ALIBABA CLOUD

Alibaba Cloud

访问控制

安全设置

文档版本：20200910

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
`Courier字体`	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.安全设置概览

本文介绍了访问控制涉及的一些安全设置基本概念，这些安全设置可以更有效的保护账号安全。

登录密码（Password）

登录密码是登录阿里云的身份凭证，用于证明用户真实身份的凭证。

> 说明 请妥善保管您的登录密码并定期更换。

关于如何设置登录密码，请参见修改云账号登录密码和修改RAM用户登录密码。

默认域名（Default domain name）

阿里云为每个云账号分配了一个默认域名，格式为：`<AccountAlias>.onaliyun.com`。默认域名可作为RAM用户登录或单点登录（SSO）等场景下该云账号的唯一标识符。

关于如何设置默认域名，请参见管理默认域名。

域别名（Domain alias）

如果您持有公网上可以解析的域名，那么您可以使用该域名替代您的默认域名，该域名称为域别名。域别名就是指默认域名的别名。

> 说明 域别名必须经过域名归属验证后才能使用。验证通过后，您可以使用域别名替代默认域名，用于所有需要使用默认域名的场景。

关于如何设置域别名，请参见创建并验证域别名。

访问密钥（AccessKey）

访问密钥指的是访问身份验证中用到的AccessKeyID和AccessKeySecret。您可以使用访问密钥（或阿里云服务SDK）创建一个API请求，RAM通过使用AccessKeyID和AccessKeySecret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。

AccessKeyID和AccessKeySecret一起使用，AccessKeyID用于标识用户，AccessKeySecret用于加密签名字符串和RAM用来验证签名字符串的密钥。

> 说明 AccessKeySecret只在创建时显示，不支持查询，请妥善保管。

关于如何创建访问密钥，请参见为RAM用户创建访问密钥。

多因素认证（MFA）

多因素认证是一种简单有效的最佳安全实践，在用户名和密码之外再增加一层安全保护。这些多重要素结合起来将为您的账号提供更高的安全保护。启用多因素认证后，再次登录阿里云时，系统将要求输入两层安全要素：

1. 第一安全要素：用户名和密码
2. 第二安全要素：多因素认证设备生成的验证码

关于如何设置多因素认证，请参见为云账号设置多因素认证和为RAM用户设置多因素认证。

2.密码

2.1. 修改云账号登录密码

为了提高账号的安全性，您可以定期修改密码，设置一个包含字母、符号或数字至少两项元素且长度超过6位的密码。

操作步骤

1. 云账号登录RAM控制台。
2. 将鼠标悬停在右上角头像的位置，单击**安全设置**。
3. 在**安全设置**页面下的**登录密码**区域，单击**修改**。
4. 在**验证身份**页面，根据页面提示选择合适的方式进行身份验证。
5. 验证成功后，输入**新的登录密码**和**确认新的登录密码**。
6. 单击**确定**。

2.2. 设置RAM用户密码强度

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等。

操作步骤

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏的**人员管理**菜单下，单击**设置**。
3. 在**安全设置**页签下，单击**编辑密码规则**，根据配置面板，配置相关参数。
   - **密码长度**：密码长度范围为8~32位。

     > **说明** 为了保护账号安全，建议至少设置8位以上密码长度。

   - **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。

     > **说明** 此设置表示登录密码必须包含勾选项。为了提高账号安全强度，上述元素中，建议至少勾选2项以上。

   - **最少包含的不同字符数**：取值范围为0~8，默认为0，表示不限制密码中的不同字符数量。
   - **密码中是否允许包含用户名**：根据需要选择允许或不允许。
     - 允许：密码中可以包含用户名。
     - 不允许：密码中不能包含用户名。
   - **密码有效期**：单位为天，取值范围为0~1095天，默认为0，表示永不过期。

     > **说明** 重置密码将重置密码过期时间。

   - **密码过期后**：表示密码过期后是否仍可以登录，根据需要勾选不可登录或不限制登录。
     - 不可登录：表示密码过期后必须由主账号重置密码，RAM用户才能正常登录。
     - 不限制登录：表示RAM用户可以在密码过期后自行更改密码，并继续以RAM用户身份登录。

