

---

# Sino SDP5.0

## 系统管理员操作手册

---

北京华夏威科软件技术有限公司

修订记录:

版本	更改内容	更改者	日期
1.1	新增钉钉行为审计，企业微信审计，效率分析新增效率饱和度。敏感数据保护页面优化改进，优化元数据检索，泄密行为检索方式为树形检索，打印文件内容页面调整。	俞学强	2022/4/26

---

## 目录

一 系统简介 .....	9
二 登录配置 SinoSDP 审计系统（平台） .....	10
2.1 登录 .....	10
2.2 许可证 .....	11
2.3 ES 存储配置 .....	12
2.4 角色管理 .....	14
2.4.1 新建角色 .....	14
2.4.2 角色查询 .....	14
2.4.3 角色删除 .....	15
2.5 管理员 .....	15
2.5.1 新建管理员 .....	15
2.5.2 删除管理员 .....	16
2.5.3 免密登录 .....	17
2.6 组织 .....	17
2.6.1 新建组织 .....	17
2.6.2 删除组织 .....	18
2.7 域配置 .....	19
2.7.1 新建域配置 .....	19
2.7.2 删除域配置 .....	20
2.8 邮箱配置 .....	20
2.9 登录配置 .....	21
2.10 其它配置 .....	22
2.11 更多配置 .....	22
2.11.1 客户端通知配置 .....	22
2.11.2 S3 配置 .....	23
2.12 管理员日志 .....	24
2.13 概览 .....	24
2.13.1 center 概览 .....	24
2.13.2 server 概览 .....	25

---

2.13.3 统计 server 概览 .....	26
2.13.4 es 概览 .....	27
2.14 es 监控 .....	27
2.15 es 迁移 .....	29
2.15.2 es 数据迁移 .....	30
2.15.3 系统日志 .....	30
2.16 应用服务器 .....	31
2.16.1 编辑应用服务器 .....	31
2.16.2 删除应用服务器 .....	34
2.16.3 关机，重启应用服务器 .....	34
2.17 统计服务器 .....	35
2.17.1 统计服务器升级下载 .....	36
2.17.2 插件管理 .....	36
2.17.3 新建插件 .....	36
2.17.4 手动执行 .....	37
2.18 终端 .....	38
2.18.1 终端列表 .....	38
2.18.2 编辑终端 .....	38
2.18.3 绑定组织 .....	39
2.18.4 启用禁用 .....	39
2.18.5 删除终端 .....	40
2.18.6 卸载终端 .....	40
2.18.7 终端明细 .....	41
2.18.8 告警配置 .....	45
2.18.9 导入关系配置 .....	45
2.18.10 导出终端 .....	46
2.18.11 标记静态 ID .....	46
2.18.12 离线许可释放 .....	47
2.18.13 批量升级 .....	47
2.18.14 联软配置 .....	48

---

2.18.15 关联 .....	48
2.18.16 自定义列 .....	48
2.19 终端升级 .....	49
2.20 Linux 终端升级 .....	50
2.20.1 安装包下载 .....	51
2.21 终端组 .....	51
2.21.1 终端组列表 .....	51
2.21.2 新建终端组 .....	52
2.21.3 编辑终端组 .....	52
2.21.4 删除终端组 .....	53
2.21.5 绑定终端 .....	53
2.22 记录策略列表 .....	54
2.22.1 新建 Windows 记录策略 .....	54
2.22.2 编辑 Windows 记录策略 .....	60
2.22.3 删除 Windows 记录策略 .....	60
2.22.4 复制 Windows 记录策略 .....	61
2.23 Windows 安全策略 .....	61
2.23.1 Windows 安全策略列表 .....	61
2.23.2 新建 Windows 安全策略 .....	62
2.23.3 编辑 Windows 安全策略 .....	65
2.23.4 删除 Windows 安全策略 .....	65
2.23.5 复制 Windows 安全策略 .....	66
2.24 Linux 记录策略 .....	66
2.24.1 Linux 记录策略列表 .....	66
2.24.2 新建 Linux 记录策略 .....	67
2.24.3 复制 Linux 记录策略 .....	67
2.25 Linux 安全策略 .....	68
2.25.1 Linux 安全策略列表 .....	68
2.25.2 新建 Linux 安全策略 .....	68
2.25.3 复制 Linux 安全策略 .....	69

---

2.26 部门 .....	69
2.26.1 新建部门 .....	70
2.26.2 删除部门 .....	70
2.26.3 编辑部门 .....	71
2.27 用户管理 .....	71
2.27.1 新建用户 .....	71
2.27.2 导出用户 .....	72
2.27.3 导入用户 .....	73
2.27.4 定时同步配置 .....	73
2.27.5 批量操作用户 .....	74
2.27.6 同步域用户 .....	74
2.28 用户组 .....	75
2.28.1 新建用户组 .....	75
2.28.2 用户组绑定关系 .....	76
2.29 用户域 .....	77
2.29.1 新建或导入域组 .....	77
2.29.2 同步域用户数据 .....	78
2.30 二次认证用户 .....	79
2.30.1 新建二次认证用户 .....	79
2.31 控制台升级 .....	79
2.32.1 定时任务列表 .....	80
2.31.1 定时任务启动 .....	80
2.32 正则列表 .....	81
2.32.1 新增正则列表 .....	81
三 敏感，风险，工作效率 .....	82
3.1 风险分析 .....	82
3.1.1 数据集 .....	82
3.1.2 新建数据集 .....	83
3.1.3 导入数据集 .....	83
3.1.4 规则类型 .....	83

---

3.1.5 新建规则类型 .....	84
3.1.6 编辑规则类型 .....	84
3.1.7 删 除 规则类型 .....	85
3.1.8 风险规则 .....	85
3.1.9 风险规则查询 .....	85
3.1.10 新建风险规则 .....	86
3.1.11 编辑风险规则 .....	88
3.1.12 删 除 风险规则 .....	88
3.1.13 风险激活 .....	89
3.1.14 关闭风险 .....	89
3.1.15 风险明细 .....	90
3.1.16 风险分析 .....	90
3.2 敏感信息 .....	92
3.2.1 信息分类配置 .....	92
3.2.2 新建信息分类 .....	92
3.2.3 信息分类配置编辑 .....	94
3.2.4 新建信息分类规则 .....	95
3.2.5 禁用/启用信息分类规则 .....	97
3.2.6 泄密等级配置 .....	97
3.2.7 泄密白名单配置 .....	98
3.2.8 泄密白名单导入/导出 .....	99
3.2.9 终端泄密记录策略 .....	99
3.2.10 文件备份 es 配置 .....	100
3.2.11 泄密行为 .....	101
3.2.12 外发文件内容 .....	101
3.2.13 打印文件内容 .....	102
3.2.14 元数据检索 .....	103
3.2.15 风险用户 .....	104
3.2.16 信息分类 .....	105
3.2.17 硬盘外拷 .....	107

---

3.2.18 打印文件 .....	107
3.2.19 文件外发 .....	108
3.2.20 隐匿外发 .....	109
3.2.22 屏幕浏览 .....	110
3.2.23 聊天外发 .....	110
3.2.24 分析总览 .....	111
3.2.25 敏感指标 .....	112
3.2.26 敏感图表 .....	113
3.2.27 敏感报表 .....	114
3.3 工作效率 .....	115
3.3.1 效率分类 .....	115
3.3.2 新建效率分类 .....	116
3.3.3 删除效率分类 .....	118
3.3.4 编辑效率分类 .....	118
3.3.5 工作时间配置 .....	118
3.3.6 新建工作时间配置 .....	119
3.3.7 编辑工作时间配置 .....	120
3.3.8 删除工作时间配置 .....	120
3.3.9 评分配置 .....	120
3.3.10 工作补时 .....	121
3.3.11 新建工作补时 .....	122
3.3.12 重新计算 .....	122
3.2.13 删除工作补时 .....	123
3.3.14 饱和度配置 .....	123
3.3.15 效率检索明细 .....	124
3.3.16 部门分析 .....	126
3.3.17 用户效率 .....	126
3.3.18 分析总览 .....	127
3.3.19 效率统计明细 .....	128
3.3.20 效率明细汇总 .....	128

---

4 行为审计 .....	130
4.1 主页（行为总览） .....	130
4.1.1 主页详情 .....	130
4.2 会话检索 .....	131
4.2.1 会话查询 .....	131
4.2.2 会话播放 .....	132
4.2.3 会话明细 .....	133
4.2.4 导出数据 .....	134
4.2.5 视频下载 .....	135
4.3 行为数据 .....	135
4.3.1 行为数据查询 .....	135
4.3.2 行为数据播放 .....	136
4.3.3 行为数据明细 .....	137
4.3.4 快捷新建风险规则 .....	138
4.3.5 行为数据收藏 .....	138
4.3.6 导出数据 .....	139
4.4 应用记录 .....	140
4.5 上网活动 .....	140
4.6 剪切板 .....	141
4.7 文件操作 .....	142
4.8 移动设备 .....	142
4.9 远程运维 .....	143
4.10 数据库 .....	143
4.11 QQ 记录 .....	144
4.12 邮件记录 .....	145
4.13 微信记录 .....	145
4.14 操作标签 .....	146
4.15 POST 报文 .....	146
4.15.1 增加表单解析规则 .....	147
4.16 Linux 记录 .....	148

---

4.17 文件外发 .....	148
4.18 打印行为 .....	149
4.19 钉钉记录 .....	150
4.20 企业微信记录 .....	150
4.21 报表--指标 .....	151
4.21.1 新建指标 .....	151
4.21.2 删除指标 .....	152
4.21.3 新建图表 .....	152
4.21.4 新建报表 .....	153
4.21.5 excel 报表 .....	155
4.21.6html 报表 .....	155
4.21.7 发送报表 .....	155
4.21.8 仪表盘 .....	156
4.21.9 报告规则 .....	158
4.21.10 生成报告 .....	159
4.21.11 报告 .....	160
4.21.12 报告下载 .....	160
4.22 表单解析规则 .....	162

## 一 系统简介

首先确保 SinoSDP 应用服务器正确安装，并且购买了相应的授权；客户端正确安装，并且将授权分配给相应的客户端。

当用户登录安装客户端的计算机登陆系统后，所有的操作行为都将被记录，SinoSDP 审计系统管理员可以自定义策略，指定记录的详细程度。这些记录详细程度的，yua\_会以文件流方式存储在 Elasticsearch 中。管理员可以在需要时播放会话，查看用户的操作，生成报

表等。SinoSDP 使用文件流功能，加快了审计记录的存取操作。本手册将描述这些功能的使用与配置。

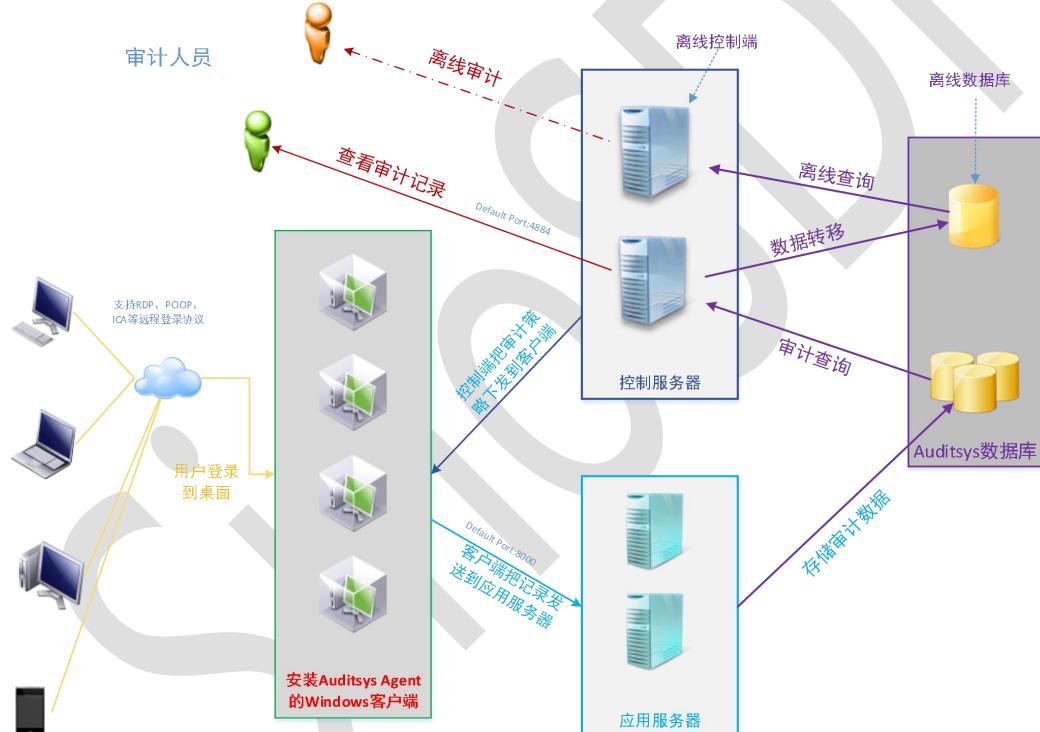
SinoSDP 审计系统由以下 4 个部分构成：

客户端：安装在需要被审计的 Windows、Linux 计算机上，当有用户登录并进行操作时，产生审计记录并发送到应用服务器。

应用服务器：接收来自客户端的审计数据，并将元数据以文件流方式存储到 Elasticsearch 中。

控制服务器：对 SinoSDP 审计进行控制，例如分配授权、设置审计策略等。

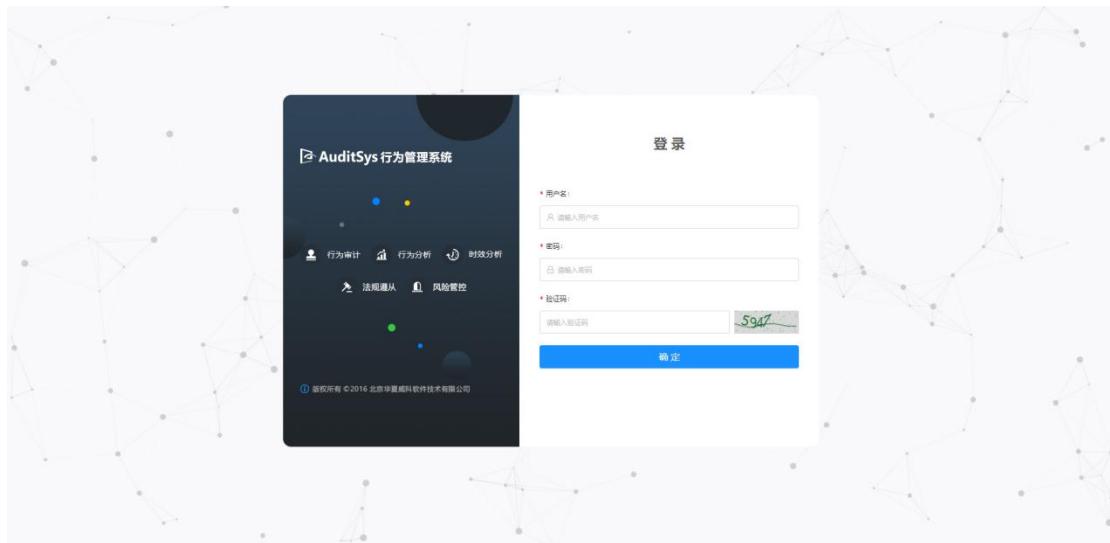
Elasticsearch 服务器集群：用于存储审计记录。



## 二 登录配置 SinoSDP 审计系统（平台）

### 2.1 登录

SinoSDP 控制服务器默认会使用 Web 界面进行管理。通过此 Web 界面，可以完成 SinoSDP 所有操作。默认情况下，使用 TCP 端口 80。使用默认 TCP80 端口时，使用以下 URL 登录到 SinoSDP 控制服务器的管理控制台：<https://<控制服务器 IP 或域名>>，如下图所示：



首次打开 SinoSDP 审计管理控制台，默认用户名：`admin` 密码：`changeme` 验证码随机生成。此账户是默认超级管理员，**此账户无法禁用、无法删除。超级管理员首次登录后，请及时修改密码。**

SinoSDP 首次运行打开，超级管理员第一次登录，进入软件授权界面。**如果没有授权码，请联系技术客服部，申请软件授权码。**

## 2.2 许可证

许可证路径：平台/系统/许可证，许可证主要是控制控制台的使用权限。没有配置许可证，只会显示许可证模块。

点击新增许可配置许可，可以添加多个许可；许可过期，相应许可数会自动减去已过期的许可数。

设备ID	总需求数	已使用	总需求数	已使用	总需求数	已使用
800705010A10355A4A0A7E0D0233E11C1	25	19	10	1	5	1
<a href="#">+ 新增许可</a>						
测试许可	无效	16	2	2	2022-01-13	<a href="#">许可证号</a>
正式许可	无效	5	2	2	2022-01-13	<a href="#">许可证号</a>
测试许可	有效	25	10	5	2022-02-13	<a href="#">许可证号</a>

注：已经使用许可数可以超申请许可数的 10%。（如申请的许可数是 100 台，实际可以使用 110 台）

申请的许可可以对行为风险监控，应用访问控制，敏感信息，工作效率分析进行权限管理。

The screenshot shows a user interface for managing permissions. The main menu includes '行为审计' (Behavior Audit), '敏感信息' (Sensitive Information), '风险分析' (Risk Analysis), '工作效率' (Work Efficiency), '权限' (Permissions), and '告警' (Alerts). The 'Permissions' tab is active. On the left, there's a sidebar with '监控' (Monitoring), '组织' (Organization), '基础配置' (Basic Configuration), '服务器' (Server), '系统配置' (System Configuration), '管理员' (Administrator), '角色管理' (Role Management), and '权限' (Permissions). The '权限' section is expanded, showing '普通通行许可证数' (Number of General Permission Licenses) as 25, '已使用' (Used) as 19, '总普通通行许可证数' (Total Number of General Permission Licenses) as 10, '已使用' (Used) as 1, '总高级服务器许可证数' (Total Number of Advanced Server Licenses) as 5, and '已使用' (Used) as 1. Below this, there are three rows of permission details:

许可类型	许可状态	线程	服务器	截至时间	许可证号	查看权限	操作
测试许可	无效	16	2	2022-01-13	8D49-C383-DD19-1744-3C10-F155-EFC5-5776- D019-1237-0C93-6651-4280-B3E0-CDF8-0990- 3F03-8316-0C9C-17C3-0986-8719-C821-7983		
正式许可	无效	5	2	2022-01-13	8D49-AB4B-AB3D-FE1A-0111-F777-AE33-BC17- 9126-8C04-B117-E516-998A-0098-9E77-C46B- 20E2-CA04-1647-C2B5-5A33-7177-0131-0148		
测试许可	有效	25	10	2022-02-13	8D49-3941-174D-0001-0002-0003-0004-0005- E88E-9E14-0006-0007-C0A4-0008-0009-000A- 9F13-0040-4701-0398-0022-48E3-8197-31A8		

## 2.3 ES 存储配置

ES 配置用来连接配置 Elasticsearch 服务器，Elasticsearch 服务器是用来接收应用服务器写入的元数据，日志数据等。

选择“系统>es 配置” 配置存储地址格式为 `http://`。（只有配置成功 ES 服务并启动，界面才能正常显示数据）如下图所示：

The screenshot shows the 'es 配置' (Elasticsearch Configuration) page. The left sidebar includes '行为审计' (Behavior Audit), '敏感信息' (Sensitive Information), '风险分析' (Risk Analysis), '工作效率' (Work Efficiency), '权限' (Permissions), and 'es 配置' (Elasticsearch Configuration). The 'es 配置' section is active. It contains the following configuration fields:

集群名称	值
集群名称	my-application
Elasticsearch 地址	http://192.168.1.73:9200
是否启用用户名密码	<input type="checkbox"/>
元数据写入时间间隔	00:00-23:59
元数据与恶意数据保留时间	100
监控数据保留时间	101
日志数据保留时间	100
风险数据保留时间	50
故障数据保留时间	50
工作效率数据保留时间	50
累计报告数据保留时间	10
会话类数据保留时间	10

集群名称：填写 ES 配置文件所配置的集群名称。

Elasticsearch 地址：格式为“`http://Elasticsearch 地址:Elasticsearch 端口`”。如果 Elasticsearch 是集群，地址之间用英文‘,’分隔。Elasticsearch 端口默认为 9200 端口。例如：`http://*.*.*:端口`,`http:// *.*.*:端口`,`http:// *.*.*:端口`。

是否启用用户名密码：默认不启用；如果 ES 配置了用户密码，需要勾选启用，输入正确的

---

用户名与密码。

元数据写入时间段：只有配置的时间段应用服务器才会写入数据到 ES，控制台才有数据展示。

元数据与录屏数据保留时间：保留视频数据和元数据的天数，过期自动删除；对应的索引信息也会被删除（元数据索引信息 meta-metadata 录屏数据索引信息 meta-session）

监控数据保留时间：保留对后台服务器组件监控数据的天数，过期自动删除；对应的索引信息也会被删除（监控数据索引信息 em-commonitor）

日志数据保留时间：保留系统日志的天数，过期自动删除。过期自动删除；对应的索引信息也会被删除（日志数据索引信息 auditsyslog）

风险数据保留时间：保留风险行为数据的天数，过期自动删除；对应的索引信息也会被删除（风险、敏感词索引信息 meta-infract）

按键数据保留时间：保留按键行为数据的天数，过期自动删除；对应的索引信息也会被删除（按键索引信息 meta-click）

工作效率数据保留时间：保留工作效率数据的天数，过期自动删除；对应的索引信息也会被删除（按键索引信息 meta-efficiency）

审计报告数据保留时间：保留审计报告数据的天数，过期自动删除；对应的索引信息不会删除，只会删除索引内过期的数据（审计报告索引信息 auditsys\_report）

会话集数据保留时间：保留会话集数据的天数，过期自动删除；对应的索引信息不会删除，只会删除索引内过期的数据（会话集索引信息 auditsys\_record）

客户端关键事件保留时间：保留终端的关键事件数据的天数，过期自动删除；对应的索引信息也会被删除（关键事件索引信息 auditsys\_event）

Sdp 元数据保留时间：保留终端产生的文本，文件在敏感渠道中产生的元数据，也就是在行为敏感检索中的数据。

敏感数据保留时间：保留终端用户产生的敏感数据，用户产生的敏感数据保留在终端敏感信息检索模块。

文件清单数据保留时间：外发文件产生的记录，所有数据展示在文件外发检索页面，超过保留时间后所有文件的外发用户数，外发次数，隐匿次数，时间全部体现为 0.

(注：以上保留时间的时间单位是‘天’；会多保留一天的数据；超过已保留时间的数据会被自动清除)

第一次配置 ES，需要点击“初始化模板”按钮进行初始化。

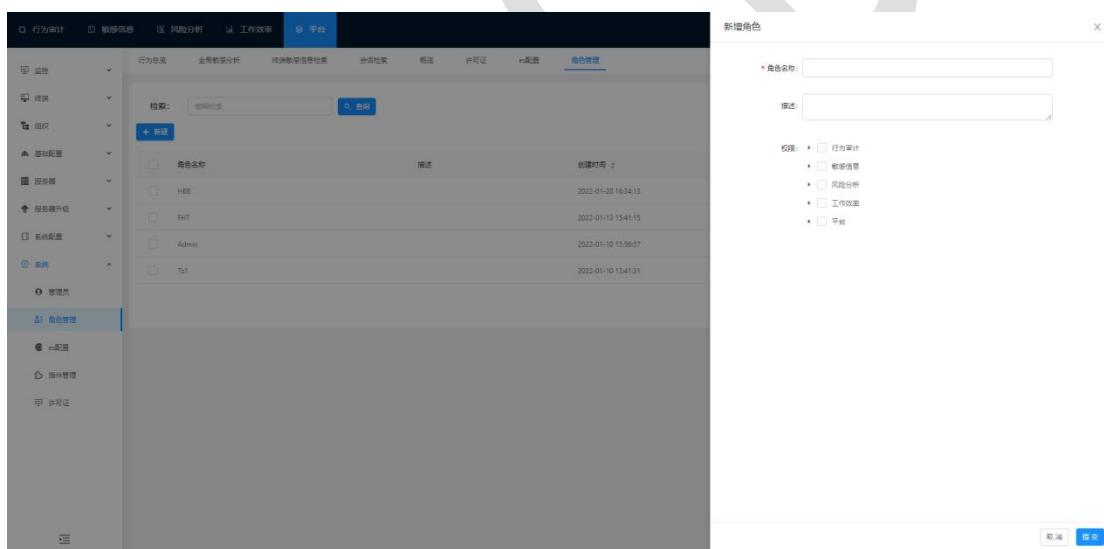
## 2.4 角色管理

角色主要是用来控制管理员菜单权限。

### 2.4.1 新建角色

选择“平台>系统>角色”。点击“新建”按钮新建新的角色。

在“角色名称”处输入角色名称（必填），在“权限”处勾选角色的权限（权限默认有主页权限，并且不可以移除主页的权限）。如下图所示：

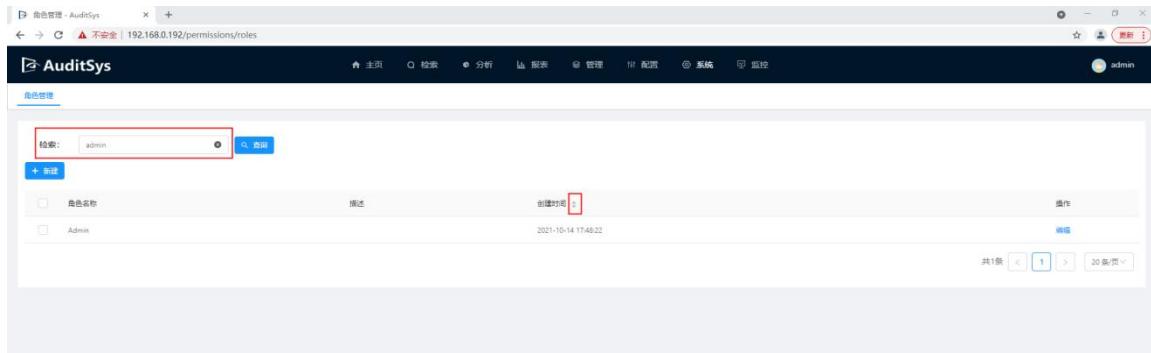


点击“提交”保存角色，成功则退回到角色列表界面，失败则有提示失败原因。

点击“取消”则不保存角色，直接退回到角色列表界面。

### 2.4.2 角色查询

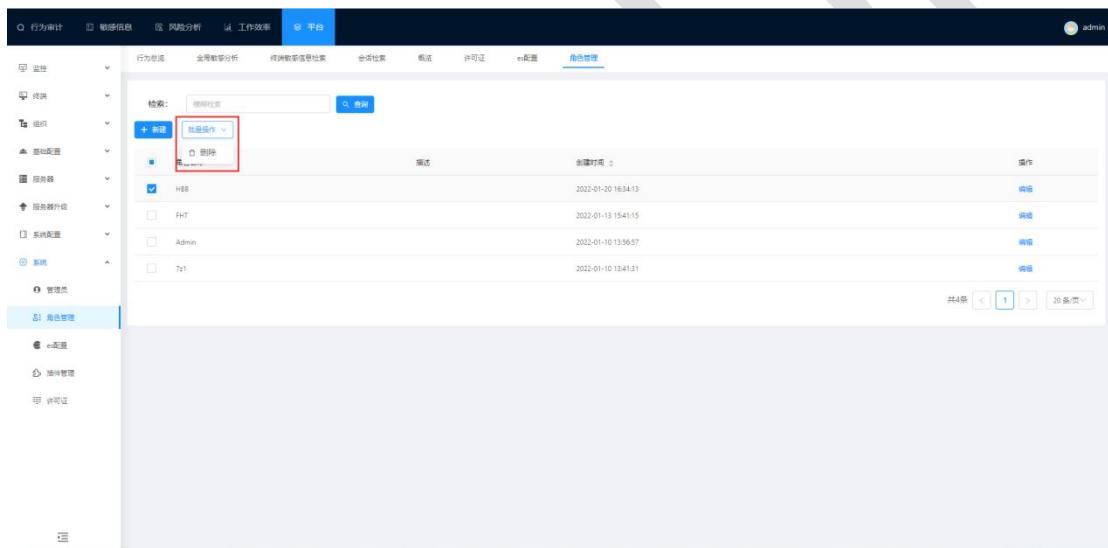
在检索处输入角色信息，检索角色。也可以点击字段名的列排序。**提示：只有字段名三**角形图案的才能排序。如下图所示：



## 2.4.3 角色删除

先勾选要删除的角色，然后点击删除按钮，再点击确定。如下图所示：

注：删除已绑定管理的角色，会提示先解除绑定管理员。



## 2.5 管理员

不同权限的管理员登录控制台查看的数据不一样。

### 2.5.1 新建管理员

选择“平台>系统>管理员”。点击“新建”按钮新增新的管理员。

(系统默认有 admin 超级管理员，超级管理员不可以删除和修改)

状态：启用，则可以登录控制台；禁用，则不可以登录控制台。

可以添加本地管理员和域管理员两种管理员：

本地管理员选择“系统”；域管理员选择“域账号”（**域管理员需先配置域配置，请查看**

## 2.7 相关操作）

角色：可以控制管理员对导航栏模块访问的权限。

组织：管理员访问控制台只能查看已绑定组织的数据审计。

用户组：管理员访问控制台只能查看已绑定用户组的数据审计。

部门：管理员访问控制台只能查看已绑定部门的数据审计。

用户域组：管理员访问控制台只能查看已绑定用户域组的数据审计。

**（注：以上多条件逻辑：用户组和用户域组是‘或’的关系；其它都是‘且’的关系）**

期限时间：超过设置的期限时间，则管理员不可再登录控制台。

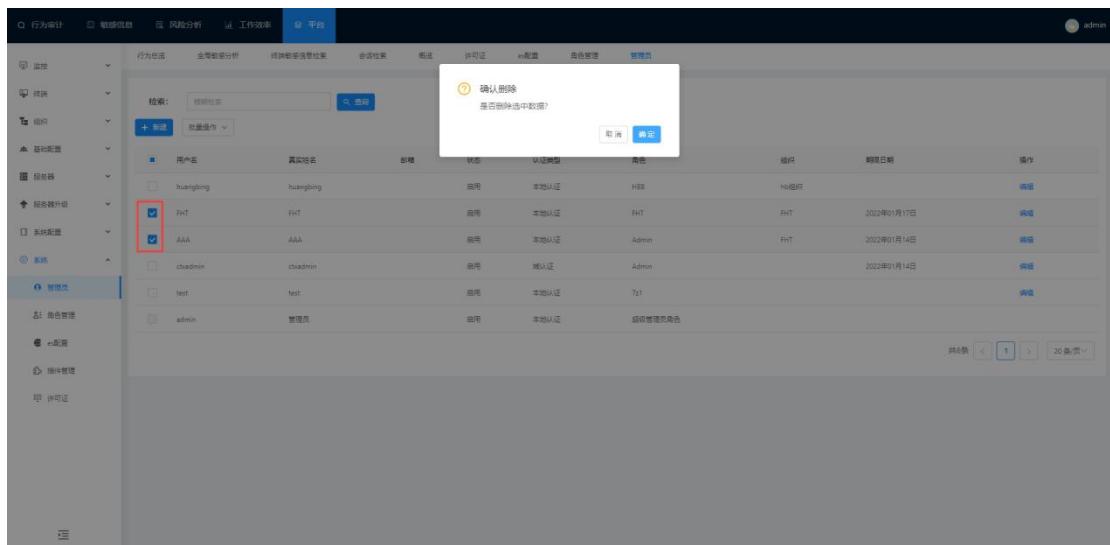
Secretkey：点击‘生成’按钮，可以生成 secretkey 值；免密登录需要使用到 secretkey 值；

**（注：只有登录控制台成功过的本地管理员才能生成 secretkey 值；域管理员不支持）**

## 2.5.2 删除管理员

先勾选要删除的管理员，然后点击删除按钮，再点击确定（超级管理员不可选中删除）

如下图所示：



## 2.5.3 免密登录

使用本地管理员生成的 secretkey 值+模块链接进行访问。如下图所示：

打开浏览器，在地址栏输入免密登录链接：

<https://192.168.1.71/permissions/users?ztoken=ZnpoQXVkaXRzeXMyMDIxMTYzMjNDgwMzI5N>

A==

规则	发生时间	风险终端名称/IP	部门/用户姓名	风险终端:登录IP	操作类型	风险名称	风险类型	操作
规则类型	2022-01-21 09:40:49	WIN10-JB	射手 卢西安	WIN10-JB:fht	文件操作	删除或者修改的文件或者目录	破坏性质的行为	
风险名称		192.168.0.254						
用户名								
终端地址								
终端名称								

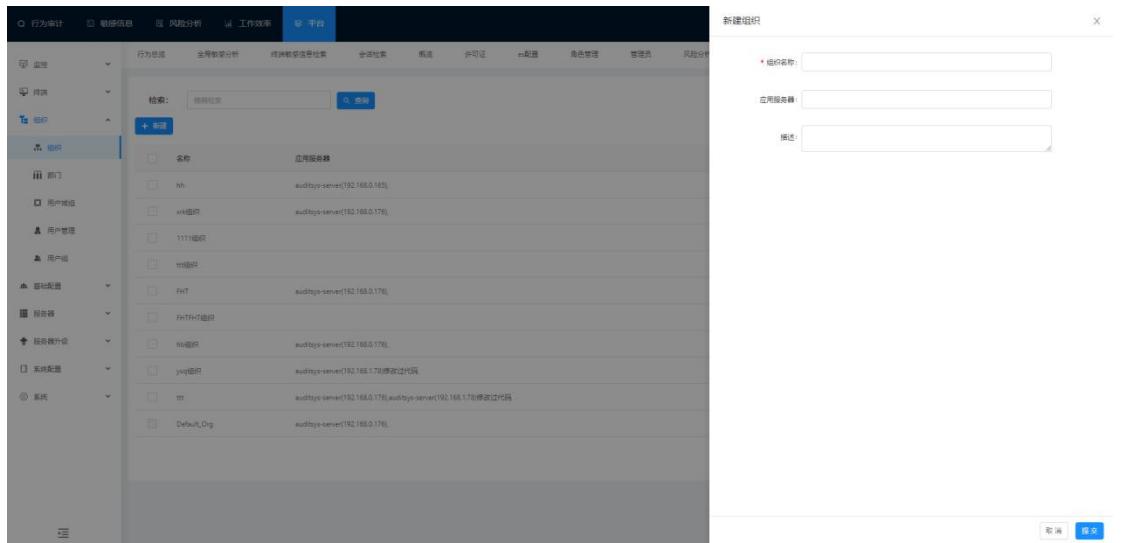
<https://192.168.1.71/permissions/users>: 是想访问的模块地址。

ztoken=本地管理员生成的 secretkey 值。

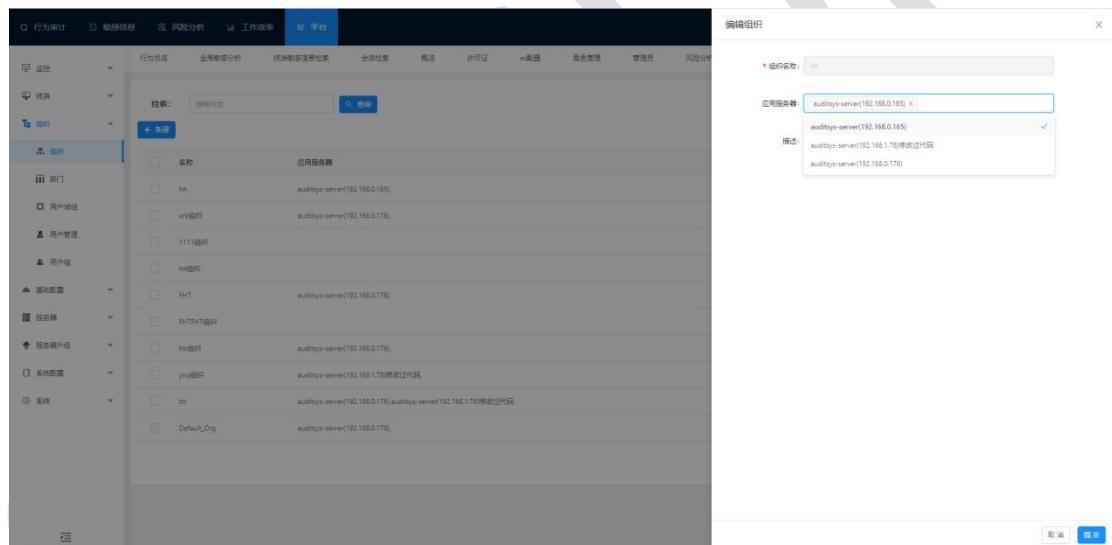
## 2.6 组织

### 2.6.1 新建组织

选择“平台>组织>组织”。点击“新建”按钮新建新的组织。（系统默认有默认组织且无法删除）



在“组织名称”处输入组织名称（必填）；在“应用服务器”下拉框选择要绑定服务器（可以选择多个服务器绑定；组织跟应用服务器是可以双向绑定）如下图所示：

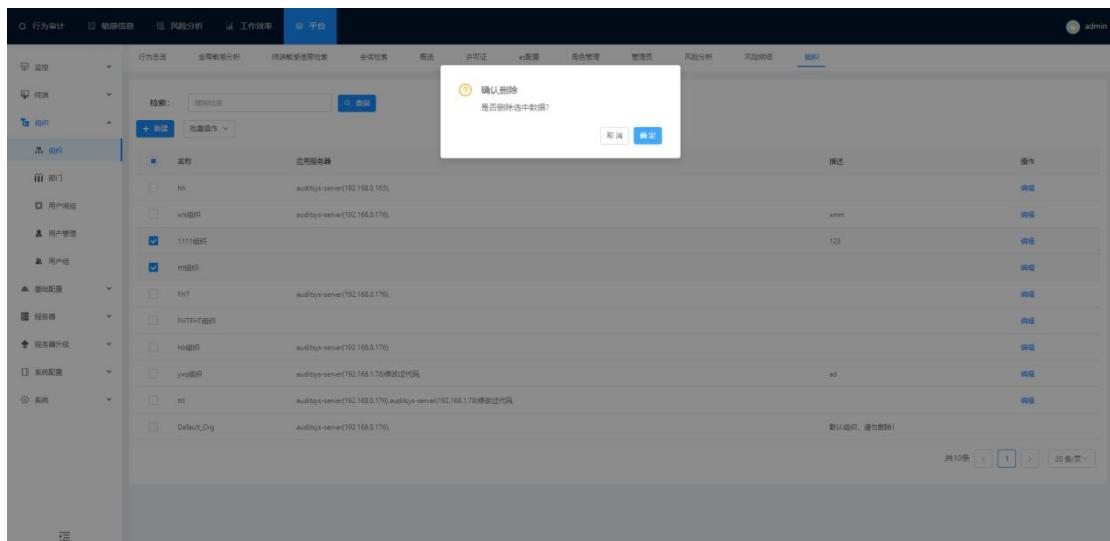


提示：新建的组织，终端组列表同时会自动生成一个对应终端组。

## 2.6.2 删除组织

删除组织时，请确认组织没有被管理员、终端组、服务器、终端、二次认证用户引用；被引用的组织在删除前要解除。

先勾选要删除的组织，然后点击删除按钮，在点击确定。如下图所示：

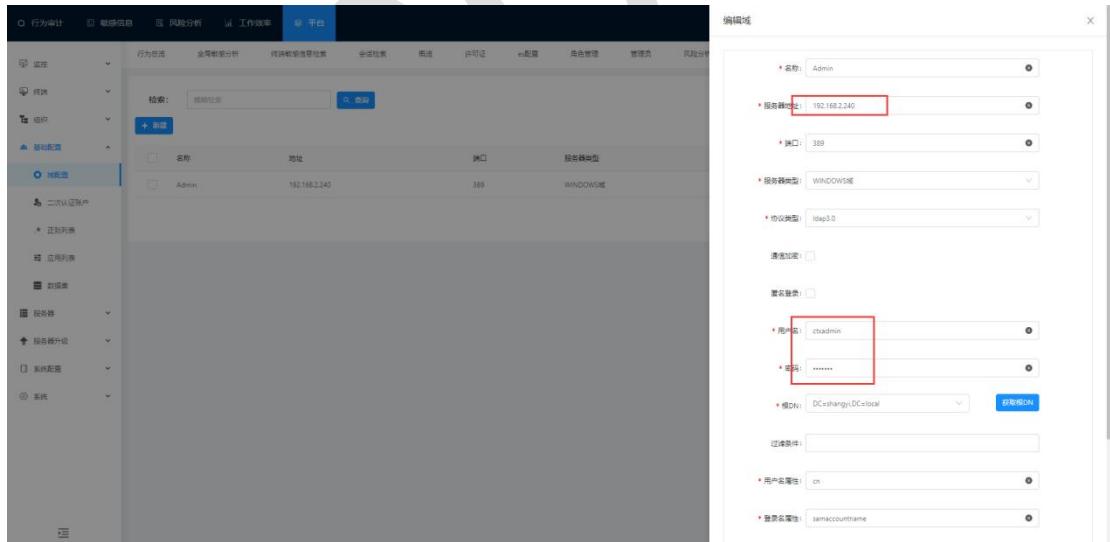


## 2.7 域配置

配置域配置才能使用该域环境内的域用户，用户域组，域管理员账户，二次认证域用户。

### 2.7.1 新建域配置

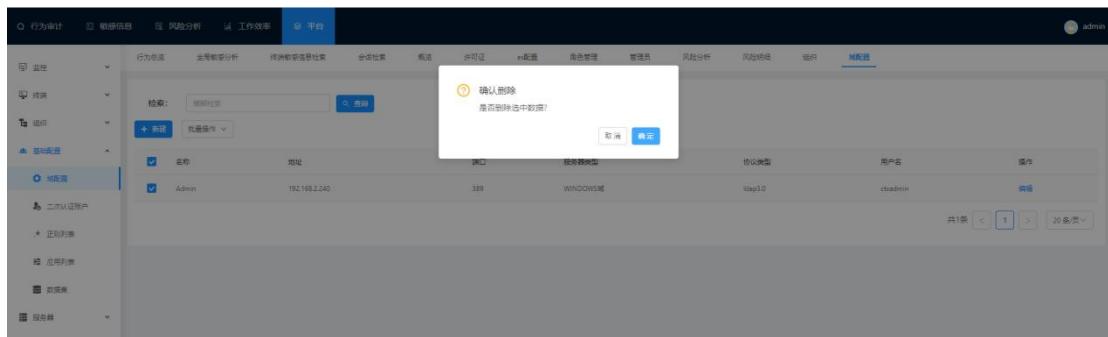
选择“平台>基础配置>域配置”，点击“新建”按钮新建新的域配置。如下图所示：



配置域配置前，需要把域服务器启动；填写正确的域服务器地址，用户名，密码，才能获取根 DN，域配置才能生效。

## 2.7.2 删除域配置

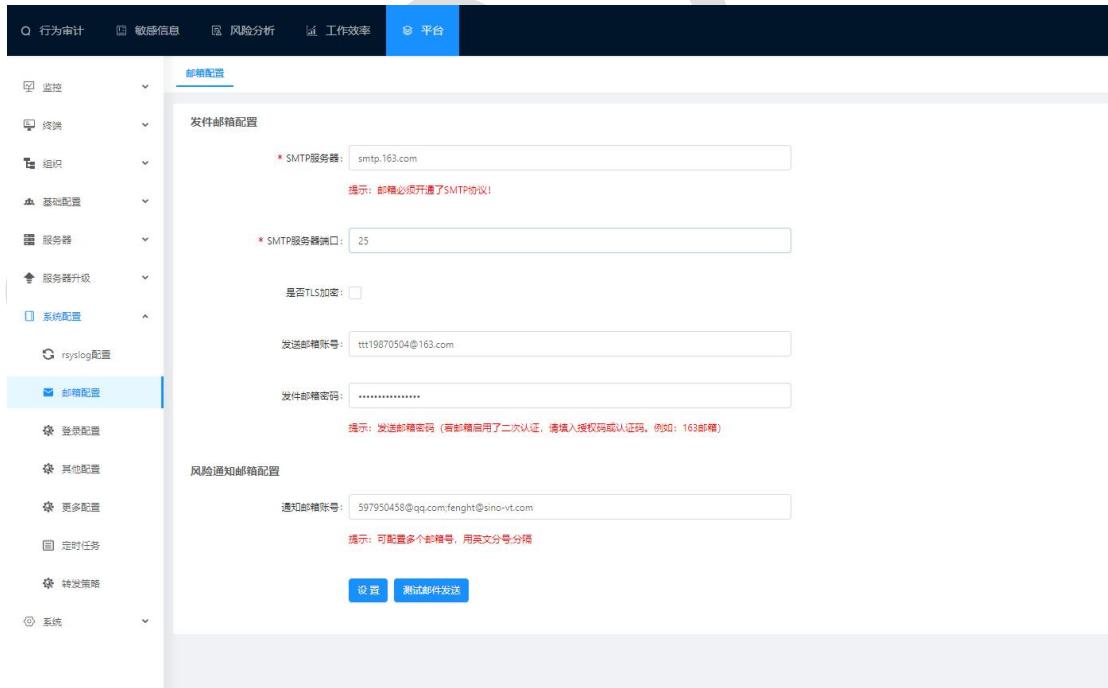
先勾选要删除的域配置（删除被引用的域配置，需要先解除），然后点击“删除”按钮，再“点击”确定。如下图所示：



## 2.8 邮箱配置

配置邮件通知，离线告警、终端告警、agent 自检告警、报表才能接收邮件通知。

选择“平台>系统配置>邮件配置” 配置邮件通知。如下图所示：

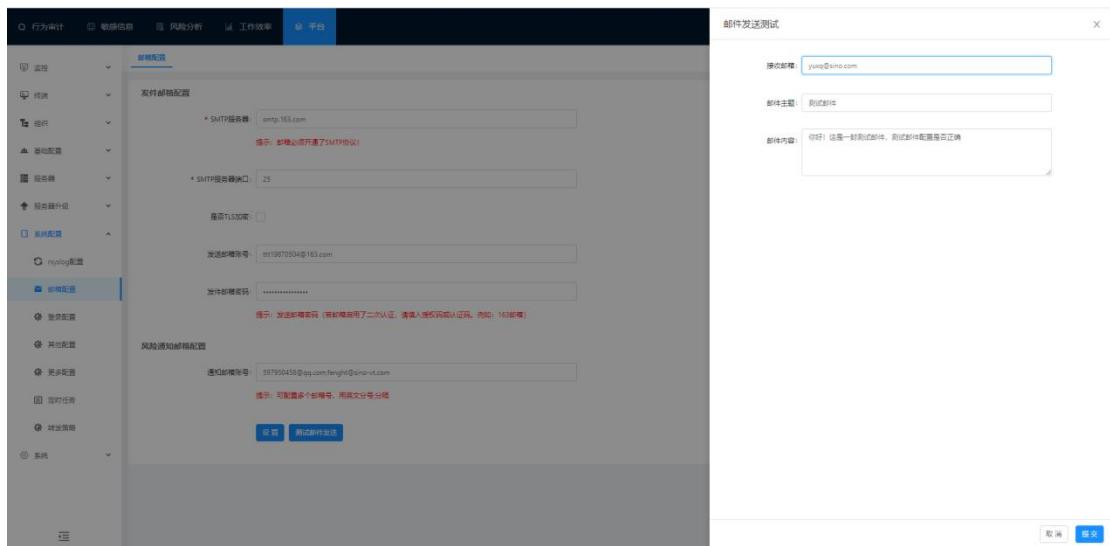


SMTP 服务器： 邮箱必须开通了 SMTP 协议。

SMTP 端口： SMTP 协议的端口默认为 25。

是否 TLS 加密： 必须勾选才能接收到邮件通知。

测试邮件通知配置是否正确，可以点击测试邮件发送。如下图所示：



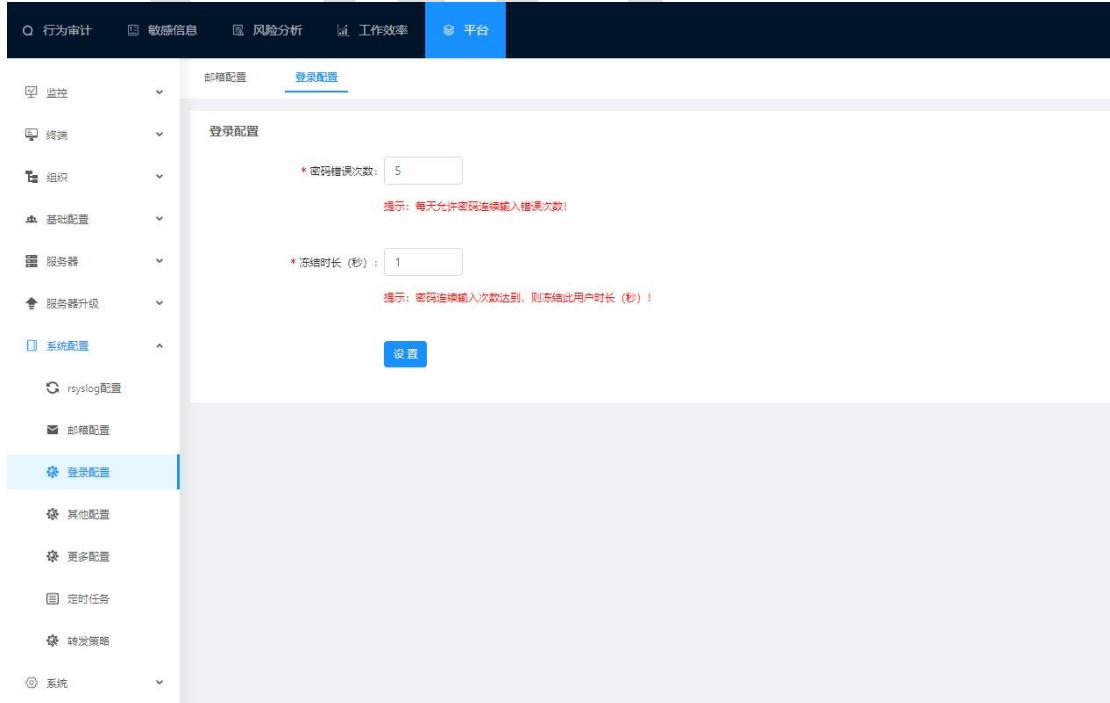
输入接收邮箱，点击“发送”按钮。查看接收邮箱是否有收到邮件。如有接收到邮件，则配置成功。否则则配置失败。

成功则点击“设置”保存邮件通知配置。

## 2.9 登录配置

登录设置：配置输入密码错误次数，输错次数后该管理员账户被冻结的时长。

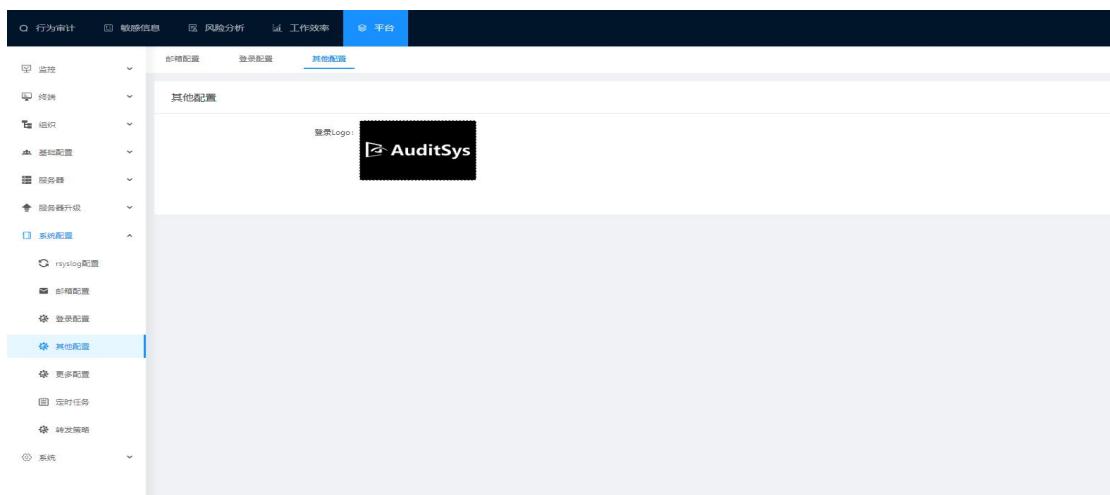
点击“平台>系统配置>登录配置”进入登录设置界面，如下图所示：



## 2.10 其它配置

其它配置：点击图片可以更换登录 LOGO

点击“平台>系统配置>其它配置”进入其它配置界面，如下图所示：



## 2.11 更多配置

### 2.11.1 客户端通知配置

客户端通知配置：配置风险行为、敏感词行为弹框通知内容和客户端弹框录入用户数据。

选择“平台>更多配置>客户端弹框配置”进入客户端弹框配置界面；如下图所示：

The screenshot shows the Magent platform's configuration interface. The top navigation bar includes tabs for 'Behavior Audit', 'Sensitive Information', 'Risk Analysis', 'Work Efficiency', and 'Platform'. The 'Platform' tab is active. On the left, a sidebar lists various configuration categories: Monitoring, Terminal, Organization, Basic Configuration, Server, Server Upgrade, System Configuration, and More Configuration. 'More Configuration' is currently selected. The main content area is titled 'Client Alert Configuration' and contains several configuration sections:

- Client Alert Frequency**: A field labeled 'Alert Frequency (seconds)' with a value of '10'. A note states: 'Clients will only receive one alert per frequency time range, even if multiple types of alerts trigger.' Below this is a note: 'Clients will only receive one alert per frequency time range, even if multiple types of alerts trigger.'
- Sensitive Word Alert Content**: A text input field containing 'This is my sensitive word: gaojing'. A note below it says: 'Clients will receive a pop-up message after triggering a sensitive word alert.'
- Risk Alert Content**: A text input field containing 'This is my risk alert'. A note below it says: 'Clients will receive a pop-up message after triggering a risk alert.'
- Client Alert User Input**: A checkbox labeled 'Client alert user input' is checked. A note below it says: 'Clients will receive a pop-up message after triggering a risk alert.'
- Client Alert Message Text**: A text input field containing 'Huawei Magent'.

