我的凭证

文档版本 01

发布日期 2025-11-06

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 我的凭证（新版）

1.1 什么是我的凭证

我的凭证是将用户的身份凭证信息进行集中展示与管理的服务。

当您通过API访问华为云时，需要使用您的身份凭证，例如账号名称、账号ID、IAM用户ID等，您可以在我的凭证新版控制台页面查看相关的身份凭证。同时还可以在我的凭证页面管理您的登录凭证、访问密钥（AK/SK）和多因素认证设备。

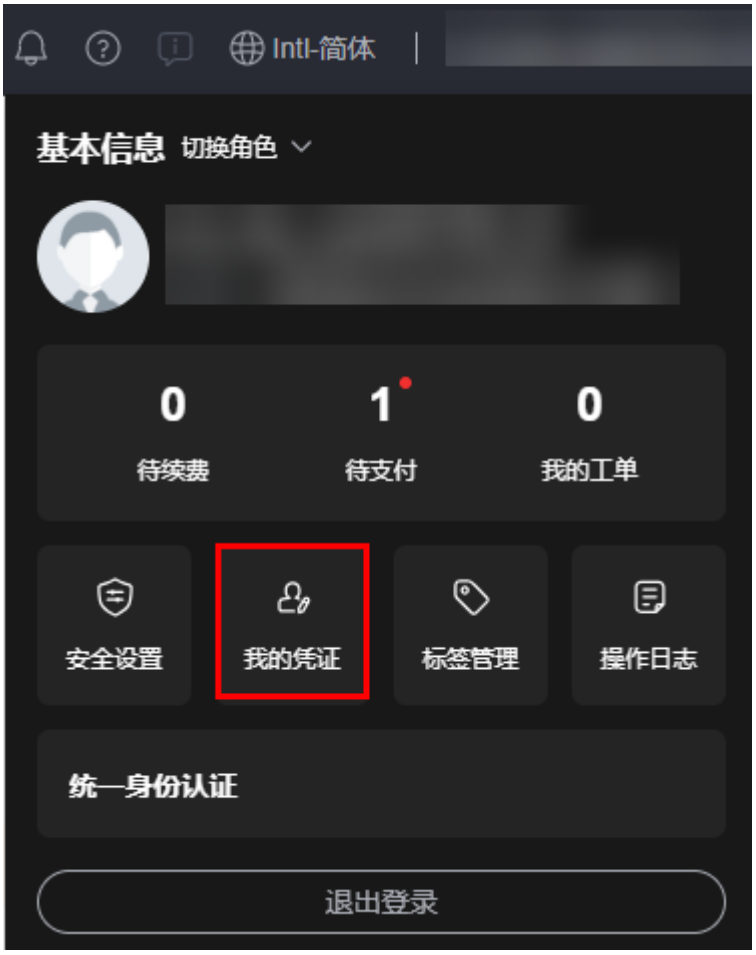
约束与限制

如果IAM用户需要查看和修改我的凭证，需要先获取相关的权限，详细的授权项请参考**IAM身份策略授权参考**。

查看我的凭证

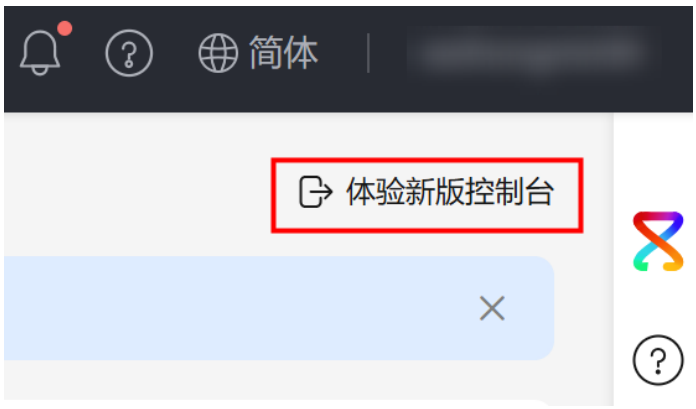
步骤1 登录**华为云控制台**，鼠标移动至右上方的用户名，在下拉列表中选择“我的凭证”。

图 1-1 选择我的凭证



步骤2 单击右上角“体验新版控制台”，进入新版我的凭证界面。

图 1-2 进入新版我的凭证



步骤3 在“我的凭证”页面，查看**登录凭证**、**访问密钥**和**多因素认证设备**。

表 1-1 我的凭证信息

基本信息		说明
身份凭证	IAM用户名	IAM用户的登录名，登录华为云时需要提供。
	IAM用户ID	IAM用户在华为云的标识ID，由系统自动生成，无法修改。
	账号名	账号的名称，账号是承担费用的主体（例如一个企业），在注册时自动创建，云服务资源按账号完全隔离。
	账号ID	账号在华为云中的标识ID，由系统自动生成，无法修改。
登录凭证		登录凭证是您登录控制台时使用的登录密码。可以重新自定义设置登录密码，查看密码过期时间和最近一次修改密码的时间。
访问密钥		用户的Access Key/Secret Key (AK/SK)，最多可创建两对。使用API访问系统时需要使用AK/SK进行签名。
多因素认证设备		启用多因素认证后，用户进行操作时，除了需要提供用户名和密码外（第一次身份验证），还需要提供验证码、插入硬件设备、提供指纹、PIN码或人脸识别（第二次身份验证），多因素身份认证结合起来将为您的账号和资源提供更高的安全保护。

