**大数据扫描系统**

**《WEB API说明文档》**

**修订版本**

|  |  |  |  |
| --- | --- | --- | --- |
| **版本** | **修订人** | **日期** | **备注** |
| V1 | 张群轼 | 2017.5.12 | 初稿 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

目录

[1 引言 5](#_Toc469277020)

[2 用户管理模块 6](#_Toc469277021)

[2.1 用户登录 6](#_Toc469277022)

[2.2 用户退出登录 6](#_Toc469277023)

[3 探针管理模块 8](#_Toc469277024)

[3.1 增加探针 8](#_Toc469277025)

[3.2 查看探针 8](#_Toc469277026)

[3.3 更改探针 9](#_Toc469277027)

[3.4 删除探针 10](#_Toc469277028)

[3.5 更改探针模式 11](#_Toc469277029)

[3.6 开始采集数据 12](#_Toc469277030)

[3.7 结束采集数据 12](#_Toc469277031)

[4 设备管理模块 14](#_Toc469277032)

[4.1 设备手动添加 14](#_Toc469277033)

[4.2 开始设备自动发现 14](#_Toc469277034)

[4.3 停止设备自动发现 15](#_Toc469277035)

[4.4 获取自动发现的设备 16](#_Toc469277036)

[5 流量管理模块 17](#_Toc469277037)

[5.1 获取正在采集的流量 17](#_Toc469277038)

[5.2 获取生成的白名单 18](#_Toc469277039)

[5.3 设定流超时时间 19](#_Toc469277040)

[5.4 获取静态流 19](#_Toc469277041)

[5.5 获取所有相关IP 20](#_Toc469277042)

[5.6 获取协议 21](#_Toc469277043)

[5.7 添加协议 22](#_Toc469277044)

[5.8 更改协议 22](#_Toc469277045)

[5.9 删除协议 23](#_Toc469277046)

[6 规则管理模块 25](#_Toc469277047)

[6.1 查看完整白名单 25](#_Toc469277048)

[6.2 新建白名单规则 25](#_Toc469277049)

[6.3 删除白名单规则 26](#_Toc469277050)

[6.4 新建审计规则 27](#_Toc469277051)

[6.5 删除审计规则 28](#_Toc469277052)

[7 规则管理模块 29](#_Toc469277053)

[7.1 获取所有异常事件 29](#_Toc469277054)

[7.2 获取特定异常事件 29](#_Toc469277055)

[7.3 获取所有审计事件 30](#_Toc469277056)

[7.4 获取受损设备情况 31](#_Toc469277057)

[8 系统管理模块 32](#_Toc469277058)

[8.1 获取操作日志 32](#_Toc469277059)

[8.2 获取系统日志 32](#_Toc469277060)

[8.3 探针引擎配置 33](#_Toc469277061)

[8.4 大数据平台配置 34](#_Toc469277062)

[8.5 获取注册用户列表 34](#_Toc469277063)

[8.6 注册新用户 35](#_Toc469277064)

[8.7 更改用户信息 36](#_Toc469277065)

[8.8 删除注册用户 37](#_Toc469277066)

# 引言

此文档是描述了Web底层（业务逻辑层）提供给Web页面层的API设计。面向的读者为Web页面层开发人员。Web底层提供给Web页面层为HTTP方式的API接口。此文档按照模块方式进行划分。

# 查看协议

此API用在首页的协议列表上。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **API名称** | 查看所有协议 | | | |
| **请求方式** | GET或POST | | | |
| **请求URL** | /api/protocols | | | |
|  | **参数名称** | **参数类型** | **参数约束** | **范围** |
| **请求参数** |  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| **请求Body** | 无 | | | |
| **正确响应** | {  "protocols": [{  "nw\_proto": "TCP",  "proto\_name": "HTTP",  "id": 1,  "port": 80  }, {  "nw\_proto": "TCP",  "proto\_name": "MELSEC-Q",  "id": 13,  "port": 5007  }  ]  } | | | |
| **错误响应** |  | | | |
| **备注** |  | | | |