# 天御业务安全防护

# 活动防刷

# 产品文档

腾讯云

# 文档目录

# 活动防刷
# 活动防刷产品简介

最近更新时间：2018-05-14 11:13:42

## 1. 天御活动防刷是什么

近年来电商、O2O 等行业用高额补贴、优惠等方式获取用户，同时也催生了“羊毛党”。“羊毛党”有选择性地参加线上活动，以零或者相对较低的成本获取物质优惠，严重破坏了活动目的、侵占了活动资源，使企业获取用户的成本提升、口碑和形象受损。因此，天御推出针对“羊毛党”的活动防刷服务，基于腾讯海量大数据分析用户的行为和账号的风险等级，有效地识别出“羊毛党”，保障企业利益。

## 2. 天御活动防刷的优势

### 2.1 完善的服务体系

快速部署服务体系，前期专业的恶意诊断，提供最优安全策略，后期重大活动专人跟进，全面分析实时数据报表。

### 2.2 腾讯同款安全服务

天御防刷服务已为腾讯多款产品和业务提供完善的帐号保护体系，经历了数亿用户十年的考验。

# 活动防刷购买指南

最近更新时间：2018-09-25 16:39:33

| 每日防护上限 | 包月价格（包年价格 = 包月价格 * 10） |
| --- | --- |
| 10 万次 | 1.5 万元 |
| 20 万次 | 3.0 万元 |
| 50 万次 | 6.0 万元 |
| 100 万次 | 12.0 万元 |
| 200 万次 | 24.0 万元 |

（注：每分钟防护峰值即每日的防护上限）

天御各服务对已企业认证的用户提供 7 天免费体验（包含 1000 次调用）。体验服务结束后，您可以通过购买对应套餐继续享受安全服务。若线上套餐仍不能满足您的需求，可通过 工单 联系我们提供定制报价。