----结束

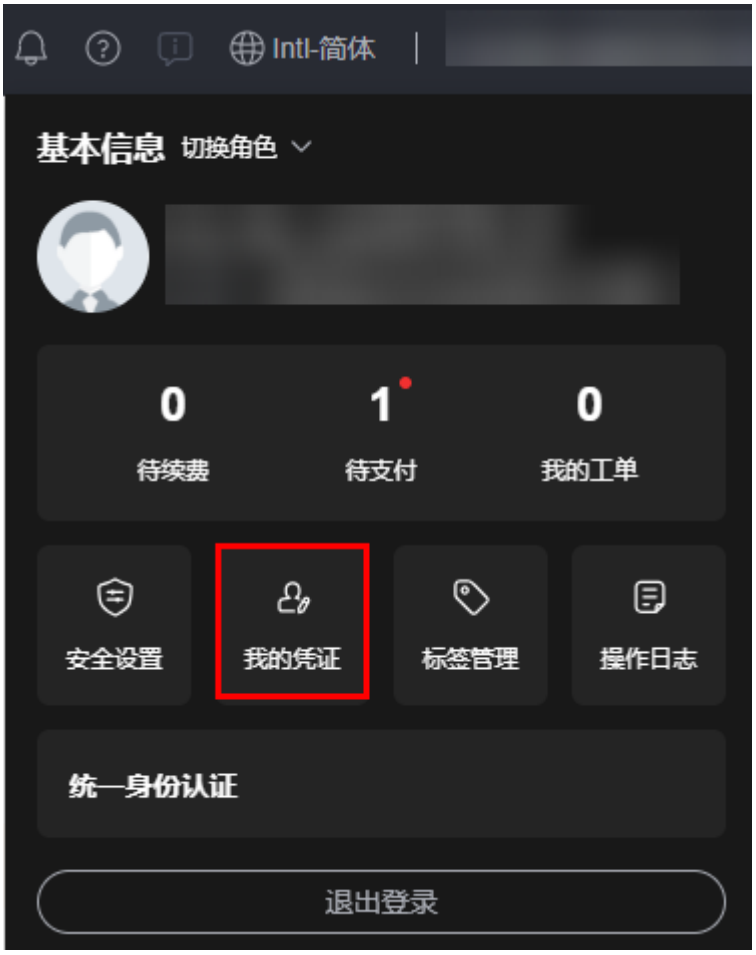
1.2 登录凭证

登录凭证是您登录控制台时使用的登录密码。拥有权限的IAM用户可以在我的凭证界面自定义修改登录密码，查看密码过期时间和最后一次修改密码的时间。

自定义修改登录密码

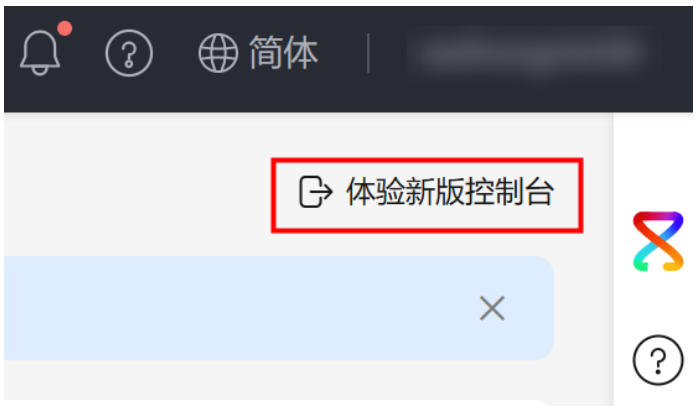
步骤1 登录华为云控制台，鼠标移动至右上方的用户名，在下拉列表中选择“我的凭证”。

图 1-3 选择我的凭证



步骤2 单击右上角“体验新版控制台”，进入新版我的凭证界面。

图 1-4 进入新版我的凭证



步骤3 单击“已设置”右侧的，在弹窗中输入旧密码、新密码以及确认新的密码。单击“确定”。

图 1-5 自定义设置登录凭证

----结束

1.3 访问密钥

访问密钥（AK/SK，Access Key ID/Secret Access Key）包含访问密钥ID（AK）和秘密访问密钥（SK）两部分，是您在华为云的长期身份凭证，您可以通过访问密钥对华为云**API的请求进行签名**。华为云通过AK识别访问用户的身份，通过SK对请求数据进行签名验证，用于确保请求的机密性、完整性和请求者身份的正确性。

我的凭证适用于管理员授权的IAM用户在可以登录控制台的情况下，主动创建、删除自己的访问密钥。

统一身份认证服务（IAM）同样也可以管理访问密钥，适用于IAM用户不能登录控制台时，由管理员在IAM中管理访问密钥，具体操作请参见：**管理IAM用户访问密钥**。

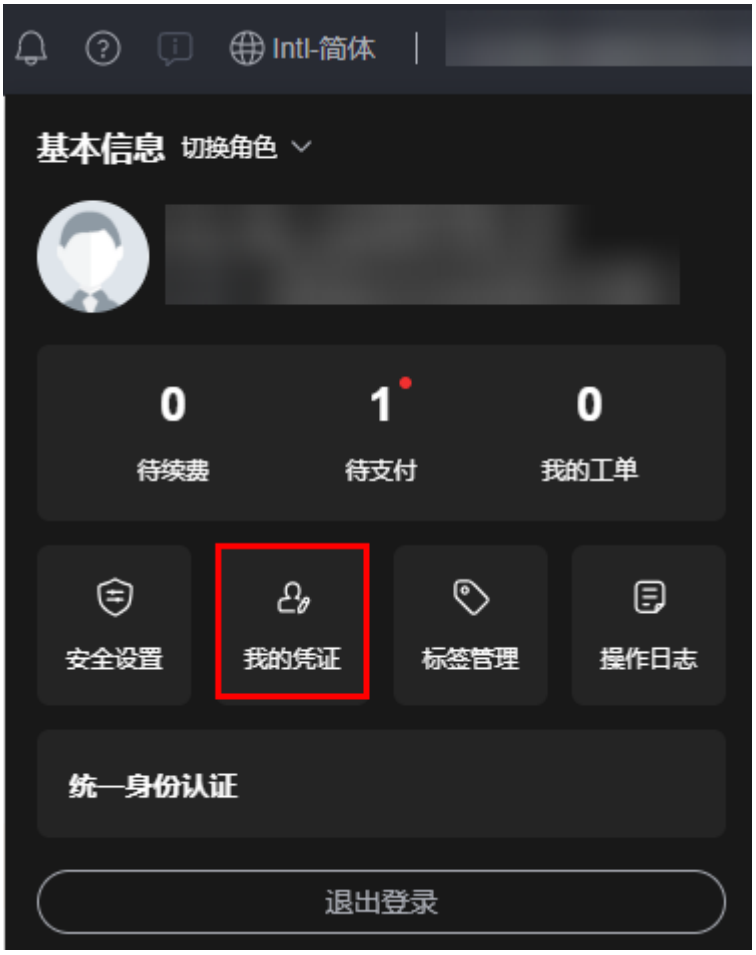
注意事项

1. **每个用户最多可创建2个访问密钥，不支持增加配额。**每个访问密钥权限相同，相互独立，包括一对AK/SK，有效期为永久，**每个访问密钥仅能下载一次**。为了账号安全性，建议您妥善保管并定期修改访问密钥。修改访问密钥的方法为删除旧访问密钥，然后重新生成。
2. 如果您无法管理您的访问密钥，请联系**管理员**：
   - 由管理员管理您的访问密钥，方法请参见：**管理IAM用户访问密钥**。
   - 请管理员为您配置权限。如需配置权限请参见：**给IAM用户授权**。
3. 管理员可以在“用户详情”页面查看IAM用户的访问密钥ID（AK），秘密访问密钥（SK）由IAM用户自行保管。

