

构建安全可靠的企业信息安全系统

网路神警上网行为管理系统 3.4.5. 使用说明书

北京盛世光明软件股份有限公司

2013 年 9 月

版权声明

北京盛世光明软件股份有限公司版权所有，保留一切权利

本文件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，除另有特别说明外，其著作权或其他相关权利均属北京盛世光明软件股份有限公司所有，受到有关产权及版权法保护。未经北京盛世光明软件股份有限公司书面许可，任何人不得擅自拷贝、传播、修改、摘录、备份本文档全部或部分内容。

免责条款

本文档仅用于为最终用户提供信息，其内容如有更改，恕不另行通知。

北京盛世光明软件股份有限公司在编写本文档时已尽最大努力保证其内容准确可靠，但北京盛世光明软件股份有限公司不对文档中的遗漏、不准确或错误导致的损失和损害承担任何责任。

联系方式

全国服务热线：400-6789-518

邮箱：services_ssgm@126.com

目 录

一 . 研发背景	6
二 . 前言	6
三 . 系统注册以及登录管理界面	7
四 . 管理界面介绍	8
4.1 【系统管理】	8
4.1.1 角色管理	8
4.1.2 人员管理	10
4.1.3 分组管理	10
4.1.4 上网人员管理	10
4.2 【基本设置】	12
4.2.1 监听设置	12
4.2.2 IP 地址段设置.....	13
4.2.3 多级管理设置	13
4.2.4 日志设置	14
4.2.5 分控中心设置	14
4.2.6 其他设置	14
4.2.7 数据库备份还原	15
4.2.8 报警设置	15
4.2.9 工作 QQ 设置.....	16
4.3 【资源搜索】	17
4.3.1 资源搜索	17

4.3.2 监控组	18
4.3.3 临时组	19
4.3.4 黑名单	20
4.3.5 未授权	20
4.4 【规则设置】	21
4.4.1 过滤规则管理	21
4.4.2 内容过滤设置	21
4.4.3 网站过滤	22
4.4.4 邮件过滤	23
4.4.5 关键词过滤	23
4.4.6 应用软件过滤	23
4.4.7 端口过滤	24
4.4.8 禁用程序设置	24
4.4.9 QQ 黑白名单设置	25
4.4.10 分时段上网	25
4.4.11 规则分时段启用	26
4.5 【日志查询】	27
4.5.1 上网日志	27
4.5.2 邮件日志	28
4.5.3 发帖日志	28
4.5.4 移动磁盘日志	29
4.5.4 虚拟身份	29

4.5.5 聊天日志	30
4.5.6 上下线日志	30
4.5.7 桌面抓拍	31
4.5.8 更改 IP/MAC 使用日志.....	31
4.5.9 虚拟身份	32
4.5.10 报警日志.....	32
4.5.11 操作日志.....	33
4.6 【网站排名】	34
4.6.1 查询网站排名	34
4.6.2 终端计算机点击排名	35
4.7 【在线时间】	35
4.8 【流量统计】	36
4.8.1 查询流量	36
4.8.2 实时流量查看	36
4.9 【资源统计】	37
4.10 【系统帮助】	38
五 . 产品部署	39
六 . 快速设置	41
6.1.基本设置>监听设置	42
6.2.基本设置>IP 网段设置	42
6.3.资源搜索>监控组	43
6.4 规则设置>过滤规则管理	44
6.5 资源搜索>监控组>批量修改规则	44

一．研发背景

本软件主要以原有的 c/s 版本的上网管理为基础进行功能移植，使软件外观和用户体验度大大提高，同时修改原有软件的 bug，以及兼容了 pppoe 拨号模式下的监控功能，兼容了 windows2008server 系统。使软件的功能更为稳定和完善。

由于 b/s 和 c/s 操作模式有本质的区别，所以此版本中实现实时查看桌面的功能以安装插件的方式查看，一些常规的右击功能更改为其他操作方式。

二．前言

本设置指南是为网路神警上网行为管理系统（以下简称上网行为管理系统）用户编写的，将引导您通过简单的操作快速地完成上网行为管理系统的常用配置。

使用网路神警之前，您应该正确安装网路神警上网行为管理系统，具体安装步骤请参照系统手册。安装完毕后，请您牢记 admin 账户名称及密码。以下操作均为 Web 管理界面的操作。

您需要通过 Web 浏览器来访问上网行为管理系统。推荐使用 Internet Explorer 6.0（更高版本请采用兼容模式浏览）以上版本的浏览器。

注意：本设置指南使用的 IP 地址、网络域名、账户和密码仅作示例使用。在使用应用环境中，请您参照具体情况作相应的调整。

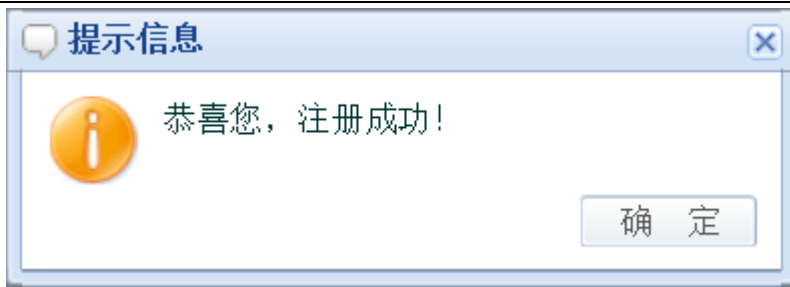
三．系统注册以及登录管理界面

使用局域网中的任何一台计算机，打开浏览器，在地址栏中输入 [http://IP 地址 : 8080/](http://IP地址:8080/)来登录上网行为管理系统，IP 地址视系统 IP 地址而定。如图：



账户为默认：admin，密码默认：111111。系统默认为试用版，可以免费试用7天，试用期结束后，请注册为正式版方可继续使用。点击系统注册，弹出注册对话框，填写注册信息，完成注册。如图：





注意：一个序列号，只能注册一台服务器。如果没有试用帐号，请直接输入帐号和密码登录系统。

四．管理界面介绍

成功登录上网行为管理系统后，其初始界面如下图所示。



左侧导航栏为“管理菜单”，右侧为快捷面板。

“管理菜单”分为以下几个大项：

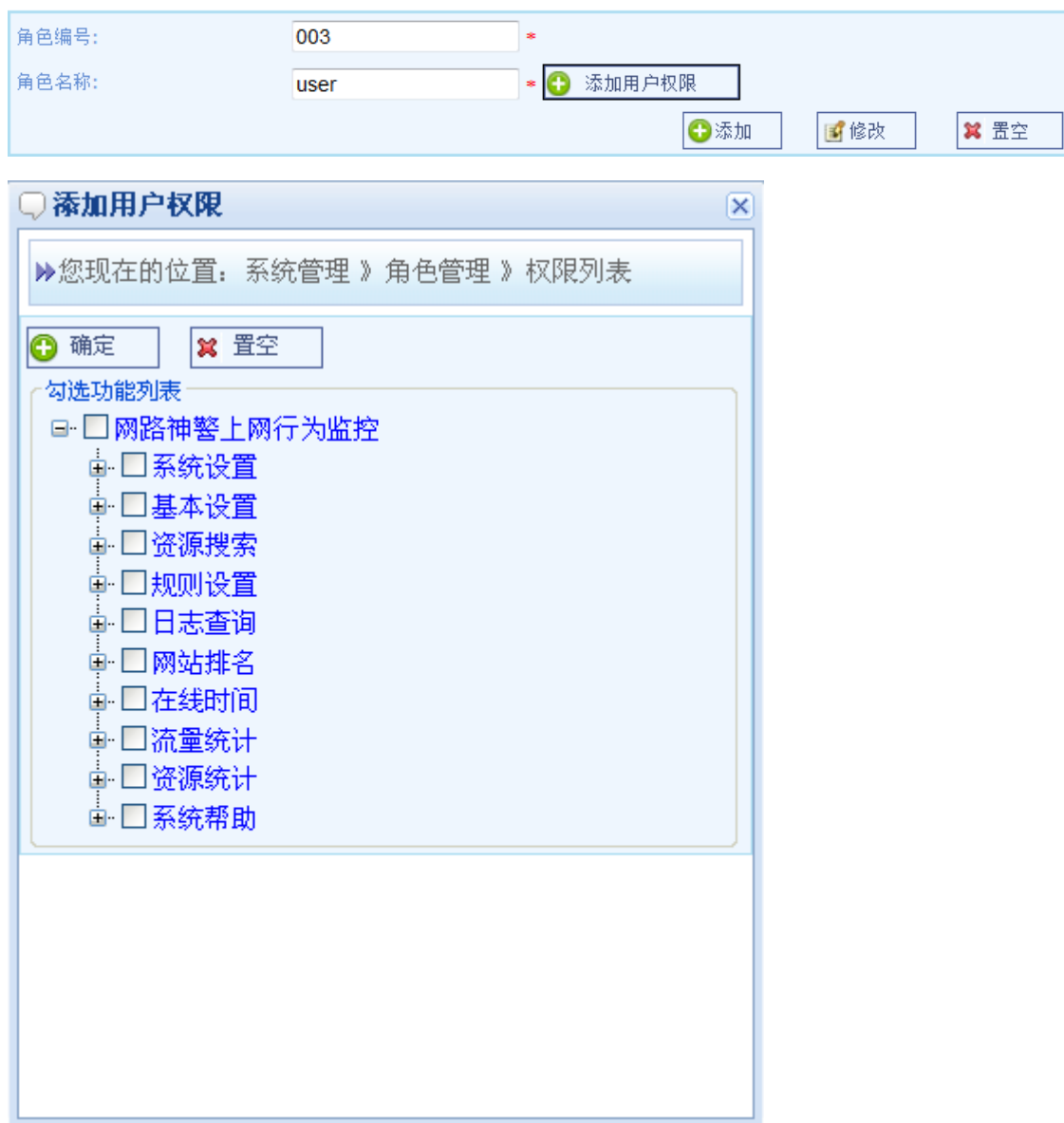
4.1【系统管理】

4.1.1 角色管理

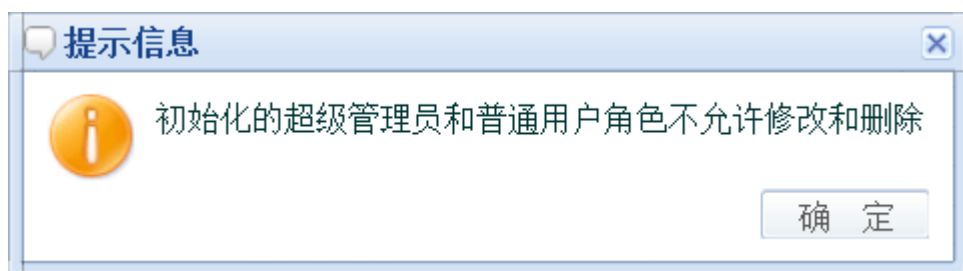
用户权限定义，分为普通用户，超级管理员。

示例：

添加角色 user，并添加用户权限。输入用户编号 003，用户编号不能重复，然后再输入角色名称 user，点击添加用户权限。勾选相应功能。如下图所示：



注意：初始化的超级管理员和普通管理员不能修改和删除。



4.1.2 人员管理

用户账户增删改，分配用户角色。

示例：添加用户 ssgm001，分配权限为 user 权限。如下图：



Form fields and values:

- 账户名称: ssgm001
- 邮箱地址: ssgm_services@126.cc
- 手机号码: (empty)
- 座机号码: (empty)
- 账户身份(角色): 普通用户 (selected from dropdown: 普通用户, 超级管理员, user)
- 密码: (masked with dots)
- 禁用账户: ☐
- 备注: (empty)

Buttons: + 添加, 修改, 清空

4.1.3 分组管理

计算机分组，不同部门划分为不同分组。

示例：根据公司不同部门，添加监控组。如下图：



序号	分组名称	负责人	联系电话	操作
1	默认分组			修改 删除
2	市场部			修改 删除
3	销售部			修改 删除
4	技术部			修改 删除
5	行政部			修改 删除
6	人力资源部			修改 删除
7	售后部			修改 删除
8	财务部			修改 删除
9	大客户部			修改 删除

Form fields and values:

- 分组名称: 大客户部 (selected from dropdown)
- 负责人: 王经理
- 联系电话: 010-82780160

Buttons: + 添加, 修改, 清空

4.1.4 上网人员管理

在此处添加需要上网人员的具体信息。

示例：根据公司人员的信息，添加的上网人员的信息。如下图：

您现在的位置：系统管理 > 上网人员管理

证件类型： 人员名称：

证件号码：

序号	姓名	性别	证件类型	证件号码	发证单位	国籍	详细描述	操作
1	1	男	其他	1		中国		修改 删除

页次：1 / 1页 共有 1记录，每页 7 条 第 1 页

姓名： 性别：

证件类型： 证件号码：

发证单位： 国籍：

详细描述：

新加上网人员密码为6个1

证件号码为客户端上网人员需要的账号

此处说明了客户端上网人员登录需要的密码

下图显示的为客户端登录实名认证的窗口：

电脑验证：“上网账号”为在“上网人员管理”里面添加的证件号码。

“账号密码”为我公司设置的默认密码“111111”。

安全上网认证

safety online authentication



 **登录个人安全上网账户**

上网认证，享受便利安全网络在线！

登录区域 **电脑验证** **手机验证**

上网账号：

账号密码：

为避免您的网上信息被窃取，请使用软键盘输入密码！！

！温馨提示 **点此添加“退出上网账号”到《收藏夹》**

为了保证您的上网账号不被他人盗用，请务必在上网结束后“退出上网账号”！退出上网账号的方法有两种：

- 1、在浏览器的《收藏夹》里面点击“退出上网账号”，如果没有请点击上面的红色链接进行添加。
- 2、在浏览器地址栏输入 <http://localhost:8080/userlogout>，点击回车即可。
- 3、[点击此连接退出](#)。

同时也可使用手机验证，通过该输入手机号和获取动态码的方式登录。



安全上网认证
 safety online authentication

 **登录个人安全上网账户**

 **上网认证，享受便利安全网络在线！**

登录区域 电脑验证 手机验证

手机号码:

动态码:
获取动态码

登 录

为避免您的网上信息被窃取，请使用软键盘输入密码！！

！ 温馨提示 [点此添加“退出上网账号”到《收藏夹》](#)

为了保证您的上网账号不被他人盗用，请务必在上网结束后“退出上网账号”！退出上网账号的方法有两种：

- 1、在浏览器的《收藏夹》里面点击“退出上网账号”，如果没有请点击上面的红色链接进行添加。
- 2、在浏览器地址栏输入 <http://localhost:8080/userlogout> ，点击回车即可。
- 3、 [点击此连接退出](#)

4.2 【基本设置】

4.2.1 监听设置

设置监听网卡。设置监控模式，启动监控服务等。


网路神警上网行为管理系统

WELCOME 欢迎您: admin 监控状态: 监控服务正在运行.....

蓝皮肤 绿皮肤 紫皮肤

功能菜单

- 系统管理
- 基本设置
- 监听设置
- IP地址设置
- 多级管理设置
- 日志设置
- 分控中心设置
- 其他设置
- 数据库备份还原
- 报警设置
- 资源搜索
- 规则设置
- 日志查询
- 网站排名
- 在线时间
- 流量统计
- 资源统计
- 消息管理
- 系统帮助
- 盛世光明软件

您现在的位置: 基本设置 > 监听设置

序号	网卡名称	IP地址	MAC地址
<input type="checkbox"/> 1	rpcap://Device\NPF_{2E5FE557-5B0B-4EE8-8FCB-C570FB8AFA40}	192.168.1.169	94DE806C320F
<input checked="" type="checkbox"/> 1	rpcap://Device\NPF_{2E5FE557-5B0B-4EE8-8FCB-C570FB8AFA40}	192.168.1.169	94DE806C320F

重新搜索
保存设置

选择监控模式: 基于Mac地址监控
☐ 按号上网(上网模式是否是按号上网)

启动监控
重启监控
停止监控

4.2.2 IP 地址段设置

设置要监控的 IP 地址段。



网路神警上网行为管理系统

WELCOME 欢迎您: admin 监控状态: 监控服务正在运行.....

您现在的位置: 基本设置 > IP地址段设置

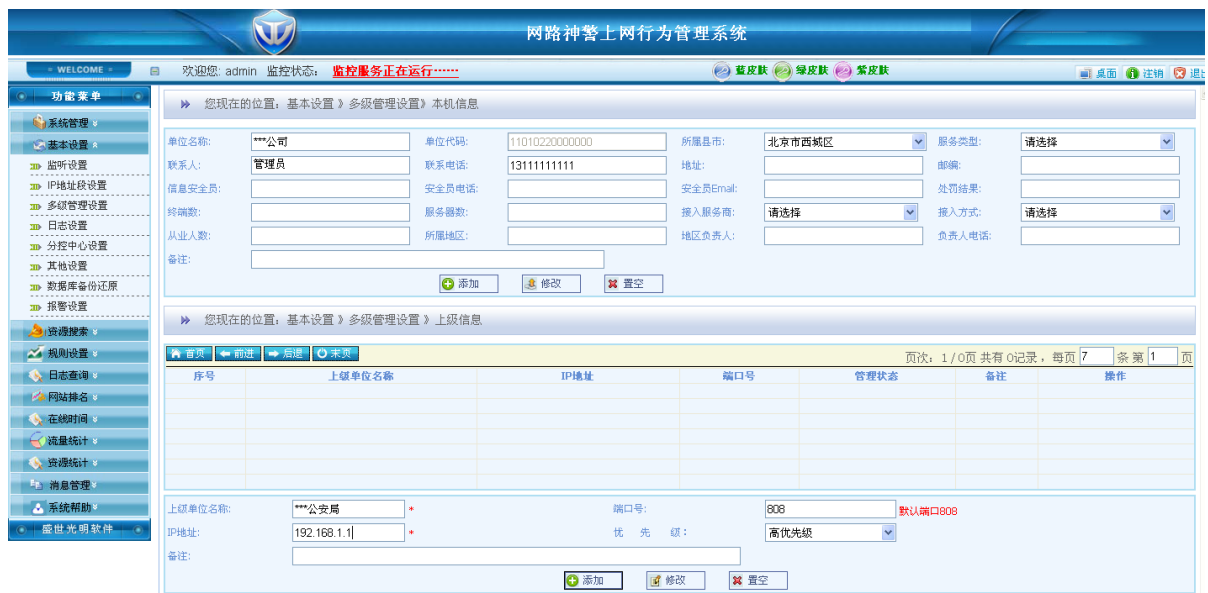
序号	IP段	操作
1	192.168.1	修改 删除

需要监控的IP段(必填)(格式: 192.168 或 192.168.1):

功能说明: 如同时存在 192.168 和 192.168.1 两种配置, 以更小的网段为准, 192.168将不起作用, 192.168.1配置起作用。

4.2.3 多级管理设置

设置上级管理服务器, 接受上级管理服务器的监控, 并上传监控日志到多级管理服务器上。



网路神警上网行为管理系统

WELCOME 欢迎您: admin 监控状态: 监控服务正在运行.....

您现在的位置: 基本设置 > 多级管理设置 > 本机信息

单位名称: ***公司 单位代码: 11010220000000 所属县市: 北京市西城区 服务类型: 请选择

联系人: 管理员 联系电话: 13111111111 地址: 邮编:

信息安全员: 安全员电话: 安全员Email: 处罚结果:

终端数: 服务器数: 接入服务商: 请选择 接入方式: 请选择

从业人数: 所属地区: 地区负责人: 负责人电话:

备注:

添加 修改 清空

您现在的位置: 基本设置 > 多级管理设置 > 上级信息

序号	上级单位名称	IP地址	端口号	管理状态	备注	操作
----	--------	------	-----	------	----	----

上级单位名称: ***公安局 端口号: 808 默认端口808

IP地址: 192.168.1.1 优先级: 高优先级

备注:

添加 修改 清空

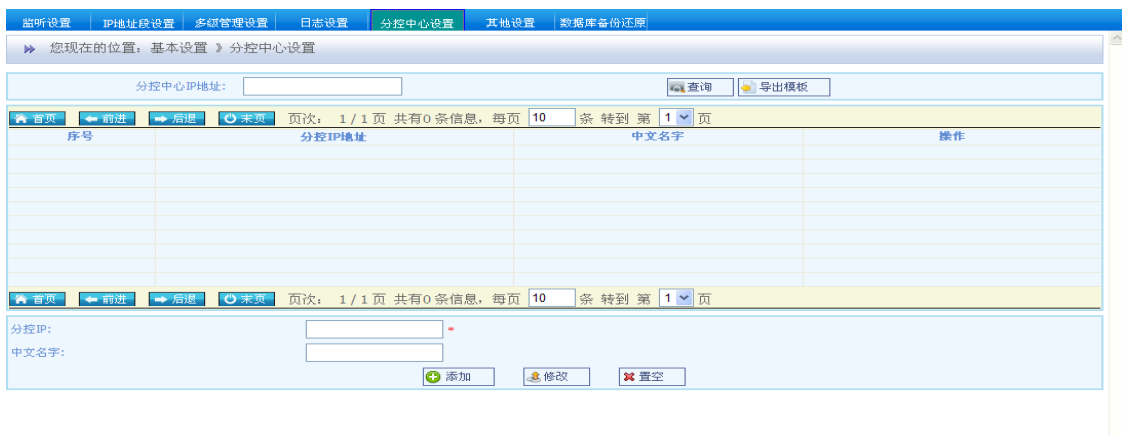
4.2.4 日志设置

设置上网管理日志，操作日志的保存时间，时候自动删除以及日志的保存路径。



4.2.5 分控中心设置

默认情况下任意一个 IP 都可以访该管理网站，但是当设置分控中心后，只有设置的 IP 才能访问，所以设置时应注意将服务器本机 IP 也加入在分控中心。



4.2.6 其他设置

自定义客户端卸载密码，自定义网页浏览提示信息。



4.2.7 数据库备份还原

手动备份与还原数据库，支持恢复出厂设置。



4.2.8 报警设置

包含邮箱报警和报警设置，设置发送邮箱和接受邮箱，还有页面弹出报警和短信报警。

WELCOME 欢迎您: admin 监控状态: **监控服务正在运行**

蓝皮肤 绿皮肤 紫皮肤

您现在的位置: 基本设置 > 报警设置

报警配置

报警时间间隔: 1 (分钟)

剩余磁盘大小: 200 G 当服务器磁盘剩余容量小于设定值时报警

内存大小: 70 % 当服务器内存小于设定百分值时报警

☒ 开启前台弹框报警

☒ 开启后台邮箱报警

发送邮件设置: 1114512060@qq.com 发送邮件应开启SMTP服务

发送邮件密码: *****

发送邮件密码确认: *****

[报警接收账户配置](#)

☐ 开启后台短信报警 (需连接短信设备)

端口: COM1 波特率: 19200,N,8,1 模式: 1

[保存设置](#)

4.2.9 工作 QQ 设置

添加 QQ 号码和密码后，登录这些工作 QQ 时不会弹出验证页面，直接就能登录 qq 且可以记录 qq 聊天信息。

盛世光明 网路神警上网行为管理

WELCOME 欢迎您: admin 监控状态: **监控服务正在运行**

蓝皮肤 绿皮肤 紫皮肤

您现在的位置: 基本设置 > 工作QQ设置

序号	QQ号码	QQ密码	操作
1	1991066720	*****	修改 删除
2	1272490532	*****	修改 删除

页次: 1 / 1页 共有 2记录, 每页 15 条 第 1 页

QQ号码: 密码: 确认密码:

[添加](#) [修改](#)

4.3 【资源搜索】

4.3.1 资源搜索

搜索局域网中被监控的计算机，并对计算机进行分组，默认只有一个监控组，要增加监控组，须在系统管理>分组管理中添加分组。

您现在的位置：资源搜索

页次：1 / 2 页 共有 15 条信息，每页 13 条 转到 第 1 页

序号	计算机名称	计算机IP	计算机MAC	所属分组	操作
1	www-ff02c3bdeef	192.168.9.1	5C638F7A5E1E	市场部	删除 修改计算机名称
2	www-ff02c3bdeef	192.168.9.88	00248C557D4F	市场部	删除 修改计算机名称
3	www-ff02c3bdeef	192.168.9.115	6CF0498F8547	市场部	删除 修改计算机名称
4	www-ff02c3bdeef	192.168.9.210	50E5492B399D	市场部	删除 修改计算机名称
5	www-ff02c3bdeef	192.168.9.230	00173164113C	市场部	删除 修改计算机名称
6	www-ff02c3bdeef	192.168.9.254	C8A350C67D8	未授权	删除 修改计算机名称
7	192.168.9.206	192.168.9.206	50E5494F5106	未授权	删除 修改计算机名称
8	ACER-PC	192.168.1.202	0026225E34A5	未授权	删除 修改计算机名称
9	WG772AIFVGQHOK6	192.168.1.203	206A8A28C0D9	未授权	删除 修改计算机名称
10	WWW-13CC0F70892	192.168.1.205	50E5494E8AD9	未授权	删除 修改计算机名称
11	MRYANG-PC	192.168.1.211	00248C557D4F	未授权	删除 修改计算机名称
12	MICROSOF-67998C	192.168.1.215	00E00000A659	未授权	删除 修改计算机名称
13	PCOS-11271641	192.168.1.217	00E04C362D11	未授权	删除 修改计算机名称

