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

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。

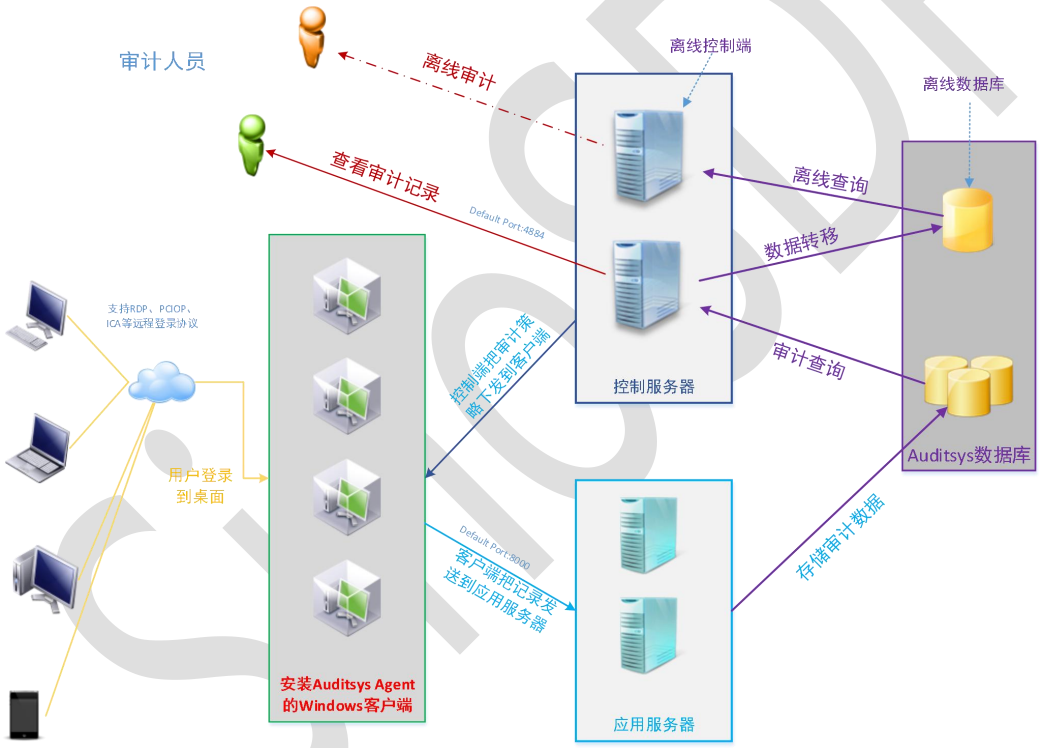
SinoSDP 审计系统由以下 4 个部分构成：

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。

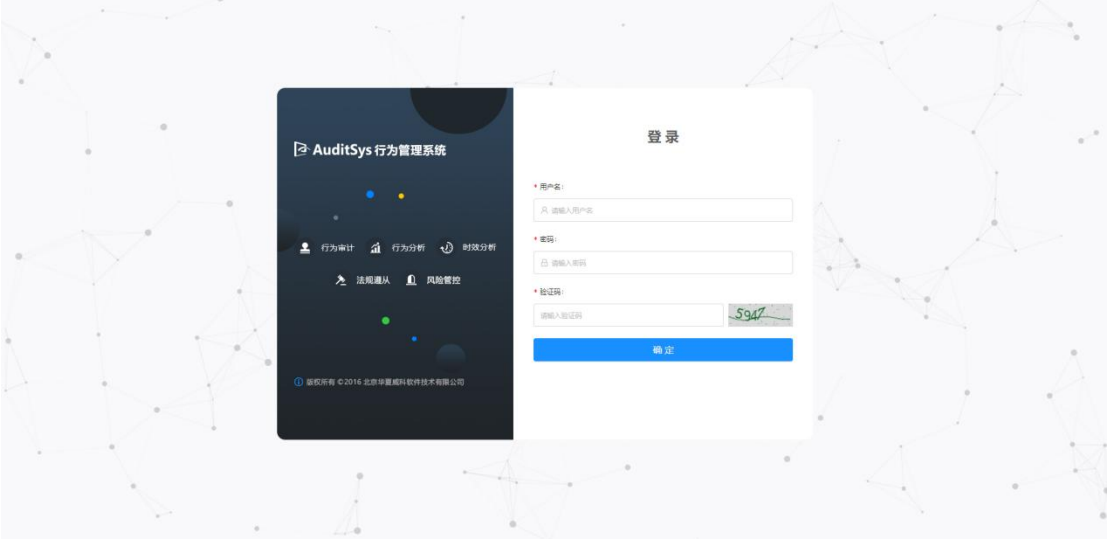
Elasticsearch 服务器集群：用于存储审计记录。



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：



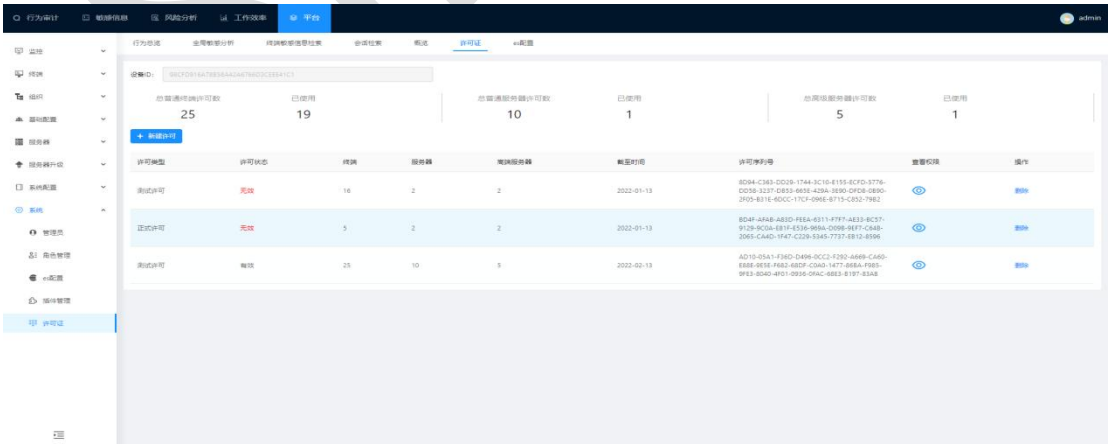
首次打开 SinoSDP 审计管理控制台，默认用户名：admin 密码：changeme 验证码随机生成。此账户是默认超级管理员，此账户无法禁用、无法删除。超级管理员首次登录后，请及时修改密码。

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

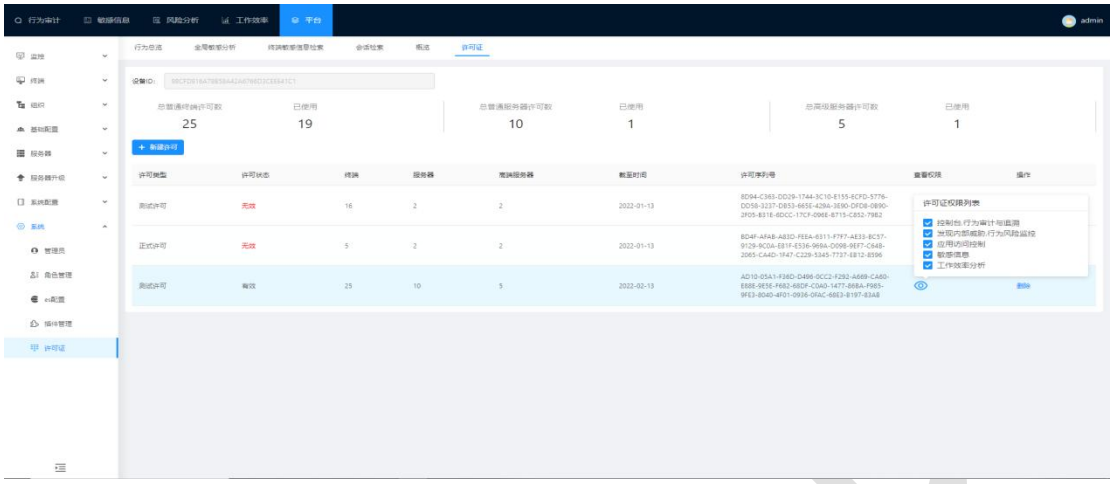
许可证路径：平台/系统/许可证，许可证主要是控制控制台的使用权限。没有配置许可证，只会显示许可证模块。

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。



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）

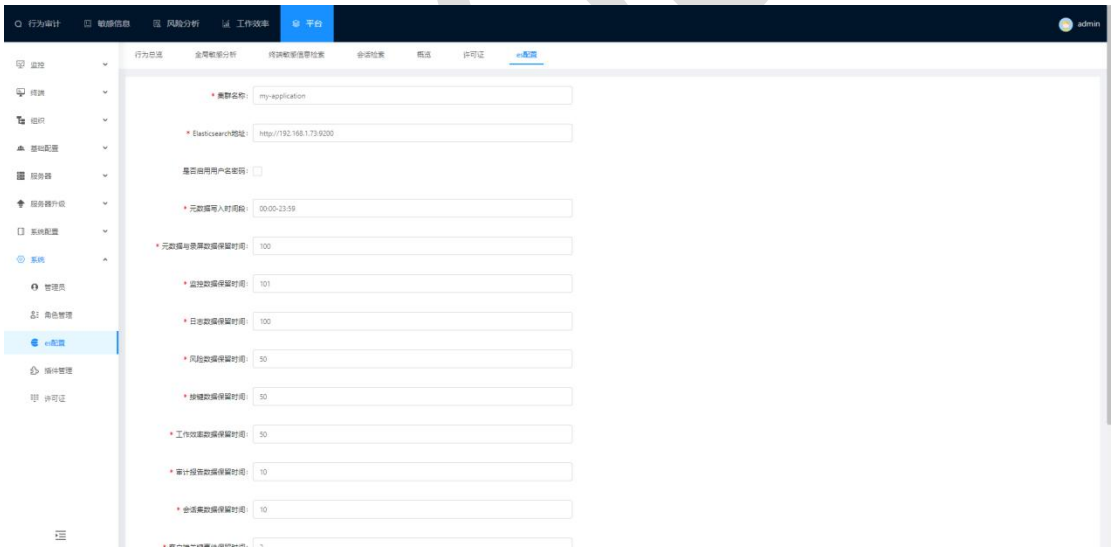
申请的许可可以对行为风险监控，应用访问控制，敏感信息，工作效率分析进行权限管理。



2.3ES 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：



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。

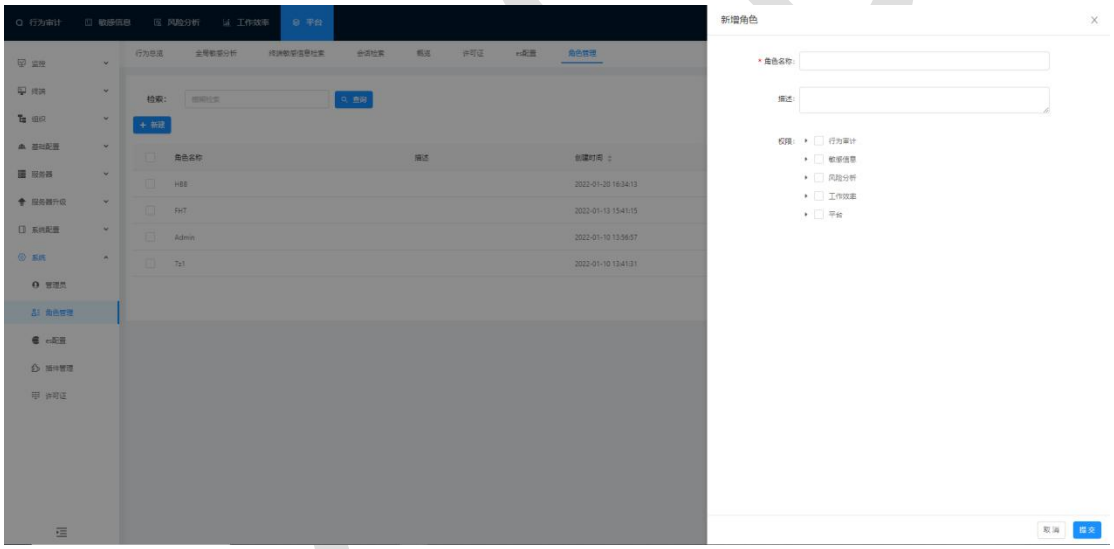
2.4 角色管理

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：

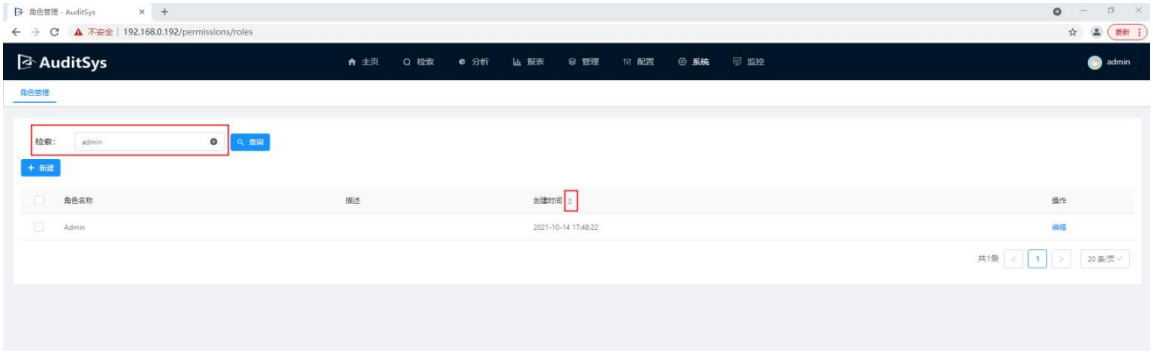


点击“提交”保存角色，成功则退回到角色列表界面，失败则有提示失败原因。

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

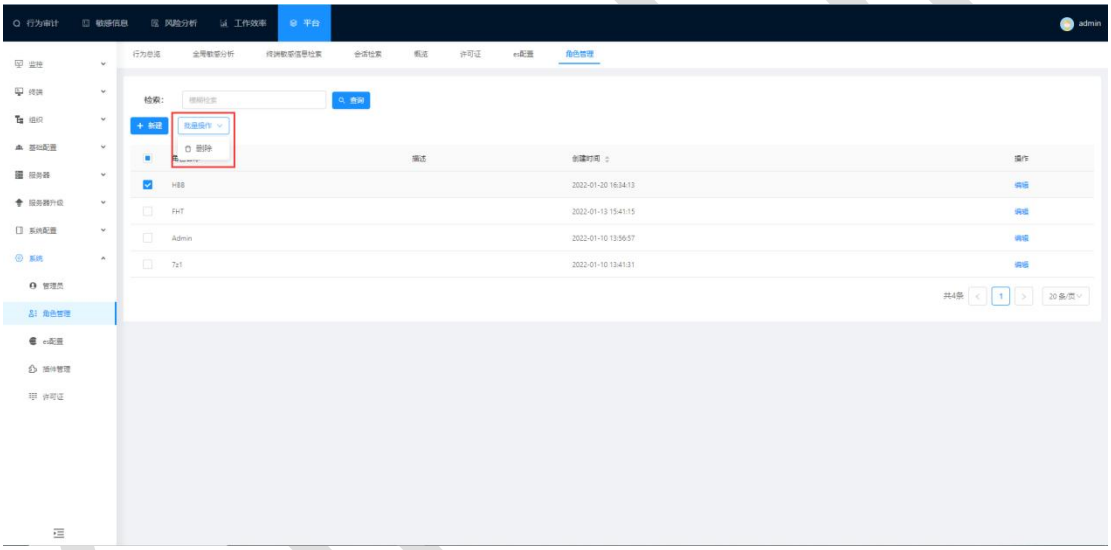
在检索处输入角色信息，检索角色。也可以点击字段名的列排序。提示：只有字段名三角形图案的才能排序。如下图所示：



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。



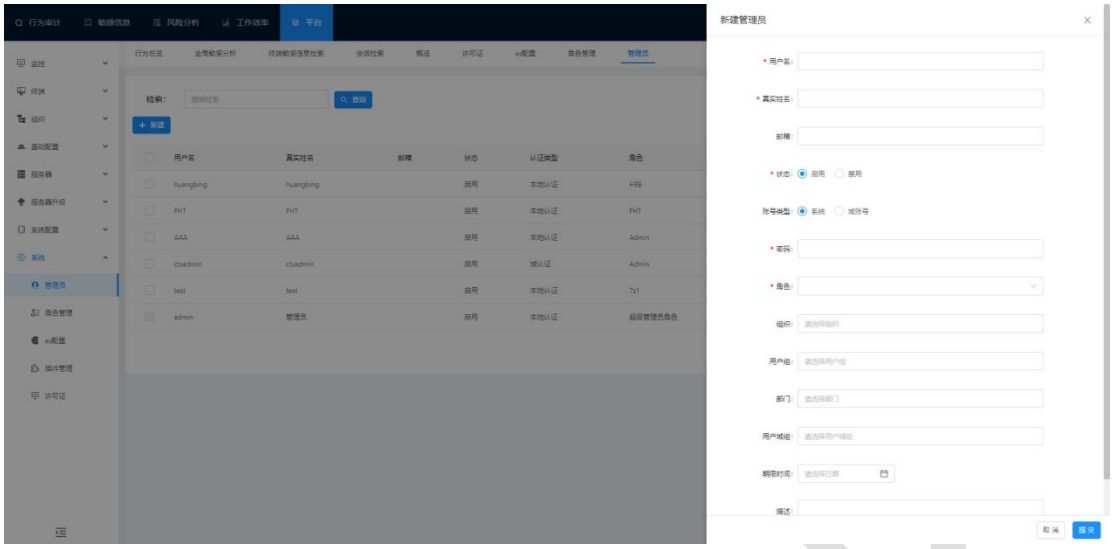
2.5 管理员

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”按钮新进新的管理员。

（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）

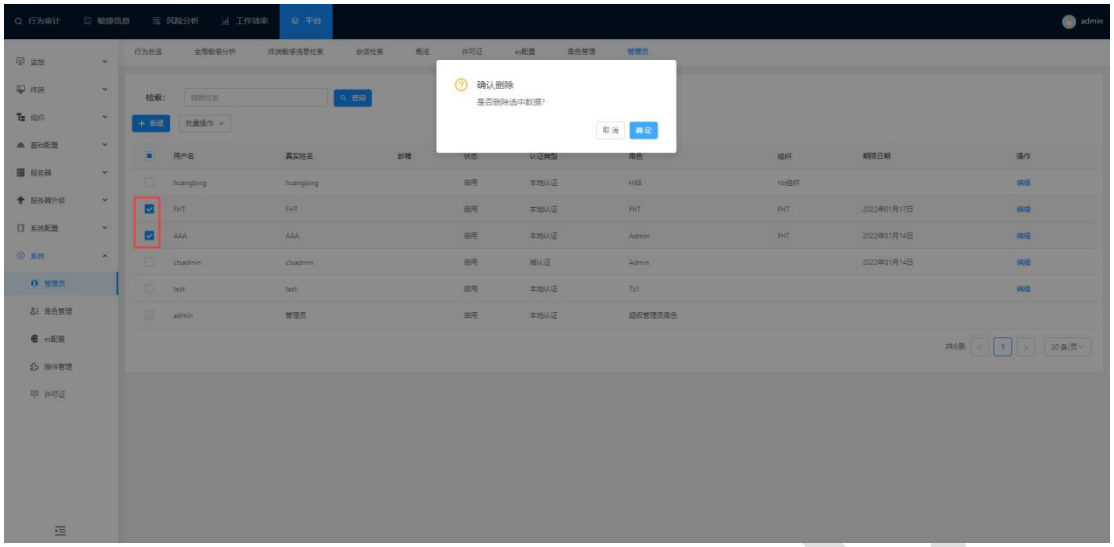
期限时间：超过设置的期限时间，则管理员不可再登录控制台。

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：

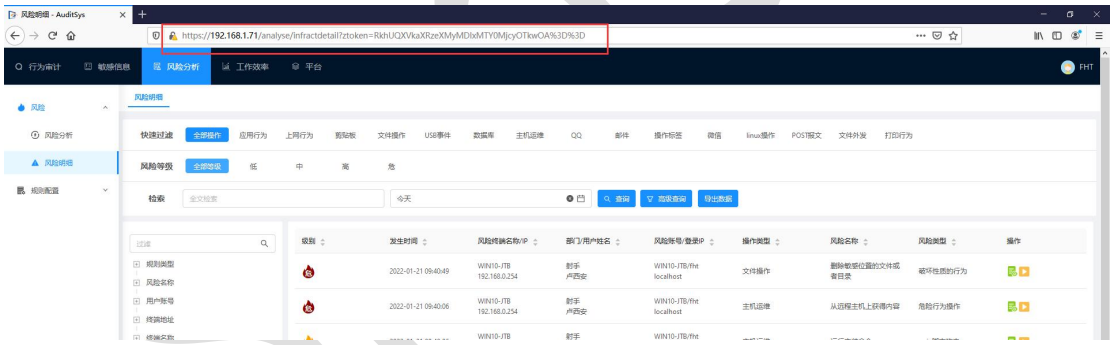


2.5.3 免密登录

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=ZnpoQXVkaXRzeXMyMDIxMTYzNDgwMzI5NA==



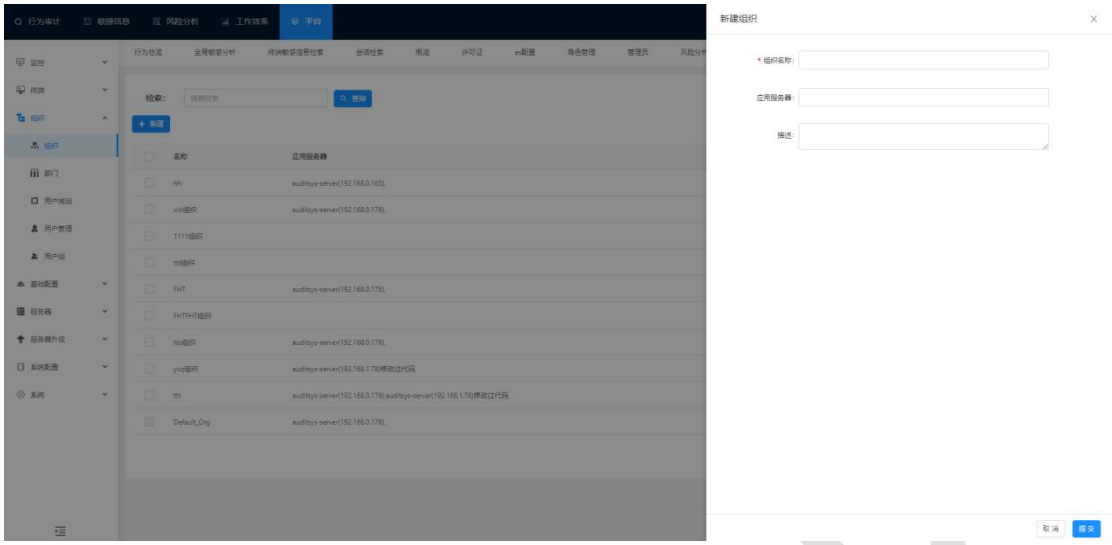
https://192.168.1.71/permissions/users：是想访问的模块地址。

ztoken=本地管理员生成的 secretkey 值。

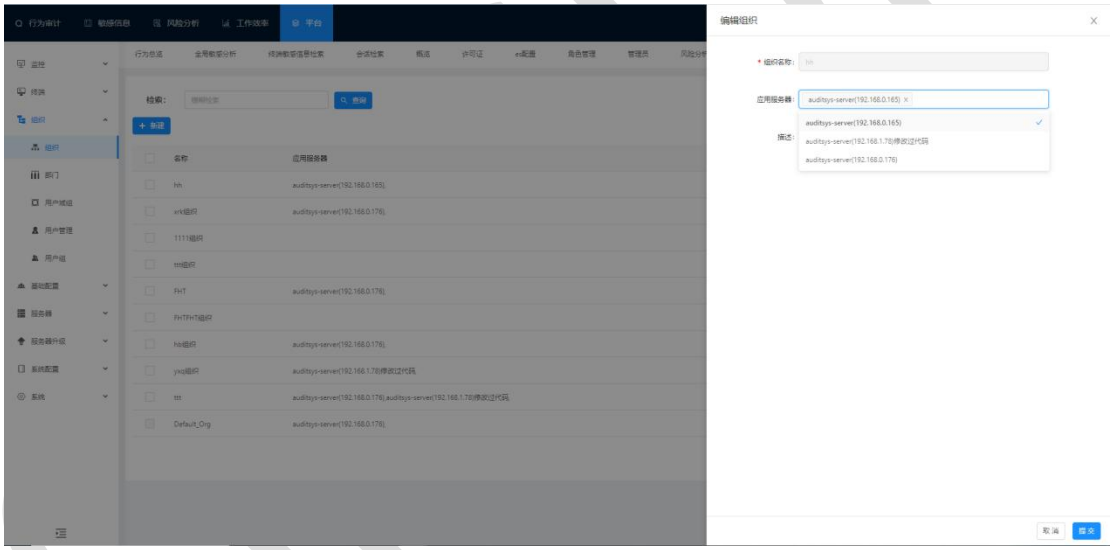
2.6 组织

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：

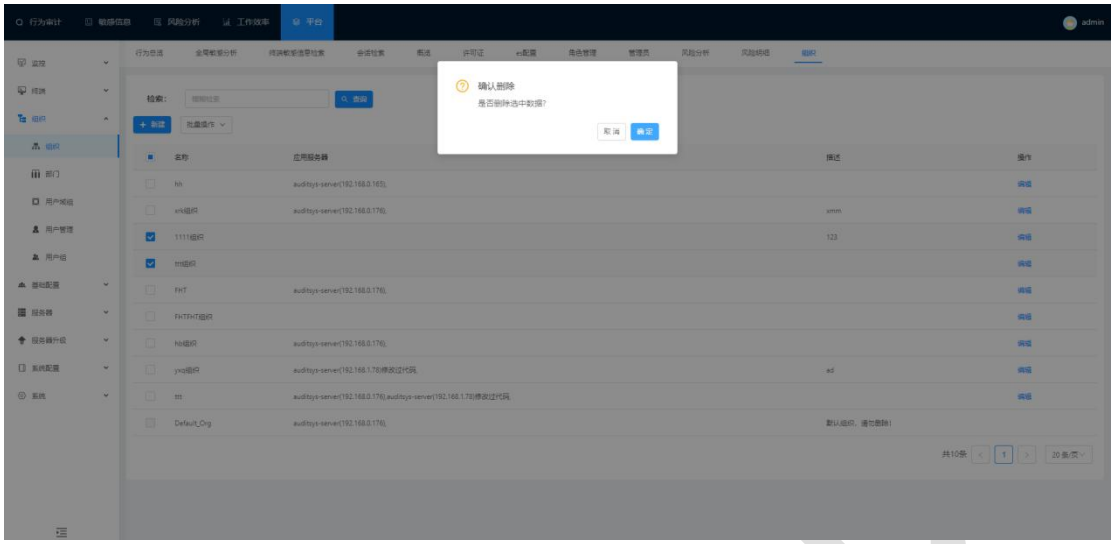


提示：新建的组织，终端组列表同时会自动生成一个对应终端组。

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：

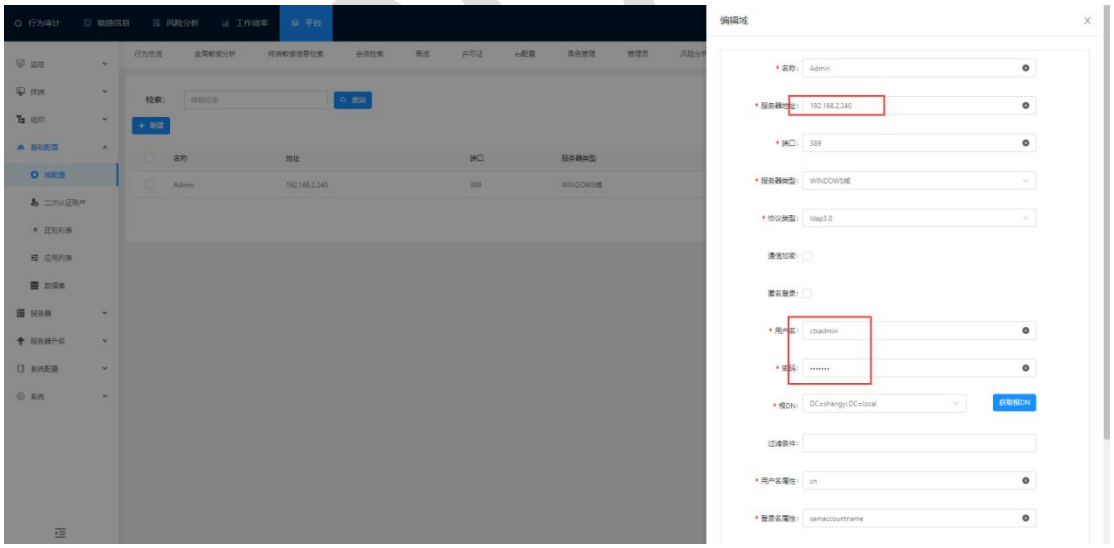


2.7 域配置

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

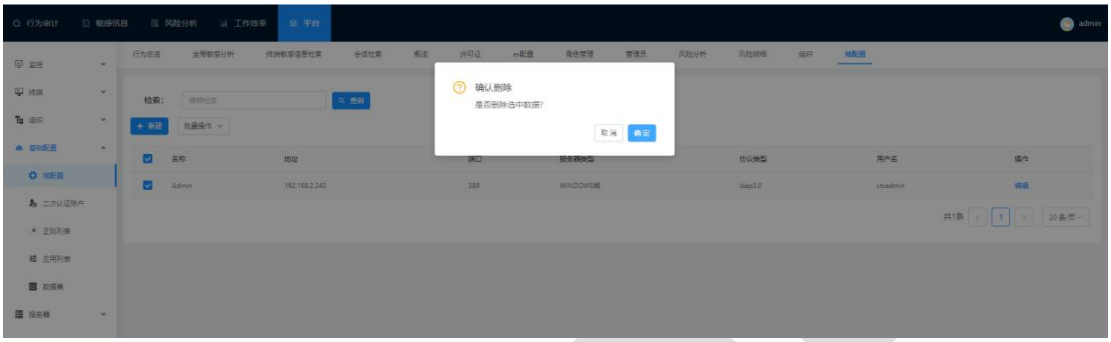
选择“平台>基础配置>域配置”，点击“新建”按钮新建新的域配置。如下图所示：



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

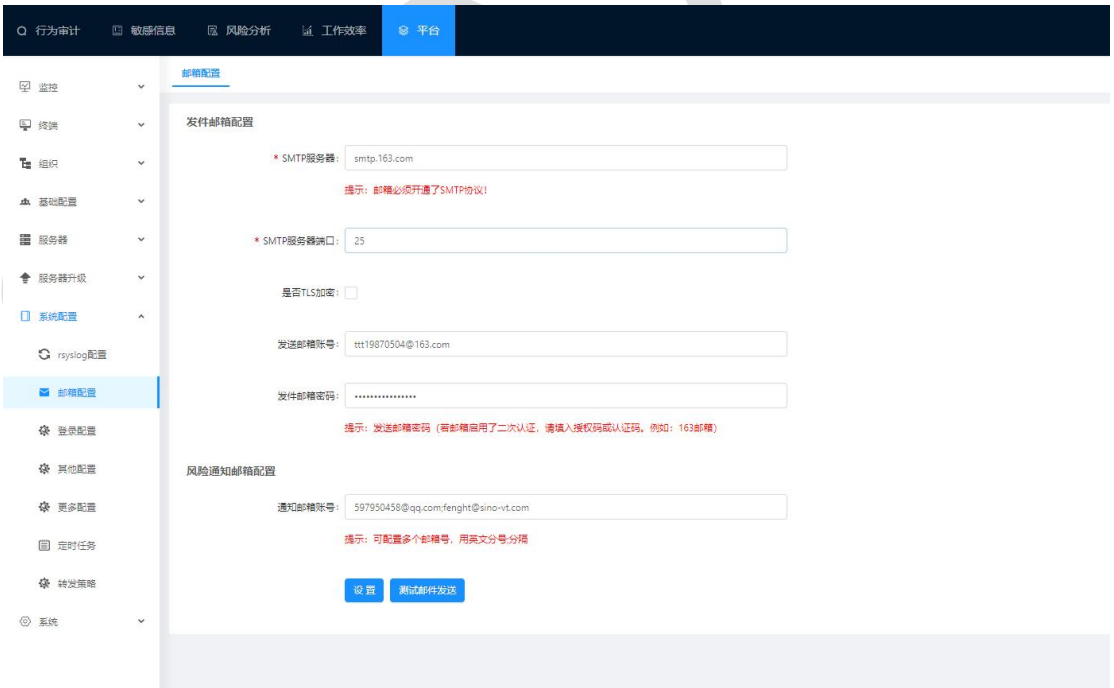
先勾选要删除的域配置（删除被引用的域配置，需要先解除），然后点击“删除”按钮，再“点击”确定。如下图所示：



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：

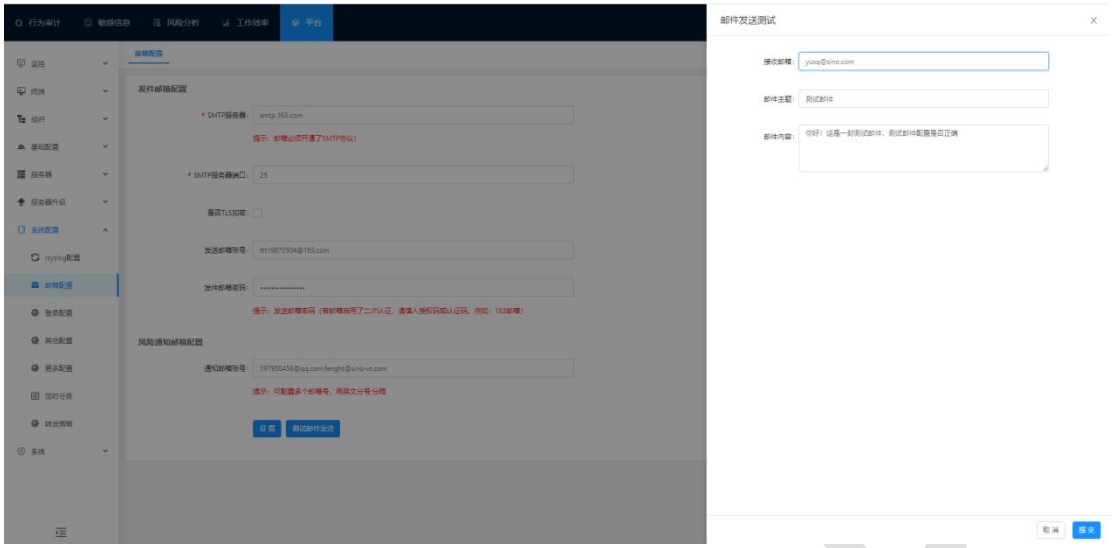


SMTP 服务器： 邮箱必须开通了 SMTP 协议。

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：



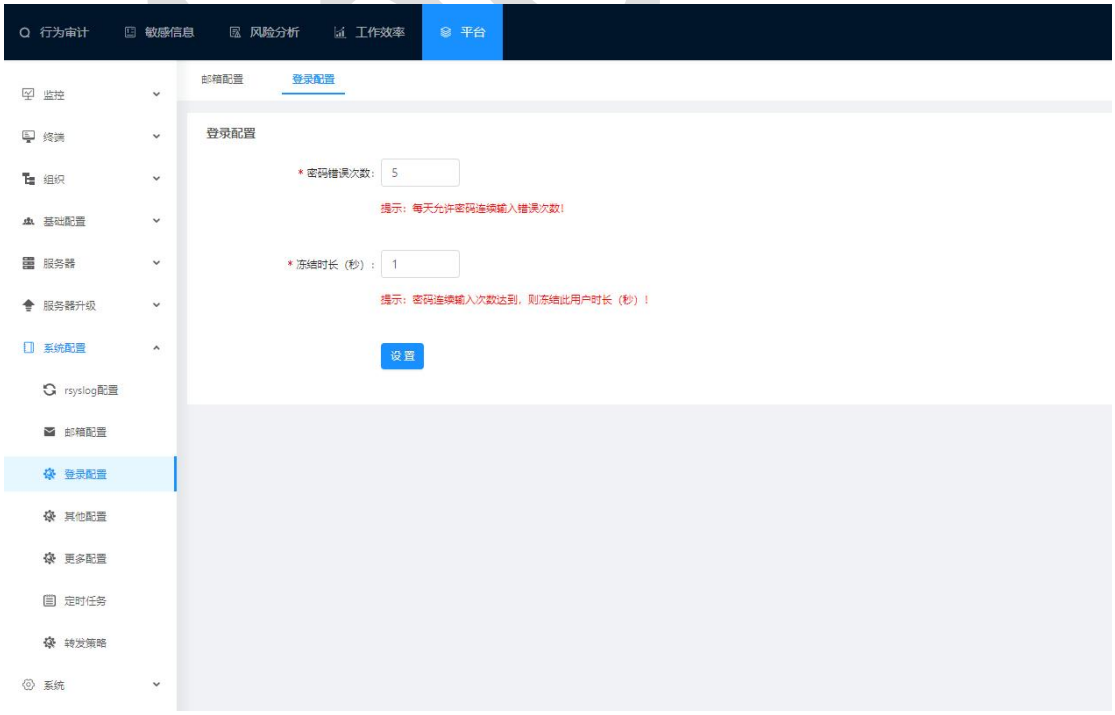
输入接收邮箱，点击“发送”按钮。 查看接收邮箱是否有收到邮件。如有接收到邮件，则配置成功。否则则配置失败。

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。

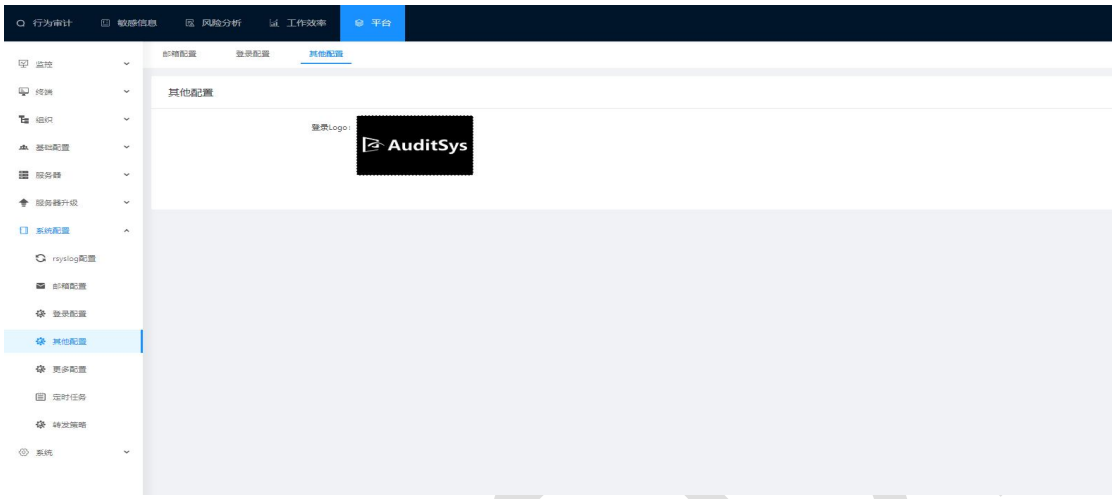
点击“平台>系统配置>登录配置”进入登录设置界面，如下图所示：



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：

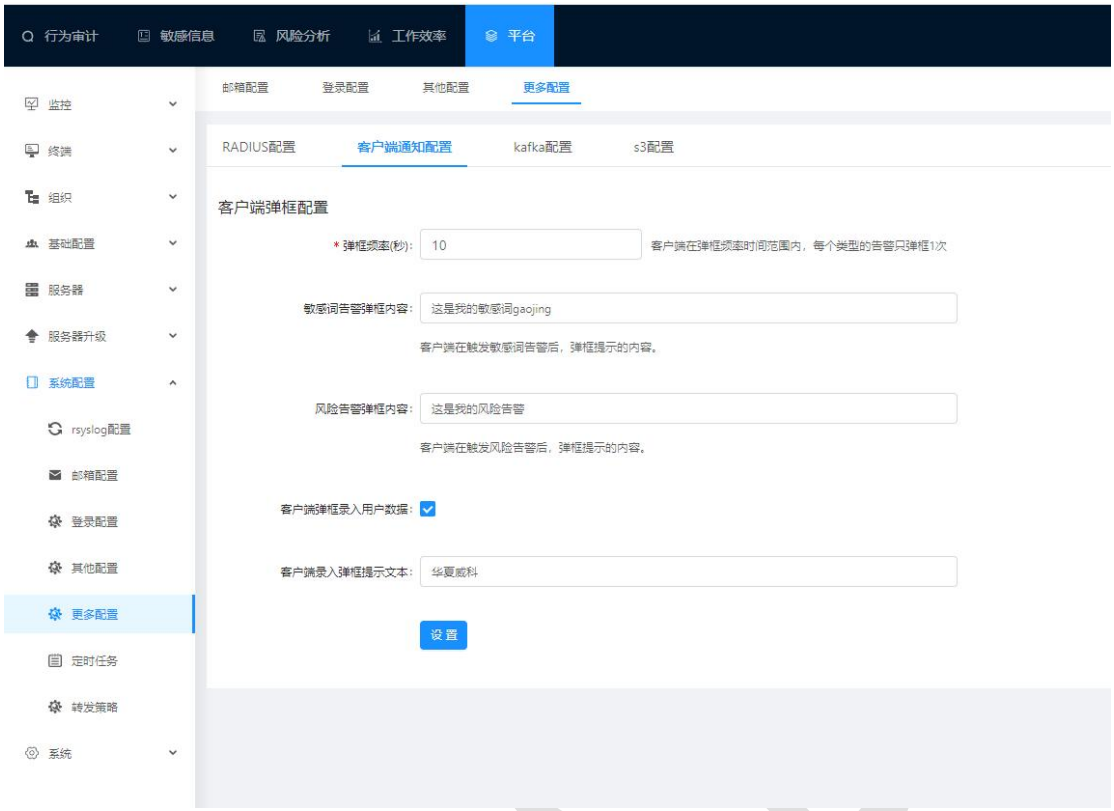


2.11 更多配置

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：



弹框频率：用户触发风险或敏感词每 10 秒弹框通知一次。

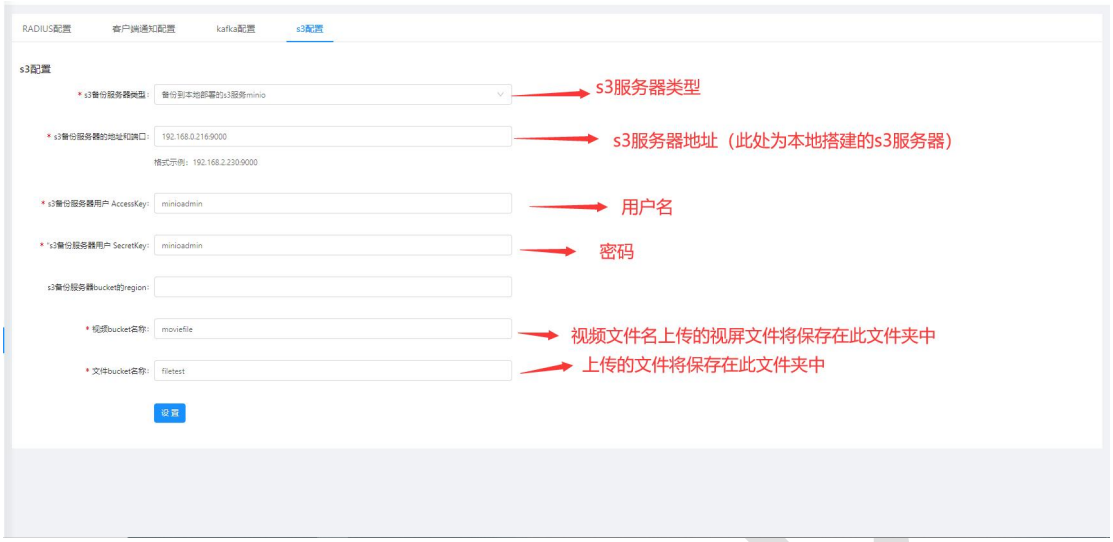
敏感词告警弹框内容：自定义通知的敏感词内容。

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。

2.11.2S3 配置

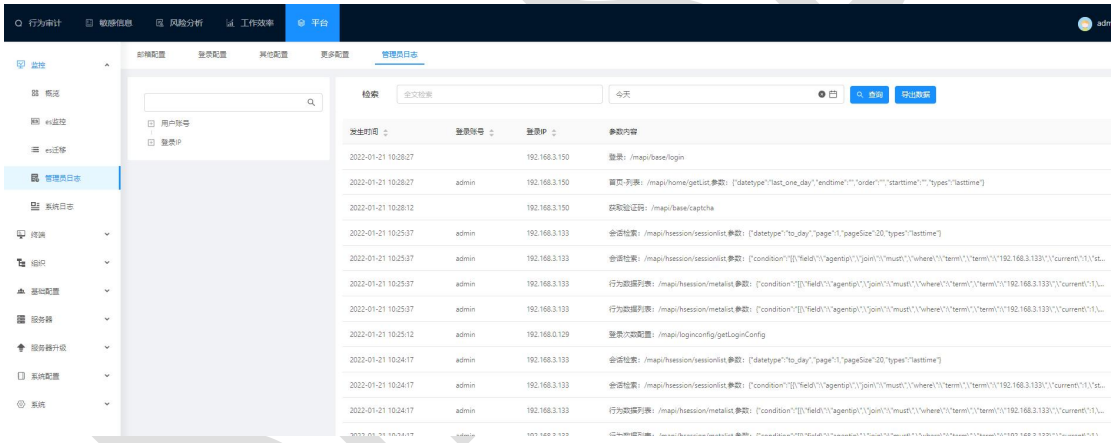
s3 配置用于配置 s3 服务器地址。点击平台>系统配置>更多配置>s3 配置，配置解释如图所示：