新增访问密钥

步骤1 登录**华为云控制台**，鼠标移动至右上方的用户名，在下拉列表中选择“我的凭证”。

图 1-6 选择我的凭证



步骤2 在“访问密钥”区域中，单击“新增访问密钥”。

图 1-7 新增访问密钥

说明

- 无法直接对已创建的访问密钥进行修改。如需修改访问密钥，请删除访问密钥后重新创建。
- 不建议您为账号根用户创建访问密钥。如果必须要创建，请确认相关安全风险。

步骤3 单击“下载访问密钥”，生成并下载访问密钥。

创建访问密钥成功后，您可以在访问密钥列表中查看访问密钥ID（AK），在下载的.csv文件中查看访问密钥（SK）。

说明

- 请及时下载保存，弹窗关闭后将无法再次获取该密钥信息，但您可重新创建新的密钥。
- 当您下载访问密钥后，可以在浏览器“下载内容”中打开相关文件。
- 为了账号安全性，建议您妥善保管并定期轮转访问密钥，轮转访问密钥的方法为删除旧访问密钥，然后重新生成。删除旧访问密钥时，可以使用最近使用时间来确认该访问密钥在一段时间内已经不再使用，确保删除后不会影响您的存量业务。

----结束

删除访问密钥

当您发现访问密钥被异常使用（包括丢失、泄露等情况），可以在我的凭证中自行删除访问密钥，或者通知管理员在IAM中删除您的访问密钥。

注意

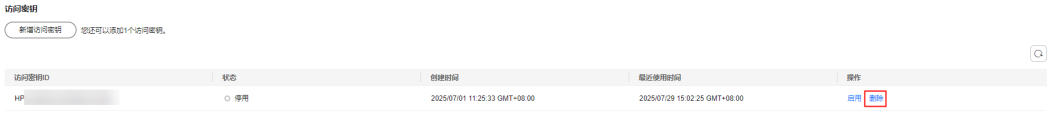
删除操作无法恢复，为保证业务连续性，建议确认访问密钥一周以上未使用后，进行删除操作。

步骤1 在“访问密钥”区域中，在需要删除的访问密钥右侧单击“停用”。

步骤2 单击“确定”，停用访问密钥。

步骤3 停用访问密钥后，单击访问密钥右侧的“删除”。请确保当前IAM用户的访问密钥删除后不会影响业务后再执行删除操作。

图 1-8 删除访问密钥



步骤4 输入“DELETE”后，单击“确定”，删除访问密钥。

----结束

启用、停用访问密钥

新创建的访问密钥默认为启用状态，如需停用该访问密钥，步骤如下：

步骤1 在“访问密钥”区域中，在需要停用的访问密钥右侧单击“停用”。

步骤2 单击“确定”，停用访问密钥。

----结束

启用访问密钥方式与停用类似，请参考以上步骤。

查看访问密钥

您可以在访问密钥页面查看访问密钥ID、状态、创建时间以及最近使用时间。

1.4 多因素认证设备

什么是多因素认证

多因素认证是一种非常简单的安全实践方法，它能够在用户名和密码之外再额外增加一层保护。启用多因素认证后，用户登录控制台进行操作时，除了需要提供用户名和密码外（第一次身份验证），还需要提供验证码、插入硬件设备、提供指纹、PIN码或人脸识别（第二次身份验证），多因素身份认证结合起来将为您的账号和资源提供更可靠的安全保护。

多因素认证支持的设备

多因素认证设备支持虚拟MFA和安全密钥。

- 虚拟MFA：虚拟MFA是一种遵循基于时间的一次性密码算法 （TOTP）的认证方式。IAM只支持基于软件的虚拟MFA，实现了TOTP的应用程序被称为虚拟MFA设备，它们可以在移动硬件设备（例如手机）上运行，非常方便。启用虚拟MFA后，当需要验证身份时，您还需要输入来自虚拟MFA设备的验证码，从而实现多因素认证。
- 安全密钥：安全密钥是一种可以替代密码的更为安全的认证方式。华为云当前支持基于FIDO2身份验证协议的安全密钥，启用安全密钥后，您可以使用电脑、手机等设备自带的指纹、人脸或PIN码，以及支持FIDO2协议的安全密钥设备来完成多因素认证。例如，启用支持FIDO2协议的安全密钥（如Yubikey）后，当需要验证身份时，您需要在当前计算机中插入该设备，并触摸后进行验证；启用Windows Hello的安全密钥后，当需要验证身份时，则需要提供指纹、PIN码或人脸识别进行验证。

多因素认证应用的场景

统一身份认证服务的多因素认证主要应用在登录保护中。可以同时绑定虚拟MFA和安全密钥，认证时二选一即可。最多可以为账号根用户或IAM用户绑定1个虚拟MFA和8个安全密钥。