本机网卡:

☒ 自动搜索 ☐ 手动搜索
 起始IP: 截止IP:

批量配置计算机>按 IP 段查看

您现在的位置：资源搜索

页次：1 / 3 页 共有 29 记录，每页 13 条 第 1 页

序号	终端名称	计算机IP	计算机MAC	所属分组	操作
1	192.168.1.12				删除 修改终端名称
2	192.168.1.24				删除 修改终端名称
3	192.168.1.31				删除 修改终端名称
4	192.168.1.33				删除 修改终端名称
5	192.168.1.42				删除 修改终端名称
6	192.168.1.42				删除 修改终端名称
7	192.168.1.44				删除 修改终端名称
8	192.168.1.46				删除 修改终端名称
9	hh				删除 修改终端名称
10	192.168.1.67				删除 修改终端名称
11	192.168.1.69				删除 修改终端名称
12	192.168.1.96				删除 修改终端名称
13	192.168.1.103				删除 修改终端名称

本机网卡:
☐ 自动搜索 ☐ 手动搜索
 起始IP: 使用分组:

批量配置计算机>按监控组查看



4.3.2 监控组

对监控组内的计算机设置监控规则或取消监控，设置 IP/MAC 地址绑定，可以批量修改监控规则，也可以对单个计算机设置监控规则。



批量修改监控规则>按 IP 段查看

☒ 按IP地址段查询
 ☐ 按分组查询
 192.168.1
 全部

首页 前进 后退 末页
 页次: 1 / 3页 共有 29记录, 每页 10 条 第 1 页

全选 反选	IP	分组
<input type="checkbox"/>	192.168.1.96	临时组
<input type="checkbox"/>	192.168.1.56	hh分组
<input type="checkbox"/>	192.168.1.129	临时组
<input type="checkbox"/>	192.168.1.169	zt
<input type="checkbox"/>	192.168.1.69	临时组
<input type="checkbox"/>	192.168.1.144	临时组
<input type="checkbox"/>	192.168.1.39	临时组
<input type="checkbox"/>	192.168.1.115	zch_分组
<input type="checkbox"/>	192.168.1.254	临时组
<input type="checkbox"/>	192.168.1.223	临时组

首页 前进 后退 末页
 页次: 1 / 3页 共有 29记录, 每页 10 条 第 1 页

所选规则
 不使用任何规则
 不使用任何规则
默认规则
zch_规则
zhh
zt
zht

修改 取消

批量修改监控规则>按分组查看

您现在的位置: 资源搜索 > 监控组

当前选中组: 监控组
 全部监控 取消全部监控 批量修改规则 IP/MAC批量绑定

首页 前进 后退 末页
 页次: 1 / 1页 共有 3记录, 每页 10 条 第 1 页

监控状态	序号	终端名称	计算机IP	计算机MAC	分组名称	客户端状态	版本号	使用规则
<input checked="" type="checkbox"/> 监控	1	hh	192.168.1.56	00E062014611	hh分组	正在运行中	3.4.5.0	zhh
<input checked="" type="checkbox"/> 监控	2	192.168.1.115	192.168.1.115	94DE806C31FE	zch_分组	正在运行中	3.4.5.0	zch_规则
<input checked="" type="checkbox"/> 监控	3	192.168.1.115	192.168.1.115	94DE806C31FE	zch_分组	正在运行中	3.4.5.0	zch_规则

首页 前进 后退 末页
 页次: 1 / 1页 共有 1记录, 每页 10 条 第 1 页

按IP地址段查询
 192.168.1
 按分组查询
 zch_分组

全选 反选
 IP
 192.168.1.115
 分组
 zch_分组

首页 前进 后退 末页
 页次: 1 / 1页 共有 1记录, 每页 10 条 第 1 页

所选规则
 zt

修改 取消

4.3.3 临时组

新搜索出的计算机，默认存放在临时组中，并可以对临时组内的计算机设置默认监控规则。

» 您现在的位置：资源搜索 » 临时组									
当前选中组： 临时组 全部监控 取消全部监控									
 首页 前进 后退 末页									
页次：1 / 3页 共有 26记录，每页 10条第 1									
序号	终端名称	计算机IP	计算机MAC	使用规则					
1	192.168.1.12	192.168.1.12	902B345D0C96	默认规则					
2	192.168.1.24	192.168.1.24	000C29636842	默认规则					
3	192.168.1.31	192.168.1.31	94DE8D6C31E4	默认规则					
4	192.168.1.33	192.168.1.39	94DE8D6C32D8	默认规则					
5	192.168.1.42	192.168.1.41	902B34BD1293	默认规则					
6	192.168.1.42	192.168.1.42	000C293F8FE8	默认规则					
7	192.168.1.44	192.168.1.44	902B34D61762	默认规则					
8	192.168.1.46	192.168.1.46	000C29F08B2B	默认规则					
9	192.168.1.67	192.168.1.67	000C296DFEC1	默认规则					
10	192.168.1.69	192.168.1.69	10BF48D87DFB	默认规则					

4.3.4 黑名单

管理员可以手动将具有恶意行为的计算机或违反 IP/MAC 地址绑定规则的计算机，移动到黑名单，并限制其网络访问。

[illegible]

4.3.5 未授权

当受监控的计算机超出上网行为管理系统的授权范围后，授权范围外的计算机
会自动进入未授权组，无法监控。

[illegible]

4.4 【规则设置】

4.4.1 过滤规则管理

查询、添加、修改、删除监控规则。

» 您现在的位置：规则设置 » 过滤规则管理

规则名称:

查询

首页

前进

后退

末页

页次: 1 / 1页 共有 5记录, 每页 10 条数据

序号	规则名称	备注	操作
1	默认规则		修改 删除
2	zch_规则		修改 删除
3	zhb		修改 删除
4	zt		修改 删除
5	zht		修改 删除

规则名称:

*

备注:

+ 添加

修改

✖ 置空

4.4.2 内容过滤设置

记录被监控计算机的邮件收发内容，网站发帖内容，IM 工具聊天内容，桌面屏幕记录，以及 U 盘拷贝文件记录，上网实名认证功能。根据需要可以强制推送客户端到被监控计算机的浏览器，未安装客户端的计算机限制其网络访问，

欢迎您: admin 监控状态: **监控服务正在运行.....**

您现在的位置: 规则设置 > 内容过滤设置

选择过滤规则: **zch 规则**

☒ 强制安装客户端软件

☒ 邮件内容记录(主要指邮件工具如foxmail等)

☒ 发帖子内容记录(包括web邮件内容的记录)

☒ 桌面抓拍的时间间隔: 分钟

☒ 聊天内容记录

☒ 启用上网实名认证

☐ 客户机U盘信息记录(需要安装客户端软件)

☒ 客户机光驱禁用

☒ 客户机U盘禁用

4.4.3 网站过滤

设置需要禁止访问的网站域名或允许访问的网站域名，要禁止某个网站的所有网页，必须使用通配符*，例如限制网易：***.163.com**

您现在的位置: 规则设置 > 网站过滤

选择过滤规则: **市场部**

☐ 启动允许访问网站过滤 格式: www.google.cn, 可以用 *.google.cn 代表所有 google 网页

序号	过滤网址	过滤规则	备注	操作

☒ 启动禁止访问网站过滤 格式: www.google.cn, 可以用 *.google.cn 代表所有 google 网页

序号	过滤网址	过滤规则	备注	操作
1	news.163.com	市场部	网易新闻	修改 删除
2	news.baidu.com	市场部	百度新闻	修改 删除
3	news.ifeng.com	市场部	凤凰咨询	修改 删除
4	news.qq.com	市场部	腾讯新闻网	修改 删除
5	news.sina.com.cn	市场部	新浪新闻网	修改 删除

批量导入归类网站

☒ 启用不良网址库

过滤网址 (必填): ***.163.com**

中文名称 (选填):

4.4.4 邮件过滤

允许某个 mail 帐号或禁止某个 mail 帐号收发邮件

您现在的位置：规则设置 > 邮件过滤

选择过滤规则：默认规则

☒ 自动允许访问Email过滤 格式:test@163.com

序号	允许Email	过滤规则	备注	操作
1	ssgm_services@126.com	默认规则		修改 删除

允许Email（必填）：
ssgm_services@126.com

备注（选填）：

[+](#) 添加 [修改](#) [清空](#)

☐ 自动禁止通过Email过滤 格式:test@163.com

序号	过滤Email	过滤规则	备注	操作

过滤Email（必填）：

备注（选填）：

[+](#) 添加 [修改](#) [清空](#)

4.4.5 关键词过滤

禁止访问含有预设关键词的网页。

您现在的位置：规则设置 > 关键词过滤

选择过滤规则：市场部

☒ 自动关键词过滤

序号	过滤关键词	过滤规则	备注	操作
1	法轮功	市场部		修改 删除
2	疆独	市场部		修改 删除
3	疆独	市场部		修改 删除

过滤关键词（必填）：
疆独

中文名称（选填）：

[+](#) 添加 [修改](#) [清空](#)

4.4.6 应用软件过滤

禁止列表内的软件访问互联网，部分软件需要配合防火墙一起使用。

您现在的位置: 规则设置 > 应用软件过滤

选择过滤规则: zch_规则 保存

全部 视频 其他

zch_规则
默认规则
zch_规则
zhzh
zt
zht

页次: 1 / 1 页 共有 11 记录, 每页 15 条 第 1 页

全选 反选 禁用状态	过滤内容	备注	类别
<input checked="" type="checkbox"/> 禁止	搜狐视频	.sohu.com;HEAD /sohu;GET /sohu;	视频
<input checked="" type="checkbox"/> 禁止	土豆	.tudou;	视频
<input type="checkbox"/> 禁止	PPLive	.pplive.cn;pplive.com;pptv.com;	视频
<input type="checkbox"/> 禁止	UUSee	uusee.;	视频
<input type="checkbox"/> 禁止	QQ视频	qq.com;	视频
<input type="checkbox"/> 禁止	奇艺	qiyi.com;	视频
<input type="checkbox"/> 禁止	新浪	sina.com.cn;video.weibo.com;	视频
<input type="checkbox"/> 禁止	乐视	.letv.com;player.letv;	视频
<input type="checkbox"/> 禁止	优酷	youku.com;	视频
<input type="checkbox"/> 禁止	暴风	.baofeng.;	视频
<input type="checkbox"/> 禁止	其他		视频

4.4.7 端口过滤

限制被监控计算机的通过某些端口访问网络。

您现在的位置: 规则设置 > 端口过滤

选择过滤规则: 默认规则

☐ 启动端口过滤 格式:80或者分段8000-9000

页次: 1 / 1 页 共有 8 记录, 每页 15 条 第 1 页

过滤端口	备注	操作
<input type="checkbox"/> 禁止 80	访问因特网	删除
<input type="checkbox"/> 禁止 25	发送邮件	删除
<input type="checkbox"/> 禁止 110	接受邮件	删除
<input type="checkbox"/> 禁止 2000	登陆联众游戏	删除
<input type="checkbox"/> 禁止 5190	英文ICQ	删除
<input type="checkbox"/> 禁止 1630	网易泡泡	删除
<input type="checkbox"/> 禁止 5050	Yahoo Messenger	删除
<input type="checkbox"/> 禁止 1863	Msn Messenger	删除

端口号:

端口描述:

全选 添加 清空 保存

4.4.8 禁用程序设置

限制被监控计算机上某些应用程序的使用, 只需要添加程序的可执行文件名称即可。

您现在的位置: 规则设置 > 禁用程序 (需要安装客户端软件才能实现此功能)

