

|  |
| --- |
| 网络安全关口监测系统  用户使用说明书 |



文档版本： ()

|  |
| --- |
| ©2015 长安通信 |

|  |
| --- |
| ■ 版权声明 |
| 本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明，版权均属长安通信科技有限责任公司（简称长安通信）所有，受到有关产权及版权法保护。任何个人、机构未经长安通信的书面授权许可，不得以任何方式复制或引用本文的任何片断。 |

---------------------------------------------------------------------------------

长安通信科技有限责任公司

网站：<http://www.chanct.com/>

电子信箱：gms-support@chanct.com

联系电话：010-63911999

---------------------------------------------------------------------------------

目录

[前言 1](#_Toc416962342)

[概述 1](#_Toc416962343)

[读者对象 1](#_Toc416962344)

[内容简介 1](#_Toc416962345)

[格式约定 1](#_Toc416962346)

[1 术语表 2](#_Toc416962347)

[1.1 名词解释 2](#_Toc416962348)

[2 章节 首页展示 3](#_Toc416962349)

[2.1 用户登录 3](#_Toc416962350)

[2.2 logo栏展示内容和功能 4](#_Toc416962351)

[2.3 今日分类事件统计 5](#_Toc416962352)

[2.4 最近流量曲线 8](#_Toc416962353)

[2.5 系统状态 10](#_Toc416962354)

[2.6 今日TOP5被攻击IP 12](#_Toc416962355)

[2.7 事件实时监控 15](#_Toc416962356)

[3 章节 查询 17](#_Toc416962357)

[3.1 流量分析 17](#_Toc416962358)

[3.1.1 用户数统计-流量分析 17](#_Toc416962359)

[3.1.2 用户归属地分布-流量分析 20](#_Toc416962360)

[3.1.3 用户浏览器/版本分布-流量分析 22](#_Toc416962361)

[3.1.4 访问时长统计-流量分析 24](#_Toc416962362)

[3.1.5 访问次数统计-流量分析 26](#_Toc416962363)

[3.1.6 用户流量统计-流量分析 28](#_Toc416962364)

[3.1.7 TCP连接成功率统计-流量分析 30](#_Toc416962365)

[3.2 恶意代码感染事件查询 32](#_Toc416962366)

[3.3 网站事件 36](#_Toc416962367)

[3.4 通信行为异常事件 40](#_Toc416962368)

[3.5 统计报表 44](#_Toc416962369)

[3.6 恶意代码传播事件查询 44](#_Toc416962370)

[3.7 恶意URL访问事件查询 49](#_Toc416962371)

[3.8 攻击尝试事件查询 52](#_Toc416962372)

[3.9 其他事件查询 56](#_Toc416962373)

[3.10 流量查询 60](#_Toc416962374)

[4 章节 报表 62](#_Toc416962375)

[4.1 报表下载 62](#_Toc416962376)

[5 章节 系统管理 64](#_Toc416962377)

[5.1 设备管理 64](#_Toc416962378)

[5.2 网络配置 66](#_Toc416962379)

[5.3 用户管理 71](#_Toc416962380)

[5.4 监听配置 72](#_Toc416962381)

[5.5 组件设置 73](#_Toc416962382)

[5.6 时间同步 76](#_Toc416962383)

[5.7 预警管理 80](#_Toc416962384)

[5.8 升级管理 82](#_Toc416962385)

[5.9 调试配置 84](#_Toc416962386)

[5.10 重要用户配置 85](#_Toc416962387)

[5.11 自定义流量配置 88](#_Toc416962388)

[5.12 白名单配置 91](#_Toc416962389)

[5.13 系统操作日志 93](#_Toc416962390)

[6 章节 授权 95](#_Toc416962391)

[6.1 申请授权 95](#_Toc416962392)

[6.2 获取license文件 97](#_Toc416962393)

[6.3 license导入授权 98](#_Toc416962394)

[6.4 授权提醒 98](#_Toc416962395)

插图

[图2-1 logo栏效果图 4](#_Toc416962641)

[图2-2 今日事件分类统计效果图 6](#_Toc416962642)

[图2-3 最近流量曲线 8](#_Toc416962643)

[图2-4 系统状态 10](#_Toc416962644)

[图2-5 拓扑图的图层 11](#_Toc416962645)

[图2-6 今日TOP5被攻击IP 13](#_Toc416962646)

[图2-7 事件实时监控展示 15](#_Toc416962647)

[图 3-1-1-1用户数统计粒度分钟查询效果 18](#_Toc416962648)

[图 3-1-1-2用户数统计粒度小时查询效果 18](#_Toc416962649)

[图 3-1-1-3用户数统计粒度天查询效果 19](#_Toc416962650)

[图 3-1-1-4用户数统计粒度月查询效果 19](#_Toc416962651)

[图 3-1-2-1用户归属地分布粒度分钟查询效果 20](#_Toc416962652)

[图 3-1-2-2用户归属地分布粒度小时查询效果 20](#_Toc416962653)

[图 3-1-2-3用户归属地分布粒度天查询效果 21](#_Toc416962654)

[图 3-1-2-4用户归属地分布粒度月查询效果 21](#_Toc416962655)

[图 3-1-3-1用户浏览器/版本分布粒度分钟查询效果 23](#_Toc416962656)

[图 3-1-3-2用户浏览器/版本分布粒度小时查询效果 23](#_Toc416962657)

[图 3-1-3-3用户浏览器/版本分布粒度天查询效果 23](#_Toc416962658)

[图 3-1-3-4用户浏览器/版本分布粒度月查询效果 24](#_Toc416962659)

[图 3-1-4-1访问时长统计粒度分钟查询效果 25](#_Toc416962660)

[图 3-1-4-2访问时长统计粒度小时查询效果 26](#_Toc416962661)

[图 3-1-4-3访问时长统计粒度天查询效果 26](#_Toc416962662)

[图 3-1-4-4访问时长统计粒度月查询效果 26](#_Toc416962663)

[图 3-1-5-1访问次数统计粒度分钟查询效果 27](#_Toc416962664)

[图 3-1-5-2访问次数统计粒度小时查询效果 28](#_Toc416962665)

[图 3-1-5-3访问次数统计粒度天查询效果 28](#_Toc416962666)

[图 3-1-5-4访问次数统计粒度月查询效果 28](#_Toc416962667)

[图 3-1-6-1用户流量统计粒度分钟查询效果 29](#_Toc416962668)

[图 3-1-6-2用户流量统计粒度小时查询效果 30](#_Toc416962669)

[图 3-1-6-3用户流量统计粒度天查询效果 30](#_Toc416962670)

[图 3-1-6-4用户流量统计粒度月查询效果 30](#_Toc416962671)

[图 3-1-7-1TCP连接成功率统计粒度分钟查询效果 31](#_Toc416962672)

[图 3-1-7-2TCP连接成功率统计粒度小时查询效果 32](#_Toc416962673)

[图 3-1-7-3TCP连接成功率统计粒度天查询效果 32](#_Toc416962674)

[图 3-1-7-4TCP连接成功率统计粒度月查询效果 32](#_Toc416962675)

[图3-1 恶意代码感染事件查询效果 33](#_Toc416962676)

[图3-2 网站事件查询效果展示图 37](#_Toc416962677)

[图3-3 网站事件查询效果展示图 41](#_Toc416962678)

[图3-4 恶意代码传播事件查询效果展示图 45](#_Toc416962679)

[图3-5 恶意URL访问事件查询 49](#_Toc416962680)

[图3-6 攻击尝试事件查询 53](#_Toc416962681)

[图3-7 其他事件查询 57](#_Toc416962682)

[图3-8 流量查询效果展示图 60](#_Toc416962683)

[图4-1 报表下载效果展示图 62](#_Toc416962684)

[图5-1 设备管理效果展示图 64](#_Toc416962685)

[图5-2 网络配置效果展示图 67](#_Toc416962686)

[图5-3 用户管理效果展示图 71](#_Toc416962687)

[图5-4 监听配置效果展示图 73](#_Toc416962688)

[图5-5 组建设置效果展示图 74](#_Toc416962689)

[图5-6 时间同步效果展示图 77](#_Toc416962690)

[图5-7 预警管理效果展示图 80](#_Toc416962691)

[图5-8 升级管理效果展示图 83](#_Toc416962692)

[图5-9 调试配置效果展示图 84](#_Toc416962693)

[图5-10 重要用户配置 86](#_Toc416962694)

[图5-11 自定义流量配置效果展示图 89](#_Toc416962695)

[图5-12 白名单配置效果展示图 91](#_Toc416962696)

[图5-13 操作日志查看效果展示图 93](#_Toc416962697)

[图6-1 授权申请填写单效果图 95](#_Toc416962698)

[图6-2 导入license文件效果图 98](#_Toc416962699)

# 前言

概述

对网络安全关口监测系统常规使用的说明。

读者对象

网络安全关口监测系统使用者。

内容简介

| 章节 | 概述 |
| --- | --- |
| 章节一 | 首页展示：今日事件分类统计，最近流量曲线，系统状态，今日TOP5被攻击IP ，事件实时监控。 |
| 章节二 | 查询：恶意代码感染事件，网站事件，恶意代码传播事件，恶意URL访问事件查询，攻击尝试事件查询，其他事件查询，流量查询 |
| 章节三 | 报表下载：日报表，周报表，月报表，年报表四种报表下载，两种格式。 |
| 章节四 | 系统管理：重要用户配置，自定义流量配置，白名单配置，设备管理，用户管理，操作日志查看，数据备份，升级管理。 |
| 章节五 | 系统授权。 |

格式约定

| 符号 | 说明 |
| --- | --- |
| 粗体字 | 菜单、命令和关键字 |
| 斜体字 | 文档名、变量 |
|  | 对描述内容的补充和引用信息 |
|  | 使用设备时的技巧和建议 |
|  | 需要特别注意的事项和重要信息 |
|  | 有可能造成人身伤害的警告信息。 |

# 术语表

## 名词解释

|  |  |
| --- | --- |
| **缩写、术语** | **解 释** |
| GMS | 网络安全关口监测系统（Gateway Monitory System）英文简称。 |
| MTX | 即中心已建设的“基于报文的实时采样监测分析子系统”的前端模块。 |
| VDS | 即中心已建设的“恶意代码捕获和分析系统”。基于原始报文对恶意代码进行监测。 |
| 流（Flow） | 专业术语。按照一定抽样比从路由器或交换机导出的包含流经该设备的数据包统计信息的连续数据，例如SFlow、NetFlow等。 |
| 特征事件 | 指特征监测获取的木马、僵尸网络恶意活动事件、恶意代码感染与传播事件。 |
| 安全事件 | 包括特征事件、恶意代码传播事件事件、通信行为异常事件、恶意URL访问事件、流量事件。 |
| 异常记录 | 基于行为分析产生的异常行为记录，通信行为异常分析引擎产生 |
| 黑名单 | 主要包括：恶意URL、域名、IP。 |
| 系统版本 | 指系统软件版本号 |
| 特征库版本 | 病毒库版本号 |
| 最大上传/下载速度 | 指跟阿里云外网交互时占用宽带的大小 |

# 章节 首页展示

## 用户登录

通过WEB登录，登录地址https：//11.11.11.11 (11.11.11.11为设备的IP地址)

**操作说明：**

1. 设备默认用户名：admin，密码：123456
2. 进入登录界面



1. 用户名和密码有一项输入错误或者用户被锁定，都会有提示，用户在5分钟内连续错误登录10 次，用户将被锁定，非管理员用户，需要管理员解锁，如果管理员被锁，2分钟后自动解锁



1. 输入正确的用户名和密码后，进入界面，如果10min内没有任何操作，系统将自动退出
2. 用户想要退出可点击首页退出按钮



## logo栏展示内容和功能

此模块展示了系统相关的logo，授权状态，用户登录的信息。



logo栏效果图

**此模块可进行的操作：**

1. 点击向右箭头标退出系统。

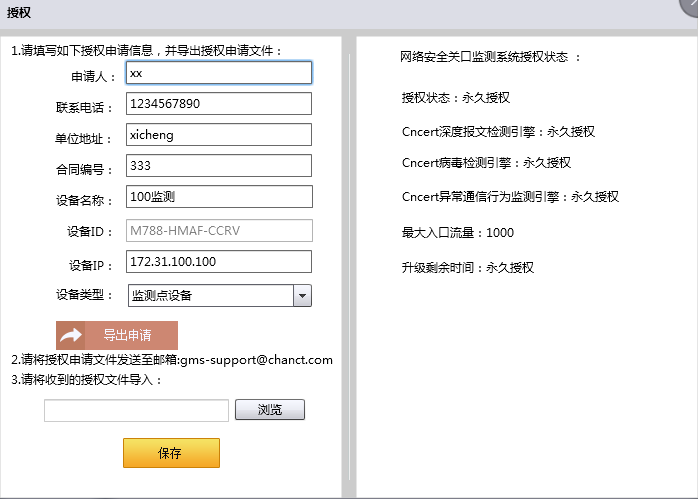


1. 点击用户名可以更改密码。





1. 点击授权状态按钮可查看当前授权状态。



## 今日分类事件统计

此模块主要提供了今日实时的事件总数和七种事件发生次数的分类统计，分别为：恶意代码感染事件、网站事件、通讯行为异常事件、恶意代码传播事件、恶意URL访问事件、攻击尝试事件和其他事件。

 今日事件总条数：通过动态的翻盘展示实时的动态信息。

 七种事件发生次数**：**以不同颜色的柱状图形式展示，鼠标移动到对应的柱状图会出现相对应的发生次数。图表标题为事件类型，横坐标为时间（年.月形势），纵坐标为事件数量。



今日事件分类统计效果图

**此模块可进行的操作：**

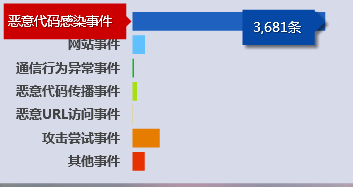
点击某类事件对应的柱状图，能够弹出图层，以柱状图显示该类事件最近7天（不含今日）的变化数量变化趋势；

**此模块的操作流程：**

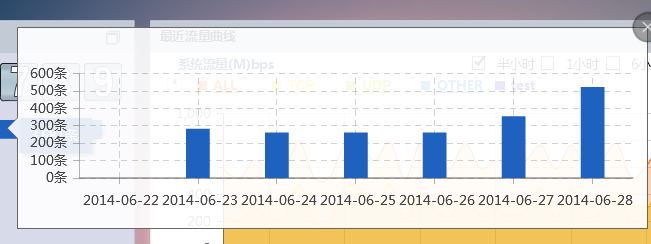
1. 进入界面；
2. 左上角可以看到今日事件的统计数以翻牌的形式在统计；



1. 将鼠标停滞在任一事件的柱状图上可看到事件的总数；

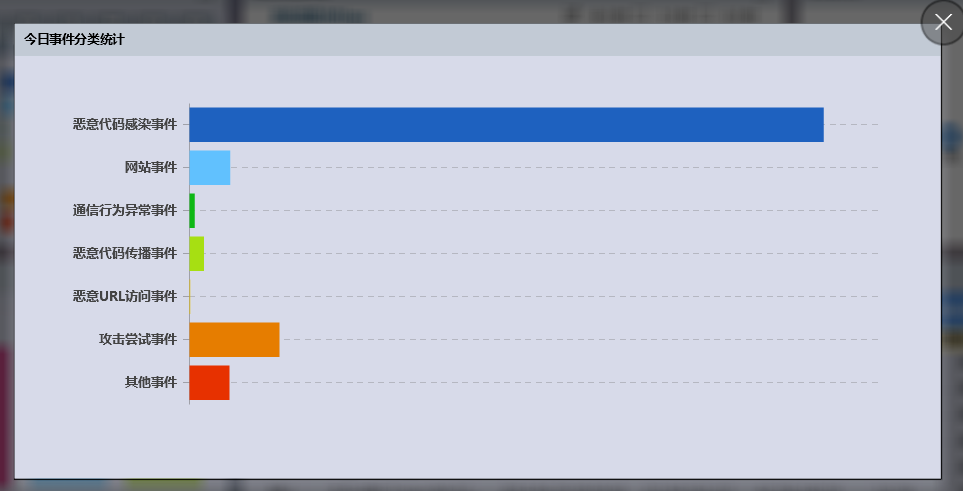


1. 单击柱状图可看到此事件最近7天的统计；



1. 如果感觉事件今日分类事件统计小的话，可以点击其右上角的放大图标“”，可放大





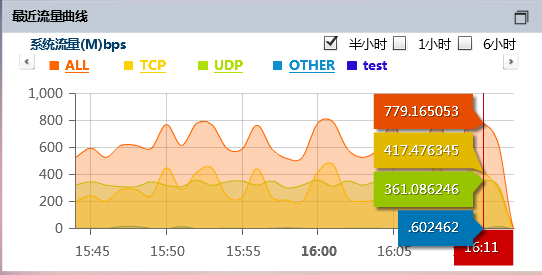
1. 如果想要某个或几个柱状图放大，可按住鼠标左键将柱状图选中，松开鼠标左键就可看到放大的效果





## 最近流量曲线

默认展示最近半小时的系统流量（ALL/TCP/UDP/OTHER）及需要在首页展示的自定义流量,展示时间提供给用户三种选择：最近半小时、最近1小时、最近6小时；用户可单独查看或组合查看某一类流量；



最近流量曲线

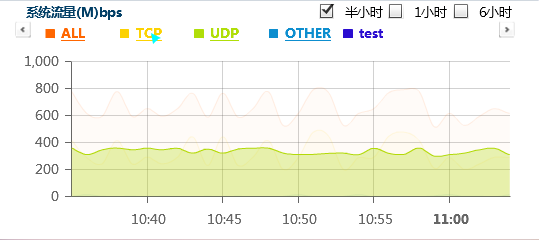
 点击流量曲线名称出现下划线，这时候鼠标浮动到流量曲线上会出现该名称的数量指示牌，数量指示牌显示的数据是光标所在位置的该曲线的数据。没有下划线不显示数量指示牌。点击名称前面的小方块，流量名称会变成灰色，不在图中显示该流量曲线。

**此模块可进行的操作：**

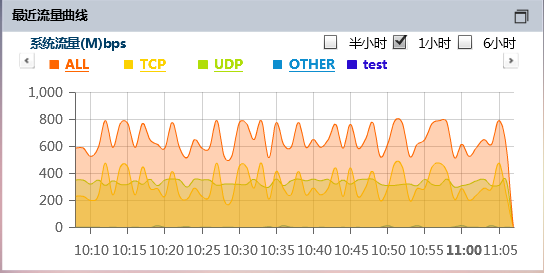
双击如图中的流量曲线页面跳转到自定义流量查询，自定义流量查询为查询里面的模块。

**此模块的操作流程：**

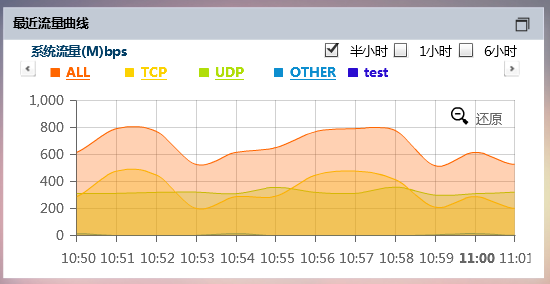
1. 可直接观看某一类型的流量曲线，例如只看“UDP”的，只要将鼠标停滞在UDP上即可