- **历史密码检查策略**：表示禁止使用前*N*次密码，取值范围为0~24。默认取值为0，表示不启用历史密码检查策略。
- **密码重试约束**：设置密码重试的次数，连续输入错误密码达到设定次数后，账号将被锁定一小时。取值范围为0~32。默认取值为0，表示不启用密码重试约束。

> **说明** 重置密码可清除尝试登录次数。

4. 单击**确定**。

执行结果

设置成功后，此密码规则适用于所有RAM用户。

相关文档

- SetPasswordPolicy

2.3. 修改RAM用户登录密码

阿里云账号可以定期为RAM用户修改登录密码以提高账号安全性。

操作步骤

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏的**人员管理**菜单下，单击**用户**。
3. 在**用户登录名称/显示名称**列表下，单击目标RAM用户名称。
4. 在**认证管理**页签下，单击**修改登录设置**。
5. 在**设置登录密码**区域下，设置登录密码。
   - 选择**重新自动生成默认密码**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**重新设置自定义密码**后，需要输入新的密码，然后单击**确定**。
6. 单击**关闭**。

> **说明** 如果阿里云账号允许RAM用户自主管理密码，RAM用户也可以登录控制台自行修改密码。

相关文档

- ChangePassword

3.基本安全设置

3.1. 检查阿里云账号安全性

通过RAM安全报告可以评估阿里云账号的安全性，定期进行阿里云账号安全检查并进行相应设置可以更有效的保护您的阿里云账号安全。

操作步骤

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏的**概览**菜单下，检查阿里云账号安全。
3. 单击目标安全项的名称，单击**前往设置**，可以快速完成相应设置。

后续步骤

单击**下载安全报告**可以获取一份安全实践报告，其中列出了您的阿里云账号中安全实践相关的状态。

- **SubUser**：表示阿里云账号中RAM用户的个数。
- **SubUserBindMfa**：表示绑定了多因素认证设备（MFA）的RAM用户的个数。
- **SubUserWithUnusedAccessKey**：表示拥有未使用访问密钥（AccessKey）的RAM用户的个数。
- **RootWithAccessKey**：表示阿里云账号创建的访问密钥（AccessKey）的个数。
- **SubUserWithOldAccessKey**：表示使用旧访问密钥（AccessKey）的RAM用户的个数。
- **SubUserPwdLevel**：表示RAM用户密码强度的等级。
- **UnusedAkNum**：表示阿里云账号中未使用的访问密钥（AccessKey）的个数。
- **OldAkNum**：表示阿里云账号中旧的访问密钥（AccessKey）的个数。
- **BindMfa**：表示阿里云账号是否绑定多因素认证设备（MFA）。
- **Score**：表示阿里云账号安全最终得分。

> 说明
>
> - 若您的得分较低，请您及时进行相应的安全设置。
> - 遵循最佳安全实践原则，可以更有效的保护阿里云账号及资产的安全。详情请参见企业上云安全实践。

3.2. 获取用户凭证报告

通过RAM您可以生成和下载云账号和RAM用户的登录凭证信息，包括控制台登录密码、访问密钥（AccessKey）和多因素认证（MFA）。您可以使用用户凭证报告进行合规性审计。

操作步骤

1. 云账号或具有管理访问控制权限（AliyunRAMFullAccess）的RAM用户登录RAM控制台。
2. 在左侧导航栏，单击**概览**。
3. 在**安全检查**区域下，单击**下载用户凭证报告**。
4. 待用户凭证报告生成后，您可以单击**下载**，将报告保存到本地。

> **说明** 用户凭证报告生成所需时间视云账号内RAM用户的数量而定，如果报告生成时间过长，您可以选择**稍后下载**。每4小时您可以在控制台生成一份新的CSV格式的用户凭证报告，如果距离上一份报告生成时间不足4小时，则直接返回已经生成好的报告，而不会生成新报告。