选择过滤规则: 默认规则

☒ 启用禁用程序功能

可执行程序名称	备注	操作
qq.exe	腾讯QQ	修改 删除
thunder.exe	迅雷	修改 删除

聊天工具
程序名字 (如: qq.exe):
thunder.exe
备注:
迅雷
+ 添加 修改 置空

可执行程序名称	备注	操作

游戏库
程序名字 (如: qq.exe):
备注:
+ 添加 修改 置空

4.4.9 QQ 黑白名单设置

添加 qq 黑白名单可以控制 qq 的登陆行为。

盛世光明 网路神警上网行为管理

WELCOME 欢迎您: admin 监控状态: 监控服务正在运行..... 蓝皮肤 绿皮肤 紫皮肤 桌面 注销 退出

您现在的位置: 规则设置 > QQ黑白名单设置

选择过滤规则: 默认规则

☐ 启用QQ黑名单

序号	QQ号码	过滤规则	备注	操作
1	1991066720	默认规则	批量导入	修改 删除

批量导入配置QQ
QQ号码 (必填):
备注 (选填):
+ 添加 修改 置空

☐ 启用QQ黑名单

序号	QQ号码	过滤规则	备注	操作
1	1991066720	默认规则	批量导入	修改 删除

批量导入配置QQ
QQ号码 (必填):
备注 (选填):
+ 添加 修改 置空

4.4.10 分时段上网

设置被监控计算机可以访问互联网的时间段, 可以单个时间设置, 也可以批量设置

您现在的位置：规则设置 > 分时段上网

选择过滤规则 zht 批量设置时间

<input type="checkbox"/> 周日	全天候监控	修改
<input checked="" type="checkbox"/> 周一	02:00-02:59	修改
<input checked="" type="checkbox"/> 周二	02:00-02:59	修改
<input checked="" type="checkbox"/> 周三	02:00-02:59	修改
<input checked="" type="checkbox"/> 周四	02:00-02:59	修改
<input checked="" type="checkbox"/> 周五	02:00-02:59	修改
<input type="checkbox"/> 周六	全天候监控	修改

您现在的位置：规则设置 > 分时段上网

选择过滤规则 默认规则

设置周日时间

添加、修改、删除时间段后，必须保存所有添加的时间段规则才会有效

序号	开始时间	结束时间	操作

上网时间段为整点时间(精确到小时)

开始时间：

结束时间：

添加 清空 保存所有时间段

您现在的位置：规则设置 > 分时段上网

选择过滤规则 zht 批量设置时间

设置总体时间

序号	开始时间	结束时间	操作
1	02:00	02:59	修改 删除

☒ 周日 ☒ 周一 ☒ 周二 ☒ 周三 ☒ 周四 ☒ 周五 ☒ 周六 保存所有时间段

开始时间(时间为XX:00):
00:00

结束时间(时间为XX:59):
00:59

添加 清空 返回

4.4.11 规则分时段启用

设置过滤规则启用时间和停止时间，也可以批量设置。

» 您现在的位置：规则设置 » 规则分时段启用

选择过滤规则 默认规则

<input checked="" type="checkbox"/> 周日	全天候监控	+ 添加
<input checked="" type="checkbox"/> 周一	全天候监控	+ 添加
<input checked="" type="checkbox"/> 周二	全天候监控	+ 添加
<input checked="" type="checkbox"/> 周三	全天候监控	+ 添加
<input checked="" type="checkbox"/> 周四	全天候监控	+ 添加
<input checked="" type="checkbox"/> 周五	全天候监控	+ 添加
<input checked="" type="checkbox"/> 周六	全天候监控	+ 添加

» 您现在的位置：规则设置 » 规则分时段启用

选择过滤规则 zl + 批量设置时间

设置 **总体** 时间

序号	开始时间	结束时间	操作
1	12:00	15:00	修改 删除

☒ 周日 ☒ 周一 ☒ 周二 ☐ 周三 ☐ 周四 ☐ 周五 ☐ 周六
 + 保存所有时间段

开始时间： 格式：12:00
 结束时间： 格式：12:00
+ 提交 清空 返回

4.5 【日志查询】

4.5.1 上网日志

按照计算机名称，ip 地址，mac 地址，计算机分组查询被监控计算机的浏览网页记录。

[illegible]

4.5.2 邮件日志

查询被监控计算机收发邮件记录。

» 您现在的位置：日志查询 » 邮件日志

计算机：

☒ 计算机名称 ☐ 计算机IP ☐ 计算机MAC ☐ 按照分组

计算机名称：

全部计算机

时间：

☐ 今天 ☐ 本周 ☐ 本月 ☐ 本年 ☒ 全部时间 ☐ 具体时间

点击查看内容，可以查看邮件的详细信息

首页

前进

后退

末页

页次：1 / 7 页 共有125 条信息，每页 20 条 转到 第 1 页

序号	终端计算机名称	终端计算机IP	终端计算机MAC	时间	发送邮件地址	接收邮件地址	状态	附件	操作
1	test123	192.168.3.188	00E062014611	2013-03-25 16:59:36	zht@ssgm.net	yangcq@ssgm.netqcz@ssgm.net,45758282@qq.com,ssgmnrz@163.com,	发送	无	查看内容
2	XP-201209251357	192.168.3.254	002421F1CE40	2013-03-25 16:55:16	zch@ssgm.net	gcz@ssgm.net45758282@qq.com,yangcq@ssgm.net,ssgmnrz@163.com,bj@ssgm.net,	发送	无	查看内容
3	XP-201209251357	192.168.3.254	002421F1CE40	2013-03-25 16:54:51	ssgmnrz@163.com	zch@ssgm.net	接收	无	查看内容
4	192.168.1.66	192.168.1.66	00016C7C9243	2013-03-25 16:53:18	wfj@ssgm.net	gaoyuan@ssgm.net,hmy@ssgm.net,th@ssgm.net	发送	无	查看内容
5	192.168.1.199	192.168.1.199	001A92800A92	2013-03-25 16:48:57	sunyy@ssgm.net	zww@ssgm.net,ydh@ssgm.net,zhangjl@ssgm.net,zhangpf@ssgm.net,wds@ssgm.net,gaoyuan@ssgm.net	发送	有	查看内容
6	192.168.1.77	192.168.1.77	00269E45A0E4	2013-03-25 16:34:06	13505375153@126.com	gx3262@126.com	发送	无	查看内容
7	PC1222UHY	192.168.3.183	00E04C380C6F	2013-03-25 16:17:49	ls@ssgm.net	lj@ssgm.net	发送	有	查看内容
8	PC0905PYT	192.168.3.101	9028344E3D38	2013-03-25 16:10:26	zhougqian_test@126.com	zhouguangqian_test@163.comzhougqian_test@126.com,	接收	无	查看内容
9	PC0905PYT	192.168.3.101	9028344E3D38	2013-03-25 16:08:29	zhougqian_test@126.com	zhouguangqian_test@163.com	发送	无	查看内容
10	PC0905PYT	192.168.3.101	9028344E3D38	2013-03-25 16:06:22	zhouguangqian_test@sina.cn	zhouguangqianzhou@tom.com	发送	无	查看内容
11	PC0905PYT	192.168.3.101	9028344E3D38	2013-03-25 16:04:36	zhougqian@yahoo.cn	guangqianzhou@tom.com;	发送	无	查看内容
12	PC0905PYT	192.168.3.101	9028344E3D38	2013-03-25 16:01:38	zhouguangqian_test@163.com	zhouguangqianzhou@tom.com;	发送	无	查看内容
13	PC0905PYT	192.168.3.101	9028344E3D38	2013-03-25 15:58:20	zhouguangqian_test@163.com	guangqianzhou@tom.com;	发送	无	查看内容
14	PC0905PYT	192.168.3.101	9028344E3D38	2013-03-25 15:50:01	zhouguangqian_test@163.com	zhouguangqianzhou@tom.com	发送	无	查看内容
15	PC0905PYT	192.168.3.101	9028344E3D38	2013-03-25 15:47:53	zhouguangqian_test@163.com	guangqianzhou@tom.com	发送	无	查看内容

4.5.3 发帖日志

查询被监控计算机网上发帖记录。

您现在的位置: 日志查询 > 发帖日志

计算机: ☒ 计算机名称 ☐ 计算机IP ☐ 计算机MAC ☐ 按照分组 计算机名称: 全部计算机

时间: ☐ 今天 ☐ 本周 ☐ 本月 ☐ 本年 ☒ 全部时间 ☐ 具体时间

关键词:

点击查看内容, 可以看到该帖子的详细内容

查询 导出

页次: 1 / 5 页 共有 85 条信息, 每页 20 条 转到第 1 页

序号	计算机名称	本地机器IP	本地计算机MAC	发帖人	发帖时间	操作
1	192.168.1.126	192.168.1.126	78ACC04C961F	270981535	2013-03-25 16:42:59	查看内容
2	JBL	192.168.3.143	902B34C9ACB1	512911143	2013-03-25 16:31:35	查看内容
3	LDM	192.168.3.236	902B34D34CBE	LDM	2013-03-25 16:13:12	查看内容
4	LDM	192.168.3.236	902B34D34CBE	LDM	2013-03-25 16:13:04	查看内容
5	LDM	192.168.3.236	902B34D34CBE	LDM	2013-03-25 16:11:42	查看内容
6	LDM	192.168.3.236	902B34D34CBE	LDM	2013-03-25 16:11:41	查看内容
7	LDM	192.168.3.236	902B34D34CBE	LDM	2013-03-25 16:11:10	查看内容
8	LDM	192.168.3.236	902B34D34CBE	LDM	2013-03-25 16:11:05	查看内容
9	LDM	192.168.3.236	902B34D34CBE	LDM	2013-03-25 16:10:31	查看内容
10	LDM	192.168.3.236	902B34D34CBE	LDM	2013-03-25 16:10:29	查看内容
11	LDM	192.168.3.236	902B34D34CBE	LDM	2013-03-25 16:06:49	查看内容
12	LDM	192.168.3.236	902B34D34CBE	LDM	2013-03-25 16:05:49	查看内容
13	LDM	192.168.3.236	902B34D34CBE	LDM	2013-03-25 16:05:38	查看内容
14	LDM	192.168.3.236	902B34D34CBE	514689488	2013-03-25 15:50:48	查看内容
15	192.168.1.234	192.168.1.234	001E90114347	843266385	2013-03-25 15:37:29	查看内容
16	192.168.1.66	192.168.1.66	00016C7C9243	192.168.1.66	2013-03-25 15:28:56	查看内容
17	192.168.1.199	192.168.1.199	001A92800A92	192.168.1.199	2013-03-25 15:25:42	查看内容
18	192.168.1.199	192.168.1.199	001A92800A92	192.168.1.199	2013-03-25 15:25:20	查看内容
19	ZRL	192.168.3.177	902B34D348EC	ZRL	2013-03-25 14:58:08	查看内容
20	192.168.1.66	192.168.1.66	00016C7C9243	192.168.1.66	2013-03-25 14:55:42	查看内容

页次: 1 / 5 页 共有 85 条信息, 每页 20 条 转到第 1 页

4.5.4 移动磁盘日志

查询被监控计算机使用移动存储设备拷贝文件记录。

您现在的位置: 日志查询 > 移动磁盘使用日志

计算机: ☒ 终端名称 ☐ 计算机IP ☐ 计算机MAC ☐ 按照分组 终端名称: 全部计算机

时间: ☒ 今天 ☐ 本周 ☐ 本月 ☐ 本年 ☐ 全部时间 ☐ 具体时间

查询 导出

页次: 1 / 1 页 共有 5 记录, 每页 20 条 第 1 页

序号	终端名称	计算机IP	计算机MAC	操作时间	操作内容
1	192.168.1.169	192.168.1.169	94DE806C320F	2013-08-27 11:30:58	移去移动磁盘: L
2	192.168.1.169	192.168.1.169	94DE806C320F	2013-08-27 11:30:58	移去移动磁盘: M
3	hh	192.168.1.56	00E062014611	2013-08-27 10:14:52	移去移动磁盘: H
4	hh	192.168.1.56	00E062014611	2013-08-27 10:14:37	添加移动磁盘: H
5	192.168.1.115	192.168.1.115	94DE806C31FE	2013-08-27 09:39:11	移去移动磁盘: H