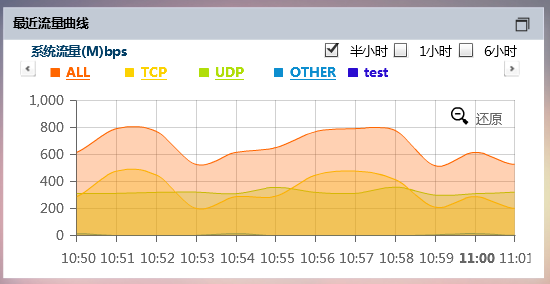


1. 可选择查看半小时、1小时和6小时的流量



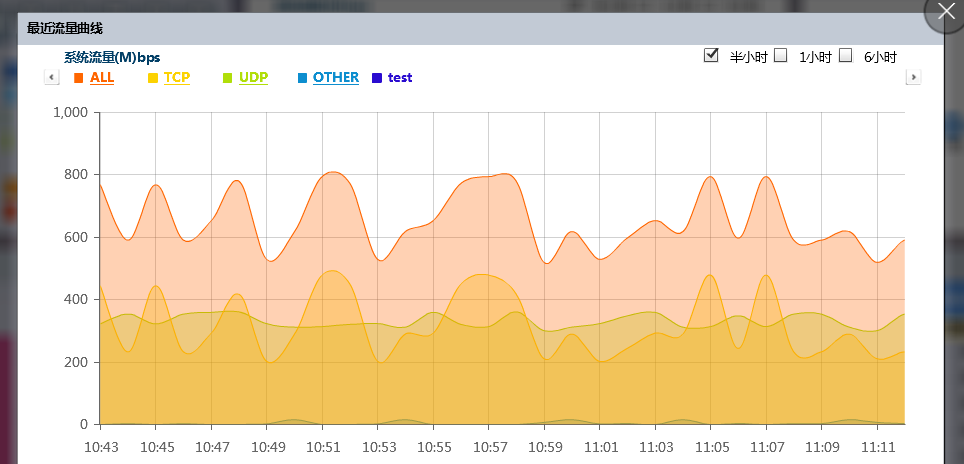
1. 用鼠标左键选中某段流量可放大





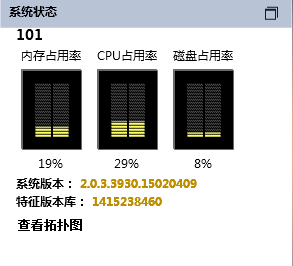
1. 点击右上角的放大图标“”，可放大





## 系统状态

默认展示了设备名称、设备的CPU占用率，内存占用率，磁盘占用率，系统版本号和特征库的版本信息，可查看设备网络拓扑图。



系统状态

**此模块可进行的操作：**

点击查看拓扑图，可查看设备的网络拓扑图。点击返回，可查看设备名称、设备的CPU占用率，内存占用率，磁盘占用率，系统版本号和特征库的版本信息。

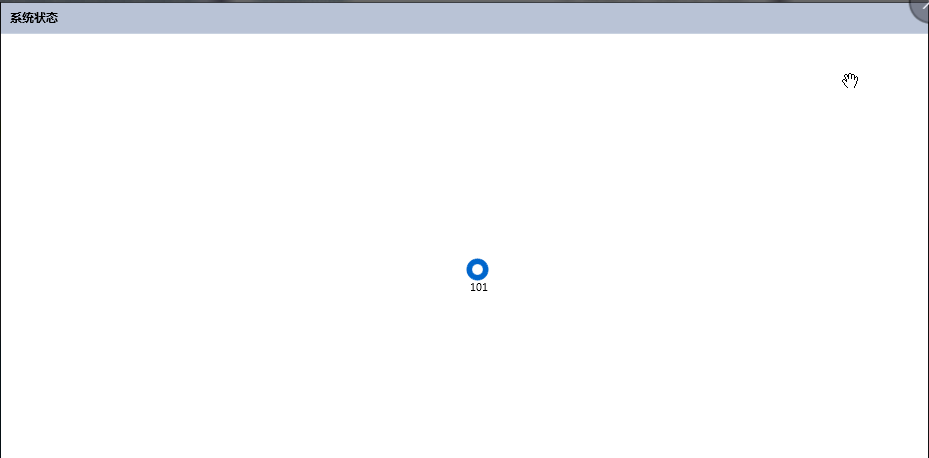
**此模块的操作流程：**

1. 点击查看拓扑图，可查看设备的网络拓扑图。



1. 点击右上角的放大图标“”，可放大

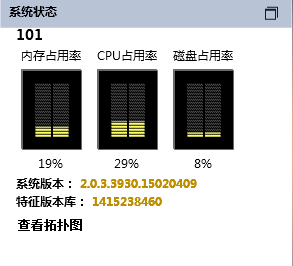




拓扑图的图层

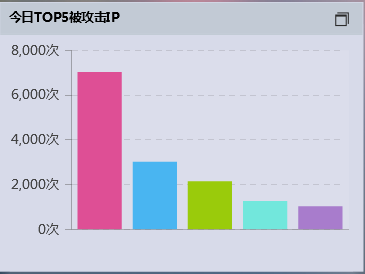
1. 点击返回，可查看设备系统状态





## 今日TOP5被攻击IP

此模块综合统计恶意代码感染事件(感染IP)/网站事件(网站IP)/攻击尝试事件(被攻击IP)/其他事件(被攻击IP)中次数最多的5个IP。



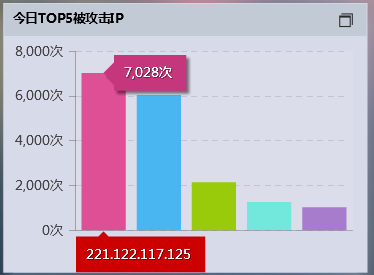
今日TOP5被攻击IP

**此模块可进行的操作：**

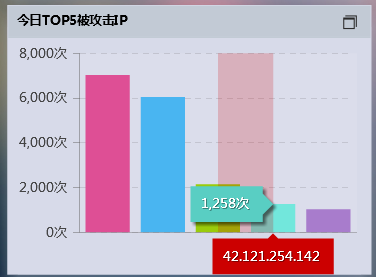
当鼠标悬浮在某一柱图上时，能够显示该柱图对应的IP及被攻击次数，鼠标移走以上内容消失。

**此模块的操作流程：**

1. 当鼠标悬浮在某一柱图上时，能够显示该柱图对应的IP及被攻击次数，鼠标移走以上内容消失。

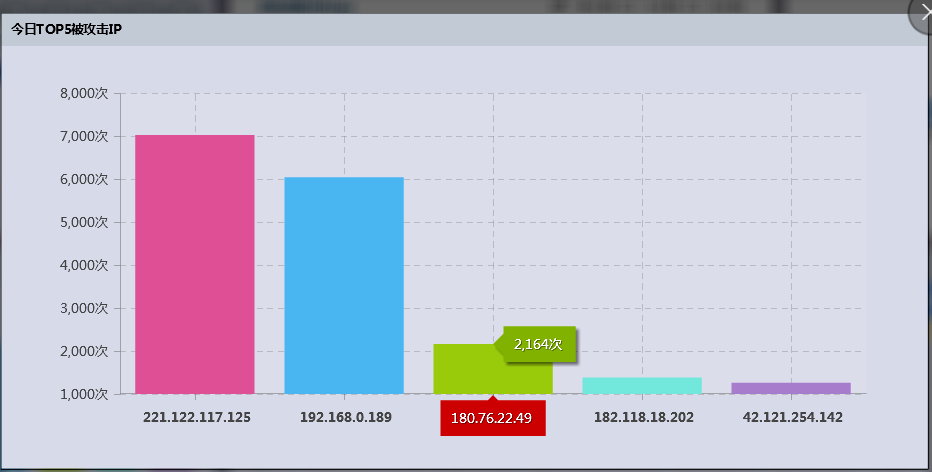


1. 鼠标选中某一柱状图可放大





1. 点击右上角的放大图标“”，可放大



## 事件实时监控

事件实时监控展示的事件类别为：恶意代码感染事件、网站事件、通信行为异常事件、恶意代码传播事件、恶意URL访问事件、攻击尝试事件、其他事件；分别为各类别最新的20条事件。



事件实时监控展示

**此模块可进行的操作：**

1、单机如图上面蓝色的部分可以跳转到对应的事件列表。

2、单击事件下面的某一条弹出对应的详细信息。

**此模块的操作流程：**

1. 选中任一事件都可看到最近20条事件，用鼠标拉动右侧的下拉框可查看。



1. 双击任一事件可查看详情



1. 点击右上角的放大图标“”，可放大



# 章节 查询

## 流量分析

流量分析是用户针对不同的报表，选择不同的时间颗粒度进行分析查询，并生成相应的结果和图表。

有如下报表可供用户进行查询：

1. 用户数统计
2. 用户归属地分布
3. 用户浏览器/版本分布
4. 访问时长统计
5. 访问次数统计
6. 用户流量统计
7. TCP连接成功率统计

用户可以选择如下粒度进行查询：

1. 分钟（查询离结束时间最近的一小时内的数据）
2. 小时 (查询离结束时间最近的一天内的数据)
3. 天 (查询离结束时间最近的一个月内的数据)
4. 月 (查询离结束时间最近的一年内的数据)

注意以下几点：

1. 开始时间不可选。
2. 默认结束时间应为当前系统时间，用户可以自行设置结束时间。
3. 通常情况下，系统里只存有系统开始运行以后的数据，系统开始运行之前是没有相应数据的，没有数据的时间段将不在趋势图中展示。

流量分析查询结果主要以以下几种图表进行展示：

1. 统计表格

统计表格主要统计该时段内PC端，移动端，以及全部的最大值，平均值，最小值情况。

PC端及移动端（最大值/最小值）=该时段内系统获取的最大值/最小值记录。

全部（最大值/最小值）=该时段内某时间粒度的全部最大值/全部最小值记录。

PC端、移动端、全部（平均值）=该时段内记录总和/该时段内记录数。

1. 趋势图

以折线图形式展示各时段内PC端，移动端，以及PC端加移动端的数据。

1. 分布图

以饼图形式展示各时段内各统计对象所在百分比情况。

1. TOP10表

统计该时段内TOP10的记录。

### 用户数统计-流量分析

用户进入流量分析界面，报表选择“用户数统计”，颗粒度选择“分钟/小时/天/月”，点击查询按钮，查询结果将以“该时段内用户变化趋势”图和“该时段内用户数量”表显示，以下是各个不同粒度时，用户数统计的查询效果：

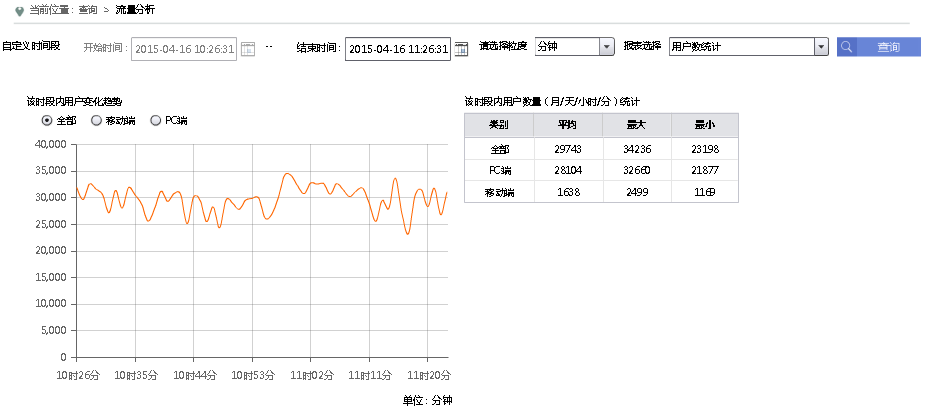


图 3-1-1-1用户数统计粒度分钟查询效果

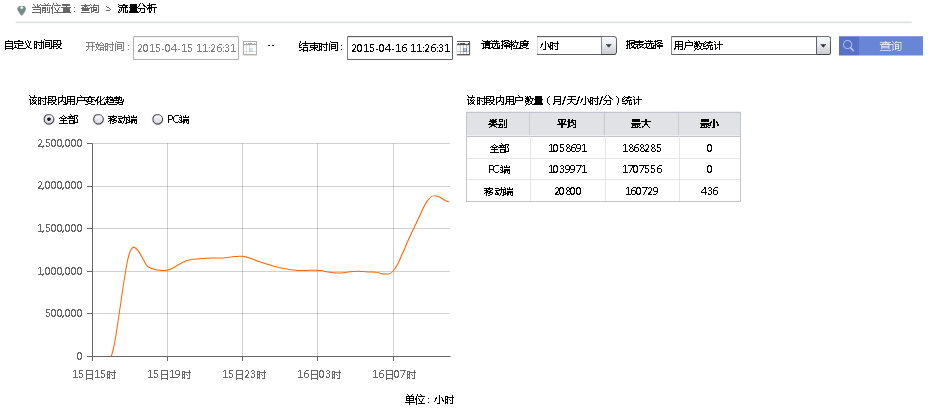


图 3-1-1-2用户数统计粒度小时查询效果

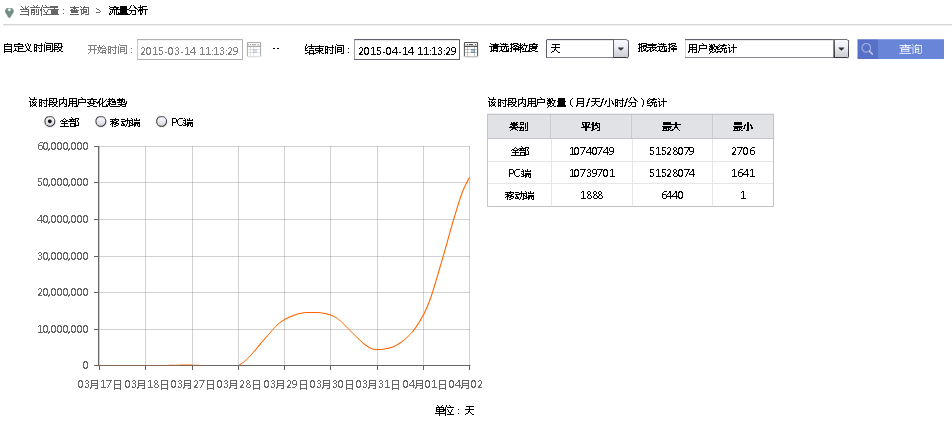


图 3-1-1-3用户数统计粒度天查询效果



图 3-1-1-4用户数统计粒度月查询效果

用户变化趋势图描述：

1. 用户可以选择“全部”选项，选择显示全部的该时段内用户变化的趋势情况。
2. 用户可以选择“移动端”选项，选择显示全部的该时段内移动端的用户变化趋势情况。
3. 用户可以选择“PC端”选项，选择显示全部的该时段内PC端的用户变化趋势情况。
4. 横坐标为粒度，纵坐标为用户数量值。

该时段内用户数量统计描述：

1. 统计该时段内全部的用户数平均值，最大值，最小值。
2. 统计该时段内PC端的用户数平均值，最大值，最小值。
3. 统计该时段内移动端的用户数平均值，最大值，最小值。

### 用户归属地分布-流量分析

用户进入流量分析界面，报表选择“用户归属地分布”，颗粒度选择“分钟/小时/天/月”，点击查询按钮，查询结果将以饼图方式显示“访问用户按国家分布”，”“国内访问用户按省份分布”，“国内访问用户按地市分布” 信息，以下是各个不同粒度时，用户数统计的查询效果：

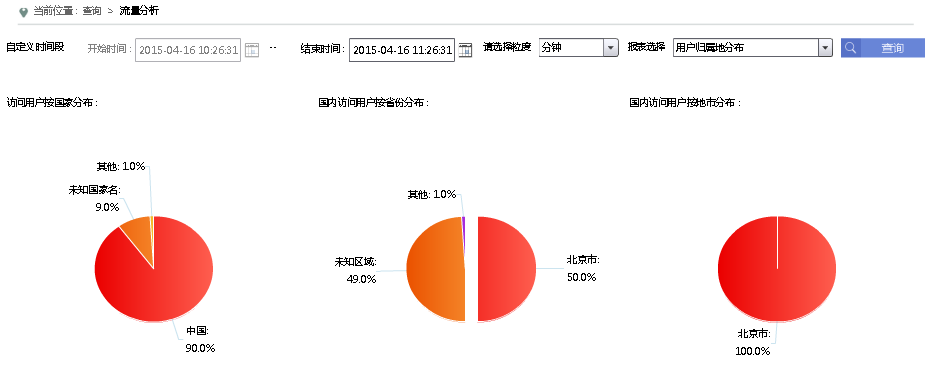


图 3-1-2-1用户归属地分布粒度分钟查询效果

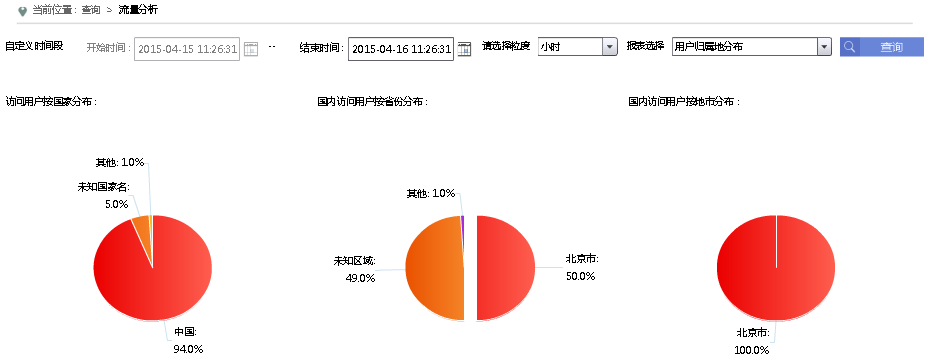


图 3-1-2-2用户归属地分布粒度小时查询效果

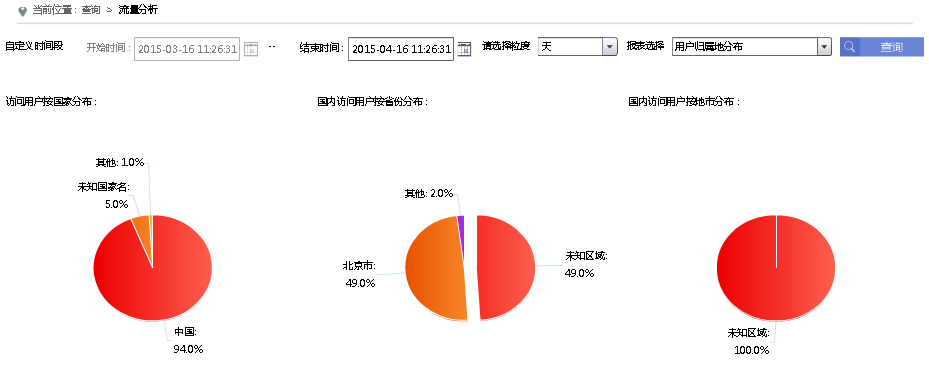


图 3-1-2-3用户归属地分布粒度天查询效果

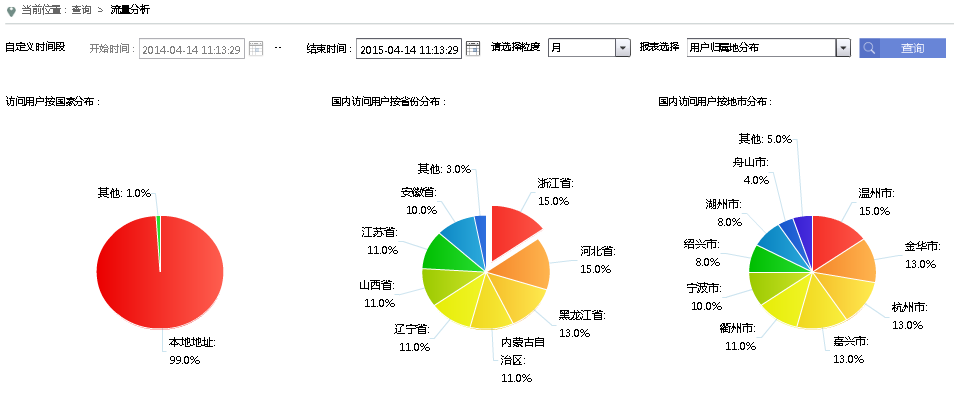


图 3-1-2-4用户归属地分布粒度月查询效果

访问用户按国家分布描述：

1. ”统计本地数据和非本地数据，数据以饼图形式呈现，用百分比作为统计单位，点击本地地址，或非本地地址颜色区，可以展开各自所在的扇形区域。

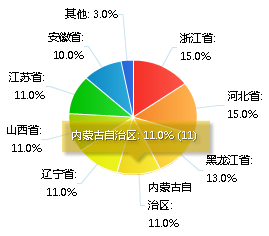
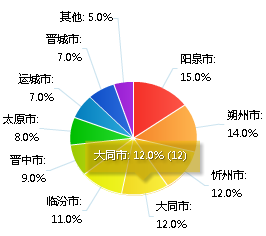
国内访问用户按省份分布描述：