登录保护：您以及账号中的IAM用户登录时，除了在登录页面输入用户名和密码外，还需要在登录验证页面进行多因素认证，再次确认登录者身份，进一步提高账号安全性。

约束与限制

- 1个IAM用户仅支持绑定1个虚拟MFA。
- 1个IAM用户最多支持绑定8个安全密钥。

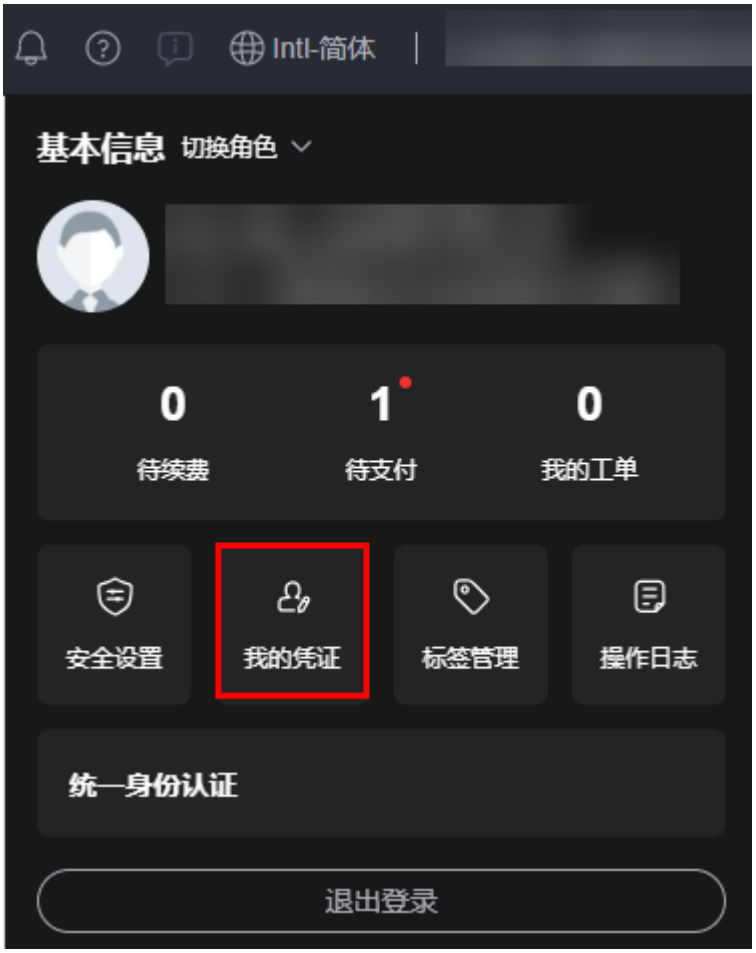
如何绑定虚拟 MFA

您需要在智能设备上安装一个虚拟MFA应用程序后（例如：Google Authenticator或Microsoft Authenticator），才能绑定虚拟MFA设备。

华为云账号和IAM用户绑定MFA后将会自动开启登录保护，并设置登录保护类型为MFA验证。IAM用户可自行在我的凭证“新版控制台”绑定虚拟MFA。

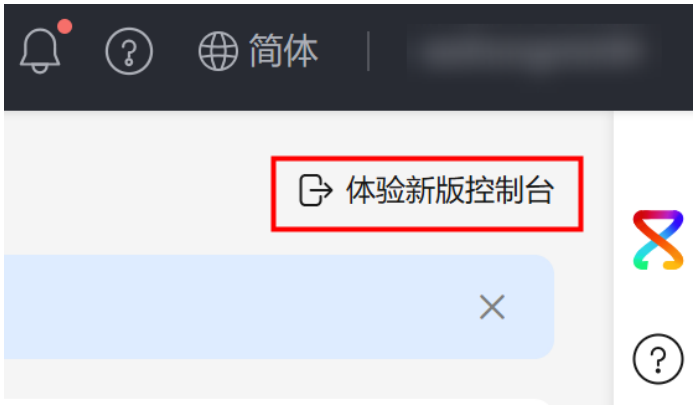
步骤1 登录华为云控制台，鼠标移动至右上方的用户名，在下拉列表中选择“我的凭证”。