4.5.4 虚拟身份

查询被监控计算机网上登录论坛、社区记录, 如: 天涯, 猫扑、百度贴吧。

您现在的位置: 日志查询 > 虚拟身份

计算机: ☒ 计算机名称 ☐ 计算机IP ☐ 计算机MAC ☐ 按照分组 计算机名称: 全部计算机

时间: ☐ 今天 ☐ 本周 ☐ 本月 ☐ 本年 ☒ 全部时间 ☐ 具体时间

序号	计算机名称	本地机器IP	本地计算机MAC	用户名	链接网址	登录时间
1	PC0905PYT	192.168.3.101	902B344E3D38	zhougqian_test	login.sina.com.cn	2013-03-25 16:58:26
2	MICROSOF-9292F3	192.168.3.96	902B340B7C2C	316264642	ptlogin2.qq.com	2013-03-25 16:53:24
3	192.168.3.69	192.168.3.69	108F480B7DFB	1137657107	ptlogin2.qq.com	2013-03-25 16:51:47
4	192.168.1.57	192.168.1.57	000AE42CB75F	106940579	ptlogin2.qq.com	2013-03-25 16:50:08
5	192.168.1.77	192.168.1.77	00269E45A0E4	93034130	ptlogin2.qq.com	2013-03-25 16:50:01
6	MICROSOF-9292F3	192.168.3.96	902B340B7C2C	zhanghui27525337@163.com	www.ymcn.org	2013-03-25 16:48:15
7	PC-20121110DWX	192.168.3.144	00E04C3821D8	eternal_kite	cwebmail.mail.163.com	2013-03-25 16:45:49
8	192.168.1.126	192.168.1.126	78AC04C961F	270981535	ptlogin2.qq.com	2013-03-25 16:42:22
9	PC201112409ORH	192.168.3.55	00E04C39C268	yc2012	www.ymcn.org	2013-03-25 16:40:47
10	192.168.1.77	192.168.1.77	00269E45A0E4	93034130	ptlogin2.qq.com	2013-03-25 16:37:58
11	192.168.3.232	192.168.3.232	001377043A4A	362367273	ptlogin2.qq.com	2013-03-25 16:37:57
12	192.168.1.77	192.168.1.77	00269E45A0E4	wzhongl	cwebmail.mail.126.com	2013-03-25 16:32:49
13	JBL	192.168.3.143	902B34C9ACB1	512911143	ptlogin2.qq.com	2013-03-25 16:31:27
14	ZRL	192.168.3.177	902B34D34BEC	30445105	ptlogin2.qq.com	2013-03-25 16:30:40
15	192.168.1.77	192.168.1.77	00269E45A0E4	wzhongl1989	newallot.im.alssoft.com	2013-03-25 16:29:51
16	192.168.1.30	192.168.1.30	00245459ACA5	775181659	login.sina.com.cn	2013-03-25 16:26:16
17	192.168.3.232	192.168.3.232	001377043A4A	362367273	ptlogin2.qq.com	2013-03-25 16:26:14
18	192.168.1.234	192.168.1.234	001E90114347	843266385	ptlogin2.qq.com	2013-03-25 16:22:02
19	192.168.1.32	192.168.1.32	88AE1D28C3CE	z6605@126.com	weibo.com	2013-03-25 16:20:40
20	192.168.1.16	192.168.1.16	001A926D21C2	357707805	ptlogin2.qq.com	2013-03-25 16:13:29

页次: 1 / 10 页 共有 198 条信息, 每页 20 条 转到 第 1 页

4.5.5 聊天日志

查询被监控计算机的聊天记录。

您现在的位置: 日志查询 > 聊天日志

计算机: ☒ 终端名称 ☐ 计算机IP ☐ 计算机MAC ☐ 按照分组 终端名称: 全部计算机

时间: ☒ 今天 ☐ 本周 ☐ 本月 ☐ 本年 ☐ 全部时间 ☐ 具体时间

聊天工具: 全部聊天工具

序号	证件号码	终端名称	本地机器IP	本地计算机MAC	操作
1	115	192.168.1.115	192.168.1.115	94010316C01E	查看内容
2	115	192.168.1.115	192.168.1.115	94010316C01E	查看内容
3	115	192.168.1.115	192.168.1.115	94010316C01E	查看内容
4	115	192.168.1.115	192.168.1.115	94010316C01E	查看内容
5	115	192.168.1.115	192.168.1.115	94010316C01E	查看内容
6	115	192.168.1.115	192.168.1.115	94010316C01E	查看内容
7	115	192.168.1.115	192.168.1.115	94010316C01E	查看内容
8	115	192.168.1.115	192.168.1.115	94010316C01E	查看内容
9	115	192.168.1.115	192.168.1.115	94010316C01E	查看内容
10	169	192.168.1.169	192.168.1.169	94010316C01E	查看内容
11	169	192.168.1.169	192.168.1.169	94010316C01E	查看内容
12	169	192.168.1.169	192.168.1.169	94010316C01E	查看内容
13	115	192.168.1.115	192.168.1.115	94010316C01E	查看内容
14	169	192.168.1.33	192.168.1.33	94010316C01E	查看内容
15	115	192.168.1.115	192.168.1.115	94010316C01E	查看内容
16	169	192.168.1.33	192.168.1.33	94010316C01E	查看内容
17	115	192.168.1.115	192.168.1.115	94010316C01E	查看内容
18	115	192.168.1.115	192.168.1.115	94010316C01E	查看内容

查看聊天内容

QQ号码: 53164089 时间: 2013-08-27 14:30:49
selenium启动错误怎么解决

QQ号码: 53164089 时间: 2013-08-27 14:32:01
[图片]

4.5.6 上下线日志

查看实名认证的帐号的上下线日志

您现在的位置: 日志查询 > 上下线日志

计算机: ☒ 终端名称 ☐ 计算机IP ☐ 计算机MAC ☐ 按照分组 终端名称: 全部计算机

时间: ☒ 今天 ☐ 本周 ☐ 本月 ☐ 本年 ☐ 全部时间 ☐ 具体时间

其他: ☒ 全部时间 ☐ 上线时间 ☐ 下线时间

证件类型: 所有类型 上网人员姓名: 证件号码:

查询 导出

分页: 1 / 1页 共有 1记录, 每页 20 条 第 1 页

序号	终端名称	计算机IP	计算机MAC	上线时间	下线时间	人员姓名	证件类型	证件号码	国籍	单位
1	192.168.1.115	192.168.1.115	94DE806C31FE	20130827093935		管理员	中国人民武装警察部队警官证	115	黎巴嫩 Lebanon	

4.5.7 桌面抓拍

查询被监控计算机桌面图片记录。

您现在的位置: 日志查询 > 桌面抓拍

计算机: ☒ 终端名称 ☐ 计算机IP ☐ 计算机MAC ☐ 按照分组 终端名称: 全部计算机

时间: ☒ 今天 ☐ 本周 ☐ 本月 ☐ 本年 ☐ 全部时间 ☐ 具体时间

查询 导出

分页: 1 / 9页 共有 42记录, 每页 5 条 第 1 页

序号	终端名称	计算机IP	计算机MAC	记录时间	图片预览
1	192.168.1.115	192.168.1.115	94DE806C31FE	2013-08-27 14:33:10	
2	192.168.1.115	192.168.1.115	94DE806C31FE	2013-08-27 14:28:10	
3	192.168.1.115	192.168.1.115	94DE806C31FE	2013-08-27 14:23:10	
4	192.168.1.115	192.168.1.115	94DE806C31FE	2013-08-27 14:18:13	

4.5.8 更改 IP/MAC 使用日志

查询客户端机器 IP/MAC 修改情况

您现在的位置: 日志查询 > 更改IP/MAC使用日志

计算机: ☒ 计算机名称 ☐ 计算机IP ☐ 计算机MAC ☐ 按照分组 计算机名称: 全部计算机

时间: ☒ 今天 ☐ 本周 ☐ 本月 ☐ 本年 ☐ 全部时间 ☐ 具体时间

查询 导出

首页 前进 后退 末页 页次: 1 / 4 页 共有80条信息, 每页 20 条 转到第 1 页

序号	本地计算机名称	修改前IP	修改后IP	修改前MAC	修改后MAC	记录时间
1	test	192.168.7.28	192.168.7.52	00E062014611	00E062014611	2012-03-23 14:51:17
2	144	192.168.7.38	192.168.7.13	00E04C3821D8	00E04C3821D8	2012-03-23 14:48:01
3	zjl	192.168.7.26	192.168.7.43	0009687AE385	0009687AE385	2012-03-23 14:47:20
4		192.168.7.31	192.168.7.26	0009687AE385	0009687AE385	2012-03-23 14:45:07
5	44	192.168.7.41	192.168.7.4	902834061762	902834061762	2012-03-23 14:41:43
6	sr	192.168.7.36	192.168.7.28	00E062014611	00E062014611	2012-03-23 14:18:57
7	zjl	192.168.7.30	192.168.7.31	0009687AE385	0009687AE385	2012-03-23 14:18:15
8	zjl	192.168.7.37	192.168.7.30	0009687AE385	0009687AE385	2012-03-23 13:58:54
9	sr	192.168.7.36	192.168.7.36	001D0F160358	00E062014611	2012-03-23 13:42:54
10	zjl	192.168.7.29	192.168.7.37	0009687AE385	0009687AE385	2012-03-23 13:40:29
11	3	192.168.7.17	192.168.7.17	002388822AA8	00028308C9CE	2012-03-23 13:34:35
12	test	192.168.7.27	192.168.7.19	00E062014611	00E062014611	2012-03-23 13:29:04
13	10	192.168.7.7	192.168.7.39	000D8743A6F3	000D8743A6F3	2012-03-23 13:28:36
14	zjl	192.168.7.21	192.168.7.29	0009687AE385	0009687AE385	2012-03-23 13:21:55
15	zjl	192.168.7.25	192.168.7.21	0009687AE385	0009687AE385	2012-03-23 13:18:11
16	zjl	192.168.7.22	192.168.7.25	0009687AE385	0009687AE385	2012-03-23 13:06:51
17	zjl	192.168.7.9	192.168.7.22	0009687AE385	0009687AE385	2012-03-23 13:04:24
18	zjl	192.168.7.13	192.168.7.20	00E04C174B46	00E04C174B46	2012-03-23 13:03:10
19	zjl	192.168.7.35	192.168.7.9	0009687AE385	0009687AE385	2012-03-23 12:55:19
20	zjl	192.168.7.33	192.168.7.35	0009687AE385	0009687AE385	2012-03-23 12:45:23

首页 前进 后退 末页 页次: 1 / 4 页 共有80条信息, 每页 20 条 转到第 1 页

4.5.9 虚拟身份

查询被监控计算机网上登录论坛、社区记录, 如: 天涯, 猫扑、百度贴吧。

您现在的位置: 日志查询 > 虚拟身份日志

计算机: ☒ 终端名称 ☐ 计算机IP ☐ 计算机MAC ☐ 按照分组 终端名称: 全部计算机

时间: ☒ 今天 ☐ 本周 ☐ 本月 ☐ 本年 ☐ 全部时间 ☐ 具体时间

用户名:

查询 导出

首页 前进 后退 末页 页次: 1 / 1 页 共有 20 记录, 每页 20 条 第 1 页

序号	终端名称	计算机IP	计算机MAC	用户名	链接网址	登录时间
1	192.168.1.223	192.168.1.223	9028340619A2	8925984	ptlogin2.qq.com	2013-08-27 13:19:56
2	192.168.1.153	192.168.1.153	94DE806D755A	1024773779	ptlogin2.qq.com	2013-08-27 12:41:40
3	192.168.1.96	192.168.1.96	902834087C2C	316264642	ptlogin2.qq.com	2013-08-27 11:40:35
4	192.168.1.33	192.168.1.39	94DE806C3208	284189983	ptlogin2.qq.com	2013-08-27 11:38:48
5	hh	192.168.1.56	00E062014611	zhfhvscj_tt49p	login.sina.com.cn	2013-08-27 11:24:19
6	192.168.1.96	192.168.1.96	902834087C2C	1955992461	ptlogin2.qq.com	2013-08-27 11:19:24
7	192.168.1.144	192.168.1.144	00E04C3821D8	278183349	ptlogin2.qq.com	2013-08-27 10:50:52
8	192.168.1.223	192.168.1.223	9028340619A2	8925984	ptlogin2.qq.com	2013-08-27 10:46:28
9	192.168.1.223	192.168.1.223	9028340619A2	8925984	ptlogin2.qq.com	2013-08-27 10:40:37
10	192.168.1.44	192.168.1.44	902834061762	1399152716	ptlogin2.qq.com	2013-08-27 10:30:51
11	192.168.1.33	192.168.1.33	94DE806C3208	1114512060	ptlogin2.qq.com	2013-08-27 10:23:21
12	192.168.1.169	192.168.1.169	94DE806C320F	314359628	ptlogin2.qq.com	2013-08-27 10:22:35
13	192.168.1.115	192.168.1.115	94DE806C31FE	237583353	ptlogin2.qq.com	2013-08-27 10:21:18
14	192.168.1.115	192.168.1.115	94DE806C31FE	757016135	ptlogin2.qq.com	2013-08-27 10:21:08
15	192.168.1.129	192.168.1.129	00E04CA37115	273197103	ptlogin2.qq.com	2013-08-27 10:11:34
16	192.168.1.115	192.168.1.115	94DE806C31FE	237583353	ptlogin2.qq.com	2013-08-27 09:47:11
17	192.168.1.223	192.168.1.223	9028340619A2	8925984	ptlogin2.qq.com	2013-08-27 09:39:12
18	192.168.1.223	192.168.1.223	9028340619A2	295563077	ptlogin2.qq.com	2013-08-27 09:35:59
19	192.168.1.153	192.168.1.153	94DE806D755A	1024773779	ptlogin2.qq.com	2013-08-27 09:23:56
20	192.168.1.153	192.168.1.153	94DE806D755A	604561296	ptlogin2.qq.com	2013-08-27 09:01:04