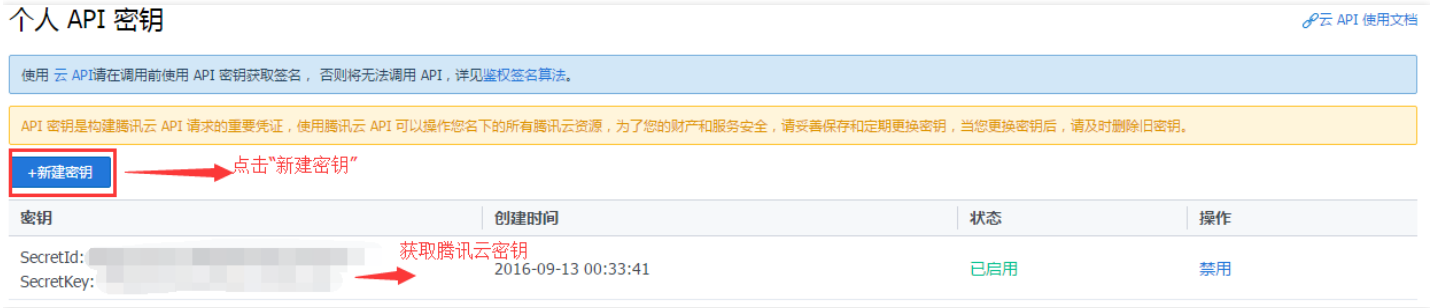
# 活动防刷开发指引

最近更新时间：2018-05-30 15:47:37


开发者需要通过调用云API的天御相关接口完成接入，接入API步骤如下：

## 1. 获取腾讯云密钥

如果您已经具有了腾讯云密钥则可以跳过这一步。进入云API密钥，选择"API密钥"，单击"新建密钥"。




## 2. 进入天御业务安全防护管理中心

进入管理中心->云产品->天御业务安全防护。


# 3. 申请权限

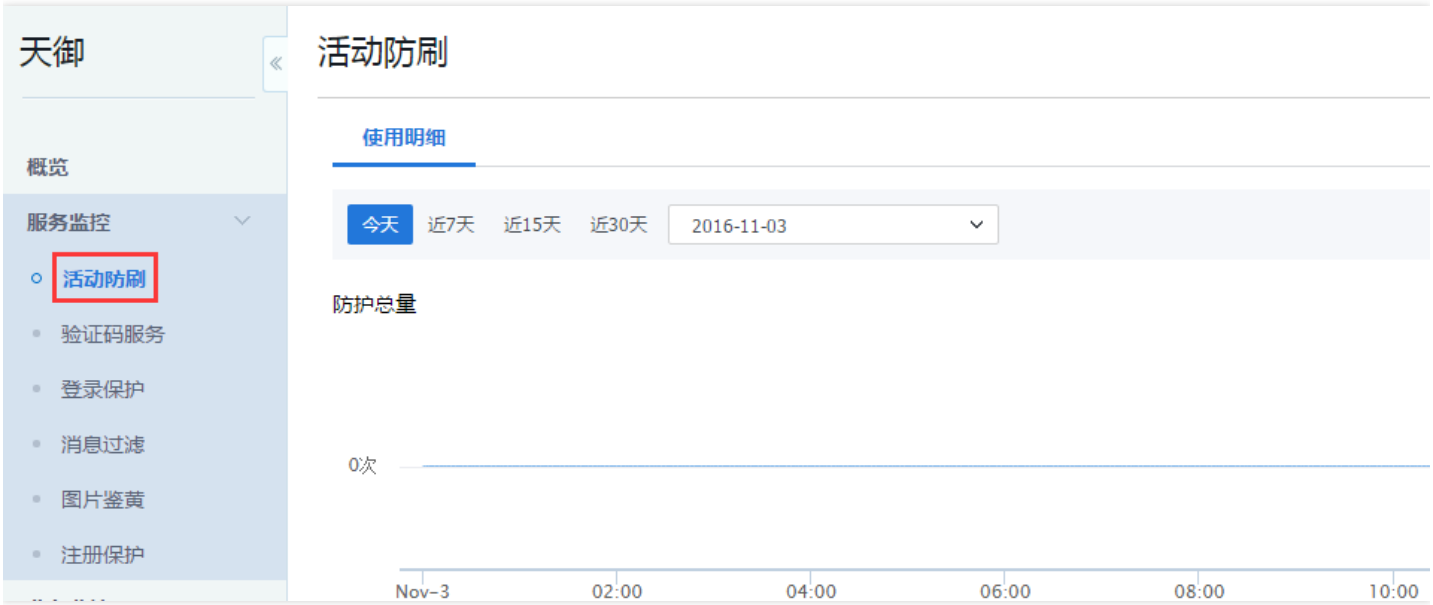
在天御业务安全防护管理中心中单击"活动防刷服务"免费体验，确定开通。


# 4. 按照指定API写代码

活动防刷API

# 5. 查询调用数据

进入天御业务安全防护管理中心，选择“服务监控”，即可查询到对应服务的调用数据。



# 活动防刷API文档

最近更新时间：2018-05-30 15:46:11

## 1. 接口描述

活动防刷接口提供抢券、红包分发、游戏道具、刷榜等活动中用户恶意行为判断能力，根据当前用户的账号、信用、行为判断用户当前操作的恶意等级。

协议：HTTPS

域名：csec.api.qcloud.com

接口名：ActivityAntiRush

## 2. 输入参数

以下请求参数列表仅列出了接口请求参数，正式调用时需要加上公共请求参数，见公共请求参数页面。其中，此接口的Action字段为ActivityAntiRush。

| 参数名称 | 是否必须 | 类型 | 描述 |
| --- | --- | --- | --- |
| accountType | 必选 | UInt | 用户账号类型<br>1：QQ开放帐号<br>2：微信开放账号<br>4：手机号<br>0：其他<br>10004： 手机号MD5 |
| uid | 必选 | String | 用户ID<br>accountType不同对应不同的用户ID。如果是QQ或微信用户，则填入对应的openid；若是手机号，则填入对应的手机号（如 15912345687） |
| userIp | 必选 | String | 用户的外网IP |
| postTime | 必选 | UInt | 用户操作时间戳，单位秒（格林威治时间精确到秒，如1501590972） |
| appId | 可选 | String | accountType是QQ或微信开放账号时，该参数必填，表示QQ或微信分配给给网站或应用的appId，用来唯一标识网站 |

