ALIBABA CLOUD

阿里云

IoT固件安全检测
API参考

文档版本：20200901

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.API概览

FSS提供的API包括提交检测任务、获取检测状态、获取检测报告、删除检测任务等。

IoT固件安全检测

API	描述
CreateScanTask	创建检测任务。
QueryTaskStatus	查询任务检测状态，如果使用检测状态通知机制，可不调用该接口。
QueryTaskReport	查询任务检测结果。
DeleteScanTask	删除任务。
QueryLicense	查询当前用户的授权信息。

> **说明** FSS的用户资源（例如检测授权等）绑定在主账号下，使用子账号在FSS中创建检测任务，将消费您主账号下的检测数量。

2.调用方式

本文介绍了用户如何通过API方式进行固件安全检测、检测任务管理。

准备工作：

- 如果还没有获取的AccessKey，请先获取AccessKey。
- 如果使用子账号，请先完成RAM鉴权。
- 检测结果解析，请查看检测结果解析。

引入依赖包

在您的项目中集成SDK，下载FSS OpenAPI SDK，将src/main/java/com/aliyuncs/fss_api文件夹拷贝到您项目中的对应位置。

引入以下包：

```
<dependency>
<groupId>com.aliyun</groupId>
<artifactId>aliyun-java-sdk-core</artifactId>
<version>[version]</version>
</dependency>
```

创建接口调用客户端实例

```
String regionId ="cn-shanghai";
String domain = "fssapi.cn-shanghai.aliyuncs.com";
String akId = "";//您账号的AccessKeyId
String akSecret = "";//您账号的AccessKeySecret
DefaultProfile.addEndpoint(regionId, "Fss-api", domain);
DefaultProfile profile = DefaultProfile.getProfile(regionId, akId, akSecret);
iAcsClient = DefaultAcsClient(profile);
```

创建检测任务

```
CreateScanTaskRequest createScanTaskRequest = new CreateScanTaskRequest();
createScanTaskRequest.setEmail("<your email address>");//邮箱地址用于接收任务检测完成通知
createScanTaskRequest.setFwId("test-fwId");
createScanTaskRequest.setFwName("固件名称");
createScanTaskRequest.setFwVersion("1.0.0");
createScanTaskRequest.setFwUrl("固件的OSS链接地址");
CreateScanTaskResponse cResponse = iAcsClient.getAcsResponse(createScanTaskRequest);
System.out.println("TaskId:"+ cResponse.getData().getTaskId());
System.out.println("Code:"+ cResponse.getCode());
System.out.println("Message:"+ cResponse.getMessage());
```

> 说明 OSS文件的权限应允许：读。

查询任务检测状态

```
QueryTaskStatusRequest queryTaskStatusRequest = new QueryTaskStatusRequest();
queryTaskStatusRequest.setTaskId("<taskId>");//创建检测任务时，返回的任务ID
QueryTaskStatusResponse response = iAcsClient.getAcsResponse(queryTaskStatusRequest);
System.out.println("code："+response.getCode());
System.out.println("description："+response.getData().getDescription());
System.out.println("scannedRate："+response.getData().getScannedRate());
System.out.println("ScanStatus："+response.getData().getScanStatus());
```

查询任务检测结果

```
QueryTaskReportRequest queryTaskReportRequest = new QueryTaskReportRequest();
queryTaskReportRequest.setTaskId("<taskId>");//创建检测任务时，返回的任务ID
QueryTaskReportResponse qtResponse = iAcsClient.getAcsResponse(queryTaskReportRequest);
System.out.println("reportJson："+qtResponse.getData().getReportJson());
System.out.println("reportUrl："+qtResponse.getData().getReportUrl());
```

删除任务

```
DeleteScanTaskRequest deleteScanTaskRequest = new DeleteScanTaskRequest();
deleteScanTaskRequest.setTaskId("<taskId>");//创建检测任务时，返回的任务ID
DeleteScanTaskResponse dResponse = iAcsClient.getAcsResponse(deleteScanTaskRequest);
System.out.println("删除任务："+dResponse.getCode()+":"+dResponse.getMessage());
```