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：



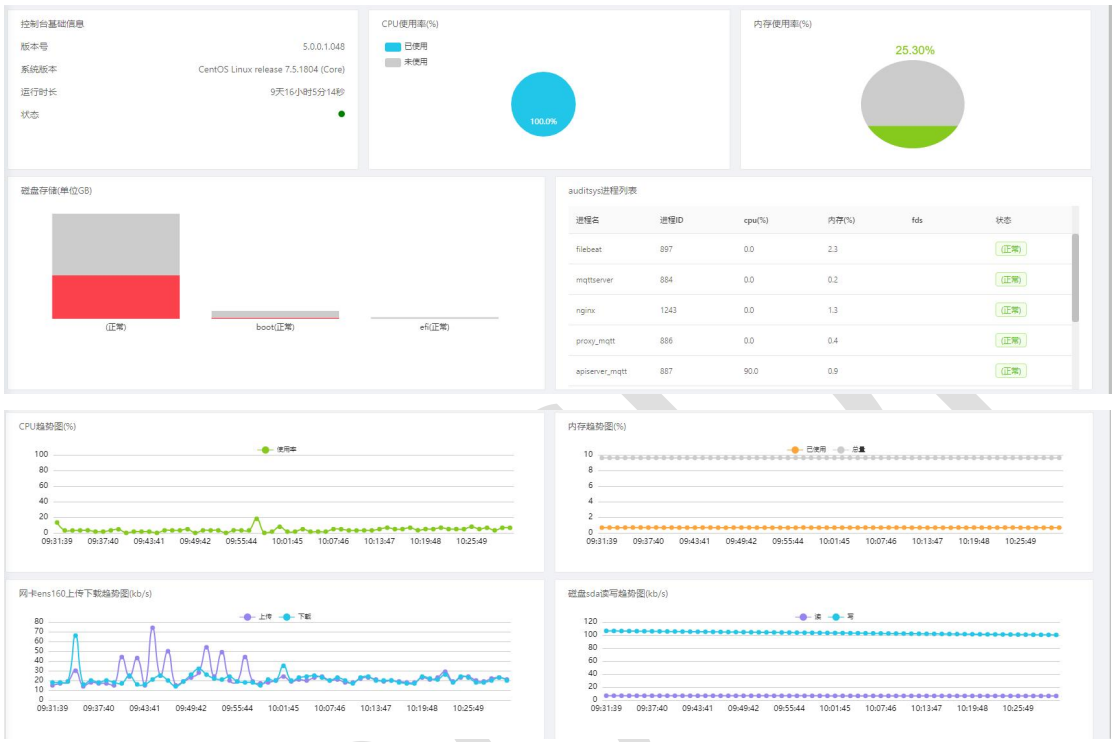
2.13 概览

2.13.1center 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：



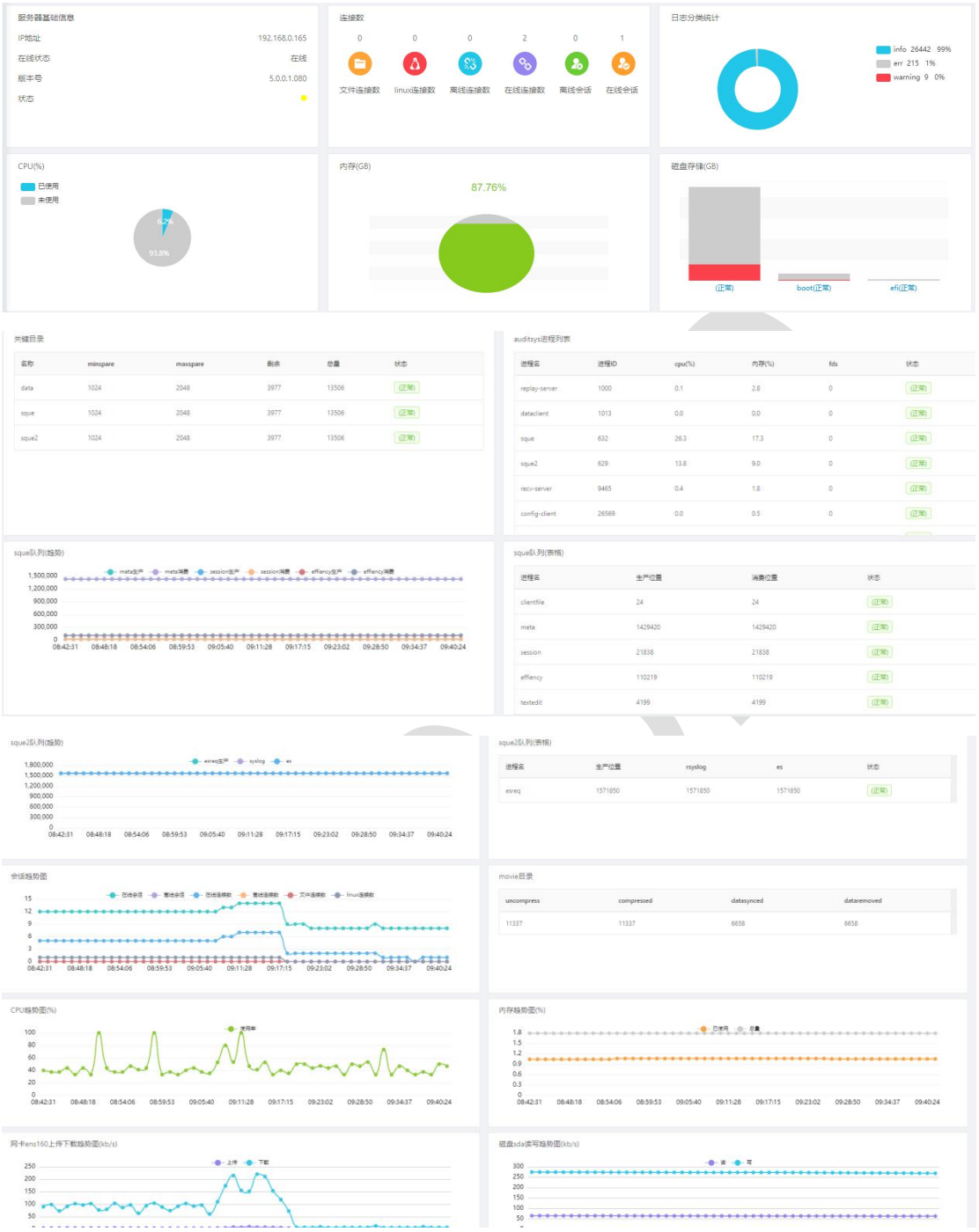
2.13.2server 概览

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。

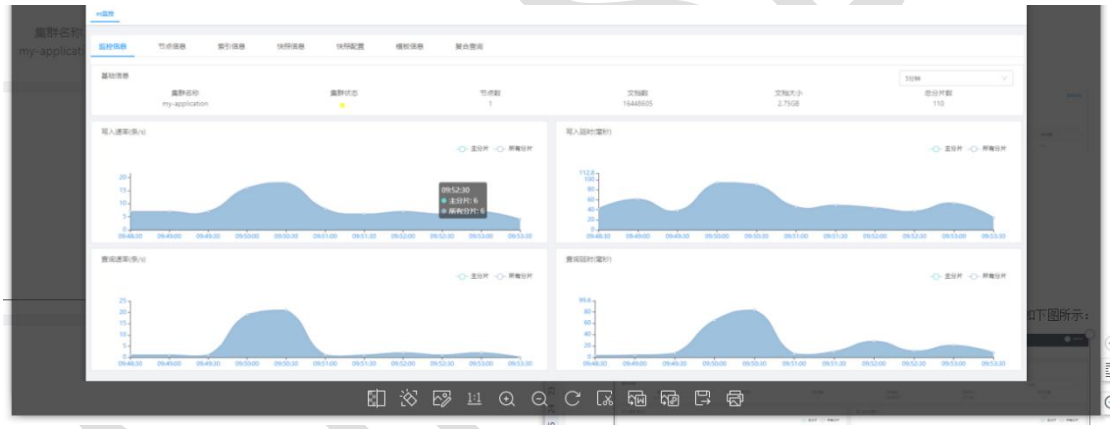
选择“平台>监控”，查看 ES 服务器的系统状态和性能。如下图所示：

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。

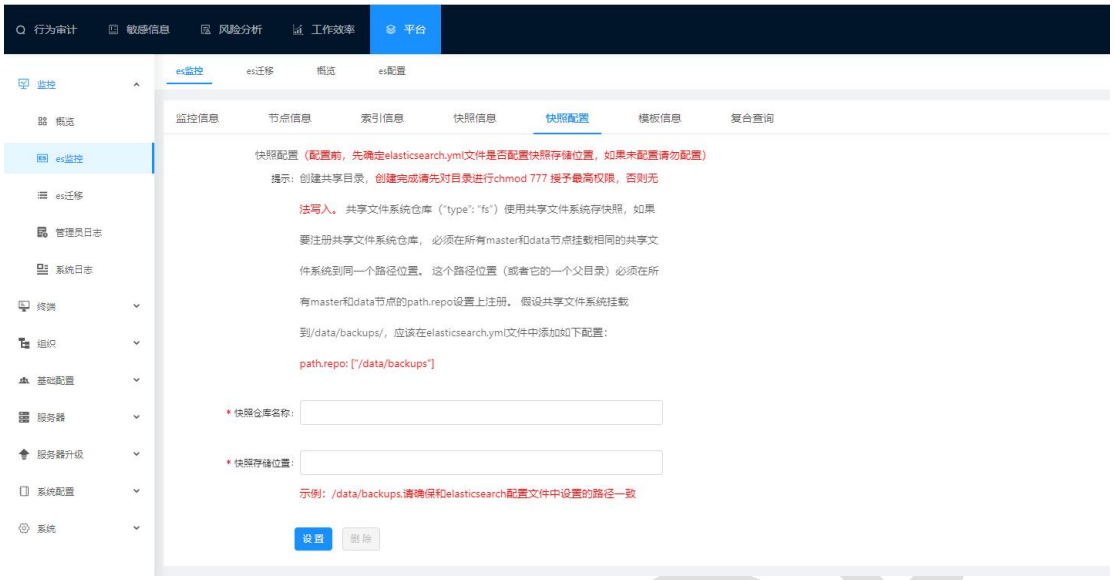
监控信息：监控 es 集群每秒写入速率，写入延时，查询速率，查询延时；如下图所示：



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：

2.14.1 快照配置

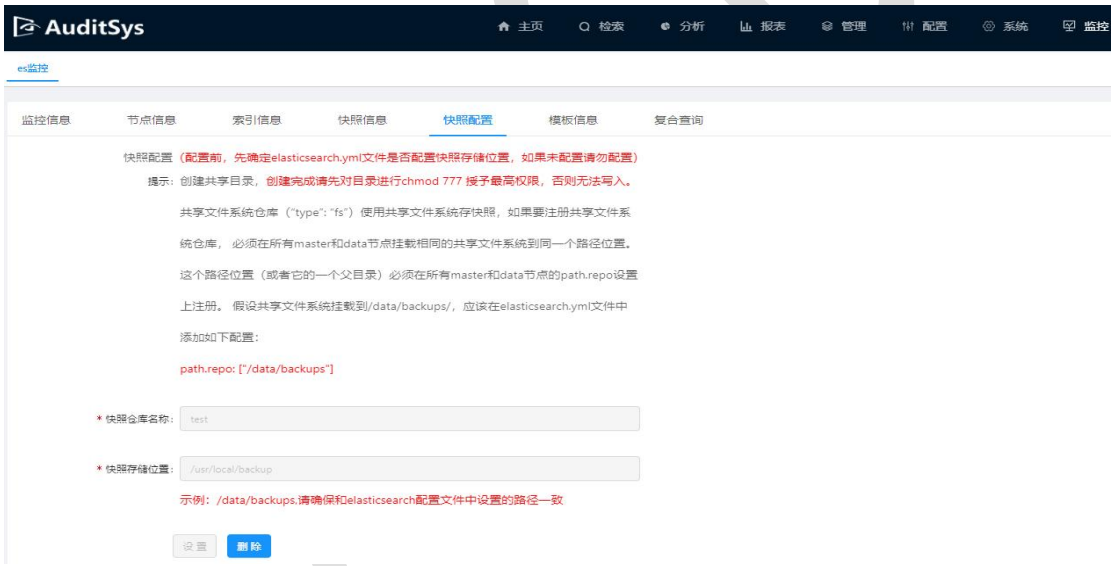
快照配置：快照仓库的配置（相当于索引信息备份的仓库）如下图所示：



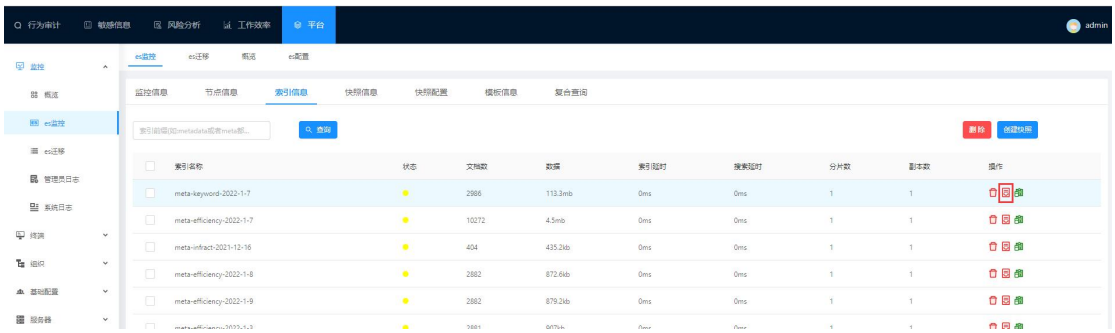
2.13.2 索引信息

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

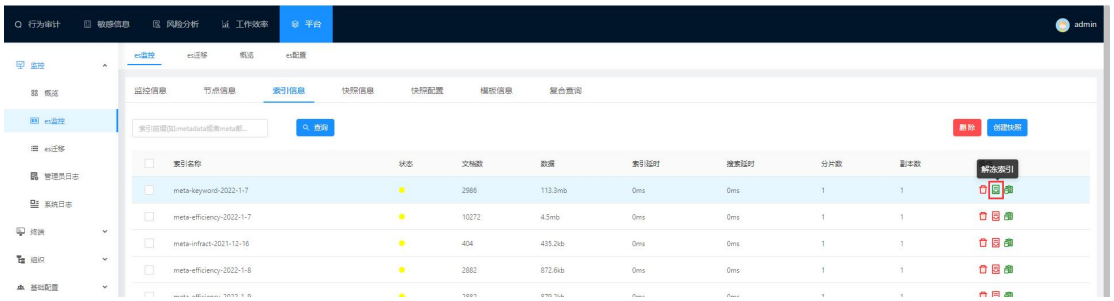


冻结索引：该索引信息不会再写入数据；例如：冻结下图索引信息；则用户在终端的元数据行为操作暂时不会写到该索引信息（被操作的数据会丢失）。如下图所示：



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：



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：

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。

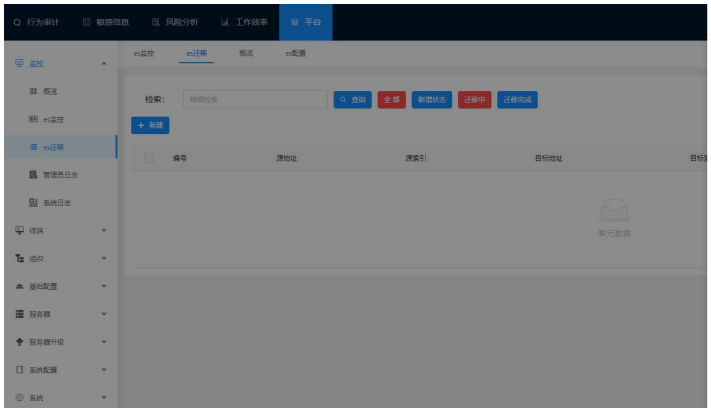
2.15es 迁移

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：

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。

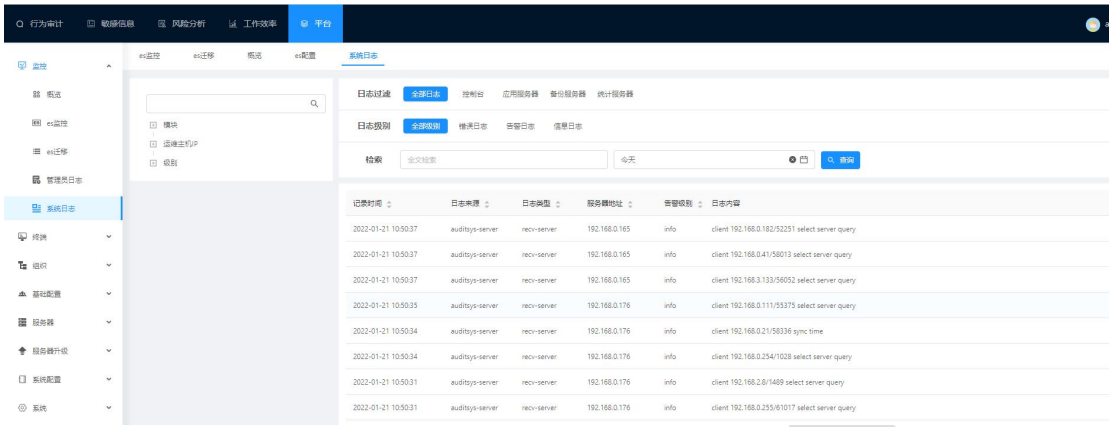
2.15.2es 数据迁移

选择要迁移的 ES 数据，点击“迁移”按钮，进行迁移；如下图所示：

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。

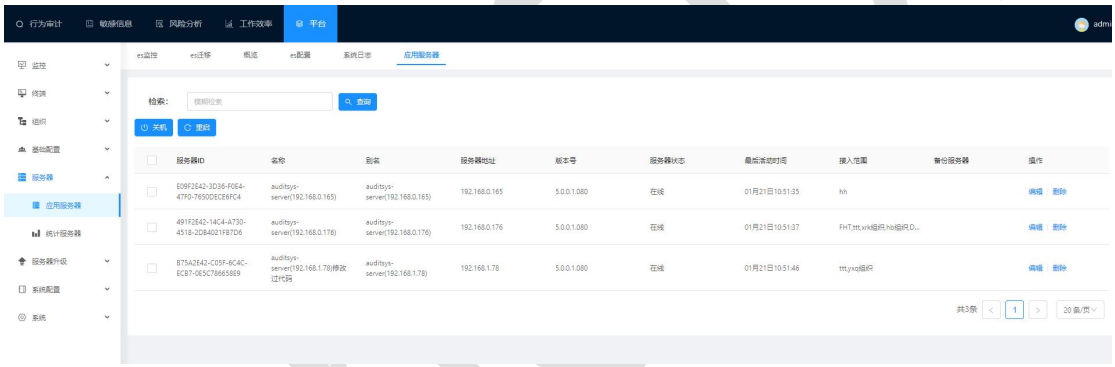
选择“平台>监控>系统日志”进入系统日志界面；如下图所示：



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。

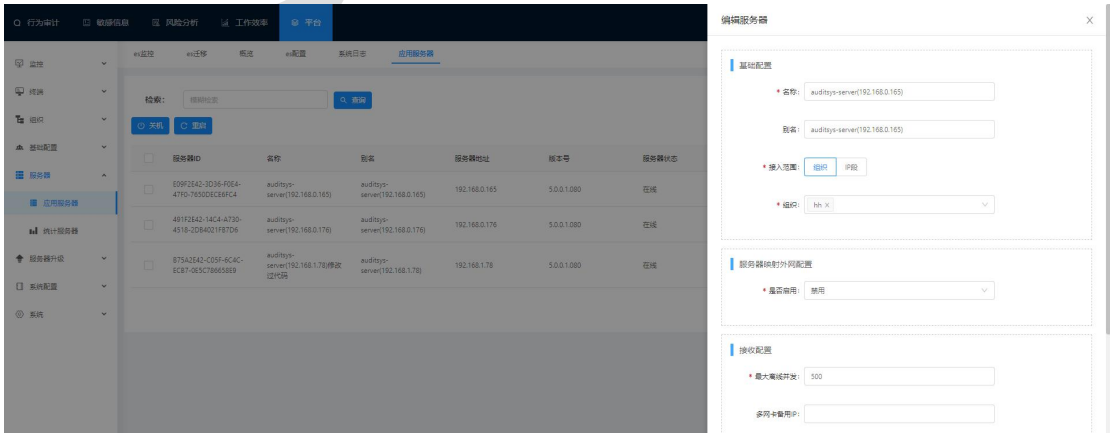
选择“平台>服务器>应用服务器”查看应用服务器信息。如下图所示：



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：

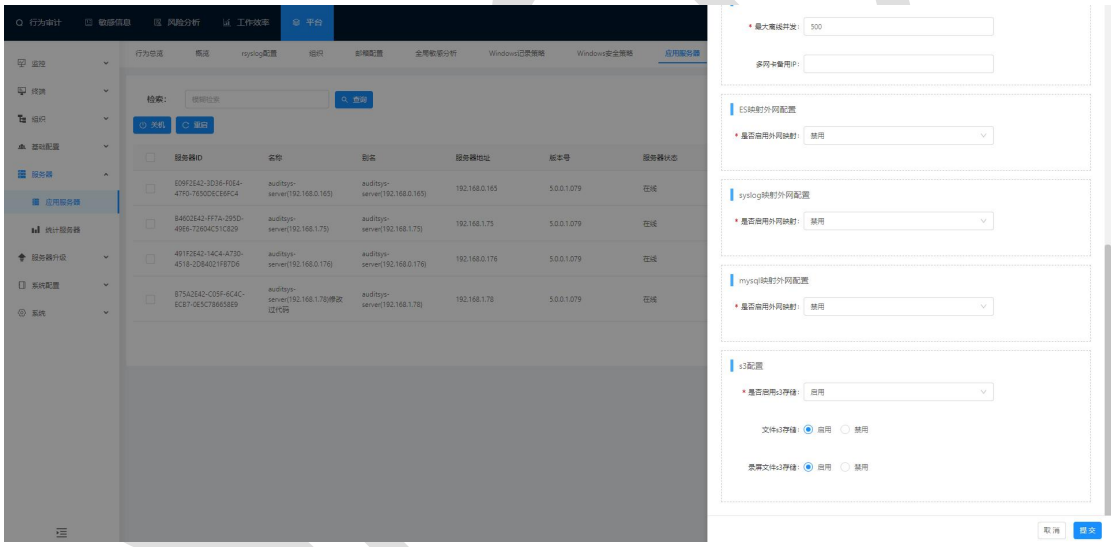
是否启用：启用，则终端的审计数据会写入外网的应用服务器。

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

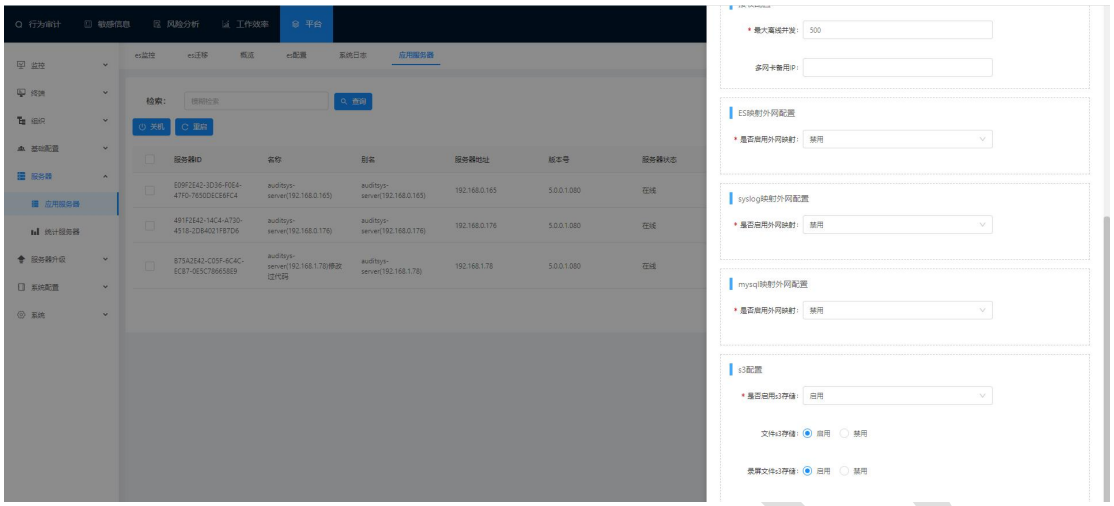
接收配置：

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。

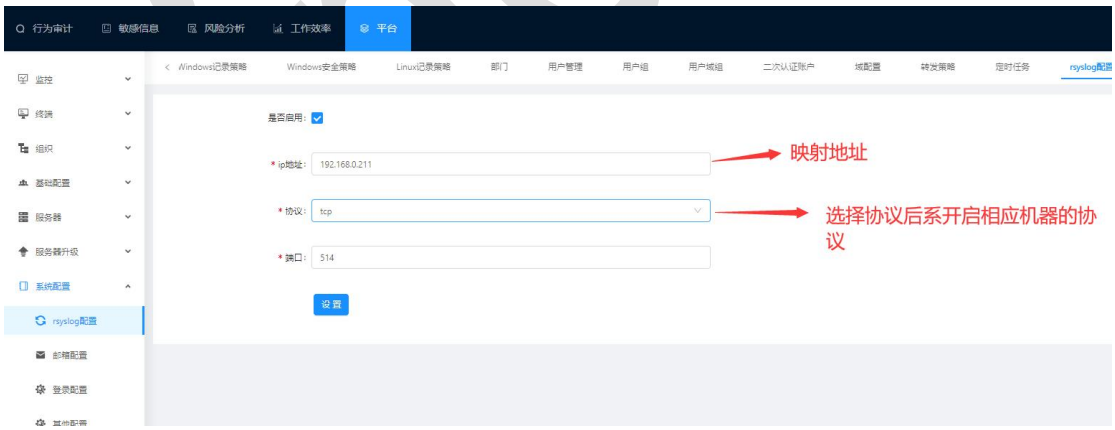
Syslog 映射外网配置：

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：

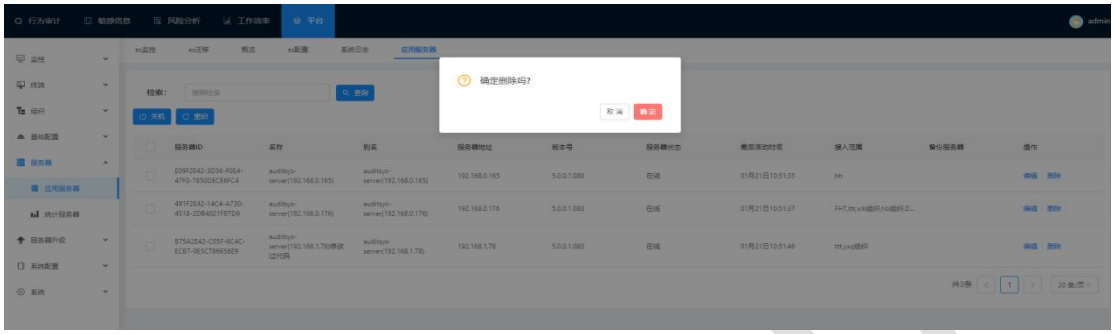
是否启用外网映射：启用，则可以使用外网 MySQL 的策略配置。

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：



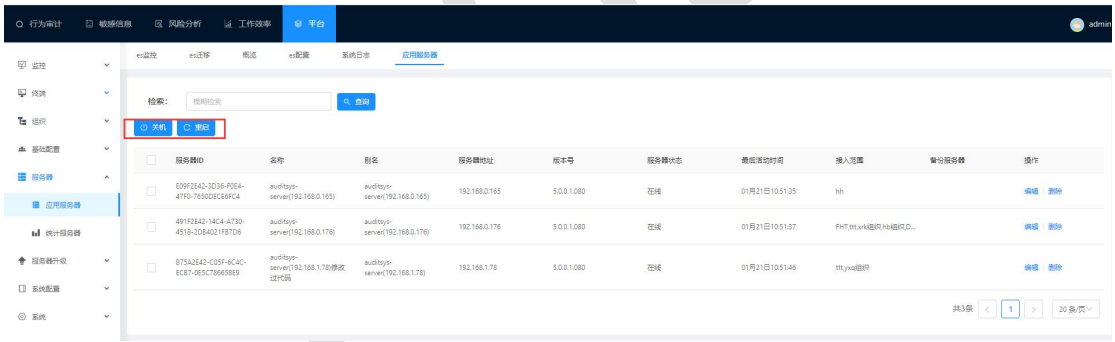
删除在线的服务器成功后，过一会儿，会重新注册上报到应用服务器界面；需要重新配置接入访问和其它配置。

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。

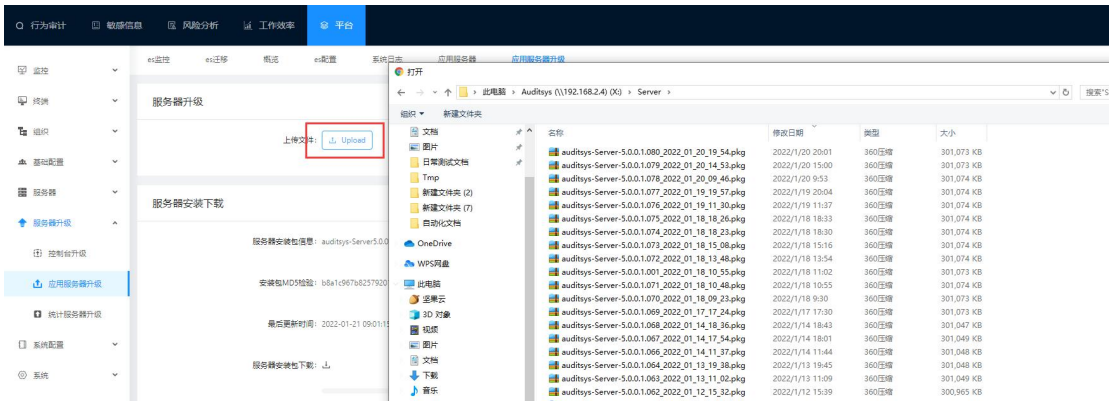
选择服务器，点击重启，此服务器重启。



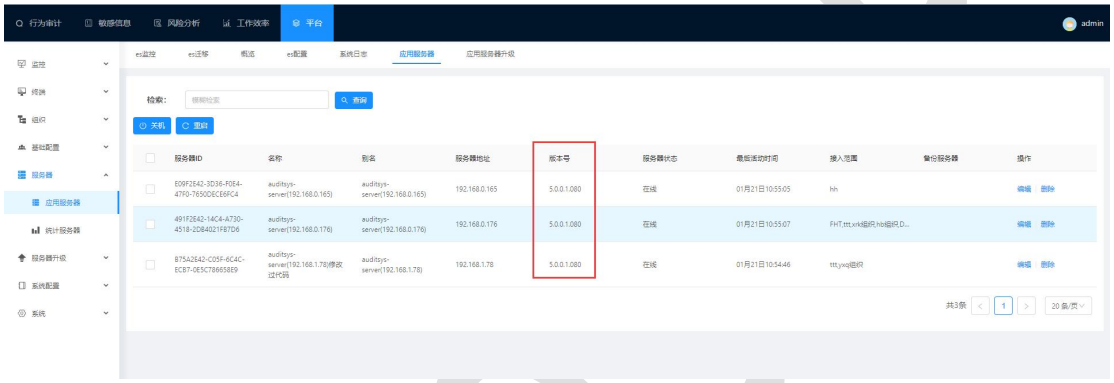
2.16.4 应用服务器升级

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：

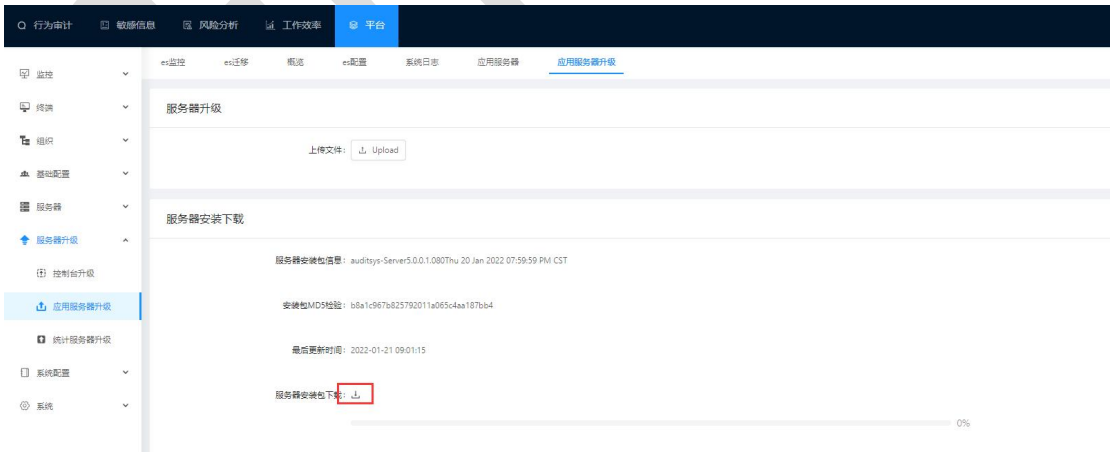


查看所有 Server 是否升级完成，请查看“应用服务器”模块，服务器列表中有版本号。如果 Server 是离线，则需要等待 Server 上线后才会升级。如下图所示：



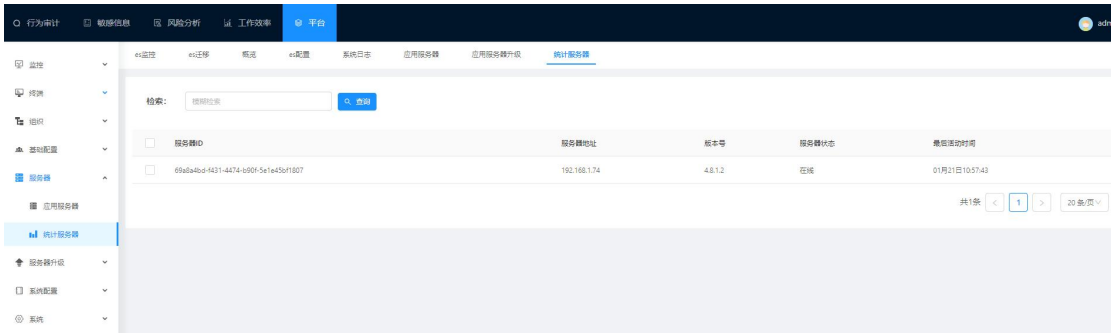
2.16.5 安装包下载

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。

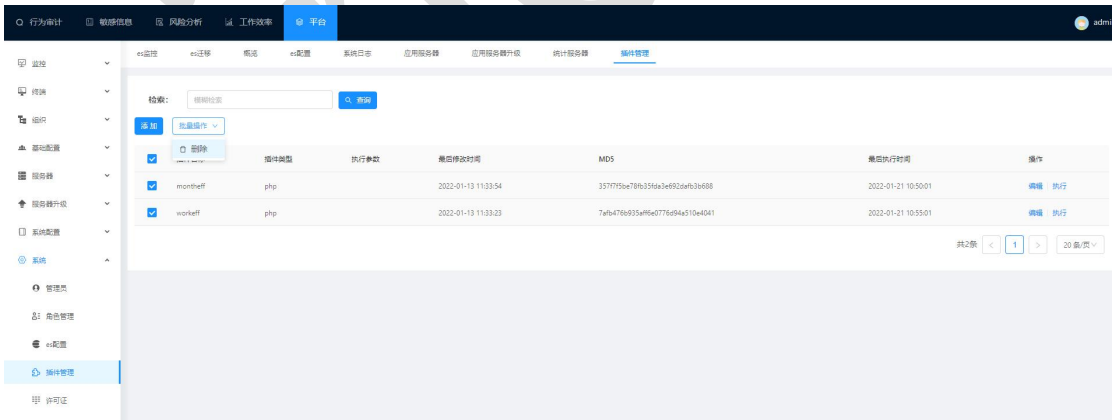
统计服务器安装包下载步骤：详见步骤 3.1.5 应用服务器安装包下载。

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）

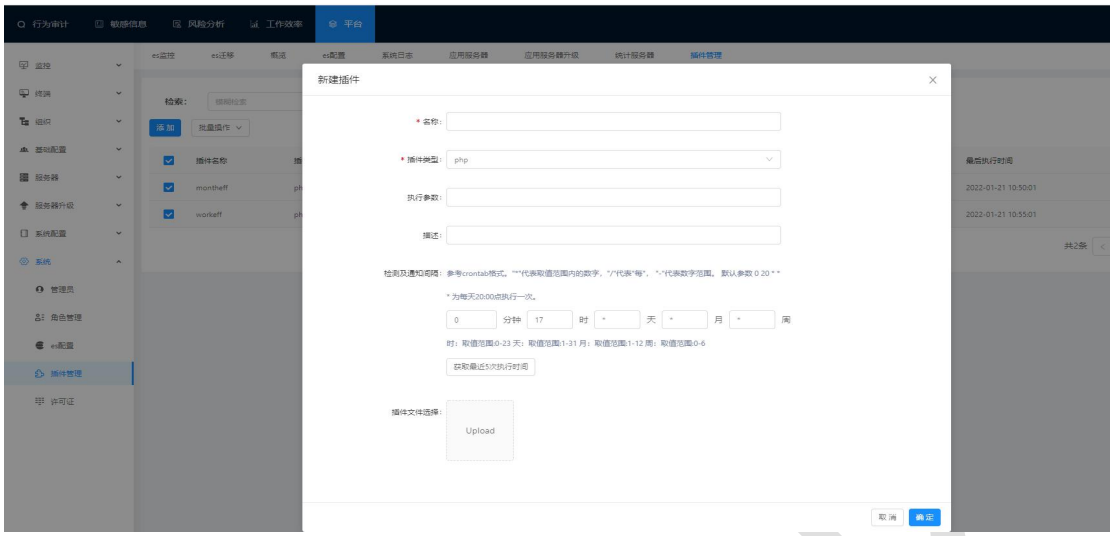
Montheff 插件：计算部门、公司以及每月数据汇总的插件，统计的数据是在 workeff 计算的基础上二次统计，默认会重算当月所有数据（效率汇总）。

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。

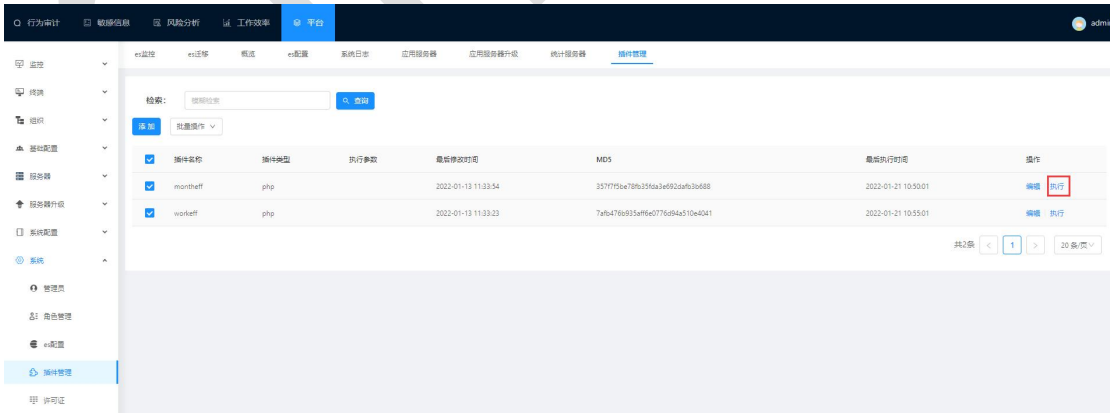
检测及通知间隔：配置自动执行时间。

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。



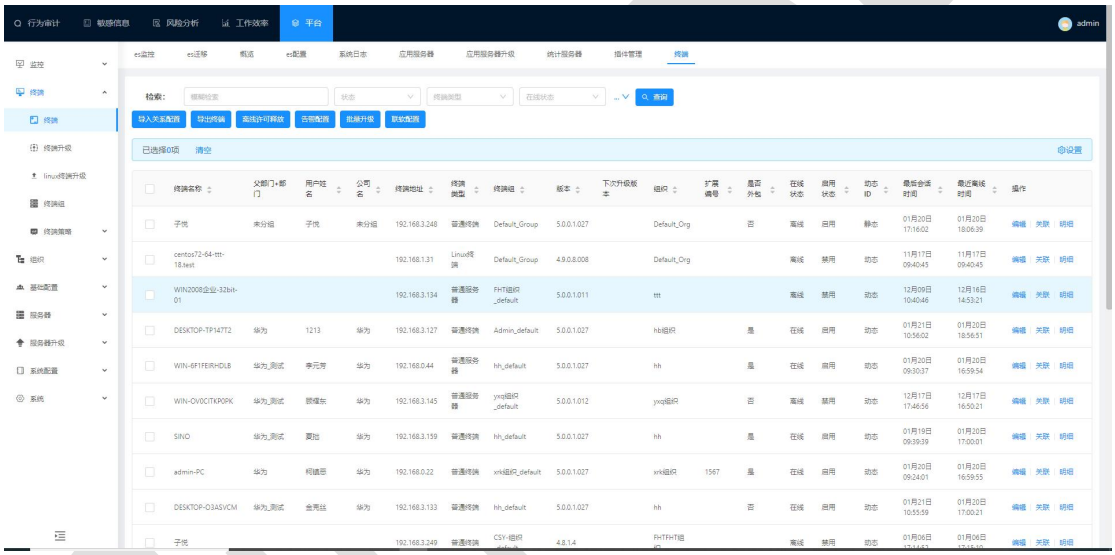
2.18 终端

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。

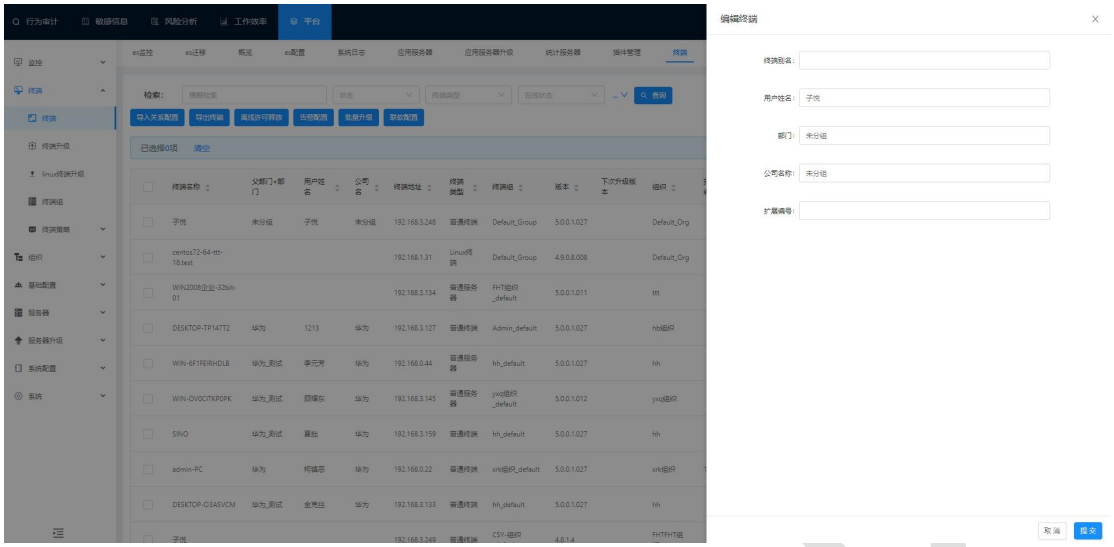
2.18.1 终端列表

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：



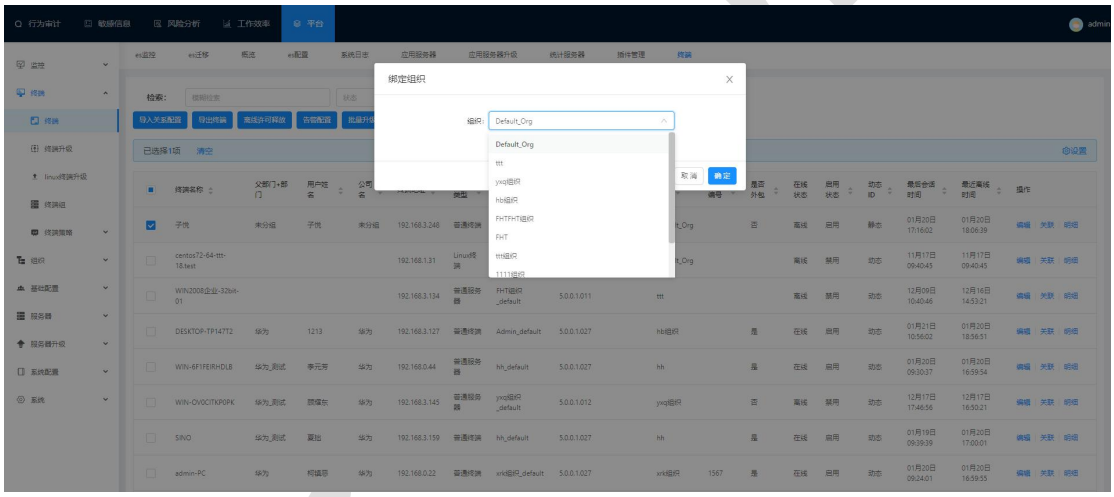
2.18.2 编辑终端

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：



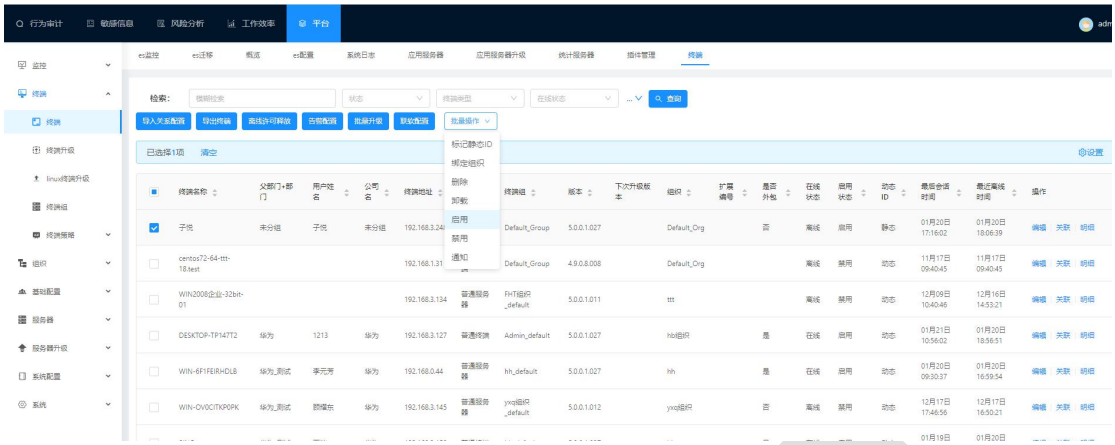
2.18.3 绑定组织

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：



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：



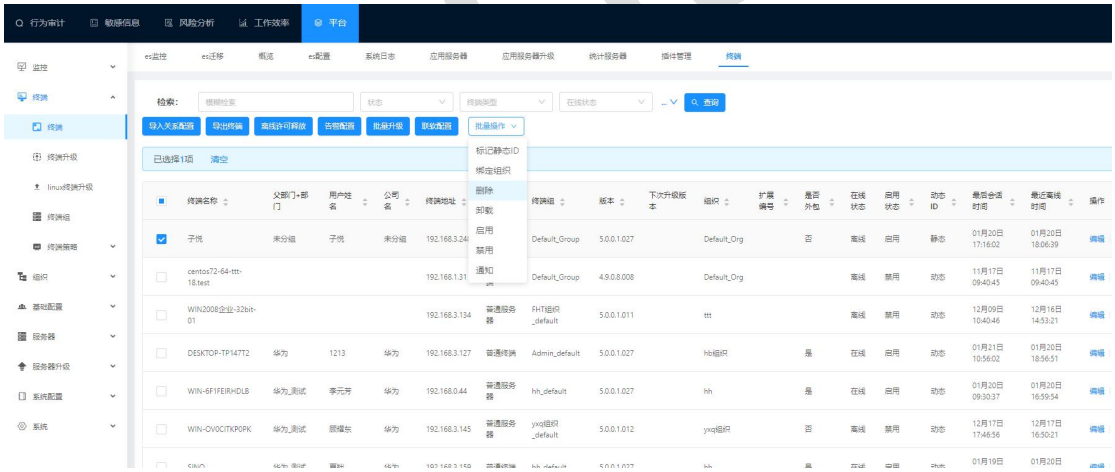
点击启用或禁用有提示确认框。点击“确定”。

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

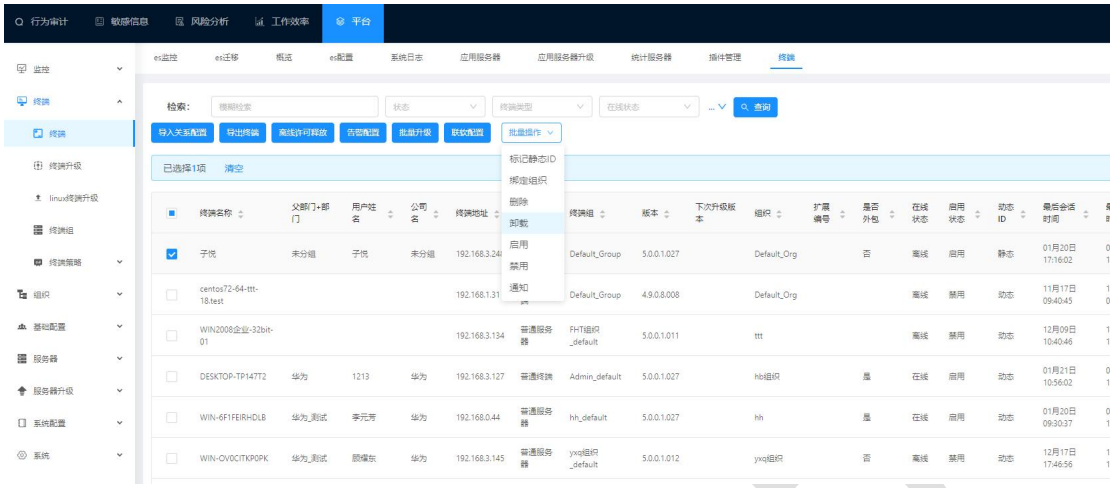
勾选需要删除的终端，点击“删除”按钮删除终端记录（只删除了界面数据）。如下图所示：



