共享资源

最近更新时间：2024-12-09 15:15:13

集团账号的管理账号或成员，可以将资源共享给本集团账号内的其他成员账号。

创建共享单元

操作步骤

1. 登录集团账号管理控制台，选择左侧导航栏中的**资源共享** > 由我共享 。
2. 选择**共享单元**页签，在页面上方选择需共享审批流模板所在地域后，单击**创建共享单元**。
3. **配置基础信息：**包括共享单元名称、地域、描述。
4. **选择共享资源：**选择资源类型后，在共享资源列表中勾选需要共享的资源。

> **说明：**
> - 目前最多支持共享10个资源。
> - 列表中为当前账号所选地域下的资源信息。

5. **选择共享账号：**

> **说明：**
> - 单次最多添加10个共享账号。
> - 一个共享单元最多支持添加20个共享账号。

5.1 单击添加共享账号。

5.2 在弹出的**添加共享账号**窗口点击添加按钮，共享账号范围选择**仅允许集团组织内共享**，添加方式按需勾选通过集团组织添加或者手动添加，在列表中选择或者手动输入被共享的腾讯云账号 ID，单击**保存**。

> **注意：**
> 管理账号和委派管理员支持通过集团组织添加，其他成员账号仅支持手动添加。

6. 单击**完成新建**即可完成创建共享单元。

其他基本操作
查看共享单元

最近更新时间：2024-12-09 15:15:13

共享者如需查看共享单元，可参考本文进行操作。

操作步骤

1. 登录集团账号管理控制台，选择左侧导航栏中的**资源共享** > 由我共享 。
2. 在共享单元列表页查看已创建的共享单元。

3. 单击共享单元名称，可以进入共享单元详情页面查看已共享的资源及对应成员账号。


shareUnit-
基础信息
共享单元名称
共享单元ID
拥有者
所属地域 广州
Arn
创建时间 2024-06-11 17:02:26
描述
共享资源
请输入共享资源ID
ID
所属地域
可用区
使用中 / 全部共享账号
1
广州
-
0 / 1
共 1 条
10 条 / 页
1
/ 1 页
共享账号记录
请输入共享账号 ID
账号
共享状态
共享时间
退出共享时间
共享中
2024-06-11 17:02:27
-
共 1 条
10 条 / 页
1
/ 1 页

编辑共享单元

最近更新时间：2024-12-09 15:15:13

完成资源共享后，如需编辑共享单元下的共享资源及共享账号信息，可参考本文进行操作。

操作步骤

1. 登录集团账号管理控制台，选择左侧导航栏中的**资源共享** > 由我共享 。
2. 选择**共享单元**页签，在页面上方选择共享单元所在地域。
3. 单击需修改共享单元所在行右侧的**编辑**。如下图所示：

4. 在**编辑共享单元**页面中，参考以下信息进行配置。
   4.1 **修改共享资源**：在**共享资源**中，勾选/取消勾选资源即可完成修改。
   4.2 **修改共享账号**：
   - **增加共享账号**：单击**添加共享账号**，在弹出的**添加共享账号**窗口中，勾选或手动添加被共享账号后，单击**保存**，具体请参见 创建共享单元 。

   - **移除共享账号**：单击需删除被共享账号所在行右侧的**移除**。如下图所示：

5. 单击**保存**即可完成编辑操作。

删除共享单元

最近更新时间：2024-12-09 15:15:13

若您无需再进行某个共享单元下的资源共享，可删除共享单元解除共享。

操作步骤

1. 登录集团账号管理控制台，选择左侧导航栏中的**资源共享** > 由我共享 。
2. 选择**共享单元**页签，在页面上方选择共享单元所在地域。
3. 单击需删除共享单元所在行右侧的**删除**。如下图所示：

> **注意：**
> 删除共享单元前请先移除共享资源和共享账号。

4. 在弹出的窗口中单击**确定**即可删除。

被共享者管理共享资源
查看被共享的资源详情

最近更新时间：2024-12-09 15:15:13

操作场景

本文介绍被共享账号如何通过集团账号管理控制台，查看被共享的资源详情。

操作步骤

1. 登录集团账号管理控制台，选择左侧导航栏中的**资源共享** > 与我共享 。
2. 在**与我共享**页面中，在页面上方选择资源所在地域。
   - 选择**共享单元**页签，即可查看共享单元。
   - 选择**共享资源**页面，即可查看共享资源。

被共享者同意/拒绝加入共享单元

最近更新时间：2024-12-09 15:15:13

在集团组织外共享资源时，被共享者需要接受共享邀请后才能正常使用该共享资源。

使用限制

只有在集团组织外共享资源时，才需要接受或拒绝资源共享邀请。在集团组织内共享资源时，系统会默认接受共享邀请，被共享者不需要做任何操作。

操作步骤

同意共享邀请

1. 登录集团账号管理控制台，选择左侧导航栏中的**资源共享** > 与我共享 。
2. 选择**共享单元**页签，在列表中的操作列选择同意。

同意后，资源使用者可访问该共享单元中的资源，且后续该共享单元新增加的资源将默认接受。

拒绝共享邀请

1. 登录集团账号管理控制台，选择左侧导航栏中的**资源共享** > 与我共享 。
2. 选择**共享单元**页签，在列表中的操作列选择拒绝。

拒绝后，资源使用者将无法访问该共享资源。

退出共享单元

最近更新时间：2024-12-09 15:15:13

在集团组织外共享资源时，对于已加入共享的被共享者，可以选择主动退出共享单元。

使用限制

- 只有在集团组织外共享资源时，被共享者才可以主动退出共享单元。
- 在集团组织内共享资源时，被共享者不能主动退出共享单元，只能由共享者移除，详情请参见 编辑共享单元 。
- 如果共享单元中包含任意一个或多个不支持退出的资源类型时，则不允许被共享者主动退出。此时只能由共享者移除，详情请参见 编辑共享单元 。

操作步骤

1. 登录集团账号管理控制台，选择左侧导航栏中的**资源共享** > 与我共享 。
2. 选择**共享单元**页签，单击共享单元名称进入共享单元详情页。
3. 在共享单元详情页的右上角，单击**退出共享单元**。
4. 在**退出共享单元**窗口中，单击**确定**。

集团服务管理
集团服务管理概述

最近更新时间：2024-03-06 18:52:29

集团服务管理是指支持与集团账号组合使用的其他腾讯云服务。集团账号允许集团服务管理访问集团账号中的成员、部门等信息。您可以使用管理账号或集团服务管理的委派管理员账号，在集团服务管理中基于组织进行业务管理，从而简化企业对云服务的统一管理。

集团服务管理使用流程

您可以通过**控制台或 API** 使用集团服务管理。下面以**控制台**为例说明使用流程。

1. 在 集团账号控制台 使用管理账号，开通集团账号。具体操作，请参见 创建集团组织 。
2. 在 集团账号控制台，使用管理账号，搭建企业的组织结构。您可以创建新的成员，也可以邀请已有的腾讯云账号加入组织。具体操作，请参见 创建部门 、添加组织成员 。
3. **（可选）**在 集团账号控制台，使用管理账号，将成员设置为集团服务管理的**委派管理员账号**。如果不设置集团服务管理的委派管理账号，则需使用管理账号在集团服务管理中进行业务管理。关于如何设置委派管理员账号，请参见 管理委派管理员账号 。

> **说明：**
> 该步骤仅适用于支持委派管理员的集团服务管理。

4. 在 集团账号控制台，使用管理账号或委派管理员账号，启用多账号管理功能。然后基于集团账号的组织结构选择需要统一管理的成员，并对已选中的成员进行业务管理。

启用或禁用集团服务管理

1. 您可以通过各集团服务管理的控制台或 API，启用或禁用集团服务管理。
2. 您可以在 集团服务管理 页面，查看集团服务管理的状态。但您不能在集团账号控制台上启用或禁用集团服务管理。
3. 有些集团服务管理会在您执行某些特定操作时，自动将集团服务管理状态更新为已启用。
4. 有些集团服务管理会在您执行某些特定操作时（例如：关闭一个功能时），自动将集团服务管理状态更新为已禁用。禁用集团服务管理意味着该集团服务管理不能再访问集团账号中的账号和资源，同时，该集团服务管理会删除本服务内与集团账号集成相关的全部资源。

集团服务管理与服务关联角色

1. 集团账号为每个成员创建了集团账号的服务关联角色（TencentCloudServiceRoleForOrganizations），该角色允许集团账号为集团服务管理创建服务所需角色的权限。该角色仅允许集团账号扮演。
2. 集团服务管理仅在需要执行管理操作的成员中创建集团服务管理的服务关联角色。该角色定义了允许集团服务管

理执行特定任务所需的权限。该角色仅允许对应的集团服务管理扮演。

3. 服务关联角色的权限策略由对应的云服务定义和使用，您不能修改或删除权限策略，也不能为服务关联角色添加或移除权限。

管理委派管理员账号

最近更新时间：2024-03-06 18:52:29

本文为您介绍委派管理员账号的定义、使用限制及基本操作。

什么是委派管理员账号

- 集团账号的管理账号可以将集团账号中的成员设置为集团服务管理的委派管理员账号。设置成功后，委派管理员账号将获得管理账号的授权，可以在对应集团账号管理中访问集团账号的组织和成员信息，并在该组织范围内进行业务管理。
- 通过委派管理员账号，可以将组织管理任务与业务管理任务相分离，管理账号执行集团账号的组织管理任务，委派管理员账号执行集团服务管理的业务管理任务，这符合安全最佳实践的建议。

使用限制

1. 委派管理员账号只能是集团账号的成员，不能是管理账号。
2. 集团服务管理允许添加的委派管理员账号数量由各集团服务管理定义。

添加委派管理员账号

1. 使用管理账号登录 集团账号控制台 。
2. 在左侧导航栏，选择 **集团账号** > 集团服务管理 。
3. 在**集团服务管理页面**，单击目标集团服务管理**操作**列的**新增**。
4. 在账号区域，**选中成员**。
5. 单击**确定**。

> **说明：**
> 添加成功后，使用该委派管理员账号访问对应集团服务管理的多账号管理模块，即可进行集团账号组织范围内的管理操作。

移除委派管理员账号

> **注意：**
> 移除操作可能会对集团服务管理的正常使用产生影响，请在移除前慎重考虑。

1. 使用管理账号登录 集团账号控制台 。
2. 在左侧导航栏，选择 **集团账号** > 集团服务管理 。
3. 在**集团服务管理**页面，单击目标集团服务管理**委派管理成员**列的**数字**。
4. 在**委派管理员**页面，单击目标账号**操作列的移除**。

5. 在移除警告对话框，单击**继续**。

> **说明：**
> 移除成功后，该账号将不能在集团服务管理中访问集团账号组织和成员信息。

成员审计
审计成员日志

最近更新时间：2024-03-06 18:55:02

集团账号管理员可通过操作审计的跟踪集，将组织各成员的日志投递到指定投递位置。

身份中心管理
身份中心简介
身份中心介绍

最近更新时间：2024-07-31 14:17:23

身份中心提供基于集团账号组织结构的多账号统一身份和权限管理。使用集团账号管理的身份中心功能，可以统一管理企业中使用腾讯云的用户，一次性配置企业身份管理系统与腾讯云的单点登录，并统一配置用户对多账号的访问权限。

功能特性

- **统一管理使用腾讯云的用户**

  身份中心为您提供用户管理模块，您可以在该模块中维护所有需要访问腾讯云的用户。您既可以手动管理用户与用户组，也可以借助 SCIM 协议从您的企业身份管理系统同步用户和用户组到身份中心中。
- **与企业身份管理系统进行统一配置单点登录**

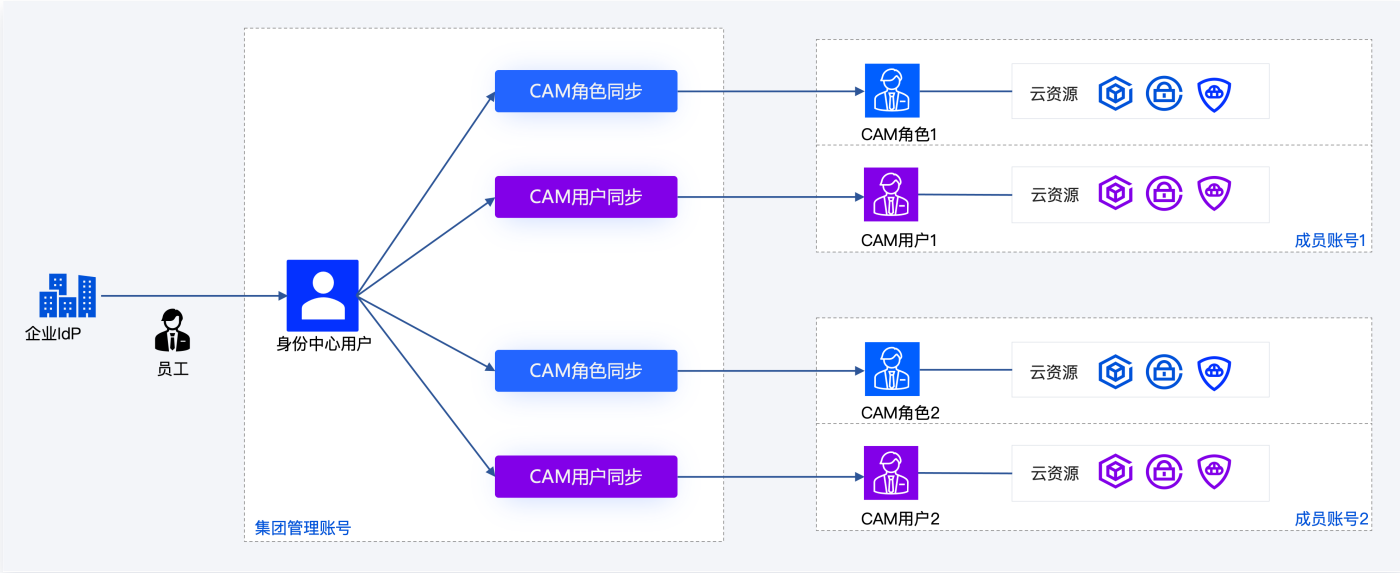
  身份中心支持基于 SAML 2.0协议的企业级单点登录，只需要在身份中心和企业身份管理系统中进行一次性配置，即可完成单点登录配置。
- **统一配置用户对多账号的访问权限**

  借助集团账号的组织结构，在身份中心中您可以统一配置用户或用户组对企业组织内任意成员账号的访问权限，且该权限可以随时修改和删除。
- **统一的登录门户**

  身份中心提供统一的登录门户，企业员工在登录门户可一站式获取其具有权限的所有账号列表，然后登录到腾讯云控制台，并可在多个账号间轻松切换。

产品架构

身份中心用户可以通过 **CAM 角色**或 **CAM 用户**访问账号的云资源。



说明：

同一个身份中心用户如果通过权限配置在账号上配置了 CAM 角色同步，同时又配置了 CAM 用户同步，则该身份中心用户可以通过 CAM 角色和 CAM 用户两种方式访问账号的云资源。

身份中心与访问管理（CAM）的关系

- 访问管理（CAM）提供单个腾讯云账号内的身份和权限管理。CAM 提供用户管理（包括用户、用户组和角色）、单点登录和权限配置，但这些仅局限在一个腾讯云账号内生效。当您的企业拥有多个腾讯云账号时，您需要在每个腾讯云账号中使用 CAM 单独管理用户、单独进行 SSO 配置和权限配置，这给管理工作带来极大的挑战。
- 身份中心在集团组织范围内提供多账号统一身份和权限管理。您可以在身份中心中进行一次性统一配置，即可完成面向多个腾讯云账号的用户管理、单点登录和权限配置。为了实现这一目标，身份中心提供了独立于 CAM 的身份管理，但其权限配置复用了 CAM 中的权限策略。此外，身份中心用户对账号的访问，本质上是身份中心用户扮演每个账号中的 CAM 角色进行的再一次单点登录。
- 当您开始使用身份中心进行集团账号统一的身份权限管理时，您将不再需要使用 CAM 来对单个账号进行管理。但是，在某些情况下，例如：您有已经存在的 CAM 用户、CAM 角色、或您需要使用访问密钥对腾讯云资源进行程序访问时，您仍然可以继续在单个账号内使用 CAM。使用身份中心不会限制 CAM 原来的功能，两个服务可以同时使用。

基本概念

最近更新时间：2024-07-31 14:17:23

本文为您介绍身份中心的基本概念。

概念	说明
空间	开通身份中心时需要创建一个空间，所有身份中心资源都在空间中维护。一个集团账号只能创建一个空间。空间名称将用在用户登录 URL 中。
用户	用户是身份中心中的一种身份类型，是指如果您开通集团账号的身份中心服务，您在身份中心新建的用户，在执行 CAM 同步操作前，身份中心的用户不具有任何功能、身份和登录、访问等权限。 您可以将所有访问腾讯云的用户统一在此创建和管理，用户可以被授予访问腾讯云账号的权限。
用户组	用户组是身份中心中的一种身份类型。您可以将用户加入用户组，然后按照用户组进行授权，方便统一权限管理。
SCIM 同步	身份中心支持基于 SCIM 协议的用户和用户组同步。使用 SCIM 同步，您只需在您的企业身份管理系统中管理身份，而不必在身份中心中手动管理用户、用户组及其成员关系，提升管理效率和安全性。
权限配置	权限配置是用户用来访问腾讯云账号的配置模板，包含权限集合。您可以使用该模板为用户针对账号进行授权。
账号	账号包括管理账号和成员账号。 • 管理账号：管理账号是企业组织的超级管理员，仅管理账号可管理身份中心。 • 成员账号：成员账号无法管理身份中心，且不可查看。
多账号授权	根据集团账号的组织结构，您可以为每个账号设置允许访问的用户或用户组，以及他们的访问权限。您可以为企业管理账号授权，也可以为任意一个成员账号授权。
权限配置部署	在为用户针对账号进行授权时，您指定的权限配置将会被部署到相关账号中，成为该账号中的 CAM 角色、CAM 策略和角色 SSO 登录的身份提供商。如果权限配置已经部署在账号中，但权限配置发生了变更，这些变更不会自动更新到对应的账号中，需要您手动重新部署才能使变更生效。
登录门户	登录门户是身份中心用户登录和使用腾讯云资源的独立门户。身份中心用户登录后，可以查看自己有权限访问的账号，并仅限在被授予权限允许的范围内访问腾讯云控制台。 您可以在身份中心的概览页面，查看登录门户的地址（URL）。
身份中心管理员	身份中心管理员是指开通身份中心的管理账号和其下具有权限（QcloudOrganizationFullAccess）的 CAM 用户。

单点登录（SSO）	身份中心支持基于 SAML 2.0的单点登录 SSO（Single Sign On）。腾讯云是服务提供商（SP），而企业自有的身份管理系统则是身份提供商（IdP）。通过单点登录，企业员工可以使用 IdP 中的用户身份直接登录身份中心。

身份中心使用案例
以腾讯云角色登录

最近更新时间：2025-07-09 17:16:01

本文提供一个示例，为身份中心的用户（user1）在成员账号（member_1）上部署权限配置 CVM-test，该权限配置定义了 CVM 相关的访问权限，实现身份中心的用户（user1）仅能访问成员账号（member_1）中的 CVM 资源。

操作步骤

步骤一：企业员工录入

将企业员工录入身份中心的用户管理中，即新建身份中心用户，目前支持手动创建、SCIM 同步 。以下示例为通过手动创建用户：

1. 进入**集团账号管理** > 身份中心 。
2. 在左侧导航栏，选择**用户管理 > 用户**，单击**新建用户**。
3. 在**新建用户**面板，设置用户基本信息，详细操作请参见 新建用户 。

> **说明：**
> 本示例用户名设置为 **user1**。

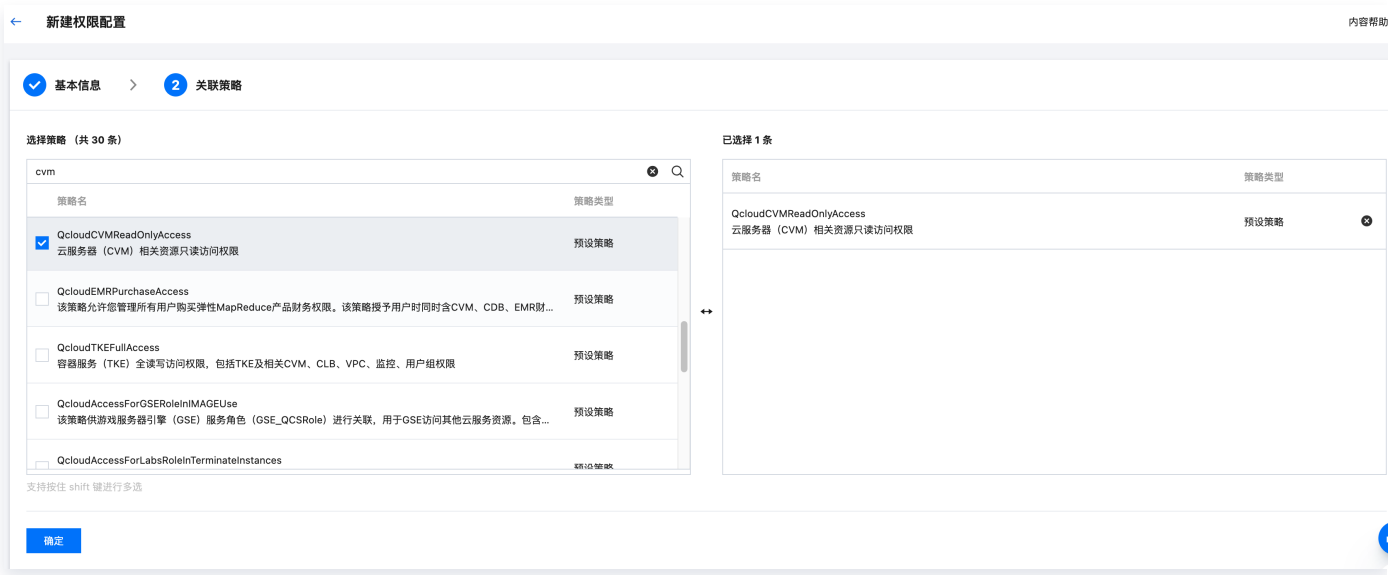
步骤二：配置权限

配置 CAM 角色同步前，需要先配置权限，权限部署到成员账号后，对应成员账号会自动生成一个 CAM 角色，角色的命名方式为 TencentCloudSSO-权限名称。

1. 在左侧导航栏，单击 **CAM 同步 > 权限配置**。
2. 在**权限配置**页面，单击**新建权限配置**。
3. 在**新建权限配置**页面，配置以下基本信息，然后单击**下一步**。

- **权限名称**：必选参数。在空间内必须唯一。此处配置 **CVM-test**。
- **权限描述**：可选参数。权限配置的描述信息。

4. 配置关联策略，按需勾选**预设策略**。此处勾选 CVM 相关资源只读访问权限的预设策略。



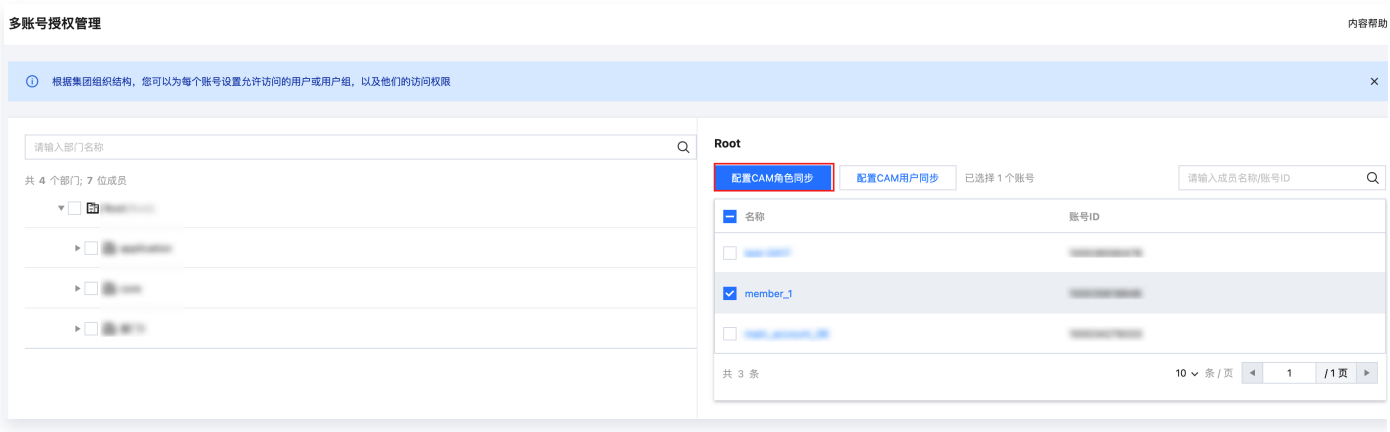
5. 单击**确定**，创建成功。

步骤三：配置 CAM 角色同步

1. 左侧导航栏，单击 **CAM 同步 > 多账号授权管理**。
2. 在**多账号授权管理**页面，选择目标账号。

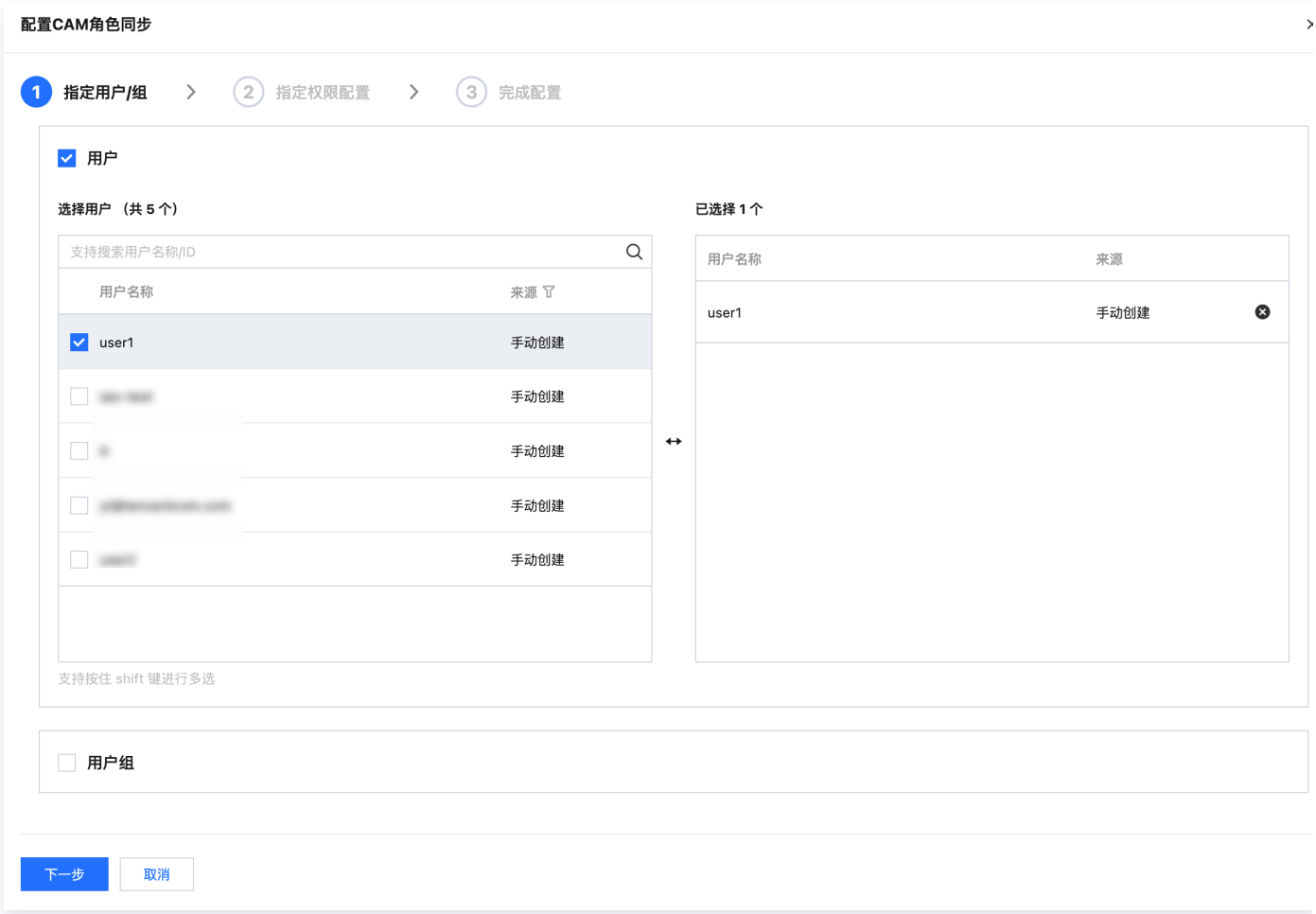
> **说明：**
> 本示例中，选择成员账号（menber_1）。

3. 单击**配置 CAM 角色同步**。



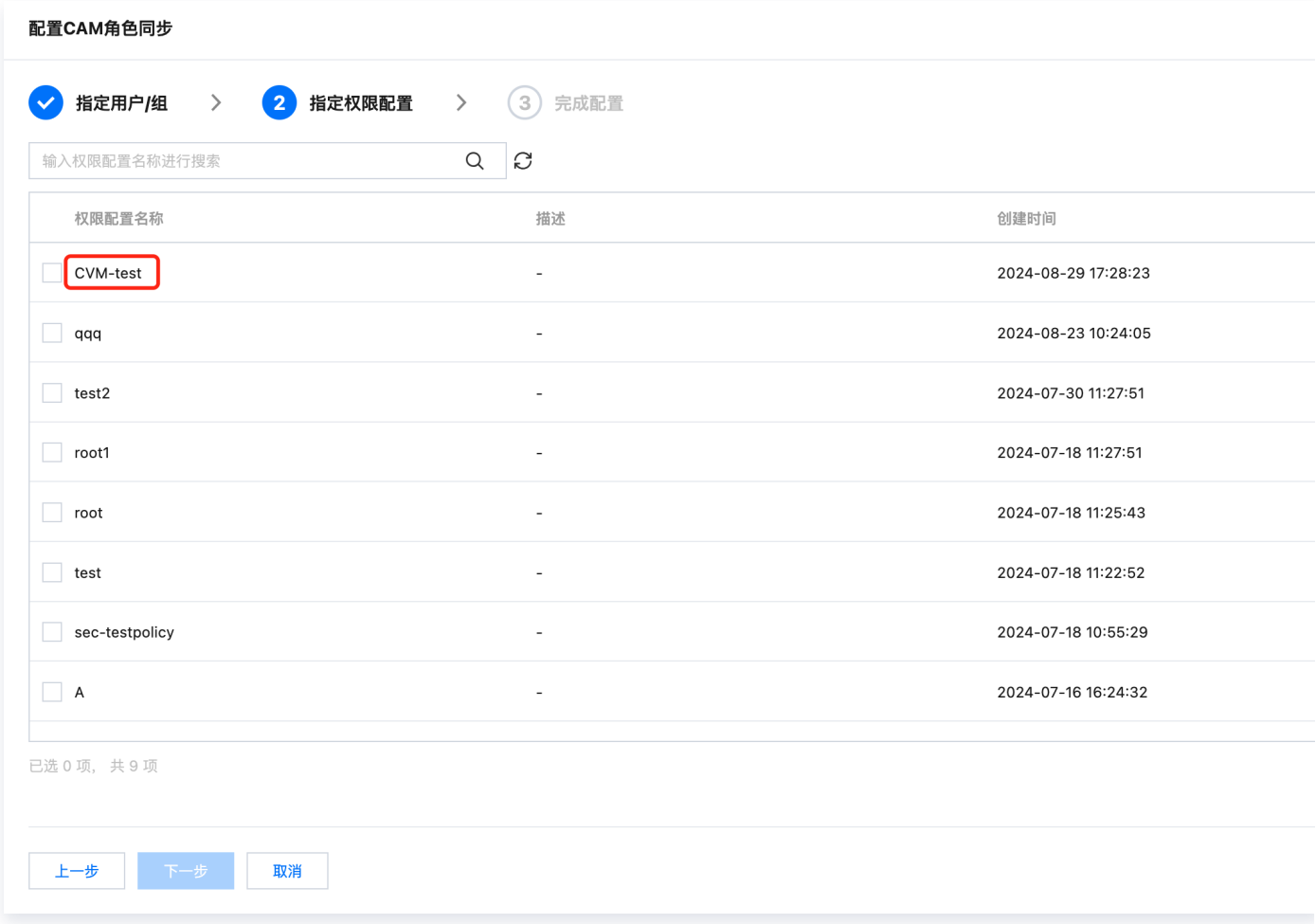
4. 在**配置 CAM 角色同步**页面，选择目标用户或用户组，单击**下一步**。

> **说明：**
> 本示例中，选择用户（user1）。



5. 选择目标**权限配置**，单击**下一步**。

> **说明：**
> 本示例中，选择（CVM-test）。



6. 浏览配置信息，然后单击**提交**。

7. 等待配置，配置成功后，单击**完成**。
8. 配置完成后，可以在**用户管理 > 用户**，user1 的用户详情页的**权限**页签中查看。

CAM 中的效果

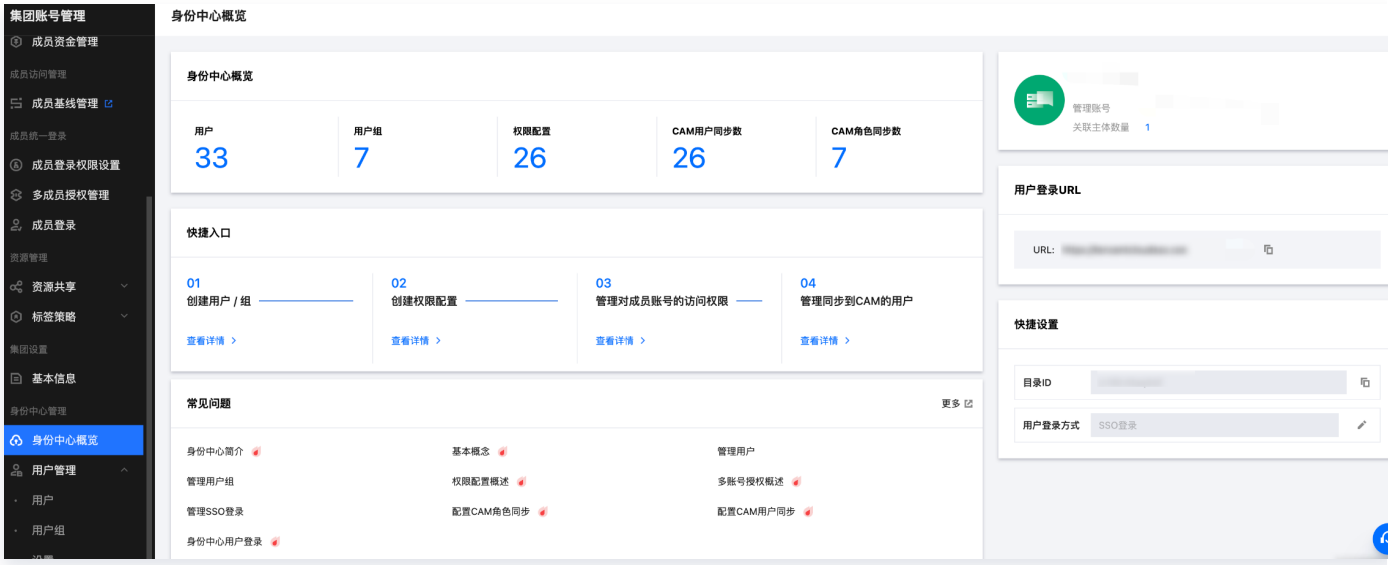
1. 配置成功后，系统会自动在成员账号（member_1）中同步创建一个角色（TencentCloudSSO-CVM-test），您可前往 角色 页面查看。

2. 在**角色**页面，您可单击目标角色名称，查看关联策略。

步骤四：角色登录

获取用户登录 URL

1. 在左侧导航栏，单击**身份中心概览**。
2. 在概览页面的右侧，查看或复制**用户登录 URL**。

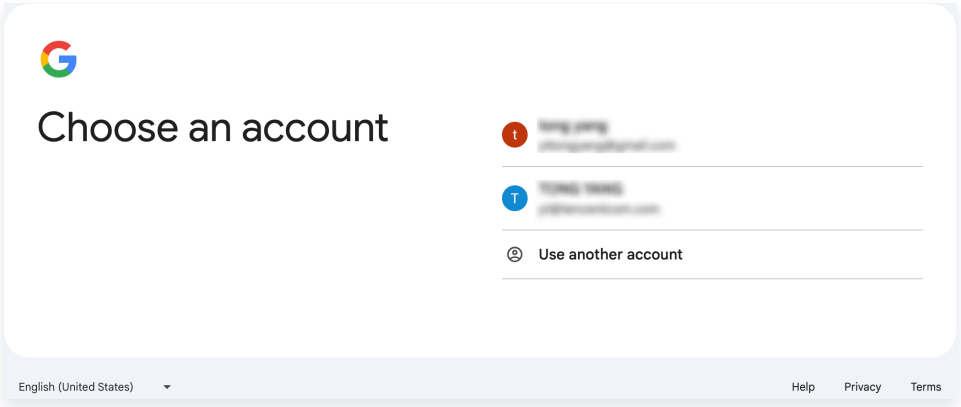


在浏览器中访问用户 URL

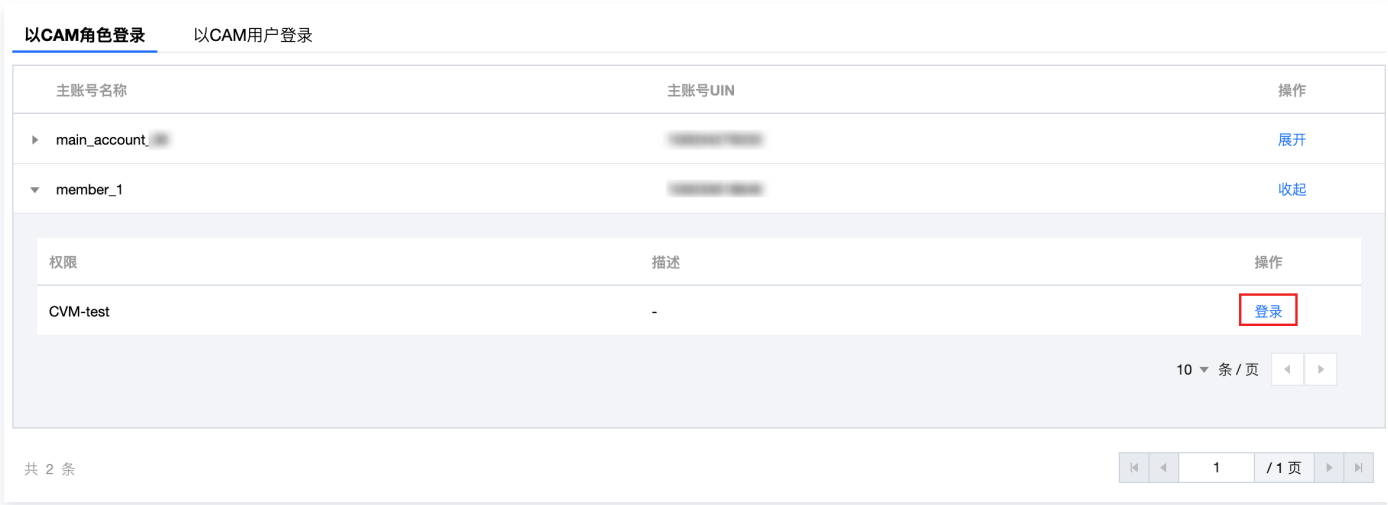
1. 在身份中心登录页面，单击**登录**。本示例使用 SSO 登录方式。

> **说明：**
> 当前支持**用户名密码登录**和 **SSO 登录**。具体登录方式，请参见 身份中心用户登录 。

2. 系统自动跳转到**企业 IdP 的登录页面**，本示例使用的是谷歌 IdP。



3. 验证通过后，进入**CAM 角色登录页签**，展开成员账号（member_1）列表，选择权限（CVM-test）登录。


以CAM角色登录
以CAM用户登录
主账号名称
主账号UIN
操作
main_account_
展开
member_1
收起
权限
描述
操作
CVM-test
-
登录
10 条 / 页
共 2 条
1
/ 1 页

以腾讯云子账号登录

最近更新时间：2025-07-09 17:16:02

本文提供一个示例，通过配置 CAM 用户同步，在成员账号（member_1）中创建一个与身份中心用户（user1）同名的 CAM 子账号（user1）。
通过 CAM 用户同步的子账号，**不授予任何权限**，需要在成员账号的 CAM 控制台对用户授权。
如果需要通过身份中心预设权限，请您选择 配置 CAM 角色同步 。

操作步骤

步骤一：企业员工录入

将企业员工录入身份中心的用户管理中，即新建身份中心用户，目前支持手动创建、SCIM 同步 。以下示例为通过手动创建用户：

1. 进入**集团账号管理** > 身份中心 。
2. 在左侧导航栏，选择**用户管理 > 用户**，单击**新建用户**。
3. 在**新建用户**面板，设置用户基本信息，详细操作请参见 新建用户 。

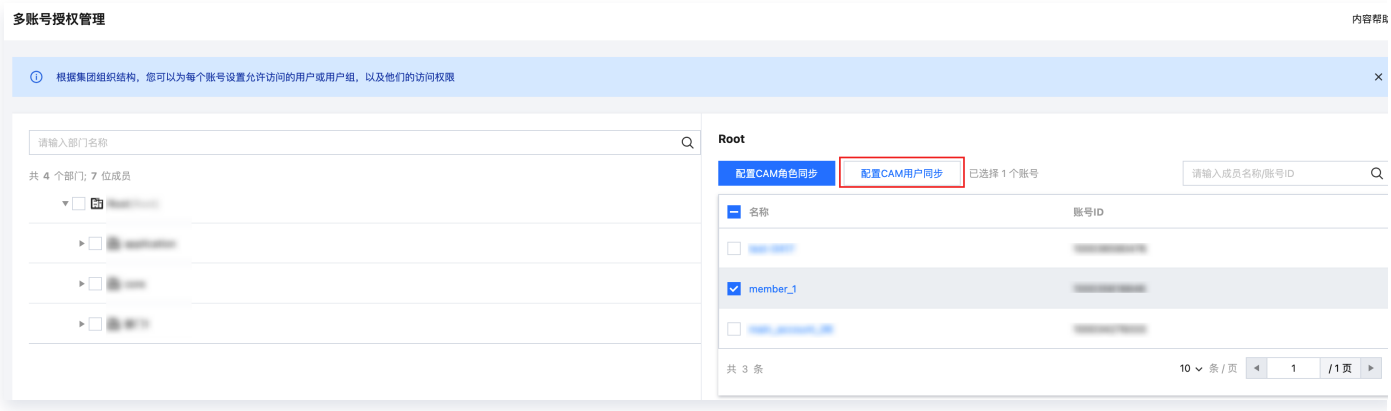
> **说明：**
> 本示例用户名设置为 **user1**。

步骤二：配置 CAM 用户同步

1. 在左侧导航栏，单击 **CAM 同步 > 多账号授权管理**。
2. 在**多账号授权管理**页面，选择目标账号。

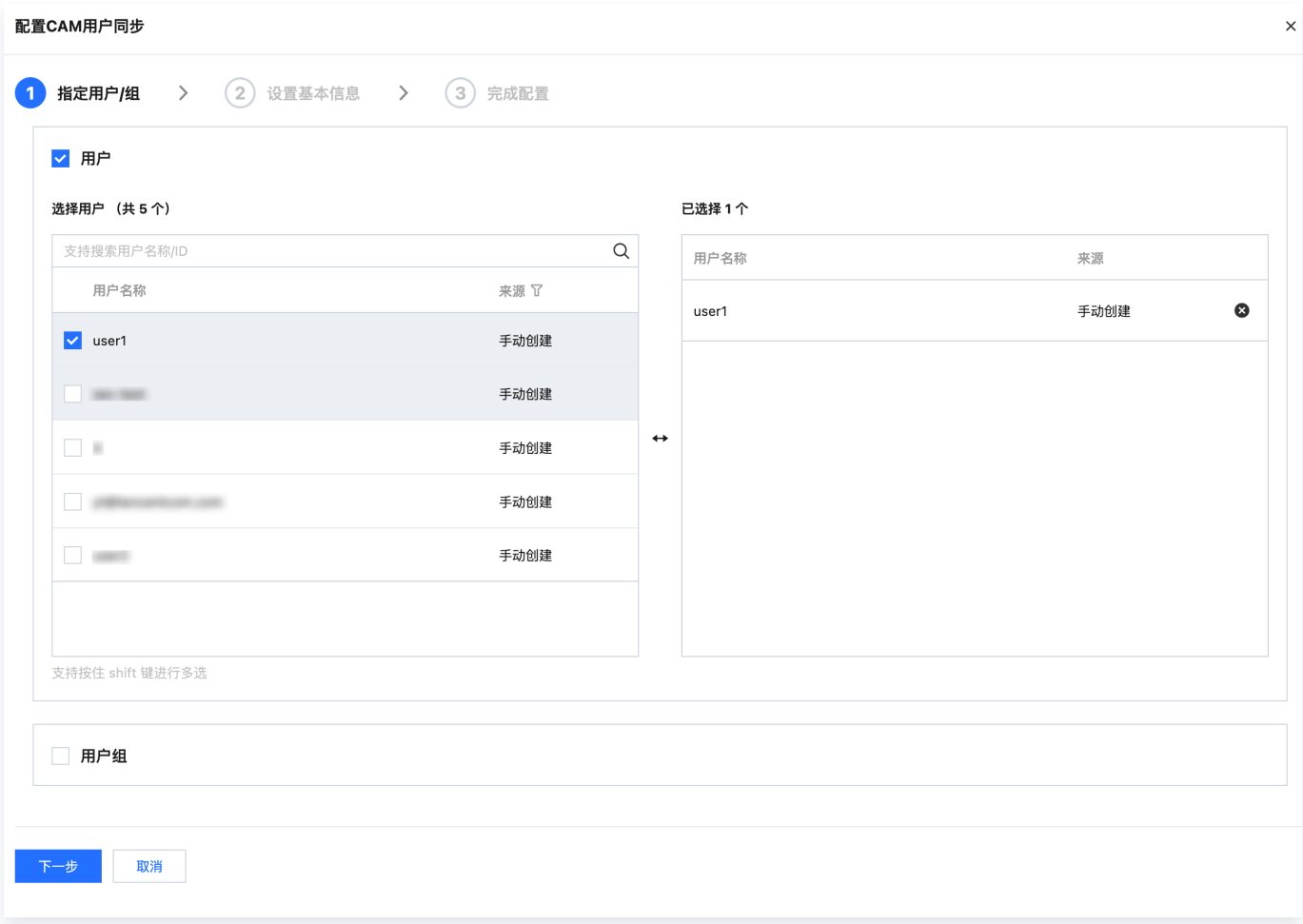
> **说明：**
> 本示例中，选择成员账号（member_1）。

3. 单击**配置 CAM 用户同步**。



4. 在**配置 CAM 用户同步**面板，选择目标用户或用户组，单击**下一步**。

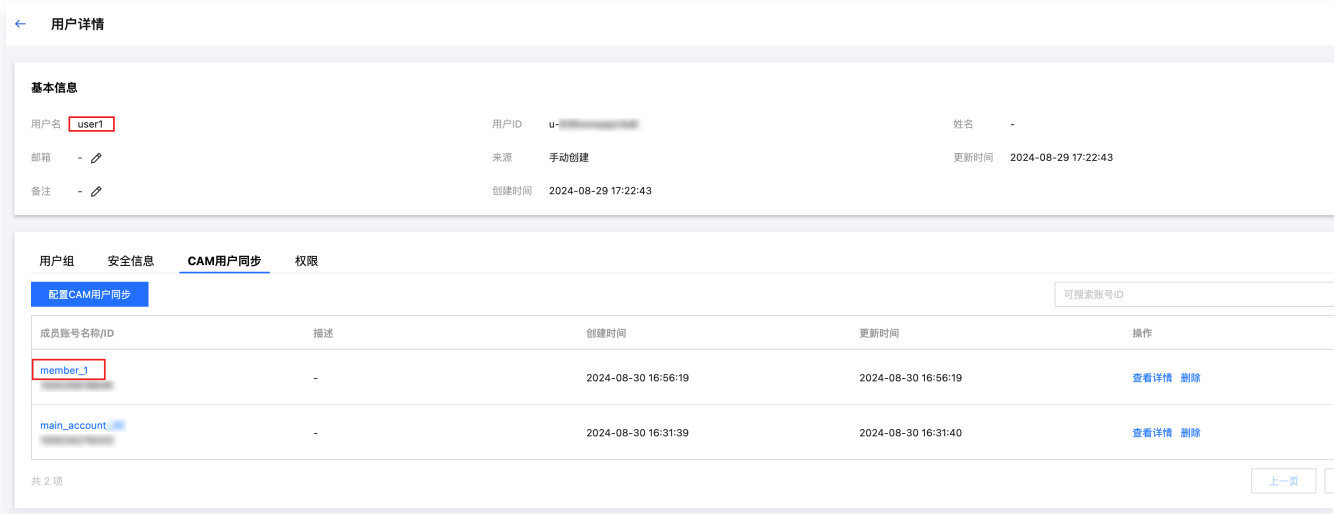
> **说明：**
> 本示例中，选择身份中心用户（user1）。



5. 设置基本信息，基本信息的具体说明，请参见 配置 CAM 用户同步 。填写完成后，单击**下一步**。

6. 单击**提交**，提示配置成功后，单击**完成**。
7. 配置成功后：
   - 可在 **CAM 同步 > 用户同步管理**中，查看用户同步列表。

   - 或在**用户管理 > 用户**，user1 的用户详情页的 **CAM 用户同步**页签中查看。



CAM 中的效果

1. 配置成功后，系统会自动在成员账号（member_1）中同步创建一个与身份中心用户（user1）同名的 **CAM 子用户**（user1）。

> **说明：**
> CAM 中的用户类型为**身份中心同步用户**。

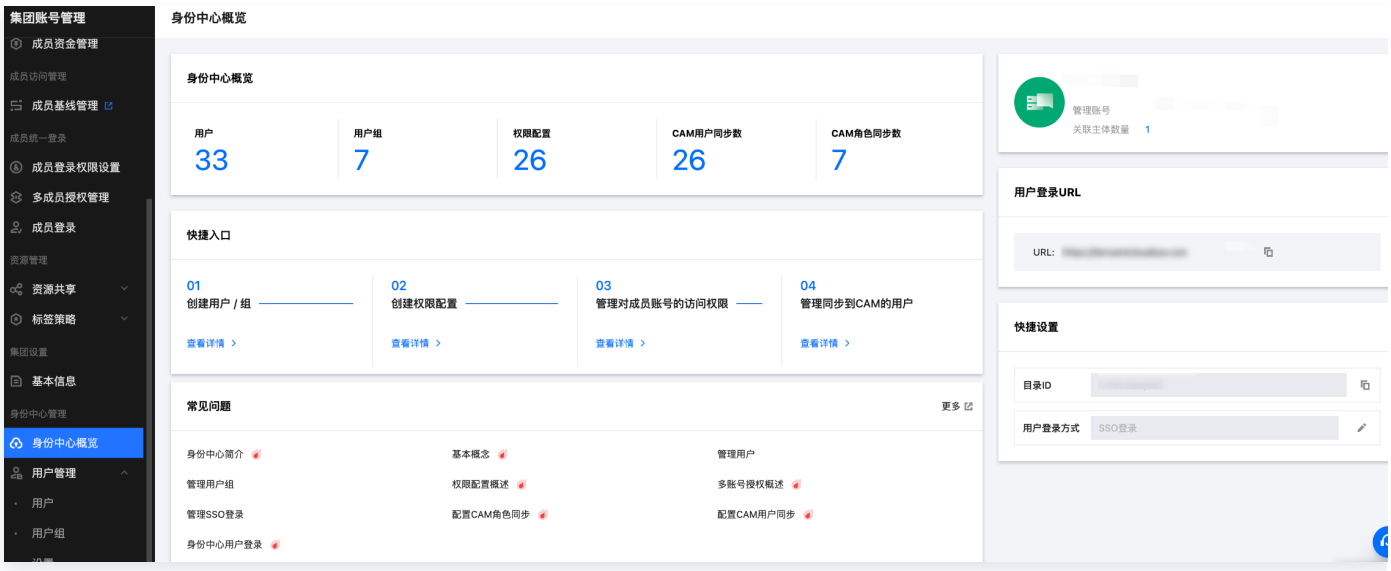
2. 单击目标用户名称，可查看关联策略。

> **注意：**
> 同步创建的子用户**无任何权限**，需要您在 CAM 中为用户（user1）配置权限策略。

步骤三：子账号登录

获取用户登录 URL

1. 在左侧导航栏，单击**身份中心概览**。
2. 在概览页面的右侧，查看或复制**用户登录 URL**。



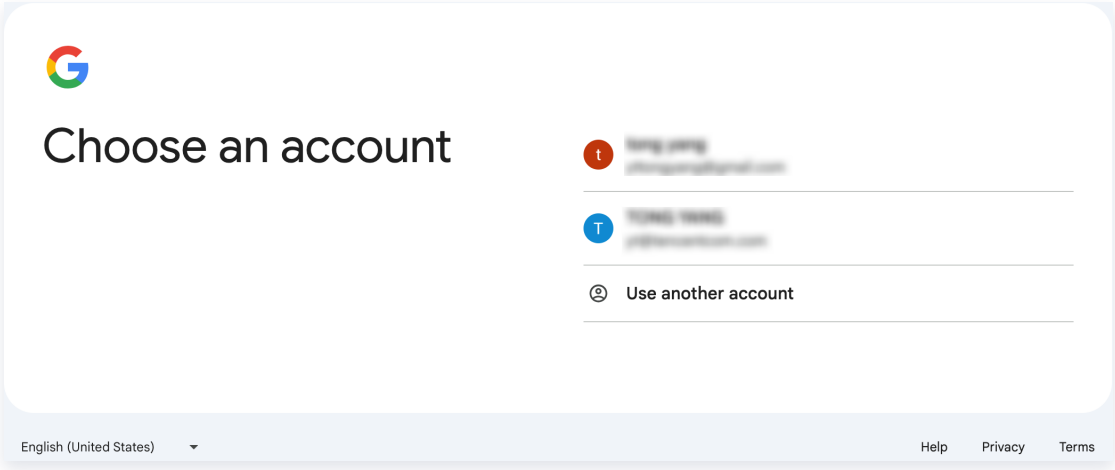
在浏览器中访问用户 URL

1. 在身份中心登录页面，单击**登录**。本示例使用 SSO 登录方式。

> **说明：**

> 当前支持**用户名密码登录**和 **SSO 登录**。具体登录方式，请参见 身份中心用户登录 。

2. 系统自动跳转到**企业 IdP 的登录页面**，本示例使用的是谷歌 IdP。



3. 验证通过后，进入以 **CAM 用户登录页签**，选择成员账号（member_1）登录。


以CAM角色登录
以CAM用户登录
主账号名称
主账号UIN
子用户名称
子用户UIN
main_account_06
member_1
10
条 / 页

开通服务

最近更新时间：2024-07-31 14:17:23

身份中心需要开通才能使用，开通后您可以免费使用本服务。

前提条件

已开通了集团账号服务，并搭建了企业的多账号组织结构。
只能使用集团账号的管理账号或管理账号下具有权限的 CAM 用户才能开通身份中心。具体如下：

- 管理账号（主账号）
- CAM 用户（子账号）
  您需要为管理账号中的 CAM 用户授予预设策略 QcloudOrganizationFullAccess。具体操作，请参见 子用户权限设置 。

操作步骤

1. 登录 集团账号管理控制台 。
2. 在集团账号管理控制台的目录中，单击**身份中心概览**。
3. 在**身份中心概览**页面中，单击**立即开通**。
4. 开通时，填写**空间名称**，名称必须全局唯一。
   - 空间名称后续会用在用户登录 URL 中，不可修改。
   - 创建空间的过程中，身份中心会自动创建服务相关角色（Orgnization_QCSLinkedRoleInCIC），用于访问您在其他云服务中的资源。
5. 单击**确定**。

管理用户

最近更新时间：2025-07-09 17:16:02

操作场景

本文为您介绍管理用户的基本操作，包括新建用户、查看用户信息、修改用户基本信息、删除用户、启用或禁用用户和重置用户密码。

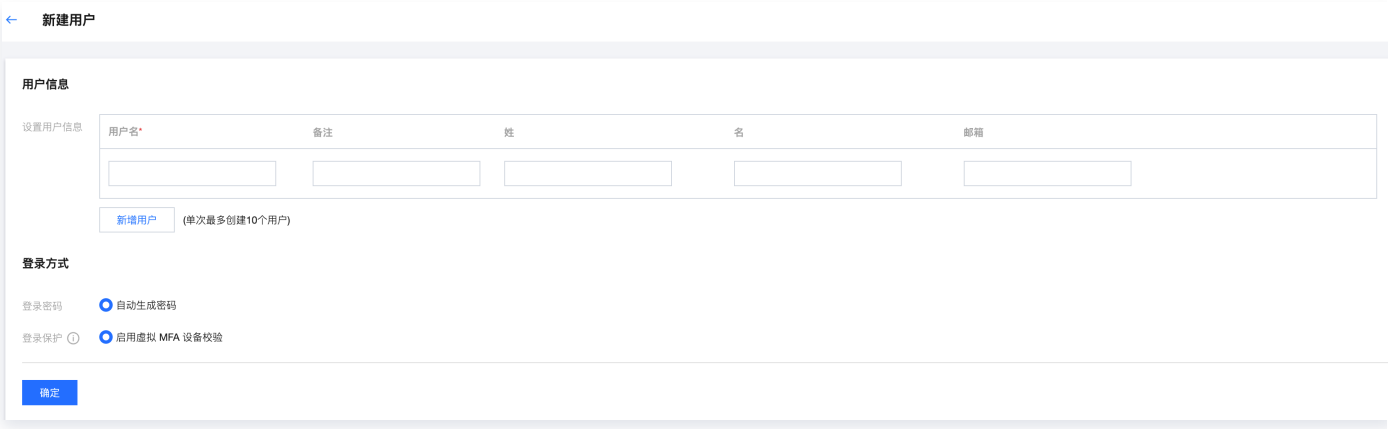
前提条件

已登录**集团账号管理** > 身份中心 。

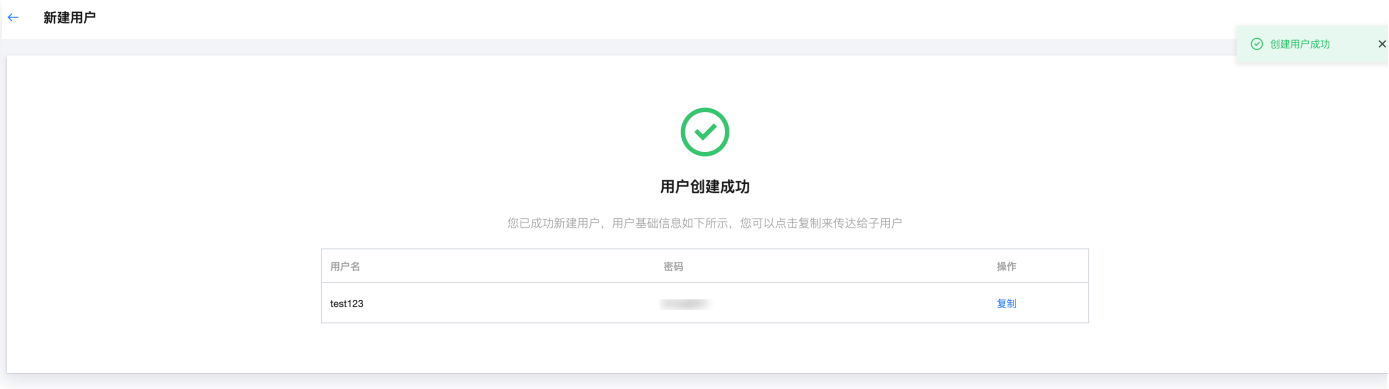
操作步骤

新建用户

1. 在左侧导航栏，选择**用户管理** > **用户**。
2. 在**用户**列表页面，单击**新建用户**。
3. 在**新建用户**面板，设置用户基本信息。



   - 用户信息：
     - **用户名**：必选，在空间内必须唯一。用户名可包含英文字母、数字和+=,.@-_字符，最大长度 64 个字符。
     - **备注、姓、名、邮箱**：可选，您可以按需输入。
   - 登录方式：
     - **登录密码**：仅支持系统自动生成密码。
     - **登录保护**：默认启用虚拟 MFA 设备校验。
4. 单击**确定**。



5. 用户创建成功后，在**操作**列单击**复制**，保存用户名密码信息。如需修改密码，请参见 重置用户密码 。

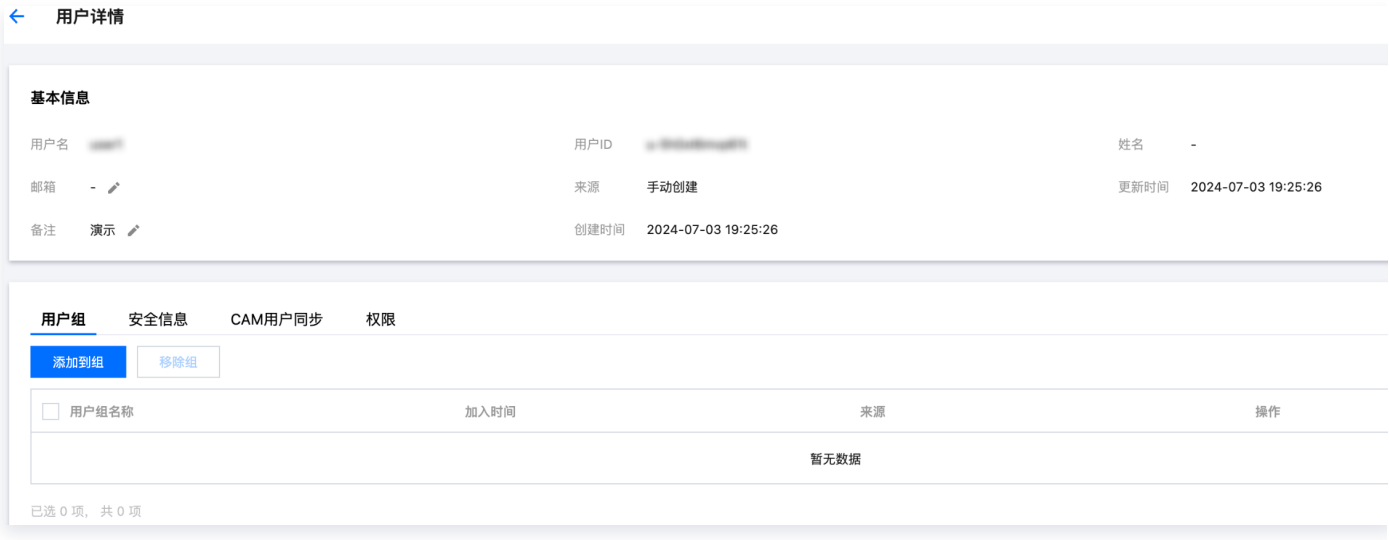
查看用户信息

1. 在左侧导航栏，选择**用户管理 > 用户**。
2. 在**用户列表**页面，单击目标用户名称，查看用户的以下信息：
   - 查看用户基本信息。
   - 单击**用户组**页签，查看用户加入的用户组。
   - 单击**安全信息**页签，查看用户的启用状态。
   - 单击 **CAM 用户同步**页签，查看配置的 CAM 用户同步信息。关于 CAM 用户同步的更多信息，请参见 多账号授权概述 。
   - 单击**权限**页签，查看用户关联的账号及权限配置信息。

