目录

安全设置概览

本文介绍了IAM涉及的一些安全设置，以下安全设置适用于所有的子用户。

登录密码

- 登录密码是登录金山云的身份凭证，用于证明用户真实身份的凭证。
- 请妥善保管您的登录密码并定期更换，通过对密码的安全设置来提升账号的安全性。

访问密钥

- 访问密钥指的是访问身份验证中用到的AccessKey ID和AccessKey Secret。您可以使用访问密钥（或金山云服务SDK）创建一个API请求，IAM通过使用AccessKey ID和AccessKey Secret对称加密的方法来验证某个请求的发送者身份，身份验证成功后将可以操作相应资源。
- AccessKey ID和AccessKey Secret一起使用，AccessKey ID用于标识用户，AccessKey Secret用于加密签名字符串和IAM用来验证签名字符串的密钥。

多因素认证

多因素认证一种简单有效的安全实践，在用户名和密码之外再增加一层安全保护，用于登录控制台或进行敏感操作时的二次身份验证，以此保护您的账号更安全。以下将为您介绍子用户支持的多因素认证方式、使用说明。

多因素认证方式

认证方式	描述	使用场景
虚拟MFA	如果用户启用了虚拟MFA设备（金山云小程序），在用户登录时，金山云将要求用户必须输入小程序上生成的6位验证码，从而避免因密码被盗而引起的非法登录。	登录控制台、敏感操作
安全手机	为子用户绑定安全手机号码，通过安全手机号码提供的验证码进行二次身份验证。	登录控制台、敏感操作
安全邮箱	为子用户绑定安全邮箱地址，通过安全邮箱提供的验证码进行二次身份验证。	敏感操作

使用说明

启用多因素认证并绑定多因素认证设备后，子用户再次登录金山云或进行敏感操作时，系统将要求输入两层安全要素：

- 第一层安全要素：输入用户名和密码。
- 第二层安全要素：输入虚拟MFA设备生成的验证码、输入安全手机验证码或输入安全邮箱验证码。

密码安全设置

为了提高账号安全性，您可以为子用户密码设置安全强度及安全策略。

密码强度设置

操作步骤

1. 登录访问控制控制台。
2. 选择**设置** > **安全设置**。
3. 在**安全设置**页面的密码强度设置区域， 单击**修改**按钮。
4. 在**密码强度设置**弹层中配置相关参数。

   密码长度：密码长度范围为8~32位，建议设置至少8位以上密码长度。 密码有效期：建议设置有效期。可填写90-365天，超过密码有效期，登录后需修改密码。 历史密码检查策略：建议设置。表示禁止使用前N次密码，取值范围为1~12。 密码中必须包含元素：请根据需要勾选大写字母、小写字母、数字和符号。建议至少勾选2项。 密码过期后是否可登录：不可登录表示密码过期后，不能登录控制台。需要通过金山云主账号或具有管理员权限的子用户重置该子用户的密码后，才能正常登录。 1小时内密码错误尝试次数：设置密码重试的次数（取值1-10），连续输入错误密码达到设定次数后，账号将被锁定一小时。

5. 单击确定，设置成功后，此密码规则适用于所有子用户。

密码安全策略设置

操作步骤

1. 登录访问控制控制台。
2. 选择**设置** > **安全设置**。
3. 在**安全设置**页面的密码安全设置区域， 单击**修改**按钮。 
4. 在**密码安全设置**弹层中配置相关参数。 （1）登录session过期时间：子用户登录有效期，单位为分钟，可填写15-1440分钟。 （2）登录掩码设置：最多设置100个地址

   网络掩码决定哪些IP地址会受到登录控制台的影响但使用AccessKey发起的API访问并不受影响。 如果指定掩码，子用户必须只能从指定的IP地址进行登录。 如果不指定任何掩码，登录控制台功能将适用于整个网络。 当需要配置多个掩码时，请使用英文分号来分隔掩码例如：10.111.23.0/24;10.111.57.52

5. 单击确定，设置成功后，此密码策略适用于所有子用户。

访问密钥管理

背景说明

为保证账号安全，强烈建议您给子用户创建访问密钥，不要给主账号创建访问密钥。

- 使用主账号密钥登录控制台，即拥有主账号名下资源的所有访问操作权限，密钥泄露即会对账号造成较大风险。
- 通过子用户密钥登录进去控制台，只拥有主用户授予给子用户的部分权限，其操作权限及操作事件是受限制和监控的，较为安全。

什么是访问密钥（AccessKey）

如果为子用户创建了访问密钥（AccessKey），子用户可以通过API或其他开发工具访问金山云资源。 在调用金山云API时您需要使用AccessKey完成身份验证。AccessKey包括AccessKey ID和AccessKey Secret，需要一起使用。具体如下：

- AccessKey ID：用于标识用户。
- AccessKey Secret：用于验证用户的密钥。AccessKey Secret必须保密。

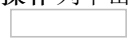
为子用户创建访问密钥

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. 在用户详情的**安全管理**页签，单击**创建密钥**。 
5. 完成敏感操作验证。 
6. 在**创建AccessKey**弹窗中，查看AccessKeyID和SecretAccessKey。
7. 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。

如果子用户不需要访问密钥（AccessKey），支持禁用其访问密钥。

为子用户禁用访问密钥

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。 
6. 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。也可点击删除，删除该密钥。 

子用户多因素认证设置

多因素认证MFA（Multi-factor Authentication）是一种简单有效的安全实践，可以在用户名和密码之外再增加一层安全保护。

使用说明

为子用户企业多因素认证后，再次登录金山云时，系统将要求输入两层安全要素：

- 第一层安全要素：输入用户名和密码。
- 第二层安全要素：输入虚拟MFA设备生成的验证码、输入安全手机验证码或输入安全邮箱验证码。

为子用户开启MFA认证

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，设置登录保护和操作保护参数。

   （1）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。 （2）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。

子用户绑定MFA虚拟设备

为子用户开启MFA认证户后，子用户在下一次登陆控制台时进入绑定MFA虚拟设备流程，未完成绑定流程不可访问控制台其他功能。

1.打开MFA设备：推荐微信直接扫码，进入金山云小助手小程序。

您也可以使用APP MFA设备，包括“金山云令”、“Google Authenticator”。

2.在金山云小助手程序中，单击**立即添加MFA**。扫描界面中绑定流程中第二步的二维码。

扫描成功后，微信小程序/APP上会每隔30秒刷新一组验证码。

3.输入绑定的MFA的连续两组安全码。 4.单击确认，完成绑定。

为子用户关闭MFA设备认证

关闭登录及操作保护后，绑定的虚拟MFA设备并不会解绑。

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，设置登录保护和操作保护参数。 （1）登录保护：设置为关闭MFA认证。（2）操作保护：设置为关闭MFA认证。

为子用户解绑MFA设备

解绑是只会解除设备，如果子用户开启了MFA认证，解绑成功后子用户下一次登陆控制会进入MFA虚拟设备绑定流程。

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. 在用户详情的在**多因素设备认证**区域，单击**解绑**按钮。
5. 在确认解绑弹窗中，单击确定。

MFA令牌删除

- 删除“金山云令”、“Google Authenticator”上的MFA令牌前，请您确保其对应的账号验证，MFA功能处于禁用状态。否则，子用户账号将无法在下一次登录时，顺利通过验证。
- 微信小程序上不支持删除MFA令牌，解绑设备自动删除MFA令牌。