执行结果

用户凭证报告包含如下字段。

字段	示例值	描述
user	username@company-alias.onaliyun.com	用户名称。第一行固定为云账号，显示为<root>，从第二行开始是RAM用户，显示为UPN（User Principal Name）格式。
user_creation_time	2019-11-11T12:33:18Z	创建用户的时间。 **说明** 时间格式按照ISO8601标准，并使用UTC时间。格式为：YYYY-MM-DDThh:mm:ssZ。
user_last_logon	2019-11-11T12:45:18Z	RAM用户的最近一次登录控制台的时间。 **说明** RAM用户可能是通过密码或用户SSO登录。如果RAM用户从未登录过，则此字段显示为 `-` 。
password_exist	TRUE	控制台登录密码是否存在。取值为 `TRUE` 或 `FALSE` 。 • 对RAM用户，取决于登录配置信息是否存在。 • 对云账号，则默认为 `TRUE` 。 **说明** 如果您的账号是在资源目录中创建的资源账号，您可以获取云账号密码相关的信息但密码实际不可用。

字段	示例值	描述
password_active	N/A	登录密码是否处于启用状态。取值为 TRUE 、 FALSE 或 N/A 。 • 如果RAM用户的登录配置信息不存在，则为 N/A 。 • 云账号默认为 N/A 。
password_last_changed	2019-11-11T12:50:18Z	最后修改密码的时间。如果RAM用户的登录配置信息不存在，则为 N/A 。 说明 RAM只记录了2016年4月5日以后的数据，如果最后一次修改时间在此之前，则为 N/A 。云账号的密码修改时间有24小时以内的延迟。
password_next_rotation	2019-11-13T12:50:18Z	下次需修改密码的时间。 • 如果密码规则设定为密码永不过期，则为 - 。 • 如果RAM用户的登录配置信息不存在，则为 N/A 。 • 云账号默认为 N/A 。
mfa_active	TRUE	是否已经绑定MFA。取值为 TRUE 、 FALSE 或 N/A 。如果RAM用户的登录配置信息不存在，则为 N/A 。
access_key_1_exist	TRUE	AccessKey1是否存在。取值为 TRUE 或 FALSE 。
access_key_1_active	TRUE	AccessKey1是否启用。取值为 TRUE 、 FALSE 或 N/A 。如果没有AccessKey，则为 N/A 。
access_key_1_last_rotated	2019-11-11T12:50:18Z	用户第1个AccessKey的创建或上次更改的时间。如果没有AccessKey，则为 N/A 。

字段	示例值	描述
access_key_1_last_used	2019-11-13T12:50:18Z	AccessKey1的最后使用时间。 • 如果AccessKey在系统开始跟踪最后使用时间后未使用过，则为 `-` 。 • 如果没有AccessKey，则为 `N/A` 。 说明 最后使用时间从2019年6月1号开始记录，有2小时以内的延迟。
access_key_2_exist	TRUE	AccessKey2是否存在。取值为 `TRUE` 或 `FALSE` 。
access_key_2_active	TRUE	AccessKey2是否启用。取值为 `TRUE` 、 `FALSE` 或 `N/A` 。如果没有AccessKey，则为 `N/A` 。
access_key_2_last_rotated	2019-11-11T12:50:18Z	用户第2个AccessKey的创建或上次更改的时间。如果没有AccessKey，则为 `N/A` 。
access_key_2_last_used	2019-11-13T12:50:18Z	AccessKey2的最后使用时间。 • 如果AccessKey在系统开始跟踪最后使用时间后未使用过，则为 `-` 。 • 如果没有AccessKey，则为 `N/A` 。 说明 最后使用时间从2019年6月1号开始记录，有2小时以内的延迟。

说明 目前RAM控制台只能创建2个AccessKey。由于历史原因，部分用户拥有2个以上AccessKey，这些额外的AccessKey会显示在CSV文件的最后，以 `additional_access_key_` 开头。

3.3. 管理RAM用户登录设置

本文为您介绍如何为RAM用户启用、修改或清空控制台登录设置。

操作步骤

1. 云账号登录RAM控制台。
2. 在左侧导航栏的人员管理菜单下，单击用户。
3. 在用户登录名称/显示名称列表下，单击目标RAM用户名称。
4. 在认证管理页签下的控制台登录管理区域，您可以根据需要启用、修改或清空控制台登录设置。
   - 启用控制台登录：如果RAM用户没有进行过控制台登录设置，您可以根据需要对以下几个选项进行设置。
     - 控制台密码登录：表示是否启用对该RAM用户的登录设置。