修改用户基本信息

> **说明：**
> 用户名不支持修改。

1. 在左侧导航栏，选择**用户管理 > 用户**。
2. 在**用户列表**页面，单击目标用户名称。
3. 在用户**详情**页面的**基本信息**区域，可修改的字段为：**备注**、**邮箱**。



删除用户

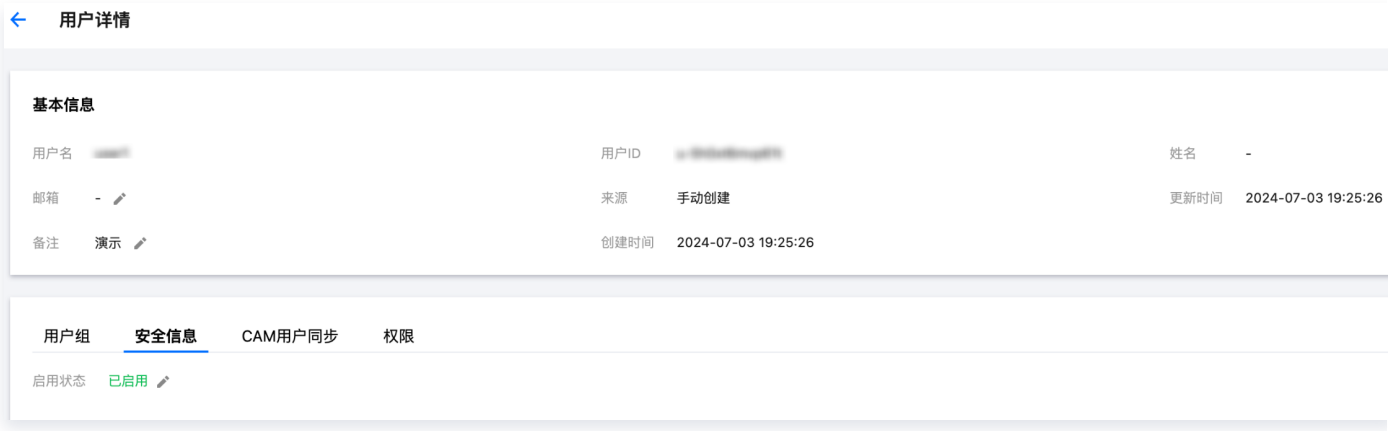
> **注意：**
> 删除用户前，请确保用户未关联以下资源，否则会删除失败。具体内容如下：
> - 用户组：您需要将用户从用户组中移除。具体操作，请参见 从用户组移除用户 。
> - 权限：您需要删除用户在账号上的授权。具体操作，请参见 查看/修改/删除授权 。
> - CAM 用户同步：您需要删除用户在账号上的同步关系。具体操作，请参见 查看/修改/删除用户同步 。

1. 在左侧导航栏，选择**用户管理 > 用户**。
2. 在**用户**列表页面，单击目标用户操作列的**删除**。
3. 在**删除用户**页面中，单击**确定**。

启用或禁用用户登录

> **警告：**
> 处于禁用状态的用户，将不能正常登录身份中心的登录门户。

1. 在左侧导航栏，选择**用户管理 > 用户**。
2. 在**用户列表**页面，单击目标用户名称。
3. 在详情页的**安全信息**区域，启用或禁用用户登录。



- 启用用户登录

  在**管理用户状态**弹窗，单击**已启用**后，单击**确定**。
- 禁用用户登录

  在**管理用户状态**弹窗，单击**已禁用**后，单击**确定**。

重置用户密码

1. 在左侧导航栏，选择**用户管理 > 用户**。
2. 在**用户列表**页面，单击目标用户名称。
3. 在**用户详情**页面的**安全信息**区域，单击**重置密码**，重置时支持**自定义密码**。

   - 密码格式：长度为8–32 个字符，包含大写字母，小写字母，数字，特殊字符（除空格）。
4. 重置成功后，可以在弹窗中复制新密码，或者**下载 .csv**。

管理用户组

最近更新时间：2024-12-30 14:42:06

操作场景

本文为您介绍用户组的基本操作，包括新建用户组、查看用户组信息、修改用户组基本信息、删除用户组、为用户组添加用户和从用户组移除用户。

前提条件

已登录**集团账号管理** > 身份中心 。

操作步骤

新建用户组

1. 在左侧导航栏，选择**用户管理** > **用户组**。
2. 在用户组页面，单击**新建用户组**。
3. 在**新建用户组**面板，输入**用户组名称**。

   用户组名称在空间内必须唯一。
4. 输入**备注**信息。
5. 单击**确定**。

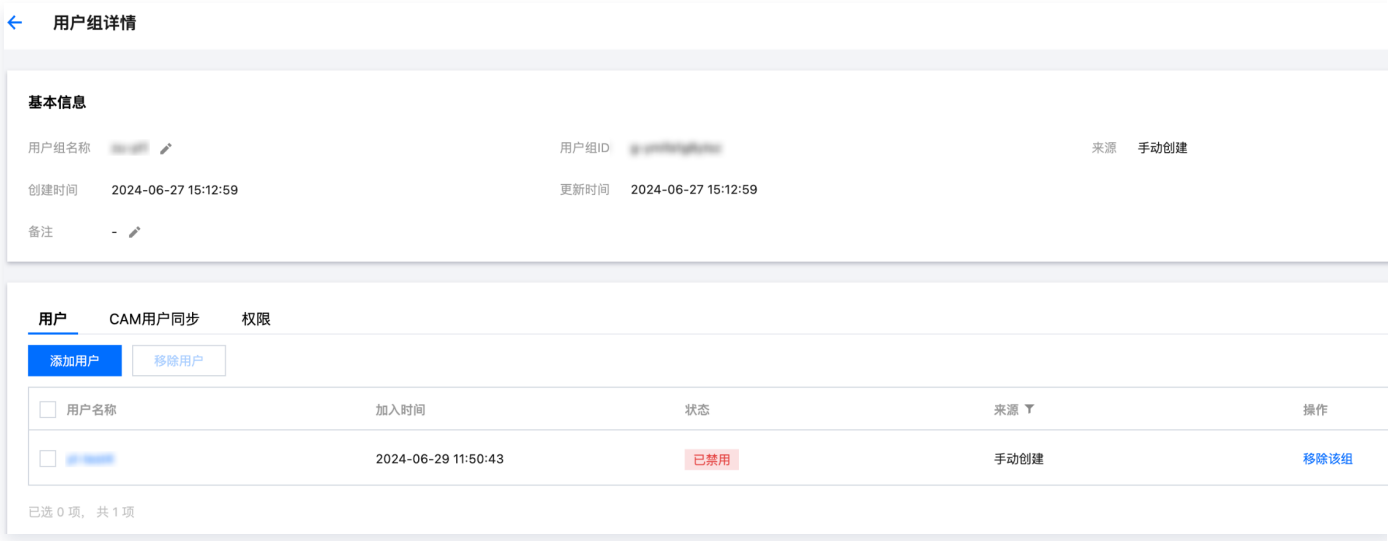
查看用户组信息

在**用户组**列表页，单击目标用户组名称，查看用户组的以下信息：

- 查看用户组基本信息。
- 单击**用户**页签，查看用户组中的用户。
- 单击**CAM用户同步**页签，查看配置的CAM用户同步信息。
- 单击**权限**页签，查看用户组关联的账号和权限配置信息。

修改用户组信息

1. 在**用户组**列表页，单击目标用户组名称。
2. 在用户组**详情**页顶部**基本信息**区域，可修改的字段为：**用户组名称**和**备注**。



删除用户组

> **注意：**
> 删除用户组前，请确保用户组未关联以下资源，否则会删除失败。具体如下：
> - 用户：您需要移除用户组中的用户。
> - 权限：您需要删除用户组在账号上的授权。
> - CAM用户同步：您需要删除用户组在账号上的同步关系。

1. 在**用户组**页面，单击目标用户组**操作**列的**删除**。

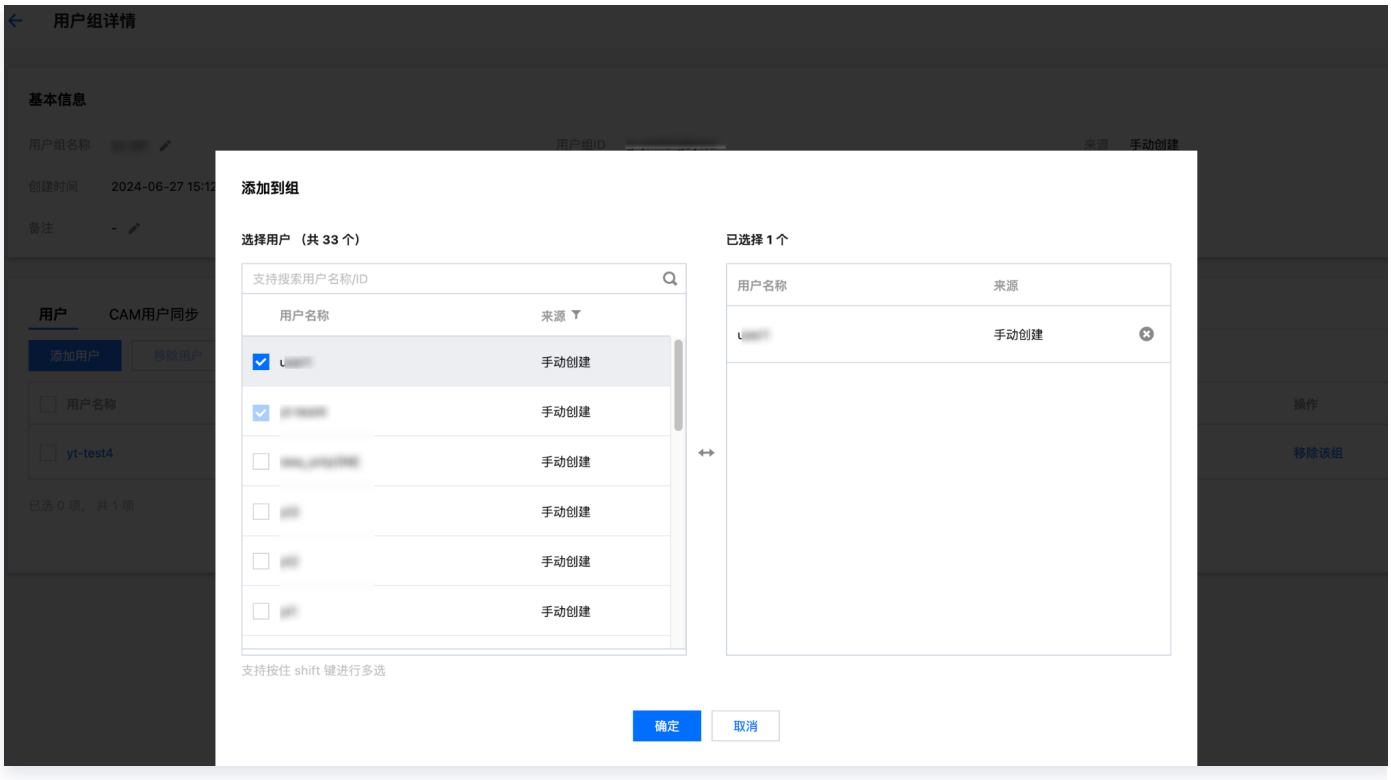
2. 在**删除用户组**对话框，单击**确定**。

为用户组添加用户

1. 在**用户组**页面，单击目标用户组名称。
2. 单击**用户**页签，然后单击添加用户。

3. 在添加到组面板，选择用户。

> **说明：**
> 一个用户可以加入多个用户组。



4. 单击**确定**。

从用户组移除用户

1. 在**用户组**页面，单击目标用户组名称。
2. 单击**用户**页签。
3. 单击目标用户**操作**列的**移除该组**。
4. 在移除用户对话框，单击**确定**。

设置
SCIM 同步
管理 SCIM 密钥

最近更新时间：2024-11-27 14:46:26

操作场景

SCIM 同步过程中需要使用 SCIM 密钥。本文为您介绍如何创建、禁用、启用和删除 SCIM 密钥的操作。

使用限制

- SCIM 密钥只在创建时显示，不支持查询，**请您及时保存 SCIM 密钥**。
- 最多可创建2个 SCIM 密钥。

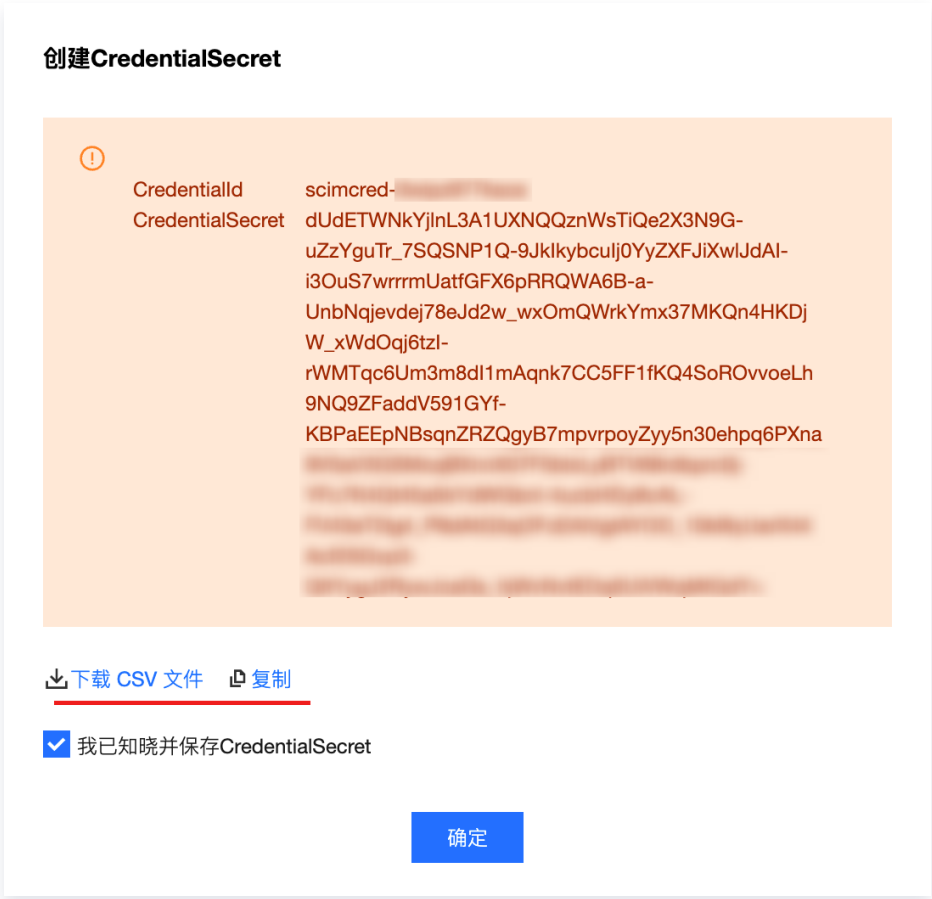
创建 SCIM 密钥

> **说明：**
> 新创建的 SCIM 密钥，默认处于启用状态。

1. 登录集团账号管理 > 身份中心 。
2. 在左侧导航栏，单击**用户管理** > **设置**。
3. 在 **SCIM 用户同步配置**区域，单击**生成新的 SCIM 密钥**。

> **说明：**
> 若您未开启 **SCIM 用户同步**，请您先开启。

4. 在**创建 CredentialSecret** 对话框中，您可以通过**下载 CSV 文件**或**复制**来保存 SCIM 密钥。保存好密钥后，单击**确定**。

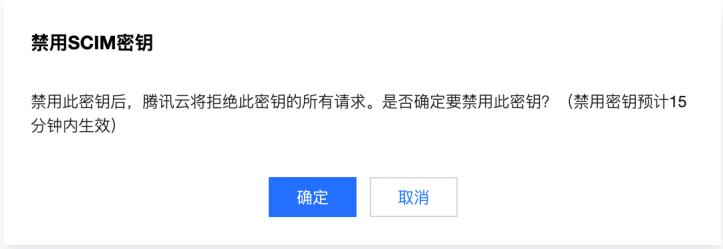


禁用 SCIM 密钥

> **警告：**
> 禁用后，使用该 SCIM 密钥的同步任务将会失败。

1. 登录集团账号管理 > 身份中心 。
2. 在左侧导航栏，单击**用户管理** > **设置**。
3. 在 **SCIM 用户同步配置**区域，单击目标 SCIM 密钥的**禁用**。

4. 在**禁用SCIM 密钥**对话框，单击**确定**。



启用 SCIM 密钥

对于处于禁用状态的 SCIM 密钥，您可以将其再次启用。

1. 登录集团账号管理 > 身份中心 。
2. 在左侧导航栏，**用户管理** > **设置**。
3. 在 **SCIM 用户同步配置**区域，单击目标 SCIM 密钥的**启用**。

4. 在**启用SCIM 密钥**对话框，单击**确定**。

删除 SCIM 密钥

对于确定不再使用的 SCIM 密钥，您可以将其删除。

> **警告：**
> 删除后，该 SCIM 密钥不可再使用。

1. 登录集团账号管理 > 身份中心 。
2. 在左侧导航栏，**用户管理** > **设置**。
3. 在 **SCIM 用户同步配置**区域，单击目标 SCIM 密钥的**删除**。

4. 在**删除 SCIM 密钥对话框**，单击**确定**。

启用或禁用 SCIM 同步

最近更新时间：2024-11-27 14:46:26

操作场景

您可以从支持 SCIM 2.0的外部 IdP 同步用户或用户组到身份中心。本文为您介绍如何获取 SCIM 服务端地址、启用 SCIM 同步、禁用 SCIM 同步的具体操作。

获取 SCIM 服务端地址

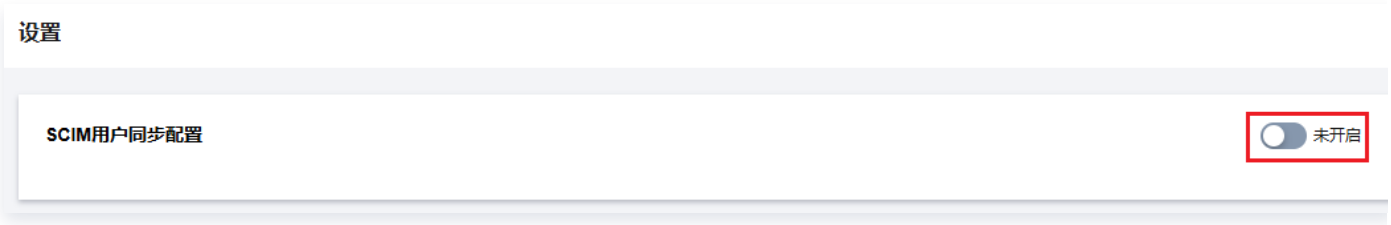
1. 登录集团账号管理 > 身份中心 。
2. 在左侧导航栏，单击**用户管理** > **设置**。
3. 在 **SCIM 用户同步配置**区域，查看或复制 **SCIM 服务端地址**，在外部 IdP 中配置 SCIM 同步时会使用该地址。
   - 中国站：https://scim.tencentcloudsso.com/scim/v2
   - 国际站：https://scim.tencentcloudssointl.com/scim/v2

启用 SCIM 同步

启用 SCIM 同步后，您才能从外部 IdP 同步用户或用户组到身份中心。同时，您还需要创建 SCIM 密钥。

1. 登录集团账号管理 > 身份中心 。
2. 在左侧导航栏，单击**用户管理** > **设置**。
3. 在 **SCIM 用户同步配置**区域，单击 ，在弹出的窗口单击开启，启用 SCIM 同步。

> **说明：**
> 在 SCIM 开启状态下，对于已同步到身份中心的 SCIM 用户和用户组，您不能修改和删除，也不能为 SCIM 用户组添加或移除用户。



禁用 SCIM 同步

禁用 SCIM 同步的影响如下：

- 您将不能从外部 IdP 同步用户或用户组到身份中心。
- 对于已同步到身份中心的 SCIM 用户和用户组，您可以修改或删除它们。

> **说明：**
> 如果您再次启用 SCIM 同步，身份中心中已修改的 SCIM 用户或用户组属性可能会被自动修改回去；已删除的 SCIM 用户可能会被重新创建出来。

1. 登录集团账号管理 > 身份中心 。
2. 在左侧导航栏，单击**用户管理** > **设置**。
3. 在 **SCIM 用户同步配置**区域，单击 ，在弹出的窗口单击关闭，禁用 SCIM 同步。

SCIM 同步示例
通过 SCIM 同步 Microsoft Entra ID(Azure AD) 示例

最近更新时间：2025-09-11 11:00:19

本文为您介绍通过 SCIM 协议，将 Microsoft Entra ID（即 Azure AD）中的用户或用户组同步到腾讯云身份中心。

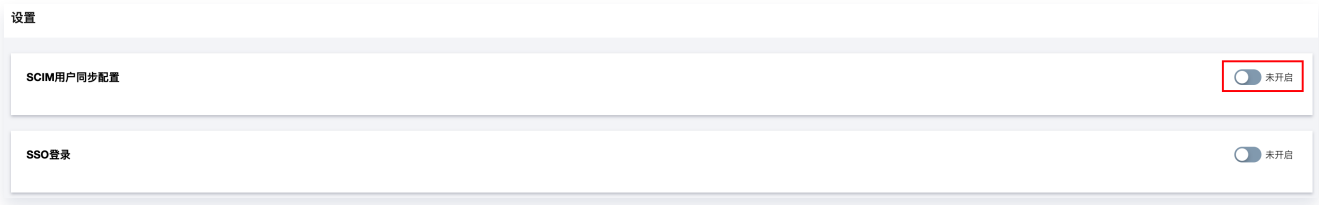
背景信息

Microsoft Entra ID 中的所有配置操作需要管理员（已授予全局管理员权限）执行。关于如何在 Microsoft Entra ID 中创建用户及授权为管理员的操作，请参见 Microsoft Entra 文档 。

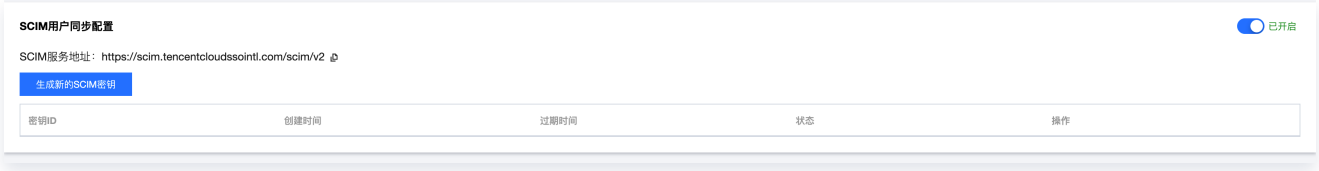
在身份中心配置

步骤一：开启 SCIM 同步

1. 登录集团账号管理 > 身份中心 。
2. 在左侧导航栏，单击**用户管理** > **设置**。
3. 在 **SCIM 用户同步配置**区域，单击，在弹出的窗口单击开启，启用 SCIM 同步。



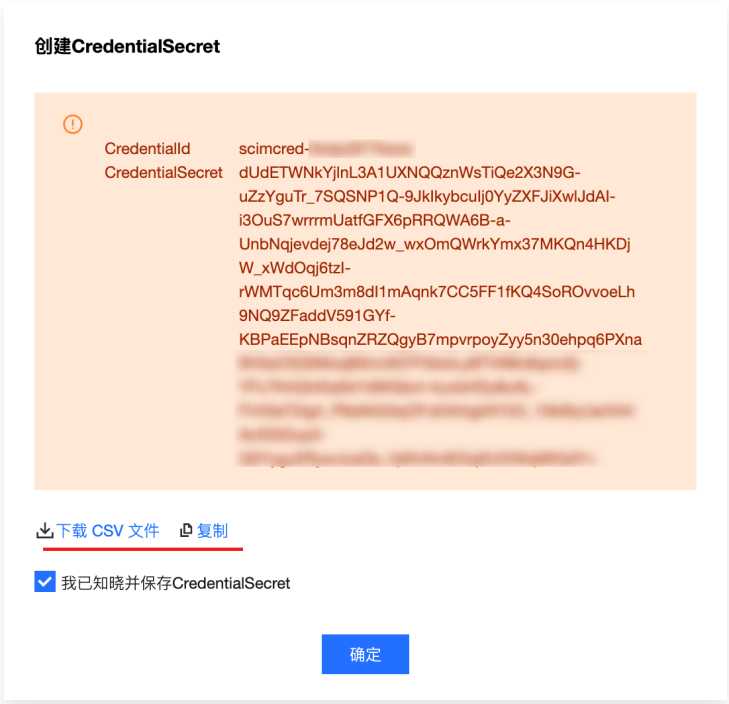
4. 启用后，在 **SCIM 用户同步配置**区域，查看或复制 **SCIM 服务端地址**，在外部 IdP 中配置 SCIM 同步时会使用该地址。
   - 中国站：https://scim.tencentcloudsso.com/scim/v2
   - 国际站：https://scim.tencentcloudssointl.com/scim/v2



步骤二：创建 SCIM 密钥

1. 在 **SCIM 用户同步配置**区域，单击**生成新的 SCIM 密钥**。

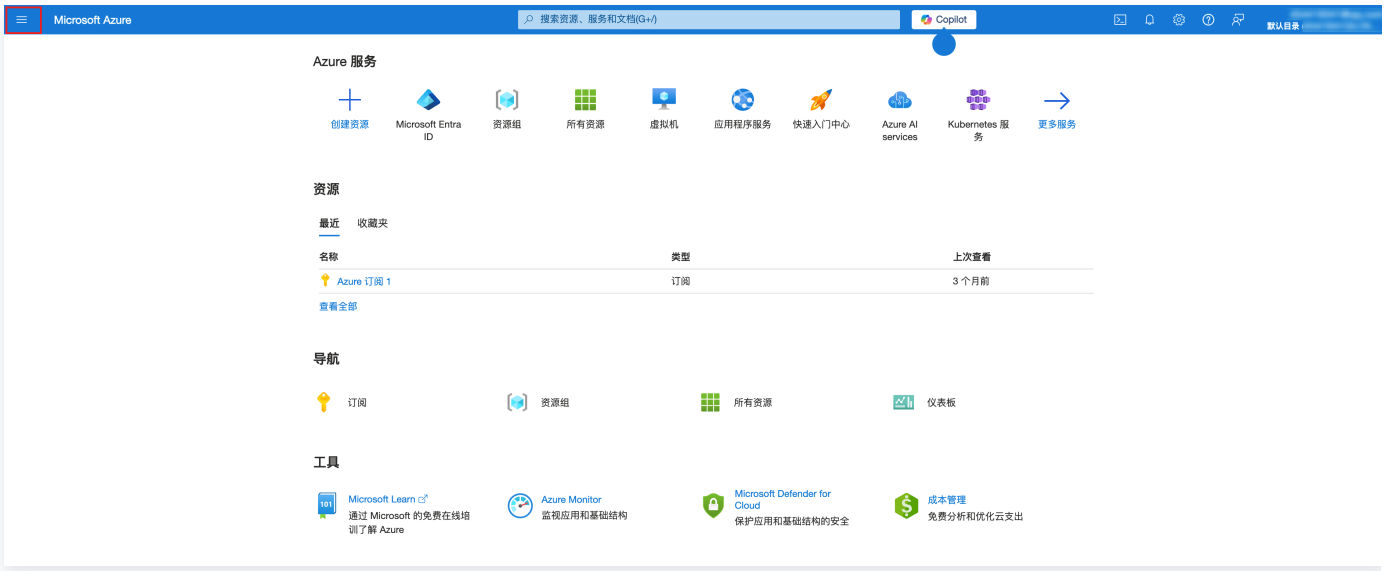
2. 在**创建 CredentialSecret** 对话框中，您可以通过**下载 CSV 文件**或**复制**来保存 SCIM 密钥。保存好密钥后，单击**确定**。



在 Azure 配置

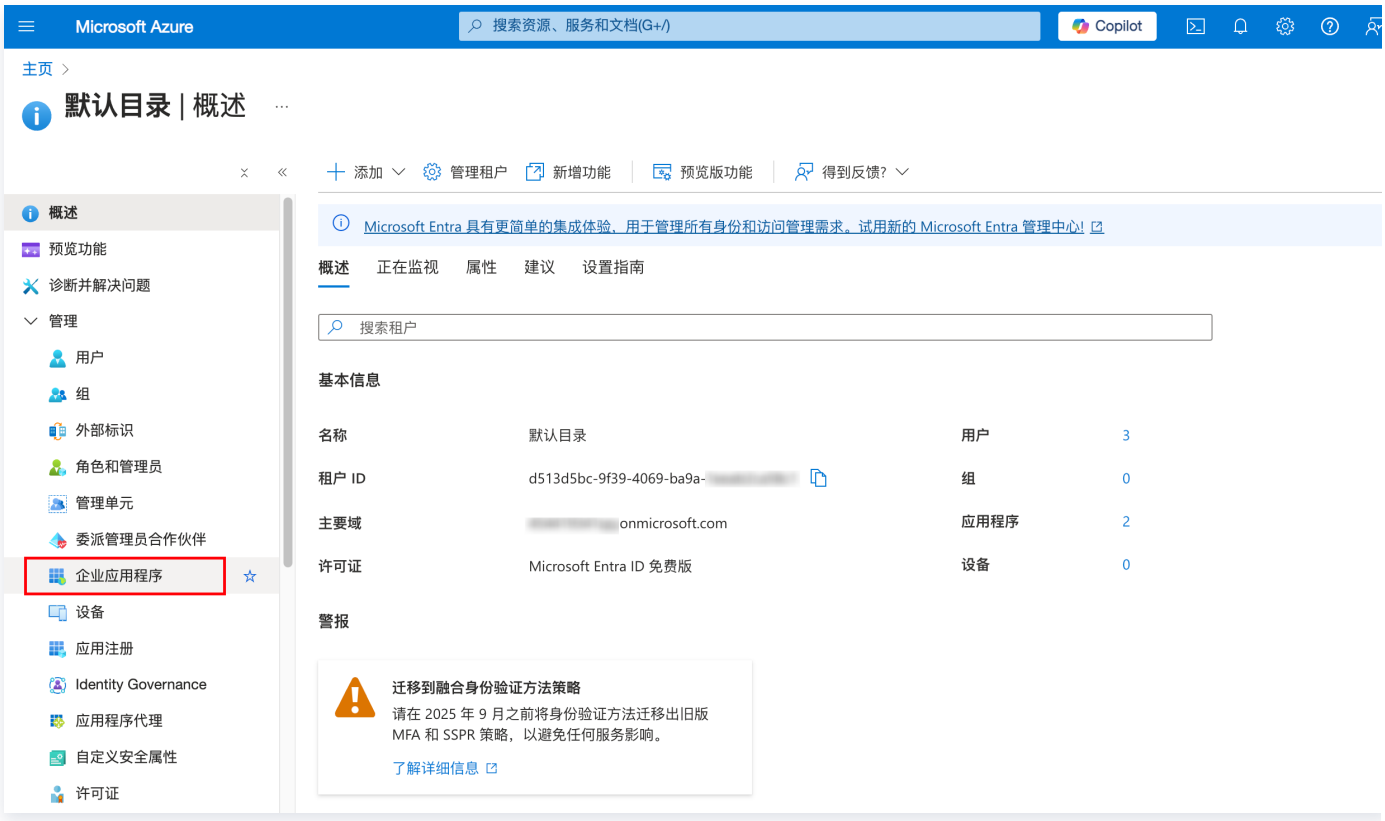
步骤一：在 Microsoft Entra ID 中创建应用程序

1. 管理员登录 Azure 门户，单击左上角菜单图标。

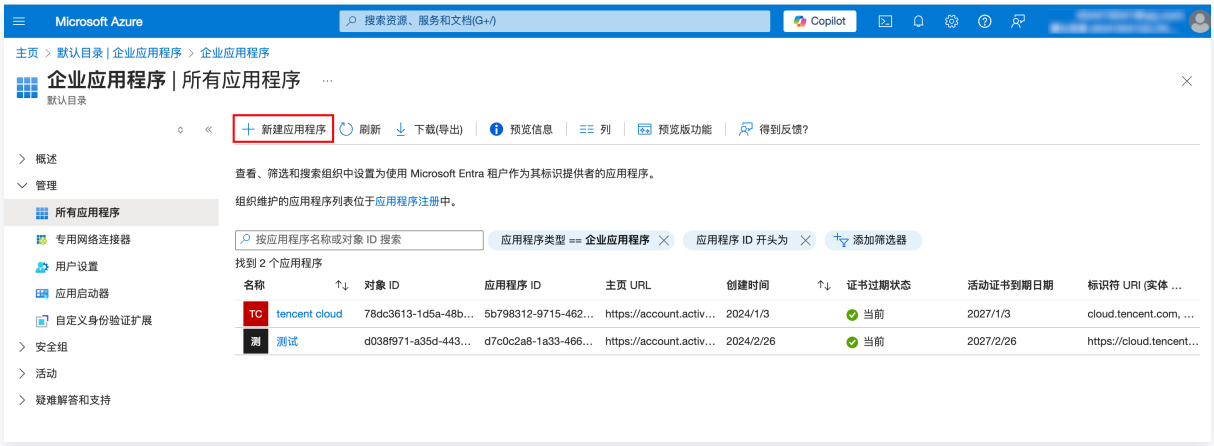


2. 在左侧导航栏，选择 Microsoft Entra ID。

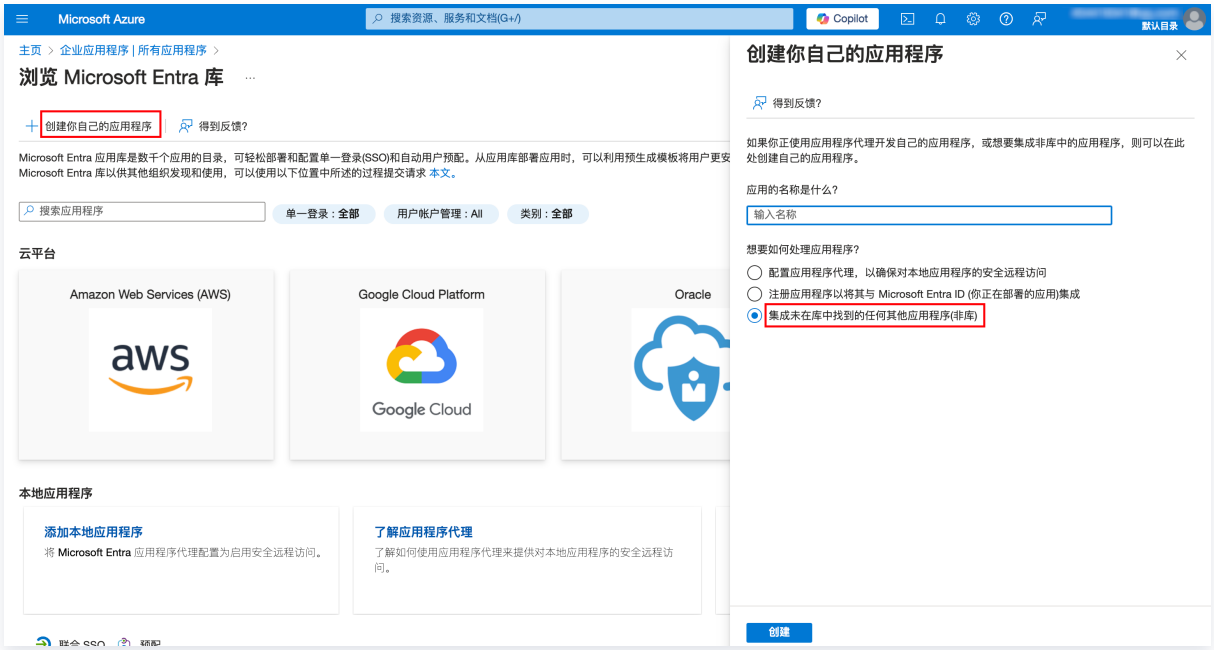
3. 在左侧导航栏，选择**管理** > **企业应用程序**后，进入**所有应用程序**。



4. 单击**新建应用程序**。



5. 在**浏览 Microsoft Entra 库**页面，单击**创建你自己的应用程序**，在右侧窗口中，输入应用名称，并选择**集成未在库中找到的任何其他应用程序(非库)**，然后单击**创建**。



步骤二：在 Microsoft Entra ID 中配置 SCIM 同步

1. 在应用程序页面，单击左侧导航栏的**预配**。

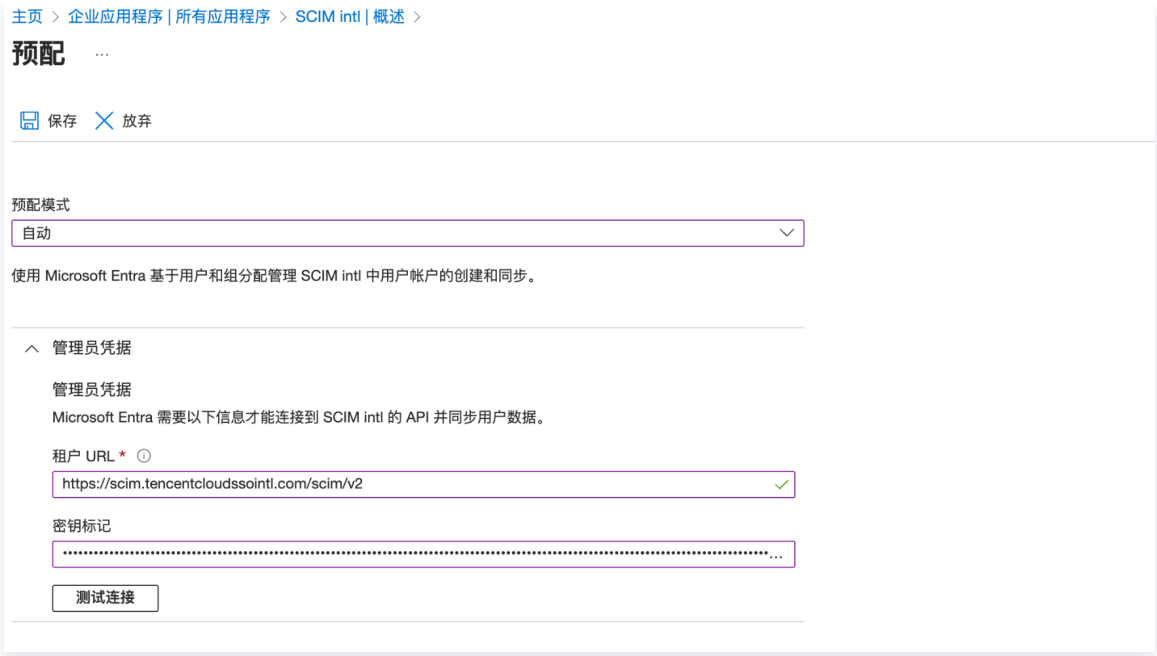
2. 在**预配**页面，单击**开始**。

3. 设置预配模式为**自动**。在**管理员凭据**区域，配置管理员凭据。
   - 在**租户 URL** 区域，输入 SCIM 服务端地址。

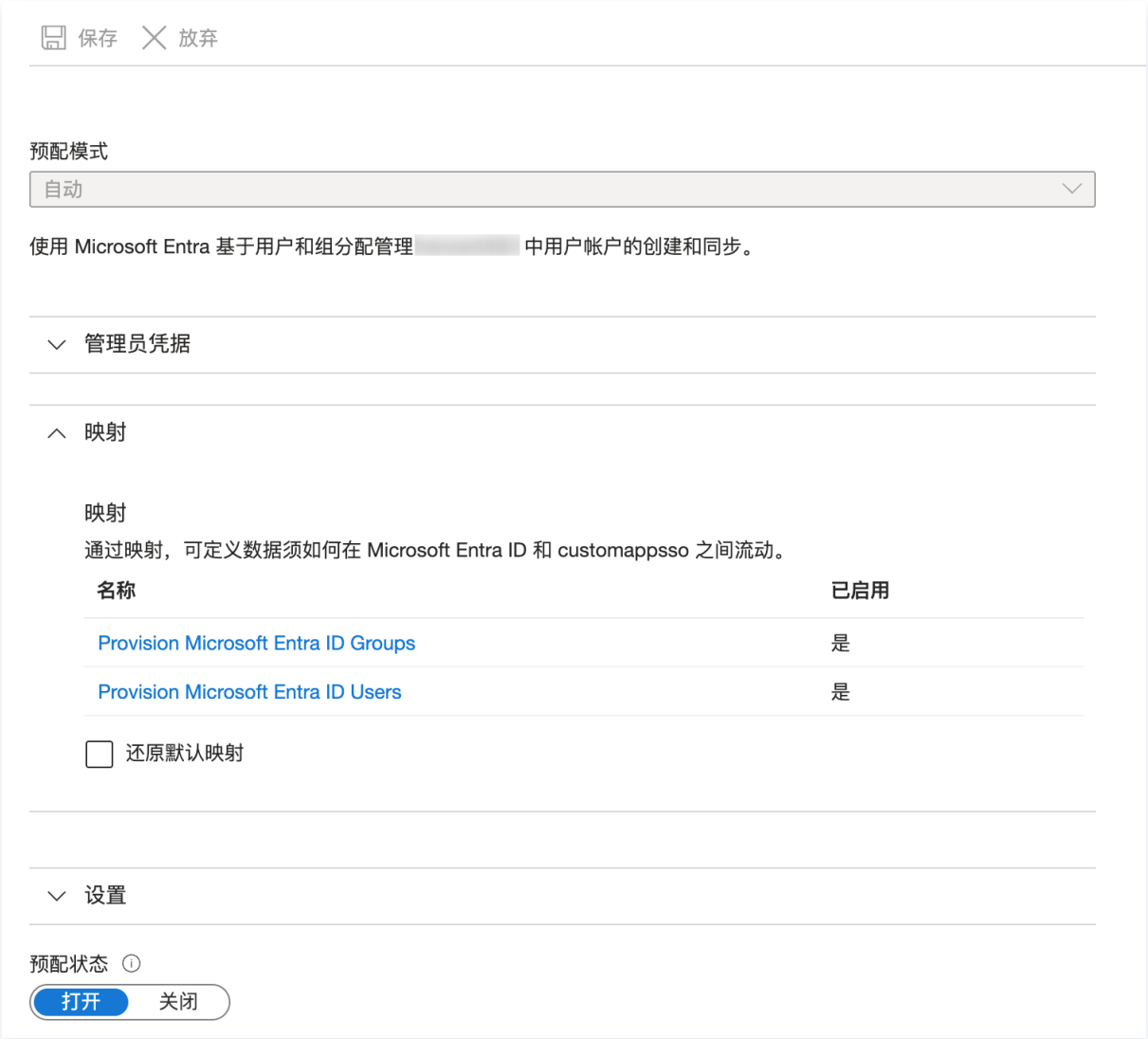
     该地址请从 步骤一：开启 SCIM 同步 获取。
   - 在**密钥标记**区域，输入 SCIM 密钥。

     该 SCIM 密钥请通过 步骤二：创建 SCIM 密钥 获取。
   - 单击**测试连接**。

     等待测试成功后，您可以继续进行下一步操作。

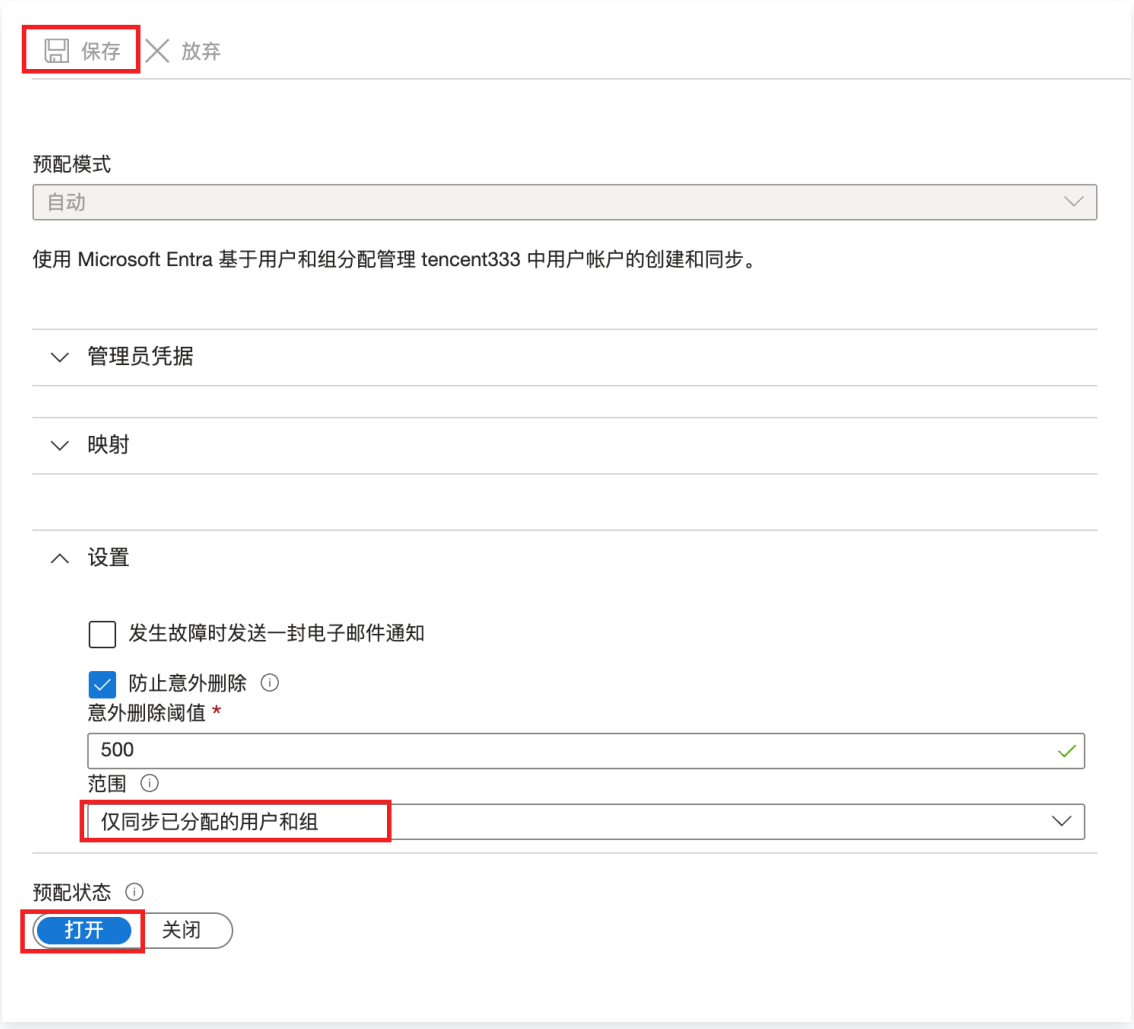


4. 在**映射**区域，可以使用默认配置，也可以按需修改属性映射。用户名默认使用 Microsoft Entra ID 的 **userPrincipalName**。



5. 在**设置**区域，**范围**模块默认选择**仅同步已分配的用户和组**，同步时需要先将用户和组分配到应用程序。

> **说明：**
> 如果选择**同步所有用户和组**，会自动同步 Microsoft Entra ID 中的所有用户和组。

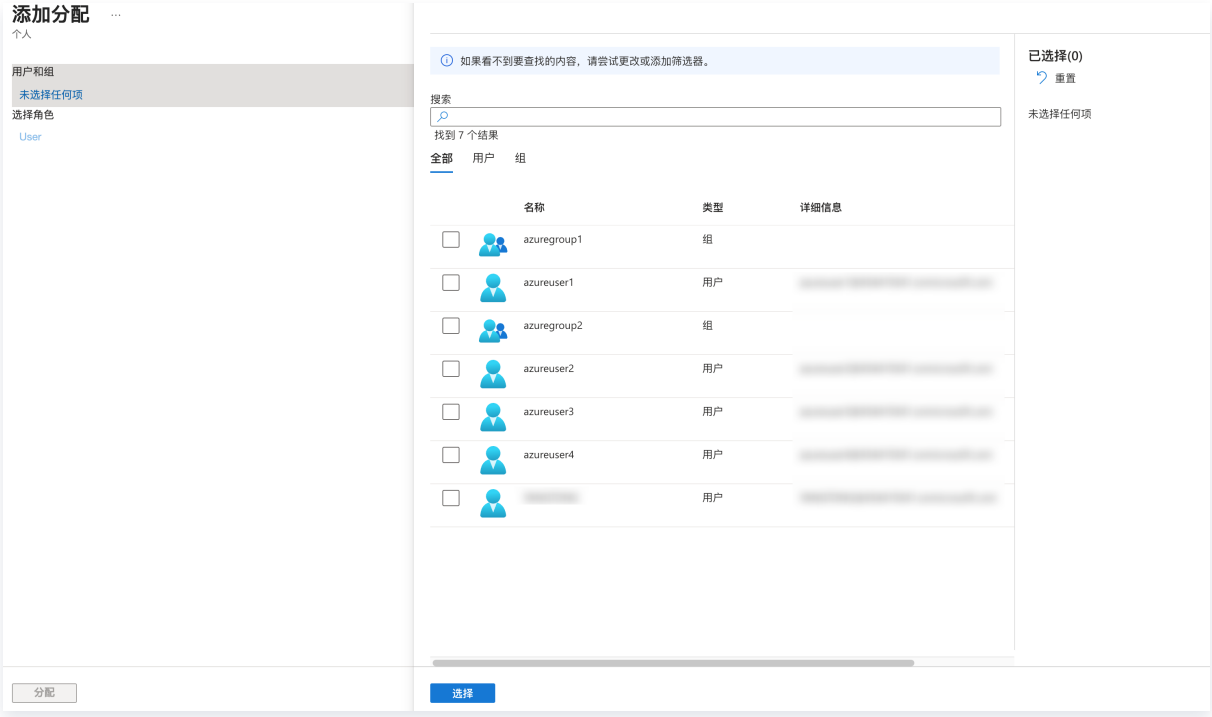


6. 单击**预配状态**区域的**打开**，单击**保存**，配置完成。

步骤三：分配用户/组

1. 在预配页面的左侧菜单，选择**用户和组**，单击**添加用户/组**。

2. 在**添加分配**页面，选择用户或用户组，单击**选择**。



3. 单击**分配**。分配成功的用户/组在列表中展示。

步骤四：同步用户/组

自动同步用户/组（非实时）

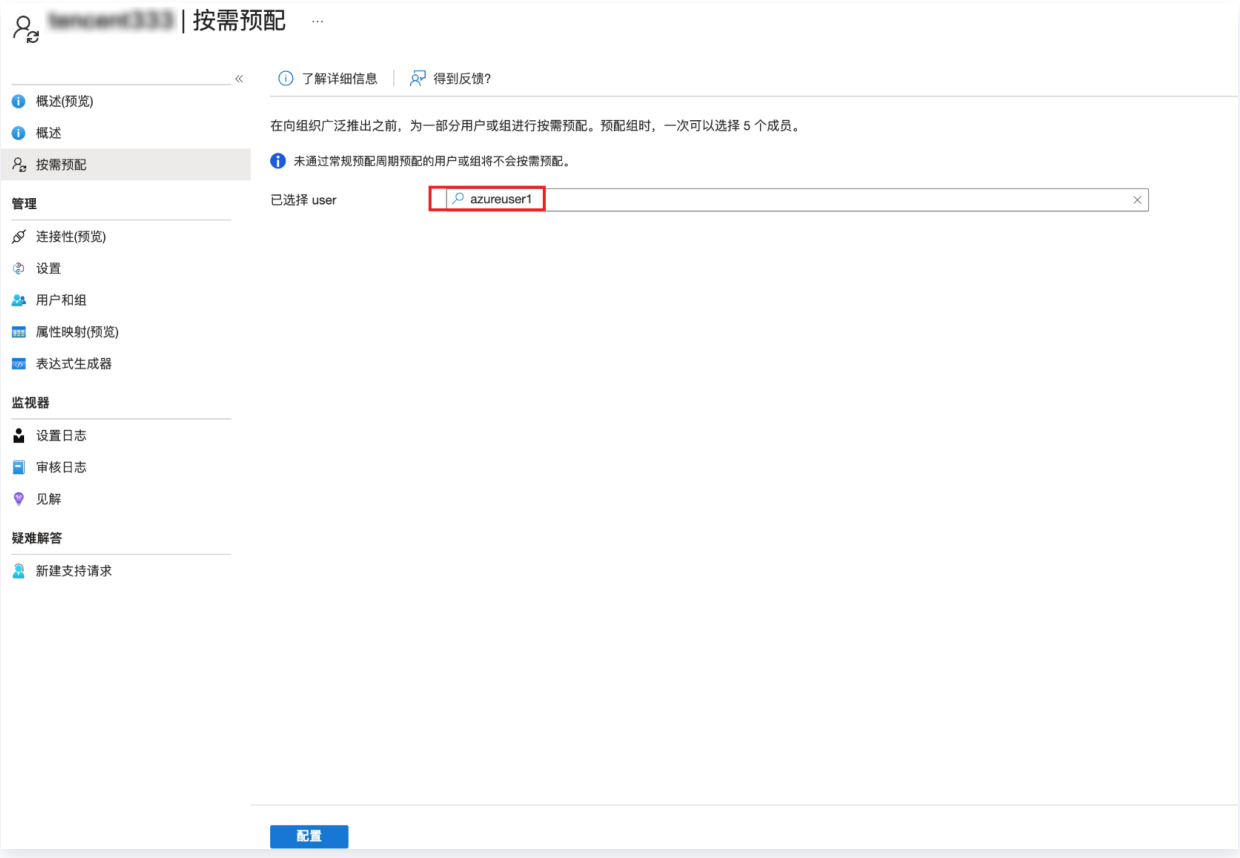
- 已分配的用户/组，会按照**预配间隔**时间自动同步到身份中心，非实时同步。
- 在 Microsoft Entra ID 中默认20~40分钟同步一次，时间不可修改。
- 已分配的用户组在同步时，会**自动同步组内用户**；组内的增量用户也会按预配间隔时间同步（非实时）。

手动同步用户/组（实时）

如果需要**立即同步**用户/组，可按如下步骤操作。

同步用户

1. 在**按需预配**页面，选择需要同步的用户，单击**配置**。

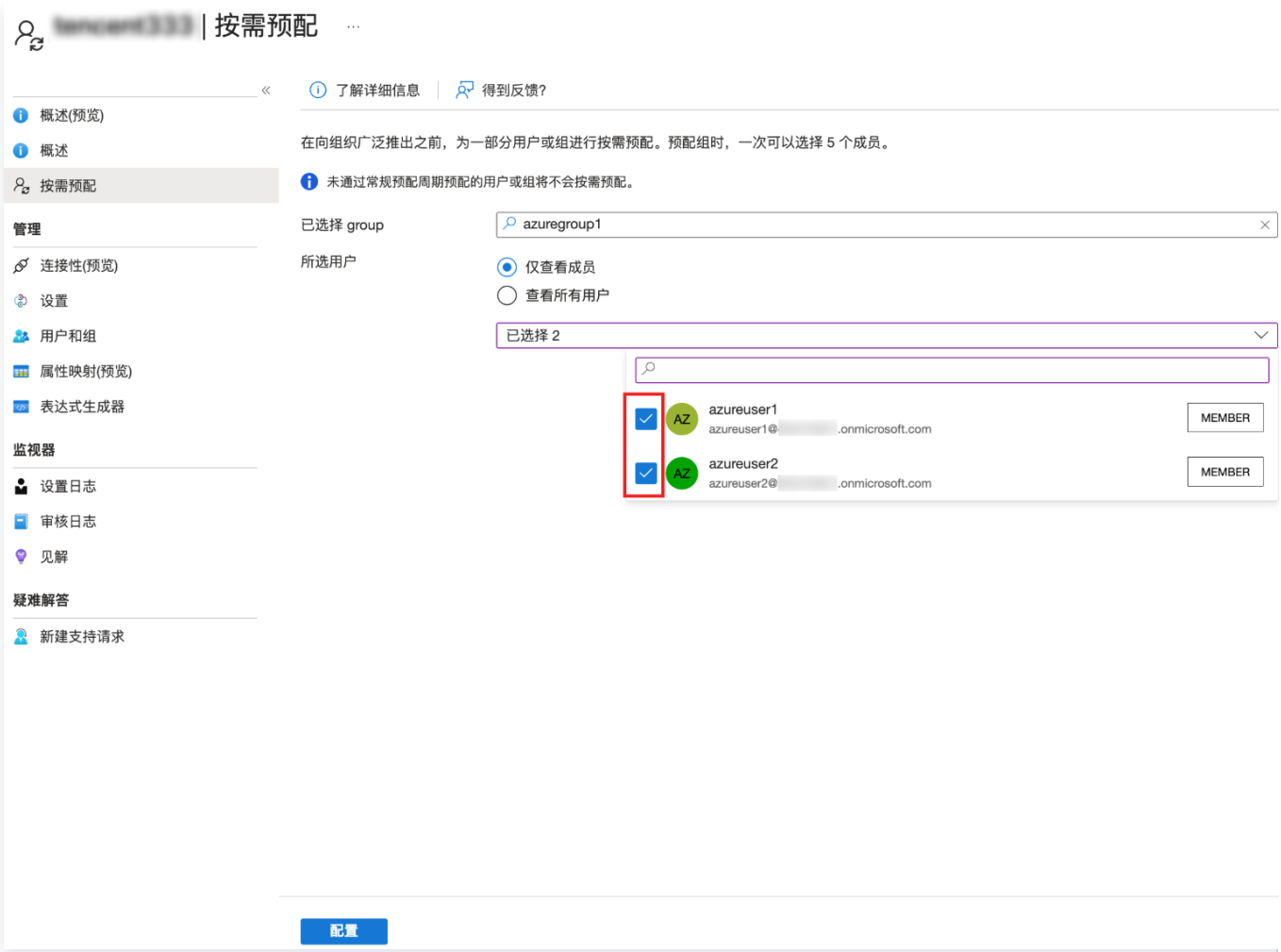


2. 配置成功。

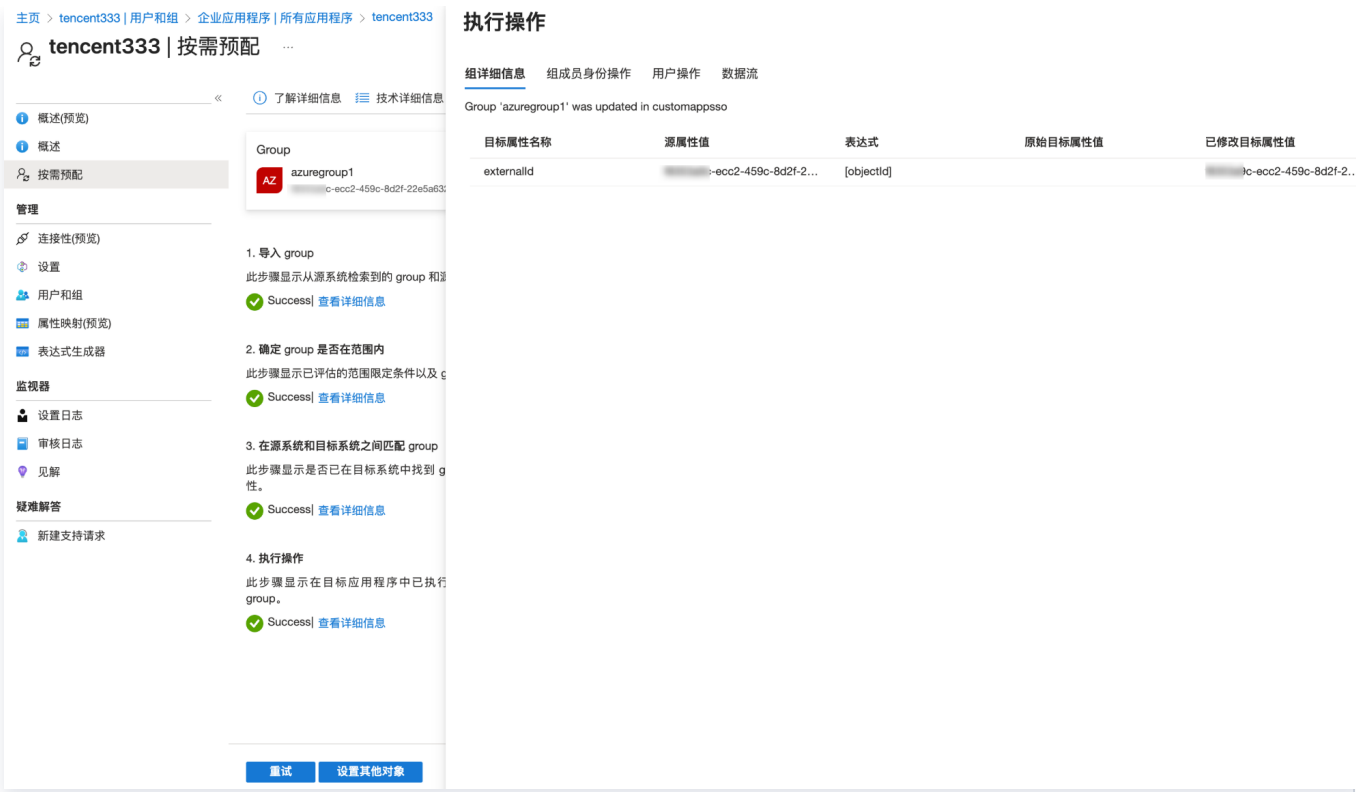
同步用户组

1. 在**按需预配**页面，选择需要同步的用户组，并同时**勾选**组内的用户，单击**配置**。

> **说明：**
> 如果没有同时勾选用户，则当次同步，**只会同步用户组，不会同步组内用户**。



2. 配置成功。



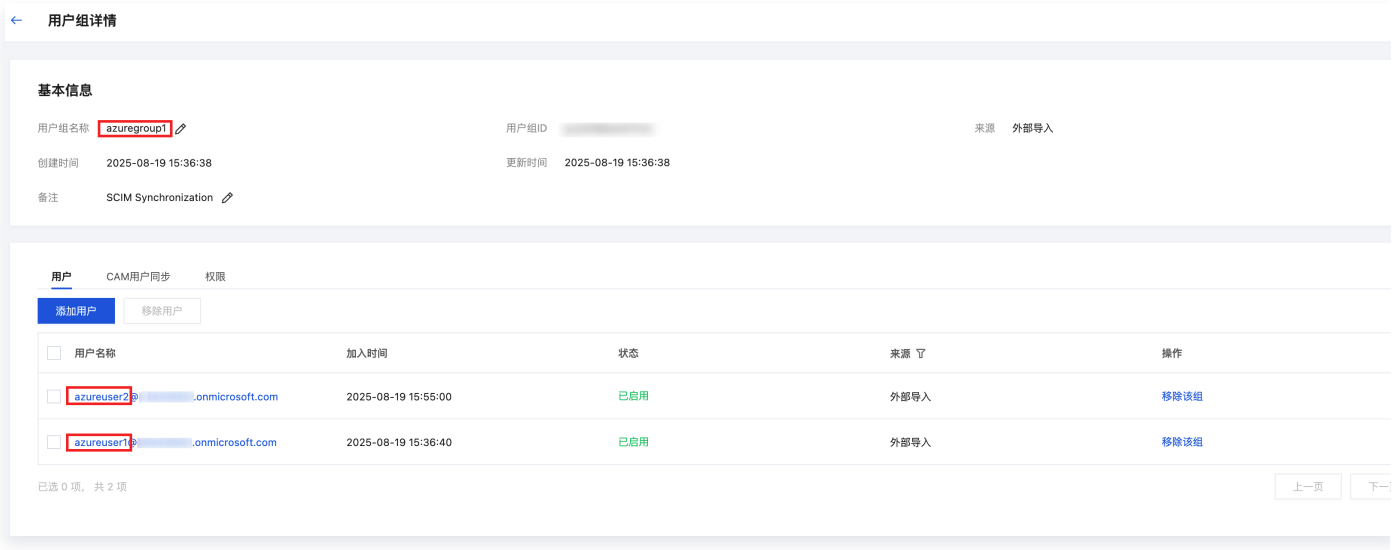
结果验证

登录集团账号管理 > 身份中心 。

- 在左侧导航栏，单击**用户管理** > **用户**，查看列表。**来源**会自动标识为**外部导入**。

- 在左侧导航栏，单击**用户管理** > **用户组**，查看列表。**来源**会自动标识为**外部导入**。

单击用户组名称，进入用户组详情页，可以查看组内用户。



通过 SCIM 同步 Okta 示例

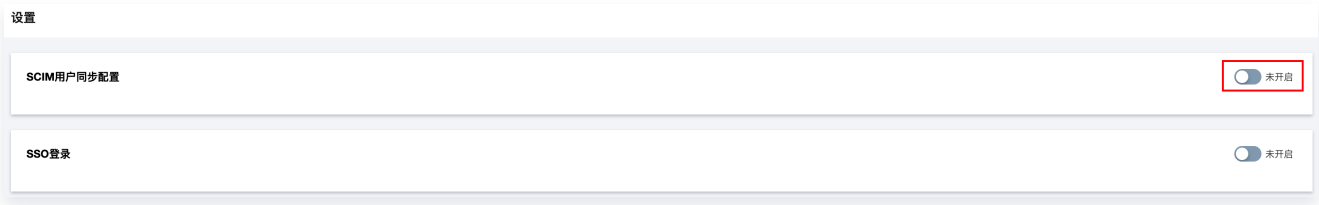
最近更新时间：2025-04-10 14:49:33

本文为您介绍通过 SCIM 协议，将 Okta 中的用户或用户组同步到腾讯云身份中心。

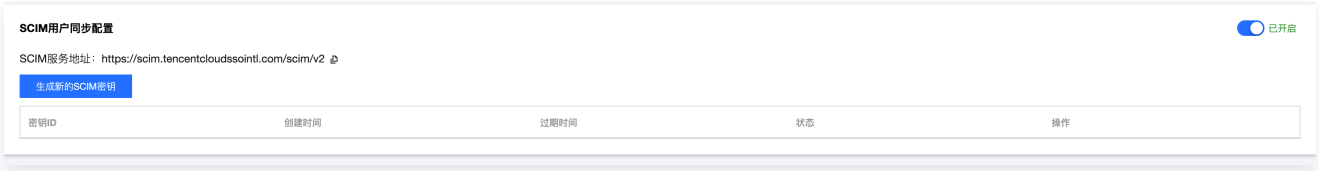
在身份中心配置

步骤一：开启 SCIM 同步

1. 登录集团账号管理 > 身份中心 。
2. 在左侧导航栏，单击**用户管理** > **设置**。
3. 在 **SCIM 用户同步配置**区域，单击，在弹出的窗口单击**开启**，启用 SCIM 同步。