4.5.10 报警日志

查询报警信息的详细内容

您现在的位置: 日志查询 > 报警日志

时间: ☒ 今天 ☐ 本周 ☐ 本月 ☐ 本年 ☐ 全部时间 ☐ 具体时间

查询条件: 报警类型:

序号	发送邮箱	接收邮箱	报警内容	时间	发送与否	操作
1	1114512060@qq.com	s8gm8008@163.com	您的监控机内存使用率高于20%，为22%，详细信息为：22%...	2012-07-23 13:28:36	已发送	查看内容
2	1114512060@qq.com	s8gm8008@163.com	您的监控机内存使用率高于20%，为22%，详细信息为：22%...	2012-07-23 13:12:36	已发送	查看内容
3	1114512060@qq.com	s8gm8008@163.com	您的监控机内存使用率高于20%，为23%，详细信息为：23%...	2012-07-23 12:54:36	未发送	查看内容
4	1114512060@qq.com	s8gm8008@163.com	您的监控机内存使用率高于20%，为23%，详细信息为：23%...	2012-07-23 12:38:36	已发送	查看内容
5	1114512060@qq.com	s8gm8008@163.com	您的监控机内存使用率高于20%，为23%，详细信息为：23%...	2012-07-23 12:22:35	已发送	查看内容
6	1114512060@qq.com	s8gm8008@163.com	您的监控机内存使用率高于20%，为22%，详细信息为：22%...	2012-07-23 12:06:34	已发送	查看内容
7	1114512060@qq.com	s8gm8008@163.com	您的监控机内存使用率高于20%，为22%，详细信息为：22%...	2012-07-23 11:50:34	已发送	查看内容
8	1114512060@qq.com	s8gm8008@163.com	您的监控机内存使用率高于20%，为22%，详细信息为：22%...	2012-07-23 11:34:33	已发送	查看内容
9	1114512060@qq.com	s8gm8008@163.com	您的监控机内存使用率高于20%，为22%，详细信息为：22%...	2012-07-23 11:18:32	已发送	查看内容

页次: 1 / 1 页 共有9条信息, 每页 20 条 转到 第 1 页

4.5.11 操作日志

查询管理员对系统操作日志。

您现在的位置: 日志查询 > 操作日志

时间: ☒ 今天 ☐ 本周 ☐ 本月 ☐ 本年 ☐ 全部时间 ☐ 具体时间

查询条件: 操作类型: 操作用户:

序号	操作类型	操作时间	登录IP	操作描述	操作用户	成功与否
1	修改下发过滤策略	2013-08-27 14:29:26	192.168.1.39	设置分时段启用规则	admin	成功
2	增加修改删除用户	2013-08-27 14:13:09	192.168.1.115	监控组批量修改规则	admin	成功
3	修改系统配置	2013-08-27 14:11:06	192.168.1.39	修改IP地址段成功	admin	成功
4	修改系统配置	2013-08-27 14:11:05	192.168.1.39	修改IP地址段成功	admin	成功
5	鉴别与登录	2013-08-27 13:18:39	192.168.1.39	系统登录	admin	成功
6	增加修改删除用户	2013-08-27 11:20:43	192.168.1.39	监控组批量修改规则	admin	成功
7	增加修改删除用户	2013-08-27 11:20:26	192.168.1.39	监控组批量IP/MAC绑定	admin	成功
8	增加修改删除用户	2013-08-27 11:20:24	192.168.1.39	监控组批量IP/MAC绑定	admin	成功
9	修改下发过滤策略	2013-08-27 11:19:06	192.168.1.56	禁用桌面抓拍	admin	成功
10	修改下发过滤策略	2013-08-27 11:19:04	192.168.1.56	禁用QQ聊天记录	admin	成功
11	增加修改删除用户	2013-08-27 11:18:42	192.168.1.33	监控组批量IP/MAC绑定	admin	成功
12	备份与恢复	2013-08-27 11:03:16	192.168.1.33	数据库还原成功	admin	成功
13	备份与恢复	2013-08-27 11:02:51	192.168.1.169	数据库还原成功	admin	成功
14	系统启动与关闭	2013-08-27 10:56:40	192.168.1.33	监控服务启动成功	admin	成功
15	系统启动与关闭	2013-08-27 10:56:36	192.168.1.33	监控服务停止	admin	成功
16	备份与恢复	2013-08-27 10:52:01	192.168.1.56	数据库还原成功	admin	成功
17	修改下发过滤策略	2013-08-27 10:50:44	192.168.1.169	设置应用软件过滤规则	admin	成功
18	修改下发过滤策略	2013-08-27 10:50:31	192.168.1.169	规则保存成功	admin	成功
19	修改系统配置	2013-08-27 10:48:40	192.168.1.33	保存报警信息设置	admin	成功
20	修改下发过滤策略	2013-08-27 10:46:56	192.168.1.169	设置应用软件过滤规则	admin	成功

页次: 1 / 11 页 共有 209 记录, 每页 20 条 第 1 页

4.6 【网站排名】

4.6.1 查询网站排名

查询局域网内所有计算机点击网站排名，并由高到低进行排序。此处还可以将访问次数过多的网址手动添加到指定的规则中。

您现在的位置：网站排名》查询网站排名

计算机：☒ 计算机名称 ☐ 计算机IP ☐ 计算机MAC ☐ 按照分组 计算机名称：全部计算机

时间：☒ 今天 ☐ 本周 ☐ 本月 ☐ 本年 ☐ 全部时间 ☐ 具体时间

显示模式：报表

首页 前进 后退 末页 页次：1 / 30 页 共有439条信息，每页15条 转到第1页

<input type="checkbox"/> 禁用网站	访问网站	访问次数
<input type="checkbox"/>	www.taobao.com	297
<input type="checkbox"/>	www.baidu.com	230
<input type="checkbox"/>	cpro.baidu.com	178
<input checked="" type="checkbox"/>	news.sina.com.cn	167
<input type="checkbox"/>	tuan.paipai.com	115
<input type="checkbox"/>	www.paipai.com	98
<input type="checkbox"/>	z.alimama.com	96
<input type="checkbox"/>	widget.weibo.com	77
<input type="checkbox"/>	topic.csdn.net	72
<input type="checkbox"/>	taojinbi.taobao.com	70
<input type="checkbox"/>	bj.house.sina.com.cn	58
<input checked="" type="checkbox"/>	zhidao.baidu.com	56
<input type="checkbox"/>	m510.mail.qq.com	40
<input type="checkbox"/>	cwebmail.mail.163.com	39
<input type="checkbox"/>	home.focus.cn	39

首页 前进 后退 末页 页次：1 / 30 页 共有439条信息，每页15条 转到第1页

<input type="checkbox"/> 规则选择	监控规则
<input type="checkbox"/>	默认规则
<input type="checkbox"/>	办公室
<input type="checkbox"/>	研发部
<input type="checkbox"/>	测试部
<input type="checkbox"/>	客服部
<input type="checkbox"/>	营销部

还可以根据不同需要查看环状图。

您现在的位置：网站排名》查询网站排名

计算机：
☒ 计算机名称 ☐ 计算机IP ☐ 计算机MAC ☐ 按照分组
 计算机名称：全部计算机

时间：
☒ 今天 ☐ 本周 ☐ 本月 ☐ 本年 ☐ 全部时间 ☐ 具体时间

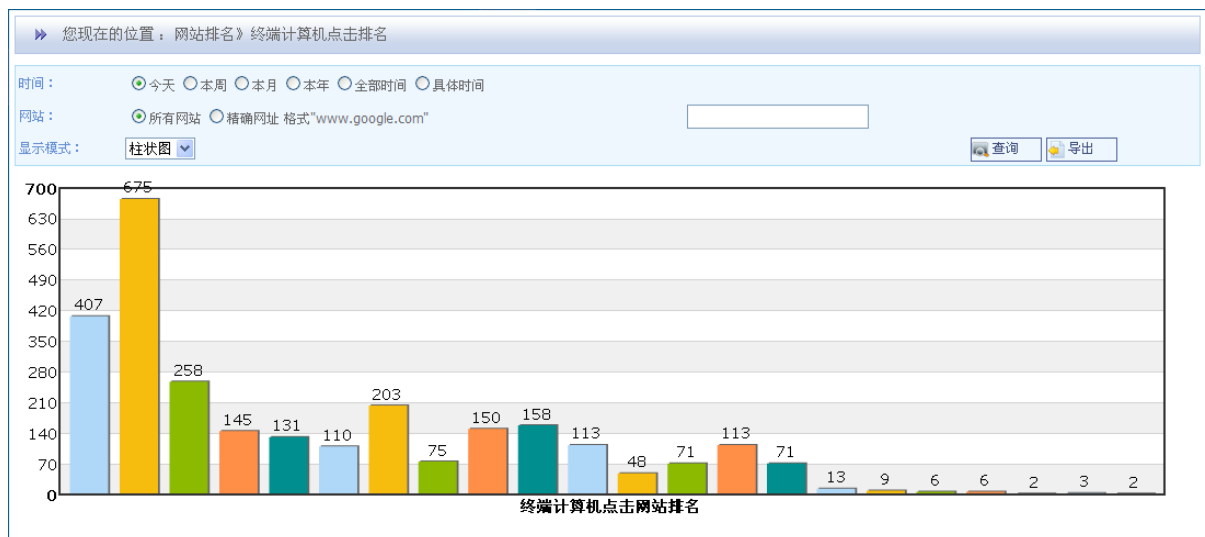
显示模式：
 环状图

查询 导出



4.6.2 终端计算机点击排名

查询某计算机点击网站次数，可以以报表、环状图和柱状图的形式显示。



4.7 【在线时间】

查询在线时间，查询被监控计算机的上网时间，可以以报表、环状图和柱状图的形式显示。

您现在的位置：在线时间》查询在线时间

计算机： ☒ 计算机名称 ☐ 计算机IP ☐ 计算机MAC ☐ 按照分组 计算机名称：全部计算机

时间： ☒ 今天 ☐ 本周 ☐ 本月 ☐ 本年 ☐ 全部时间 ☐ 具体时间

显示模式： 报表

排名	计算机名称	计算机IP	计算机MAC	在线时间(小时)
1	hmy	192.168.7.8	001C253AF73E	3.92
2	135	192.168.7.48	00262D987D0D	3.42
3	155	192.168.7.50	902B3406147E	3.25
4	sqh	192.168.7.46	000AE42CB75F	3.00
5	wl	192.168.7.14	E811328A11A9	2.83
6	1	192.168.7.15	001E90114347	2.50
7	wfj	192.168.7.23	001C2536DFD4	2.08
8	srr	192.168.7.21	001D0F18035B	2.08
9	3	192.168.7.11	001377043A4A	1.75
10	zh	192.168.7.18	001E9012AF4C	1.58
11	wj	192.168.7.5	0008749592D0	1.42
12	2	192.168.7.45	902B340619A2	1.25
13	wfj	192.168.7.20	001C2536DFD4	1.17
14	test	192.168.7.43	00E062014611	1.08
15	test	192.168.7.36	00E062014611	0.92

