目录

密码强度设置

为了保护账号安全，您可以编辑密码规则，包括密码长度、密码有效期和历史密码检查策略、密码元素等。

> 该设置仅对子用户有效。 1、主账号登录session过期时间为12小时； 2、主账号密码连续输入错误3次，则会锁定账号30分钟，可通过修改密码或等待30分解除。

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。需要通过金山云账号或具有管理员权限的IAM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1-32），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**。

执行结果

设置成功后，此密码规则适用于所有IAM子用户。

安全策略设置

为了保护账号安全，您可以为IAM子用户设置安全策略等。

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**页面的密码强度密码区域， 单击**修改**按钮。
4. 在**密码安全设置**弹层中配置相关参数。 （1）保存MFA登录状态7天：表示是否允许IAM子用户登录时保存多因素认证设备登录状态，有效期为7天，默认为不允许。 （2）登录session过期时间：表示IAM子用户登录有效期，单位为分钟，可填写15-1440分钟。 （3）登录掩码设置：登录掩码决定哪些IP地址会受到登录控制台的影响。默认为空字符串，不限制登录IP。如果设置了登录掩码，使用密码登录或单点登录（SSO）时会受到影响，只能只能从指定的IP地址进行登录，但使用访问密钥发起的API访问不受影响。

5.单击**确定**。

子用户MFA认证

多因素认证MFA（Multi-factor Authentication）是一种简单有效的最佳安全实践，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。

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。

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。