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：

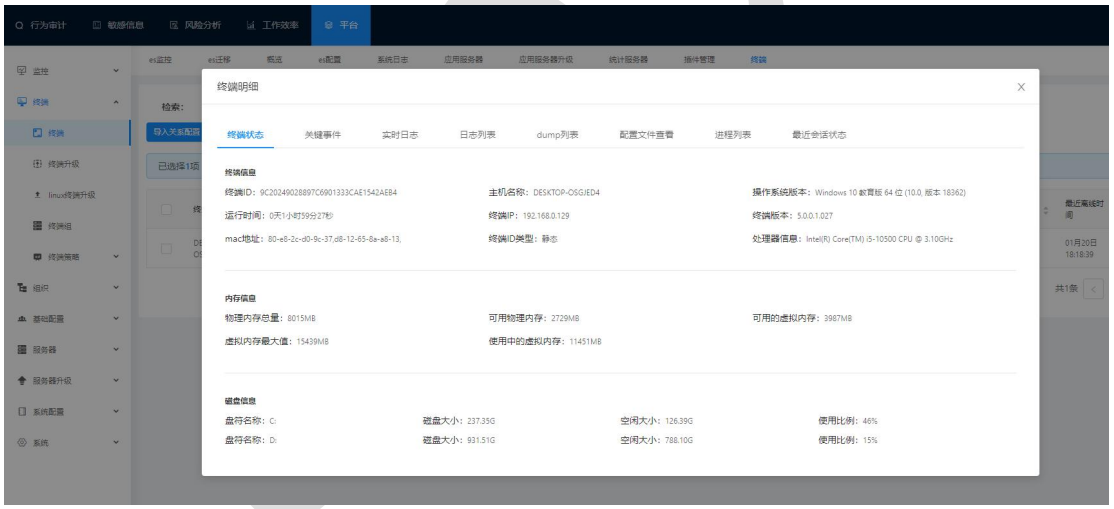


提示：离线终端需等待上线才会执行卸载！

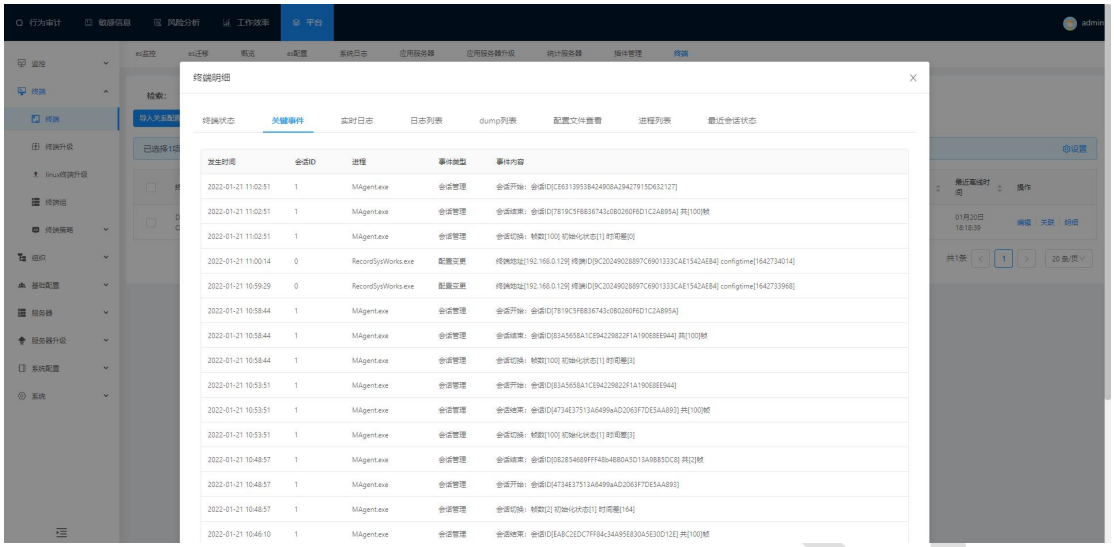
2.18.7 终端明细

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。

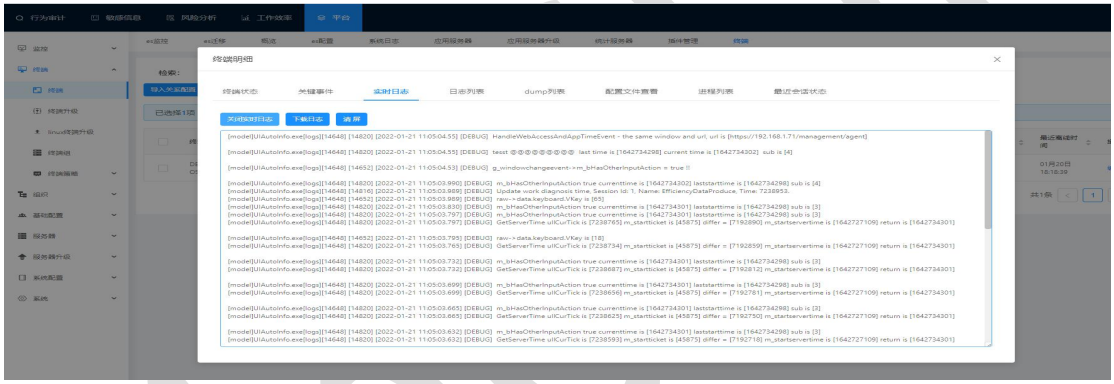


关键事件：更改终端对应的策略，终端名，终端 IP，终端重启，关机，注销，应用服务器配置更改，时间修改，终端解锁屏，应用阻断，Magent 重启等操作都会记录相应关键事件。如图所示：

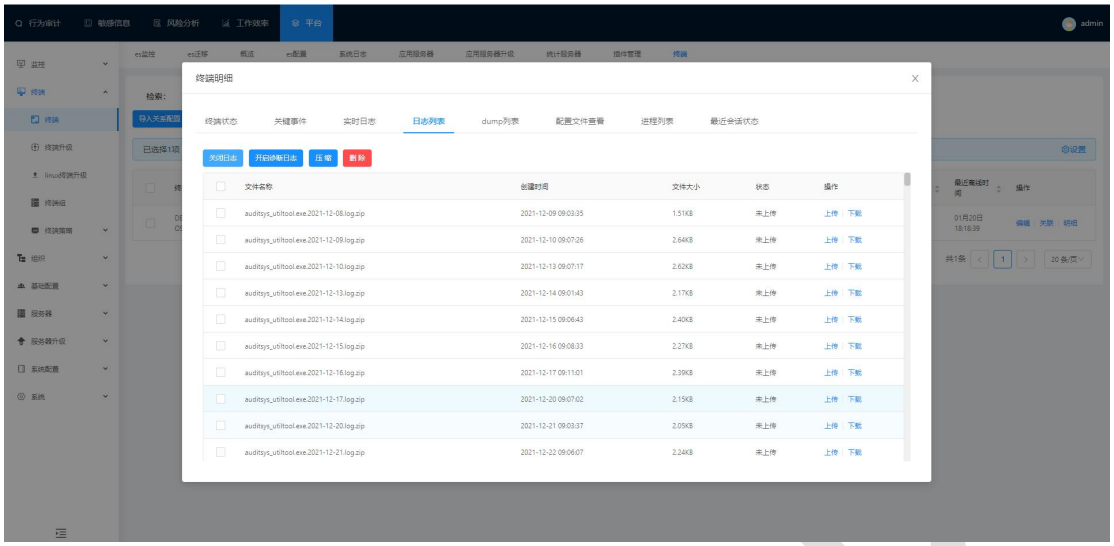


实时日志:点击开启实时日志记录终端实时操作所产生的日志，如下图所示：

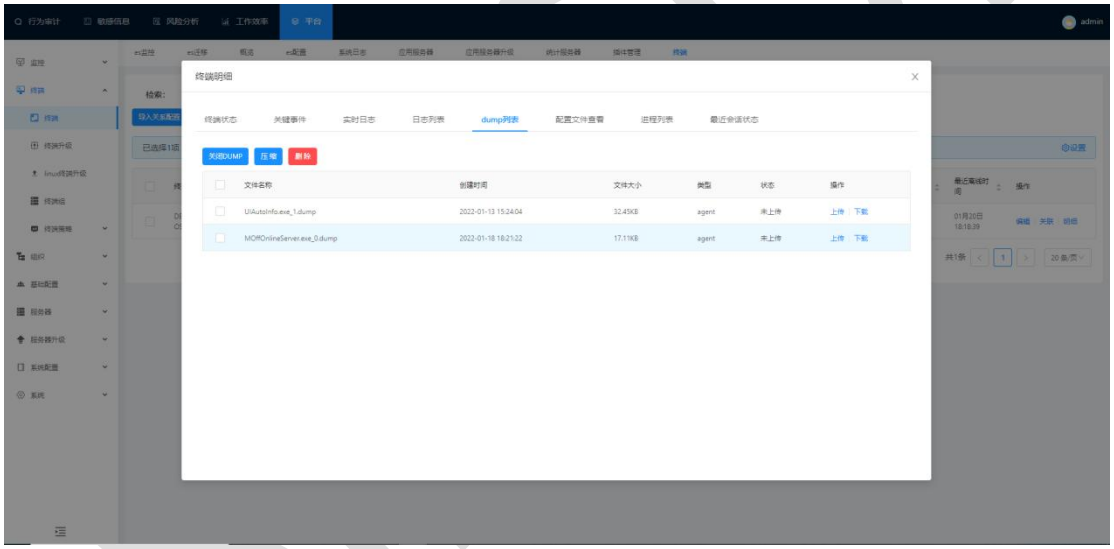
（注：开启实时日志或在日志列表开启日志，才会记录 DEBUG 日志）



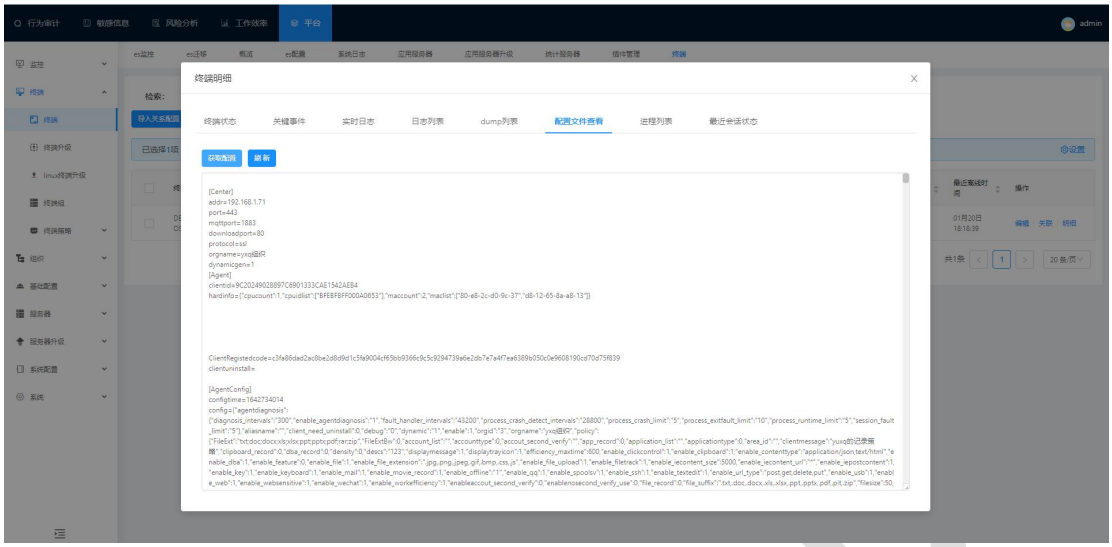
日志列表：开启日志，记录终端操作产生的日志和 DEBUG 日志，支持上传下载（日志状态显示是已上传才能下载）；删除日志列表的日志，安装目录下 log 日志文件下所对应的日志也被删除;支持日志文件压缩；开启诊断工具，则会产生一个 Diagnosis.log 日志文件；如下图所示：



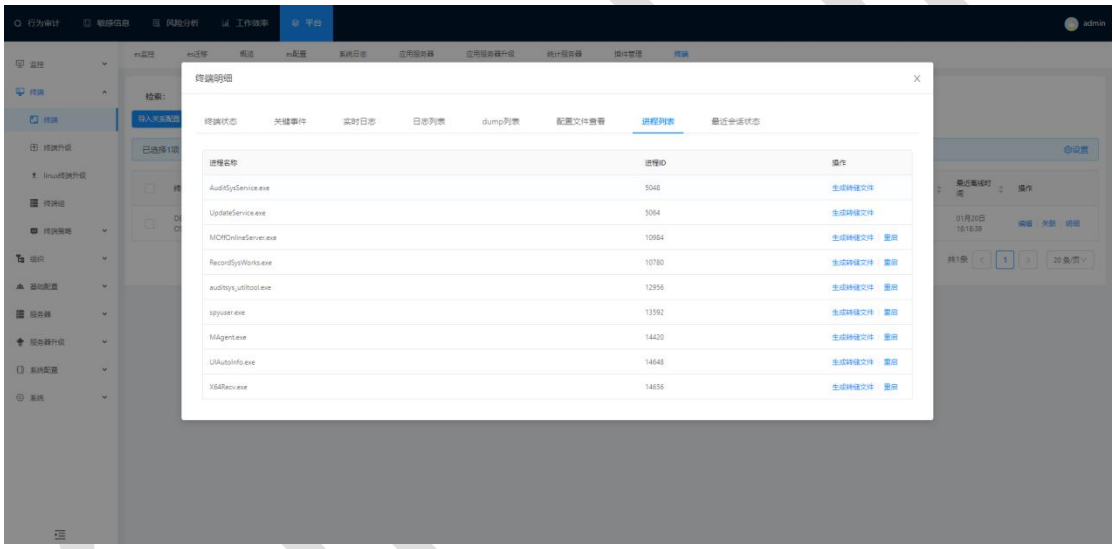
Dump 文件：点击查看 dump 文件，支持下载上传（日志状态显示是已上传才能下载）；删除 dump 列表的日志，安装目录下 dump 日志文件下所对应的日志也被删除;支持日志文件压缩；如下图所示：



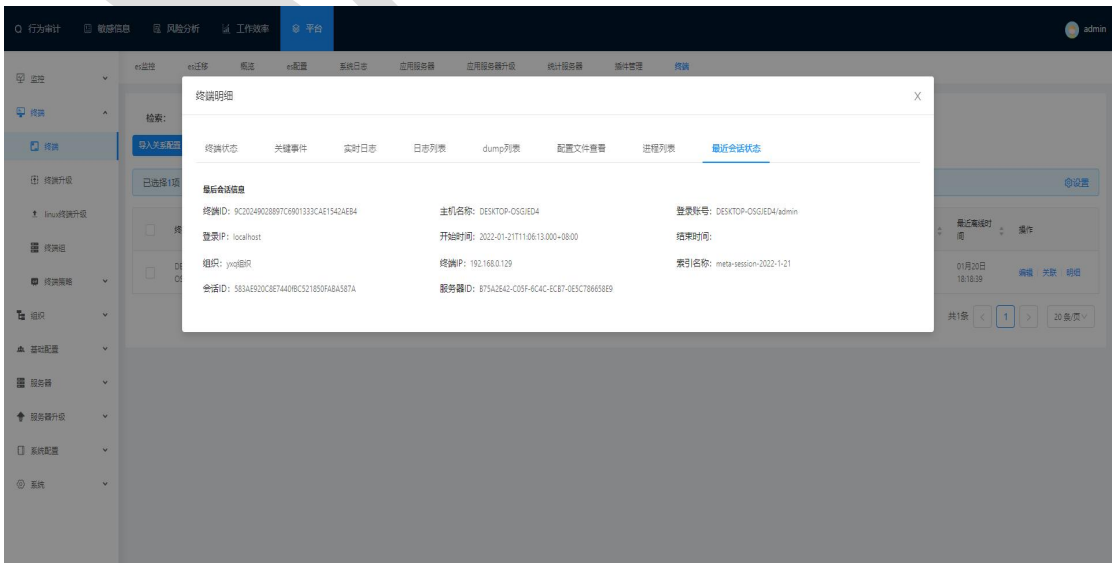
配置文件获取：点击获取配置文件，查看 agent 文件配置详情，如下图所示：



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：

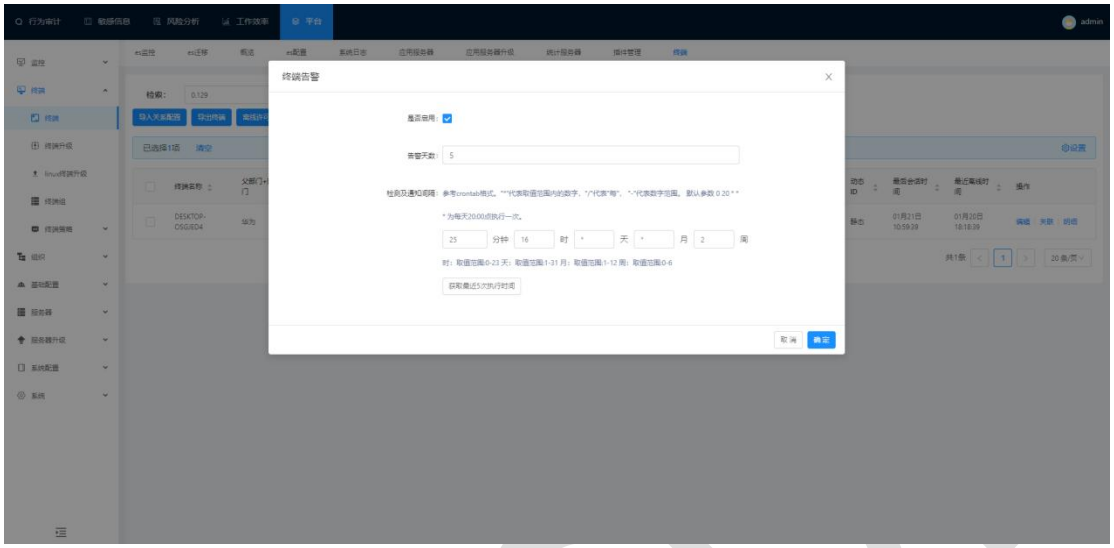


最近会话状态：点击最近会话状态，查看最近的会话相应详情；如下图所示：



2.18.8 告警配置

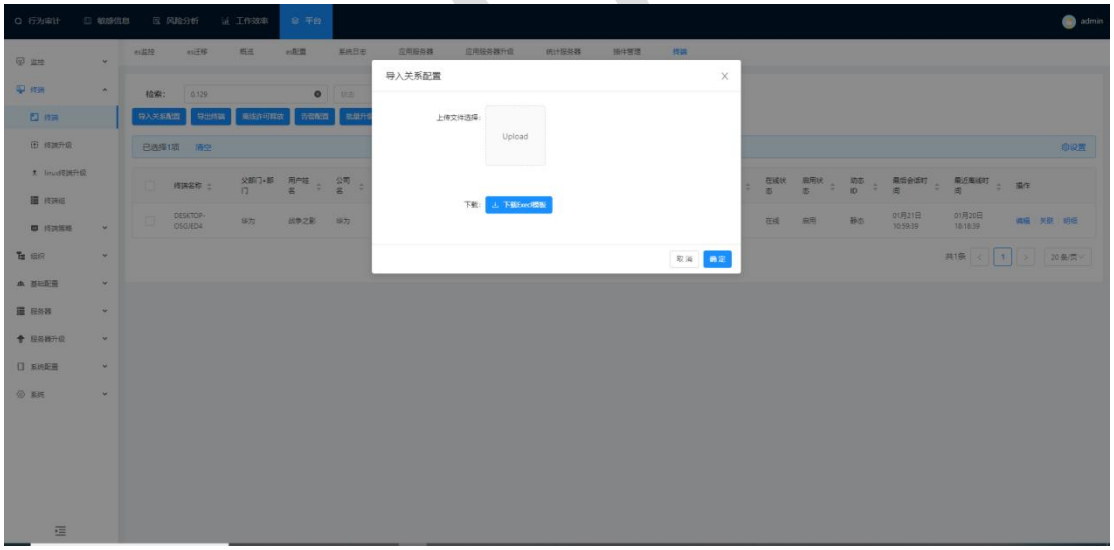
点击“告警配置”按钮，跳转至终端告警界面。如图：



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

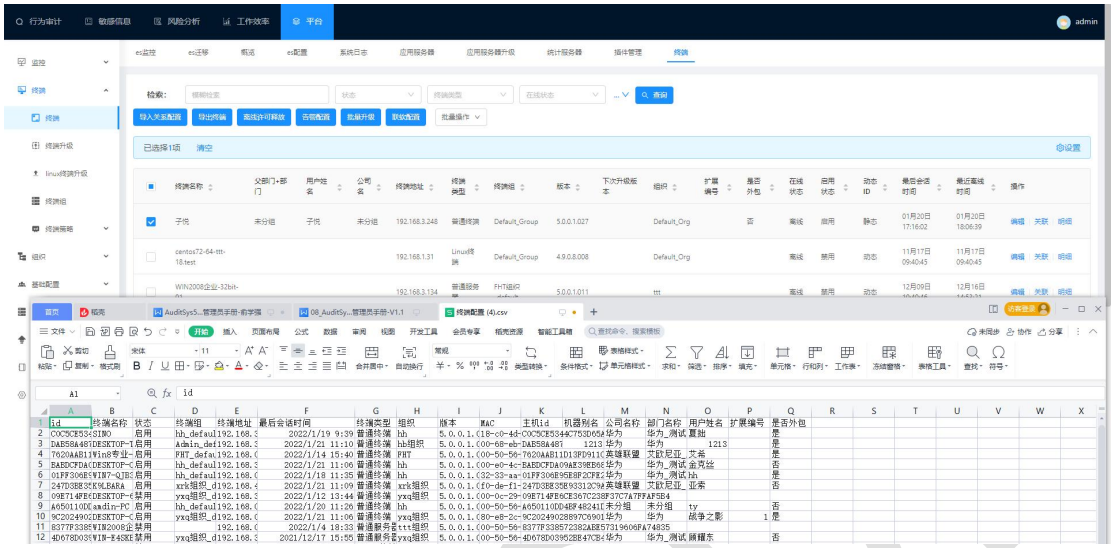
点击“导入关系配置”按钮，进入导入关系配置界面，如图：



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。

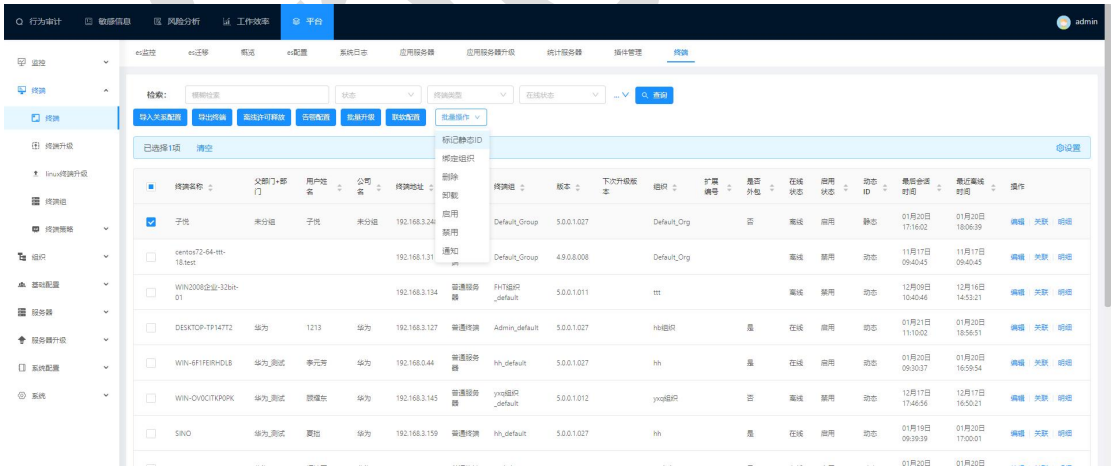
2.18.10 导出终端

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：



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：



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。

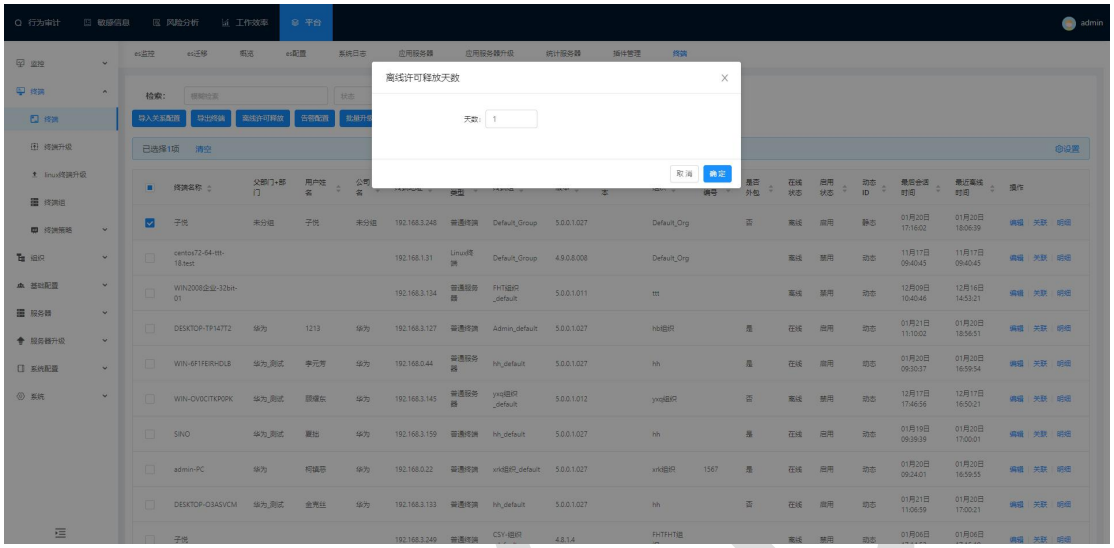
ID 类型为静态的终端，mac 地址和 cpuid 发生变化时，终端 id 不发生变化。

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。

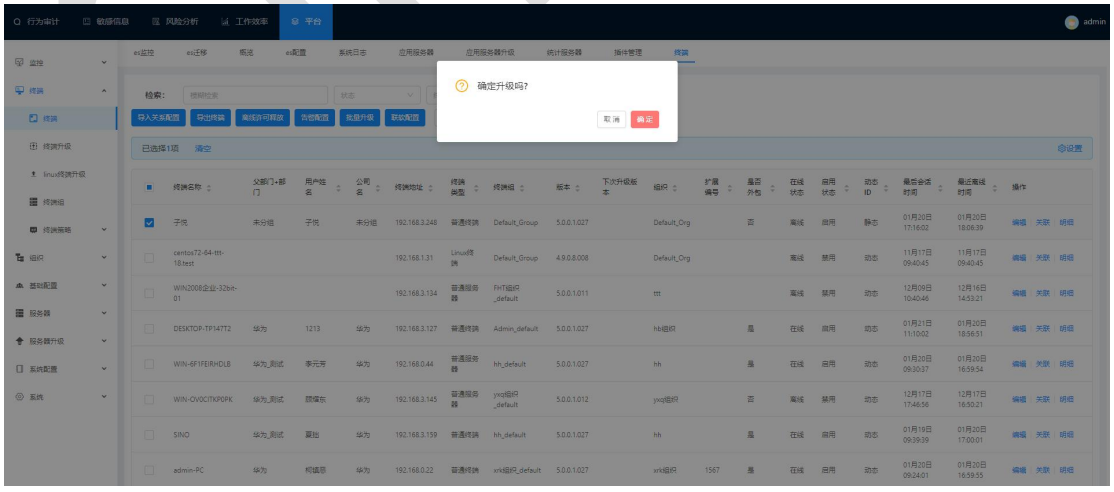
2.18.12 离线许可释放

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。



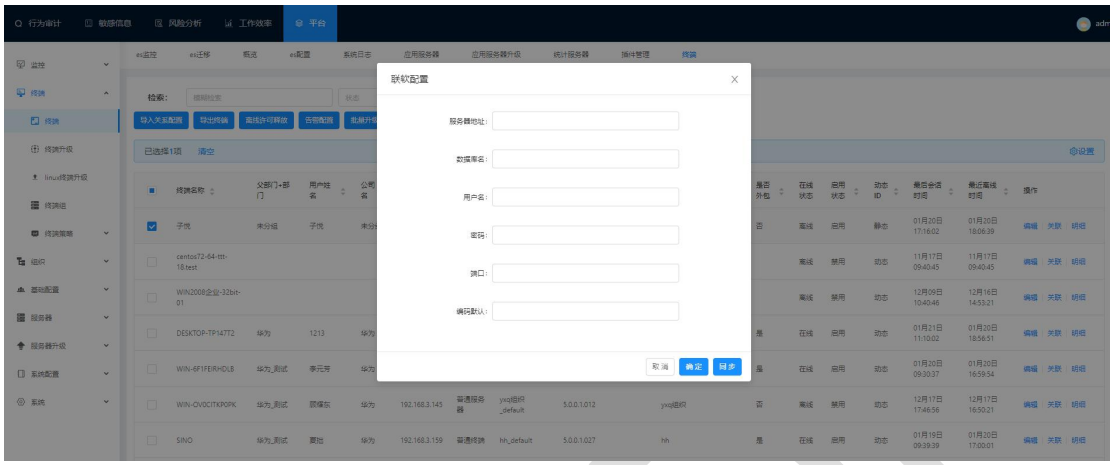
2.18.13 批量升级

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）



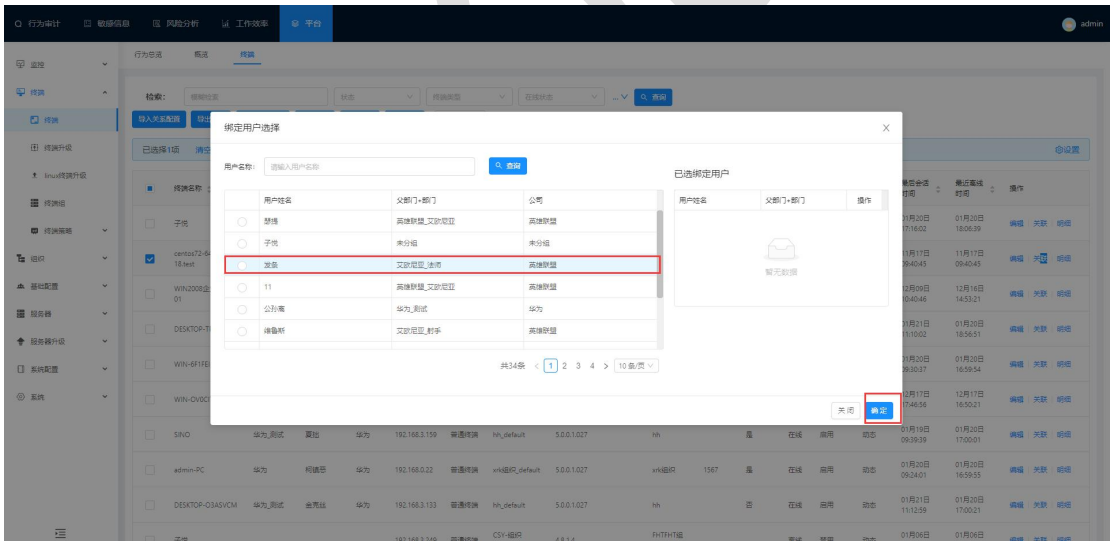
2.18.14 联软配置

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。



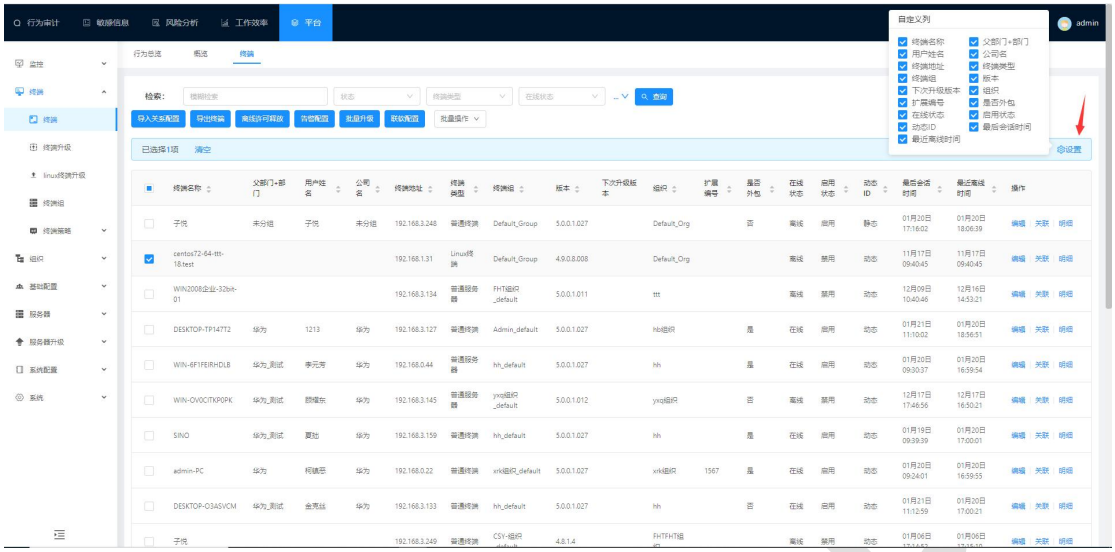
2.18.15 关联

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：



2.19 终端升级

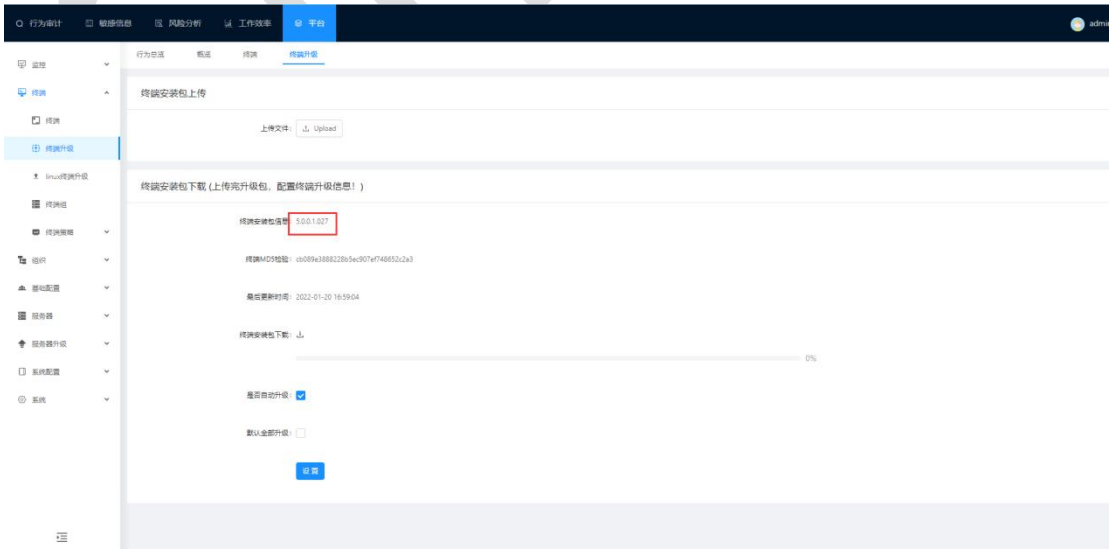
终端升级：对所有 Windows 终端的升级进行管理。

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：

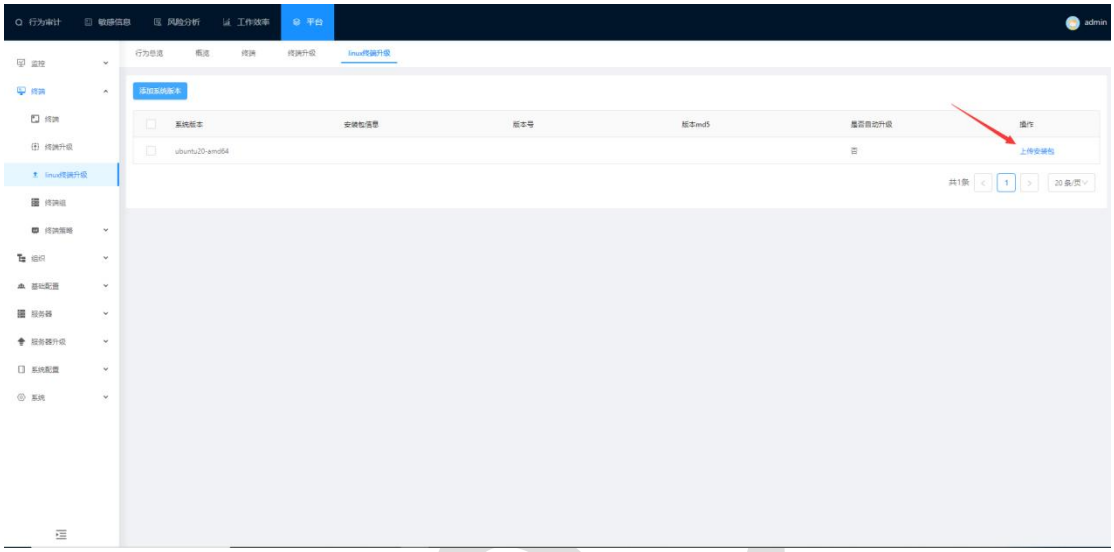


2.20 Linux 终端升级

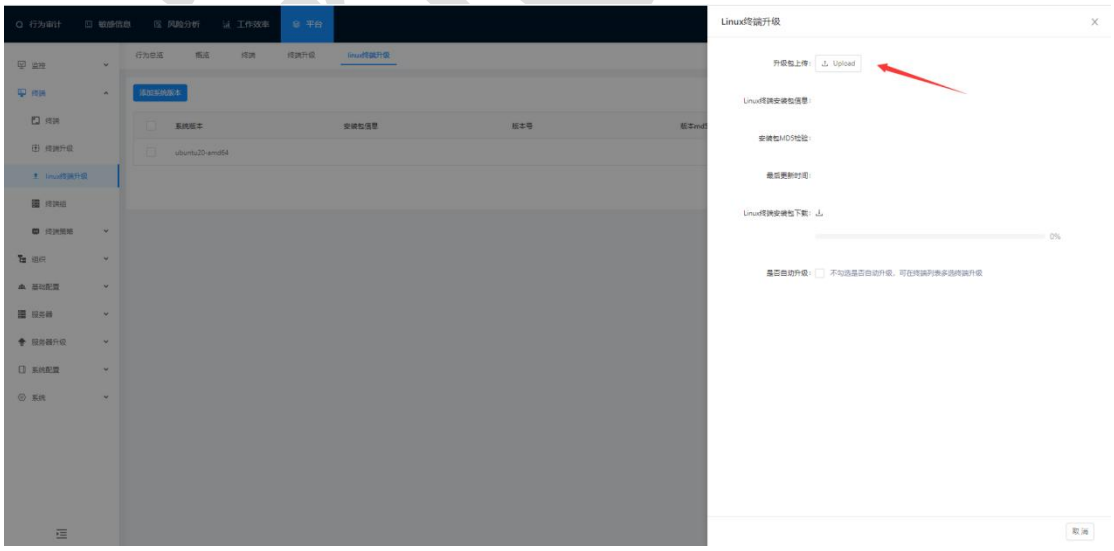
Linux 终端升级：对所有 Linux 终端的升级进行管理。

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：



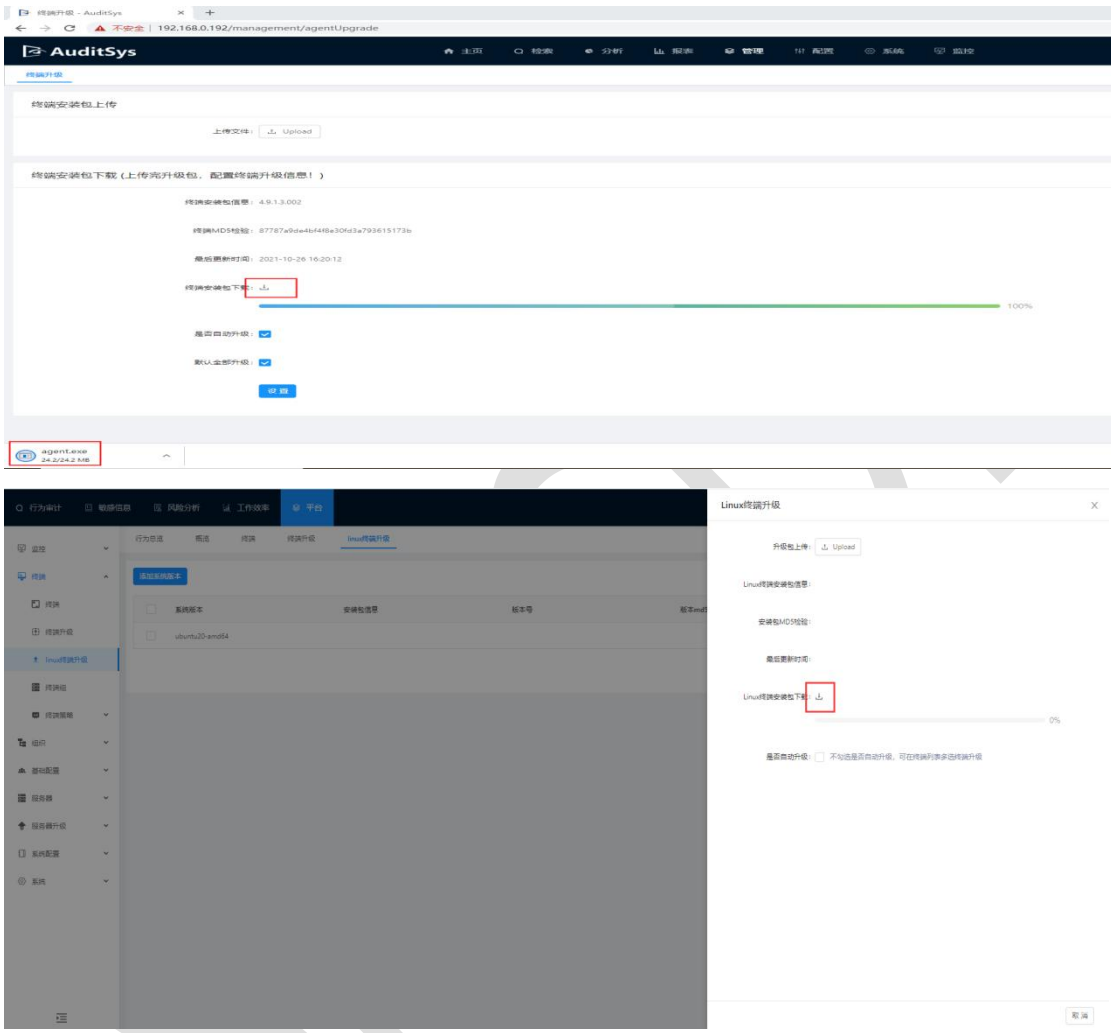
勾选是否自动升级，则对应的 Linux 系统版本的终端全部升级，不勾选是否自动升级，则需在“终端”模块，选择对应的 Linux 系统版本的终端，进行批量升级；如下图所示：