图 1-9 选择我的凭证



步骤2 单击右上角“体验新版控制台”，进入新版我的凭证界面。

图 1-10 进入新版我的凭证



步骤3 在“多因素认证设备”区域，单击“添加MFA设备”。

步骤4 指定MFA设备名称。仅支持大小写字母、数字或特殊字符(-_)。

步骤5 选择MFA设备。“设备类型”选择“虚拟MFA”，然后单击“下一步”。

步骤6 根据绑定虚拟MFA的页面，在您的MFA应用程序中添加虚拟MFA设备。您可以通过扫描二维码、手动输入两种方式绑定MFA设备：

- 扫描二维码

  打开手机上已安装好的MFA应用程序，选择“扫描条形码”，扫描“添加MFA设备”侧边栏中的二维码。扫描成功后，应用程序会自动添加虚拟MFA设备。

- 手动输入

  打开手机上已安装好的MFA应用程序，选择“输入提供的密钥”，手动添加虚拟MFA设备。

  说明

  手动输入添加MFA设备方式只支持基于时间模式的虚拟MFA，建议在移动设备中开启自动设置时间功能。

步骤7 在返回MFA应用程序首页，查看虚拟MFA的动态码。动态码每30秒自动更新一次。

步骤8 在“添加MFA设备”页面输入连续的两组虚拟MFA动态码，然后单击“确定”，完成绑定虚拟MFA设备的操作。

----结束

如何解绑虚拟 MFA

步骤1 在“多因素认证设备”区域，单击虚拟MFA设备“操作”列的“解绑”。

步骤2 在弹出的对话框中，输入“YES”。

图 1-11 确认解绑

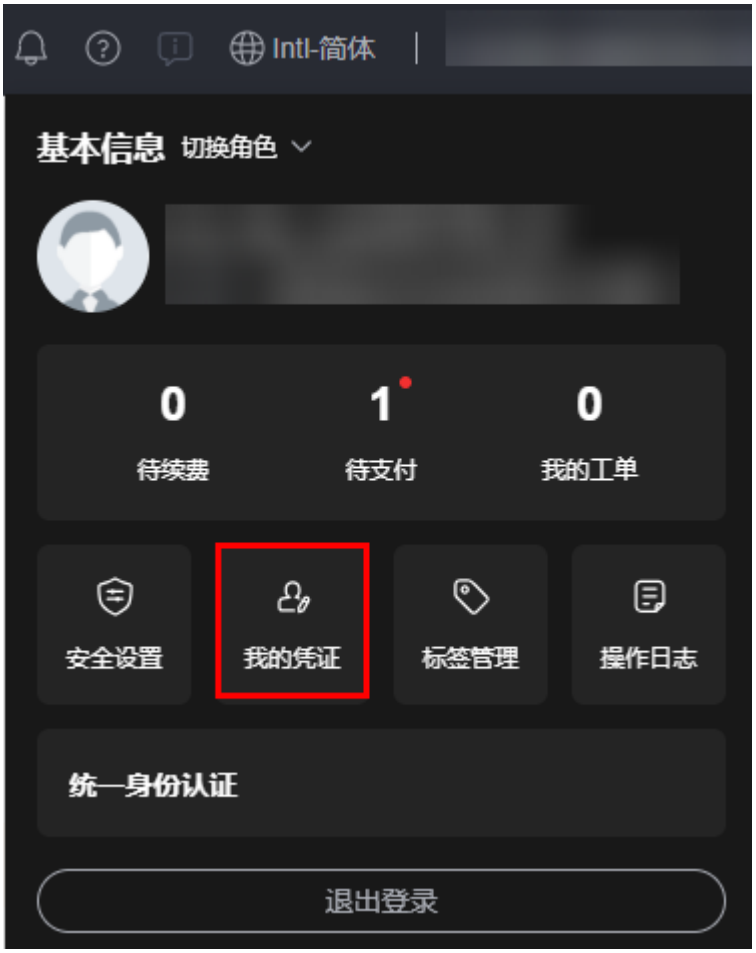
步骤3 单击“确定”，完成解绑MFA操作。

----结束

如何绑定安全密钥

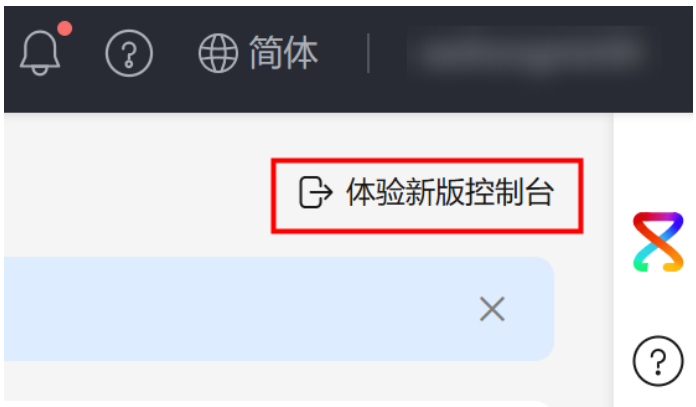
步骤1 登录华为云控制台，鼠标移动至右上方的用户名，在下拉列表中选择“我的凭证”。