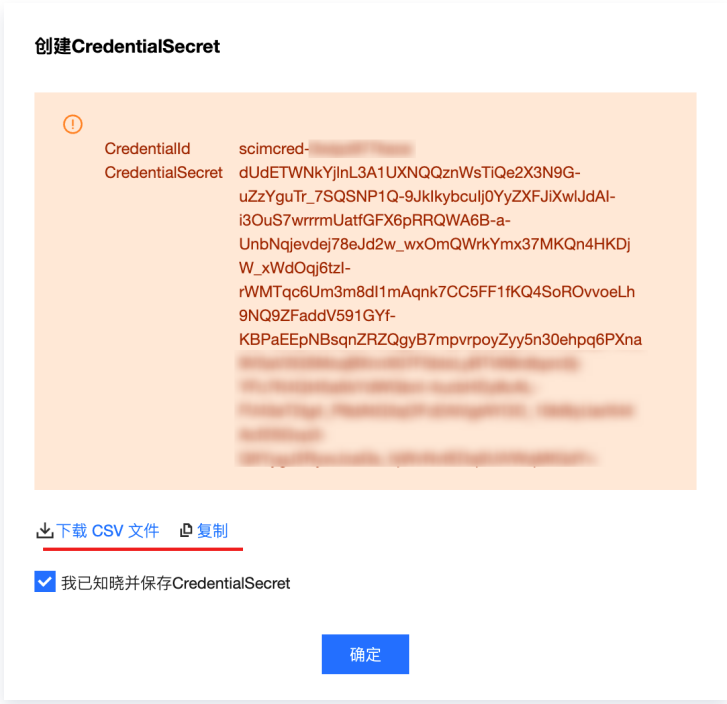
4. 启用后，在 **SCIM 用户同步配置**区域，查看或复制 **SCIM 服务端地址**，在外部 IdP 中配置 SCIM 同步时会使用该地址。
   - 中国站：https://scim.tencentcloudsso.com/scim/v2
   - 国际站：https://scim.tencentcloudssointl.com/scim/v2



步骤二：创建 SCIM 密钥

1. 在 **SCIM 用户同步配置**区域，单击**生成新的 SCIM 密钥**。

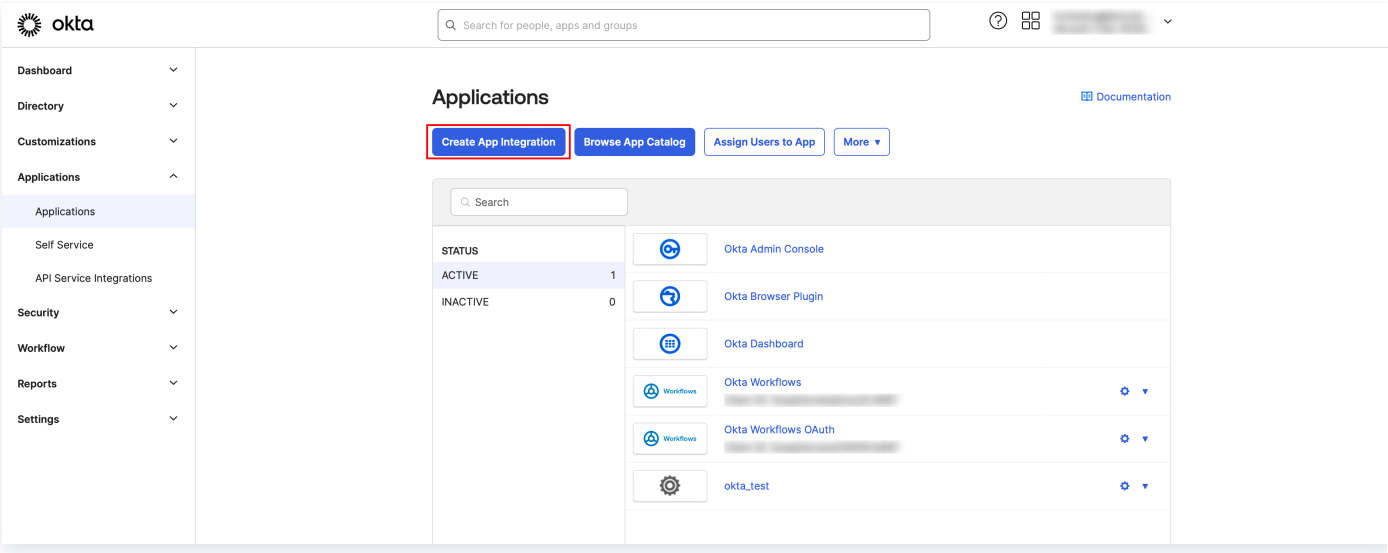
2. 在**创建 CredentialSecret** 对话框中，您可以通过**下载 CSV 文件**或**复制**来保存 SCIM 密钥。保存好密钥后，单击**确定**。



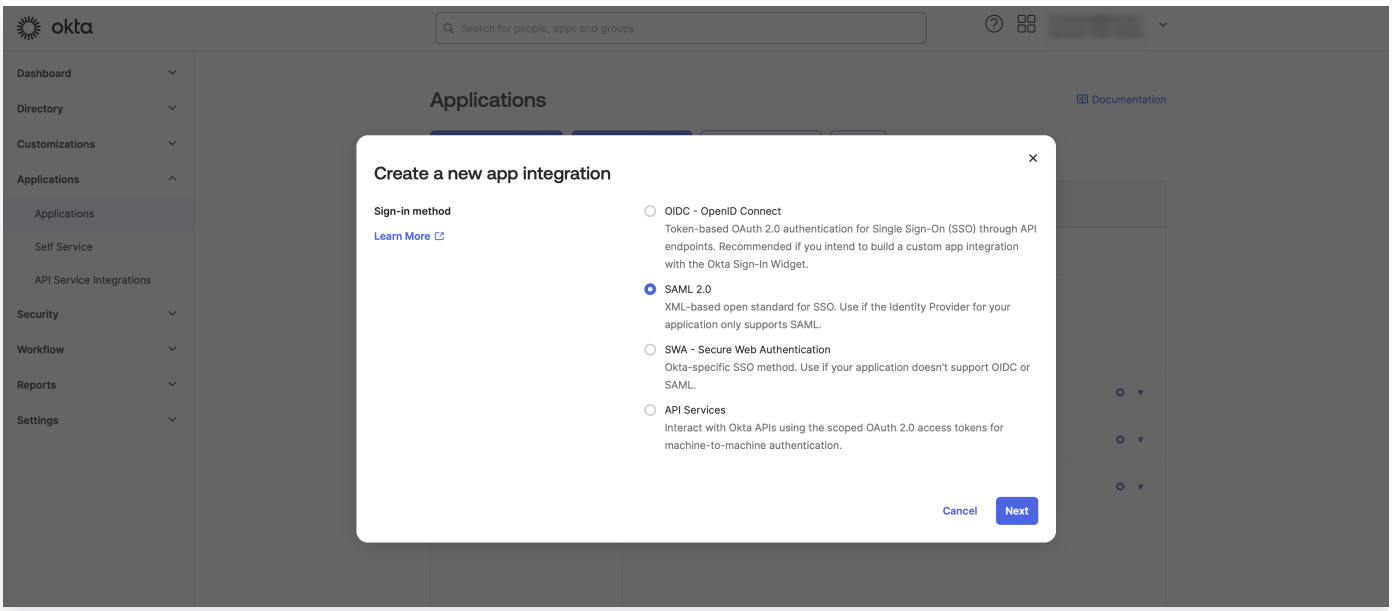
在 Okta 配置

步骤一：在 Okta 中创建应用程序

1. 登录 Okta，在左侧导航栏中，选择 Applications > Applications 后，进入全部应用，单击 Create APP Intergration，创建应用程序。

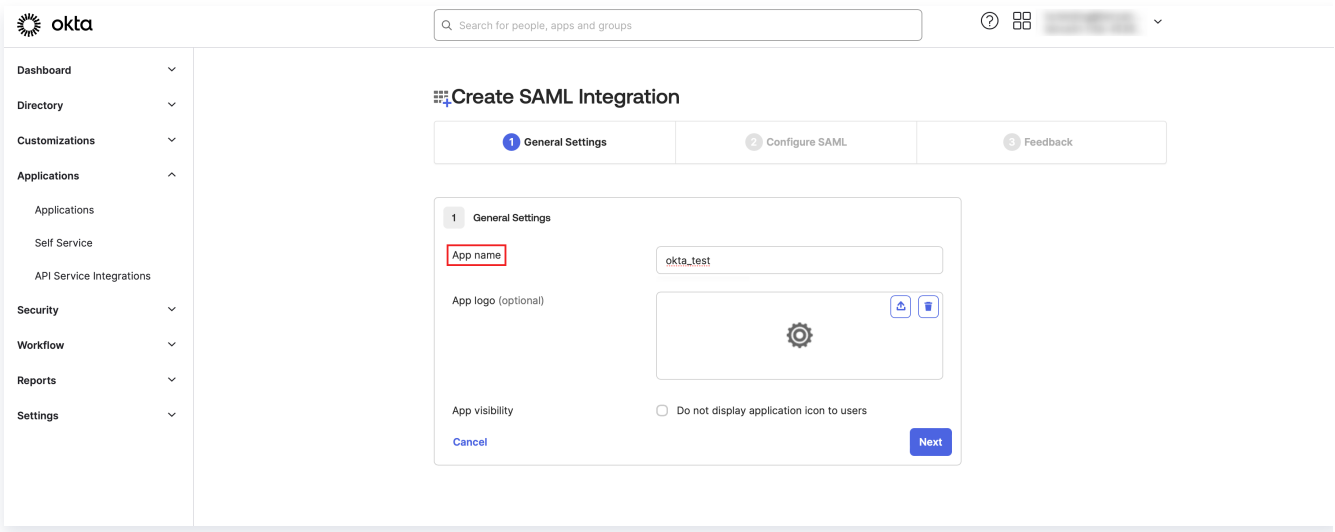


2. 在弹出的 Create a new app integration 窗口中，选择 SAML 2.0，单击 Next。

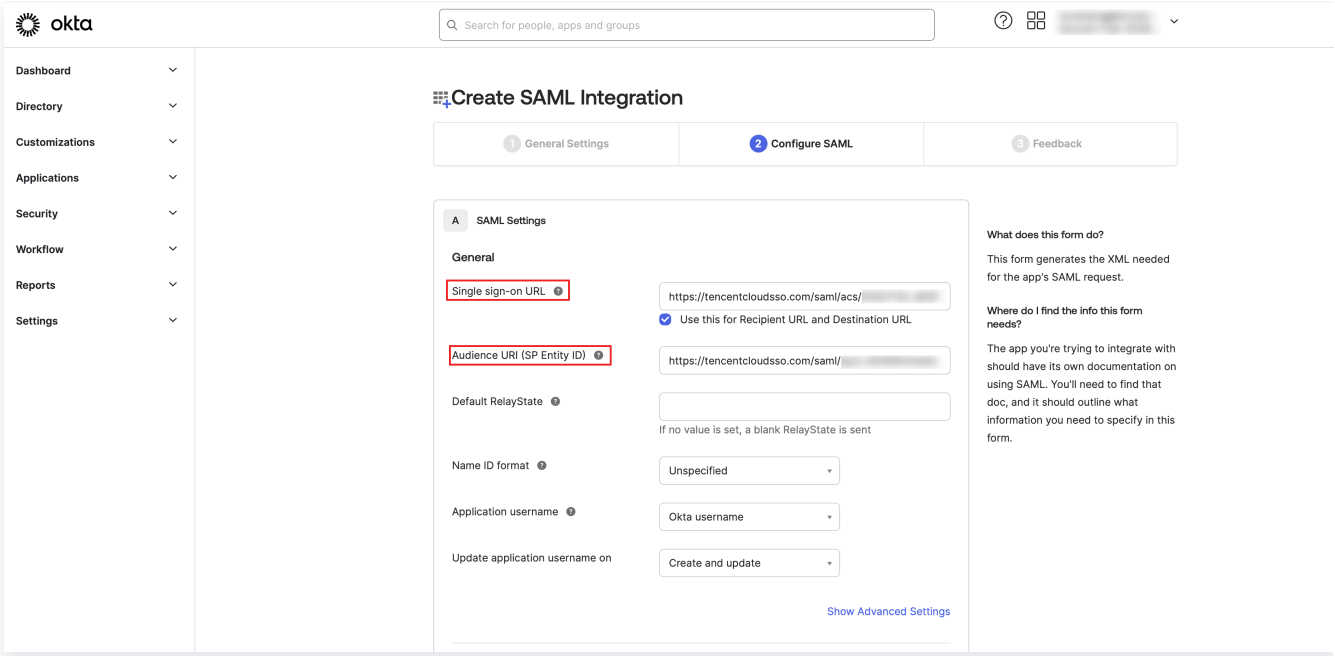


3. 进入 Create SAML Integration 页面，完成应用基础配置。

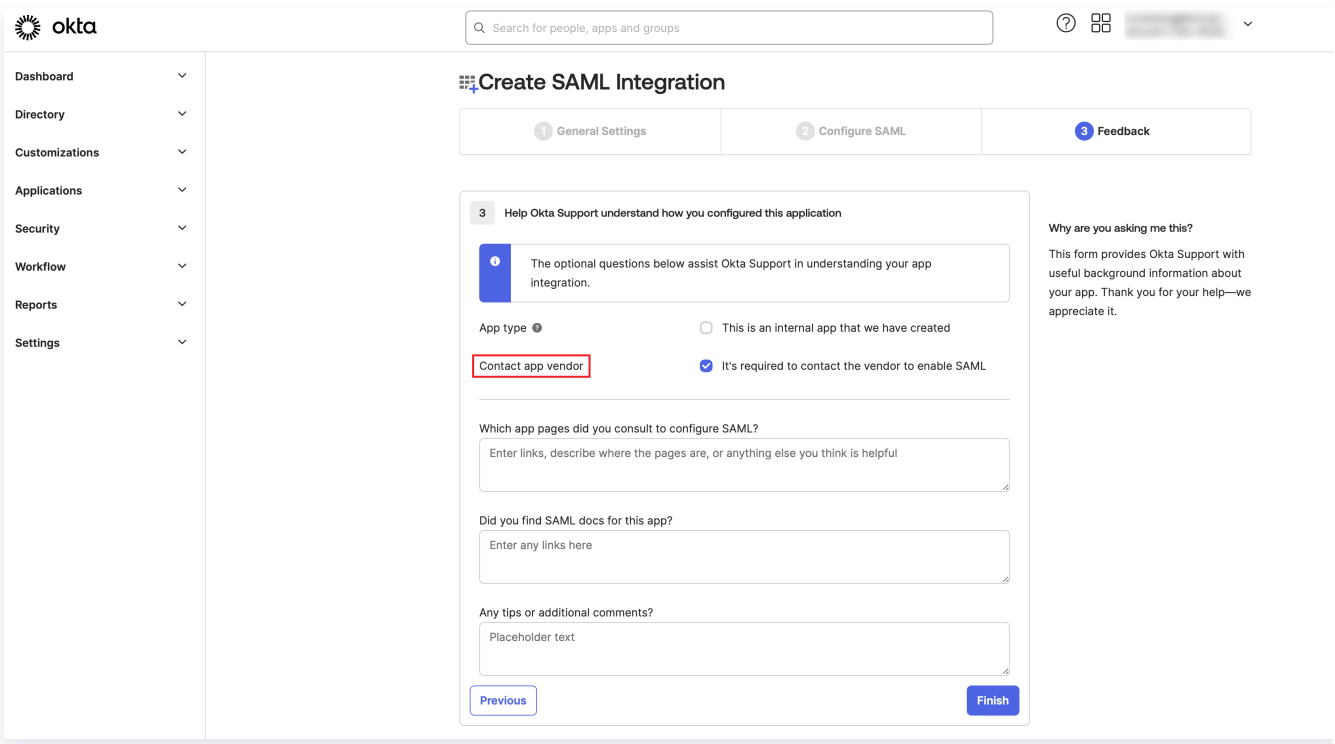
3.1 在 General Settings 页面，填写 App name，单击 Next。



3.2 在 Configure SAML 页面，填写 Single sign-on URL 和 Audience URL(SP Entity ID)，该信息对应**身份中心** > **用户管理** > 设置 > **SSO 登录**，**服务提供商(SP)信息**中的 ACS URL 和 Entity ID，填写完成后，单击 Next。

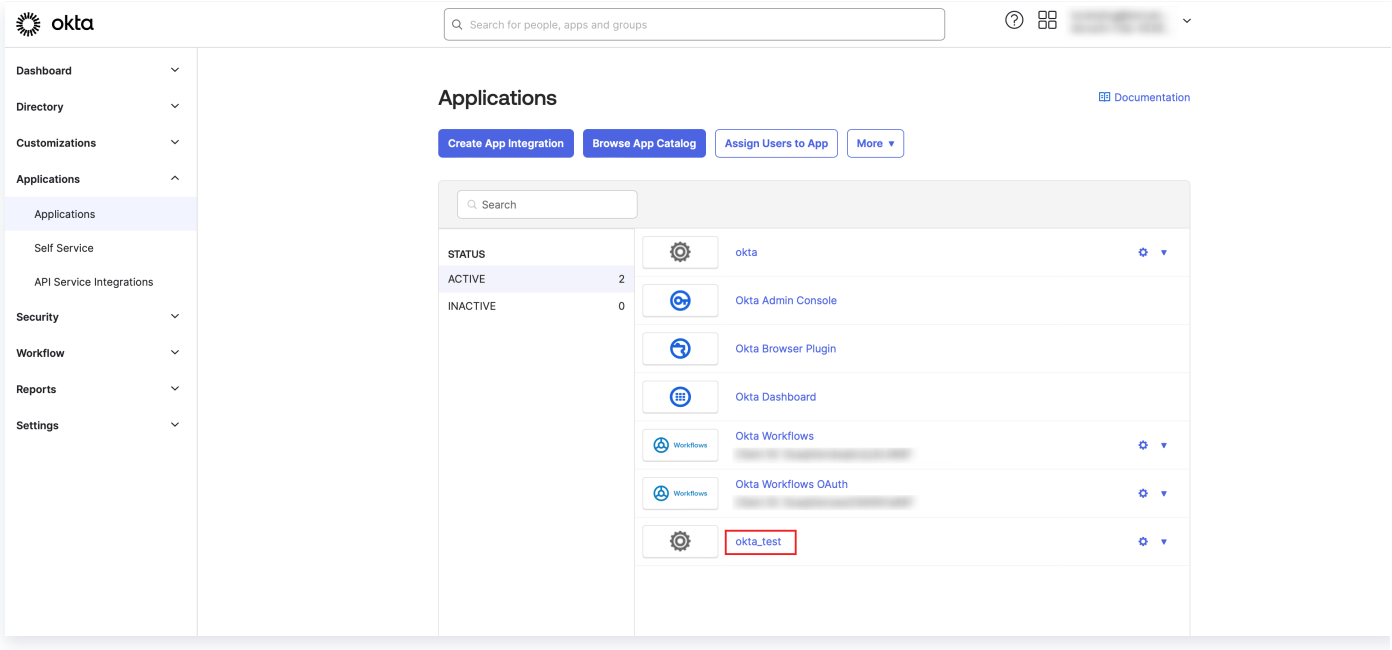


3.3 在 Feedback 页面，勾选 Contact app vendor，单击 Finish，完成应用创建。

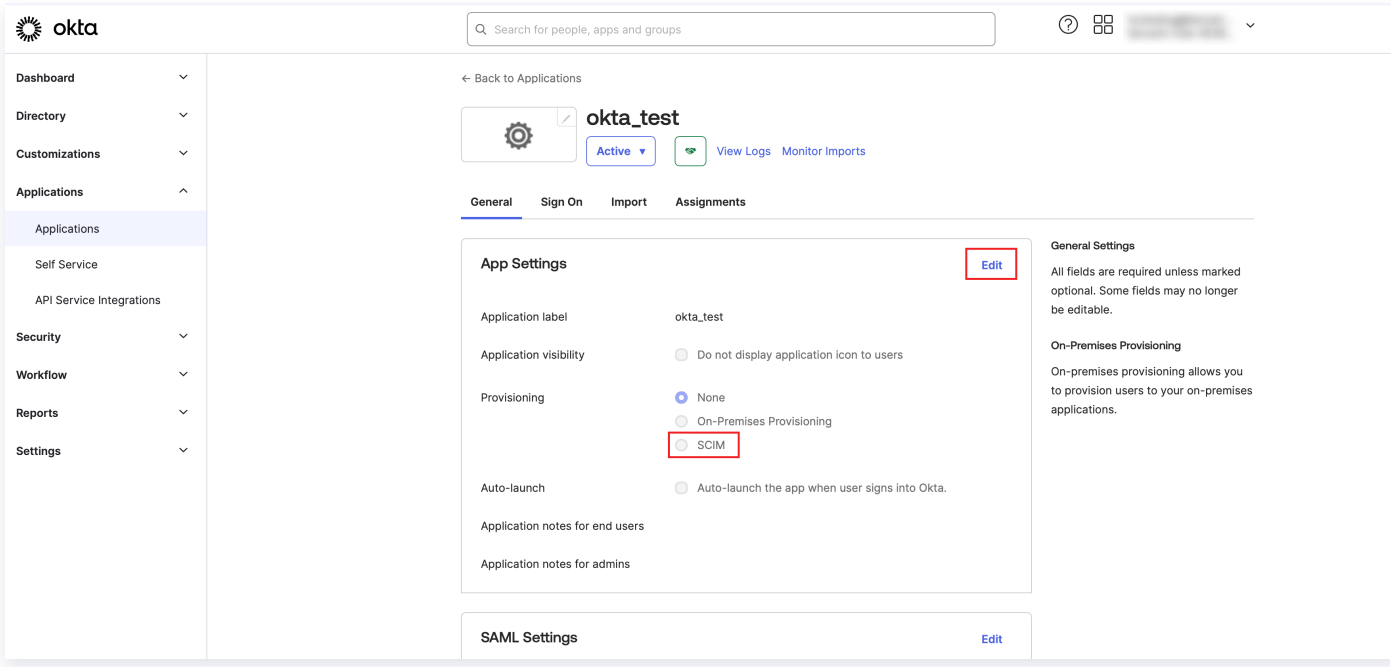


步骤二：配置 SCIM 同步基础信息

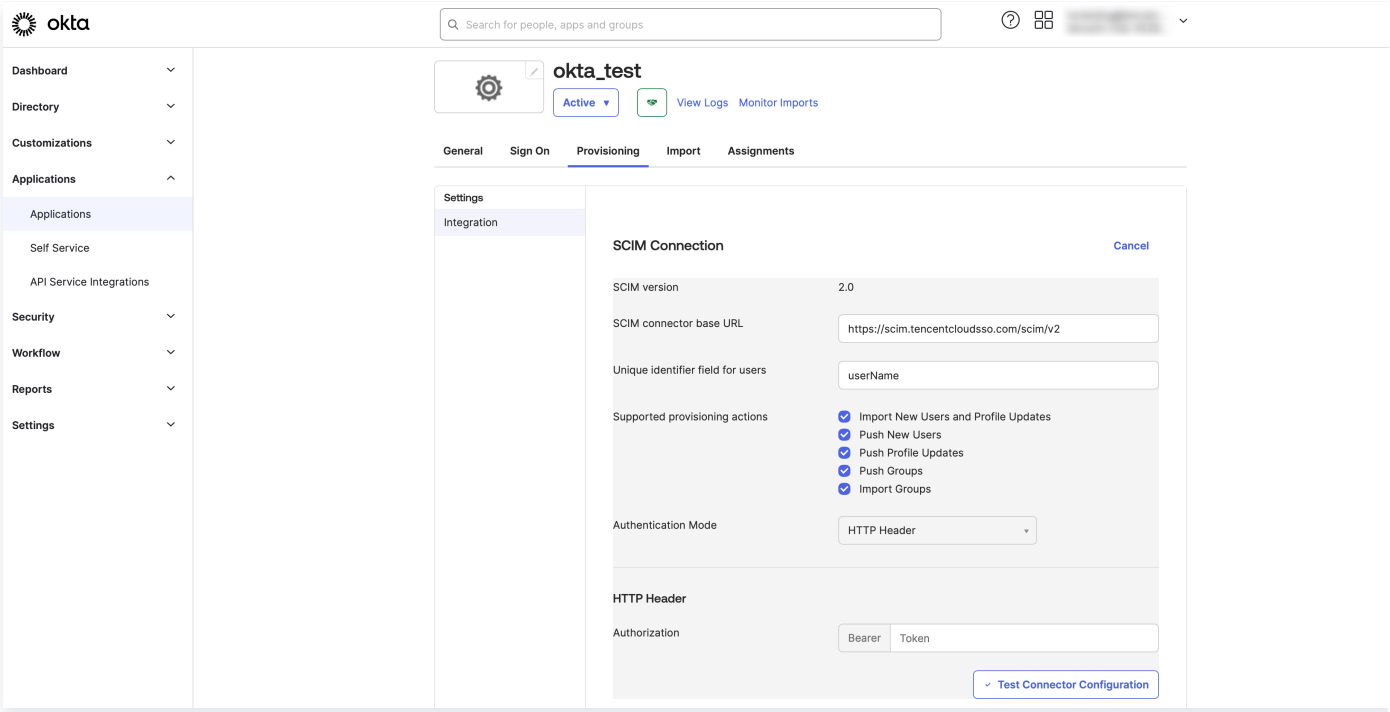
1. 在左侧导航栏，选择 Applications > Applications 后，进入全部应用，选中目标应用。



2. 在 General 页面，单击 Edit 后，将 Provisioning 的选项置为 SCIM，单击 Save 后，出现 Provisioning 页签。

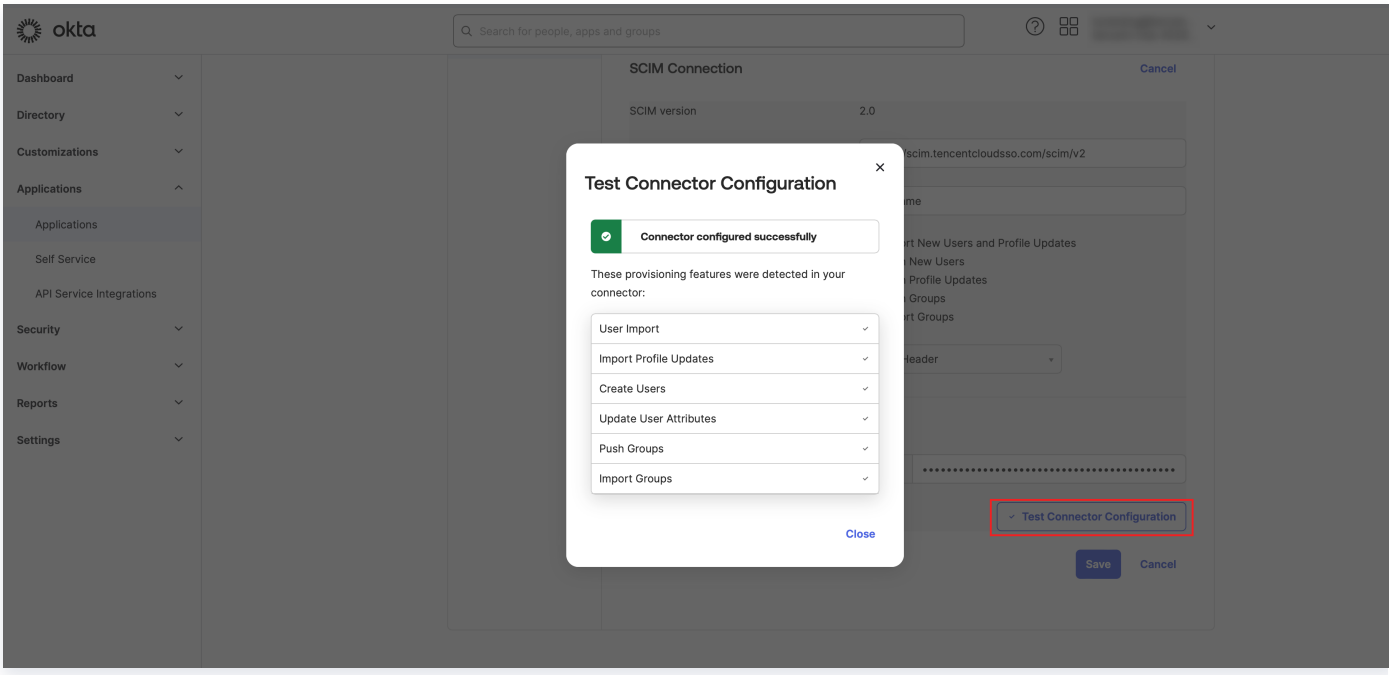


3. 在 **Provisioning** 页面，单击 **Edit** 进行编辑，填写内容如下：
   - SCIM connector base URL：填写 **SCIM 服务端地址**。
     - 中国站：https://scim.tencentcloudsso.com/scim/v2
     - 国际站：https://scim.tencentcloudssointl.com/scim/v2
   - Unique identifier field for users：填写 **userName**。
   - Supported provisioning actions：勾选**全部**。
   - Authentication Mode：选择 **HTTP Header**。
   - Authorization：填写 步骤二：创建 SCIM 密钥 获取的 **CredentialSecret**。



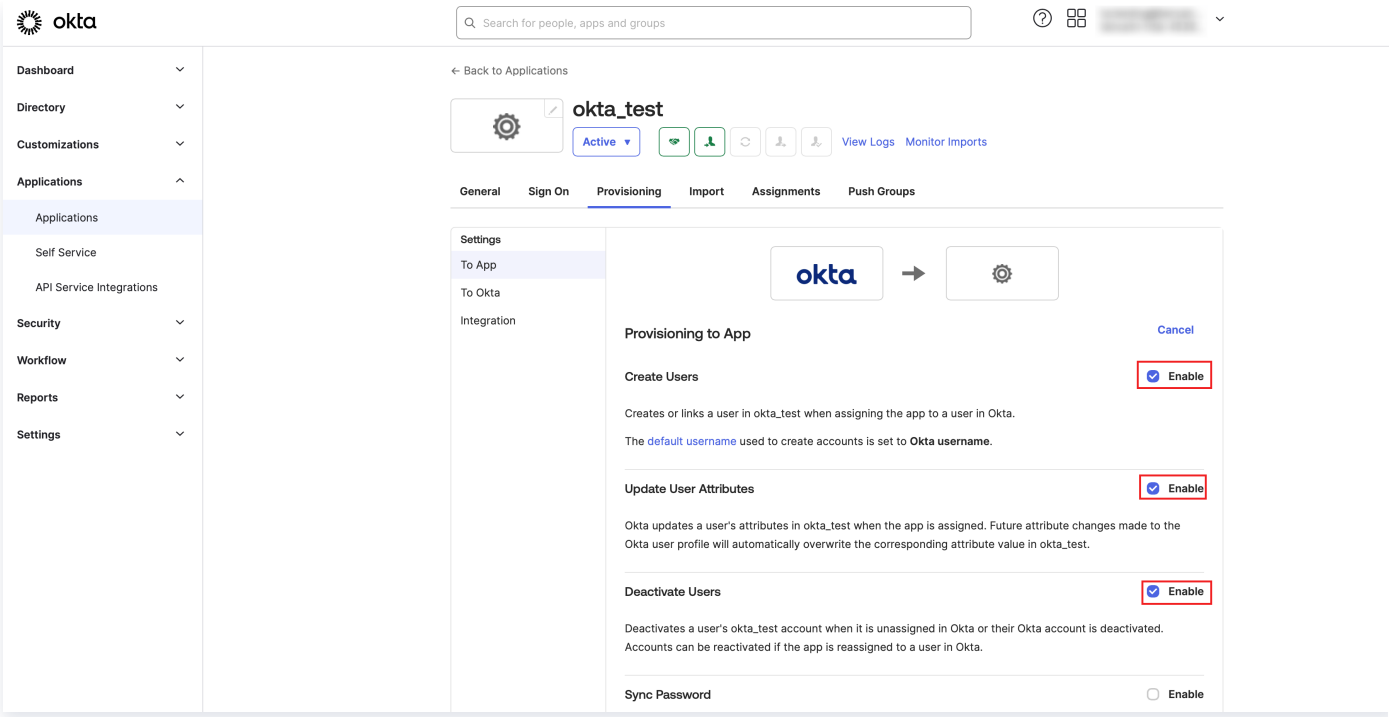
4. 测试连接，单击 **Test Connector Configuration** 后，查看测试结果。

   如果测试成功，单击 **Save**。否则，请修改配置，直到测试成功。



5. 测试成功后，在 **Provisioning** 页面左侧出现 **To App** 页签。在 **To App** 页面的 **Provisioning to App** 区域，单击 **Edit**。

   勾选 **Create Users**、**Update User Attributes** 和 **Deactivate Users** 中的 **Enable**，单击 **Save**，完成配置。

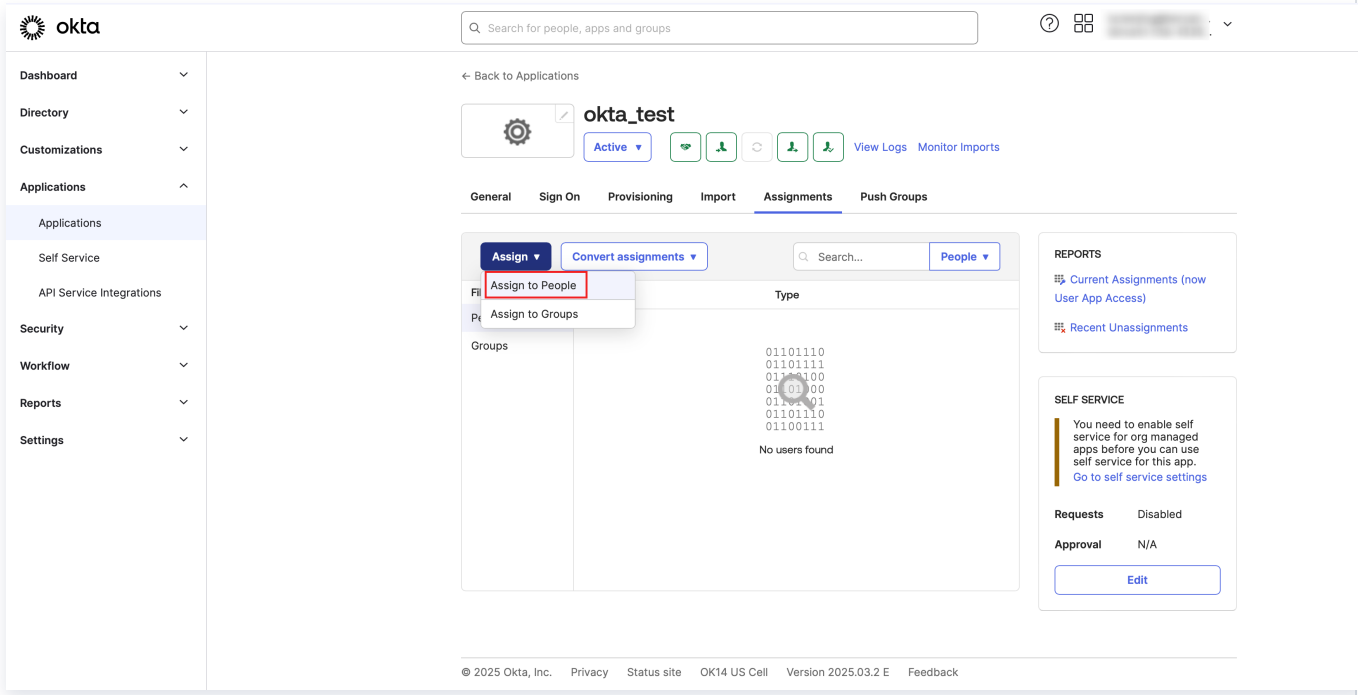


步骤三：同步用户/同步用户组

同步用户

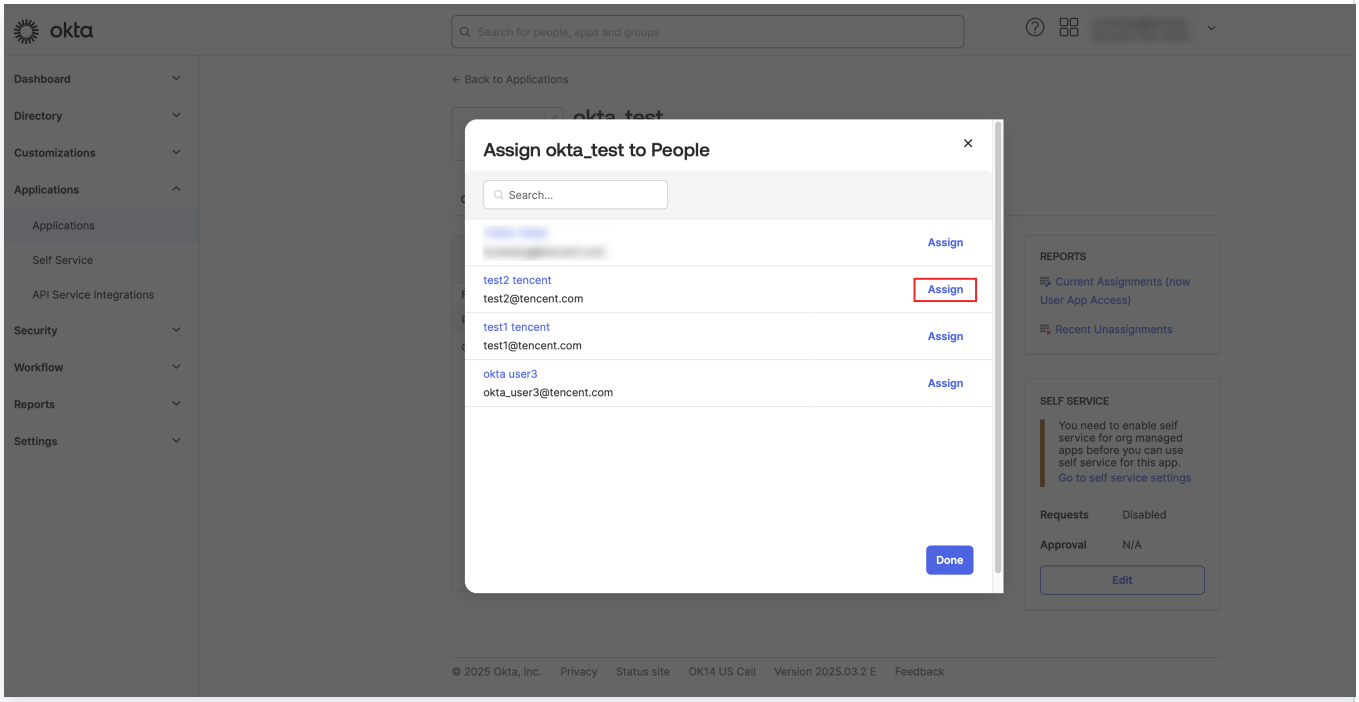
同步用户

1. 在 Assignments 页面，单击 Assign，选择 Assign to People，将用户分配到应用。

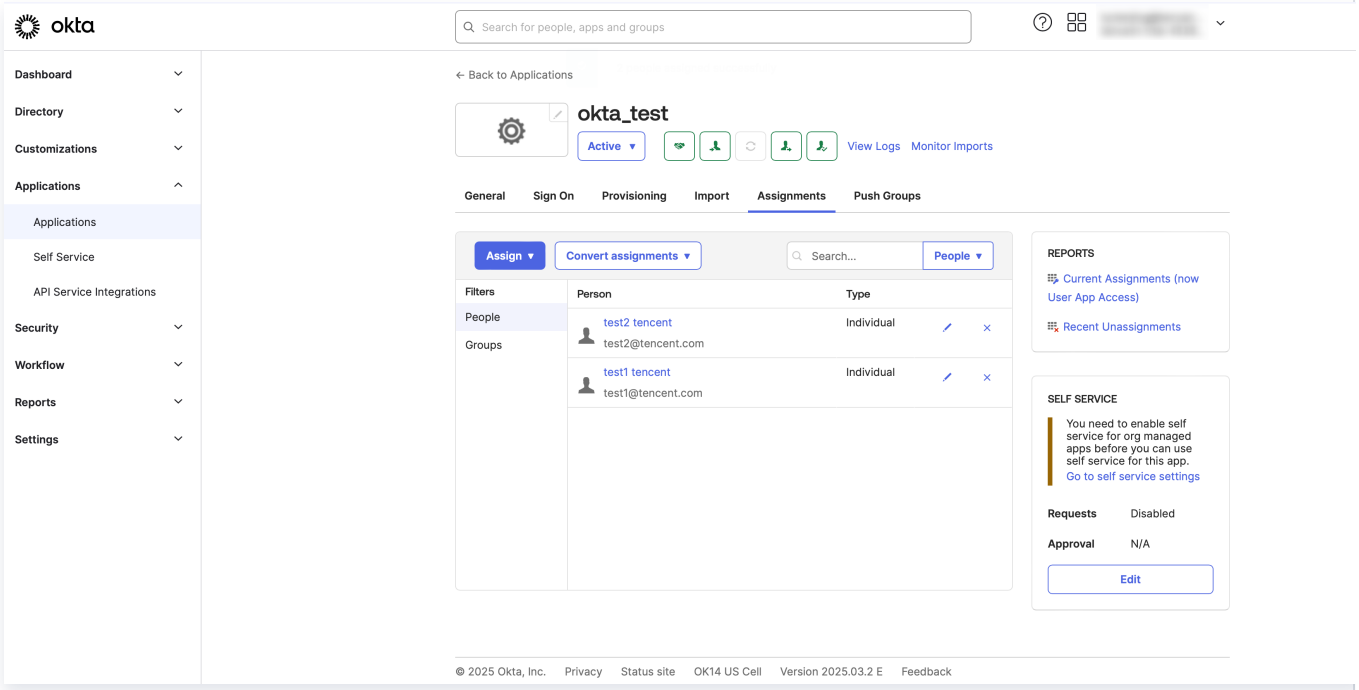


2. 在 Assign okta_test to People 弹窗中，选择目标用户，单击 Assign。在新窗口单击 Save and Go

Back，开始同步。



3. 同步成功的用户展示在 **People** 页面。



结果验证

1. 登录**集团账号管理** > 身份中心 。
2. 单击左侧导航栏的**用户管理** > **用户**，查看**用户列表**页面，同步的用户**来源**会自动标识为**外部导入**。

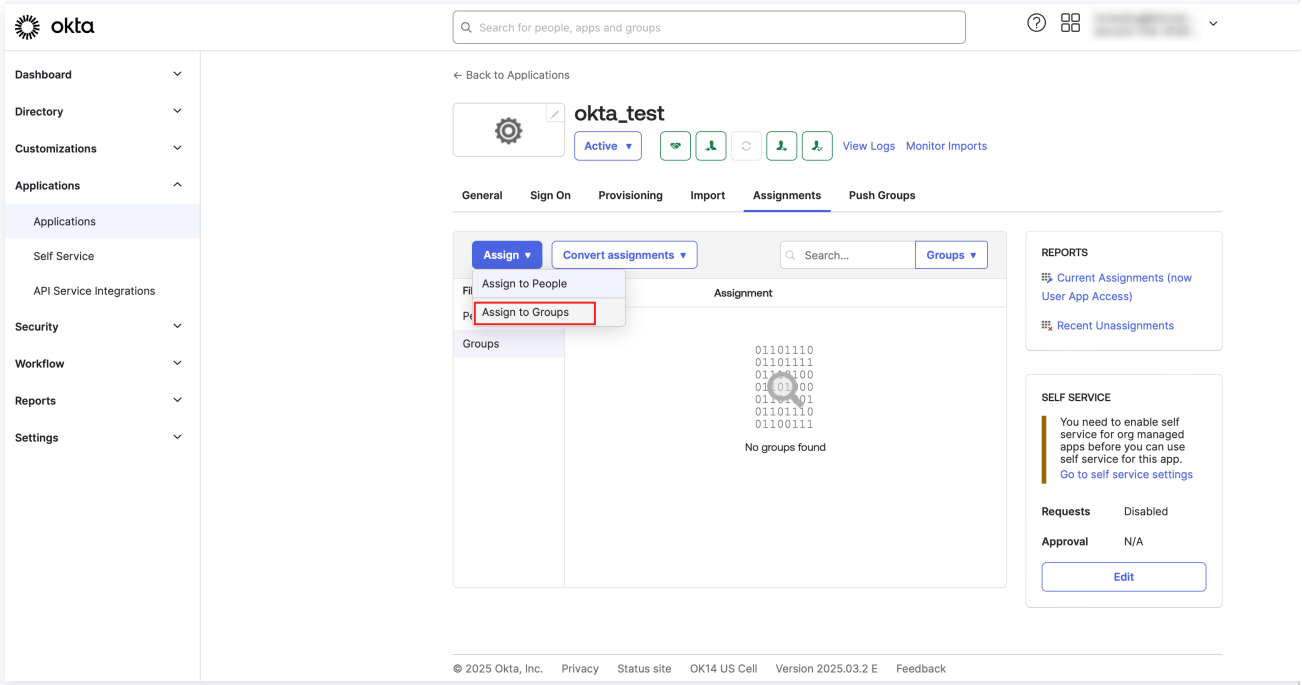
同步用户组

同步用户组

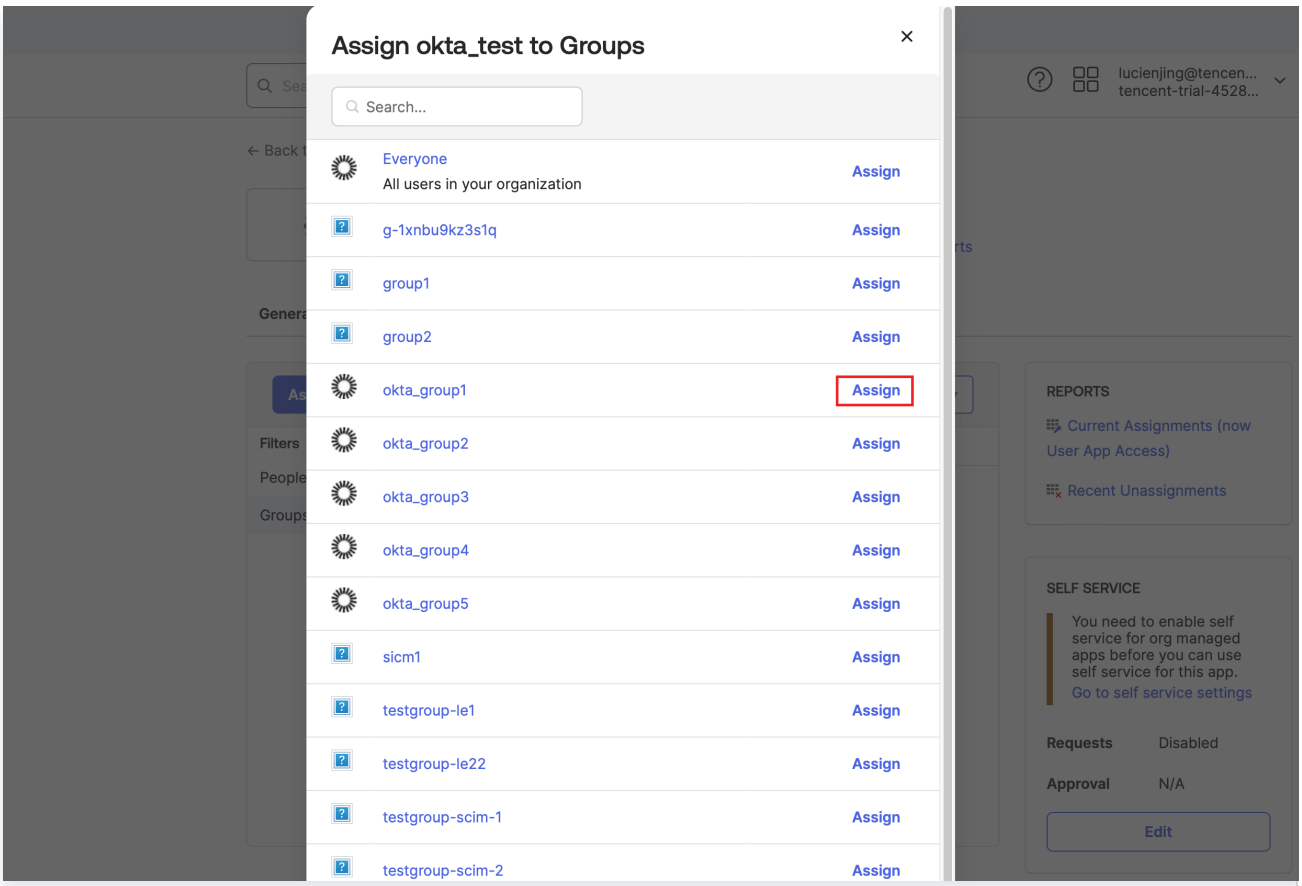
同步用户组需要两步：先通过 Assignments 将用户组分配到应用，再通过 Push Groups 将用户组同步到身份中心。

1. 将用户组分配到应用。

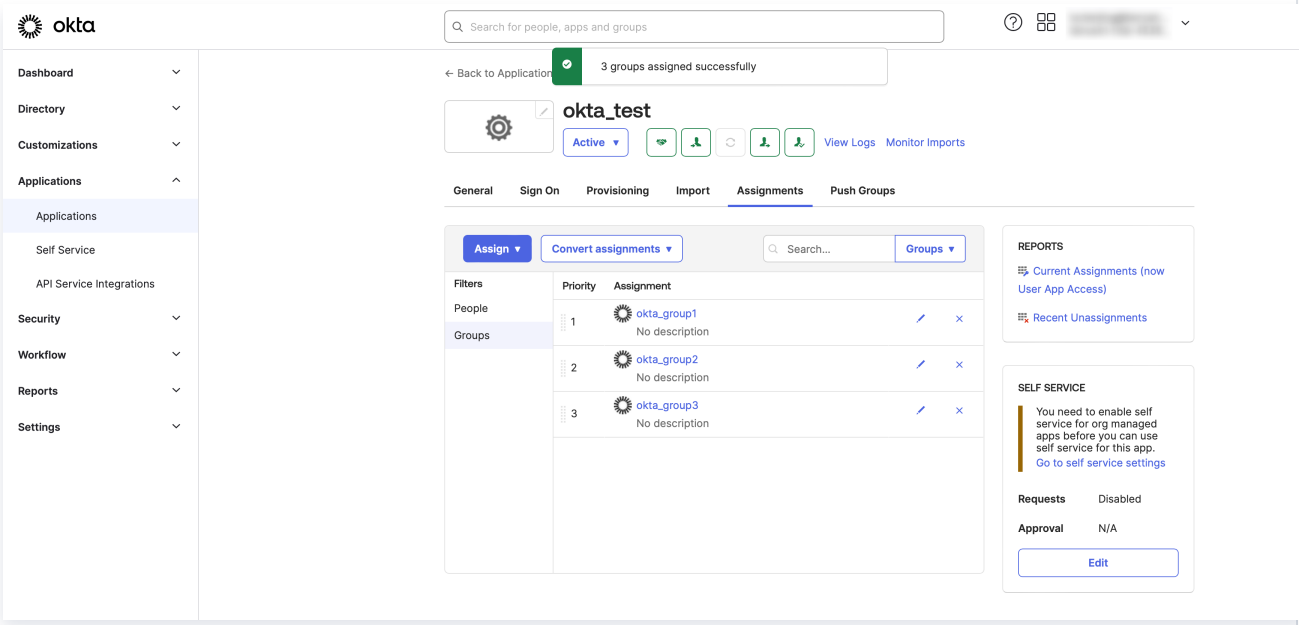
   1.1 在 Assignments 页面，单击 Assign 按钮，选择 Assign to Groups。



   1.2 在 Assign okta_test to Groups 弹窗中，选择目标用户组，单击 Assign。在新窗口单击 Save and Go Back，完成分配。

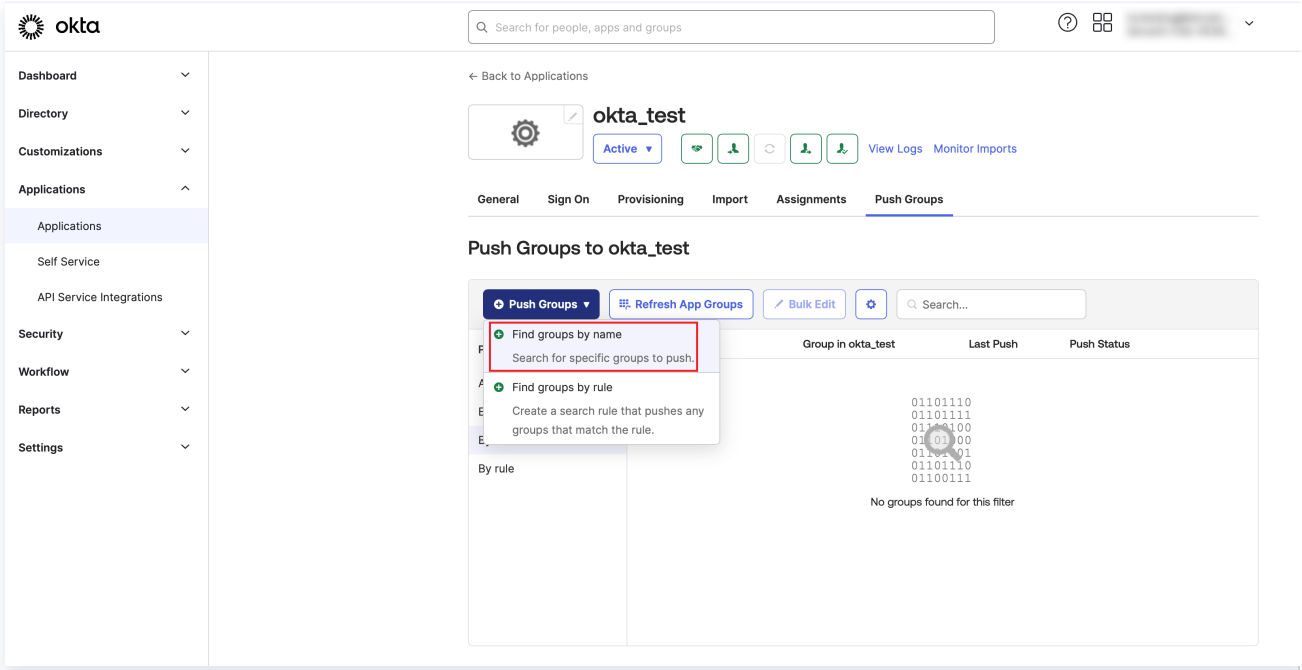


1.3 已分配的用户展示在 Groups 页面。

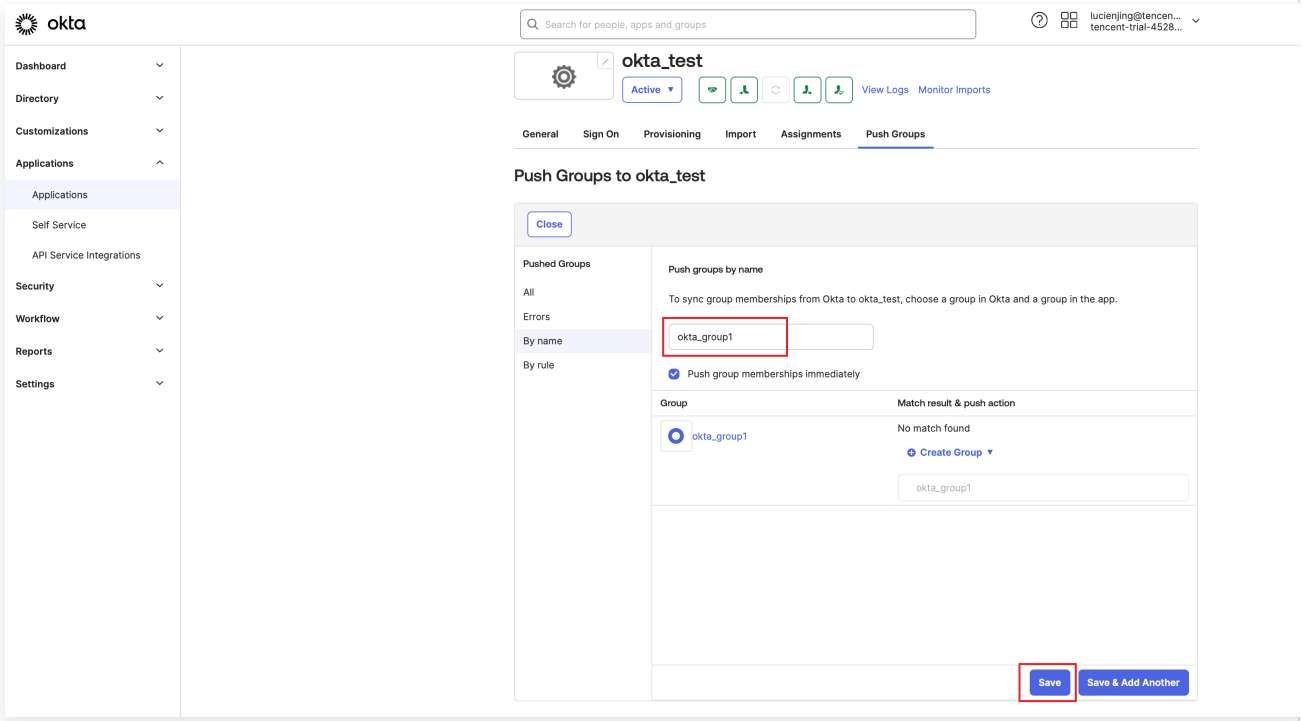


2. 通过 Push Groups 将用户组同步到身份中心。

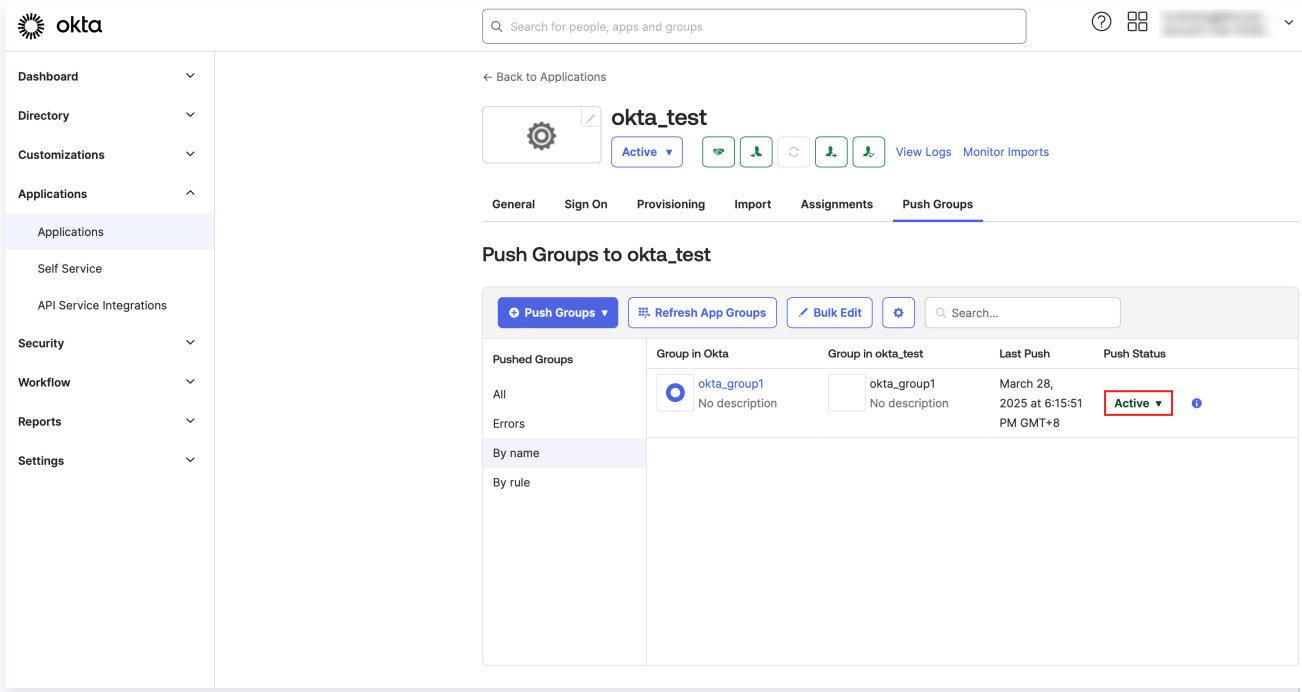
2.1 在 Push Groups 页面，单击 Push Groups，选择 Find groups by name。