页次：1 / 3 页 共有37条信息，每页 15 条 转到第 1 页

4.8 【流量统计】

4.8.1 查询流量

查询被监控计算机所产生的网络流量，并由高到低的顺序进行排序。

您现在的位置：流量统计》查询流量

计算机： ☒ 计算机名称 ☐ 计算机IP ☐ 计算机MAC ☐ 按照分组 计算机名称：全部计算机

时间： ☒ 今天 ☐ 本周 ☐ 本月 ☐ 本年 ☐ 全部时间 ☐ 具体时间

显示模式： 报表

排名	计算机名称	计算机IP	计算机MAC	流量(MB)
1	www-ff02c3bdeef	192.168.9.206	50E5494F5106	6.1
2	www-ff02c3bdeef	192.168.9.230	00173164113C	0
3	www-ff02c3bdeef	192.168.9.211	00248C557D4F	0
4	www-ff02c3bdeef	192.168.9.88	00248C557D4F	0
5	www-ff02c3bdeef	192.168.9.210	50E5492B399D	0
6	www-ff02c3bdeef	192.168.9.1	5C63BF7A5E1E	0
7	www-ff02c3bdeef	192.168.9.60	6CF0498FB538	0
8	www-ff02c3bdeef	192.168.9.115	6CF0498FB547	0
9	www-ff02c3bdeef	192.168.9.254	C83A350C67D8	0

页次：1 / 1 页 共有9条信息，每页 15 条 转到第 1 页

4.8.2 实时流量查看

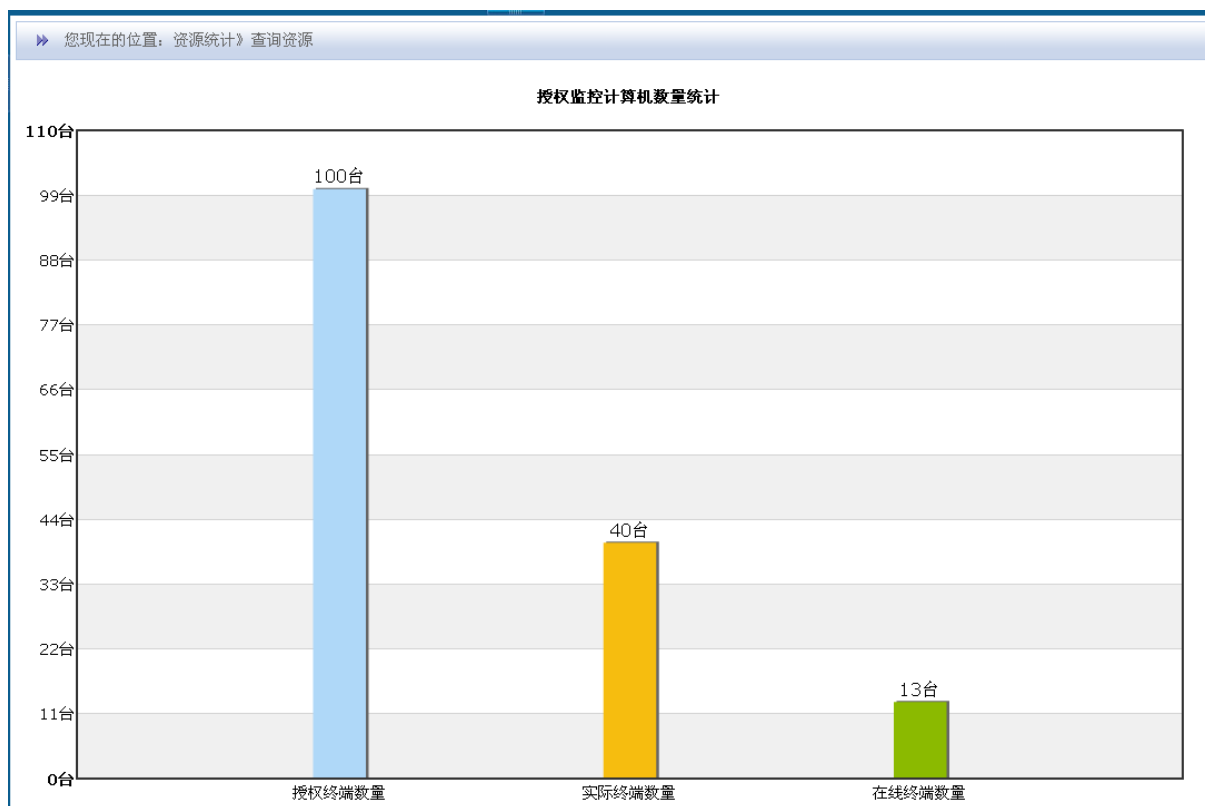
查看被监控计算机的实时流量。



4.9 【资源统计】

查询资源，查询局域网内实际计算机数量，在线计算机数量以及软件授权监控

数量。



4.10 【系统帮助】

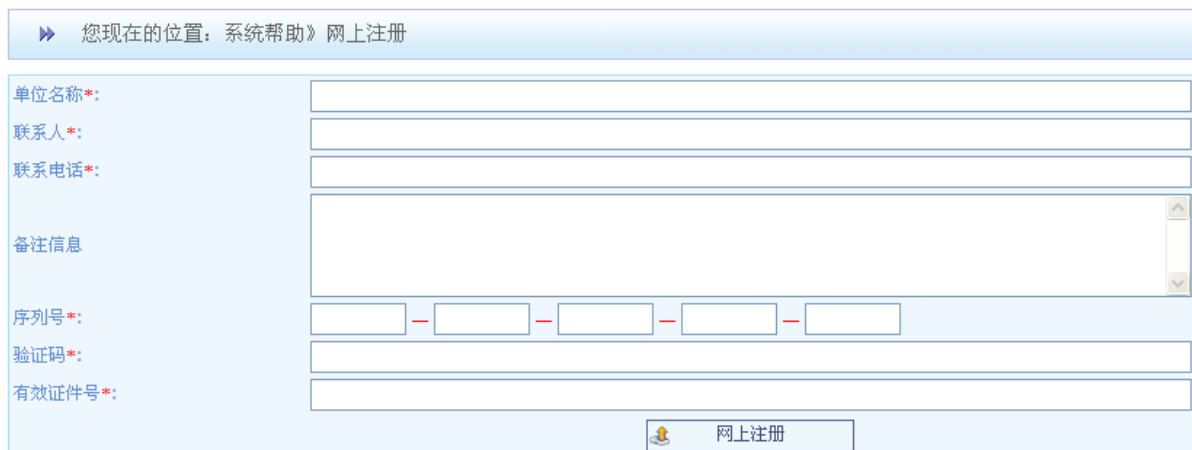
帮助文档，查看系统帮助文档。

技术支持，提供在线技术支持。

关于系统，显示系统版本号等信息。



网上注册。试用版本提供注册界面，已注册版本查看注册信息。



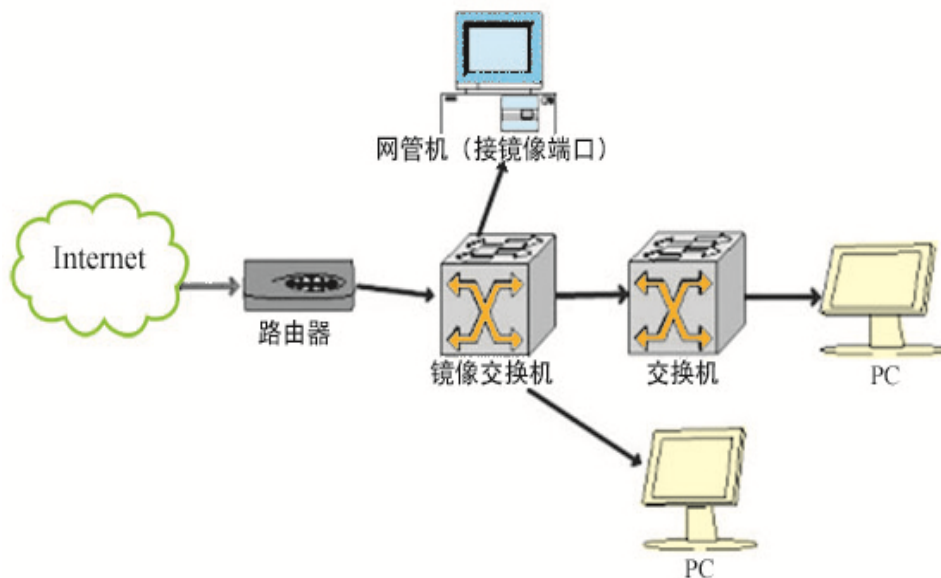
点击窗体上方蓝色、绿色、紫色按钮，可以改变管理系统的主题。点击右上角桌面，显示系统快捷面板，点击相应按钮，可以快速打开对应管理界面。点击右上角注销按钮，注销本次登录，点击退出按钮，关闭当前窗口。

五．产品部署

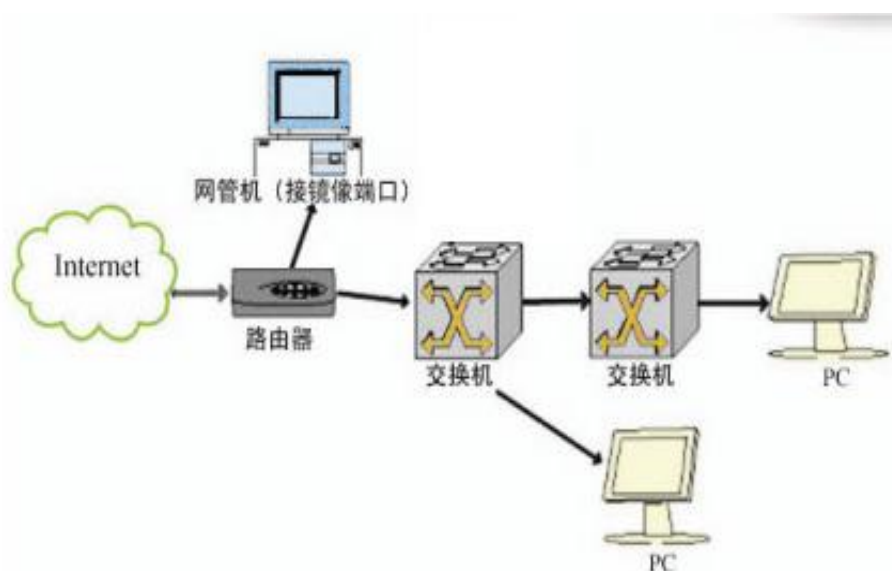
Windows 版本上网行为管理系统目前分为旁路监听、双网卡模式、网桥模式三种模式，目前使用最普遍的为旁路监听模式。

1、旁路监听有三个方案

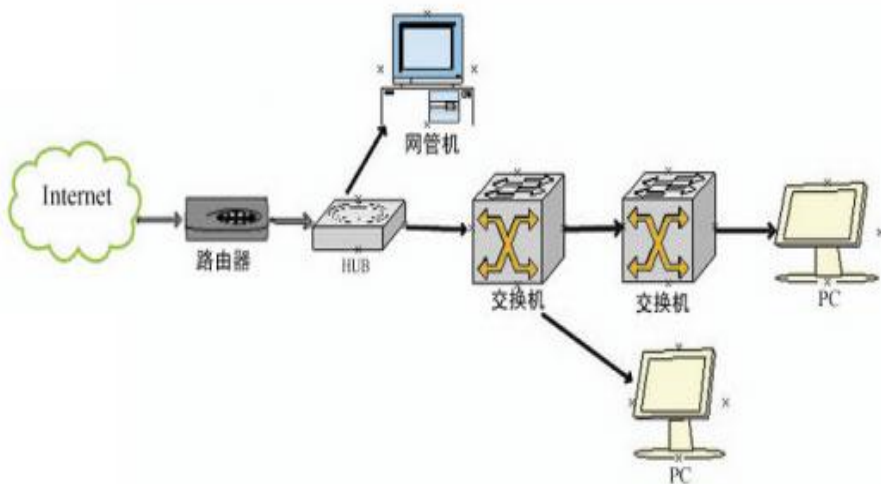
方案一：路由器+镜像交换机，镜像交换机下支持多个交换机的使用。支持多个交换使用。