A blue 'Save' button is located at the bottom right of the configuration panel.

弹框频率：用户触发风险或敏感词每 10 秒弹框通知一次。

敏感词告警弹框内容：自定义通知的敏感词内容。

风险告警弹框内容：自定义通知的风险内容。

客户端弹框录入用户数据：勾选，则没有绑定用户信息的终端 Magent 重启就会弹出用户信息输入窗口。

## 2.11.2 S3 配置

s3 配置用于配置 s3 服务器地址。点击平台>系统配置>更多配置>s3 配置，配置解释如图所示：

**S3配置**

\* s3备份服务器类型: 备份到本地部署的s3服务minio → **s3服务器类型**

\* s3备份服务器地址和端口: 192.168.0.216:9000 → **s3服务器地址 (此处为本地搭建的s3服务器)**

\* s3备份服务器用户 AccessKey: minicadmin → **用户名**

\* s3备份服务器用户 SecretKey: minicadmin → **密码**

s3备份服务器bucket的region:

\* 视频bucket名称: moviefile → **视频文件名上传的视屏文件将保存在此文件夹中**

\* 文件bucket名称: filetest → **上传的文件将保存在此文件夹中**

**设置**

## 2.12 管理员日志

管理员日志: 记录登录 center 的管理员的操作详情。

点击“平台>监控>管理员日志”进入管理员日志界面, 如下图所示:

发生时间	登录账号	登录IP	参数内容
2022-01-21 10:28:27		192.168.3.150	登录: /api/base/login
2022-01-21 10:28:27	admin	192.168.3.150	首页-列表: /api/home/getList, 参数: {"datatype":"last_one_day","endtime":"","order":"","starttime":"","types":"lasttime"}
2022-01-21 10:28:12		192.168.3.150	获取验证码: /api/base/captcha
2022-01-21 10:29:37	admin	192.168.3.133	会话列表: /api/session/sessionList, 参数: {"datatype":"to_day","page":1,"pageSize":20,"types":"lasttime"}
2022-01-21 10:29:37	admin	192.168.3.133	会话地图: /api/session/sessionList, 参数: {"condition":[{"field":"agentip","join":"must","where":1,"term":1,"term":1,"value":192.168.3.133,"current":1,"size":1}]}>行为数据列表: /api/session/metaList, 参数: {"condition":[{"field":"agentip","join":"must","where":1,"term":1,"term":1,"value":192.168.3.133,"current":1,"size":1}]}>行为数据列表: /api/session/metaList, 参数: {"condition":[{"field":"agentip","join":"must","where":1,"term":1,"term":1,"value":192.168.3.133,"current":1,"size":1}]}>行为数据列表: /api/session/metaList, 参数: {"condition":[{"field":"agentip","join":"must","where":1,"term":1,"term":1,"value":192.168.3.133,"current":1,"size":1}]}>会话次数配置: /api/loginConfig/getLoginConfig
2022-01-21 10:29:37	admin	192.168.3.133	会话地图: /api/session/sessionList, 参数: {"datatype":"to_day","page":1,"pageSize":20,"types":"lasttime"}
2022-01-21 10:24:17	admin	192.168.3.133	会话地图: /api/session/sessionList, 参数: {"condition":[{"field":"agentip","join":"must","where":1,"term":1,"term":1,"value":192.168.3.133,"current":1,"size":1}]}>行为数据列表: /api/session/metaList, 参数: {"condition":[{"field":"agentip","join":"must","where":1,"term":1,"term":1,"value":192.168.3.133,"current":1,"size":1}]}>行为数据列表: /api/session/metaList, 参数: {"condition":[{"field":"agentip","join":"must","where":1,"term":1,"term":1,"value":192.168.3.133,"current":1,"size":1}]}>会话次数配置: /api/loginConfig/getLoginConfig
2022-01-21 10:24:17	admin	192.168.3.133	会话地图: /api/session/sessionList, 参数: {"condition":[{"field":"agentip","join":"must","where":1,"term":1,"term":1,"value":192.168.3.133,"current":1,"size":1}]}>行为数据列表: /api/session/metaList, 参数: {"condition":[{"field":"agentip","join":"must","where":1,"term":1,"term":1,"value":192.168.3.133,"current":1,"size":1}]}>行为数据列表: /api/session/metaList, 参数: {"condition":[{"field":"agentip","join":"must","where":1,"term":1,"term":1,"value":192.168.3.133,"current":1,"size":1}]}>会话次数配置: /api/loginConfig/getLoginConfig
2022-01-21 10:24:17	admin	192.168.3.133	会话地图: /api/session/sessionList, 参数: {"condition":[{"field":"agentip","join":"must","where":1,"term":1,"term":1,"value":192.168.3.133,"current":1,"size":1}]}>行为数据列表: /api/session/metaList, 参数: {"condition":[{"field":"agentip","join":"must","where":1,"term":1,"term":1,"value":192.168.3.133,"current":1,"size":1}]}>行为数据列表: /api/session/metaList, 参数: {"condition":[{"field":"agentip","join":"must","where":1,"term":1,"term":1,"value":192.168.3.133,"current":1,"size":1}]}>会话次数配置: /api/loginConfig/getLoginConfig
2022-01-21 10:24:17	admin	192.168.3.133	会话地图: /api/session/sessionList, 参数: {"condition":[{"field":"agentip","join":"must","where":1,"term":1,"term":1,"value":192.168.3.133,"current":1,"size":1}]}>行为数据列表: /api/session/metaList, 参数: {"condition":[{"field":"agentip","join":"must","where":1,"term":1,"term":1,"value":192.168.3.133,"current":1,"size":1}]}>行为数据列表: /api/session/metaList, 参数: {"condition":[{"field":"agentip","join":"must","where":1,"term":1,"term":1,"value":192.168.3.133,"current":1,"size":1}]}>会话次数配置: /api/loginConfig/getLoginConfig

## 2.13 概览

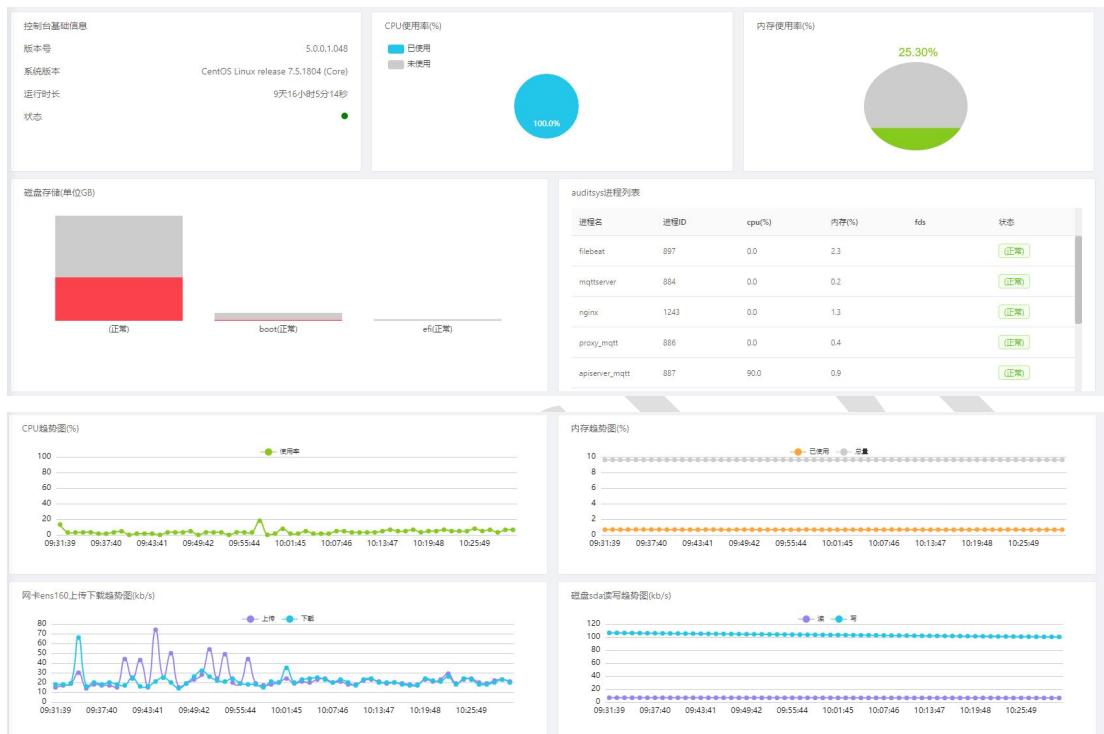
### 2.13.1 center 概览

Center 概览: 对 center 服务器的系统状态和性能使用情况实时更新记录。

选择“平台>监控>概览”，查看 Center 服务器的系统状态和性能。如下图所示:



可以点击“查看详情”按钮查看 center 服务器的系统状态详细情况；如下图所示：



## 2.13.2 server 概览

Server 概览：对 Server 服务器的系统状态和性能使用情况实时更新记录。

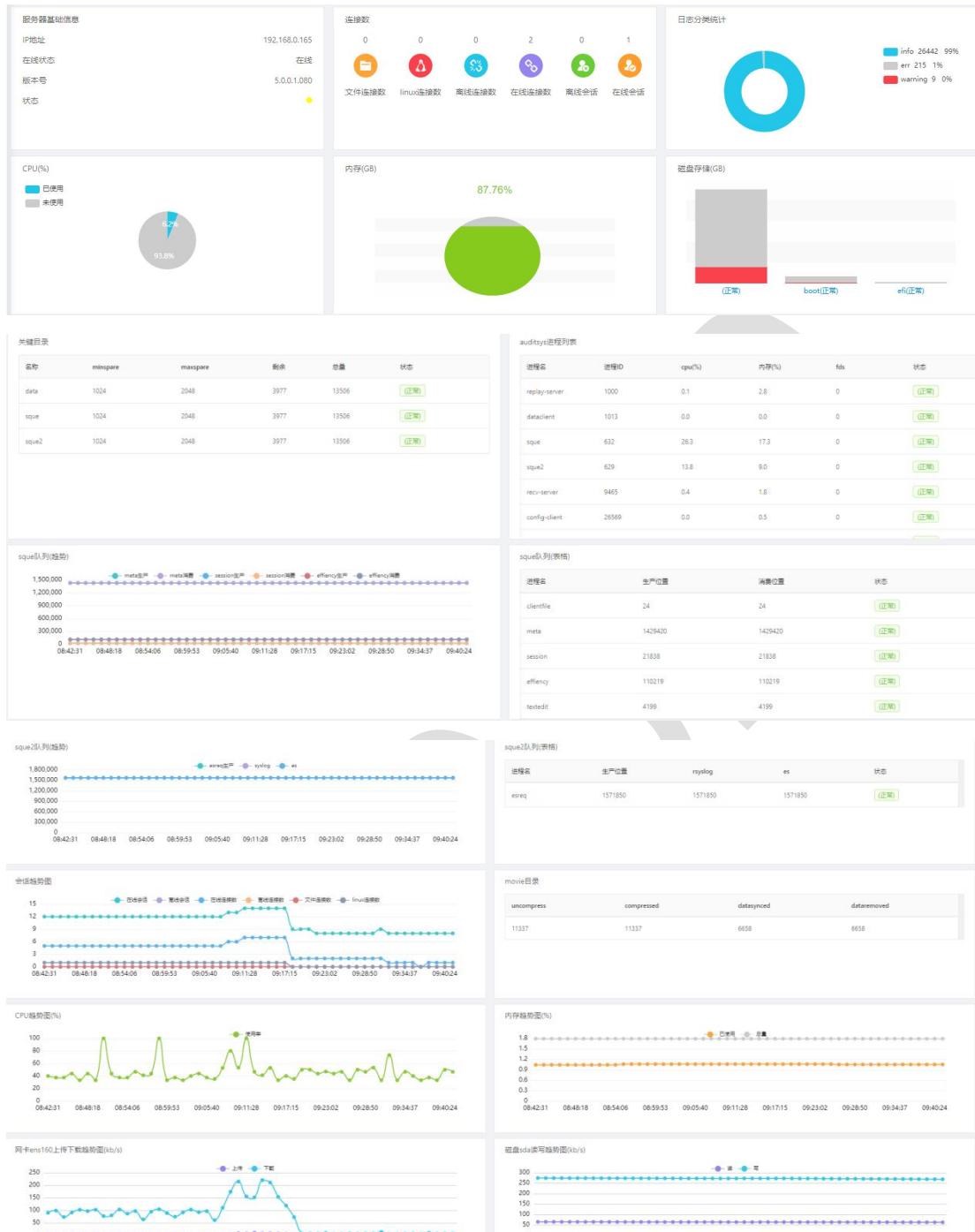
选择“平台>监控>概览”，查看 Server 服务器的系统状态和性能。如下图所示：



多个 server 服务器，可以点击下拉框按钮切换服务器查看详情。



可以点击“查看详情”按钮查看 server 服务器的系统状态详细情况；如下图所示：



### 2.13.3 统计 server 概览

**统计 Server 概览：**对统计 Server 服务器的系统状态和性能使用情况实时更新记录。

统计 Server 概览步骤请参照 9.3server 概览的步骤查看详情。

## 2.13.4es 概览

ES 概览：对 ES 服务器的系统状态和性能使用情况实时更新记录。

选择“平台>监控”，查看 ES 服务器的系统状态和性能。如下图所示：

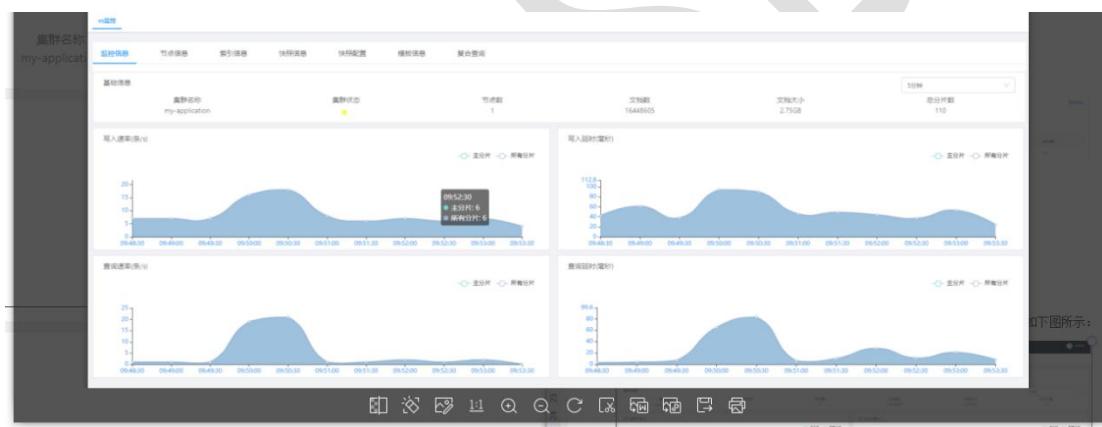
The screenshot shows the 'ElasticSearch' monitoring page. At the top, it displays the cluster name 'my-application', cluster status (green), and document count (16447936). Below this, a table provides detailed information for the single node 'node-1': IP (192.168.0.113), version (7.8.1), available disk space (4.3gb), JVM usage (40%), memory usage (91%), CPU usage (10%), 1-second latency (0.13), 5-second latency (0.17), and 15-second latency (0.14).

## 2.14es 监控

ES 监控：对 ES 服务器的系统状态和性能使用情况实时更新记录。

选择“平台>监控>es 监控”，查看 ES 服务器的系统状态和性能。

监控信息：监控 es 集群每秒写入速率，写入延时，查询速率，查询延时；如下图所示：



节点信息：记录 ES 集群节点的运行系统状态和性能实时更新；如下图所示：

The screenshot shows the '平台' (Platform) section of the interface. Under the 'es 监控' (es Monitoring) tab, the '节点信息' (Node Info) sub-tab is selected. It displays a table with node details: node type (主节点), node name (node-1), IP (192.168.1.73), version (7.8.1), available disk space (10gb), memory usage (70%), CPU usage (13%), 1-second latency (0.11), 5-second latency (0.17), and 15-second latency (0.15).

### 2.14.1 快照配置

快照配置：快照仓库的配置（相当于索引信息备份的仓库）如下图所示：

The screenshot shows the AuditSys platform's monitoring interface. The top navigation bar has tabs for '行为审计', '敏感信息', '风险分析', '工作效率', and '平台'. The 'es监控' tab is selected. On the left, there's a sidebar with sections like '监控' (Monitoring), 'es迁移' (es Migration), '管理员日志' (Administrator Log), '系统日志' (System Log), '终端' (Terminal), '组织' (Organization), '基础配置' (Basic Configuration), '服务器' (Server), '服务器升级' (Server Upgrade), '系统配置' (System Configuration), and '系统' (System). The main content area is titled '快照配置' (Snapshot Configuration). It contains a note: '快照配置 (配置前, 先确定elasticsearch.yml文件是否配置快照存储位置, 如果未配置请勿配置)' (Before configuration, make sure the elasticsearch.yml file has configured the snapshot storage location, do not configure if not configured). Below it is a warning: '提示: 创建共享目录, 创建完成后对目录进行chmod 777 授予最高权限, 否则无法写入' (Tip: Create a shared directory, after creation, change the directory permissions to chmod 777 to grant maximum permission, otherwise it cannot be written to). A note follows: '共享文件系统仓库 ("type": "fs") 使用共享文件系统存快照, 如果要注册共享文件系统仓库, 必须在所有master和data节点挂载相同的共享文件系统到同一个路径位置, 这个路径位置 (或者它的父目录) 必须在所有master和data节点的path.repo设置上注册. 假设共享文件系统挂载到 /data/backups/, 应该在elasticsearch.yml文件中添加如下配置: path.repo: ["/data/backups"]' (Shared file system repository ("type": "fs") stores snapshots using a shared file system. If you want to register a shared file system repository, you must mount the same shared file system to the same path on all master and data nodes. This path (or its parent directory) must be registered in the path.repo setting on all master and data nodes. Assuming the shared file system is mounted to /data/backups/, you should add the following configuration to the elasticsearch.yml file: path.repo: ["/data/backups"]). There are input fields for '快照仓库名称' (Snapshot Repository Name) and '快照存储位置' (Snapshot Storage Location), both with placeholder text. At the bottom are '设置' (Set) and '删除' (Delete) buttons.

## 2.13.2 索引信息

快照配置：快照仓库的配置（相当于索引信息备份的仓库）如下图所示：

SS

This screenshot is identical to the one above, showing the '快照配置' (Snapshot Configuration) page in the AuditSys platform. It displays the same configuration fields and notes about shared file system repositories and their registration requirements.

冻结索引：该索引信息不会再写入数据；例如：冻结下图索引信息，则用户在终端的数据行为操作暂时不会写到该索引信息（被操作的数据会丢失）。如下图所示：

The screenshot shows the '索引信息' (Index Information) page under the 'es监控' (es Monitoring) tab. The table lists several indices:

索引名称	状态	文档数	数据	索引延时	搜索延时	分片数	副本数	操作
meta-keyword-2022-1-7	正常	2986	113.3mb	0ms	0ms	1	1	<span style="color: green;">冻结</span>
meta-efficiency-2022-1-7	正常	10272	4.5mb	0ms	0ms	1	1	<span style="color: green;">冻结</span>
meta-ifact-2022-1-16	正常	404	435.2kb	0ms	0ms	1	1	<span style="color: green;">冻结</span>
meta-efficiency-2022-1-8	正常	2882	872.6kb	0ms	0ms	1	1	<span style="color: green;">冻结</span>
meta-efficiency-2022-1-9	正常	2882	879.2kb	0ms	0ms	1	1	<span style="color: green;">冻结</span>
meta-ifact-2022-1-23	正常	7881	907.4kb	0ms	0ms	4	4	<span style="color: green;">冻结</span>

解冻索引：该索引信息继续写入数据；用户在终端操作的行为操作继续写入该索引信息；如

下图所示：

索引名称	状态	文档数	数据	索引延时	延迟延时	分片数	副本数	操作
meta-keyword-2022-1-7	yellow	2966	113.3mb	0ms	0ms	1	1	
meta-efficiency-2022-1-7	yellow	10272	4.5mb	0ms	0ms	1	1	
meta-infract-2021-12-16	yellow	404	435.2kb	0ms	0ms	1	1	
meta-efficiency-2022-1-8	yellow	2862	872.6kb	0ms	0ms	1	1	
meta-auditlog-2022-1-6	green	0	0mb	0ms	0ms	0	0	

创建快照：相当于把该索引信息进行备份到快照仓库；如下图所示：

索引名称	状态	文档数	数据	索引延时	延迟延时	分片数	副本数	操作
meta-keyword-2022-1-7	yellow	2966	113.3mb	0ms	0ms	1	1	
meta-efficiency-2022-1-7	yellow	10272	4.5mb	0ms	0ms	1	1	

删除索引：则该时间段索引对应的用户在终端操作数据都被删除。

注：索引信息对应的操作行为：

元数据索引信息：meta-metadata; 录屏索引信息：meta-session;

系统日志索引信息：auditsyslog; 风险数据索引信息：meta-infract;

效率明细索引信息：meta-efficiency; 按键数据索引信息：meta-click;

概览详情索引信息 auditsys\_sysstate 每 4 天清除一次；

Es 监控信息索引信息：em-commonitor;

终端事件索引信息：auditsys\_event 60 天清理一次；

管理员日志索引信息：auditsys\_manager 永久保存。

## 2.15es 迁移

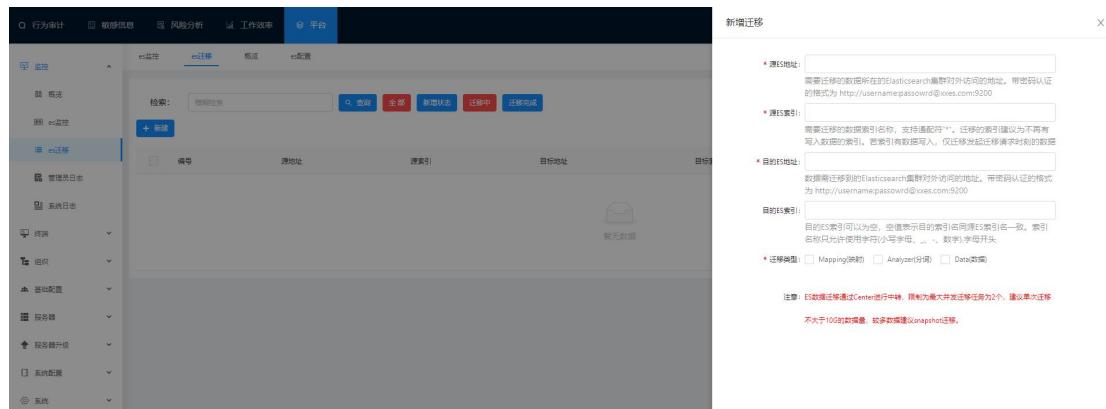
ES 迁移：相当于把 ES 数据迁移备份到另一 ES 服务器。

选择“平台 > 监控 > ES 迁移”进入 ES 迁移界面；如下图所示：

编号	原地址	原索引	目标地址	目标索引	修改时间	状态	操作
1	http://192.168.0.113:9200	meta*-2021-10-27	http://192.168.2.119:9200	meta*	2021-10-28 10:43:06	正常	

## 2.15.1 新建 es 迁移

点击“新建”按钮新建 ES 迁移；如下图所示：



源 ES 地址：输入要迁移的 ES 服务器地址。

源 ES 索引：输入要迁移的 ES 索引数据。

目的 ES 地址：接收迁移的 ES 服务器地址。

源 ES 索引：接收迁移的 ES 索引数据。

## 2.15.2 es 数据迁移

选择要迁移的 ES 数据，点击“迁移”按钮，进行迁移；如下图所示：

The screenshot shows a list of migration tasks. Task 1 (ID 1) has a status of 'Pending' (待迁移) and was modified on 2021-10-28 10:43:06. Task 2 (ID 2) has a status of 'In Progress' (迁移中) and was modified on 2021-11-02 10:33:03. Both tasks have a 'Details' (详情) button.

ID	源地址	源索引	目标地址	目标索引	修改时间	状态	操作
1	http://192.168.0.113:9200	meta-metadata-2021-10-27	http://192.168.2.119:9200	meta-metadata-2021-10-27_0blk	2021-10-28 10:43:06	迁移完成	详情
2	http://192.168.0.113:9200	meta-metadata-2021-10-27	http://192.168.0.178:9200	meta-metadata-2021-10-31_0blk	2021-11-02 10:33:03	迁移中	详情

## 2.15.3 系统日志

系统日志：对 center、服务器的日志实时更新记录。

选择“平台>监控>系统日志”进入系统日志界面；如下图所示：

## 2.16 应用服务器

应用服务器用来接收终端操作所产生的视频数据，元数据，日志数据。

选择“平台>服务器>应用服务器”查看应用服务器信息。如下图所示：

服务器数据：安装了 AuditSys-Server 服务器包后，此服务器的信息则会显示在服务器列表中。

### 2.16.1 编辑应用服务器

点击“编辑”按钮进入编辑界面。如下图所示：

基础配置：

名称：不可修改。

别名：可修改。

接入范围：组织，则可选择一个或多个（组织是控制终端（Agent）绑定的组织范围，该组织下的终端产生的视频数据都存入到此服务器）；选择IP段，则输入一个IP段，在这个IP段的终端产生的审计数据才可以写入此服务器。

服务器映射外网配置：

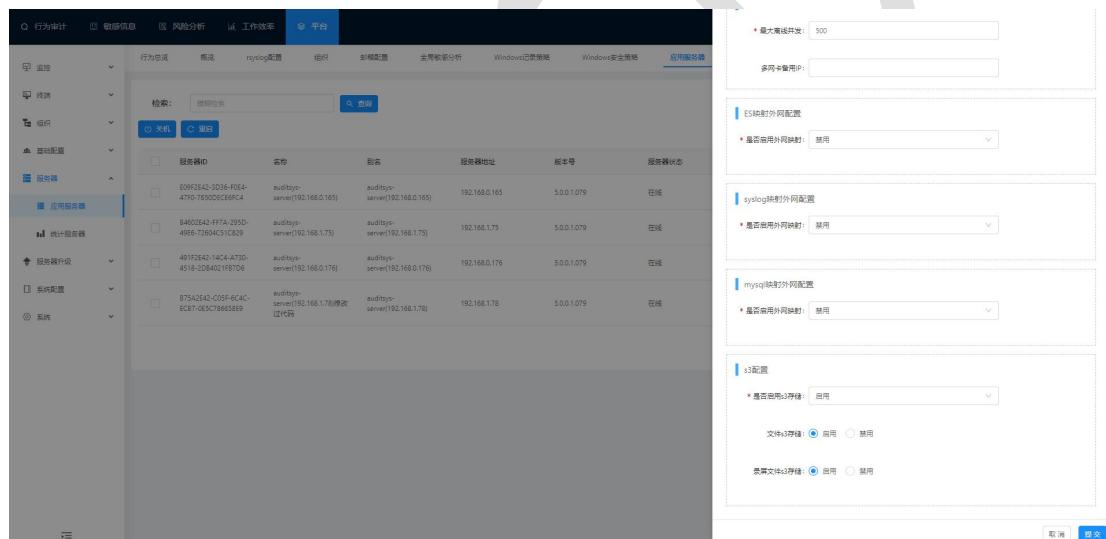
是否启用：启用，则终端的审计数据会写入外网的应用服务器。

服务器IP：外网的应用服务器IP地址。

端口号：默认是3454。

接入范围：选择需要被写入的组织信息。

（服务器映射外网配置不支持IP段）



S3配置：

文件s3存储启用后上传的文件将存储到s3服务器上，禁用后保存在本地服务器。

录屏文件s3存储启用后，视频会话将保存在s3服务器上，禁用后保存在本地服务器上

接收配置：

最大离线并发：例如配置100，那么只能100个离线会话同时上传。

多网卡备用IP：当应用服务器出现异常时，终端数据就会写入到备用IP的服务器。

压缩配置：

启动条件：例如配置100，那么小于100个会话视频文件将不会压缩，不会备份迁移。

#### ES 映射外网配置：

是否启用外网映射：启用，则该服务器数据会写入外网 ES。

Elasticsearch 地址：输入正确外网 ES 地址。

内部通信地址：输入正确通信地址。

#### Syslog 映射外网配置：

是否启用外网映射：启用，则该服务器日志写入外网 syslog。

外网 syslog 地址：输入正确外网 syslog 地址。

端口号：输入正确端口号。

**(注：需要先启用 rsyslog 配置；syslog 映射外网才会生效)**

#### MySQL 映射外网配置：

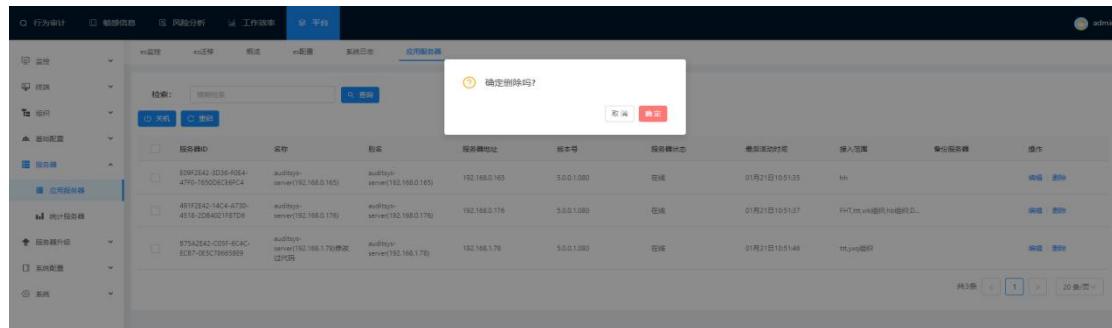
是否启用外网映射：启用，则可以使用外网 MySQL 的策略配置。

外网 MySQL 映射：输入正确外网 MySQL 地址。

端口号：默认是 3306。

## 2.16.2 删除应用服务器

选择要删除的服务器，点击“删除”按钮，再点击确定。如下图所示：



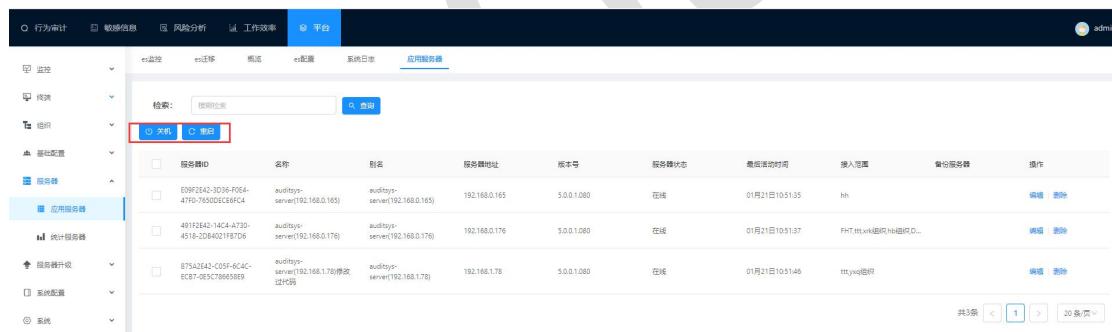
删除在线的服务器成功后，过一会儿，会重新注册上报到应用服务器界面；需要重新配置接入访问和其它配置。

删除离线的服务器成功后，需要待服务器开启后再重新注册上报到应用服务器界面。

## 2.16.3 关机，重启应用服务器

选择服务器，点击关机，此服务器关机。

选择服务器，点击重启，此服务器重启。

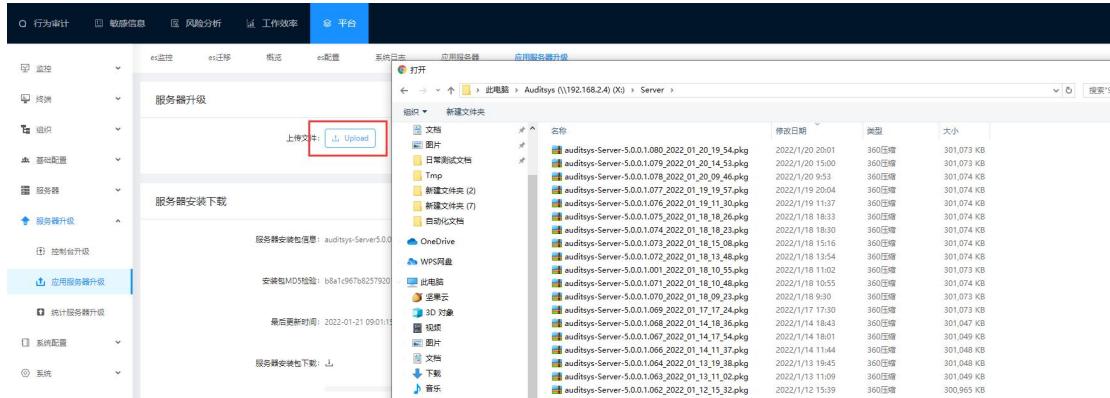


## 2.16.4 应用服务器升级

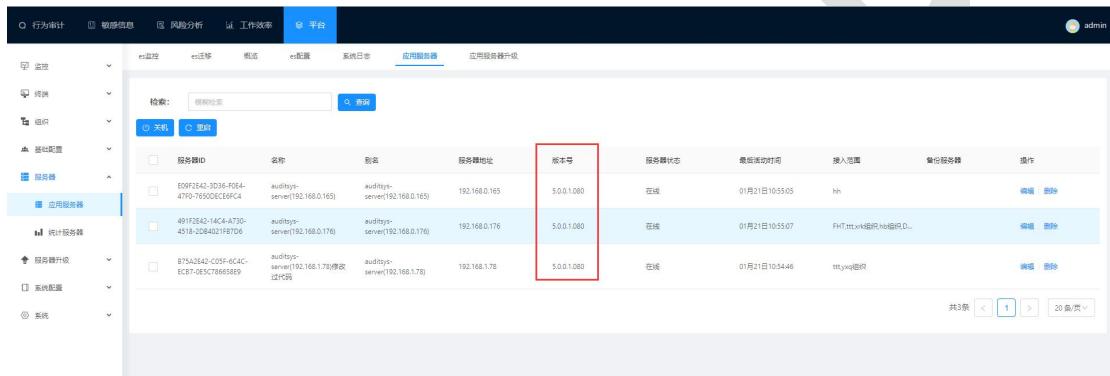
选择“平台>服务器升级>应用服务器升级”进入应用服务器升级界面；

选择 Server 升级包上传。提示：Server 升级需要一点点时间(先上传升级包再进行升级)，

请不要重复点击上传按钮。如下图所示：

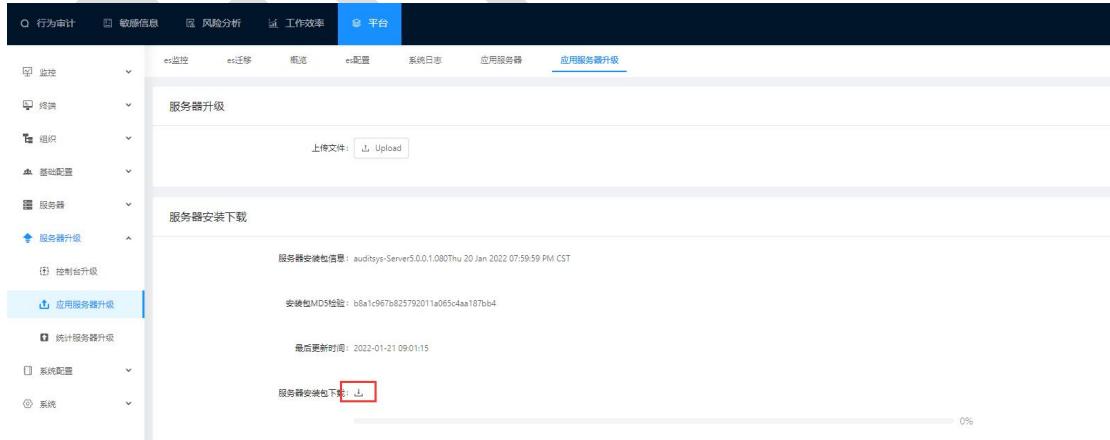


查看所有 Server 是否升级完成，请查看“应用服务器”模块，服务器列表中有版本号。如果 Server 是离线，则需要等待 Server 上线后才会升级。如下图所示：



## 2.16.5 安装包下载

选择“平台>服务器升级>应用服务器升级”，点击“服务器安装下载”的下载按钮下载安装包。如下图所示：



## 2.17 统计服务器

安装注册统计服务器，工作效率数据才会进行效率汇总。

## 2.17.1 统计服务器升级下载

统计服务器升级步骤：详见步骤 3.1.4 应用服务器升级。

统计服务器安装包下载步骤：详见步骤 3.1.5 应用服务器安装包下载。

## 2.17.2 插件管理

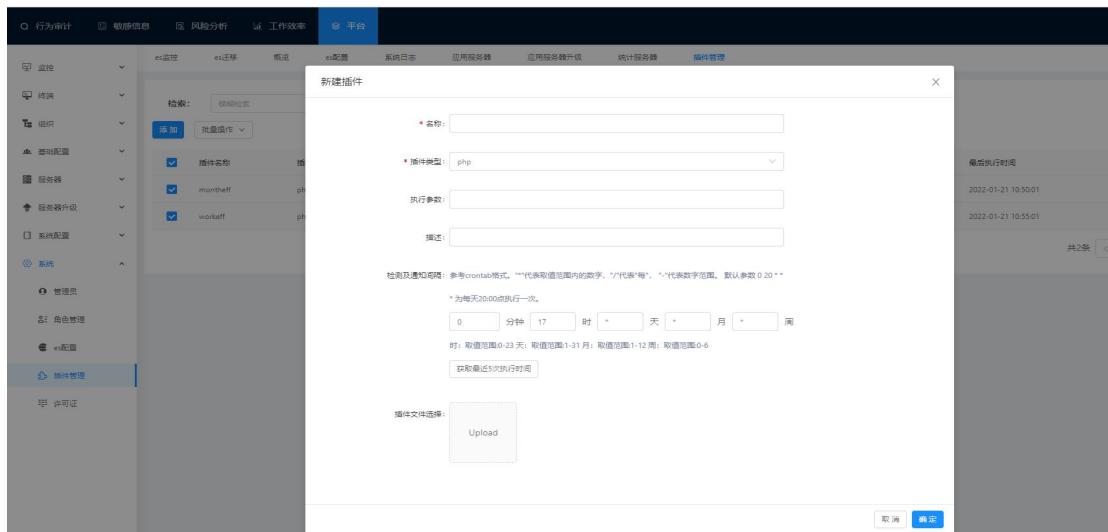
**Workeff 插件：**只计算每人每天的数据（默认计算 7 天，若当天的效率数据总条数没有变化，则不会重新计算）

**Montheff 插件：**计算部门、公司以及每月数据汇总的插件，统计的数据是在 workeff 计算的基础上二次统计，默认会重算当月所有数据（效率汇总）。

**注：配置 Workeff 插件自动执行时间不要大于 Montheff 插件自动执行时间。**

## 2.17.3 新建插件

选择“系统>插件管理”点击“添加”按钮，跳转至新建插件界面，如下图所示：



名称：插件命名（只限英文字母和数字）。

插件类型：目前只支持 PHP。

执行参数：无需配置

描述：对插件进行描述。

检测及通知间隔：配置自动执行时间。

插件文件选择：上传插件文件，点击上传，待上传成功。

**注：新添加的插件需要手动执行一次**

## 2.17.4 手动执行

点击“执行”按钮，可以进行手动执行一次插件，重新计算更新效率数据。

操作	操作
编辑	<a href="#">执行</a>
删除	
更多	

## 2.18 终端

终端：对所有 Windows 终端和 Linux 终端进行管理。

选择“管理->终端->终端” 查看终端信息。

### 2.18.1 终端列表

根据搜索条件，选择组织、部门、终端组、终端类型、版本、在线状态等搜索终端，或者输入终端的地址、名称等模糊搜索终端。也可以点击列表表头进行排序。**提示：只有列表上三角形图案的才能排序。**如下图所示：

The screenshot shows a web-based terminal management interface. At the top, there's a navigation bar with tabs: 行为审计, 敏感信息, 风险分析, 工作效率, 平台 (Platform), and a user icon labeled 'admin'. Below the navigation bar is a search bar with fields for 检索 (Search), 状态 (Status), and 在线状态 (Online Status). There are also buttons for 导入 (Import), 导出 (Export), and 搜索 (Search). To the left, there's a sidebar with various filters and categories: 直接, 终端, 终端升级, Linux终端升级, 终端组, 终端策略, 电源, 基础配置, 端口映射, 端口映射升级, 系统配置, and 系统。The main content area displays a table of terminal information. The table has columns: 终端名称 (Terminal Name), 父部门/部门 (Parent Department/Department), 用户姓名 (User Name), 公司 (Company), 终端地址 (Terminal Address), 类型 (Type), 组 (Group), 版本 (Version), 下次升级版本 (Next Upgrade Version), 地址 (Address), 扩展端口 (Extended Port), 是否外挂 (Is External), 在线状态 (Online Status), 使用状态 (Usage Status), ID (ID), 会话会话时间 (Session Session Time), 最近会话时间 (Recent Session Time), and 操作 (Operation). The table contains several rows of terminal data, such as 'centos72-64-tt: 18-test' and 'DESKTOP-TP147T2'. The '操作' column for each row includes buttons for 编辑 (Edit), 关联 (Associate), and 锁定 (Lock).

终端名称	父部门/部门	用户姓名	公司	终端地址	类型	组	版本	下次升级版本	地址	扩展端口	是否外挂	在线状态	使用状态	ID	会话会话时间	最近会话时间	操作
子机	来分组	李锐	来分组	192.168.3.248	普通终端	Default_Group	5.0.0.1027		Default_Org	否	离线	启用	静态	01月20日 17:16:02	01月20日 18:06:39	编辑 关联 锁定	
centos72-64-tt: 18-test				192.168.1.31	Linux终端	Default_Group	4.9.0.808		Default_Org	否	离线	禁用	动态	09:40:45	09:40:45	编辑 关联 锁定	
WIN2008企业-32bit-01				192.168.3.134	普通服务器	FHT组织	5.0.0.1011		tt	离线	禁用	动态	12月09日 10:04:46	12月16日 14:53:21	编辑 关联 锁定		
DESKTOP-TP147T2	华为	1213	华为	192.168.3.127	普通终端	Admin_default	5.0.0.1027		FHT组织	是	在线	启用	动态	01月03日 10:56:02	01月20日 18:56:31	编辑 关联 锁定	
WIN-BF1FEDHDLB	华为,测试	李元芳	华为	192.168.0.44	普通服务器	hh_default	5.0.0.1027		hh	是	在线	启用	动态	01月20日 09:30:37	01月20日 16:59:54	编辑 关联 锁定	
WIN-DV0C7KPKP	华为,测试	顾维东	华为	192.168.3.145	普通终端	yyq组织_default	5.0.0.1012		yyq组织	否	离线	禁用	动态	12月17日 17:46:56	12月17日 16:50:21	编辑 关联 锁定	
SINO	华为,测试	夏阳	华为	192.168.3.159	普通终端	hh_default	5.0.0.1027		hh	是	在线	启用	动态	01月19日 09:39:39	01月20日 17:00:01	编辑 关联 锁定	
admin-PC	华为	何植恩	华为	192.168.0.22	普通终端	xk组织_default	5.0.0.1027		xk组织	1567	是	在线	启用	01月20日 09:24:01	01月20日 16:59:55	编辑 关联 锁定	
DESKTOP-Q3ASVCM	华为,测试	金亮强	华为	192.168.3.133	普通终端	hh_default	5.0.0.1027		hh	否	在线	启用	动态	01月20日 10:55:39	01月20日 17:00:21	编辑 关联 锁定	
子机				192.168.3.249	普通终端	CSY-组织_default	4.8.1.4		FHT-T1组	否	离线	禁用	动态	01月06日 07:14:43	01月06日 07:14:50	编辑 关联 锁定	

### 2.18.2 编辑终端

点击“操作”列中的“编辑”按钮进行编辑终端信息，只能修改终端别名；使用终端别名，该终端的会话数据和行为数据的终端名称都是显示终端别名；如下图所示：

The screenshot shows a terminal management interface with a search bar and a table of terminal details. A modal window titled "Bind Organization" is overlaid, asking for the terminal name, user name, department, and organization name. The organization name field is highlighted.

## 2.18.3 绑定组织

勾选需要绑定到同一组织下的终端（**终端刚注册默认绑定默认组织**），点击“绑定组织”修改终端的组织。此终端同时也会绑定到对应组织默认的终端组下。如下图所示：

The screenshot shows a terminal management interface with a search bar and a table of terminal details. A modal window titled "Bind Organization" is overlaid, showing the selected organization "Default\_Org" and a list of terminals grouped by organization. The organization "Default\_Org" is highlighted.

## 2.18.4 启用禁用

选择终端，点击“批量操作”下拉框，选择启用或禁用。如下图所示：

The screenshot shows a terminal management interface with a list of terminals. One terminal entry has its checkbox checked, indicating it is selected for deletion.

点击启用或禁用有提示确认框。点击“确定”。

**提示：**当终端类型的启用数与许可证对应的许可数相等，那么该类型的终端不可启动。

禁用的终端做任何操作将不会审计。

**解决方案：**1：先停用对应的终端类型，在启动。2：重新申请许可证，扩大许可数。

## 2.18.5 删 除 终 端

勾选需要删除的终端，点击“删除”按钮删除终端记录（只删除了界面数据）。如下图所示：

The screenshot shows a terminal management interface with a list of terminals. One terminal entry has its checkbox checked, indicating it is selected for deletion.

如果终端没有卸载，点击删除后，界面会删除掉终端信息，待该终端上线时，终端信息会重新注册上来。

## 2.18.6 卸 载 终 端

勾选需要卸载的终端，点击“卸载”按钮卸载终端。如下图所示：

The screenshot shows a terminal management interface with a search bar and various buttons like 'Import/Export Configuration' and 'Batch Unload'. A table lists terminals with columns for name, department, user name, company, address, status, and more. One terminal is selected for action.

终端名称	父部门+部门	用户名	公司名	终端地址	状态	下次升级版本	组名	扩展编号	是否外网	在线状态	启用状态	动态ID	最后会话时间
子悦	未分组	子悦	未分组	192.168.3.24	启用	5.0.0.1.027	Default_Group		否	离线	启用	静态	01月20日 17:16:02
centos72-64-tt-18.test				192.168.1.31	通知	4.9.0.8.008	Default_Group		否	离线	禁用	动态	11月17日 09:40:45
WIN2008企业-32bit-01				192.168.3.134	普通服务器	5.0.0.1.011	_default	ttt	是	离线	禁用	动态	12月09日 10:40:46
DESKTOP-TP14T72	华为	1213	华为	192.168.3.127	普通终端	5.0.0.1.027	Admin_default		是	在线	启用	动态	01月21日 10:56:02
WIN-6F1FEIRHDLB	华为_测试	李元秀	华为	192.168.0.44	普通服务器	5.0.0.1.027	hh_default		是	在线	启用	动态	01月20日 09:30:37
WIN-OVOCITKPOPK	华为_测试	顾伟东	华为	192.168.3.145	普通服务器	5.0.0.1.012	yxq组织_default		否	离线	禁用	动态	12月17日 17:46:56

提示：离线终端需等待上线才会执行卸载！

## 2.18.7 终端明细

点击“操作”列中的“明细”按钮查看终端详细信息。如下图所示：

终端状态：记录该终端的 ID，主机名，操作系统，运行时间，IP 地址，版本信息，mac 地址，终端 ID 类型，处理器信息，内存信息，磁盘信息。

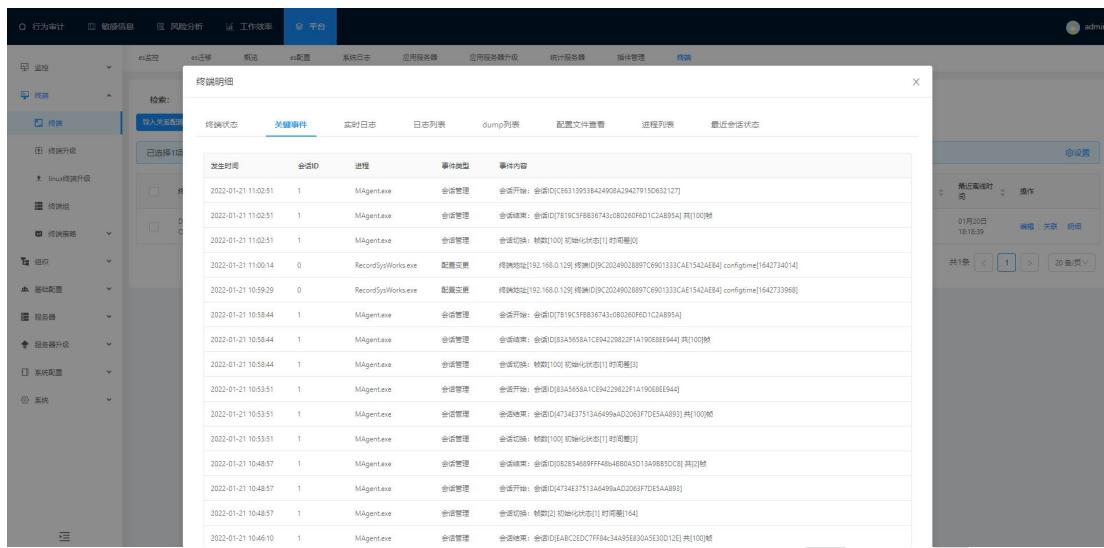
The screenshot shows a detailed view of a terminal's configuration. It includes sections for terminal status, memory, and disk information. The terminal ID is 9C20249028897C6901333CAE1542AE84, the host name is DESKTOP-CSGED4, and the operating system is Windows 10 家庭版 64 位 (10.0 版本 18362). The memory section shows total memory of 8015MB and virtual memory of 15439MB. The disk section shows two drives: C and D.