2.2 搜索用户组名称并选中，单击 **Save**，开始同步目标用户组。



2.3 同步成功的用户组展示在 **Push Groups** 页面。



结果验证

1. 登录集团账号管理 > 身份中心 。
2. 单击左侧导航栏的**用户管理** > **用户组**，查看用户组列表，同步的用户组的**来源**会自动标识为**外部导入**。

通过 SCIM 同步 Onelogin 示例

Onelogin 同步用户

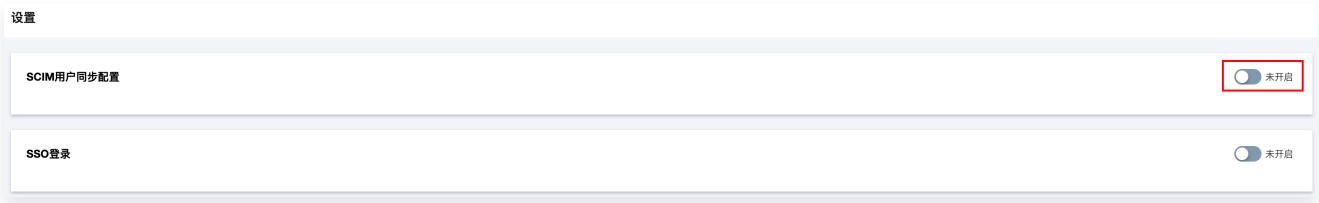
最近更新时间：2025-01-06 15:09:58

本文主要为您介绍通过 SCIM 协议，将 Onelogin 中的用户同步到腾讯云身份中心。

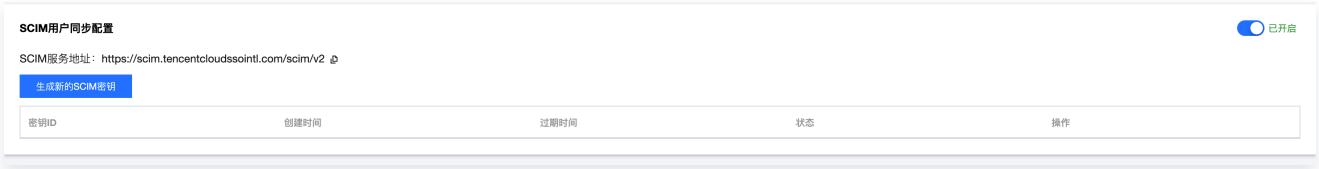
在身份中心配置

步骤一：开启 SCIM 同步

1. 登录集团账号管理 > 身份中心 。
2. 在左侧导航栏，单击**用户管理** > **设置**。
3. 在 **SCIM 用户同步配置**区域，单击，在弹出的窗口单击开启，启用 SCIM 同步。



4. 启用后，在 **SCIM 用户同步配置**区域，查看或复制 **SCIM 服务端地址**，在外部 IdP 中配置 SCIM 同步时会使用该地址。
   - 中国站：https://scim.tencentcloudsso.com/scim/v2
   - 国际站：https://scim.tencentcloudssointl.com/scim/v2

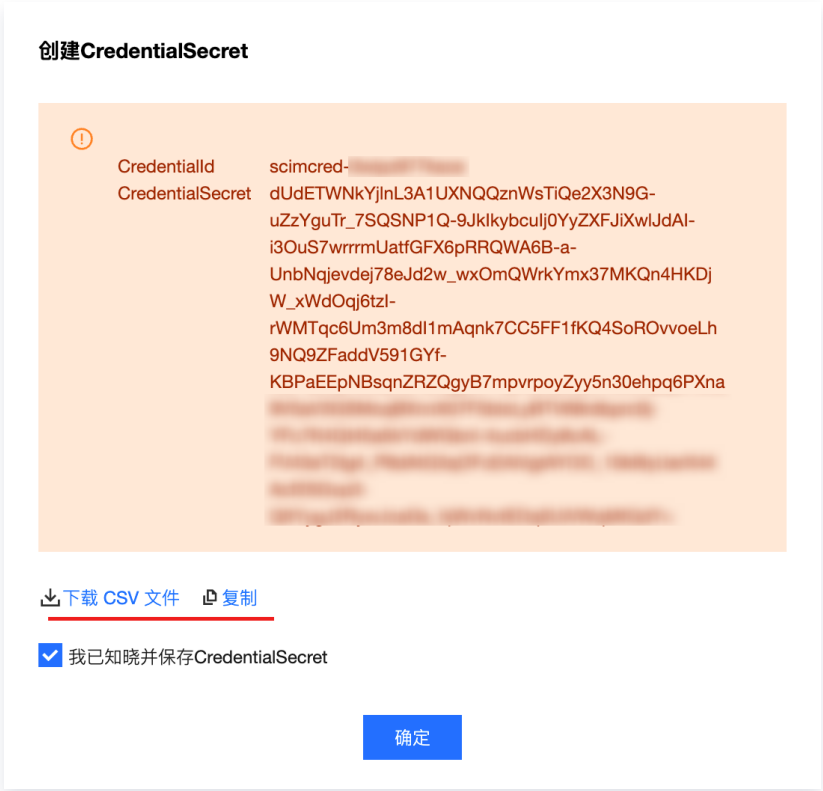


步骤二：创建 SCIM 密钥

1. 在 **SCIM 用户同步配置**区域，单击**生成新的 SCIM 密钥**。

2. 在**创建 CredentialSecret** 对话框中，您可以通过**下载 CSV 文件**或**复制**来保存 SCIM 密钥。保存好密钥后，单击**确定**。

> ⚠ **注意：**
> 在 IdP 仅粘贴 **CredentialSecret** 的部分，不需要 **CredentialId**，请注意检查。

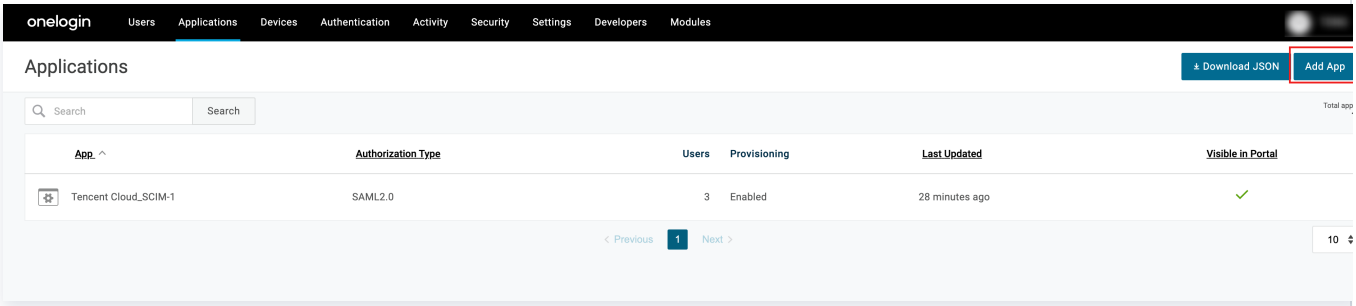


在 Onelogin 管理 SCIM 同步用户

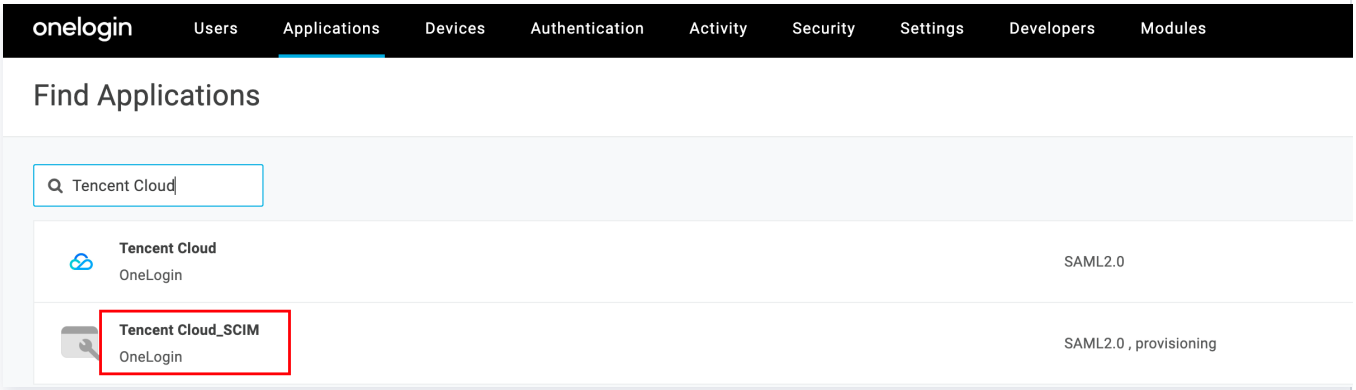
在 Onelogin 配置 SCIM 同步用户

步骤一：创建应用程序

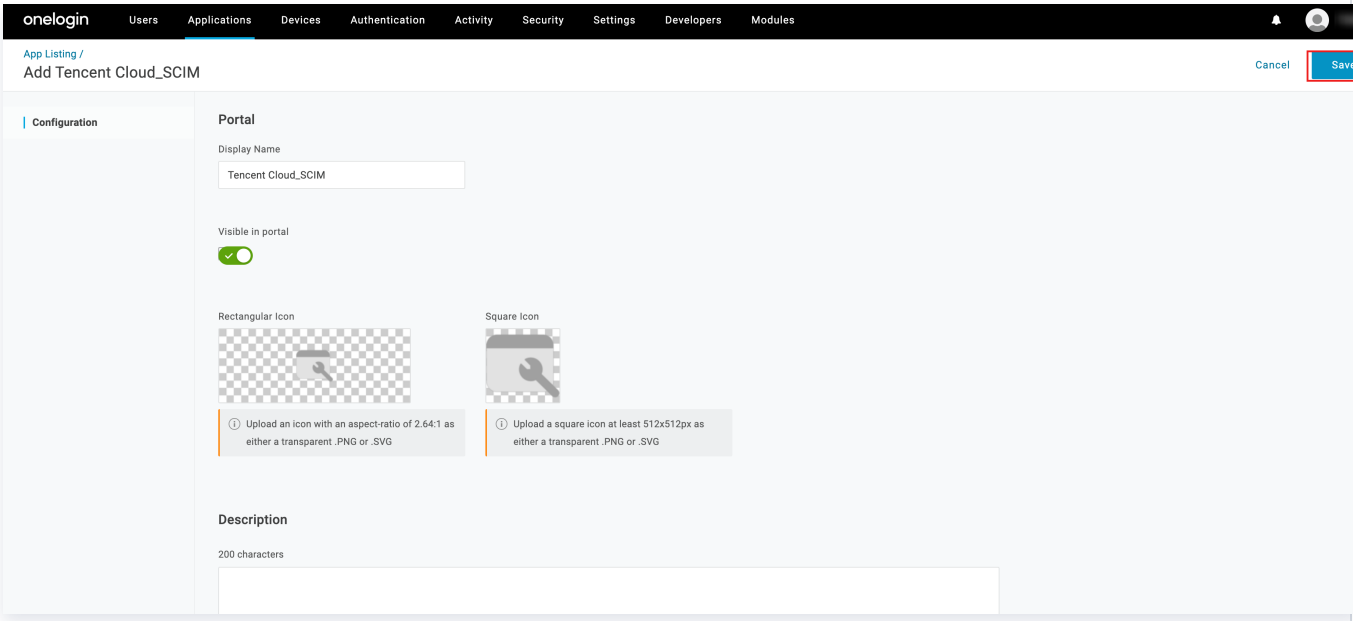
1. 管理员登录 Onelogin，在顶部菜单选择 **Applications** > **Applications**。
2. 在 **Applications** 页面，单击 **Add App**。



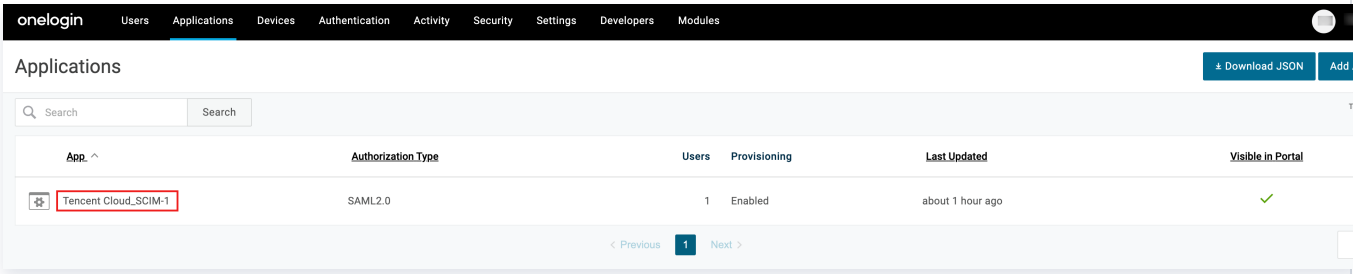
3. 在 Find Applications 页面，单击选择 Tencent Cloud_SCIM。



4. 进入Tencent Cloud_SCIM 应用，修改名称后，单击 Save。



5. 创建完成，可以在列表中查看。

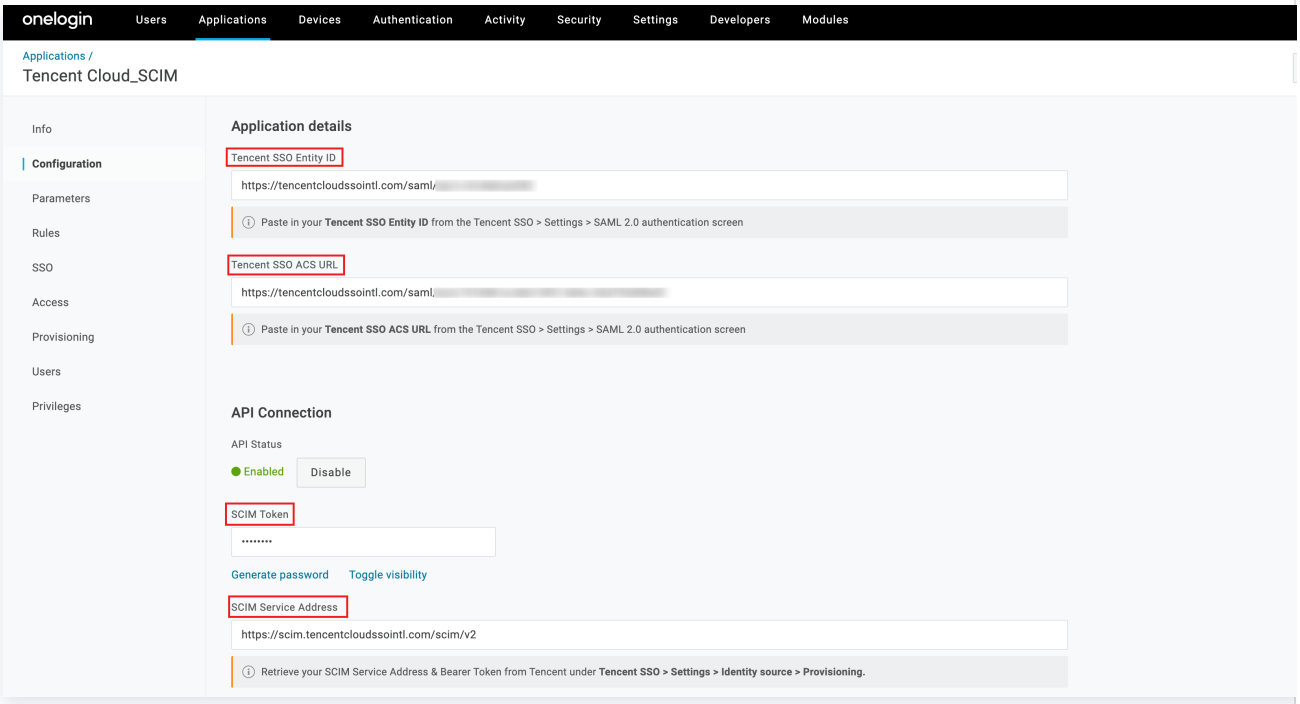


步骤二：配置应用程序

1. 在 Configuration 页面填写信息，获取方式如下：
   - 在 Applications details 区域，输入 ACS URL、Entity ID。

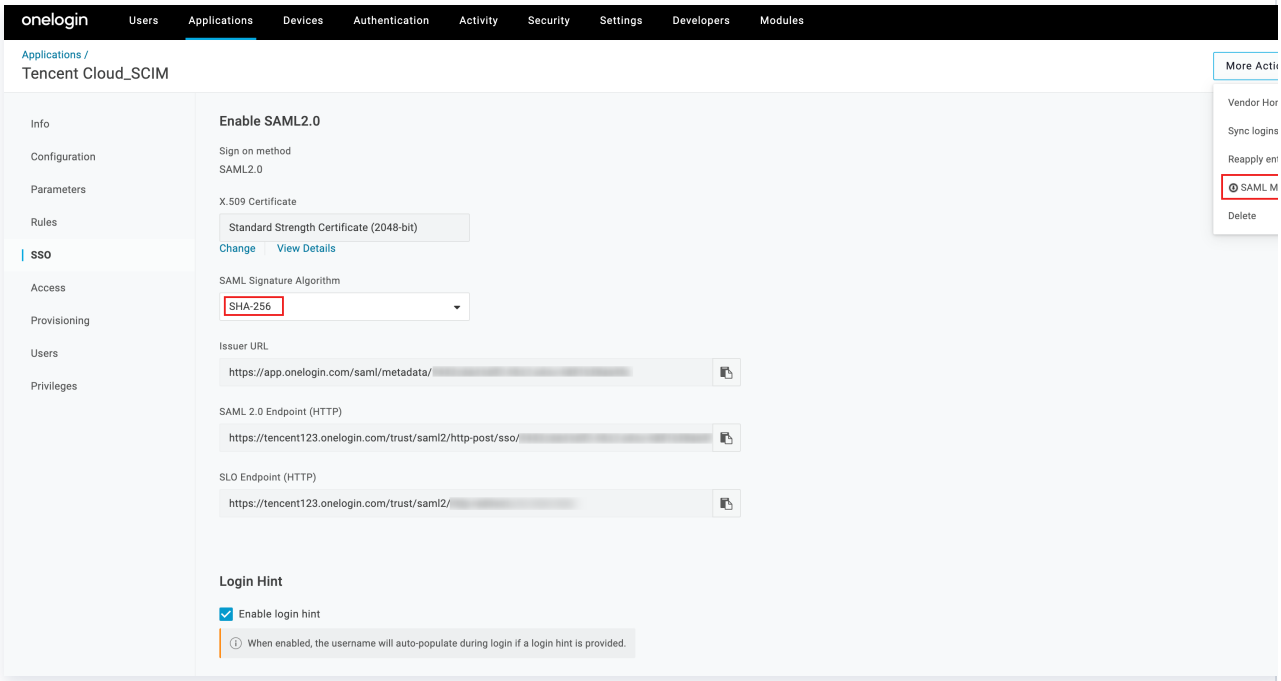
     该地址从 管理服务提供商（SP）信息 获取。
   - 在 API Connection 区域，输入SCIM Token（CredentialSecret）、SCIM 服务端地址。并将状态改为 Enabled。

     该 SCIM 密钥请通过 步骤二：创建 SCIM 密钥 获取。

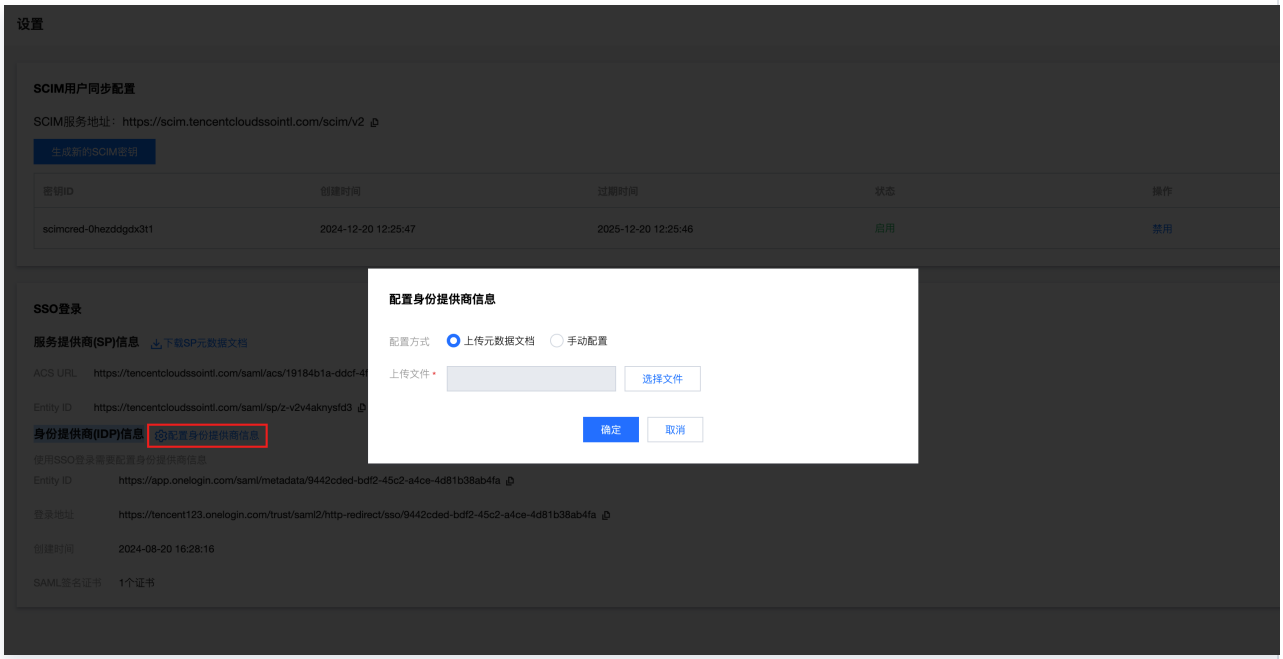


2. 在 SSO 中，SAML Signature Algorithm 协议切换成 SHA-256（默认为 SHA-1，身份中心不支持该协议）。

   2.1 单击 Save，在 More Actions 中下载 SAML Metadata。

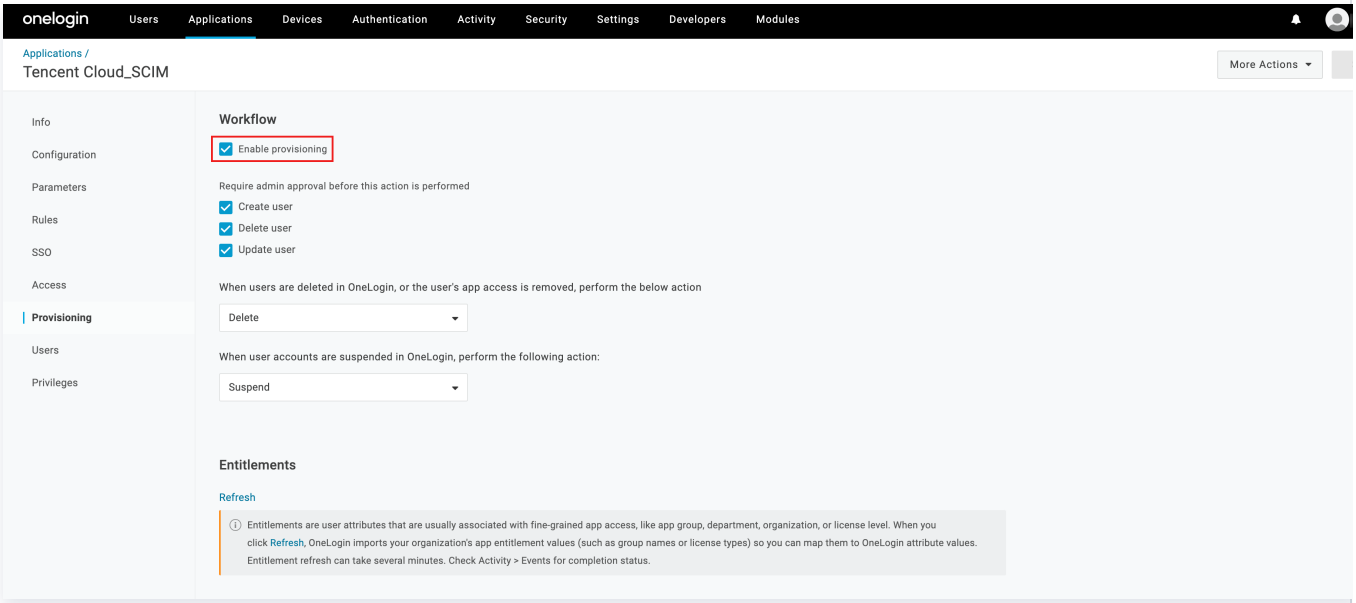


2.2 在**集团账号管理** > **身份中心管理** > 设置 > SSO 登录的**身份提供商(IDP)信息**中，上传元数据文档，选择上的 SAML Metadata 文件。



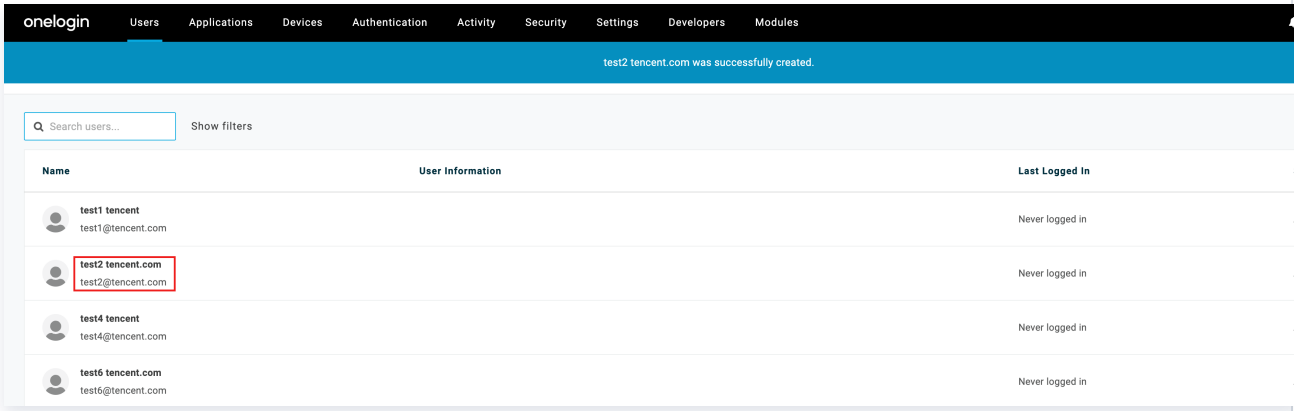
2.3 至此，完成了身份中心和 Onelogin 关联的 SSO 配置、SCIM 配置。

3. 在 **Provisioning** 中，打开自动同步开关：勾选 **Workflow** 中的 **enable Provisioning**，单击 **Save**。

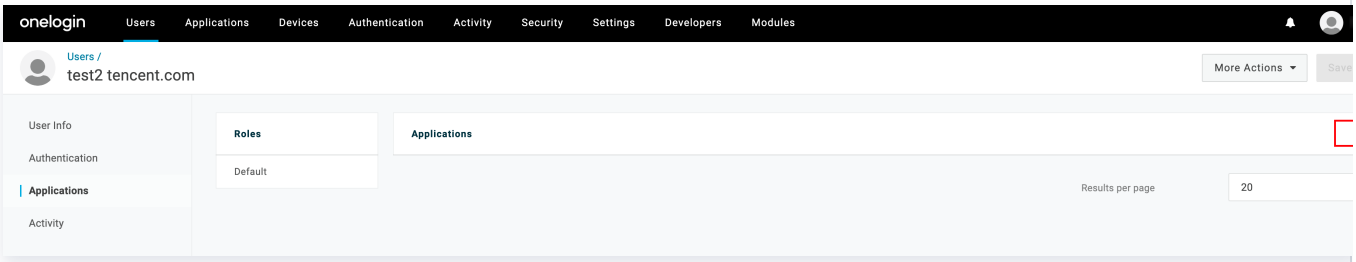


步骤三：同步用户

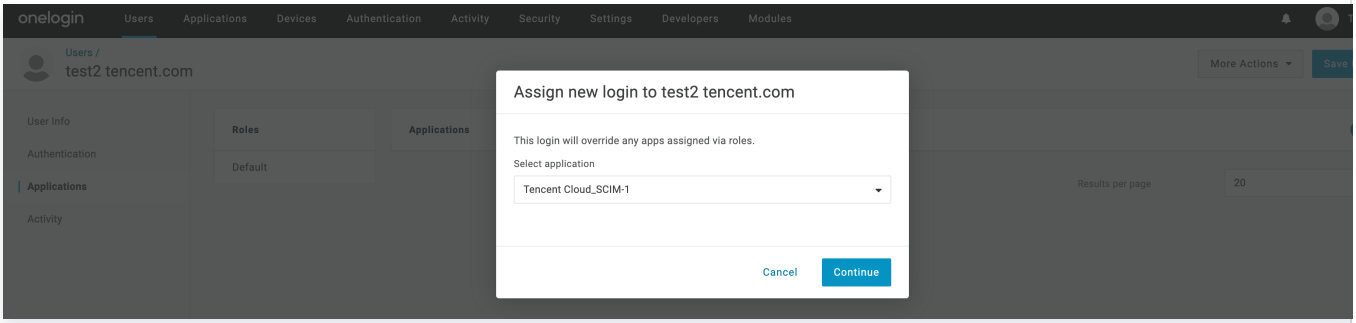
1. 在 Users > Users 用户列表，单击需要同步的用户名称，进入用户详情页。此处选择的是用户 test2。



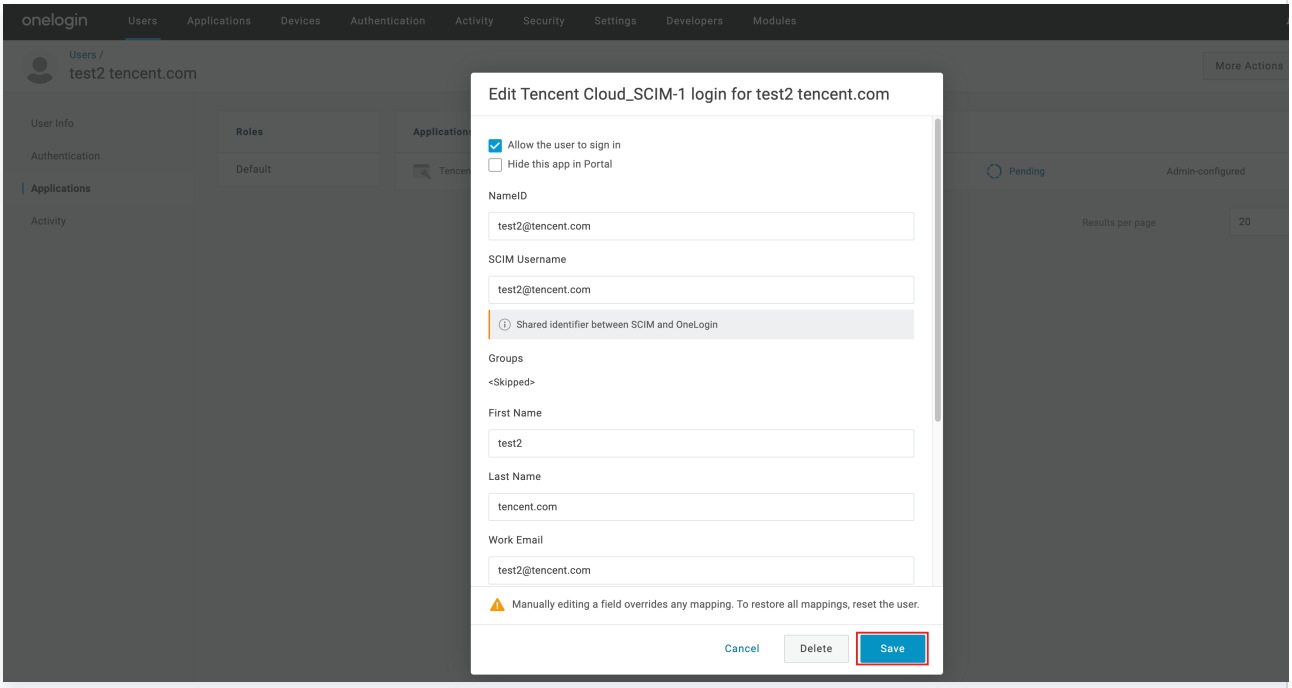
2. 左侧选择 Applications，单击+，将 test2 分配到目标应用中。



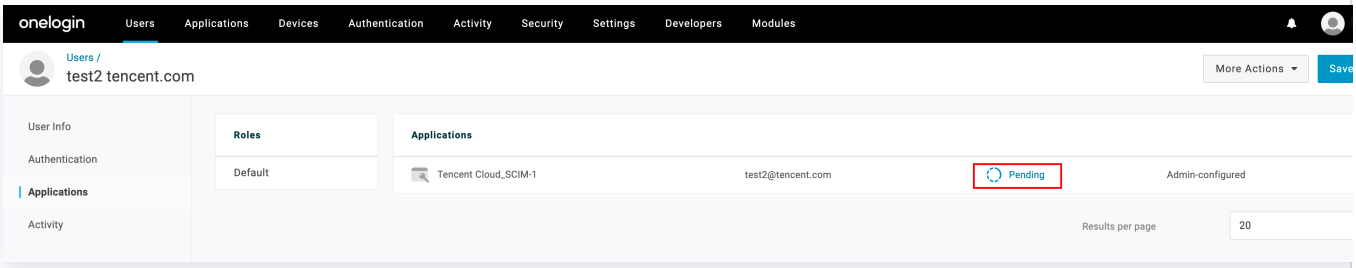
3. 在 Select application 中，选择 步骤一中创建的应用 ，单击 Continue。



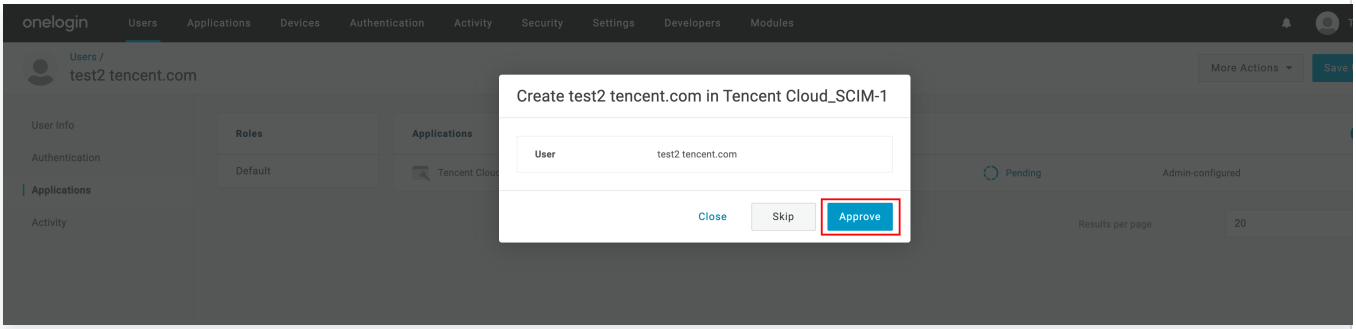
4. 在编辑表单中，修改用户名、邮箱等信息（可选），单击 **Save**。



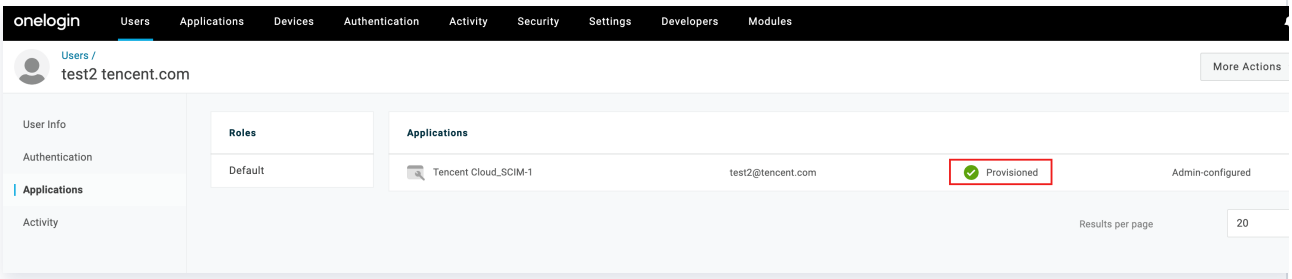
5. 此时，同步状态是 Pending，单击 **Pending**。



6. 确认同步信息，单击 **Approve**。



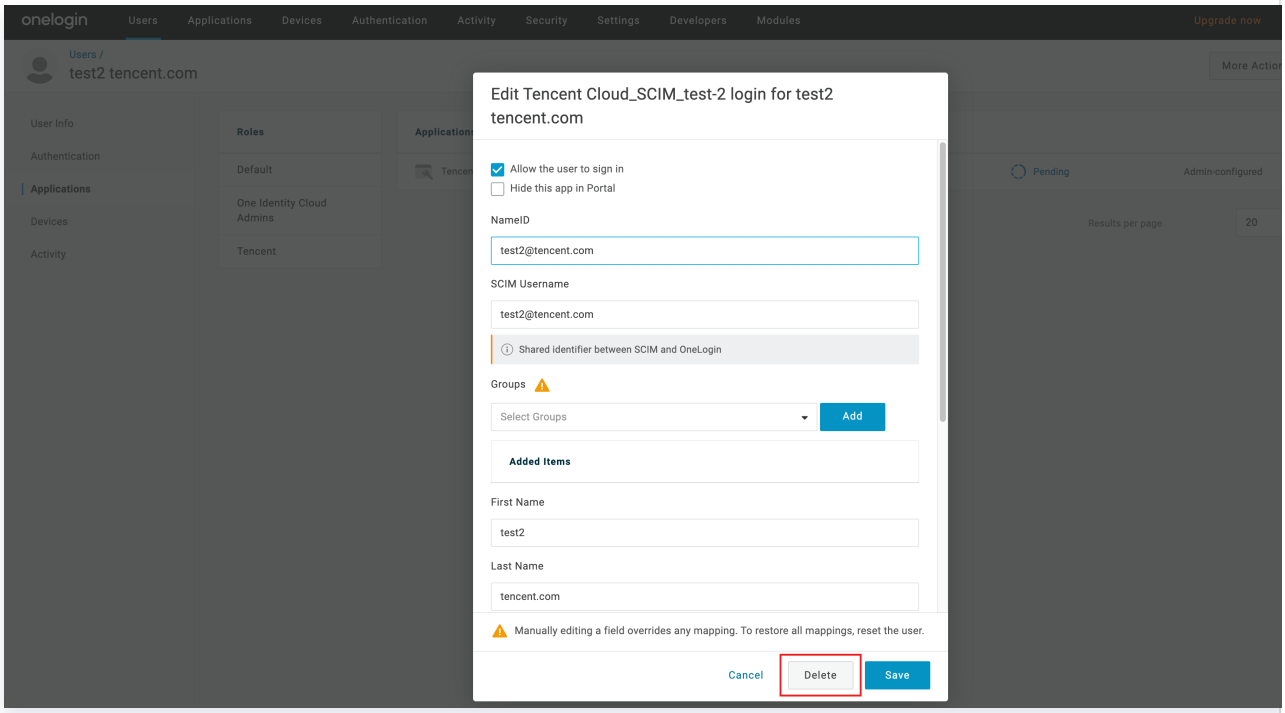
7. 等待状态从 **Provisioning**，变更为 **Provisioned**，即为同步成功。



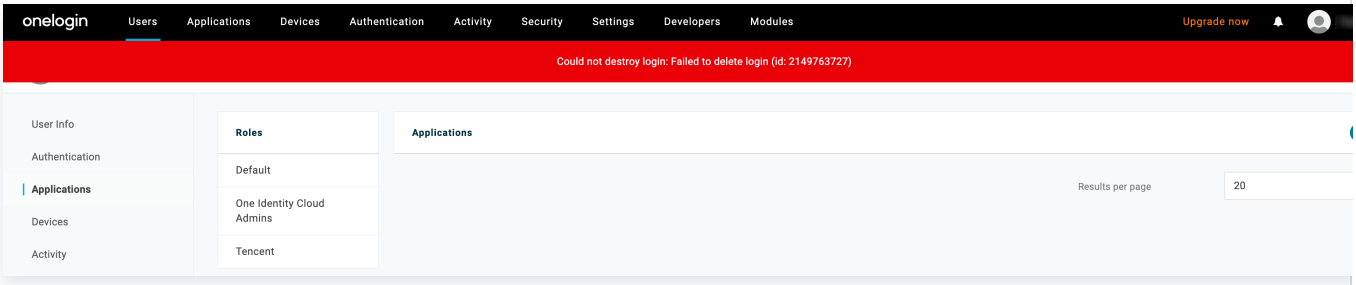
8. 在 身份中心 > **用户管理** > **用户**，查看同步结果，test2同步成功，来源为**外部导入**。

在 Onelogin 删除 SCIM 同步用户

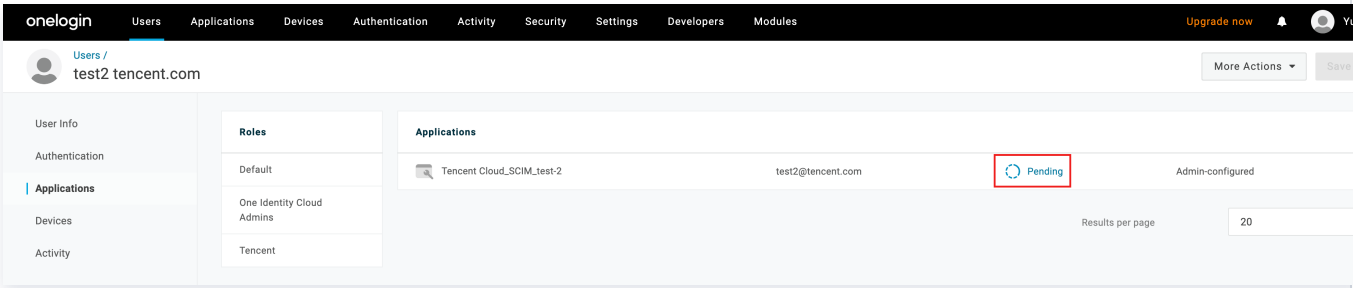
1. 管理员登录 Onelogin，在 **Users** > **Users** 进入用户 **test2** 的详情页，左侧选择 **Applications**， 在 Tencent
   用弹窗单击 **Delete**。



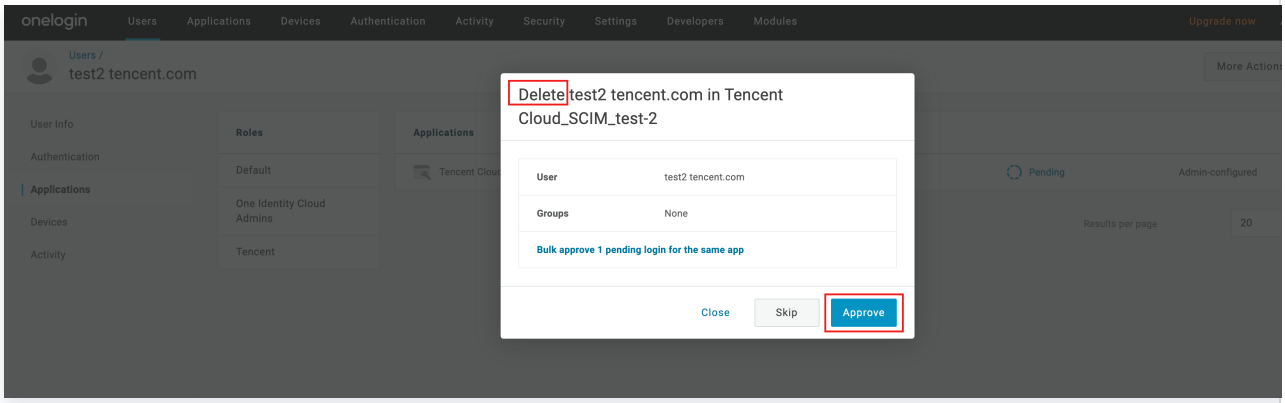
2. 提示删除失败，此时需要刷新该页面。



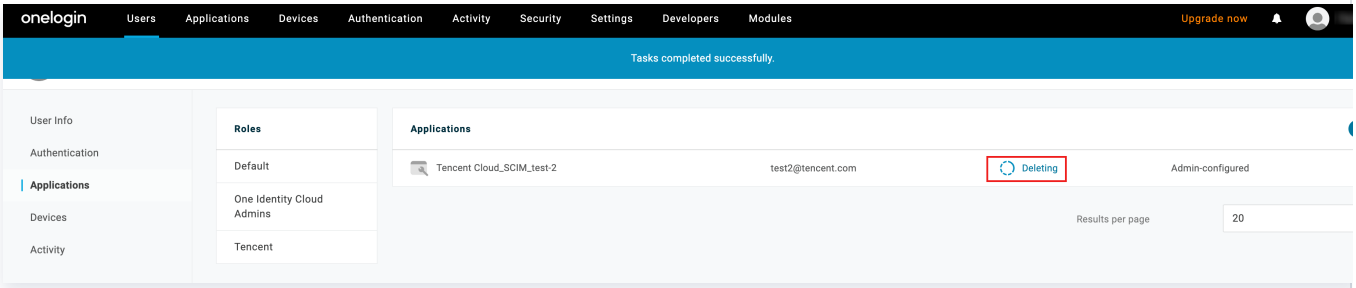
3. 刷新后，点击 **Pending** 区域。



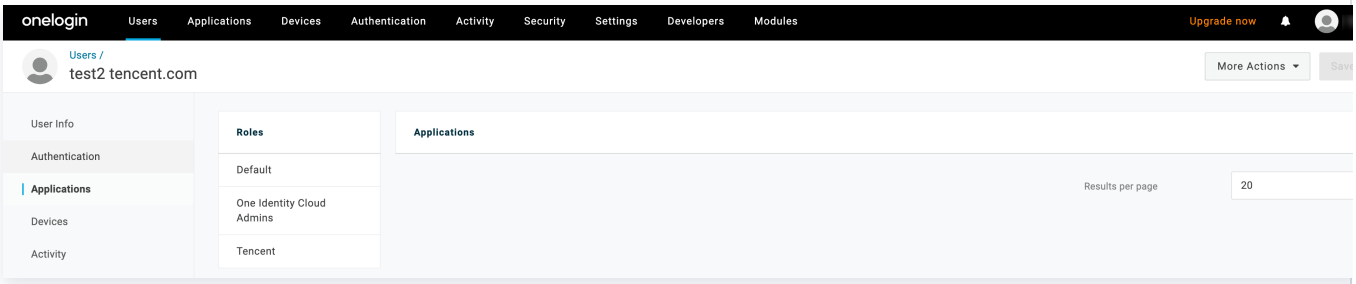
4. 在 Delete 弹窗，确认信息后，单击 **Approve**。



5. 提示任务成功，状态变更为 **Deleting**。



6. 删除成功后，应用为空。



7. 在 身份中心 > **用户管理** > **用户**，查看删除结果，test2 删除成功。

Onelogin 同步用户组

最近更新时间：2025-01-06 15:09:58

操作场景

Onelogin 同步用户组操作较为特殊，不是将 Onelogin 的用户组同步到身份中心，而是 Onelogin 反向拉取身份中心的用户组后，将用户添加到组。

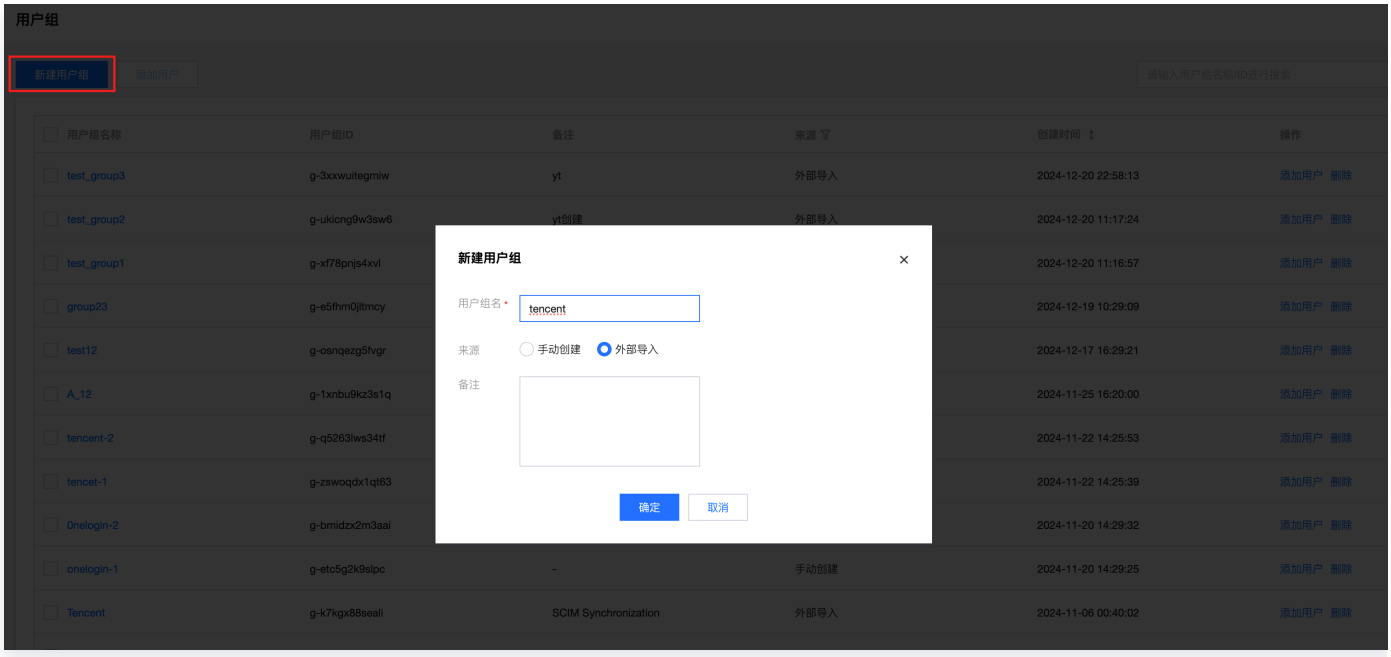
- 方法一：在 Onelogin 先拉取身份中心的用户组。配置用户同步时，Groups 选择身份中心的用户组。
- 方法二：直接在身份中心，将同步的用户添加到组。

操作步骤

方法一 拉取身份中心的用户组

步骤一：在身份中心新建用户组

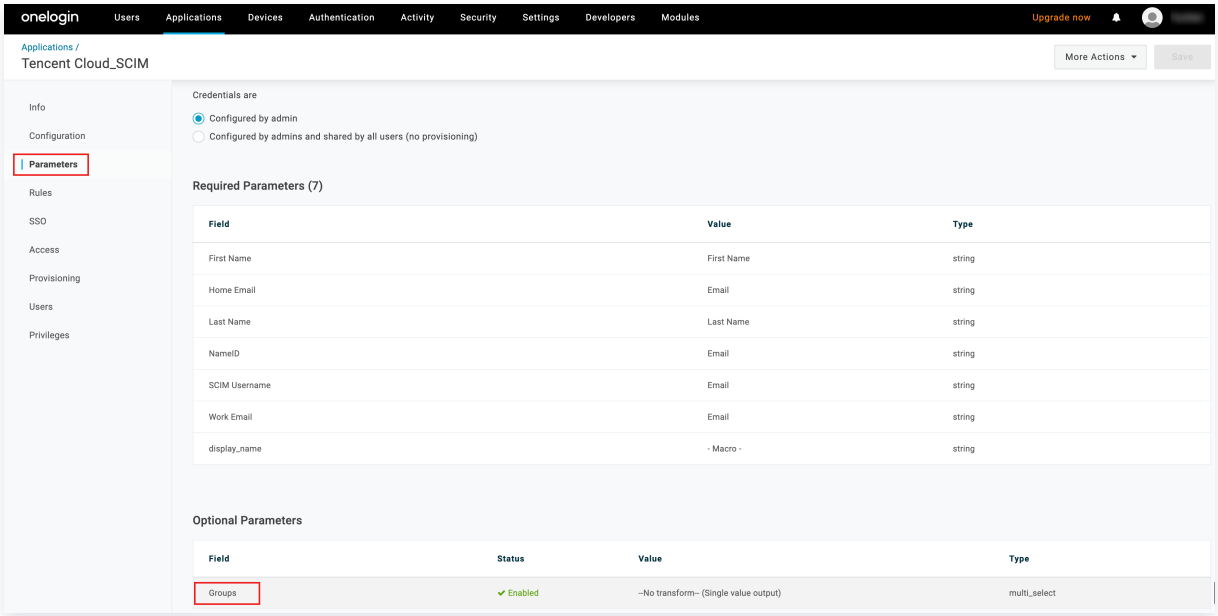
1. 在 身份中心 > **用户管理** > **用户组**，新建用户组，来源选择为**外部导入**，单击**确定**，创建用户组成功。
   - 可以通过 接口 创建外部导入类型的用户组，GroupType 选 Synchronized。
   - 通过控制台创建，需要加入白名单才可更改**来源**。



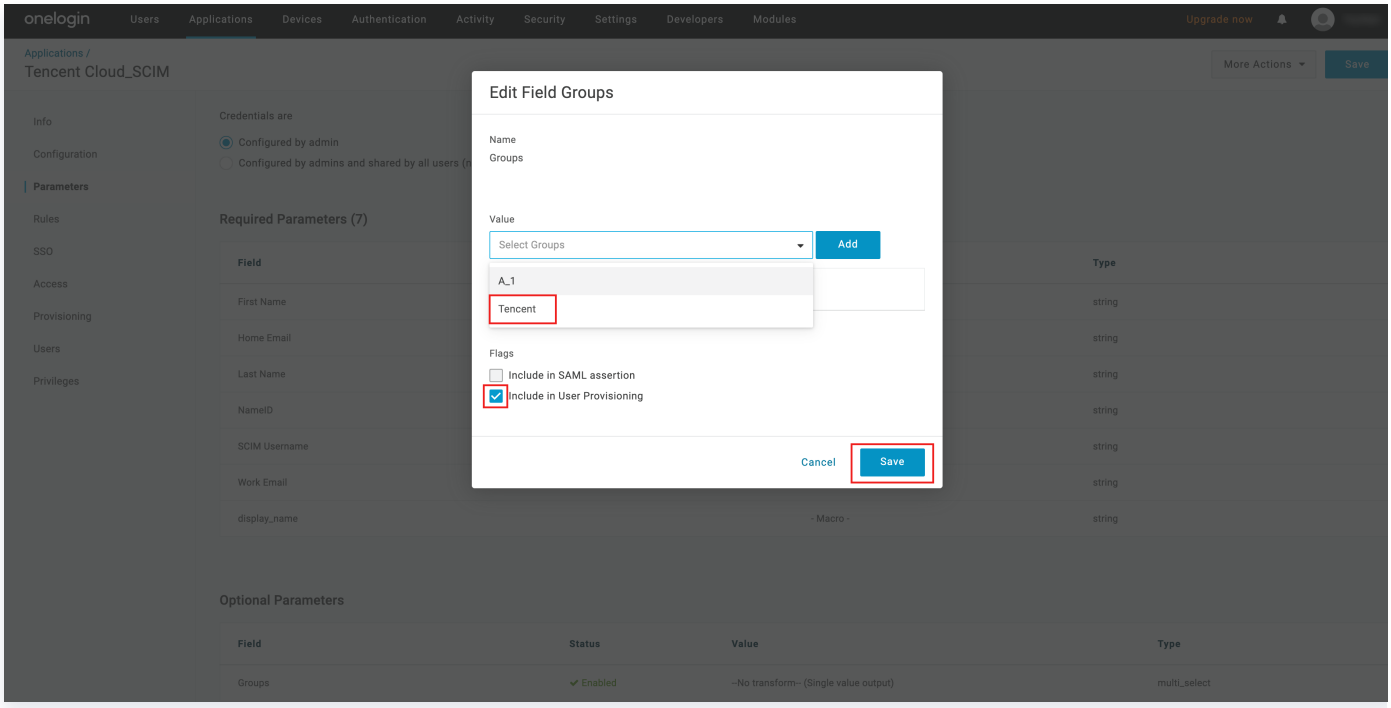
步骤二：在 Onelogin 拉取身份中心的用户组

1. 管理员登录 Onelogin，在顶部菜单选择 Applications > Applications。

2. 在 Tencent Cloud_SCIM 应用中的选择 **Parameters**，在 **Optional Parameters** 中，单击 **Group**。

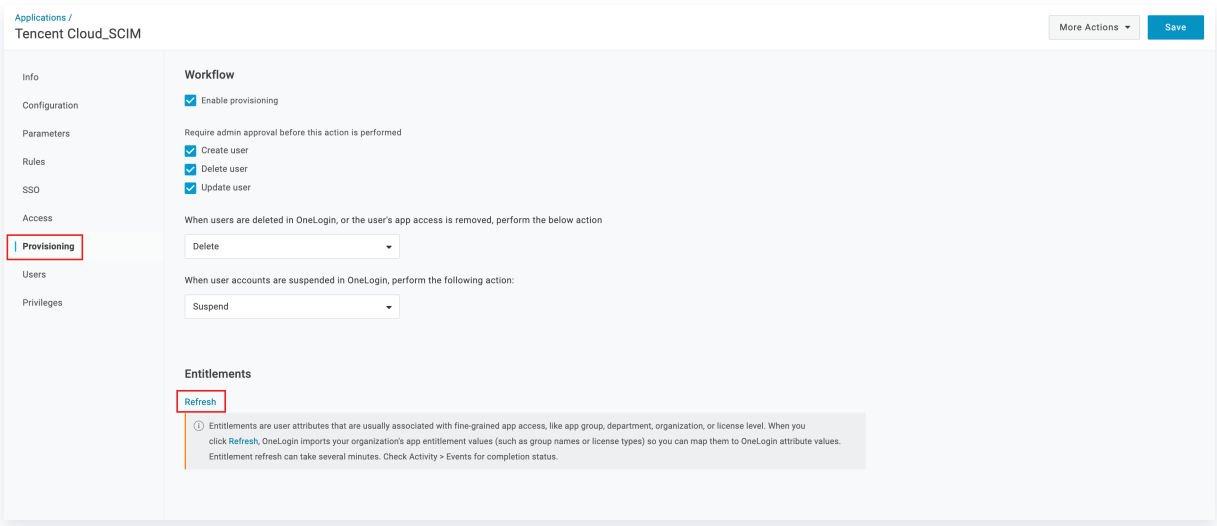


3. 在 **Edit Field Group** 中，在 Value 下拉框，可以看到身份中心的用户组，选择目标用户组后，单击 **Add** 添加到表单，勾选 **Include in User Provisioning**，单击 **Save** 。