方案二：带镜像端口的路由器，镜像交路由器下支持多个交换机的使用。



方案三：带 HUB 的连接方式。（注：此方式适用于机器数量少且带宽窄的情况，如机器多数据量大的话会严重影响网速）



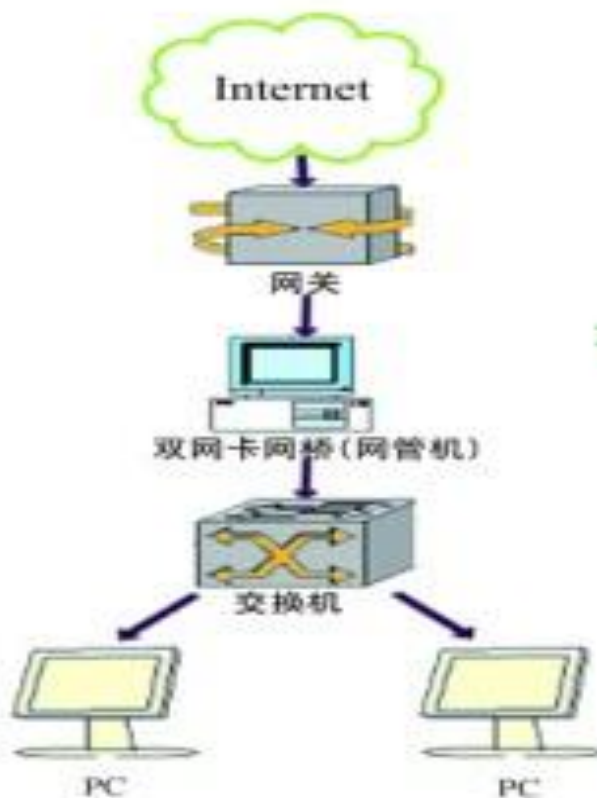
2、双网卡代理

双网卡代理服务，此方案在机器多的情况下影响网速。



3、网桥模式

网桥模式，该部署模式一般不需要改变其网络环境和原有设备的配置。



六．快速设置

本系统安装完毕后，做以下设置后，即可进行正常监控。

6.1.基本设置>监听设置



搜索监控网卡，勾选，并点击保存配置，根据实际的结构进行选择监控模式，然后再点击重启监控按钮。

6.2.基本设置>IP 网段设置



如果是多网段上网模式，在这里必须添加需要监控的网段，才能监控和控制该网段内的机器，否则将无法监控。

6.3.资源搜索>监控组



网路神警上网行为管理系统

欢迎您: admin 监控状态: 监控服务正在运行.....

您现在的位置: 资源搜索

页次: 1 / 3页 共有 26记录, 每页 13 条 第 1 页

序号	终端名称	计算机IP	计算机MAC	所属分组	操作
1	192.168.1.12	192.168.1.12	9028345D0C96	临时组	删除 修改终端名称
2	192.168.1.24	192.168.1.24	000C29636942	临时组	删除 修改终端名称
3	192.168.1.31	192.168.1.31	94DE806C31E4	临时组	删除 修改终端名称
4	192.168.1.33	192.168.1.39	94DE806C3208	临时组	删除 修改终端名称
5	192.168.1.42	192.168.1.41	902834BD1293	临时组	删除 修改终端名称
6	192.168.1.42	192.168.1.42	000C293F8FE8	临时组	删除 修改终端名称
7	192.168.1.44	192.168.1.44	902834061762	临时组	删除 修改终端名称
8	192.168.1.46	192.168.1.46	000C29F0882B	临时组	删除 修改终端名称
9	hh	192.168.1.56	00E062014611	hh分组	删除 修改终端名称
10	192.168.1.67	192.168.1.67	000C296DFEC1	临时组	删除 修改终端名称
11	192.168.1.69	192.168.1.69	10F48C87CDB	临时组	删除 修改终端名称
12	192.168.1.96	192.168.1.96	9028340B7C2C	临时组	删除 修改终端名称
13	192.168.1.103	192.168.1.103	ACE21589408F	临时组	删除 修改终端名称

本机网卡: VDevice\NPF_{2E6FE557-5B0B-4EE8-8F08-C570FB8AFA40} 按照IP排序 批量配置计算机

☒ 自动搜索 ☐ 手动搜索 起始IP: 截止IP: 搜索 手动添加 保存配置

对新搜索出的计算机进行分组操作，默认只有一个监控组，把计算机放到默认组中。



网路神警上网行为管理系统

欢迎您: admin 监控状态: 监控服务正在运行.....

您现在的位置: 资源搜索

页次: 1 / 3页 共有 26记录, 每页 13 条 第 1 页

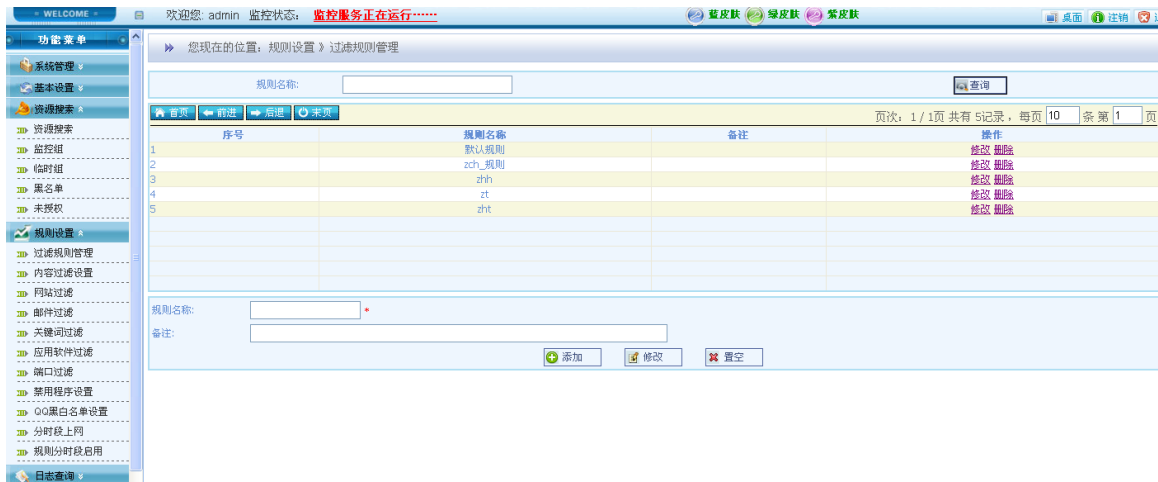
序号	终端名称	计算机IP	计算机MAC	所属分组	操作
1	192.168.1.12	192.168.1.12	9028345D0C96	临时组	删除 修改终端名称
2	192.168.1.24	192.168.1.24	000C29636942	临时组	删除 修改终端名称
3	192.168.1.31	192.168.1.31	94DE806C31E4	临时组	删除 修改终端名称
4	192.168.1.33	192.168.1.39	94DE806C3208	临时组	删除 修改终端名称
5	192.168.1.42	192.168.1.41	902834BD1293	临时组	删除 修改终端名称
6	192.168.1.42	192.168.1.42	000C293F8FE8	临时组	删除 修改终端名称
7	192.168.1.44	192.168.1.44	902834061762	临时组	删除 修改终端名称
8	192.168.1.46	192.168.1.46	000C29F0882B	临时组	删除 修改终端名称
9	hh	192.168.1.56	00E062014611	hh分组	删除 修改终端名称
10	192.168.1.67	192.168.1.67	000C296DFEC1	临时组	删除 修改终端名称
11	192.168.1.69	192.168.1.69	10F48C87CDB	临时组	删除 修改终端名称
12	192.168.1.96	192.168.1.96	9028340B7C2C	临时组	删除 修改终端名称
13	192.168.1.103	192.168.1.103	ACE21589408F	临时组	删除 修改终端名称

本机网卡: VDevice\NPF_{2E6FE557-5B0B-4EE8-8F08-C570FB8AFA40} 按照IP排序 批量配置计算机

☒ 自动搜索 ☐ 手动搜索 起始IP: 截止IP: 搜索 手动添加 保存配置

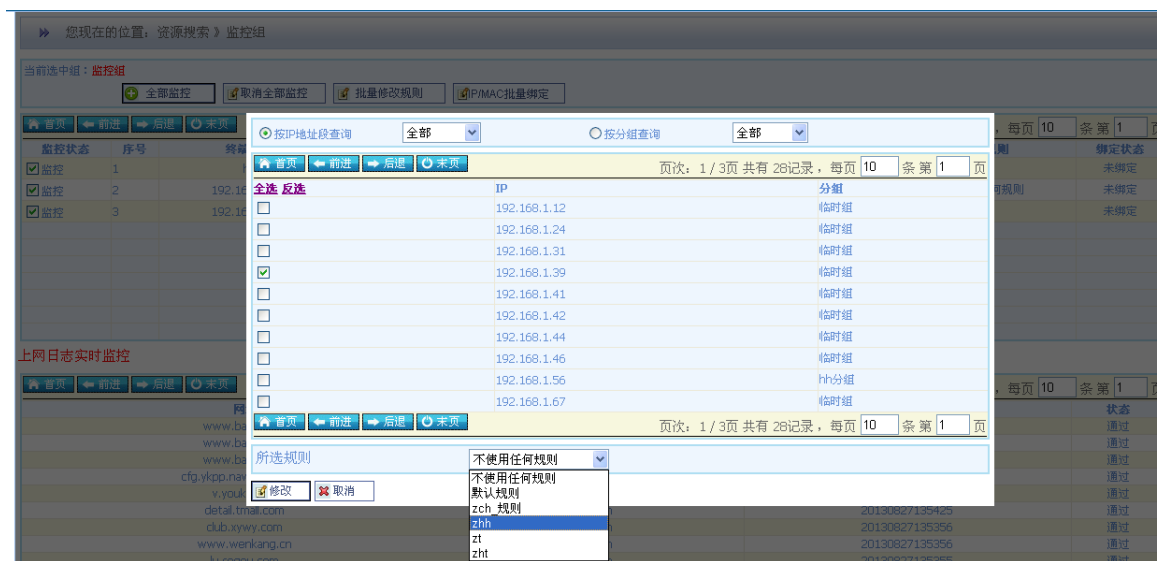
使用分组: 临时组 (selected), 黑名单, 默认分组, zch_分组, hh_分组

6.4 规则设置>过滤规则管理



根据实际需求，编辑监控规则。对不需要的功能可以不用设置。

6.5 资源搜索>监控组>批量修改规则



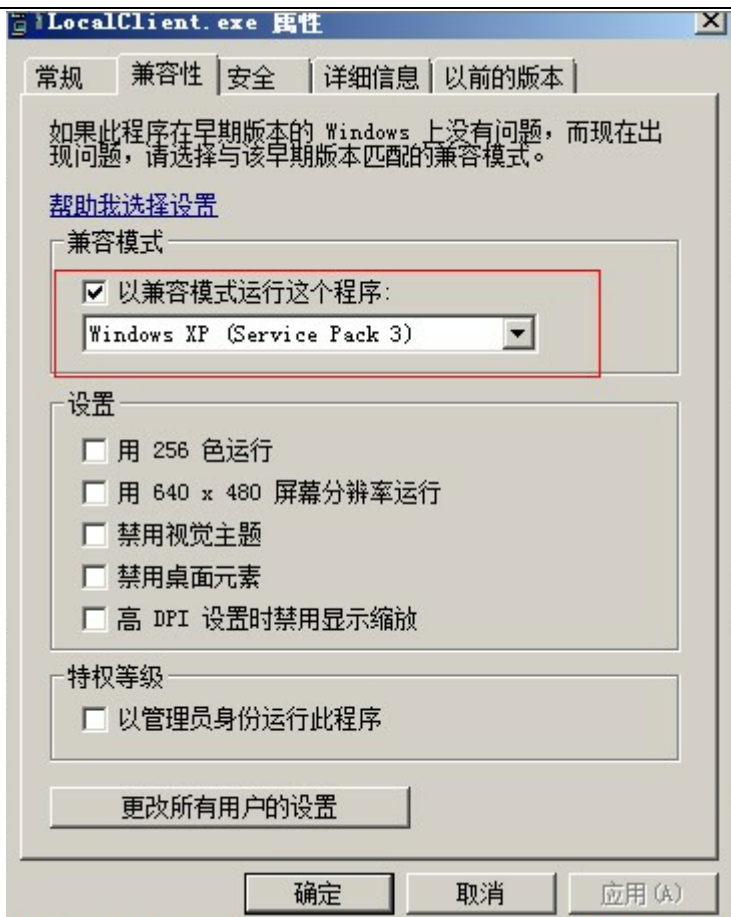
设置单个计算机或分组的监控规则，然后点击修改，给监控组设置过滤规则完毕。

经过以上 6 步设置后，即可进行正常监控。

6.6 注意事项

在 Windows server 2008 以上，需要开启文件的兼容模式。





通过以上的描述，大家应该对本软件有个一感性的认识，希望该文档能在一定程度上帮助大家了解软件的基本功能，如果需要了解具体的安装,请查看安装手册。