内存信息	物理内存总量: 8015MB	可用物理内存: 2729MB	可用的虚拟内存: 3987MB
内存信息	虚拟内存最大值: 15439MB	使用中的虚拟内存: 11451MB	

磁盘信息	盘符名称: C:	磁盘大小: 237.35G	空闲大小: 126.39G	使用比例: 46%
磁盘信息	盘符名称: D:	磁盘大小: 931.51G	空闲大小: 788.10G	使用比例: 15%

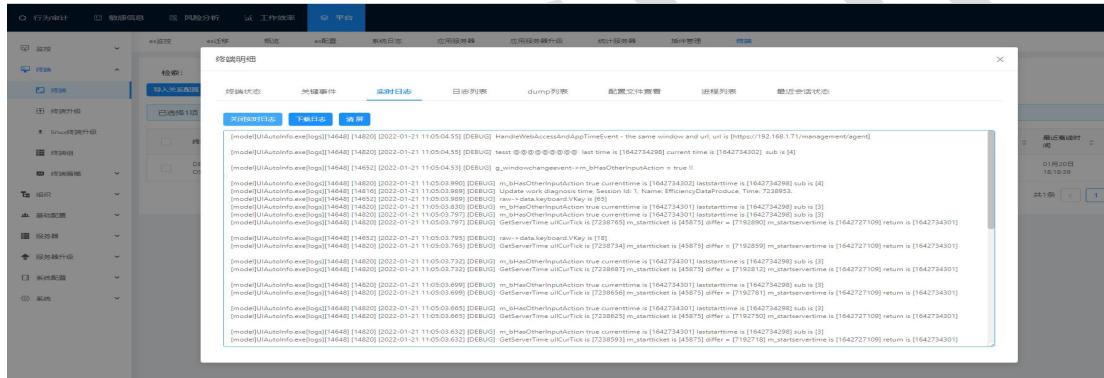
关键事件：更改终端对应的策略，终端名，终端 IP，终端重启，关机，注销，应用服务器配置更改，时间修改，终端解锁屏，应用阻断，Magent 重启等操作都会记录相应关键事件。

如图所示：



实时日志:点击开启实时日志记录终端实时操作所产生的日志, 如下图所示:

(注: 开启实时日志或在日志列表开启日志, 才会记录 DEBUG 日志)



日志列表: 开启日志, 记录终端操作产生的日志和 DEBUG 日志, 支持上传下载 (日志状态显示是已上传才能下载); 删除日志列表的日志, 安装目录下 log 日志文件下所对应的日志也被删除;支持日志文件压缩; 开启诊断工具, 则会产生一个 Diagnosis.log 日志文件; 如下图所示:

auditlog\_uithool.exe.2021-12-08.log.zip  
auditlog\_uithool.exe.2021-12-09.log.zip  
auditlog\_uithool.exe.2021-12-10.log.zip  
auditlog\_uithool.exe.2021-12-13.log.zip  
auditlog\_uithool.exe.2021-12-14.log.zip  
auditlog\_uithool.exe.2021-12-14.log.zip  
auditlog\_uithool.exe.2021-12-15.log.zip  
auditlog\_uithool.exe.2021-12-16.log.zip  
auditlog\_uithool.exe.2021-12-17.log.zip  
auditlog\_uithool.exe.2021-12-20.log.zip  
auditlog\_uithool.exe.2021-12-21.log.zip  
auditlog\_uithool.exe.2021-12-22.log.zip

Dump 文件：点击查看 dump 文件，支持下载上传（日志状态显示是已上传才能下载）；删除 dump 列表的日志，安装目录下 dump 日志文件下所对应的日志也被删除；支持日志文件压缩；如下图所示：

UiAutofill.exe\_1.dump  
MOROnlineServer.exe\_0.dump

配置文件获取：点击获取配置文件，查看 agent 文件配置详情，如下图所示：

The screenshot shows the Audit Center platform. A modal window titled '终端明细' (Terminal Details) is open, displaying terminal session logs and configuration details. The logs include command history and session details. The configuration section shows various system parameters like ports, protocols, and file paths. A '生成转储文件' (Generate Dump File) button is visible at the bottom left of the modal.

进程列表：点击获取进程列表查看审计中心运行时相应进程详情；点击‘生成转储文件’可以生成相应 dump 文件；点击‘重启’可以进程重启；如下图所示：

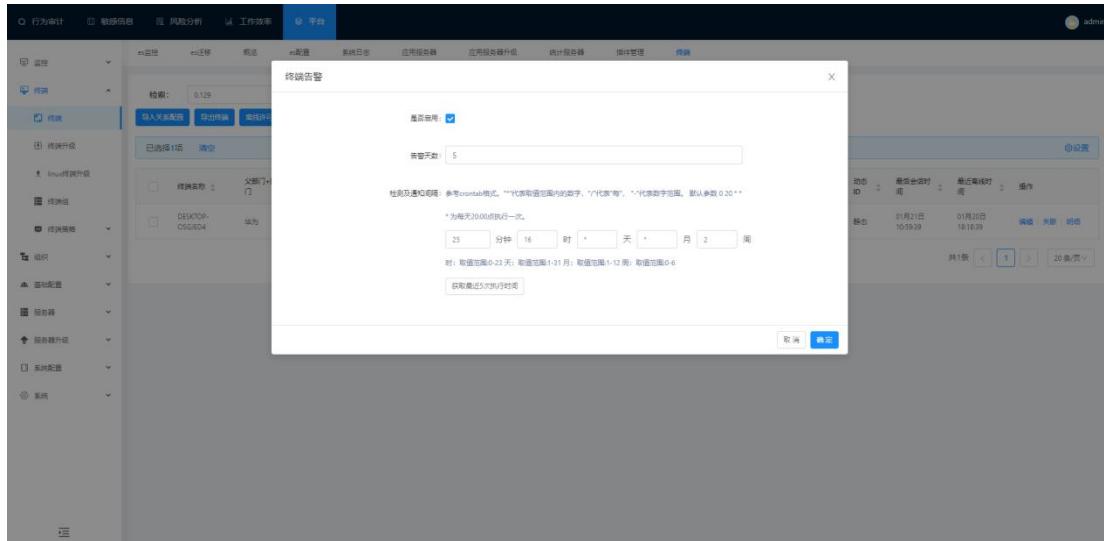
The screenshot shows the Audit Center platform. A modal window titled '进程列表' (Process List) is open, listing system processes such as AudiTaskService.exe, UpdateService.exe, MCHDriveServer.exe, RecycleSysWorker.exe, audiosys\_utool.exe, spyware.exe, Magent.exe, and UAAutoInfo.exe. Each process entry includes its ID and an '生成转储文件' (Generate Dump File) action button. The main interface shows system monitoring and audit logs.

最近会话状态：点击最近会话状态，查看最近的会话相应详情；如下图所示：

The screenshot shows the Audit Center platform. A modal window titled '最近会话状态' (Recent Session Status) is open, displaying session details. It includes fields for session ID, host name, start time, end time, and session ID. The main interface shows system monitoring and audit logs.

## 2.18.8 告警配置

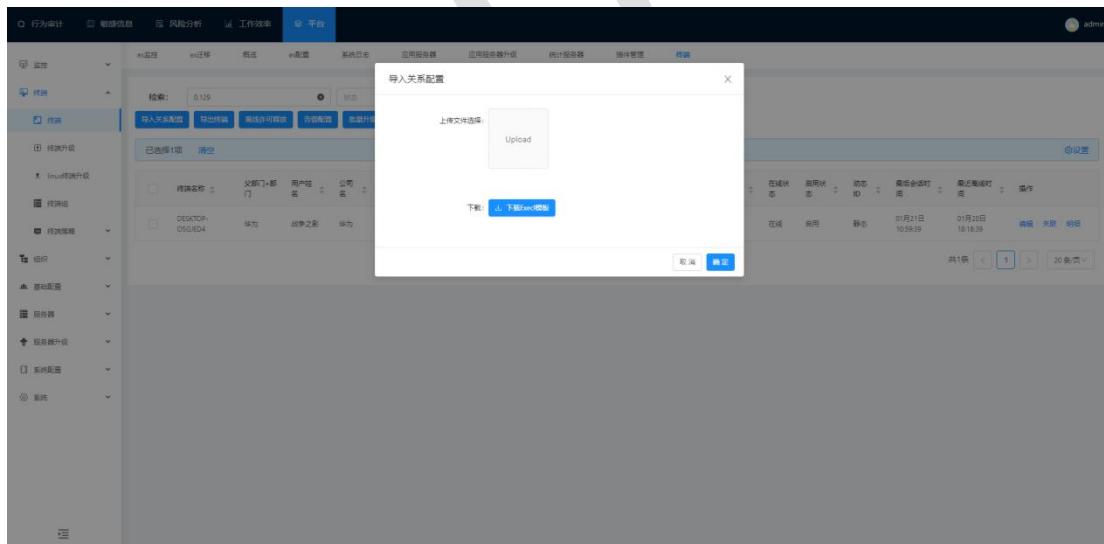
点击“告警配置”按钮，跳转至终端告警界面。如图：



勾选是否启用，才会发送告警邮件；**邮件只记录无会话告警天数启用的终端信息。**

## 2.18.9 导入关系配置

点击“导入关系配置”按钮，进入导入关系配置界面，如图：



提示：在导入关系配置界面点击“下载 excel 模板”，再在模板里配置好数据保存，再上传。

## 2.18.10 导出终端

点击导出终端按钮，可以把所有终端信息下载成 excel 文档格式；如下图所示：

The screenshot shows the terminal management interface with the 'Export' button highlighted. A large Excel file is displayed below the interface, containing detailed information about multiple terminals, such as their names, IP addresses, and connection status.

## 2.18.11 标记静态 ID

勾选需要标记为静态的 ID 类型为动态且在线的终端，点击“标记静态 ID”按钮。如下图所示：

The screenshot shows the terminal management interface with the 'Mark Static ID' button highlighted. A confirmation dialog box is visible, asking if the user wants to mark the selected dynamic and online terminals as static. The interface displays a list of terminals with their current status and configuration.

弹出确认提示框，点击确定后，静态 ID 标记成功。界面显示 ID 类型由动态变为静态。

ID 类型为静态的终端，mac 地址和 cpuid 发生变化时，终端 id 不发生变化。

ID 类型为动态的终端，mac 地址和 cpuid 发生变化时，终端 id 发生变化，重新注册新的终端且之前的终端离线。

Linux 终端不支持标记静态 ID。

## 2.18.12 离线许可释放

配置离线许可释放的天数，当终端离线的最后会话时间超过配置的离线许可释放的天数时，该终端就会被软禁用，相应许可使用数释放。

The screenshot shows a modal dialog titled "离线许可释放天数" (Offline License Release Days) with a search bar and a dropdown menu. Below the dialog is a table listing terminal details, including terminal name, department, user, company, IP address, model, version, and various status indicators like online/offline, enable/disable, and last session time.

终端名称	父部门/部门	用户名	公司	终端地址	终端类型	版本	下次升级版	插件	扩展	是否分区	在线	启用	状态	最后会话时间	最近连接时间	操作
子流	未分组	子流	未分组	192.168.3.248	普通终端	Default_Group	5.0.0.1.027	Default_Org	否	离线	禁用	静态	01月20日 17:16:02	01月20日 18:06:39	<a href="#">编辑</a> <a href="#">关联</a> <a href="#">禁用</a>	
centos72-64-itt-18-test				192.168.1.31	Linux终端	Default_Group	4.9.0.0.008	Default_Org	是	离线	禁用	动态	11月17日 09:40:45	11月17日 09:40:45	<a href="#">编辑</a> <a href="#">关联</a> <a href="#">禁用</a>	
WIN2008企业-12bit-01				192.168.3.134	普通服务器	FHT组织	5.0.0.1.011	是	离线	禁用	动态	12月份 10:40:46	12月份 14:52:21	<a href="#">编辑</a> <a href="#">关联</a> <a href="#">禁用</a>		
DESKTOP-TP147T2	华为	1213	华为	192.168.3.127	普通终端	Admin_default	5.0.0.1.027	H组织	是	在线	启用	动态	01月21日 11:10:02	01月20日 18:56:51	<a href="#">编辑</a> <a href="#">关联</a> <a href="#">禁用</a>	
WIN-6F1FEDHDLB	华为_测试	李元芳	华为	192.168.0.44	普通服务器	hh_default	5.0.0.1.027	hh	是	在线	启用	动态	01月20日 09:50:37	01月20日 16:59:54	<a href="#">编辑</a> <a href="#">关联</a> <a href="#">禁用</a>	
WIN-DIVISION0SPK	华为_测试	顾维东	华为	192.168.3.145	普通服务器	yy组织	5.0.0.1.012	yy组织	否	离线	禁用	动态	12月17日 17:46:38	12月17日 16:50:21	<a href="#">编辑</a> <a href="#">关联</a> <a href="#">禁用</a>	
SINO	华为_测试	莫言	华为	192.168.3.159	普通终端	hh_default	5.0.0.1.027	hh	是	在线	启用	动态	01月19日 09:39:39	01月20日 17:00:01	<a href="#">编辑</a> <a href="#">关联</a> <a href="#">禁用</a>	
admin-PC	华为	何基基	华为	192.168.0.22	普通终端	xx组织	5.0.0.1.027	xx组织	是	在线	启用	动态	01月20日 09:34:01	01月20日 16:59:55	<a href="#">编辑</a> <a href="#">关联</a> <a href="#">禁用</a>	
DESKTOP-Q3AGVCM	华为_测试	金光锐	华为	192.168.3.133	普通终端	hh_default	5.0.0.1.027	hh	否	在线	启用	动态	11月份 11:06:59	11月份 17:00:21	<a href="#">编辑</a> <a href="#">关联</a> <a href="#">禁用</a>	
子流				192.168.3.249	普通终端	CSV组织	4.8.1.4	FHT组织	是	离线	禁用	静态	01月06日 01:00:00	01月06日 01:00:00	<a href="#">编辑</a> <a href="#">关联</a> <a href="#">禁用</a>	

## 2.18.13 批量升级

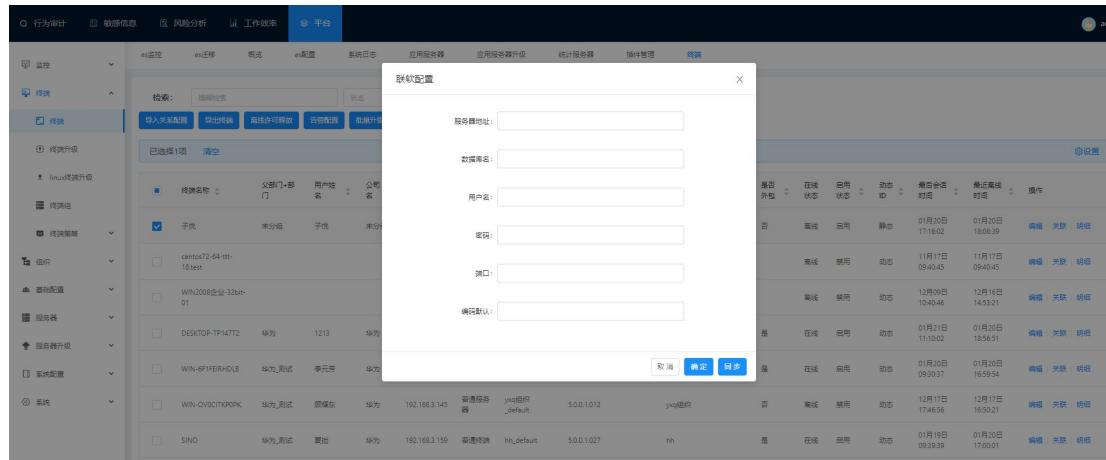
选择要升级的终端，点击批量升级，下次升级版本就会显示要升级的版本号信息；离线的终端待在线时会升级（前提需在终端升级模块上传升级包且勾选“是否自动升级”；详见步骤 3.6）

The screenshot shows a modal dialog titled "确定升级吗？" (Confirm Upgrade?) with a "取消" (Cancel) button and a red "确定" (Confirm) button. Below the dialog is a table listing terminal details, similar to the previous screenshot, showing various configurations and status information.

终端名称	父部门/部门	用户名	公司	终端地址	终端类型	版本	下次升级版	插件	扩展	是否分区	在线	启用	状态	最后会话时间	最近连接时间	操作
子流	未分组	子流	未分组	192.168.3.248	普通终端	Default_Group	5.0.0.1.027	Default_Org	否	离线	禁用	静态	01月20日 17:16:02	01月20日 18:06:39	<a href="#">编辑</a> <a href="#">关联</a> <a href="#">禁用</a>	
centos72-64-itt-18-test				192.168.1.31	Linux终端	Default_Group	4.9.0.0.008	Default_Org	是	离线	禁用	动态	11月17日 09:40:45	11月17日 09:40:45	<a href="#">编辑</a> <a href="#">关联</a> <a href="#">禁用</a>	
WIN2008企业-12bit-01				192.168.3.134	普通服务器	FHT组织	5.0.0.1.011	是	离线	禁用	动态	12月份 10:40:46	12月份 14:52:21	<a href="#">编辑</a> <a href="#">关联</a> <a href="#">禁用</a>		
DESKTOP-TP147T2	华为	1213	华为	192.168.3.127	普通终端	Admin_default	5.0.0.1.027	H组织	是	在线	启用	动态	01月21日 11:10:02	01月20日 18:56:51	<a href="#">编辑</a> <a href="#">关联</a> <a href="#">禁用</a>	
WIN-6F1FEDHDLB	华为_测试	李元芳	华为	192.168.0.44	普通服务器	hh_default	5.0.0.1.027	hh	是	在线	启用	动态	01月20日 09:50:37	01月20日 16:59:54	<a href="#">编辑</a> <a href="#">关联</a> <a href="#">禁用</a>	
WIN-DIVISION0SPK	华为_测试	顾维东	华为	192.168.3.145	普通服务器	yy组织	5.0.0.1.012	yy组织	否	离线	禁用	动态	12月17日 17:46:38	12月17日 16:50:21	<a href="#">编辑</a> <a href="#">关联</a> <a href="#">禁用</a>	
SINO	华为_测试	莫言	华为	192.168.3.159	普通终端	hh_default	5.0.0.1.027	hh	是	在线	启用	动态	01月19日 09:39:39	01月20日 17:00:01	<a href="#">编辑</a> <a href="#">关联</a> <a href="#">禁用</a>	
admin-PC	华为	何基基	华为	192.168.0.22	普通终端	xx组织	5.0.0.1.027	xx组织	是	在线	启用	动态	01月20日 09:34:01	01月20日 16:59:55	<a href="#">编辑</a> <a href="#">关联</a> <a href="#">禁用</a>	

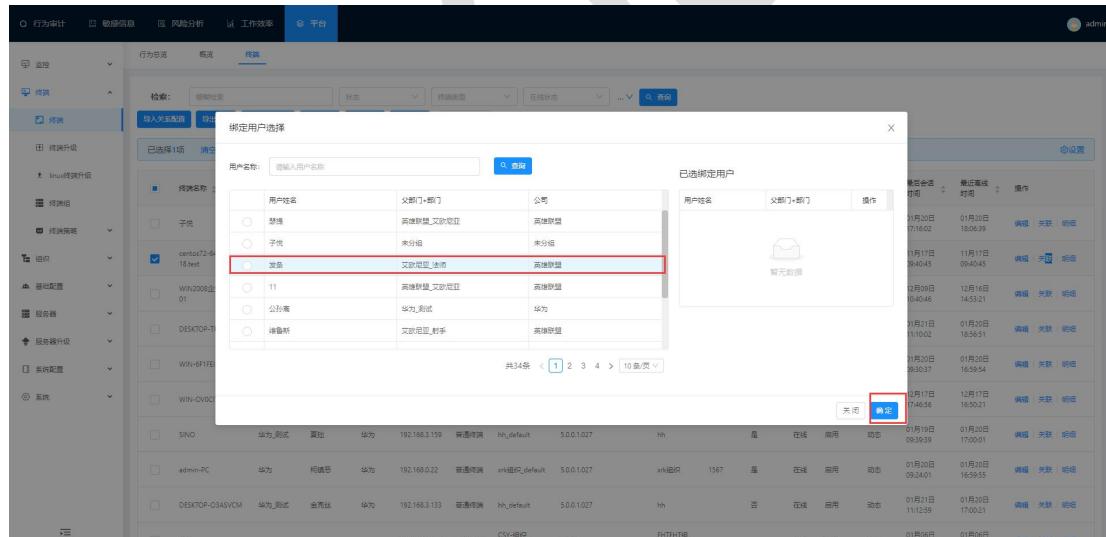
## 2.18.14 联软配置

配置联软配置，可以同步服务器内与终端信息匹配的用户信息到终端列表中。



## 2.18.15 关联

点击“关联”按钮，弹出绑定用户选择窗口；选择要绑定的用户，点击“确定”按钮进行绑定（一个终端只能绑定一个用户）；已绑定用户的终端，点击“删除”按钮，进行解除用户绑定。（注：需先配置部门、用户信息）如下图所示：



## 2.18.16 自定义列

点击“设置”按钮，弹出自定义列框，勾选则显示，不勾选则不显示；如下图所示：

The screenshot shows a terminal management interface with a sidebar containing categories such as Audit, Data Information, Risk Analysis, Work Efficiency, and Terminal Management. The Terminal Management section is active, showing a sub-menu for Upgrade. A search bar at the top allows filtering by name, status, and other parameters. Below the search bar is a table listing 18 terminals. The columns include: Name, Department, User Type, Company, Terminal Address, Terminal Type, Group, Version, Next Upgrade Version, Organization, Whether Offline, Status, Status ID, Last Connection Time, and Last Upgrade Time. One terminal, 'centos72-64-bit-18-test', is selected, indicated by a blue checkmark.

## 2.19 终端升级

终端升级：对所有 Windows 终端的升级进行管理。

选择“管理>终端>终端升级”；点击“upload”按钮上传 agent 升级包。

**必须勾选是否自动升级和默认全部升级，终端才会升级；否则不会升级；不勾选默认全部升级，可以选择部分终端进行批量升级。**

**提示： Agent 升级是一台一台的升级，请不要重复点击升级，如果 Agent 是离线，则需要等待 Agent 上线后才会升级。**

查看所有 Agent 是否升级完成，请查看“终端”模块，终端列表有版本号。如下图所示：

This screenshot shows the 'Upgrade' tab within the terminal management module. On the left, there's a sidebar with various system management categories. The main area is titled 'Terminal Installation Package Upload'. It features a 'Upload File' button and a progress bar for a download named '终端安装包下载 (上传完成升级信息!)'. The progress bar shows '0%' completion. Below the progress bar, there are checkboxes for '是否自动升级' (Automated Upgrade) and '默认全部升级' (Default All Upgrade). At the bottom right of the main area is a large blue '提交' (Submit) button.

## 2.20 Linux 终端升级

Linux 终端升级：对所有 Linux 终端的升级进行管理。

选择“管理>终端>Linux 终端升级”进入 Linux 终端升级界面。

Linux 终端升级：先添加系统版本，再上传 Linux 终端升级包；离线 Linux 终端需等在线才能升级。勾选是否自动升级，注：目前 Linuxagent 版本有七个；如下图所示：

The screenshot shows the 'Linux Terminal Upgrade' interface. On the left is a sidebar with categories like '行为审计', '敏感信息', '风险分析', '工作效率', '平台', '终端', '终端升级', '终端组', '运维', '基础配置', '服务器', '服务器升级', '系统配置', and '系统'. The '终端升级' tab is selected. In the main area, there's a table with columns: '系统版本' (System Version), '安装包信息' (Install Package Information), '版本号' (Version Number), '版本md5' (Version md5), '是否自动升级' (Automatic Upgrade), and '操作' (Operation). A red arrow points to the 'Upload' button in the '操作' column for the 'ubuntu20-x64d64' row. The table shows 1 item.

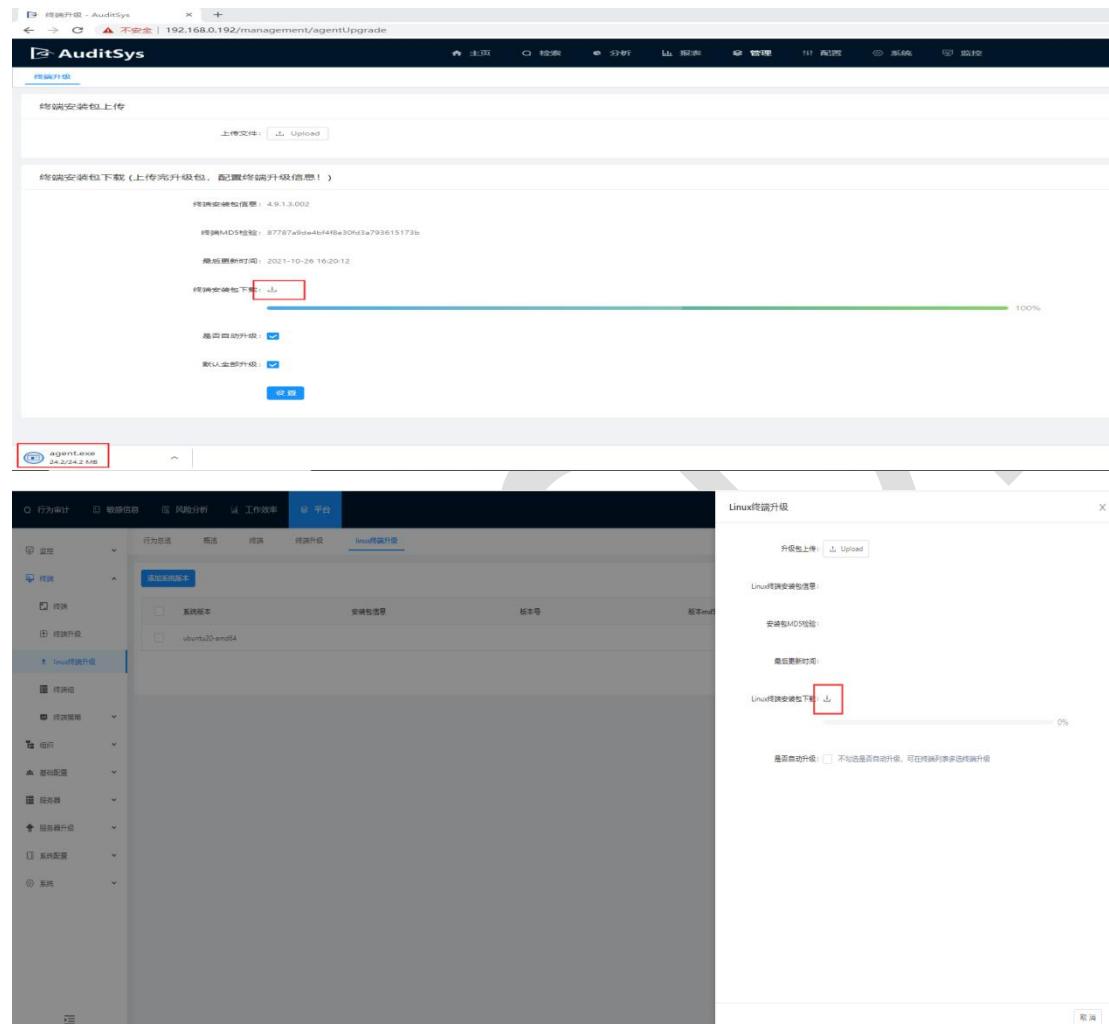
勾选是否自动升级，则对应的 Linux 系统版本的终端全部升级，不勾选是否自动升级，则需在“终端”模块，选择对应的 Linux 系统版本的终端，进行批量升级；如下图所示：

This screenshot shows the same 'Linux Terminal Upgrade' interface as the previous one, but the right side is expanded to show the configuration details. It includes sections for '升级包上载' (Upgrade Package Upload) with an 'Upload' button, 'Linux终端安装包信息' (Linux Terminal Installation Package Information), '安装包MD5校验' (Installation Package MD5 Check), '最后更新时间' (Last Update Time), 'Linux终端安装包下载' (Linux Terminal Installation Package Download) with a progress bar at 0%, and '是否自动升级' (Automatic Upgrade) with a note: '不勾选是否自动升级，可在终端列表多选终端升级' (If not checked for automatic upgrade, you can select multiple terminals in the terminal list for batch upgrade). A red arrow points to the 'Upload' button in the configuration panel.

## 2.20.1 安装包下载

选择平台>终端>终端升级，终端安装包下载。

选择平台>终端>Linux 终端升级，Linux 终端安装包下载。如下图所示：



## 2.21 终端组

终端组：对终端的记录策略，安全策略进行管理。

### 2.21.1 终端组列表

选择“平台>终端>终端组”。根据搜索条件，选择终端组组织搜索终端组，或者输入终端组的名称等模糊搜索终端组。如下图所示：

The screenshot shows a table listing 11 terminal groups. The columns include: 终端名称 (Terminal Name), 组织 (Organization), 终端数量 (Number of Terminals), Windows记录策略 (Windows Log Policy), Windows安全策略 (Windows Security Policy), Linux记录策略 (Linux Log Policy), Linux安全策略 (Linux Security Policy), 描述 (Description), and 操作 (Operations). The table includes rows for 'hh\_default' (组织: hh, 终端数量: 5), 'vri组织默认' (组织: vri组织, 终端数量: 4), '1111组织默认' (组织: 1111组织, 终端数量: 0), 'ttt组织默认' (组织: ttt组织, 终端数量: 0), 'ha组织' (组织: ha组织, 终端数量: 0), 'FHT\_default' (组织: FHT, 终端数量: 4), 'CSV-组织默认' (组织: CSV-组织, 终端数量: 1), 'Admin\_default' (组织: Admin, 终端数量: 2), 'yng组织默认' (组织: yng组织, 终端数量: 6), 'FHT组织默认' (组织: FHT, 终端数量: 1), and 'Default\_Group' (组织: Default\_Org, 终端数量: 10). A search bar at the top allows filtering by terminal name.

## 2.21.2 新建终端组

点击“新建”按钮创建新的终端组。如下图所示：

The screenshot shows a modal dialog titled "新建终端组" (Create New Terminal Group) overlaid on the main terminal group list. It contains fields for: 名称 (Name) [必填], 组织 (Organization) [Default\_Org], Windows记录策略 (Windows Log Policy) [Default\_Policy], Windows安全策略 (Windows Security Policy) [Default\_Security\_Policy], Linux记录策略 (Linux Log Policy) [Default\_Policy], and Linux安全策略 (Linux Security Policy) [Default\_Policy]. A "提交" (Submit) button is at the bottom right.

输入终端组名称，选择组织。点击“提交”按钮保存新建的终端组。

如果需要选择其他的记录策略或安全策略。请先新建记录策略或安全策略。

新建记录策略参考 3.8 步骤。新建安全策略参考 3.9 步骤。

## 2.21.3 编辑终端组

点击“编辑”按钮编辑终端组信息。**自动生成的终端组，不可以修改终端组名称和组织。**

**提示：终端组下有终端，则不可以修改终端组的组织信息。**如下图所示：

The screenshot shows a list of terminal groups on the left and a detailed configuration dialog on the right. The configuration dialog includes fields for Name (hh\_default), Organization (hh), Windows Logon Policy (Default\_Policy), Windows Security Policy (Default\_Security\_Policy), Linux Logon Policy (Default\_Policy), and Linux Security Policy (Default\_Policy). A large watermark 'OK' is overlaid across the center of the screen.

## 2.21.4 删除终端组

勾选需要删除的终端组，点击“删除”按钮删除终端组。**自动生成的终端组不可手动删除，只能删除对应的组织才能被删除；**如下图所示：

The screenshot shows a list of terminal groups with checkboxes next to them. A confirmation dialog box is centered, asking "是否删除选中数据？" (Delete selected data?). The bottom right corner of the dialog has a red note: "如果终端组下有绑定终端，删除终端组，终端绑定到对应组织下的默认终端组里。" (If there are bound terminals under the terminal group, deleting the terminal group will bind the terminals to the default terminals under the corresponding organization.) A large watermark 'OK' is overlaid across the center of the screen.

如果终端组下有绑定终端，删除终端组，终端绑定到对应组织下的默认终端组里。

## 2.21.5 绑定终端

点击“绑定终端”进行绑定终端。选择要绑定的终端，再点击“确定”。点击“删除”按钮可以解除终端绑定。绑定成功的终端，则可使用该终端组所绑定的记录策略和安全策略如下图所示：

终端名称	IP地址	状态	类型	所属终端组	操作
1111组织_A		启用	普通终端	Admin_default	<a href="#">编辑</a>
T914772	192.168.3.127	启用	普通终端	Admin_default	<a href="#">编辑</a>
WIN2016服务器-64-01	192.168.0.42	启用	普通服务器	Admin_default	<a href="#">编辑</a>
Default_Group	Default_Org	10	Default_Policy	Default_Security_Policy	Default_Policy

## 2.22 Windows 记录策略

Windows 记录策略：控制 Windows 终端的行为数据审计、用户录像、应用录像、按键录像、离线缓存、效率明细审计、文件上传、二次认证。

## 2.22 记录策略列表

选择“平台>终端策略>Windows 记录策略”。输入记录策略的名称模糊可进行查询。如下图所示：

名称	是否录像	二次认证	描述	操作
默认	启用	禁用	<a href="#">修改</a>	
lh	启用	禁用	<a href="#">修改</a>	
tt	启用	禁用	<a href="#">修改</a>	
rk记录策略	启用	禁用	<a href="#">修改</a>	
No记录策略	启用	禁用	<a href="#">修改</a>	
FHT记录策略	启用	禁用	<a href="#">修改</a>	
yyw安全策略	启用	禁用	<a href="#">修改</a>	
Default_Policy	启用	禁用	默认记录策略 <a href="#">修改</a>	

### 2.22.1 新建 Windows 记录策略

点击“新建”按钮创建 Windows 记录策略，部分配置移至敏感记录策略中，功能不变。

## 基础配置：

策略名称：此项为必填项。

描述：可以描述此策略。

是否录像：控制终端是否录像。勾选则录像，可以查看录像回放。

只记录远程会话：勾选则只记录远程终端会话，不是远程终端操作不会记录。

是否显示托盘图标：勾选则会在终端电脑右下角任务栏中会显示 AuditSys 的图标。不勾选则不会显示。

是否显示隐私声明：提示用户此电脑已被监控，用户注意操作行为。勾选则终端 Magent 起来，会弹出一个提示框。

图像格式：录像的图像颜色。**此选项只有在勾选了“是否录像”才生效**

离线缓存视频大小：终端离线后，录像视频最大保存的大小。提示：**此选项只有勾选了“是否录像”才生效。**

离线上传限速：控制上传离线会话文件的速度。

录制密度：开启录制密度，打开 Windows 终端不操作，只要有画面变化，就会录屏；

录制密度为空，则关闭录制密度。如下图所示：



## 探针记录规则：

是否记录上网活动：勾选则浏览网页被记录。

是否记录剪贴板：勾选则复制剪切被记录。

是否记录 USB：勾选则终端连接移动设备被记录。

是否记录数据库：勾选则操作数据库命令被记录。

是否记录 QQ：勾选则 QQ 聊天被记录。

是否记录邮件：勾选则发送邮件内容被记录。

是否记录文件操作：勾选则文件新建、重命名、删除、复制、剪切被记录。

是否记录远程运维：勾选则使用运维工具操作 linux 命令被记录。

是否记录按键：勾选则使用键盘或鼠标按键被记录。

是否记录网页敏感内容：勾选则在 IE 和谷歌浏览器访问网页中的敏感词被记录。

是否记录操作标签：勾选则操作标签被记录。

是否记录微信：勾选则微信聊天消息被记录。

是否记录文档编辑：勾选则在记事本、word、excel 中编辑带有敏感词的文字被记录。

是否记录 POST 报文：勾选则在 IE 和谷歌浏览器访问网页中的报文被记录。

是否记录文件外发：勾选则本地文件发送到外部设备被记录。

是否记录打印行为：勾选则打印行为被记录。

如下图所示：

探针记录规则

是否记录上网活动: <input checked="" type="checkbox"/>	是否记录剪贴板: <input checked="" type="checkbox"/>
是否记录usb: <input checked="" type="checkbox"/>	是否记录数据库: <input checked="" type="checkbox"/>
是否记录QQ: <input checked="" type="checkbox"/>	是否记录邮件: <input checked="" type="checkbox"/>
是否记录文件操作: <input checked="" type="checkbox"/>	是否记录远程运维: <input checked="" type="checkbox"/>
是否记录按键: <input checked="" type="checkbox"/>	是否记录网页敏感内容: <input checked="" type="checkbox"/>
是否记录操作标签: <input type="checkbox"/>	是否记录微信: <input checked="" type="checkbox"/>
是否记录文档编辑: <input type="checkbox"/>	是否记录文件外发: <input checked="" type="checkbox"/>
是否记录POST报文: <input type="checkbox"/>	是否记录打印行为: <input type="checkbox"/>

报文触发规则：

触发网址：填写需要触发 post 报文的网址。

排除 url 后缀名：添加的后缀名的报文将不会被记录。

内容类型：选择类型后，get 的报文记录会记录报文详情（目前只对 IE 浏览器生效）。

限制报文大小：限制获取报文最长字节长度。

如下图所示：

**报文触发规则**

报文类型:	<input checked="" type="checkbox"/> POST	<input checked="" type="checkbox"/> GET	<input type="checkbox"/> PUT	<input type="checkbox"/> DELETE
触发网址:	空则不记录, **所有			
示例:	www.baidu.com			
<b>添加</b> <b>移除</b>				
内容类型:	<input type="checkbox"/> text/html <input checked="" type="checkbox"/> application/json			
排除URL后缀名:	<input type="checkbox"/> .JPG <input type="checkbox"/> .png <input type="checkbox"/> .jpeg <input type="checkbox"/> .gif <input type="checkbox"/> .bmp <input type="checkbox"/> .css <input type="checkbox"/> .js			
示例:	.jpg			
<b>添加</b> <b>移除</b>				
限制报文大小:	5000			

工作效率分析规则:

是否启用: 勾选则效率明细才会记录数据。

是否启用在线非活跃: 勾选则效率明细的在线非活跃才会记录数据。

是否记录软件输入: 勾选则工作效率明细记录软件操作时间。

待机时长: 网页/应用打开不操作, 效率明细会记录一条网页/应用打开所用的时长+待机时长的数据。

最大记录时长: 每条效率明细数据记录的操作时长不会大于最大记录时长。

如下图所示:

**工作效率分析规则**

是否启用:	<input type="checkbox"/>
是否记录软件输入:	<input type="checkbox"/>
* 待机时长:	120
是否启用在线非活跃:	<input type="checkbox"/>
* 最大记录时长:	600

录像触发规则:

是否启用录像按键: 勾选则配置的按键键值操作才会录像。

触发录像按键键值: 可以添加或移除按键键值, 被添加的按键才能触发录像。

组合键：同时按组合键可以触发录像并产生按键记录。

录像按键间隔：配置按键间隔 N 毫秒，那么在 N 毫秒内所有操作只录像 1 帧。

如下图所示：

The screenshot shows the 'Recording Trigger Rules' configuration interface. It includes a checkbox for enabling recording via keyboard, a list of trigger keys (Mouse Left Click, Mouse Right Click, Enter, Alt, Delete, 1, 5), a key input field, and a section for defining key combinations. A note at the bottom specifies a recording interval of 1 millisecond.

文件上传：

是否启用：勾选则配置的文件类型后缀规则才会生效。

文件类型后缀：可以添加或删除文件类型（被添加的文件类型后缀才能触发记录）。

文件大小：只记录配置的大小内的文件。

注：启用文件上传功能，则文件敏感词，微信文件敏感词，QQ 文件敏感词，邮件文件敏感词才会触发。

如下图所示：

The screenshot shows the 'File Upload' configuration interface. It includes a checkbox for enabling file upload, a list of supported file extensions (.txt, .doc, .docx, .xls, .xlsx, .ppt, .pptx, .pdf), a sample file input field, and a size limit configuration (50 MB).

二次认证：

是否认证：勾选则二次认证登录生效，还需配置认证范围。

域：支持域用户二次认证，支持多个域（配置域才可以使用域用户二次认证登录）。

认证范围：只有在此范围内的才会进行二次认证（\*支持所有，空则不会二次认证）。

添加二次认证范围。输入机器名，和用户名，点击添加“按钮”。

移除二次认证范围：先选择认证范围中的用户，然后点击“移除”按钮移除（支持多选

按住 **Ctrl** 进行多选)。

二次认证

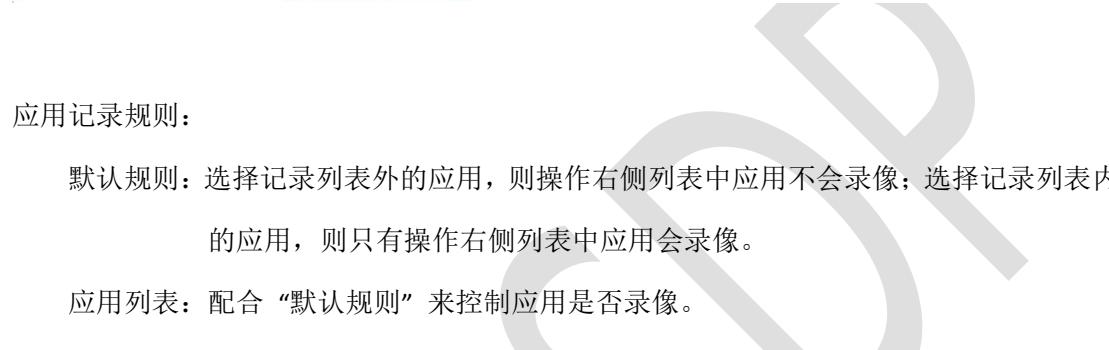
是否认证:

域:

认证范围:

机器名  用户名

添加



应用记录规则:

默认规则: 选择记录列表外的应用, 则操作右侧列表中应用不会录像; 选择记录列表内的应用, 则只有操作右侧列表中应用会录像。

应用列表: 配合“默认规则”来控制应用是否录像。

应用记录规则

默认规则:  记录列表外的应用  记录列表内的应用

应用列表:

记录列表外的应用 (526 项)

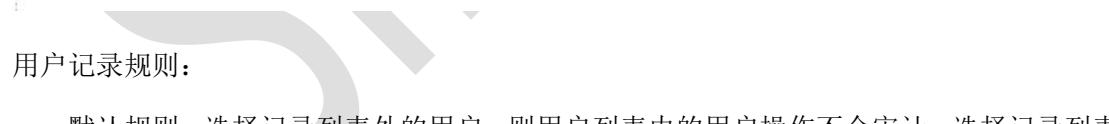
请输入搜索内容

2345好压 (HaoZip)  
 2345安全卫士中心  
 2345游戏大厅  
 2345王牌输入法  
 2345软件管家

记录列表内的应用 (2 项)

请输入搜索内容

2345加速浏览器  
 2345CEFRender



用户记录规则:

默认规则: 选择记录列表外的用户, 则用户列表内的用户操作不会审计, 选择记录列表内的用户, 则只有用户列表内的用户操作会审计。

用户列表: 配合“默认规则”来控制用户操作是否被审计。

### 用户记录规则

默认规则：  记录列表外的用户  记录列表内的用户

用户列表：

(支持\*匹配所有) 示例:DESKTOP/Administrator

### 2.22.2 编辑 Windows 记录策略

点击“编辑”按钮进行编辑 Windows 记录策略。如下图所示：

名称	是否启用	二次认证	描述	操作
默认	启用	禁用	gdb	<input type="button" value="编辑"/> <input type="button" value="复制"/>
bh	启用	禁用		<input type="button" value="编辑"/> <input type="button" value="复制"/>
tt	启用	禁用		<input type="button" value="编辑"/> <input type="button" value="复制"/>
viki记录策略	启用	禁用		<input checked="" type="button" value="编辑"/> <input type="button" value="复制"/>
hbo记录策略	启用	禁用	111	<input type="button" value="编辑"/> <input type="button" value="复制"/>
FHT记录策略	启用	禁用		<input type="button" value="编辑"/> <input type="button" value="复制"/>
yuxq安全策略	启用	禁用	123	<input type="button" value="编辑"/> <input type="button" value="复制"/>
Default_Policy	启用	禁用	默认已禁策略	<input type="button" value="编辑"/> <input type="button" value="复制"/>

### 2.22.3 删除 Windows 记录策略

勾选要删除的 Windows 记录策略，点击“删除”按钮删除记录（默认记录策略和被绑定的记录策略无法删除）如下图所示：

The screenshot shows a list of Windows log strategies. One entry, 'ttt', is selected and highlighted with a red box. A confirmation dialog box is displayed in the center, containing the text '确认删除' (Delete confirmed) and '是否删除选中数据?' (Delete selected data?).

名称	是否开启	二次认证	描述	操作
默认	启用	禁用	gds	编辑 复制
kh	启用	禁用		编辑 复制
ttt	启用	禁用		编辑 <b>复制</b>
ark日志策略	启用	禁用		编辑 复制
hui日志策略	启用	禁用	111	编辑 复制
FHT日志策略	启用	禁用		编辑 复制
yunx安全策略	启用	禁用	123	编辑 复制
Default_Policy	启用	禁用	默认日志策略	编辑 复制

## 2.22.4 复制 Windows 记录策略

选择一个策略，点击“复制”按钮，可以复制一条除了名称不同，其它所有内容都相同的记录策略且被终端组绑定后可以正常使用；如下图所示。

The screenshot shows the same list of Windows log strategies as the previous one. The 'ttt' entry is selected and highlighted with a red box. The 'Copy' button in the '操作' (Operation) column for this row is also highlighted with a red box.

名称	是否开启	二次认证	描述	操作
默认	启用	禁用	gds	编辑 复制
kh	启用	禁用		编辑 复制
<b>ttt</b>	启用	禁用		编辑 <b>复制</b>
ark日志策略	启用	禁用		编辑 复制
hui日志策略	启用	禁用	111	编辑 复制
FHT日志策略	启用	禁用		编辑 复制
yunx安全策略	启用	禁用	123	编辑 复制
Default_Policy	启用	禁用	默认日志策略	编辑 复制

## 2.23 Windows 安全策略

Windows 安全策略：控制终端的水印显示、非法应用阻断、非法网页阻断。

### 2.23.1 Windows 安全策略列表

选择平台>终端策略>Windows 安全策略”；可以输入策略名称查询。如下图所示：

Windows安全策略				
名称	状态	水印名称	描述	操作
默认	启用			<a href="#">编辑</a> <a href="#">复制</a>
hh	禁用			<a href="#">编辑</a> <a href="#">复制</a>
1111	禁用	1111		<a href="#">编辑</a> <a href="#">复制</a>
xrl安全策略	启用	无		<a href="#">编辑</a> <a href="#">复制</a>
hb安全策略	启用	华夏源科		<a href="#">编辑</a> <a href="#">复制</a>
yuan安全策略	启用			<a href="#">编辑</a> <a href="#">复制</a>
Default_Security_Policy	启用		默认安全策略	<a href="#">编辑</a> <a href="#">复制</a>

## 2.23.2 新建 Windows 安全策略

点击“新建”按钮，添加安全策略，部分配置移至敏感信息安全策略中。

基础配置：

名称：安全策略名称；此项为必填项。

描述：对安全策略的描述。

启用：安全策略的状态，勾选则策略生效（注：不勾选则水印功能，应用阻断，网页阻断都不会生效）。

基础配置

* 名称：	FHT安全策略2021101418145866_bak
描述：	FHT策略
启用：	<input checked="" type="checkbox"/>

水印配置：

应用水印启用：勾选则应用显示水印（前提此安全策略是启用状态）。

桌面水印启用：勾选则桌面显示水印（前提此安全策略是启用状态）

建议应用水印或桌面水印只开启其一。

水印名称：自定义命名。

水印显示日期：勾选则水印显示当日日期。

水印行间隔：水印的行间隔大小。

水印列间隔：水印的列间隔大小（提示：列间距只对应用水印生效）

水印倾斜角度：水印的倾斜角度大小。

水印字体高度：水印的字体大小。

水印深度：深度配置越大，显示的效果越明显。

水印字体颜色：水印的字体颜色显示。

显示账户：勾选则水印显示账户信息。

如下图所示：

水印配置

应用水印启用：

桌面水印启用： 此功能启用只对桌面生效

水印名称：

水印显示日期：

\* 水印行间隔：

\* 水印列间隔：

此功能只在应用水印启用生效

水印倾斜度：

应用水印建议只选择0,5,10,15四个选项(其他水印负数也可选择)

\* 水印字体高度：

\* 水印深度：

输入值为0到255的整数

水印字体颜色：

显示账户：

水印账户格式：勾选则水印账户就会以终端名/用户的格式显示。

账户列表：只有被添加到列表内的账户才会显示水印。

IP 端范围：对指定 IP 端范围内的终端显示水印。

水印账户格式：  格式：域/主机

账户列表：

AMDIN-PC/amdin

添加 移除

IP端范围：

提示：多个IP段以英文逗号分割，如

192.168.2.0/24,192.168.2.1/24

应用水印进程：此功能只在应用水印启用生效。

默认规则：选择白名单，则只显示右侧进程列表内的应用水印；选择黑名单，则不显示右侧进程列表内的应用水印。

进程列表：可以选择进程，点击“>”“<”按钮进行黑白名单分类。

进程列表的进程是在应用列表模块获取。

应用水印进程（此功能只在应用水印启用生效）

\* 默认规则： 白名单 黑名单

进程列表： 774 项

请输入搜索内容

- 2345Associate.exe
- 2345CEFRender.exe
- 2345Explorer.exe
- 2345ExplorerAssista...
- 2345GameHall.exe

非法应用程序：

2 项

- WeChat.exe
- DingTalk.exe

默认规则：选择禁用列表外的应用，则只有右侧列表内的应用可以打开使用；选择禁用列表内的应用，则右侧列表内的应用不可以打开使用

应用列表：选择应用，点击“>”“<”按钮进行黑白名单分类。



非法访问 web 网址：

默认规则：选择禁用列表外的网站，则只能使用列表内的网站。

选择禁用列表内的网站，则列表内的网站不能使用。

跳转规则：选择本地跳转，访问非法网页阻断后，提示的是本地相关信息。

选择服务端跳转，访问非法网页阻断后，提示的是服务端相关信息。

网站列表：可添加可移除需要被阻断的非法网站。



### 2.23.3 编辑 Windows 安全策略

点击“编辑”进行编辑安全策略。如下图所示：

### 2.23.4 删除 Windows 安全策略

勾选要删除的安全策略，点击“删除”按钮删除记录（默认安全策略不可删除）如下图所示：

The screenshot shows a web-based management platform with a dark header bar containing tabs: 行为审计, 编辑信息, 风险分析, 工作效率, 平台 (Platform), and a user icon labeled 'admin'. The main content area has a sidebar on the left with categories like 监控, 终端, 终端升级, 终端组, 终端策略, Windows记录策略, Windows安全策略, Linux记录策略, Linux安全策略, 选项, 启动配置, and 服务器. The 'Windows安全策略' section is currently selected. A search bar at the top of this section allows for模糊搜索 (fuzzy search). Below it is a table listing security policies:

名称	状态	备注	操作
默认	启用		编辑 复制
hh	启用		编辑 复制
1111	启用	1111	编辑 复制
xxk安全策略	启用	无	编辑 复制
hh安全策略	启用	华夏医科	编辑 复制
yuan安全策略	启用		编辑 复制
Default_Security_Policy	启用	默认安全策略	编辑 复制

At the bottom right of the table, there are pagination controls: 共7条, 1/1, 20条/页.

## 2.23.5 复制 Windows 安全策略

选择一个策略，点击“复制”按钮，可以复制一条除了名称不同，其它所有内容都相同的安全策略且被终端组绑定后可以正常使用；如下图所示。

This screenshot is identical to the one above, but the 'Copy' button for the 'Default\_Security\_Policy' row is highlighted with a red box. All other elements, including the table data and navigation controls, remain the same.

