

## 目录

目录	1
简介	2
创建IAM子用户	2
前提条件	2
操作步骤	2
后续步骤	2
删除IAM子用户	2
操作步骤	2
修改IAM子用户基本信息	2
操作步骤	2
修改控制台登陆设置	3
操作步骤	3
修改IAM子用户登录密码	3
操作步骤	3
为IAM子用户开启MFA认证	3
操作步骤	3
后续步骤	4
为IAM子用户创建访问密钥	4
背景说明	4
操作步骤	4
为IAM子用户禁用访问密钥	4
操作步骤	4
为IAM子用户授权	4
方式一：在用户页面为IAM子用户授权	4
方式二：在授权页面为IAM子用户授权	4
方式三：在策略页面为IAM子用户授权	4
查看IAM子用户权限	5
查看IAM子用户的个人权限	5
查看IAM子用户继承用户组的权限	5
为IAM子用户移除权限	5
方式一：在用户页面为IAM子用户移除权限	5
方式二：在授权页面为IAM子用户移除权限	5
方式三：在策略页面为IAM子用户移除权限	5

## 简介

IAM子用户是IAM的一种实体身份类型，有确定的身份ID和身份凭证，它通常与某个确定的人或应用程序一一对应。

- 一个云账号下可以创建多个IAM子用户，对应企业内的员工、系统或应用程序。
- IAM子用户不拥有资源，不能独立计量计费，由所属云账号统一控制和付费。
- IAM子用户归属于云账号，只能在所属云账号的空间下可见，而不是独立的云账号。
- IAM子用户必须在获得云账号的授权后才能登录控制台或使用API操作云账号下的资源。

## 创建IAM子用户

本文介绍如何快速创建IAM子用户。IAM子用户是一种身份，对应操作实体可以是具体的运维人员，也可以是某个应用程序。

新建的IAM子用户默认无任何权限，需要为其授权后才可以访问相应资源。

### 前提条件

已登录主账号（root用户）或拥有（IAMFullAccess）的子用户，才可以操作IAM子用户添加。

### 操作步骤

1. 登录[访问控制控制台](#)。
2. 选择**人员管理** > **子用户**，进入到子用户管理页面。
3. 单击**新建用户**按钮，进入**新建用户**页面。
4. 在**新建用户**页面用户登录信息区域按提示填写信息。

**登录账号**：必填，为子用户的用户名，一旦创建无法修改。**显示名称**：必填，方便按照自身业务定义使用者对应名称。**邮箱**：选填，用于接收消息。**手机号**：选填，用于接收消息。**同时接收消息**：开启后，邮箱与手机号为必填内容。

5. 在**访问方式**区域，选择访问方式。为了保障账号安全，建议只选择一种登录方式。

**控制台访问**：设置控制台登录密码、重置密码策略、多因素认证策略、操作保护策略，是否允许查看所有项目。**编程访问**：自动为子用户用户生成访问密钥（AccessKey），支持通过API或其他开发工具访问金山云。

6. 单击**确定**，完成子用户创建。

### 后续步骤

- 可以为IAM子用户添加权限策略，使IAM子用户具有资源的访问能力。
- 可以将IAM子用户添加到用户组，对IAM子用户进行分类并授权。
- IAM子用户创建成功并授权策略后，可以使用IAM子用户登录控制台。

## 删除IAM子用户

当不再需要某个IAM子用户时，可以删除该子用户。删除后，子用户将无法登录金山云、无法接收消息通知，且删除子用户AccessKey，解除MFA绑定，撤销权限。

### 操作步骤

1. 登录[访问控制控制台](#)。
2. 选择**人员管理** > **子用户**，进入到子用户管理页面。
3. 在子用户列表管理页面，找到需要删除的子用户。
4. 单击操作列的**更多** > **删除**。
5. 在弹出的确认是否删除用户窗口，单击**确定**，完成删除子用户操作。

## 修改IAM子用户基本信息

IAM子用户的用户名不可修改，仅支持修改显示名称、邮箱、手机号码。本文为您介绍如何修改IAM子用户的基本信息。

### 操作步骤

1. 登录[访问控制控制台](#)。

2. 选择**人员管理** > **子用户**，进入到子用户管理页面。
3. 在子用户列表管理页面，单击目标用户的**用户名或详情**，进入到用户详情页。
4. 在用户详情的**用户信息**区域，单击**编辑**。
5. 在**编辑用户信息**的弹窗里，编辑要修改的信息。
6. 单击**确定**，完成编辑。