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：

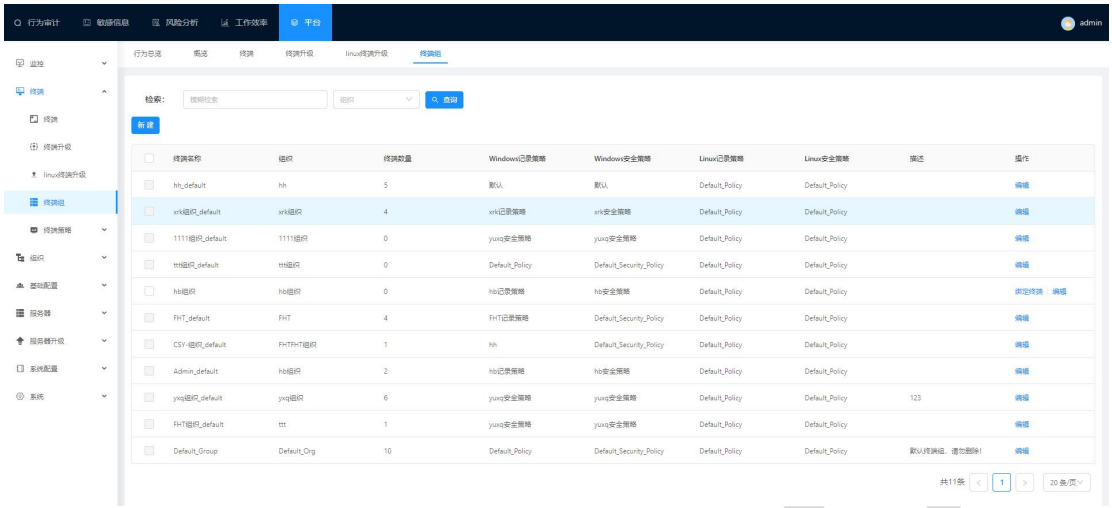


2.21 终端组

终端组：对终端的记录策略，安全策略进行管理。

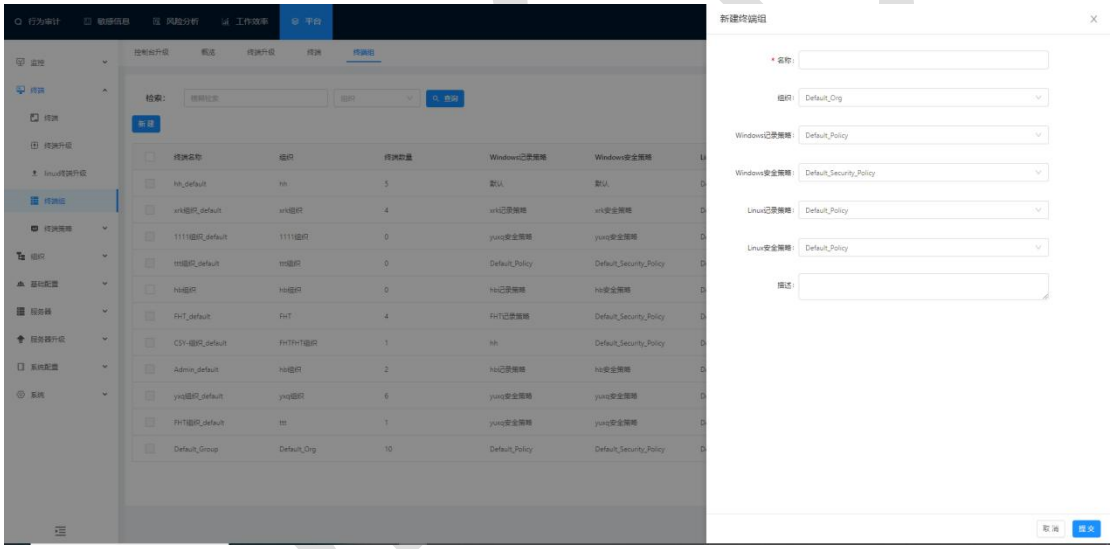
2.21.1 终端组列表

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：



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：



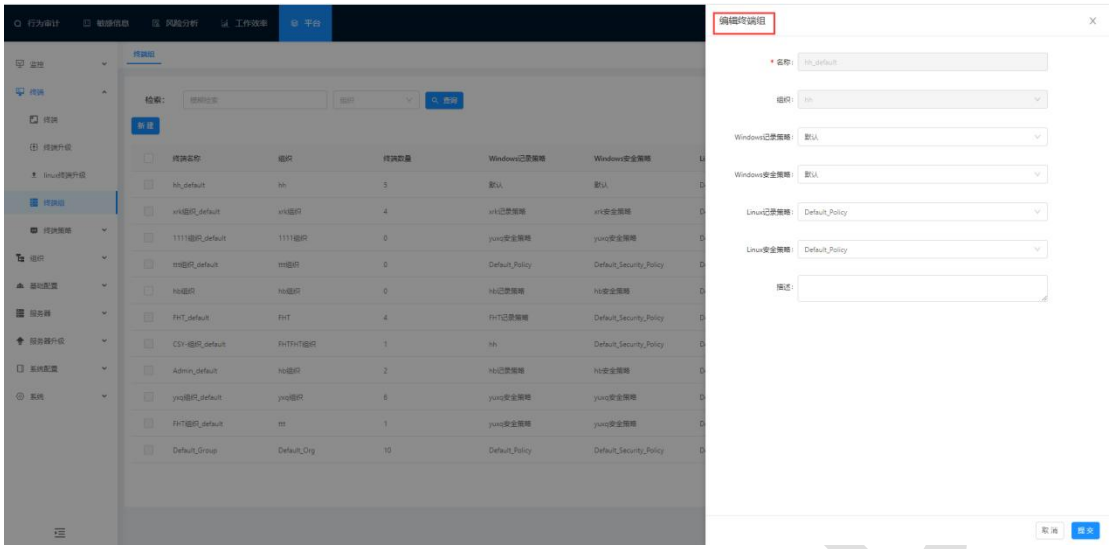
输入终端组名称，选择组织。点击“提交”按钮保存新建的终端组。

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。

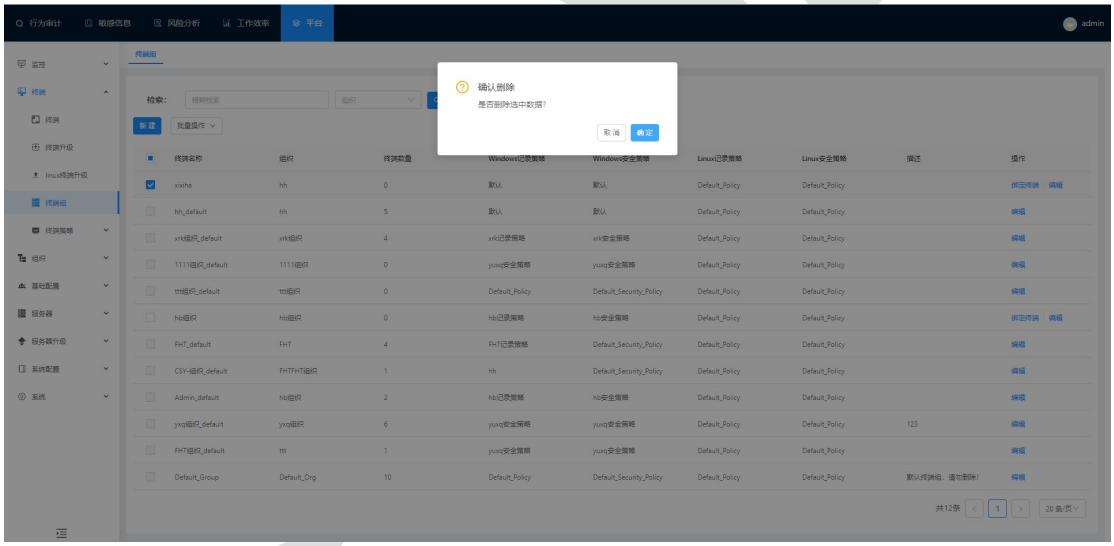
2.21.3 编辑终端组

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：



2.21.4 删除终端组

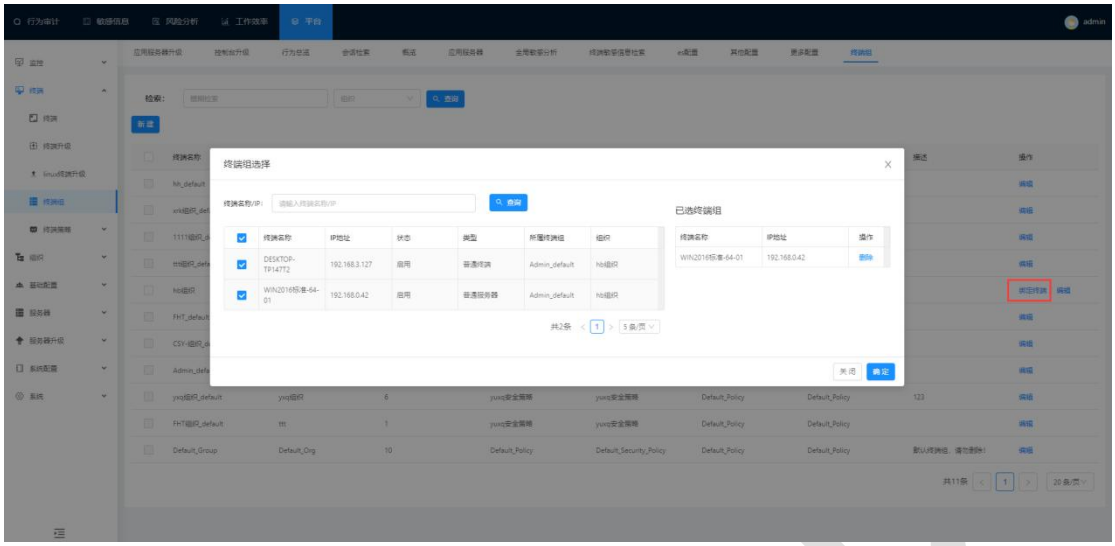
勾选需要删除的终端组，点击“删除”按钮删除终端组。自动生成的终端组不可手动删除，只能删除对应的组织才能被删除；如下图所示：



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：

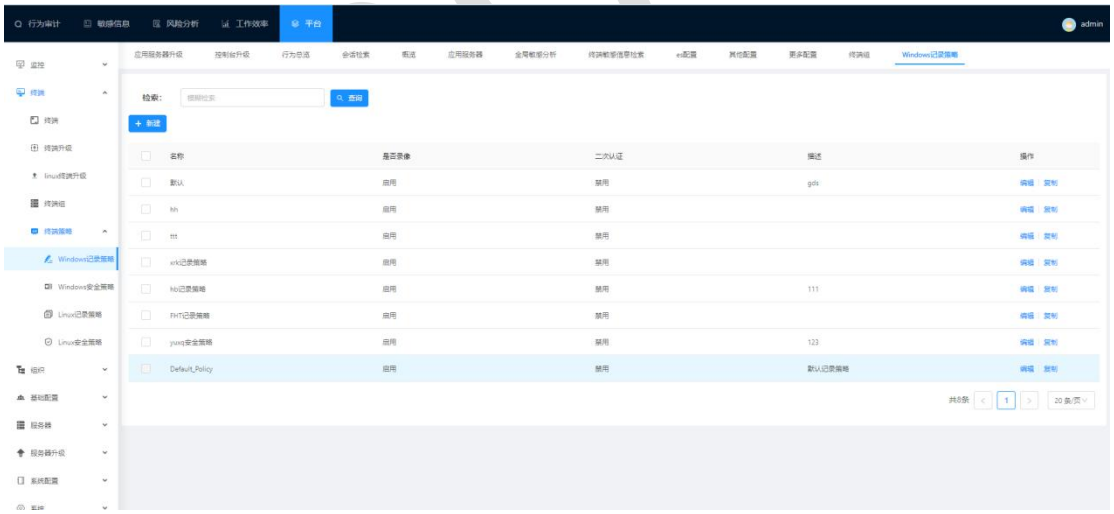


2.22Windows 记录策略

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：



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、world、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：

报文触发规则：

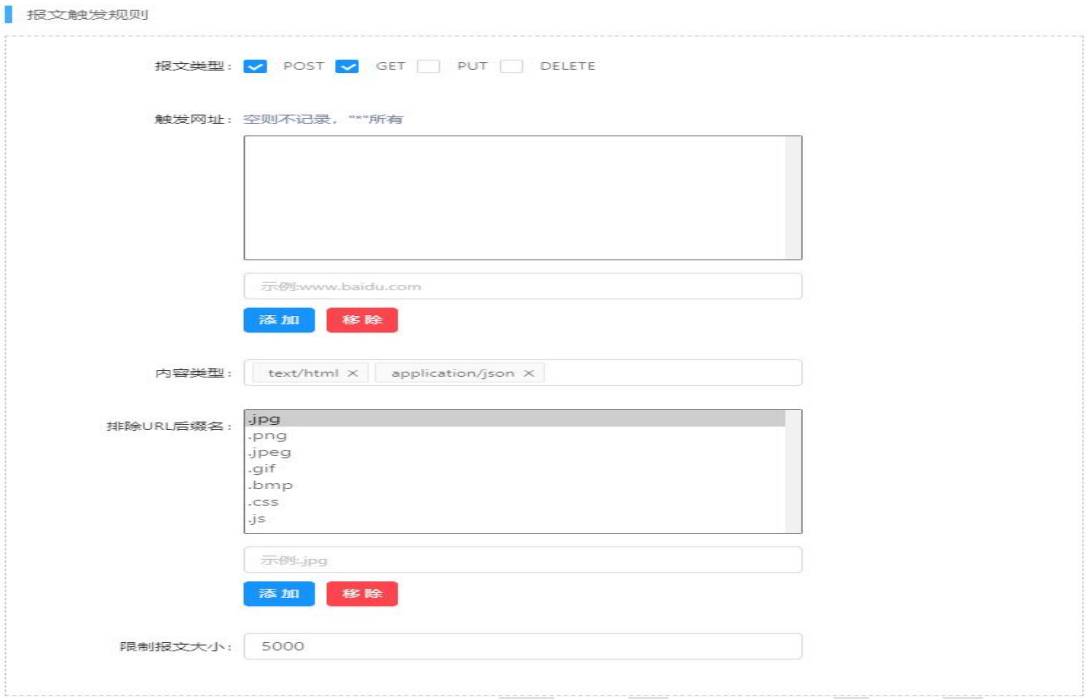
触发网址：填写需要触发 post 报文的网址。

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：



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。

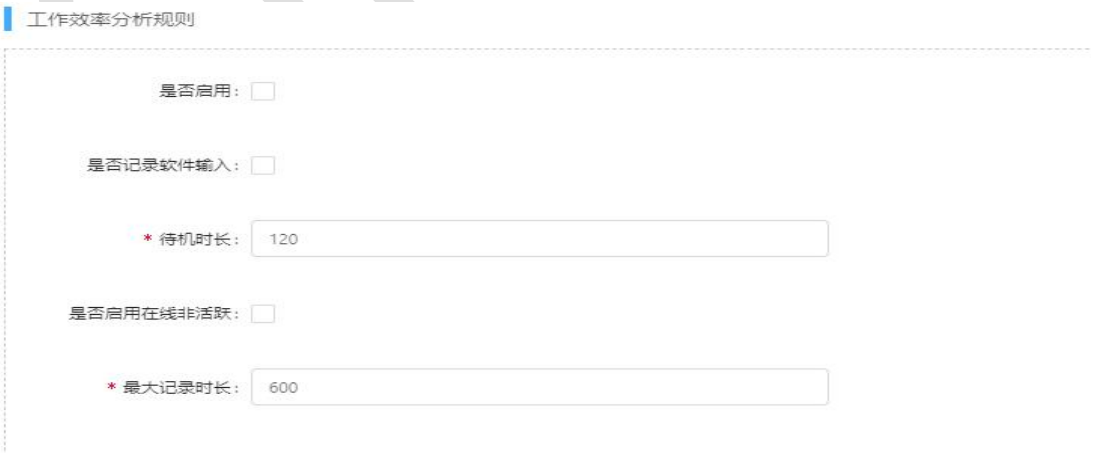
是否启用在线非活跃：勾选则效率明细的在线非活跃才会记录数据。

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：



录像触发规则：

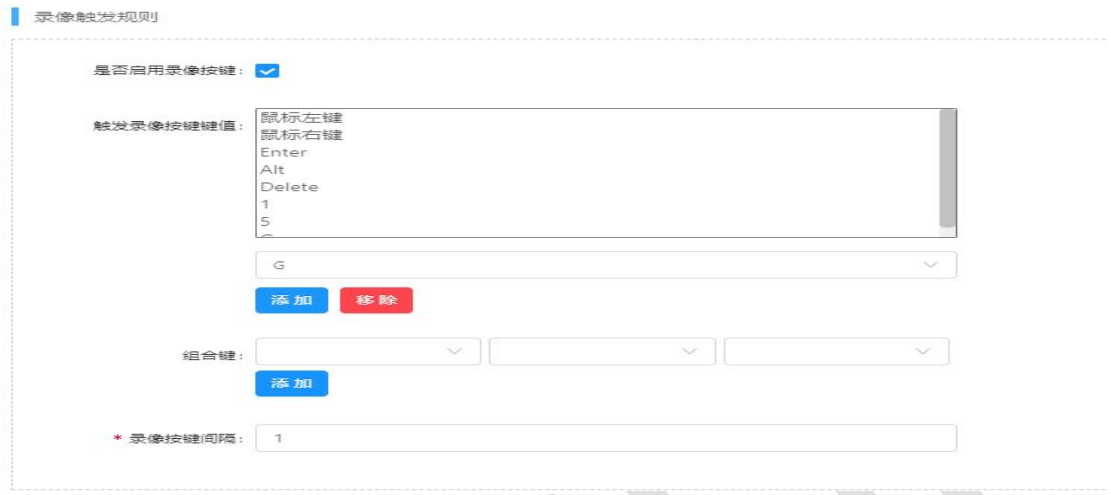
是否启用录像按键：勾选则配置的按键键值操作才会录像。

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：



文件上传：

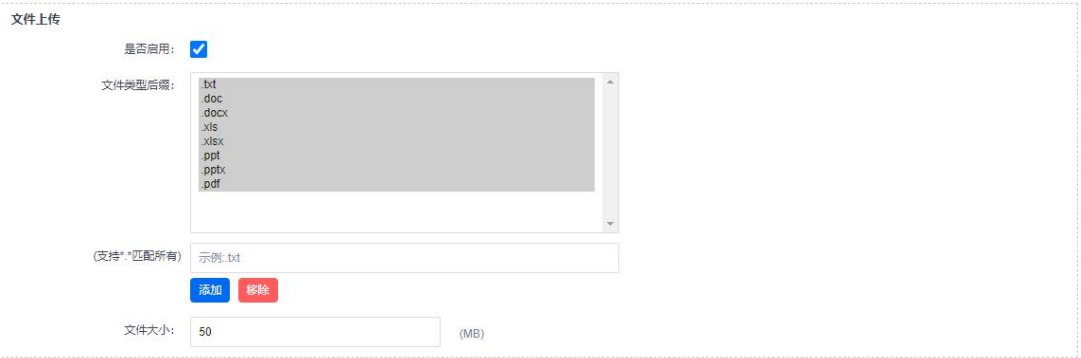
是否启用：勾选则配置的文件类型后缀规则才会生效。

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：



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）。

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。

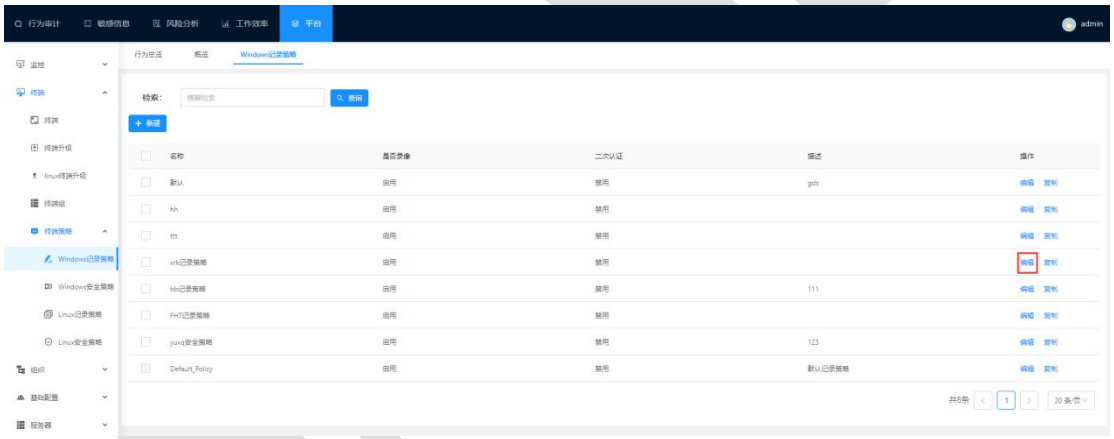
用户记录规则：

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。

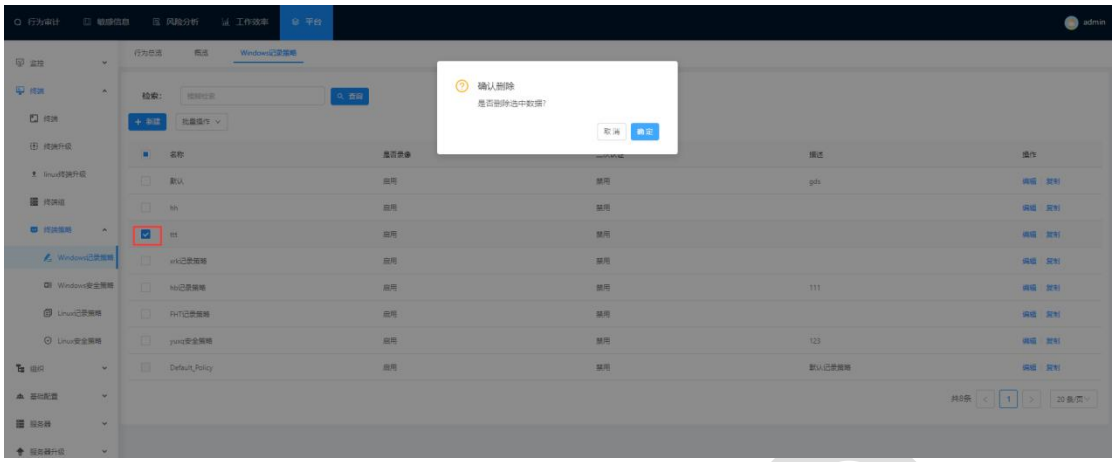
2.22.2 编辑 Windows 记录策略

点击“编辑”按钮进行编辑 Windows 记录策略。如下图所示：



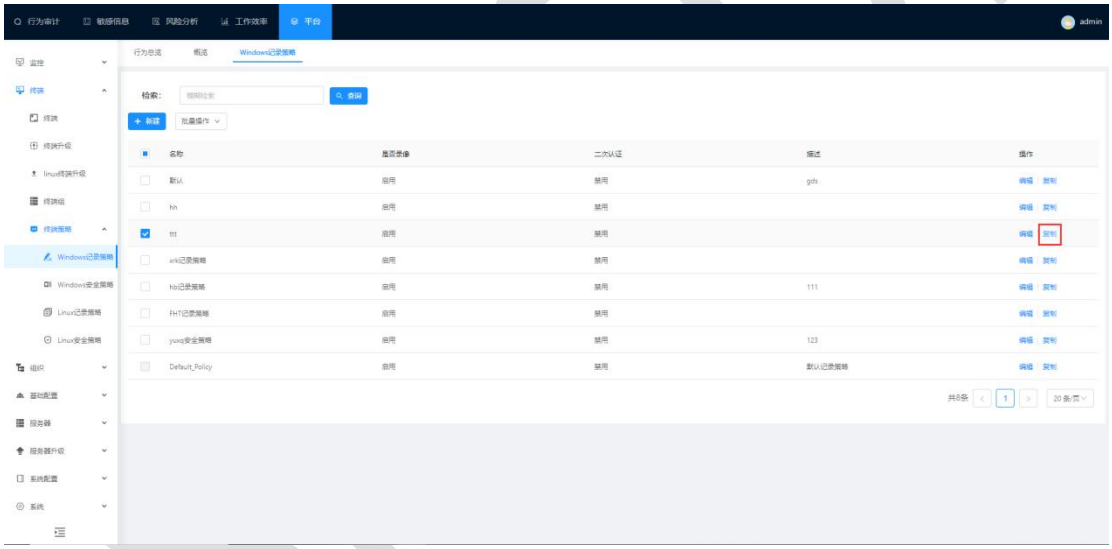
2.22.3 删除 Windows 记录策略

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：



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。

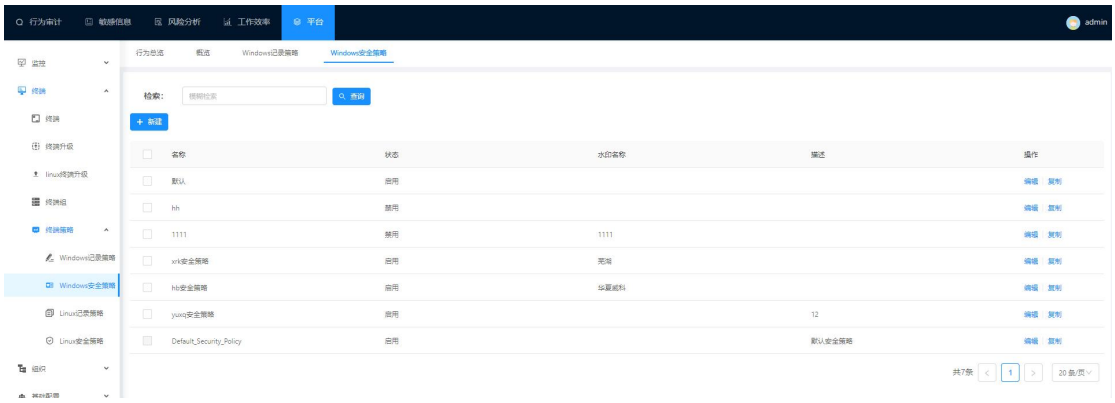


2.23Windows 安全策略

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：



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）。

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。

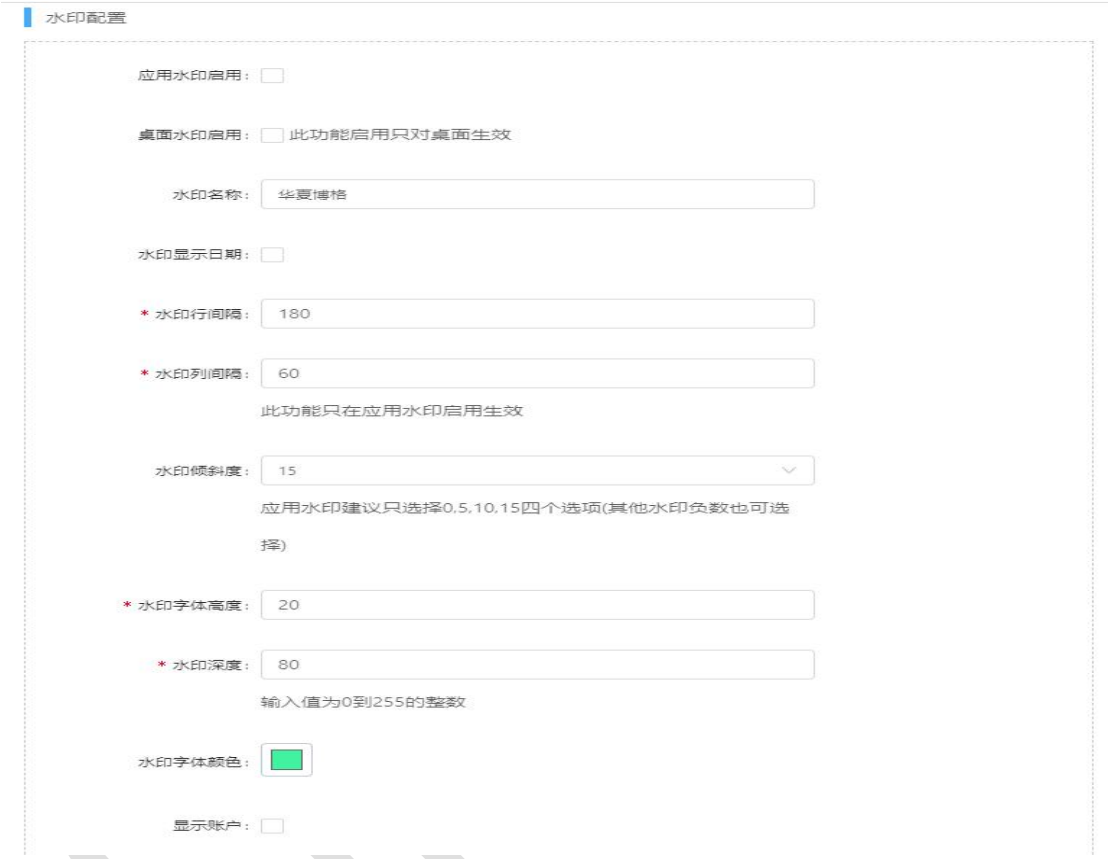
水印字体高度：水印的字体大小。

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。

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。

非法应用程序：

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。

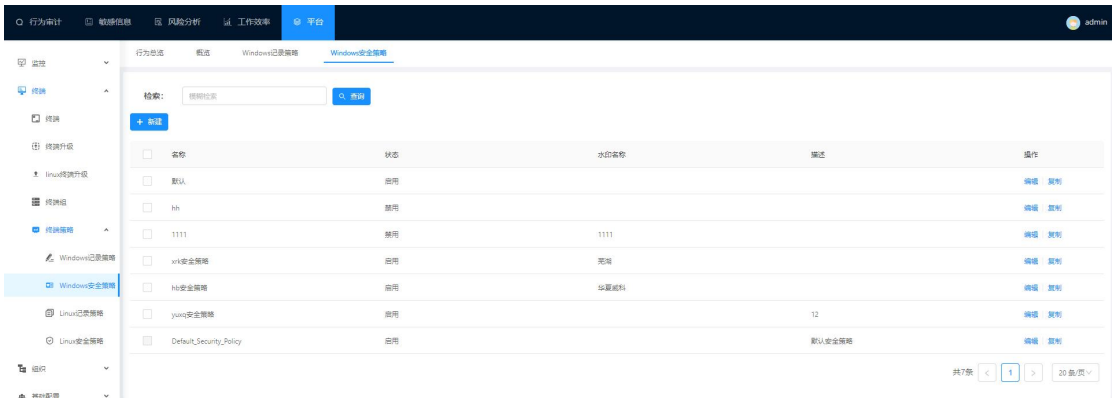
网站列表：可添加可移除需要被阻断的非法网站。

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：

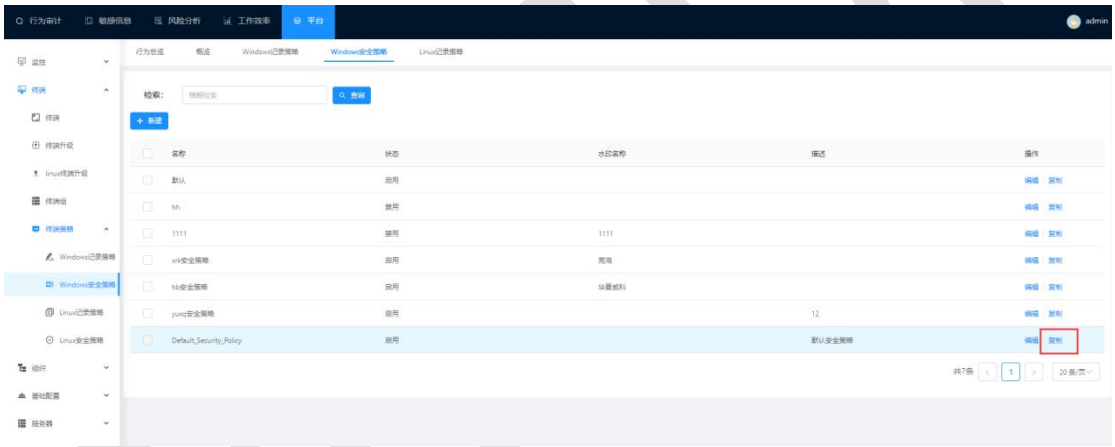
2.23.4 删除 Windows 安全策略

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：



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。



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。

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。

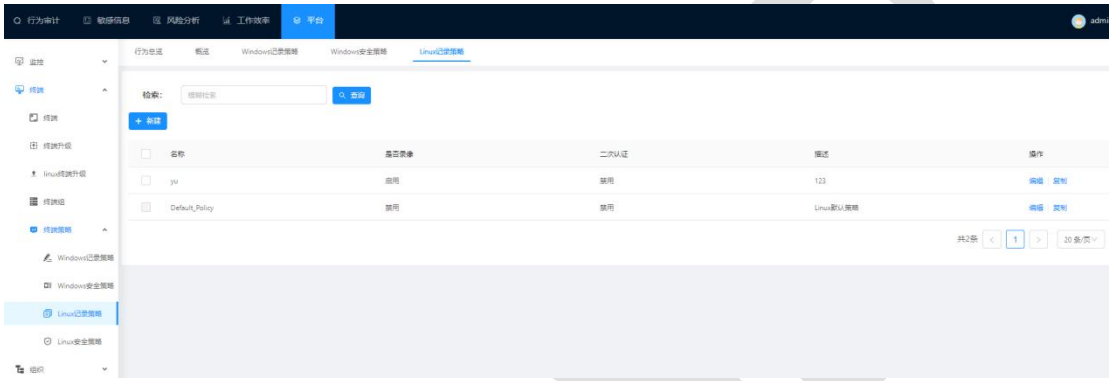
2.25 Linux 安全策略

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：



2.25.2 新建 Linux 安全策略

点击“新建”按钮创建 Linux 安全策略。

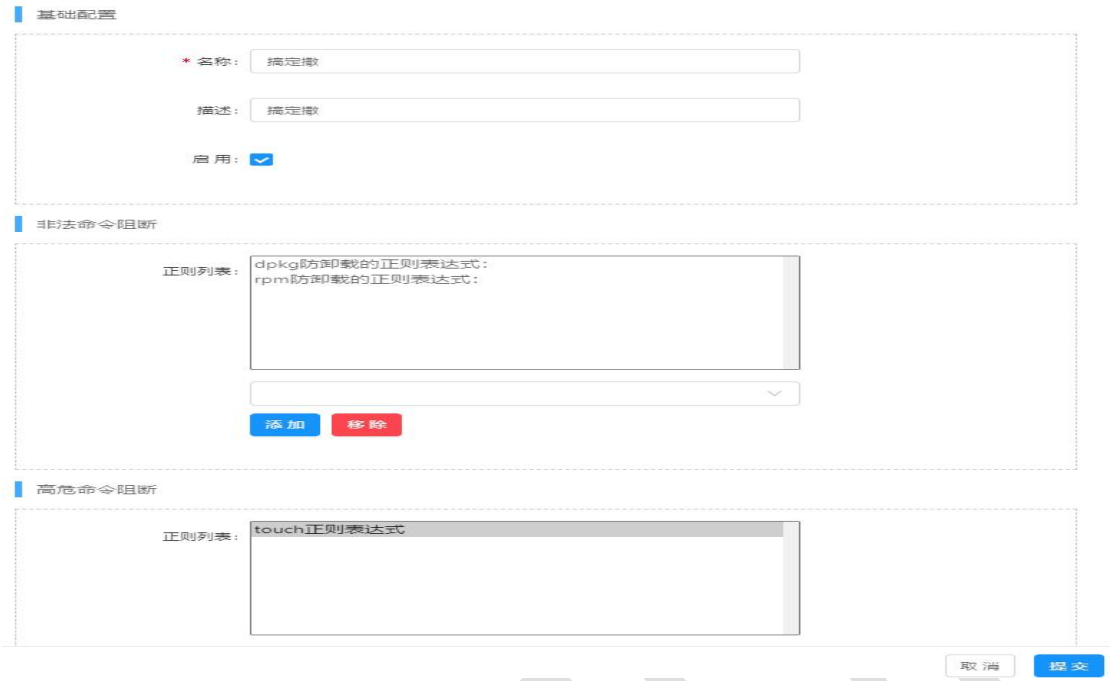
基础配置：

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》。



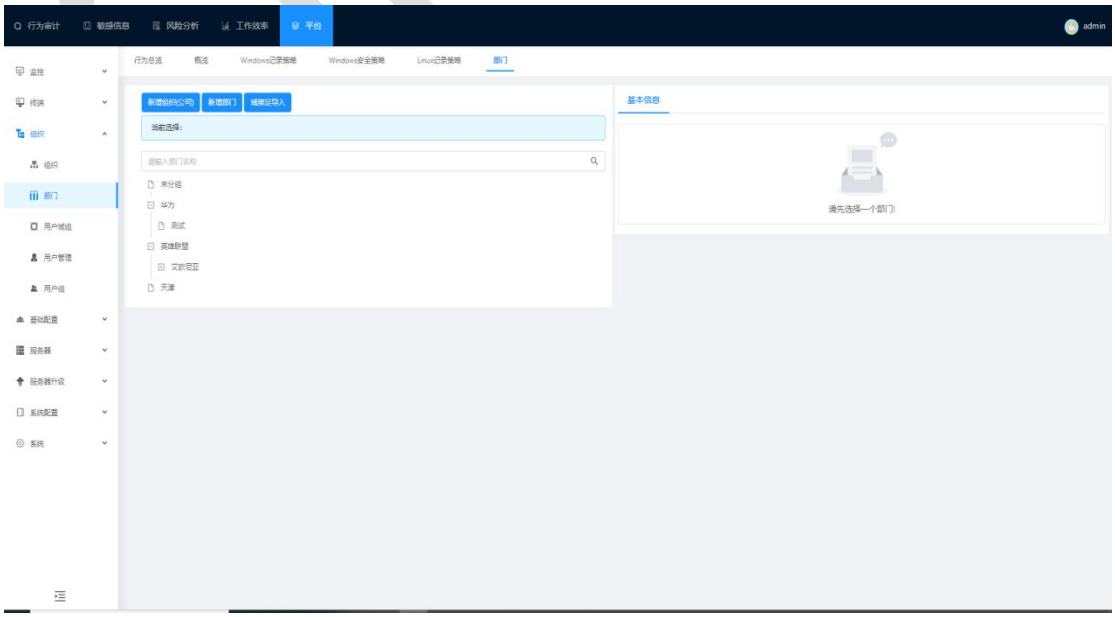
2.25.3 复制 Linux 安全策略

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

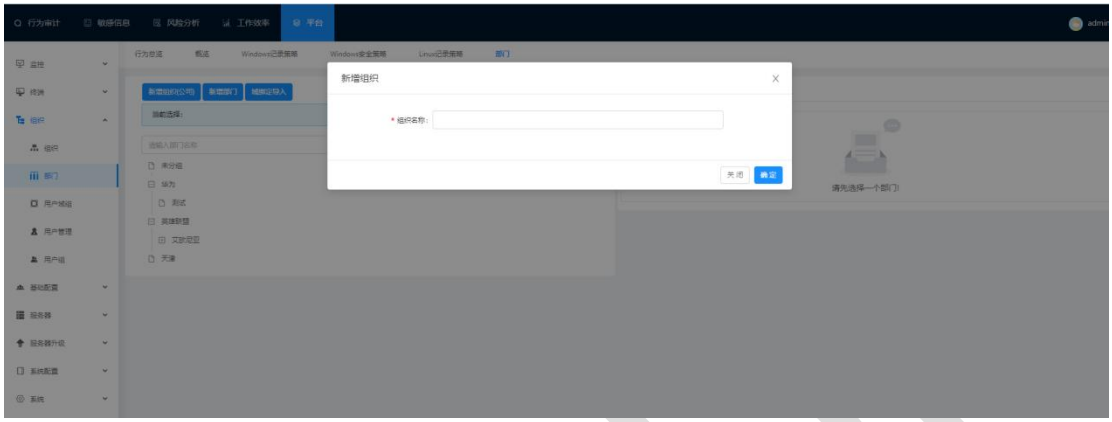
部门是对终端进行部门分类管理。

选择“平台>组织>部门”进入部门界面；如下图所示：

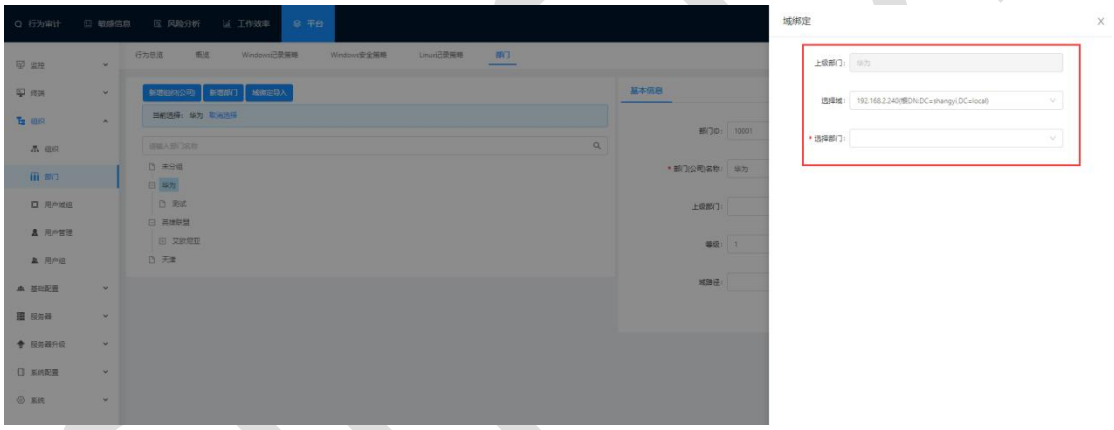


2.26.1 新建部门

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：

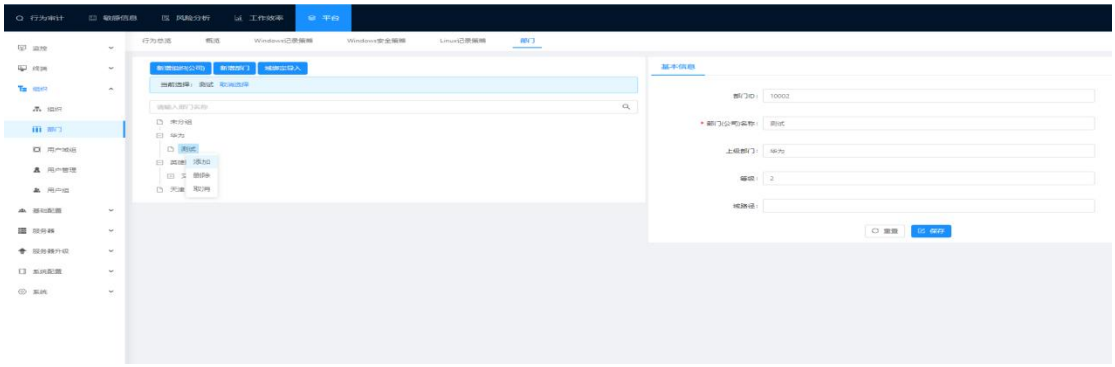


域绑定导入是导入域部门，需先配置域配置（详见步骤 2.7 域配置）；如下图所示：



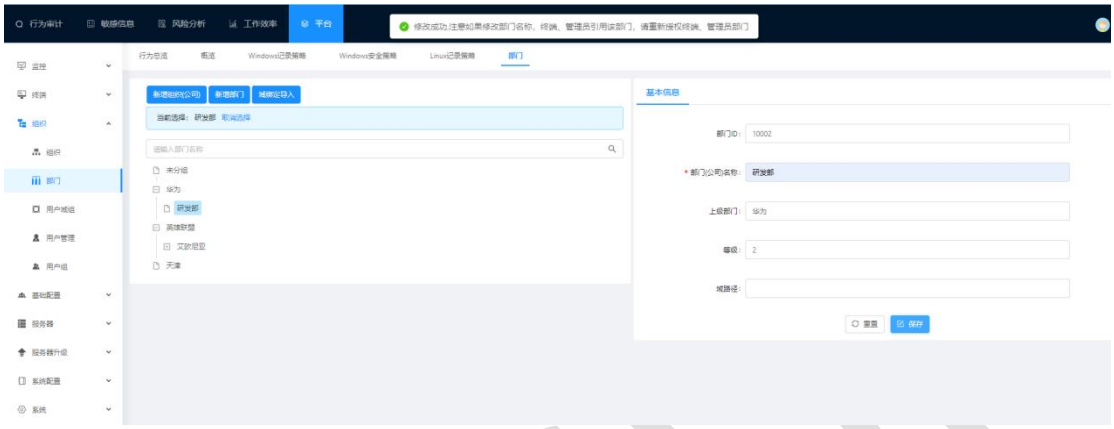
2.26.2 删除部门

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

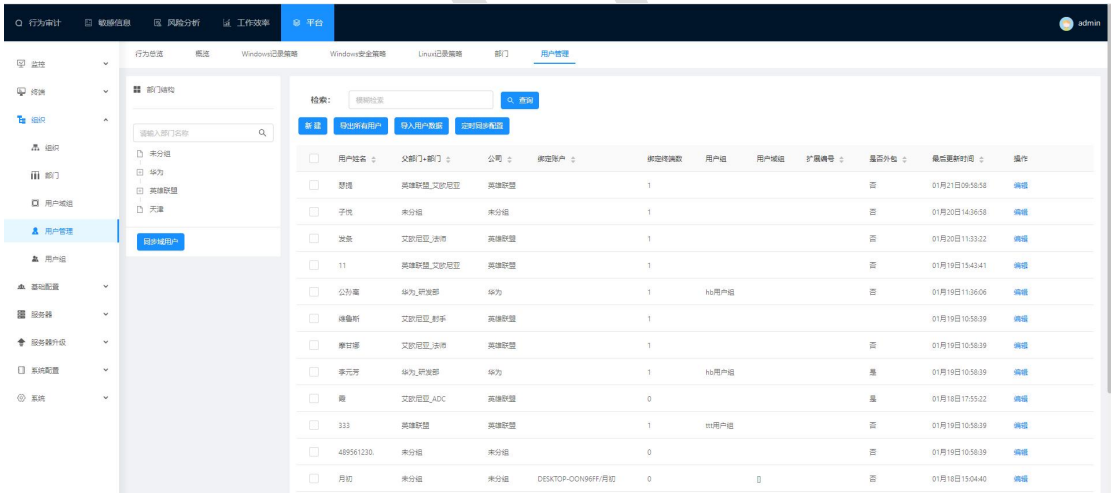
选择要编辑的部门，点击部门名称，在右侧进行编辑；编辑成功会弹出相应提示；如图下所示：