1. 按省市统计用户分布情况，点击各省市所在扇形区域使之展开，将会在“国内访问用户按地市分布”图中展示省市对应的地市用户分布情况。

注意以下几点：

1. 国内访问用户按地市分布图只能展示最近展开的省市扇形图所对应的地市数据。
2. 鼠标停留在任意饼图的扇形区域上面，将突出显示该扇形区的区域信息及百分比数据。

如下图所示：

### 用户浏览器/版本分布-流量分析

用户进入流量分析界面，报表选择“用户浏览器/版本分布”，颗粒度选择“分钟/小时/天/月”，点击查询按钮，查询结果将以饼图方式显示“用户浏览器/版本分布”，具体数据以表格形式展示，以下是各个不同粒度时，用户数统计的查询效果：



图 3-1-3-1用户浏览器/版本分布粒度分钟查询效果

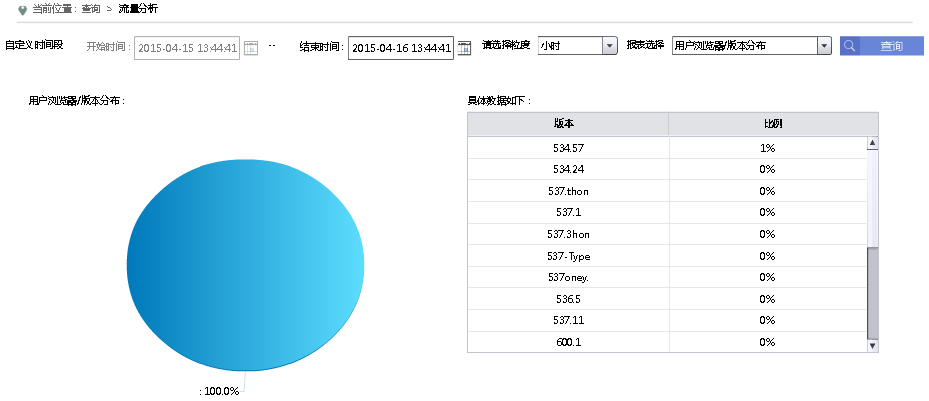


图 3-1-3-2用户浏览器/版本分布粒度小时查询效果

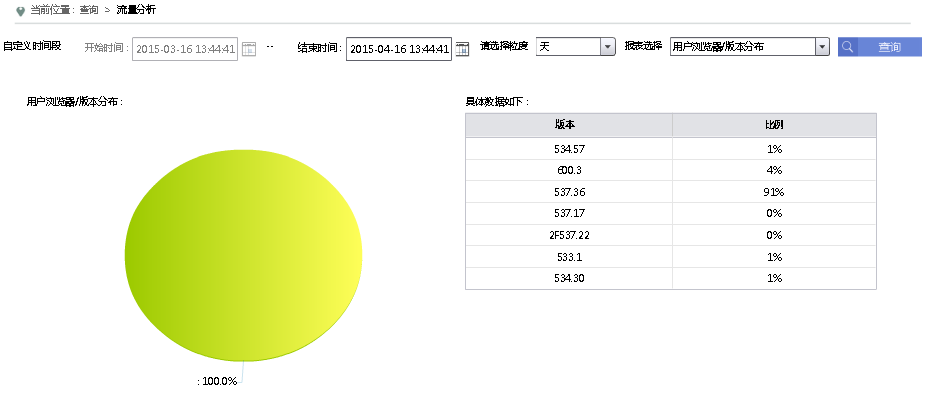


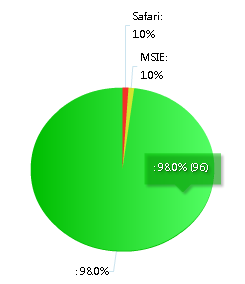
图 3-1-3-3用户浏览器/版本分布粒度天查询效果



图 3-1-3-4用户浏览器/版本分布粒度月查询效果

用户浏览器/版本分布图描述：

1. 以饼图显示各个浏览器的百分比分布情况。
2. 鼠标停留在扇形区，将会显示所在扇形区浏览器的百分比状况。



1. 点击不同的浏览器扇形区，相应的数据表将会在“具体数据表”中显示。

具体数据报表描述：

1. 显示所选扇形区浏览器的版本和各个版本所占的比例。

### 访问时长统计-流量分析

用户进入流量分析界面，报表选择“访问时长统计”，颗粒度选择“分钟/小时/天/月”，点击查询按钮，查询结果将显示“该时段内按分钟统计”表，“该时段内用户平均访问时长变化趋势”图，“该时段内用户访问时长top10”表，以下是各个不同粒度时，访问时长统计的查询效果：

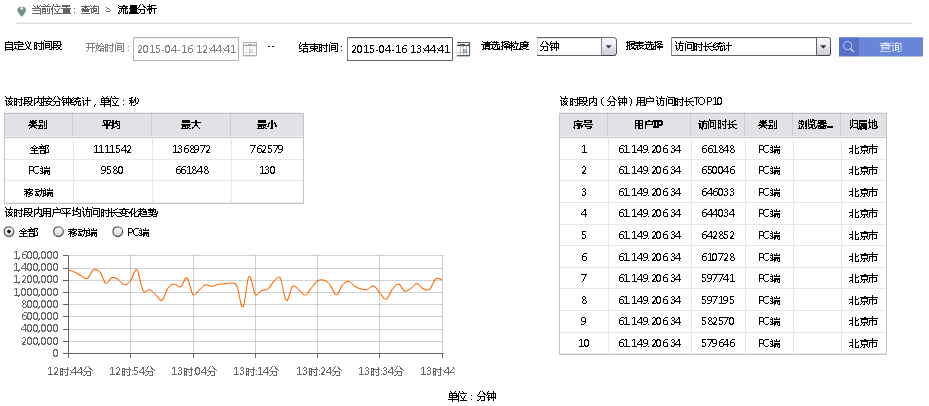


图 3-1-4-1访问时长统计粒度分钟查询效果

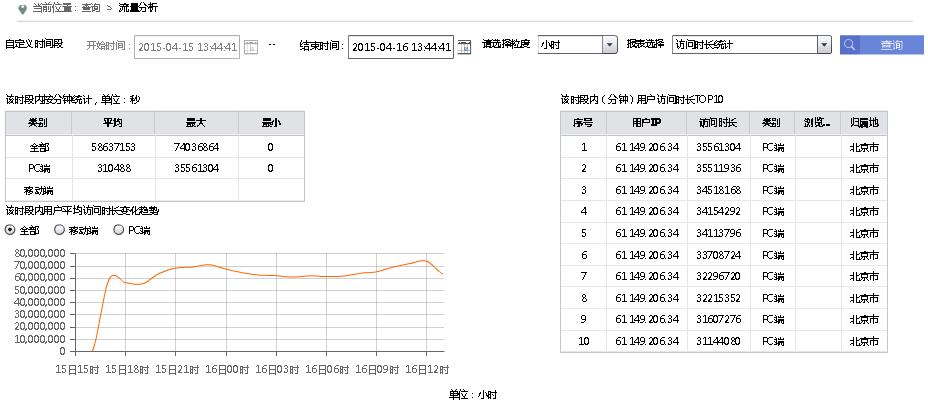


图 3-1-4-2访问时长统计粒度小时查询效果

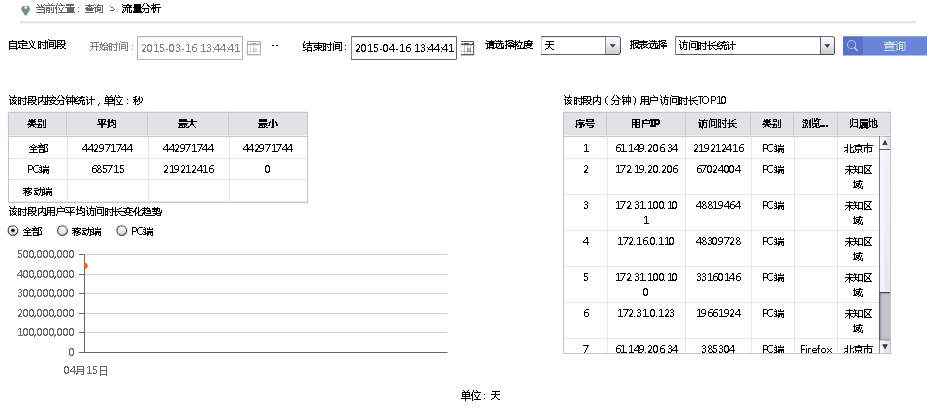


图 3-1-4-3访问时长统计粒度天查询效果



图 3-1-4-4访问时长统计粒度月查询效果

该时段内用户访问时长统计表描述：

1. 分类统计PC端，移动端，及全部的访问时长平均值，最大值，最小值，单位为秒。

该时段内用户平均访问时长变化趋势图描述：

1. 以曲线图形式分类统计PC端，移动端，及全部的用户平均访问时长变化趋势，横坐标为粒度，纵坐标为访问时长单位秒。

该时段内用户访问时长TOP10描述：

1. 统计TOP10的用户IP，访问时长，类别（PC或者手机端），浏览器版本，归属地信息。

### 访问次数统计-流量分析

用户进入流量分析界面，报表选择“访问次数统计”，颗粒度选择“分钟/小时/天/月”，点击查询按钮，查询结果将显示“该时段内用户访问次数统计”表，“该时段内平均访问次数变化趋势”图，“该时段内用户访问次数top10”表，以下是各个不同粒度时，访问次数统计的查询效果：

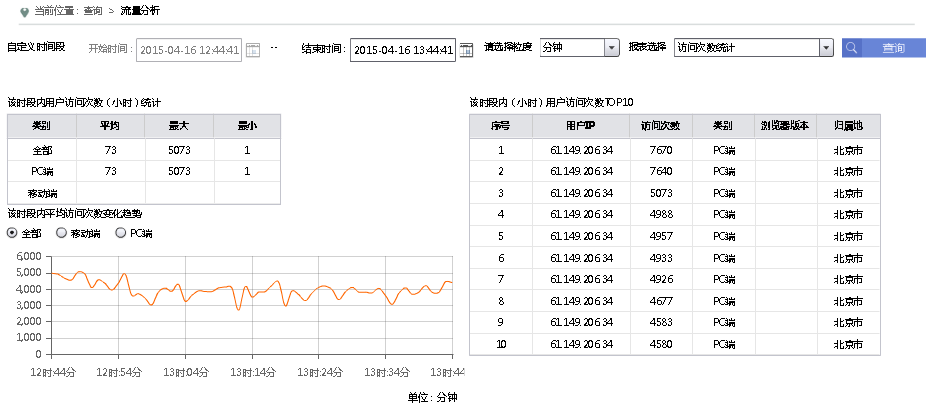


图 3-1-5-1访问次数统计粒度分钟查询效果

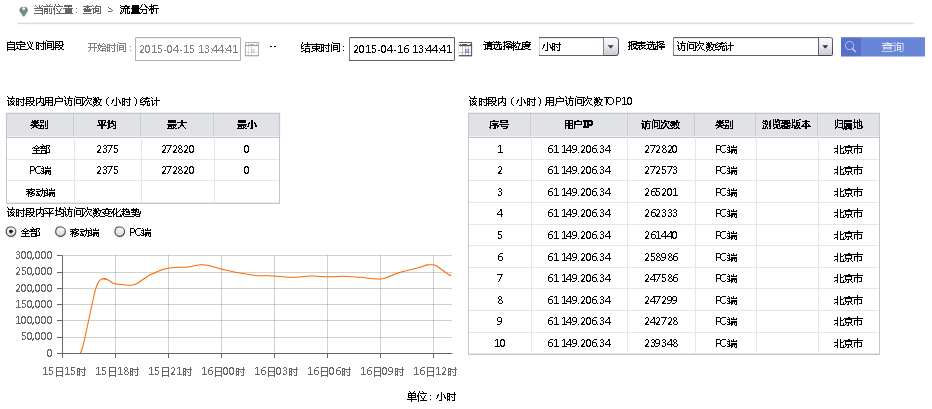


图 3-1-5-2访问次数统计粒度小时查询效果

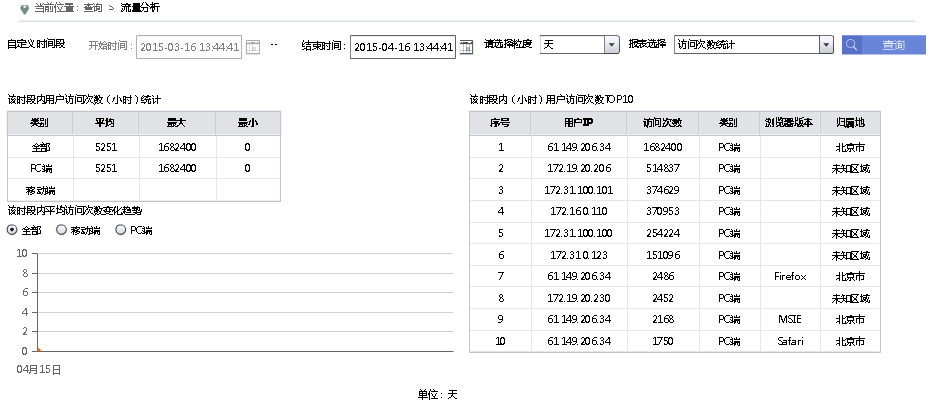


图 3-1-5-3访问次数统计粒度天查询效果

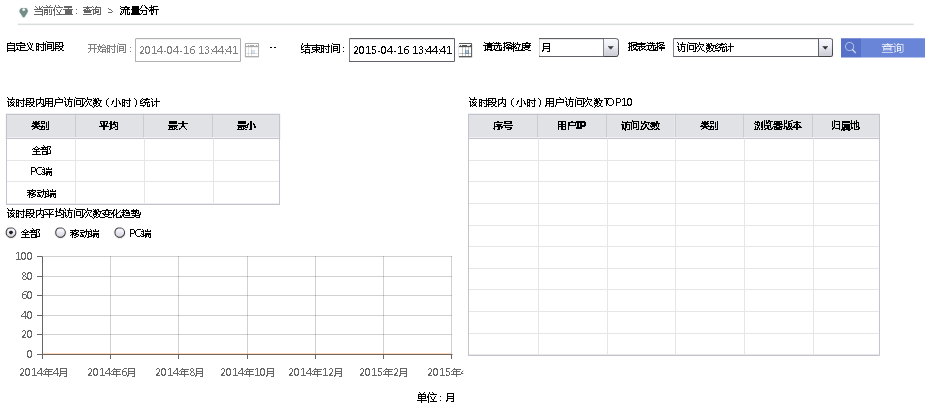


图 3-1-5-4访问次数统计粒度月查询效果

该时段内用户访问次数统计表描述：

1. 分类统计PC端，移动端，及全部的访问时长平均值，最大值，最小值。

该时段内用户平均访问次数变化趋势图描述：

1. 以曲线图形式分类统计PC端，移动端，及全部的用户平均访问次数变化趋势，横坐标为粒度，纵坐标为数值。

该时段内用户访问次数TOP10描述：

1. 统计TOP10的用户IP，访问次数，类别（PC或者手机端），浏览器版本，归属地信息。

### 用户流量统计-流量分析

用户进入流量分析界面，报表选择“用户流量统计”，颗粒度选择“分钟/小时/天/月”，点击查询按钮，查询结果将显示“该时段内用户流量统计”表，“该时段内用户流量变化趋势”图，“该时段内用户流量top10”表，以下是各个不同粒度时，用户流量统计的查询效果：

