**针对Windows平台的工业软件运行行为监控模块**

数据交互接口说明

2021年01月08日

广州道本信息科技有限公司

**所有权声明**

本文档的内容将做定期性的变动，且不另行通知。更改的内容将会补充到本手册中。

除特别声明外，此文档所用的公司名称、个人姓名及数据均属为说明的目的而模拟。

本文档的版权属广州道本科技有限公司所有，受中华人民共和国法律的保护。

本文档所含的任何构思、设计、工艺及其他技术信息均属本公司所有，受中华人民共和国法律的保护。未经本公司书面同意，任何单位和个人不得擅自摘抄、全部或部分复制本书内容，或者以其他任何方式使第三方知悉。

目 录

[1 方案概述 4](#_Toc63600493)

[1.1 业务概念 4](#_Toc63600494)

[1.2 缩略语和术语 4](#_Toc63600495)

[2 接口定义 4](#_Toc63600496)

[2.1 接口规范总述 4](#_Toc63600497)

[2.1.1 系统级别参数 5](#_Toc63600498)

[2.1.2 安全相关通用参数 5](#_Toc63600499)

[2.1.3 返回内容格式 5](#_Toc63600500)

[2.1.4 错误重试 6](#_Toc63600501)

[2.2 统一门户接入说明 6](#_Toc63600502)

[2.2.1 接入前准备 6](#_Toc63600503)

[2.3 获取access\_token接口说明 6](#_Toc63600504)

[2.4 任务下发相关接口 7](#_Toc63600505)

[2.4.1 监控系统的软件列表查询 7](#_Toc63600506)

[2.4.2 启动监听任务 8](#_Toc63600507)

[2.5 数据上报相关接口 9](#_Toc63600508)

[2.5.1 监控任务实时同步 9](#_Toc63600509)

[2.5.2 监控记录实时上报 10](#_Toc63600510)

[2.6 通用响应及错误码说明 12](#_Toc63600511)

# 方案概述

## 业务概念

本项目主要目的是为使用工业软件运行行为监控模块与统一门户平台进行数据交互和任务下发管理等功能进行数据交互的接口说明。

## 缩略语和术语

| **缩略语/术语** | **全称** | **说明** |
| --- | --- | --- |
| API | Application PrograMMing Interface | 应用程序接口 |
| HTTP | HyperText Transfer Protocol | 超文本传输协议 |
| URL | Uniform Resource Locator | 统一资源定位符 |
| WWW | World Wide Web | 万维网 |
| SI | Service Integrator | 服务集成 |

# 接口定义

## 接口规范总述

* 接口由集成平台的用户中心、消息中心后台提供给外围系统使用；
* 接口应采用基于HTTP的REST架构，POST提交数据；
* 接口方法的各参数使用FORM-DATA格式提交，复杂数据类型使用JSON字符串字段，返回结果使用JSON格式；
* 数据编码格式UTF-8
* http请求content-type: application/x-www-form-urlencoded
* 时间格式为yyyy-MM-dd HH24:mm:ss (如2011-01-05 23:00:59)
* 接口方法的返回值为JSON字符串；
* 接口字段长度单位：字节；
* 测试接口地址：待定
* 正式接口地址：待定。

### 系统级别参数

### 安全相关通用参数

接口均需要在header中加入如下参数，所有平台对平台接口均需要传入access\_token。 获取方式参考[access\_token接口说明](#_获取access_token接口说明)详细接口定义。

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 是否必填 | 参数说明 |
| X-Dbsv1-App-Key | String | 是 | 应用appkey （由接口提供方分配） |
| X-Dbsv1- Timestamp | String | 否 | 时间戳，24小时制，格式为yyyy-MM-dd HH:mm:ss，例如：2011-06-16 13:23:30 |
| Authorization | String | 是 | 根据OAuth 2.0标准定义的用户的访问令牌，需要授权访问的接口此项必填，access token可由登录接口返回值中获取  其中格式为：  Authorization: Bearer xxxxxxxxxxxxx  Bearer空格后面带的为token值 |