       > 说明
       > - 只有选择为开启，RAM用户才可以使用密码登录控制台。
       > - 如果您需要禁止RAM用户通过控制台访问阿里云，但又不希望删除密码以及MFA等设置，您可以选择禁用。选择禁用后，您仍可修改RAM用户的登录配置，但不会生效。直到再次选择为开启，登录配置才会生效。

     - 设置登录密码：表示为RAM用户自动生成默认密码或自定义登录密码。

       > 说明 设置完成后，请您妥善保管新密码。

     - 是否要求重置密码：表示是否要求RAM用户下次登录时重置密码。
     - 是否开启多因素认证：表示是否要求RAM用户开启多因素认证。

       > 说明 如果云账号要求RAM用户开启多因素认证，RAM用户在登录时会直接进入多因素认证绑定流程。

   - 修改登录设置：如果RAM用户已经进行过控制台登录设置，您可以根据需要再次修改上述控制台登录的相关设置。
   - 清空登录设置：如果RAM用户已经进行过控制台登录设置，通过清空登录设置可以删除RAM用户的所有登录设置，包括密码以及MFA等。

     > 说明 登录设置一旦被清空，无法自动恢复，请您慎重操作。您可以再次启用控制台登录，但必须重新设置各个选项。

相关文档

- CreateLoginProfile
- GetLoginProfile
- UpdateLoginProfile
- DeleteLoginProfile

3.4. 设置RAM用户安全策略

阿里云账号可以通过修改RAM用户安全设置更好的管理RAM用户的权限。

操作步骤

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏的人员管理菜单下，单击设置。
3. 在安全设置页签下，单击修改RAM用户安全设置，配置相关参数。
   - 保存MFA登录状态7天：表示是否允许RAM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。
   - 自主管理密码：表示是否允许RAM用户修改密码。
   - 自主管理AccessKey：表示是否允许RAM用户管理访问密钥。
   - 自主管理多因素设备：表示是否允许RAM用户绑定或解绑多因素认证设备。
   - 登录Session过期时间：表示RAM用户登录有效期，单位为小时。

     > 说明 通过切换角色或角色SSO登录控制台时，登录会话有效期也会受到登录Session过期时间的限制，即最终的登录会话有效期将不会超过此参数设置的值。详情请参见使用RAM角色、角色SSO的SAML响应。

   - 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，但使用访问密钥发起的API访问不受影响。
4. 单击确定。

   > 说明 设置成功后，此规则适用于所有RAM用户。

相关文档

- SetSecurityPreference

3.5. 为云账号设置登录掩码

通过设置登录掩码，云账号只能从指定的IP地址进行登录，进一步提高了账号的安全性。

操作步骤

1. 云账号登录阿里云控制台。
2. 将鼠标悬停在右上角头像的位置，单击安全设置。
3. 在安全设置页面下的登录掩码区域，单击设置。
4. 在登录掩码页面，输入正确的登录掩码。

   > 说明 当需要配置多个登录掩码时，请使用分号来分隔登录掩码，例如：192.168.0.0/16;10.0.0.0/8。

5. 单击保存。

   > 说明 设置完成后，云账号使用密码登录或单点登录（SSO）时会受到影响，但使用访问密钥发起的API访问不受影响。

4.高级设置

4.1. 管理默认域名

每个云账号都有一个默认域名，RAM用户可以通过默认域名登录RAM控制台。本文为您介绍如何修改登录名后缀，便于用户记忆登录名称。

操作步骤

1. 云账号登录RAM控制台。
2. 在左侧导航栏的**人员管理**菜单下，单击**设置**。
3. 在**高级设置**页签下，可以查看或更新**默认域名**。
   - 查看**默认域名**：**默认域名**格式为 `<AccountAlias>.onaliyun.com` 。账号别名（AccountAlias）的默认值为*AccountID*，如果未设置过账号别名，此时**默认域名**的格式为 `<AccountID>.onaliyun.com` 。
   - 更新**默认域名**：单击**更新**，输入新的账号别名，单击**确定**。

