

统一身份认证服务

我的凭证

文档版本 08
发布日期 2025-04-28



版权所有 © 华为云计算技术有限公司 2025。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI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。

目 录

1 什么是我的凭证.....	1
2 API 凭证.....	3
3 访问密钥.....	5
4 临时访问密钥（企业联邦用户）.....	9

1 什么是我的凭证

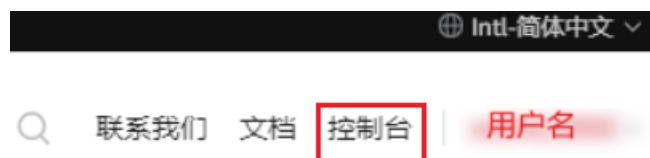
我的凭证是将用户的身份凭证信息进行集中展示与管理的服务。

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 1-1 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 1-2 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 1-1 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：[临时访问密钥（企业联邦用户）](#)。

----结束

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 2-1 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，“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 2-3 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。
- 如果您是企業联邦用户，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

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](#)。

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SecurityToken），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 3-1 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 3-2 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 3-3 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.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 3-4 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。

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：[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**