图 1-12 选择我的凭证



步骤2 单击右上角“体验新版控制台”，进入新版我的凭证界面。

图 1-13 进入新版我的凭证



步骤3 在“多因素认证设备”区域，单击“添加MFA设备”。

步骤4 指定MFA设备名称。仅支持大小写字母、数字或特殊字符(-_)。

步骤5 选择MFA设备。此处选择“安全密钥”。

步骤6 单击“下一步”。

步骤7 如需要设置Windows Hello的验证方式，需要在弹窗中选择验证方式（如PIN码、面孔、指纹等）。

图 1-14 设置 Windows Hello

说明

如果Windows设备不支持开启人脸识别和指纹，将不会出现“面孔”、“指纹”等选项。FIDO2协议将会根据您设备支持的认证类型弹出对应的选项。

步骤8 输入PIN码（或识别面孔、指纹），系统认证成功后，将会出现绑定成功的提示弹窗。单击“确定”，安全密钥将出现在多因素认证设备列表中。

图 1-15 绑定成功

步骤9 如需要设置FIDO2类型的安全密钥，则在弹窗中选择“使用其他设备”并将安全密钥设备插入计算机USB端口。

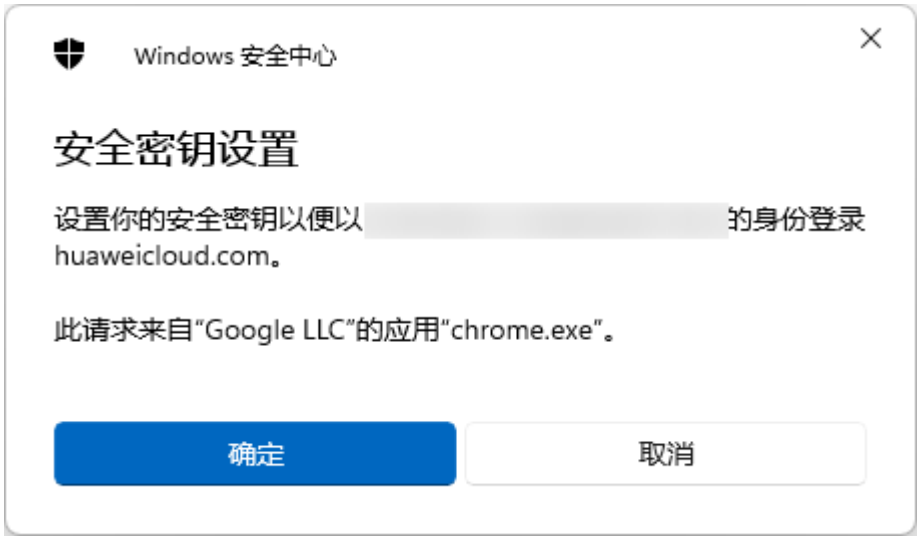
图 1-16 使用其他设备

步骤10 在新的弹窗中，选择“安全密钥”，单击“下一页”。

图 1-17 安全密钥

步骤11 单击“确定”，确认安全密钥设置。

图 1-18 确认安全密钥设置

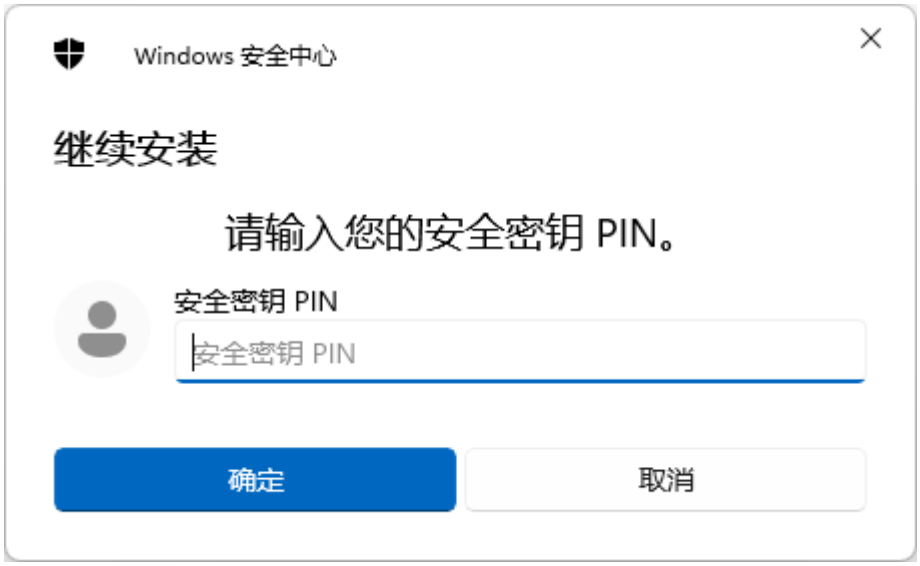


步骤12 单击“确定”，继续安装安全密钥。

图 1-19 继续安装安全密钥

步骤13 输入安全密钥的PIN码，单击“确定”。

图 1-20 输入安全密钥 PIN 码



步骤14 触摸安全密钥进行绑定。

图 1-21 触摸安全密钥

步骤15 系统认证成功后，将会出现绑定成功的提示弹窗。单击“确定”，安全密钥将出现在多因素认证设备列表中。

图 1-22 绑定成功

----结束

如何解绑安全密钥

IAM用户或账号可以在界面自助完成解绑安全密钥的操作。

步骤1 在“多因素认证设备”区域，单击安全密钥设备“操作”列的“解绑”。

步骤2 在弹出的对话框中，输入“YES”。

图 1-23 确认解绑

步骤3 单击“确定”，完成解绑安全密钥操作。

----结束

2 我的凭证（旧版）

2.1 什么是我的凭证

我的凭证是将用户的身份凭证信息进行集中展示与管理的服务。

当您通过API访问华为云时，需要使用您的身份凭证，例如账号名称、项目ID等，您可以在“我的凭证>API凭证”页面查看这些身份凭证；还可以在“我的凭证>访问密钥”页面管理您的访问密钥（AK/SK）。

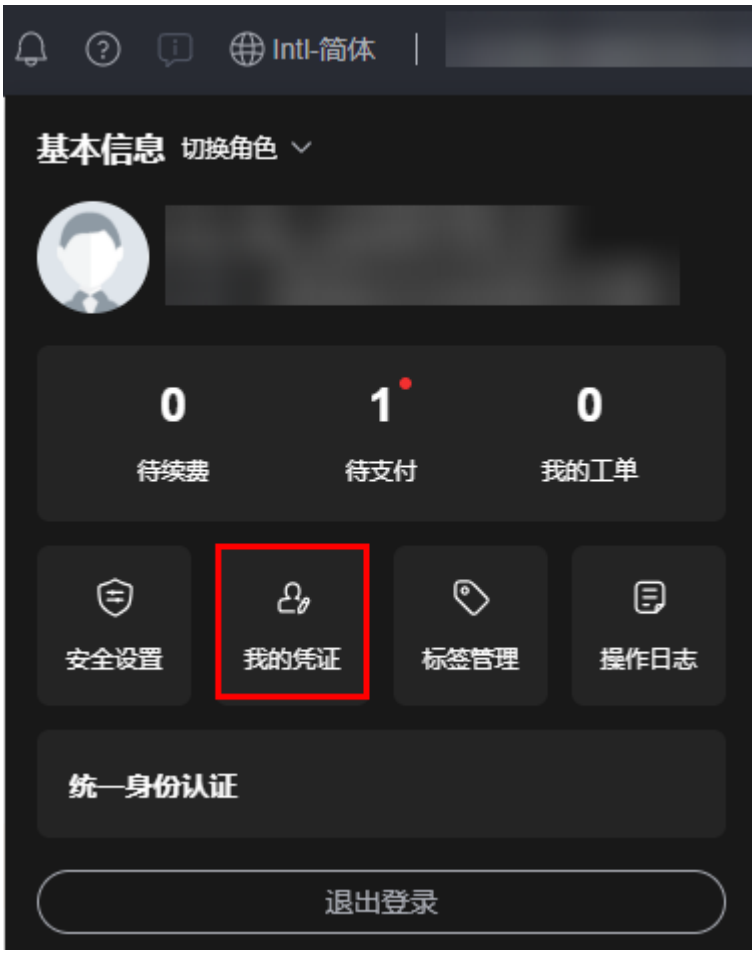
操作步骤

步骤1 登录华为云，在右上角单击“控制台”。

图 2-1 进入控制台

步骤2 在“控制台”页面，鼠标移动至右上方的用户名，在下拉列表中选择“我的凭证”。

图 2-2 选择我的凭证



步骤3 在“我的凭证”页面，查看“**API凭证**”和“**访问密钥**”。

表 2-1 我的凭证信息

基本信息		说明
API凭证	IAM用户名	IAM用户的登录名，登录华为云时需要提供。
	IAM用户ID	IAM用户在华为云的标识ID，由系统自动生成，无法修改。
	账号名	账号的名称，账号是承担费用的主体（例如一个企业），在注册时自动创建，云服务资源按账号完全隔离。
	账号ID	账号在华为云中的标识ID，由系统自动生成，无法修改。
	项目ID	项目在华为云的标识ID，由系统自动生成，无法修改。
	项目	项目用于将物理区域间的资源（计算资源、存储资源和网络资源等）进行分组和隔离。用户拥有的资源必须挂载在项目下，项目可以是一个部门或者项目组。
访问密钥		用户的Access Key/Secret Key (AK/SK)，最多可创建两对，使用API访问系统时需要使用AK/SK进行加密签名。

说明

如果您是企业联邦用户，属于虚拟IAM用户，我的凭证信息将产生如下变化：

- 不显示“IAM用户名”、“IAM用户ID”信息。
- “访问密钥”页签转为“临时访问密钥”。详情请参见：**2.4 临时访问密钥（企业联邦用户）**。

----结束

2.2 API 凭证

在API凭证中可以查看IAM用户名、IAM用户ID、账号名、账号ID、项目ID等信息。项目ID是系统所在区域的ID，是您在调用API接口进行云资源管理（如创建VPC）时，需要提供的身份凭证。