后续步骤

RAM用户登录RAM控制台时可以使用默认域名登录。

此时RAM用户登录名称为 `<username>@<AccountAlias>.onaliyun.com` ，即RAM用户登录名称@默认域名。详情请参见RAM用户登录控制台。

另外，使用默认域名可以简化SAML SSO的配置流程，详情请参见进行用户SSO时阿里云SP的SAML配置。

4.2. 创建并验证域别名

域别名就是指默认域名的别名，创建并验证域别名成功后，RAM用户便可以使用该域别名登录RAM控制台。

前提条件

进行操作前，请确保您已经持有公网上可以解析的域名。

操作步骤

1. 登录RAM控制台，创建域别名。
   i. 使用云账号登录RAM控制台。
   ii. 在左侧导航栏的**人员管理**菜单下，单击**设置**。
   iii. 在**高级设置**页签下，单击**创建域别名**。
   iv. 填写**域名称**。
   v. 单击**确定**，然后复制验证码。
2. 登录您持有的域名对应的域名解析平台，添加域名解析TXT记录。 如果您使用阿里云云解析DNS服务，在**记录值**中输入上面获取的验证码，具体操作方法请参见添加解析记录。

3. 登录RAM控制台，进行域名归属验证。
   i. 在左侧导航栏的**人员管理**菜单下，单击**设置**。
   ii. 在**高级设置**页签下，单击**域名归属验证**。
   iii. 单击**确定**。

后续步骤

创建域别名后，RAM用户登录RAM控制台时可以使用域别名登录。

此时RAM用户登录名称为 `<$username>@<$DomainAlias>` ，即RAM用户登录名称@域别名。详情请参见RAM用户登录控制台。

另外，使用域别名可以简化SAML SSO的配置流程，详情请参见进行用户SSO时阿里云SP的SAML配置。

5.访问密钥

5.1. 为RAM用户创建访问密钥

访问密钥（AccessKey）是RAM用户的长期凭证。如果为RAM用户创建了访问密钥，RAM用户可以通过API或其他开发工具访问阿里云资源。

背景信息

为保证账号安全，强烈建议您给RAM用户创建访问密钥，不要给云账号（主账号）创建访问密钥。

操作步骤

1. 云账号登录RAM控制台。
2. 在左侧导航栏，单击**人员管理 > 用户**。
3. 在**用户登录名称/显示名称**列表下，单击目标RAM用户名称。
4. 在**用户AccessKey**区域，单击**创建AccessKey**。
5. 单击**关闭**。

> 说明
> - AccessKey Secret只在创建时显示，不提供查询，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。

相关文档

- CreateAccessKey

5.2. 查看访问密钥基本信息

本文为您介绍如何查看访问密钥基本信息，目前可以查询的信息包括AccessKey ID、状态、最后使用时间和创建时间等信息。

操作步骤

1. 云账号登录RAM控制台。
2. 在左侧导航栏的**人员管理**菜单下，单击**用户**。
3. 在**用户登录名称/显示名称**列表下，单击目标RAM用户名称。
4. 在**用户AccessKey**区域下，可以查看访问密钥基本信息。

> 说明 AccessKeySecret只在创建时显示，不提供查询。

5.3. 轮换访问密钥

每个RAM用户最多可以创建两个访问密钥。如果您的访问密钥已经使用3个月以上，建议您及时轮换访问密钥，降低访问密钥被泄露的风险。

操作步骤

1. 创建用于轮换的第二个访问密钥。详情请参见为RAM用户创建访问密钥。
2. 在使用访问密钥的所有应用程序或系统中，更新正在使用的访问密钥为新创建的第二个访问密钥。

   > 说明 您可以登录RAM控制台，在用户详情页的用户AccessKey列表中，查看访问密钥的最后使用时间，以此初步判断第二个访问密钥是否已经被使用，原来的访问密钥是否已经不用。