## 2.24 Linux 记录策略

Linux 记录策略：控制 Linux 终端的用户录像、视频离线缓存大小、二次认证、高危命令授权账号。

### 2.24.1 Linux 记录策略列表

选择“平台”->“终端策略”->“Linux 记录策略”；输入记录策略的名称模糊可进行查询。如下图所示：

## 2.24.2 新建 Linux 记录策略

点击“新建”按钮创建 Linux 记录策略。

基础配置：

策略名称：此项为必填项。

描述：可以描述此策略。

是否录像：控制 Linux 终端是否录像。勾选则录像，可以查看录像回放。

(注：只对 Linux 桌面会话有效)

是否显示隐私声明：4.9Linux 终端暂时不支持此功能。

图像格式：录像的图像颜色。**此选项只有在勾选了“是否录像”才生效**

离线缓存视频大小：终端离线后，录像视频最大保存的大小。

录制密度：开启录制密度；打开 Linux 终端桌面不操作只要有画面变化就会录屏；

为空是不开启录制密度。

基础配置

* 策略名称:	ttt记录策略202110271727255,	描述:		
是否录像:	<input checked="" type="checkbox"/>	是否显示隐私声明:	<input checked="" type="checkbox"/>	
* 图像格式:	灰度图像	彩色图像	隐私声明内容:	搞定撒
* 离线缓存视频大小:	50	录制密度(秒):	1	

二次认证、高危命令授权账号：怎么使用详见\\192.168.2.4\发布版本及文档\Auditsys4.9  
发布\01\_发布文档汇总-4.9 的《08\_Auditsys4.9 LinuxAgent 操作手册-v1.1.doc》。

## 2.24.3 复制 Linux 记录策略

选择一个策略，点击“复制”按钮，可以复制一条除了名称不同，其它所有内容都相同的记录策略且被终端组绑定后可以正常使用。

## 2.25 Linux 安全策略

Linux 安全策略：控制 Linux 终端非法命令阻断、高危命令阻断。

非法命令阻断和高危命令阻断区别：高危命令阻断账号授权后，可以正常输入高危命令。

### 2.25.1 Linux 安全策略列表

选择“平台>终端策略>Linux 安全策略”，可以输入策略名称查询。如下图所示：

名称	是否启用	二次认证	描述	操作
yu	启用	禁用	123	<a href="#">编辑</a> <a href="#">复制</a>
Default_Policy	启用	禁用	Linux默认策略	<a href="#">编辑</a> <a href="#">复制</a>

### 2.25.2 新建 Linux 安全策略

点击“新建”按钮创建 Linux 安全策略。

基础配置：

名称：必填项。

描述：对 Linux 安全策略描述。

启用：勾选则策略生效。

非法命令阻断、高危命令阻断：怎么使用详见\\192.168.2.4\发布版本及文档\\Auditsys4.9 发布\01\_发布文档汇总-4.9 的《08\_Auditsys4.9 LinuxAgent 操作手册-v1.1.doc》。

基础配置

\* 名称: 指定授权

描述: 指定撤

启用:

日志命令阻断

正则列表: dpkg 防御命令的正则表达式:  
rpm 防御命令的正则表达式:

添加 移除

高危命令阻断

正则列表: touch 正则表达式

取消 提交

### 2.25.3 复制 Linux 安全策略

复制 Linux 安全策略步骤参考复制 Linux 记录策略步骤 3.10.2。

## 2.26 部门

部门是对终端进行部门分类管理。

选择“平台>组织>部门”进入部门界面，如下图所示：

行为审计 策略信息 风险分析 工作效率 平台 部门

新增组织公司 新建部门 批量导入

当前选择: 请插入部门名称

部门

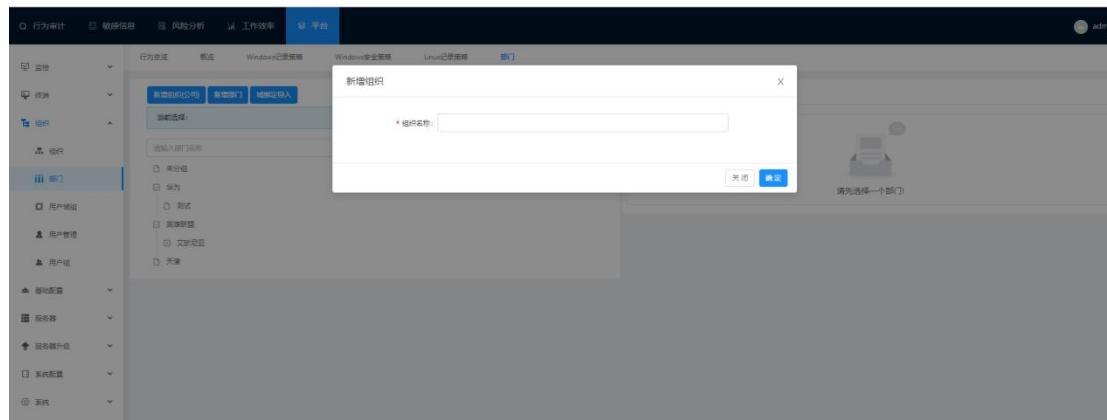
- 华为
- 测试
- 英雄联盟
- 艾伦西亚
- 天津

基本信息

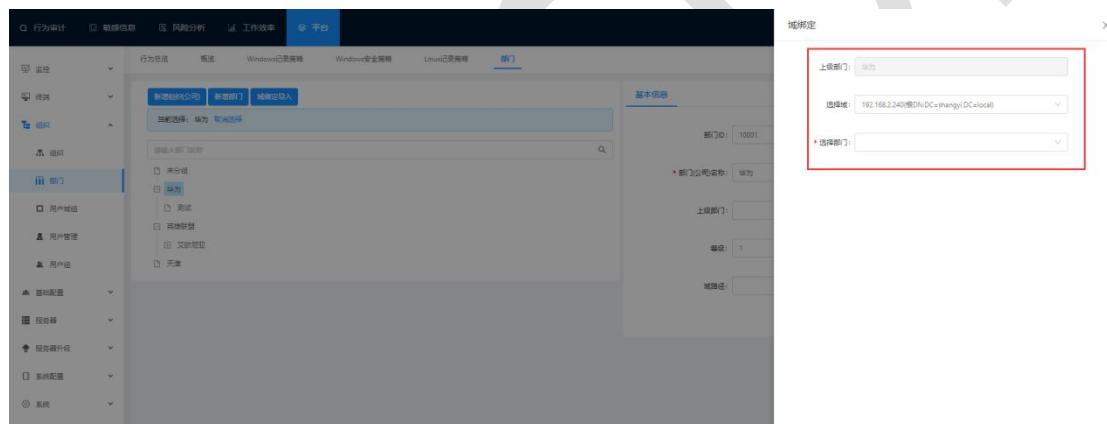
请先选择一个部门

## 2.26.1 新建部门

点击“新增组织（公司）、新增部门、域绑定导入”按钮可以新增公司、部门；新增部门必须先新增公司，支持多层级关系；如下图所示：

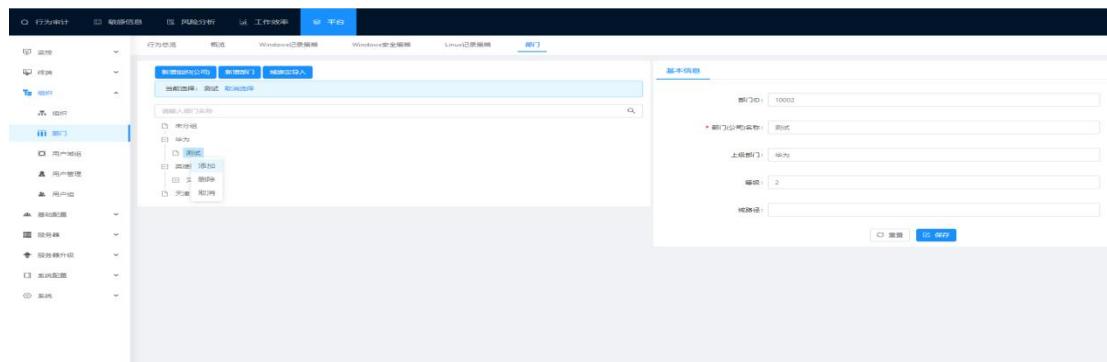


域绑定导入是导入域部门，需先配置域配置（详见步骤 2.7 域配置）；如下图所示：



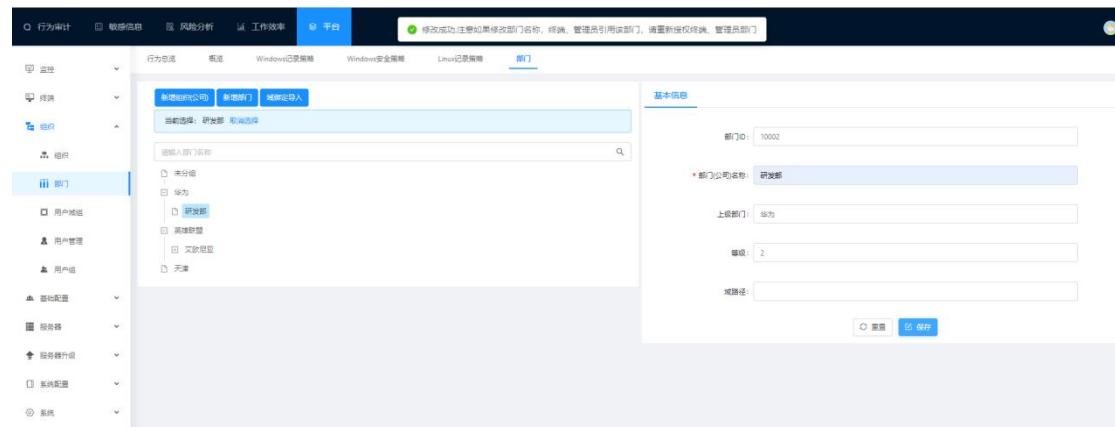
## 2.26.2 删除部门

选择要删除的部门；右键鼠标弹出“删除”按钮；再点击“删除”按钮（已绑定终端的部门信息不可删除，删除会弹出相应提示）如下图所示：



## 2.26.3 编辑部门

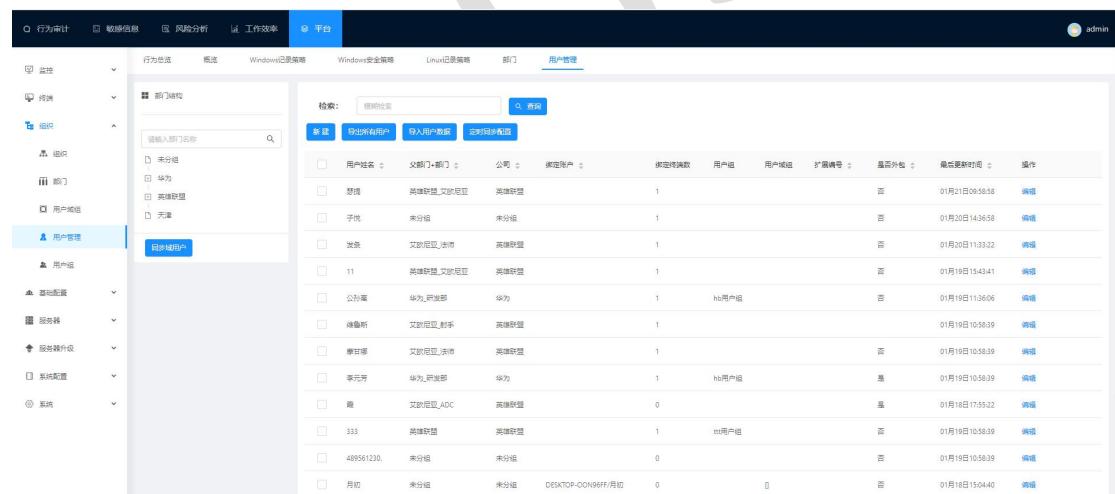
选择要编辑的部门，点击部门名称，在右侧进行编辑；编辑成功会弹出相应提示；如图下所示：



## 2.27 用户管理

用户管理是给终端关联用户信息。

选择“平台>组织>用户管理”进入用户管理界面；如下图所示：



## 2.27.1 新建用户

点击“新建”按钮进行新增用户；如下图所示：

绑定关系：

部门：选择要绑定的部门（需先新建部门；详见部门步骤 3.12）

真实姓名：输入用户姓名。

公司：选择要绑定的公司（需先新建公司；详见部门步骤 3.12）

扩展编号：输入扩展编号。

账户：绑定终端的登录账户信息。

用户组：选择要绑定的用户组（需先新建用户组）

用户域组：选择要绑定的用户域组。

关联 agent：只有终端关联了此用户信息，才会显示 agent 信息（新建的用户关联 agent 信息为空）

## 2.27.2 导出用户

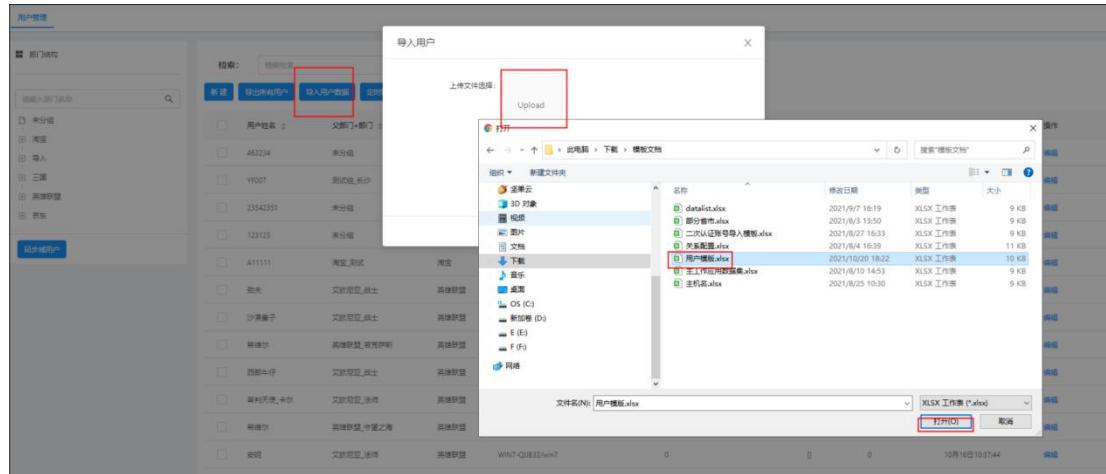
导出所有用户是导出所有用户信息以 excel 表展示。

点击“导出所有用户”按钮，导出用户信息；如下图所示：

## 2.27.3 导入用户

导入用户数据是可以把在 excel 编辑好的用户信息导入到用户管理。

点击“导入用户数据”按钮，上传已编辑好的用户信息的文件进行导入（已存在的用户信息不可导入；没有所匹配的公司部门信息导入成功后绑定到“未分组”部门）如下图所示：



## 2.27.4 定时同步配置

定时同步配置：

是否定时同步域部门用户数据：勾选，则每半小时同步更新一次域部门用户信息数据（需先配置域配置；详见域配置的步骤 2.7）

是否定时同步域组用户数据：勾选，则每半小时同步更新一次域组用户信息数据（需先配置域配置，详见域配置的步骤 2.7 和导入相应的用户域组信息）

使用账号作为姓名自动创建用户：勾选，则终端注册上报时，会自动根据终端的登录账户创建一个用户且绑定此终端。

点击“定时同步配置”按钮；弹出定时同步配置窗口；如下图所示：

## 2.27.5 批量操作用户

批量操作用户是可以对多用户进行批量绑定用户组、批量绑定用户域组、批量删除用户。

选择要批量操作的用户进行批量操作；如下图所示：

## 2.27.6 同步域用户

同步域用户：把域部门下的域用户同步到用户管理。

选择域部门，点击“同步域用户”按钮进行同步（选择普通部门，点击同步域用户不生效）如下图所示：

平台 > 组织 > 用户组

用户名	部门	公司	锁定账户	锁定操作数	用户组	用户或组	扩展编号	是否外包	最后更新时间	操作
公孙离	华为_研发部	华为	1	1	h3用户组			否	01月19日11:36:06	<a href="#">编辑</a>
李元芳	华为_研发部	华为	1	1	h3用户组			是	01月19日10:58:39	<a href="#">编辑</a>
夏姑	华为_研发部	华为	1	1	111			是	01月19日10:58:39	<a href="#">编辑</a>
顾家东	华为_研发部	华为	3	111	111			否	01月19日10:58:39	<a href="#">编辑</a>
NH	华为_研发部	华为	1	111	111			是	01月19日10:58:39	<a href="#">编辑</a>
金克丝	华为_研发部	华为	1	111	111			否	01月19日10:58:39	<a href="#">编辑</a>

## 2.28 用户组

用户组：把风险规则、敏感词规则、时间配置、评分配置、效率分类、用户信息绑定到用户组；只有在此用户组下的用户在终端操作才能触发相应的规则、配置。

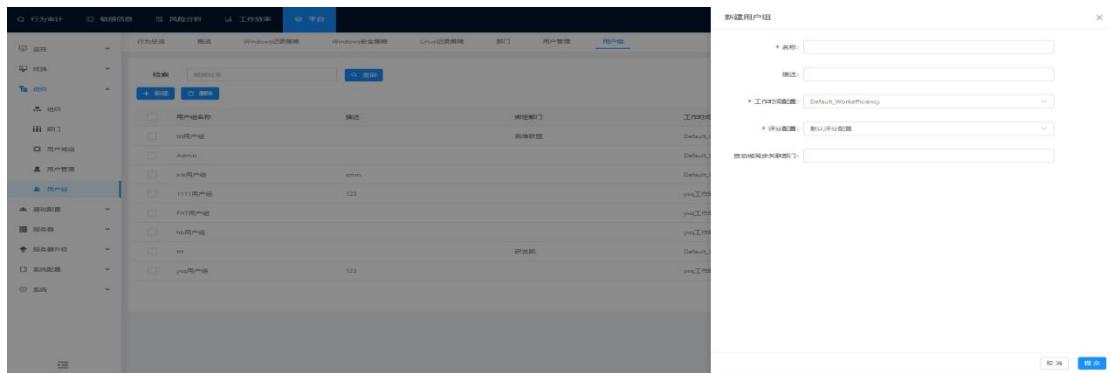
选择“平台>组织>用户组”进入用户组界面；如下图所示：

平台 > 组织 > 用户组

用户组名称	描述	所属部门	工作时间配置	评分配置	操作
ttt用户组		英雄联盟	Default_WorkEfficiency	默认评分配置	<a href="#">编辑</a> <a href="#">用户</a>
Admin			Default_WorkEfficiency	默认评分配置	<a href="#">编辑</a> <a href="#">用户</a>
xmm用户组	xmm		Default_WorkEfficiency	默认评分配置	<a href="#">编辑</a> <a href="#">用户</a>
1111用户组	123		yqq工作时间	默认评分配置	<a href="#">编辑</a> <a href="#">用户</a>
FLHT用户组			yqq工作时间	随机测试	<a href="#">编辑</a> <a href="#">用户</a>
h3用户组			yqq工作时间	默认评分配置	<a href="#">编辑</a> <a href="#">用户</a>
111		研发部	Default_WorkEfficiency	随机测试	<a href="#">编辑</a> <a href="#">用户</a>
yvo用户组	123		yqq工作时间	默认评分配置	<a href="#">编辑</a> <a href="#">用户</a>

### 2.28.1 新建用户组

点击“新建”按钮进行新建用户组；如下图所示：



名称：给用户组命名。

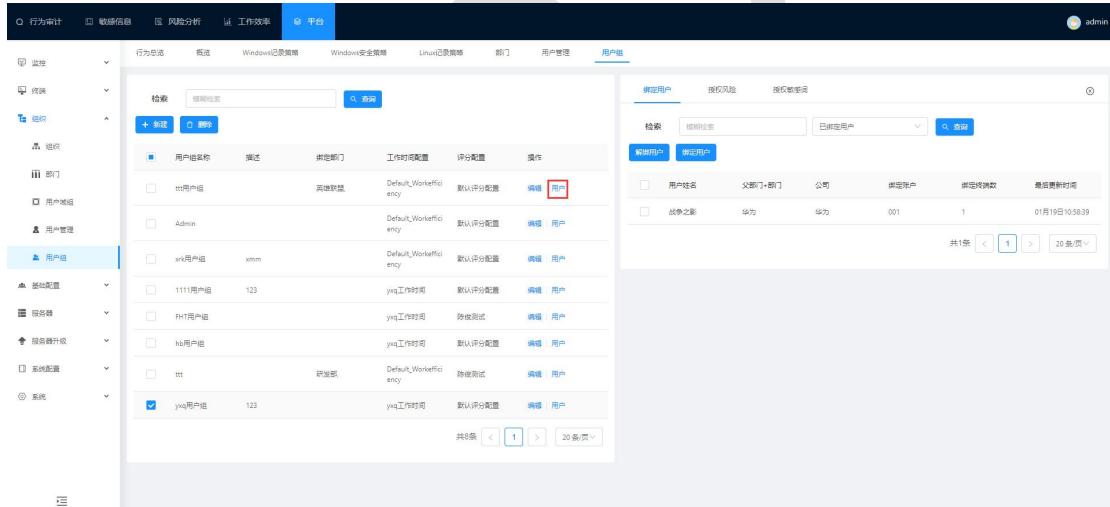
工作时间配置：选择相应的工时时间配置；默认是选择默认的工作时间配置。

评分配置：选择相应的评分配置；默认是选择默认的评分配置。

自动域同步关联部门：选择域部门，在用户管理界面点击同步域用户；才能自动把域部门下的域用户全部绑定到此用户组。

## 2.28.2 用户组绑定关系

点击“用户”按钮，进行用户组绑定；如下图所示：



例如：绑定用户：先查询未分配用户信息；再选择用户信息；点击“绑定用户”按钮进行绑定；（授权风险和授权敏感词借鉴此操作步骤）所下图所示：

The screenshot shows a user management interface with a sidebar containing navigation items like '行为审计', '敏感信息', '风险分析', '工作效率', '平台', '监控', '终端', '组织', '部门', '用户管理', and '用户组'. The '用户组' item is selected. A central search bar has '搜索' and '查询' buttons. Below it is a table with columns: '用户名', '描述', '所属部门', '工作时间配置', '操作'. A modal window titled '确认绑定' asks '是否将选中数据绑定到此组?' with '取消' and '确定' buttons. To the right is another table titled '授权风险' with a search bar '搜索风险' and a dropdown '未分配用户'. A red box highlights the '未分配用户' dropdown. The main table lists several users, including '子悦' which is also highlighted with a red box.

## 2.29 用户域组

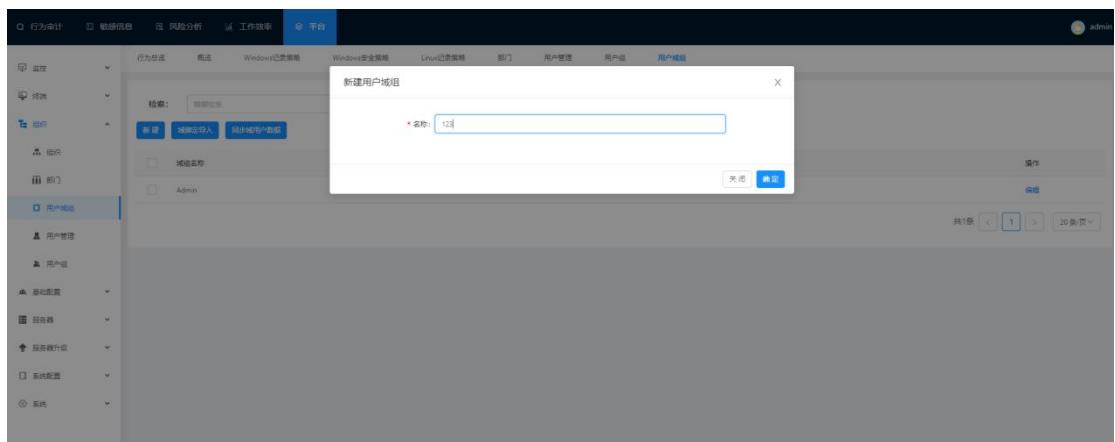
用户域组：对域组下的用户进行管理。

选择“平台>组织>用户域组”进入用户域组界面；如下图所示：

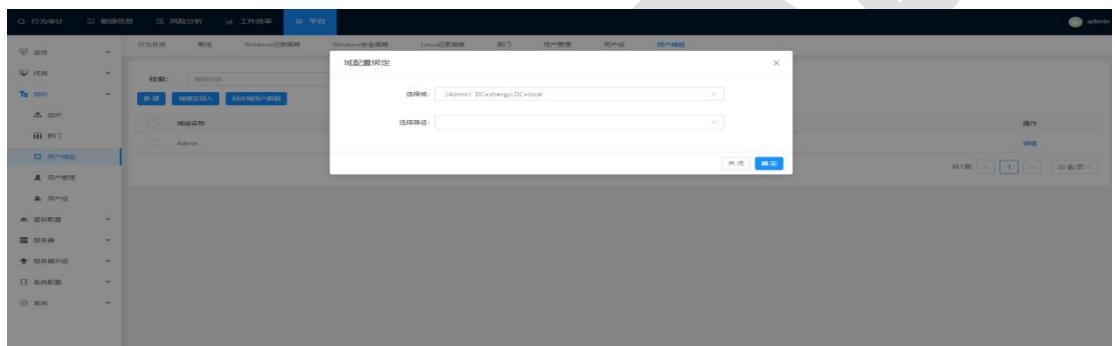
This screenshot shows the 'User Group Management' interface. The sidebar includes '行为审计', '敏感信息', '风险分析', '工作效率', '平台', '监控', '终端', '组织', '部门', '用户管理', and '用户组'. The '用户组' item is selected. The main area contains a search bar with '搜索' and '查询' buttons. Below is a table with columns: '组名名称' and '操作'. It lists one group named 'Admin'. At the bottom, there is a pagination indicator '共1条 < 1 > 20条/页'.

### 2.29.1 新建或导入域组

点击“新建”按钮；可以新建域组；如下图所示：

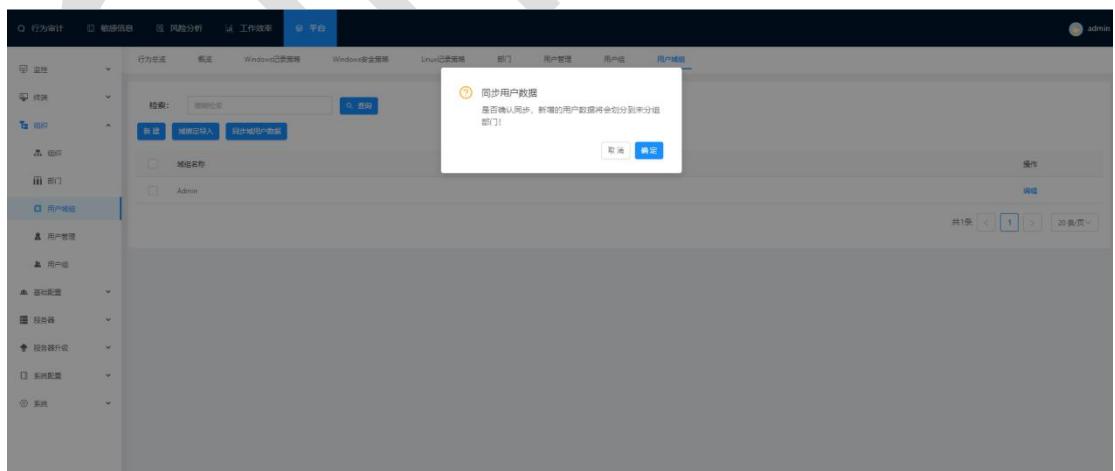


点击“域绑定导入”可以导入用户域组（需先配置域配置；详见域配置步骤 2.6）如下图所示：



## 2.29.2 同步域用户数据

点击“同步域用户数据”按钮可以把域组下的域用户同步到用户管理；如下图所示：

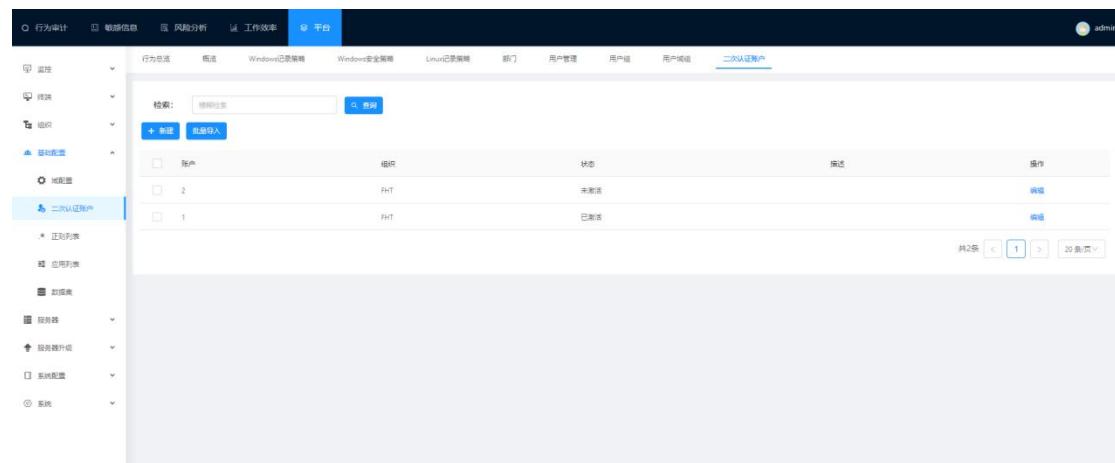


## 2.30 二次认证用户

二次认证用户：是配置终端二次登录的用户信息。

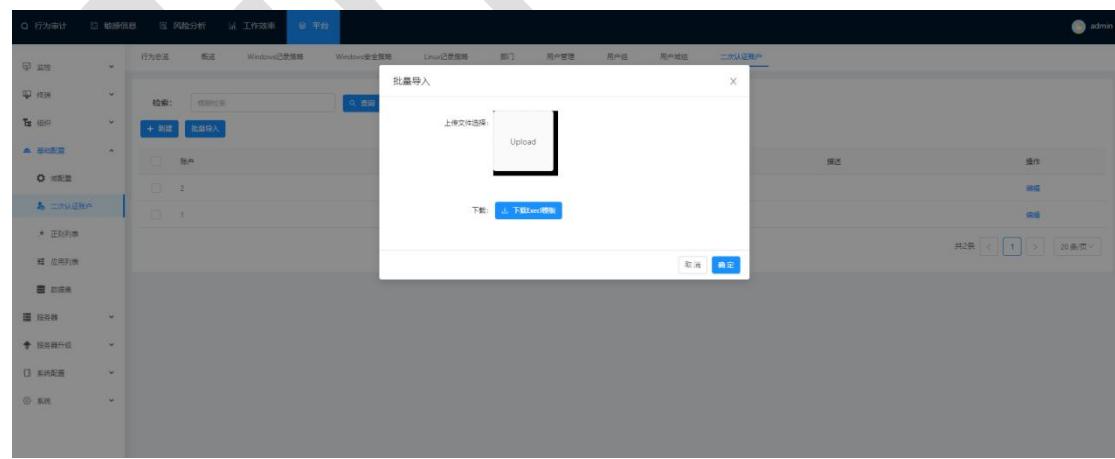
提示：开启二次认证需在 Windows 记录策略勾选是否启用二次认证规则；二次认证用户登录终端操作的行为数据都会审计在此二次认证用户下。

选择“平台>基础配置>二次认证用户”进入二次认证用户界面；如下图所示：



### 2.30.1 新建二次认证用户

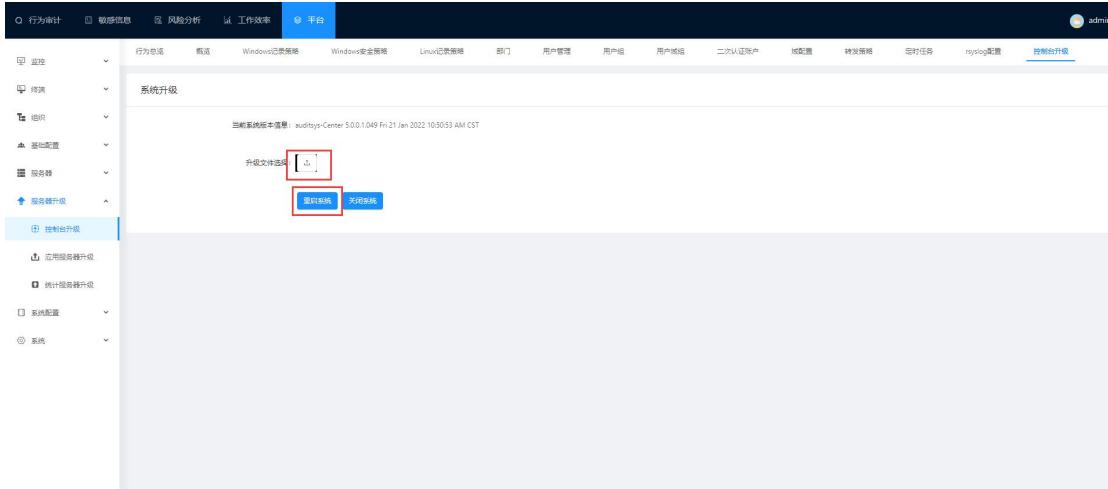
点击“新建”按钮进行新建二次认证用户（需要增加多个二次认证用户，可以选择批量导入）如下图所示：



## 2.31 控制台升级

控制台升级点击上传升级版本的升级压缩包，上传完毕后提示升级成功。之后重启系统

即可。



## 2.32 定时任务

### 2.32.1 定时任务列表

定时任务列表展示所有定时器任务详情。

任务名	表达式	处理器	最近执行时间	执行结果	描述	操作
发送邮件报告	0 17 * * *	SendEmailReport	2022-01-21 15:00:26	执行成功	每四五分钟执行一次	执行一次
计划任务启动与清理	0 5 * * *	AgentCreateSessionSet			每六个小时执行	执行一次
清理文件夹的垃圾	0 0 2 * * ?	ClearSDData			每天凌晨执行	执行一次
健康报告	0 0 0 * * ?	HealthReport			每天三点半执行	执行一次
同步计划	55 * /30 * * * ?	AutosyncUser	2022-01-21 15:00:55	执行成功	每分钟30秒执行	执行一次
释放内存	0 0 2 * * ?	LastTimeReleaseAgent			每六个小时执行	执行一次
检测下载	35 * /2 * * * ?	DownloadVideo	2022-01-21 15:02:35	执行成功	每分钟2秒执行	执行一次
过期检测	0 0 1 * * ?	LoopCheck			每天1点执行	执行一次
计划任务更新	45 * /5 * * * ?	UpdateAgentOfflineLastTime	2022-01-21 15:00:45	执行成功	每五秒钟执行	执行一次
清除数据	23 * * * * ?	AgentWarmingSend	2022-01-21 15:00:35	执行成功	每四分钟执行一次	执行一次
关闭会话	25 0 1 * * ?	EndSession	2022-01-21 15:00:25	执行成功	每小时执行一次	执行一次
清理日志	15 0 12 * * ?	ClearData	2022-01-21 14:00:16	执行成功	每两小时执行	执行一次
清理脚本缓存	10 15 * * * ?	SendReport	2022-01-21 15:00:10	执行成功	每四五分钟执行一次	执行一次

### 2.31.1 定时任务启动

定时任务手动启动/定时任务重启。

任务名	表达式	处理器	最长执行时间	执行结果	描述	操作
发送SDP邮件报告	10/5 * * * ?	SendSDPReport	2022-01-21 15:00:28	执行成功	每隔五分钟执行一次	执行一次
规程灯自动清理	0 5 * * ?	AgentCreateSessionSet			每天两点五分执行	执行一次
清理文件归档数据	0 0 2 * * ?	ClearSDPData			每天两点执行	执行一次
健康报告	0 0 3 * * ?	HealthReport			每天三点半执行	执行一次
同步部门、域组	55/10 * * * ?	AutoSyncUser	2022-01-21 15:00:55	执行成功	每隔30分钟执行	执行一次
释放资源	0 0 2 * * ?	LastTimeReleaseAgent			每天两点执行	执行一次
视频下载	35 * 2 * * * ?	DownloadVideo	2022-01-21 15:00:35	执行成功	每隔两分钟执行	执行一次
过期检查	0 0 1 * * ?	LoopCheck			每天一点执行	执行一次
终端状态更新	45 * 5 * * * ?	UpdateAgentOfflineLastTime	2022-01-21 15:00:45	执行成功	每隔五分钟	执行一次
终端告警	35 * 5 * * * ?	AgentWarningSend	2022-01-21 15:00:35	执行成功	每隔五分钟执行一次	执行一次
关闭会话	25 0 1 * * ?	EndSession	2022-01-21 15:00:25	执行成功	每小时执行一次	执行一次
清理归档	15 0 * 2 * * ?	ClearData	2022-01-21 14:00:16	执行成功	每隔两个小时执行	执行一次
发送邮件报告	10/5 * * * ?	SendReport	2022-01-21 15:00:10	执行成功	每隔五分钟执行一次	执行一次

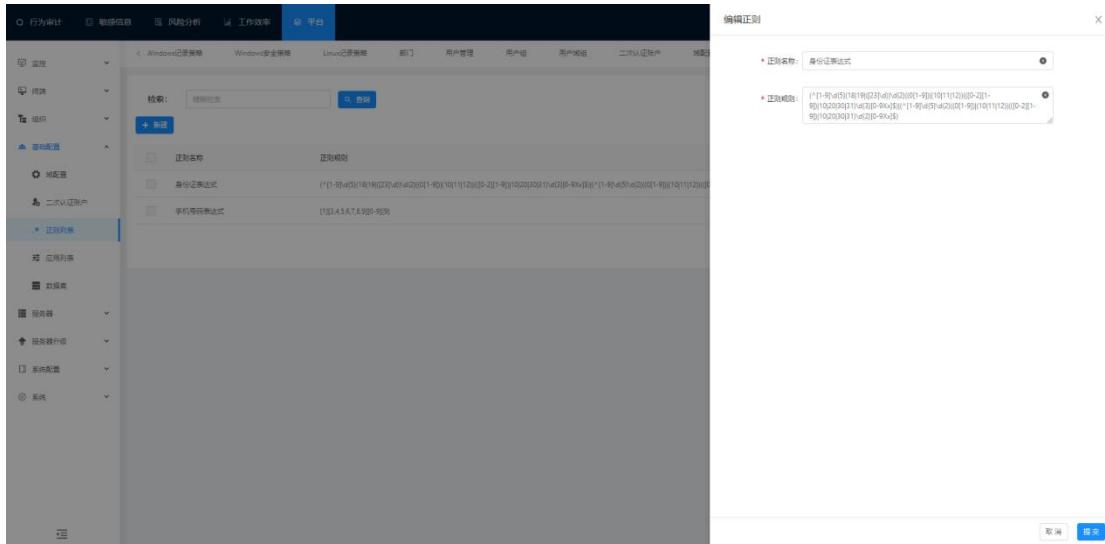
## 2.32 正则列表

### 2.32.1 新增正则列表

点击新增正则列表，填写正则列表名称和正则表达式。提交保存。

正则名称	正则规则
身份证表达式	(^  )([1-9][0-9]{5}[0-9]{4}[0-9]{3}[0-9]{2}[0-9]{1})[0-9]{1}(20 19)[0-9]{2}(1[0-2] 0[1-9])[0-9]{2}(0[1-9] 1[0-2])[0-9]{2}(0[1-9] 1[0-2])[0-9]{2}
手机号码表达式	[13456789]([0-9]{9})

正则列表编辑。



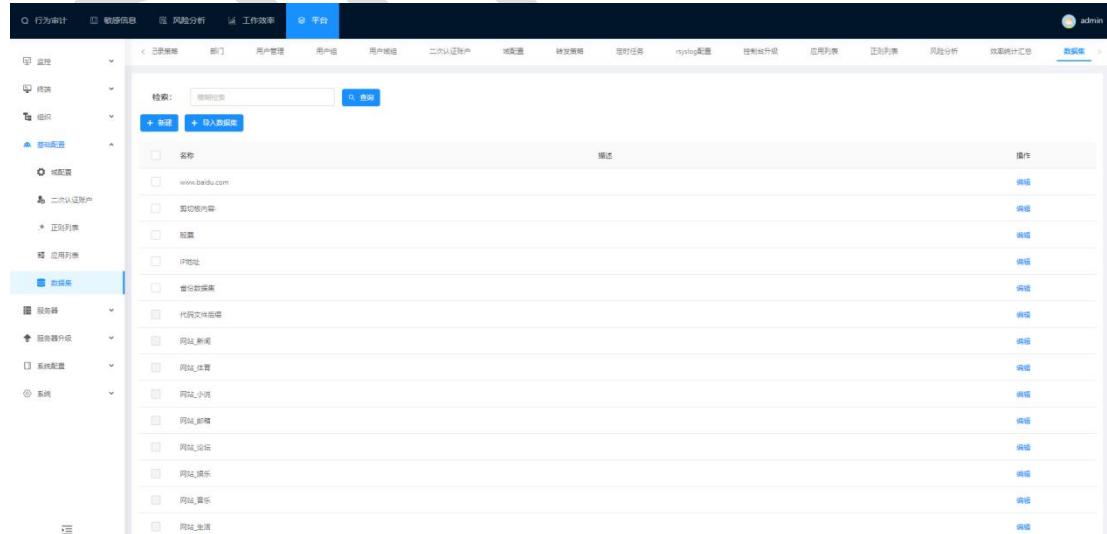
## 三 敏感，风险，工作效率

### 3.1 风险分析

#### 3.1.1 数据集

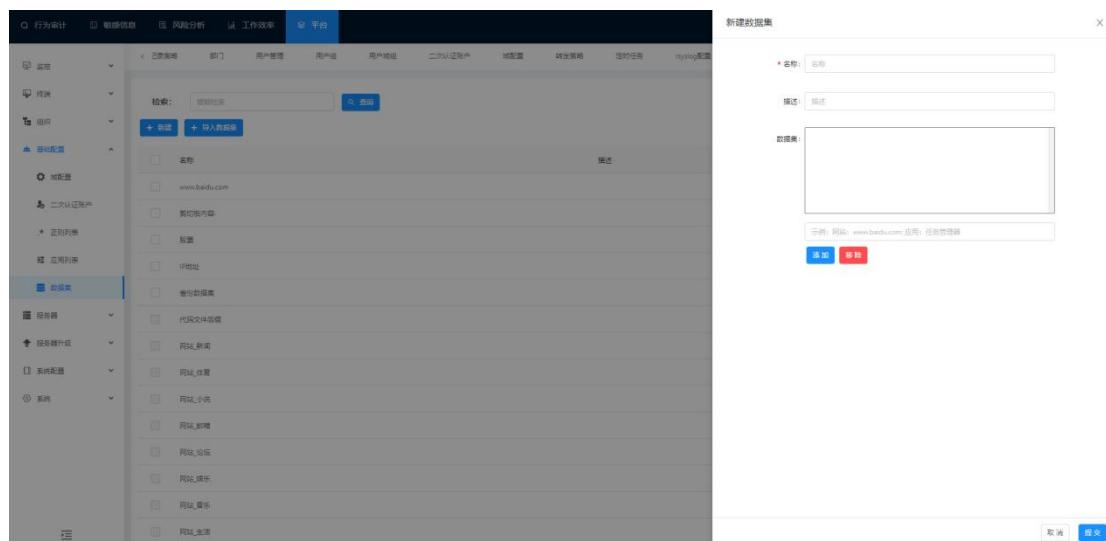
数据集是把数据条件集合起来；可以用于风险行为条件、敏感行为条件、效率分类条件。

选择“配置>应用配置>数据集”进入数据集界面；如下图所示：



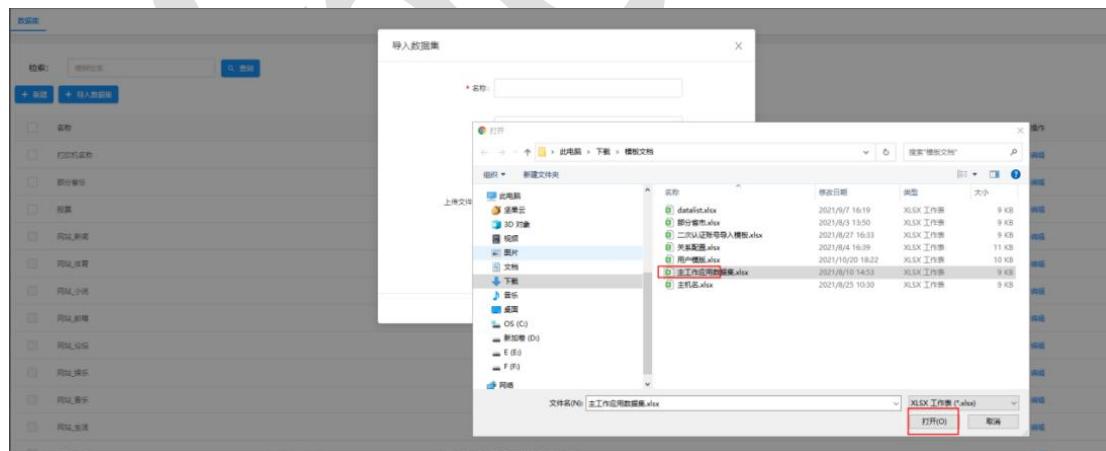
### 3.1.1.1 新建数据集

点击“新建”按钮进行新建数据集（数据集一般是填写网站信息或应用名称信息）如下图所示：



### 3.1.1.2 导入数据集

点击“导入数据集”按钮进行导入数据集（需先下载数据集模板编辑好数据集内容再上传导入）如下图所示：



### 3.1.2 规则类型

规则类型：对风险规则进行分类。

点击“风险分析>规则配置>风险类型”跳转至规则类型界面；在检索输入框输入要查询的检索条件，点击搜索；如下图所示：

The screenshot shows the 'Risk Analysis' section of a web-based management system. At the top, there are tabs for 'Behavior Audit', 'Audit Information', 'Risk Analysis', 'Work Efficiency', and 'Platform'. Below the tabs, there's a navigation bar with links like 'Risk', 'Risk Configuration', 'Risk Rule', and 'Risk Type'. A search bar with placeholder text '搜索: 检测对象' and a 'Search' button are present. A table lists various risk types with columns for 'Name', 'Operation', and 'Action'. The listed items include: FHT Risk Rule, ha Risk, xs Risk, YUQI Risk, Linux Risk Detection Command, Database Rule, Using Port, Executing Unauthorized Shell Command, unix User Operation, Breakthrough Behavior, Executing Unauthorized Shell Command, unix User Operation, Using Dangerous Linux System Operations, Using External Tools, and Executing Unauthorized Management Tasks.

### 3.1.2.1 新建规则类型

点击‘新建’按钮，弹出新建类型窗口界面；如下图所示：

This screenshot shows the 'New Rule Type' dialog box overlaid on the main 'Risk Type' list. The dialog has a title '新建类型' and a single input field labeled '风险类型名称:' with a placeholder '请输入名称' (Please enter name). There are '取消' (Cancel) and '确定' (Confirm) buttons at the bottom right of the dialog.

### 3.1.2.2 编辑规则类型

点击‘编辑’按钮，弹出编辑类型窗口界面

This screenshot shows the 'Edit Rule Type' dialog box overlaid on the main 'Risk Type' list. It is identical in structure to the 'New Rule Type' dialog, with a title '编辑类型' and an input field '风险类型名称:' containing the value 'FHT Risk Rule'. The '取消' (Cancel) and '确定' (Confirm) buttons are also visible.

### 3.1.2.3 删除规则类型

选择一个或多个规则类型，点击‘批量操作’下拉框，再点击‘删除’，如下图所示：

The screenshot shows a list of risk types under the 'Risk Type' tab. Each item has a checkbox next to it. A dropdown menu labeled '操作' (Operation) is open over the first few items, indicating a bulk selection mode. The risk types listed include: FHT Risk Rule, hb Risk, xii Risk, YUXQ Risk, Linux Risk Command, Database Rule, Malicious Use, Unix Shell Command, Malicious Behavior, Executing Shell Command, URL Risk, and Special Unix System Operation.

### 3.1.3 风险规则

风险规则：可以配置终端的行为风险规则

选择“配置>风险配置>风险规则”查看风险规则信息。如下图所示：

The screenshot shows a list of configured risk rules under the 'Risk Rule' tab. The columns include: Rule Name, Status, Last Update, Rule Type, Related User, and Operation. The rules listed are: 打印告警 (Print Alert), 文件外发告警 (File External Transmission Alert), POST投文 (POST Document), 剪切报警 (Cut Alert), 邮件报警 (Email Alert), QQ Risk, hb web Risk, yxxj打印风险 (yxxj Print Risk), yxxj敏感风险 (yxxj Sensitive Risk), yqq敏感风险 (yqq Sensitive Risk), and yqq剪切风险 (yqq Cut Risk). Most rules are marked as '已激活' (Active).

#### 3.1.3.1 风险规则查询

左侧可以输入或选择规则类型进行查询；也可以选择快速过滤、风险级别和输入关键字

进行过滤；点击列表上三角形图案可以字段排序。如下图所示：

The screenshot shows the 'Risk Rule Management' section of a web-based security platform. On the left, there's a sidebar with navigation tabs: '行为审计', '敏感信息', '风险分析', '工作效果', and '平台'. Under '风险分析', the '风险规则' tab is selected. A search bar at the top has a placeholder '过滤' and dropdown options for '日志' (Logs), '用户组' (User Groups), and '规则模型' (Rule Models). Below the search bar are three buttons: '快速过滤' (Quick Filter), '全部规则' (All Rules), and '未激活' (Inactive). A sorting dropdown menu shows '规则' (Rule) as the current sort field, with options '规则名称' (Rule Name), '更新时间' (Last Update), '规则类型' (Rule Type), and '相关用户' (Related User). The main area displays a table of risk rules. Each rule entry includes a checkbox, a red warning icon, the rule name, its status ('已激活' or '未激活'), the last update time, the rule type ('FHT风险规则' or 'YUQI风险'), the related user group ('所有用户组' or '授权1个用户组'), and two buttons: '编辑' (Edit) and '复制' (Copy). The table has columns for '规则' (Rule), '规则名称' (Rule Name), '激活状态' (Activation Status), '更新时间' (Last Update), '规则类型' (Rule Type), '相关用户' (Related User), and '操作' (Operations).

### 3.1.3.2 新建风险规则

The screenshot shows the '新建风险规则' (Create New Risk Rule) dialog box. The background is dimmed to show the underlying 'Risk Rule Management' interface. The dialog has a title bar '新建风险规则' and a close button 'X'. It contains several input fields and dropdown menus:

- \* 规则名称: (必填) (Required field)
- 规则描述: (Optional description)
- \* 规则类别: (必填) (Required category): '至键关键软件'
- \* 操作系统: (必填) (Required operating system): 'Windows'
- 激活状态: (Activation status): '已激活' (Activated) is selected.
- 告警状态: (Alert status): Icons for '低' (Low), '中' (Medium), and '高' (High) severity.
- 用户组: (User Group): '所有用户组' (All User Groups) is selected.
- 事件: (Event): A dropdown menu with a '+' sign to add more events.
- 时间范围: (Time Range): '00:00-23:59'.
- 幕后行为: (Background Behavior): '无操作' (No Operation).