| | | | |
|---|---|---|---|
| | | | 或应用 |
| associateAccount | 可选 | String | accountType是QQ或微信开放账号时，用于标识QQ或微信用户登录后关联业务自身的账号ID |
| nickName | 可选 | String | 昵称，utf8编码 |
| phoneNumber | 可选 | String | 手机号。若accoutType 选4（手机号）、或10004（手机号MD5），则无需重复填写。否则填入对应的手机号（如15912345687） |
| emailAddress | 可选 | String | 用户邮箱地址（非系统自动生成） |
| registerTime | 可选 | UInt | 注册时间戳，单位秒 |
| registerIp | 可选 | String | 注册来源的外网IP |
| cookieHash | 可选 | String | 用户Http请求中的cookie进行2次hash的值，只要保证相同cookie的hash值一致即可 |
| passwordHash | 可选 | String | 用户密码进行2次hash的值，只要保证相同密码hash值一致即可 |
| loginSource | 可选 | UInt | 登录来源<br>0：其他<br>1：PC网页<br>2：移动页面<br>3：APP<br>4：微信公众号 |
| loginType | 可选 | UInt | 登录方式<br>0：其他<br>1：手动帐号密码输入<br>2：动态短信密码登录<br>3：二维码扫描登录 |
| loginSpend | 可选 | UInt | 登录耗时，单位秒 |
| rootId | 可选 | String | 用户操作的目的ID<br>比如：点赞，该字段就是被点 赞的消息 id，如果是投票，就是被投号码的 ID |
| referer | 可选 | String | 用户Http请求的referer值 |
| jumpUrl | 可选 | String | 登录成功后跳转页面 |
| userAgent | 可选 | String | 用户Http请求的userAgent |
| | | | |

| | | | |
|---|---|---|---|
| xForwardedFor | 可选 | String | 用户Http请求中的x_forward_for |
| mouseClickCount | 可选 | UInt | 用户操作过程中鼠标单击次数 |
| keyboardClickCount | 可选 | UInt | 用户操作过程中鼠标单击次数 |
| macAddress | 可选 | String | mac地址或设备唯一标识 |
| vendorId | 可选 | String | 手机制造商ID，如果手机注册，请带上此信息 |
| imei | 可选 | String | 手机设备号 |
| appVersion | 可选 | String | APP客户端版本 |
| businessId | 可选 | UInt | 业务ID<br>网站或应用在多个业务中使用此服务，通过此ID区分统计数据 |

## 3. 输出参数

| 参数名称 | 类型 | 描述 |
|---|---|---|
| code | Int | 返回码 |
| codeDesc | String | 业务侧错误码。成功时返回Success，错误时返回具体业务错误原因。 |
| message | String | UTF-8编码，出错消息 |
| Nonce | UInt | 随机正整数，与 Timestamp 联合起来, 用于防止重放攻击（公共参数） |
| associateAccount | String | accountType是QQ或微信开放账号时，用于标识QQ或微信用户登录后关联业务自身的账号ID |
| postTime | String | 操作时间戳，单位秒 |
| uid | String | 用户ID<br>accountType不同对应不同的用户ID。如果是QQ或微信用户则填入对应的openId |
| rootId | String | 用户操作的目的ID<br>比如：点赞，该字段就是被点 赞的消息 id，如果是投票，就是被投号码的 ID |
| userIp | String | 操作来源的外网IP |
| level | Int | 0：表示无恶意<br>1～4：恶意等级由低到高 |

| riskType | Array | 风险类型 |
| --- | --- | --- |

riskType详细说明

| 风险类型 | 风险详情 | 风险码 |
| --- | --- | --- |
| 账号风险 | 帐号信用低 | 1 |
| | 垃圾帐号 | 2 |
| | 无效帐号 | 3 |
| | 黑名单 | 4 |
| 行为风险 | 批量操作 | 101 |
| | 自动机 | 102 |
| 环境风险 | 环境异常 | 201 |
| | js上报异常 | 202 |
| | 撞库 | 203 |