## 修改控制台登陆设置

本文为您介绍如何修改IAM子用户登录设置信息。

### 操作步骤

1. 登录[访问控制控制台](#)。
2. 选择**人员管理** > **子用户**，进入到子用户管理页面。
3. 在子用户列表管理页面，单击目标用户的**用户名或详情**，进入到用户详情页。
4. 在用户详情的**安全管理**页签区域，单击**修改设置**。
5. 在**修改设置**的面板里，设置控制台登陆参数。
  - 控制台密码登录：关闭后，则不允许子用户登录控制台，仅可通过AccessKey以API或其他开发工具访问。
  - 子用户登录密码：支持生产默认密码或者自定义登录密码。请按需设置。
  - 要求重置密码：勾选后，下次子用户登录时需重置密码。
  - 登录保护：如果要求开启MFA认证，用户登录时需要通过二次身份校验。
  - 操作保护：如果要求开启MFA认证，用户进行敏感操作时需要通过二次身份校验。
  - 子用户查看所有项目：开启后，子用户登录控制台可以查看所有项目组，包括未来新建的项目组。
  - 登陆或操作保护任一项要求MFA认证，子用户在下次登录时需绑定MFA设备。
6. 单击**确定**，完成控制台登陆设置。

## 修改IAM子用户登录密码

本文为您介绍如何为IAM子用户修改登录账号密码。

### 操作步骤

1. 登录[访问控制控制台](#)。
2. 选择**人员管理** > **子用户**，进入到子用户管理页面。
3. 在子用户列表管理页面，单击目标用户的**用户名或详情**，进入到用户详情页。
4. 在用户详情的**安全管理**页签区域，单击**修改设置**。
5. 在**修改设置**的面板里，找到子用户登录密码区域。
  - 选择自动生成默认密码，然后单击确定，会自动生成登录密码，请记录并妥善保管新密码。
  - 选择自定义登录密码，然后输入新的密码。输入的新密码必须符合密码强度要求。
6. 单击**确定**，完成密码修改。

## 为IAM子用户开启MFA认证

通过为子用户进行登录保护和操作保护设置，可以为其启用多因素MFA认证。启用后可以为您的IAM的子账号提供更高的安全保护。

### 操作步骤

1. 登录[访问控制控制台](#)。
2. 选择**人员管理** > **子用户**，进入到子用户管理页面。
3. 在子用户列表管理页面，单击目标用户的**用户名或操作列详情**，进入到用户详情页。
4. 在用户详情的**安全管理**页签区域，单击**修改设置**。
5. 在\***修改设置**的面板里，设置登录保护和操作保护参数。
  - 登录保护：如果要求开启MFA认证，用户登录时需要通过二次身份校验。
  - 操作保护：如果要求开启MFA认证，用户进行敏感操作时需要通过二次身份校验。
6. 单击**确定**，完成设置。

## 后续步骤

登陆或操作保护任一项要求MFA认证，子用户在下次登录时需绑定MFA设备。

# 为IAM子用户创建访问密钥

如果为IAM子用户创建了访问密钥（AccessKey），IAM子用户可以通过API或其他开发工具访问金山云资源。

## 背景说明

为保证账号安全，强烈建议您给IAM子用户创建访问密钥，不要给金山云账号（主账号）创建访问密钥。

## 操作步骤

1. 登录[访问控制控制台](#)。
2. 选择**人员管理** > **子用户**，进入到子用户管理页面。
3. 在子用户列表管理页面，单击目标用户的**用户名**，进入到用户详情页。
4. 在用户详情页的**安全管理**页签，单击**创建秘钥**。
5. 在**创建AccessKey**弹窗中，查看AccessKeyID和SecretAccessKey。
6. 您可以点击下载凭证或复制AccessKey信息保存子用户的密钥。

SecretAccessKey只在创建时显示，不支持查询，请妥善保管。若AccessKey泄露或丢失，则需要创建新的AccessKey，最多可以创建2个AccessKey。