3. 禁用原来的访问密钥。详情请参见禁用访问密钥。
4. 验证使用访问密钥的所有应用程序或系统是否正常运行。
   - 如果运行正常，说明访问密钥更新成功，您可以放心地删除原来的访问密钥。
   - 如果运行异常，您需要暂时激活原来的访问密钥，然后重复步骤2~4的操作，直至更新成功。
5. 删除原来的访问密钥。详情请参见删除访问密钥。

后续步骤

建议您定期重复上述步骤，再次轮换访问密钥。

5.4. 禁用访问密钥

当RAM用户权限发生变化时或不再需要通过API访问阿里云资源，可以禁用其访问密钥。

操作步骤

1. 云账号登录RAM控制台。
2. 在左侧导航栏的人员管理菜单下，单击用户。
3. 在用户登录名称/显示名称列表下，单击目标RAM用户名称。
4. 在用户AccessKey区域下，单击禁用。

   > 说明 单击激活可以重新激活访问密钥。

5. 单击确定。

相关文档

- UpdateAccessKey

5.5. 删除访问密钥

当您不再需要通过API或其他开发工具访问阿里云资源时，可以删除访问密钥。

前提条件

删除访问密钥前，可以通过访问密钥的最后使用时间确认访问密钥的使用情况。关于如何查看访问密钥的最后使用时间，请参见查看访问密钥基本信息。

> 说明 删除访问密钥需慎重，在使用中的访问密钥一旦删除，可能会造成您的应用系统故障。

操作步骤

1. 云账号登录RAM控制台。
2. 在左侧导航栏的人员管理菜单下，单击用户。

3. 在**用户登录名称/显示名称**列表下，单击目标RAM用户名称。
4. 在**用户AccessKey**区域下，单击**删除**。
5. 勾选**我已知晓风险，确认删除**。
6. 单击**确定**。

相关文档

- DeleteAccessKey

6.多因素认证

6.1. 为云账号设置多因素认证

本文以Google Authenticator应用为例介绍如何为云账号开启多因素认证（Multi-factor authentication，MFA）。开启多因素认证后，可以为您的账号提供更高的安全保护。

操作步骤

1. 云账号登录阿里云控制台。
2. 将鼠标悬停在右上角头像的位置，单击**安全设置**。
3. 在**安全设置**页面下的**账号保护**区域，单击**查看**。

   > **说明** 多因素认证（MFA）已更名为TOTP。

4. 在**开启账号保护**页面下，选择开启保护的场景和验证方式，单击**确定**。
5. 在**验证身份**页面，选择合适的方式并根据页面提示进行身份验证。
6. 单击**立即验证**，输入验证码后，单击**下一步**。
7. 在移动设备端，下载并安装Google Authenticator应用，安装完成后单击**下一步**。
   - iOS：在App Store中搜索Google Authenticator。
   - Android：在应用市场中搜索Google Authenticator。

   > **说明** 安卓版Google Authenticator还依赖外部二维码扫描组件，所以您还需要在应用市场中搜索安装条行码扫描器。

8. 在移动设备端，登录Google Authenticator应用。
9. 选择合适的方式添加多因素认证设备。
   - 扫码添加（推荐）：在移动设备端，单击**开始设置 > 扫描条形码**，扫描阿里云控制台**绑定MFA**步骤页面出现的二维码。
   - 手动添加：在移动设备端，单击**开始设置 > 手动输入验证码**，填写账号和密钥，单击√。

   > **说明** 账号和密钥可以通过阿里云控制台获取，在**验证身份**页面下的**绑定MFA**步骤，鼠标悬停在**扫描失败**处便可以进行查看。

10. 在阿里云控制台，输入移动设备端显示的动态验证码，单击**下一步**，完成绑定。

    > **说明** 移动设备端的阿里云应用会显示您当前账号的动态验证码，每30秒更新一次。

后续步骤

绑定多因素认证设备后，云账号再次登录阿里云时，系统将要求输入两层安全要素：

1. 第一安全要素：用户名和密码
2. 第二安全要素：多因素认证设备生成的验证码

> 说明
> - 为云账号绑定多因素认证设备后，不影响RAM用户的登录。
> - 卸载MFA应用或删除绑定好的MFA前，请先前往阿里云停用MFA，否则可能无法正常登录阿里云。