# 4. 示例代码

代码下载： Python示例 PHP示例 Java示例 .Net示例

一个完整的请求需要两类请求参数：公共请求参数和接口请求参数。这里只列出了接口请求参数，并未列出公共请求参数，有关公共请求参数的说明可见公共请求参数小节。

请求示例 ：
<https://csec.api.qcloud.com/v2/index.php?Action=ActivityAntiRush
&<公共请求参数>
&secretId=AKIDmQtAxYTAB2iBS8s2DCzazCD2g7OUq4Zw
&accountType=1
&uid=D692D87319F2098C3877C3904B304706
&userIp=127.0.0.1
&postTime=11254

# 5. 响应示例

```
{
"Nonce":516529719,
"associateAccount":"373909726",
"code":0,"
level":1,
"message":"NoError",
"postTime":"11254",
"rootId":"sdsds234sd",
"uid":"D692D87319F2098C3877C3904B304706",
"userIp":"10.23.23.20"
"riskType":[1]
}
```


## 6.错误码说明

参考返回的message字段描述

# 天御打击羊毛党方案

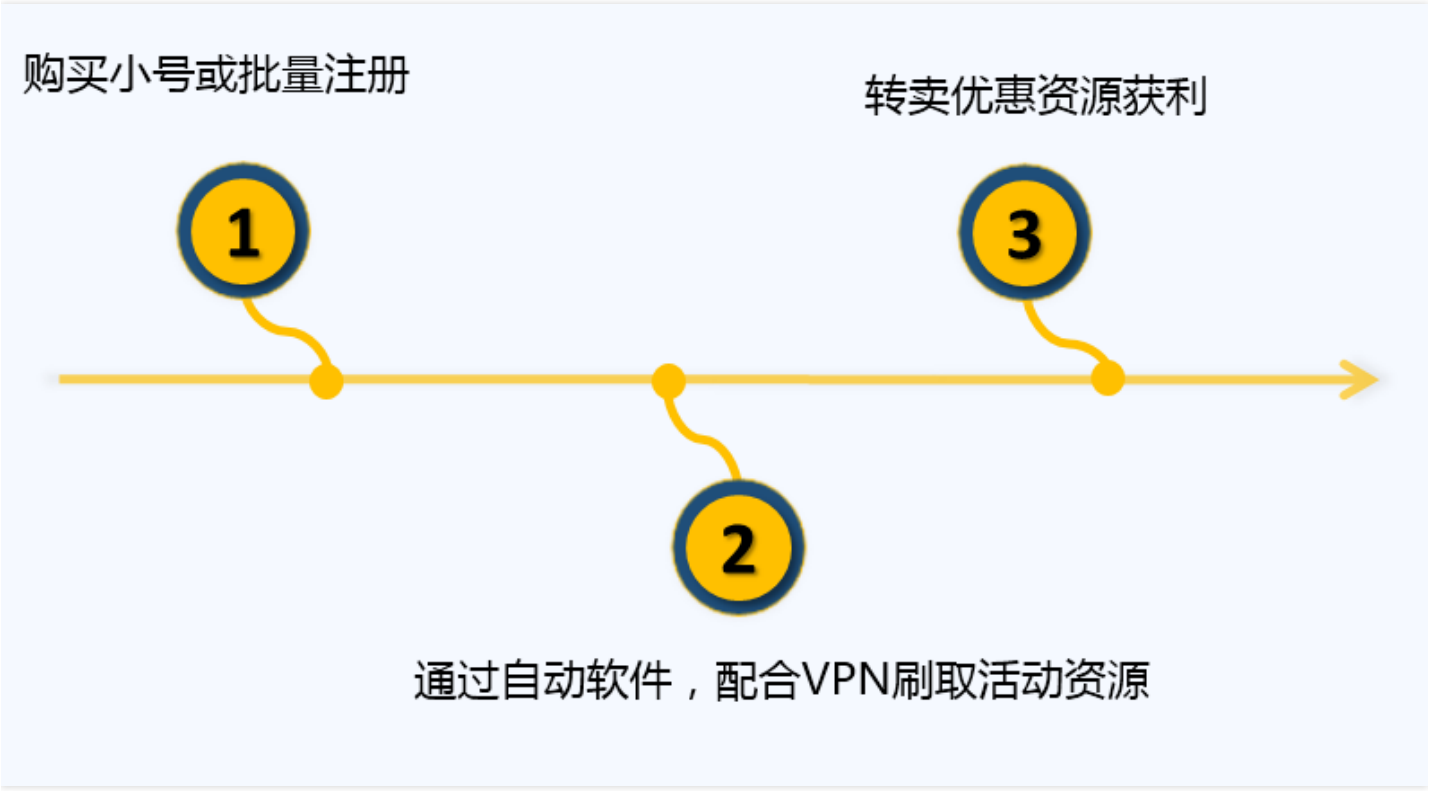
最近更新时间：2017-03-09 04:20:15