规则详情：

规则名称：此规则的名称。

规则描述：对此规则的描述。

规则类别：对规则进行分类。

操作系统：暂时只支持 windows 系统。

激活状态：规则的状态；“已激活”表示启用规则。

告警级别：代表此风险规则的严重性。

用户组：选择指定用户组，则只有在此用户组的终端用户才能触发此风险。

默认选择所有用户组，则所有终端用户都可以触发风险。

#### 事件：触发此风险规则的条件

先选择事件，然后点击“+”按钮添加条件，可以点“x”删除条件。如下图所示：

提示：例如下图情况：事件选择文件操作事件，条件选择操作属性（可以配置 delete OR rename；OR 是或的意思；下面这个风险只有终端的 IP 是 192.168.3.115 删除或重命名文件才能触发此风险规则）。

事件： 文件操作事件

A	操作属性	包含	delete OR rename	X
B	主机IP	包含	192.168.3.115	X
且	A&&B			

如需自定义，请输入正确格式。例:A&&(B||C)

条件的逻辑关系有：‘包含’，‘不包含’，‘等于’，‘不等于’，‘在...之内（精准）’，‘在...之内（模糊）’，‘在...之外（精准）’，‘在...之外（模糊）’，‘正则表达式’，‘且’，‘或’，‘自定义’；如下图所示：

事件： 剪贴板事件

A	剪贴板内容	包含	可使用 OR 分隔多个值	X
且				

时间范围： 00:00-23:59

多个时间段用英文逗号分隔

\* 事后行为： 无操作

包含  
不包含  
等于  
不等于  
在...之内(精准)  
在...之内(模糊)  
在...之外(精准)  
在...之外(模糊)  
正则表达式

正确格式。例:A&&(B||C)

在...之内：是匹配数据集条件；当数据集内的风险关键词有“湖南”

例如：触发剪切板风险条件是在...之内（模糊）：复制粘贴“我是湖南的”

例如：触发剪切板风险条件是在...之内（精准）：复制粘贴“湖南”

事件： 文件操作事件

A 操作属性 包含 delete OR rename

B 主机IP 包含 192.168.3.115

且 A&&B

如需自定义，请输入正确格式。例:A&&(B||C)

或

时间范围： 自定义

时间范围：代表此风险规则的有效时间段。

事后行为：选择‘通知客户端’，则触发该风险后，会弹出告警提示；选择无操作，则触发该风险，不会弹出告警提示。

### 3.1.3.3 编辑风险规则

点击“编辑”按钮编辑记录策略。如下图所示：

规则名	状态	更新时间	规则类型	相关用户组	操作
new风险规则10月27日18:18:55	已激活	10月27日18:18:56	删除关键软件	所有用户组	<span style="border: 1px solid red; padding: 2px;">编辑</span> <span style="border: 1px solid red; padding: 2px;">删除</span>
new风险规则10月27日18:10:48	已激活	10月27日18:10:49	删除关键软件	所有用户组	<span style="border: 1px solid red; padding: 2px;">编辑</span> <span style="border: 1px solid red; padding: 2px;">删除</span>
new风险规则10月27日17:28:12	已激活	10月27日17:28:13	删除关键软件	所有用户组	<span style="border: 1px solid red; padding: 2px;">编辑</span> <span style="border: 1px solid red; padding: 2px;">删除</span>
linux应用refox	已激活	10月26日17:11:45	删除关键软件	所有用户组	<span style="border: 1px solid red; padding: 2px;">编辑</span> <span style="border: 1px solid red; padding: 2px;">删除</span>
linux启动	已激活	10月26日16:04:23	删除关键软件	所有用户组	<span style="border: 1px solid red; padding: 2px;">编辑</span> <span style="border: 1px solid red; padding: 2px;">删除</span>

### 3.1.3.4 删除风险规则

选择要删除的风险，点击“批量操作”下拉框，再点击“删除”按钮进行风险规则删除。

如下图所示：

The screenshot shows the 'Risk Rule Management' section of a web application. A modal dialog box is centered, asking '确认删除' (Delete Confirmation) and '是否删除选中数据?' (Delete selected data?). Below the dialog, a table lists several risk rules. One rule, '打印机告警', has its checkbox checked and is highlighted with a red border. The table columns include: 规则名称 (Rule Name), 状态 (Status), 更新时间 (Last Update), 规则类型 (Rule Type), 相关用户 (Related User), and 操作 (Operation). The operation column for the selected rule shows '编辑' (Edit) and '复制' (Copy).

### 3.1.3.5 风险激活

选择需要“激活”风险规则，点击“批量操作”下拉框，再“激活”按钮。如下图所示：

This screenshot is similar to the previous one, showing the 'Risk Rule Management' interface. A modal dialog box asks '确认激活' (Activation Confirmation) and '是否激活选中数据?' (Activate selected data?). The table below lists risk rules, with the first rule, 'ssh暴力破解', having its checkbox checked. The table structure is identical to the previous screenshot.

### 3.1.3.6 关闭风险

选择需要“激活”风险规则，点击“批量操作”下拉框，再“激活”按钮。如下图所示：

The screenshot shows a list of risk rules in a table format. A modal dialog box titled "确认关闭" (Confirm Close) is displayed, asking "是否确定选中数据?" (Do you want to delete the selected data?). The table columns include: 规则 (Rule), 规则名称 (Rule Name), 策略状态 (Policy Status), 更新时间 (Update Time), 操作类型 (Operation Type), 相关用户 (Related User), and 操作 (Operation). The data in the table includes various system log entries and command-line activities.

### 3.1.4 风险明细

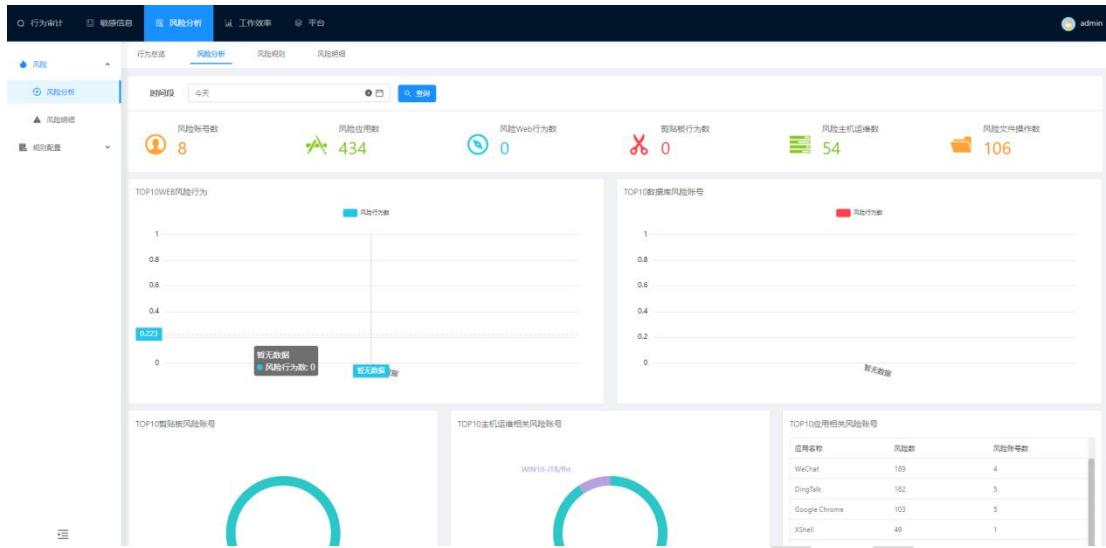
点击“”按钮查看风险明细详情；点击“”播放风险触发定帧，左侧可对风险类型进行筛选，快速过滤如下图所示：

The screenshot shows the Risk Detail interface. It features a search bar at the top and a table below displaying risk events. The table columns include: 事件 (Event), 发生时间 (Occurrence Time), 风险终端名称/IP (Risk Terminal Name/IP), 部门/用户名 (Department/User Name), 操作行为 (Operational Behavior), 风险名称 (Risk Name), 风险类型 (Risk Type), and 操作 (Operation). A red box highlights the "过滤" (Filter) button in the search bar and the "高级过滤" (Advanced Filter) section in the table header. Another red box highlights the "播放" (Play) button in the table header. On the left side, there is a sidebar for "Risk Type" filtering.

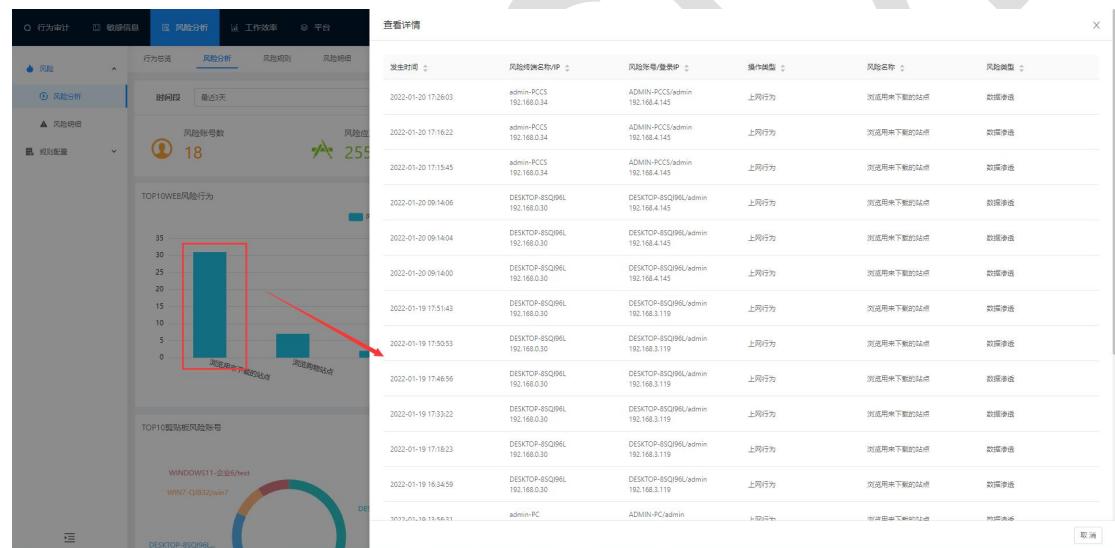
### 3.1.5 风险分析

风险分析是对用户在终端触发的所有风险行为数据进行分析展示。

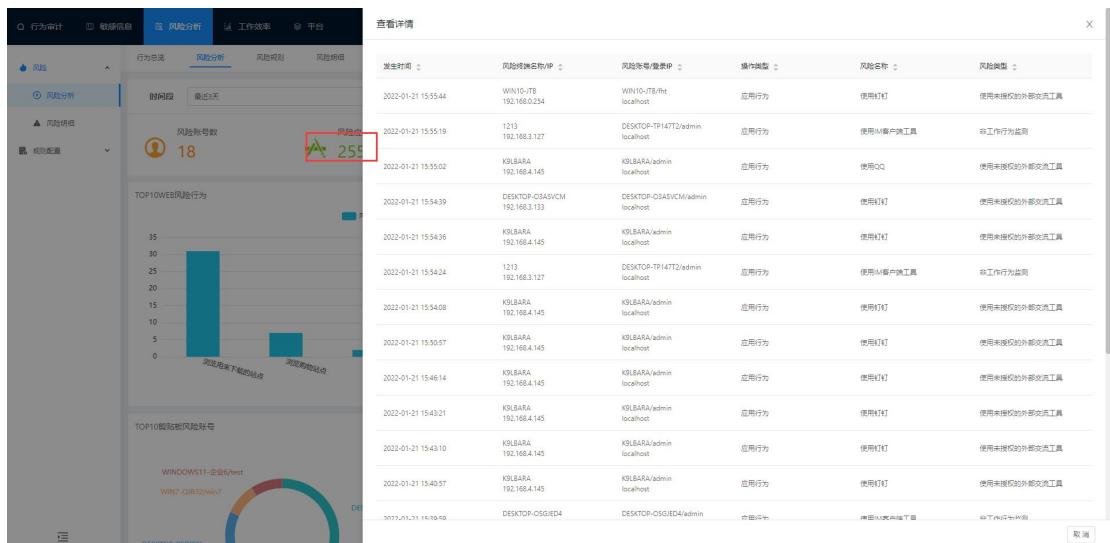
选择“分析>风险>风险分析”；不同风险行为操作统计展示（支持时间段进行过滤查询）  
如下图所示：



风险分析界面所展示的所有风险行为数都可以点击图表弹出风险明细查看详情。例如  
TOP10WEB 风险行为，点击浏览购物站点柱状图，如图所示：



例如：点击风险应用数，查看应用风险明细详情



## 3.2 敏感信息

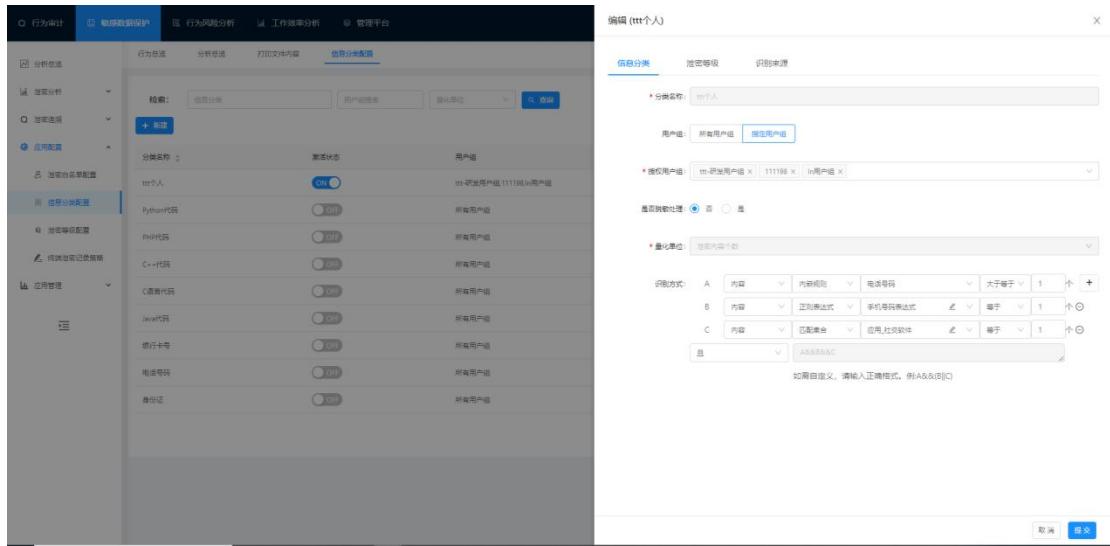
### 3.2.1 信息分类配置

点击“敏感信息>敏感分类配置”进入敏感词分类界面，如下图：

分类名称	激活状态	用户组	量化单位	操作
个人信息	ON	ttt-研发用户组,1111111111111111用户组	范围内每个数	编辑   删掉
Python代码	OFF	所有用户组	范围内每个数	编辑
PHP代码	OFF	所有用户组	范围内每个数	编辑
C++代码	OFF	所有用户组	范围内每个数	编辑
C语言代码	OFF	所有用户组	范围内每个数	编辑
Java代码	OFF	所有用户组	范围内每个数	编辑
银行卡号	OFF	所有用户组	范围内每个数	编辑
电话号码	OFF	所有用户组	范围内每个数	编辑
身份证	OFF	所有用户组	范围内每个数	编辑

#### 3.2.1.1 新建信息分类

点击“新建”按钮，弹出新建敏感词分类界面，如图：



**匹配逻辑:** 选择“匹配集合”，可以匹配条件数据集（数据集：可以自定义或选择默认的数据集，点击可选择，更换，编辑，新增数据集）。选择“内嵌规则”“正则表达式”，可以配置身份证、电话号码、银行卡敏感词分词。

**量化单位:** 选择敏感词个数为文本操作或文件操作中敏感词数量范围。

选择文件大小为操作文件的所有字节数量即文件所占用的物理内存为多少作为敏感统计范围。

选择打印页数为打印操作所打印的文件页数为敏感统计范围。

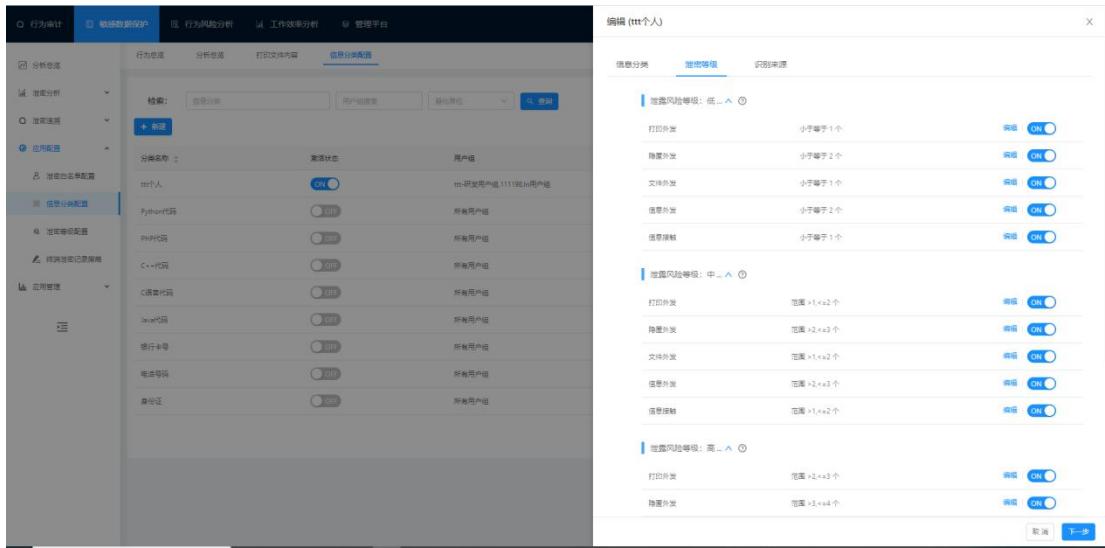
**识别方式:** 选择内容为文本操作或文件操作中的内容进行解析。

选择文件名为在文件操作中文件名称是否含有敏感词进行解析。

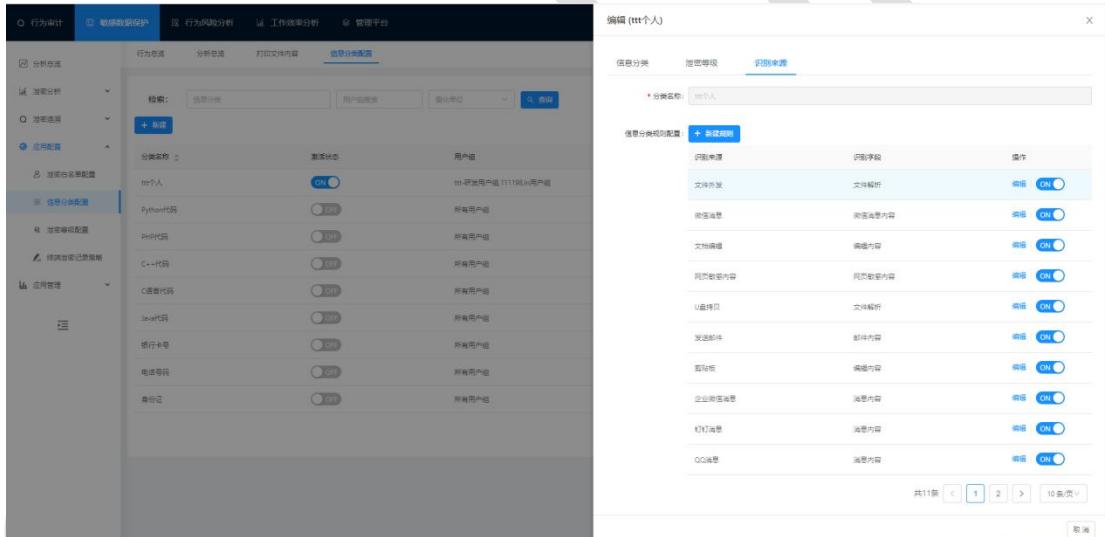
选择原始文件名为在文件操作前对文件进行重命名操作后在进行发送，解析其重命名前的文件名是否含有敏感词。

**匹配条件:** 可以选择自定义或默认的数据集。

点击保存并完善等级，配置敏感内容数量不同区间为不同敏感等级后提交，如下图所示：



配置启用后点击下一步，选择需要识别的来源开启后新建敏感分类过程结束。



### 3.2.1.2 信息分类配置编辑

点击完善规则，选择相应规则点击编辑如下图所示：

行为审计 敏感数据保护 行为风险分析 工作效率分析 管理平台

行为过滤 分析过滤 打印文件内容 信息分类规则

搜索: 搜索内容 用户ID搜索 启动状态

分类名称 激活状态 用户组

ttt个人	开关	ttt_研发用户组,1111981n用户组
Python代码	开关	所有用户组
Java代码	开关	所有用户组
C++代码	开关	所有用户组
C语言代码	开关	所有用户组
JavaScript	开关	所有用户组
银行账号	开关	所有用户组
敏感号码	开关	所有用户组
身份证	开关	所有用户组

编辑 (ttt个人)

信息分类 敏感等级 敏感来源

\* 分类名称: ttt个人

信息分类规则配置 + 新建规则

识别来源	识别字数	操作
文件发送	文件解析	编辑
动态消息	消息消息内容	编辑
文档阅读	读取内容	编辑
网页数据内容	网页数据内容	编辑
U盘拷贝	文件解析	编辑
发送邮件	邮件内容	编辑
剪贴板	消息内容	编辑
企业微信消息	消息内容	编辑
钉钉消息	消息内容	编辑
QQ消息	消息内容	编辑

共11条 < 1 2 > 10条/页 取消

### 3.2.1.3 新建信息分类规则

点击“新建”按钮弹出敏感词规则界面，如下图所示：

行为审计 敏感数据保护 行为风险分析 工作效率分析 管理平台

行为过滤 分析过滤 打印文件内容 信息分类规则

搜索: 搜索内容 用户ID搜索 启动状态

分类名称 激活状态 用户组

ttt个人	开关	ttt_研发用户组,1111981n用户组
Python代码	开关	所有用户组
Java代码	开关	所有用户组
C++代码	开关	所有用户组
C语言代码	开关	所有用户组
JavaScript	开关	所有用户组
银行账号	开关	所有用户组
敏感号码	开关	所有用户组
身份证	开关	所有用户组

编辑 (ttt个人)

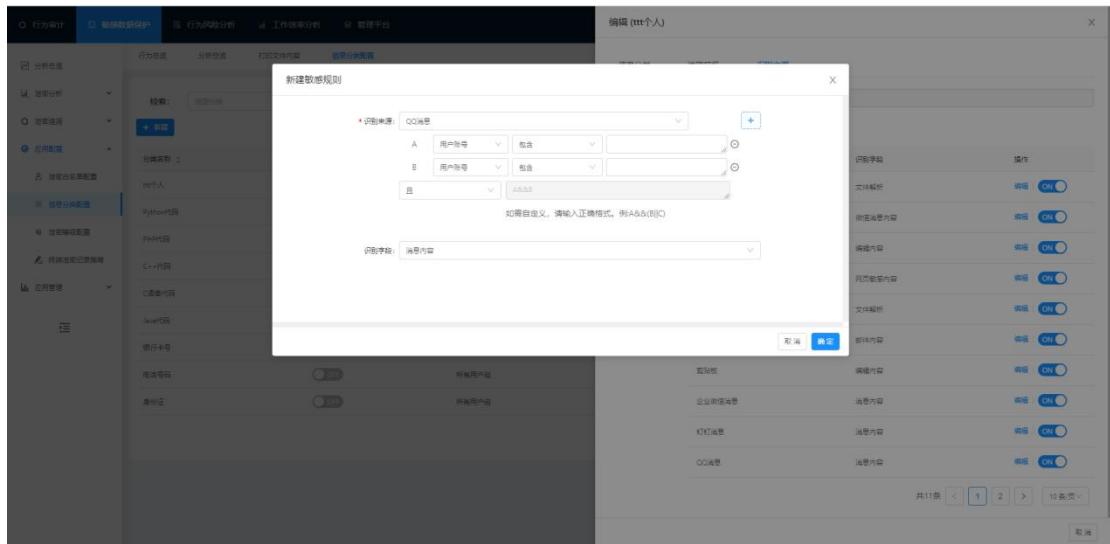
信息分类 敏感等级 敏感来源

\* 分类名称: ttt个人

信息分类规则配置 + 新建规则

识别来源	识别字数	操作
文件发送	文件解析	编辑
动态消息	消息消息内容	编辑
文档阅读	读取内容	编辑
网页数据内容	网页数据内容	编辑
U盘拷贝	文件解析	编辑
发送邮件	邮件内容	编辑
剪贴板	消息内容	编辑
企业微信消息	消息内容	编辑
钉钉消息	消息内容	编辑
QQ消息	消息内容	编辑

共11条 < 1 2 > 10条/页 取消



### 新建敏感词规则：

规则类型：选择规则类型（目前规则类型支持：QQ 消息，U 盘拷贝，剪贴板，文档编辑，发送邮件，网页敏感内容，微信消息，文件外发，打印行为），点击“+”添加规则条件，点击“-”删除规则条件，规则条件支持“且”，“或”多个条件，只有同时满足多个条件才可以触发；可以选择包含，不包含，等于，不等于或在...之内（**注：条件选择在...之内，需匹配一个数据集；这个数据集必须先配置敏感词分词，才能配置规则**）。

建议：一般不建议条件选择在...之内，这样的规则触发范围小。

关键词识别方式：选择“编辑内容”，则是文本信息带有敏感词；选择“文件解析”，则是文件内容带有敏感词。

关键词识别分词：选择要触发的敏感词分词内容。

怎么触发敏感词规则（需在 Windows 记录策略勾选相应行为审计的探针）：

文件操作敏感词：连接移动设备（USB）进行文件上传下载时，文件内容包含敏感词。

发送邮件：**foxmail** 或 **outlook** 邮件正文和附件内容包含敏感词（暂只支持审计 **outlook** 附件敏感词内容）。

剪贴板：在文本复制剪切粘贴的内容包含敏感词。

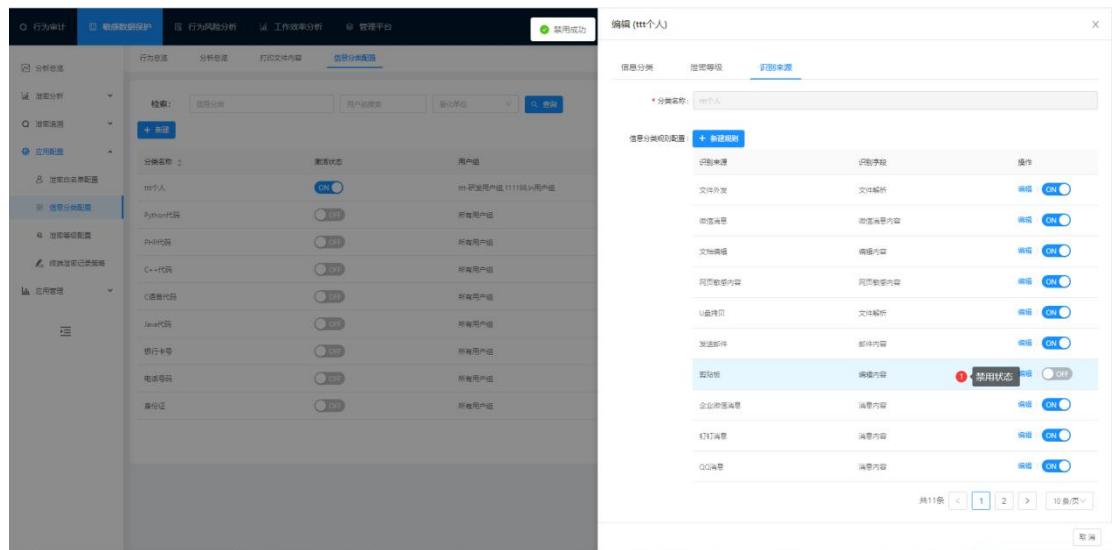
微信消息、QQ 消息：发送\接收聊天消息和文件内容包含敏感词。

网页敏感词内容：访问带有敏感词的网页（目前只支持 IE8 以上版本浏览器和部分谷歌浏览器版本）

文档编辑：编辑文档内容包含敏感词（暂只支持记事本、excel、word）

### 3.2.1.4 禁用/启用信息分类规则

选择要删除的敏感词规则，点击“OFF/ON”按钮，弹出提示禁用成功/启用成功如下图所示：



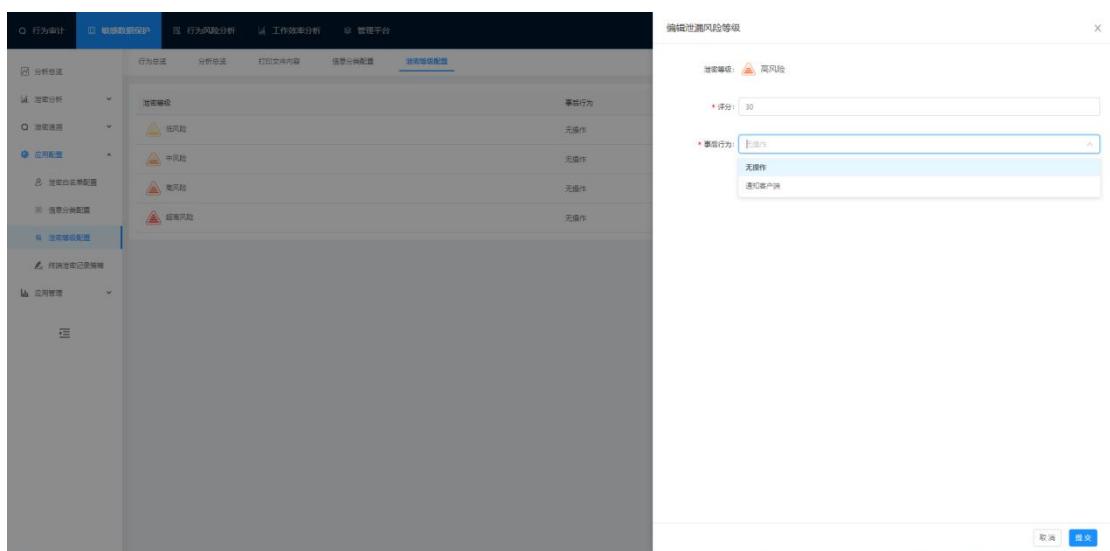
### 3.2.2 泄密等级配置

泄露风险等级配置为对敏感分类中所有风险等级进行相应的分数值设置。

点击编辑，设置风险评分以及事后行为，无操作或则通知客户端。

无操作：在触发敏感后不做反应。

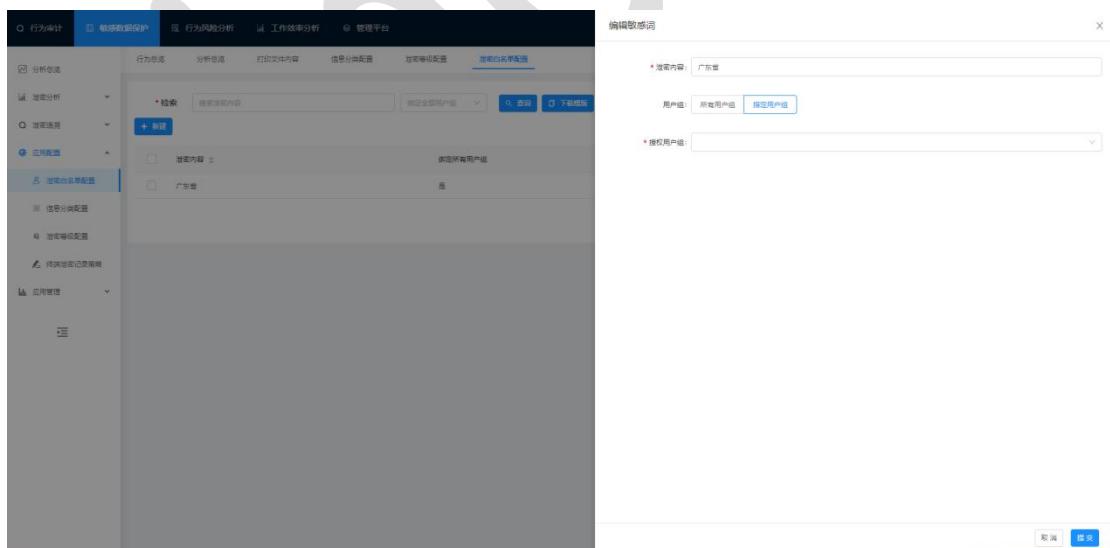
通知客户端：在触发敏感后在桌面右下方弹出敏感提示弹窗。



完善规则：通过设置敏感量的范围，来区分敏感等级；效果与敏感分类配置中编辑的泄露风险等级一致。

### 3.2.3 泄密白名单配置

原是可以触发的敏感词加入敏感白名单中后再去通过发送或剪切等其他方式触发该敏感词的行为将不会被记录，其中白名单可授权所有用户组和个别用户组。新建白名单如下图所示：



### 3.2.3.1 泄密白名单导入/导出

敏感白名单那导入。先下载模板填写敏感词，用户组等信息后点击导入该文档即可。

敏感白名单导出，点击导出按键，下载相应文档。如下图所示：

The screenshot shows two views of the 'Sensitive White List Configuration' section in a web-based management system.

**Top View (Import):** The 'Import' button is highlighted in red. The table lists three entries:

过滤内容	指定所有用户组	授权用户组	操作
江西备	否	所有用户组	编辑、删除
广东备	是	所有用户组	编辑、删除

**Bottom View (Export):** The 'Export' button is highlighted in red. A file selection dialog is open, showing two files: '敏感词泄密内容数据.csv' and '泄密内容数据模板.csv'. The 'yq报表(2022\_4\_21)报表(1).xlsx' file is selected, indicated by a red circle with a question mark.

### 3.2.4 终端泄密记录策略

终端敏感策略与终端策略同步，终端敏感策略不可新建，终端策略新建后自动生成。终端敏感策略：

**探针记录规则：**勾选探针后该探针类型触发记录，未勾选不记录。

文件上传：勾选后文件才可上传至服务器，文件后缀类型可自主添加，未在表内的后缀不可触发敏感词记录。文件最大支持 50MB,超过不上传。

网页敏感词规则：添加网站站点，该站点下的网址含有敏感词则记录。未添加的站点不记录敏感词。

The screenshot shows a system interface with a sidebar navigation on the left containing '行为审计' (Behavior Audit), '敏感数据保护' (Sensitive Data Protection) (selected), '行为风险分析' (Behavior Risk Analysis), '工作效率分析' (Work Efficiency Analysis), and '管理平台' (Management Platform). The main content area has tabs for '分析概述' (Analysis Overview), '策略分析' (Policy Analysis), '应用配置' (Application Configuration), and '文件备份' (File Backup). The '文件备份' tab is selected. On the right, there are three configuration panels: 1) '针对记录规则' (Record Rule Configuration) with checkboxes for '是否记录网页内容' (Check if web page content is recorded) and '是否记录文件内容' (Check if file content is recorded), and a dropdown for '是否记录打印行为' (Check if print behavior is recorded). 2) '文件上传' (File Upload) with a list of supported file types: 'txt', 'doc', 'docx', 'pdf', 'ppt', and 'pt'. A text input field shows '\*.txt (支持\*.html和\*.htm)' and a file size limit of '10'. 3) '网页敏感词内容规则' (Webpage Sensitive Content Rules) with a dropdown for '默认规则' (Default Rule) set to '记录列表外的网页' (Record pages outside the list) and a '网页列表' (Webpage List) input field.

### 3.2.5 文件备份 es 配置

文件 es 配置：储存已上传的文件信息。

The screenshot shows a system interface with a sidebar navigation on the left containing '行为审计' (Behavior Audit), '敏感数据保护' (Sensitive Data Protection) (selected), '行为风险分析' (Behavior Risk Analysis), '工作效率分析' (Work Efficiency Analysis), and '管理平台' (Management Platform). The main content area has tabs for '分析概述' (Analysis Overview), '策略分析' (Policy Analysis), '应用配置' (Application Configuration), and '文件备份' (File Backup). The '文件备份' tab is selected. On the right, there is a configuration panel for '文件备份ES配置' (File Backup ES Configuration) with fields for '集群名称' (Cluster Name) set to 'my-application', 'Elasticsearch地址' (Elasticsearch Address) set to 'http://192.168.0.133:9200', and '是否启用用户名密码' (Enable Username and Password) checked. Below these are radio buttons for '是否记录打印内容' (Check if print content is recorded) and '是否记录文件内容' (Check if file content is recorded), both set to '是' (Yes). There are also dropdowns for '外部文件元数据保留时间' (External file metadata retention time) set to '10 天' (10 days) and '打印信息元数据保留时间' (Print information metadata retention time) set to '10 天' (10 days). At the bottom are '配置' (Configure) and '初始化' (Initialize) buttons.

### 3.2.6 泄密行为

泄密行为：展示所有触发敏感规则信息，筛选类型包含行为类型，渠道，风险等级。

树形检索：检索条件包含：部门名称；用户名；应用名称；终端地址终端列表；用户列表中存在的终端用户都可被检索。附加搜索框未展示的标签可通过搜索框搜索。

设置：点击设置可自主选择需要展示的字段。

This screenshot shows the 'Leakage Behavior' section of the platform. It includes filters for 'Behavior Type' (Information Disclosure, Information Leakage, Information External Release, File External Release, Directory External Release, Non-defined Behavior), 'Channel' (Email, WeChat, Network, Terminal, Device Management, Process Monitoring, Remote Disk, Document Management, USB Drive, Print), and 'Risk Level' (All, High, Medium, Low). A search bar allows filtering by keyword and selecting specific departments or users. The main area displays a table of leaked files with columns: Time, Department, Risk Level, File Type, Operation, and Action. Each row shows details like '2022-04-27 10:05:12 研发部:小小 高 do/files 1个 信息接触 文档阅读 Excel'.

This screenshot shows the same 'Leakage Behavior' section but with a tree search interface overlaid on the search bar. The tree search allows users to select specific departments or users directly from a dropdown menu. A red arrow points to the 'Tree Search' button, and another red circle highlights the 'Add page display settings' link in the top right corner of the search bar.

### 3.2.7 外发文件内容

检索关键词，可检索出所有外发文件中含有该关键词的文件，并将所有文件分为含有敏感，不含敏感，是否隐匿方式分类。

文件详情跳转：点击文件敏感分类名称或文件名称跳转至文件详细信息查看数据，并且支持相应文件下载。

行为审计 敏感数据保护 行为风险管理 工作效率分析 管理平台

文件备份与配置 泄密行为 **外发文件内容**

分析总述 泄密分析 泄密追溯 泄密行为 外发文件内容 打印文件内容 元数据检索 应用配置 应用管理

输入关键词

是否搜索 全部 近期 最近30天 检索

年华.txt

身份证 电话号码 日期 yyyd敏感分类

k 15179986325 湖南省衡阳市 江西省南昌市 今天是个好日子 湖南省 湖南省

外发用户数: 1 外发次数: 1 隐匿次数: 0 时间: 2022-04-21 09:24

西河2.txt

身份证 电话号码 日期 yyyd敏感分类

今天是个好日子 15179986325 160321199608082018

外发用户数: 1 外发次数: 1 隐匿次数: 0 时间: 2022-04-21 09:24

12345.txt

身份证 电话号码 日期 yyyd敏感分类

湖南省 长沙市 江西省 南昌市 15179986325 湖南省 长沙市 360321199608082018 从南昌 15642313胡慧分 湖南省

外发用户数: 1 外发次数: 1 隐匿次数: 0 时间: 2022-04-21 09:24

查看详情

综合信息

操作时间: 2022-04-21 09:24  
部门: 行政办  
用户名: admin  
终端IP: DESKTOP-OSGED8/admin/localhost  
终端名称: IP: DESKTOP-OSGED8/192.168.0.129

泄密信息

信息分类: yyyd敏感分类  
行为分类: 文件外发  
跳窗方式: 无跳窗  
渠道分类: USB存储  
泄密等级: 黄色  
泄密评分: 10  
泄密内容: 15179986325.15179986523.360321199608082018  
泄密信息量: 3个  
泄密上下文: 15179986325.15179986523.360321199608082018

应用信息

应用名称: 年华.txt 上 1 文件下载  
目的文件夹: F:\

取消 下载

### 3.2.8 打印文件内容

选择部门用户后，检索关键词，可检索出所有的含有该关键词的所有打印记录，并把它们分为敏感和不含敏感两类展示数据。点击敏感分类标签或文件名查看详情，或下载打印文件。

The top screenshot shows a software interface with a dark header containing navigation items like '行为审计' (Behavior Audit), '敏感数据保护' (Sensitive Data Protection), '行为风险分析' (Behavior Risk Analysis), '工作效率分析' (Work Efficiency Analysis), and '管理平台' (Management Platform). A user 'admin' is logged in. The left sidebar has sections for '分析报告' (Analysis Report), '敏感分析' (Sensitive Analysis), '敏感追溯' (Sensitive Traceback), '敏感行为' (Sensitive Behavior), '外发文件内容' (Content of External Files), '打印文件内容' (Content of Printed Files) (which is selected), '云数据搜索' (Cloud Data Search), '应用配置' (Application Configuration), and '应用管理' (Application Management). A search bar at the top right contains the placeholder '请输入关键词'. The main area features a large blue printer icon.

The bottom screenshot shows a detailed view of a print record. The header is identical to the top one. The left sidebar includes '是否敏感' (Is it sensitive) with tabs '全部' (All), '敏感' (Sensitive), and '未分类' (Unclassified). A search bar shows '15179986325' and a date range '最近30天'. Below this is a table with two rows. The first row is for a file named '12138.txt - 记事本' (12138.txt - Notepad) from '湖南省 长沙市 雷阳市 江西省 南昌市' (Hunan Province Changsha City Leiyang City Jiangxi Province Nanchang City) with ID '15179986325'. The second row is for a file named '西河2.txt - 记事本' (Xihe2.txt - Notepad) from '今天是个好日子 15179986325' (Today is a good day 15179986325) with ID '15179986358'. The right side of the screen displays a '查看详情' (View Details) modal with tabs for '操作信息' (Operational Information), '泄密信息' (Leakage Information), and '应用信息' (Application Information). The '操作信息' tab shows details like '操作时间: 2022-04-20 17:49' and '操作人: 研发部/乔峰'. The '泄密信息' tab shows '敏感分类: 个人隐私类' (Sensitive Category: Personal Privacy Class) and a list of 6 sensitive words. The '应用信息' tab shows '打印机名: OneNote (Desktop)' and a download button for the file.

1.点击敏感分类

### 3.2.9 元数据检索

行为明细检索中记录所有渠道支持范围内产生的明细数据，通过处理将这些明细数据分为敏感与不含敏感两类。筛选方式与终端敏感检索中的分类方式一致。左侧设置部门用户精确检索，关键字检索采取 ik 分词器逻辑。

**树状检索：**检索条件包含：部门名称；用户名；应用名称；终端地址终端列表；用户列表中存在的终端用户都可被检索。附加搜索框未展示的标签可通过搜索框搜索。

时间	部门/姓名	终端名称/IP	用户名/登录IP	行为分类	传播分类	敏感程度	应用名称	信息内容	文件名	网页URL	操作		
2022-04-27 10:30:18	研发部/小小	192.168.3.112	ADMIN/logging localhost	信息接触	通讯	否	WeChat	2022年4月27...					
2022-04-27 10:30:08	研发部/小小	admin	ADMIN/logging localhost	信息接触	文件编辑	是	Excel	1. SecureCRT6...					
2022-04-27 10:30:06	研发部/小小	admin	ADMIN/logging localhost	信息接触	文件编辑	是	Excel	1. SecureCRT6...					
2022-04-27 10:29:59	市场部/何德基	DESKTOP-CSGJED8	DESKTOP-CSGJED8\admin	信息接触	通讯	否	腾讯QQ	https://tvp.co...					
2022-04-27 10:29:38	研发部/小小	admin	ADMIN/logging localhost	信息接触	剪贴板	是	audio/audio...						
2022-04-27 10:29:29	市场部/何德基	DESKTOP-CSGJED8	DESKTOP-CSGJED8\admin	信息接触	通讯	否	腾讯QQ	https://tvp.co...					
2022-04-27 10:29:06	研发部/小小	admin	ADMIN/logging localhost	信息接触	通讯	否	腾讯QQ	24.9信号均衡...					
2022-04-27 10:28:34	研发部/小小	admin	ADMIN/logging localhost	信息接触	通讯	否	腾讯QQ	[图片] 00【第...					

1. 树状检索：展开后可选择部门名称；用户姓名；应用名称；终端地址；终端名称进行检索。如下图所示：

- 请选择部门/用户/应用/终端地址/终端名称 ^
- 
- + 部门名称
  - 
  - + 用户姓名
  - 
  - + 应用名称
  - 
  - + 终端地址
  - 
  - + 终端名称

### 3.2.10 风险用户

风险用户对终端上产生泄密行为的用户进行统计，检索方式以部门/用户方式检索;统计范围包含用户触发泄密分类总评分；敏感分类类型；触发敏感分类详情等。页面详情功能请查看以下图片。

**Top Screenshot: User Rating Ranking**

排名	部门姓名	评分
1	市场部/树镇慈	151700
2	市场部/阳阳	321170
3	市场部/张飞	12450
4	研发部/唐诗婷	6770
5	品质部/徐三	5520
6	产品部/芦青青	5360
7	研发部/小小	3710
8	研发部/陈来	2080
9	销售部/王一	1980

**Bottom Screenshot: Risk User Analysis**

Summary Card Data:

- 部门姓名: 市场部/树镇慈
- 总评分: 151700
- 泄密等级分布: 超高 (14089), 高 (3026), 中 (13627), 低 (1132)
- 泄密行为分布: 信息接触 (15,000), 信息外发 (9,000)
- 泄密行为趋势: 泄密行为总次数 14089 (Trend from 2022-04-24 to 2022-04-26)

Leakage Behavior Details:

序号	信息分类	泄密行为
1	qq群聊分块	13528 次
2	ttt	553 次
3	ttt个人	8 次

1. **用户排行榜:** 点击跳转至检索时间段内触发了泄密行为的所有用户，按照用户触发的行为分类总评分来排名。
2. **检索模块:** 以在检索时间段内用户管理中的所有用户，若产生行为的用户无法找到在搜索框中输入部门/用户名直接检索即可。
3. **检索用户触发的行为分类:** 点击行为分类可以跳转到相应的行为分类详情。
4. **泄密行为统计，趋势图展示。**
5. **泄密行为详情展示:** 可点击详情，播放，收藏。

### 3.2.11 信息分类

信息分类统计用户触发的敏感分类集合，并对所有敏感分类次数进行统计。检索时间段

内的敏感分类可查看该时间段内的某个敏感分类的触发次数。

The screenshot shows a dashboard titled 'Sensitive Classification'. On the left, there's a sidebar with various monitoring categories like 'File Audit', 'Data Protection', 'Behavior Risk Analysis', etc. The main area has a search bar with filters for time range and search terms. Below it is a table titled 'Information Classification Ranking' with columns for rank, classification, and trigger count. The top entry is '敏感分类' with 14091 triggers.

排序	信息分类	道密行为次数
1	敏感分类	14091
2	...	5121
3	敏感分类	179
4	文件大小	113
5	... 敏感	111
6	... 个人	102
7	电话号码	44
8	个人座机	38
9	... 敏感	33
10	身份证	14

1.时间戳：分为快捷时间段和自定义时间段，可通过设置选择检索该时间段的所有敏感分类。

2.搜索框：可检索触发的敏感分类。

3.点击快捷选项：直接跳转至相应的敏感分类。

This screenshot displays the 'Leakage User' analysis section. It includes several charts and tables: 'Leakage User Top 10' (with a user named '市场部-张飞' at the top), 'Leakage Application Top 10' (listing browser extensions like 'explorer'), 'Leakage URL Top 10' (listing website URLs), and 'Leakage Behavior Distribution' (a bar chart showing counts for '信息接触', '信息外发', and '文件外发'). A large red box highlights the total leakage count of 14091.