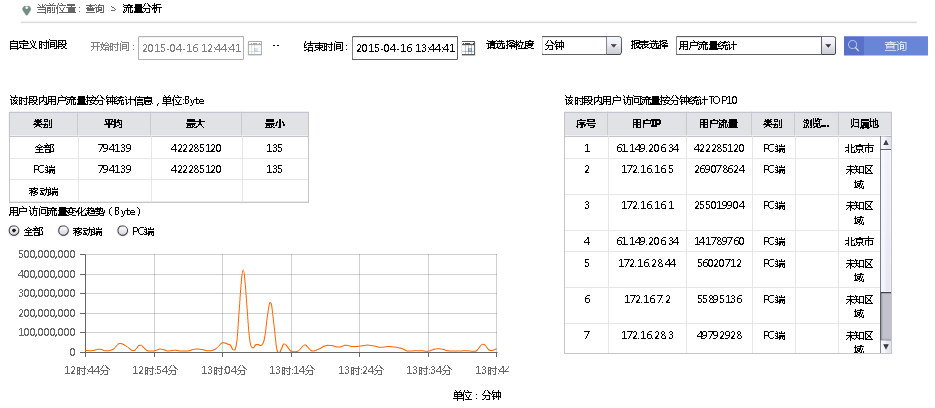


图 3-1-6-1用户流量统计粒度分钟查询效果

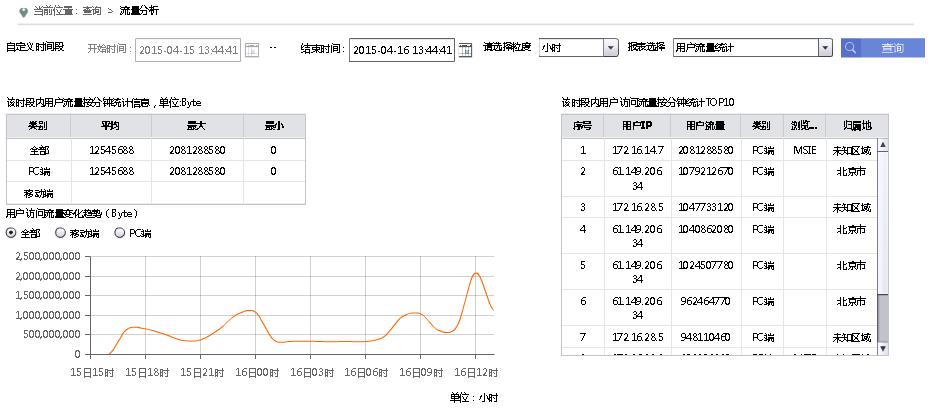


图 3-1-6-2用户流量统计粒度小时查询效果

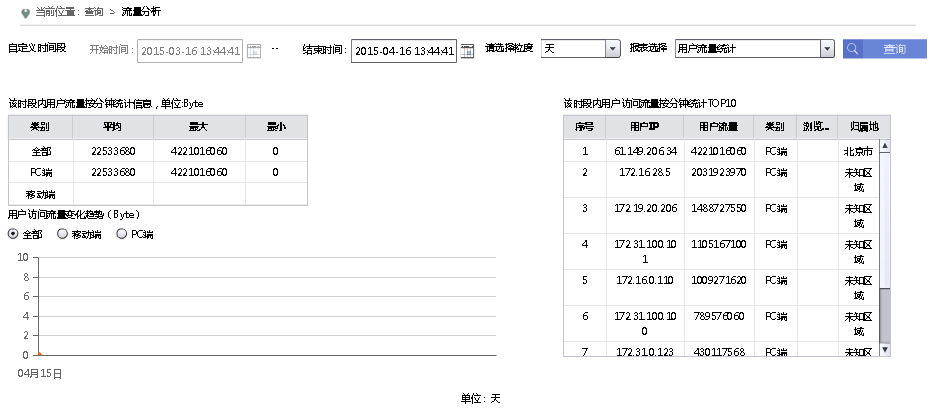


图 3-1-6-3用户流量统计粒度天查询效果



图 3-1-6-4用户流量统计粒度月查询效果

该时段内用户流量统计表描述：

1. 分类统计PC端，移动端，及全部的访问时长平均值，最大值，最小值，单位为Bytes。

该时段内用户流量变化趋势图描述：

1. 以曲线图形式分类统计PC端，移动端，及全部的用户平均访问次数变化趋势，横坐标为粒度，纵坐标为Bytes。

该时段内用户流量TOP10描述：

1. 统计TOP10的用户IP，用户流量，类别（PC或者手机端），浏览器版本，归属地信息。

### TCP连接成功率统计-流量分析

用户进入流量分析界面，报表选择“TCP连接成功率统计”，颗粒度选择“分钟/小时/天/月”，点击查询按钮，查询结果将显示“该时段内TCP连接成功率变化趋势”图，“该时段内TCP连接成功率”表，以下是各个不同粒度时，TCP连接成功率统计的查询效果：

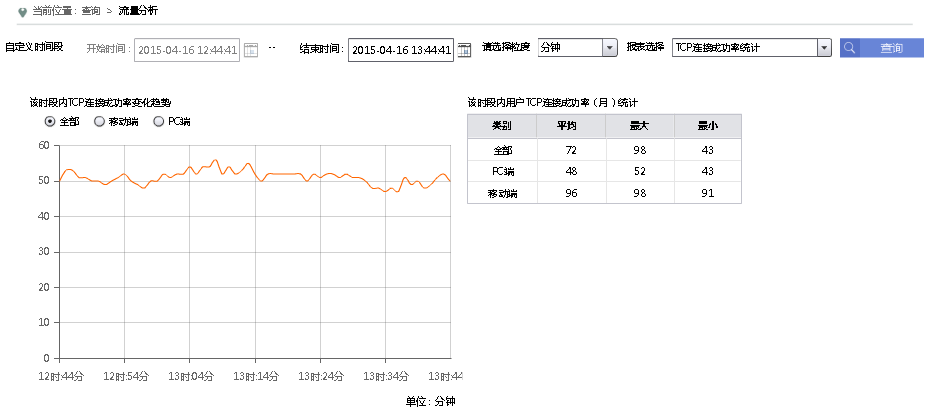


图 3-1-7-1TCP连接成功率统计粒度分钟查询效果

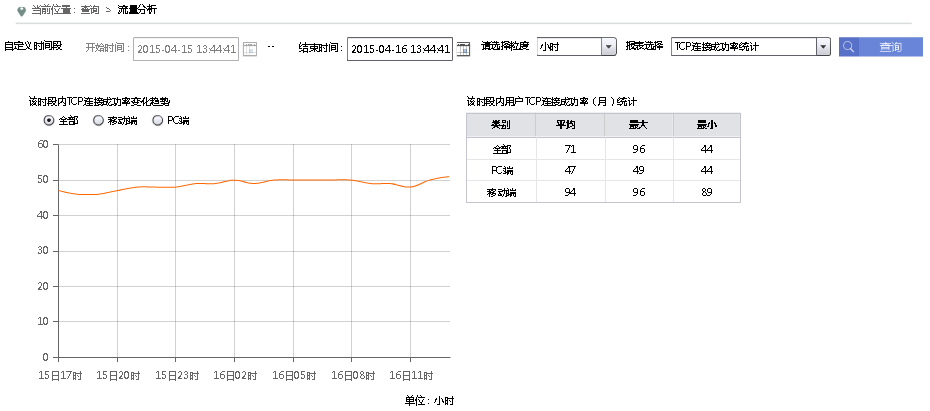


图 3-1-7-2TCP连接成功率统计粒度小时查询效果

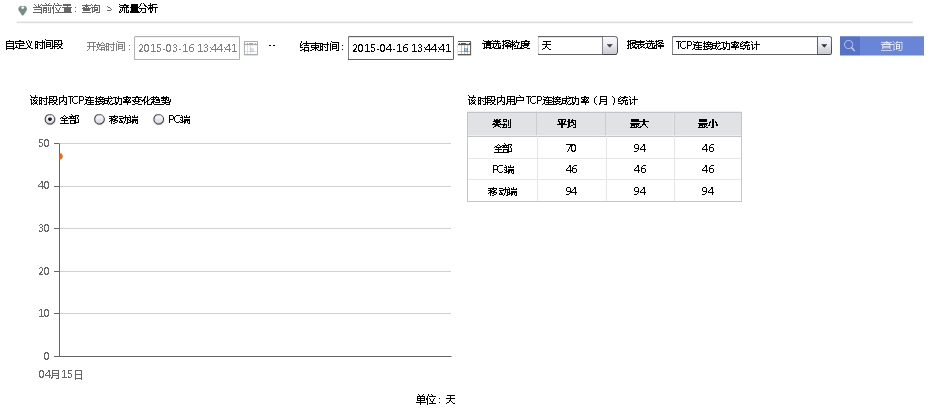


图 3-1-7-3TCP连接成功率统计粒度天查询效果



图 3-1-7-4TCP连接成功率统计粒度月查询效果

该时段内TCP连接成功率变化趋势描述：

1. 以曲线图形式分类统计PC端，移动端，及全部的TCP连接成功率变化趋势，横坐标为粒度，纵坐标为百分比。

该时段内TCP连接成功率统计表描述：

1. 统计PC端，移动端，及全部的TCP连接成功率平均值，最大值，最小值。

## 恶意代码感染事件查询

查询分默认查询及高级查询，进入查询页显示默认查询（开始时间、结束时间、设备名称（管理点独有）），点击“高级查询”按钮进入高级查询条件（感染IP、控制端IP、感染端口、控制端端口、事件名、重要用户、威胁等级）。查询结果包括：威胁等级、事件名、发生次数、开始时间、结束时间、感染IP、控制端IP、感染端口、控制端端口、设备名称，详细信息。



恶意代码感染事件查询效果

**此模块可进行的操作：**

1、查询：查询后的结果包括了威胁等级、事件名、发生次数、开始时间、结束时间、感染IP、控制端IP、感染端口、控制端端口、设备名称，详细信息。右击感染IP或控制端IP能够查询该IP同一时间段内相关的其他6类事件。

2、导出：支持用户对查询结果进行导出，导出文件格式支持TXT/CSV。

3、详细：点击“详情”按钮，可查看事件详细信息，除索引信息外，还包括处置建议、事件描述。

**具体操作说明：**

**时间段的查询：**

1、点击开始时间或结束时间的查询框，会弹出时间选择框（如图所示），点击欲查询的日期，选择后时间选择框会消失。

2、选择某个时间点通过时间选择框左上角的两个时间点的下拉列表可以选择具体的时间点进行查询。

3、点击右上角清除，对已选时间进行清除。

4、点击今天在选择框里会出现当前的时间点（开始时间默认框时间为今天零点，结束时间框默认时间为当前的时间）。



**高级查询：**

点击查询框中的向下的箭头即可进入高级查询，高级查询会出现七个查询框，分别为感染端IP，控制端P，重要用户，事件名，感染端口，控制端口，威胁等级。需要说明的有：

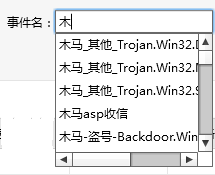
1. 感染端IP和控制端IP需要手动输入1.0.0.0~255.255.255.255范围内的IP，否则校验无法通过。



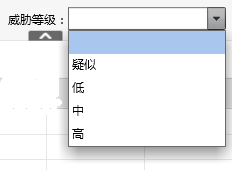
1. 感染端口和控制端口需要手动输入2~65534范围内的端口（包括2和65534），否则校验无法通过。



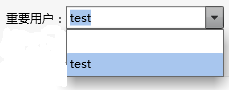
1. 关于事件名查询为模糊查询，如输入“木”后，会出现一个下拉列表，下拉列表里面会出现含有“木”字的一些事件名，如果有想查询的可以直接点击进行查询。如果只输入“木”会查询出所有包含其的事件名，也就是说模糊查询。



1. 威胁等级查询框，此查询框为一个下拉选择框，下拉列表里面包括五项，空、疑似、低、中和高这几个选项可以进行选择查询，如果选择空那么代表此查询框为空。



1. 重要用户查询，在系统设置里面我们可以设置一个IP或者一个IP端为重要用户，设置的这个重要用户会出现在高级查询的下拉列表中，如我们设置一个重要用户test，IP为211.94.163.18。随后在重要用这个下拉会出现test这个重要用户，选择这个重要用户进行查询。

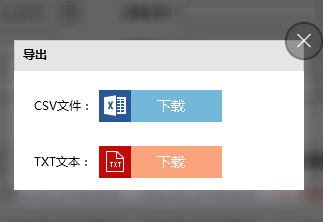


1. 查询出的结果为这个重要用户的IP，211.94.163.18。而且会标记为红色。（不对重要用户查询包含有这个IP的事件也会标记为红色）。



**导出功能：**

1. 导出功能可以导出CSV和TXT两种格式的文件，导出文件的默认名称为report。



1. 导出的文件为当前查询的结果，如查询重要用户，那么导出的文件内容就为重要用户的事件。



**事件详细信息和选择页码：**

1. 点击查询事件列表每条时间最后一个操作的按钮会出现该条时间的详细信息。如图。



1. 如果查询结果过多，通过点击分页下面的下拉列表选择某页，点击go按钮，可以直接跳转到该页。



## 网站事件

查询分默认查询及高级查询，进入查询页显示默认查询（开始时间、结束时间、设备名称（管理点独有）），点击“高级查询”按钮进入高级查询条件（攻击IP、网站IP、攻击端口、网站端口、事件名、重要用户、威胁等级）。查询结果包括：威胁等级、事件名、发生次数、开始时间、结束时间、攻击IP、网站IP、攻击端口、网站端口、设备名称，详细信息。



网站事件查询效果展示图

**此模块可进行的操作：**

1、查询：查询后的结果包括了威胁等级、事件名、发生次数、开始时间、结束时间、攻击IP、网站IP、攻击端口、网站端口、设备名称，详细信息。右击攻击IP或网站IP能够查询该IP同一时间段内相关的其他6类事件。

2、导出：支持用户对查询结果进行导出，导出文件格式支持TXT/CSV。

3、详细：点击“详情”按钮，可查看事件详细信息，除索引信息外，还包括处置建议、事件描述。

**具体操作说明：**

**时间段的查询：**

1、点击开始时间或结束时间的查询框，会弹出时间选择框（如图所示），点击欲查询的日期，选择后时间选择框会消失。

2、选择某个时间点通过时间选择框左上角的两个时间点的下拉列表可以选择具体的时间点进行查询。

3、点击右上角清除，对已选时间进行清除。

4、点击今天在选择框里会出现当前的时间点（开始时间默认框时间为今天零点，结束时间框默认时间为当前的时间）。



**高级查询：**

点击查询框中的向下的箭头即可进入高级查询，高级查询会出现七个查询框，分别为攻击IP，网站IP，重要用户，事件名，攻击端口、网站端口和威胁等级。需要说明的有：

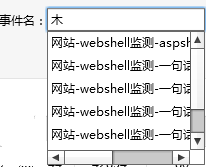
1. 攻击IP和网站IP需要手动输入1.0.0.0~255.255.255.255范围内的IP，否则校验无法通过。



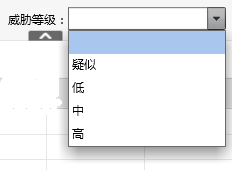
1. 攻击端口和网站端口需要手动输入2~65534范围内的端口（包括2和65534），否则校验无法通过。



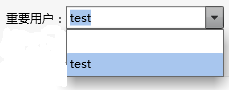
1. 关于事件名查询为模糊查询，如输入“木”后，会出现一个下拉列表，下拉列表里面会出现含有“木”字的一些事件名，如果有想查询的可以直接点击进行查询。如果只输入“木”会查询出所有包含其的事件名，也就是说模糊查询。



1. 威胁等级查询框，此查询框为一个下拉选择框，下拉列表里面包括五项，空、疑似、低、中和高这几个选项可以进行选择查询，如果选择空那么代表此查询框为空。



1. 重要用户查询，在系统设置里面我们可以设置一个IP或者一个IP端为重要用户，设置的这个重要用户会出现在高级查询的下拉列表中，如我们设置一个重要用户test，IP为59.188.253.173。随后在重要用这个下拉会出现test这个重要用户，选择这个重要用户进行查询。

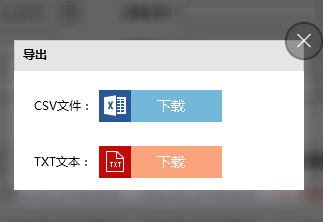


查询出的结果为这个重要用户的IP，59.188.253.173。而且会标记为红色。（不对重要用户查询包含有这个IP的事件也会标记为红色）。



**导出功能：**

1. 导出功能可以导出CSV和TXT两种格式的文件，导出文件的默认名称为report。



1. 导出的文件为当前查询的结果，如查询重要用户，那么导出的文件内容就为重要用户的事件。



**事件详细信息和选择页码：**

1. 点击查询事件列表每条时间最后一个操作的按钮会出现该条时间的详细信息。如图。

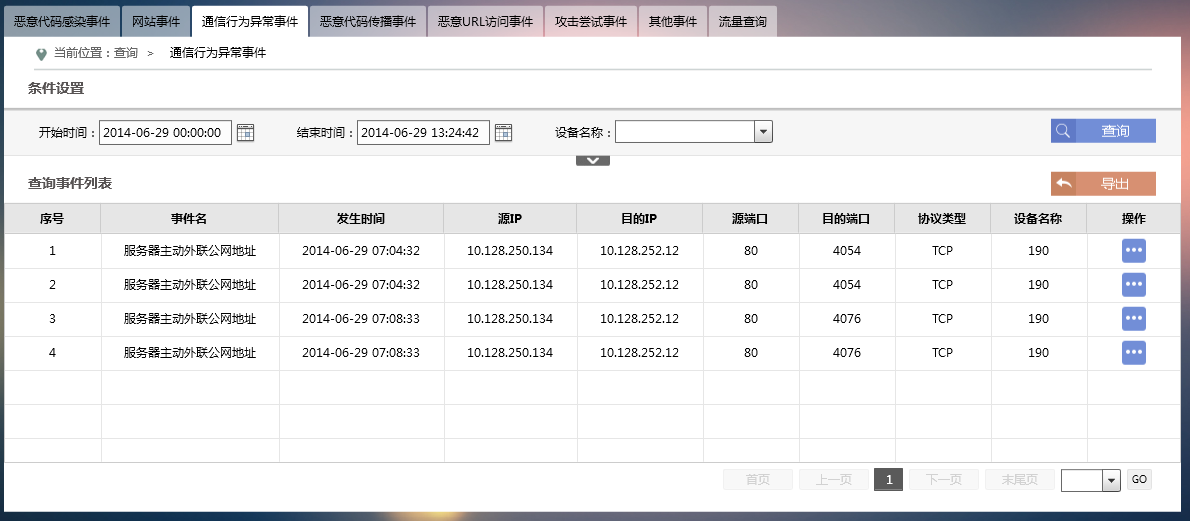


1. 如果查询结果过多，通过点击分页下面的下拉列表选择某页，点击go按钮，可以直接跳转到该页。



## 通信行为异常事件

查询分默认查询及高级查询，进入查询页显示默认查询（开始时间、结束时间、设备名称（管理点独有）），点击“高级查询”按钮进入高级查询条件（源IP、目的IP、源端口、目的端口、事件名、重要用户、威胁等级）。查询结果包括：威胁等级、事件名、发生次数、开始时间、结束时间、源IP、目的IP、源端口、目的端口、设备名称，详细信息。



网站事件查询效果展示图

**此模块可进行的操作：**

1、查询：查询后的结果包括了威胁等级、事件名、发生次数、开始时间、结束时间、源IP、目的IP、源端口、目的端口、设备名称，详细信息。右击源IP或目的IP能够查询该IP同一时间段内相关的其他6类事件。

2、导出：支持用户对查询结果进行导出，导出文件格式支持TXT/CSV。

3、详细：点击“详情”按钮，可查看事件详细信息，除索引信息外，还包括处置建议、事件描述。

**时间段的查询：**

1、点击开始时间或结束时间的查询框，会弹出时间选择框（如图所示），点击欲查询的日期，选择后时间选择框会消失。

2、选择某个时间点通过时间选择框左上角的两个时间点的下拉列表可以选择具体的时间点进行查询。

3、点击右上角清除，对已选时间进行清除。

4、点击今天在选择框里会出现当前的时间点（开始时间默认框时间为今天零点，结束时间框默认时间为当前的时间）。



**高级查询：**

点击查询框中的向下的箭头即可进入高级查询，高级查询会出现七个查询框，分别为源IP，目的IP，重要用户，事件名，源端口，目的端口，威胁等级。需要说明的有：

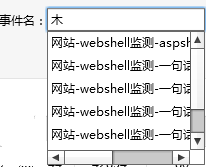
1. 源IP和目的IP需要手动输入1.0.0.0~255.255.255.255范围内的IP，否则校验无法通过。