# 为IAM子用户禁用访问密钥

如果IAM子用户不需要访问密钥（AccessKey），支持禁用其访问密钥。

## 操作步骤

1. 登录[访问控制控制台](#)。
2. 选择**人员管理** > **子用户**，进入到子用户管理页面。
3. 在子用户列表管理页面，单击目标用户的**用户名**，进入到用户详情页。
4. 在用户详情页的**安全管理**页签，在目标密钥**操作**列单击**禁用**按钮。
5. 在确认弹窗中单击**确定**按钮，完成禁用。

对于已禁用的访问密钥，可以单击操作列的**启用**，重新启用该访问密钥。

# 为IAM子用户授权

为IAM子用户授权后，IAM子用户将可以访问相应的金山云资源。

## 方式一：在用户页面为IAM子用户授权

1. 登录[访问控制控制台](#)。
2. 选择**人员管理** > **子用户**，进入到子用户管理页面。
3. 在子用户列表，找到目标IAM子用户，单击**操作**列的**添加权限**按钮。
4. 在添加权限页面，为IAM子用户选择要添加权限。
5. 单击**确定**，完成权限添加。

## 方式二：在授权页面为IAM子用户授权

1. 登录[访问控制控制台](#)。
2. 选择**权限管理** > **授权**。
3. 在**授权列表**页面，单击**新建授权**按钮。
4. 在**新建授权**面板，选择要授权的IAM子用户和授权的策略。
5. 单击**确定**，完成权限添加。

## 方式三：在策略页面为IAM子用户授权

1. 登录[访问控制控制台](#)。
2. 选择**权限管理** > **授策**。
3. 在**策略列表**页面，找到要授权的目标策略，单击**操作**列的**关联对象**按钮。
4. 在**关联对象**面板，选择要授权的IAM子用户。

5. 单击**确定**，完成权限添加。

## 查看IAM子用户权限

本文为您介绍如何查看IAM子用户的权限，包括查看IAM子用户的个人权限和查看IAM子用户继承用户组的权限。

### 查看IAM子用户的个人权限

1. 登录[访问控制控制台](#)。
2. 选择**人员管理** > **子用户**，进入到子用户管理页面。
3. 在子用户列表管理页面，单击目标用户的**用户名**或**详情**，进入到用户详情页。
4. 单击用户详情的**关联策略**页签。
5. 在**个人权限**页签，查看IAM子用户的个人权限。

### 查看IAM子用户继承用户组的权限

1. 登录[访问控制控制台](#)。
2. 选择**人员管理** > **子用户**，进入到子用户管理页面。
3. 在子用户列表管理页面，单击目标用户的**用户名**，进入到用户详情页。
4. 单击用户详情的**关联策略**页签。
5. 在**继承用户组的权限**页签，查看IAM子用户的继承用户组的权限。

## 为IAM子用户移除权限

当IAM子用户不再需要某些权限或离开组织时，可以将这些权限移除。

### 方式一：在用户页面为IAM子用户移除权限

1. 登录[访问控制控制台](#)。
2. 选择**人员管理** > **子用户**，进入到子用户管理页面。
3. 在子用户列表管理页面，单击目标用户的**用户名**或**详情**，进入到用户详情页。
4. 单击用户详情的**关联策略**页签。
5. 在**个人权限**页签，单击目标权限策略操作列的**解除**操作按钮。
6. 在确认弹窗中，单击**确定解除**。

### 方式二：在授权页面为IAM子用户移除权限

1. 登录[访问控制控制台](#)。
2. 选择**权限管理** > **授权**。
3. 在**授权列表**页面，单击目标授权操作列的**解除**操作按钮。
4. 在确认弹窗中，单击**确定解除**。

### 方式三：在策略页面为IAM子用户移除权限

1. 登录[访问控制控制台](#)。
2. 选择**权限管理** > **授策**。
3. 在策略列表页面，找到要授权的目标策略，单击**策略名称**。
4. 在**策略详情**，单击**关联对象**页签。
5. 在**关联对象**列表中，单击目标对象操作列的**移出**操作按钮。
6. 在确认弹窗中，单击**确定移出**。