查询主账号授权

```
QueryLicenseRequest queryLicenseRequest = new QueryLicenseRequest();
QueryLicenseResponse qlrResponse = iAcsClient.getAcsResponse(queryLicenseRequest);
System.out.println("MaxCount："+qlrResponse.getData().getMaxCount());
System.out.println("UsedCount："+qlrResponse.getData().getUsedCount());
System.out.println("scanningCount：" + qlrResponse.getData().getScanningCount());
```

3.CreateScanTask

创建一个固件安全检测任务。

请求参数

名称	类型	是否必选	示例值	说明
FwName	String	否	摄像头	固件名称。最大长度为50字节。
FwVersion	String	否	1.0	固件版本号。最大长度为50字节。
FwUrl	String	是	https://fss-store-bins.oss-cn-shanghai.aliyuncs.com/18/91fd9e86f53b4429b68b5266a9cebc78?Expires=1572506923&OSSAccessKeyId=LTxxxxxxxb31QS&Signature=f2deFrds/Aefd	固件文件存储的URL，供FSS检测时下载，目前FSS只支持FwUrl为阿里云OSS存储的链接地址。
Email	String	否	<用户名>@<公司域名>	用于接收固件检测完成通知的邮箱地址。最大长度为128字节。
FwId	String	否	dT7HdBSANYYc9chZRajy84eBCMQAP6MG	用户自定义固件ID，用于标识一个检测任务。可以为空。最大长度为64字节。
DetectionRuleCodes	String	否	CPoC2_3	检测规则，取值可为空值、“BASIC”、“CPoC2_2”、“CPoC2_3”。当不填写该字段或设置为空值时，系统默认以“BASIC”处理。“BASIC”表示基础检测）、“CPoC2_2”表示等保2.0二级检测、“CPoC2_3”表示等保2.0三级检测。

返回参数

名称	类型	示例值	说明
Code	Integer	200	错误码
Message	String	成功	返回提示信息
Data	Struct		返回数据
RequestId	String	A07E3902-B92E-44A6-B6C5-6AA1111111359	为公共参数，每个请求的 ID 都是唯一的，可用于排查和定位问题

Data结构说明

名称	类型	示例值	说明
TaskId	String	cfecd128592941f48c2da09492a47aec	检测任务唯一ID。

返回值

当Code为200时，表示检测任务创建成功。

如果返回300时，表示没有可用的检测数量，您可以在这里

错误码请见“错误码定义”。

4.QueryTaskStatus

用于查询检测任务当前的状态。该接口会逐步弃用，建议使用QueryTaskReportUrls接口获取检测报告。

请求参数

名称	类型	是否必选	示例值	说明
TaskId	String	是	cfecd128592941f48c2da0FFFFFFFFFF	检测任务唯一ID。

返回参数

名称	类型	示例值	说明
Code	Integer	200	错误码。
Message	String	成功	返回提示信息。
Data	Struct	NULL	返回数据。
RequestId	String	A07E3902-B92E-44A6-B6C5-FFFFFFFFFF	为公共参数，每个请求的 ID 都是唯一的，可用于排查和定位问题。

Data结构说明

名称	类型	示例值	说明
ScanStatus	String	SCAN_STATUS_SCAN_COMPLETE	检测状态名称。
Description	String		检测状态描述。
ScannedRate	String	91.3	已完成检测比例。

检测状态说明

状态值	说明
SCAN_STATUS_QUEUING	检测排队中。
SCAN_STATUS_DOWNLOADING	固件下载中。
SCAN_STATUS_DOWNLOAD_FAILED	固件下载失败，为检测结束状态。
SCAN_STATUS_PARSING	固件解析中。
SCAN_STATUS_PARSE_COMPLETE	固件解析完成。
SCAN_STATUS_SCANNING	固件检测中。
RPT_GENERATING	检测报告生成中。
RPT_GENERATE_FAILED	检测报告生成失败，为检测结束状态。
SCAN_STATUS_SCAN_EXCEPTION	固件检测失败，检测出现异常，为检测结束状态。
SCAN_STATUS_SCAN_COMPLETE	固件检测成功，检测完成，为检测结束状态。