### 返回内容格式

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 名称 | 类型(长度) | 内容说明 |
|  | code | String(10) | 正常0，异常非0，详细见状态码说明 |
|  | message | String(256) | 处理结果说明 |
|  | pageNo | Integer | 当前页码（有分页请求参数时才会返回） |
|  | pageSize | Integer | 每页大小（有分页请求参数时才会返回） |
|  | data | String | 返回请求数据结果集，JSON对象字符串 |

**返回内容示例：一个JSON对象的字符串**

{

“code”: “0”,

“message“: “成功”,

“data”: {

“xxxxxxx”: 20.00

}

}

### 错误重试

接口使用方收到调用结果code!= “0” 后根据业务需要自行决定是否重试调用接口。

## 统一门户接入说明

### 接入前准备

需提供用于方法回调的统一门户URL，并且双方约定对应的appkey和appsecret。

## 获取access\_token接口说明

access\_token是集成平台的全局唯一接口调用凭据，业务系统调用各接口时都需使用access\_token。开发者需要进行妥善保存。access\_token的存储至少要保留512个字符空间。access\_token的有效期目前为2个小时，需定时刷新，重复获取将导致上次获取的access\_token失效。

|  |  |  |  |
| --- | --- | --- | --- |
| 地址：https://地址待定/v1/oauth2/access\_token | | | |
| 方法：POST | | | |
| 参数说明 | | | |
| 名称 | 类型 | 是否必填 | 备注 |
| appkey | String | 是 | 应用appkey （由接口提供方分配） |
| appsecret | String | 是 | 应用appsecret （由接口提供方分配） |
| grant\_type | String | 是 | 填写为client\_credential |
| 响应报文 | | | |
| 名称 | 类型 | | 备注 |
| access\_token | String | | 平台对平台接口凭证 |
| expires\_in | int | | access\_token接口调用凭证超时时间，单位（秒） |

请求报文样例：

appkey=APPKEY &appsecret=APPSECRET &grant\_type=client\_credential

响应报文样例：

{

"code": "0",

"message": "成功",

"data": {

" access\_token": "ACCESS\_TOKEN",

"expires\_in": 7200

}

}

## 任务下发相关接口

该部分接口由统一门户向由工业软件运行行为监控模块进行数据查询或者任务下发请求。

### 监控系统的软件列表查询

|  |  |  |  |
| --- | --- | --- | --- |
| 地址：https://地址待定/v1/software/list | | | |
| 方法：GET | | | |
| 参数说明 | | | |
| 名称 | 类型 | 是否必填 | 备注 |
| 无 |  |  |  |
| 响应报文 |
| 名称 | 类型 | 是否必填 | 备注 |
| softwareName | String(255) | 是 | 软件名称 |
| commandLine | String(255) | 是 | 启动命令行/可执行文件路径 |
| executePath | String(255) | 是 | 启动目录 |
| exeName | String(255) | 否 | 可执行程序名称 |
| exePath | String(255) | 否 | 可执行文件路径 |
| 说明： | | | |

请求报文样例：

https://xxxxxxxxxxxxxx/v1/software/list

响应报文样例：

{

"code": "0",

"message": "成功",

"data": {

"softwareName": "TIM",

"commandLine": "/software/tim/tim.exe",

"executePath": "/software/tim/”,

"exeName": “tim.ext",

“exePath”: "/software/tim/tim.exe"