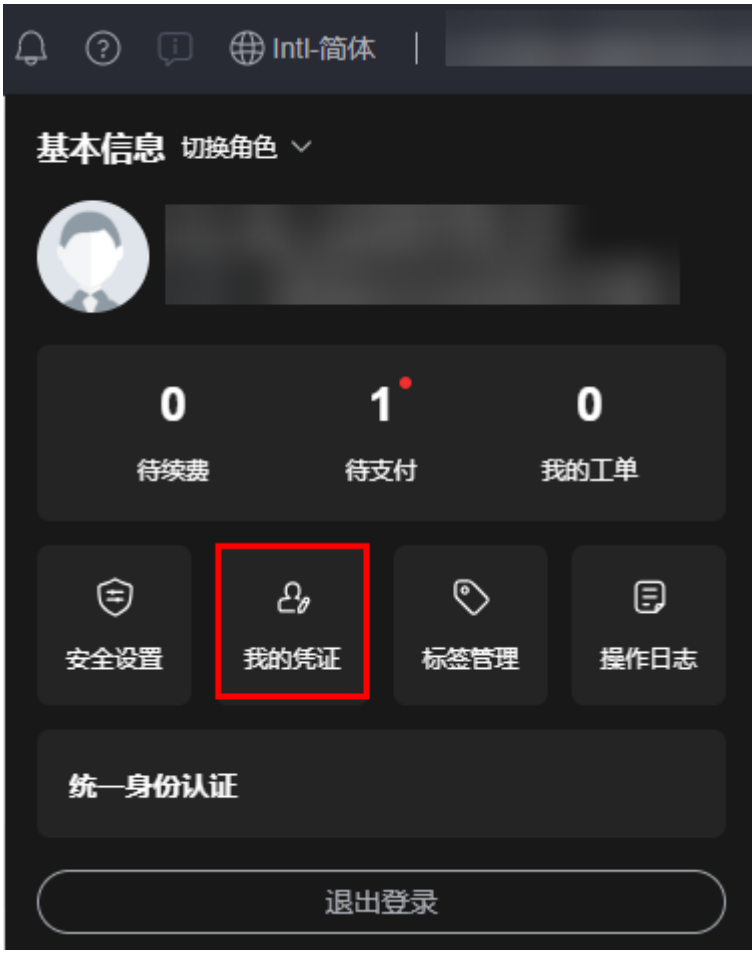
操作步骤

步骤1 登录华为云，在右上角单击“控制台”。

图 2-3 进入控制台

步骤2 在“控制台”页面，鼠标移动至右上方的用户名，在下拉列表中选择“我的凭证”。

图 2-4 选择我的凭证



步骤3 在“我的凭证”页面，“API凭证”页签中查看IAM用户名、IAM用户ID、账号名、账号ID、项目ID等信息。

图 2-5 查看信息

说明

- 如果项目列表未显示待查看的区域、项目，请单击左上角“控制台”并切换至待查看区域后，重新进入我的凭证。
- 如果您是企业联邦用户，属于虚拟IAM用户，“API凭证”页面将不显示“IAM用户名”、“IAM用户ID”信息。

----结束

2.3 访问密钥

访问密钥（AK/SK，Access Key ID/Secret Access Key）包含访问密钥ID（AK）和秘密访问密钥（SK）两部分，是您在华为云的长期身份凭证，您可以通过访问密钥对华为云**API的请求进行签名**。华为云通过AK识别访问用户的身份，通过SK对请求数据进行签名验证，用于确保请求的机密性、完整性和请求者身份的正确性。

我的凭证适用于管理员授权的IAM用户在可以登录控制台的情况下，主动创建、删除自己的访问密钥。

统一身份认证服务（IAM）同样也可以管理访问密钥，适用于IAM用户不能登录控制台时，由管理员在IAM中管理访问密钥，具体操作请参见：**管理IAM用户的访问密钥**。

说明

给IAM用户设置不同的访问模式，其可以使用的凭证类型将不同，请正确选择访问模式。

- 如果IAM用户**仅需登录管理控制台访问云服务**，建议访问方式选择**管理控制台访问**，凭证类型为**密码**。
- 如果IAM用户**仅需编程访问云服务**，建议访问方式选择**编程访问**，凭证类型为**访问密钥**。
- 如果IAM用户**需要使用密码作为编程访问的凭证**（部分API要求），建议访问方式选择**编程访问**，凭证类型为**密码**。
- 如果IAM用户使用部分云服务时，需要在其**控制台验证访问密钥**（由IAM用户输入），建议访问方式选择**编程访问和管理控制台访问**，凭证类型为**密码和访问密钥**。例如IAM用户在控制台使用云数据迁移CDM服务创建数据迁移，需要通过访问密钥进行身份验证。

注意事项

1. 每个用户最多可创建**2**个访问密钥，不支持增加配额。每个访问密钥权限相同，相互独立，包括一对AK/SK，有效期为永久，**每个访问密钥仅能下载一次**。为了账号安全性，建议您妥善保管并定期修改访问密钥。修改访问密钥的方法为删除旧访问密钥，然后重新生成。
2. 企业联邦用户不能创建访问密钥，但可以创建临时访问凭证（临时AK/SK和SecurititytToken），具体内容请参见：**临时访问密钥**。
3. 如果您是IAM用户，请在“安全设置>敏感操作>访问密钥保护”确认所属账号是否开启**访问密钥保护**。
   - **访问密钥保护**关闭时，所有IAM用户可以管理（包含创建、启用/停用或删除）自己的访问密钥。
   - **访问密钥保护**开启时，仅管理员可以管理用户的访问密钥。
4. 如果您无法管理您的访问密钥，请联系**管理员**：
   - 由管理员管理您的访问密钥，方法请参见：**管理IAM用户的访问密钥**。
   - 请管理员为您配置权限或修改访问密钥保护状态。如需配置权限请参见：**给IAM用户授权**，如需修改访问密钥状态请参见：**访问密钥保护**。