说明 当Code为200时，表示查询成功。

当ScanStatus为“SCAN_STATUS_SCAN_COMPLETE”时，调用QueryTaskReport接口获取完整检测报告。

5.QueryTaskReportUrls

查询任务检测结果。

请求参数

名称	类型	是否必选	示例值	说明
TaskId	String	是	cfecd128592941f48c2da09492a47aec	检测任务唯一ID。

返回参数

名称	类型	示例值	说明
Code	Integer	200	错误码
Message	String	成功	返回提示信息
Data	Struct		返回数据
RequestId	String	A07E3902-B92E-44A6-B6C5-6AA1111111359	为公共参数，每个请求的ID 都是唯一的，可用于排查和定位问题

Data结构说明：

名称	类型	示例值	说明
PdfURL	String	http://report.oss-cn-shanghai.aliyuncs.com/baaac03062bbbeab96cf63cccc5f3ddd.pdf?Expires=1597659875	PDF检测报告URL地址链接。
JsonURL	String	http://report.oss-cn-shanghai.aliyuncs.com/baaac03062bbbeab96cf63cccc5f3ddd.json?Expires=1597659875	Json检测报告URL地址链接。
HtmlURL	String	https://fss.iot.aliyun.com/reporthtml/cfecd128592941f48c2da09492a 47aec	HTML检测报告URL地址链接。

当Code为200时，表示查询成功。

错误码请见“错误码定义”一节。

6.QueryTaskReport

用于查询检测任务的结果。

请求参数

名称	类型	是否必选	示例值	说明
TaskId	String	是	cfecd128592941f48cFFFFFFFFFFFF	检测任务唯一ID。

返回参数

名称	类型	示例值	说明
Code	Integer	200	错误码。返回200表示成功。
Message	String	成功	返回提示信息。
Data	Struct		返回数据。
RequestId	String	A07E3902-B92E-44A6-B6C5-FFFFFFFFFFFF	为公共参数，每个请求的ID 都是唯一的，可用于排查和定位问题。

Data结构说明：

名称	类型	示例值	说明
ReportJson	String	参考“检测结果格式”	检测结果，以JSON格式存储。详细格式见“检测结果格式”一节。
ReportUrl	String	https://fss.iot.aliyun.com/reporthtml/FFFFFFFFFFFF	检测报告URL地址。

> **说明** 当Code为200时，表示查询成功。

7.DeleteScanTask

用于删除指定TaskId的检测任务。

请求参数

名称	类型	是否必选	示例值	说明
TaskId	String	是	cfecd128592941f48c2da09492a47aec	检测任务唯一ID。

返回参数

名称	类型	示例值	说明
Code	Integer	200	错误码。返回200表示成功；返回304表示未找到该任务。
Message	String	成功	返回提示信息。
RequestId	String	A07E3902-B92E-44A6-B6C5-6AA1111111359	为公共参数，每个请求的 ID 都是唯一的，可用于排查和定位问题。

8.QueryLicense

查询主账号的授权信息。

请求参数

无。

返回参数

名称	类型	示例值	说明
Code	Integer	200	错误码。返回200表示成功。
Message	String	成功	返回提示信息。
Data	Struct		返回数据。
RequestId	String	A07E3902-B92E-44A6-B6C5-FFFFFFFFFFFF	为公共参数，每个请求的 ID 都是唯一的，可用于排查和定位问题。

Data结构说明：

名称	类型	示例值	说明
UsedCount	Integer	10	已使用检测授权数量。
MaxCount	Integer	100	总授权检测授权数量。
ScanningCount	Integer	1	正在检测中的任务数量（包括正在排队中的任务）。