2.27 用户管理

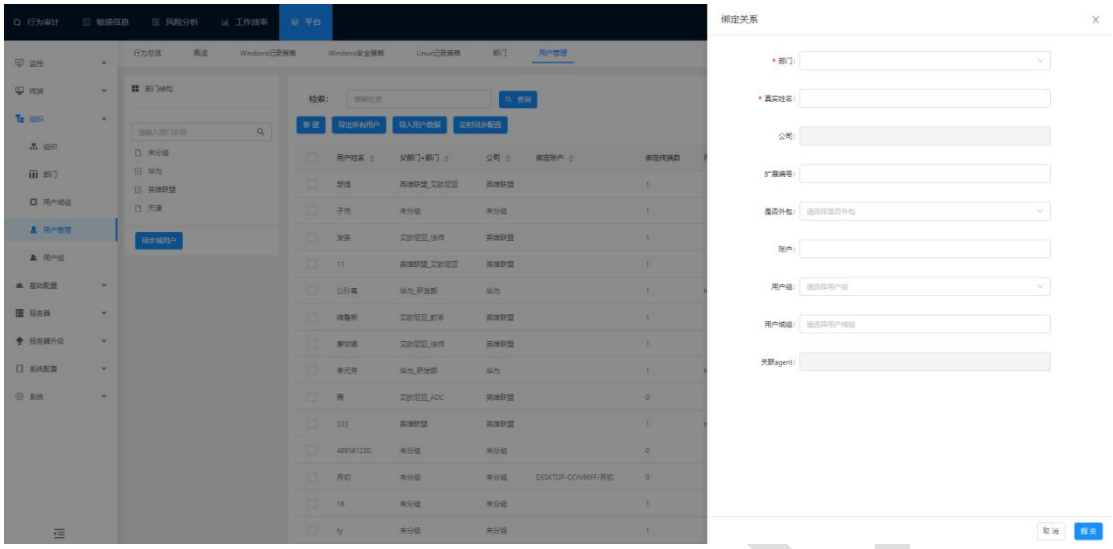
用户管理是给终端关联用户信息。

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）

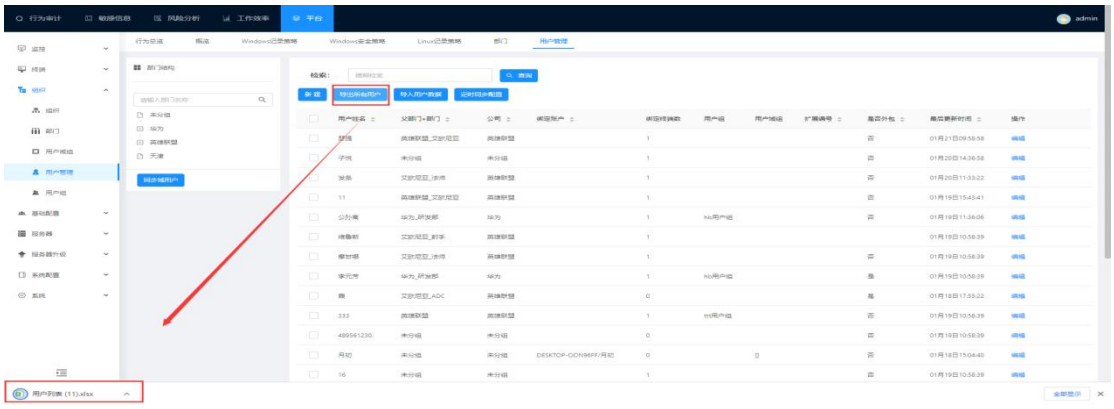
用户域组：选择要绑定的用户域组。

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。

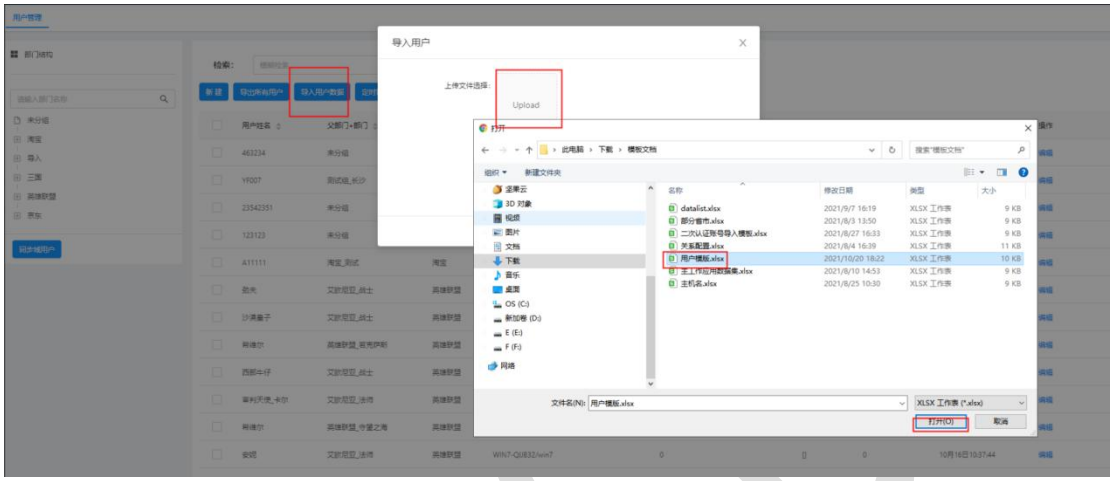
点击“导出所有用户”按钮，导出用户信息；如下图所示：



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

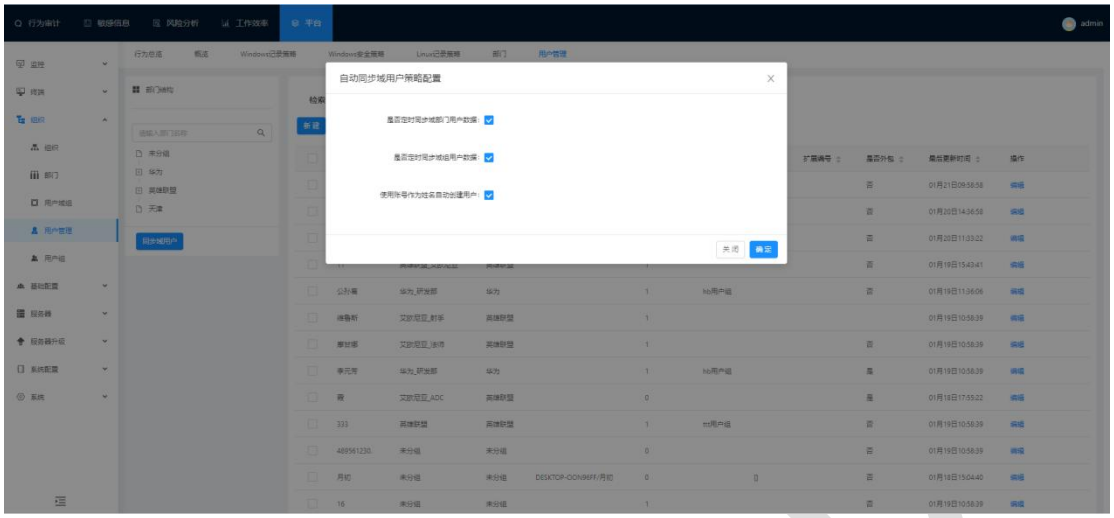
定时同步配置：

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。

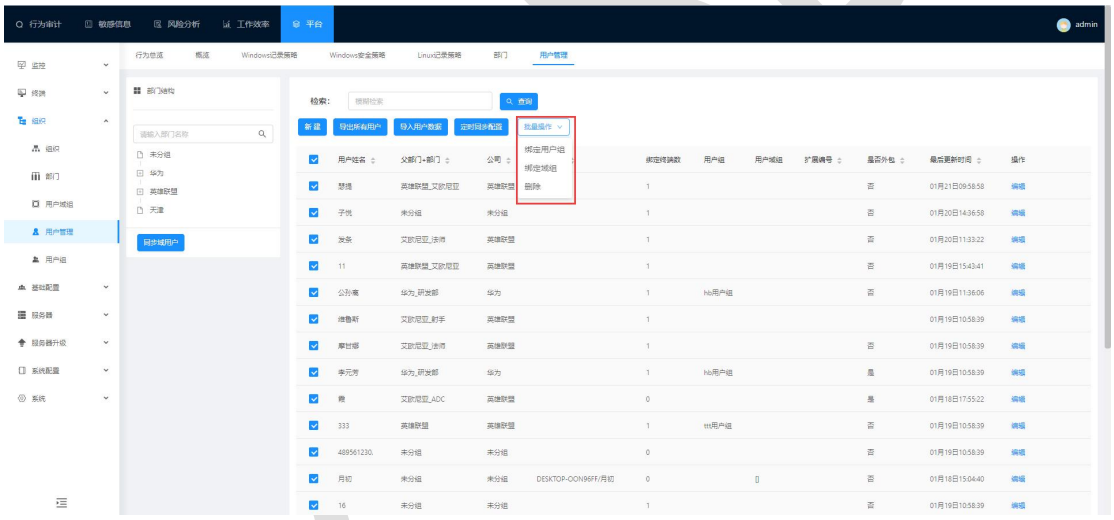
点击“定时同步配置”按钮；弹出定时同步配置窗口；如下图所示：



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。

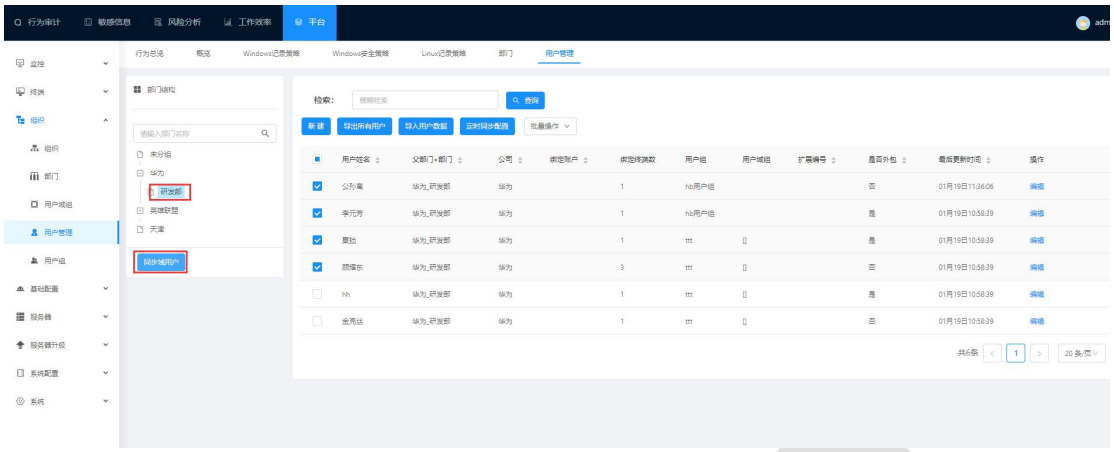
选择要批量操作的用户进行批量操作；如下图所示：



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。

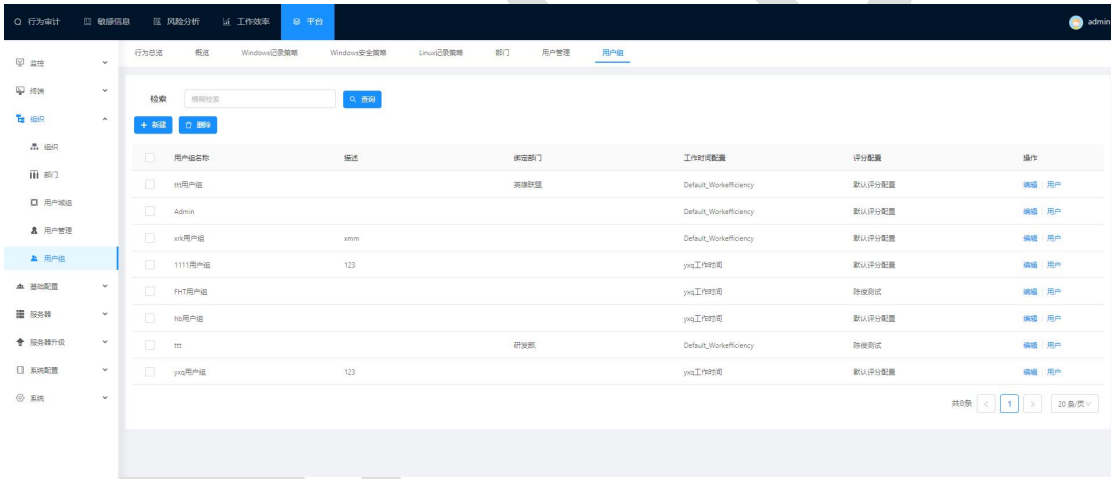
选择域部门，点击“同步域用户”按钮进行同步（选择普通部门，点击同步域用户不生效）如下图所示：



2.28 用户组

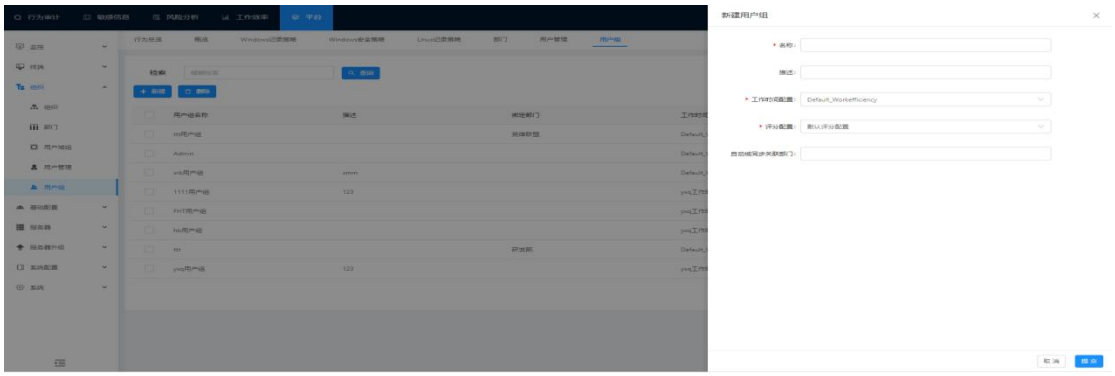
用户组：把风险规则、敏感词规则、时间配置、评分配置、效率分类、用户信息绑定到用户组；只有在此用户组下的用户在终端操作才能触发相应的规则、配置。

选择“平台>组织>用户组”进入用户组界面；如下图所示：



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。

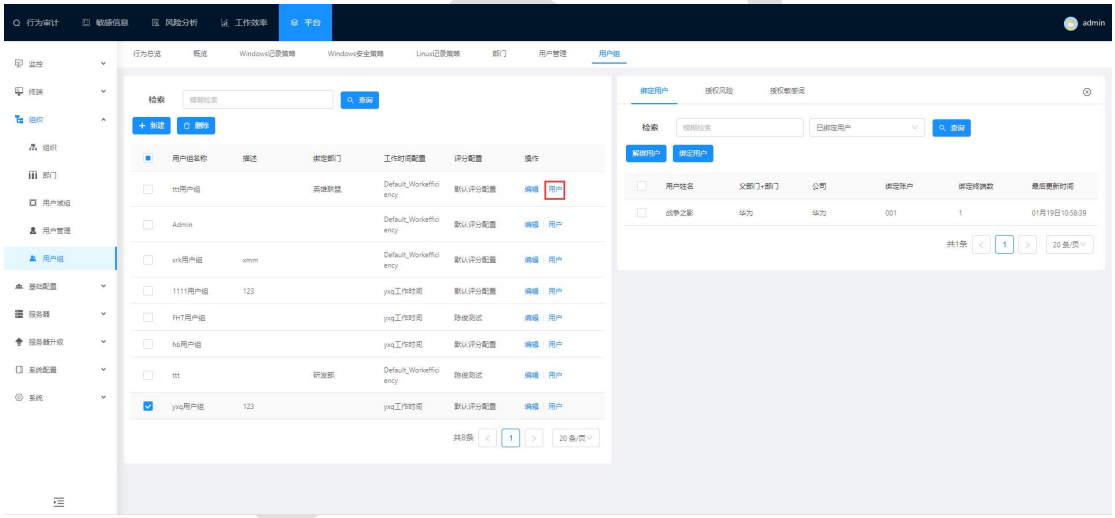
工作时间配置：选择相应的工时时间配置；默认是选择默认的工作时间配置。

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。

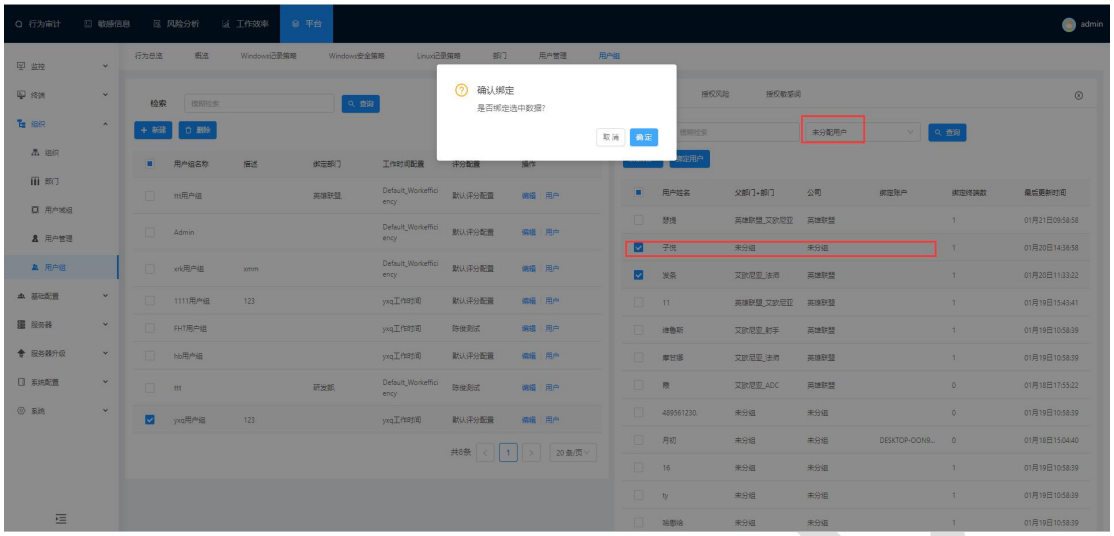
自动域同步关联部门：选择域部门，在用户管理界面点击同步域用户；才能自动把域部门下的域用户全部绑定到此用户组。

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：



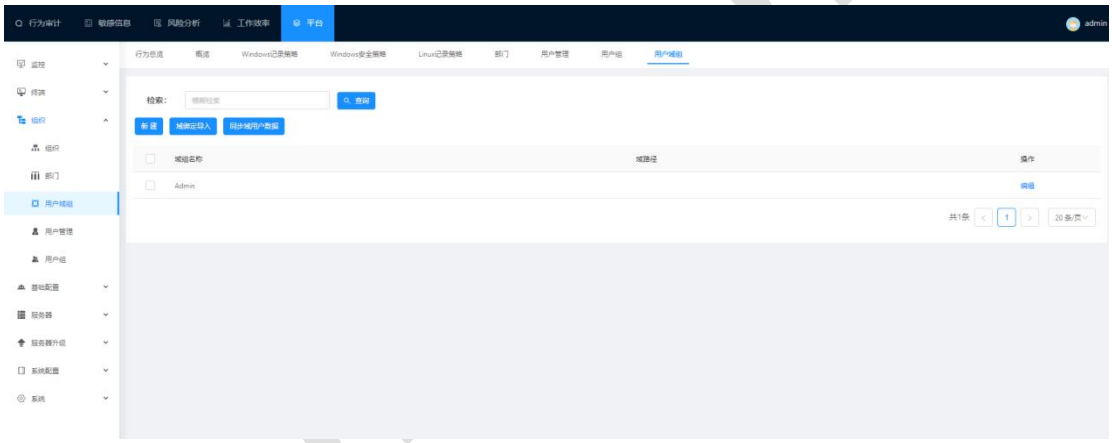
例如：绑定用户：先查询未分配用户信息；再选择用户信息；点击“绑定用户”按钮进行绑定；（授权风险和授权敏感词借鉴此操作步骤）所下图所示：



2.29 用户域组

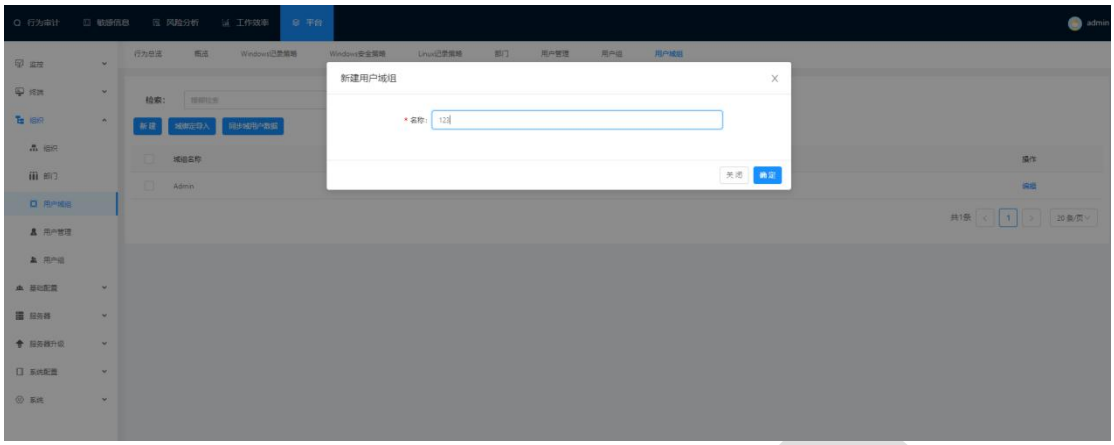
用户域组：对域组下的用户进行管理。

选择“平台>组织>用户域组”进入用户域组界面；如下图所示：

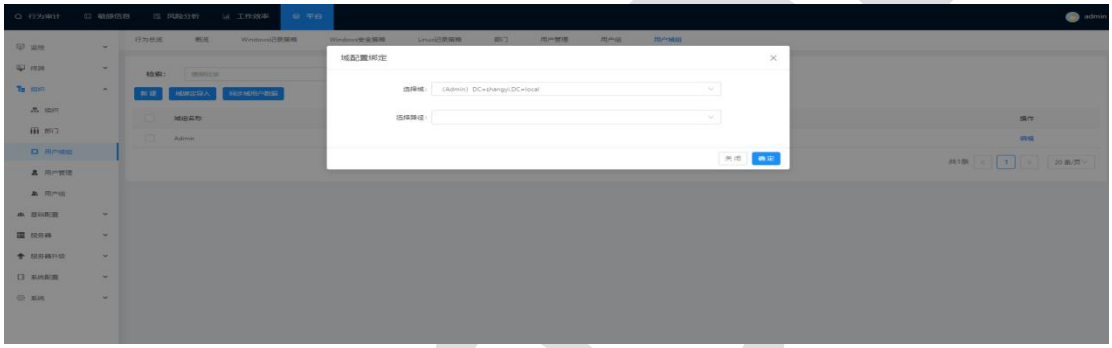


2.29.1 新建或导入域组

点击“新建”按钮；可以新建域组；如下图所示：

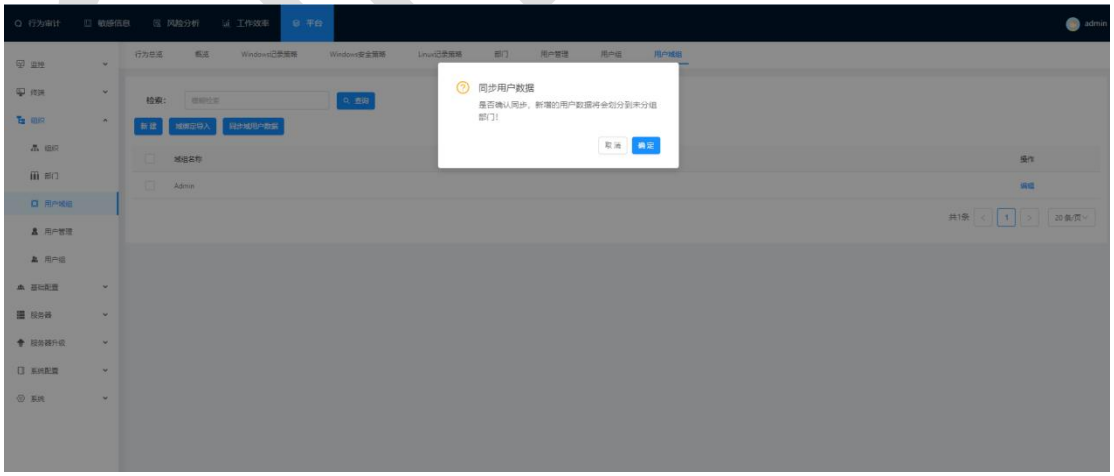


点击“域绑定导入”可以导入用户域组（需先配置域配置；详见域配置步骤 2.6）如下图所示：



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：

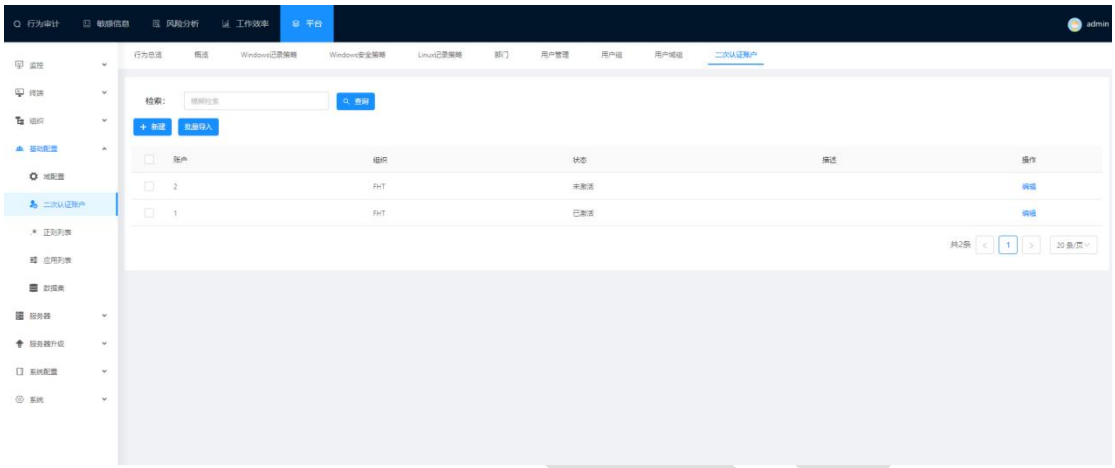


2.30 二次认证用户

二次认证用户：是配置终端二次登录的用户信息。

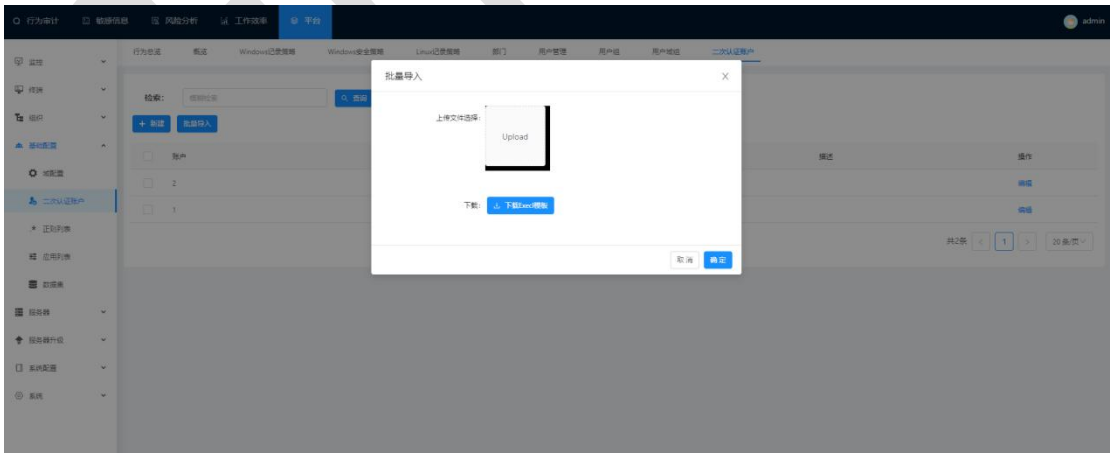
提示：开启二次认证需在 Windows 记录策略勾选是否启用二次认证规则；二次认证用户登录终端操作的行为数据都会审计在此二次认证用户下。

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

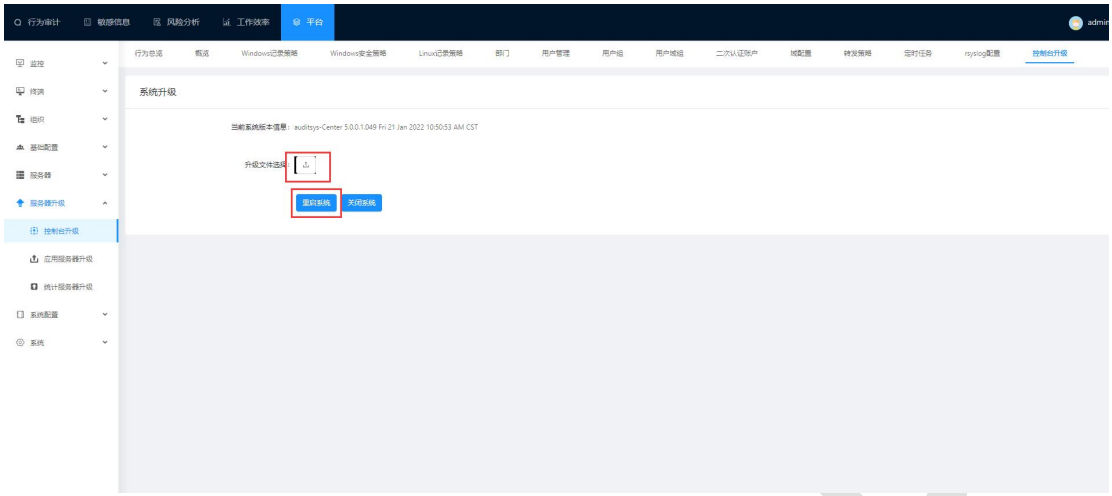
点击“新建”按钮进行新建二次认证用户（需要增加多个二次认证用户，可以选择批量导入）如下图所示：



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

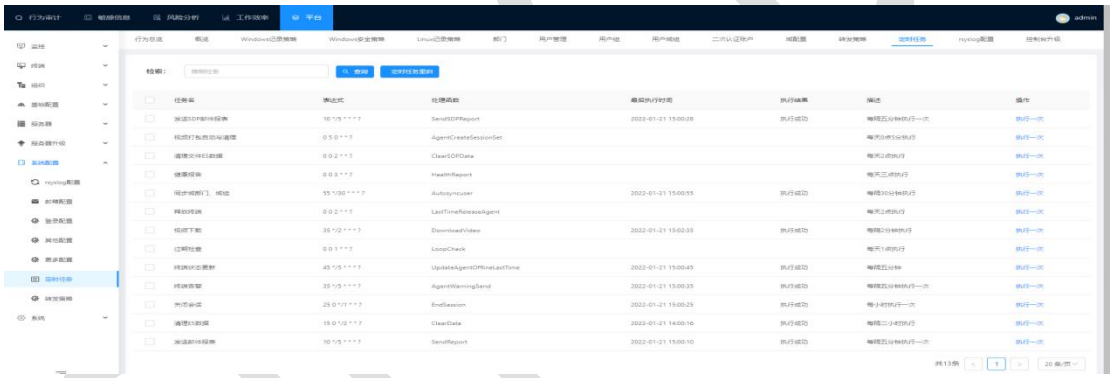
即可。



2.32 定时任务

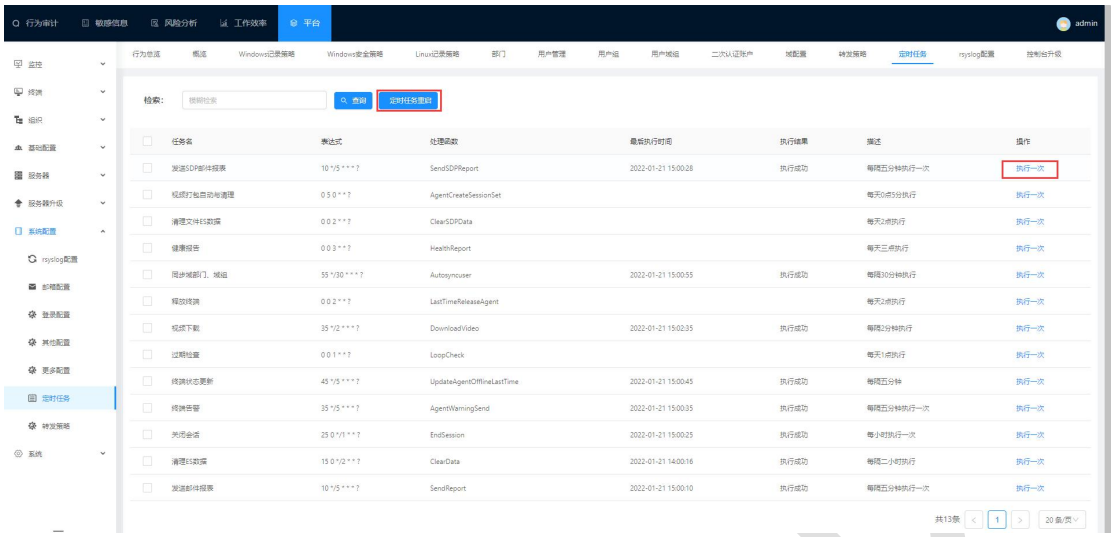
2.32.1 定时任务列表

定时任务列表展示所有定时器任务详情。



2.31.1 定时任务启动

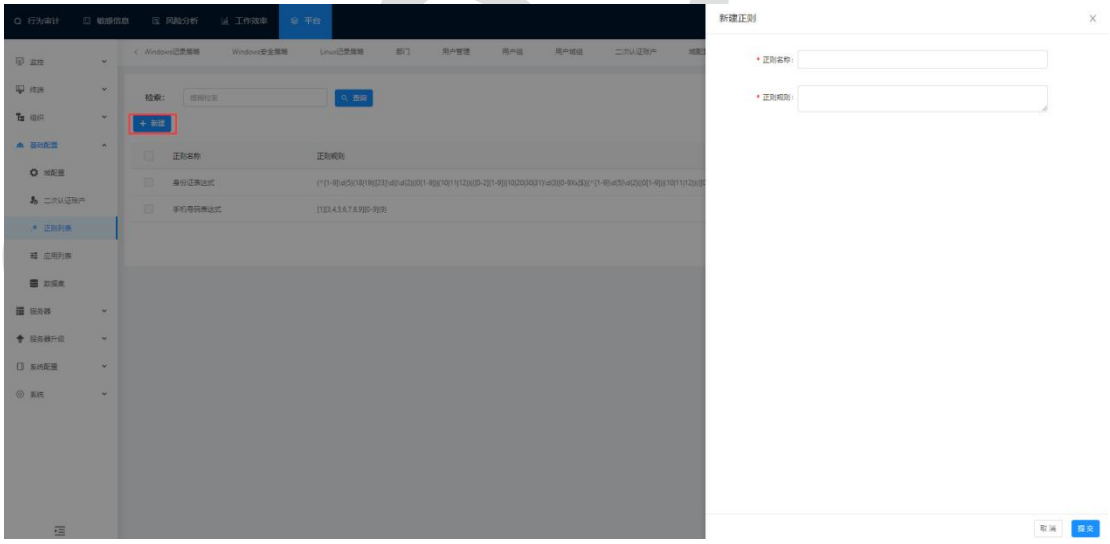
定时任务手动启动/定时任务重启。



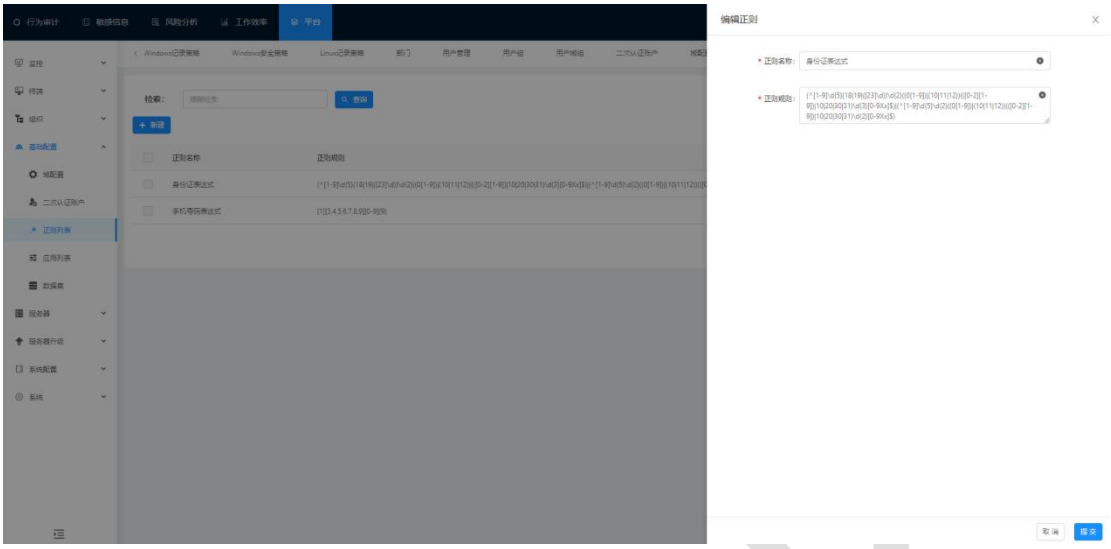
2.32 正则列表

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。



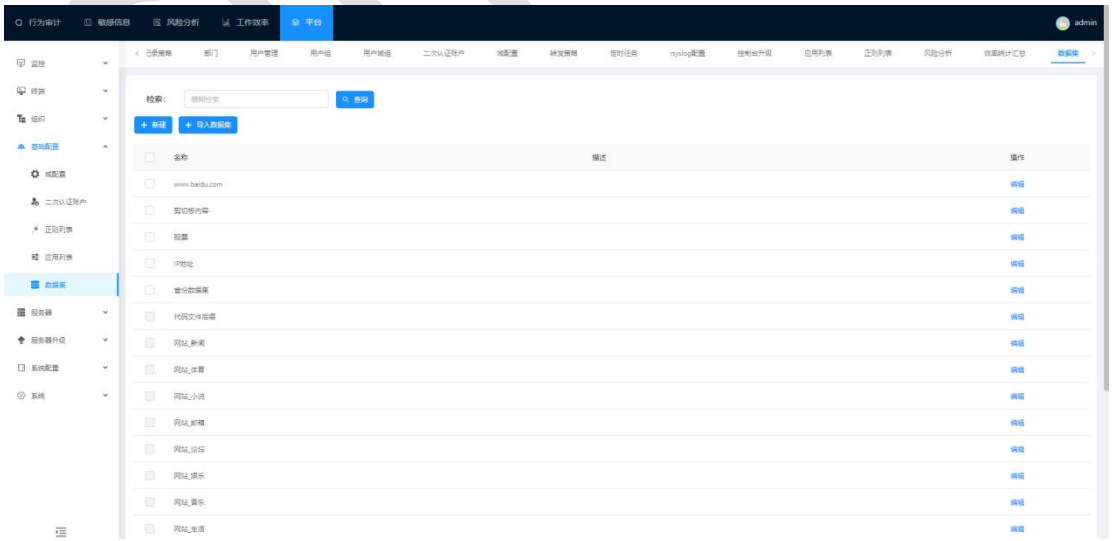
三 敏感，风险，工作效率

3.1 风险分析

3.1.1 数据集

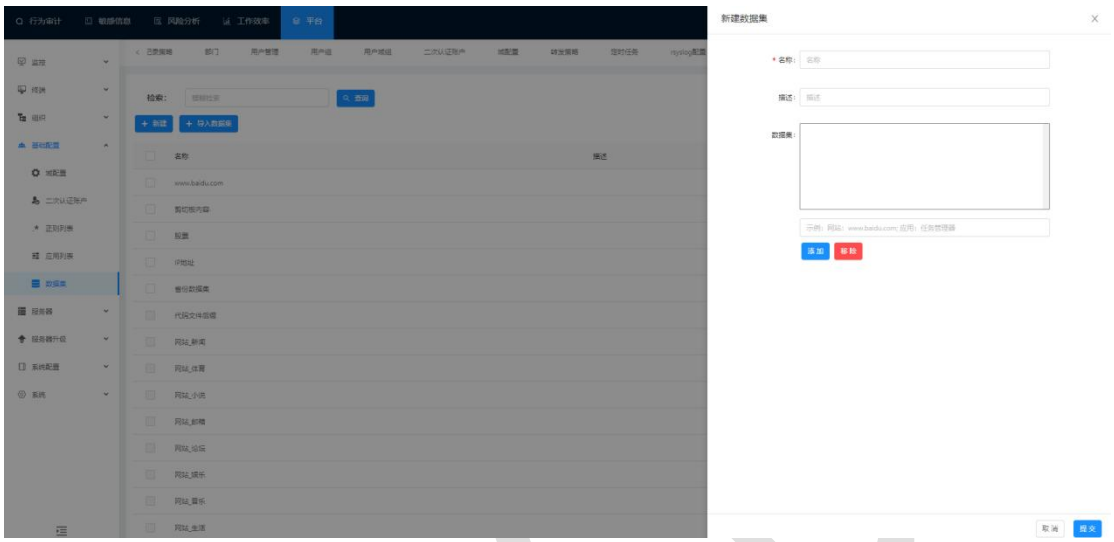
数据集是把数据条件集合起来；可以用于风险行为条件、敏感行为条件、效率分类条件。

选择“配置>应用配置>数据集”进入数据集界面；如下图所示：



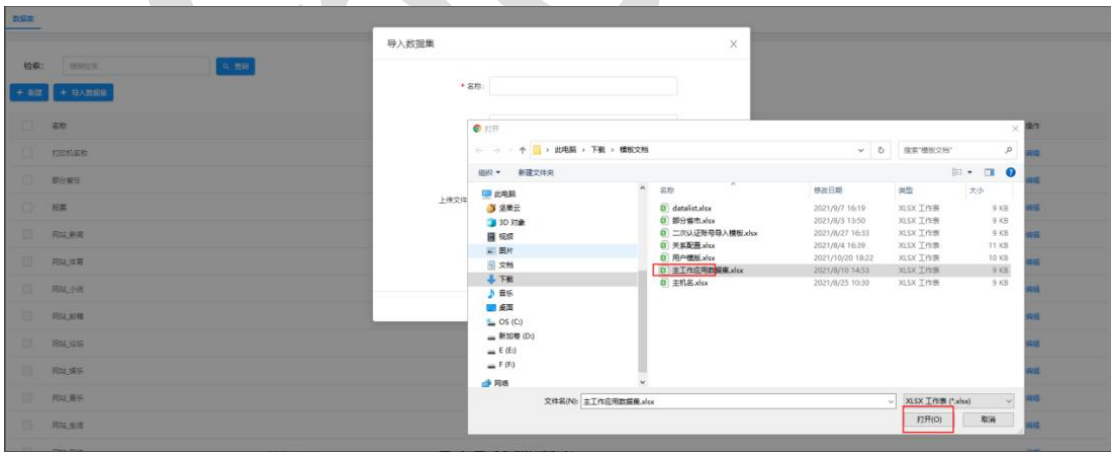
3.1.1.1 新建数据集

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

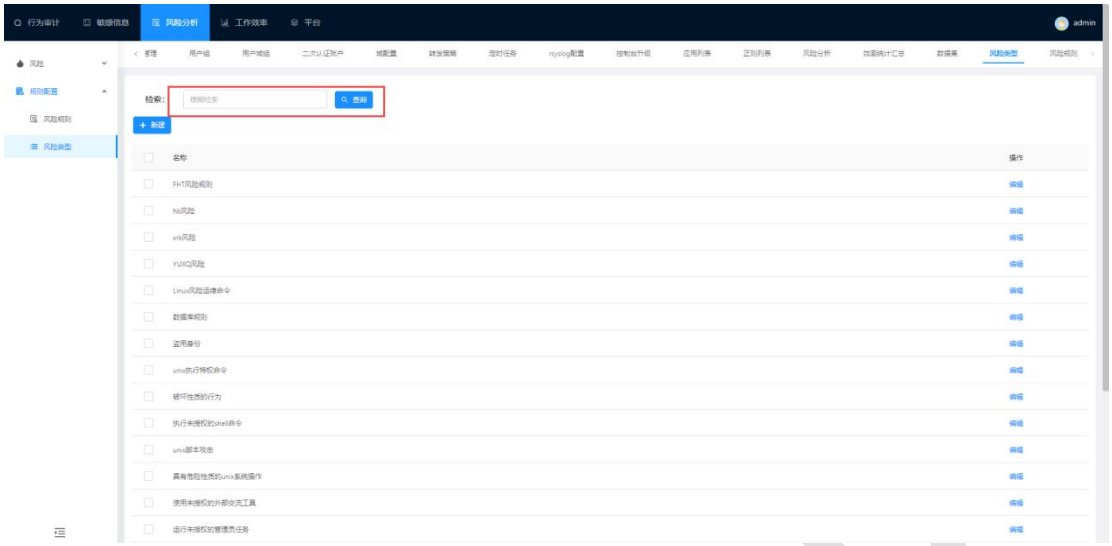
点击“导入数据集”按钮进行导入数据集（需先下载数据集模板编辑好数据集内容再上传导入）如下图所示：