}

}

### 启动监听任务

|  |  |  |  |
| --- | --- | --- | --- |
| 地址：https://地址待定/v1/task/start | | | |
| 方法：Post | | | |
| 参数说明 | | | |
| 名称 | 类型 | 是否必填 | 备注 |
| id | String | 是 | 任务唯一ID |
| softwareName | String(255) | 是 | 对应软件名称 |
| exePath | String(255) | 是 | 对应软件运行路径 |
|  |  |  |  |
| 响应报文 |
| 名称 | 类型 | 是否必填 | 备注 |
| id | String | 是 | 任务唯一ID |
| startTime | DateTime | 是 | yyyy-MM-dd HH:mm:ss 启动时间 |
| endTime | DateTime | 否 | yyyy-MM-dd HH:mm:ss 结束时间 |
| softwareName | String(255) | 是 | 对应软件名称 |
| exePath | String(255) | 是 | 对应软件运行路径 |
| pids | Long数组 | 是 | 用户进程号列表 |
| complete | Boolean | 是 | 是否完成监控 |

请求报文样例：

https://xxxxxxxxxxxxxx/v1/task /start

id=15234131&softwareName=TIM&exePath=/software/tim/tim.exe

响应报文样例：

{

"code": "0",

"message": "成功",

"data": {

"id": "15234131",

“startTime”: “2021-01-02 12:12:35”

“softwareName”: “TIM”,

“exePath”: "/software/tim/tim.exe"

“pids”: [123324,12329],

“complete”: false;

}

}

## 数据上报相关接口

该部分接口由工业软件运行行为监控模块 向 统一门户进行主动数据请求。

### 监控任务实时同步

|  |  |  |  |
| --- | --- | --- | --- |
| 地址：https://地址待定/v1/task/create | | | |
| 方法：POST必须在header Authorization中传入access\_token | | | |
| 参数说明 | | | |
| 名称 | 类型 | 是否必填 | 备注 |
| id | String | 是 | 任务唯一ID |
| startTime | DateTime | 是 | yyyy-MM-dd HH:mm:ss 启动时间 |
| endTime | DateTime | 否 | yyyy-MM-dd HH:mm:ss 结束时间 |
| softwareName | String(255) | 是 | 对应软件名称 |
| exePath | String(255) | 是 | 对应软件运行路径 |
| pids | Long数组 | 是 | 用户进程号列表 |
| complete | Boolean | 是 | 是否完成监控 |
| 响应报文 |  |  |  |
| 说明： | | | |
|  | | | |

请求样例：

id=1203201812041020030001&startTime=2018-10-15 16:47:39&softwareName=TIM&exePath=/software/tencent/tim/tim.exe&pids=2344&pids=123954&complete=false

响应报文样例：

{

"code": "0",

"message": "成功"