9.检测结果解析

这篇文档介绍了如何解析FSS的检测结果，检测结果以JSON格式存储。

检测结果的组成

检测结果分为三部分固件基本信息、检测结果统计和检测风险列表。例如：

```
{
"fwBasicInfo": { //固件基本信息
"fwFileSize": 0,
"arch": "",
"fwSha256": "",
"filesystem": "",
"scanStartTime": 0
},
"riskStatistics": { //检测结果统计
"severityStatistics": [ //风险等级漏洞数统计
{ "name": "严重", "count": 0 },
{ "name": "高危", "count": 0 },
{ "name": "中危", "count": 0 },
{ "name": "低危", "count": 0 },
{ "name": "通告", "count": 0 }
],
"riskBrief": [ //按风险等级及分类统计
{
"risks": [{"riskType": "", "suggestion": "", "count": 0, "description": ""}],
"name": "严重", "count": 0
}
]
},
"risks": [ //检测风险列表
{
"name": "", "code": "", "enCategory": "", "category": "",
"description": "", "suggestion": "",
"vulnInfos": [
{
"severity": "", "filename": "",
"detail": [],
"cve": {}
}
]
}
]
}
```

固件基本信息

基本信息的key为“fwBasicInfo”，类型为JSONObject。格式为：

```
"fwBasicInfo": {
"fwFileSize": 0,
"arch": "",
"fwSha256": "",
"filesystem": "",
"scanStartTime": 0
}
```

字段定义参考：

字段名	类型	说明
fwFileSize	long	固件文件大小
arch	String	固件的CPU体系
fwSha256	String	固件文件的SHA256
filesystem	String	固件的文件系统
scanStartTime	Date	检测时间

检测结果统计

检测结果统计的key为“riskStatistics”，类型为JSONObject。格式为：

```
"riskStatistics": {
"severityStatistics": [ //风险等级漏洞数统计
{ "name": "严重", "count": 0 },
{ "name": "高危", "count": 0 },
{ "name": "中危", "count": 0 },
{ "name": "低危", "count": 0 },
{ "name": "通告", "count": 0 }
],
"riskBrief": [ //按风险等级及分类统计
{
"risks": [{"riskType": "", "suggestion": "", "count": 0, "description": ""}],
"name": "严重", "count": 0
}
]
}
```

检测结果统计分为2部分：

1）风险等级漏洞数统计：按风险等级统计的当前固件风险结果，风险等级分为严重、高危、中危、低危和通告。key为severityStatistics，类型为JSONArray，每个item格式为：

字段名	类型	说明
name	String	风险等级名
count	int	风险数量

2）按风险等级及分类统计：按风险等级及分类统计的当前固件风险结果，每个风险等级下检测到了哪些风险类型及风险数量等。 key为riskBrief，类型为JSONArray，每个item格式为：

字段名	类型	说明
name	String	风险等级名
count	int	风险数量
risks	JSONArray	风险列表

risks格式为：

字段名	类型	说明
riskType	String	风险类型名
count	int	风险数量
description	String	风险描述
suggestion	String	描述修复紧急程度

检测风险列表

检测结果统计的key为“risks”，类型为JSONArray，格式如下：

```
"risks": [
{
"name": "", "code": "", "enCategory": "", "category": "",
"description": "", "suggestion": "",
"vulnInfos": [
{
"severity": "", "filename": "",
"detail": [],
"cve": {}
}
]
}
]
```

字段定义如下：

字段	类型	描述
name	String	风险类型中文名称
code	String	风险类型英文名称或风险类型代码
category	String	风险类型分组中文名称
enCategory	String	风险类型分组英文名称
description	String	风险描述
suggestion	String	修复建议
vulnInfos	JSONArray<VulnInfo>	风险详细情况列表