## 1. 背景介绍

最近1 ~2年电商行业飞速发展，各路人马包括大量的创业公司都在O2O这一领域深挖、布局，都想抢占这个一个万亿级的市场先机，商家不惜通过各种活动形式的高额补贴来获取用户、培养用户的消费习惯。整个行业的补贴可以说是放血式的，一张优惠券少则几块多则几十块，尤其是P2P理财更高达上百块，根据之前一家权威媒体的估计，打车行业因为补贴亏损高达29亿，团购行业28亿，都处于大幅度投入期。但是，高额的补贴、优惠在获取用户的同时了也催生了“羊毛党”。“羊毛党”有选择性的参加线上的活动，从而以相对较低或者零成本获取物质上的优惠，他们的行为距离欺诈只有一步之遥，他们严重破坏了活动的目的、侵占了活动的资源，使得企业获取用户的成本在提升、损坏企业口碑和形象；因此，针对“羊毛党”的打击势在必行。

## 2. 羊毛党现状

“羊毛党”一般先利用自动机注册大量的目标网站的账号，当目标网站搞促销、优惠等活动的时候，利用这些账号参与活动刷取较多的优惠，最后通过各类平台转卖获益，“羊毛党”获利基本过程如图所示：



# 3. 天御对抗思路

一般的活动，都会限制一个账号的参与次数，要想获取高额的收益，“羊毛党”就必须掌握大量的虚假账号。因此，对抗的本质就是识别虚假账号，一般来
讲主要从三个环节入手：

### 3.1 注册环节

识别虚假注册、减少“羊毛党”能够使用的账号量。在注册环节识别虚假注册的账号，并进行拦截和打击。

### 3.2 登录场景

提高虚假账号登录门槛，从而减少能够到达活动环节的虚假账号量。比如，登录环节通过验证码、短信验证码等手段来降低自动机的登录效率，从而达到
减少虚假账号登录量，减轻活动现场安全压力的目的。

### 3.3 活动环节

这个是防刷单对抗的主战场，也是减少“羊毛党”获利的直接战场；这里的对抗措施，一般有两个方面：

**3.3.1 通过验证码（短信、语音）降低黑产刷单的效率。**

**3.3.2 大幅度降低异常账号的优惠力度。**

# 4. 天御解决方案

针对注册、登录和活动环节，天御提供了对应的接口用于保障业务系统的安全。