

阿里云 视觉智能开放平台

权限控制

文档版本：20200624

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. 阿里云文档中所有内容，包括但不限于图片、架构设计、页面布局、文字描述，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
	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。	 禁止： 重置操作将丢失用户配置数据。
	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。
	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。
	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。	执行 <code>cd /d C:/window</code> 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	<code>bae log list --instanceid Instance_ID</code>
[]或者[a b]	表示可选项，至多选择一个。	<code>ipconfig [-all]-t</code>
{ }或者[a b]	表示必选项，至多选择一个。	<code>switch {active stand}</code>

目录

法律声明.....	I
通用约定.....	I
1 使用RAM Policy控制访问权限.....	1

1 使用RAM Policy控制访问权限

为RAM用户授权后，RAM用户就可以使用阿里云视觉智能开放平台的相关服务。

授权操作步骤

1. 登录[RAM控制台](#)。

2. 新建RAM用户。

详细操作步骤请参见[#unique_4](#)。

3. 新建权限策略。

新建权限策略时请使用[脚本配置](#)的配置模式。细粒度授权设置支持：[IP段](#)、[时间](#)、[MFA](#)、[角色STS](#)。关于新建权限策略操作请参见[#unique_5](#)。

4. 为用户进行授权。

详细授权操作请参见[#unique_6](#)。

全部权限

- 方式一：直接授予用户系统权限策略**AliyunVIAPIFullAccess**（管理视觉智能API的权限）。
- 方式二：自定义权限。拥有视觉智能所有能力的全部权限，policy定义如下所示。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "viapi-imageenhan:*",
      "Resource": "acs:viapi-imageenhan:*:*:*"
    },
    {
      "Effect": "Allow",
      "Action": "viapi-imagerecog:*",
      "Resource": "acs:viapi-imagerecog:*:*:*"
    },
    {
      "Effect": "Allow",
      "Action": "viapi-imageseg:*",
      "Resource": "acs:viapi-imageseg:*:*:*"
    },
    {
      "Effect": "Allow",
      "Action": "viapi-imageaudit:*",
      "Resource": "acs:viapi-imageaudit:*:*:*"
    },
    {
      "Effect": "Allow",
      "Action": "viapi-ocr:*",
      "Resource": "acs:viapi-ocr:*:*:*"
    },
    {
      "Effect": "Allow",
      "Action": "viapi-facebody:*",
```

```
    "Resource": "acs:viapi-facebody:*:*:*"
  },
  {
    "Effect": "Allow",
    "Action": "viapi-objectdet:*",
    "Resource": "acs:viapi-objectdet:*:*:*"
  },
  {
    "Effect": "Allow",
    "Action": "viapi-goodstech:*",
    "Resource": "acs:viapi-goodstech:*:*:*"
  }
],
"Version": "1"
}
```

IP/SSL限制

支持带IP/SSL限制的授权。该授权策略在满足以下两个条件时可以访问所有资源。

- RAM用户当前的IP网段为42.120.99.0/24。
- RAM用户正在使用HTTPS访问阿里云控制台或OpenAPI。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "viapi-imageenhan:*",
      "Resource": "acs:viapi-imageenhan:*:*:*",
      "Condition": {
        "IpAddress": {
          "acs:SourceIp": "42.120.99.0/24"
        },
        "Bool": {
          "acs:SecureTransport": "true"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "viapi-imagerecog:*",
      "Resource": "acs:viapi-imagerecog:*:*:*",
      "Condition": {
        "IpAddress": {
          "acs:SourceIp": "42.120.99.0/24"
        },
        "Bool": {
          "acs:SecureTransport": "true"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "viapi-imageseg:*",
      "Resource": "acs:viapi-imageseg:*:*:*",
      "Condition": {
        "IpAddress": {
          "acs:SourceIp": "42.120.99.0/24"
        },
        "Bool": {
```

```
"acs:SecureTransport": "true"
}
}
},
{
  "Effect": "Allow",
  "Action": "viapi-imageaudit:*",
  "Resource": "acs:viapi-imageaudit:*:*:*",
  "Condition": {
    "IpAddress": {
      "acs:SourceIp": "42.120.99.0/24"
    },
    "Bool": {
      "acs:SecureTransport": "true"
    }
  }
}
},
{
  "Effect": "Allow",
  "Action": "viapi-ocr:*",
  "Resource": "acs:viapi-ocr:*:*:*",
  "Condition": {
    "IpAddress": {
      "acs:SourceIp": "42.120.99.0/24"
    },
    "Bool": {
      "acs:SecureTransport": "true"
    }
  }
}
},
{
  "Effect": "Allow",
  "Action": "viapi-facebody:*",
  "Resource": "acs:viapi-facebody:*:*:*",
  "Condition": {
    "IpAddress": {
      "acs:SourceIp": "42.120.99.0/24"
    },
    "Bool": {
      "acs:SecureTransport": "true"
    }
  }
}
},
{
  "Effect": "Allow",
  "Action": "viapi-objectdet:*",
  "Resource": "acs:viapi-objectdet:*:*:*",
  "Condition": {
    "IpAddress": {
      "acs:SourceIp": "42.120.99.0/24"
    },
    "Bool": {
      "acs:SecureTransport": "true"
    }
  }
}
},
{
  "Effect": "Allow",
  "Action": "viapi-goodstech:*",
  "Resource": "acs:viapi-goodstech:*:*:*",
  "Condition": {
    "IpAddress": {
      "acs:SourceIp": "42.120.99.0/24"
    },