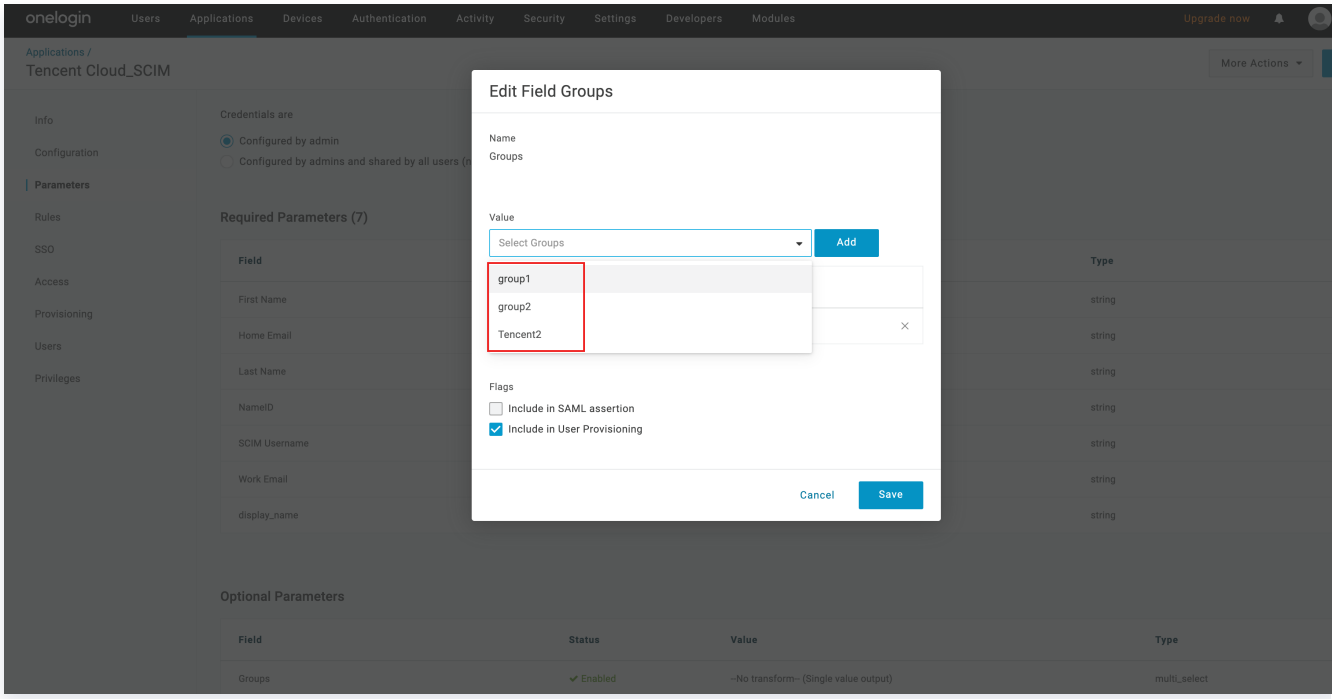


4. 当身份中心新建了用户组，需要在 Onelogin 手动刷新，才能在 **Edit Field Group** 弹框中出现。

   4.1 单击左侧 **Provisioning**，在页面点击 **Refresh**，完成刷新。

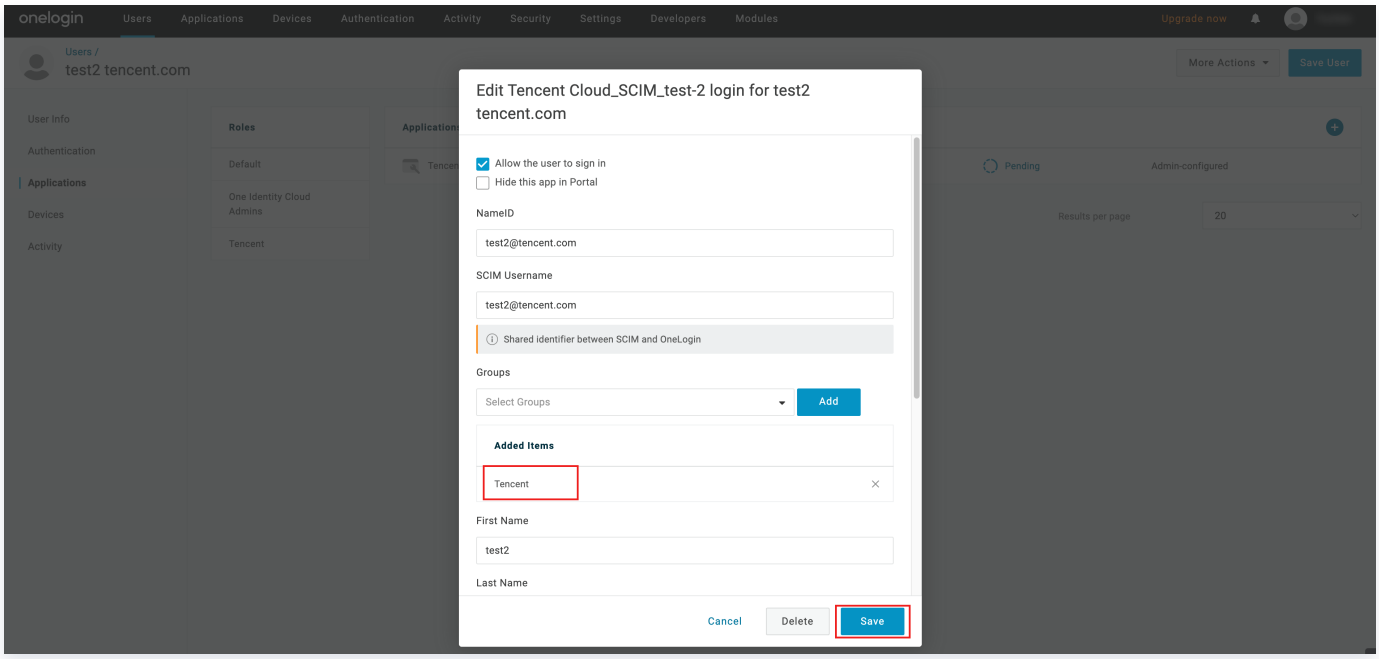


4.2 回到 **Parameters**，在 **Edit Field Group** 中，下拉框可以看到新的用户组。

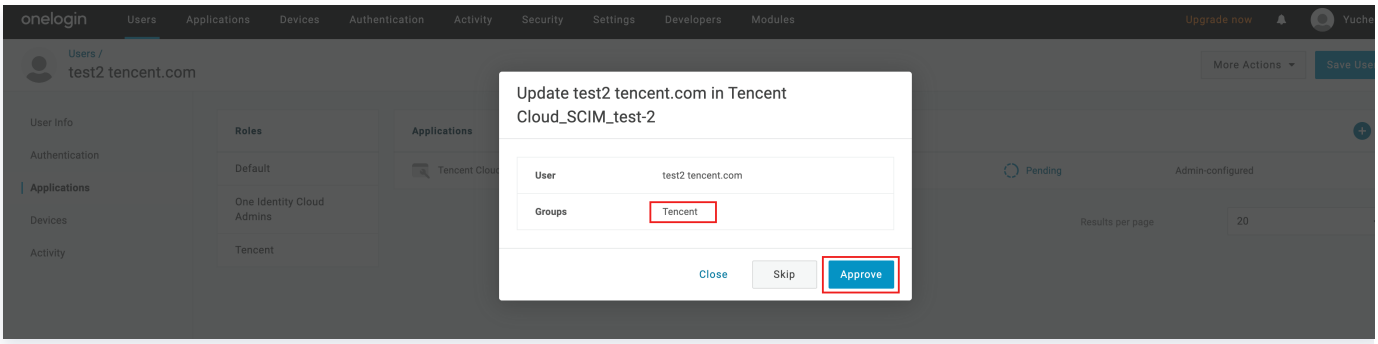


步骤三：同步用户组

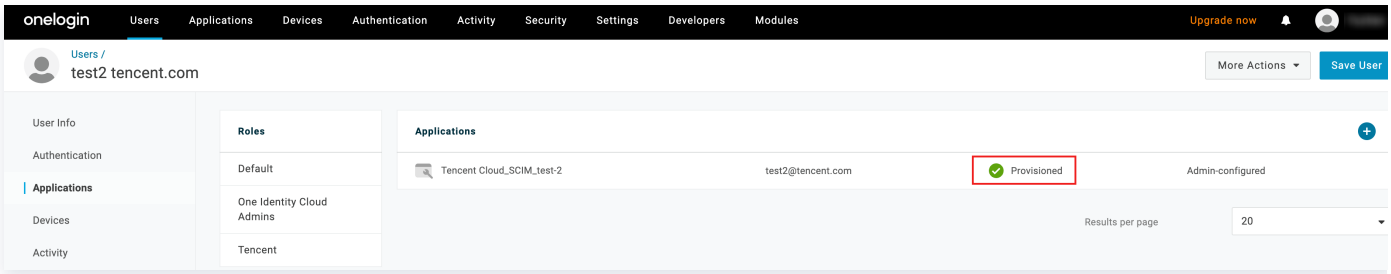
1. 以上操作完成后，在 同步用户 的配置中，**Groups** 会从 <skipped> 变更成可选，选择 test2 需要关联的用户组，此处选择的是 Tencent。



2. 单击状态 **Pending** 区域，弹窗确认同步的用户、用户组信息后，单击 **Approve**。



3. 等待状态从 **Provisioning**，变更为 **Provisioned**，即为同步成功。

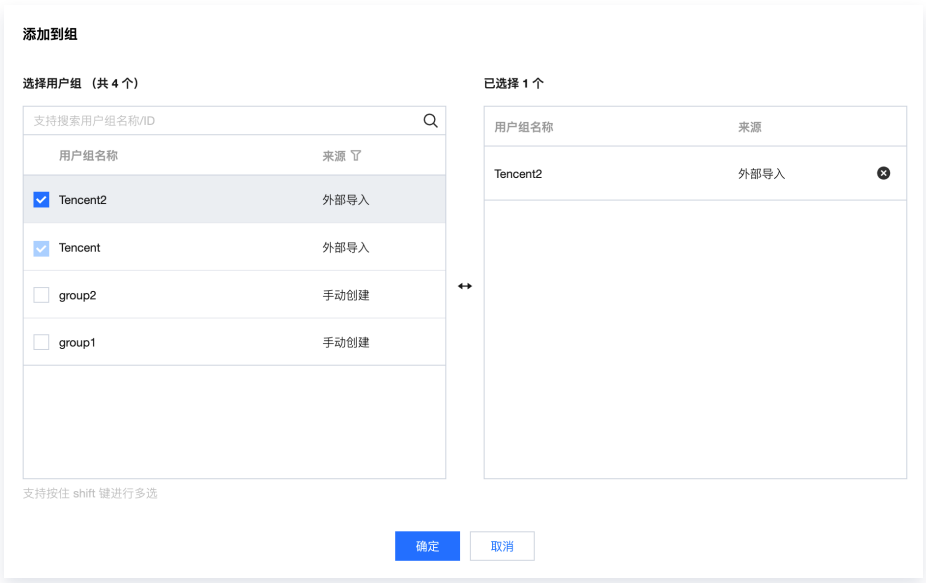


4. 检查结果，在 身份中心 > **用户管理** > **用户**，test2 的用户详情页，看到已加入用户组 **Tencent**。

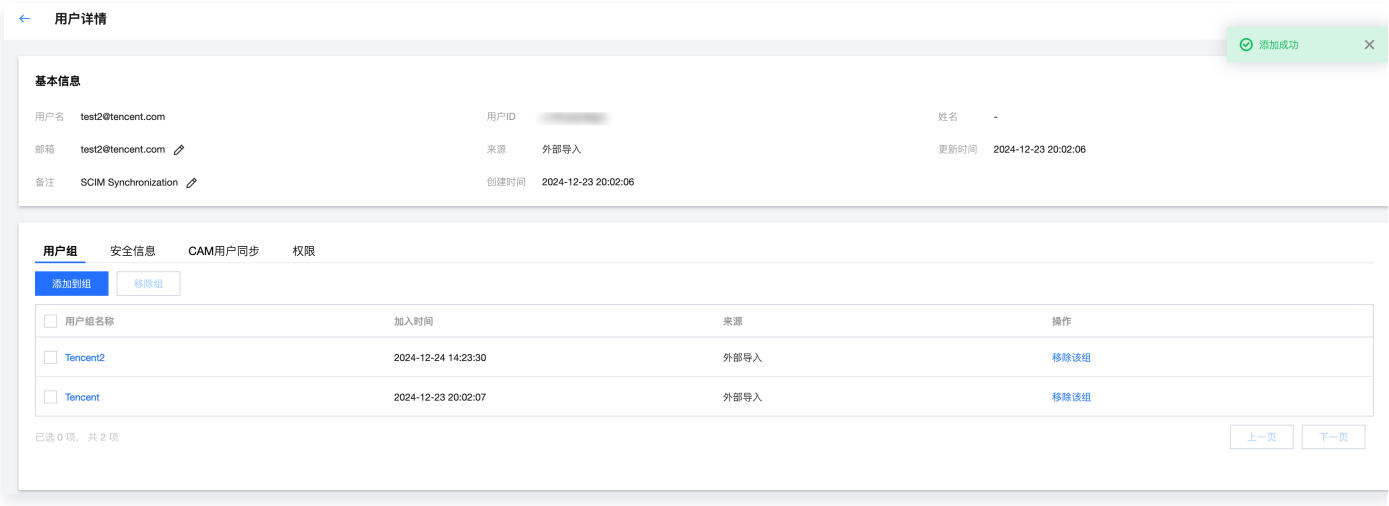
方法二 在身份中心，将用户添加到组

1. 在 身份中心 > **用户管理** > **用户**，test2 的用户详情页，单击**添加到组**。

2. 选择任一用户组，单击**确定**。



3. 添加成功，在用户详情页的用户组中查看。



SCIM2.0接口

最近更新时间：2024-11-27 14:46:27

如果自建 IdP 需要集成 SCIM 协议，将用户或用户组同步到身份中心 – 用户管理时，需要关注本文档。使用各身份提供商（例如：Okta、Azure AD等）提供的 SCIM 同步能力时，通常不需要关注本文档。

使用说明

SCIM 2.0接口的实现遵循 RFC 7644，具体请求说明请参见 RFC文档 。
SCIM服务对应的接入点（Endpoint）：

- 中国站：https://scim.tencentcloudsso.com/scim/v2
- 国际站：https://scim.tencentcloudssointl.com/scim/v2

SCIM 接口协议

Discovery Endpoint

/ServiceProviderConfig

功能描述

- 获取服务端支持的功能。

使用约束

- 不需要认证。

请求示例

```
curl https://scim.tencentcloudsso.com/scim/v2/ServiceProviderConfig -H
"Content-type:application/json"
```

返回示例

```
{
    "authenticationSchemes": [
        {
            "description": "Authentication scheme using the OAuth Bearer
Token Standard",
            "documentationUri": "",
            "name": "OAuth Bearer Token",
            "primary": true,
            "specUri": "",
            "type": "oauthbearertoken"
```

```
        }
    ],
    "bulk": {
        "maxOperations": 1000,
        "maxPayloadSize": 1048576,
        "supported": false
    },
    "changePassword": {
        "supported": false
    },
    "documentationUri": "",
    "etag": {
        "supported": false
    },
    "filter": {
        "maxResults": 100,
        "supported": true
    },
    "patch": {
        "supported": true
    },
    "schemas": [
        "urn:ietf:params:scim:schemas:core:2.0:ServiceProviderConfig"
    ],
    "sort": {
        "supported": false
    }
}
```

返回结果显示：

- 支持的功能：patch, filter。
- 不支持的功能：bulk、changePassword、sort、etag。

/ResourceTypes

功能描述

- 获取服务端支持的资源类型，返回 User 和 Group。

请求示例

```
curl https://scim.tencentcloudsso.com/scim/v2/ResourceTypes --header
'Authorization: Bearer <your scim credential>' --header "content-
type:application/json"
```

返回示例

```
{
    "Resources": [
        {
            "description": "User Account",
            "endpoint": "/Users",
            "id": "User",
            "name": "User",
            "schema": "urn:ietf:params:scim:schemas:core:2.0:User",
            "schemaExtensions": [],
            "schemas": [
                "urn:ietf:params:scim:schemas:core:2.0:ResourceType"
            ]
        },
        {
            "description": "Group",
            "endpoint": "/Groups",
            "id": "Group",
            "name": "Group",
            "schema": "urn:ietf:params:scim:schemas:core:2.0:Group",
            "schemaExtensions": [],
            "schemas": [
                "urn:ietf:params:scim:schemas:core:2.0:ResourceType"
            ]
        }
    ],
    "itemsPerPage": 100,
    "schemas": [
        "urn:ietf:params:scim:api:messages:2.0:ListResponse"
    ],
    "startIndex": 1,
    "totalResults": 2
}
```

/Schemas

功能描述

- 获取服务端支持的 Schema，返回 User 和 Group 的详细 Schema。

使用约束

- 支持按资源类型查询。
- 对协议中约定的字段名和字段值不区分大小写。
- 只支持下文文档描述的字段。

请求示例

```
The schema to request all resources.
    curl https://scim.tencentcloudsso.com/scim/v2/Schemas --header
'Authorization: Bearer <your scim credential>' --header "content-
type:application/json"
The schema to request users.
    curl
https://scim.tencentcloudsso.com/scim/v2/Schemas/urn:ietf:params:scim:sc
hemas:core:2.0:User --header 'Authorization: Bearer <your scim
credential>' --header "content-type:application/json"
The schema to request user groups.
    curl
https://scim.tencentcloudsso.com/scim/v2/Schemas/urn:ietf:params:scim:sc
hemas:core:2.0:Group --header 'Authorization: Bearer <your scim
credential>' --header "content-type:application/json"
```

返回示例

- 用户资源 Schema

```
{
      "attributes": [
        {
          "caseExact": false,
          "description": "Unique identifier for the User, typically
used by the user to directly authenticate to the service provider.
Each User MUST include a non-empty userName value. This identifier
MUST be unique across the service provider's entire set of Users.
REQUIRED.",
          "multiValued": false,
          "mutability": "readWrite",
```

```
          "name": "userName",
          "required": true,
          "returned": "default",
          "type": "string",
          "uniqueness": "server"
        },
        {
          "description": "The components of the user's real name.
Providers MAY return just the full name as a single string in the
formatted sub-attribute, or they MAY return just the individual
component attributes using the other sub-attributes, or they MAY
return both. If both variants are returned, they SHOULD be describing
the same name, with the formatted name indicating how the component
attributes should be combined.",
          "multiValued": false,
          "mutability": "readWrite",
          "name": "name",
          "required": false,
          "returned": "default",
          "subAttributes": [
            {
              "caseExact": false,
              "description": "The family name of the User, or last
name in most Western languages (e.g., 'Jensen' given the full name
'Ms. Barbara J Jensen, III').",
              "multiValued": false,
              "mutability": "readWrite",
              "name": "familyName",
              "required": false,
              "returned": "default",
              "type": "string",
              "uniqueness": "none"
            },
            {
              "caseExact": false,
              "description": "The given name of the User, or first
name in most Western languages (e.g., 'Barbara' given the full name
'Ms. Barbara J Jensen, III').",
              "multiValued": false,
              "mutability": "readWrite",
```

```
            "name": "givenName",
            "required": false,
            "returned": "default",
            "type": "string",
            "uniqueness": "none"
          }
        ],
        "type": "complex"
      },
      {
        "caseExact": false,
        "description": "The name of the User, suitable for display
to end-users. The name SHOULD be the full name of the User being
described, if known.",
        "multiValued": false,
        "mutability": "readWrite",
        "name": "displayName",
        "required": false,
        "returned": "default",
        "type": "string",
        "uniqueness": "none"
      },
      {
        "description": "A Boolean value indicating the User's
administrative status.",
        "multiValued": false,
        "mutability": "readWrite",
        "name": "active",
        "required": false,
        "returned": "default",
        "type": "boolean"
      },
      {
        "description": "Email addresses for the user. The value
SHOULD be canonicalized by the service provider, e.g.,
'bjensen@example.com' instead of 'bjensen@EXAMPLE.COM'. Canonical type
values of 'work', 'home', and 'other'.",
        "multiValued": true,
        "mutability": "readWrite",
        "name": "emails",
```

```
          "required": false,
          "returned": "default",
          "subAttributes": [
            {
              "caseExact": false,
              "description": "Email addresses for the user. The value
SHOULD be canonicalized by the service provider, e.g.,
'bjensen@example.com' instead of 'bjensen@EXAMPLE.COM'. Canonical type
values of 'work', 'home', and 'other'.",
              "multiValued": false,
              "mutability": "readWrite",
              "name": "value",
              "required": false,
              "returned": "default",
              "type": "string",
              "uniqueness": "none"
            },
            {
              "canonicalValues": [
                "work",
                "home",
                "other"
              ],
              "caseExact": false,
              "description": "A label indicating the attribute's
function, e.g., 'work' or 'home'.",
              "multiValued": false,
              "mutability": "readWrite",
              "name": "type",
              "required": false,
              "returned": "default",
              "type": "string",
              "uniqueness": "none"
            },
            {
              "description": "A Boolean value indicating the 'primary'
or preferred attribute value for this attribute, e.g., the preferred
mailing address or primary email address. The primary attribute value
'true' MUST appear no more than once.",
              "multiValued": false,
```

```
            "mutability": "readWrite",
            "name": "primary",
            "required": false,
            "returned": "default",
            "type": "boolean"
          }
        ],
        "type": "complex"
      }
    ],
    "description": "User Account",
    "id": "urn:ietf:params:scim:schemas:core:2.0:User",
    "name": "User",
    "schemas": [
      "urn:ietf:params:scim:schemas:core:2.0:Schema"
    ]
  }
```

- 用户组资源 Schema

```
{
    "attributes": [
      {
        "caseExact": false,
        "description": "A human-readable name for the Group.
REQUIRED.",
        "multiValued": false,
        "mutability": "readWrite",
        "name": "displayName",
        "required": true,
        "returned": "default",
        "type": "string",
        "uniqueness": "none"
      },
      {
        "description": "A list of members of the Group.",
        "multiValued": true,
        "mutability": "readWrite",
        "name": "members",
```

```
          "required": false,
          "returned": "default",
          "subAttributes": [
            {
              "caseExact": false,
              "description": "Identifier of the member of this
Group.",
              "multiValued": false,
              "mutability": "immutable",
              "name": "value",
              "required": false,
              "returned": "default",
              "type": "string",
              "uniqueness": "none"
            },
            {
              "caseExact": false,
              "description": "A human-readable name for the group
member, primarily used for display purposes.",
              "multiValued": false,
              "mutability": "immutable",
              "name": "display",
              "required": false,
              "returned": "default",
              "type": "string",
              "uniqueness": "none"
            }
          ],
          "type": "complex"
        }
      ],
      "description": "Group",
      "id": "urn:ietf:params:scim:schemas:core:2.0:Group",
      "name": "Group",
      "schemas": [
        "urn:ietf:params:scim:schemas:core:2.0:Schema"
      ]
    }
```

Users

POST /Users

功能描述

- 同步用户。

使用约束

- 如果身份中心中存在同名的手动方式创建的用户，则会创建失败。

请求示例

```
curl https://scim.tencentcloudsso.com/scim/v2/Users --
header 'Authorization: Bearer <your scim credential>' --header "content-
type:application/json" -X POST -d '<data>'
```

其中，data 结构示例如下：

```
{
    "displayName": "<user display name>",
    "emails": [
        {
            "primary": true,
            "type": "work",
            "value": "<user email>"
        }
    ],
    "name": {
        "familyName": "<user family name>",
        "givenName": "<user given name>"
    },
    "userName": "<user name>"
}
```

返回示例

```
{
    "active": true,
    "displayName": "<user display name>",
    "emails":
    [
```

```
        {
            "primary": true,
            "type": "work",
            "value": "<user email>"
        }
    ],
    "id": "u-00vrs1119d6gbsi5****",
    "meta":
    {
        "created": "2023-08-01T13:16:30.000Z",
        "lastModified": "2023-08-01T13:16:30.000Z",
        "resourceType": "User"
    },
    "name":
    {
        "familyName": "<user family name>",
        "givenName": "<user given name>"
    },
    "schemas":
    [
        "urn:ietf:params:scim:schemas:core:2.0:User"
    ],
    "userName": "<user name>"
}
```

GET /Users/{id} 和 GET /Users

功能描述

- GET /Users/{id}：查询指定 ID 的用户。
- GET /Users：按条件查询用户信息或查询所有用户列表。

使用约束

- 如果带 /{id}，则返回该 ID 对应的用户。如果 {id} 不是已存在的用户，则拒绝请求。
- 如果不带 /{id} 且有 filter，则过滤相应的用户返回，filter 只支持 userName 字段，且只支持 eq 操作符。
- 如果不带 /{id}且没有 filter，则返回所有用户列表，支持 SCIM 协议的标准分页方式，每页最多返回100条记录，如果记录条数大于100（count>100），则按100处理。
- 仅能查询被同步的用户。

1. **示例1：查询指定 ID 的用户。**

   请求示例

```
curl https://scim.tencentcloudsso.com/scim/v2/Users/<userId> --
header 'Authorization: Bearer <your scim credential>' --
header "content-type:application/json" -X GET
```

返回示例

```
{
    "active": true,
    "displayName": "<user display name>",
    "emails":
    [
        {
            "primary": true,
            "type": "work",
            "value": "<user email>"
        }
    ],
    "id": "u-00vrs1l19d6gbsi5****",
    "meta":
    {
        "created": "2023-08-01T13:16:30.000Z",
        "lastModified": "2023-08-01T13:16:30.000Z",
        "resourceType": "User"
    },
    "name":
    {
        "familyName": "<user family name>",
        "givenName": "<user given name>"
    },
    "schemas":
    [
        "urn:ietf:params:scim:schemas:core:2.0:User"
    ],
    "userName": "<user name>"
}
```

2. 示例2：按条件查询用户信息或查询所有用户列表。

   请求示例

```
  curl https://scim.tencentcloudsso.com/scim/v2/Users<?parameters> --
header 'Authorization: Bearer <your scim credential>' --
header "content-type:application/json" -X GET
```

返回示例

GET /Users?filter=userName eq "Test_User"

```
{
    "Resources":
    [
        {
            "active": true,
            "displayName": "<user display name>",
            "emails":
            [
                {
                    "primary": true,
                    "type": "work",
                    "value": "<user email>"
                }
            ],
            "id": "u-0015b4962vrywtzb****",
            "meta":
            {
                "created": "2023-07-07T17:21:07.000Z",
                "lastModified": "2023-07-07T17:21:07.000Z",
                "resourceType": "User"
            },
            "name":
            {
                "familyName": "<user family name>",
                "givenName": "<user given name>"
            },
            "schemas":
            [
                "urn:ietf:params:scim:schemas:core:2.0:User"
            ],
            "userName": "<user name>"
        },
```

```
        {
            "active": true,
            "displayName": "<user display name>",
            "emails":
            [
                {
                    "primary": true,
                    "type": "work",
                    "value": "<user email>"
                }
            ],
            "id": "u-00vrs1119d6gbsi5****",
            "meta":
            {
                "created": "2023-08-01T13:16:30.000Z",
                "lastModified": "2023-08-01T13:16:30.000Z",
                "resourceType": "User"
            },
            "name":
            {
                "familyName": "<user family name>",
                "givenName": "<user given name>"
            },
            "schemas":
            [
                "urn:ietf:params:scim:schemas:core:2.0:User"
            ],
            "userName": "<user name>"
        }
    ],
    "itemsPerPage": 10,
    "schemas":
    [
        "urn:ietf:params:scim:api:messages:2.0:ListResponse"
    ],
    "startIndex": 1,
    "totalResults": 2
}
```

```
{
    "Resources": [],
    "itemsPerPage": 10,
    "schemas": [
        "urn:ietf:params:scim:api:messages:2.0:ListResponse"
    ],
    "startIndex": 1,
    "totalResults": 0
}
```

PUT /Users/{id} 和 PATCH /Users/{id}

描述

- PUT /Users/{id}：替换用户信息。
- PATCH /Users/{id} ： 更新用户信息。

使用约束

- {id} 必传，修改的字段范围为 Schema 中定义的字段。
- PUT 为覆盖原有属性。
- Patch 支持 Add、Replace.
- 仅能修改被同步的用户。

请求示例

1. 替换用户信息（PUT）。

```
curl https://scim.tencentcloudsso.com/scim/v2/Users/<userId> --
header 'Authorization: Bearer <your scim credential>' --
header "content-type:application/json" -X PUT -d '<data>'
```

其中，data 结构示例如下：

```
  {
    "active": false,
    "displayName": "<user display name>",
    "emails":
    [
        {
            "primary": true,
            "type": "work",
            "value": "<user email>"
```

```
        }
    ],
    "name":
    {
        "familyName": "<user family name>",
        "givenName": "<user given name>"
    },
    "userName": "<user name>"
}
```

2. 更新用户信息（PATCH）。

```
curl https://scim.tencentcloudsso.com/scim/v2/Users/<userId> --
header 'Authorization: Bearer <your scim credential>' --
header "content-type:application/json" -X PATCH -d '<data>'
```

其中，data 结构示例如下：

```
// replace操作
{
    "Operations": [
        {
            "op": "replace",
            "path": "",
            "value": {
                "active": false,
                "displayName": "displayName",
                "name": {
                    "familyName": "familyName",
                    "givenName": "givenName"
                }
            }
        }
    ],
    "schemas": [
        "urn:ietf:params:scim:api:messages:2.0:PatchOp"
    ]
}
// add操作
```

```
{
    "Operations": [
        {
            "op": "add",
            "path": "",
            "value": {
                "displayName": "displayName",
                "name": {
                    "familyName": "familyName",
                    "givenName": "givenName"
                }
            }
        },
        {
            "op": "add",
            "path": "active",
            "value": true
        }
    ],
    "schemas": [
        "urn:ietf:params:scim:api:messages:2.0:PatchOp"
    ]
}
```

返回示例

```
//replace
{
    "active": false,
    "displayName": "displayName",
    "emails":
    [
        {
            "primary": true,
            "type": "work",
            "value": "<user email>"
        }
    ],
    "id": "u-00vrs1l19d6gbsi5****",
```

```
    "meta":
    {
        "created": "2023-08-01T13:16:30.000Z",
        "lastModified": "2023-08-01T13:16:30.000Z",
        "resourceType": "User"
    },
    "name":
    {
        "familyName": "<user family name>",
        "givenName": "<user given name>"
    },
    "schemas":
    [
        "urn:ietf:params:scim:schemas:core:2.0:User"
    ],
    "userName": "<user name>"
}

//add
{
    "active": true,
    "displayName": "displayName",
    "emails":
    [
        {
            "primary": true,
            "type": "work",
            "value": "<user email>"
        }
    ],
    "id": "u-00vrs1l19d6gbsi5****",
    "meta":
    {
        "created": "2023-08-01T13:16:30.000Z",
        "lastModified": "2023-08-01T13:16:30.000Z",
        "resourceType": "User"
    },
    "name":
    {
        "familyName": "<user family name>",
```

```
        "givenName": "<user given name>"
    },
    "schemas":
    [
        "urn:ietf:params:scim:schemas:core:2.0:User"
    ],
    "userName": "<user name>"
}
```

DELETE /Users/{id}

功能描述

- 删除指定 ID 的用户。

使用约束

- {id} 必传。
- 仅能删除被同步的用户。

请求示例

```
curl https://scim.tencentcloudsso.com/scim/v2/Users/<userId> --
header 'Authorization: Bearer <your scim credential>' --header "content-
type:application/json" -X DELETE
```

返回示例

```
HTTP/1.1 204
Date: Tue, 31 Mar 2020 02:36:15 GMT
Content-Type: application/json
x-RequestId: abbf9e53-9ecc-46d2-8efe-104a66ff128f
```

/Group

POST /Groups

功能描述

- 同步用户组。

使用约束

- 如果身份中心中存在同名的手动方式创建的用户组，则会创建失败。

请求示例

```
curl https://scim.tencentcloudsso.com/scim/v2/Groups --
header 'Authorization: Bearer <your scim credential>' --header "content-
type:application/json" -X POST -d '<data>'
```

其中，data 结构示例如下：

```
{
    "displayName": "<group name>",
    "schemas": [
        "urn:ietf:params:scim:schemas:core:2.0:Group"
    ]
}
```

返回示例

```
{
    "displayName": "<group name>",
    "id": "g-00nqnd7hoevd1unv****",
    "members": [],
    "meta":
    {
        "created": "2023-08-01T13:30:23.000Z",
        "lastModified": "2023-08-01T13:30:23.000Z",
        "resourceType": "Group"
    },
    "schemas":
    [
        "urn:ietf:params:scim:schemas:core:2.0:Group"
    ]
}
```

GET /Groups/{id} 和 GET /Groups

功能描述

- GET /Groups/{id}：查询指定 ID 的用户组。
- GET /Groups：按条件查询用户组信息或查询所有用户组列表。

使用约束

- 支持使用 id 查询和 filter 查询。

- filter 只支持 displayName 字段，且只支持 eq 操作符。
- 如果带 /{id}，则返回该 ID 对应的用户组，且包含 members 参数值，如果 {id} 不是已存在的用户组，则拒绝请求。
- 如果不带 /{id} 且没有 filter，则返回所有用户组列表，且 members 的值为空（即列表方法不返回 members）。支持 SCIM 协议的标准分页方式，最多返回100条记录，如果记录条数大于100（count>100），按100处理。
- 仅能查询被同步的用户组。

1. **示例1：查询指定 ID 的用户组。**

   请求示例

```
  curl https://scim.tencentcloudsso.com/scim/v2/Groups/<groupId> --
header 'Authorization: Bearer <your scim credential>' --
header "content-type:application/json" -X GET
```

   返回示例

```
  {
    "displayName": "<group name>",
    "id": "g-00nqnd7hoevd1unv****",
    "members":
    [
        {
            "display": "xxx",
            "value": "u-00vrs1l19d6gbsi5****"
        }
    ],
    "meta":
    {
        "created": "2023-08-01T13:30:23.000Z",
        "lastModified": "2023-08-01T13:30:23.000Z",
        "resourceType": "Group"
    },
    "schemas":
    [
        "urn:ietf:params:scim:schemas:core:2.0:Group"
    ]
}
```

2. 示例2：按条件查询用户组信息或查询所有用户组列表。

请求示例

```
  curl https://scim.tencentcloudsso.com/scim/v2/Groups<?parameters> --
header 'Authorization: Bearer <your scim credential>' --
header "content-type:application/json" -X GET
```

返回示例

```
{
    "Resources":
    [
        {
            "displayName": "<group name>",
            "id": "g-00nqnd7hoevd1unv****",
            "members": [],
            "meta":
            {
                "created": "2023-08-01T13:30:23.000Z",
                "lastModified": "2023-08-01T13:30:23.000Z",
                "resourceType": "Group"
            },
            "schemas":
            [
                "urn:ietf:params:scim:schemas:core:2.0:Group"
            ]
        }
    ],
    "itemsPerPage": 10,
    "schemas":
    [
        "urn:ietf:params:scim:api:messages:2.0:ListResponse"
    ],
    "startIndex": 1,
    "totalResults": 1
}
```

PUT /Groups/{id} 和 PATCH /Groups/{id}

功能描述

- PUT /Groups/{id}：替换用户组信息。
- PATCH /Groups/{id}：更新用户组信息。

使用约束

- {id} 必传，修改的字段范围为 Schema 中定义的字段。
- PUT 为覆盖原有属性，支持替换 member。
- Patch 支持 Add、Replace 和 Remove。
- 仅能修改被同步的用户组。

请求示例

- 替换用户组信息（PUT）

```
curl https://scim.tencentcloudsso.com/scim/v2/Groups/<groupId> --
header 'Authorization: Bearer <your scim credential>' --
header "content-type:application/json" -X PUT -d '<data>'
```

其中，data 结构示例如下：

```
{
    "displayName": "<group name>",
    "schemas": [
        "urn:ietf:params:scim:schemas:core:2.0:Group"
    ]
}
```

- 更新用户组信息（PATCH）

```
curl https://scim.tencentcloudsso.com/scim/v2/Groups/<groupId> --
header 'Authorization: Bearer <your scim credential>' --
header "content-type:application/json" -X PATCH -d '<data>'
```

其中，data 结构示例如下：

```
//从<groupId>对应的组内移除指定的用户<userId>
{
    "Operations": [
        {
            "op": "remove",
```

```
            "path": "members",
            "value": [
                {
                    "value": "<userId>"
                }
            ]
        }
    ],
    "schemas": [
        "urn:ietf:params:scim:api:messages:2.0:PatchOp"
    ]
}
//从<groupId>对应的组内移除所有用户
{
    "Operations": [
        {
            "op": "remove",
            "path": "members"
        }
    ],
    "schemas": [
        "urn:ietf:params:scim:api:messages:2.0:PatchOp"
    ]
}
//向<groupId>对应的组内添加3个用户
{
    "Operations": [
        {
            "op": "add",
            "path": "members",
            "value": [
                {
                    "display": "<userName1>",
                    "value": "<userId1>"
                },
                {
                    "display": "<userName2>",
                    "value": "<userId2>"
                },
                {
```

```
                    "display": "<userName3>",
                    "value": "<userId3>"
                }
            ]
        }
    ],
    "schemas": [
        "urn:ietf:params:scim:api:messages:2.0:PatchOp"
    ]
}
```

返回示例

```
HTTP/1.1 204 No Content
HTTP/1.1 204
Date: Tue, 07 Apr 2020 23:59:09 GMT
Content-Type: application/json
x-RequestId: dad0c91c-1ea8-4b36-9fdb-4f099b59c1c9
```

DELETE /Groups/{id}

功能描述

- 删除指定 ID 的用户组。

使用约束

- {id} 必传。
- 存在 member 的时候不允许删除组。
- 仅能删除被同步的用户组。

请求示例

```
curl https://scim.tencentcloudsso.com/scim/v2/Groups/<groupId> --
header 'Authorization: Bearer <your scim credential>' --header "content-
type:application/json" -X DELETE
```

返回示例

```
HTTP/1.1 204
Date: Mon, 06 Apr 2020 22:21:24 GMT
Content-Type: application/json
```

```
x-RequestId: abbf9e53-9ecc-46d2-8efe-104a66ff128
```

登录设置
设置登录方式

最近更新时间：2025-07-09 17:26:00

本文为您介绍如何设置身份中心用户的登录方式，包括**用户名密码登录**和**单点登录（SSO 登录）**。

登录方式

身份中心提供了以下两种用户登录方式，且**只能启用一种登录方式**。例如：启用用户名密码登录的时候，会自动禁用单点登录，反之亦然。

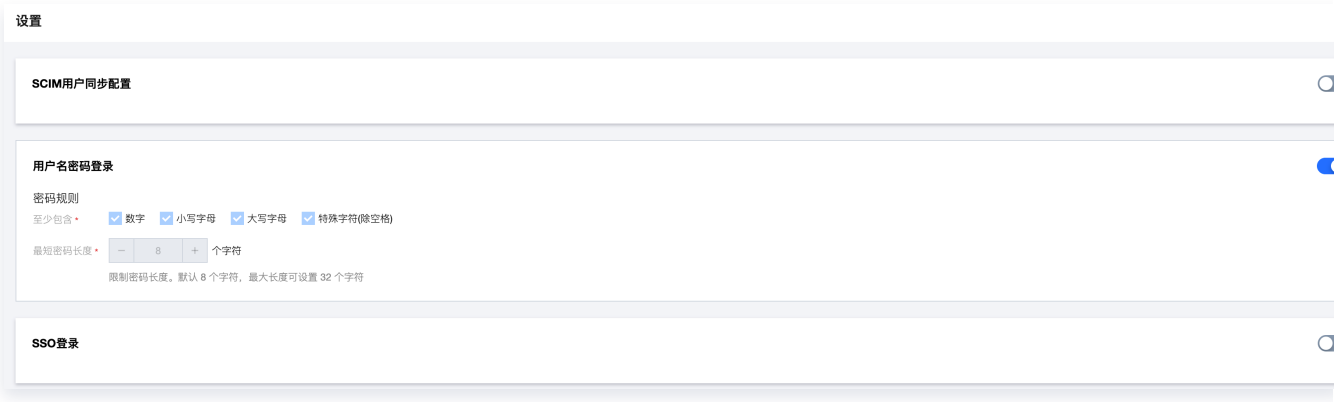
- **用户名密码登录**：当身份中心用户访问腾讯云时，您需要使用用户名和密码登录。
- **单点登录（SSO 登录）**：当外部身份提供商（IdP）提供的用户身份访问腾讯云时，您需要启用 SSO 登录。

启用或禁用用户名密码登录

默认情况下，用户名密码登录处于启用状态。如果禁用用户名密码登录，则会同时启用单点登录。

1. 登录**集团账号管理 > 身份中心管理 >** 设置 页面。
2. 在**设置**页面的**用户名密码登录**区域。
   - 启用用户名密码登录：开启用户名密码登录开关，同时自动禁用单点登录。

     > **说明：**
     > 密码规则仅展示，不可修改。

   - 禁用用户名密码登录：关闭用户名密码登录开关，同时自动启用单点登录。

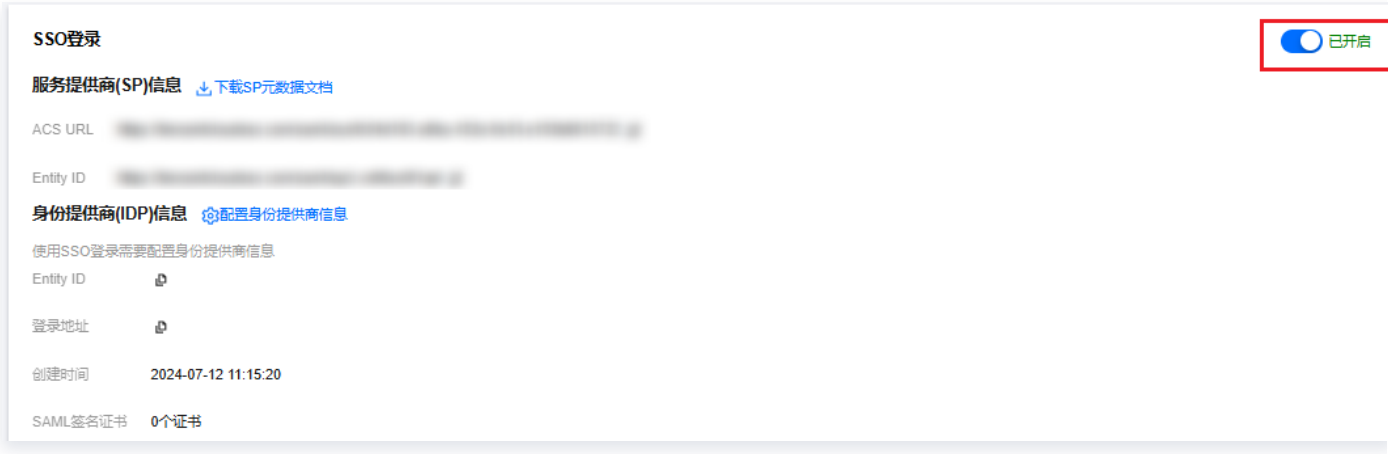
启用或禁用单点登录

启用单点登录

启用单点登录后，将自动禁用用户名密码登录。具体操作，请参见 管理 SSO 登录 。

禁用单点登录

1. 登录**集团账号管理 > 身份中心管理 >** 设置 页面。
2. 在**设置**页面的**SSO 登录**区域，关闭 **SSO 登录**开关，同时自动启用用户名密码登录。



3.在弹出的窗口中，单击**确定**。

管理 SSO 登录

最近更新时间：2025-07-09 17:16:02

操作场景

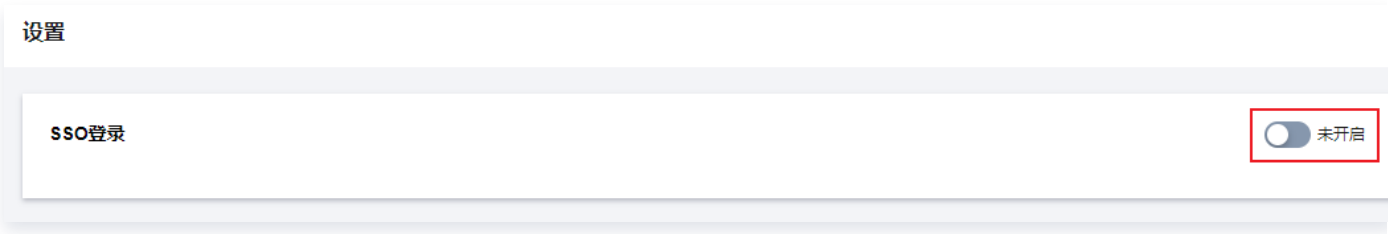
集团账号管理身份中心支持基于 SAML 2.0 的单点登录（SSO 登录）。腾讯云是服务提供商（SP），而企业自有的身份管理系统则是身份提供商（IdP）。通过 SSO 登录，企业员工可以使用 IdP 中的用户直接登录身份中心。

操作步骤

启用 SSO 登录

启用 SSO 登录后，您可进行身份提供商信息配置。

1. 登录**集团账号管理 > 身份中心管理 >** 设置 页面，在 **SSO 登录**区域，打开 SSO 登录开关。



2. 在**启用 SSO 登录**对话框，单击**确定**。

管理服务提供商（SP）信息

您在外部 IdP 中配置单点登录时，需要使用 SP 元数据文档，您可以在**集团账号管理 > 身份中心管理 >** 设置 **> SSO 登录**的**服务提供商（SP）信息**区域，单击**下载 SP 元数据文档**，下载 SP 元数据文档。同时，您也可以查看或复制 **ACS URL**、**Entity ID**，直接用于外部 IdP 的手动配置。

管理身份提供商（IdP）信息

您需要配置身份提供商（IdP）信息，并开启 SSO 登录开关，才能正常使用 SSO 登录功能。
支持手动配置和上传元数据文件两种方式配置身份提供商信息。

- 其中手动配置仅能配置 SSO 登录所必须的属性：Entity ID、登录地址和 SAML 签名证书。
- 如果您需要配置更多 IdP 信息，请在 IdP 端生成元数据文件并使用上传元数据的方式进行配置。

配置身份提供商（IdP）信息

您需要先配置身份提供商信息，才能启用单点登录。

1. 登录**集团账号管理 > 身份中心管理 >** 设置 页面。
2. 在 SSO 登录的**身份提供商（IdP）信息**区域，单击**配置身份提供商信息**。

3. 在**配置身份提供商信息**对话框，选择**上传元数据文档**或**手动配置**，配置身份提供商信息。

   以下两种方式您可以任选其一进行配置，相关元数据文件或配置信息请从身份提供商处获取。

   - 上传元数据文档

     单击**选择文件**，上传身份提供商元数据文件。

- 手动配置

  - **Entity ID**：身份提供商标识。
  - **登录地址**：身份提供商登录地址。
  - **证书**：身份提供商用于 SAML 响应签名的证书。您可以单击**选择文件**，上传身份提供商的证书。

4. 单击**确定**。

更新身份提供商（IdP）信息

当单点登录处于开启或禁用状态时，您都可以更新身份提供商信息。但在开启状态下更新时，如果新配置的身份提供商信息与原有的信息不匹配，可能会导致用户单点登录失败，请谨慎操作。

1. 在 SSO **登录的身份提供商（IdP）信息**区域，单击**配置身份提供商信息**。

2. 在**配置身份提供商信息**对话框，选择配置方式，并修改配置信息、重新上传证书或元数据文件等，单击**确定**。

单点登录示例
身份中心与 Microsoft Entra ID(Azure AD) 单点登录示例

最近更新时间：2025-07-09 17:16:02

本文为您提供 Microsoft Entra ID（即 Azure AD）与身份中心进行单点登录（SSO 登录）的示例。

背景信息

Microsoft Entra ID 中的所有配置操作需要管理员（已授予全局管理员权限）执行。关于如何在 Microsoft Entra ID 中创建用户及授权为管理员的操作，请参见 Microsoft Entra 文档 。

准备工作

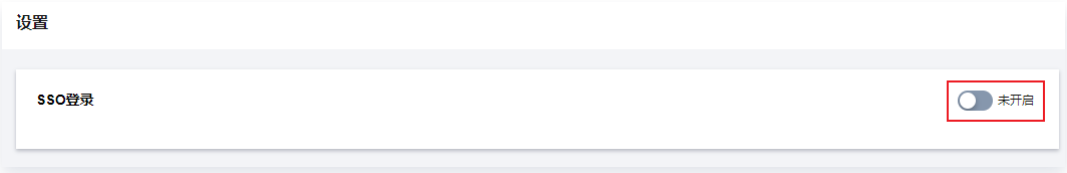
配置 SSO 登录前，您需要完成用户创建：从 Microsoft Entra ID 同步用户到身份中心，或者在身份中心创建同名用户。

- 从 Microsoft Entra ID 同步用户到身份中心：适用于 Microsoft Entra ID 中拥有大量用户的情况。具体操作，请参见 通过 SCIM 同步 Microsoft Entra ID (Azure AD) 示例 。
- 在身份中心创建同名用户：适用于 Microsoft Entra ID 中仅有少量用户的情况，可用于**快速验证**。创建时，身份中心的用户名需要和 Microsoft Entra ID 的用户名**保持一致**。具体操作，请参见 管理用户 。

在身份中心配置

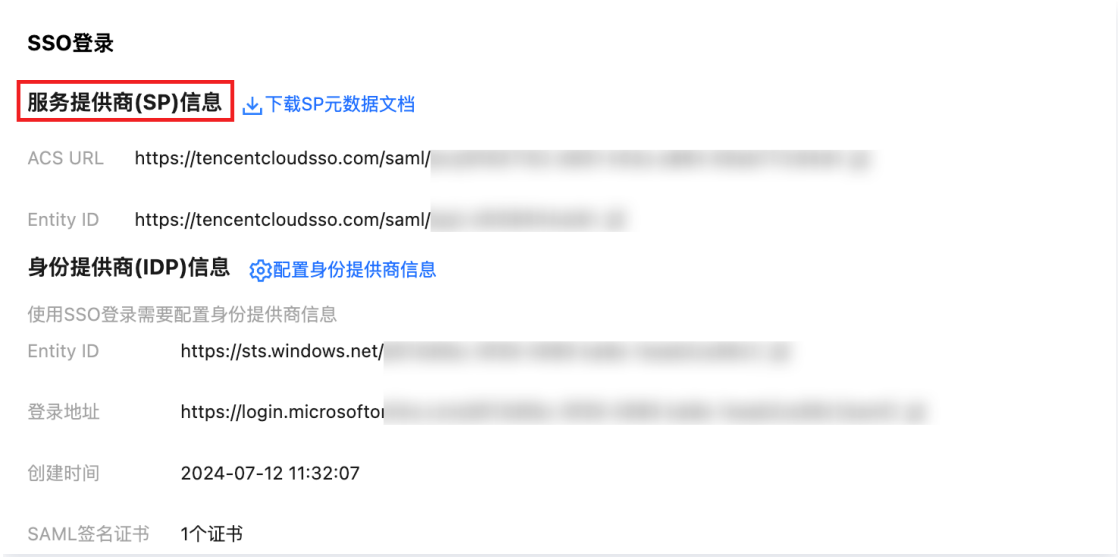
步骤一：开启 SSO 登录

1. 登录**集团账号管理** > 身份中心 。
2. 在左侧导航栏，单击**用户管理** > **设置**。
3. 在 **SSO登录** 区域，单击，在弹出的窗口单击开启，启用 SSO 登录。



步骤二：复制服务提供商（SP）信息

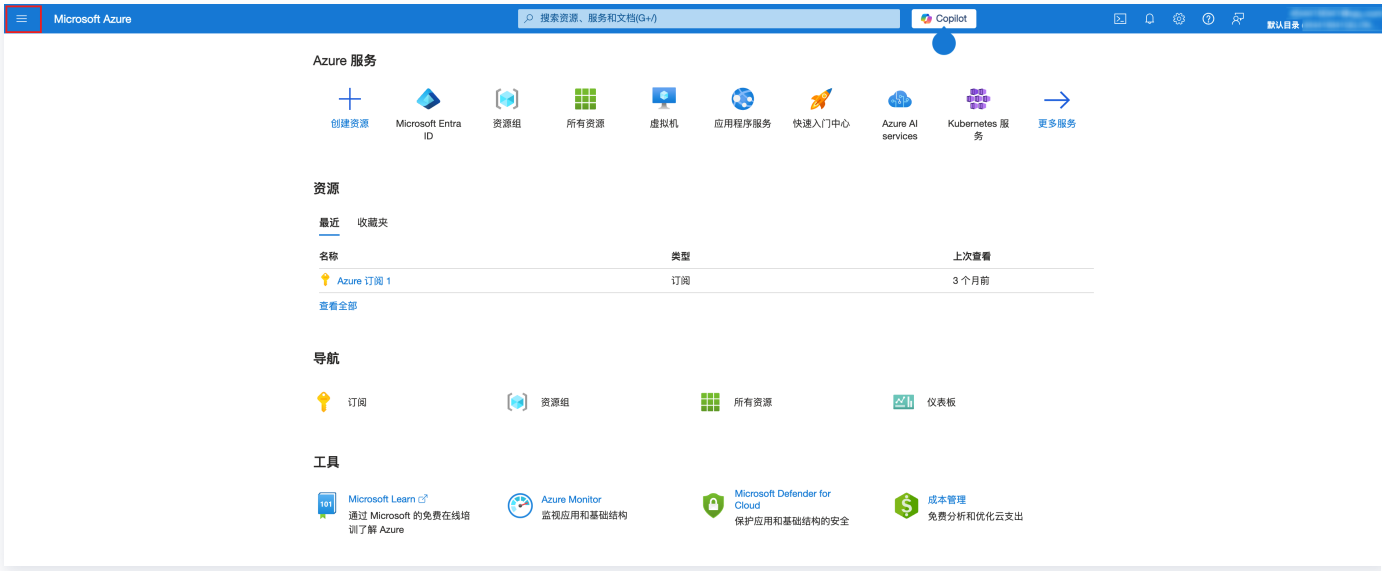
在**服务提供商（SP）信息**区域，查看并复制 ACS URL、Entity ID，直接用于外部 IdP 的手动配置。



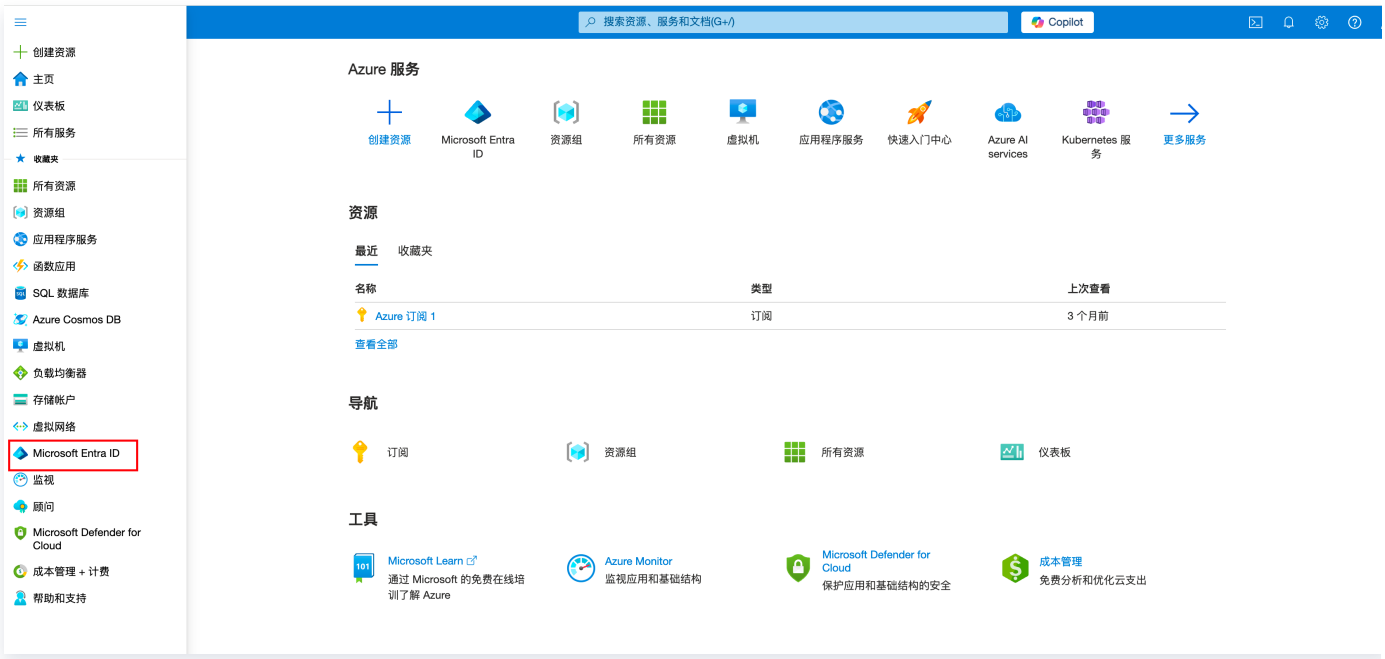
在 Microsoft Entra ID 配置

步骤一：在 Microsoft Entra ID 中创建应用程序

1. 管理员登录 Azure 门户，单击左上角菜单图标。

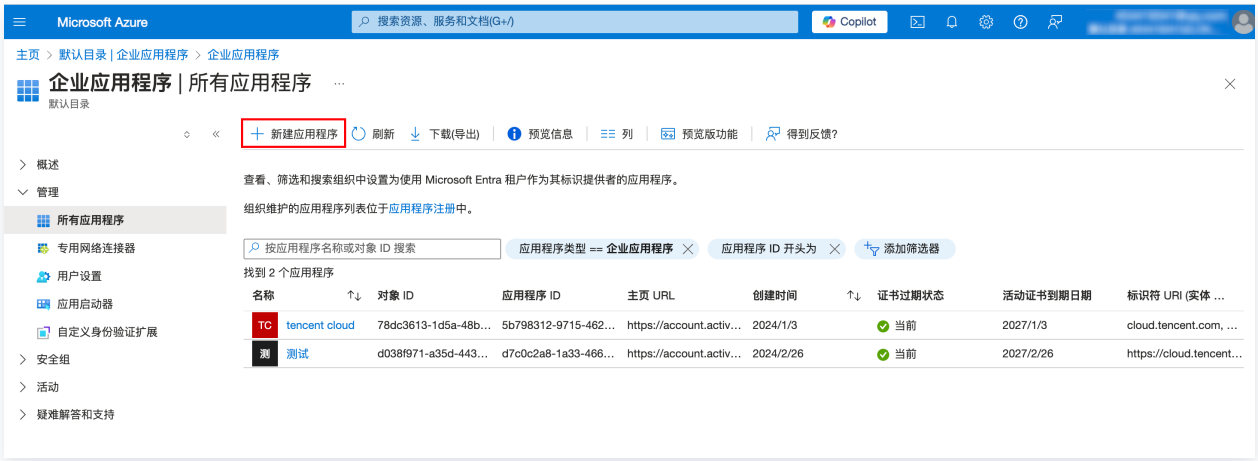


2. 在左侧导航栏，选择 Microsoft Entra ID。

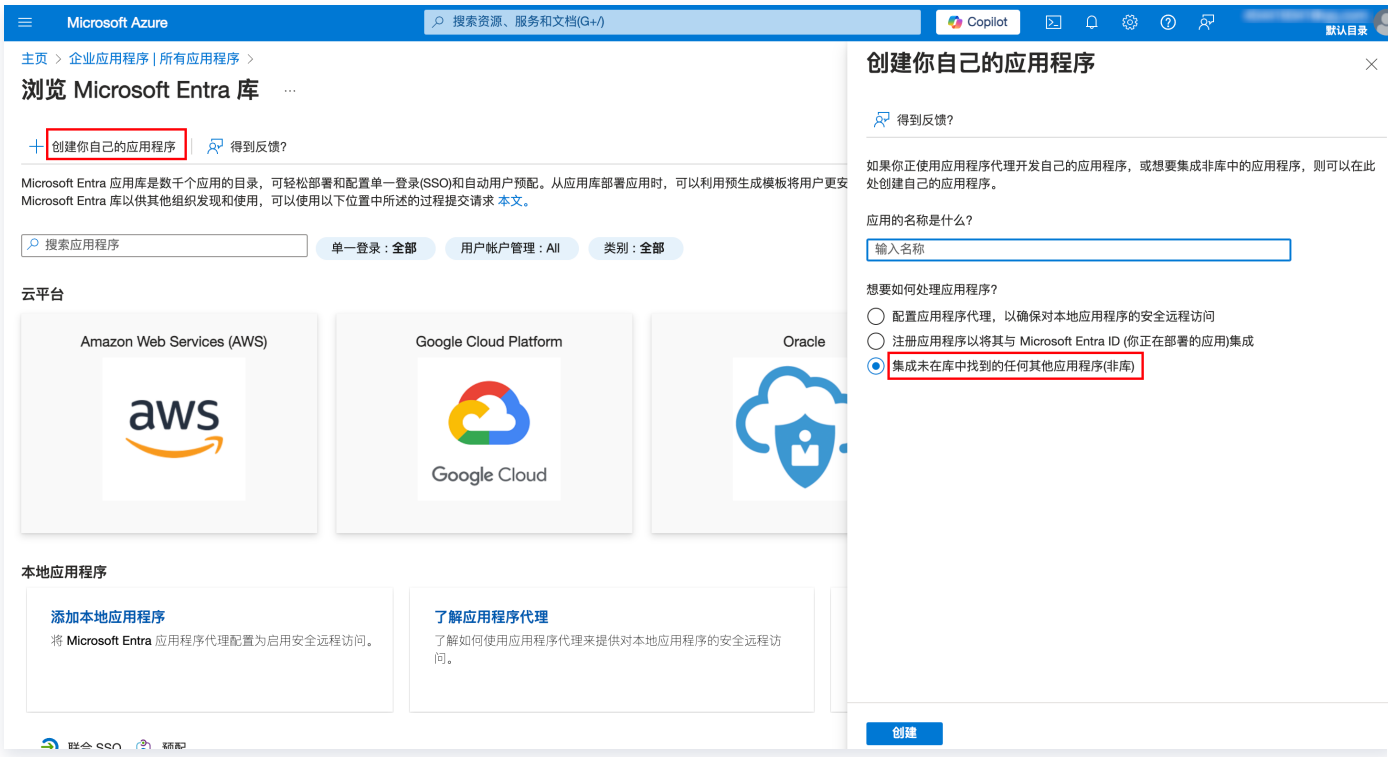


3. 在左侧导航栏，选择**管理** > **企业应用程序**后，进入**所有应用程序**。

4. 单击**新建应用程序**。



5. 在**浏览 Microsoft Entra 库**页面，单击**创建你自己的应用程序**，在右侧窗口中，输入应用名称（例如：SCIM intl），并选择**集成未在库中找到的任何其他应用程序(非库)**，然后单击**创建**。