3.1.2 规则类型

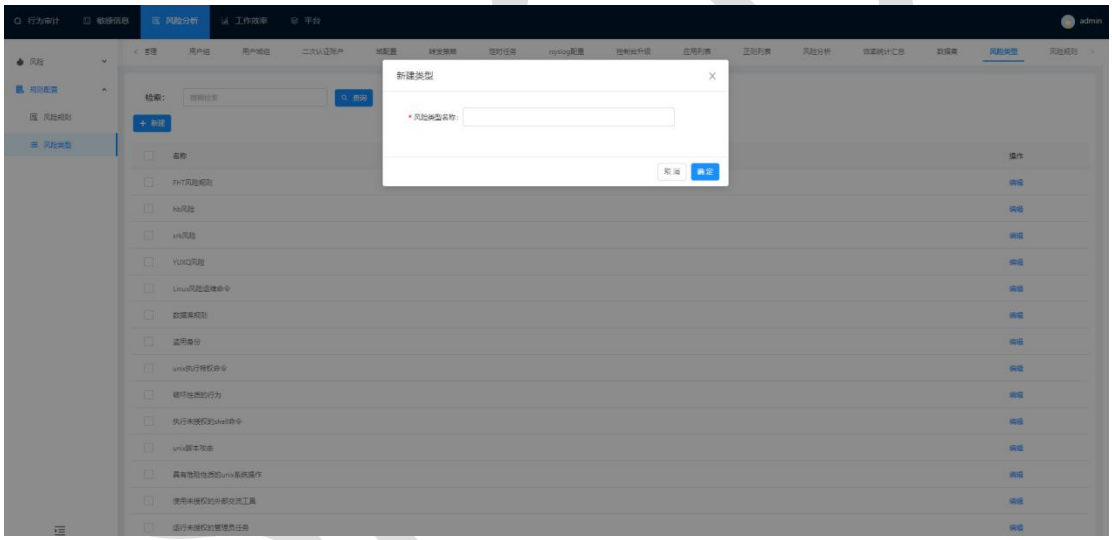
规则类型：对风险规则进行分类。

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：



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：

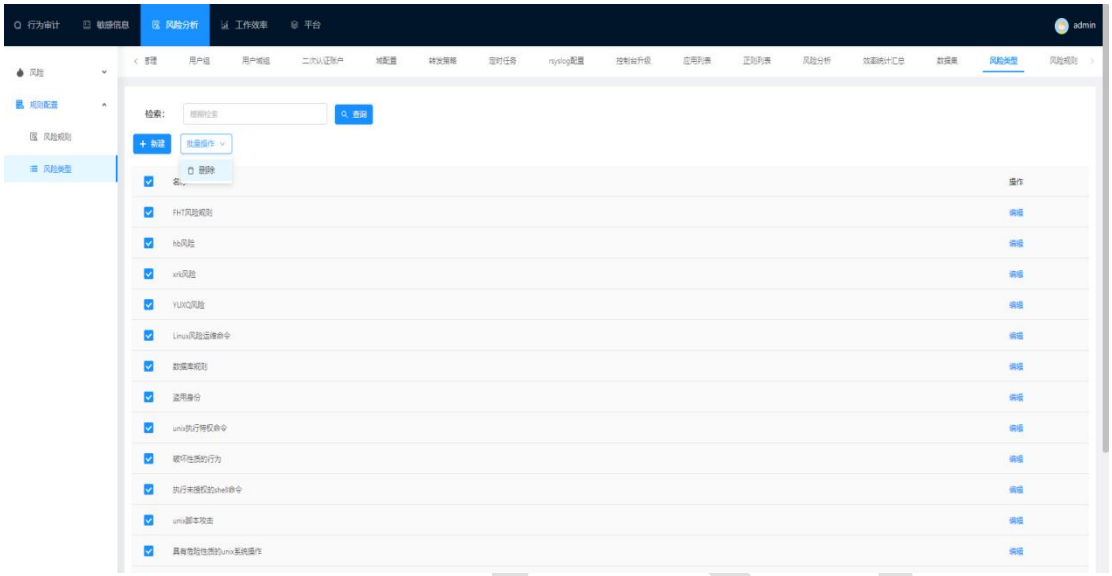


3.1.2.2 编辑规则类型

点击‘编辑’按钮，弹出编辑类型窗口界面

3.1.2.3 删除规则类型

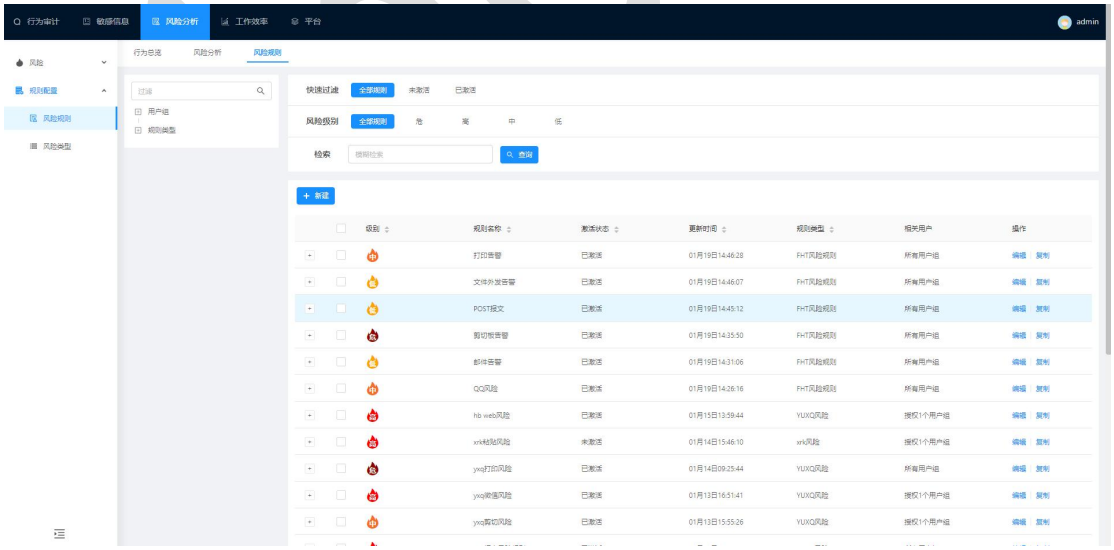
选择一个或多个规则类型，点击‘批量操作’下拉框，再点击‘删除’，如下图所示：



3.1.3 风险规则

风险规则：可以配置终端的行为风险规则

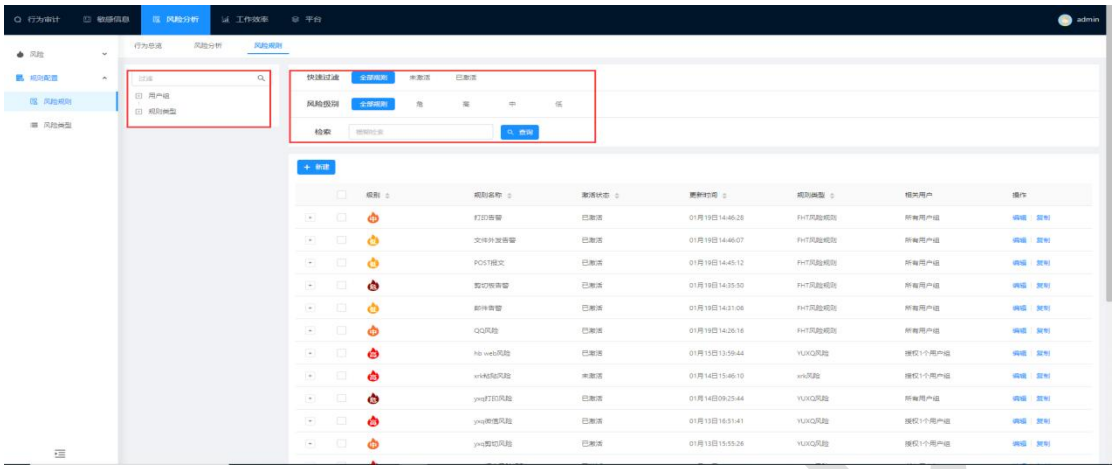
选择“配置>风险配置>风险规则”查看风险规则信息。如下图所示：



3.1.3.1 风险规则查询

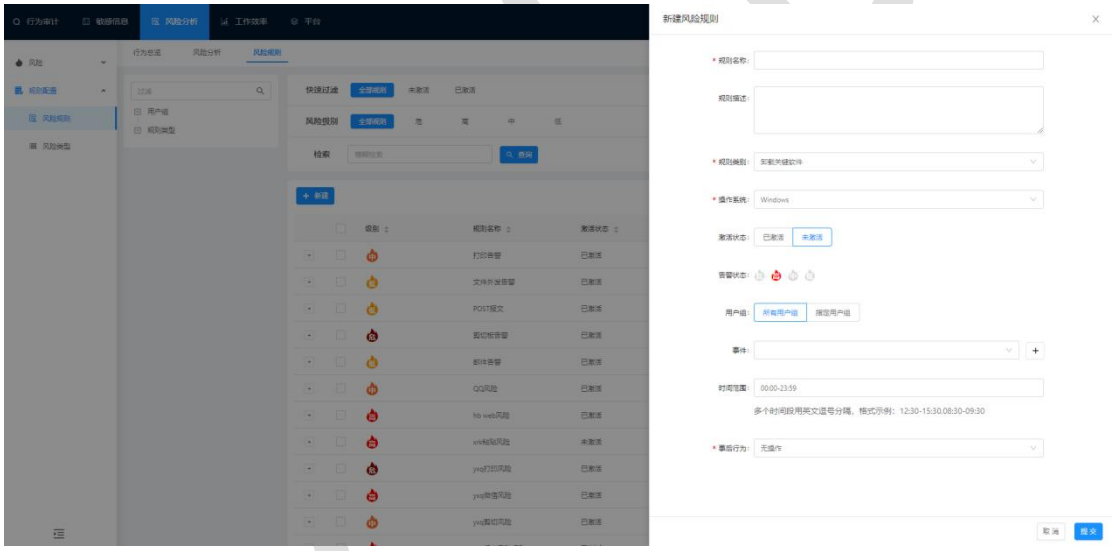
左侧可以输入或选择规则类型进行查询；也可以选择快速过滤、风险级别和输入关键字

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：



3.1.3.2 新建风险规则

点击“新增”按钮弹出新建规则界面；如下图所示：



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。

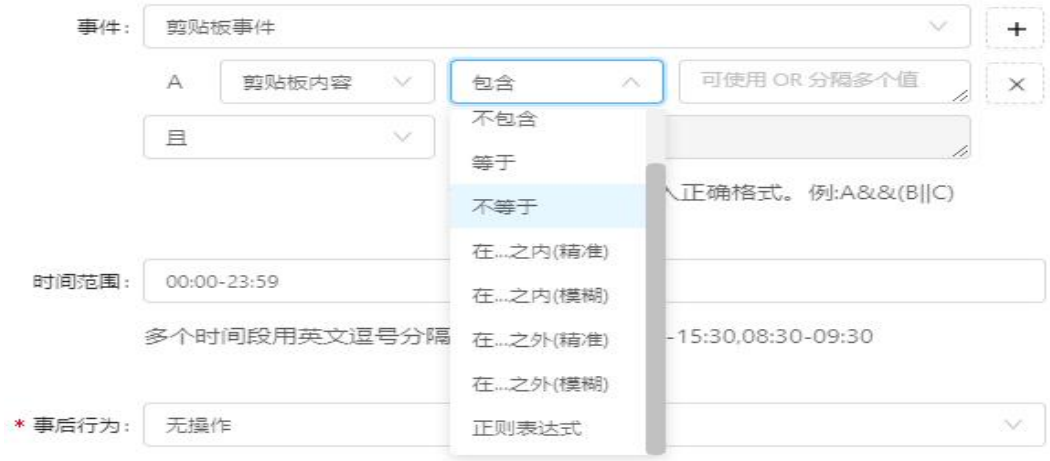
默认选择所有用户组，则所有终端用户都可以触发风险。

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）。

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：



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”

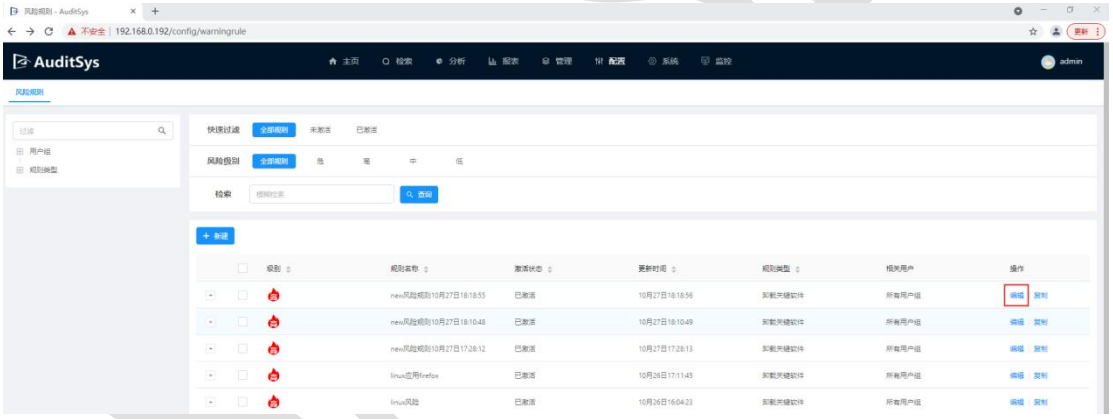
例如：触发剪切板风险条件是在...之内（精准）：复制粘贴“湖南”

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。

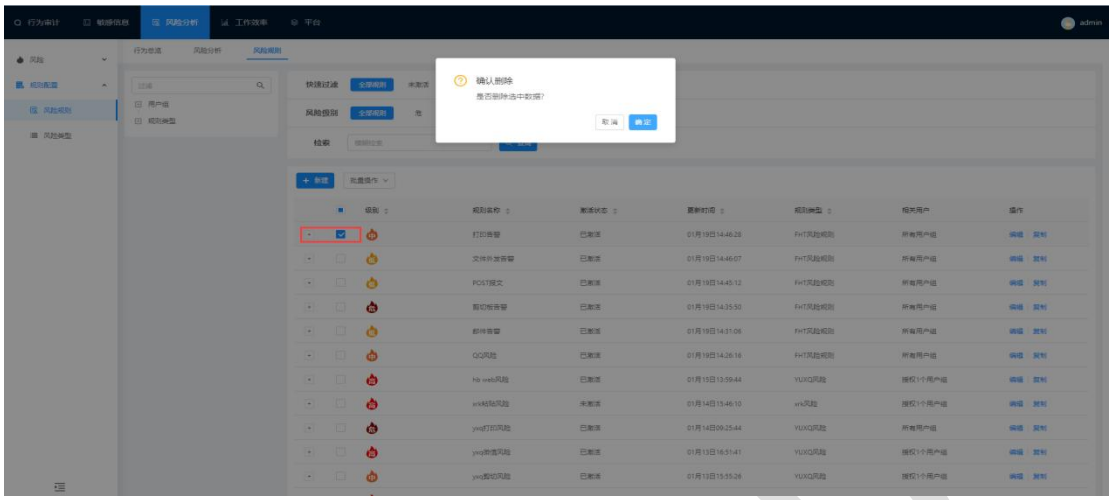
3.1.3.3 编辑风险规则

点击“编辑”按钮编辑记录策略。如下图所示：



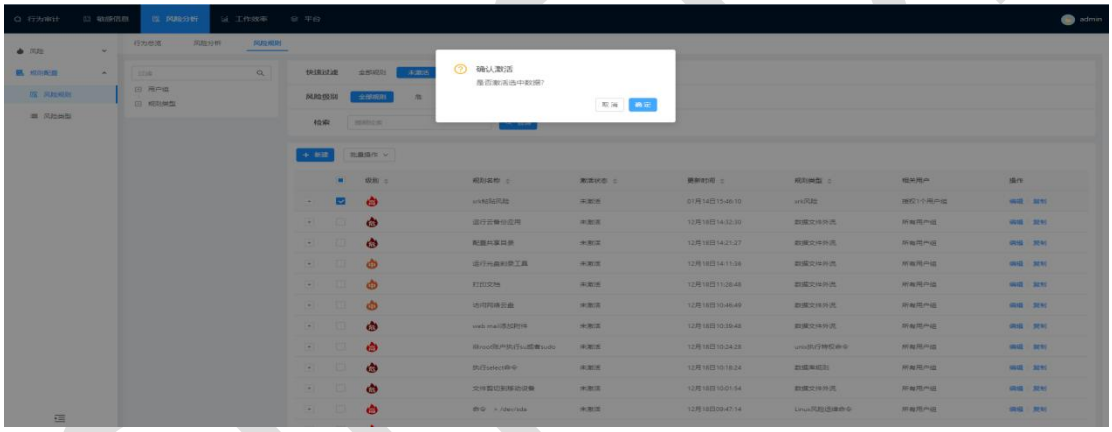
3.1.3.4 删除风险规则

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：



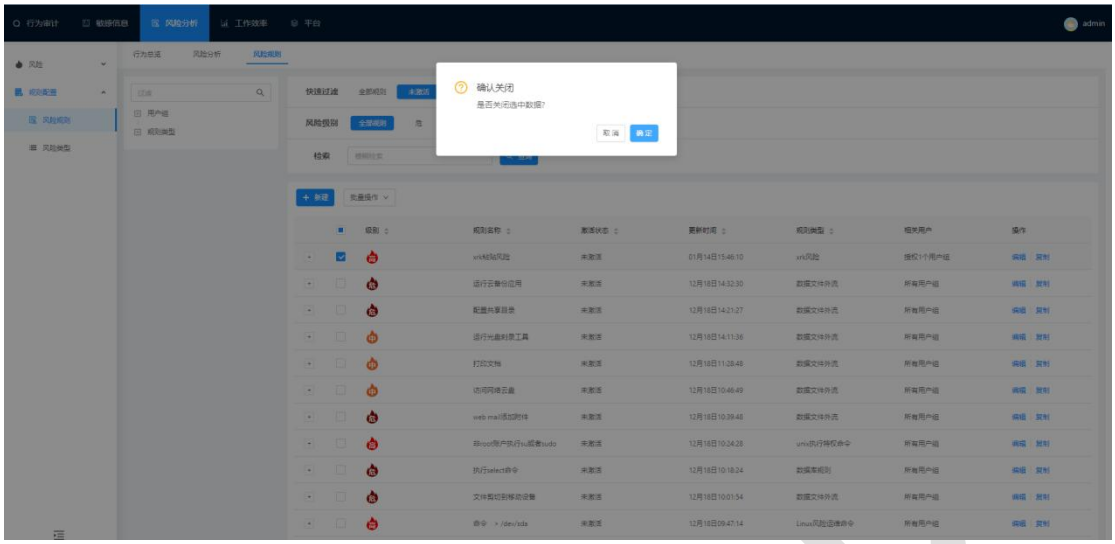
3.1.3.5 风险激活

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：



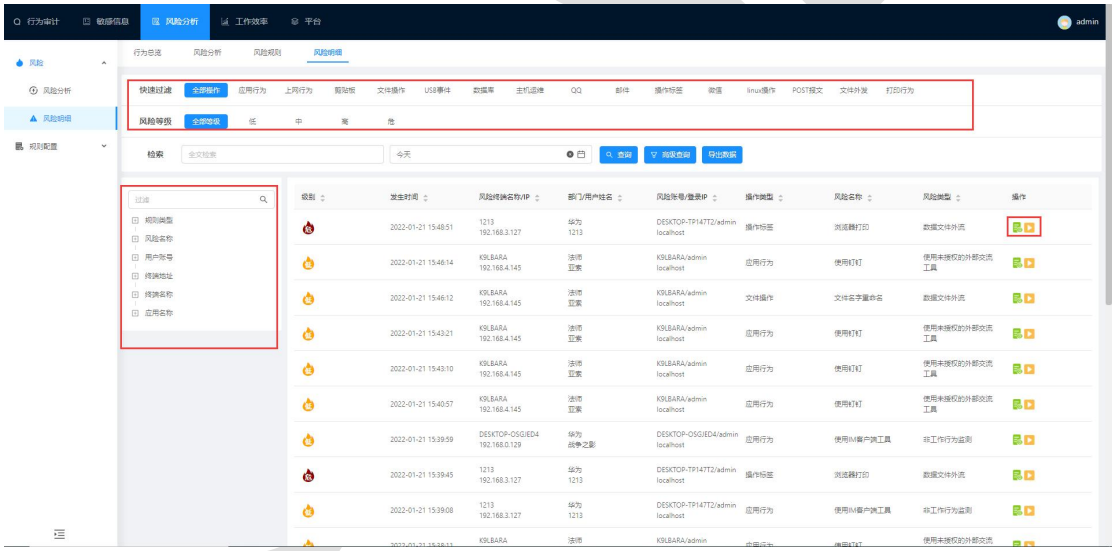
3.1.3.6 关闭风险

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：



3.1.4 风险明细

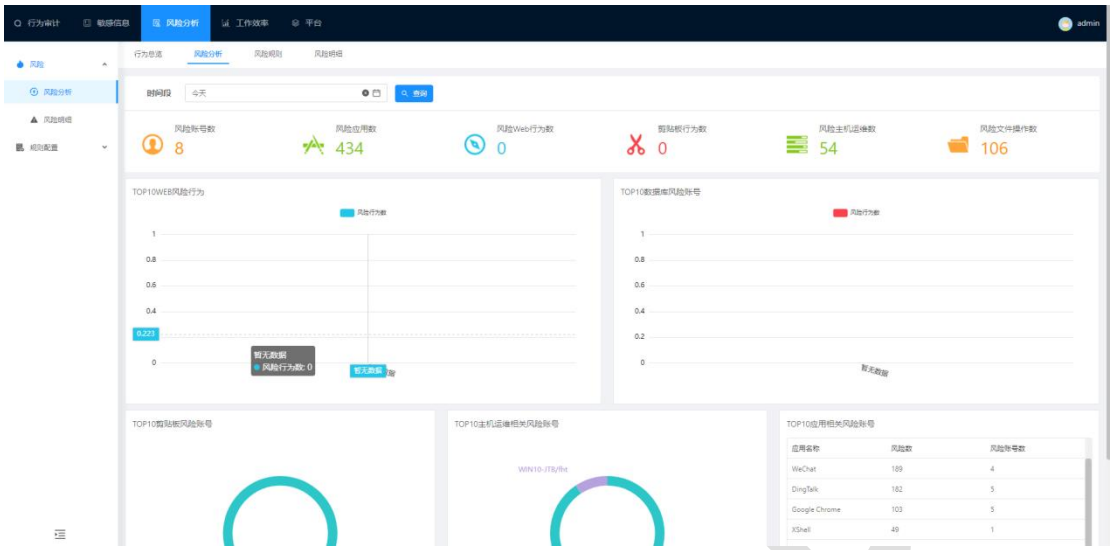
点击“ ”按钮查看风险明细详情；点击“ ”播放风险触发定帧，左侧可对风险类型进行筛选，快速过滤如下图所示：



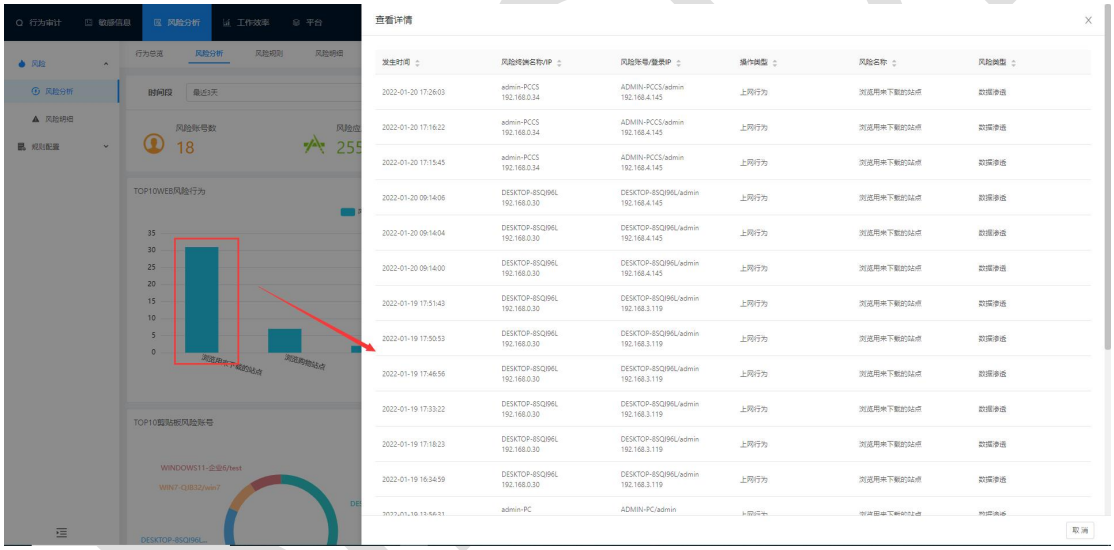
3.1.5 风险分析

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：

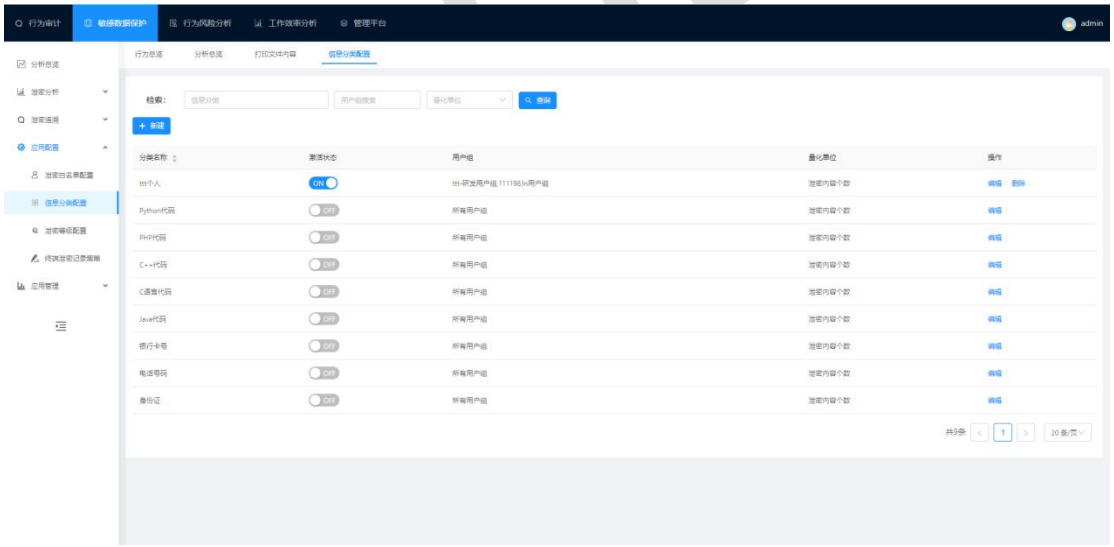


例如：点击风险应用数，查看应用风险明细详情

3.2 敏感信息

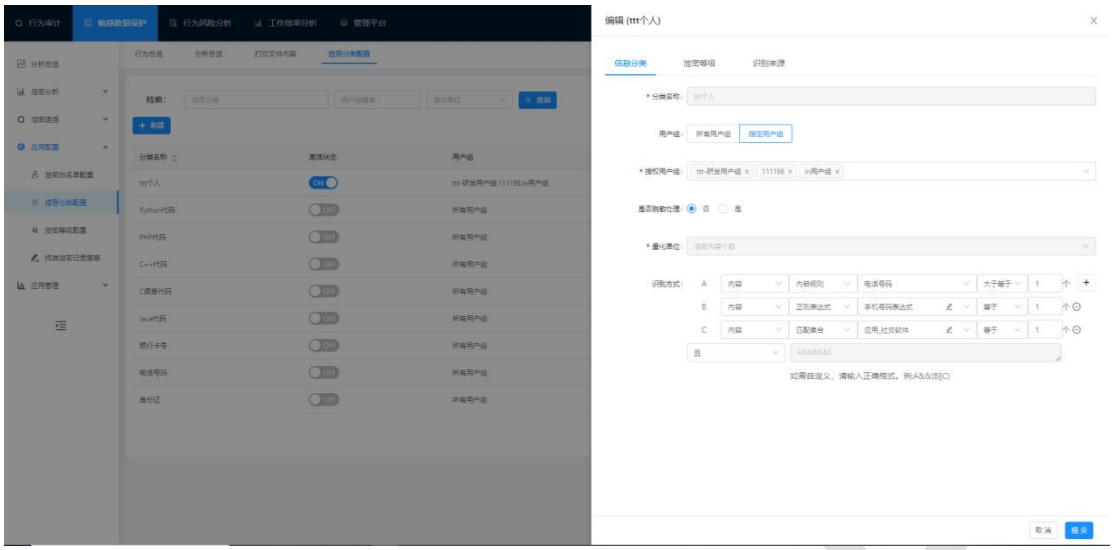
3.2.1 信息分类配置

点击“敏感信息>敏感分类配置”进入敏感词分类界面，如下图：



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。

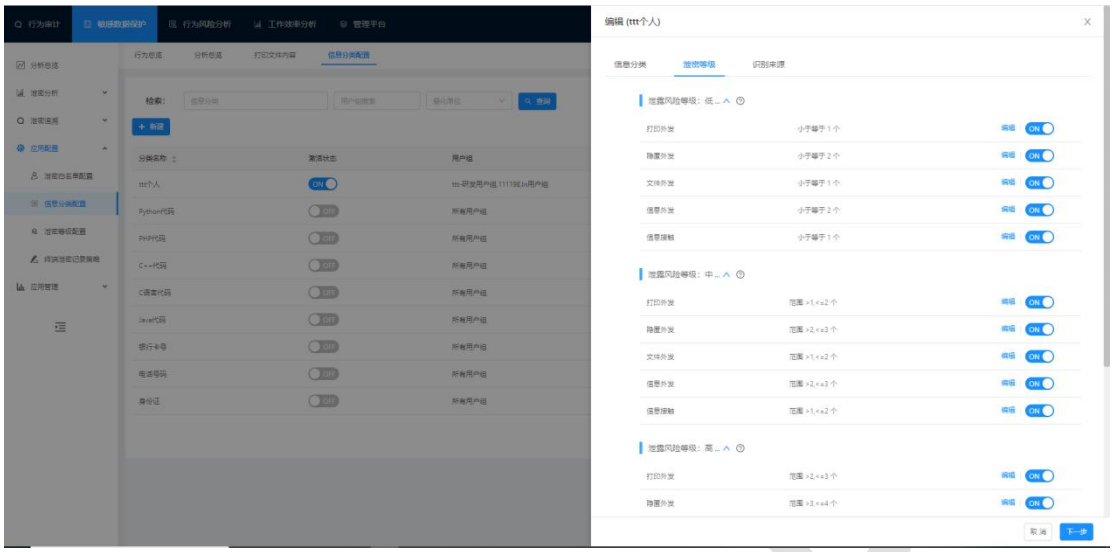
识别方式：选择内容为文本操作或文件操作中的内容进行解析。

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。

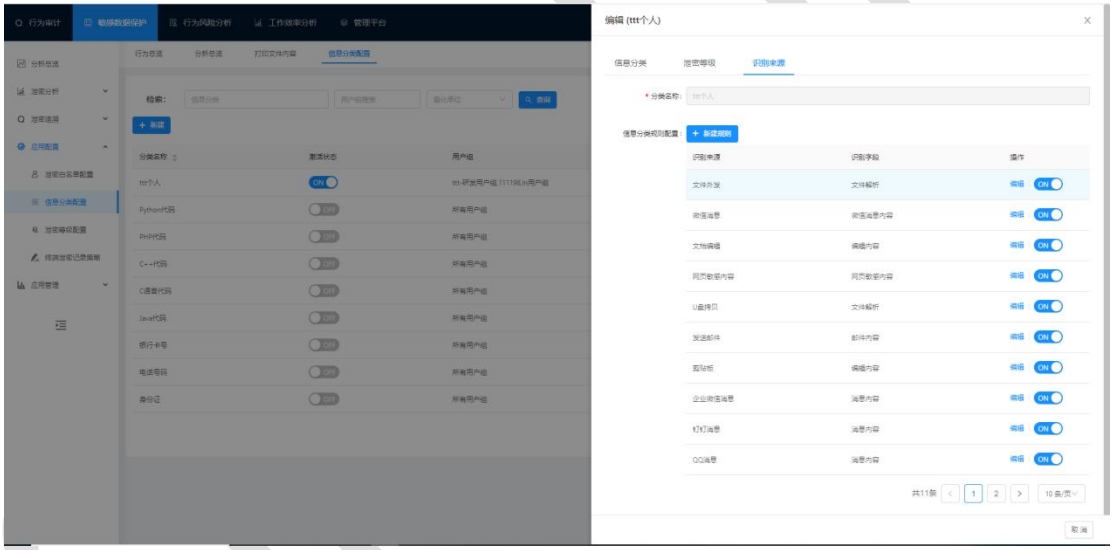
选择原始文件名为在文件操作前对文件进行重命名操作后在进行发送，解析其重命名前的文件名是否含有敏感词。

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：

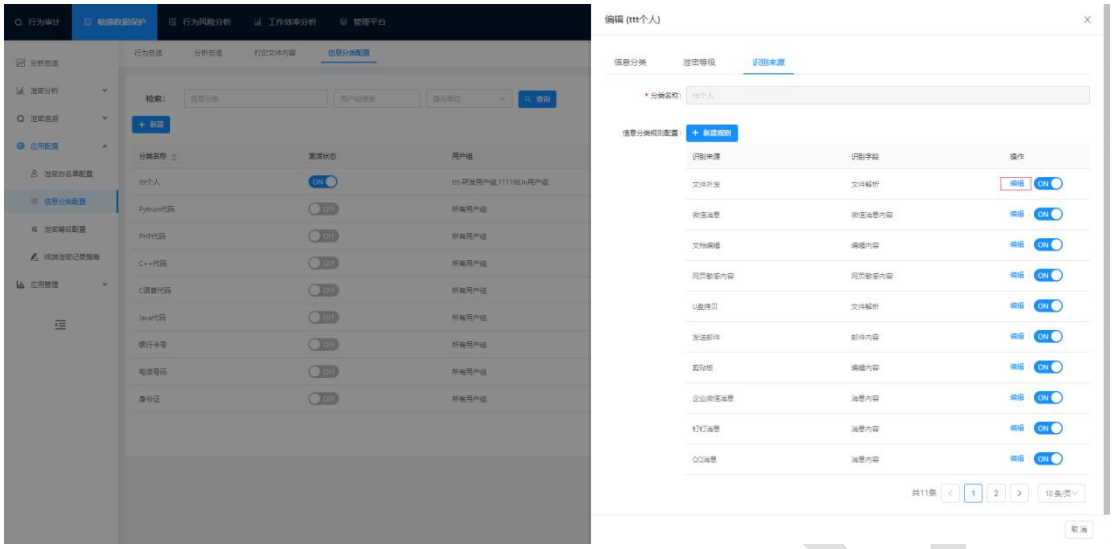


配置启用后点击下一步，选择需要识别的来源开启后新建敏感分类过程结束。



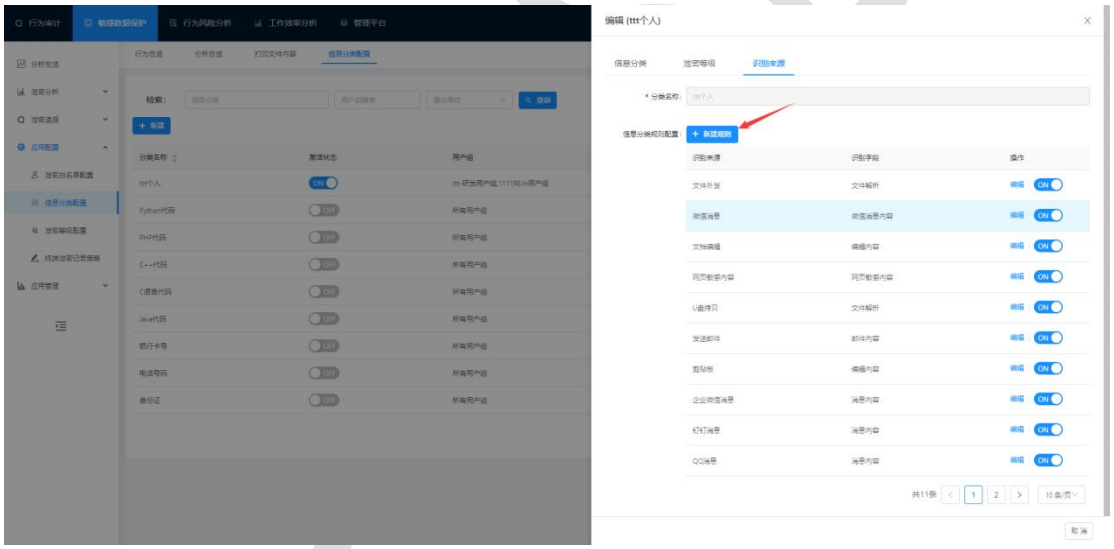
3.2.1.2 信息分类配置编辑

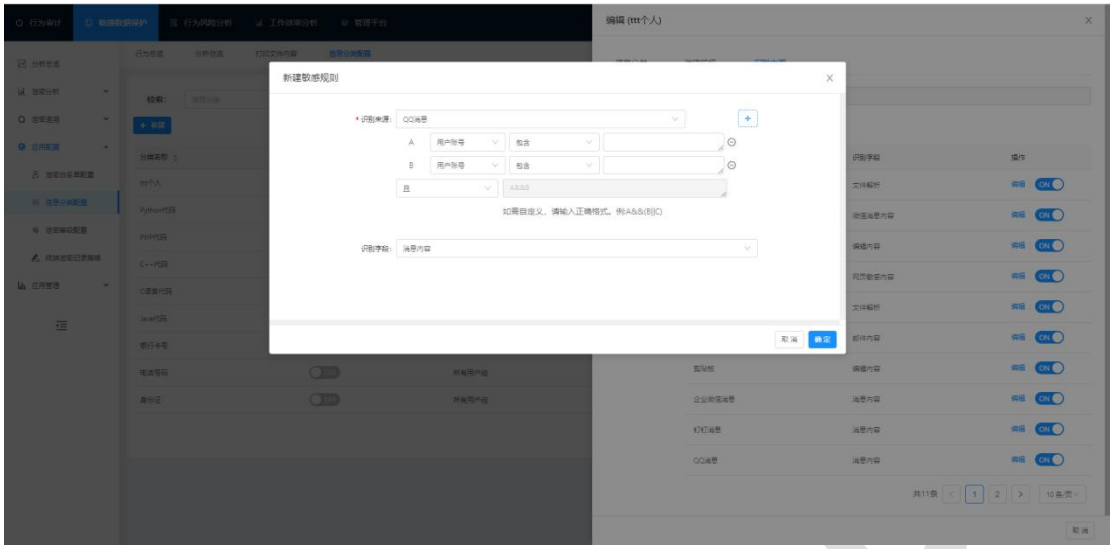
点击完善规则，选择相应规则点击编辑如下图所示：



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：





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。

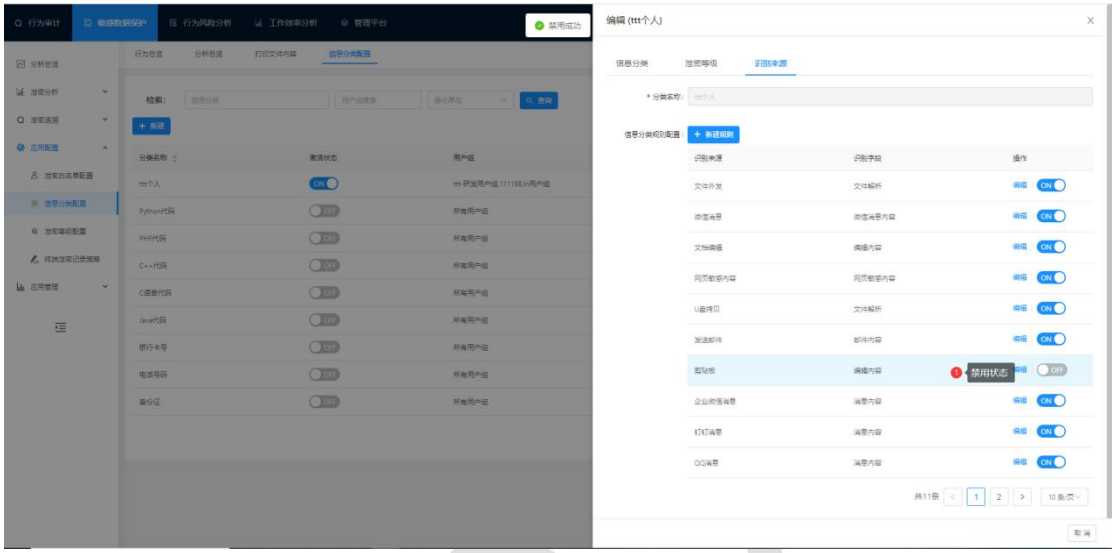
微信消息、QQ 消息：发送\接收聊天消息和文件内容包含敏感词。

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：



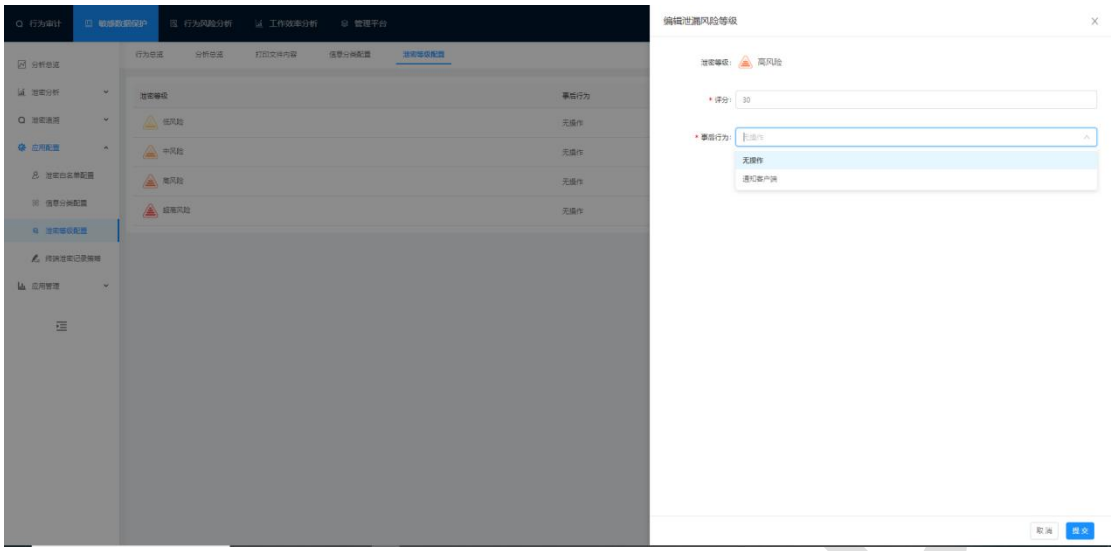
3.2.2 泄密等级配置

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。

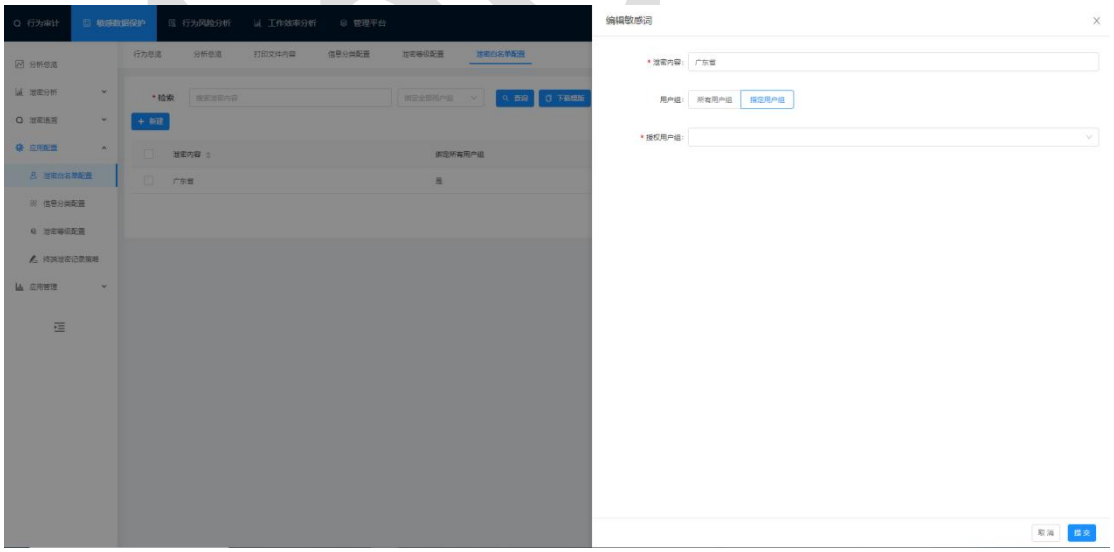
通知客户端：在触发敏感后在桌面右下方弹出敏感提示弹窗。



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

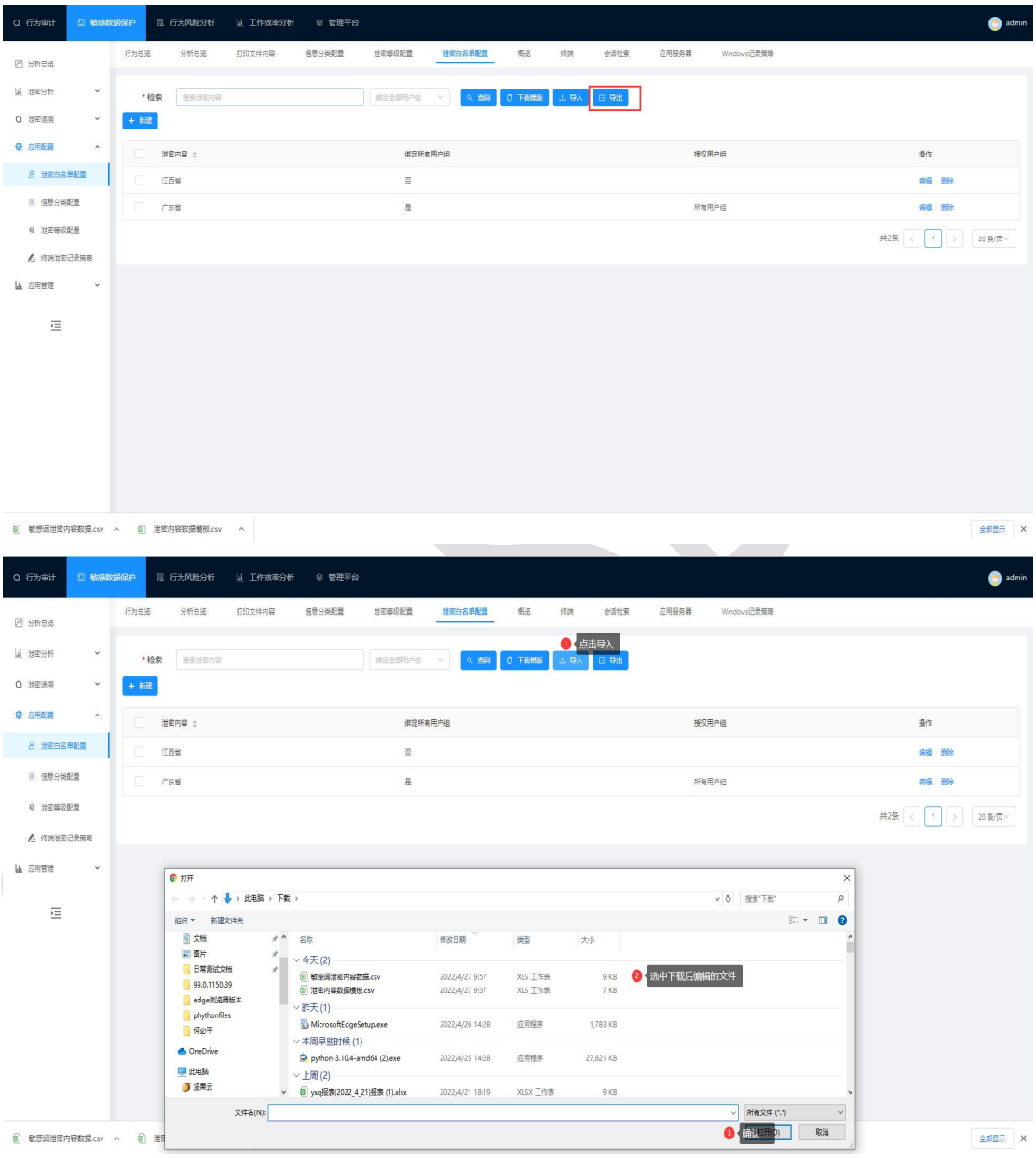
原是可以触发的敏感词加入敏感白名单中后再去通过发送或剪切等其他方式触发该敏感词的行为将不会被记录，其中白名单可授权所有用户组和个别用户组。新建白名单如下图所示：