VulnInfo定义如下：

字段	类型	描述
filename	String	受影响的文件名
severity	String	风险安全等级
detail	JSONArray	风险详细描述，不同风险描述也不相同
cve	JSONObject	CVE漏洞列表，只有当前分组为CVE漏洞（CveVuln），该字段才有效。

detail字段，保存检测到的非CVE漏洞的详细信息，定义如下：

字段	类型	描述
cnName	String	详细信息的中文描述名
enName	String	详细信息的英文描述名
value	JSONArray<String>	风险详细信息，以JSONArray<String>存储。

cve字段，保存检测到的CVE漏洞的详细信息，定义如下：

字段	类型	描述
cveId	String	CVE漏洞标识
cweId	String	CVE漏洞类型标识
impact	JSONObject	定义漏洞攻击向量、风险等级等。优先使用cvssV3，其中vectorString为攻击向量、severity为风险等级。
cpe	JSONObject	为Common Platform Enumeration的缩写，描述软硬件产品的唯一标识符。 参考下面的cpe结构说明。
description	String	漏洞描述信息。
references	JSONArray<JSONObject>	参考信息。其中referenceType为参考类型，referenceSource为参考源，referenceUrl为参考链接地址。

cpe结构说明：

```
"cpe": {
"cpeName": "",
"cpeType": "",
"allFixedVersion": {
"expression": "",
"version": ""
},
"highCriticalFixedVersion": {
"expression": "",
"version": ""
}
}
```

说明 其中cpeName为cpe名称，cpeType 为cpe类型。

allFixedVersion为修复当前版本所有漏洞，需要升级到的版本建议。其中version表示版本号，expression表示version包含关系，如果为“>”表示需要升级到在大于version的版本；如果为”>=“表示需要升级到在大于或等于version的版本。

如果version为空，表示目前还没有可用的修复版本号。highCriticalFixedVersion，为修复当前版本中严重、高危漏洞，需要升级到的版本建议。

10.错误码定义

FSS使用过程中可能遇到的错误码。

错误码

Code	描述
0	未分配
200	成功
300	没有可用的检测数量
307	文件大小超出最大限制
303	此文件已存在
304	未找到该任务
308	任务创建失败
350	账户状态异常
352	主账户未实人认证
356	不支持的账号类型
357	账号没有操作权限
450	无效的链接
453	任务检测未完成
500	服务异常
600	请求参数错误
601	不支持的文件类型
603	邮箱格式不正确
606	不支持的操作
900	未知错误

11.RAM鉴权

在使用RAM账号调用 IoT固件安全检测（FSS）API前，需要主账号通过创建授权策略对RAM账号进行授权。在授权策略中，使用资源描述符（Alibaba Cloud Resource Name, ARN）指定授权资源。

可授权的资源类型

在进行RAM子账号授权时，FSS的权限描述如下：

权限策略名称	备注
AliyunFSSFullAccess	管理IoT固件安全检测（FSS）的权限。
AliyunFssReadOnlyAccess	只读访问IoT固件安全检测（FSS）的权限。

关于创建RAM用户的具体操作步骤，请参见创建RAM用户

12.获取AccessKey

您可以为阿里云主账号和子账号创建一个访问密钥（AccessKey）。在调用阿里云API时您需要使用AccessKey完成身份验证。

背景信息

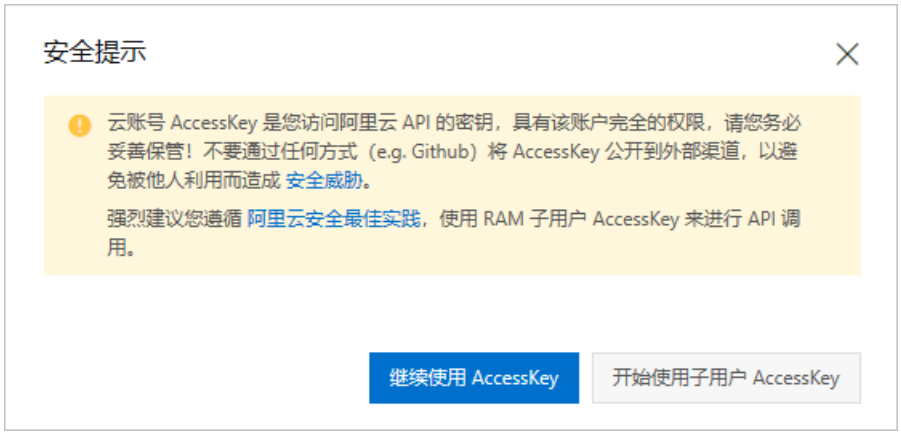
AccessKey包括AccessKey ID和AccessKey Secret。