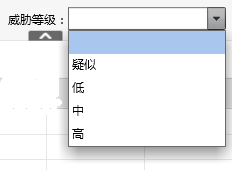
1. 源端口和目的端口需要手动输入2~65534范围内的端口（包括2和65534），否则校验无法通过。



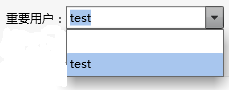
1. 关于事件名查询为模糊查询，如输入“木”后，会出现一个下拉列表，下拉列表里面会出现含有“木”字的一些事件名，如果有想查询的可以直接点击进行查询。如果只输入“木”会查询出所有包含其的事件名，也就是说模糊查询。



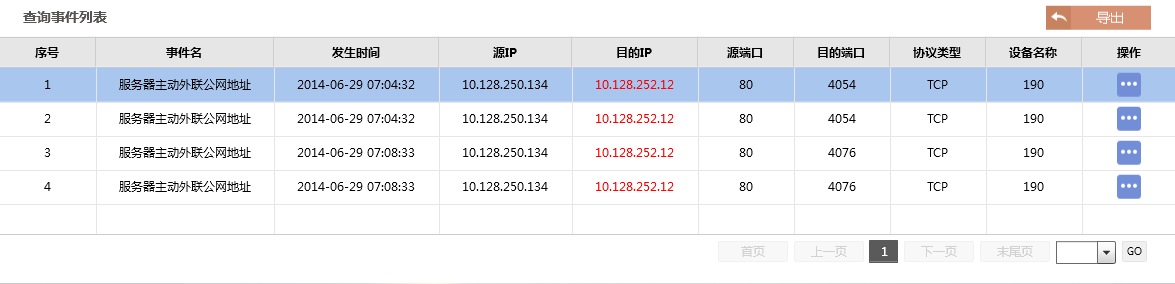
1. 威胁等级查询框，此查询框为一个下拉选择框，下拉列表里面包括五项，空、疑似、低、中和高这几个选项可以进行选择查询，如果选择空那么代表此查询框为空。



1. 重要用户查询，在系统设置里面我们可以设置一个IP或者一个IP端为重要用户，设置的这个重要用户会出现在高级查询的下拉列表中，如我们设置一个重要用户test，IP为10.128.252.12。随后在重要用这个下拉会出现test这个重要用户，选择这个重要用户进行查询。

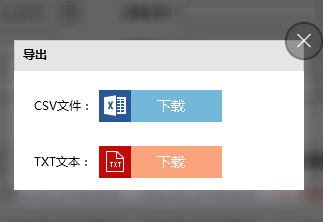


查询出的结果为这个重要用户的IP，10.128.252.12。而且会标记为红色。（不对重要用户查询包含有这个IP的事件也会标记为红色）。



**导出功能：**

1. 导出功能可以导出CSV和TXT两种格式的文件，导出文件的默认名称为report。



1. 导出的文件为当前查询的结果，如查询重要用户，那么导出的文件内容就为重要用户的事件。



**事件详细信息和选择页码：**

1. 点击查询事件列表每条时间最后一个操作的按钮会出现该条时间的详细信息。如图。



1. 如果查询结果过多，通过点击分页下面的下拉列表选择某页，点击go按钮，可以直接跳转到该页。



## 统计报表

## 恶意代码传播事件查询

查询分默认查询及高级查询，进入查询页显示默认查询（开始时间、结束时间、病毒类型、设备名称（管理点独有）），点击“高级查询”按钮进入高级查询条件（传播IP、受害IP、传播端口、受害端口、病毒名、重要用户、威胁等级、协议类型）。查询结果包括：威胁等级、病发生时间开始时间、结束时间、传播IP、受害IP、传播端口、受害端口、设备名称、协议类型，详细信息。



恶意代码传播事件查询效果展示图

**此模块可进行的操作：**

1、查询：查询后的结果包括了威胁等级、病发生时间开始时间、结束时间、传播IP、受害IP、传播端口、受害端口、设备名称、协议类型，详细信息。右击传播IP或受害IP能够查询该IP同一时间段内相关的其他6类事件

2、导出：支持用户对查询结果进行导出，导出文件格式支持TXT/CSV。

3、详细：点击“详情”按钮，可查看事件详细信息，除索引信息外，还包括处置建议、事件描述。

**时间段的查询：**

1、点击开始时间或结束时间的查询框，会弹出时间选择框（如图所示），点击欲查询的日期，选择后时间选择框会消失。

2、选择某个时间点通过时间选择框左上角的两个时间点的下拉列表可以选择具体的时间点进行查询。

3、点击右上角清除，对已选时间进行清除。

4、点击今天在选择框里会出现当前的时间点（开始时间默认框时间为今天零点，结束时间框默认时间为当前的时间）。



**普通查询：**

* 1. 病毒类型查询框为一个下拉列表，可以在下拉列表中选取将要查询的病毒名称进行查询。
  2. 设备名称查询框为一个下拉列表，管理点设备在下拉列表里面会出现下级的设备名称，选择设备名称进行查询。

**高级查询：**

点击查询框中的向下的箭头即可进入高级查询，高级查询会出现七个查询框，分别为传播源IP，受害IP，重要用户，协议类型，传播端口，受害端口，威胁等级和病毒名称。需要说明的有：

* 1. 传播源IP和目的IP需要手动输入1.0.0.0~255.255.255.255范围内的IP，否则校验无法通过。



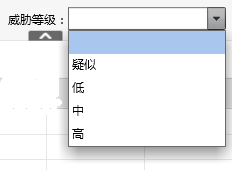
* 1. 传播端口和受害端口需要手动输入2~65534范围内的端口（包括2和65534），否则校验无法通过。



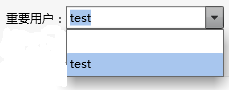
* 1. 关于病毒名称查询为模糊查询，如输入“V”后，查询出的结果病毒名称里面都含有字母“V”



* 1. 威胁等级查询框，此查询框为一个下拉选择框，下拉列表里面包括五项，空、疑似、低、中和高这几个选项可以进行选择查询，如果选择空那么代表此查询框为空。



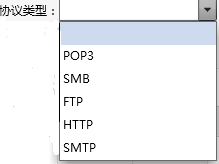
* 1. 重要用户查询，在系统设置里面我们可以设置一个IP或者一个IP端为重要用户，设置的这个重要用户会出现在高级查询的下拉列表中，如我们设置一个重要用户test，IP为10.128.252.12。随后在重要用这个下拉会出现test这个重要用户，选择这个重要用户进行查询。



* 1. 查询出的结果为这个重要用户的IP，10.128.252.12。而且会标记为红色。（不对重要用户查询包含有这个IP的事件也会标记为红色）。

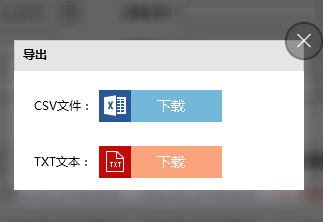


* 1. 协议类型查询框为一个下拉列表，通过选择下拉列表里面的协议类型进行查询，下拉列表包括POP3,SMB,FTP,HTTP和SMTP五中协议类型。

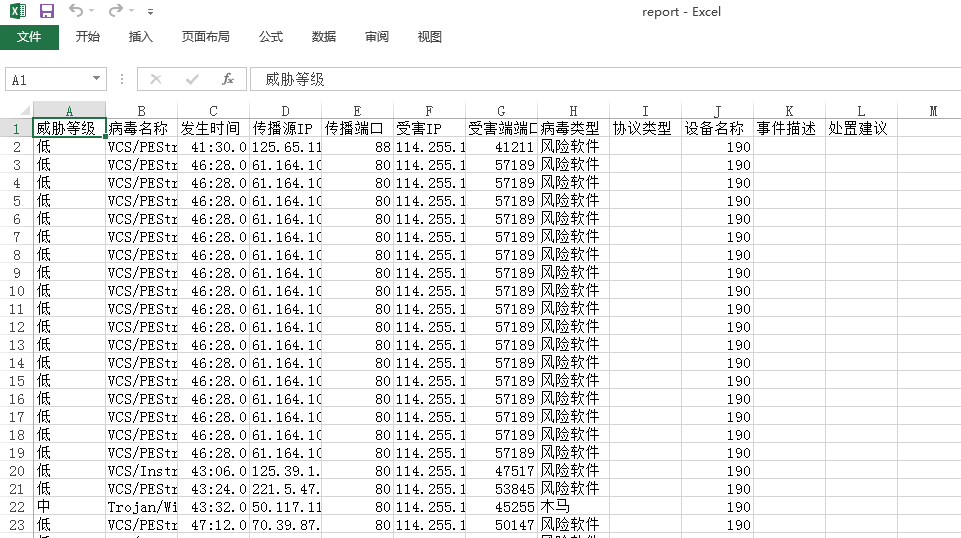


**导出功能：**

1. 导出功能可以导出CSV和TXT两种格式的文件，导出文件的默认名称为report。



1. 导出的文件为当前查询的结果，如查询重要用户，那么导出的文件内容就为重要用户的事件。



**事件详细信息和选择页码：**

1. 点击查询事件列表每条时间最后一个操作的按钮会出现该条时间的详细信息。如图。



1. 如果查询结果过多，通过点击分页下面的下拉列表选择某页，点击go按钮，可以直接跳转到该页。



## 恶意URL访问事件查询

查询分默认查询及高级查询，进入查询页显示默认查询（开始时间、结束时间、病毒类型、设备名称（管理点独有）），点击“高级查询”按钮进入高级查询条件（访问IP、服务器IP、访问端口、服务器端口、URL）。查询结果包括：威胁等级、事件名、发生次数、开始时间、结束时间、攻击IP、被攻击IP、攻击端口、被攻击端口、设备名称，详细信息。



恶意URL访问事件查询

**此模块可进行的操作：**

1、查询：查询后的结果包括了威胁等级、事件名、发生次数、开始时间、结束时间、攻击IP、被攻击IP、攻击端口、被攻击端口、设备名称，详细信息。右击攻击IP或被攻击IP能够查询该IP同一时间段内相关的其他6类事件

2、导出：支持用户对查询结果进行导出，导出文件格式支持TXT/CSV。

3、详细：点击“详情”按钮，可查看事件详细信息，除索引信息外，还包括处置建议、事件描述。

**时间段的查询：**

1、点击开始时间或结束时间的查询框，会弹出时间选择框（如图所示），点击欲查询的日期，选择后时间选择框会消失。

2、选择某个时间点通过时间选择框左上角的两个时间点的下拉列表可以选择具体的时间点进行查询。

3、点击右上角清除，对已选时间进行清除。

4、点击今天在选择框里会出现当前的时间点（开始时间默认框时间为今天零点，结束时间框默认时间为当前的时间）。



**普通查询：**

设备名称查询框为一个下拉列表，管理点设备在下拉列表里面会出现下级的设备名称，选择设备名称进行查询。

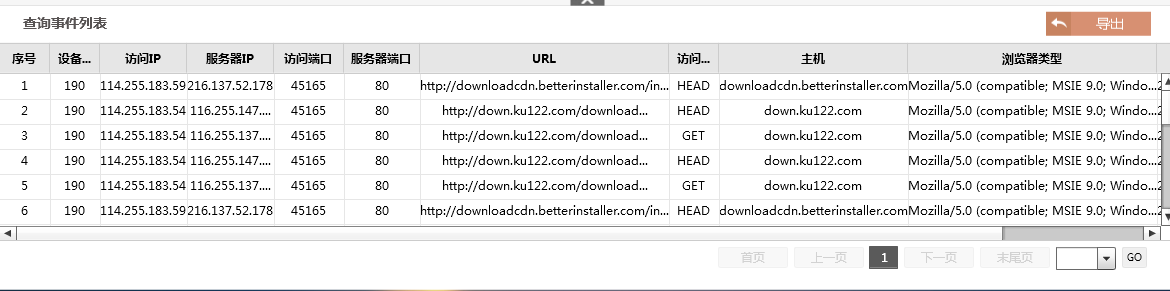
**高级查询：**

点击查询框中的向下的箭头即可进入高级查询，高级查询会出现七个查询框，分别为传播源IP，受害IP，重要用户，协议类型，传播端口，受害端口，威胁等级和病毒名称。需要说明的有：

1. 访问IP和服务器IP需要手动输入1.0.0.0~255.255.255.255范围内的IP，否则校验无法通过。



1. 关于主机查询为模糊查询，如输入“d”后，查询出的结果病毒名称里面都含有字母“V”



1. 关于URL查询为模糊查询，如输入“2”后，查询出的结果病毒名称里面都含有数字“2”

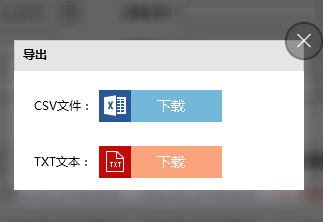


1. 协议类型查询框为一个下拉列表，通过选择下拉列表里面的协议类型进行查询，下拉列表包括GET和POST两种协议类型。



**导出功能：**

1. 导出功能可以导出CSV和TXT两种格式的文件，导出文件的默认名称为report。



1. 导出的文件为当前查询的结果，如查询访问方式为GET，那么导出的文件内容就为访问方式为GET的事件。



**事件详细信息和选择页码：**

1. 点击查询事件列表每条时间最后一个操作的按钮会出现该条时间的详细信息。如图。



1. 如果查询结果过多，通过点击分页下面的下拉列表选择某页，点击go按钮，可以直接跳转到该页。



## 攻击尝试事件查询

查询分默认查询及高级查询，进入查询页显示默认查询（开始时间、结束时间、设备名称（管理点独有）），点击“高级查询”按钮进入高级查询条件（攻击IP、被攻击IP、攻击端口、被攻击端口、事件名、重要用户、威胁等级）。查询结果包括：威胁等级、事件名、发生次数、开始时间、结束时间、攻击IP、被攻击IP、攻击端口、被攻击端口、设备名称，详细信息。



攻击尝试事件查询

**此模块可进行的操作：**

1、查询：查询后的结果包括了威胁等级、事件名、发生次数、开始时间、结束时间、攻击IP、被攻击IP、攻击端口、被攻击端口、设备名称，详细信息。右击攻击IP或被攻击IP能够查询该IP同一时间段内相关的其他6类事件

2、导出：支持用户对查询结果进行导出，导出文件格式支持TXT/CSV。

3、详细：点击“详情”按钮，可查看事件详细信息，除索引信息外，还包括处置建议、事件描述。

**时间段的查询：**

1、点击开始时间或结束时间的查询框，会弹出时间选择框（如图所示），点击欲查询的日期，选择后时间选择框会消失。

2、选择某个时间点通过时间选择框左上角的两个时间点的下拉列表可以选择具体的时间点进行查询。

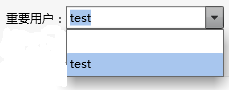
3、点击右上角清除，对已选时间进行清除。

4、点击今天在选择框里会出现当前的时间点（开始时间默认框时间为今天零点，结束时间框默认时间为当前的时间）。



**普通查询：**

1. 重要用户查询，在系统设置里面我们可以设置一个IP或者一个IP端为重要用户，设置的这个重要用户会出现在高级查询的下拉列表中，如我们设置一个重要用户test，IP为211.94.163.5。随后在重要用这个下拉会出现test这个重要用户，选择这个重要用户进行查询。



查询出的结果为这个重要用户的IP，211.94.163.5。而且会标记为红色。（不对重要用户查询包含有这个IP的事件也会标记为红色）。



**高级查询：**

点击查询框中的向下的箭头即可进入高级查询，高级查询会出现七个查询框，分别为感染端IP，控制端P，重要用户，事件名，感染端口，控制端口，威胁等级。需要说明的有：

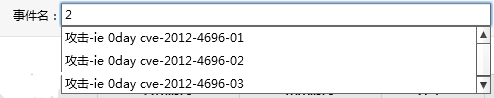
1. 攻击IP和被攻击IP需要手动输入1.0.0.0~255.255.255.255范围内的IP，否则校验无法通过。



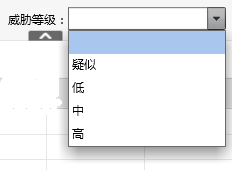
1. 攻击端口和被攻击端口需要手动输入2~65534范围内的端口（包括2和65534），否则校验无法通过。



1. 关于事件名查询为模糊查询，如输入“2”后，会出现一个下拉列表，下拉列表里面会出现含有“2”字的一些事件名，如果有想查询的可以直接点击进行查询。如果只输入“2”会查询出所有包含其的事件名，也就是说模糊查询。

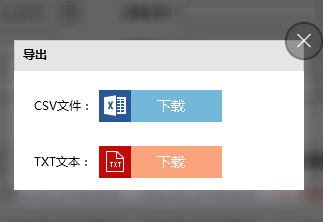


1. 威胁等级查询框，此查询框为一个下拉选择框，下拉列表里面包括五项，空、疑似、低、中和高这几个选项可以进行选择查询，如果选择空那么代表此查询框为空。

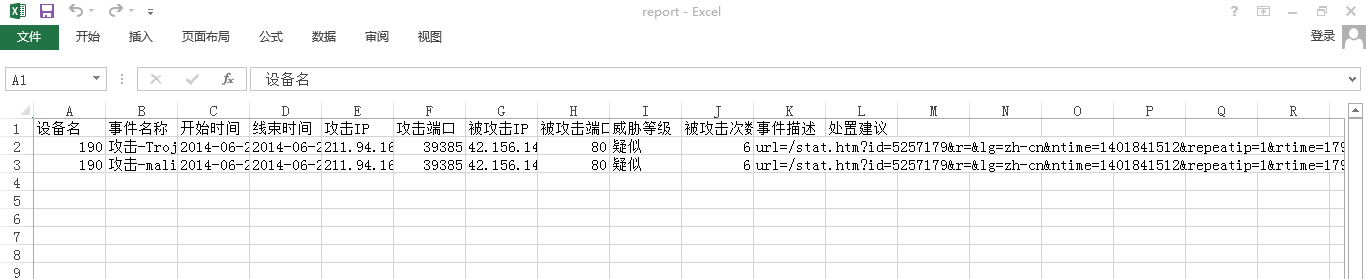


**导出功能：**

1. 导出功能可以导出CSV和TXT两种格式的文件，导出文件的默认名称为report。



1. 导出的文件为当前查询的结果，如查询重要用户，那么导出的文件内容就为重要用户的事件。



**事件详细信息和选择页码：**

1. 点击查询事件列表每条时间最后一个操作的按钮会出现该条时间的详细信息。如图。



1. 如果查询结果过多，通过点击分页下面的下拉列表选择某页，点击go按钮，可以直接跳转到该页。



## 其他事件查询

查询分默认查询及高级查询，进入查询页显示默认查询（开始时间、结束时间、设备名称（管理点独有）），点击“高级查询”按钮进入高级查询条件（攻击IP、被攻击IP、攻击端口、被攻击端口、事件名、重要用户、威胁等级）。查询结果包括：威胁等级、事件名、发生次数、开始时间、结束时间、攻击IP、被攻击IP、攻击端口、被攻击端口、设备名称，详细信息。