步骤二：在 Microsoft Entra ID 中设置单一登录

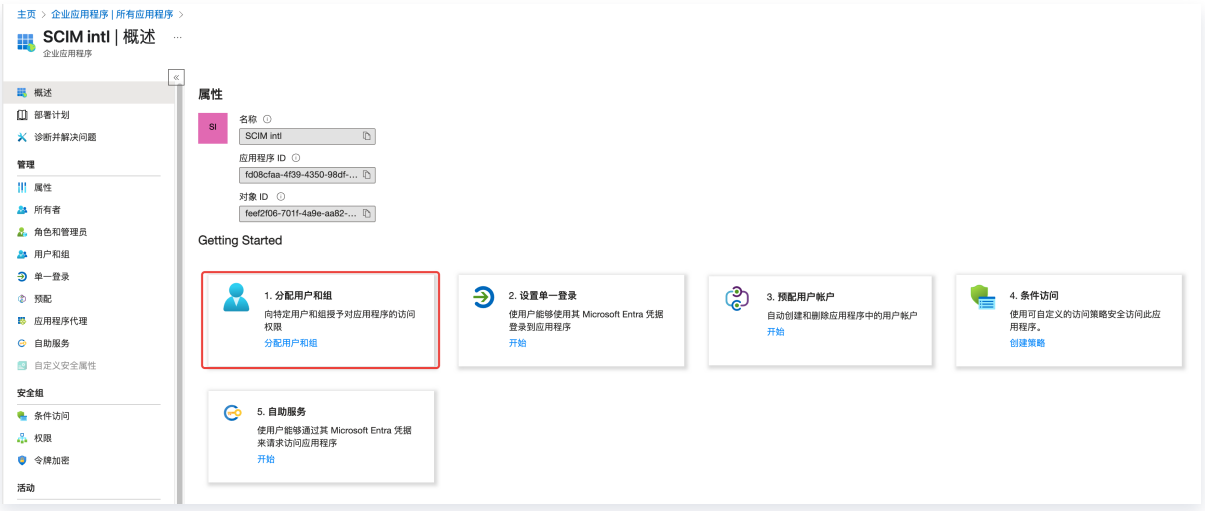
1. 在应用程序 SCIM intl 页面，在**设置单一登录**卡片，单击**开始**。

2. 在**基本 SAML 配置**模块，单击**编辑**，**标识符(实体 ID)**填写 步骤二 中的 **Entity ID**，**回复 URL (断言使用者服务 URL)** 填写 **ACS URL**。

3. 下载 **SAML 证书**模块的**联合元数据 XML**。

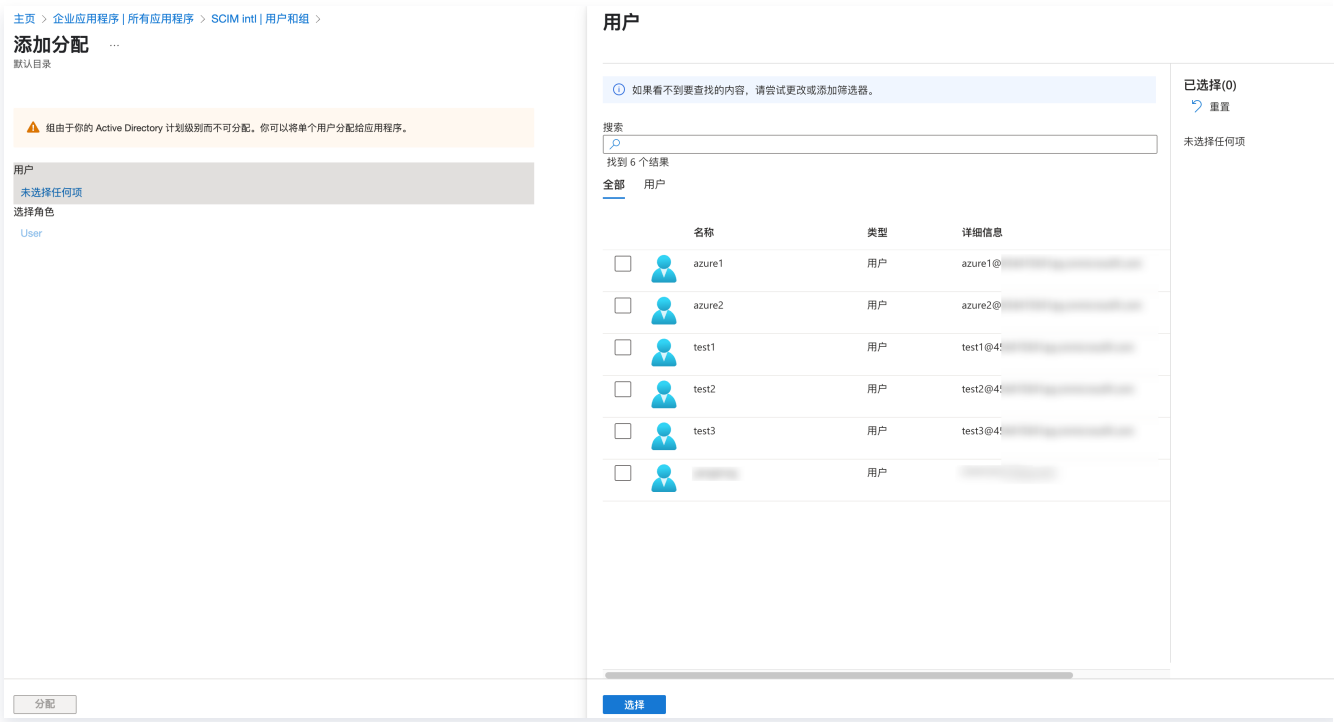
4. 在应用程序 SCIM intl 分配用户和组。

4.1 单击**分配用户和组**。



4.2 单击**添加用户/组**。

4.3 勾选用户后，单击**选择**。



4.4 分配成功后，列表中显示用户名称。

步骤三：在身份中心上传联合元数据 XML

1. 在**集团账号管理 > 身份中心管理 >** 设置 **> SSO 登录**的**身份提供商(IDP)信息**区域，单击**配置身份提供商信息**。

2. 单击**选择文件**，上传在 Microsoft Entra ID 下载的**联合元数据 XML**。

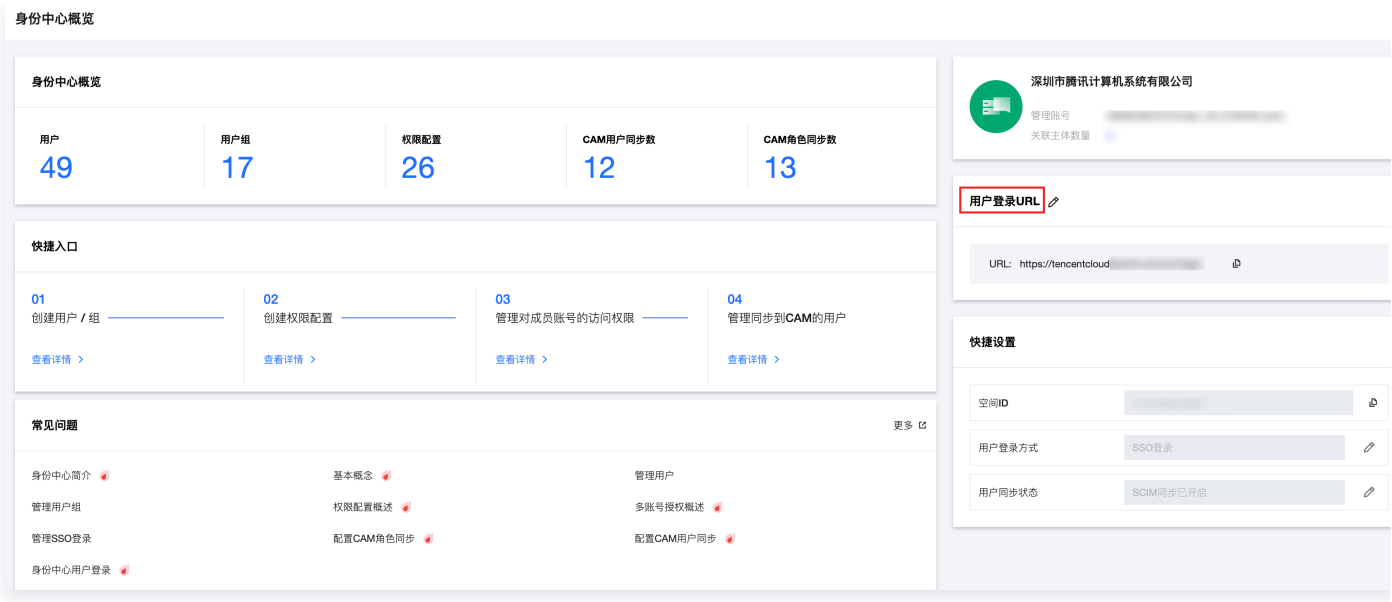
结果验证

完成 SSO 登录配置后，您可以从腾讯云发起 SSO 登录。

> **前提**：在身份中心需要创建和 Microsoft Entra ID 应用中同名的用户，进入**集团账号管理> 身份中心管理 >** 用户 中创建。

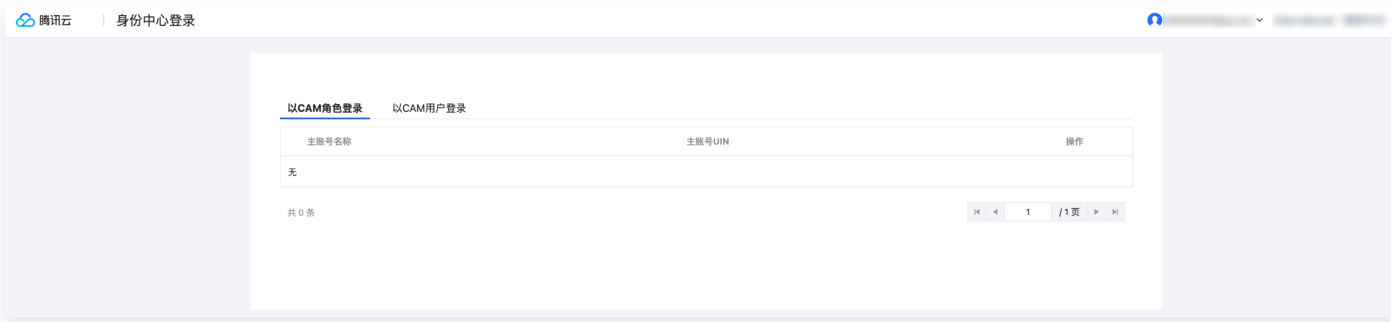
登录流程：

1. 身份中心管理员进入**集团账号管理 > 身份中心管理 >** 身份中心概览 的页面的右侧，查看并复制**用户登录 URL**。



2. 单击访问**用户登录 URL**，单击**登录**。

3. 重定向到 Microsoft 登录页面，选择账户后输入密码登录。
4. 登录成功，进入身份中心账号列表页。



身份中心与 Okta 单点登录示例

最近更新时间：2025-06-11 14:35:45

本文为您提供 Okta 与身份中心进行单点登录（SSO 登录）的示例。

准备工作

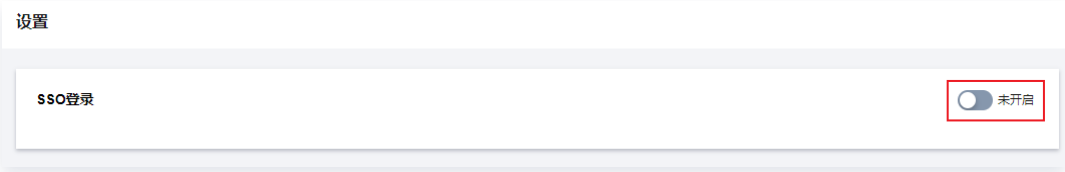
配置 SSO 登录前，您需要完成用户创建：从 Okta 同步用户到身份中心，或者在身份中心创建同名用户。

- 从 Okta 同步用户到身份中心：适用于 Okta 中拥有大量用户的情况。具体操作，请参见 通过 SCIM 同步 Okta 示例 。
- 在身份中心创建同名用户：适用于 Okta 中仅有少量用户的情况，可用于**快速验证**。创建时，身份中心的用户名需要和 Okta 的用户名**保持一致**。

在身份中心配置

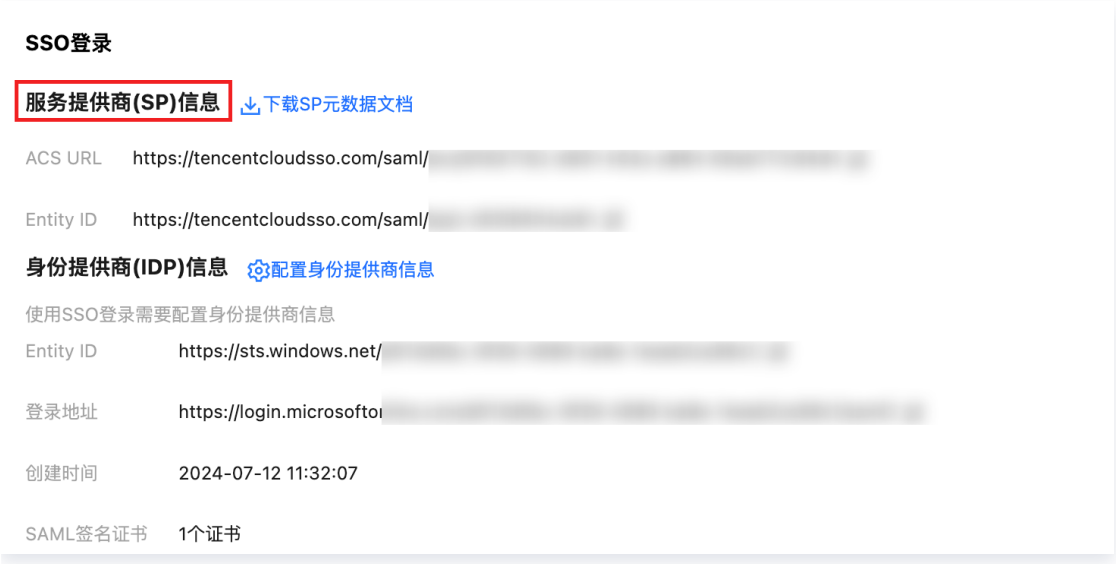
步骤一：开启 SSO 登录

1. 登录**集团账号管理** > 身份中心 。
2. 在左侧导航栏，单击**用户管理** > **设置**。
3. 在 **SSO登录** 区域，单击，在弹出的窗口单击开启，启用 SSO 登录。



步骤二：复制服务提供商（SP）信息

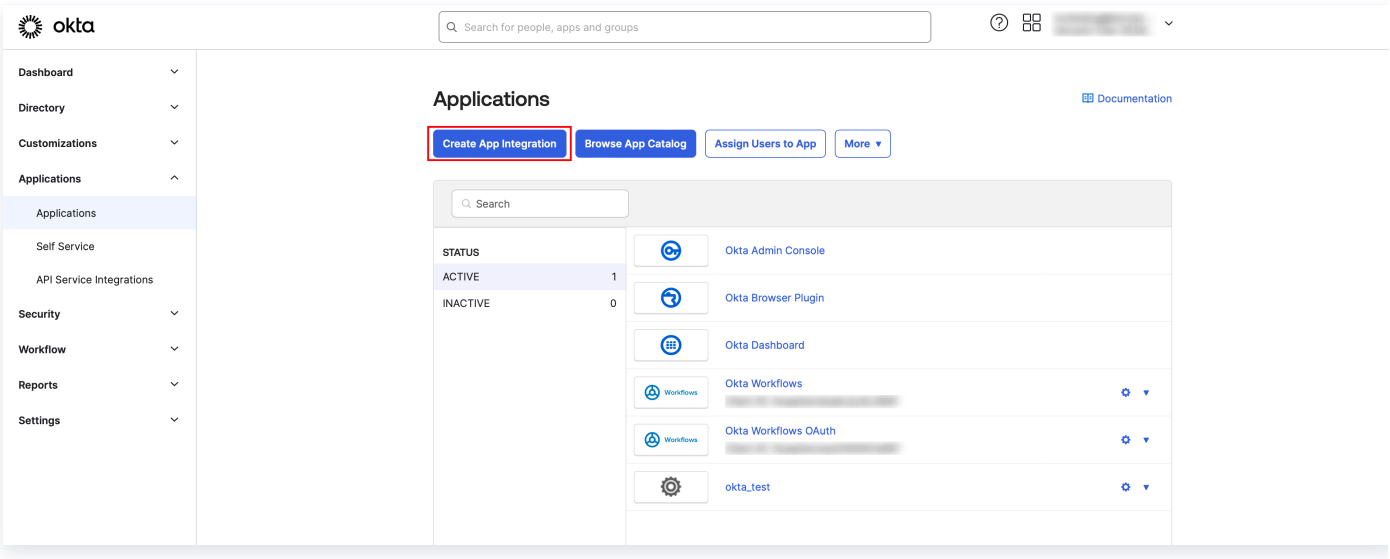
在**服务提供商（SP）信息**区域，查看并复制 ACS URL、Entity ID，直接用于外部 IdP 的手动配置。



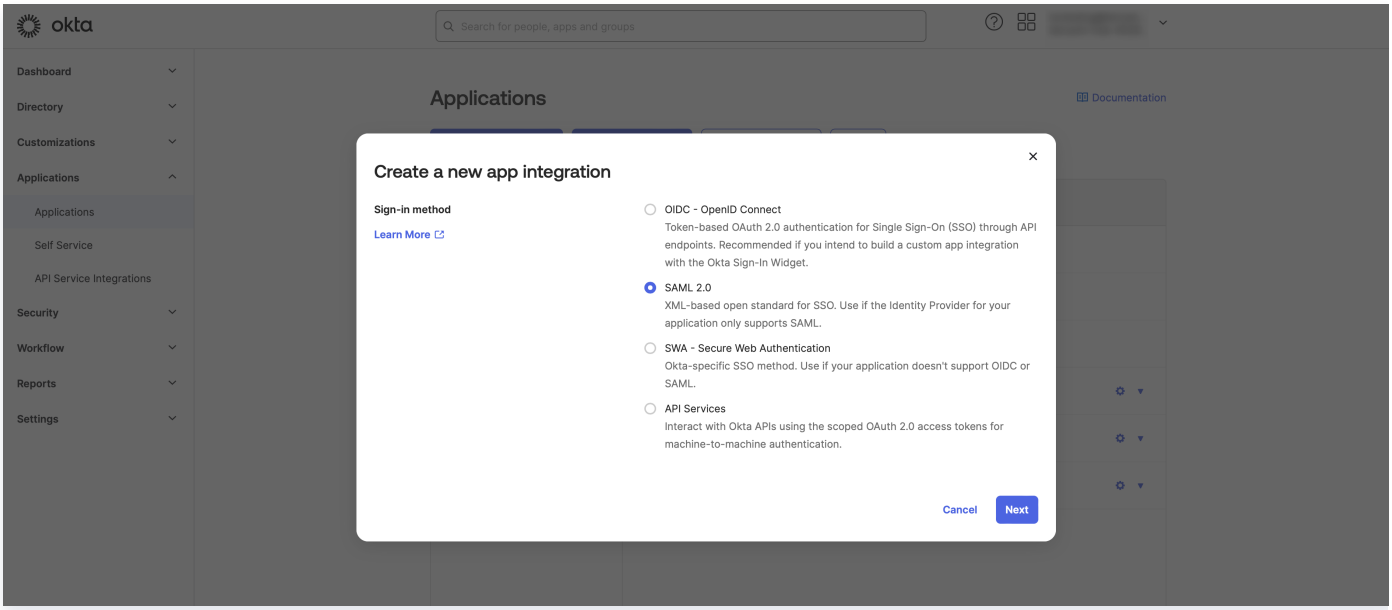
在 Okta 配置

步骤一：在 Okta 中创建应用程序

1. 登录 Okta，在左侧导航栏中，选择 Applications > Applications 后，进入全部应用，单击 Create APP Intergration，创建应用程序。

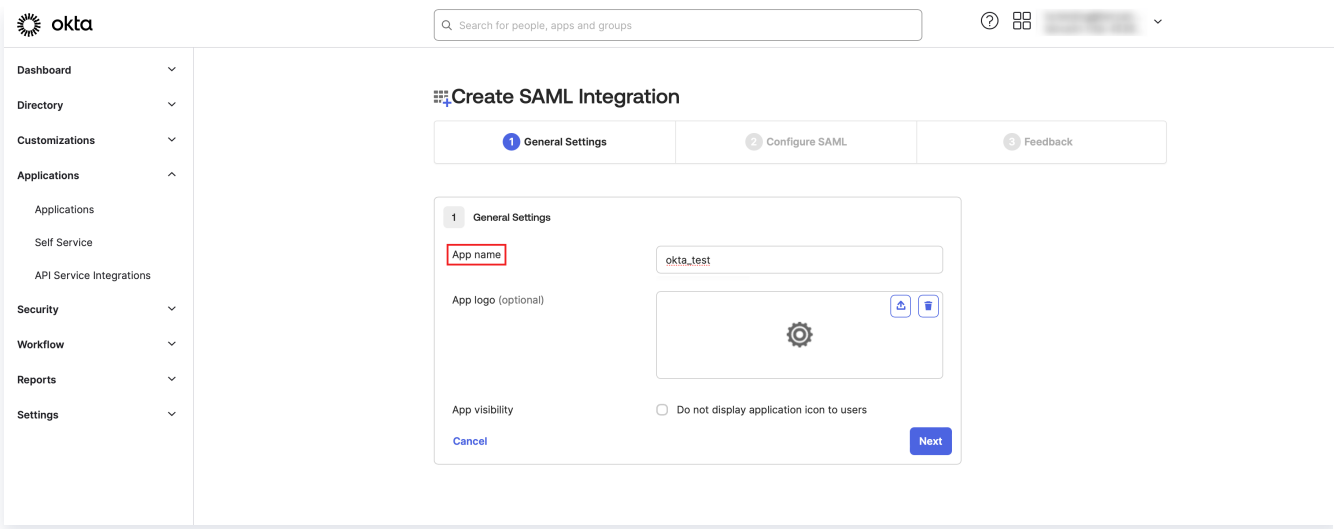


2. 在弹出的 Create a new app integration 窗口中，选择 SAML 2.0，单击 Next。

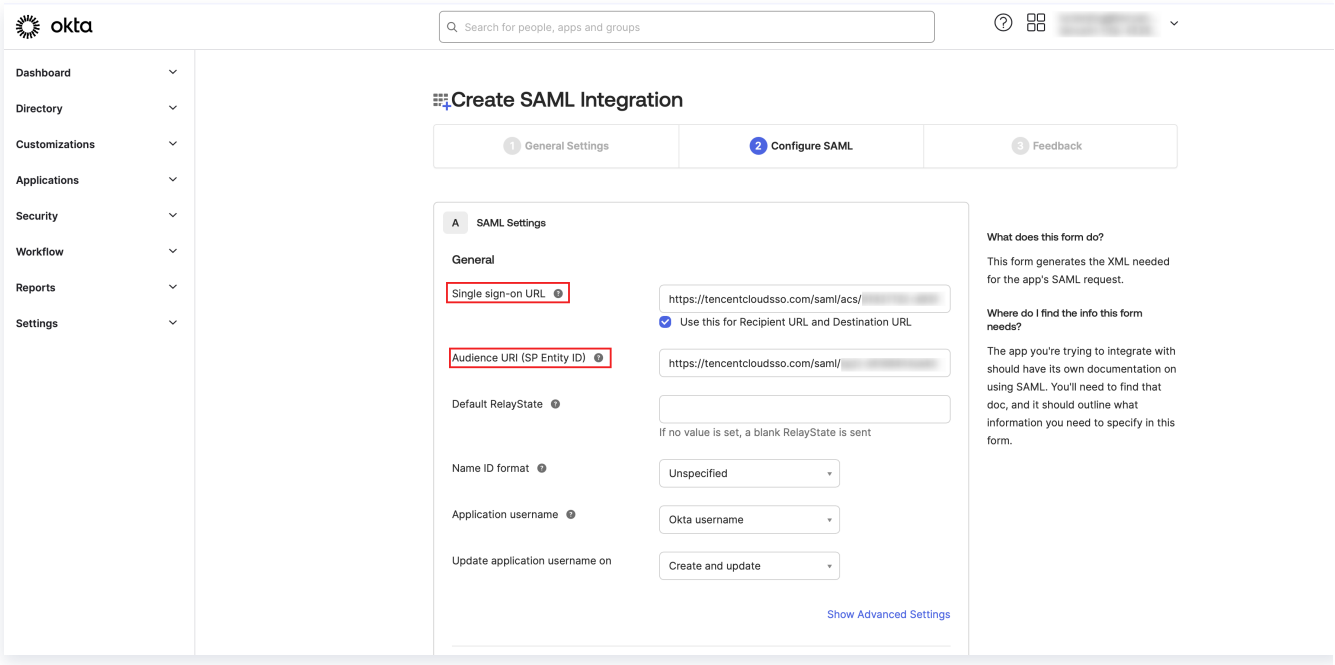


3. 进入 Create SAML Integration 页面，完成应用基础配置。

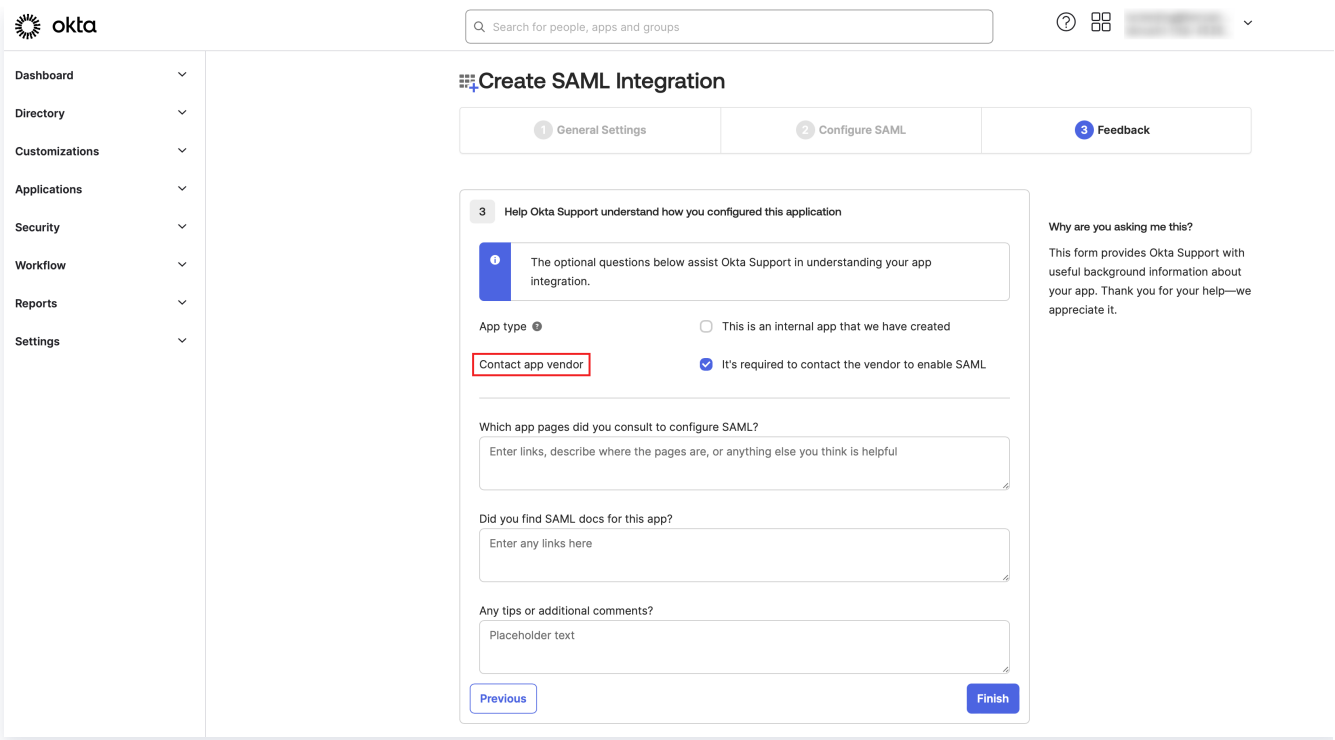
   3.1 在 General Settings 页面，填写 App name，单击 Next。



3.2 在 Configure SAML 页面，填写 Single sign-on URL 和 Audience URL(SP Entity ID)。该信息对应 服务提供商(SP)信息 中的 ACS URL 和 Entity ID，填写完成后，单击 Next。



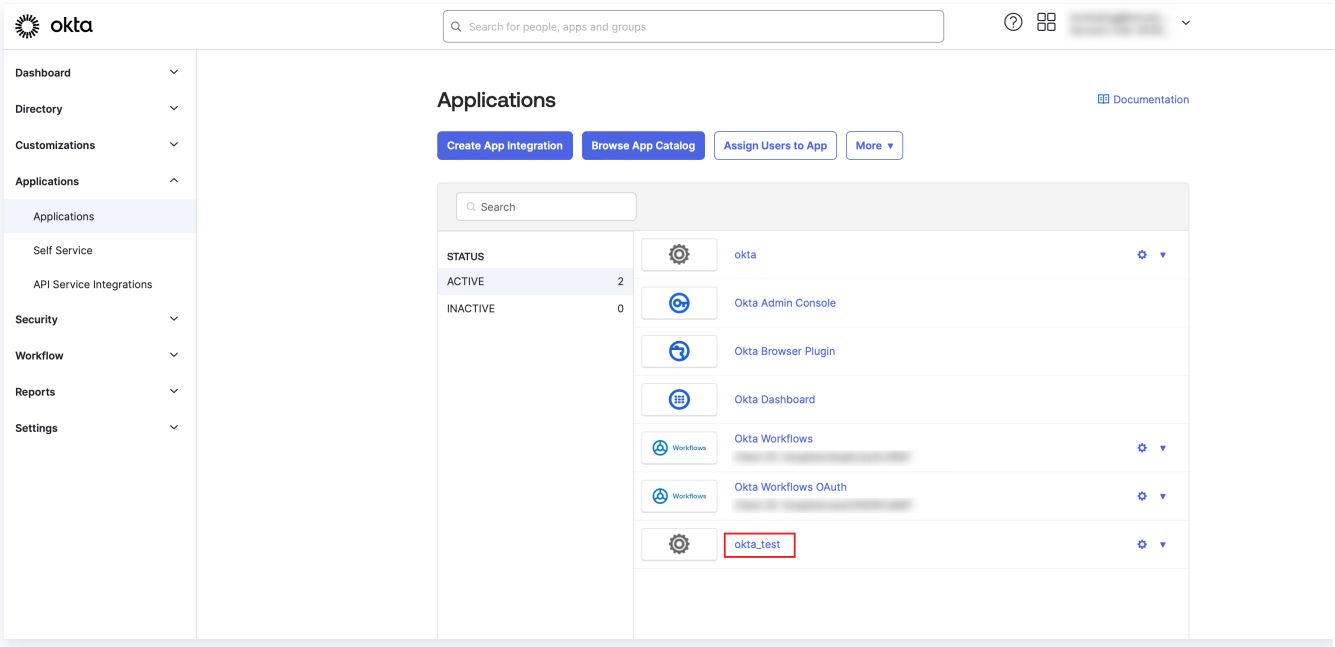
3.3 在 Feedback 页面，勾选 Contact app vendor，单击 Finish，完成应用创建。



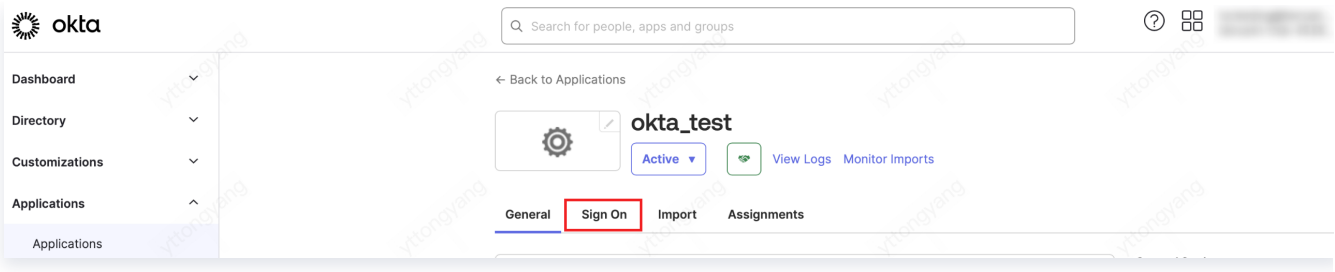
步骤二：在 Okta 中设置单一登录

1. 下载联合元数据 XML。

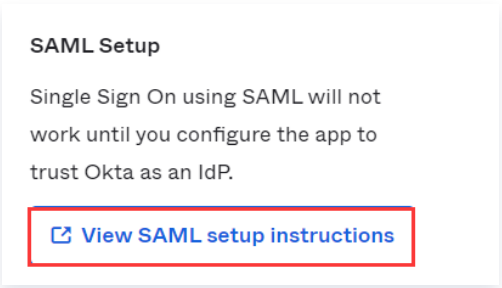
   1.1 在左侧导航栏，选择 **Applications** > **Applications** 后，进入全部应用，选中目标应用。



   1.2 进入应用详情页，单击 **Sign On**。

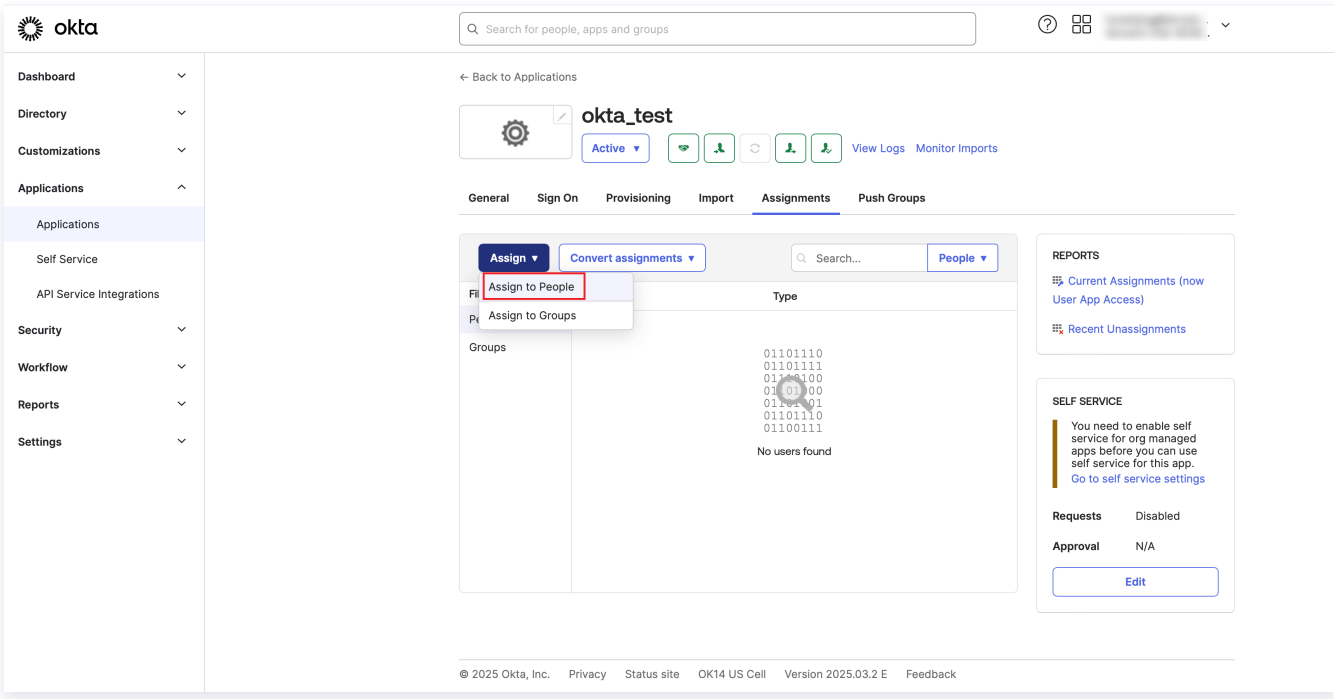


1.3 在 Sign On 页面，单击右下角 View SAML setup instructions 查看身份提供商元数据，并保存至本地。

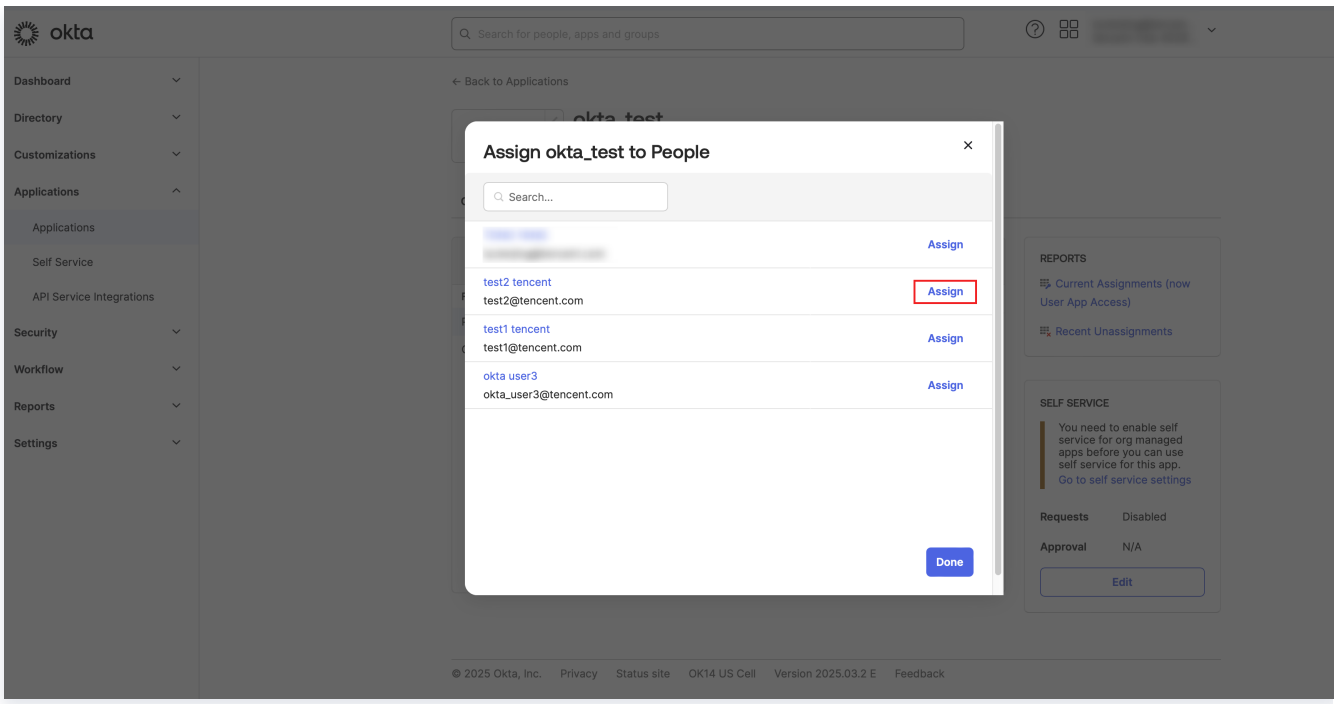


2. 向应用程序分配用户。

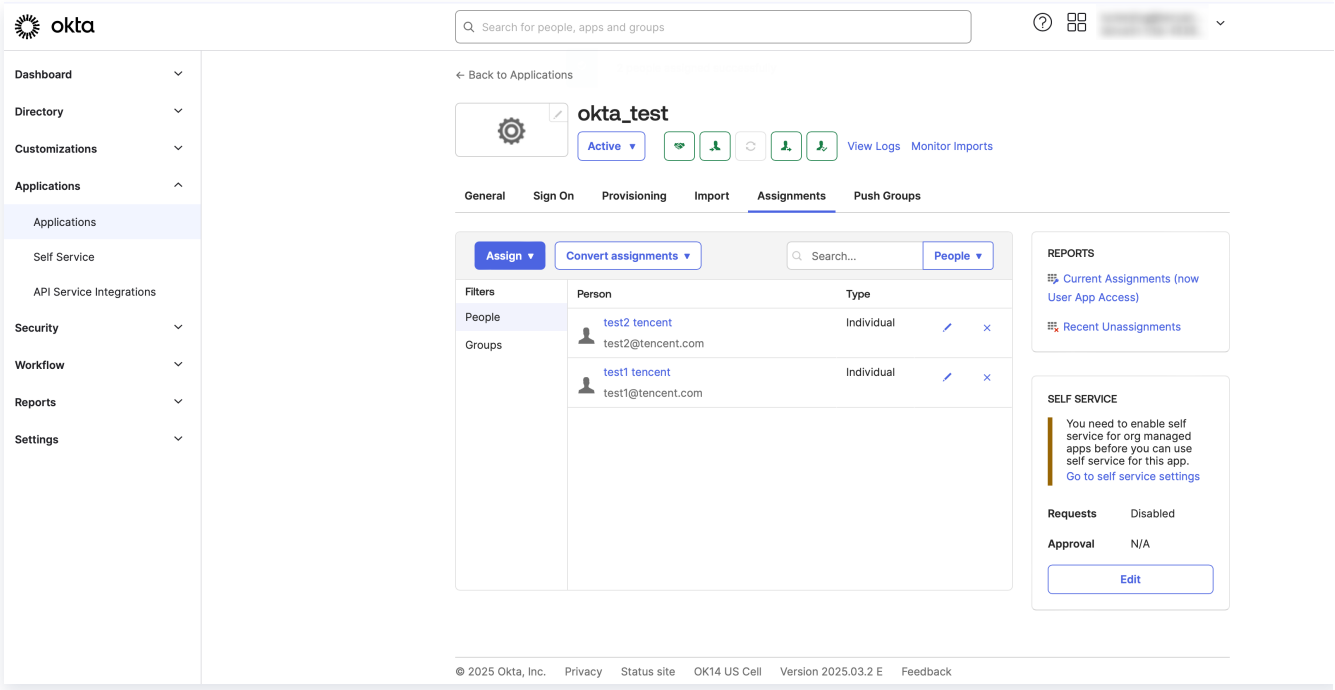
2.1 在 Assignments 页面，单击 Assign，选择 Assign to People，将用户分配到应用。



2.2 在 Assign okta_test to People 弹窗中，选择目标用户，单击 Assign。在新窗口单击 Save and Go Back，启动分配。



2.3 分配成功的用户展示在 People 页面。



步骤三：在身份中心上传联合元数据 XML

1. 在**集团账号管理** > **身份中心管理** > 设置 > SSO 登录的**身份提供商(IDP)信息**区域，单击**配置身份提供商信息**。

2. 单击**选择文件**，上传在 Okta下载的**联合元数据 XML**。

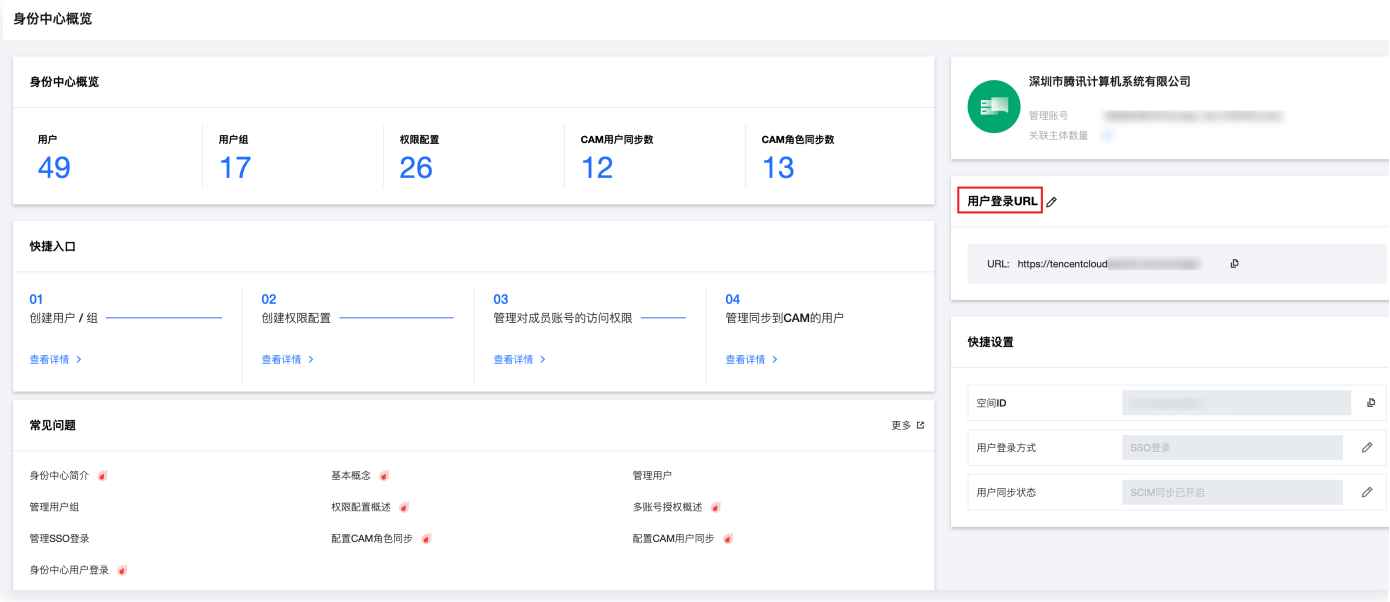
结果验证

完成 SSO 登录配置后，您可以从腾讯云发起 SSO 登录。

> **前提**：在身份中心需要创建和 Okta 应用中同名的用户，进入**集团账号管理> 身份中心管理 >** 用户 中创建。

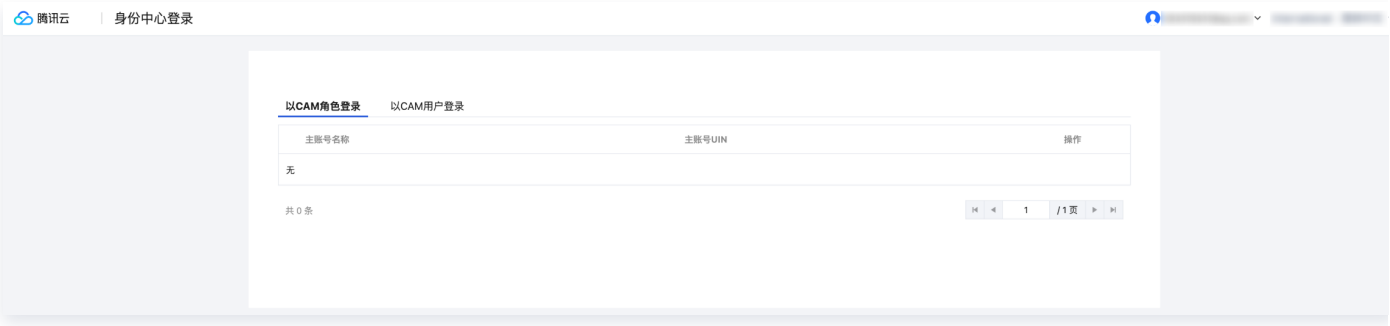
登录流程：

1. 身份中心管理员进入**集团账号管理 > 身份中心管理 >** 身份中心概览 的页面的右侧，查看并复制**用户登录 URL**。



2. 单击访问**用户登录 URL**，单击**登录**。

3. 重定向到 Okta 登录页面，输入账号密码登录。
4. 登录成功，进入身份中心账号列表页。



身份中心与 Onelogin 单点登录示例

最近更新时间：2025-06-11 14:35:46

本文为您提供 Onelogin 与身份中心进行单点登录（SSO 登录）的示例。

准备工作

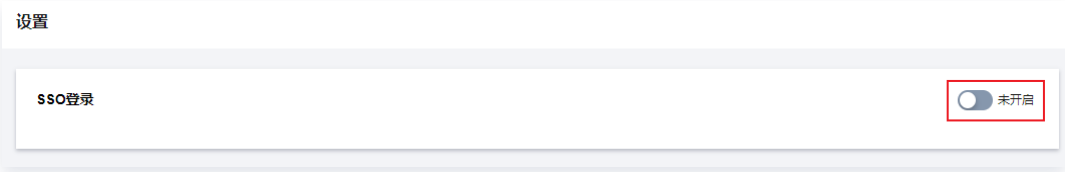
配置 SSO 登录前，您需要完成用户创建：从 Onelogin 同步用户到身份中心，或者在身份中心创建同名用户。

- 从 Onelogin 同步用户到身份中心：适用于 Onelogin 中拥有大量用户的情况。具体操作，请参见 通过 SCIM 同步 Onelogin 示例 。
- 在身份中心创建同名用户：适用于 Onelogin 中仅有少量用户的情况，可用于**快速验证**。创建时，身份中心的用户名需要和 Onelogin 的用户名**保持一致**。

在身份中心配置

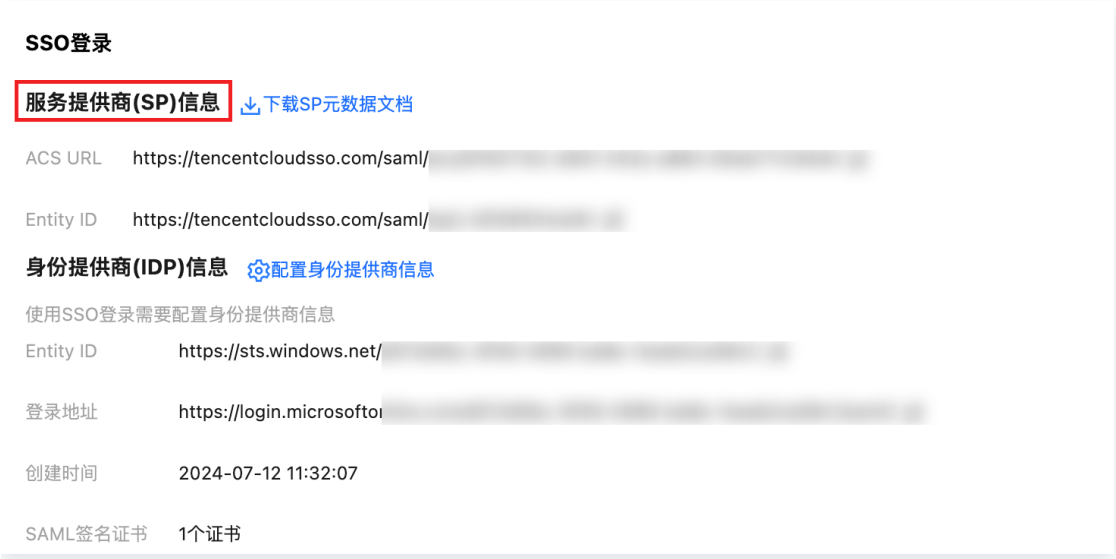
步骤一：开启 SSO 登录

1. 登录**集团账号管理** > 身份中心 。
2. 在左侧导航栏，单击**用户管理** > **设置**。
3. 在 **SSO登录** 区域，单击，在弹出的窗口单击开启，启用 SSO 登录。



步骤二：复制服务提供商（SP）信息

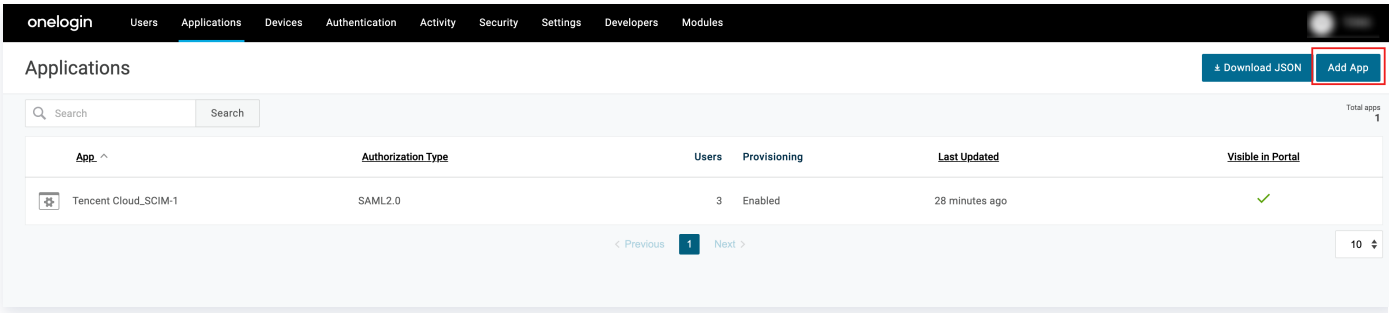
在**服务提供商（SP）信息**区域，查看并复制 ACS URL、Entity ID，直接用于外部 IdP 的手动配置。



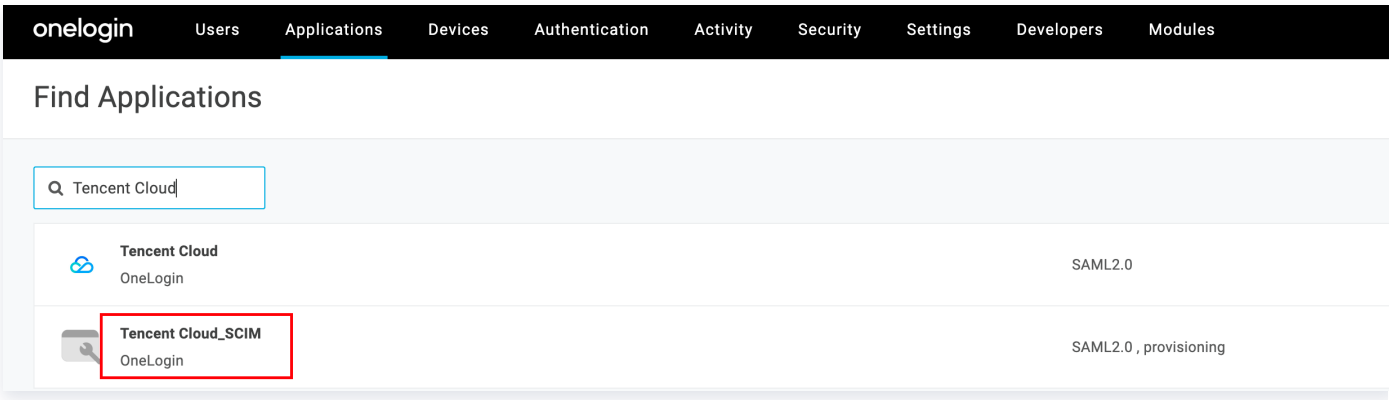
在 Onelogin 配置

步骤一：在 Onelogin 中创建应用程序

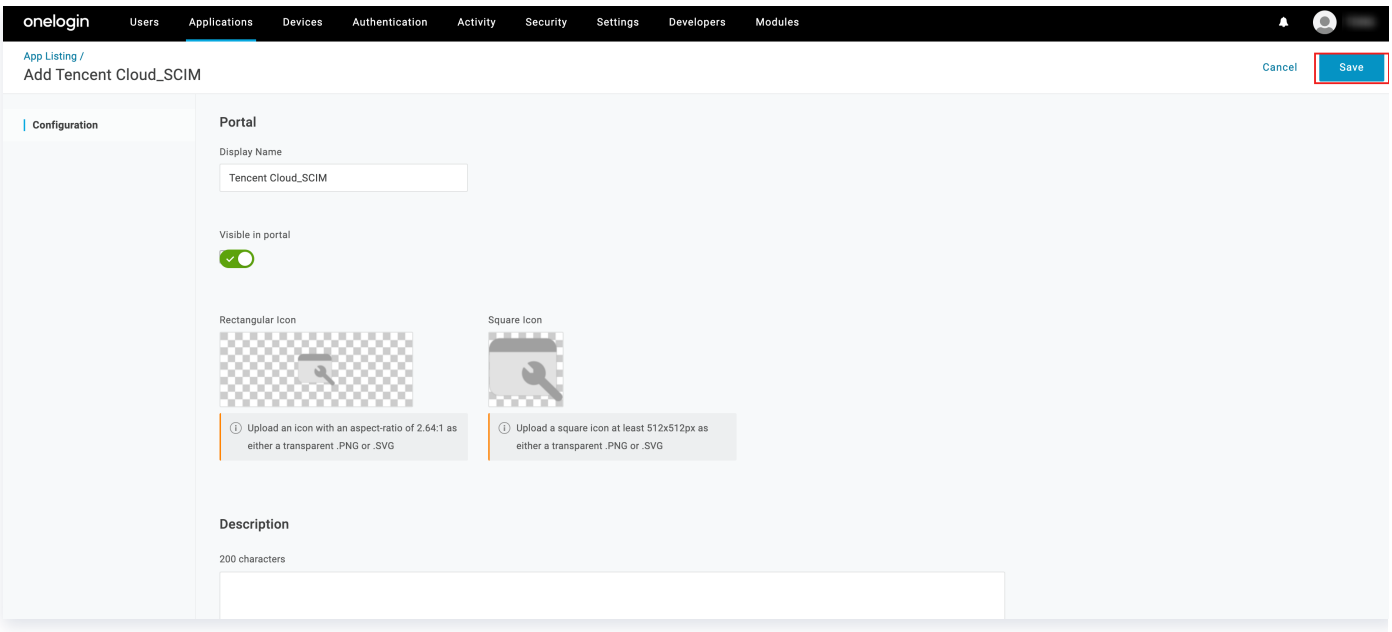
1. 管理员登录 Onelogin，在顶部菜单选择 Applications > Applications。
2. 在 Applications 页面，单击 Add App。



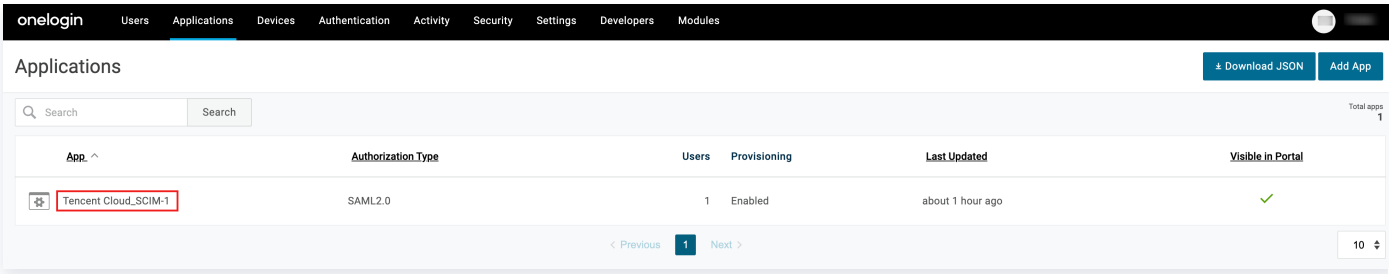
3. 在 Find Applications 页面，单击选择 Tencent Cloud_SCIM。



4. 进入 Tencent Cloud_SCIM 应用，修改名称后，单击 Save。

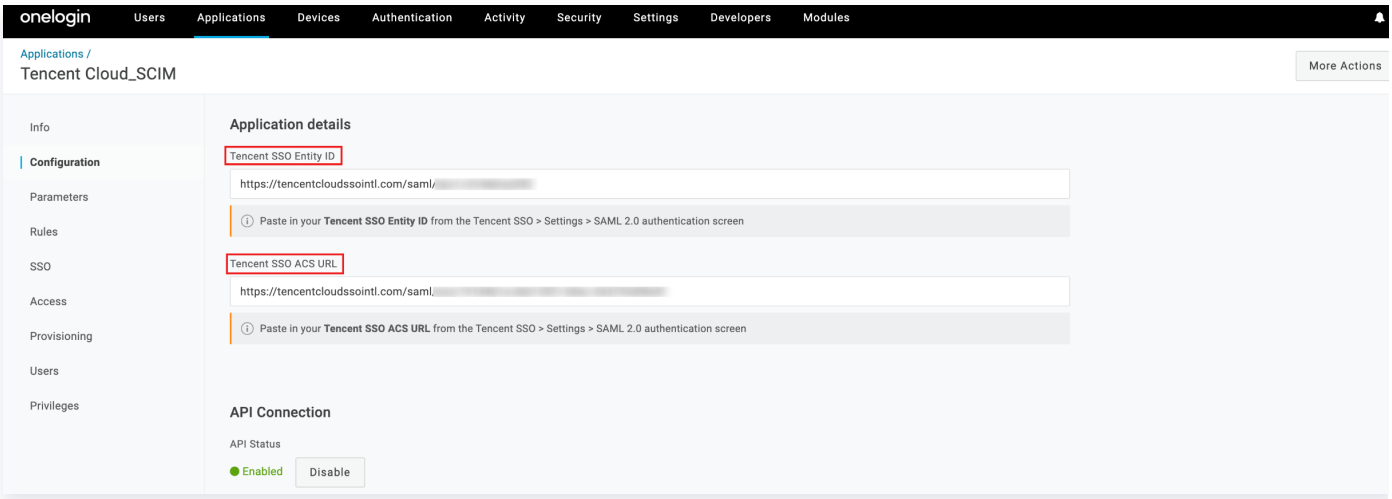


5. 创建完成，可以在列表中查看。



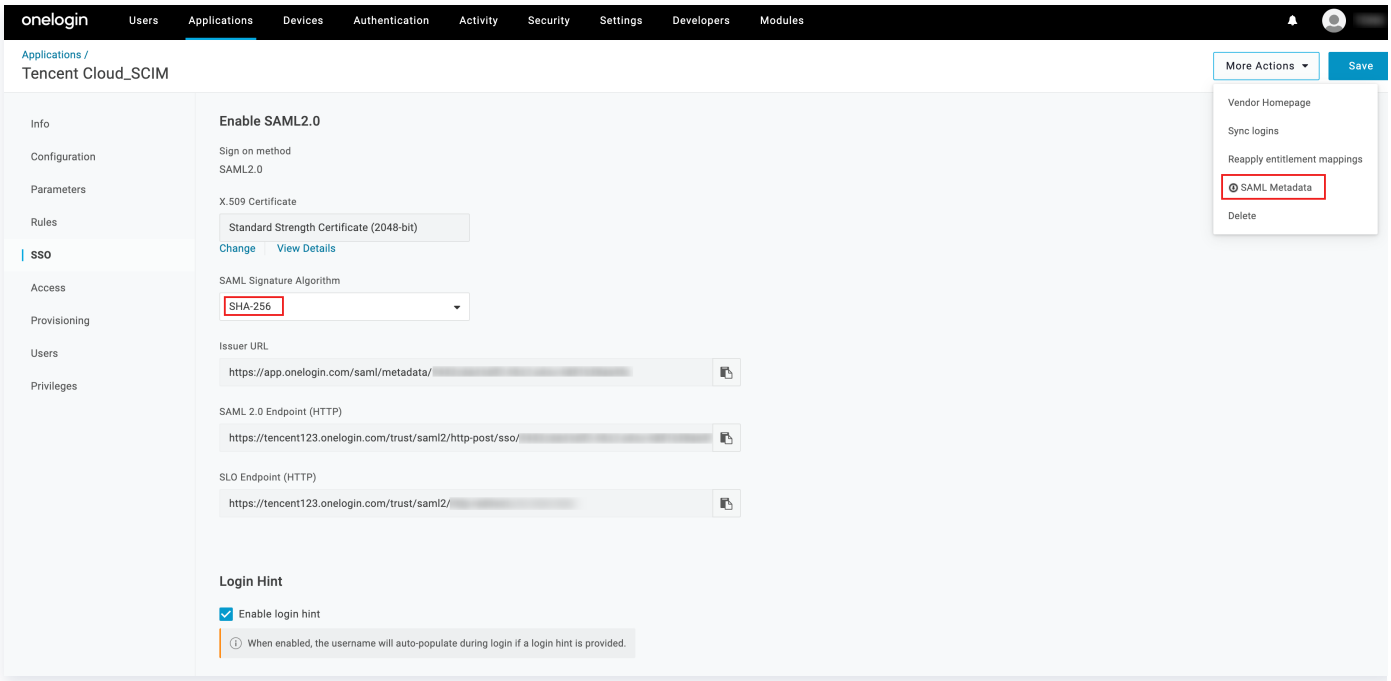
步骤二：在 Onelogin 中设置 SSO

1. 在 Configuration 页面填写信息，在 Applications details 区域，输入 ACS URL、Entity ID。
该信息对应 服务提供商（SP）信息 中的 ACS URL 和 Entity ID。