5. 管理员可以在“用户详情”页面查看IAM用户的访问密钥ID（AK），秘密访问密钥（SK）由IAM用户自行保管。

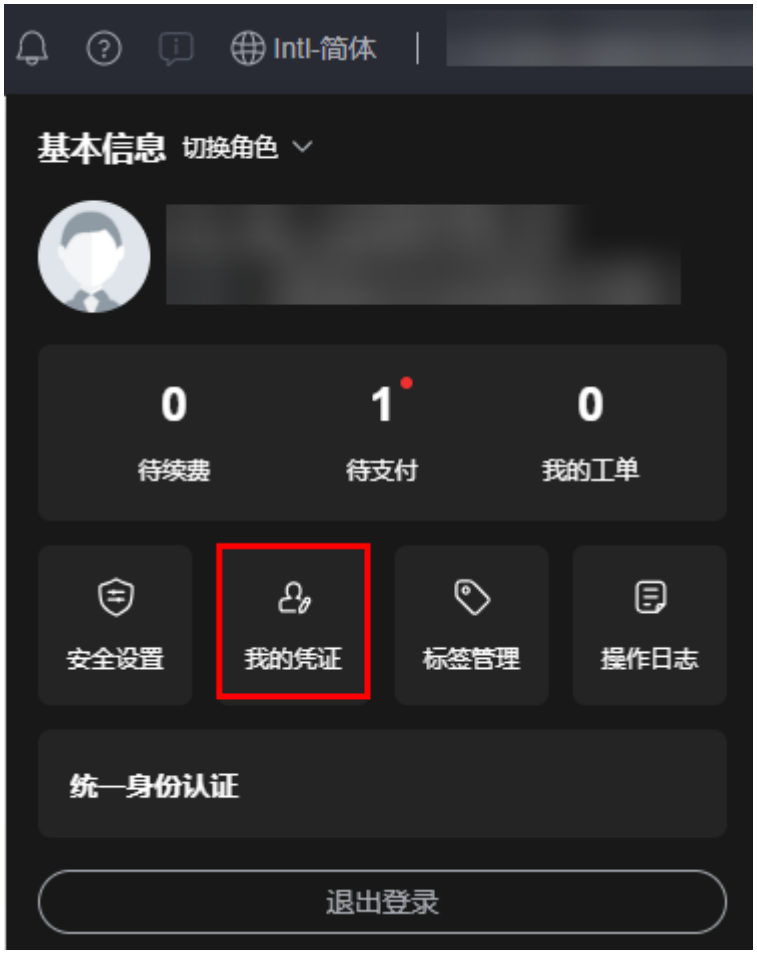
新增访问密钥

步骤1 登录华为云，在右上角单击“控制台”。

图 2-6 进入控制台

步骤2 在“控制台”页面，鼠标移动至右上方的用户名，在下拉列表中选择“我的凭证”。

图 2-7 选择我的凭证



步骤3 在“我的凭证”页面，单击“访问密钥”页签。

步骤4 单击“新增访问密钥”。

如开启操作保护，则创建访问密钥时需要进行身份验证，管理员需输入验证码或密码。

图 2-8 新增访问密钥

说明

- 每个用户最多可创建2个访问密钥，**不支持增加配额**。如果您已拥有2个访问密钥，将无法创建访问密钥。
- 如需修改访问密钥，请删除访问密钥后重新创建。
- 为了保证历史兼容性，我们会使用访问密钥创建时间作为最近使用时间的初始值。在您使用该访问密钥时，系统将自动刷新最近使用时间。

步骤5 单击“立即下载”，生成并下载访问密钥。

创建访问密钥成功后，您可以在访问密钥列表中查看访问密钥ID（AK），在下载的.csv文件中查看访问密钥（SK）。

说明

- 请及时下载保存，弹窗关闭后将无法再次获取该密钥信息，但您可重新创建新的密钥。
- 当您下载访问密钥后，可以在浏览器页面左下角打开格式为.csv的访问密钥文件，或在浏览器“下载内容”中打开。
- 为了账号安全性，建议您妥善保管并定期修改访问密钥，修改访问密钥的方法为删除旧访问密钥，然后重新生成。

----结束

删除访问密钥

当您发现访问密钥被异常使用（包括丢失、泄露等情况），可以在我的凭证中自行删除访问密钥，或者通知管理员在IAM中删除您的访问密钥。

说明

删除操作无法恢复，为保证业务连续性，建议确认访问密钥一周以上未使用后，进行删除操作。

步骤1 在“访问密钥”页签中，在需要删除的访问密钥右侧单击“停用”。

步骤2 单击“确定”，停用访问密钥。

步骤3 停用访问密钥后，单击访问密钥右侧的“删除”。请确保当前IAM用户的访问密钥删除后不会影响业务后再执行删除操作。

如开启操作保护，则删除访问密钥时需要进行身份验证，管理员需输入验证码或密码。

图 2-9 删除访问密钥

步骤4 单击“是”，删除访问密钥。

----结束

启用、停用访问密钥

新创建的访问密钥默认为启用状态，如需停用该访问密钥，步骤如下：

步骤1 在“访问密钥”页签中，在需要停用的访问密钥右侧单击“停用”。

步骤2 单击“是”，停用访问密钥。

----结束

启用访问密钥方式与停用类似，请参考以上步骤。

查看访问密钥

您可以在访问密钥页面查看访问密钥ID、状态、创建时间。

2.4 临时访问密钥（企业联邦用户）

临时访问密钥是**具备临时访问权限**的身份凭证，包含访问密钥ID（AK，Access Key ID）和秘密访问密钥（SK，Secret Access Key）两部分。云服务平台通过AK识别访问用户的身份，通过SK对请求数据进行签名验证，用于确保请求的机密性、完整性和请求者身份的正确性。

我的凭证适用于管理员授权的用户在可以登录控制台的情况下，主动创建、删除自己的**临时访问密钥**。仅企业联邦用户可以在我的凭证创建临时访问密钥，账号和IAM用户请参考： **2.3 访问密钥**。

统一身份认证服务（IAM）同样也可以管理访问密钥，适用于用户不能登录控制台或没有权限访问我的凭证时，由管理员在IAM中为用户管理**永久访问密钥**。

如果您是企业联邦用户，建议使用临时访问密钥。

临时访问密钥与永久访问密钥的差异

临时访问密钥与永久访问密钥的工作方式几乎相同，仅存在小量差异。

- 临时访问密钥存在有效期，可以在15分钟至24小时之间进行设置；永久访问密钥的有效期为永久，并且不能进行设置。
- 临时访问密钥没有数量限制，可以多次生成；每个IAM用户最多可创建2个永久访问密钥。
- 临时访问密钥为动态生成，即时使用，不能嵌入应用程序中，或者进行存储，到期后无法重复使用，只能重新创建，请参考**创建临时访问密钥**。
- 临时访问密钥不支持删除、启用、停用，会在到达有效期时，自动失效并清除；管理员可以在IAM删除、启用、停用用户的永久访问密钥。

注意事项

1. 为了账号安全性，建议您妥善保管并为临时访问密钥设置合适的有效时间。
2. 管理员可以在“用户详情”页面查看IAM用户的访问密钥ID（AK），秘密访问密钥（SK）由IAM用户自行保管。

创建临时访问密钥

步骤1 在“控制台”页面，鼠标移动至右上方的用户名，在下拉列表中选择“我的凭证”。

步骤2 在“我的凭证”页面，单击“临时访问密钥”页签。

步骤3 在页面右上角，选择临时访问密钥有效期，可以在**15分钟至24小时**之间进行设置。

步骤4 单击“操作”列的“创建”，系统生成临时访问密钥。

创建成功后，您可以在访问密钥列表中查看访问密钥ID（AK）、秘密访问密钥（SK）、STS Token。

说明

刷新“临时访问密钥”页面，AK、SK、STS Token内容将被清空，有效期内的临时访问密钥依然有效，建议及时保存访问密钥。

----结束