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：



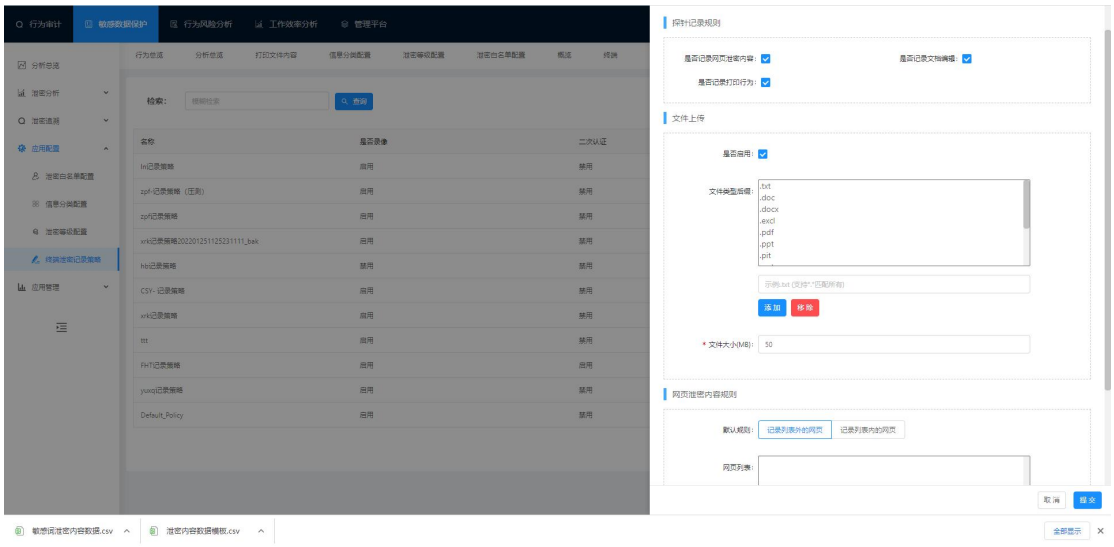
3.2.4 终端泄密记录策略

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。

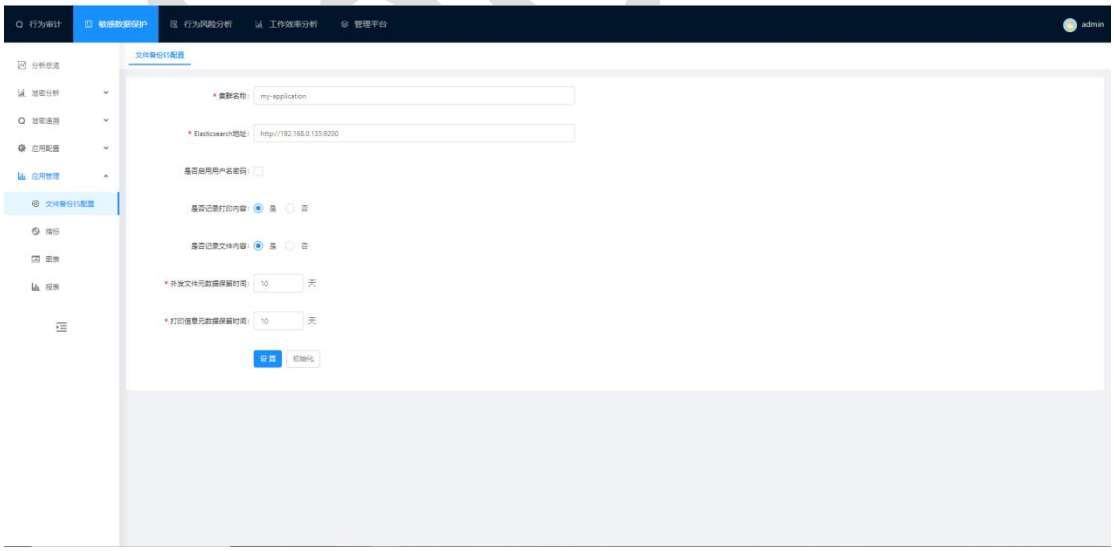
文件上传：勾选后文件才可上传至服务器，文件后缀类型可自主添加，未在表内的后缀不可触发敏感词记录。文件最大支持 50MB,超过不上传。

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。



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。

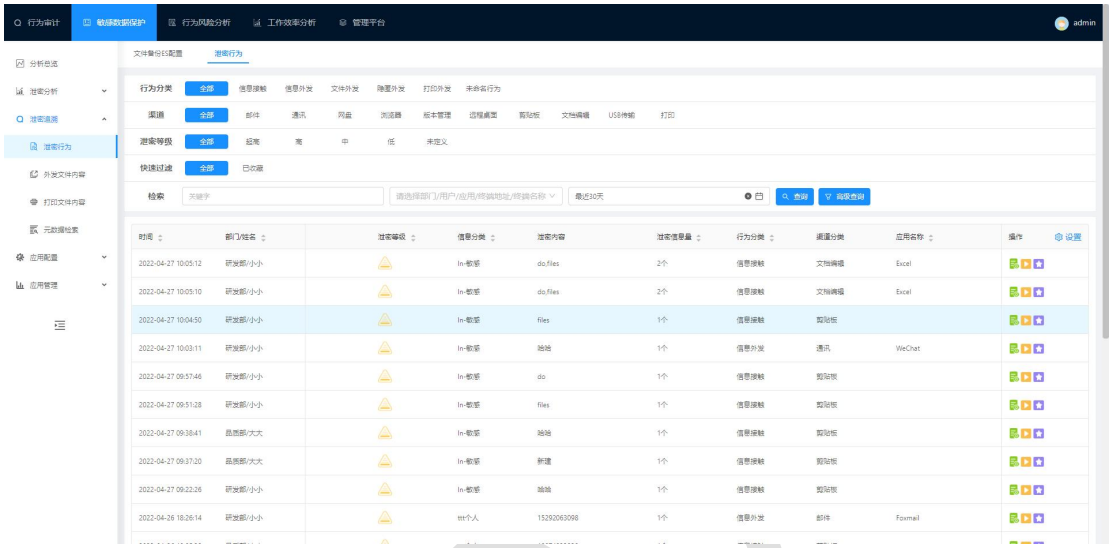


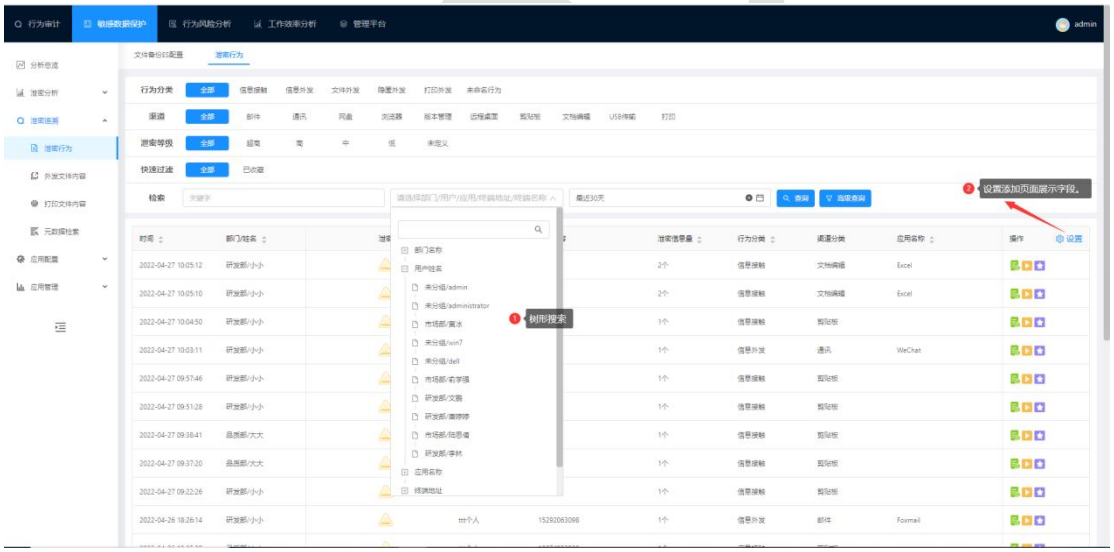
3.2.6 泄密行为

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；用户姓名；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。

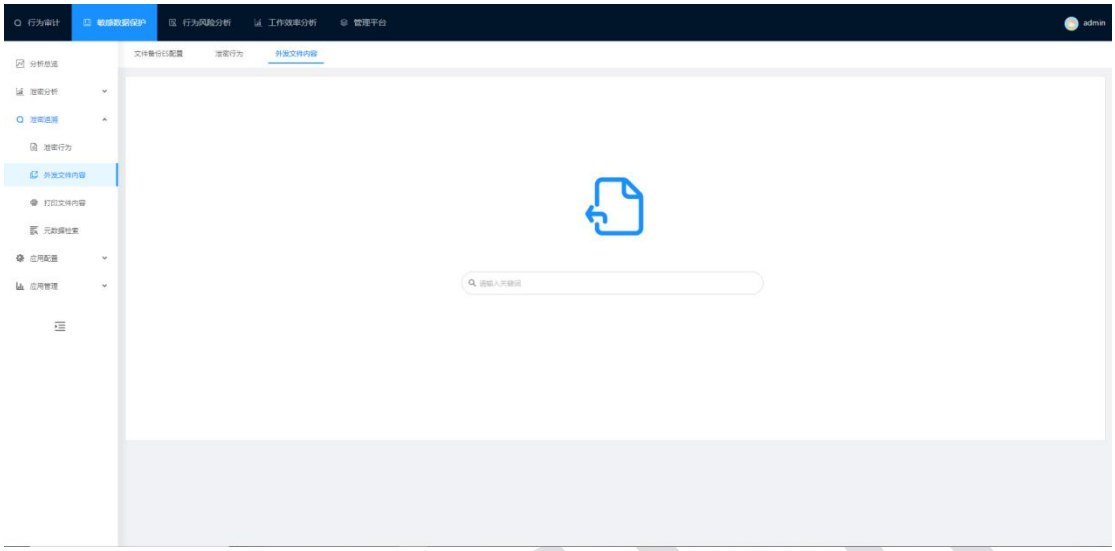


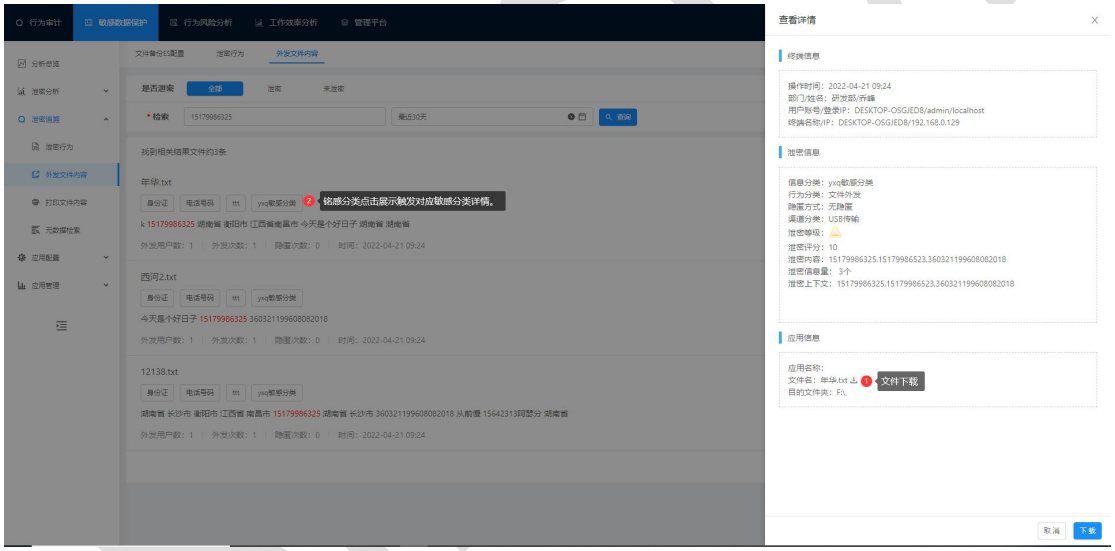


3.2.7 外发文件内容

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。

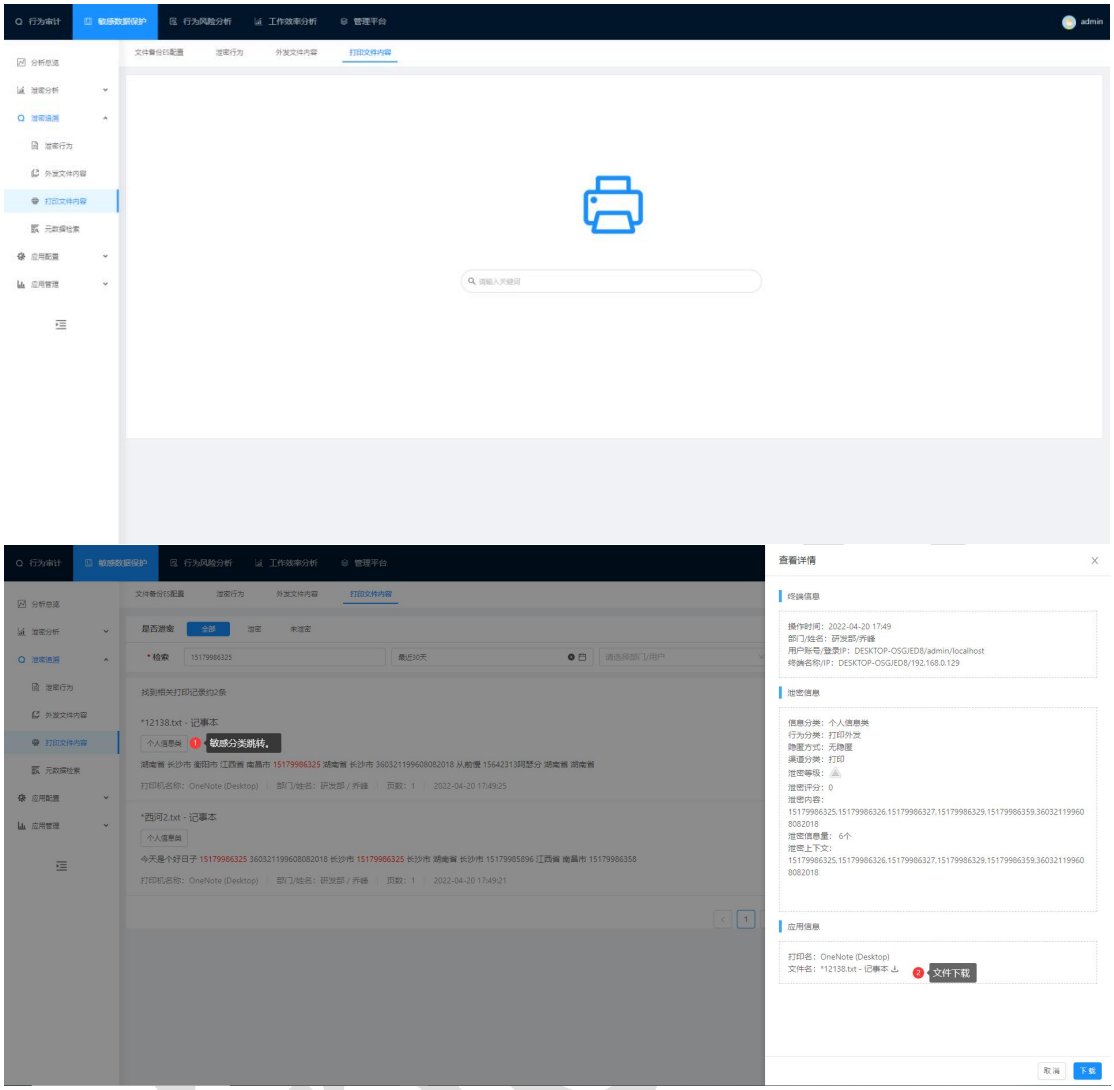
文件详情跳转：点击文件敏感分类名称或文件名称跳转至文件详细信息查看数据，并且支持相应文件下载。





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。

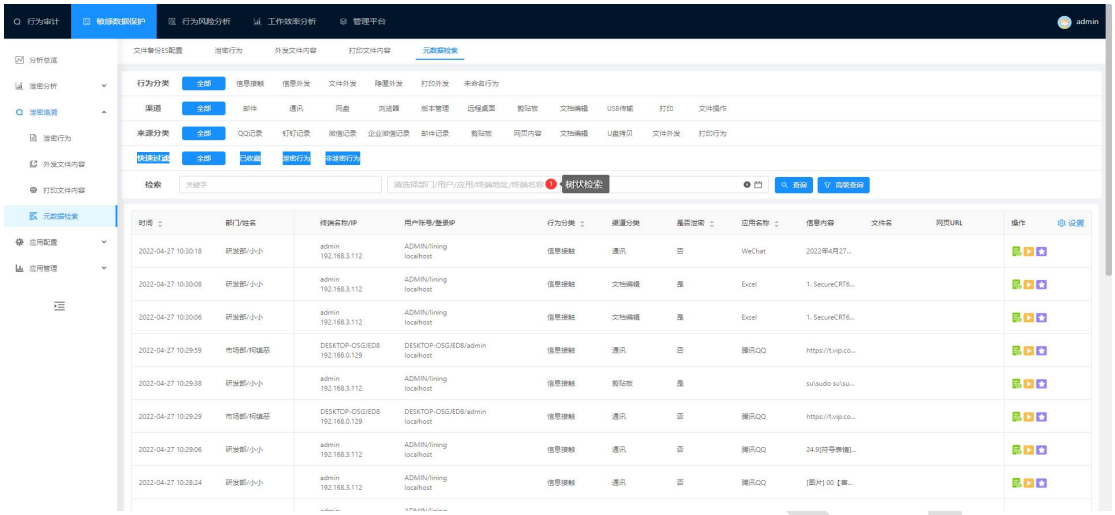


1.点击敏感分类

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。

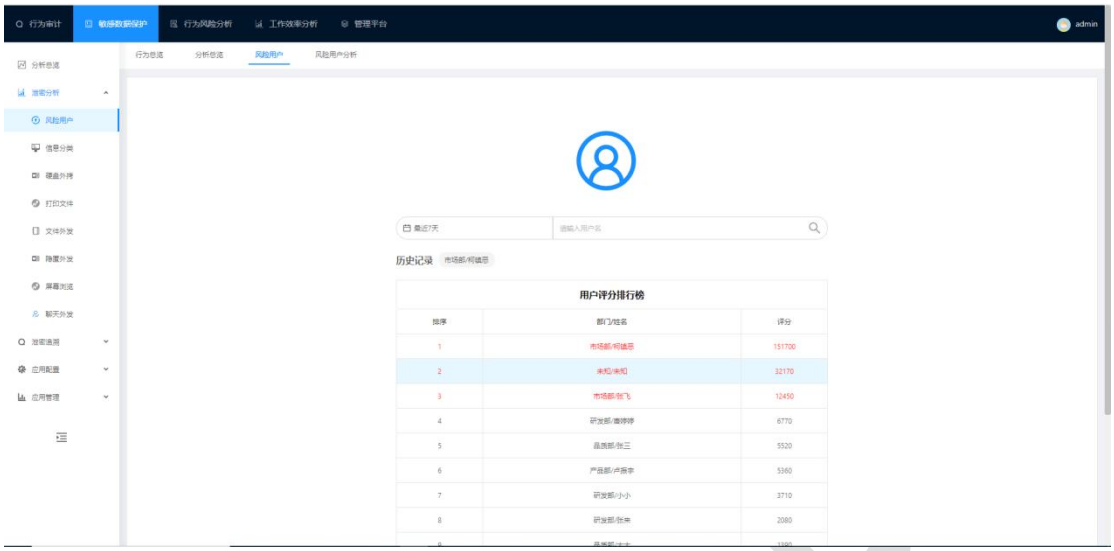
树状检索：检索条件包含：部门名称；用户姓名；应用名称；终端地址终端列表；用户列表中存在的终端用户都可被检索。附加搜索框未展示的标签可通过搜索框搜索。

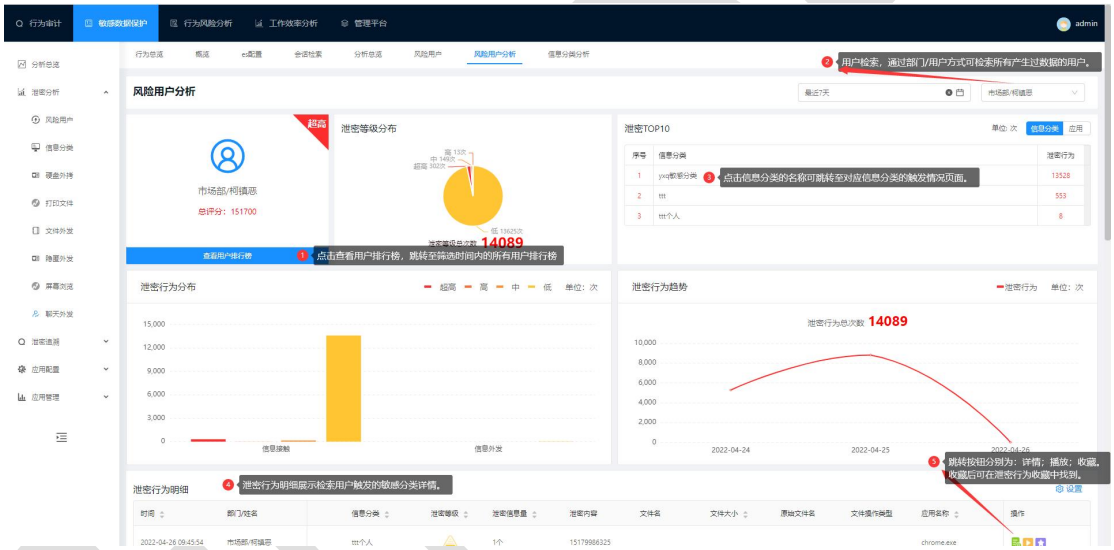


1. 树状检索：展开后可选择部门名称；用户姓名；应用名称；终端地址；终端名称进行检索。如下图所示：

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。





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。

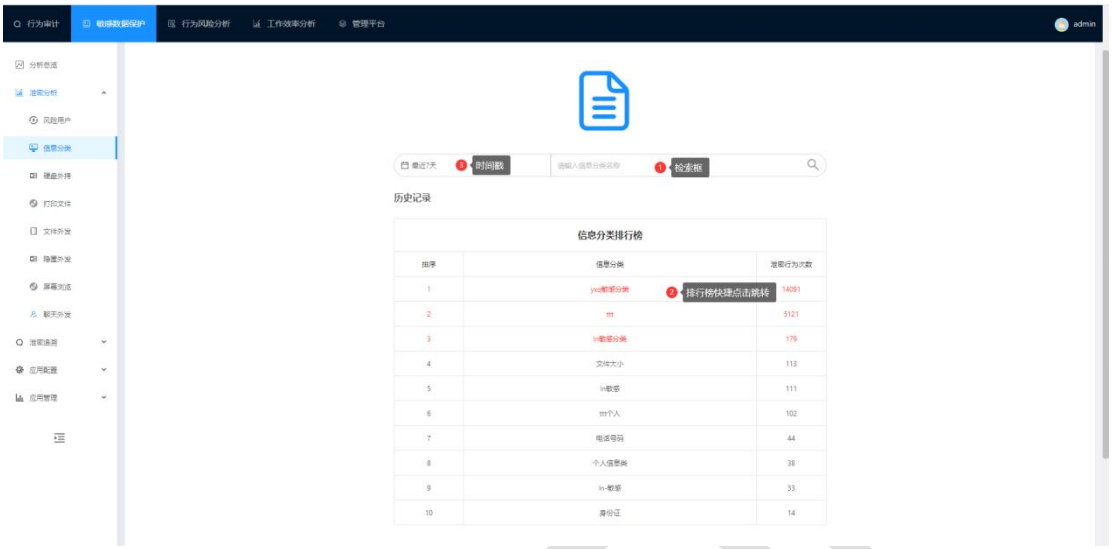
4. 泄密行为统计，趋势图展示。

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

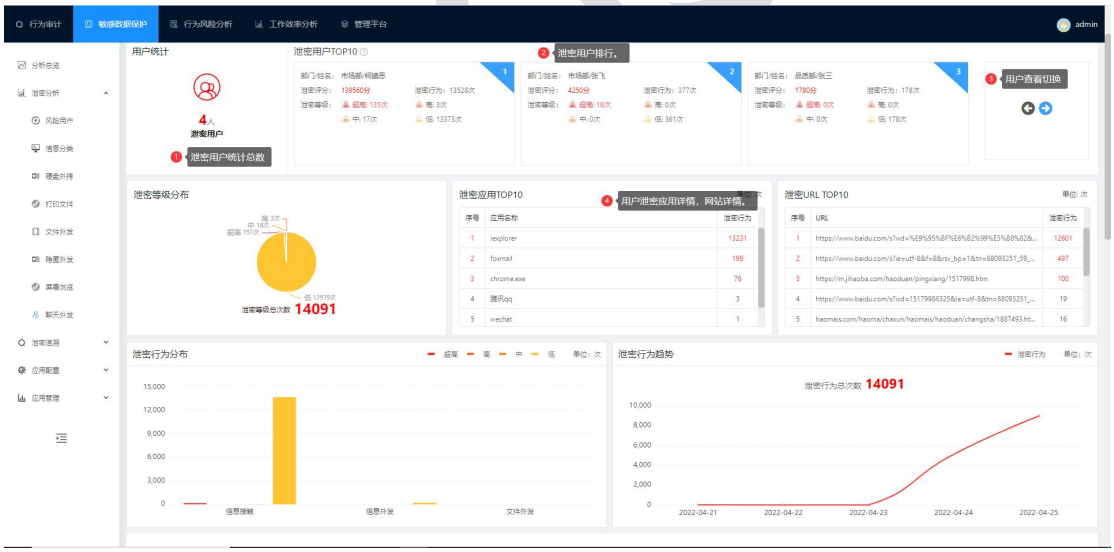
内的敏感分类可查看该时间段内的某个敏感分类的触发次数。



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。



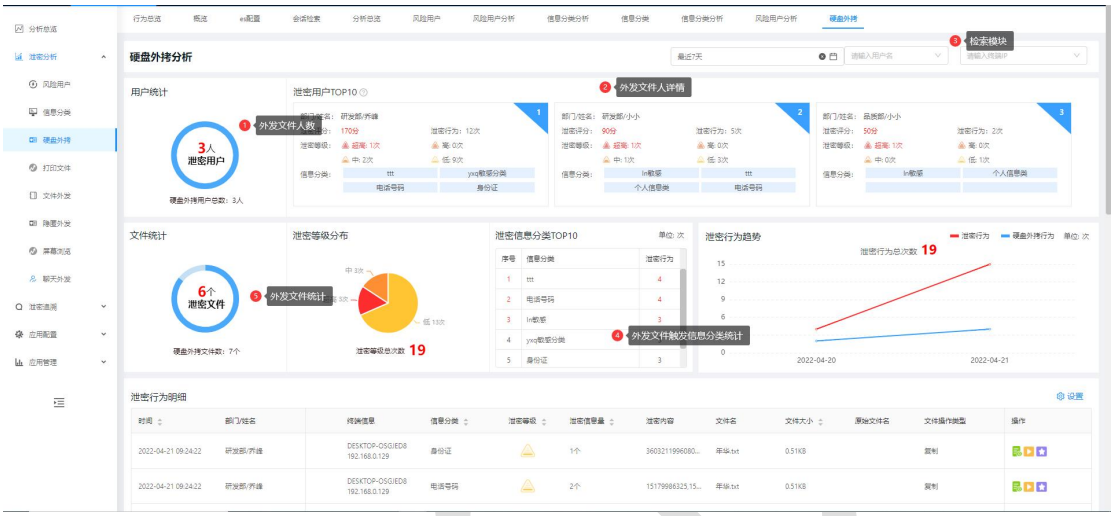
2. 用户排行，通过用户泄密等级评分计算进行排列，点击用户名可跳转至对应用户风险页面。

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。

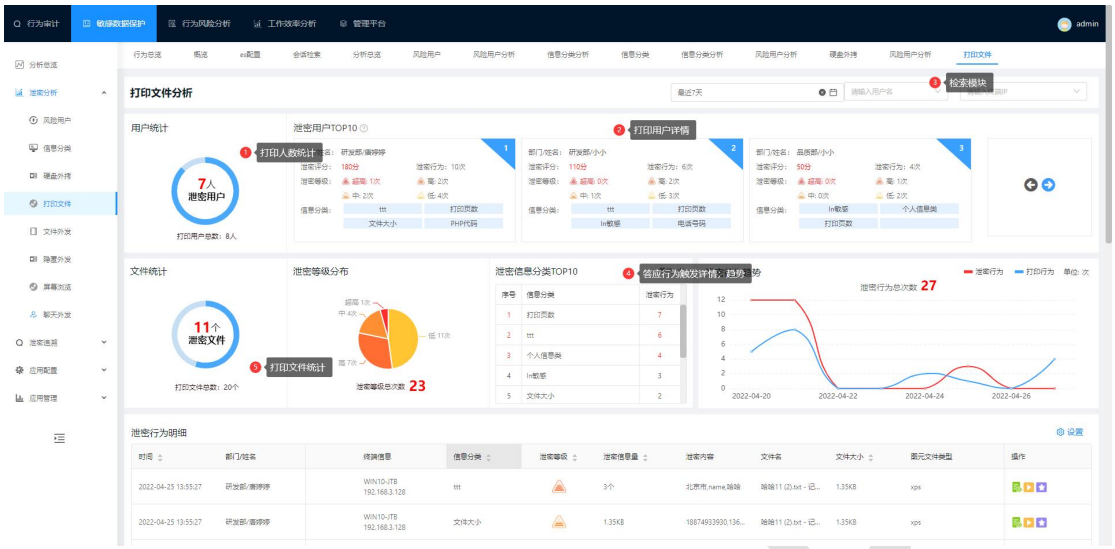
2. 硬盘外拷用户详情：包含外发用户，外发泄密文件泄密等级，触发信息分类名称。点击部门/用户可进行跳转至风险用户页面，点击信息分类标签可跳转对应信息分类。

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

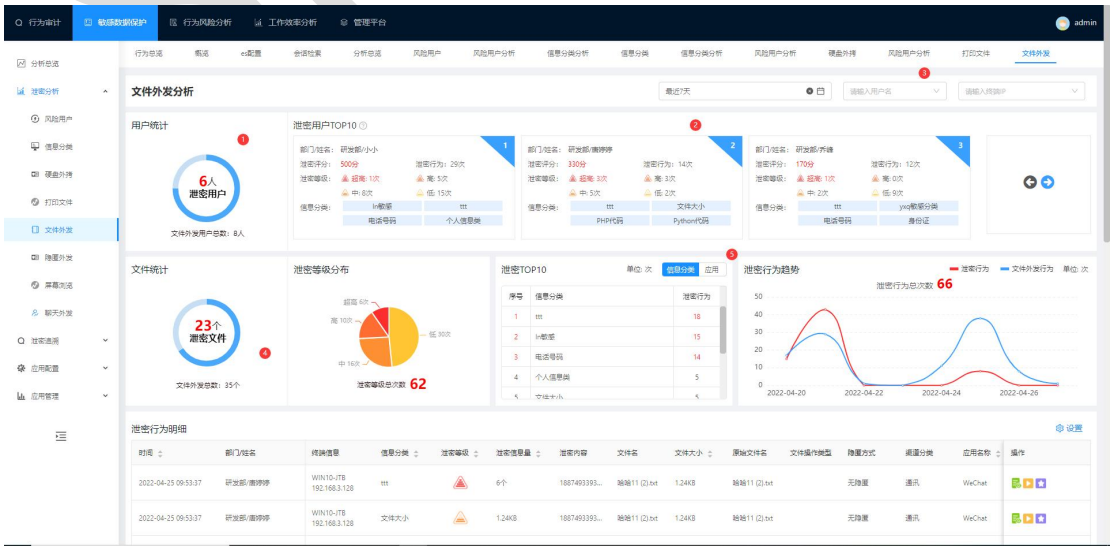
打印文件对用户打印文件中的泄密行为进行统计。



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。



1. 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。

2. 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。

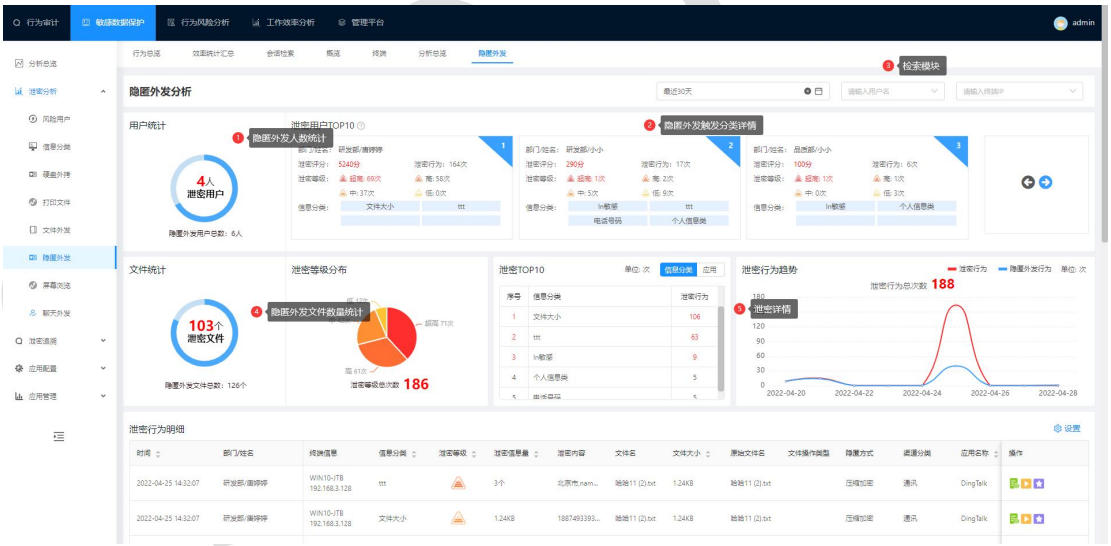
3. 检索模块：时间戳检索（快捷时间段以及自定义时间段）；用户部门及终端/ip 检索检索可选择产生过泄密信息的所有用户，未在列表中的用户/IP 请完整输入部门/用户或者直接输入 ip 直接检索。

4. 所有文件外发数目统计：泄密文件及所有外发文件。

5. 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。



1. 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。

2. 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。

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

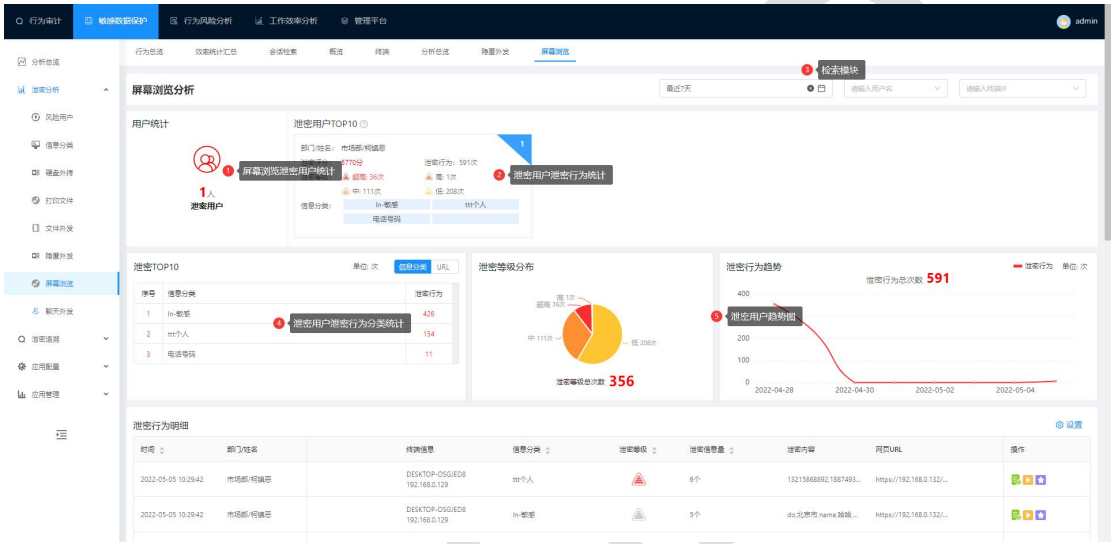
检索检索可选择产生过泄密信息的所有用户，未在列表中的用户/IP 请完整输入部门/用户或者直接输入 ip 直接检索。

4. 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。

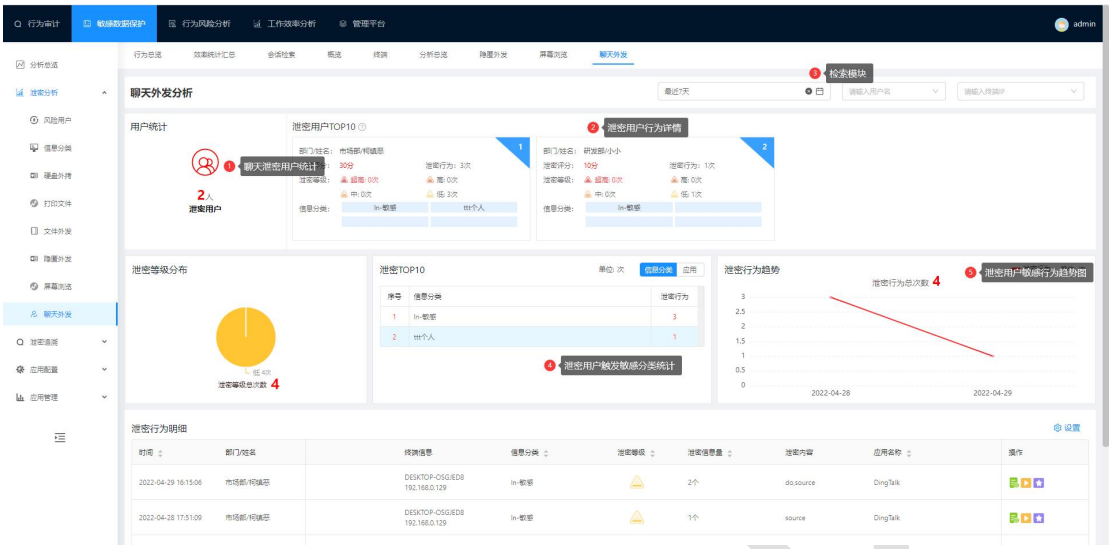
3. 检索模块：时间戳检索（快捷时间段以及自定义时间段）；用户部门及终端/ip 检索检索可选择产生过泄密信息的所有用户，未在列表中的用户/IP 请完整输入部门/用户或者直接输入 ip 直接检索。