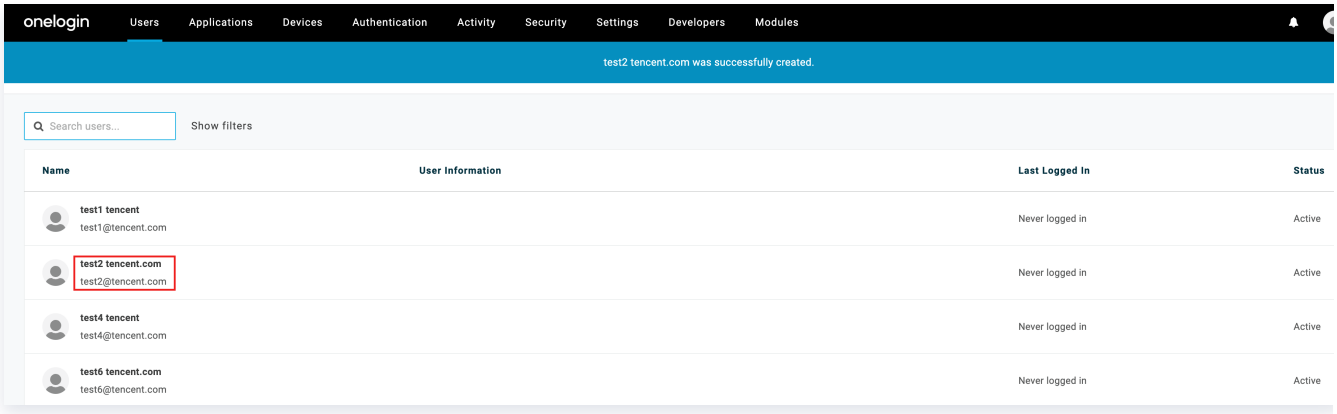
2. 在 SSO 页面中，将 SAML Signature Algorithm 协议切换成 SHA-256（默认为 SHA-1，身份中心不支持该协议），单击 Save。

   在 More Actions 中下载 SAML Metadata。

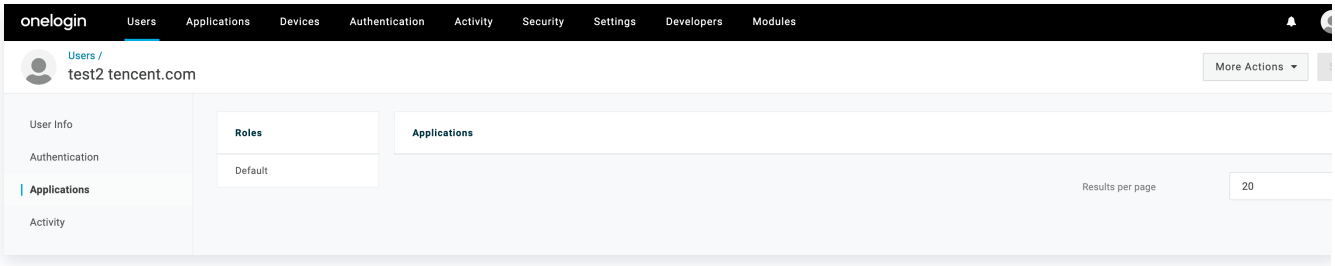


3. 将用户分配到应用。

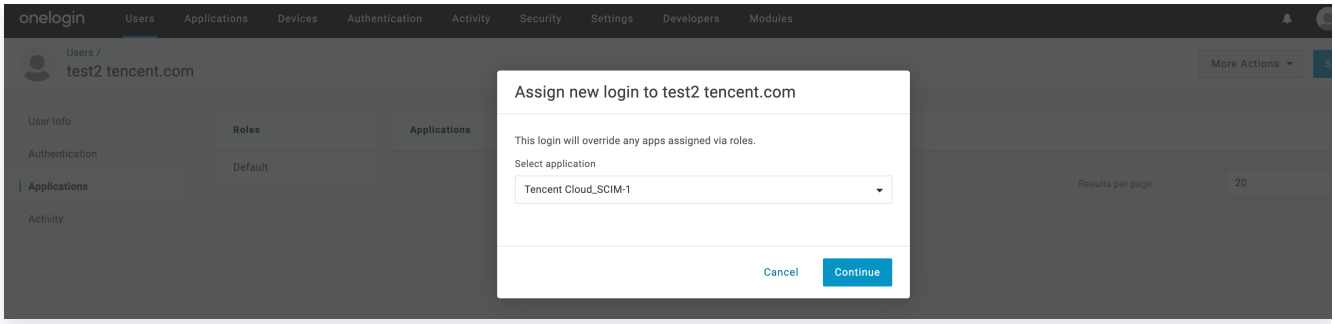
   3.1 在顶部菜单选择 Users > Users 进入用户列表，单击需要同步的用户名称，进入用户详情页。



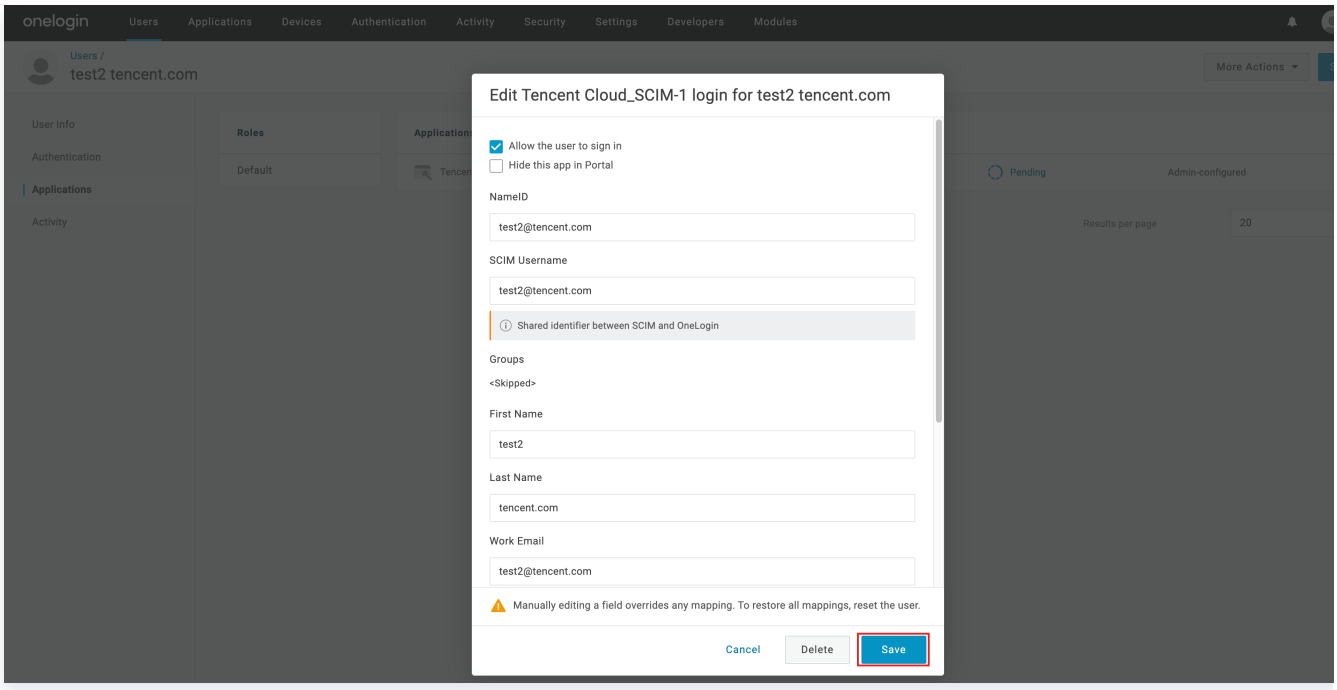
   3.2 左侧选择 Applications，单击+，将用户分配到目标应用中。



3.3 在 **Select application** 中选择应用，单击 **Continue**。



3.4 在编辑表单中，修改用户名、邮箱等信息（可选），单击 **Save**。



步骤三：在身份中心上传联合元数据 XML

1. 在**集团账号管理** > **身份中心管理** > 设置 > **SSO 登录**的**身份提供商(IDP)信息**区域，单击**配置身份提供商信息**。

2. 单击**选择文件**，上传在 Onelogin 下载的**联合元数据 XML**。

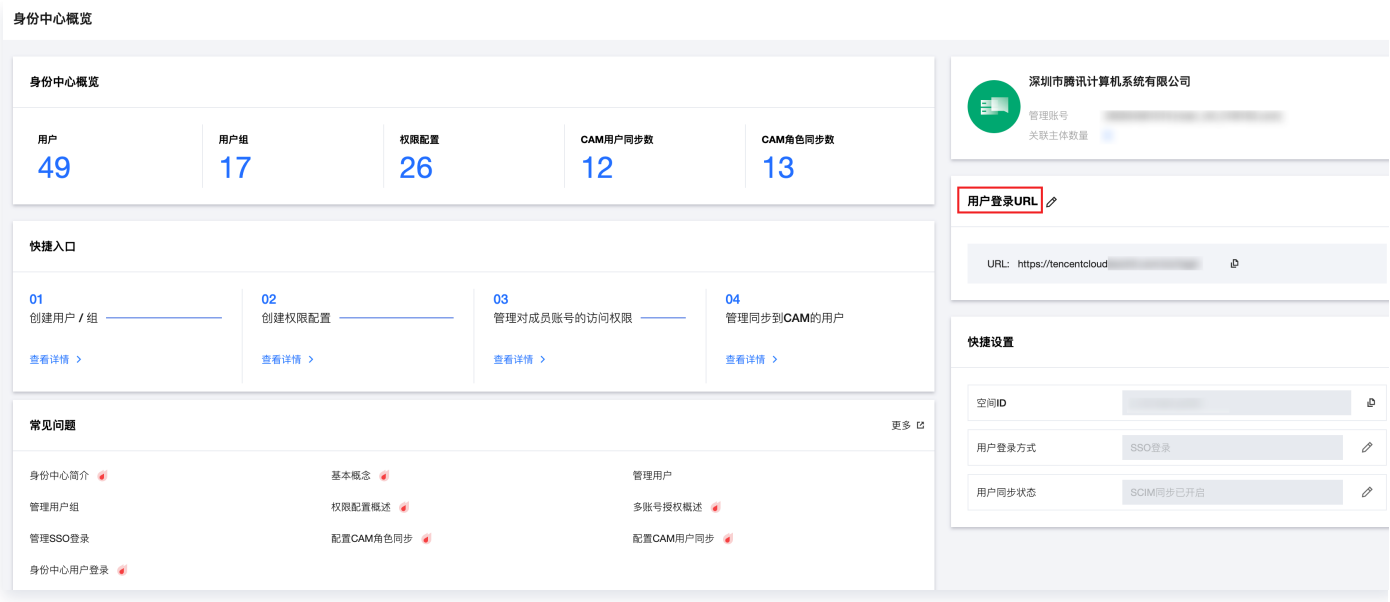
结果验证

完成 SSO 登录配置后，您可以从腾讯云发起 SSO 登录。

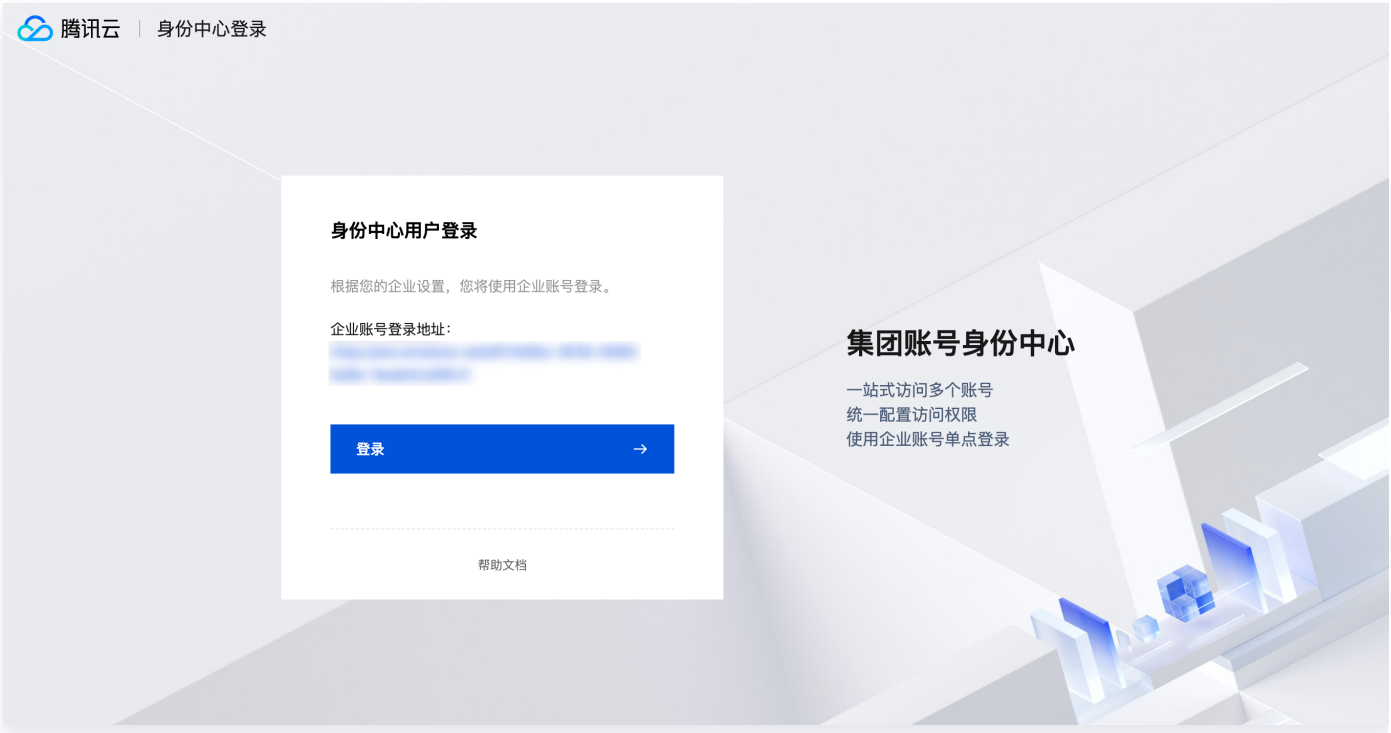
> **前提**：在身份中心需要创建和 Onelogin 应用中同名的用户，进入**集团账号管理> 身份中心管理 >** 用户 中创建。

登录流程：

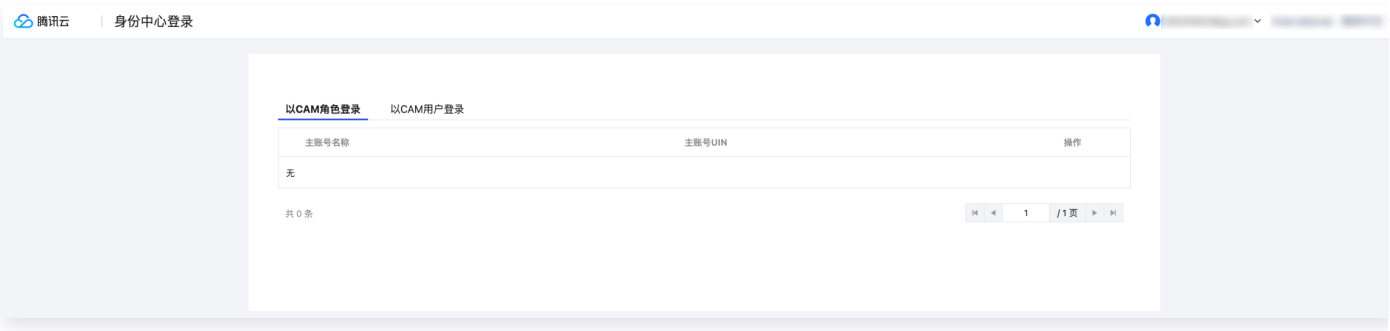
1. 身份中心管理员进入**集团账号管理 > 身份中心管理 >** 身份中心概览 的页面的右侧，查看并复制**用户登录 URL**。



2. 单击访问**用户登录 URL**，单击**登录**。



3. 重定向到 Onelogin 登录页面，输入账号密码登录。
4. 登录成功，进入身份中心账号列表页。



管理权限配置
权限配置概述

最近更新时间：2024-07-31 14:17:23

权限配置是身份中心用户用来访问账号的配置模板，其中包含 CAM 的预设策略，暂不支持自定义策略。您可以使用该模板为身份中心用户在账号上授权。

首次部署权限配置

当您为用户或用户组设置在账号中的权限时，需要指定一个权限配置。如果没有其他用户或用户组在该账号中部署过权限配置，则身份中心将会为您在账号的 CAM 中进行权限配置的部署操作。在 CAM 中部署的内容如下：

- 创建一个类型为**身份中心同步**的 **CAM角色**。
- 在CAM 角色上，将**绑定权限配置**中指定的系统策略，暂不支持自定义策略。
- 如果账号中还未进行过任何授权，则将**创建**一个**身份提供商**，以使身份中心用户可以使用角色 SSO 登录该账号。
- 您在账号的 CAM 控制台上可以查看上述 CAM 角色和身份提供商，但**不能**对其进行任何**修改**或**删除**操作。

重新部署权限配置

如果权限配置已经部署在账号中，但权限配置发生了变更，这些变更不会自动更新到对应的账号中，此时需要您手动重新部署（添加或移除系统策略）才能使变更生效。

权限配置

最近更新时间：2025-02-07 15:51:47

操作场景

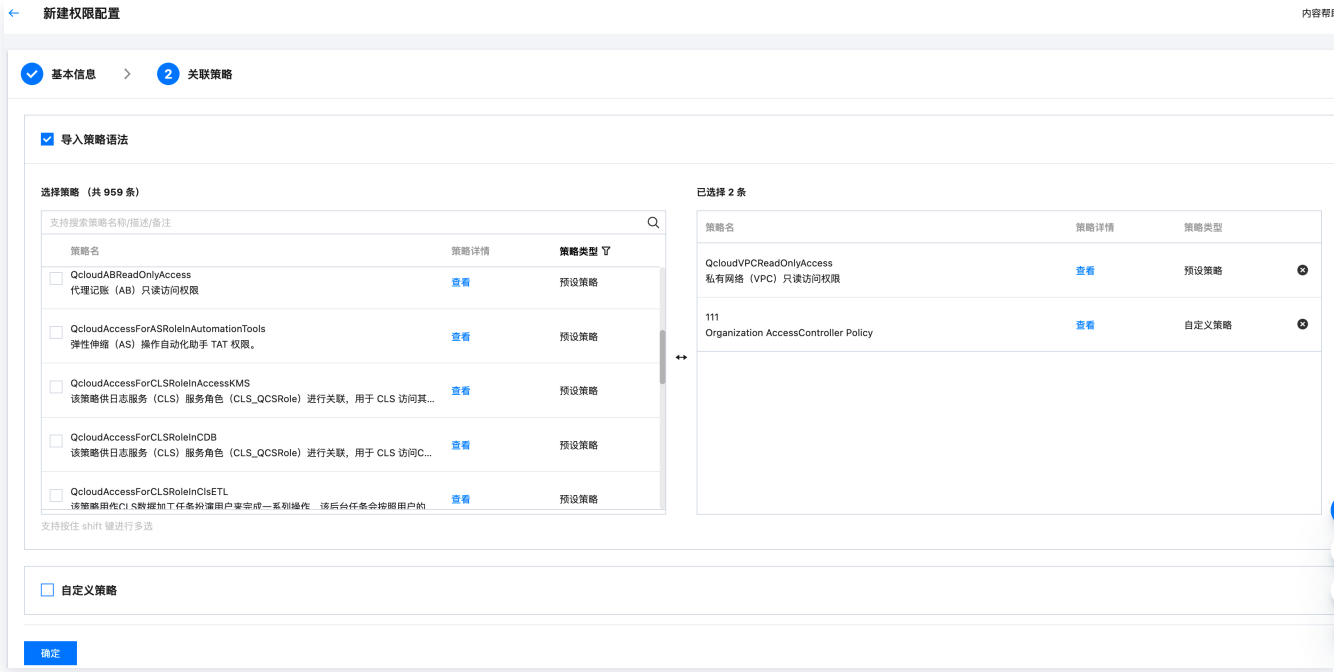
本文为您介绍新建权限配置、查看权限配置、删除权限配置的操作。

操作步骤

新建权限配置

1. 已登录**集团账号管理** > 身份中心 。
2. 在左侧导航栏，单击 **CAM 同步** > **权限配置**。
3. 在**权限配置**页面，单击**新建权限配置**。
4. 在**新建权限配置**面板，配置以下基本信息，然后单击**下一步**。
   - **权限名称**：必选参数。在空间内必须唯一。
   - **权限描述**：可选参数。权限配置的描述信息。

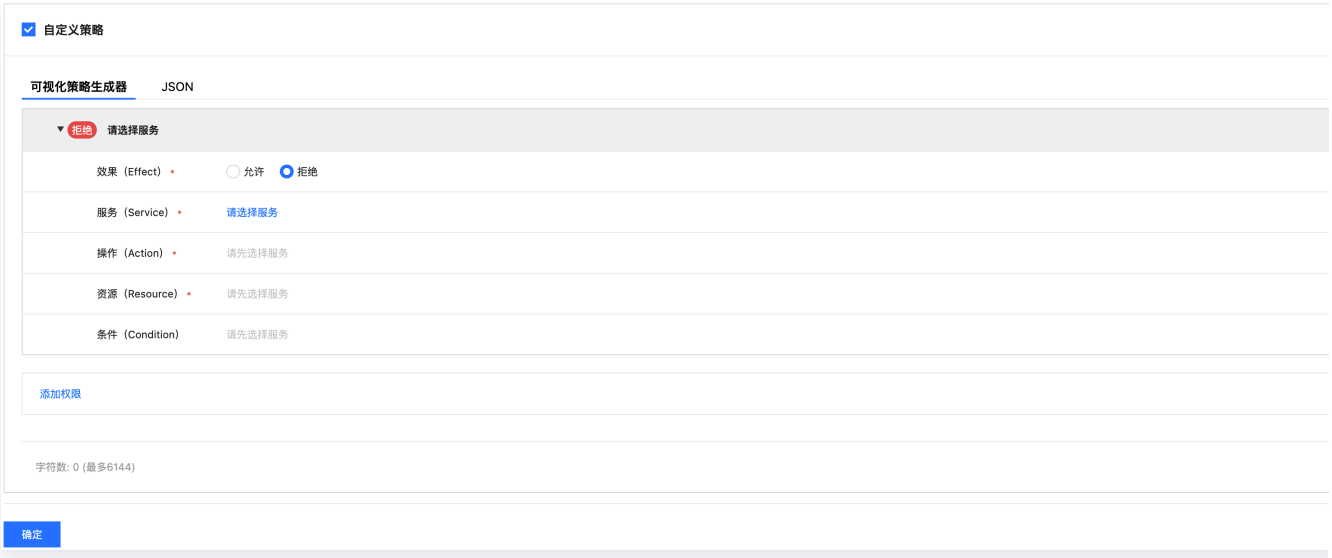
5. 配置关联策略，可以选择导入已有**预设策略**和**自定义策略**。
   - 导入策略语法



- 添加自定义策略。自定义策略复用 CAM 的策略语法，语法逻辑，请参见 语法结构 。

  可以通过可视化策略生成器创建自定义策略。配置方法，请参见 通过策略生成器创建自定义策略 。

  或者通过 JSON 创建自定义策略。配置方法，请参见 通过策略语法创建自定义策略 。



6. 单击**确定**。

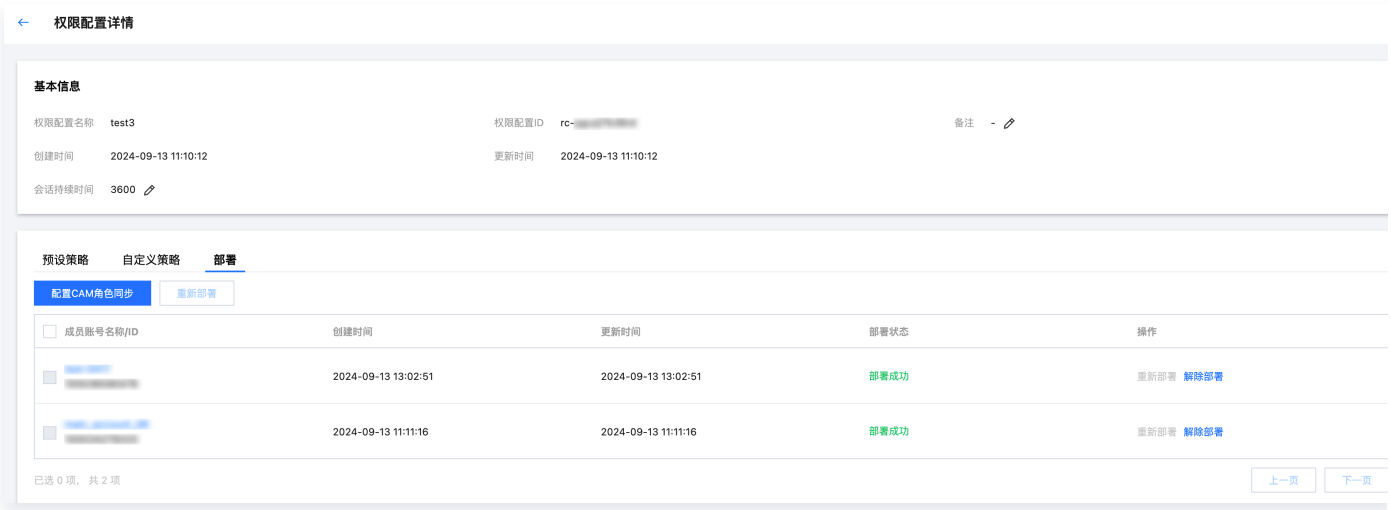
查看权限配置

1. 已登录**集团账号管理** > 身份中心 。
2. 在左侧导航栏，单击 **CAM 同步** > **权限配置**。
3. 在**权限配置**页面，单击目标权限配置名称。
4. 查看权限配置的**基本信息**。

5. 单击**预设策略**页签，查看权限配置的预设策略。

6. 单击**自定义策略**页签，查看权限配置的自定义策略。

7. 单击**部署**页签，查看该权限配置已部署的成员账号。



删除权限配置

前提条件

删除权限配置前，请确保权限配置已解除以下关联：

- 预设策略：您需要删除权限配置中的预设策略。
- 自定义策略：您需要删除权限配置中的自定义策略。
- 部署：您需要解除该权限配置在成员账号中的部署。

操作步骤

1. 已登录**集团账号管理** > 身份中心 。
2. 在左侧导航栏，单击 **CAM 同步** > **权限配置**。
3. 在**权限配置**页面，单击目标权限配置**操作**列的**删除**。
4. 在**删除权限配置**对话框，单击**确定**。

管理预设策略

最近更新时间：2025-02-07 15:52:03

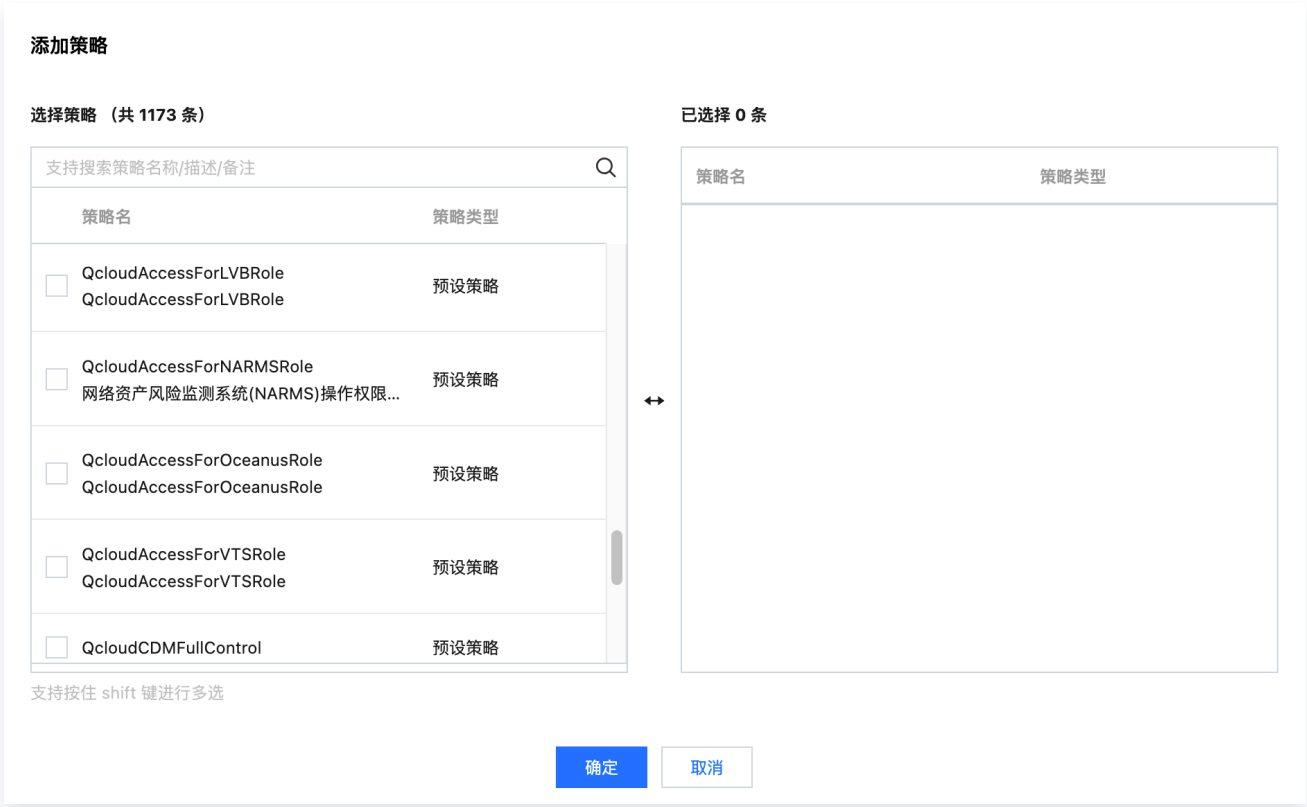
本文为您介绍管理预设策略的操作，包括添加预设策略、删除预设策略。每个权限配置默认最多可以配置20条预设策略。

> **注意：**
> 添加或删除预设策略后，如果权限配置已经被部署在账号中，您需要重新部署权限配置，才能在账号中生效。具体操作，请参见 重新部署权限配置 。

添加预设策略

1. 已登录**集团账号管理** > 身份中心 。
2. 在左侧导航栏，单击 **CAM 同步** > **权限配置**。
3. 在**权限配置**页面，单击目标权限配置名称。
4. 在**预设策略**页签，添加或删除预设策略。
5. 单击**添加策略**。

6. 在**添加策略**面板，按需勾选**预设策略**，单击**确定**。



删除预设策略

1. 单击目标预设策略**操作列**的**删除**。
2. 在弹出的对话框，单击**确定**。

管理自定义策略

最近更新时间：2025-02-07 15:51:20

本文为您介绍管理自定义策略的操作，包括添加自定义策略、修改自定义策略和删除自定义策略。自定义策略内容的最大长度为6144个字符。

> **注意：**
> 添加、修改或删除自定义策略后，如果权限配置已经被部署在成员账号中，您需要重新部署访问配置，才能在成员账号中生效。具体操作，请参见 重新部署权限配置 。

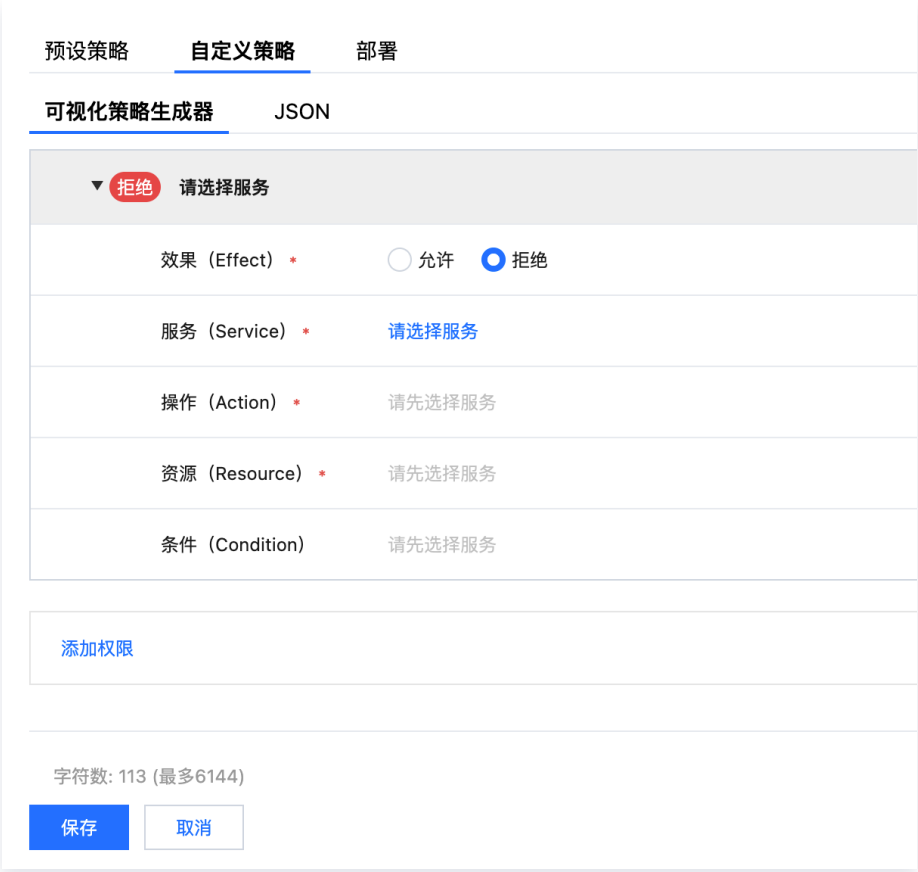
添加自定义策略

1. 登录**集团账号管理** > 身份中心 。
2. 在左侧导航栏，单击 **CAM 同步** > **权限配置**。
3. 在**权限配置**页面，单击目标权限配置名称。
4. 在**自定义策略**页签，管理自定义策略。

方式一：添加策略

1. 单击**添加策略**。自定义策略复用 CAM 的策略语法，语法逻辑，请参见 语法结构 。

   - 可以通过可视化策略生成器创建自定义策略，配置方法，请参见 通过策略生成器创建自定义策略 。

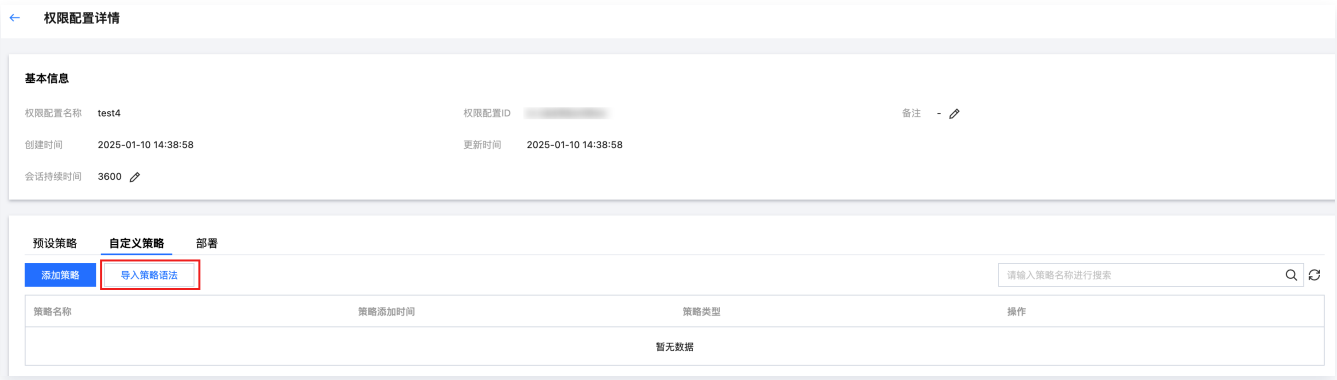


- 或者通过 JSON 创建自定义策略。配置方法，请参见 通过策略语法创建自定义策略 。

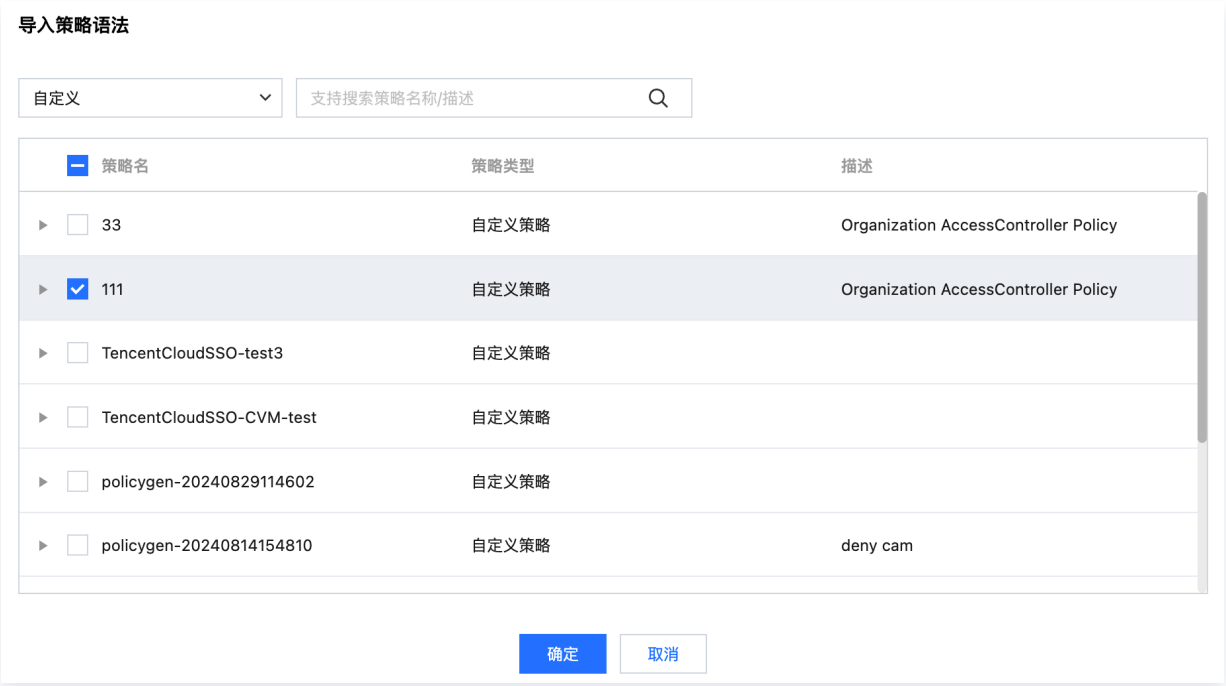
2. 添加好后，单击**保存**。

方式二：导入策略语法

1. 通过导入已有策略添加自定义策略，单击**导入策略语法**。

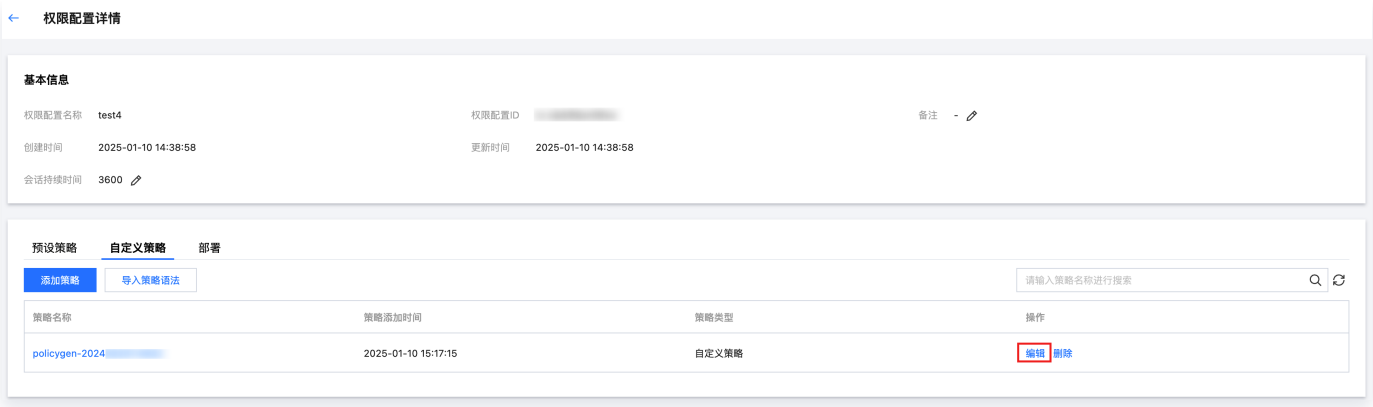


2. 勾选 CAM 中已有的自定义策略，单击**确定**。



修改自定义策略

1. 登录**集团账号管理** > 身份中心 。
2. 在左侧导航栏，单击 **CAM 同步** > **权限配置**。
3. 在**权限配置**页面，单击目标权限配置名称。
4. 在**权限配置详情**页面，单击操作列的**编辑**按钮。



5. 修改自定义策略内容后，单击**保存**。

删除自定义策略

1. 登录**集团账号管理** > 身份中心 。
2. 在左侧导航栏，单击 **CAM 同步** > **权限配置**。
3. 在**权限配置**页面，单击目标权限配置名称。
4. 在**权限配置详情**页面，单击操作列的**删除**按钮，在弹出的对话框，单击**确定**。


权限配置详情
基本信息
权限配置名称 test4
权限配置ID
备注 -
创建时间 2025-01-10 14:38:58
更新时间 2025-01-10 14:38:58
会话持续时间 3600
预设策略
自定义策略
部署
添加策略
导入策略语法
请输入策略名称进行搜索
策略名称
策略添加时间
策略类型
操作
policygen-2024
2025-01-10 15:17:15
自定义策略
编辑
删除

重新部署权限配置

最近更新时间：2024-07-31 14:17:23

操作场景

如果权限配置已经部署在账号中，当权限配置发生了变更，这些变更不会自动更新到对应的账号中，需要您手动重新部署才能使其生效。

前提条件

权限配置（添加或删除预设策略）发生变更时，需要您重新部署。

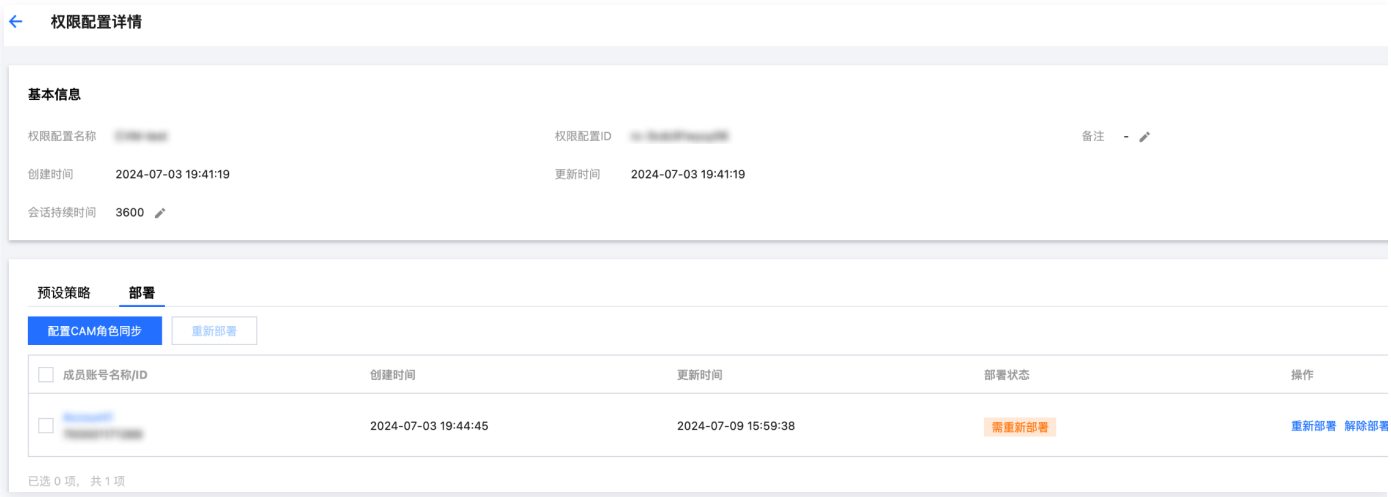
操作步骤

在权限配置页面重新部署权限配置

1. 登录**集团账号管理** > 身份中心 。
2. 在左侧导航栏，单击 **CAM 同步** > **权限配置**。
3. 在**权限配置**页面，单击目标权限配置名称。

   系统会自动标识需要重新部署的权限配置，其**部署状态**显示为**需要重新部署**。
4. 单击**部署**页签。
5. 选择目标账号名称。

   系统会自动标识需要重新部署访问配置的RD账号，其**部署状态**显示为**需要重新部署**。



6. 单击**重新部署**，在**重新部署**页面，确认以下信息，确认无误后单击**下一步**。

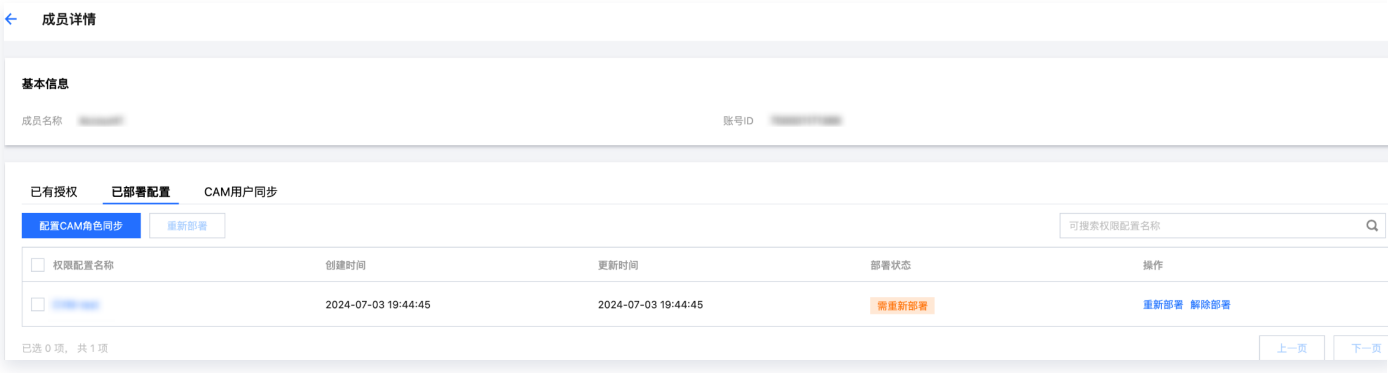
7. 单击**确定**。

8. 部署完成后，**部署状态**显示为**部署成功**。

在多账号权限管理页面重新部署权限配置

1. 登录**集团账号管理** > 身份中心 。
2. 在左侧导航栏，单击 **CAM 同步** > **多账号权限管理**。
3. 在**多账号权限管理**页面，选择目标账号。
4. 单击**已部署配置**页签。
5. 选择需要重新部署的访问配置。

   系统会自动标识需要重新部署的访问配置，其**部署状态**显示为**需要重新部署**。



6. 单击**重新部署**，根据页面指引进行操作即可。
7. 部署完成后，**部署状态**显示为**部署成功**。

解除权限配置部署

最近更新时间：2024-07-31 14:17:23

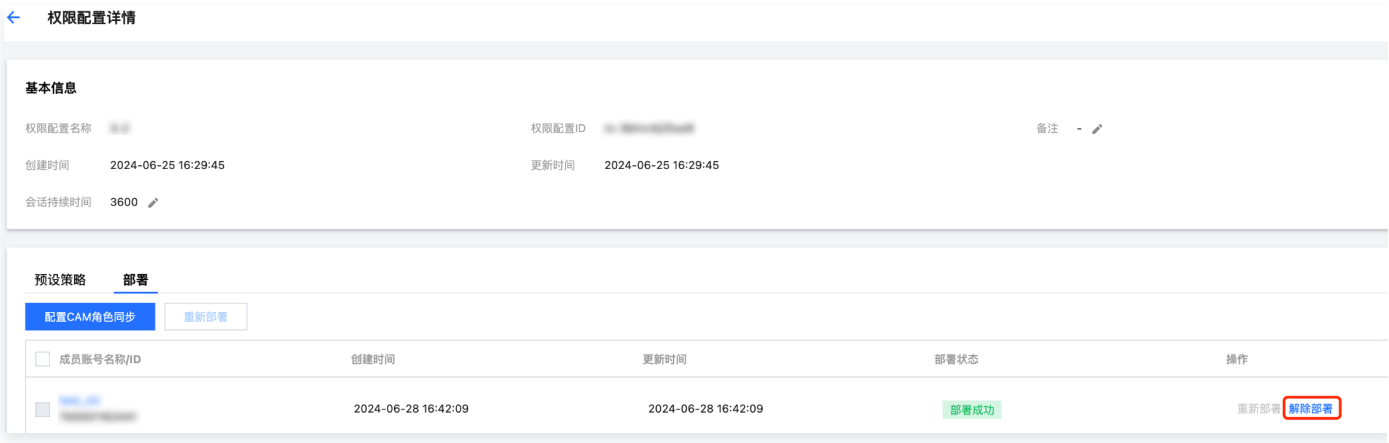
操作场景

您可以主动解除权限配置在一个账号中的部署。本文为您介绍解除权限配置部署。

操作步骤

在权限配置页面解除部署权限配置

1. 登录**集团账号管理** > 身份中心 。
2. 在左侧导航栏，单击 **CAM 同步** > **权限配置**。
3. 在**权限配置**页面，单击目标权限配置名称。
4. 单击**部署**页签。
5. 单击目标账号**操作**列的**解除部署**。



6. 在**解除部署**的对话框。
   - 确认移除授权信息，单击**下一步**，移除此权限配置对用户/用户组的授权。

- 确认解除部署信息，单击**下一步**，解除此权限配置在账号中的部署。

- 单击**完成**。

在多账号权限管理页面解除部署权限配置

1. 登录**集团账号管理** > 身份中心 。
2. 在左侧导航栏，单击 **CAM 同步** > **多账号权限管理**。
3. 在**多账号权限管理**页面，选择目标账号。
4. 单击**已部署配置**页签。
5. 单击目标权限配置**操作**列的**解除部署**。

6. 单击**解除部署**。
   - 确认移除授权信息，单击**下一步**，移除此权限配置对用户/用户组的授权。
   - 确认解除部署信息，单击**下一步**，解除此权限配置在账号中的部署。
   - 单击**完成**。

管理多账号授权
多账号授权概述

最近更新时间：2024-07-31 14:17:23

在多账号授权页面，您可以根据集团账号的目录结构，配置 CAM 用户同步、配置 CAM 角色同步。

差异说明

身份中心用户可以通过 **CAM 角色**或 **CAM 用户**访问账号的云资源，两种方式的差异如下表所示。

访问方式	说明	同步方式	相关文档
配置 CAM 角色同步	企业在集团账号身份中心管理访问腾讯云的用户，通过权限配置和 CAM 角色同步，实现用户通过单点登录的方式登录到成员账号内的 CAM 角色，然后访问该成员账号的云资源。	在配置 CAM 角色同步时，身份中心会针对每个三元组（用户-账号-权限配置）启动任务。 同步后在 CAM 中的访问权限已确定，且在 CAM 中不可修改。	• 权限配置 • 配置 CAM 角色同步
配置 CAM 用户同步	企业在集团账号身份中心管理访问腾讯云的用户，通过配置 CAM 用户同步，实现用户登录到成员账号内的 CAM 用户，然后访问该成员账号的云资源。	在配置 CAM 用户同步时，身份中心会针对每个二元组（用户-账号）启动任务。 同步后在 CAM 中的访问权限为空，需要在 CAM 中配置。	配置 CAM 用户同步

CAM 角色同步说明

如果您想对多个账号、多个身份和多个访问配置进行一次性批量授权，您可以进入**集团账号管理 >** 身份中心 的多账号权限管理页面，浏览账号目录树并进行以下操作：

1. 在账号树中选择一个或多个账号，作为授权目标。
2. 选择一个或多个身份中心身份。
3. 选择一个或多个访问配置。
4. 单击配置 CAM 角色同步，身份中心服务将为您批量完成授权。
    - 在批量授权中，对于部分已经存在的批量授权，如果对其进行重复授权，会操作失败。但同一批中的新增授权会操作成功。
    - 每一次添加权限的过程中，身份中心将会针对每个三元组（身份-账号-权限配置），启动一个异步任务。

CAM 用户同步说明

如果您想对多个账号、多个身份进行一次性批量授权，您可以进入**集团账号管理 >** 身份中心 的多账号权限管理页面，浏览账号目录树并进行以下操作：

1. 在账号目录树中选择一个或多个账号。
2. 选择一个或多个身份中心身份。
3. 单击配置 CAM 用户同步，身份中心服务将为您批量完成同步。
    - 在批量同步中，对于部分已经存在的同步，如果对其进行重复操作，会操作失败。但同一批中的新增同步会操作成功。
    - 配置成功后，会在目标账号中创建一个与身份中心用户同名的 CAM 用户。
        - 授权：访问目标账号，为上一步创建的 CAM 用户授权。

          CAM 用户默认没有任何权限，您需要授予其对应资源的权限。
        - 身份中心用户通过 CAM 用户身份访问目标账号中的有权限的资源。

具体操作，请参见 配置 CAM 用户同步 。

配置 CAM 角色同步

最近更新时间：2024-07-31 14:17:23

操作场景

根据集团账号组织结构，您可以为每个账号设置允许访问的用户或用户组，以及他们的权限配置。
本文将提供一个示例，为身份中心的用户（user1）在成员账号（Account1）上部署权限配置，该权限配置仅定义了 CVM 的访问权限，实现身份中心的用户（user1）仅能访问成员账号（Account1）中的 CVM 资源。

前提条件

- 请确保您已创建了权限配置。

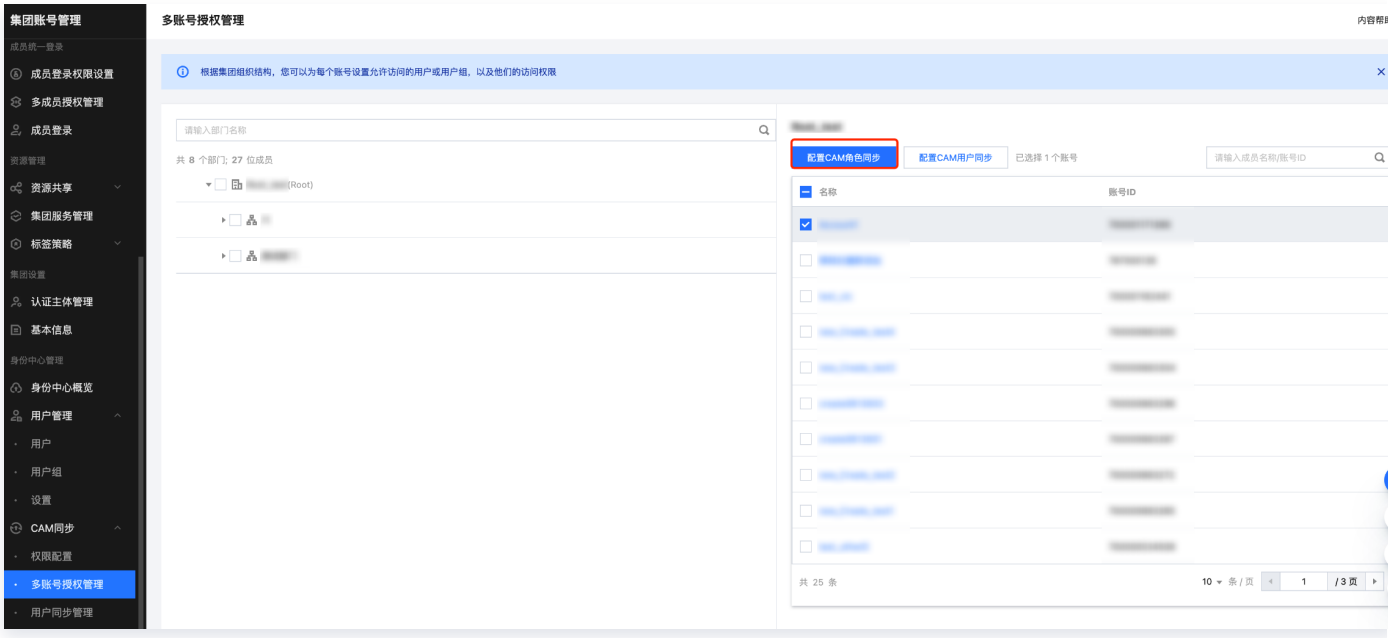
  本示例中，使用的权限配置已绑定预设策略，不创建自定义策略。
- 请确保您已创建或同步了用户。

  本示例中，使用身份中心创建的用户（user1）。具体操作，请参见 管理用户 。

操作步骤

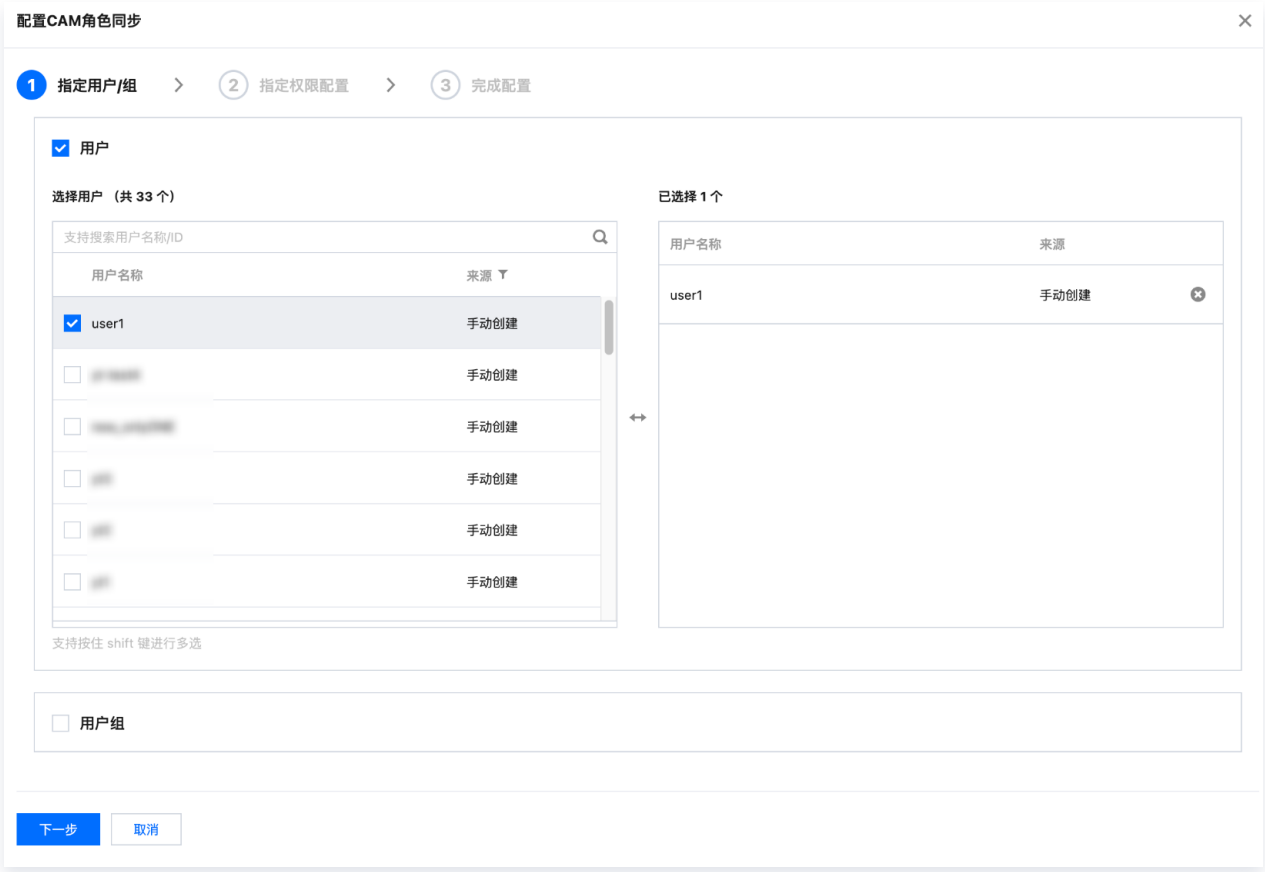
1. 进入**集团账号管理 >** 身份中心 。
2. 在左侧导航栏，单击 **CAM 同步 > 多账号授权管理**。
3. 在**多账号授权管理**页面，选择目标账号。