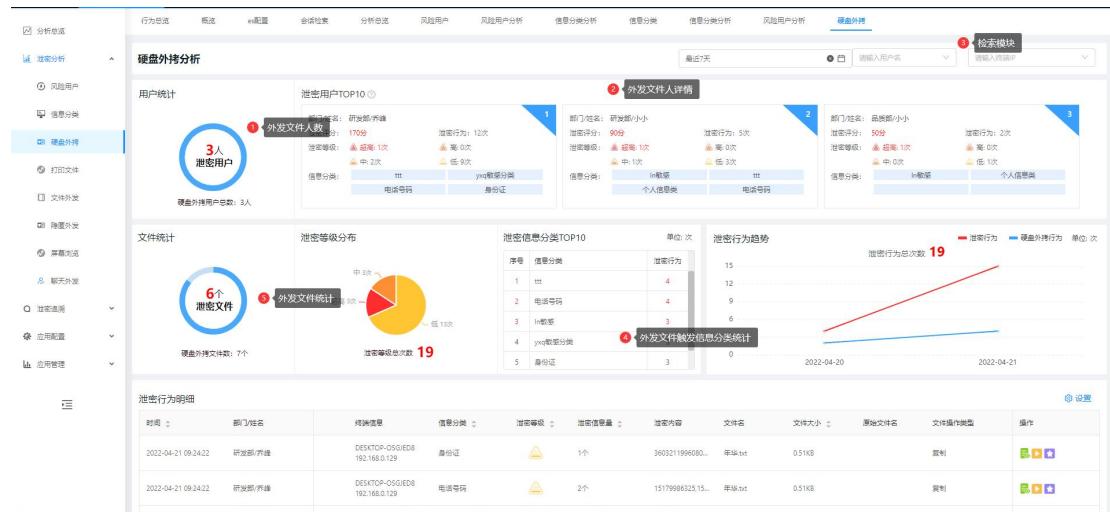
2. 用户排行，通过用户泄密等级评分计算进行排列，点击用户名可跳转至对应应用户风险页面。

3. 切换查看所有用户

4. 用户在排列中的应用触发了敏感，将对这些应用，网站进行统计次数展示。

### 3.2.12 硬盘外拷

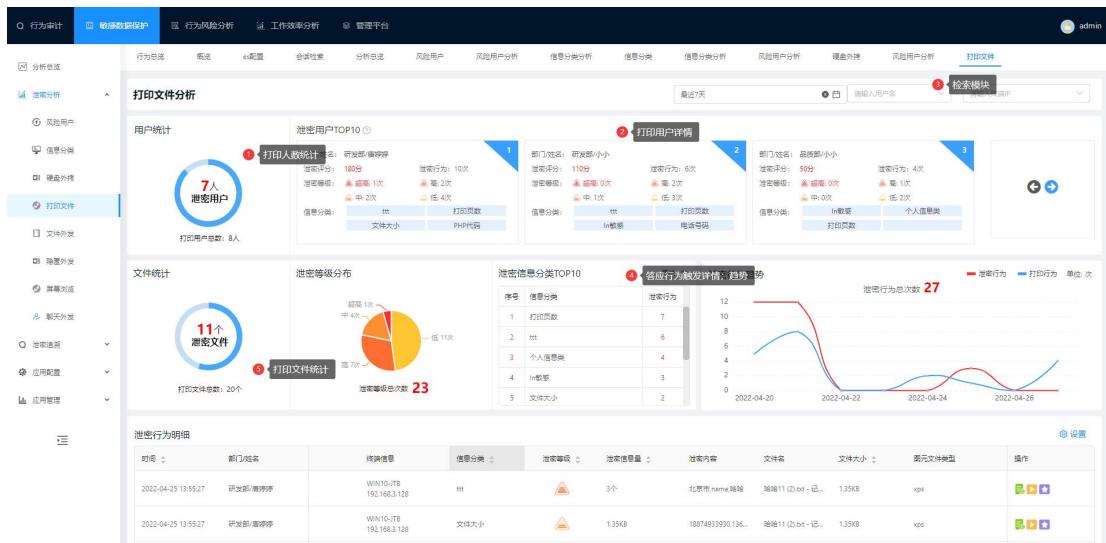
硬盘外拷统计通过硬盘，usb 等外设传输文件，当文件中含有泄密信息将对此文件进行记录。统计范围为文件解析范围。



1. 硬盘外拷人数统计：分为外发泄密文件人数统计；外磁盘外拷用户总数：所有外发文件人数统计。
2. 硬盘外拷用户详情：包含外发用户，外发泄密文件泄密等级，触发信息分类名称。点击部门/用户可进行跳转至风险用户页面，点击信息分类标签可跳转对应信息分类。
3. 检索模块：时间戳检索（快捷时间段以及自定义时间段）；用户部门及终端/ip 检索检索可选择产生过泄密信息的所有用户，未在列表中的用户/IP 请完整输入部门/用户或者直接输入 ip 直接检索。
4. 点击可跳转至信息分类详情页面

### 3.2.13 打印文件

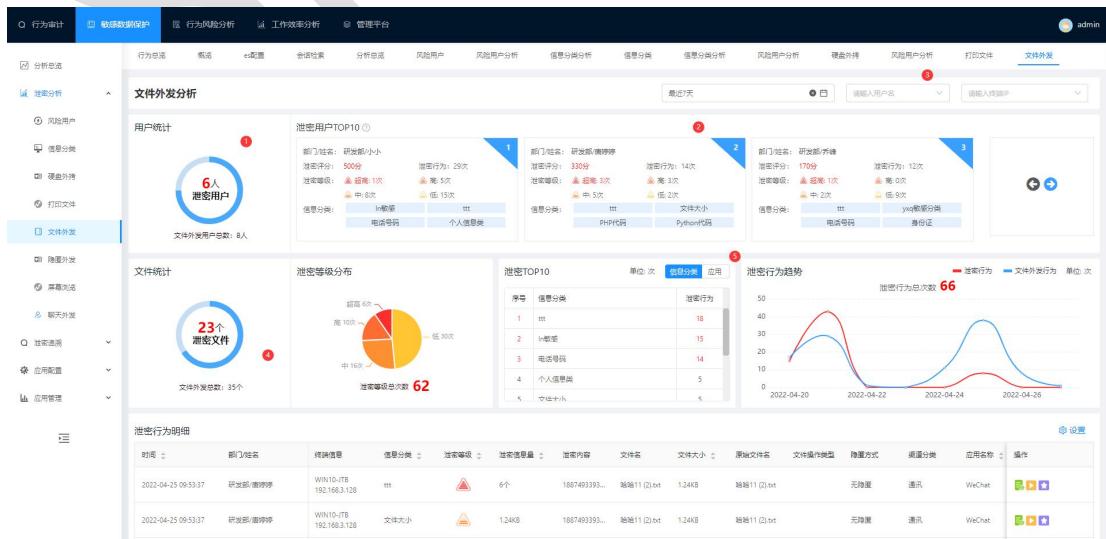
打印文件对用户打印文件中的泄密行为进行统计。



1. 打印文件人数统计：分为打印泄密文件人数统计；所有打印文件人数统计。
2. 打印文件用户详情：包含打印用户，打印泄密文件泄密等级，触发信息分类名称。点击部门/用户可进行跳转至风险用户页面，点击信息分类标签可跳转对应信息分类。
3. 检索模块：时间戳检索（快捷时间段以及自定义时间段）；用户部门及终端/IP检索检索可选择产生过泄密信息的所有用户，未在列表中的用户/IP 请完整输入部门/用户或者直接输入 ip 直接检索。
4. 打印文件统计：包含打印泄密文件和所有打印文件。

### 3.2.14 文件外发

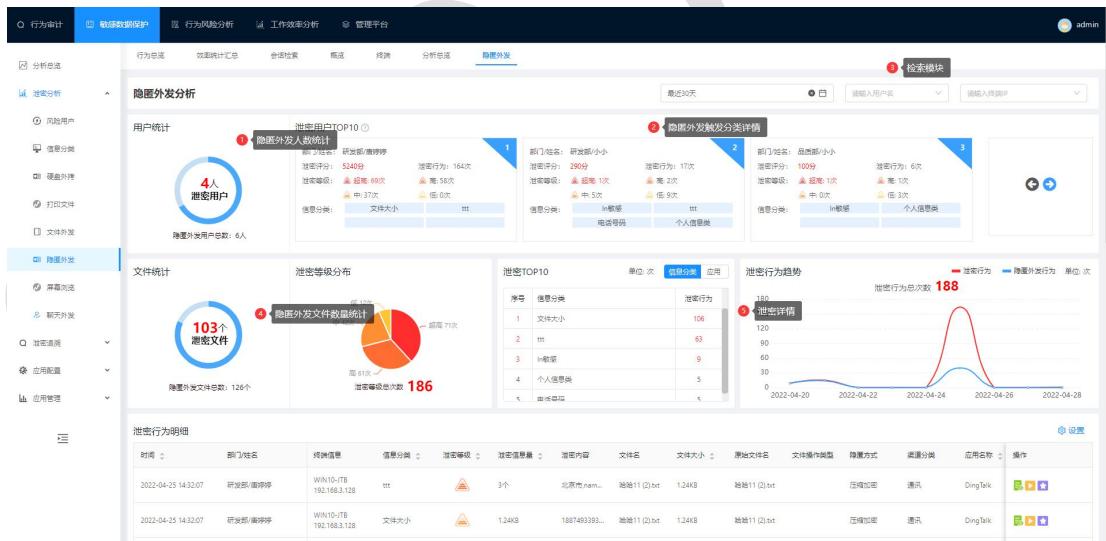
外发文件对用户外发文件中的泄密行为进行统计。



- 文件外发人数统计：分为外发泄密文件人数统计；文件外发用户总数：所有外发文件人数统计。
- 文件外发用户详情：包含外发用户，外发泄密文件泄密等级，触发信息分类名称。点击部门/用户可进行跳转至风险用户页面，点击信息分类标签可跳转对应信息分类。
- 检索模块：时间戳检索（快捷时间段以及自定义时间段）；用户部门及终端/ip检索检索可选择产生过泄密信息的所有用户，未在列表中的用户/IP 请完整输入部门/用户或者直接输入 ip 直接检索。
- 所有文件外发数目统计：泄密文件及所有外发文件。
- 点击可跳转至信息分类详情页面

### 3.2.15 隐匿外发

隐匿外发统计隐匿外发方式：修改后缀；压缩，加密压缩。



- 隐匿外发文件人数统计：分为外发泄密文件人数统计；隐匿文件外发用户总数：所有隐匿外发文件人数统计。
- 隐匿外发文件用户详情：包含隐匿外发用户，外发泄密文件泄密等级，触发信息分类名称。点击部门/用户可进行跳转至风险用户页面，点击信息分类标签可跳转对应信息分类。
- 检索模块：时间戳检索（快捷时间段以及自定义时间段）；用户部门及终端/ip

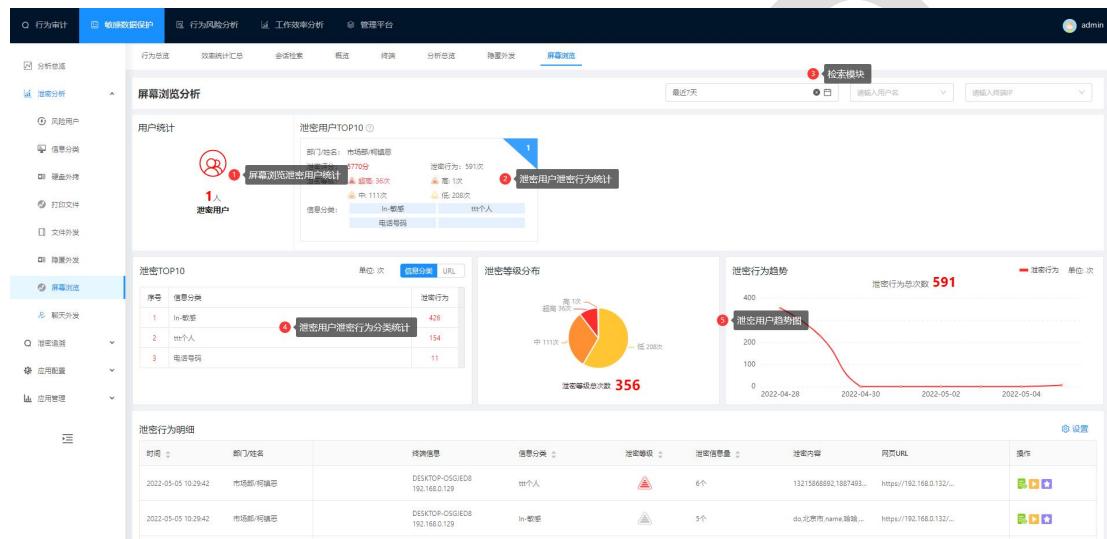
检索检索可选择产生过泄密信息的所有用户，未在列表中的用户/IP 请完整输入部门/用户或者直接输入 ip 直接检索。

4. 所有文件外发数目统计：泄密文件及所有隐匿外发文件。

5. 点击可跳转至信息分类详情页面

### 3.2.16 屏幕浏览

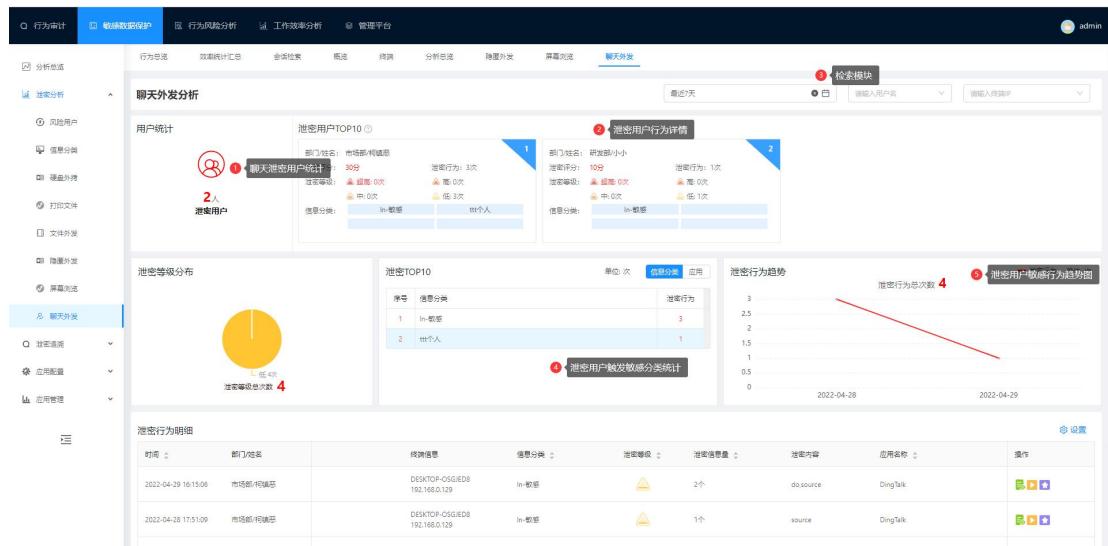
屏幕浏览为网页敏感词统计；网页敏感词。



1. 屏幕浏览人数统计：浏览器页面浏览过程存在泄密行为的用户统计。
2. 屏幕浏览用户详情：包含屏幕浏览用户，泄密等级，触发信息分类名称。点击部门/用户可进行跳转至风险用户页面，点击信息分类标签可跳转对应信息分类。
3. 检索模块：时间戳检索（快捷时间段以及自定义时间段）；用户部门及终端/ip 检索检索可选择产生过泄密信息的所有用户，未在列表中的用户/IP 请完整输入部门/用户或者直接输入 ip 直接检索。
4. 点击可跳转至信息分类详情页面。
5. 检索时间段内屏幕浏览泄密行为趋势图。

### 3.2.17 聊天外发

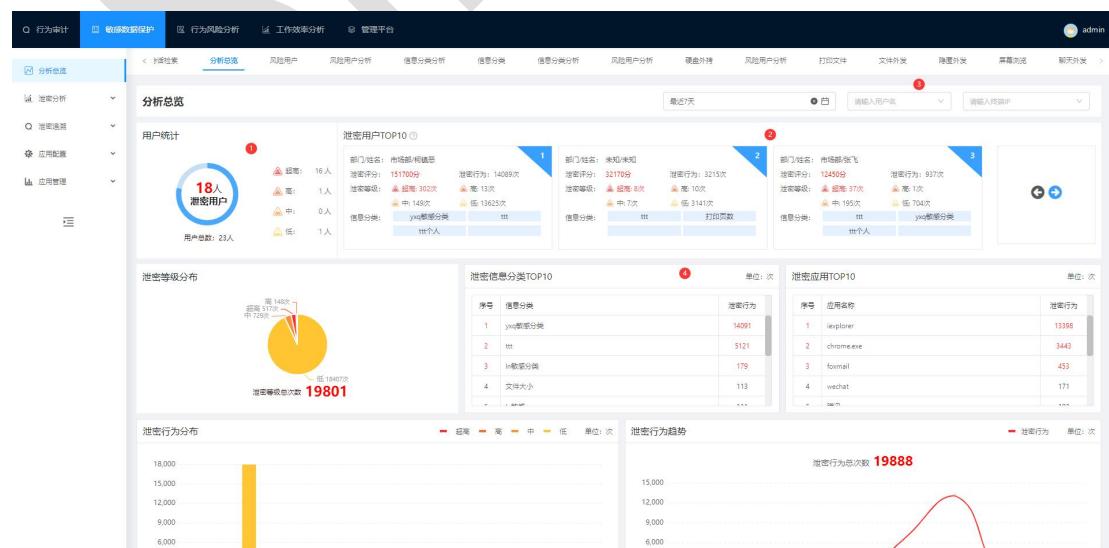
聊天外发统计用户在支持的聊天程序的所有泄密



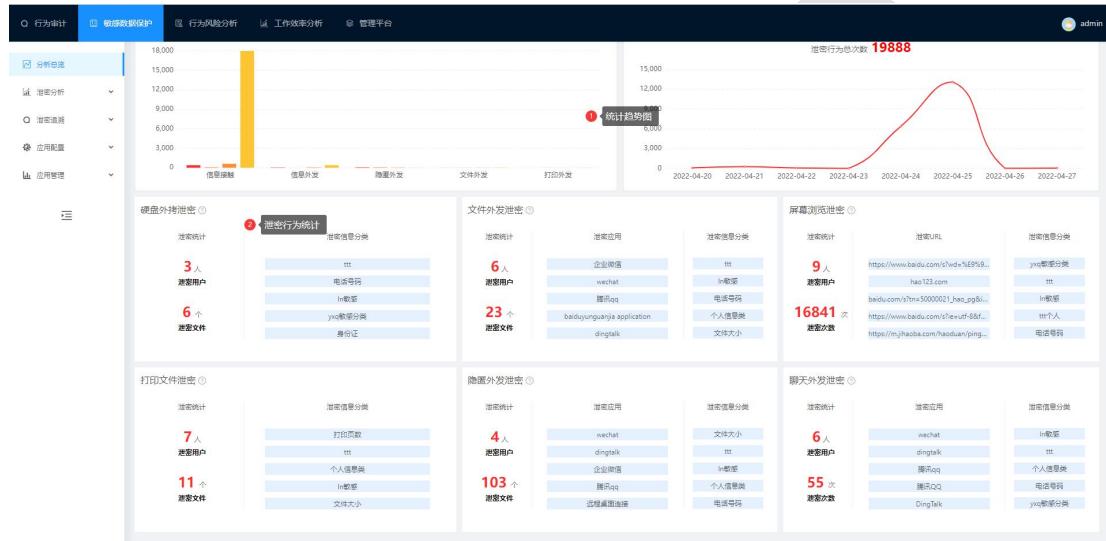
1. 聊天外发人数统计：产品支持审计的交友软件消息外发过程存在泄密行为的用户统计。
2. 聊天外发用户详情：包含聊天外发用户，泄密等级，触发信息分类名称。点击部门/用户可进行跳转至风险用户页面，点击信息分类标签可跳转对应信息分类。
3. 检索模块：时间戳检索（快捷时间段以及自定义时间段）；用户部门及终端/ip 检索检索可选择产生过泄密信息的所有用户，未在列表中的用户/IP 请完整输入部门/用户或者直接输入 ip 直接检索。
4. 点击可跳转至信息分类详情页面。
5. 检索时间段内屏幕浏览泄密行为趋势图。

### 3.2.18 分析总览

分析总览是所有泄密行为的一个统计，展示在页面。



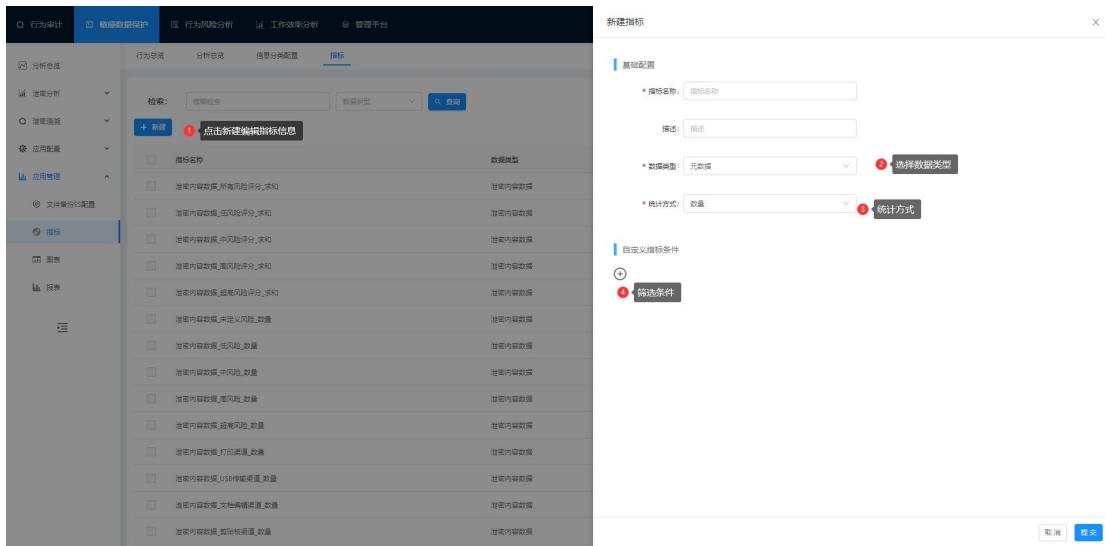
- 所有泄密用户人数统计：分为泄密文件统计；用户泄密总评分：所有泄密行为人数统计。
- 所有泄密用户详情：包含所有用户，泄密文件，泄密等级，触发信息分类名称。点击部门/用户可进行跳转至风险用户页面，点击信息分类标签可跳转对应信息分类。
- 检索模块：时间戳检索（快捷时间段以及自定义时间段）；用户部门及终端/ip 检索检索可选择产生过泄密信息的所有用户，未在列表中的用户/IP 请完整输入部门/用户或者直接输入 ip 直接检索。
- 点击可跳转至信息分类详情页面



1. 泄密趋势图
2. 对所有泄密行为进行一个统计排列展示；其中点击其中用户，文件或敏感分类都将跳转到对应的泄密行为模块。

### 3.2.19 敏感指标

指标设置统计数据类型和统计泄密行为方式，有初步筛选数据作用。新建指标方式如下：



1. 新建点击弹出指标新建页面。
2. 数据类型可选择元数据/泄密内容数据；选择元数据统计以元数据检索模块为标准；选择泄密内容数据以泄密行为模块展示数据为标准。
3. 统计方式有：数量（统计数据数量），求和（将统计数据值求和）；最大值/最小值（提取统计数据中的最大值/最小值）；平均值（统计数据平均值）；基数计数（对统计数据进行去重）。
4. 筛选条件：对数据进行过滤筛选。

### 3.2.20 敏感图表

图表功能主要是将指标统计数据以图像形式展示出来。且对数据进行归类，和并同类，并增加二次筛选的过程。详情如下图所示：

1. 图表点击新建。
2. 图表类型：将统计数据以柱状图，折线图，扇形图，表图四种方式可供选择。
3. 数据类型：元数据和泄密内容数据和指标数据类型对应选择。
4. 统计维度：将由指标统计的数据进行数据分类，以类别展示所有数据。
5. 时间段：对统计数据进行时间段筛选。
6. 统计指标：选择对应的指标，展示对应的筛选数据
7. 总体过滤条件：提供二次筛选数据作用。

### 3.2.21 敏感报表

敏感报表中以所有行为数据检索中的行为数据为数据源通过各种筛选方式进行数据筛选，敏感报表如下图所示：

**所属部门选择：**选择所属部门只命中该部门的所有数据，支持多部门选择。

**选择元数据/敏感词数据：**选择元数据展示所有行为明细检索中的数据，选择敏感词数据展示所有终端敏感词检索中的数据。

**行为分类：**行为明细检索和终端敏感信息检索的筛选渠道。

**风险等级：**敏感词数据中风险等级的筛选渠道。

**是否展示明细数据：**勾选后在 html/excel 中可以看到该属性。

定时发送：设置时间后获取最近 5 次执行时间，在这个时间将自动发送报表。

状态：启用后定时发送正常，禁用后阻断定时发送，但支持手动发送。



数据排序：选择属性后对该属性进行升序降序排序。

名称	行为分类	数据类型	修改人	修改时间	描述	状态	定时发送	下次执行时间	HTML报表	EXCEL报表	操作
yun报表	文件外发,隐藏外发	连室内存数据	admin	04月21日18:23:27	12	启用	启用	04月21日18:36:00			发送报表
元数据报表	信息外发,文件外发,隐藏外发,打印外发	元数据	admin	03月04日10:29:50		启用	启用			发送报表	
数据报表	信息外发,文件外发,文件外发,隐藏外发,打印外发	连室内存数据	admin	03月28日14:45:45		启用	启用			发送报表	
一个月的数据报表	信息外发,信息外发,文件外发,隐藏外发,打印外发,未命名行为	连室内存数据	admin	03月09日14:42:47		启用	启用			发送报表	
测试报表	文件外发,隐藏外发	连室内存数据	admin	02月10日10:42:37	111	启用	启用			发送报表	
CSV-元数据报表	连室内存数据	元数据	admin	01月24日11:16:10		禁用	禁用			发送报表	
yu	信息外发,文件外发	元数据	admin	01月23日20:46:34	123	启用	启用	04月10日20:00:00			发送报表
aaa	元数据	admin	01月23日20:46:03			启用	启用			发送报表	
新手	元数据	admin	01月23日20:43:55			禁用	禁用			发送报表	
WQRW	信息外发	元数据	admin	01月23日20:40:17		禁用	禁用			发送报表	
Admin	元数据	admin	01月23日20:34:32			禁用	禁用			发送报表	

点击生成 HTML 报表：筛选出设置的数据以 html 方式展示。

点击生成 excel 报表：自动下载一个 excel 文档保存至本地，内容为筛选设置的数据。

### 3.3 工作效率

#### 3.3.1 效率分类

效率分类是用户在终端操作应用/访问网页行为的效率明细数据进行分类。

选择“配置>效率配置>效率分类”进入效率分类界面；可以选择用户组、模糊检索、工

作状态进行查询；如下图所示：

The screenshot shows a web-based management platform interface. The top navigation bar includes tabs for '行为审计' (Behavior Audit), '敏感数据保护' (Sensitive Data Protection), '行为风险管理' (Behavior Risk Management), '工作绩效分析' (Work Performance Analysis), and '效率分类' (Efficiency Classification). The current tab is '效率分类'. On the left, there is a sidebar with sections like '分析', '检索', '规则配置', '工作计划', and '效率分类'. Under '效率分类', there is a tree view of user groups: '所有用户组', 'yqj用户组', 'ark用户组', 'FHT用户组', 'tt-研发用户组', 'CSV用户组', 'hbt用户组', 'zpf用户组', 'xml\_test', '111198', and 'lv用户组'. The main content area displays a table with columns: '名称' (Name), '用户组' (User Group), '工作状态' (Work Status), '描述' (Description), and '操作' (Operation). The table contains five rows: 'tt其他' (Work), 'tt主工作' (Main Work), 'tt其他工作' (Other Work), 'tt怠工' (Idle Work), and 'DOCUMENT' (Work). A search bar at the top allows filtering by '姓名' (Name) and '工作状态' (Work Status). At the bottom right, there are pagination controls for '共5条' (5 items) and '20条/页' (20 items per page).

### 3.3.1.1 新建效率分类

点击“新建”按钮新建效率分类；如下图所示：

The screenshot shows a modal dialog box titled '新建行为分类' (Create New Behavior Classification). It has several input fields: '分类名称' (Classification Name) with placeholder '请输入分类名称', '用户组' (User Group) with a dropdown menu showing '所有用户组' (All User Groups) and '指定用户组' (Selected User Groups), '行为分类' (Behavior Classification) with a dropdown menu showing '主工作' (Main Work), '描述' (Description) with placeholder '请输入分类描述', and '分类条件' (Classification Conditions) with a dropdown menu showing '分类类型' (Classification Type). On the right side of the dialog, there is a preview table with columns '描述' (Description) and '操作' (Operation), showing five entries: '其他' (Work), '主工作' (Main Work), '其他' (Work), '其他' (Work), and '怠工' (Idle Work). At the bottom right of the dialog are '取消' (Cancel) and '确定' (Confirm) buttons.

分类配置：

分类名称：分类的名称。

用户组：可选择所有用户组和指定的用户组（指定用户组下的用户才能触发此效率分类规则）。

行为分类：主工作、非工作、其他、怠工行为。

分类描述：分类的描述。

## 分类条件：

分类类型：运行应用和浏览器应用。点击“+”添加搜索条件。点击“x”则删除搜索条件；支持多条件逻辑“且”、“或”；

例如：下图规则：用户操作 SecureCRT 和 Xshell 在效率明细的工作状态是“非主工作”。

The screenshot shows the configuration of a new behavior classification rule. In the '新建行为分类' dialog, the '分类名称' (Classification Name) is set to 'yq工作效果'. The '行为分类' (Behavior Classification) is set to '非主工作'. The '分类条件' (Classification Conditions) section is expanded, showing two conditions under '运行应用' (Running Application): '或' (Or) followed by '应用名称' (Application Name) '包含' (Contains) 'SecureCRT' and another '或' (Or) followed by '应用名称' (Application Name) '包含' (Contains) 'Xshell'. This configuration is highlighted with a red box.

Below the dialog, the '效率明细' report interface is shown. It lists two entries for the user 'DESKTOP-0SG0E04\administrator' on 01月20日 (January 20). Both entries show '应用' (Application) as 'SecureCRT' and '姓名/部门公司' (Name/Department/Company) as '张三'. The first entry has '行为类型' (Behavior Type) as '命令' (Command) and the second as '命令行' (Command Line). The report also includes columns for '开始时间/结束时间' (Start/End Time), '终端名称/IP' (Terminal Name/IP), '用户名' (Username), '行为类型' (Behavior Type), '用户名/网址路径' (Username/Web Path), '是否工作' (Is Working), '总时长' (Total Duration), '上机时长' (On-machine Duration), and '加权时长' (Weighted Duration).

分类条件：逻辑关系支持：‘包含’ ‘不包含’ ‘等于’ ‘不等于’ ‘在...之内（模糊）’

‘在...之内（精准）’ ‘在...之外（模糊）’ ‘在...之外（精准）’；条件之间关系支持：

‘且’ ‘或’；如下图所示：

在...之内：是匹配数据集条件，当数据集中包含“QQ”。

例如：触发应用名称行为分类在...之内(模糊)：只要应用名称包含“QQ”。

例如：触发应用名称行为分类在...之内(精准)：应用名称一定是“QQ”。

This screenshot shows the '新建行为分类' dialog with the '分类条件' (Classification Conditions) section expanded. It displays a dropdown menu for '包含' (Contains) which includes options like '包含' (Contains), '不包含' (Does not contain), '等于' (Equal), '不等于' (Not equal), '在...之内(模糊)' (In... (Fuzzy)), '在...之内(精准)' (In... (Precise)), '在...之外(模糊)' (Out... (Fuzzy)), and '在...之外(精准)' (Out... (Precise)). The '或' (Or) condition for 'SecureCRT' is selected, and the 'And' condition for 'Xshell' is also visible. The right side of the dialog shows the same classification rules and reports as the previous screenshot.

### 3.3.1.2 删除效率分类

选择要删除的分类，点击“删除”按钮删除分类。如下图所示：

The screenshot shows the 'Efficiency Classification' section of the management platform. A modal dialog box titled 'Confirm Deletion' is displayed, asking if the user wants to delete selected data. The main table lists several efficiency categories with checkboxes. One row, 'ttt勤工', has its checkbox checked and is highlighted with a blue border. The '操作' (Operation) column for this row contains a red-bordered 'Delete' button.

名称	用户组	工作状态	备注	操作
ttt其他	所有用户组	其他		编辑
ttt主工作	所有用户组	主工作		编辑
ttt副工作	所有用户组	副主工作		编辑
<input checked="" type="checkbox"/> ttt勤工	所有用户组	勤工		Delete
DOCUMENT	所有用户组	主工作	文档	编辑

### 3.3.1.3 编辑效率分类

点击“编辑”按钮编辑效率分类。如下图所示：

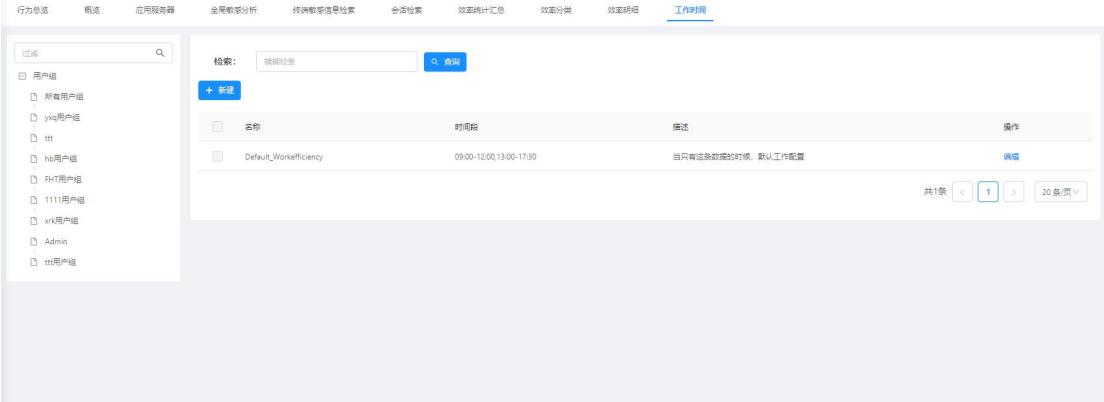
The screenshot shows the same 'Efficiency Classification' page as the previous one, but now the row for 'ttt勤工' is highlighted with a blue selection bar at the bottom of the table. The '操作' (Operation) column for this row contains a red-bordered 'Edit' button.

名称	用户组	工作状态	备注	操作
ttt其他	所有用户组	其他		编辑
ttt主工作	所有用户组	主工作		编辑
ttt副工作	所有用户组	副主工作		编辑
<input checked="" type="checkbox"/> ttt勤工	所有用户组	勤工		Edit
DOCUMENT	所有用户组	主工作	文档	编辑

### 3.3.2 工作时间配置

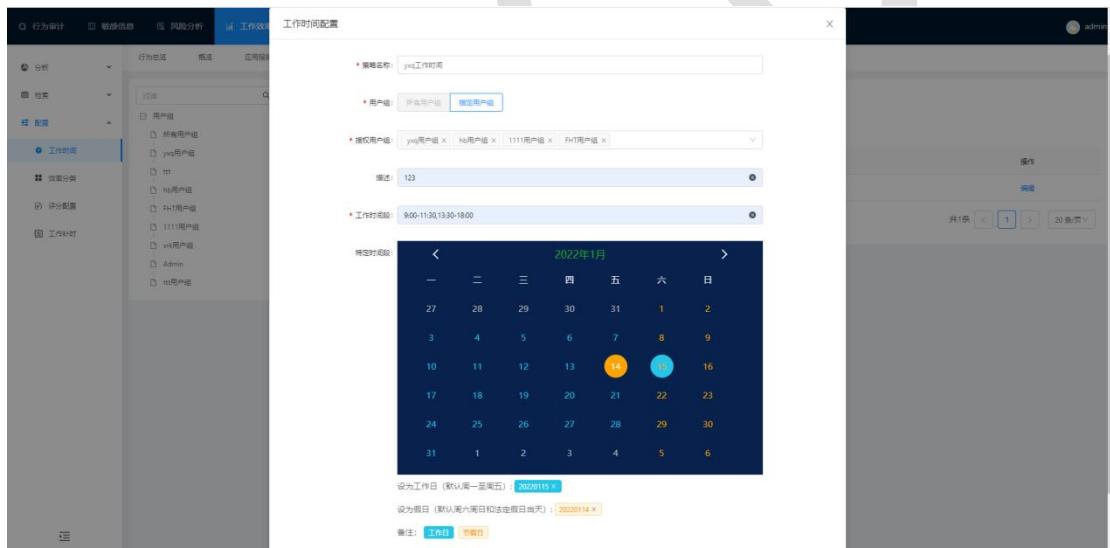
工作时间配置是配置用户在终端的上班工作的时长。

选择“工作效率>配置>工作时间”进入工作时间配置；可以选择用户组和模糊检索进行过滤查询；如下图所示：



### 3.3.2.1 新建工作时间配置

点击“新建”按钮新建工作时间配置；如下图所示：



策略名称：给工作时间配置命名。

授权用户组：授权之后该配置只对该用户组下的用户生效；一个用户组选择一个工作时间配置（新建的工作时间配置不支持所有用户组）

工作时间段：自定义上班工作时间段。

特定时间段：可以自定义配置特定时间段为工作或非工作日。

默认周一至周五为工作日，周六周日为假日（注：淡蓝色字体为工作日，橘黄色字体为假日。）

当点击淡蓝色字体时，该日期将被设为假日。当点击橘黄色字体时，该日期将被设为工作日）

（正常情况下：工作日时间段内是上班时长；假日和工作日时间段外加班时长。）

### 3.3.2.2 编辑工作时间配置

点击“编辑”按钮进行工作时间配置编辑；如下图所示：

名称	时间段	描述	操作
yxl的工作时间	9:00-11:30,13:30-18:00	123	<span style="border: 2px solid red; padding: 2px;">编辑</span>
Default_WorkEfficiency	09:00-12:00,13:00-17:30	当只有这条数据的时候，默认工作配置	<span>编辑</span>

### 3.3.2.3 删除工作时间配置

选择要删除的配置，点击“删除”按钮进行删除；**已绑定用户组的配置被删除后，该用户组下的用户会自动使用默认工作时间配置；默认的工作时间配置不可删除；**如下图所示：

② 确认删除  
是否删除选中数据?

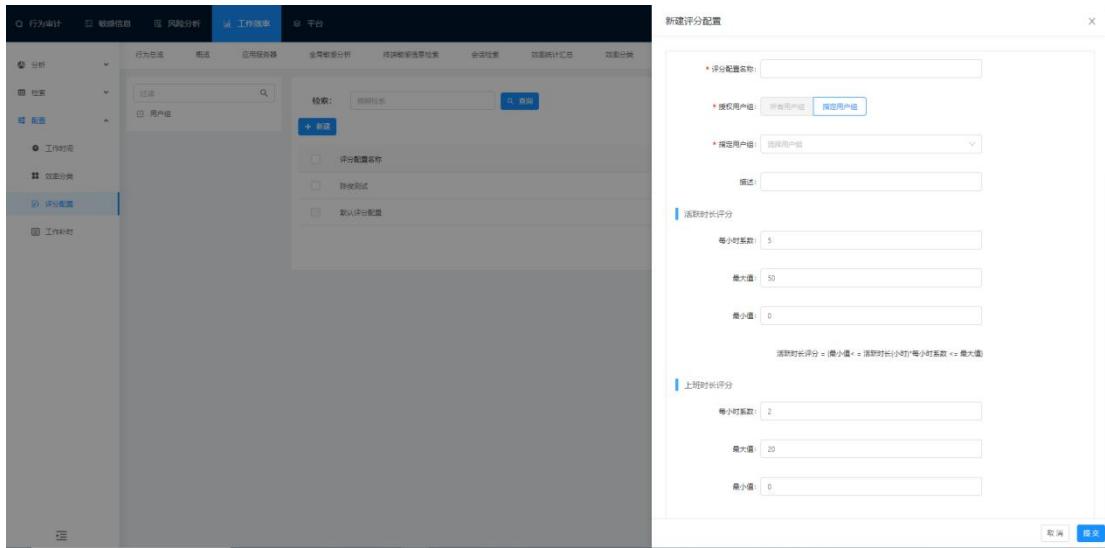
取消 确定

### 3.3.3 评分配置

评分配置是对用户在终端的工作效率进行评分。

选择“工作效率>配置>评分配置”进入评分配置界面；如下图所示：

点击“新建”按钮，进行新建评分配置；如下图所示：



**授权用户组:** 指定用户组，则该用户组下的用户在终端操作的工作效率数据都用此评分配置来计算评分。

**活跃时长评分:** 活跃时长评分 = {最小值 <= 活跃时长(小时)\*每小时系数 <= 最大值}。

其它时长评分可根据上图内容提示进行配置；

**注：**时长配置为空、每小时系数>=最大值、每小时系数<=最小值，则不计算该时长。

例如：计算下图的活跃时长评分：先把时长换算成小时约等于 5.83\*评分配置活跃时长对应的每小时系数。

**总评分计算：**所有时长计算评分的结果相加\*100/8

统计时间	终端名/终端IP	部门/用户名	用户账号	活跃时长	主工作时长	非主工作时长	其他时长	怠工时长	上班时长	加班时长	上班非强班时长	在线非强班时长	补时时长	当天开始时间	评分
2021年11月01日	WIN10-JTB	法润-审判开庭_卡尔	WIN10-JTB/rht	05:49:53	05:39:13	00:04:03	00:01:48	00:04:49	05:20:13	00:29:40	01:04:22	02:41:24	00:00:00	2021-11-01 09:13:26	474.00

### 3.3.4 工作补时

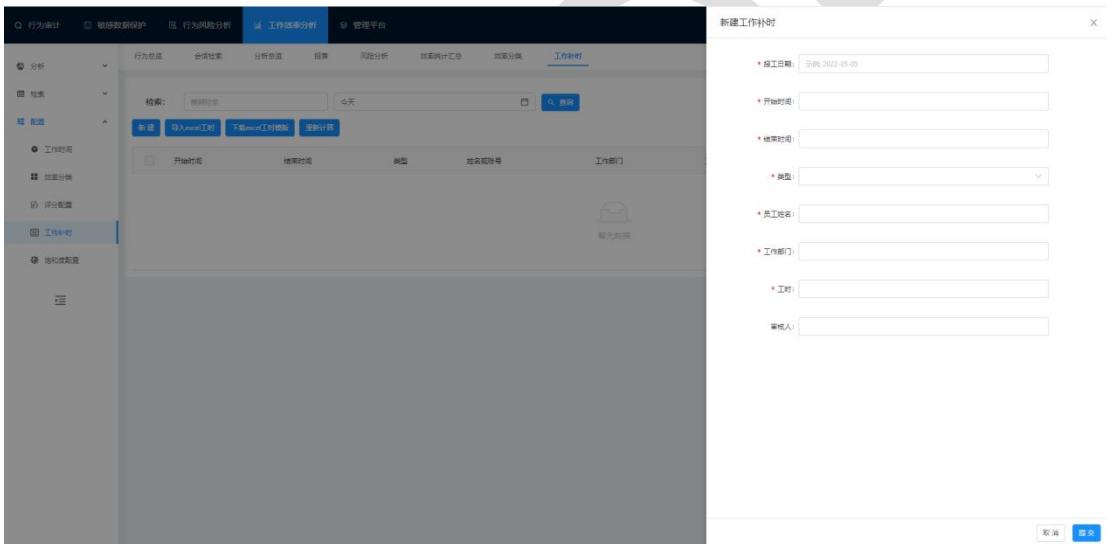
**工作补时:** 当用户因其它工作未操作终端产生的非活跃时长，可以通过工作补时来进行补时清除非活跃时长。

选择“工作效率>配置>工作补时”进入补时界面；如下图所示：



### 3.3.4.1 新建工作补时

点击“新建”按钮进行新建工作补时；（当有多个用户需要补时时，可以选择导入工作补时；先下载 excel 工时模板填写要工作补时的用户信息）如图下图所示：



报工日期：填写用户哪天要补时的日期。

开始时间、结束时间：用户要补时的时间段。

类型：选择按姓名，则输入用户的姓名和部门信息；选择按账号，则输入用户的登录账户信息。

工时：计算要补时的时长；不足半小时也填写 0.5；

审核人：填写审核人信息

### 3.3.4.2 重新计算

点击“重新计算”按钮；去效率明细查看此用户的所补时时间段的非活跃记录是否补时

成功；再去效率统计明细查看此用户的效率统计明细补时时长计算是否正常。

The screenshot shows the 'Work Efficiency Analysis' section of a management platform. On the left, there's a sidebar with various analysis categories like Behavior Audit, Data Protection, Risk Analysis, and Work Efficiency. Under Work Efficiency, 'Work Overtime' is selected. The main area displays a table of work overtime records. One record is shown in detail: Start Time 2022-05-05 13:00:00, End Time 2022-05-05 18:00:00, Type 补班补时 (Overtime), Employee ID Admin, Department 测试部, Hours 5.0, and Last Updated 2022-05-05 14:52:00. At the top of the table, there are several buttons: 新建 (New), 导入Excel (Import Excel), 下载Excel (Download Excel), 批量计算 (Batch Calculation), 检索 (Search), and a search input field. A red box highlights the 'Batch Calculation' button.

### 3.3.4.3 删除工作补时

选择要删除的工作补时，点击“批量操作>删除”按钮进行删除（删除已补时成功的工  
作补时数据，被补时的时长会还原，该用户的补时时长会清零）如下图所示：

This screenshot shows the same 'Work Efficiency Analysis' interface as the previous one, but with a modal dialog box in the center asking for confirmation to delete selected data. The dialog has a yellow warning icon and the text '确认删除' (Delete Confirmation) and '是否删除选中的数据?' (Are you sure you want to delete the selected data?). Below the dialog, the table of work overtime records is partially visible, showing two rows of data with checkboxes next to them. The 'Batch Operation' dropdown menu is open, and the 'Delete' option is highlighted.

### 3.3.5 饱和度配置

新增饱和度配置，将用户在主工作时间在工作时间内占比做一个比例展示为百分比，称  
为该用户的工作饱和度。且将不同范围内的占比分为：低，中，高三个等级展示到页面。

新增饱和度如下：

1: 饱和度名称：饱和度名称自主设置。

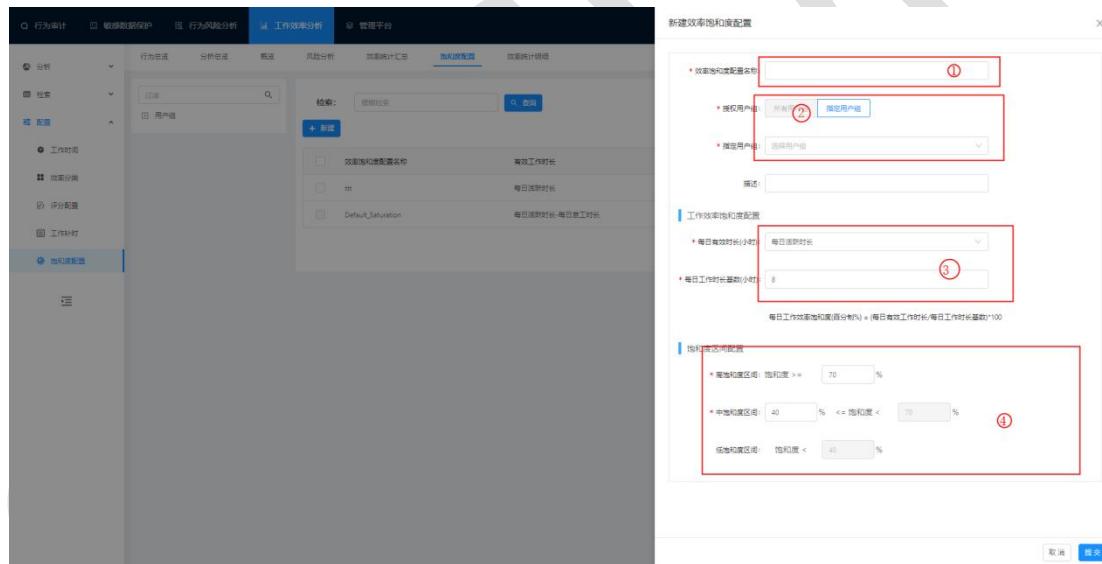
2: 指定用户组：全部用户组为所有用户组将以此饱和度设置计算饱和度。

选中指定用户组时候可选中一个或多个用户组，选中用户组将以此饱和度设置计算饱和度。

3. 工作效率饱和度配置：每日有效时长可选：每日活跃时长/每日活跃时长-每日怠工时长，每日工作时长基数为配置工作时间内的总时长，饱和度计算公式如下：

每日工作效率饱和度（百分制）=（每日有效工作时长/每日工作时长基数）\*100%；

4: 饱和度区间设置：设置的饱和度区间决定该区间内对应的饱和度等级。饱和度区间最大值为 100；最小值为 1。



### 3.3.6 效率检索明细

左边菜单过滤：输入过滤条件，选择效率分类、用户账号、终端名称等条件过滤。

条件搜索：可以选择快速过滤条件和基础操作过滤条件进行搜索。可以输入全文检索数据，也可以选择时间段查询数据。如下图所示：

The screenshot shows the 'Efficiency Details' tab selected. The interface includes a sidebar with filters for '分析' (Analysis), '检索' (Search), '效率明细' (Efficiency Details), and '配置' (Configuration). The main content area has a search bar and a summary table for '综合TOP10排序' (Comprehensive TOP10 Ranking) with columns for application name, cumulative time, days, work status, and average cumulative time percentage. Below the table are two pie charts: '工作状态工时分析(秒)' (Work Status Work Hours Analysis (Seconds)) and '用户行为分类工时分析(秒)' (User Behavior Classification Work Hours Analysis (Seconds)).

点击‘切换列表’可以跳转到效率明细列表界面进行查看数据；如下图所示：

This screenshot is identical to the one above, showing the 'Efficiency Details' tab selected. The '切换列表' button is highlighted with a red box at the bottom right of the search bar.

**注 1：非活跃数据需要去 Windows 记录策略的工作效率分析规则配置待机时长，默认是 120 秒；当终端超过 120 秒没有作任何操作，就会产生一条非活跃记录（非活跃时长=实际待机时长-120）。**

注 2：非工作，工作，其他需要去配置效率分类。

### 3.3.7 部门分析

部门效率分析是对部门的工作效率进行统计。

选择“分析>工作效率>部门效率分析”进入部门效率分析界面，如下图所示：

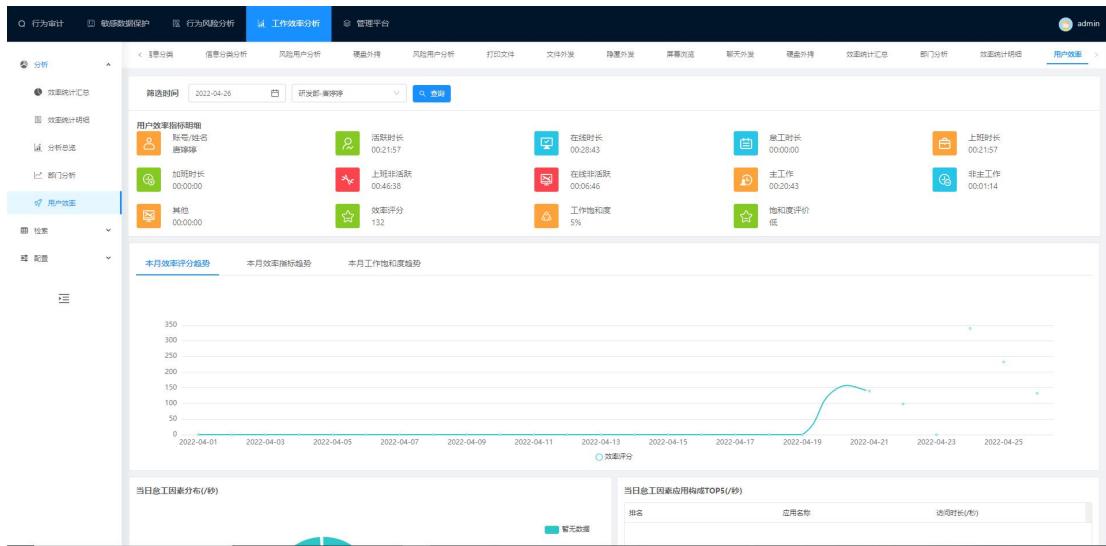
The screenshot shows the 'Department Efficiency Analysis' interface. On the left, there's a sidebar with navigation items: 行为审计, 效率数据保护, 行为风险分析, 工作效率分析 (highlighted in blue), and 管理平台. Under '工作效率分析', there are sub-options: 效率统计汇总, 效率统计明细, 部门分析 (highlighted in blue), 用户效率, 检索, and 配置. The main content area has a search bar at the top with '今天' selected. Below it is a table with two sections: '关键指标以人均时长为参考' and '效率评分趋势'. The first section shows average values for '总计人数' (3), '平均时长' (1.65 小时), and '平均工作时长' (28%). The second section shows '总计时长' (2.228 小时) and '总计工时长' (0 小时). At the bottom, there's a chart titled '效率评分趋势' with a legend for '效率评分' (0 to 210) and a date range from 2022-04-27 to 2022-04-27.

This screenshot shows the same 'Department Efficiency Analysis' interface as the previous one, but with different data. The main content area now features a large teal circle with the text '暂无数据' (No data available). To the right, there's a table titled '本月总工时长分布(1/秒)' with one entry: '1 货币数据'. Below this is a chart titled '用户分类(TOP5效率评分排名, 小于40分为低效, 40分-70分为尚好, 大于70分为高效)' with a legend for '高效' (blue bar), '尚好' (orange bar), and '低效' (red bar). A table below the chart shows the '效率TOP10排序' with columns: '低效排名', '高效排名', '尚好排名', '低效和尚好排名', and '尚好和低效排名'. The table has one entry: '1.43' under '低效排名'.