其他事件查询

**此模块可进行的操作：**

1、查询：查询后的结果包括了威胁等级、事件名、发生次数、开始时间、结束时间、攻击IP、被攻击IP、攻击端口、被攻击端口、设备名称，详细信息。右击攻击IP或被攻击IP能够查询该IP同一时间段内相关的其他6类事件。

2、导出：支持用户对查询结果进行导出，导出文件格式支持TXT/CSV。

3、详细：点击“详情”按钮，可查看事件详细信息，除索引信息外，还包括处置建议、事件描述。

**时间段的查询：**

1、点击开始时间或结束时间的查询框，会弹出时间选择框（如图所示），点击欲查询的日期，选择后时间选择框会消失。

2、选择某个时间点通过时间选择框左上角的两个时间点的下拉列表可以选择具体的时间点进行查询。

3、点击右上角清除，对已选时间进行清除。

4、点击今天在选择框里会出现当前的时间点（开始时间默认框时间为今天零点，结束时间框默认时间为当前的时间）。



**高级查询：**

点击查询框中的向下的箭头即可进入高级查询，高级查询会出现七个查询框，分别为感染端IP，控制端P，重要用户，事件名，感染端口，控制端口，威胁等级。需要说明的有：

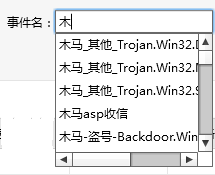
1. 攻击IP和被攻击IP需要手动输入1.0.0.0~255.255.255.255范围内的IP，否则校验无法通过。



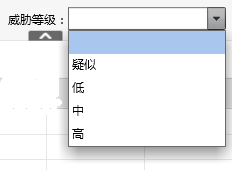
1. 攻击端口和被攻击端口需要手动输入2~65534范围内的端口（包括2和65534），否则校验无法通过。



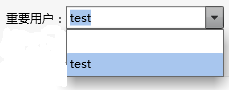
1. 关于事件名查询为模糊查询，如输入“木”后，会出现一个下拉列表，下拉列表里面会出现含有“木”字的一些事件名，如果有想查询的可以直接点击进行查询。如果只输入“木”会查询出所有包含其的事件名，也就是说模糊查询。



1. 威胁等级查询框，此查询框为一个下拉选择框，下拉列表里面包括五项，空、疑似、低、中和高这几个选项可以进行选择查询，如果选择空那么代表此查询框为空。



1. 重要用户查询，在系统设置里面我们可以设置一个IP或者一个IP端为重要用户，设置的这个重要用户会出现在高级查询的下拉列表中，如我们设置一个重要用户test，IP为111.205.62.201。随后在重要用这个下拉会出现test这个重要用户，选择这个重要用户进行查询。

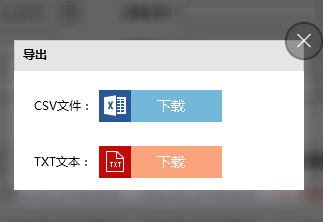


1. 查询出的结果为这个重要用户的IP，111.205.62.201。而且会标记为红色。（不对重要用户查询包含有这个IP的事件也会标记为红色）。



**导出功能：**

1. 导出功能可以导出CSV和TXT两种格式的文件，导出文件的默认名称为report。



1. 导出的文件为当前查询的结果，如查询重要用户，那么导出的文件内容就为重要用户的事件。



**事件详细信息和选择页码：**

1. 点击查询事件列表每条时间最后一个操作的按钮会出现该条时间的详细信息。如图。



1. 如果查询结果过多，通过点击分页下面的下拉列表选择某页，点击go按钮，可以直接跳转到该页。



## 流量查询

流量查询模块默认展示的为最近半小时流量。此处不同于首页最近流量曲线的是可以对历史的流量进行查询。通过输入查询条件：开始时间、结束时间、流量单位、设备名称、自定义流量来进行查询。



流量查询效果展示图

**此模块可进行的操作：**

* 1. 查询：输入开始时间、结束时间、流量单位、设备名称、自定义流量来进行查询，其中自定义流量为下拉框形式。

**时间段的查询：**

1、点击开始时间或结束时间的查询框，会弹出时间选择框（如图所示），点击欲查询的日期，选择后时间选择框会消失。

2、选择某个时间点通过时间选择框左上角的两个时间点的下拉列表可以选择具体的时间点进行查询。

3、点击右上角清除，对已选时间进行清除。

4、点击今天在选择框里会出现当前的时间点（开始时间默认框时间为今天零点，结束时间框默认时间为当前的时间）。

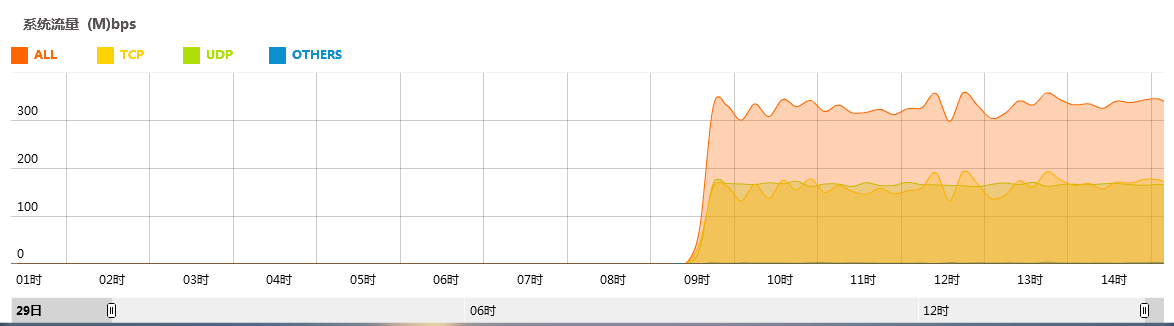


**普通查询：**

1. 流量类型查询框为一个下拉列表，可以在下拉列表中选取将要查询的流量类型进行查询。（流量类型包括两种分别为bps和pps）
2. 设备名称查询框为一个下拉列表，管理点设备在下拉列表里面会出现下级的设备名称，选择设备名称进行查询。
3. 在系统管理里面，添加一个自定义流量“test”，添加过后会在此查询框显示自定义流量名称“test”，点击这个名称进行查询。

**系统流量查询结果：**

* 1. 流量查询结果是以坐标轴和曲线形式展现给用户的，用户可以通过点击坐标轴上方的流量名称来选择自己想要关注的流量曲线，每种流量曲线以颜色区分，横轴为时间轴，纵轴为流量轴。



* 1. 用户可以在流量曲线上横向拖动光标，来放大要观察的流量曲线，点击还原流量曲线回到初始位置。
  2. 用户可以通过拖动时间轴下面的两个滑块来选择要观察的时间段的范围。

# 章节 报表

## 报表下载

报表类型包括：日报/周报/月报/年报。每类报表均支持word格式。

报表命名规范：

日报：yyyy-mm-dd日报表.doc；

周报：yyyy年第n周(mm月dd日-mm月dd日)周报表.doc；（以周一作为一周开始,周跨年/月时，以周一所在年月为准）

月报：yyyy-mm月报表.doc；

年报：yyyy年报表.doc



报表下载效果展示图

**此模块可进行的操作：**

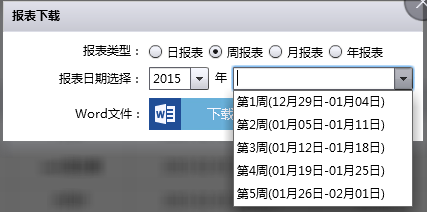
1、下载：进行日报/周报/月报/年报的下载。

**此模块的操作流程：**

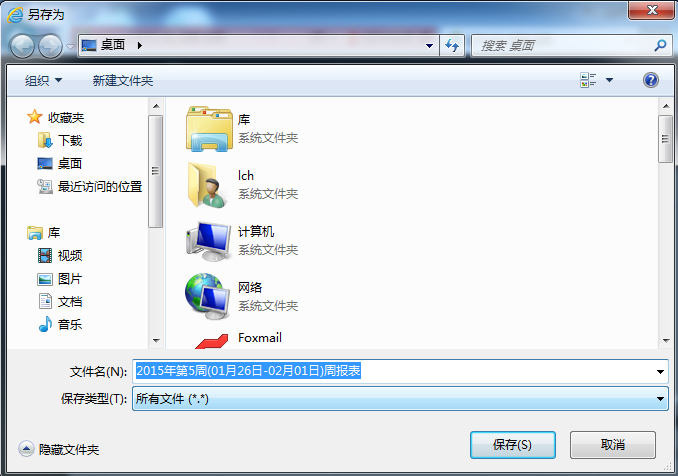
1. 点击“报表下载”，会弹出图3-1报表下载页
2. 选择报表类型



1. 选择报表日期



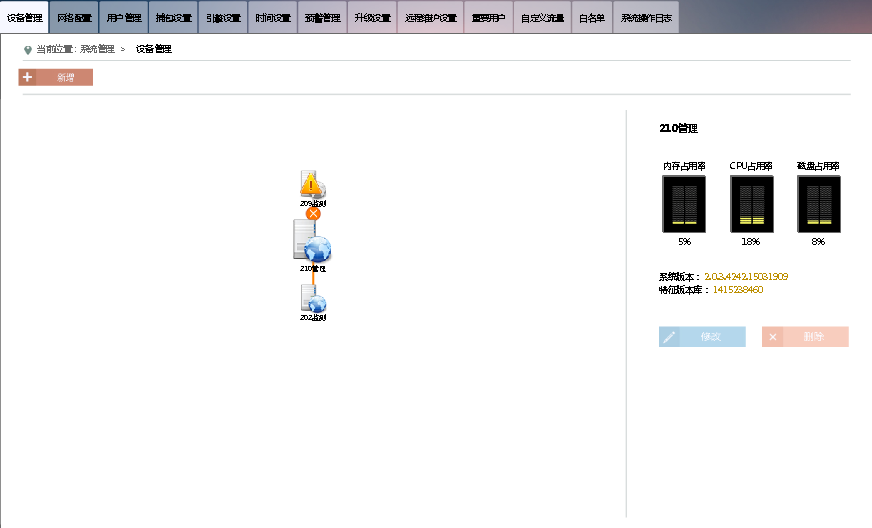
1. 点击，将报表下载到本地，可选任意路径存放。



# 章节 系统管理

## 设备管理

设备管理信息分左右两栏显示，左边显示设备拓扑图，右边默认显示当前设备的资源占用情况；详情包括：内存占用率，CPU占用率，磁盘占用率，系统版本和特征库版本。在设备状态树上展示设备正常/异常(异常叹号)、通讯正常/异常（异常虚线、叉号）、注册进行中/完成



设备管理效果展示图

**对于监测点此模块不能进行任何操作**

**对于管理点/顶级节点此模块可进行的操作：**

1、新增设备：增加设备名称、设备IP、文件通道端口、命令通道端口、联系人、联系方式、备注，是否接入云，保存后直接将设备添加到拓扑中。

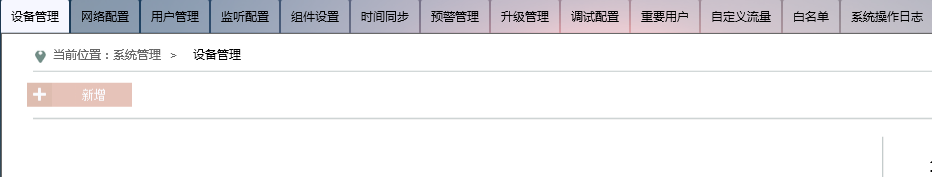
2、首页展示：新增设备后会在首页系统状态下“设备拓扑图中展示”。

3、修改设备信息：在设备管理界面中选择需要修改的设备，右边显示所选设备的资源占用情况，点击下方的修改按钮，可以进行相关信息的修改，可修改的信息包括联系人，联系电话，备注。

4、删除设备：点击删除按钮进行设备的删除。注意：不可删除根节点；若删除普通管理点，其对应下级设备一并删除。

**此模块的操作流程：**

1. 进入“系统管理”，点击“设备管理”
2. 如果用户想要添加设备，点击“新增”



点击新增按钮，会弹出

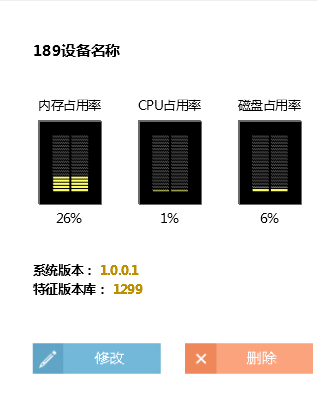


根据上图进行填写然后点击“保存”，设备就添加成功了

1. 添加成功后，设备就会在首页系统状态和设备管理中显示



1. 根据设备的显示可以判断设备的连接情况，如果像上图中185的状态就说明，185没有与上级连接，而189的状态是连接正常状态
2. 点击除本机以外任一设备，都可在右侧看到它的系统状态



1. 对添加的设备，可做修改操作，点击



会弹出



可进行修改

1. 点击可将设备删除

## 网络配置

此模块主记录了网络配置的相关信息，代理的启动与关闭操作。

主要展示信息;设备名称、最大上传速度、最大下载速度、设备IP地址、子网掩码、网关地址、DNS1、DNS2、命令端口、文件传输端口、启动代理、代理协议、代理服务器域名/IP、服务器PORT、用户名、密码。



网络配置效果展示图

**此模块可进行的操作：**

1、修改：可对设备名称、IP地址、子网掩码、网关地址、DNS1、DNS2、命令端口、文件传输端口进行更改。

2、根节点选择：可选择设备是否为根节点，设备选为根节点之后，可对是否接入阿里云、最大上传速度、最大下载速度进行修改。

3、启动代理：启动代理的前提条件是设备连云，选择启动代理之后，可对代理协议、代理服务器域名/IP、服务器PORT、用户名、密码进行修改。

**此模块的操作流程：**

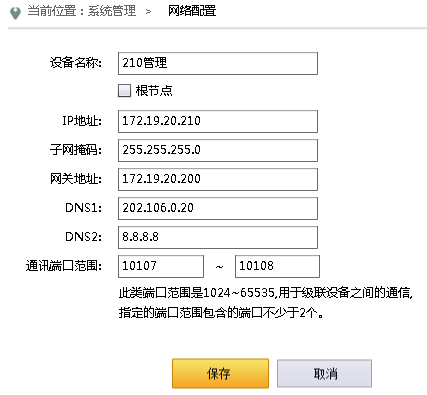
1. 进入“系统管理”，点击“网络配置”
2. 默认显示当前的网络配置相关信息；
3. 如果用户想更改网络配置，在预修改信息显示框里输入相关配置信息，点击“保存”；可输入信息包括：设备名称、IP地址、子网掩码、网关地址、DNS1、DNS2、命令端口、文件传输端口。



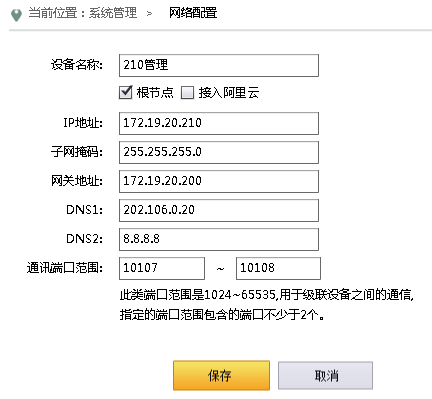
备注：

a、设备名称长度不能超过32byte；

1. IP地址、子网掩码、网关地址、DNS1、DNS2输入规范正确的地址；
2. 命令端口：默认为10108，建议不要修改；
3. 文件端口：默认为10107，建议不要修改。
4. 可以根据自身需要设置设备是否为根节点，设备设为根节点之后，可选是否接入阿里云，并可设置最大上传速度、最大下载速度。



点击根节点“”按钮，会弹出



点击接入阿里云“”按钮，会弹出



可对最大上传速度、最大下载速度进行修改

1. 开启代理设置，可对代理协议、代理服务器域名/IP、服务器PORT、用户名、密码进行修改。



点击启动代理“”按钮，会弹出



根据上图进行填写，点击连接测试

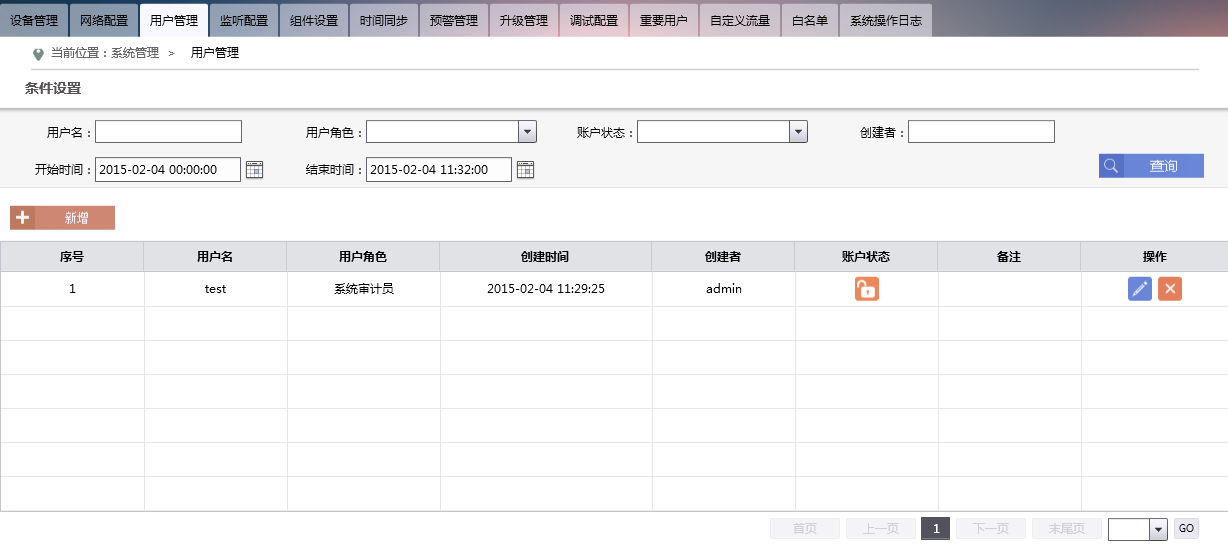
## 用户管理

本系统共设置3种用户角色：系统管理员、系统配置员、系统审计员。

系统管理员：拥有系统最高权限，可查看、操作所有模块。

系统配置员：不可对用户管理模块进行修改、删除操作，但可进行查看操作；可操作系统其他所有模块。

系统审计员：不可操作系统管理模块及授权申请模块。



用户管理效果展示图

**此模块可进行的操作：**

1、查询：可根据用户名、用户角色、账户状态、创建者、事件查询用户记录

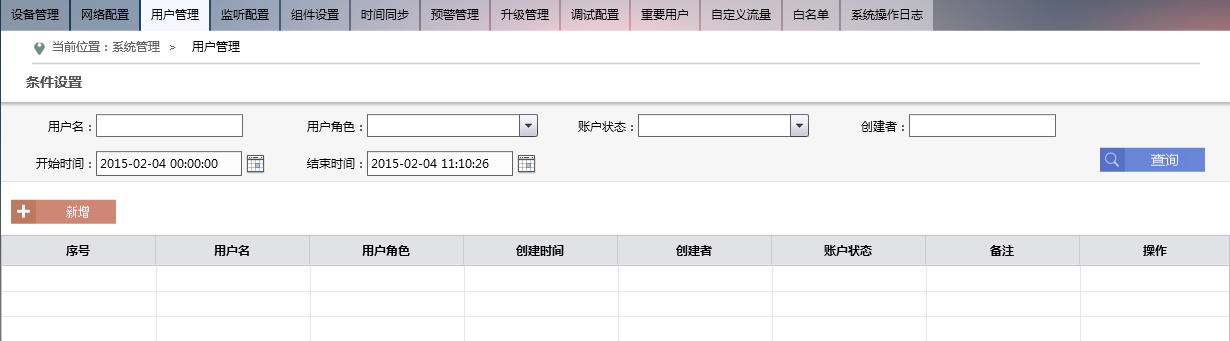
2、新增用户：需要填写用户名（可输入中文）、密码、密码确认、用户角色、备注信息。