- AccessKeyId：用于标识用户。
- AccessKeySecret：用于验证用户的密钥。AccessKeySecret必须保密。

> **警告** 主账号Accesskey泄露会威胁您所有资源的安全。建议使用子账号（RAM用户）Accesskey进行操作，可以有效降低Accesskey泄露的风险。

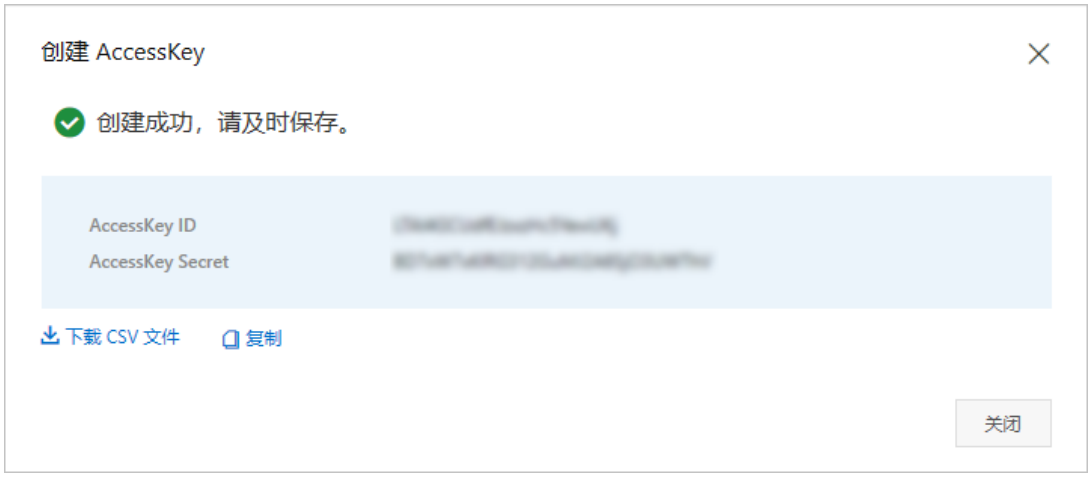
操作步骤

1. 以主账号登录阿里云管理控制台。
2. 将鼠标置于页面右上方的账号图标，单击accesskeys。
3. 在安全提示页面，选择获取主账号还是子账号的Accesskey。



4. 获取账号Accesskey。
   - 获取主账号AccessKey
     a. 单击继续使用AccessKey。
     b. 在安全信息管理页面，单击创建AccessKey。
     c. 在手机验证页面，获取验证码，完成手机验证，单击确定。

d. 在**新建用户AccessKey**页面，展开**AccessKey详情**，查看AccessKeyId和AccessKeySecret。可以单击**保存AK信息**，下载AccessKey信息。



- 获取子账号AccessKey
  a. 单击**开始使用子用户AccessKey**。
  b. 如果未创建RAM用户，在系统跳转的RAM访问控制台的**新建用户**页面，创建RAM用户。如果是获取已有RAM用户的Accesskey，则跳过此步骤。
  c. 在RAM访问控制台的左侧导航栏，选择**人员管理 > 用户**，搜索需要获取AccessKey的用户。
  d. 单击用户登录名称，在用户详情页**认证管理**页签下的**用户AccessKey**区域，单击**创建新的AccessKey**
  e. 在**手机验证**页面，获取验证码，完成手机验证，单击**确定**。
  f. 在**创建AccessKey**页面，查看AccessKeyId和AccessKeySecret。可以单击**下载CSV文件**，下载AccessKey信息或者单击**复制**，复制AccessKey信息。