   本示例中，选择成员账号（Account1）。
4. 单击**配置 CAM 角色同步**。

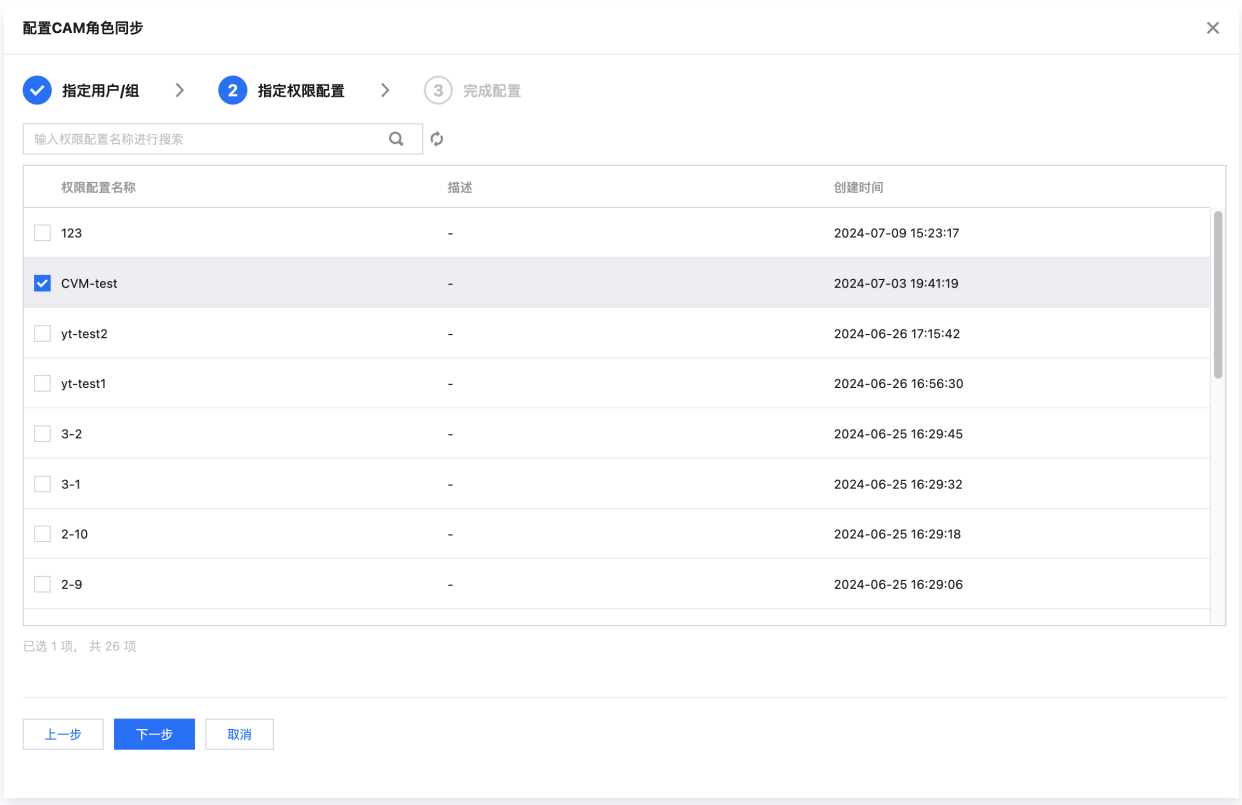


5. 在**配置 CAM 角色同步**页面，选择目标用户或用户组，然后单击下一步。

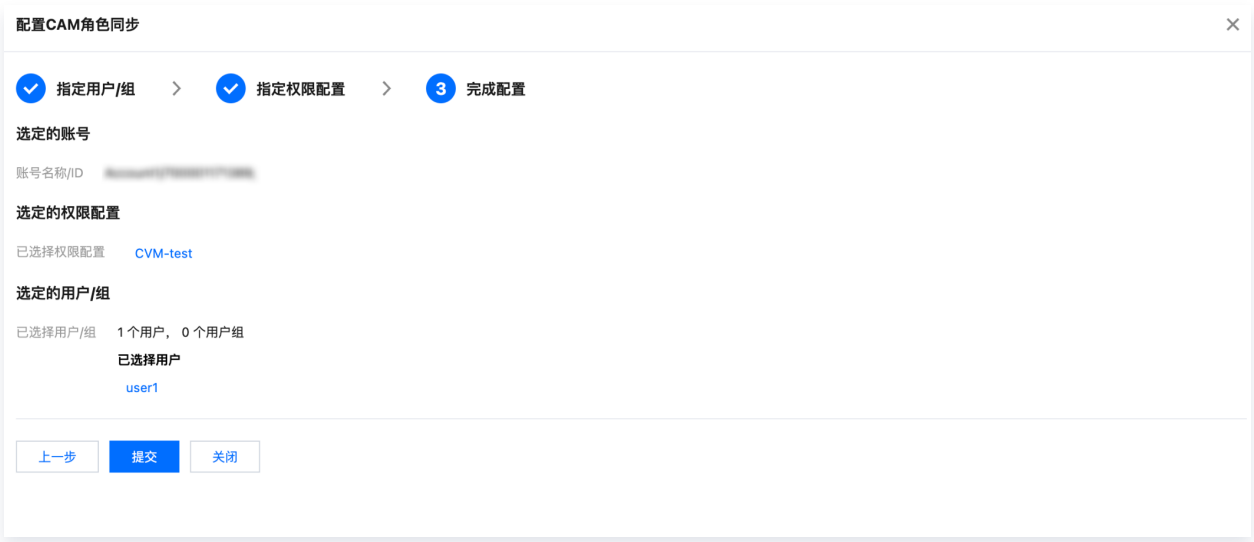
   本示例中，选择用户（user1）。



6. 选择目标**权限配置**，然后单击下一步。



7. 浏览配置信息，然后单击**提交**。

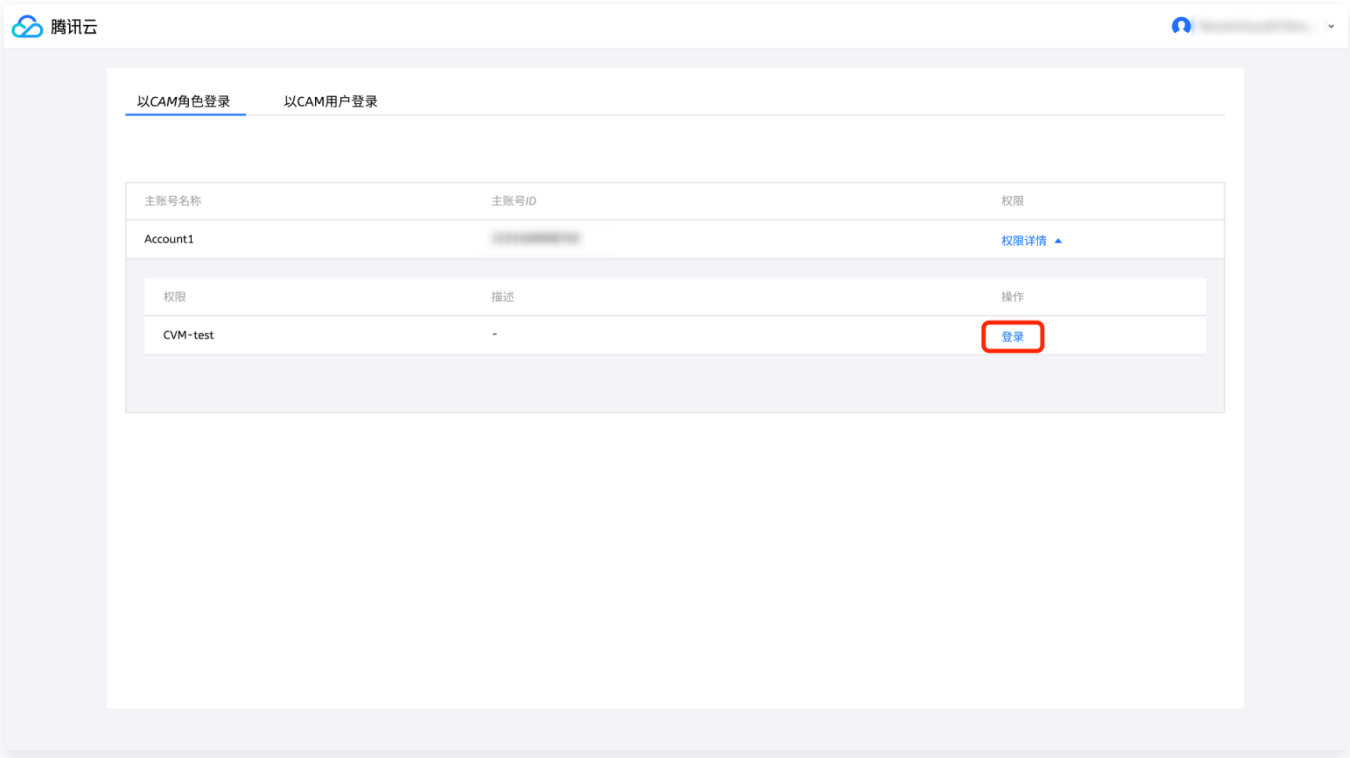


8. 等待配置完成，然后单击**完成**。

结果验证

1. 使用身份中心用户（user1）登录集团账号身份中心门户。

   具体操作，请参见 身份中心用户登录 。
2. 在**以 CAM 角色登录**页签，单击成员账号（Account1）权限列的显示详情。
3. 在权限面板，单击目标权限配置**操作**列的**登录**。



4. 以 CAM 角色身份访问成员账号（Account1）中的 CVM 资源。

> **说明：**
> 因为只配置了 CVM 的访问权限，所以仅能访问 CVM 资源。如需访问其他资源，请修改权限配置中的策略，并重新部署权限配置。

查看/修改/删除授权

最近更新时间：2024-07-31 14:17:23

操作场景

本文为您介绍如何查看账号的授权信息、修改账号的授权和删除账号的授权。

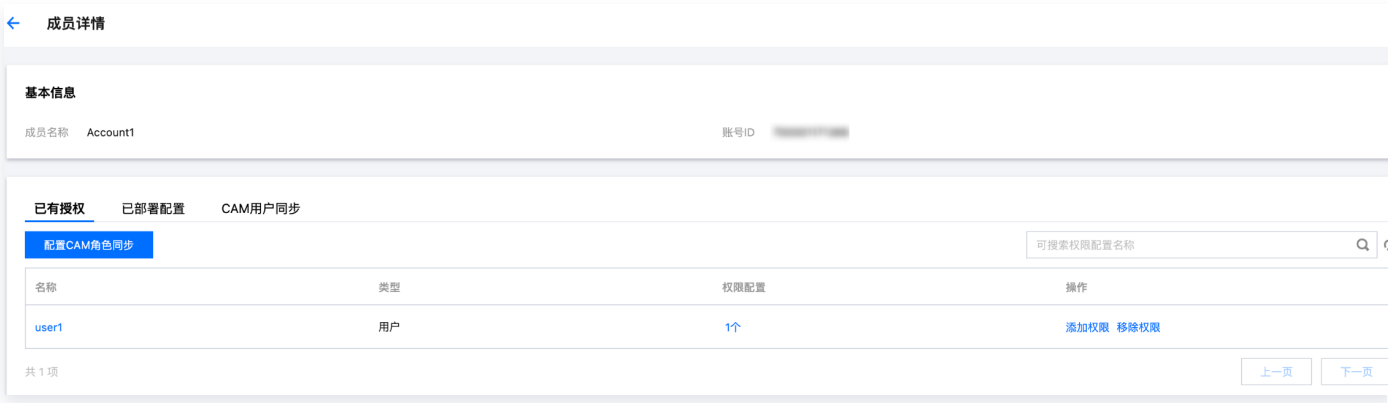
操作步骤

查看授权信息

1. 进入**集团账号管理** > 身份中心 。
2. 在左侧导航栏，单击 **CAM 同步** > **多账号授权管理**。
3. 在**多账号授权管理**页面，单击目标账号名称。
4. 查看账号的授权信息。
   - 在**基本信息**区域，查看账号基本信息。
   - 在**已有授权**页签，查看账号关联的用户或用户组。
   - 在**已部署配置**页签，查看账号中部署的权限配置。
   - 在 **CAM 用户同步**页签，查看配置的 CAM 用户同步信息。

修改账号的授权

1. 进入**集团账号管理** > 身份中心 。
2. 在左侧导航栏，单击 **CAM 同步** > **多账号授权管理**。
3. 在**多账号授权管理**页面，单击目标账号名称。
4. 单击**已有授权**页签。
5. 单击**配置 CAM 角色同步**。



6. 在**配置CAM角色同步**面板，重新指定用户、用户组和权限配置。
    - 选择用户或用户组，然后单击**下一步**。
    - 选择权限配置，然后单击**下一步**。
    - 浏览配置信息，然后单击**开始配置**。
    - 等待部署完成，然后单击**完成**。

删除账号的授权

1. 进入**集团账号管理** > 身份中心 。
2. 在左侧导航栏，单击 **CAM 同步** > **多账号授权管理**。
3. 在**多账号授权管理**页面，单击目标账号名称。
4. 单击**已有授权**页签。
5. 单击目标用户或用户组操作列的**移除权限**。
6. 在确认删除对话框，单击**确定**。
7. 单击**完成**。

管理 CAM 用户同步
配置 CAM 用户同步

最近更新时间：2024-07-31 14:17:23

操作场景

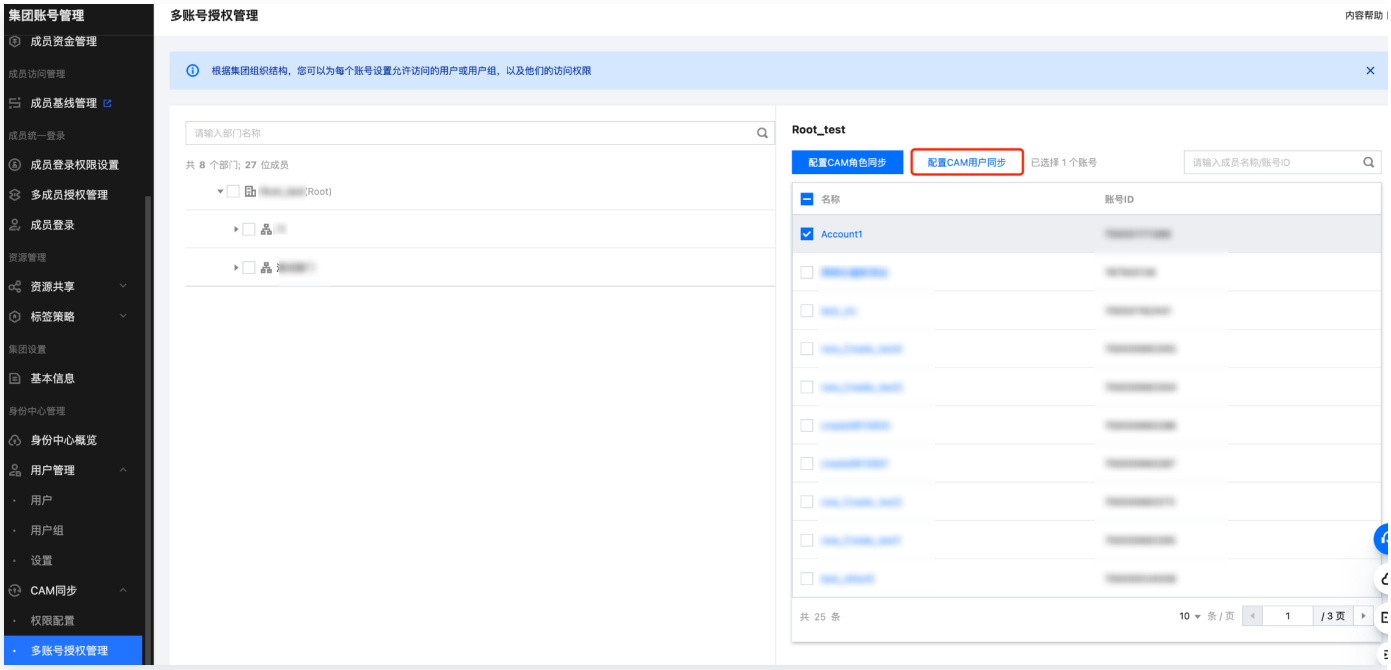
您可以配置 CAM 用户同步，在目标账号中同步创建一个与身份中心用户同名的 CAM 用户，然后通过该 CAM 用户访问该账号中的资源。
本文将提供一个示例，通过配置 CAM 用户同步，在成员账号（Account1）中创建一个与身份中心用户（user1）同名的 CAM 用户（user1@tencent），然后为 CAM 用户（user1@tencent）授予 CVM 的管理权限，实现通过 CAM 用户（user1@tencent）身份访问成员账号（Account1）中的 CVM 资源。

操作步骤

步骤一：配置 CAM 用户同步

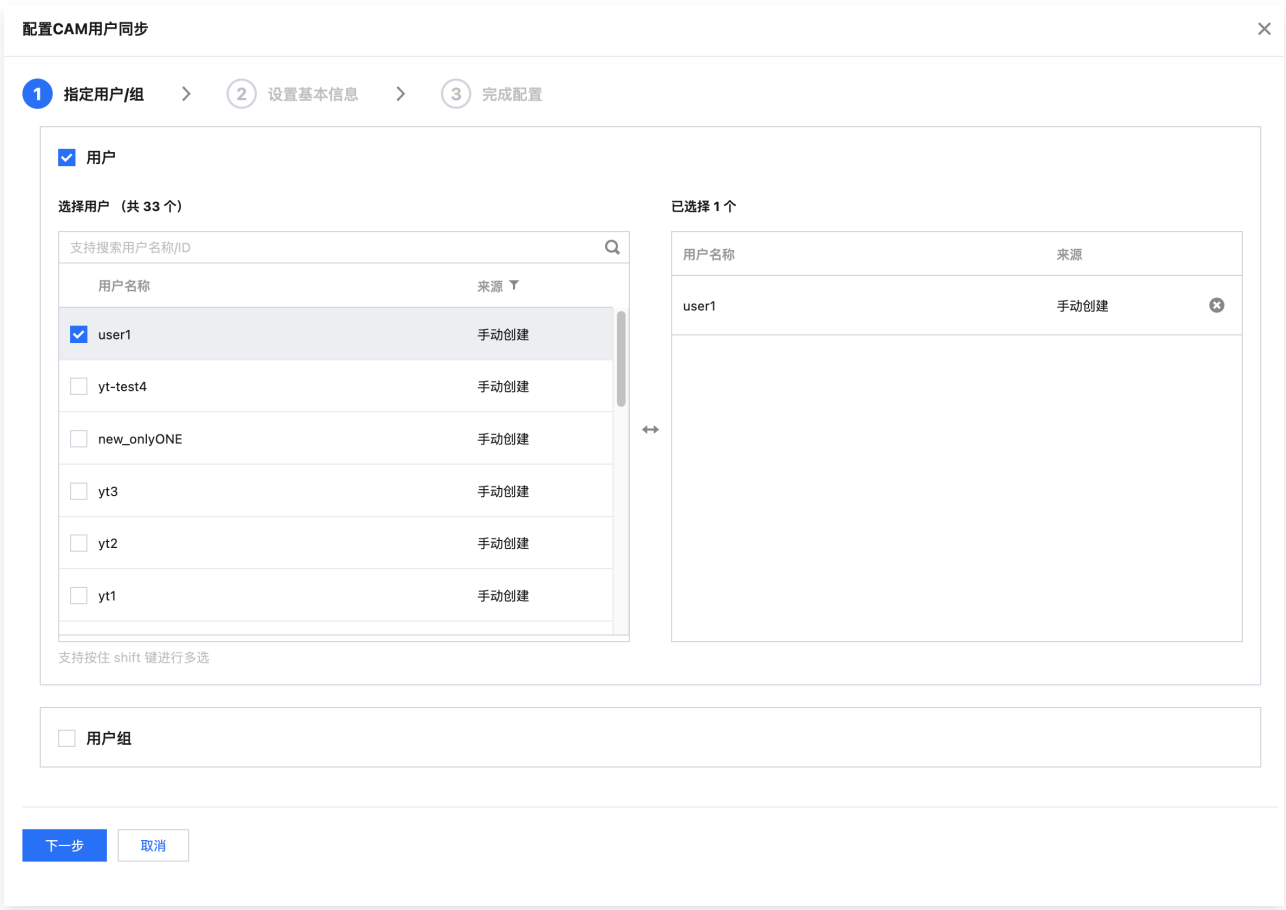
使用管理账号在身份中心中配置 CAM 用户同步。

1. 进入**集团账号管理** > 身份中心 。
2. 在左侧导航栏，单击 **CAM 同步** > **多账号授权管理**。
3. 在**多账号授权管理**页面，选择目标账号。
   本示例中，选择成员账号（Account1）。
4. 单击**配置 CAM 用户同步**。



5. 在**配置 CAM 用户同步**面板，选择目标用户或用户组，然后单击**下一步**。

   本示例中，选择身份中心用户（user1）。



6. 设置以下基本信息，然后单击**下一步**。
   6.1 输入 CAM 用户同步的描述。
   6.2 配置**冲突策略**。
   - 冲突策略：当目标账号内存在同名 CAM 用户时的处理策略。
     - **替换**：新创建的CAM用户会覆盖已存在的 CAM 用户。
     - **两者都保留**：新创建的 CAM 用户会被系统重命名，新旧两个 CAM 用户会同时保留。

   6.3 配置**删除策略**。
   - 删除策略：删除 CAM 用户同步时，对已同步的 CAM 用户的处理策略。
     - **保留**：删除 CAM 用户同步时，会保留已同步的 CAM 用户。
     - **删除**：删除 CAM 用户同步时，会删除已同步的 CAM 用户。

7. 单击**完成**。

   配置成功后，会在目标账号内创建一个同名的CAM用户。本示例中，将会在成员账号（Account1）中同步创建一个与身份中心用户（user1）同名的CAM用户（user1@tencent）。

步骤二：为 CAM 用户授权

通过 身份中心 > **配置 CAM 用户同步**，同步到 CAM 的子用户未授予任何权限，需要在 CAM 控制台对用户授权。如需要通过身份中心预设权限，请您选择配置 CAM 角色同步。

1. 登录成员账号（Account1）。
2. 为 CAM 用户（user1@tencent）授权。

   本示例中，将授予 CAM 用户（user1@tencent）CVM 的管理权限。具体操作，请参见 子用户权限设置 。

步骤三：身份中心用户访问腾讯云

身份中心用户（user1）通过CAM用户（user1@tencent）身份访问成员账号（Account1）中的CVM资源。

1. 身份中心用户（user1）登录身份中心用户门户。

   具体操作，请参见 身份中心用户登录 。
2. 以 CAM 用户身份访问成员账号（Account1）中的 CVM 资源。

查看/修改/删除用户同步

最近更新时间：2024-07-31 14:17:23

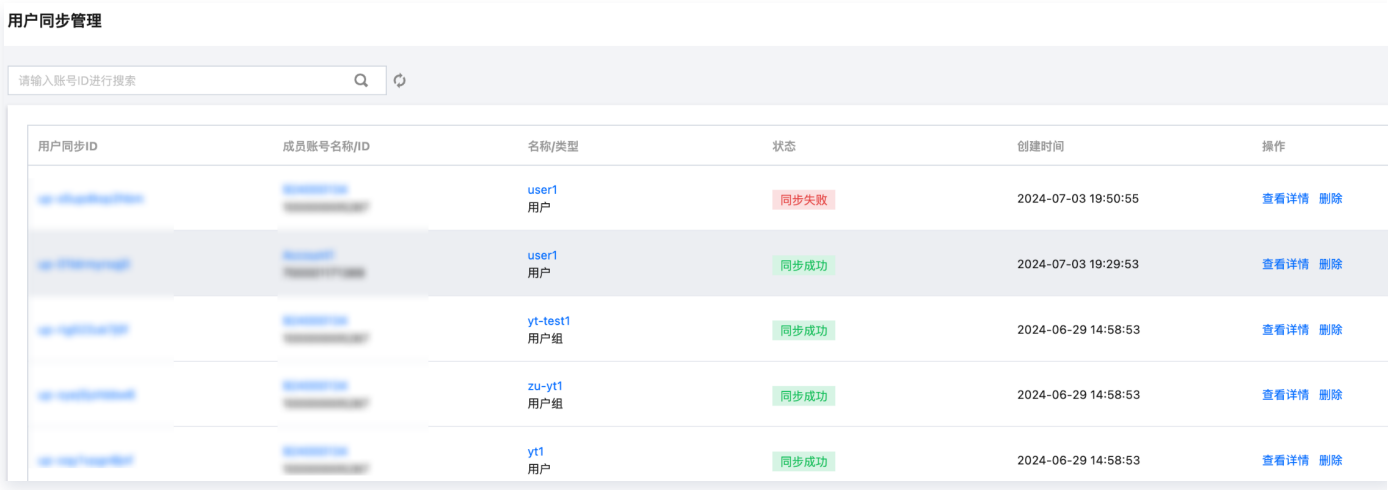
操作场景

本文为您介绍如何查看 CAM 用户同步详情、修改 CAM 用户同步和删除 CAM 用户同步。

操作步骤

查看 CAM 用户同步

1. 进入**集团账号管理** > 身份中心 。
2. 在左侧导航栏，选择 **CAM 同步** > **用户同步管理**。

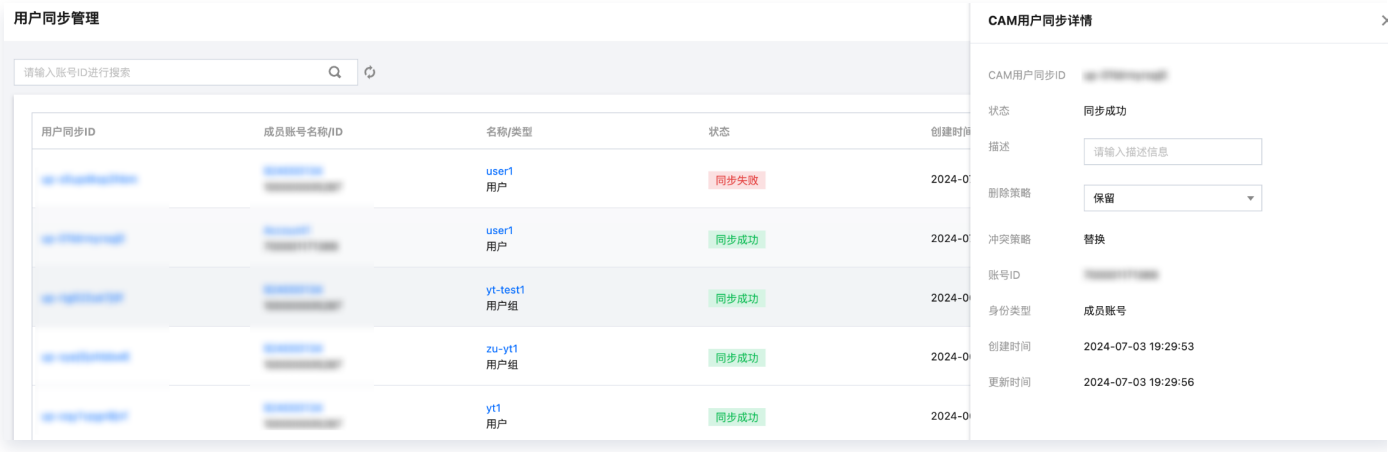


3. 在**用户同步管理**页面，单击目标用户同步**操作**列的**查看详情**。
4. 在**用户同步详情**面板，查看用户同步详情。包括 CAM 用户同步 ID、状态、删除策略、冲突策略、创建时间等。

修改 CAM 用户同步

1. 进入**集团账号管理** > 身份中心 。
2. 在左侧导航栏，选择 **CAM 同步** > **用户同步管理**。
3. 在**用户同步管理**页面，单击目标用户同步**操作**列的**查看详情**。
4. 在**用户同步详情**面板，单击**编辑**，修改描述或删除策略。

   关于配置项的含义，请参见 配置 CAM 用户同步 。



删除 CAM 用户同步

1. 进入**集团账号管理** > 身份中心 。
2. 在左侧导航栏，选择 **CAM 同步** > **用户同步管理**。
3. 在**用户同步管理**页面，单击目标用户同步**操作**列的**删除**。
4. 在弹出的对话框，单击**确定**。

用户登录
身份中心用户登录

最近更新时间：2025-07-09 17:16:03

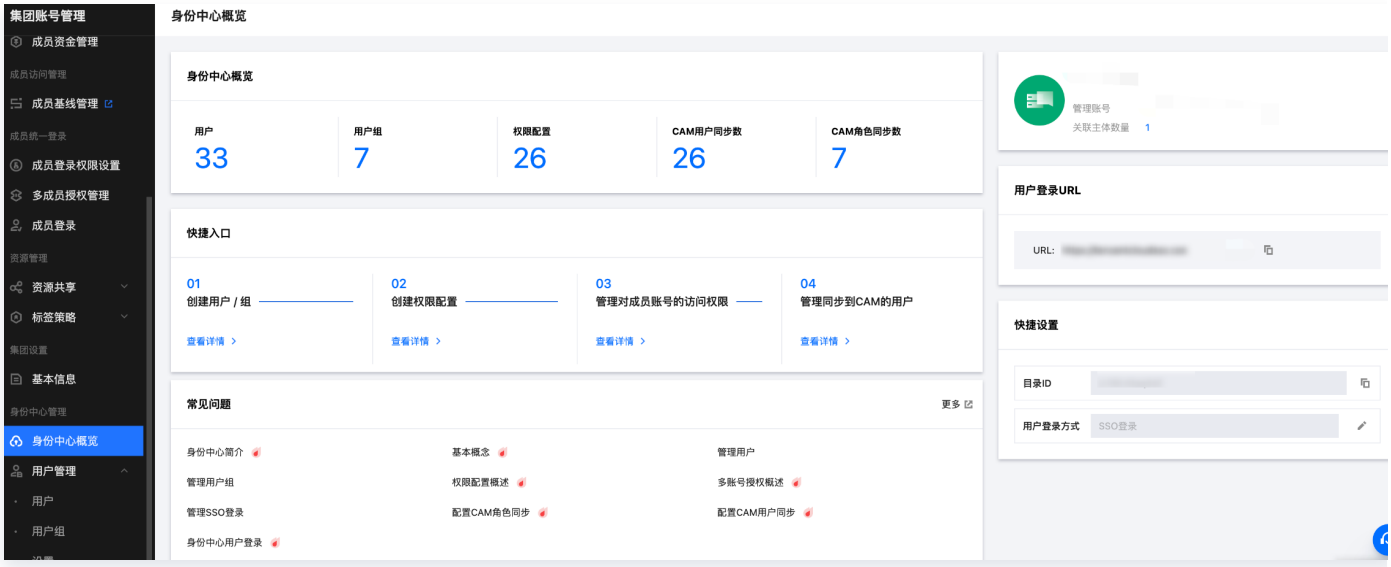
操作场景

当身份中心用户登录用户门户后，可以查看自己有权限访问的账号，并以 CAM 角色或 CAM 用户访问账号的对应资源。

操作步骤

步骤一：获取登录门户访问地址

1. 身份中心管理员进入**集团账号管理** > 身份中心 。
2. 在左侧导航栏，单击**身份中心概览**。
3. 在概览页面的右侧，查看或复制**用户登录 URL**。



步骤二：登录身份中心用户门户

1. 身份中心用户点击访问**用户登录 URL**。
2. 根据已配置的登录方式，登录身份中心用户门户。
    - 用户名密码登录

- 输入身份中心用户名和密码，然后单击**登录**。如需修改密码，请参考 重置用户密码 。
- 默认启用 MFA，用户需要完成 MFA 验证。详情请参见 添加 MFA 设备 。
  - 如果是首次登录用户门户，则需要添加 MFA 设备。
  - 如果 MFA 设备已经绑定，请直接输入从移动设备端获取的验证码，然后单击**验证**。

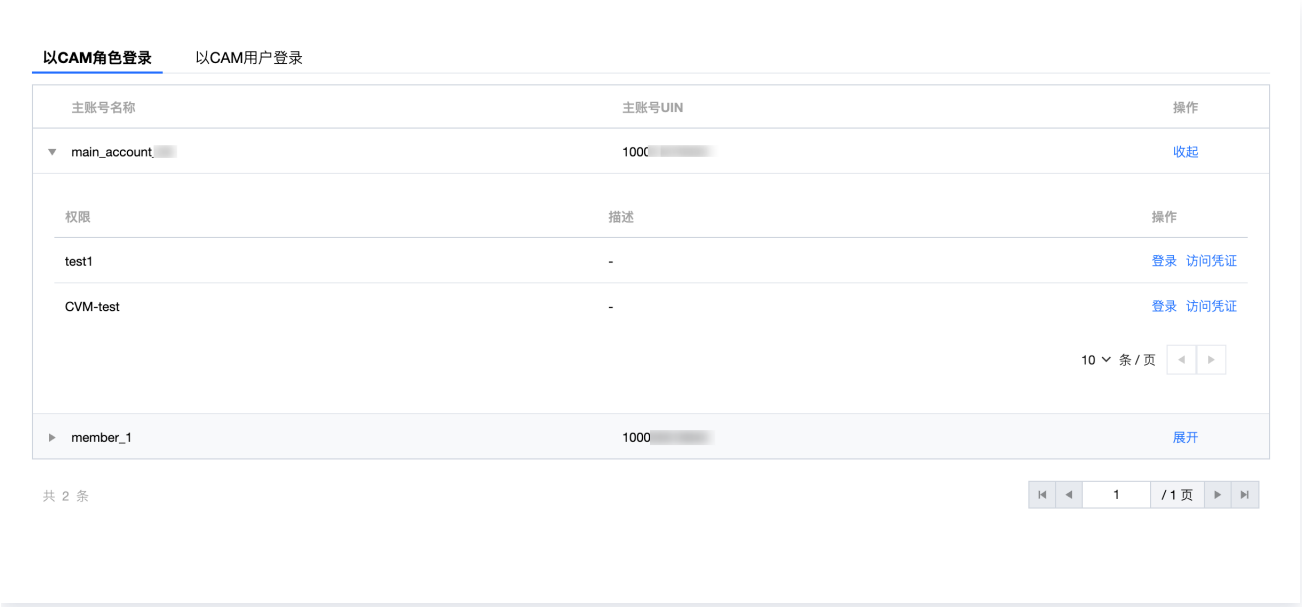
- SSO 登录

- 在 SSO 登录页面，单击**登录**，系统会自动跳转到企业 IdP 的登录页面。
- 使用企业 IdP 的用户名和密码登录。

步骤三：访问账号

以 CAM 角色登录

在身份中心中通过权限配置设置了访问权限，就可以通过 CAM 角色访问账号资源。该方式适用于大部分的云服务。配置方法，请参见 配置 CAM 角色同步 。



1. 在**以 CAM 角色登录**页签，单击目标账号**操作**列的**展开**。

> **说明：**
> - 如果列表为空，表示您没有访问任何账号的权限。
> - 当您有多个账号的访问权限时，您可以在该页面灵活选择想要访问的账号。

2. 单击目标权限**操作**列的**登录**，即可以**角色身份**进入目标账号。

> **说明：**
> 当您有多个账号的访问权限时，您可以在该页面灵活选择想要访问的账号。

以 CAM 用户登录

对于不支持 CAM 角色的云服务，且在身份中心中配置了 CAM 用户同步，就可以通过 CAM 用户访问账号资源。配置方法，请参见 配置 CAM 用户同步 。

在**以 CAM 用户登录**页签，单击目标账号**操作**列的**登录**。

说明：

- 如果列表为空，表示您没有任何账号的访问权限。
- 当您有多个账号的访问权限时，您可以在该页面灵活选择想要访问的账号。

添加或删除 MFA 设备

最近更新时间：2025-07-09 17:26:00

操作背景

MFA （Multi-Factor Authentication） 即多因子认证，是种简单有效的安全认证方法。它可以在用户名和密码之外，再增加一层保护。使用集团账号身份中心的账号密码登录时，将为您强制开启 MFA 认证，用于加强云服务的安全防护。本文为您介绍身份中心用户添加或删除 MFA 设备的具体操作。

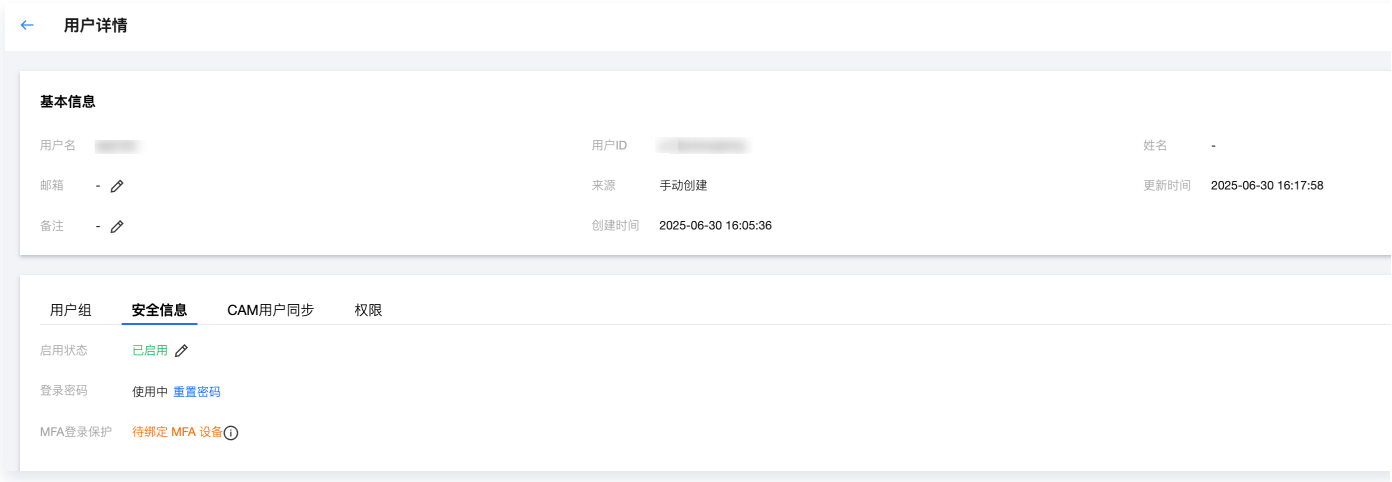
操作步骤

添加 MFA 设备

MFA 登录保护默认启用，当身份中心用户通过**用户名密码登录**用户门户，MFA 登录保护状态为**待绑定 MFA 设备**时，会被要求添加 MFA 设备。

MFA登录保护状态为**待绑定 MFA 设备**有两种情况：

- 用户首次登录
- 管理员已删除 MFA 设备

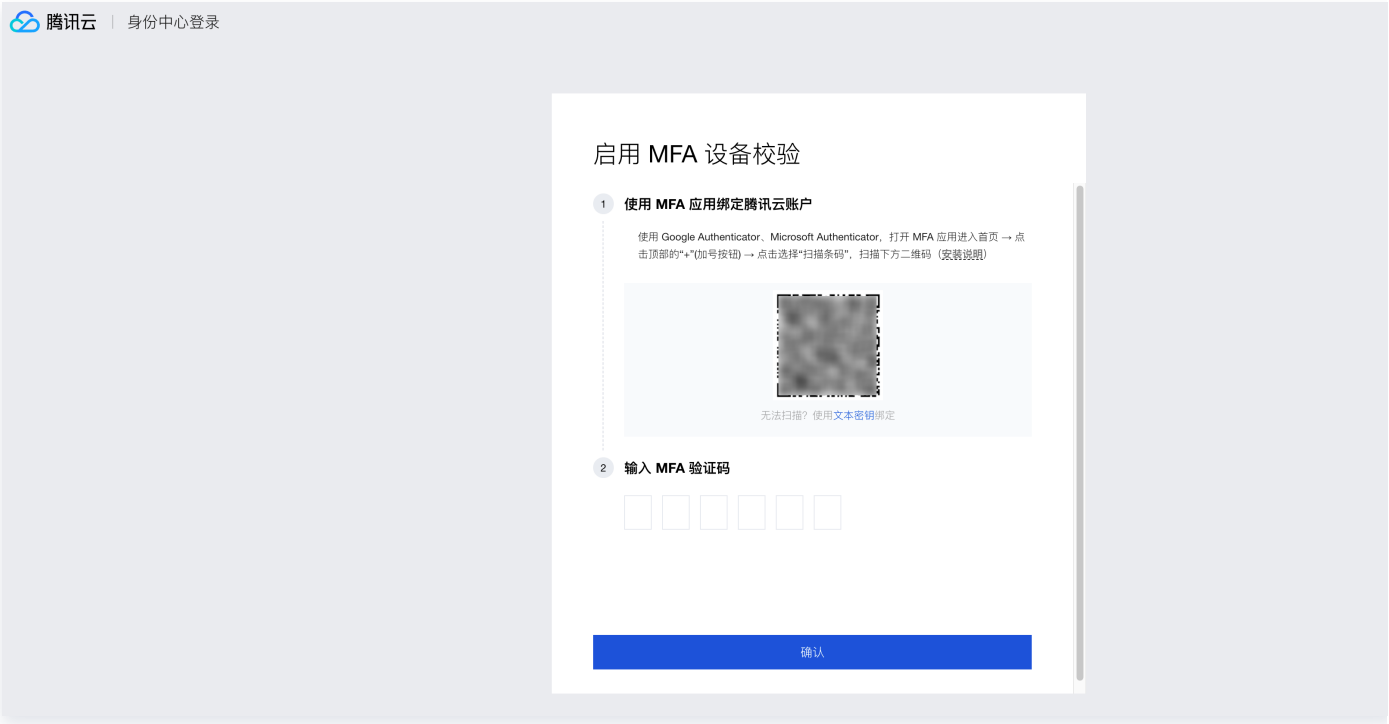


添加 MFA 设备步骤

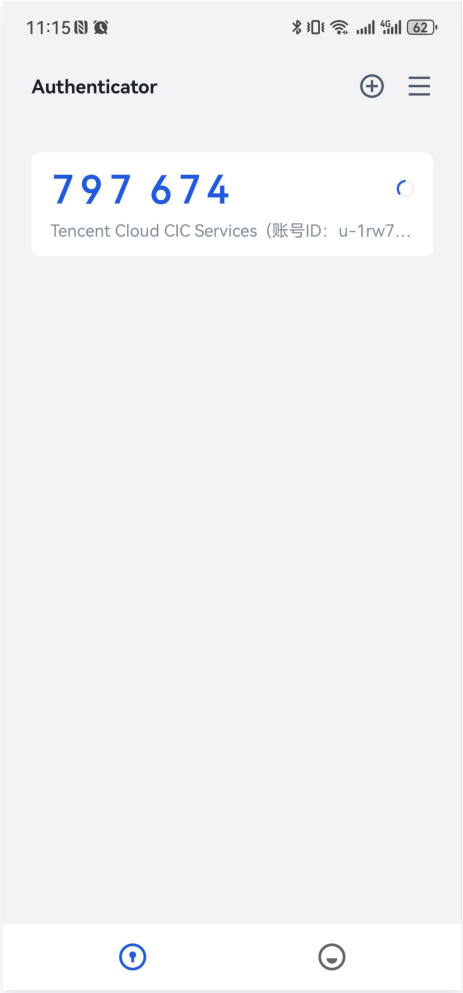
1. 身份中心用户单击访问**用户登录 URL**，输入用户名、密码后，单击**登录**。

2. 进入**启用 MFA 设备校验**页面。本示例以 Android 手机在 **Google Authenticator** 的操作为例。

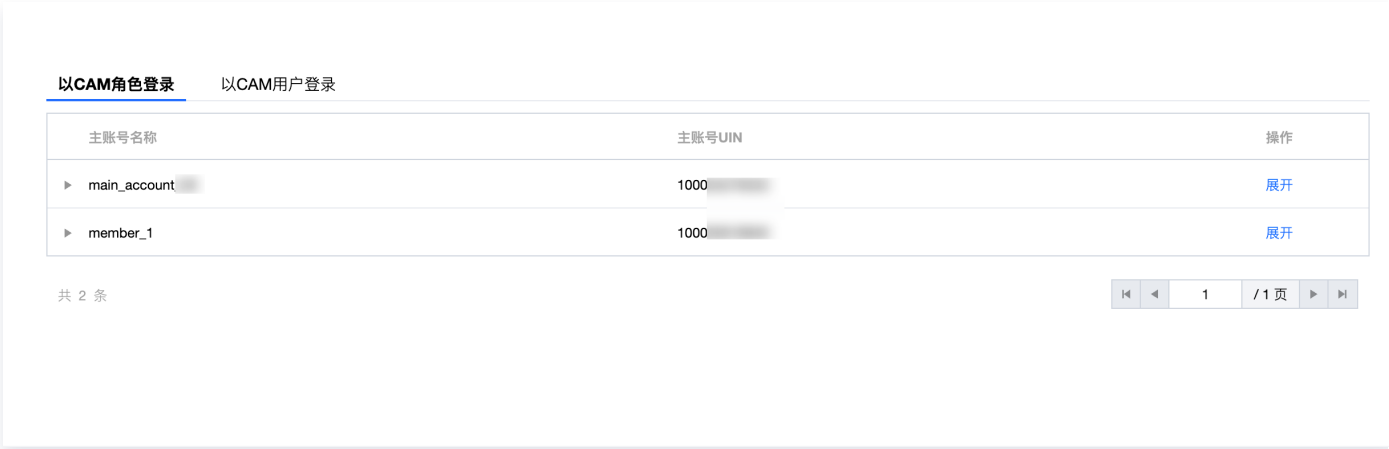
> **说明：**
> 需要用户在移动设备端（例如：手机）下载支持 MFA 设备的应用，目前已支持 **Google Authenticator**、**Microsoft Authenticator**。



3. 在 Android 手机打开 **Microsoft Authenticator** 应用，单击**扫描二维码**，扫描**启用 MFA 设备校验**页面中的二维码添加设备。
4. 添加成功后，手机端增加 **Tencent Cloud CIC Services** 应用，将显示的 6 位数字验证码填写到**启用 MFA 设备校验**页面中**输入MFA 验证码**位置，单击**确认**。

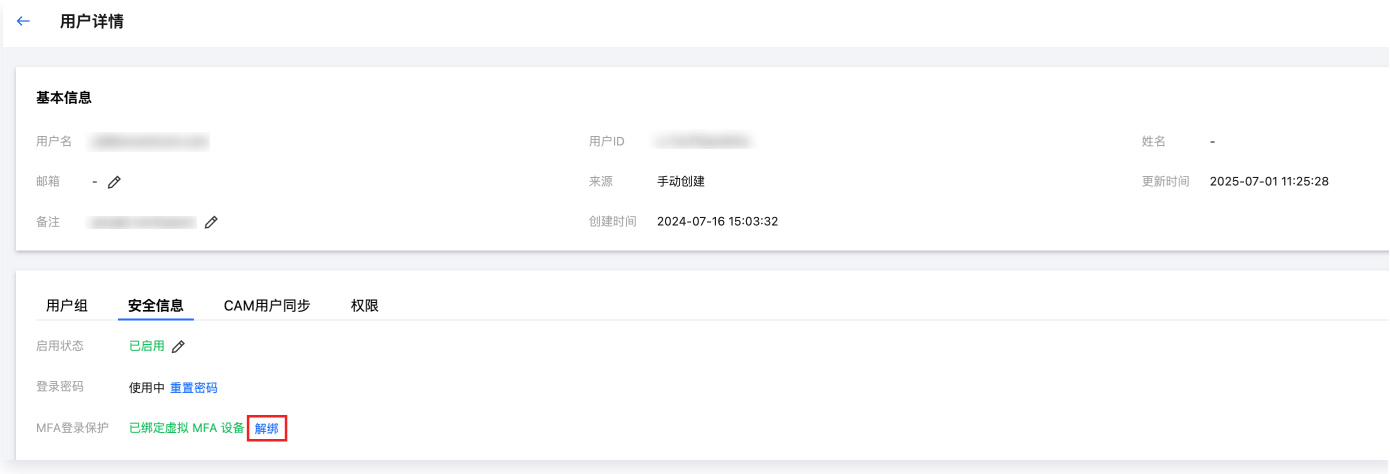


5. 验证成功后，进入身份中心账号选择页面。



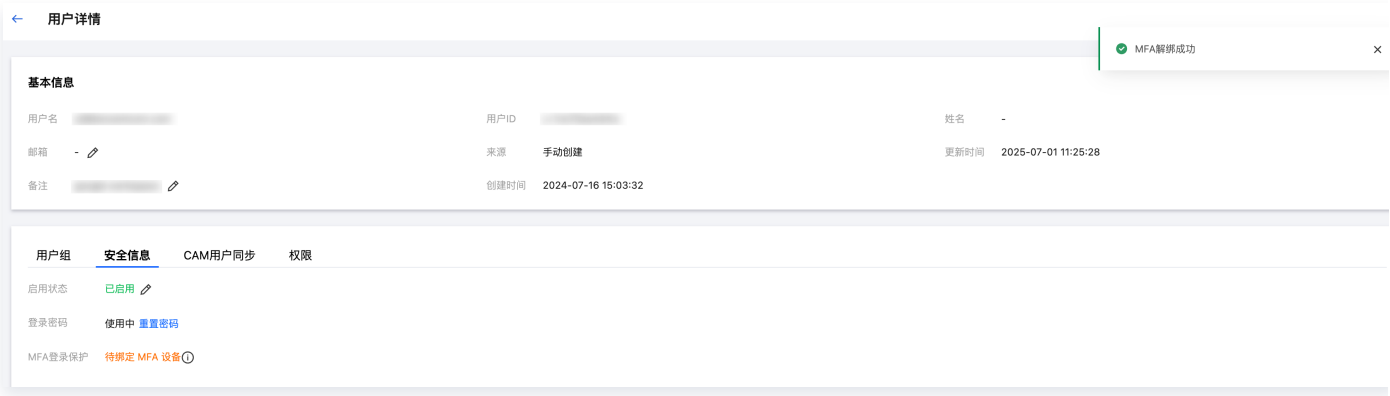
删除 MFA 设备

1. 登录**集团账号管理** > 身份中心 。
2. 在左侧导航栏，选择**用户管理 > 用户**。
3. 在**用户列表**页面，单击目标用户名称，进入**用户详情**页面。
4. 单击**安全信息**页签，在 MFA **登录保护**单击**解绑**。



5. 在删除 MFA 设备对话框，单击**确定解绑**，完成删除。

> **注意：**
> 下次用户登录时需要重新绑定 MFA 设备。



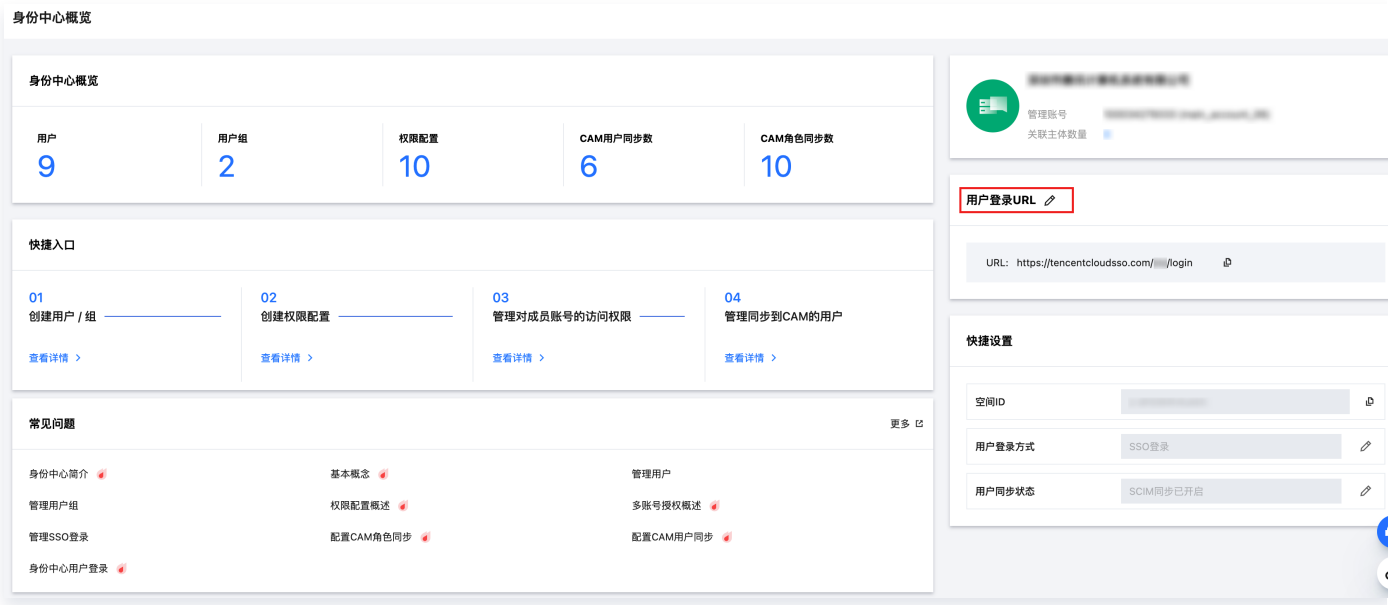
使用 TCCLI 登录

最近更新时间：2025-08-19 17:56:07

身份中心已与腾讯云命令行工具 TCCLI 进行了集成。用户除了使用浏览器登录身份中心用户门户，也可以通过 TCCLI 登录。登录后，选择对应账号和权限，通过 TCCLI 命令行访问云资源。本文为您介绍身份中心用户使用腾讯云命令行工具 TCCLI 登录的操作方法。

前提条件

1. 已安装 TCCLI，详情参见 安装 TCCLI 。
2. 已获取身份中心登录门户访问地址，获取方式：
   2.1 身份中心管理员进入**集团账号管理** > 身份中心 。
   2.2 在左侧导航栏，单击**身份中心概览**。
   2.3 在概览页面的右侧，查看或复制**用户登录 URL**。



3. 已开启 SSO 登录，并配置身份提供商（IdP）信息。具体配置方式，请参见 管理 SSO 登录 。

> **说明：**
> **使用 TCCLI 登录，请在设置中开启 SSO 登录；不支持用户名密码登录。**

操作步骤

1. 在终端中执行以下命令，开始配置登录信息。

```
tccli sso login
```

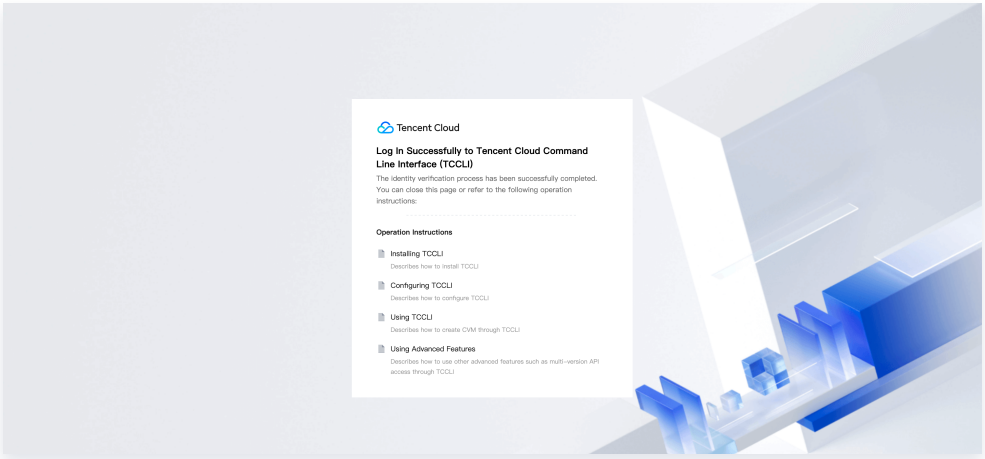
2. 在终端中执行以下命令，输入用户登录 URL，TCCLI 将通过默认浏览器自动打开身份中心 SSO 登录页面。

```
tccli sso configure --url https://tencentcloudssointl.com/*****/login
```

3. 浏览器自动打开 SSO 登录页面，在 SSO 页面点击**登录**：

3.1 系统会自动跳转到企业 IdP 的登录页面。

3.2 使用企业 IdP 的用户名和密码登录成功后，进入登录成功的页面。



4. 浏览器完成登录后返回终端，在 TCCLI 账号列表，选择需要登录的腾讯云账号和权限。
5. 在终端中执行以下测试命令，验证 TCCLI 是否可用。

```
tccli cvm DescribeInstances
```

请求成功示例：

```
[redacted]-MC1 ~ % tccli cvm DescribeInstances
{
    "TotalCount": 0,
    "InstanceSet": [],
    "RequestId": "617b0a3c-5723-4508-b74d-[redacted]"
}
```

6. 如需退出登录，可在终端使用以下命令。

```
tccli sso logout
```

获取临时访问凭证

最近更新时间：2025-07-09 17:16:03

用户登录身份中心用户门户后，可以以 CAM 角色方式访问账号，也可以在页面上一键获取临时访问凭证（STS Token）。本文为您介绍云身份中心用户如何获取 STS Token。

使用说明

Token 权限

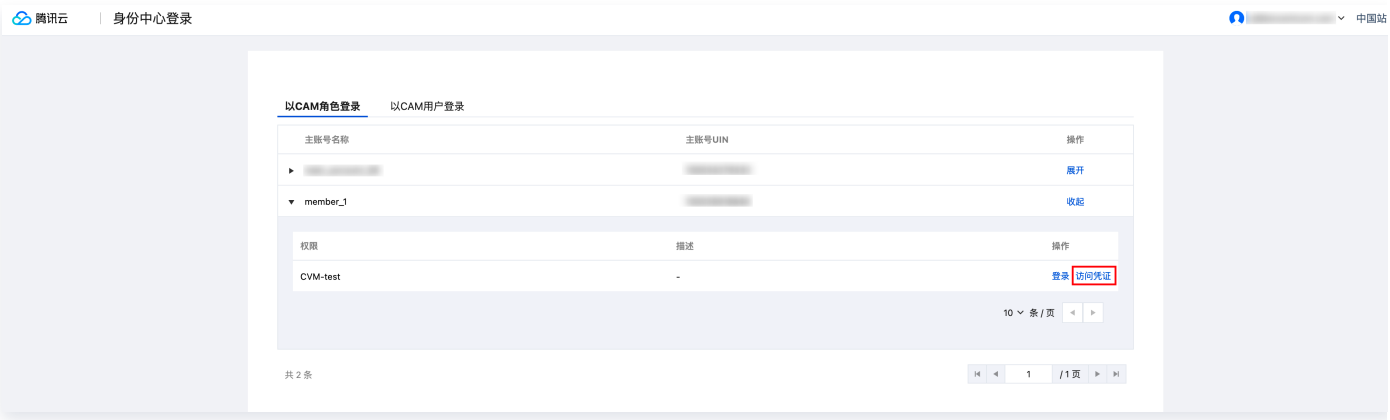
当您给身份中心用户或用户组授予账号的权限配置后，权限配置将在成员账号内部署一个 CAM 角色。该角色的 STS Token 权限范围在身份中心权限配置中定义。

Token 有效期

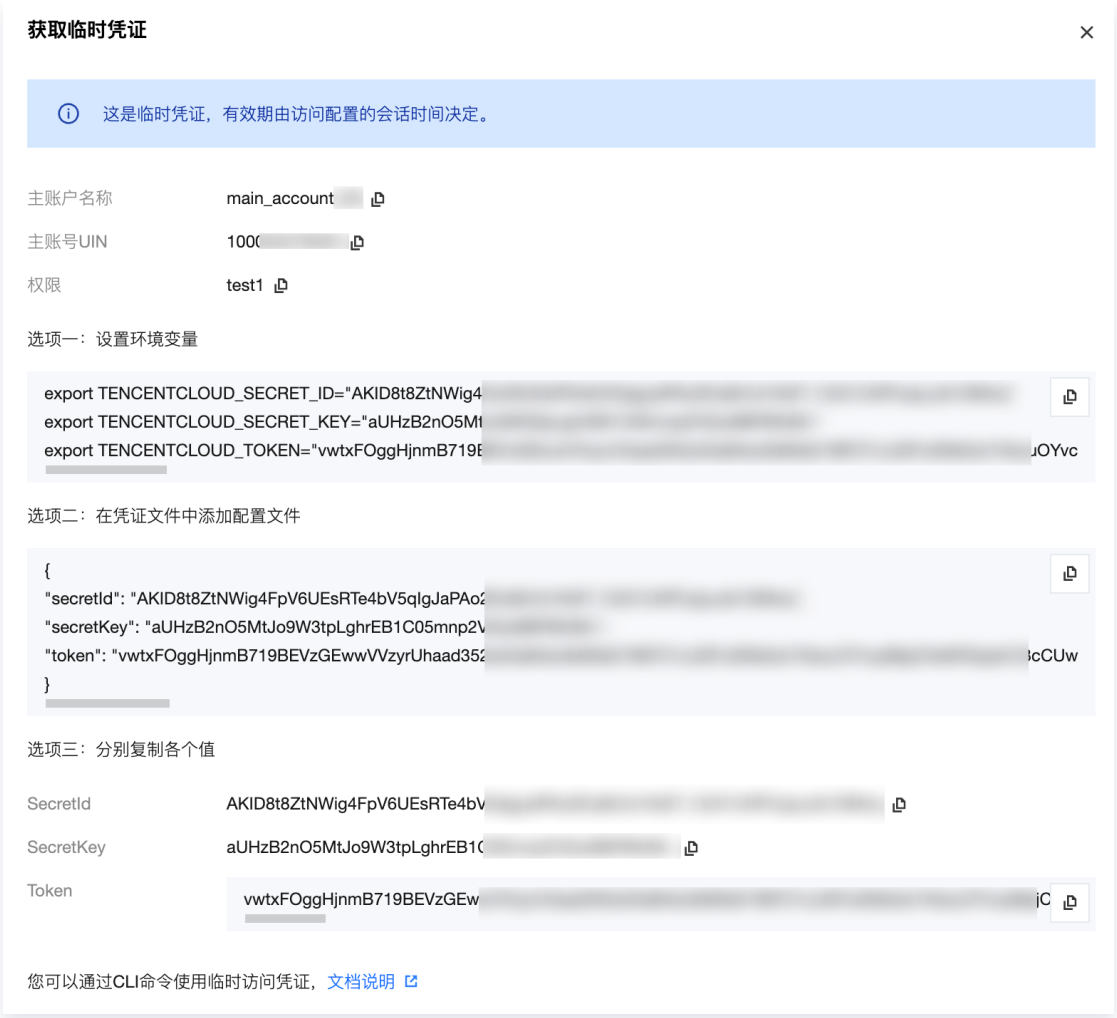
以 CAM 角色访问方式获取的 STS Token 是短期的临时访问凭证，有效期取决于权限配置中定义的会话持续时间，到期后将自动失效。

获取临时秘钥

1. 登录身份中心用户门户。具体操作，请参见 身份中心用户登录 。
   1.1 从管理员处获取用户登录 URL。
   1.2 通过 SSO 登录身份中心用户门户。
2. 在**以 CAM 角色登录**页签，单击目标账号操作列的**展开**。
3. 单击目标操作列的**访问凭证**。



4. 查看和复制临时访问凭证。



获取临时凭证

这是临时凭证，有效期由访问配置的会话时间决定。

主账户名称 main_account

主账号UIN 100

权限 test1

选项一：设置环境变量

```
export TENCENTCLOUD_SECRET_ID="AKID8t8ZtNWig4
export TENCENTCLOUD_SECRET_KEY="aUHzB2nO5Mt
export TENCENTCLOUD_TOKEN="vwtxFOggHjnmB719E
```

选项二：在凭证文件中添加配置文件

```
{
"secretId": "AKID8t8ZtNWig4FpV6UEsRTe4bV5qlgJaPAo2
"secretKey": "aUHzB2nO5MtJo9W3tpLghrEB1C05mnp2V
"token": "vwtxFOggHjnmB719BEVzGEwwVVzyrUhaad352
}
```

选项三：分别复制各个值

SecretId AKID8t8ZtNWig4FpV6UEsRTe4bV

SecretKey aUHzB2nO5MtJo9W3tpLghrEB1C

Token vwtxFOggHjnmB719BEVzGEw

您可以通过CLI命令使用临时访问凭证，文档说明