```

```
    "Bool": {
      "acs:SecureTransport": "true"
    }
  }
},
"Version": "1"
}
```

时间限制

该授权策略的含义是：在北京时间2019年09月25日下午12:30之前，RAM用户拥有IVPD的所有权限。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "viapi-imageenhan:*",
      "Resource": "acs:viapi-imageenhan:*:*:*",
      "Condition": {
        "DateLessThan": {
          "acs:CurrentTime": "2019-09-25T12:30:00+08:00"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "viapi-imagerecog:*",
      "Resource": "acs:viapi-imagerecog:*:*:*",
      "Condition": {
        "DateLessThan": {
          "acs:CurrentTime": "2019-09-25T12:30:00+08:00"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "viapi-imageseg:*",
      "Resource": "acs:viapi-imageseg:*:*:*",
      "Condition": {
        "DateLessThan": {
          "acs:CurrentTime": "2019-09-25T12:30:00+08:00"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "viapi-imageaudit:*",
      "Resource": "acs:viapi-imageaudit:*:*:*",
      "Condition": {
        "DateLessThan": {
          "acs:CurrentTime": "2019-09-25T12:30:00+08:00"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "viapi-ocr:*",
      "Resource": "acs:viapi-ocr:*:*:*",
      "Condition": {
```



```
    "DateLessThan": {
      "acs:CurrentTime": "2019-09-25T12:30:00+08:00"
    }
  },
  {
    "Effect": "Allow",
    "Action": "viapi-facebody:*",
    "Resource": "acs:viapi-facebody:*:*:*",
    "Condition": {
      "DateLessThan": {
        "acs:CurrentTime": "2019-09-25T12:30:00+08:00"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": "viapi-objectdet:*",
    "Resource": "acs:viapi-objectdet:*:*:*",
    "Condition": {
      "DateLessThan": {
        "acs:CurrentTime": "2019-09-25T12:30:00+08:00"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": "viapi-goodstech:*",
    "Resource": "acs:viapi-goodstech:*:*:*",
    "Condition": {
      "DateLessThan": {
        "acs:CurrentTime": "2019-09-25T12:30:00+08:00"
      }
    }
  }
],
"Version": "1"
}
```

MFA

如果一个RAM用户仅被授予该授权策略，那么只有当该RAM用户启用MFA并使用MFA登录时，才具有IVPD的权限。此RAM用户的AK也没有权限，需要使用AK+正确的MFA六位Code调用STS服务获取一个临时AK（15分钟失效），此临时AK才具有相应的权限。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "viapi-imageenhan:*",
      "Resource": "acs:viapi-imageenhan:*:*:*",
      "Condition": {
        "Bool": {
          "acs:MFAPresent": "true"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "viapi-imagerecog:*",
```

```
"Resource": "acs:viapi-imagerecog:*:*:*",
"Condition": {
  "Bool": {
    "acs:MFAPresent": "true"
  }
},
{
  "Effect": "Allow",
  "Action": "viapi-imageseg:*",
  "Resource": "acs:viapi-imageseg:*:*:*",
  "Condition": {
    "Bool": {
      "acs:MFAPresent": "true"
    }
  }
},
{
  "Effect": "Allow",
  "Action": "viapi-imageaudit:*",
  "Resource": "acs:viapi-imageaudit:*:*:*",
  "Condition": {
    "Bool": {
      "acs:MFAPresent": "true"
    }
  }
},
{
  "Effect": "Allow",
  "Action": "viapi-ocr:*",
  "Resource": "acs:viapi-ocr:*:*:*",
  "Condition": {
    "Bool": {
      "acs:MFAPresent": "true"
    }
  }
},
{
  "Effect": "Allow",
  "Action": "viapi-facebody:*",
  "Resource": "acs:viapi-facebody:*:*:*",
  "Condition": {
    "Bool": {
      "acs:MFAPresent": "true"
    }
  }
},
{
  "Effect": "Allow",
  "Action": "viapi-objectdet:*",
  "Resource": "acs:viapi-objectdet:*:*:*",
  "Condition": {
    "Bool": {
      "acs:MFAPresent": "true"
    }
  }
},
{
  "Effect": "Allow",
  "Action": "viapi-goodstech:*",
  "Resource": "acs:viapi-goodstech:*:*:*",
  "Condition": {
    "Bool": {
      "acs:MFAPresent": "true"
    }
  }
}
```

```
}  
}  
}  
},  
"Version": "1"  
}
```

控制台角色STS

STS Token是一种临时身份，用来解决跨帐号及跨服务的资源访问的问题。STS Token由以下三部分组成：

- AccessKeyId
 - AccessKeySecret
 - SecurityToken
1. 在RAM控制台创建本账户的RAM角色，并为该角色授予该产品的管理权限或者AdministratorAccess。
 2. 创建一个RAM用户，给RAM用户授予AliyunSTSAssumeRoleAccess权限。
 3. 用创建的RAM用户登录[RAM控制台](#)。
 4. 将鼠标悬停在右上角头像的位置，查看**企业别名**并保存。
 5. 单击**切换身份**。
 6. 在**角色切换**页面，输入已保存的企业别名和步骤1创建的角色名。



说明：

如果没有别名，输入主账户ID。

7. 切换到角色后，在浏览器里输入产品控制台的地址。