3、修改用户信息：通过点击预修改用户信息后面的修改按钮可以进行修改，创建时间则更新为修改时间。

4、删除用户：点击预删除用户后面的按钮，对用户进行单条删除。

**此模块的操作流程：**

1. 进入“系统管理”，点击“用户管理”
2. 如果要新增，点击“新增”



点击新增按钮，会弹出



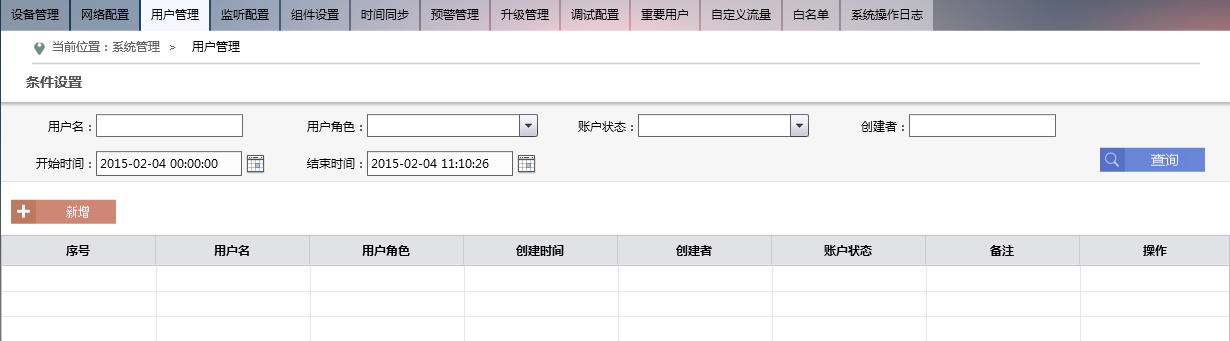
根据上图进行填写然后点击“保存”，新用户就添加成功了

**注意：**系统配置员只能进入首页和系统管理（不包括用户管理）；

系统审计员只能进入首页、查询和报表下载；

系统管理员拥有的权限最高，可进入所有模块进行查看和配置

1. 用户管理中用户可根据用户名、用户角色、账户状态、创建者、事件查询用户记录



1. 如果任何一个用户被锁，那么它的账户状态就会变为锁定



1. 系统管理员可以为其他用户角色解锁，操作如下：

以系统管理员的身份登录进去

点击被锁用户的按钮，会弹出



点击“确定”，被锁的用户就解锁了

## 监听配置

此模块记录了设备监测口的连通状态及捕包情况。



监听配置效果展示图

**此模块可进行的操作：**

1、连通设置：可将监测口进行物理连通，则连通状态显示为绿色

2、捕包设置：可对已经连通的监测口（连通状态显示为绿色）进行捕包设置。

3、如果连接状态始终显示红色，那说明该端口没有运行起来。

**此模块的操作流程：**

1. 进入“系统管理”，点击“监听配置”
2. 如果用户想将某一网口设为捕包口，先将预设捕包口进行物理连通，则连通状态显示为绿色，点击捕包设置的“”按钮，捕包设置一栏变为“”，捕包口设置成功。





捕包口设置成功

## 组件设置

此模块主要记录了Cncert深度报文检测引擎、Cncert病毒检测引擎、Cncert异常通信行为监测引擎

的运行状态及内网信息配置表。



组建设置效果展示图

**此模块可进行的操作：**

1、开启与关闭Cncert深度报文检测引擎。

2、开启与关闭Cncert病毒检测引擎。

3、开启与关闭Cncert异常通信行为监测引擎

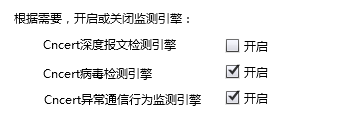
4、新增内网配置信息记录：需要填写名称、IP/IP段、IP类型、备注信息。

5、修改内网配置信息记录：通过点击预修改内网配置信息后面的修改按钮可以进行修改，创建时间则更新为修改时间。

6、删除内网配置信息记录：点击预删除记录条后面的删除按钮，对内网信息配置表进行单条删除。

**此模块的操作流程：**

1. 进入“系统管理”，点击“组建设置”
2. 开启与关闭：点击开启与关闭“”按钮，点击“保存”。



点击“”按钮



点击保存按钮，开启成功

在开启cncert异常通信行为监测引擎时，必须添加相应的内网信息配置；内网信息配置表主要是配置用户需要监测的内网服务器，以及内网主机，以便APT引擎监测服务器的异常行为；如果用户需新增内网配置信息记录，点击“新增”按钮。名称和IP可以根据自己需求设置，IP类型包括内网服务器IP、内网主机IP、邮件服务器IP、web服务器IP，备注可填也可不填。

APT引擎会根据内网信息配置，监测如下几种异常通信行为情况，监测结果会实时的在首页“”

* 1. 协议不匹配的异常通信行为。
  2. 晚八点到早八点时间段之外的通信异常行为情况。
  3. 内网服务器主动连接外网IP的异常通信行为。
  4. 内网主机主动连接外网IP的异常行为。



点击“新增”按钮会弹出



根据上图进行填写然后点击“保存”，内网配置信息就添加成功了

1. 可对已添加的内网信息配置表做修改，点击笔状的图标



然后，会弹出



进行修改

1. 可删除已经配置的内网信息配置表，只需点击该条配置的按钮。

## 时间同步

此模块记录的设备的时间，可以进行时间手动设置、自动同步。



时间同步效果展示图

**此模块可进行的操作：**

1、自动同步：可对同步NTP服务器IP地址、同步服务器端口号进行配置修改。

2、手动设置：可对当前时间、时区进行配置。

**此模块的操作流程：**

1. 进入“系统管理”，点击“时间配置”
2. 如果用户想将设备时间设为自动同步，选择同步方式为“自动同步”，对同步NTP服务器IP地址、同步服务器端口号进行配置修改，点击保存时立即同步时间“”按钮，点击“保存”按钮，则时间同步设置成功。



将同步方式选为“自动”



对同步NTP服务器IP地址及端口号进行设置



点击保存时立即同步时间“”按钮，点击“保存”，时间自动同步完成

**备注：**必须点击保存时立即同步时间“”按钮，否则时间将无法自动同步。

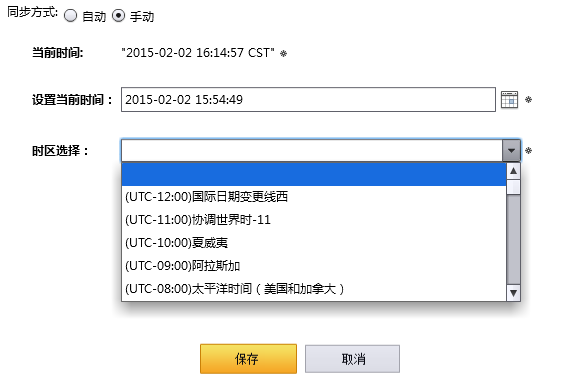
1. 如果用户想手动设置时间，将同步方式选为“手动”，对当前时间及时区进行设置，点击保存，则手动设置时间成功。



将同步方式选为“手动”



点击“”按钮，对当前时间进行设置



在下拉菜单进行时区选择



点击“保存按钮”，手动设置时间完成。

## 预警管理

此模块记录了预警设置的相关信息，包括：Syslog接收服务器IP地址、Syslog接受服务器端口、Syslog程序模块（facility）、Syslog严重级别（severity）的详细信息。



预警管理效果展示图

**此模块可进行的操作：**

1、开启预警设置：可对Syslog接收服务器IP地址、Syslog接受服务器端口、Syslog程序模块（facility）、Syslog严重级别（severity）进行修改。

2、关闭预警设置。

用户需要自行搭建syslog服务器，端口默认为514。

程序模块分为local和all。

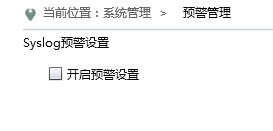
1. Local 代表模块日志
2. All 代表系统日志

严重级别分为，高、中、低、疑似。

1. 高
2. 中
3. 低
4. 疑似

**此模块的操作流程：**

1. 进入“系统管理”，点击“预警管理”
2. 如果用户需开启预警设置，点击开启预警设置“”按钮，开启预警设置变为“”，对对Syslog接收服务器IP地址、Syslog接受服务器端口、Syslog程序模块（facility）、Syslog（severity）进行配置，点击“保存”按钮，预警设置成功。



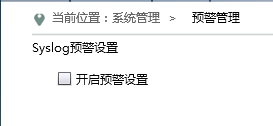
点击“”按钮，会弹出



根据上图进行信息填写，点击保存

1. 如果用户需要关闭预警设置，点击开启预警设置“”按钮，开启预警设置变为“” ，关闭预警管理。





关闭预警功能

## 升级管理

~~当升级服务器有升级包可用时，需要在标题栏有醒目升级提醒，点击该升级提醒，可看到如下信息：当前版本、待升级版本、版本描述、现在升级、稍后升级；~~

~~若用户点击稍后升级，升级提醒不会消失，直至用户进行升级。~~

用户从阿里云上下载最新的升级包，升级过程中用户界面处于不可用状态。升级成功logo栏会显示升级后的版本。



升级管理效果展示图

**此模块可进行的操作：**

1、升级日志查询：可根据升级时间、操作用户对升级日志进行查询。查询结果对用户的每次升级操作进行记录，记录信息包括升级时间、升级内容（事件库升级/系统升级）、升级前版本、升级后版本、升级结果（成功/失败）、操作者、操作者IP

2、离线升级：支持用户将通过其他方式（网站下载、厂商索取）获取的升级包进行导入，进行补救升级。

**此模块的操作流程：**

1. 进入“系统管理”，点击“升级管理”
2. 用户可进行离线升级



点击离线升级按钮，会弹出

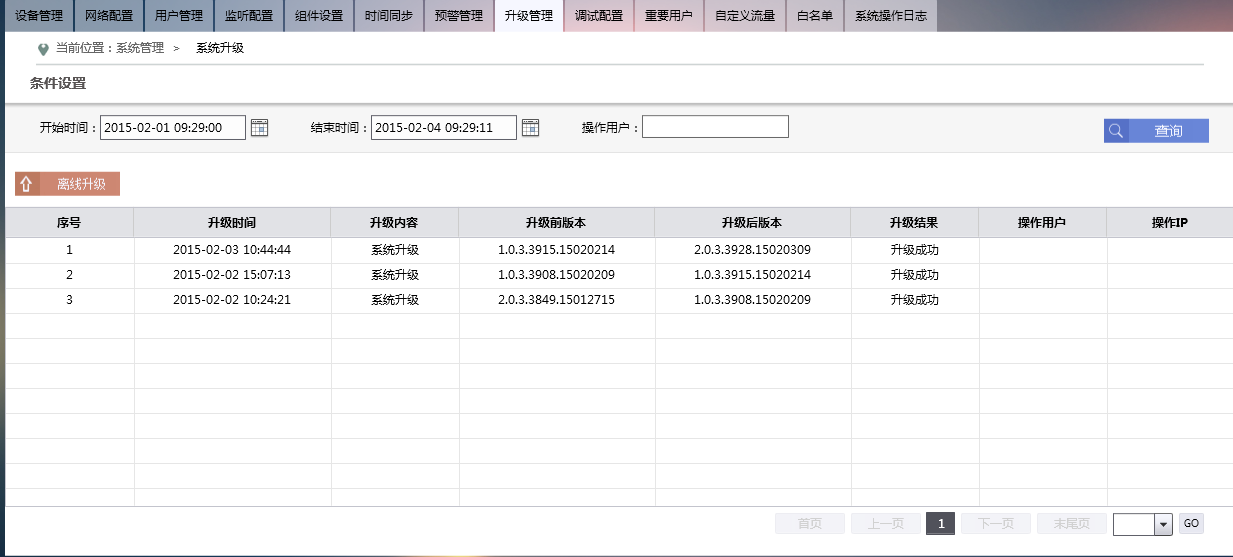


将升级包导入，点击保存，升级成功

1. 升级完成后，升级管理会记录此次升级的信息和结果

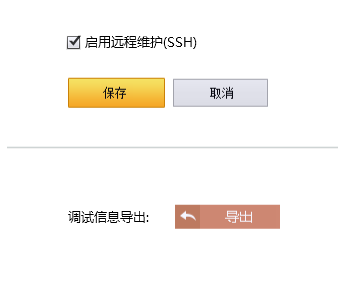


1. 升级管理，用户可根据升级时间、操作用户对升级日志进行查询



查询结果示意图

## 调试配置



调试配置效果展示图

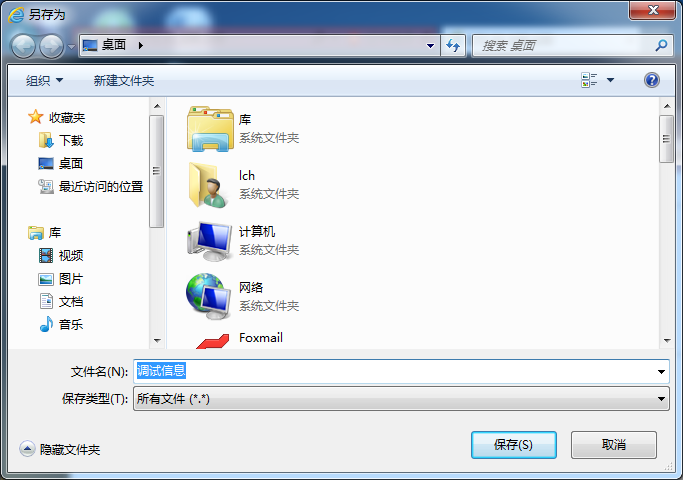
**此模块可进行的操作：**

1、开启与关闭远程维护SSH功能。

2、调试信息导出：可将调试信息（TXT文件）导出到本地。

**此模块的操作流程：**

1. 进入“系统管理”，点击“调试配置”
2. 开启：点击开启“”按钮，启用远程维护（SSH）变为“”状态，开启成功， 远程维护SSH开启后，用户可以用putty等支持ssh登录方式的工具进行系统后台登陆操作。
3. 导出：点击调试信息导出，会弹出

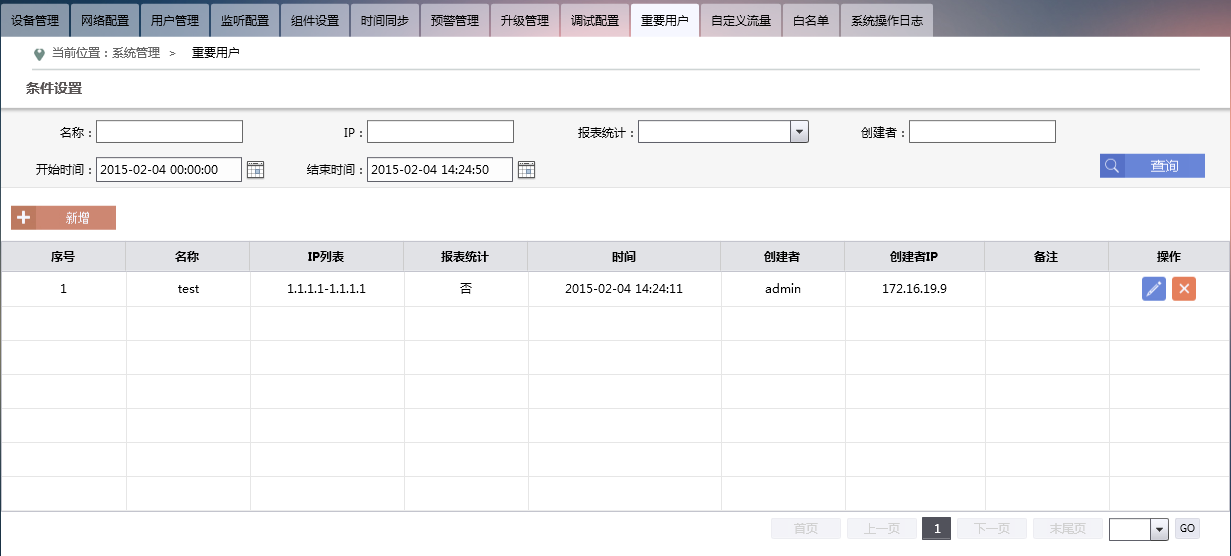


将调试信息保存到本地即可,可选任意路径存放。

1. 关闭：点击开启“”按钮，启用远程维护（SSH）变为“”状态，关闭成功。

## 重要用户配置

此模块记录了一些重要用户的信息



重要用户配置

**此模块可进行的操作：**

1、查询：支持用户按名称、IP、是否报表统计、创建者、创建时间进行记录查询。

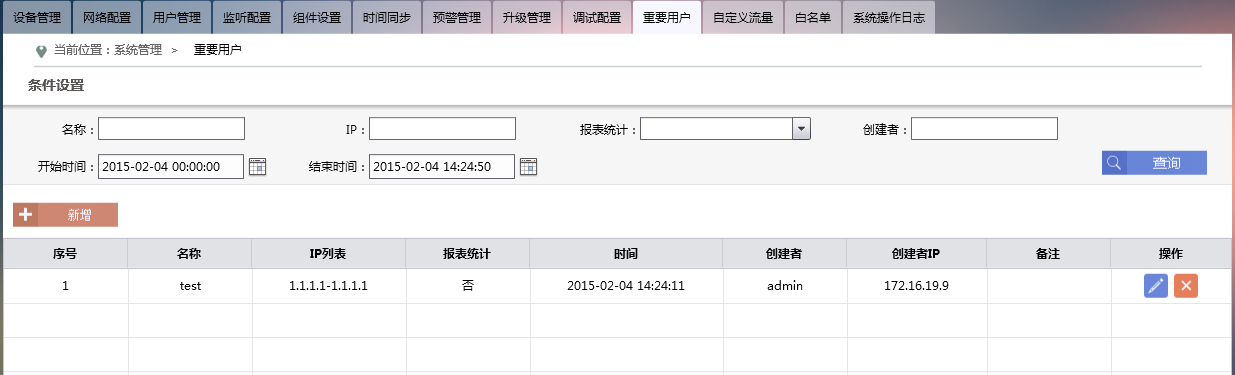
2、新增用户：用户通过点击"新增"按钮添加记录,可配置信息包括:配置项名称、IP/IP段、是否进行报表统计、备注信息。