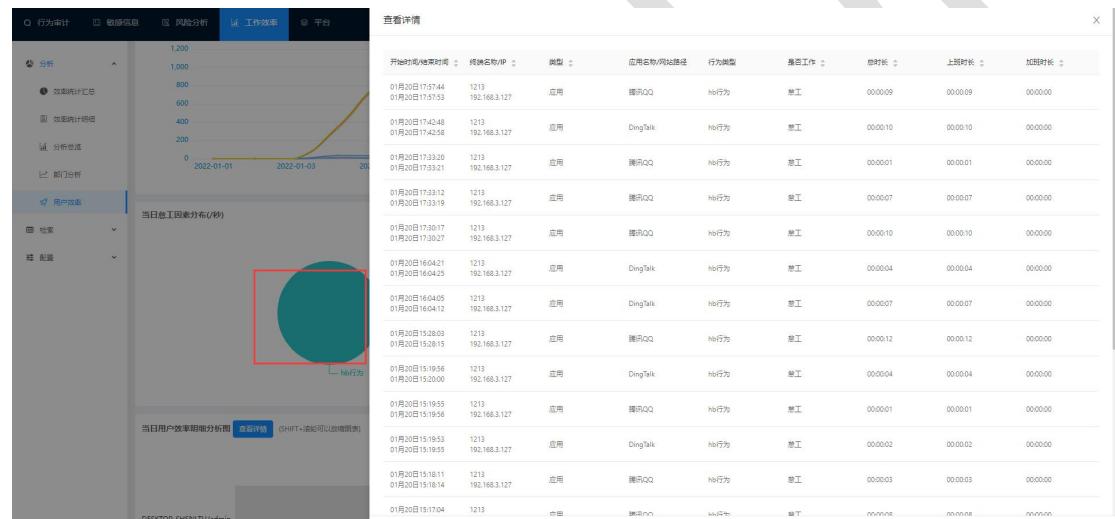
### 3.3.8 用户效率

用户效率是对单个用户的效率明细进行统计。

选择“分析>工作效率>用户效率”进入用户效率界面，如下图所示：



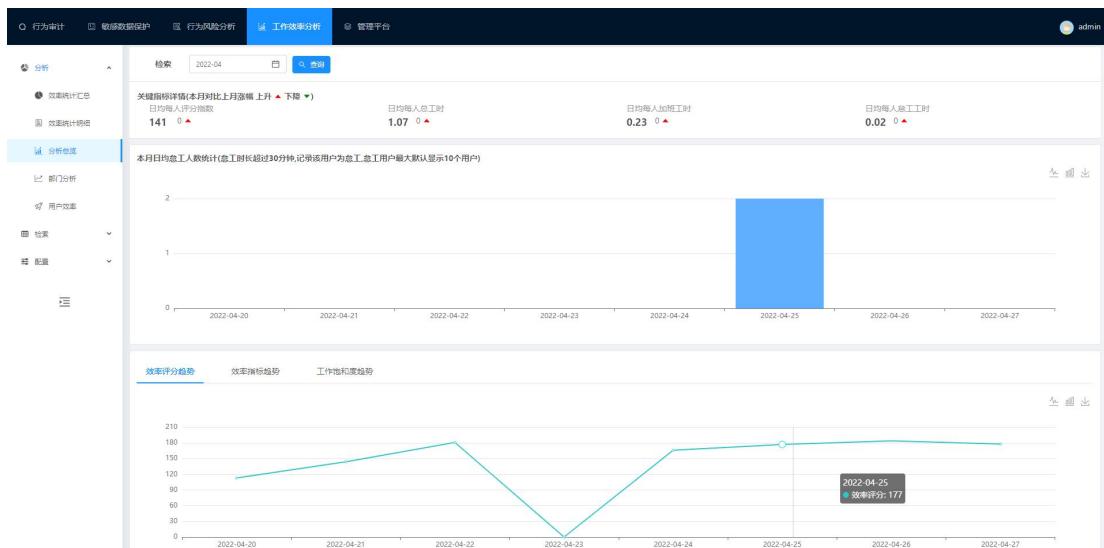
点击相应工时数据可以弹出效率明细详情窗口查看详情；例如：用户行为分类工时分析，点击要查看的行为分类饼图查看详情；如下图所示：



### 3.3.9 分析总览

分析总览是对效率统计汇总每月数据以图表的方式统计展示。

选择“分析>工作效率>分析总览”进入分析总览界面；如下图所示：

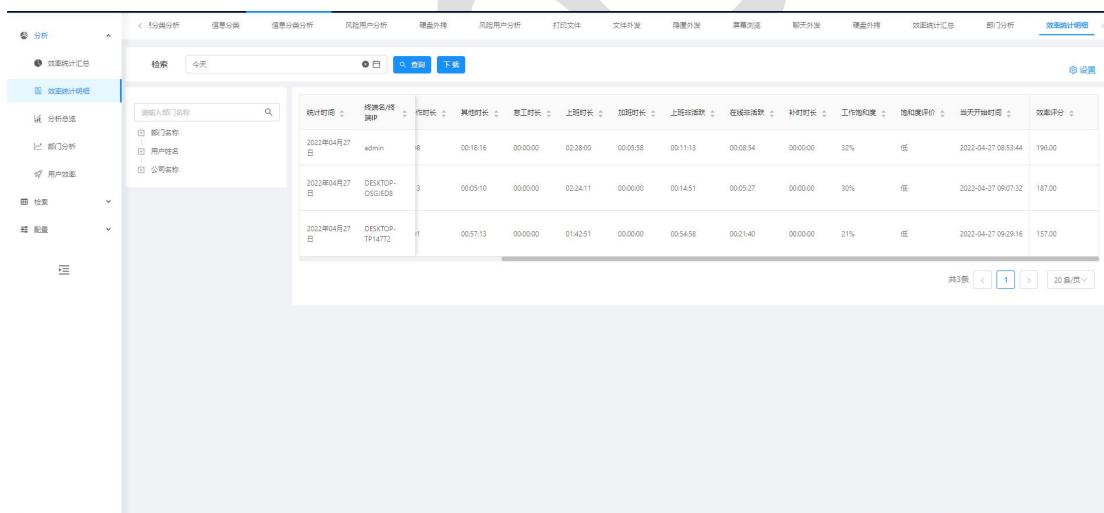


### 3.3.10 效率统计明细

效率统计明细是用户在终端操作的所有效率明细时长进行统计。

**提示:** 需先配置统计服务器、效率分类、效率统计插件才会有数据。

选择“工作效率>分析>效率统计明细”进入效率统计明细界面；如下图所示：



### 3.3.11 效率明细汇总

效率明细汇总是统计每个终端用户以部门月维度、部门天维度、用户月维度、总用户月维度、总用户天维度、公司月维度、公司天维度的方式对用户总时长、非主工作、主工作、

怠工、上班、加班等时长进行统计；如图所示：

**提示：需先配置统计服务器、效率分类、效率统计插件才会有数据。**

选择“分析>工作效率>效率明细”进入效率统计汇总界面；如下图所示：

The screenshot shows the 'Efficiency Summary' interface. At the top, there are tabs for 'Behavior Audit', 'Data Protection', 'Risk Analysis', 'Efficiency Analysis', and 'Management Platform'. The 'Efficiency Analysis' tab is selected. Below the tabs, there are several filter options: 'Data Type' (All Work), 'Department Month Dimension', 'Department Day Dimension', 'User Month Dimension', 'User Day Dimension', 'Public Month Dimension', and 'Public Day Dimension'. A search bar with 'Today' and 'Search' buttons is present. On the left, there is a sidebar with sections for 'Analysis' (selected), 'Efficiency Summary' (selected), 'Analysis Color Map', 'Front-end Analysis', 'User Efficiency', 'Search', and 'Configuration'. The main content area displays a table of efficiency data:

统计时间	统计部门公司	计算参数	数据类型	总时长	得分	怠工时长	上班时长	加班时长	怠工人数	主工作时长	非主工作时长
2023年04月27日	部门：研发部	1	部门天维度	31%	194.00	02:28:12	02:23:14	00:05:58	000000	0人	02:06:48
2023年04月27日	部门：市场部	2	部门天维度	24%	170.00	01:58:39	01:58:39	00:00:00	000000	0人	01:20:00
2023年04月27日		3	总用户天维度	26%	178.00	02:08:50	02:06:51	00:01:59	000000	0人	01:35:36
2023年04月27日	公司：比亚迪	3	公共天维度	26%	178.00	02:08:50	02:06:51	00:01:59	000000	0人	01:35:36

At the bottom right, there is a page number '共4页' and a '1' button.

下载按钮：可以下载成 excel 文档格式进行查看。

总时长=上班时长+加班时长。

上班非活跃=工作时间段内离线时长之和。

加班时长=工作时间段外离线时长之和。

活跃时长：用户当天所有工作状态应用或网站时长之和。

在线时长：终端 00:00-23:59 分内的活跃时长+在线非活跃时长。

怠工时长：用户当天工作状态为怠工的应用或网站时长之和。

上班时长：用户所配置工作时间的上班时长内的活跃时长。

上班非活跃：用户所配置上班时间内离线+在线非活跃时长。

在线非活跃：用户一天内终端离线+非活跃时长。

主工作：用户当天工作状态为主工作应用或网站时长之和。

非主工作：用户当天工作状态为非主工作应用或网站时长之和。

其他：用户当天工作状态为其他应用或网站时长之和。

部门月维度：统计部门当月效率汇总的平均值。

部门天维度：统计部门当天效率汇总的平均值。

用户月维度：统计每个用户的当月效率汇总的平均值。

总用户天维度：统计所有用户的当天效率汇总的平均值。

总用户月维度：统计所有用户的当月效率汇总的平均值。

公司月维度：统计公司的当月效率汇总的平均值。

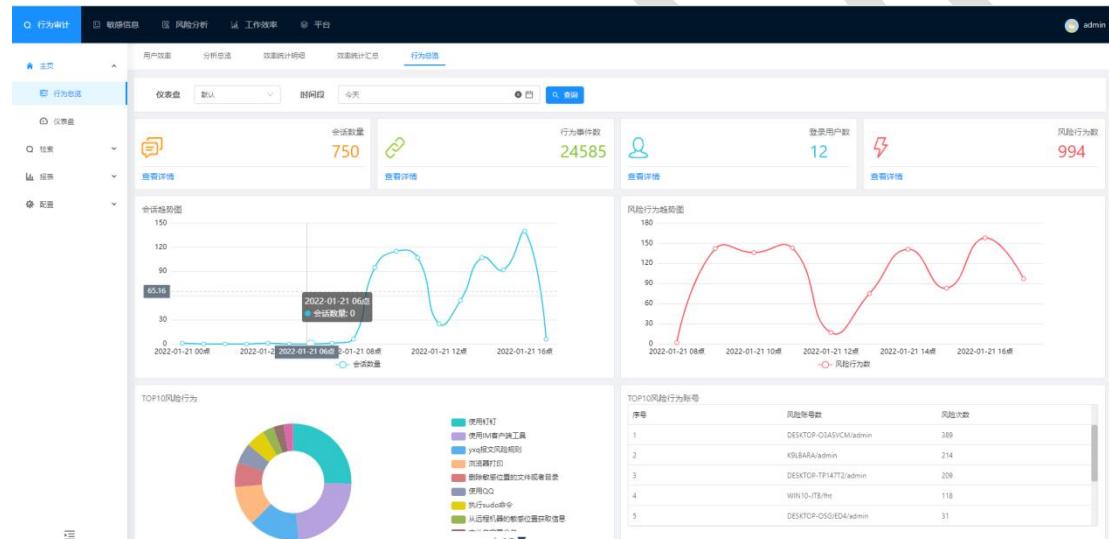
公司天维度：统计公司的当天效率汇总的平均值。

## 4 行为审计

### 4.1 主页（行为总览）

主页是终端操作的行为数据以图表的形式展示。

点击“主页”按钮，进入主页查看详情；如下图所示：



检索：终端的行为操作审计数据展示；分为‘会话数据’和‘行为数据’两大类。

#### 4.1.1 主页详情

可点击“查看详情”按钮查看对应数据相应；也可以点击趋势图和图表查看数据详情；  
如下图所示：

The screenshot shows the AuditSys behavioral audit interface. On the left, there's a sidebar with navigation tabs: 行为审计 (Behavior Audit), 数据信息 (Data Information), 风险分析 (Risk Analysis), 工作效率 (Work Efficiency), and 平台 (Platform). The main area has a title '行为审计' (Behavior Audit) and a sub-section '会话检索' (Session Search). A chart titled '会话数量' (Session Count) shows a sharp increase from 0 to 750 over time. Below it is a donut chart labeled 'TOP10风险行为' (Top 10 Risky Behaviors). To the right is a table titled '会话详细' (Session Details) with columns: '发生时间' (Occurrence Time), '风险终端名称/IP' (Risk Terminal Name/IP), '风险账号/登录IP' (Risk Account/Login IP), '操作类型' (Operation Type), '风险名称' (Risk Name), and '风险类型' (Risk Type). The table lists 15 rows of session data, with the 16th row being the current selection, indicated by a red arrow.

## 4.2 会话检索

会话检索是录制用户在终端操作行为进行审计记录。

选择“检索>会话检索”进入会话检索界面；如下图所示：

The screenshot shows the AuditSys session search interface. At the top, there's a navigation bar with 'AuditSys' and various menu items like '主页' (Home), '搜索' (Search), '分析' (Analysis), '报表' (Report), '管理' (Management), '配置' (Configuration), '系统' (System), and '监控' (Monitoring). The user 'admin' is logged in. The main area has a title '会话检索' (Session Search) and a sub-section '会话数据' (Session Data). There are two tabs: '会话数据' (Session Data) and '行为数据' (Behavior Data). Below is a '分类过滤' (Category Filter) section with options like '全部会话' (All Sessions), '断线会话' (Lost Session), '正在录制' (Recording), '已尚成会话' (Completed Session), '已归档会话' (Archived Session), 'Linux会话' (Linux Session), and '屏幕会话' (Screen Session). A search bar with '全文检索' (Full-text search) and '最近三天' (Last three days) is followed by buttons for '清空' (Clear), '查询' (Search), '高级查询' (Advanced Query), and '导出数据' (Export Data). The main table is titled '类别 (TOP20)' (Category (TOP20)) and lists sessions with columns: '最近时间' (Recent Time), '终端名称/IP' (Terminal Name/IP), '部门/用户名' (Department/User Name), '用户名/登录IP' (User Name/Login IP), '会话类型' (Session Type), '登录类型' (Login Type), '会话状态' (Session Status), '耗时' (Duration), and '操作' (Operation). The table lists 10 sessions, each with a small triangle icon for sorting.

### 4.2.1 会话查询

左边类别菜单过滤：输入过滤条件或选择用户账号、终端地址、终端名称、部门等条件过滤。输入全文检索内容查询，也可以选择‘分类过滤’、‘时间段’、‘高级查询’进行过滤。点击列表上三角形图案进行排序；如下图所示：

分类 (TOP20)

起止时间	终端名称/IP	部门/用户名	用户账号/登录IP	会话类型	登录类型	会话状态	帧数	操作
01月21日17:12:32	WIN10-JTB 192.168.0.254	射手 卢西安	WIN10-JTB:80 localhost	联网会话	本地登录	录制中	0	
01月21日17:12:28	DESKTOP-0SGIED4 192.168.0.129	华为 星辰之影	DESKTOP-0SGIED4\admin localhost	联网会话	本地登录	录制中	0	
01月21日17:12:21	DESKTOP-C3ASVCM 192.168.3.193	研究员 卢西安	DESKTOP-C3ASVCM\admin localhost	联网会话	本地登录	录制中	0	
01月21日17:11:55	K9JBARA 192.168.4.145	法师 亚索	K9JBARA\admin localhost	联网会话	本地登录	录制中	0	
01月21日17:11:45 01月21日17:12:32	WIN10-JTB 192.168.0.254	射手 卢西安	WIN10-JTB:80 localhost	联网会话	本地登录	已完成	100	
01月21日17:10:30 01月21日17:11:34	K9JBARA 192.168.4.145	法师 亚索	K9JBARA\admin localhost	联网会话	本地登录	已完成	23	
01月21日17:09:08 01月21日17:09:09	K9JBARA 192.168.4.145	法师 亚索	K9JBARA\admin localhost	联网会话	本地登录	已完成	23	
01月21日17:08:44 01月21日17:08:46	K9JBARA 192.168.4.145	法师 亚索	K9JBARA\admin localhost	联网会话	本地登录	已完成	2	
01月21日17:08:35 01月21日17:11:44	WIN10-JTB 192.168.0.254	射手 卢西安	WIN10-JTB:80 localhost	联网会话	本地登录	已完成	100	
01月21日17:07:50 01月21日17:12:20	DESKTOP-C3ASVCM 192.168.3.193	研究员 卢西安	DESKTOP-C3ASVCM\admin localhost	联网会话	本地登录	已完成	100	

点击会话检索内容的‘终端名称/IP、部门/用户名、用户账号/登录 IP’也可以查询；如下图所示：

用户姓名: 卢西安 X 终端名称: WIN10-JTB X 用户账号: WIN10-JTB:80 X

分类 (TOP20)

起止时间	终端名称/IP	部门/用户名	用户账号/登录IP	会话类型	登录类型	会话状态	帧数	操作
01月21日17:13:54	WIN10-JTB 192.168.0.254	射手 卢西安	WIN10-JTB:80 localhost	联网会话	本地登录	录制中	0	
01月21日17:12:32	WIN10-JTB 192.168.0.254	射手 卢西安	WIN10-JTB:80 localhost	联网会话	本地登录	已完成	100	
01月21日17:11:45 01月21日17:12:32	WIN10-JTB 192.168.0.254	射手 卢西安	WIN10-JTB:80 localhost	联网会话	本地登录	已完成	100	
01月21日17:08:35 01月21日17:11:44	WIN10-JTB 192.168.0.254	射手 卢西安	WIN10-JTB:80 localhost	联网会话	本地登录	已完成	100	
01月21日17:07:15 01月21日17:08:34	WIN10-JTB 192.168.0.254	射手 卢西安	WIN10-JTB:80 localhost	联网会话	本地登录	已完成	100	
01月21日17:05:34 01月21日17:07:15	WIN10-JTB 192.168.0.254	射手 卢西安	WIN10-JTB:80 localhost	联网会话	本地登录	已完成	100	
01月21日17:03:34 01月21日17:05:34	WIN10-JTB 192.168.0.254	射手 卢西安	WIN10-JTB:80 localhost	联网会话	本地登录	已完成	100	
01月21日17:02:11 01月21日17:03:34	WIN10-JTB 192.168.0.254	射手 卢西安	WIN10-JTB:80 localhost	联网会话	本地登录	已完成	100	
01月21日17:00:31 01月21日17:02:11	WIN10-JTB 192.168.0.254	射手 卢西安	WIN10-JTB:80 localhost	联网会话	本地登录	已完成	100	

## 4.2.2 会话播放

单屏会话：点击“”按钮进行播放。

多屏会话：可以选择全屏播放和播放不同的分屏。全屏播放则点击“”，分屏播放则点击“”，然后选择要播放的屏幕号。

提示：会话记录没有“”按钮，是终端的记录策略没有勾选是否录像。如下图所示：

播放画面：点击 可以查看按键事件信息；点击 拉出播放列表信息和会话列表信息，可以选择播放列表信息进行播放，也可以选择会话列表信息进行播放；还可以选择播放倍速；

点击 播放下一个会话；点击 播放上一个会话；点击 播放上一帧；点击 播放下一帧；点击 开始播放；点击“打包”按钮可以进行视频下载。如下图所示：

### 4.2.3 会话明细

点击“+”按钮可以展开查看会话明细。带“”是该会话明细存在风险行为；会话明细中“播放”按钮，可以直接播放到该事件的帧位置画面。如下图所示：

The screenshot shows a web-based monitoring or audit interface. At the top, there are tabs for '行为审计' (Behavior Audit), '数据信息' (Data Information), '风险分析' (Risk Analysis), '工作效率' (Work Efficiency), and '平台' (Platform). The '行为审计' tab is selected. On the left, there are navigation menus for '主页' (Home), '检索' (Search), and '会话检索' (Conversation Search). Under '会话检索', there are sub-options: '会话检索' (Conversation Search), '会议检索' (Meeting Search), and '视图下载' (View Download). The main content area displays two tables. The first table lists conversations with columns: 起始时间 (Start Time), 终端名称/终端IP (Terminal Name/Terminal IP), 部门/用户名 (Department/User Name), 用户账号/登录IP (User Account/Login IP), 会话类型 (Session Type), 登录类型 (Login Type), 会话状态 (Session Status), and 操作 (Operation). The second table lists application activity with columns: 应用名称 (Application Name), 标签名称 (Label Name), 发生时间 (Occurrence Time), and 操作 (Operation). A red box highlights the 'WPS Office' entry in the application activity table.

## 4.2.4 导出数据

导出数据：把会话检索页面数据导出以 excel 文档格式显示。

可以先查询要导出的数据，再点击导出数据按钮；如下图所示：

This screenshot shows the same 'Conversation Search' interface as the previous one, but with a focus on the export functionality. The '会话检索' tab is selected. In the bottom right corner of the main content area, there is a red box highlighting the '导出数据' (Export Data) button. The rest of the interface is identical to the previous screenshot, showing the conversation list and application activity tables.

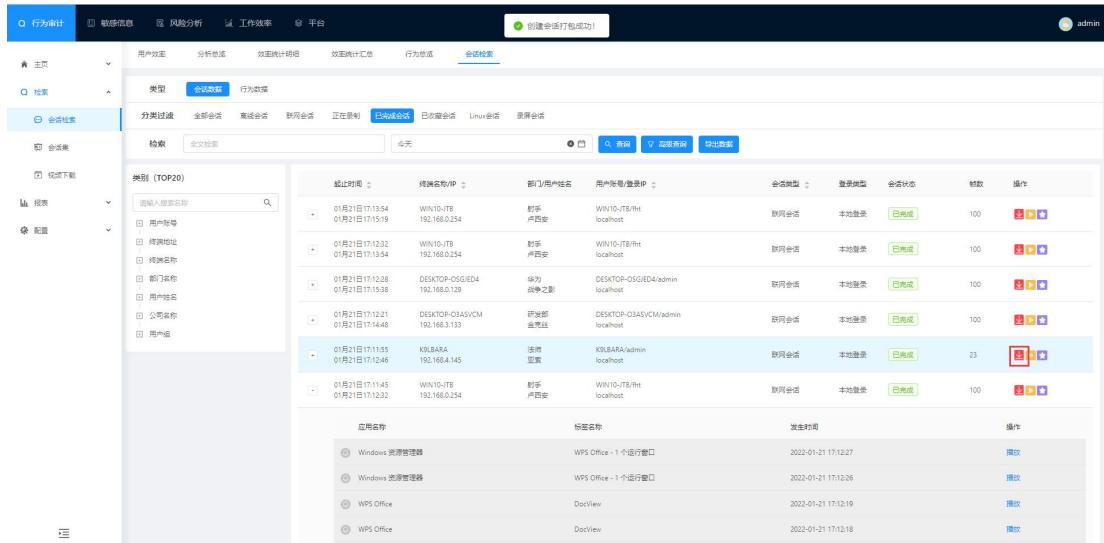
导出数据以 excel 文档格式显示，如下图所示：

This screenshot shows an Excel spreadsheet titled '会话检索 (3).csv'. The data is organized into several columns: 起始时间 (Start Time), 终端名称/终端IP (Terminal Name/Terminal IP), 部门/用户名 (Department/User Name), 用户账号/登录IP (User Account/Login IP), 会话类型 (Session Type), 登录类型 (Login Type), 会话状态 (Session Status), and 次数 (Count). The data consists of multiple rows of conversation logs, such as '2021-10-28 10:40:45至2021-10-28 10:43:29 WIN10-JTB 192.168.3.115 法师 审判天使|卡尔WIN10-JTB/fht localhost 联网会话 本地登录 已完成 100'.

## 4.3.5 视频下载

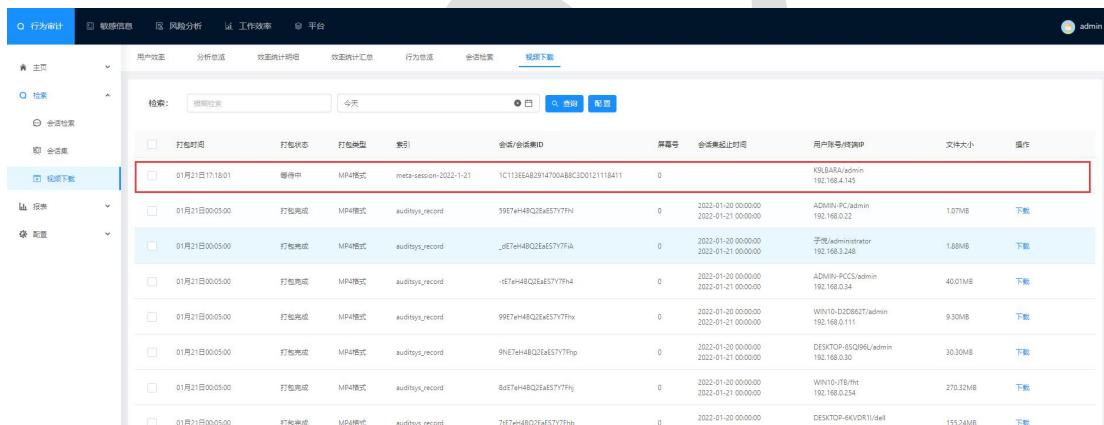
视频下载：把打包完成的会话视频数据，下载到本地进行播放。

点击“”下载按钮，把会话数据以 mp4 格式打包到视频下载界面；如下图所示：



The screenshot shows a web-based management interface for video download. At the top, there are tabs for '行为审计' (Behavior Audit), '敏感信息' (Sensitive Information), '风险分析' (Risk Analysis), '工作效率' (Work Efficiency), and '平台' (Platform). The '行为审计' tab is selected. Below the tabs, there are sections for '会话检索' (Session Search) and '视频下载' (Video Download). The '会话检索' section includes a search bar, date range, and filter buttons for '会话类型' (Session Type) like '会话集' (Session Set) and '行为会话' (Behavior Session). The '视频下载' section has a '类别 (TOP20)' dropdown menu with options such as '输入设备名称' (Input Device Name), '用户名' (User Name), '终端地址' (Terminal Address), '终端名称' (Terminal Name), '部门名称' (Department Name), '岗位名称' (Job Position), '公司名称' (Company Name), and '用户组' (User Group). A table lists session details: 起止时间 (Start/End Time), 终端名称/IP (Terminal Name/IP), 部门/用户名 (Department/User Name), 用户账号/登录IP (User Account/Login IP), 会话类型 (Session Type), 集会状态 (Meeting Status), 会议状态 (Meeting Status), 帧数 (Frame Count), and 操作 (Operation). One row is highlighted in blue. Below the table is a smaller table for application logs: 应用名称 (Application Name), 标签名称 (Label Name), 发生时间 (Occurrence Time), and 操作 (Operation). One row is highlighted in blue.

点击“检索>视频下载”进入视频下载界面，点击‘下载’按钮，可以把打包完成的视频下载到本地（注：只有下载打包‘会话集’的会话视频才会显示会话集起止时间）如下图所示：



This screenshot shows the 'Video Download' interface after performing a search. The '检索' (Search) field contains '视频下载'. The table below lists recorded sessions with a red border around the first row. The columns include: 打包时间 (Packaging Time), 打包状态 (Packaging Status), 打包类型 (Packaging Type), 索引 (Index), 会话/会话集ID (Session/Session Set ID), 屏幕号 (Screen Number), 会话集起止时间 (Session Set Start/End Time), 用户账号/终端IP (User Account/Terminal IP), 文件大小 (File Size), and 操作 (Operation). The first row is highlighted with a red border. The other rows show various session details, such as session IDs starting with 'meta-session-' or 'auditlog\_record'.

## 4.3 行为数据

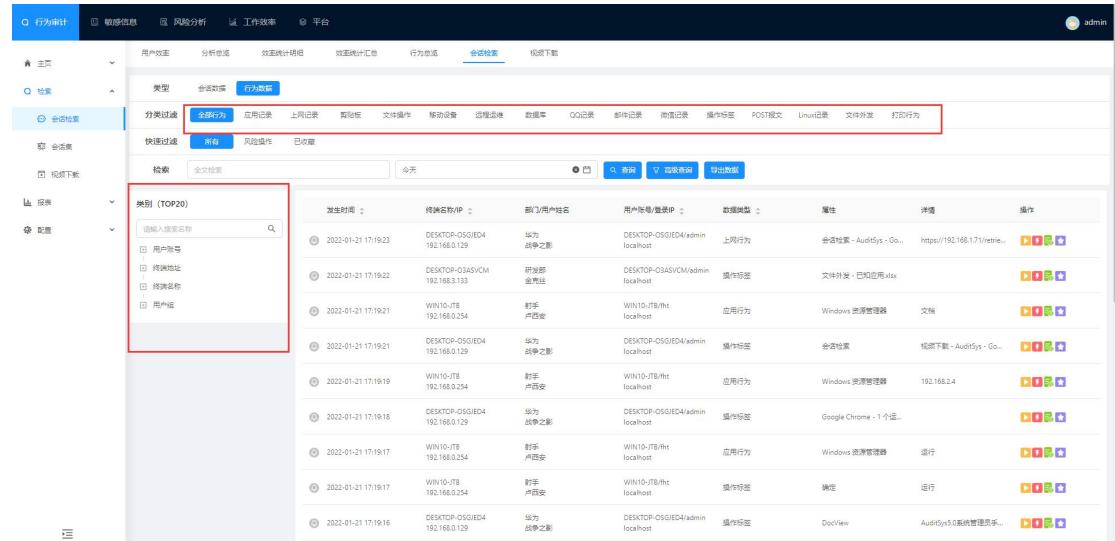
行为数据：对终端的操作所有行为审计记录。

全部行为：对终端的操作所有行为审计记录。

### 4.3.1 行为数据查询

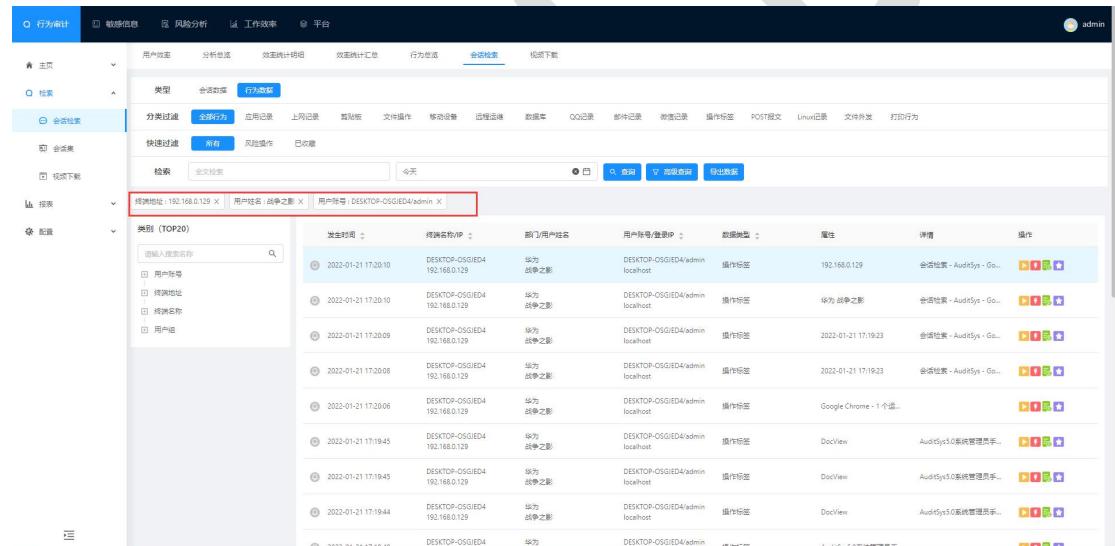
左边类别菜单过滤：输入过滤条件，可以选择用户账户、终端地址、终端名称、用户组

进行过滤；也可以选择快速过滤、全文检索、时间段、高级查询进行查询。点击列表上三角形图案进行排序；带‘'是风险行为数据；如下图所示：



The screenshot shows the 'Behavior Audit' section of a web-based monitoring system. The top navigation bar includes tabs for '行为审计' (Behavior Audit), '敏感信息' (Sensitive Information), '风险分析' (Risk Analysis), '工作效率' (Work Efficiency), and '平台' (Platform). The '行为审计' tab is selected. Below the navigation is a search bar with a placeholder '会话检索' (Session Search) and a date range '今天' (Today). A red box highlights the '会话检索' tab and the search bar. The main content area displays a table titled '类别 (TOP20)' (Category TOP20) with 20 rows of session data. Each row includes columns for '发生时间' (Occurrence Time), '终端名称/IP' (Terminal Name/IP), '部门/用户名' (Department/User Name), '用户账号/登录IP' (User Account/Login IP), '数据类型' (Data Type), '属性' (Attribute), '详情' (Details), and '操作' (Operation). The first few rows show sessions from 'DESKTOP-0SGIED4' and 'WIN10-7B-BT' terminals, with various user names like 'admin' and '��争之影'.

点击会话检索内容的‘终端名称/IP、部门/用户名、用户账号/登录 IP’也可以查询；如下图所示：



This screenshot is similar to the previous one but with specific filters applied in the search bar. The search bar now contains three entries: '终端地址: 192.168.0.129', '用户名: DESKTOP-0SGIED4\admin', and '用户账号: DESKTOP-0SGIED4\admin'. A red box highlights these filter inputs. The rest of the interface and data table are identical to the first screenshot.

### 4.3.2 行为数据播放

点击“>”按钮播放。提示：行为数据记录没有“>”按钮，是终端的记录策略没有勾选是否录像。行为数据播放都是定帧播放。如下图所示：

The screenshot displays two windows of the AuditSys system. The top window is a list view of behavioral data, likely network logs, with columns for '发生时间' (Time), '终端设备/IP' (Terminal Device/IP), '前段用户名' (Front-end Username), '用户账号/登录IP' (User Account/Login IP), '数据类型' (Data Type), '属性' (Attributes), '详情' (Details), and '操作' (Operations). The bottom window is a detailed view of a specific log entry, showing expanded fields such as '终端设备/IP' (Terminal Device/IP), '前段用户名' (Front-end Username), '用户账号/登录IP' (User Account/Login IP), '数据类型' (Data Type), '属性' (Attributes), '详情' (Details), and '操作' (Operations). The expanded details include the URL (<https://192.168.1.71/player?param=meta-metadata-2022-1-21%7C%7C0449BE591CEC4fdeA72B82AED640222F&findex=44&ticket=0&isGoto=1&screenno=1&...>), '浏览器' (Browser) as 'AuditSys - Google Chrome', and '操作系统' (Operating System) as 'Windows 资源管理器'.

### 4.3.3 行为数据明细

点击“”按钮弹出行为数据明细窗口界面查看明细详情。如下图所示：

#### 4.3.4 快捷新建风险规则

点击“”按钮，会弹出新建风险规则窗口。如下图所示：

#### 4.3.5 行为数据收藏

点击“”按钮，可以对此行为数据进行收藏，点击“”按钮取消收藏；如下图所示：

The screenshot shows the 'Behavior Audit' interface with the 'Export Data' button highlighted in red. The interface includes various filters and a table of audit logs.

发生时间	终端名称/IP	部门/用户名	用户账号/登录IP	数据类型	属性	详情	操作
2022-01-21 17:20:10	DESKTOP-0SGIED4 192.168.0.129	华为 战争之影	DESKTOP-0SGIED4/admin localhost	操作标签	192.168.0.129	会话结束 - AuditSys - Go...	
2022-01-21 17:20:10	DESKTOP-0SGIED4 192.168.0.129	华为 战争之影	DESKTOP-0SGIED4/admin localhost	操作标签	华为 战争之影	会话结束 - AuditSys - Go...	
2022-01-21 17:20:09	DESKTOP-0SGIED4 192.168.0.129	华为 战争之影	DESKTOP-0SGIED4/admin localhost	操作标签	2022-01-21 17:19:23	会话结束 - AuditSys - Go...	
2022-01-21 17:20:08	DESKTOP-0SGIED4 192.168.0.129	华为 战争之影	DESKTOP-0SGIED4/admin localhost	操作标签	2022-01-21 17:19:23	会话结束 - AuditSys - Go...	
2022-01-21 17:20:06	DESKTOP-0SGIED4 192.168.0.129	华为 战争之影	DESKTOP-0SGIED4/admin localhost	操作标签	Google Chrome - 1 个进...	AuditSys3.0系统管理员手...	
2022-01-21 17:19:45	DESKTOP-0SGIED4 192.168.0.129	华为 战争之影	DESKTOP-0SGIED4/admin localhost	操作标签	DocView	AuditSys3.0系统管理员手...	
2022-01-21 17:19:45	DESKTOP-0SGIED4 192.168.0.129	华为 战争之影	DESKTOP-0SGIED4/admin localhost	操作标签	DocView	AuditSys3.0系统管理员手...	
2022-01-21 17:19:44	DESKTOP-0SGIED4 192.168.0.129	华为 战争之影	DESKTOP-0SGIED4/admin localhost	操作标签	DocView	AuditSys3.0系统管理员手...	
2022-01-21 17:19:44	DESKTOP-0SGIED4	华为	DESKTOP-0SGIED4/admin	stUser			

## 4.3.6 导出数据

导出数据：把行为数据导出以 excel 文档格式显示。

可以先查询要导出的数据，再点击导出数据按钮；如下图所示：

The screenshot shows the 'Behavior Audit' interface with the 'Export Data' button highlighted in red. A red box highlights the 'Behavior Data (25).csv' link at the bottom left of the page.

导出数据以 excel 文档格式显示，如下图所示：

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
1	高危	起始时间	结束时间	部门	用户名	/	权限类型	属性	详细																		
2	无风险	*****DESKTOP-华为	战争	DESKTOP-C	操作者名	Google Chrome - 1 个运行窗口																					
3	无风险	*****DESKTOP-华为	战争	DESKTOP-C	操作者名	AudiSys&AudiSys5.0系统管理员手册-前字强.docx - WPS Office																					
4	无风险	*****DESKTOP-华为	战争	DESKTOP-C	操作者名	AudiSys&AudiSys5.0系统管理员手册-前字强.docx - WPS Office																					
5	无风险	*****DESKTOP-华为	战争	DESKTOP-C	操作者名	AudiSys&AudiSys5.0系统管理员手册-前字强.docx - WPS Office																					
6	无风险	*****DESKTOP-华为	战争	DESKTOP-C	操作者名	AudiSys&AudiSys5.0系统管理员手册-前字强.docx - WPS Office																					
7	无风险	*****DESKTOP-华为	战争	DESKTOP-C	操作者名	DocView AudiSys5.0系统管理员手册-前字强.docx - WPS Office																					
8	无风险	*****DESKTOP-华为	战争	DESKTOP-C	操作者名	AudiSys&AudiSys5.0系统管理员手册-前字强.docx - WPS Office																					
9	无风险	*****DESKTOP-华为	战争	DESKTOP-C	操作者名	WPS Office - 1 个运行窗口																					
10	无风险	*****DESKTOP-华为	战争	DESKTOP-C	操作者名	WPS Office - 1 个运行窗口																					
11	无风险	*****DESKTOP-华为	战争	DESKTOP-C	操作者名	WPS Office - 1 个运行窗口																					
12	无风险	*****DESKTOP-华为	战争	DESKTOP-C	操作者名	WPS Office - 1 个运行窗口																					
13	无风险	*****DESKTOP-华为	战争	DESKTOP-C	操作者名	Google Chrome - 1 个运行窗口																					
14	无风险	*****DESKTOP-华为	战争	DESKTOP-C	操作者名	AudiSys&AudiSys5.0系统管理员手册-前字强.docx - WPS Office																					
15	无风险	*****DESKTOP-华为	战争	DESKTOP-C	操作者名	AudiSys&AudiSys5.0系统管理员手册-前字强.docx - WPS Office																					
16	无风险	*****DESKTOP-华为	战争	DESKTOP-C	操作者名	AudiSys&AudiSys5.0系统管理员手册-前字强.docx - WPS Office																					
17	无风险	*****DESKTOP-华为	战争	DESKTOP-C	操作者名	AudiSys&AudiSys5.0系统管理员手册-前字强.docx - WPS Office																					
18	无风险	*****DESKTOP-华为	战争	DESKTOP-C	操作者名	AudiSys&AudiSys5.0系统管理员手册-前字强.docx - WPS Office																					
19	无风险	*****DESKTOP-华为	战争	DESKTOP-C	操作者名	AudiSys&AudiSys5.0系统管理员手册-前字强.docx - WPS Office																					
20	无风险	*****DESKTOP-华为	战争	DESKTOP-C	操作者名	DocView AudiSys5.0系统管理员手册-前字强.docx - WPS Office																					
21	无风险	*****DESKTOP-华为	战争	DESKTOP-C	操作者名	DocView AudiSys5.0系统管理员手册-前字强.docx - WPS Office																					
22	无风险	*****DESKTOP-华为	战争	DESKTOP-C	操作者名	DocView AudiSys5.0系统管理员手册-前字强.docx - WPS Office																					
23	无风险	*****DESKTOP-华为	战争	DESKTOP-C	操作者名	DocView AudiSys5.0系统管理员手册-前字强.docx - WPS Office																					
24	无风险	*****DESKTOP-华为	战争	DESKTOP-C	操作者名	DocView AudiSys5.0系统管理员手册-前字强.docx - WPS Office																					
25	无风险	*****DESKTOP-华为	战争	DESKTOP-C	操作者名	腾讯QQ - 腾大天哥																					
26	有风险	*****DESKTOP-华为	战争	DESKTOP-C	操作者名	腾讯QQ - 腾大天哥																					
27	无风险	*****DESKTOP-华为	战争	DESKTOP-C	操作者名	麦讯QQ - 1 个运行窗口																					
28	无风险	*****DESKTOP-华为	战争	DESKTOP-C	操作者名	WPS Office - 1 个运行窗口																					
29	无风险	*****DESKTOP-华为	战争	DESKTOP-C	操作者名	Google Chrome - 1 个运行窗口																					
30	无风险	*****DESKTOP-华为	战争	DESKTOP-C	操作者名	AudiSys&AudiSys5.0系统管理员手册-前字强.docx - WPS Office																					
31	无风险	*****DESKTOP-华为	战争	DESKTOP-C	操作者名	DocView AudiSys5.0系统管理员手册-前字强.docx - WPS Office																					
32	无风险	*****DESKTOP-华为	战争	DESKTOP-C	操作者名	AudiSys&AudiSys5.0系统管理员手册-前字强.docx - WPS Office																					
33	无风险	*****DESKTOP-华为	战争	DESKTOP-C	操作者名	AudiSys&AudiSys5.0系统管理员手册-前字强.docx - WPS Office																					
34	无风险	*****DESKTOP-华为	战争	DESKTOP-C	操作者名	AudiSys&AudiSys5.0系统管理员手册-前字强.docx - WPS Office																					
35	无风险	*****DESKTOP-华为	战争	DESKTOP-C	操作者名	AudiSys&AudiSys5.0系统管理员手册-前字强.docx - WPS Office																					
36	无风险	*****DESKTOP-华为	战争	DESKTOP-C	操作者名	AudiSys&AudiSys5.0系统管理员手册-前字强.docx - WPS Office																					
37	无风险	*****DESKTOP-华为	战争	DESKTOP-C	操作者名	AudiSys&AudiSys5.0系统管理员手册-前字强.docx - WPS Office																					
38	无风险	*****DESKTOP-华为	战争	DESKTOP-C	操作者名	WPS Office - 1 个运行窗口																					
39	无风险	*****DESKTOP-华为	战争	DESKTOP-C	操作者名	QQ - 会话搜索 - AudiSys - Google Chrome																					
40	无风险	*****DESKTOP-华为	战争	DESKTOP-C	操作者名	会话搜索 - https://192.168.1.71/retrieval/session																					
41	无风险	*****DESKTOP-华为	战争	DESKTOP-C	操作者名	Google Chrome - 1 个运行窗口																					
42	无风险	*****DESKTOP-华为	战争	DESKTOP-C	操作者名	Google Chrome - 1 个运行窗口																					
43	无风险	*****DESKTOP-华为	战争	DESKTOP-C	操作者名	AudiSys&AudiSys5.0系统管理员手册-前字强.docx - WPS Office																					
44	无风险	*****DESKTOP-华为	战争	DESKTOP-C	操作者名	AudiSys&AudiSys5.0系统管理员手册-前字强.docx - WPS Office																					

## 4.3.7 应用记录

应用记录针对所有的审计记录，按照应用类型进行分类统计，以便于管理员查找应用程序操作记录。

The screenshot shows a detailed audit log for a specific user ('\*\*\*\*\*DESKTOP-华为') over a period from January 21, 2022, to January 22, 2022. The log includes various system events such as file operations (e.g., 'AudiSys&AudiSys5.0系统管理员手册-前字强.docx - WPS Office'), network connections (e.g., 'QQ - 会话搜索 - AudiSys - Google Chrome'), and browser activity (e.g., 'Google Chrome - 1 个运行窗口'). Each entry provides details like the event type, timestamp, source IP, destination IP, application name, and a visual representation of the session.

发生时间	终端名称/IP	部门/用户姓名	用户账号/登录IP	应用名称	窗口图标	操作
2022-01-21 17:26:11	DESKTOP-03ASVCM	研究院 金昊	DESKTOP-03ASVCM/admin	Google Chrome		CAE #6690 [V5.0] [本地连接]
2022-01-21 17:25:53	1213	华为	1213	DESKTOP-TP14772/admin		外发文件检索 - AudiSys - Google Chrome
2022-01-21 17:25:47	DESKTOP-0SGIED4	华为 战争之影	DESKTOP-0SGIED4/admin	WPS Office		行为数据 (25).csv - WPS Office
2022-01-21 17:25:08	DESKTOP-0SGIED4	华为 战争之影	DESKTOP-0SGIED4/admin	Google Chrome		会议检索 - AudiSys - Google Chrome
2022-01-21 17:25:08	192.168.1.145	法博 亚蒙	192.168.1.145	Windows 资源管理器		Program Manager
2022-01-21 17:25:04	192.168.1.145	法博 亚蒙	192.168.1.145	WeChat		图片查看
2022-01-21 17:24:55	1213	华为	1213	DESKTOP-TP14772/admin		行为时间检索 - AudiSys - Google Chrome
2022-01-21 17:24:54	1213	华为	1213	DESKTOP-TP14772/admin		会议检索 - AudiSys - Google Chrome
2022-01-21 17:24:52	1213	华为	1213	DESKTOP-TP14772/admin		行为日志 - AudiSys - Google Chrome

应用记录的查询、播放、创建风险规则、明细、收藏、导出数据等操作请借鉴全部行为步骤

## 4.3.1-->4.3.6。

o

## 4.3.8 上网活动

对用户在终端的浏览器上的所有网页浏览操作审计（目前支持的浏览器：谷歌、火狐、IE8 及以上、360 极速和安全浏览器）

**注：需要勾选 Windows 记录策略的是否记录上网活动探针才会审计。**

发生时间	终端名称/IP	部门/用户名	用户账号/登录IP	端口/端	URL地址	操作
2022-01-21 17:27:20	DESKTOP-Q3ASVCM	研发部 金亮娃	DESKTOP-Q3ASVCM/admin	localhost	AuditSys5.0-用例 - 增添 - Google...	<span style="color: orange;">高危</span> <span style="color: green;">正常</span> <span style="color: blue;">未知</span> <span style="color: purple;">敏感</span>
2022-01-21 17:27:17	DESKTOP-Q3ASVCM	研发部 金亮娃	DESKTOP-Q3ASVCM/admin	localhost	用例库-修改用例 - 增添 - Go...	<span style="color: orange;">高危</span> <span style="color: green;">正常</span> <span style="color: blue;">未知</span> <span style="color: purple;">敏感</span>
2022-01-21 17:27:04	DESKTOP-Q3ASVCM	研发部 金亮娃	DESKTOP-Q3ASVCM/admin	localhost	用例库-修改用例 - 增添 - Go...	<span style="color: orange;">高危</span> <span style="color: green;">正常</span> <span style="color: blue;">未知</span> <span style="color: purple;">敏感</span>
2022-01-21 17:26:58	DESKTOP-Q3ASVCM	研发部 金亮娃	DESKTOP-Q3ASVCM/admin	localhost	CASE #6686 【v5.0】【修改外...	<span style="color: orange;">高危</span> <span style="color: green;">正常</span> <span style="color: blue;">未知</span> <span style="color: purple;">敏感</span>
2022-01-21 17:26:54	DESKTOP-Q3ASVCM	研发部 金亮娃	DESKTOP-Q3ASVCM/admin	localhost	CASE #6686 【v5.0】【修改外...	<span style="color: orange;">高危</span> <span style="color: green;">正常</span> <span style="color: blue;">未知</span> <span style="color: purple;">敏感</span>
2022-01-21 17:26:53	DESKTOP-Q3ASVCM	研发部 金亮娃	DESKTOP-Q3ASVCM/admin	localhost	用例库-修改用例 - 增添 - Go...	<span style="color: orange;">高危</span> <span style="color: green;">正常</span> <span style="color: blue;">未知</span> <span style="color: purple;">敏感</span>
2022-01-21 17:26:46	DESKTOP-Q3ASVCM	研发部 金亮娃	DESKTOP-Q3ASVCM/admin	localhost	CASE #6687 【v5.0】【文件外...	<span style="color: orange;">高危</span> <span style="color: green;">正常</span> <span style="color: blue;">未知</span> <span style="color: purple;">敏感</span>
2022-01-21 17:26:42	DESKTOP-Q3ASVCM	研发部 金亮娃	DESKTOP-Q3ASVCM/admin	localhost	CASE #6687 【v5.0】【文件外...	<span style="color: orange;">高危</span> <span style="color: green;">正常</span> <span style="color: blue;">未知</span> <span style="color: purple;">敏感</span>
2022-01-21 17:26:40	DESKTOP-Q3ASVCM	研发部 金亮娃	DESKTOP-Q3ASVCM/admin	localhost	用例库-修改用例 - 增添 - Go...	<span style="color: orange;">高危</span> <span style="color: green;">正常</span> <span style="color: blue;">未知</span> <span style="color: purple;">敏感</span>

上网记录的查询、播放、创建风险规则、明细、收藏、导出数据等操作请借鉴全部行为步骤

4.3.1-->4.3.6。

### 4.3.9 剪切板

剪贴板是记录用户在终端对所有文本剪贴的操作。

**注：需要勾选 Windows 记录策略的是否记录剪切板探针才会审计。**

发生时间	终端名称/IP	部门/用户名	用户账号/登录IP	类型	剪贴内容	操作
2022-01-21 17:21:20	WN10-1TB	财务 卢西安	WN10-1TB\lu...	文本剪贴	AuditSys5.0-安装配置手册_v1.0	<span style="color: orange;">高危</span> <span style="color: green;">正常</span> <span style="color: blue;">未知</span> <span style="color: purple;">敏感</span>
2022-01-21 17:21:02	DESKTOP-B5Q96L	英伟联想	DESKTOP-B5Q96L\admin	文本剪贴	<sunli@sino-vt.com>	<span style="color: orange;">高危</span> <span style="color: green;">正常</span> <span style="color: blue;">未知</span> <span style="color: purple;">敏感</span>
2022-01-21 17:21:02	KUBERA	法律 黎墨	KUBERA\admin	文本剪贴	<sunli@sino-vt.com>	<span style="color: orange;">高危</span> <span style="color: green;">正常</span> <span style="color: blue;">未知</span> <span style="color: purple;">敏感</span>
2022-01-21 17:19:06	DESKTOP-SHSNLTU	华为 阿拉腾	DESKTOP-SHSNLTU\admin	文本剪贴	\\\192.168.2.4\ct\03_AuditSys5.0...	<span style="color: orange;">高危</span> <span style="color: green;">正常</span> <span style="color: blue;">未知</span> <span style="color: purple;">敏感</span>
2022-01-21 17:19:05	window11-企业54	研发部 赵生	WINDOW11-企业54	文本剪贴	\\\192.168.2.4\ct\03_AuditSys5.0...	<span style="color: orange;">高危</span> <span style="color: green;">正常</span> <span style="color: blue;">未知</span> <span style="color: purple;">敏感</span>
2022-01-21 17:19:05	WIN-6F1FEIRHDLB	研发部 李元芳	WIN-6F1FEIRHDLB\administrator	文本剪贴	\\\192.168.2.4\ct\03_AuditSys5.0...	<span style="color: orange;">高危</span> <span style="color: green;">正常</span> <span style="color: blue;">未知</span> <span style="color: purple;">敏感</span>
2022-01-21 17:19:05	DESKTOP-Q3ASVCM	研发部 金亮娃	DESKTOP-Q3ASVCM/admin	文本剪贴	\\\192.168.2.4\ct\03_AuditSys5.0...	<span style="color: orange;">高危</span> <span style="color: green;">正常</span> <span style="color: blue;">未知</span> <span style="color: purple;">敏感</span>
2022-01-21 17:17:43	DESKTOP-KVDR11	采购组 陈玲	DESKTOP-KVDR11\chen	文本剪贴	000001733971000	<span style="color: orange;">高危</span> <span style="color: green;">正常</span> <span style="color: blue;">未知</span> <span style="color: purple;">敏感</span>
2022-01-21 17:16:36	WIN-6F1FEIRHDLB	研发部 李元芳	WIN-6F1FEIRHDLB\administrator	文本剪贴	server操作成功，命令consume...	<span style="color: orange;">高危</span> <span style="color: green;">正常</span> <span style="color: blue;">未知</span> <span style="color: purple;">敏感</span>

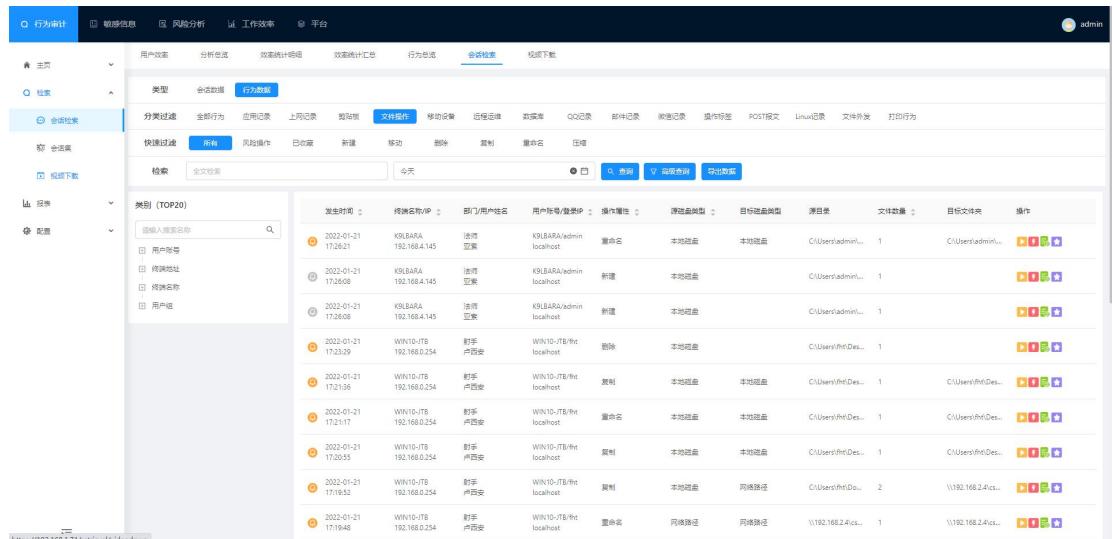
剪切板的查询、播放、创建风险规则、明细、收藏、导出数据等操作请借鉴全部行为步骤

4.3.1-->4.3.6。

## 4.3.10 文件操作

文件操作是用户在终端上对所有文件的操作，包括移动，复制，删除，新建，重命名等。

注：需要勾选 Windows 记录策略的是否记录文件操作探针才会审计。



The screenshot shows the behavioral audit interface with the 'File Operation' tab selected. The left sidebar includes sections for '行为审计' (Behavior Audit), '敏感信息' (Sensitive Information), '风险分析' (Risk Analysis), '工作效率' (Work Efficiency), and '平台' (Platform). Under '会话检索' (Session Search), there are filters for '类型' (Type) set to '会话数据' (Session Data), '分类过滤' (Category Filter) for '全部行为' (All Behaviors), and '快速过滤' (Quick Filter) for '所有' (All). The main area displays a table of log entries with columns: '发生时间' (Time), '终端名称/IP' (Terminal Name/IP), '部门/用户名' (Department/User Name), '用户账号/登录IP' (User Account/Login IP), '操作属性' (Operation Attribute), '操作描述' (Operation Description), '目标磁盘类型' (Target Disk Type), '源目录' (Source Directory), '文件数量' (File Count), '目标文件夹' (Target Folder), and '操作' (Operation). The table lists various file operations such as creation, deletion, and renaming by users like 'KB1BARA/admin' and 'localhost' on Windows 10 hosts.