相关文档

- BindMFADevice

6.2. 为云账号解绑多因素认证

如果您不再需要为云账号绑定多因素认证设备或需要更换多因素认证设备时，可以将绑定的多因素认证设备进行解绑。本文以Google Authenticator应用为例介绍如何为云账号解绑多因素认证设备。

操作步骤

1. 云账号登录阿里云控制台。
2. 将鼠标悬停在右上角头像的位置，单击**安全设置**。
3. 在**安全设置**页面下的**账号保护** 区域，单击**查看**。

> 说明 多因素认证（MFA）已更名为TOTP。

4. 在**账号保护设置**区域，单击**停用**。
5. 在移动设备端，登录Google Authenticator应用。
6. 在阿里云控制台，输入Google Authenticator应用生成的动态验证码，单击**确定**，完成解绑。

6.3. 为RAM用户设置多因素认证

本文以Google Authenticator应用为例介绍如何为RAM用户开启多因素认证（Multi-factor authentication，MFA）。开启多因素认证后，可以为您的账号提供更高的安全保护。

操作步骤

1. 云账号登录RAM控制台。

> 说明
> - 如果云账号要求RAM用户开启多因素认证，那么RAM用户登录时会直接进入多因素认证绑定流程，请直接从第5步开始操作。
> - 如果云账号允许RAM用户自主管理多因素认证设备，RAM用户也可以登录控制台绑定MFA。将鼠标悬停在右上角头像的位置，单击**安全信息管理**，在**MFA设备管理**菜单下，单击**启用MFA设备**。

2. 在左侧导航栏的**人员管理**菜单下，单击**用户**。
3. 在**用户登录名称/显示名称**列表下，单击目标RAM用户名称。
4. 在**认证管理**页签下，单击**启用虚拟MFA设备**。
5. 在移动设备端，下载并安装Google Authenticator应用。
   - iOS：在App Store中搜索Google Authenticator

- iOS：在App Store中搜索Google Authenticator。
- Android：在应用市场中搜索Google Authenticator。

> 说明 安卓版Google Authenticator还依赖外部二维码扫描组件，所以您还需要在应用市场中搜索安装条行码扫描器。

6. 在移动设备端，登录Google Authenticator应用。
7. 选择合适的方式添加多因素认证设备。
   - 扫码添加（推荐）：在移动设备端，单击**开始设置 > 扫描条形码**，扫描RAM控制台**扫码获取**页签下的二维码。
   - 手动添加：在移动设备端，单击**开始设置 > 手动输入验证码**，填写账号和密钥，单击**√**。

> 说明 账号和密钥可以通过RAM控制台获取，在**手输信息获取**页签下可以进行查看。

8. 在RAM控制台，输入移动设备端显示的两组连续的动态验证码，单击**确定启用**，完成绑定。

> 说明 移动设备端的阿里云应用会显示您当前账号的动态验证码，每30秒更新一次。

后续步骤

绑定多因素认证设备后，RAM用户再次登录阿里云时，系统将要求输入两层安全要素：

1. 第一安全要素：用户名和密码。
2. 第二安全要素：多因素认证设备生成的验证码。

> 说明 卸载MFA应用或删除绑定好的MFA前，请先前往阿里云停用MFA，否则可能无法正常登录阿里云。

相关文档

- BindMFADevice

6.4. 为RAM用户解绑多因素认证

如果您不再需要为RAM用户绑定多因素认证设备或需要更换多因素认证设备时，云账号可以为RAM用户解绑多因素认证设备。

操作步骤

1. 云账号登录RAM控制台。

> 说明 如果云账号允许RAM用户自主管理多因素认证设备，RAM用户也可以登录控制台解绑MFA。单击**安全信息管理**，在 **MFA设备管理**菜单下，单击**停用MFA设备**。

2. 在左侧导航栏的**人员管理**菜单下，单击**用户**。
3. 在**用户登录名称/显示名称**列表下，单击目标RAM用户名称。
4. 在**认证管理**页签下，单击**停用虚拟MFA设备**。
5. 单击**确定**，完成解绑。

相关文档

- UnbindMFADevice