3、修改用户信息：用户可以对已配置信息进行修改，可修改项包括：配置项名称、IP/IP段、是否进行报表统计、备注信息，若用户进行了修改，则时间对应更新为修改时间。

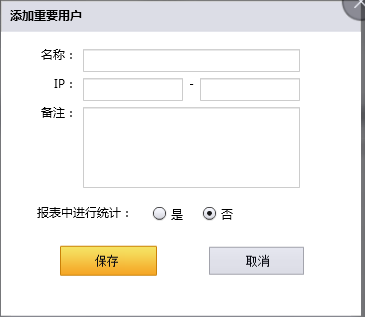
4、删除用户：点击预删除用户后面的删除按钮，对用户进行单条删除。

**此模块的操作流程：**

1. 进入“系统管理”，默认为“重要用户”
2. 如果用户想要查看某一段的IP，可点击“新增”



点击新增按钮，会弹出

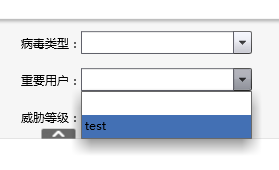


根据上图进行填写然后点击“保存”，重要用户就添加成功了

1. 重要用户配置的IP，在首页和查询中就会被标红



1. 新增的重要用户名称会在查询条件“重要用户”的下拉菜单中显示；



1. 重要用户也可根据名称、IP、是否报表统计、创建者和时间查询



1. 可对已添加的重要用户做修改，点击笔状的图标



然后，会弹出

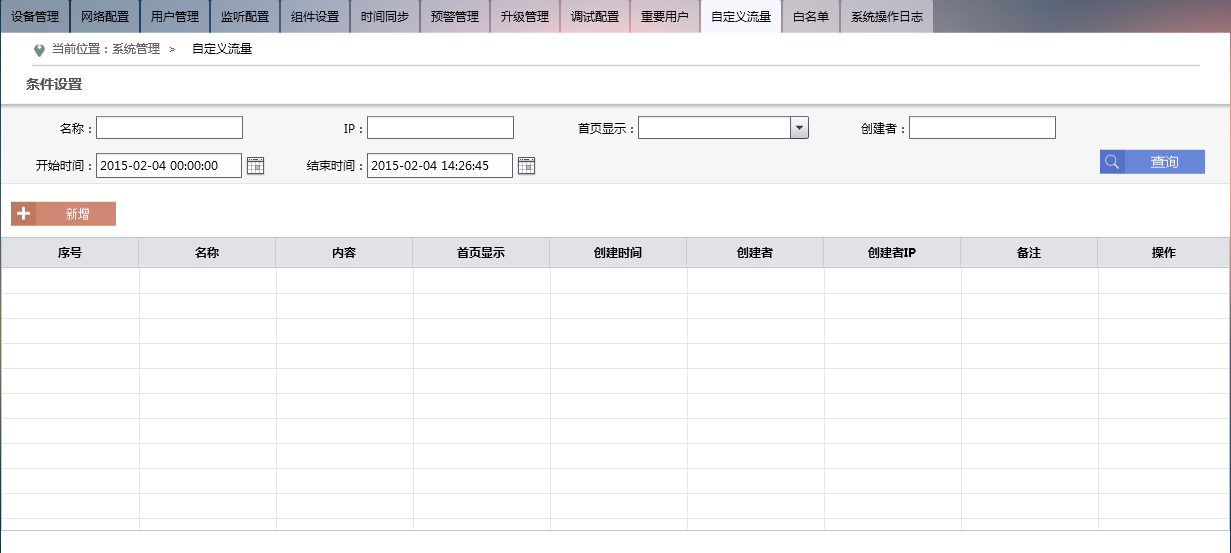


进行修改

1. 可删除已经配置的重要用户，只需点击该条配置的按钮

## 自定义流量配置

此模块记录了一些自定义流量配置的信息。



自定义流量配置效果展示图

**此模块可进行的操作：**

1、查询：支持用户按名称、IP、是否首页显示、创建者、创建时间查询。

2、新增用户：用户通过点击“新增”按钮添加记录，可配置信息包括：名称、IP/IP段、是否首页显示、备注。

3、修改用户信息：通过点击预修改用户信息后面的修改按钮可以进行修改，时间则对应更新为修改时间。

4、删除用户：点击预删除用户后面的按钮，对用户进行单条删除。

**此模块的操作流程：**

1. 进入“系统管理”，点击“自定义流量”
2. 如果用户想要查看某段IP的流量可点击“新增”

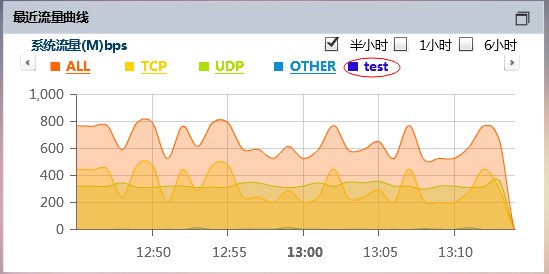


点击新增按钮，会弹出

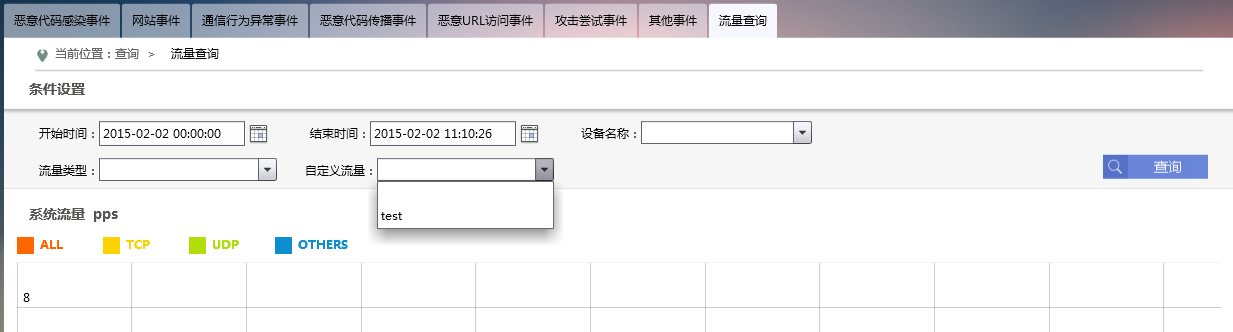


根据上图进行填写然后点击“保存”，自定义流量就添加成功了

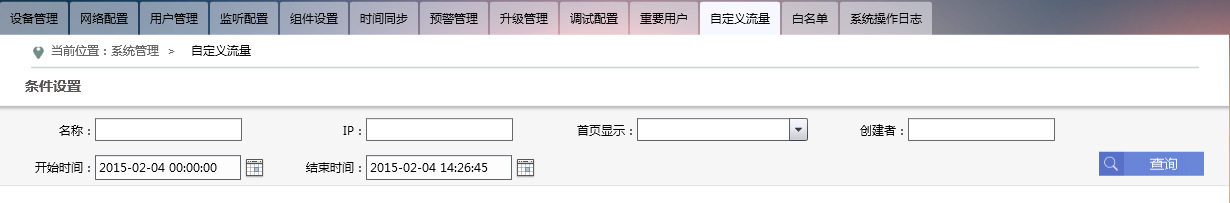
1. 在首页中的最近流量曲线中就会显示添加的自定义流量



1. 新增的自定义流量，会在流量查询的条件设置中看到



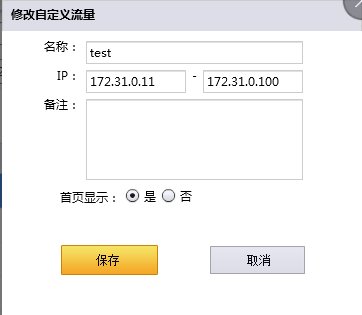
1. 自定义流量也可根据名称、IP、首页显示、创建者和时间查询



1. 可对已添加的自定义流量做修改，点击笔状的图标



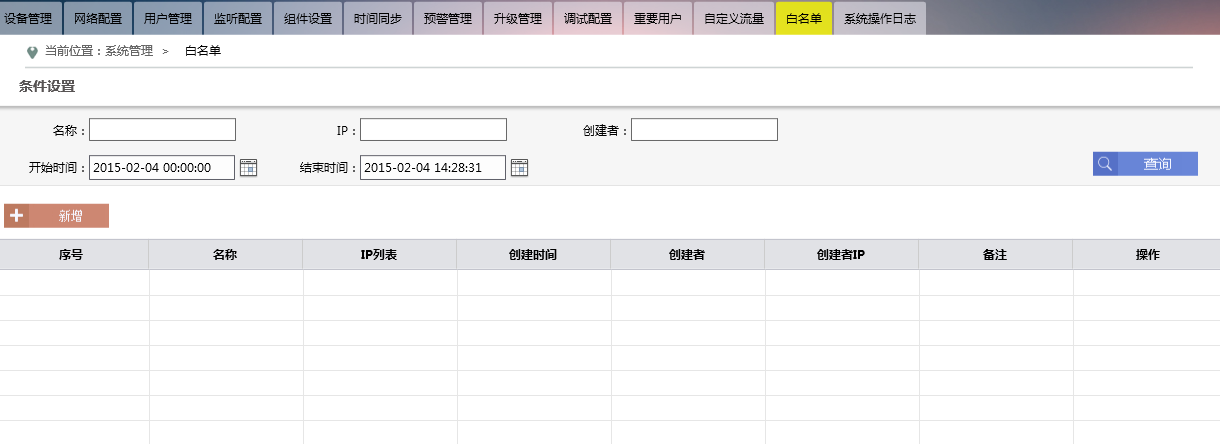
然后，会弹出



进行修改

1. 可删除已经添加的自定义流量，只需点击该条的按钮

## 白名单配置



白名单配置效果展示图

**此模块可进行的操作：**

1、查询：用户可按名称、IP、创建者、时间进行配置查询。

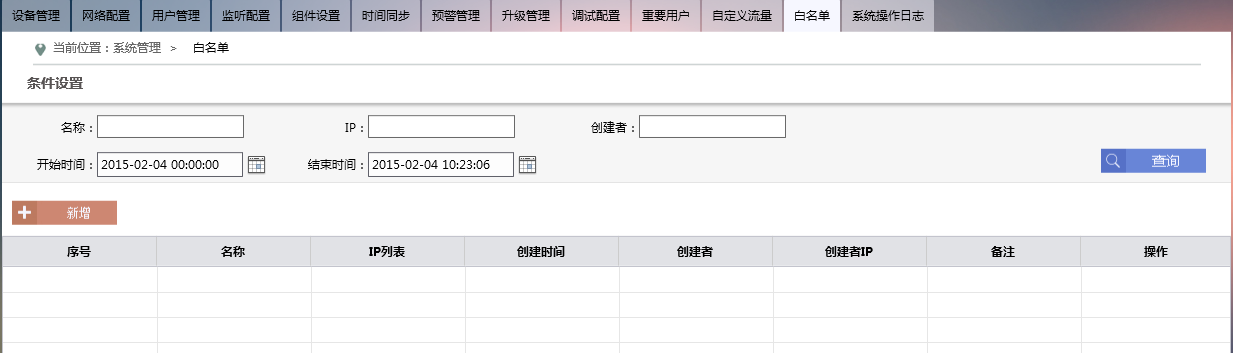
2、新增用户：用户通过点击"新增"按钮添加记录,可配置信息包括:配置项名称、IP/IP段、备注信息。

3、修改用户信息：通过点击预修改用户信息后面的修改按钮可以进行修改，并将时间更新为修改时间。

4、删除用户：点击预删除用户后面的按钮，对用户进行单条删除。

**此模块的操作流程：**

1. 进入“系统管理”，点击“白名单配置”
2. 如果用户不需要看到某段IP的事件可点击“新增”

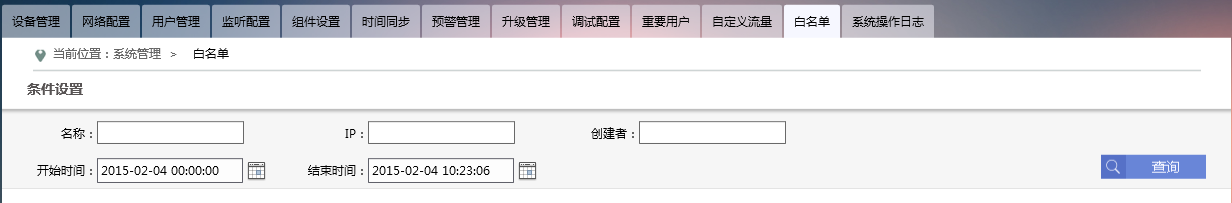


点击新增按钮，会弹出



根据上图进行填写然后点击“保存”，白名单就添加成功了

1. 在“查询”模块中就不会看到这段ip的事件了
2. 白名单用户可按名称、IP、创建者、时间进行配置查询



1. 可对已添加的白名单做修改，点击笔状的图标



然后，会弹出



进行修改

1. 可删除已经添加的白名单，只需点击该条的按钮

## 系统操作日志

此模块记录了重要用户配置，自定义流量配置，白名单配置、用户管理和数据备份的增删改操作。

主要展示了：用户名、用户IP、操作时间、操作模块（重要用户配置，自定义流量配置，白名单配置和用户管理）、操作类型（增删改）、操作描述。



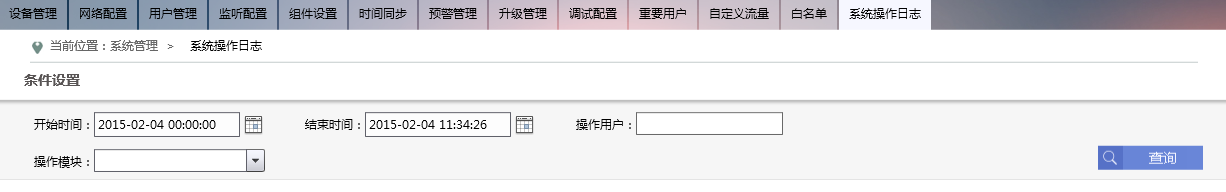
操作日志查看效果展示图

**此模块可进行的操作：**

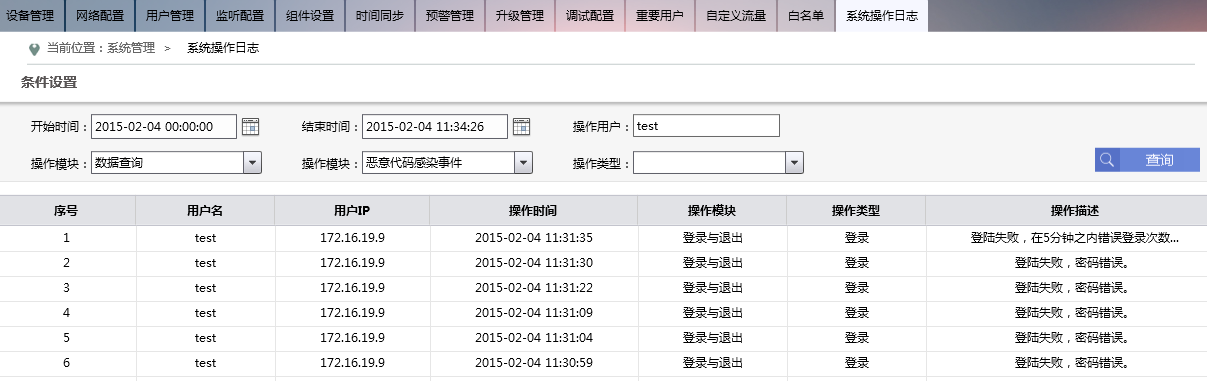
1. 查询：对操作用户、操作模块、操作时间、操作类型几个作为条件进行查询。注意操作类型查询条件是在选择操作模块条件下进行查询的。

**此模块的操作流程：**

1. 进入“系统管理”，点击“系统日志”
2. 此模块主要记录用户的操作，记录用户名，用户ip，操作时间，操作模块，操作描述
3. 系统操作日志，用户可根据对操作用户、操作模块、操作时间、操作类型几个作为条件进行查询。注意操作类型查询条件是在选择操作模块条件下进行查询的。



选择操作模块进行查询，会弹出



# 章节 授权

## 申请授权

授权申请，是系统需要开通服务和系统一些基本信息的填写，填写信息包括：申请人、联系电话、单位地址、合同编号、设备名称、设备ID、设备IP、设备类型。



授权申请填写单效果图

申请授权之后，选择导出申请，会下载一个授权申请文件(authreq)到本地。

**此模块的操作流程：**

* 1. 填写授权申请：系统首次登陆界面需要对系统进行授权。



**填写规范**：

申请人：支持中文，长度不能超过16byte；

联系电话：只能填写11个数字；

单位地址：支持中文，长度不能超过32byte；

合同编号：长度不能超过64byte；

设备名称：支持中文，长度不能超过32byte；

设备IP：请填写规范的IP地址；

设备类型：只有两种类型（监测点、管理点），请根据自身需要选择；

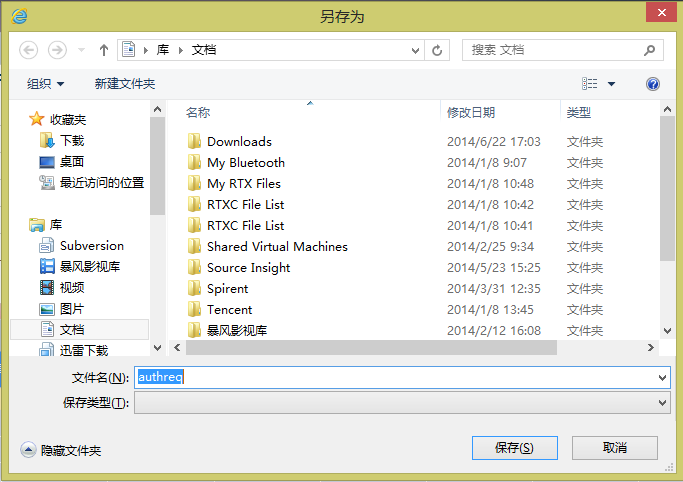
设备ID会默认显示在框中，如不显示说明设备有问题，请联系销售人员。

* 1. 导出申请

(1)授权信息填写无误后，点击“导出申请”



(2)点击“导出申请”后，可选择任意路径存放



## 获取license文件

[将5.1导出的授权申请文件发送至邮箱gms-support@chanct.com](mailto:将5.1导出的授权申请文件发送至邮箱gms-support@chanct.com)，将会收到一份license文件。

## license导入授权

licence文件导入，即可成功授权。

**此模块的操作流程：**

登录界面->点击“授权”->将license文件导入->保存



导入license文件效果图

选择license文件的存放路径，点击“保存”

## 授权提醒

将license文件导入一分钟后，会出现授权提醒：如果授权成功，会出现成功的提示。



否则就会出现失败的提示



如果授权成功，查询模块、报表下载、系统管理都可使用