}

### 监控记录实时上报

|  |  |  |  |
| --- | --- | --- | --- |
| 地址：https://地址待定/v1/action/upload | | | |
| 方法：POST 必须在header Authorization中传入access\_token | | | |
| 参数说明 | | | |
| 名称 | 类型 | 是否必填 | 备注 |
| uuid | String(255) | 是 | 唯一标识符 |
| timestamp | Date | 是 | yyyy-MM-dd HH:mm:ss 格式  行为时间戳 |
| withAttachment | Boolean | 否 | 本行为是否有对应附件 |
| taskId | Long | 是 | 关联的任务ID |
| pid | Long | 是 | 进程ID |
| actionGroup | Integer | 是 | 行为类别：  1：文件读写  2：网络访问  3：注册表  4：进程调用  5：设备控制  6：对象权限 |
| type | Int | 是 | 具体操作类型：  0 监控开始  4095 监控结束  4096 发起网络连接  4097 TCP数据发送  4098 TCP数据接收  4099 UDP数据发送  4100 UDP数据接收  8192 文件打开  8198 文件删除  8201 设备访问  12288 注册表打开或创建键  12294 注册表设置值键  16384 启动进程  20480 创建远程线程  20481 WM\_COPYDATA发送  24576 修改对象安全描述符 |
| host | String(255) | 否 | 目标主机 |
| port | String(255) | 否 | 目标端口 |
| bytes | Long | 否 | 数据包大小 |
| path | String(255) | 否 | 文件路径/如果创建远程线程时执行的thread  为可下载文件url |
| fileName | String(255) | 否 | 文件名称 |
| access | Long | 否 | 打开文件时要求的访问权限  该值为位序列（以32位无符号数承载），需要用对应的位掩码进行位运算获得。具有使用含义的掩码目前包括：  0x80000000 – 一般读  0x40000000 – 一般写  0x20000000 – 一般执行  0x10000000 – 全部 |
| generalFile | Boolean | 否 | 文件是否普通文件 |
| backup | String(255) | 否 | 备份路径  为可下载文件url |
| offset | Long | 否 | 写入数据偏移量 |
| where | Integer | 否 | 从何处开始偏移。0 - 从文件起始位置偏移；1 - 从当前位置偏移（即上一次读写操作后的文件偏移量）；2 - 从文件末尾向前偏移 |
| parent | String(255) | 否 | 注册表父键 |
| key | String(255) | 否 | 注册表目标 |
| valueName | String(255) | 否 | 值键 |
| valueType | String(255) | 否 | 值键类型 |
| data | String | 否 | 值键值/发送数据(HEX编码) |
| oldValueType | String(255) | 否 | 值键原类型 |
| oldData | String | 否 | 值键原有值 |
| cmdLine | String(255) | 否 | 启动进程的完整命令行数据 |
| cmdPid | String(255) | 否 | 执行命令的PID |
| cmd | String(255) | 否 | 执行的命令 |
| args | String[] | 否 | 执行命令时的参数（数组） |
| threadEntryAddress | String(255) | 否 | 创建远程线程时提供的入口函数地址 |
| destPid | Long | 否 | 消息发送目标的PID |
| destPName | String(255) | 否 | 目标进程名称 |
| destHwnd | Long | 否 | 消息发送目标窗口的句柄 |
| destTitle | String(255) | 否 | 目标窗口标题 |
| srcHwnd | Long | 否 | 消息发送源窗口的句柄 |
| srcTitle | String(255) | 否 | 源窗口标题 |
| deviceName | String(255) | 否 | 设备名称 |
| target | String(255) | 否 | 目标对象名 |
| owner | String(255) | 否 | 本次修改操作需要修改的目标用户 |
| group | String(255) | 否 | 本次修改操作需要修改的目标用户组 |
| daclSdString | String(255) | 否 | DACL安全描述符字符串 |
| mode | String(255) | 否 | 权限掩码 |
| 响应报文 | | | |
| 说明： | | | |

请求样例：

uuid=1203201812041020030001&timestamp=2021-01-01 10:12:12&type=0&actionGroup=1&pid=12353&taskId=5343122

响应报文样例：

{

"code": "0",

"message": "成功"

}

## 通用响应及错误码说明

通用结果响应报文如下：

{

"path": "/patient-api/webapi/hello/test",

"code": "system-name.400.10001",

"message": "数据校验错误",

“system”: “system-name”

}

其中code不为0时表示接口错误，错误码如下

错误时错误码code为三级节点结构，由system-name.httpcode.errorcode组成。

其中system-name为业务系统对应appkey

Httpcode包括 400 和500， 400表示接口传入数据有误， 500表示集成平台处理有误

Errorcode为集成平台逻辑处理错误码

错误码合集

|  |  |  |
| --- | --- | --- |
| 模块 | 省略应用简称的错误码 |  |
| 通用 | 400.10001 | Access Token不正确或已过期 |
| 400.10002 | appkey或appsecret错误 |
| 400.10003 | 接口参数错误 |
| 500.99999 | 系统繁忙，请稍候再试 |
| 授权相关 | 400.11001 | redirect\_uri域名与后台配置不一致 |
| 400.11002 | 用户GUID不存在 |
| 400.11003 | code无效 |
| 400.11004 | Access\_token无效 |
| 400.11005 | Refresh\_token无效 |
| 400.11006 | grant\_type错误 |
|  |  |  |
|  |  |