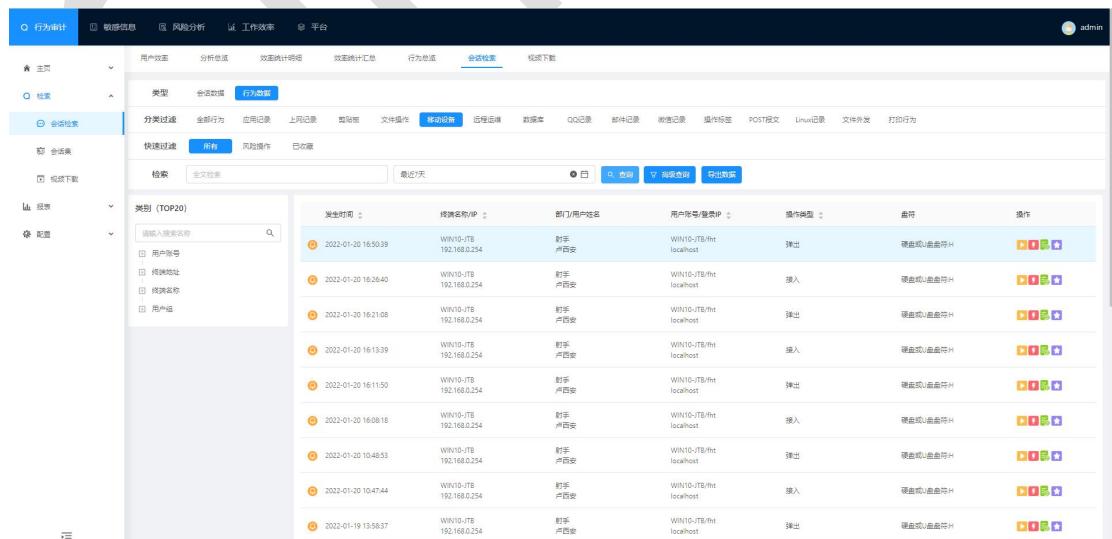
文件操作的查询、播放、创建风险规则、明细、收藏、导出数据等操作请借鉴全部行为

步骤 4.3.1-->4.3.6。

## 4.3.11 移动设备

终端插入或移除移动磁盘等操作记录（暂只支持 U 盘，读卡器，移动硬盘）。

注：需要勾选 Windows 记录策略的是否记录 USB 探针才会审计。



This screenshot shows the behavioral audit interface with the 'Mobile Device' tab selected. The left sidebar includes sections for '行为审计' (Behavior Audit), '敏感信息' (Sensitive Information), '风险分析' (Risk Analysis), '工作效率' (Work Efficiency), and '平台' (Platform). Under '会话检索' (Session Search), there are filters for '类型' (Type) set to '移动设备' (Mobile Device), '分类过滤' (Category Filter) for '全部行为' (All Behaviors), and '快速过滤' (Quick Filter) for '所有' (All). The main area displays a table of log entries with columns: '发生时间' (Time), '终端名称/IP' (Terminal Name/IP), '部门/用户名' (Department/User Name), '用户账号/登录IP' (User Account/Login IP), '操作类型' (Operation Type), '盘符' (Drive Letter), and '操作' (Operation). The table lists various disk insertion and removal operations by users like 'KB1BARA/admin' and 'localhost' on Windows 10 hosts.

移动设备的查询、播放、创建风险规则、明细、收藏、导出数据等操作请借鉴全部行为

步骤 4.3.1-->4.3.6。

## 4.3.12 远程运维

远程运维是用户在终端上所执行的 linux 命令和 CMD 命令。(暂时支持的软件包含：  
SecureCRT、XShell、Putty)。

注：需要勾选 Windows 记录策略的是否记录远程运维探针才会审计。

The screenshot shows a web-based behavioral audit system. The top navigation bar includes tabs for '行为审计' (Behavior Audit), '敏感信息' (Sensitive Information), '风险分析' (Risk Analysis), '工作效率' (Work Efficiency), and '平台' (Platform). The current view is under the '行为审计' tab, specifically in the '会话检索' (Session Search) section. On the left, there are filters for '类型' (Type) set to '会话数据' (Session Data), '分类过滤' (Category Filter) set to '全部行为' (All Behaviors), and '快速过滤' (Quick Filter) set to '所有' (All). The main area displays a table of session data with columns: '发生时间' (Occurrence Time), '终端名称/IP' (Terminal Name/IP), '部门/用户名' (Department/User Name), '用户账号/登录IP' (User Account/Login IP), '应用名称' (Application Name), '连接主机IP' (Connected Host IP), '连接帐号' (Connected Account), '远程命令' (Remote Command), '回显' (Echo), and '操作' (Operation). The table lists 10 entries from January 21, 2022, at 17:29:54 to 17:39:49, involving users like '胡安' and '胡勇' connecting via SecureCRT to hosts like 'WIN10-JTB' and 'DESKTOP-C3A5VCM'. Each entry includes a small icon representing the command type.

远程运维的查询、播放、创建风险规则、明细、收藏、导出数据等操作请借鉴全部行为  
步骤 4.3.1-->4.3.6。

## 4.3.13 数据库

数据库是记录用户在终端上所执行的数据库命令。暂支持数据库有 Oracle、MySQL、SQL server；(暂时支持的软件包含：Plsql developer、Navicat、SQL server)  
注：MySQL 暂时只支持在 Navicat10.1.7 和 Navicat11.0 连接操作 SQL 语句审计。

注：需要勾选 Windows 记录策略的是否记录数据库探针才会审计。

数据库的查询、播放、创建风险规则、明细、收藏、导出数据等操作请借鉴全部行为步骤

4.3.1-->4.3.6。

## 4.3.14 QQ 记录

QQ 记录是记录用户在终端上使用 QQ 所发送、接收的 QQ 消息内容审计。（目前能登录的 QQ 版本都可以审计、TIM 聊天记录也可以审计）。

**注：需要勾选 Windows 记录策略是否记录 QQ 记录探针才会审计。**

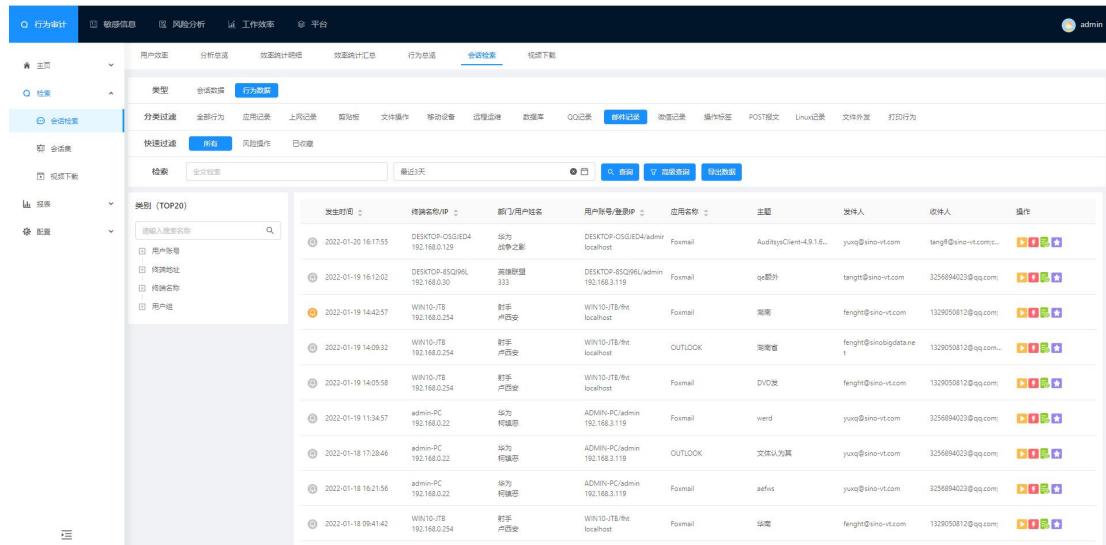
QQ 记录的查询、播放、创建风险规则、明细、收藏、导出数据等操作请借鉴全部行为步骤

4.3.1-->4.3.6。

## 4.3.15 邮件记录

邮件记录是用户在终端发送邮件进行审计；暂支持在 foxmail、outlook 上发送邮件审计。

注：需要勾选 Windows 记录策略的是否记录邮件记录探针才会审计。



发生时间	终端名/IP	部门/用户名	用户账号/登录IP	应用名称	主题	发件人	收件人	操作
2022-01-20 16:17:55	DESKTOP-0SGJED04 192.168.3.129	华为 战狼之影	DESKTOP-0SGJED04/admin localhost	Foxmail	AuditSysClient-4.9.1...	yuq@sinovt.com	tang@sinovt.com...	<span style="color: orange;">发送</span> <span style="color: green;">接收</span> <span style="color: blue;">发送失败</span> <span style="color: red;">接收失败</span>
2022-01-19 16:12:02	DESKTOP-8SQ96L 192.168.3.119	英雄联盟	DESKTOP-8SQ96L/admin localhost	Foxmail	qq群发	tang@sinovt.com	3256894023@qq.com;	<span style="color: orange;">发送</span> <span style="color: green;">接收</span> <span style="color: blue;">发送失败</span> <span style="color: red;">接收失败</span>
2022-01-19 14:42:57	WIN10-TB 192.168.0.254	射手 卢西安	WIN10-TB\tht localhost	Foxmail	寒霜	fenght@sinovt.com	1329050812@qq.com;	<span style="color: orange;">发送</span> <span style="color: green;">接收</span> <span style="color: blue;">发送失败</span> <span style="color: red;">接收失败</span>
2022-01-19 14:09:32	WIN10-TB 192.168.0.254	射手 卢西安	WIN10-TB\tht localhost	OUTLOOK	王者荣耀	fenght@sinobigdata.net	1329050812@qq.com;	<span style="color: orange;">发送</span> <span style="color: green;">接收</span> <span style="color: blue;">发送失败</span> <span style="color: red;">接收失败</span>
2022-01-19 14:05:58	WIN10-TB 192.168.0.254	射手 卢西安	WIN10-TB\tht localhost	Foxmail	DVD发	fenght@sinovt.com	1329050812@qq.com;	<span style="color: orange;">发送</span> <span style="color: green;">接收</span> <span style="color: blue;">发送失败</span> <span style="color: red;">接收失败</span>
2022-01-19 11:34:57	admin-PC 192.168.0.22	华为 杨德恩	ADMIN-PC\admin 192.168.3.119	Foxmail	verd	yuq@sinovt.com	3256894023@qq.com;	<span style="color: orange;">发送</span> <span style="color: green;">接收</span> <span style="color: blue;">发送失败</span> <span style="color: red;">接收失败</span>
2022-01-18 17:28:46	admin-PC 192.168.0.22	华为 杨德恩	ADMIN-PC\admin 192.168.3.119	OUTLOOK	文件认为真	yuq@sinovt.com	3256894023@qq.com;	<span style="color: orange;">发送</span> <span style="color: green;">接收</span> <span style="color: blue;">发送失败</span> <span style="color: red;">接收失败</span>
2022-01-18 16:21:56	admin-PC 192.168.0.22	华为 杨德恩	ADMIN-PC\admin 192.168.3.119	Foxmail	aeinus	yuq@sinovt.com	3256894023@qq.com;	<span style="color: orange;">发送</span> <span style="color: green;">接收</span> <span style="color: blue;">发送失败</span> <span style="color: red;">接收失败</span>
2022-01-18 09:41:42	WIN10-TB 192.168.0.254	射手 卢西安	WIN10-TB\tht localhost	Foxmail	华重	fenght@sinovt.com	1329050812@qq.com;	<span style="color: orange;">发送</span> <span style="color: green;">接收</span> <span style="color: blue;">发送失败</span> <span style="color: red;">接收失败</span>

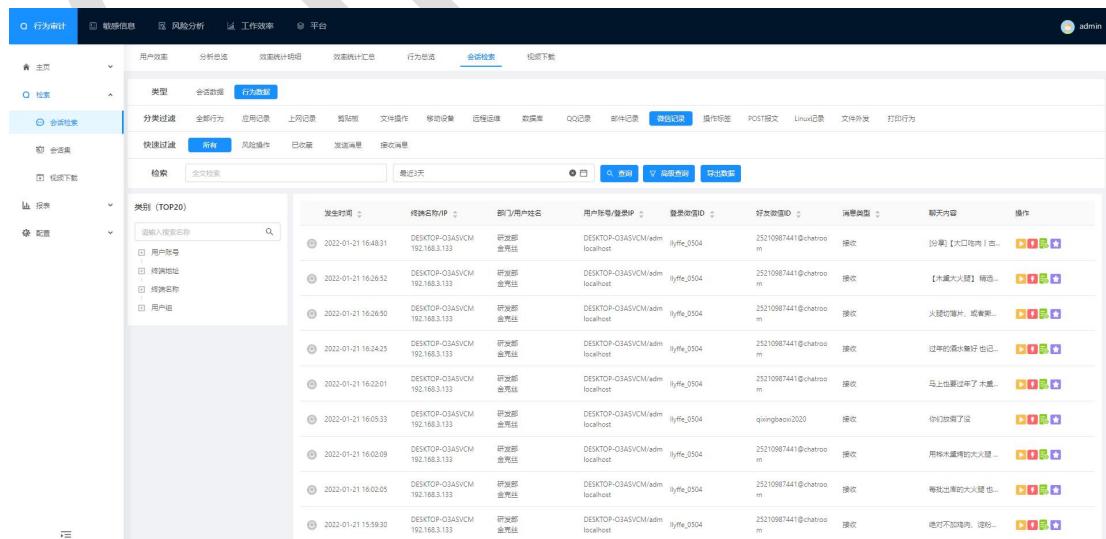
邮件记录的查询、播放、创建风险规则、明细、收藏、导出数据等操作请借鉴全部行为步骤

4.2.1-->4.3.6。

## 4.3.16 微信记录

微信记录是用户在终端使用微信进行聊天记录审计。

注：需要勾选 Windows 记录策略的是否记录微信记录探针才会审计。



发生时间	终端名/IP	部门/用户名	用户账号/登录IP	类型ID	消息类型	聊天内容	操作
2022-01-21 16:48:31	DESKTOP-Q3ASVCM 192.168.3.133	研发部 金贵强	DESKTOP-Q3ASVCM/admin localhost	lyffe_2504	25210987441@chatroom	分享【大口吃肉】...	<span style="color: orange;">发送</span> <span style="color: green;">接收</span> <span style="color: blue;">发送失败</span> <span style="color: red;">接收失败</span>
2022-01-21 16:26:32	DESKTOP-Q3ASVCM 192.168.3.133	研发部 金贵强	DESKTOP-Q3ASVCM/admin localhost	lyffe_2504	25210987441@chatroom	【木熏火烈】精选...	<span style="color: orange;">发送</span> <span style="color: green;">接收</span> <span style="color: blue;">发送失败</span> <span style="color: red;">接收失败</span>
2022-01-21 16:26:50	DESKTOP-Q3ASVCM 192.168.3.133	研发部 金贵强	DESKTOP-Q3ASVCM/admin localhost	lyffe_2504	25210987441@chatroom	火腿切片机、或者...	<span style="color: orange;">发送</span> <span style="color: green;">接收</span> <span style="color: blue;">发送失败</span> <span style="color: red;">接收失败</span>
2022-01-21 16:24:25	DESKTOP-Q3ASVCM 192.168.3.133	研发部 金贵强	DESKTOP-Q3ASVCM/admin localhost	lyffe_2504	25210987441@chatroom	过年的酒真好 也记...	<span style="color: orange;">发送</span> <span style="color: green;">接收</span> <span style="color: blue;">发送失败</span> <span style="color: red;">接收失败</span>
2022-01-21 16:22:01	DESKTOP-Q3ASVCM 192.168.3.133	研发部 金贵强	DESKTOP-Q3ASVCM/admin localhost	lyffe_2504	25210987441@chatroom	马上也要过年了 十重...	<span style="color: orange;">发送</span> <span style="color: green;">接收</span> <span style="color: blue;">发送失败</span> <span style="color: red;">接收失败</span>
2022-01-21 16:05:33	DESKTOP-Q3ASVCM 192.168.3.133	研发部 金贵强	DESKTOP-Q3ASVCM/admin localhost	lyffe_2504	qxinglao2020	你们放假了没	<span style="color: orange;">发送</span> <span style="color: green;">接收</span> <span style="color: blue;">发送失败</span> <span style="color: red;">接收失败</span>
2022-01-21 16:02:09	DESKTOP-Q3ASVCM 192.168.3.133	研发部 金贵强	DESKTOP-Q3ASVCM/admin localhost	lyffe_2504	25210987441@chatroom	用木熏烤的大火腿...	<span style="color: orange;">发送</span> <span style="color: green;">接收</span> <span style="color: blue;">发送失败</span> <span style="color: red;">接收失败</span>
2022-01-21 16:02:05	DESKTOP-Q3ASVCM 192.168.3.133	研发部 金贵强	DESKTOP-Q3ASVCM/admin localhost	lyffe_2504	25210987441@chatroom	每我出席的大火腿 也...	<span style="color: orange;">发送</span> <span style="color: green;">接收</span> <span style="color: blue;">发送失败</span> <span style="color: red;">接收失败</span>
2022-01-21 15:59:30	DESKTOP-Q3ASVCM 192.168.3.133	研发部 金贵强	DESKTOP-Q3ASVCM/admin localhost	lyffe_0504	25210987441@chatroom	绝对不加鸡肉、淀粉...	<span style="color: orange;">发送</span> <span style="color: green;">接收</span> <span style="color: blue;">发送失败</span> <span style="color: red;">接收失败</span>

微信记录的查询、播放、创建风险规则、明细、收藏、导出数据等操作请借鉴全部行为步骤

4.2.1-->4.3.6。

### 4.3.17 操作标签

操作标签是用户在终端使用鼠标的点击事件审计。

注：需要勾选 Windows 记录策略的是否记录操作标签探针才会审计。

The screenshot shows the 'Behavior Audit' section of a security monitoring tool. The left sidebar includes '行为审计' (Behavior Audit), '敏感信息', '风险分析', '工作效率', and '平台'. Under '行为审计', there are sections for '会话统计' (Session Statistics) and '报告'. The main area displays a table of audit results for '操作标签' (Operation Tags). The columns include: '发生时间' (Time), '终端名/IP' (Terminal Name/IP), '部门/用户名' (Department/User Name), '用户账号/登录IP' (User Account/Login IP), '应用名称' (Application Name), '标签名称' (Label Name), '窗口标题' (Window Title), and '操作' (Action). The table lists 10 entries from January 21, 2022, at 17:35:06, showing various user interactions like Google Chrome, WeChat, and WPS Office.

操作标签的查询、播放、创建风险规则、明细、收藏、导出数据等操作请借鉴全部行为步骤

4.2.1-->4.3.6。

### 4.3.18 POST 报文

POST 报文是用户在终端的 IE 或谷歌浏览器提交 POST 表单行为审计；支持 IE9 或 IE9 以上版本浏览器。

注：需要勾选 Windows 记录策略的是否记录 POST 报文探针才会审计。

**POST 报文的查询、播放、创建风险规则、明细、收藏、导出数据等操作请借鉴全部行为步骤 4.2.1-->4.2.6。**

### 4.3.18.1 增加表单解析规则

点击“”，会弹出新建表单解析规则窗口，如下图所示：

规则名称：表单命名。

规则秒速：表单描述。

匹配 URL 路径：在此 URL 路径才能触发 POST 报文表单规则。

匹配优先级：两个相同表单规则，优先级越高就优先触发规则表单

**(注：优先级最高填 99)。**

表单字段转换规则：把原本的表单条件名称转换一个自定义表单条件名称显示

(可以自定义转换多个)。

表单解析规则增加成功后，再回到 POST 表单界面，再次选择被创建表单解析规则的数据，点击明细就可以查看表单解析详情。如下图所示：

The screenshot shows the 'Form Detail' page with two main sections: 'Form Data' and 'Parse Rule'.  
In the 'Form Data' section, there are three entries:

- 号码: 湖南长沙
- 姓名: chenjun
- 部门: 长沙研发中心

In the 'Parse Rule' section, the details are:

- Rule Name: new表单解析10月28日15:20:02
- Matched URL: https://192.168.1.95/index/index/testdata
- Rule Details: [{"field": "testphone", "content": "号码"}, {"field": "name", "content": "姓名"}, {"field": "dept", "content": "部门"}]

### 4.3.19 Linux 记录

Linux 记录是用户在 Linux 终端执行命令操作审计<支持软件工具:SecureCRT、putty、xshell;  
支持的连接方式操作命令: ssh、telnet、rsh; 对 Linux 终端系统版本支持: Redhat6、Redhat7、  
centos6、centos7、ubuntu16、ubuntu18、ubuntu20、Uos-arm、Uos-amd>

The screenshot shows the 'Behavior Audit' interface with the '行为数据' tab selected. The search results table displays audit logs for the user 'admin'. The columns include:

- 发生时间 (Occurrence Time)
- 终端名称/IP (Terminal Name/ IP)
- 部门/用户名 (Department/User Name)
- 用户账号/登录IP (User Account/Login IP)
- 命令 (Command)
- 操作 (Operation)

The table shows one entry: '智云数据' (Zhiyun Data) at '2024-01-01 10:00:00'.

Linux 记录的查询、播放、创建风险规则、明细、收藏、导出数据等操作请借鉴全部行为步骤 4.2.1-->4.2.6。

### 4.3.20 文件外发

文件外发是用户在终端本地剪贴、拷贝、上传文件到外部应用的操作审计（上传文件到

百度云、360云盘、腾讯微云、QQ、微信、U盘、邮件等)

注：需要勾选 Windows 记录策略的是否记录文件外发探针才会审计。

注：目前文件外发还没有支持的 agent 包发布。

The screenshot shows the behavioral audit interface with the 'Print Behavior' tab selected. The left sidebar includes sections for 'User Behavior', 'Risk Analysis', 'Work Efficiency', and 'Platform'. Under 'Behavior Audit', there are 'File Download' and 'Print Behavior' sections. The main area displays a table titled 'Category (TOP20)' with columns for '发生时间' (Time), '终端名称/IP' (Terminal Name/IP), '部门/用户名' (Department/User Name), '进程名称' (Process Name), '进程描述' (Process Description), '像数类型' (Image Type), '文件名称' (File Name), '文件路径' (File Path), '文件大小' (File Size), and '操作' (Operation). The table lists various print jobs from different users and terminals, such as '1213' (华为) printing 'QQ.exe' and 'Windows11\_企业' (研发部) printing 'rdpclip.exe'.

### 4.3.21 打印行为

打印行为是用户在终端进行打印操作审计（支持网页、文档、应用等打印操作）

注：需要勾选 Windows 记录策略的是否记录打印行为探针才会审计。

The screenshot shows the behavioral audit interface with the 'Print Behavior' tab selected. The left sidebar includes sections for 'User Behavior', 'Risk Analysis', 'Work Efficiency', and 'Platform'. Under 'Behavior Audit', there are 'File Download' and 'Print Behavior' sections. The main area displays a table titled 'Category (TOP20)' with columns for '发生时间' (Time), '终端名称/IP' (Terminal Name/IP), '部门/用户名' (Department/User Name), '打印机名称' (Printer Name), '文件名' (File Name), '打印机类型' (Printer Type), '打印批次时间' (Print Batch Time), and '操作' (Operation). The table lists various print jobs from different users and terminals, such as 'DESKTOP-O3ASVCM' (研发部) printing 'OneNote 2010' and 'DESKTOP-TP14772' (华为) printing 'OneNote for Windows 10'.

打印行为的查询、播放、创建风险规则、明细、收藏、导出数据等操作请借鉴全部行为步骤

4.2.1-->4.2.6。

## 4.3.22 钉钉记录

记录钉钉应用中消息记录，文件记录等。

The screenshot shows a web-based management platform for DingTalk records. The interface includes a top navigation bar with tabs like '行为审计' (Behavior Audit), '数据数据保护' (Data Protection), '行为风险分析' (Behavior Risk Analysis), '工作效率分析' (Work Efficiency Analysis), and '管理平台' (Management Platform). A sidebar on the left contains sections for '主页' (Home), '社畜' (Office Worker), '会议记录' (Meeting Records), '会议下载' (Meeting Downloads), '权限' (Permissions), and '配置' (Configuration). The main content area is titled '会议记录' (Meeting Records) and shows a table of logs. The table columns include: '发生时间' (Time), '终端名称/IP' (Terminal Name/IP), '部门/用户名' (Department/User Name), '用户账号/登录IP' (User Account/Login IP), '好友类型' (Friend Type), '发送者昵称' (Sender Nickname), '接收者昵称' (Recipient Nickname), and '内容' (Content). Each log entry also includes a '操作' (Operation) column with icons for video playback, risk creation, and message details. The table lists several entries from April 2022, such as messages from '市场部' (Marketing Department) users like '莫冰' and '陈思英'.

1. **查询模块：**模糊查询在搜索框中搜索关键字检索。高级查询可从文档名；好友类型（可分为好友消息；群消息；好友文件；群文件）；接收人/发送人昵称；群备注等检索相应消息记录。
2. **过滤模块：**通过过滤模块中的条件过滤。
3. 点击播放视频；点击新建风险，条件自动生成；点击查看消息详情。

## 4.3.23 企业微信记录

企业微信记录企业微信消息记录，文件记录等。

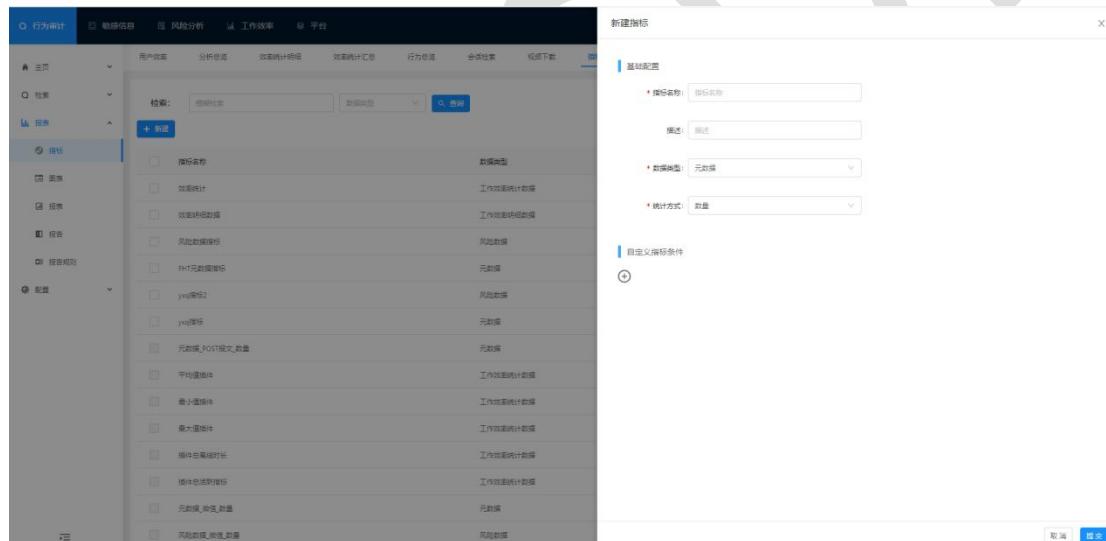
The screenshot shows a web-based management platform for WeChat Business records. The interface is similar to the DingTalk one, with a top navigation bar and a sidebar for various functions. The main content area is titled '企业微信记录' (WeChat Business Records) and displays a table of logs. The table columns are identical to the DingTalk version: '发生时间' (Time), '终端名称/IP' (Terminal Name/IP), '部门/用户名' (Department/User Name), '用户账号/登录IP' (User Account/Login IP), '好友类型' (Friend Type), '发送者昵称' (Sender Nickname), '接收者昵称' (Recipient Nickname), '内容' (Content), and '操作' (Operation). The table lists messages from April 2022, such as '世界和平' (World Peace) from '莫冰' and 'gdsaa' (likely a typo for 'gds') from '陈思英'.

1. 查询模块：模糊查询在搜索框中搜索关键字检索。高级查询可从文档名；好友类型（可分为好友消息；群消息；好友文件；群文件）；接收人/发送人昵称；群备注等检索相应消息记录。
2. 过滤模块：通过过滤模块中的条件过滤。
3. 点击 播放视频；点击 新建风险，条件自动生成；点击 查看消息详情。

## 4.4 报表--指标

### 4.21.1 新建指标

点击“新建”按钮进行新建指标；如下图所示：



基础配置：

名称：指标的名称。

数据类型：选择指标的数据类型。

统计方式：按指标数据类型的数量、求和、求最大值、求最小值、求平均值来统计。

自定义指标条件：自定义需要查询的指标条件；支持‘且’、‘或’、‘非’逻辑关系；多条件需要同时满足才能查询到数据。支持‘精确查找’、‘模糊查找’、‘区间查找’。

点击“+”添加搜索条件。点击“x”则删除搜索条件。

**注：新建完成的指标需要在“图表”模块才能查询数据。**

## 4.21.2 删除指标

选择要删除的指标，点击“删除”按钮删除指标（提示：默认指标无法被选中删除）。

如下图所示：

名称	数据类型	统计类型	最后操作时间	描述	操作
效果统计	工作效统计数据	数量	01月20日13:45:29		编辑
效果明细数据	工作效明细数据	数量	01月20日11:17:56		编辑
风险数据指标	风险数据	数量	01月20日11:16:18		编辑
FHT元数据指标	元数据	基础计数	01月20日15:17:45		编辑
yes指标2	风险数据	数量	01月14日14:29:01	12345	编辑
yes报表	元数据	数量	01月14日14:02:44	1234	编辑
元数据_POST文件数量	元数据	数量	09月10日09:27:26		编辑
平均重叠件	工作效统计数据	平均值	12月11日15:38:21	1	编辑
最小重叠件	工作效统计数据	最小值	12月11日15:20:04		编辑
最大重叠件	工作效统计数据	最大值	12月11日15:04:37		编辑
操作总耗时(秒)	工作效统计数据	求和	12月10日17:29:51		编辑
操作总耗时(分钟)	工作效统计数据	求和	12月10日17:29:21		编辑
元数据_浓度_数量	元数据	数量	09月10日09:27:26		编辑
风险数据_标准_数量	风险数据	数量	09月10日09:27:08		编辑

## 4.21.3 新建图表

图表：把终端操作的行为数据以图表的形式展示。

点击“新建”按钮进行新建图表；如下图所示：

名称	数据类型	最后修改时间	描述	操作
效果统计	工作效统计数据	01月20日13:46:16		编辑
效果明细	工作效明细数据	01月20日11:20:23		编辑
风险图表	风险数据	01月20日11:16:47		编辑
元数据报表	元数据	01月20日15:59:18		编辑
yes指标2	风险数据	01月18日16:53:46	123	编辑
yes报表	元数据	01月15日09:13:51	123	编辑
元数据_用户_修改聊天_次数	元数据	09月10日09:33:07		编辑
元数据_浓度_聊天_次数	元数据	09月10日09:34:43		编辑
风险_新增聊天_次数	风险数据	09月10日09:34:12		编辑
邮件	元数据	06月25日11:34:20		编辑
工作效统计数据	工作效明细数据	06月20日10:05:36		编辑
风险_运维主机_次数	风险数据	06月24日15:30:10		编辑
风险_事件类型_次数	风险数据	06月24日15:29:05		编辑
风险_网址_次数	风险数据	06月24日15:28:25		编辑

基础配置：

名称：图表的名称。

图表类型：选择图表的展示类型。

数据类型：选择图表的数据类型。

统计维度：可选择按登录用户、时间段、事件类型、终端名称、终端 IP 等维度来统计。

数据时间段：选择要查询的时间段的数据以图表展示。

统计指标：选择指标信息；点击“+”添加统计指标。点击“x”则删除统计指标。

总体过滤条件：输入条件进行查询。

例如：查看用户的剪切板元数据以表格的方式显示；如下图所示：

The screenshot shows a reporting interface with a sidebar on the left containing navigation links like '行为统计', '敏感信息', '风险分析', '工作效果', and '平台'. The main area has tabs for '报表' and '报告'. A search bar at the top is set to '剪切板'. On the left, there's a list of report entries with columns for '报告名称', '数据类型', and '最后修改'. One entry, '元数据\_剪切板\_数量', is highlighted with a red box. To the right, there's a configuration panel for this report, including dropdowns for '统计指标' (set to '元数据\_剪切板\_数量'), '统计维度' (set to '用户账号'), '数据时间段' (set to '今天'), and a '描述' field. Below this is a preview section titled '统计指标' showing a bar chart with data for '元数据\_剪切板\_数量' over time, and a '总体过滤条件' section below it.

#### 4.21.4 新建报表

点击“新建”按钮进行新建报表；如下图所示：

The screenshot shows the 'New Report' dialog box overlaid on the reporting interface. The dialog has several sections: '基础配置' (Basic Configuration) with fields for '名称' (Report Name), '所属模块' (Module), '描述' (Description), '启用' (Enabled) (radio button selected), '定时发送' (Scheduled Send) (radio button selected), '数据类型' (Data Type) (set to '元数据'), '事件类型' (Event Type) (set to '所有事件'), and '数据时间段' (Data Time Range) (set to '今天'); '统计图表' (Statistical Chart); '自定义报表过滤条件' (Custom Report Filter Conditions); and '是否显示明细数据' (Show Detailed Data). At the bottom are '取消' (Cancel) and '确定' (Confirm) buttons.

基础配置：

名称：报表的名称。

所属组织：选择组织，支持多选（为空则显示所有数据）。

描述：对报表的描述。

启用：报表的状态；启用，则启用的定时发送生效；禁用，则不生效。

定时发送：启用，配置好定时发送时间，会自动定时发送报表邮件；禁用，则不发送报表邮件

间隔时间：配置定时发送报表邮件的时间间隔。

接收邮箱：接收报表的邮箱号。

数据类型：选择数据类型。

事件类型：选择事件类型。

数据时间段：查询数据时间段。

统计图表：可以选择添加一个或多个图表，所添加的图表就会在报表里展示。

点击“+”添加图表，点击“x”删除图表。

The screenshot shows a reporting system's configuration page. On the left, there is a list of existing reports with columns for Name, Event Type, Data Type, Reporter, Report Time, and Description. On the right, there is a panel for configuring a new chart. It includes sections for 'Custom Report Filter Conditions' (with options for AND, OR, NOT), 'Is Displaying Detailed Data' (with radio buttons for 'Yes' or 'No'), and 'Data Sorting' (with a dropdown for sorting by User ID and Order type). There are also checkboxes for selecting specific event types and data types.

自定义报表过滤条件：自定义需要查询的指标条件；支持‘且’、‘或’、‘非’逻辑关系；多条件需要同时满足才能查询到数据。支持‘精确查找’、‘模糊查找’、‘区间查找’。

是否显示明细数据：可以自定义选择报表显示字段。默认全部勾选上（**不同的事件类型对于不同的明细数据字段**）

数据排序：可以选择字段‘升序’或‘降序’进行排序。

## 4.21.5 excel 报表

点击 “” 导出 Excel 报表。或者先点击 “” 生成 HTML 报表，再在 HTML 界面，在点击 “导出 EXCEL” 导出 excel。

The screenshot shows a list of audit events with columns for Name, Event Type, Data Type, Reporter, Modify Time, Description, Status, Scheduled Delivery, Next Execution Time, HTML Report, and EXCEL Report. The EXCEL Report column contains green icons for each row.

## 4.21.6html 报表

点击 “” 按钮生成 HTML 报表；如下图所示：

The screenshot shows a detailed data list with columns for Date, Event Type, User ID, Location, Device Model, Location Type, Organization Name, User Type, Department Name, Job Type, Application Name, Work Time, Break Time, Idle Time, and Web Address. At the bottom right, there are buttons for 'Total Data: 3752', 'Cancel', and 'Export as Excel'.

## 4.21.7 发送报表

手动发送报表，点击 “发送报表” 按钮进入发送报表邮件；如下图所示：

**提示：报表必须配置了定时发送，并输入了接收邮箱。**

名称	事件类型	数据类型	修改人	修改时间	描述	状态	定时发送	下次执行时间	HTML报表	EXCEL报表	操作
艾葫芦亚	所有事件	工作效能明细数据	admin	01月20日09:58:51		禁用	禁用				<a href="#">编辑</a> <a href="#">发送报表</a>
7200	所有事件	工作效能明细数据	admin	01月19日17:19:57		禁用	禁用				<a href="#">编辑</a> <a href="#">发送报表</a>
法律	所有事件	工作效能明细数据	admin	01月19日17:06:45		禁用	禁用				<a href="#">编辑</a> <a href="#">发送报表</a>
风险数据报表	所有事件	元数据	admin	01月19日15:58:46		禁用	禁用				<a href="#">编辑</a> <a href="#">发送报表</a>
FHT行为报告	文件操作	元数据	admin	01月19日15:41:22		禁用	禁用				<a href="#">编辑</a> <a href="#">发送报表</a>
Admin	所有事件	元数据	admin	01月20日09:57:15	待办	启用	启用				<a href="#">编辑</a> <a href="#">发送报表</a>
ceht报表	所有事件	元数据	admin	01月15日09:43:13	123	启用	启用	01月21日20:00:00			<a href="#">编辑</a> <b>发送报表</b>
72	所有事件	元数据	admin	01月14日15:43:43		禁用	禁用				<a href="#">编辑</a> <a href="#">发送报表</a>

## 4.21.8 仪表盘

仪表盘是用来展示图表统计数据。

选择“主页>仪表盘”进入仪表盘界面；如下图所示：

点击“新建”按钮，新建仪表盘；如下图所示：

新增仪表盘

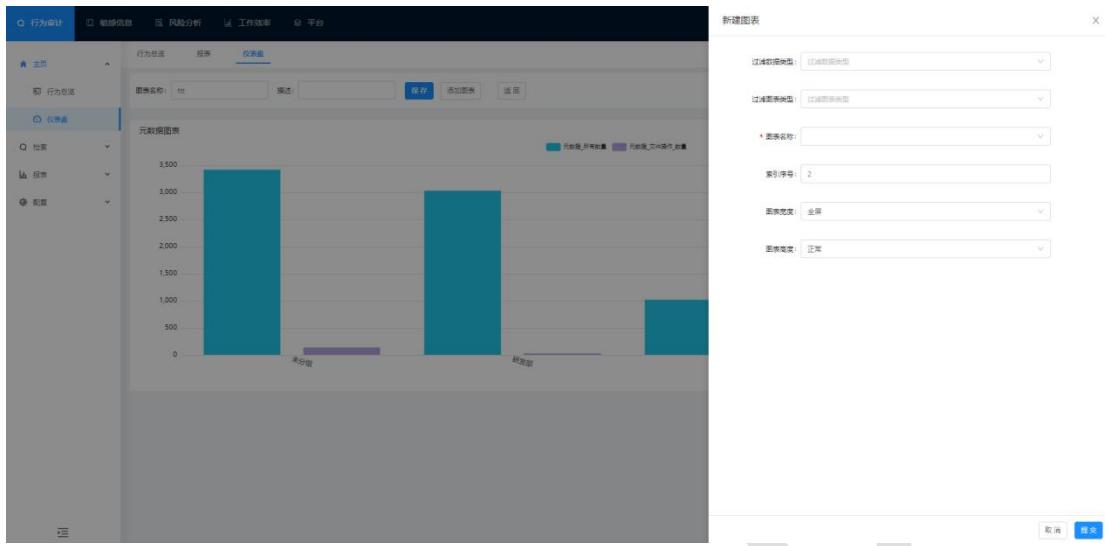
\* 仪表盘名称:

描述:

[取消](#) [确定](#)

### 仪表盘编辑

点击“编辑”按钮，进入编辑仪表盘界面；点击**添加图表**如下图所示：



可以在编辑的仪表盘内点击“添加图表”；

过滤数据类型：筛选数据类型。

过滤图表类型：筛选图表类型。

图表名称：选择要展示的图表数据。

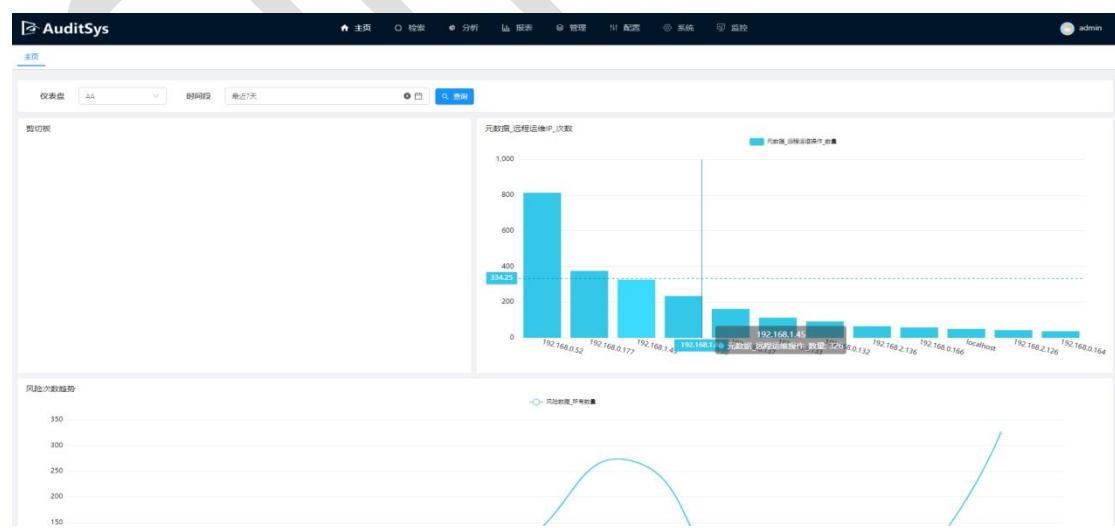
索引序号：在仪表盘添加的第一个图表。

图表宽度：图表的展示宽度。

图表高度：图表的展示高度。

## 仪表盘展示

可在主页选择仪表盘展示；选择仪表盘后，不同的管理员再次登录可以展示不同仪表盘数据；仪表盘展示的时间默认是 7 天。



## 4.21.9 报告规则

报告规则是自定义选择时间范围从多个维度（系统报告、风险报告、敏感词报告、工作效率报告）制定规则生成报告。

点击“报表>报告规则”进入报告规则界面；如下图所示：

The screenshot shows the 'Report Rules' section of the system. At the top, there are tabs for '行为审计', '敏感信息', '风险分析', '工作效率', and '平台'. Below these are sections for '主页', '搜索', '报表', '报告', and '报告规则'. The '报告规则' section is currently selected. A sub-menu on the left lists '日报表', '周报', '月报', '日报', and '报告规则'. The main area displays a table with columns: 名称 (Name), 生成范围 (Generate Range), 部门范围 (Department Range), 状态 (Status), 定时发送 (定时), 系统状态 (System Status), 用户报告 (User Report), 风险报告 (Risk Report), 工作效率报告 (Work Efficiency Report), 下次执行时间 (Next Execution Time), 描述 (Description), and 操作 (Operation). There are four entries in the table: AA, Admin, 12306, and 7z. Each entry includes a checkbox for selecting. At the bottom right of the table, there are buttons for '共4条' (4 items total), page navigation, and '20多页' (More than 20 pages).

新建报告规则

点击“新建”新建报告规则；如下图所示：

The screenshot shows the 'New Audit Report' configuration dialog. The 'Basic Configuration' tab is active. It includes fields for '报告名称' (Report Name) and '描述' (Description). Under 'Data Range', there are two dropdowns: '组织范围' (Organizational Range) and '部门范围' (Department Range), both set to '请选择部门为空则不报'. Under '定时配置' (Timing Configuration), it says '定时生成' (定时 generation) with '启用' (Enabled) checked. Under '发送配置' (Delivery Configuration), there is a field '接收邮箱列表' (List of receiving email addresses) with the placeholder '多个地址用逗号分隔' (Separate multiple addresses with commas). Under 'System Report' (System Report), it says '系统状态' (System status) with '启用' (Enabled) checked. At the bottom right are '取消' (Cancel) and '确定' (Confirm) buttons. The background shows the same report rule list as the previous screenshot.

基础配置：

启用：勾选启用，则可定时生成报告和发送报告邮件（前提配置定时配置）；

勾选禁用，则不定时生成报告和发送报告邮件。

数据范围：

组织范围：可选择单个或多个组织进行过滤。

部门范围：可选择单个或多个部门进行过滤。

数据时间段：可选择时间或自定义时间过滤。

定时配置：

定时生成：勾选启用，则可定时发送报告邮件；

勾选禁用，则不可定时发送报告邮件。

系统报告：勾选启用，则统计显示系统 CPU、内存、进程状态、运行状态等信息报告。

用户报告：勾选启用，则统计显示用户的会话信息、行为数据信息等信息报告。

风险报告：勾选启用，则统计显示用户的风险行为数据信息报告。

敏感词报告：勾选启用，则统计显示用户的敏感行为数据信息报告。

工作效率报告：勾选启用，则统计显示部门的效率分析报告。

## 4.21.10 生成报告

点击“生成”按钮，生成报告信息，生成的报告在报告模块界面显示；如下图所示：

The screenshot shows a user interface for generating reports. At the top, there is a navigation bar with tabs: 行为审计, 敏感信息, 风险分析, 工作效率, 平台, and 报告规则. The 报告规则 tab is currently selected. A success message '已建报告成功' (Report created successfully) is displayed in a red-bordered box at the top right. On the left, there is a sidebar with categories: 主页, 搜索, 报表, 报告, and 报告规则. The 报告规则 category is highlighted with a blue background. The main content area displays a table of generated reports. The table columns include: 名称 (Name), 组织范围 (Organization Scope), 部门范围 (Department Scope), 状态 (Status), 定时发送 (Scheduled Send), 系统状态 (System Status), 用户报告 (User Report), 风险报告 (Risk Report), 工作效率报告 (Work Efficiency Report), 下次执行时间 (Next Execution Time), 描述 (Description), and 操作 (Operation). One row in the table has a red box around the '操作' column, specifically around the '生成' (Generate) button. The table shows four rows of data. At the bottom right of the table, there is a pagination control with '共4条' (4 items total), page numbers 1, 2, and a '20条/页' (20 items per page) dropdown.

报告时间	报告名称	组织范围	部门范围	时间范围	系统状态报告	风险报告	用户会话报告	工作效率报告	操作
2022-01-21 17:51:39	AA1642758699			今天	否	否	否	否	下载
2022-01-21 09:13:09	Admin1642727589	FHT	射手	今天	是	是	是	是	下载
2022-01-19 17:50:14	Admin1642585814	FHT	射手	今天	是	是	是	是	下载
2022-01-19 17:49:59	AA1642585799			今天	否	否	否	否	下载
2022-01-19 15:36:40	123061642577800	法德·艾斯尼亞		今天	否	否	否	否	下载

## 4.21.11 报告

报告是对多个维度（系统状态、用户行为、风险行为、敏感行为、工作效率分析）数据统计生成运行报告。

点击“报表>报告”进入报告界面；如下图所示：

报告时间	报告名称	组织范围	部门范围	时间范围	系统状态报告	风险报告	用户会话报告	工作效率报告	操作
2022-01-21 17:51:39	AA1642758699			今天	否	否	否	否	下载
2022-01-21 09:13:09	Admin1642727589	FHT	射手	今天	是	是	是	是	下载
2022-01-19 17:50:14	Admin1642585814	FHT	射手	今天	是	是	是	是	下载
2022-01-19 17:49:59	AA1642585799			今天	否	否	否	否	下载
2022-01-19 15:36:40	123061642577800	法德·艾斯尼亞		今天	否	否	否	否	下载

## 4.21.12 报告下载

点击“下载”按钮；下载报告查看数据报告统计详情；如下图所示：

The screenshot shows the AuditSys reporting interface. On the left, there's a sidebar with navigation items like '行为审计', '敏感信息', '风险分析', '工作效率', and '平台'. Under '报告', there are sub-options: '报告', '报告规则', and '报告模板'. The main area displays a table of reports with columns: 报告时间 (Report Time), 报告名称 (Report Name), 组织范围 (Organization Scope), 部门范围 (Department Scope), 时间范围 (Time Range), 系统状态报告 (System Status Report), 风险报告 (Risk Report), 用户会话报告 (User Session Report), 工作效率报告 (Work Efficiency Report), and 操作 (Operation). One row is highlighted with a red box around the '操作' column, which contains a '下载' (Download) link. At the bottom right of the table, it says '共5条' (5 results) and has navigation buttons.

对下载的报告进行解压；打开 index.html 文件查看报告统计详情；

This screenshot shows a file explorer window. It lists two files: '1a02912545b7f5e5a1411a510a0d5a0c' and 'Admin1638433139.zip'. Below the file list, there's a preview panel showing the contents of 'Admin1638433139.zip'. Inside, there are three folders: 'img', 'js', and 'styles'. The 'index.html' file is highlighted with a red box. The preview panel also shows the file path 'file:///C:/Users/fht/Downloads/1a02912545b7f5e5a1411a510a0d5a0c/index.html'.

This screenshot shows the AuditSys audit report page. At the top, there's a navigation bar with tabs: 概览 (Overview), 系统状态报告 (System Status Report), 风险报告 (Risk Report), 敏感词报告 (Sensitive Word Report), 用户会话报告 (User Session Report), and 工作效率报告 (Work Efficiency Report). The main content area is divided into several sections: '概览' (Overview), '系统状态报告' (System Status Report), '许可证' (Licenses), and '控制台' (Control Panel). The '控制台' section shows detailed resource usage for an IP address: 192.168.0.192. It includes tables for CPU, Memory, Disk, and Process usage.

## 4.5 表单解析规则

表单解析规则：是对 POST 报文的 post 类型报文进行表单解析。

选择“配置>应用配置>表单解析规则”进入表单解析规则界面（新建表单解析规则可以参考步骤 5.14.1）如下图所示：

The screenshot shows a software interface for managing form parsing rules. The top navigation bar includes tabs for '行为审计' (Behavior Audit), '敏感信息' (Sensitive Information), '风险分析' (Risk Analysis), '工作效率' (Work Efficiency), '平台' (Platform), '表单解析规则' (Form Parsing Rule), and '告警拉警' (Alert). On the left, a sidebar menu lists '主页' (Home), '政策' (Policies), '报告' (Reports), and '配置' (Configuration), with '表单解析规则' (Form Parsing Rule) currently selected. The main content area features a search bar with placeholder '搜索规则' (Search rule) and a '搜索' (Search) button. Below the search bar is a table with columns: '规则名称' (Rule Name), '描述' (Description), '匹配URL' (Match URL), '优先级' (Priority), and '操作' (Operations). A single row is visible in the table, labeled '123' under '规则名称' and 'http://192.168.1.100/zentao/search-buildquery.html' under '匹配URL'. At the bottom right of the table are buttons for '共1条' (1 item), page navigation, and a '刷新' (Refresh) button.