

目录

目录	1
概述	2
获取AK/SK	2
主账号AK/SK获取	2
子账号AK/SK获取	2

概述

金山云OpenAPI支持以下两种签名算法，您可以根据业务需要选择所使用的签名算法，请注意两种签名算法所使用的公共参数有所区别。（1）简化版签名算法，相比AWS签名算法，签名机制更加简单。

- [公共参数](#)
- [签名算法](#)

（2）AWS签名算法版本4，具体可以参考[AWS文档](#)

- [公共参数](#)
- [签名算法](#)

在构造API请求前，我们需要获取以下信息，用于构造API请求参数。

	信息项	说明
Endpoint	接入地址，格式：{service}.api.ksyun.com 不同服务的接入地址不同，请参考各云服务API文档中 调用方式>请求结构 章节和获取。	
URI	API接口的调用路径及参数。 请参考各云服务API文档中 详细接口 章节获取。	
AK/SK	访问密钥对，包含密钥ID与密钥。AK/SK用于对请求内容进行签名。 获取方式请参考 获取AK/SK ，推荐使用IAM子用户AK/SK。	

获取AK/SK

主账号AccessKey具有本账号内所有产品API的最高权限。一旦泄露将导致极大的安全风险，为保证账号安全，强烈建议您给IAM子用户创建访问密钥，不要给金山云账号（主账号）创建访问密钥。

- 如果已生成过AK/SK，则可跳过此步骤，找到原来已下载的AK/SK的txt文件，文件名一般为：accesskey。文件包括了访问密钥ID（AK）和私有访问密钥（SK）。
- 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，主账号或每个子用户最多可以创建2个AccessKey。

主账号AK/SK获取

1. 主账号登录[金山云控制台](#) 2. 单击右上角用户名，在下拉列表中单击 [Access Keys](#)。 3. 在AK密钥管理页面，单击**新建密钥**。 4. 在风险预警弹窗中，单击**继续使用**，AccessKey创建成功。 5. 您可以点击下载凭证或复制AccessKey信息保存子用户的密钥。

子账号AK/SK获取

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. 在**创建AccessKey**弹窗中，查看AccessKeyID和SecretAccessKey。
6. 您可以点击下载凭证或复制AccessKey信息保存子用户的密钥。