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

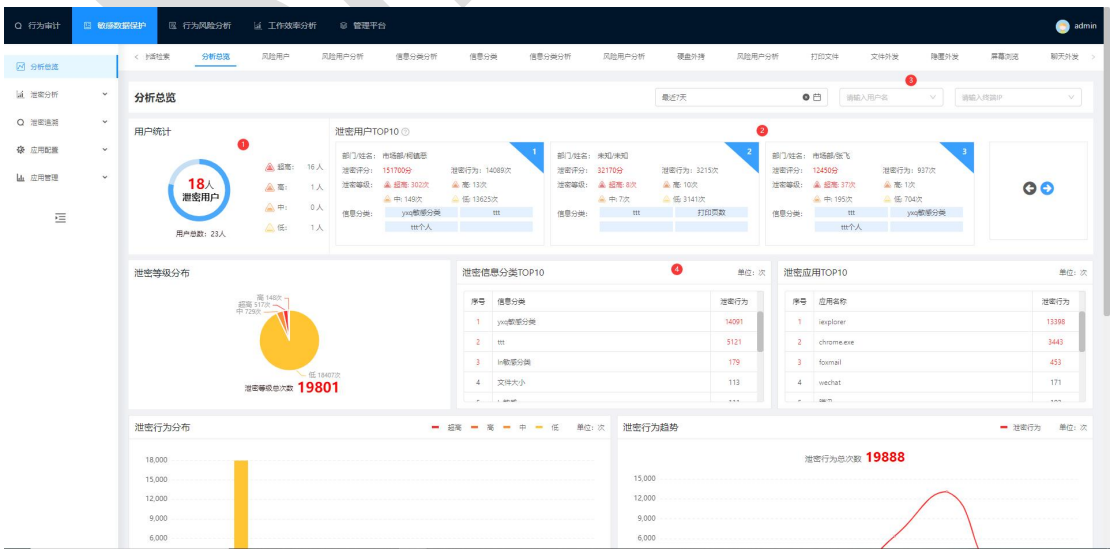
聊天外发统计用户在支持的聊天程序的所有泄密



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。

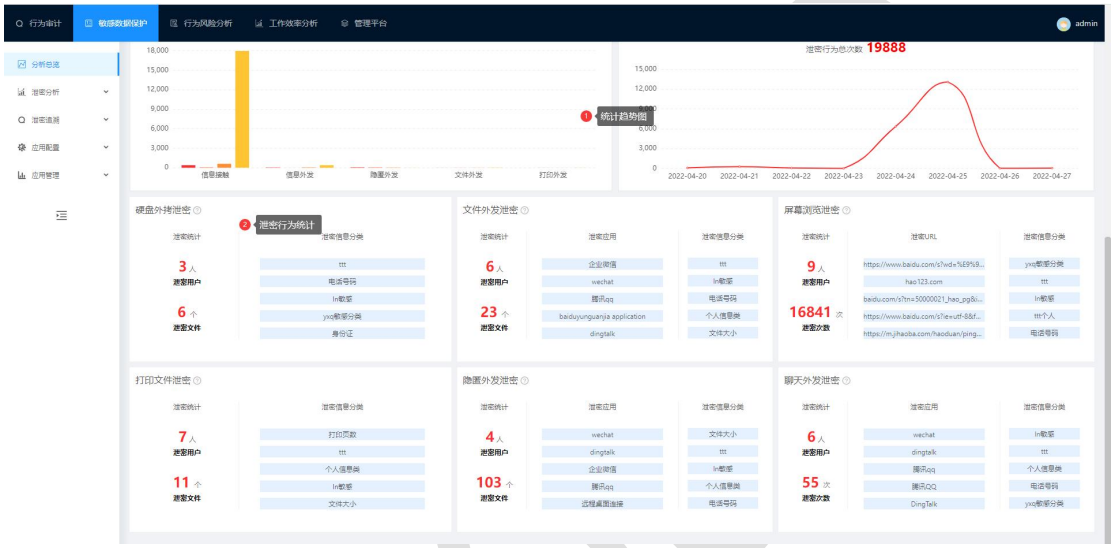


1. 所有泄密用户人数统计：分为泄密文件统计；用户泄密总评分：所有泄密行为人数统计。

2. 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。

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

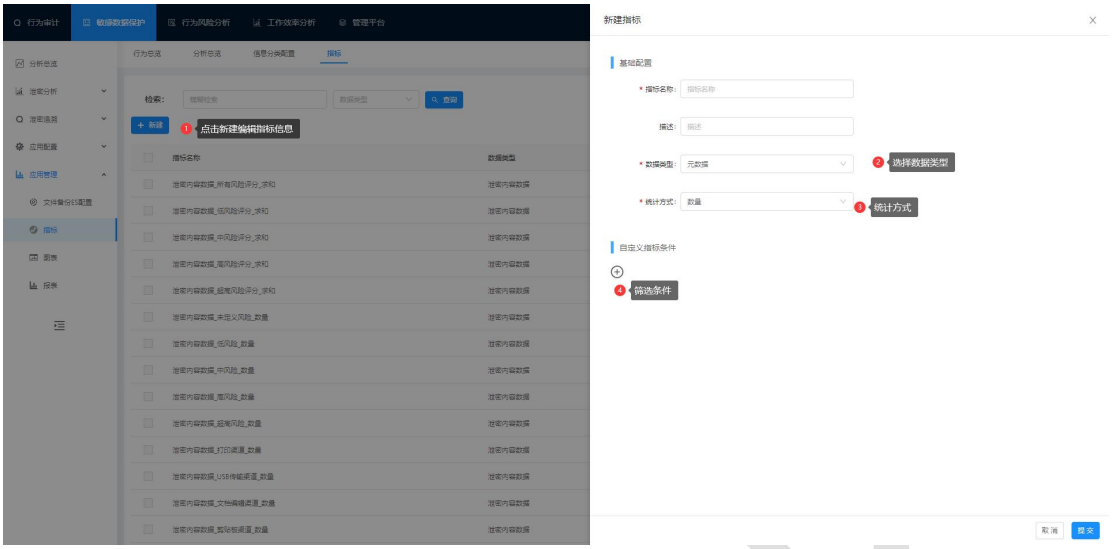


1. 泄密趋势图

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。

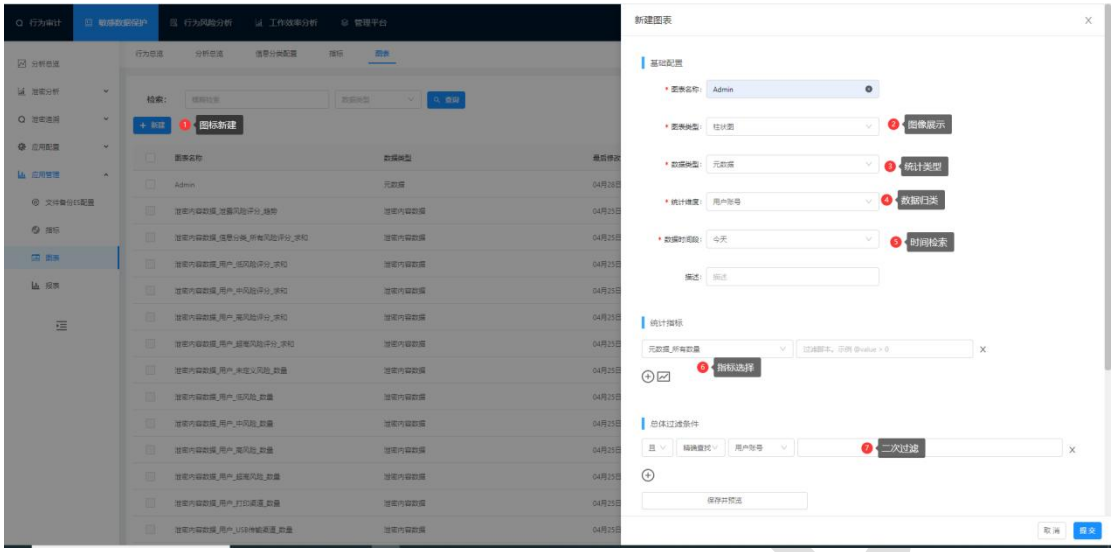
3. 数据类型：元数据和泄密内容数据和指标数据类型对应选择。

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。

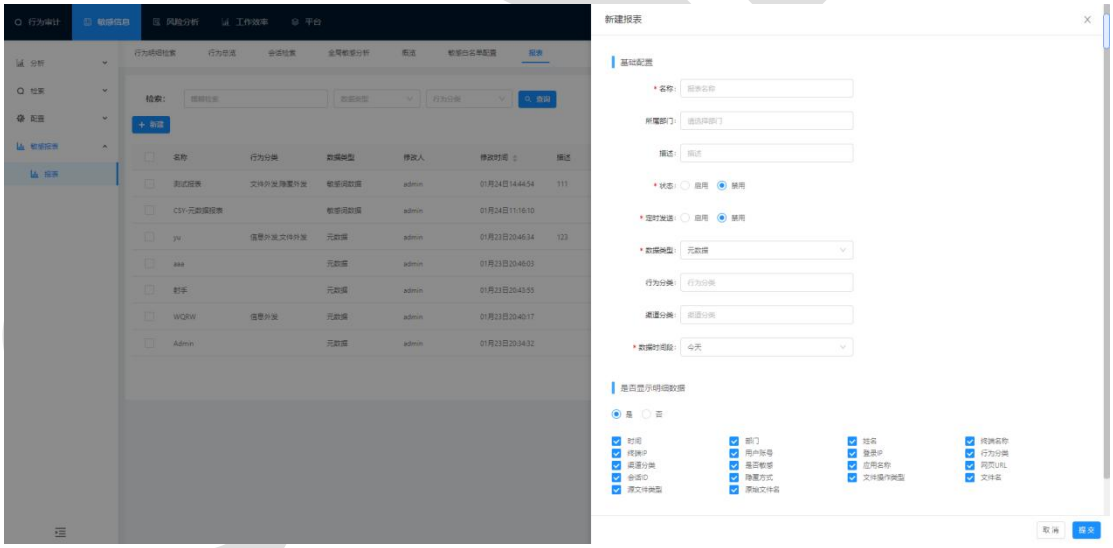
6. 统计指标：选择对应的指标，展示对应的筛选数据

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。

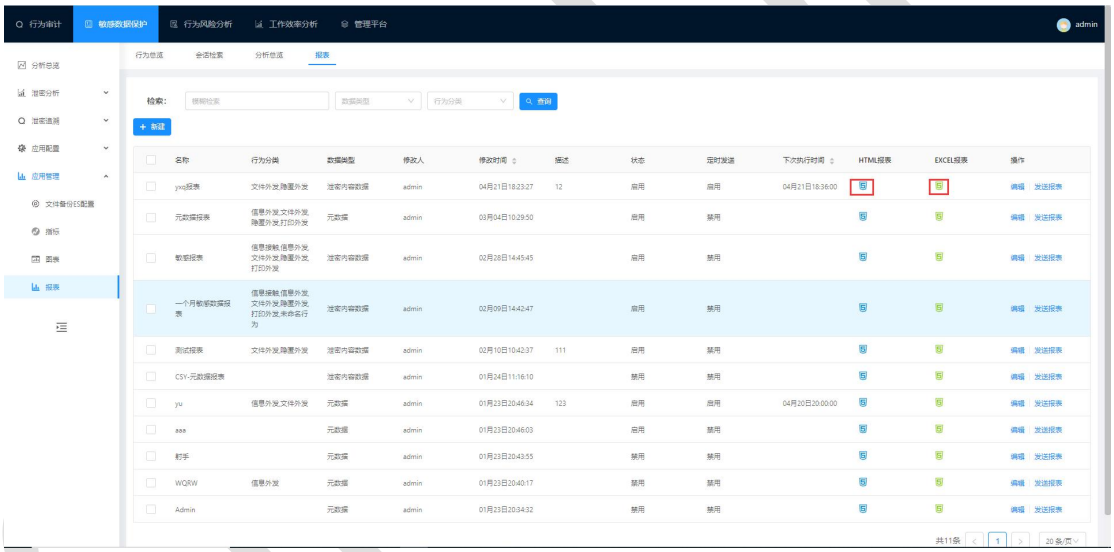
风险等级：敏感词数据中风险等级的筛选渠道。

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。



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。

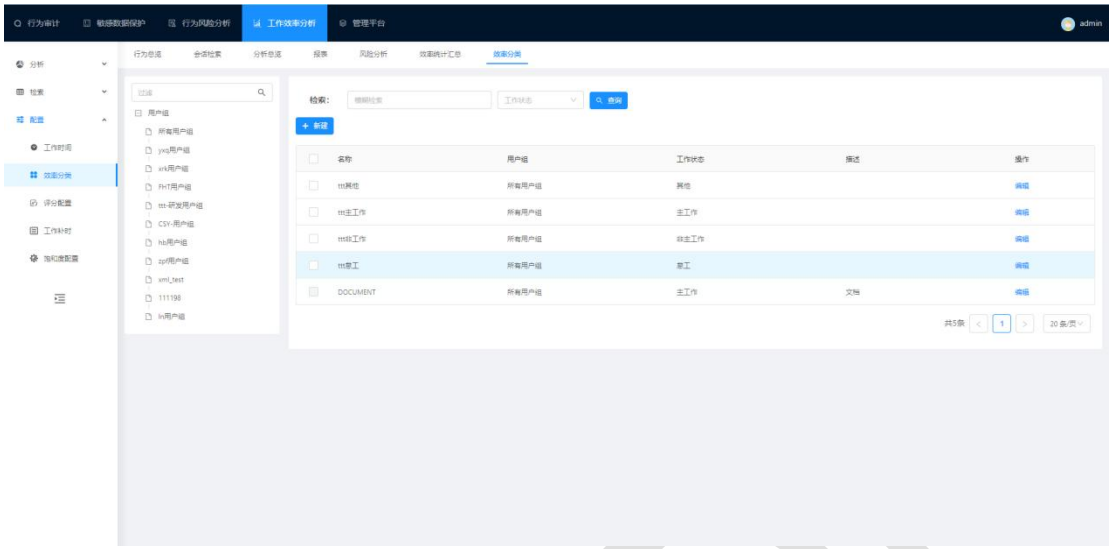
3.3 工作效率

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。

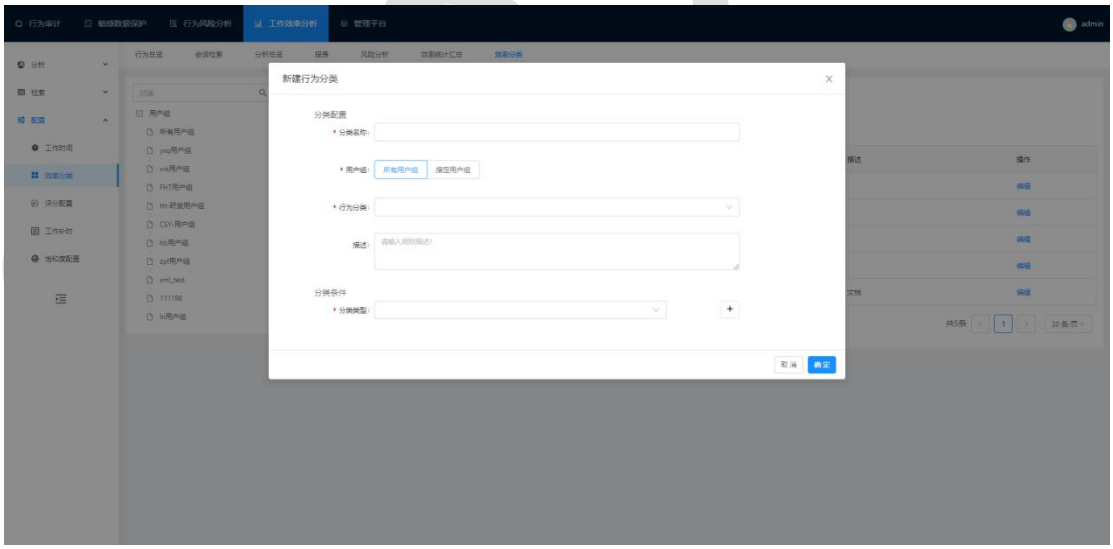
选择“配置>效率配置>效率分类”进入效率分类界面；可以选择用户组、模糊检索、工

作状态进行查询；如下图所示：



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：



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）。

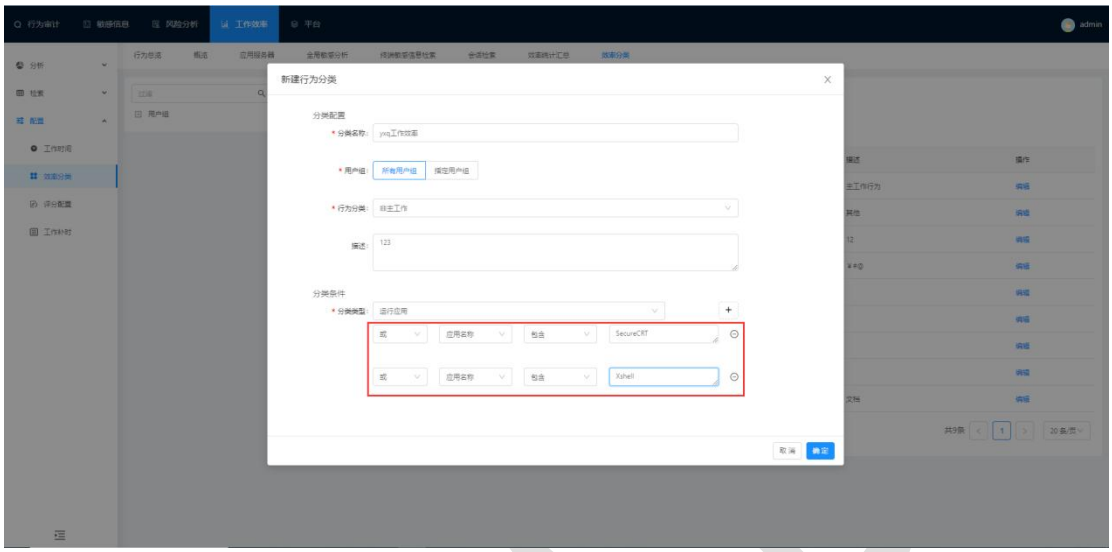
行为分类：主工作、非工作、其他、怠工行为。

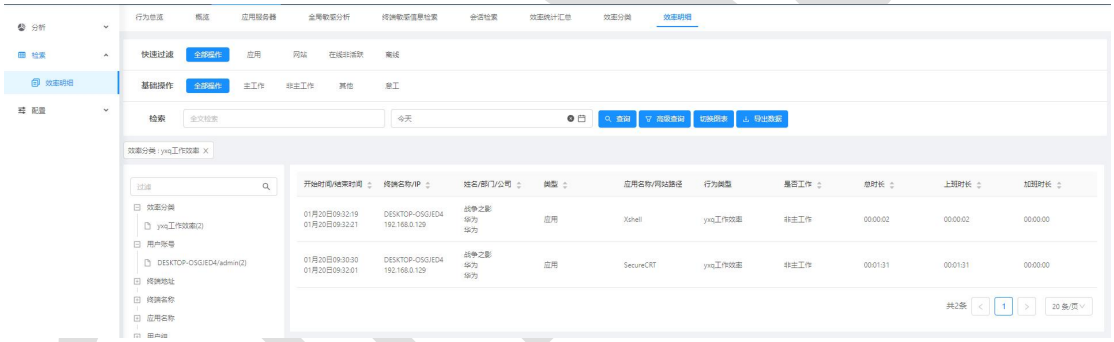
分类描述：分类的描述。

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”。





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：

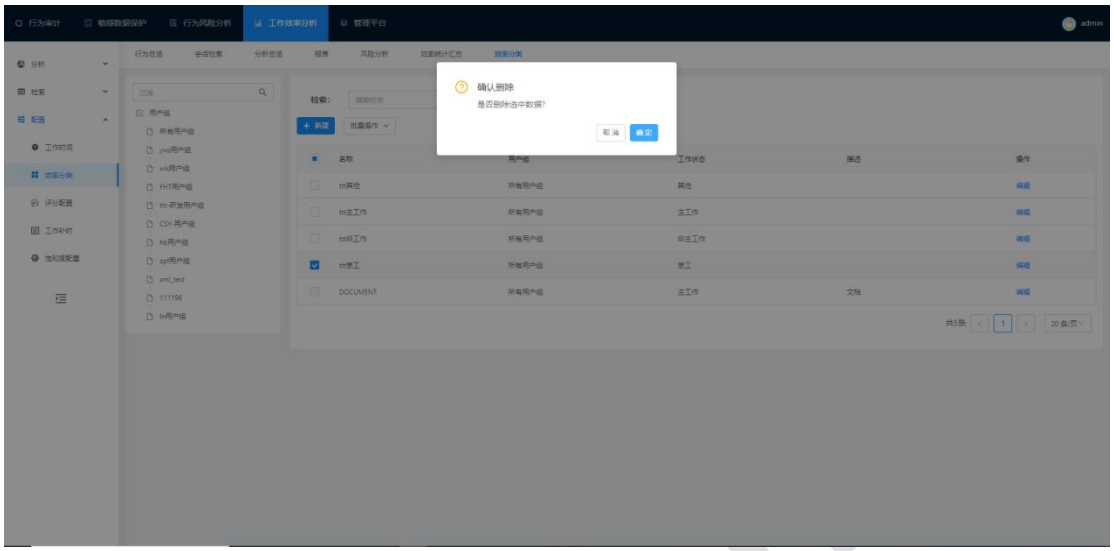
在...之内：是匹配数据集条件，当数据集内包含“QQ”。

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”。

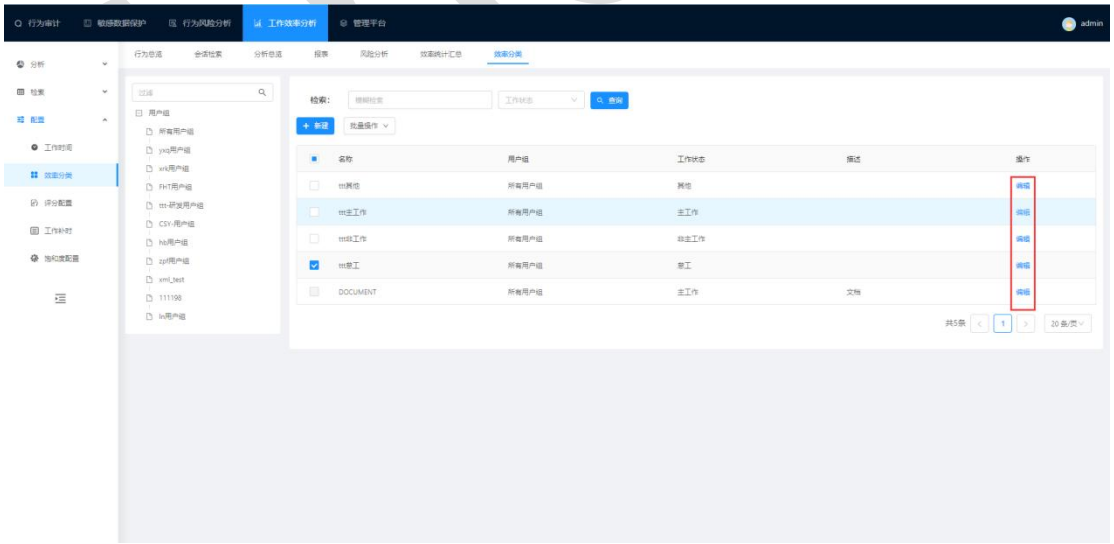
3.3.1.2 删除效率分类

选择要删除的分类，点击“删除”按钮删除分类。如下图所示：



3.3.1.3 编辑效率分类

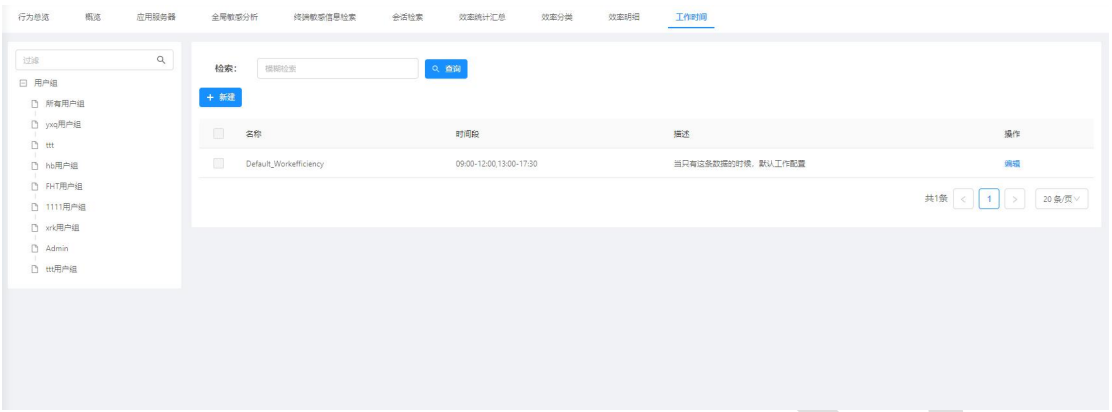
点击“编辑”按钮编辑效率分类。如下图所示：



3.3.2 工作时间配置

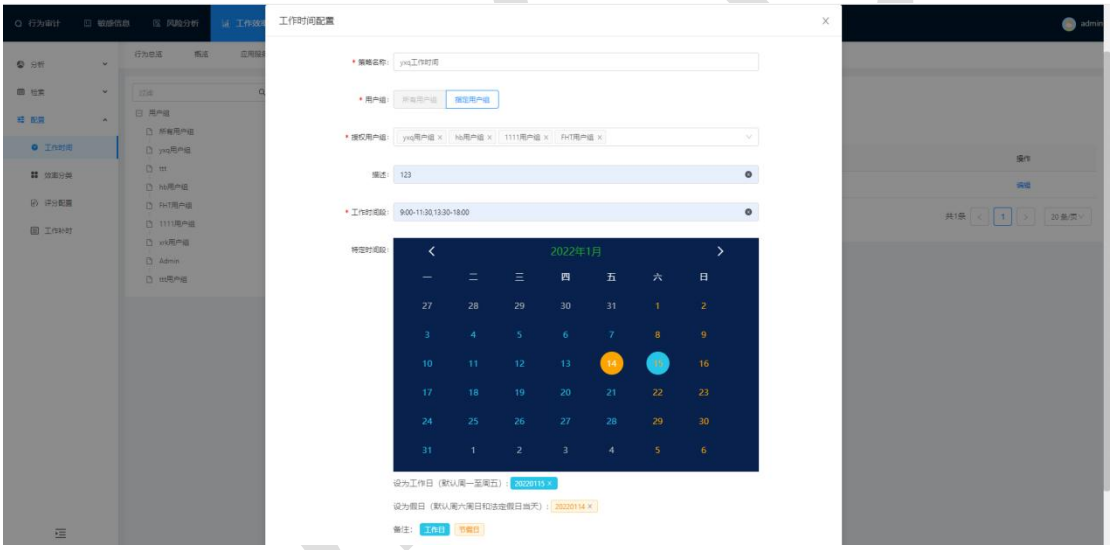
工作时间配置是配置用户在终端的上班工作的时长。

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）

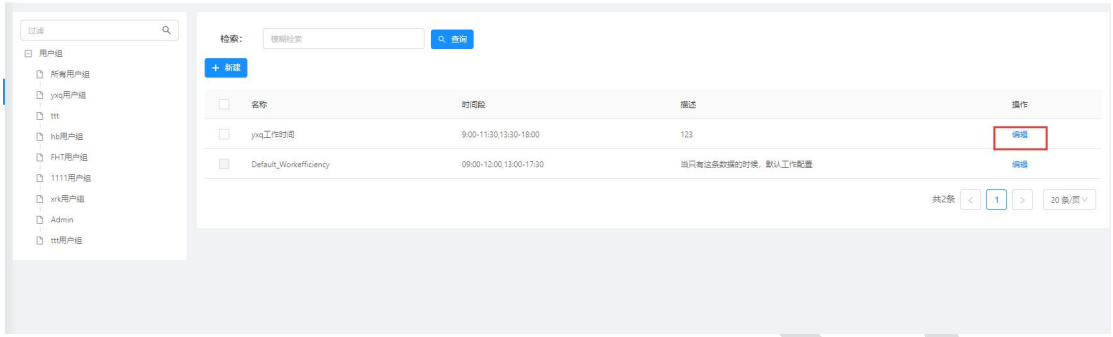
工作时间段：自定义上班工作时间段。

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：



3.3.2.3 删除工作时间配置

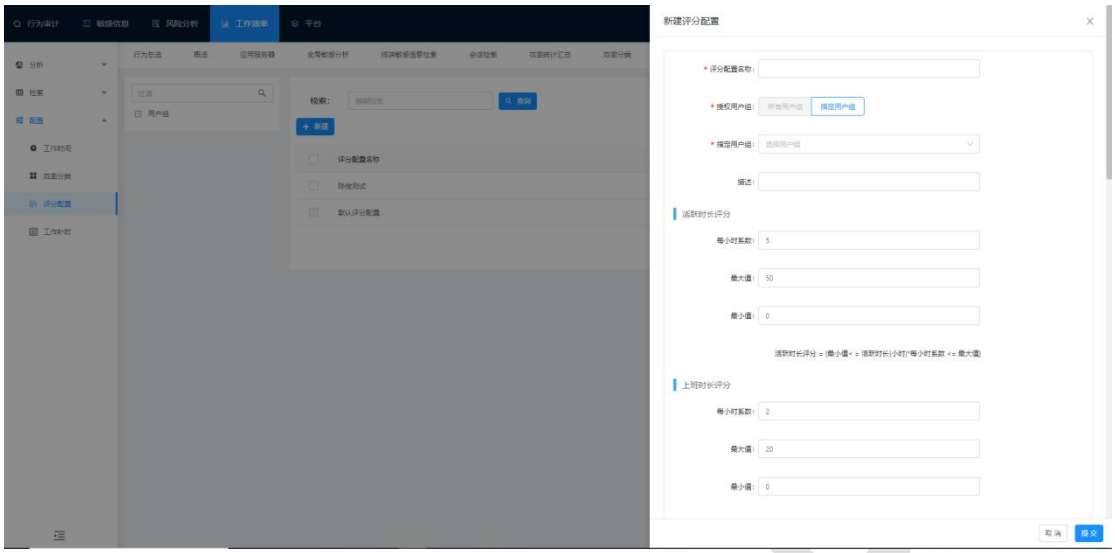
选择要删除的配置，点击“删除”按钮进行删除；已绑定用户组的配置被删除后，该用户组下的用户会自动使用默认工作时间配置；默认的工作时间配置不可删除；如下图所示：

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。

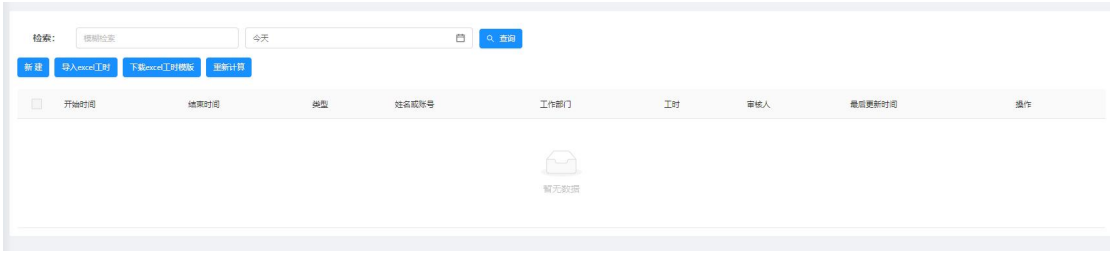
例如：计算下图的活跃时长评分：先把时长换算成小时约等于 5.83*评分配置活跃时长对应的每小时系数。

总评分计算：所有时长计算评分的结果相加*100/8

3.3.4 工作补时

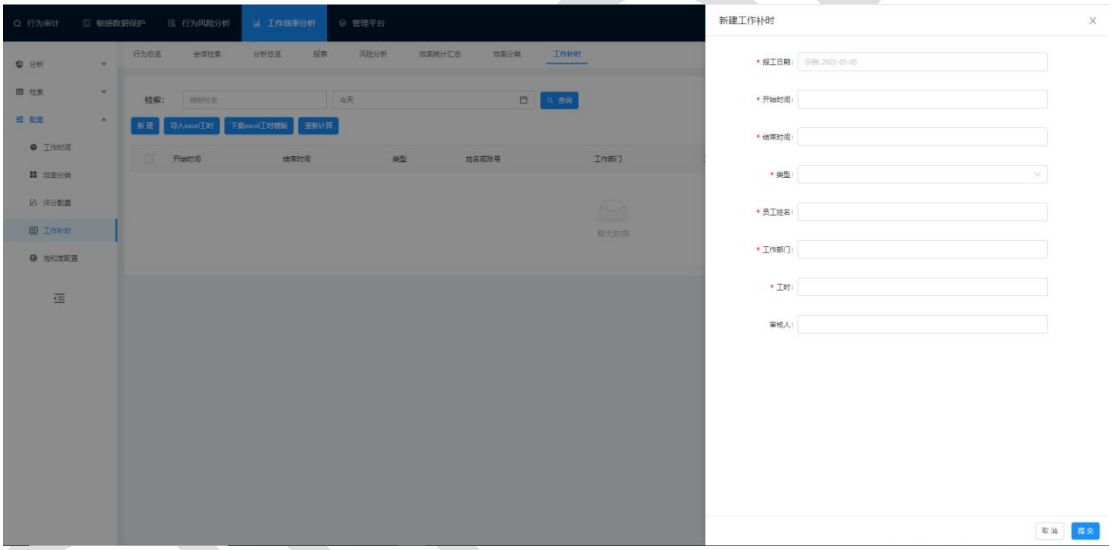
工作补时：当用户因其它工作未操作终端产生的非活跃时长，可以通过工作补时来进行补时清除非活跃时长。

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。

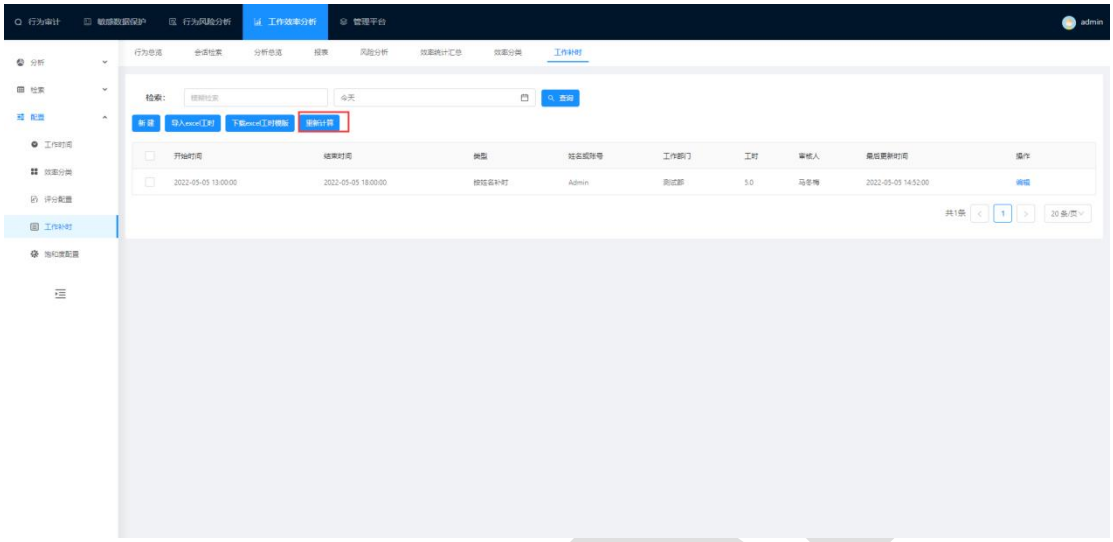
工时：计算要补时的时长；不足半小时也填写 0.5；

审核人：填写审核人信息

3.3.4.2 重新计算

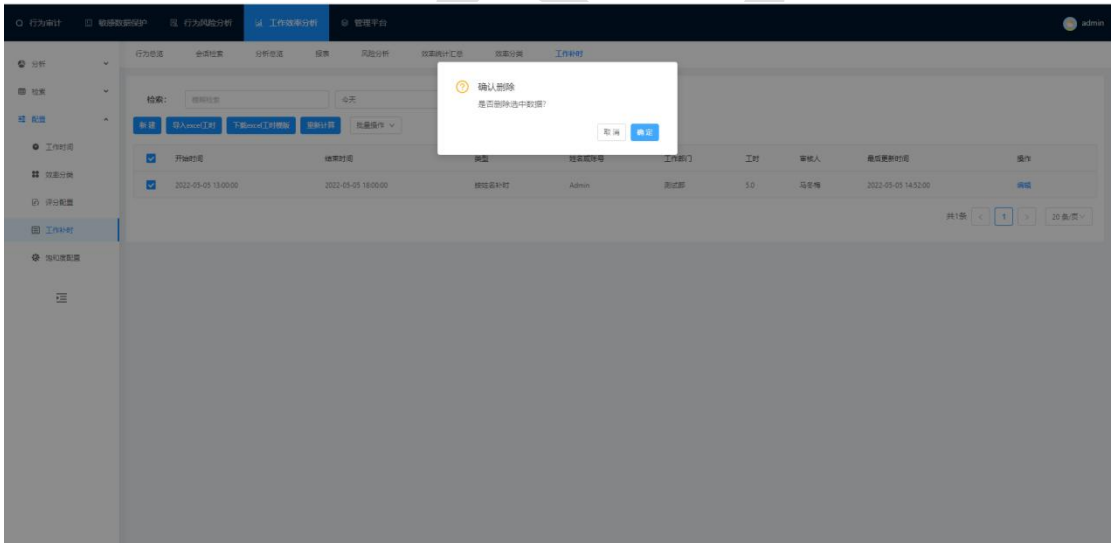
点击“重新计算”按钮；去效率明细查看此用户的所补时时间段的非活跃记录是否补时

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。



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：



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。

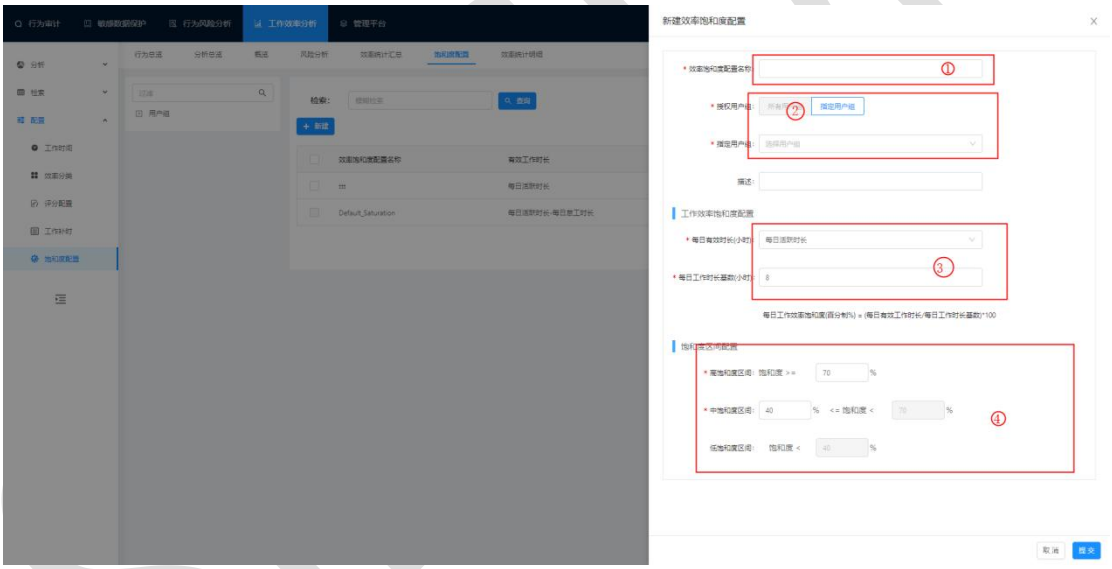
2：指定用户组：全部用户组为所有用户组将以此饱和度设置计算饱和度。

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%；

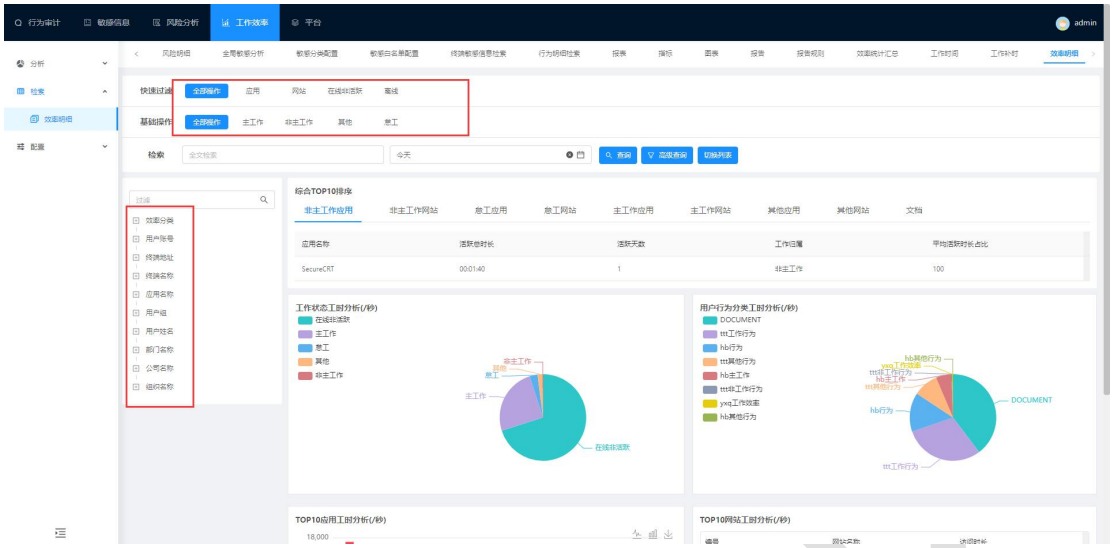
4：饱和度区间设置：设置的饱和度区间决定该区间内对应的饱和度等级。饱和度区间最大值为 100；最小值为 1。



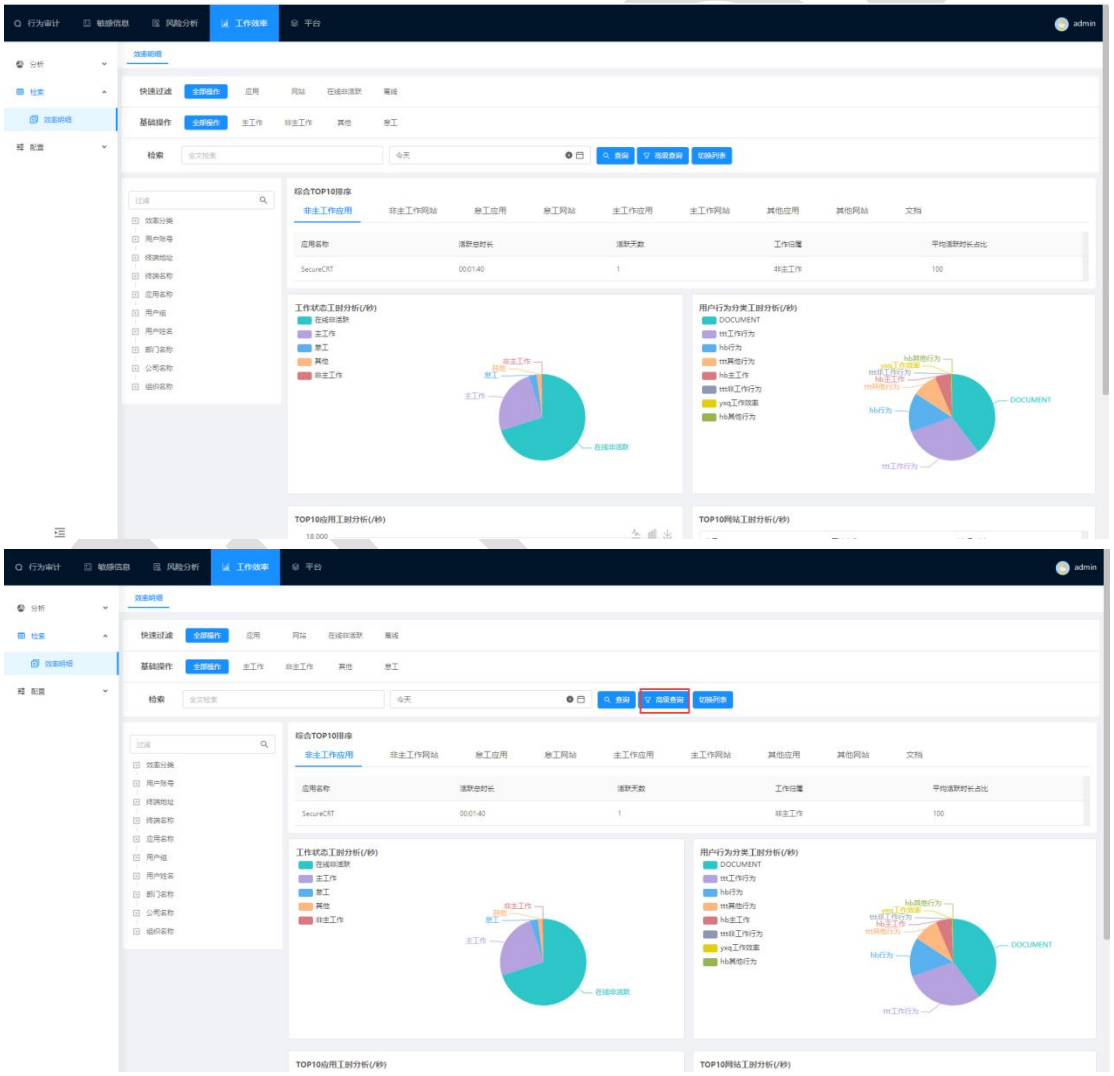
3.3.6 效率检索明细

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：



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：



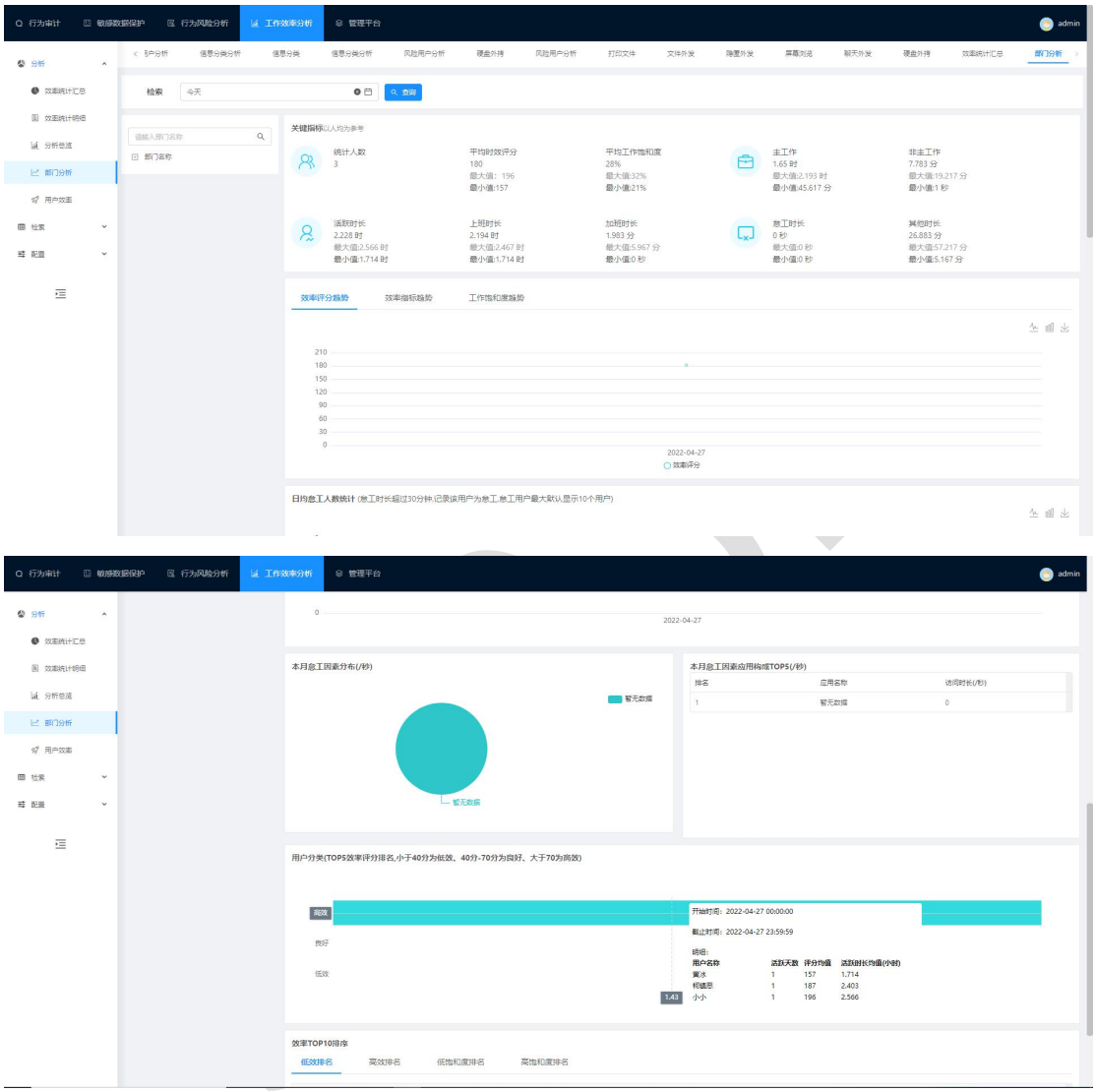
注 1：非活跃数据需要去 Windows 记录策略的工作效率分析规则配置待机时长，默认是 120 秒；当终端超过 120 秒没有作任何操作，就会产生一条非活跃记录（非活跃时长=实际待机时长-120）。

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。

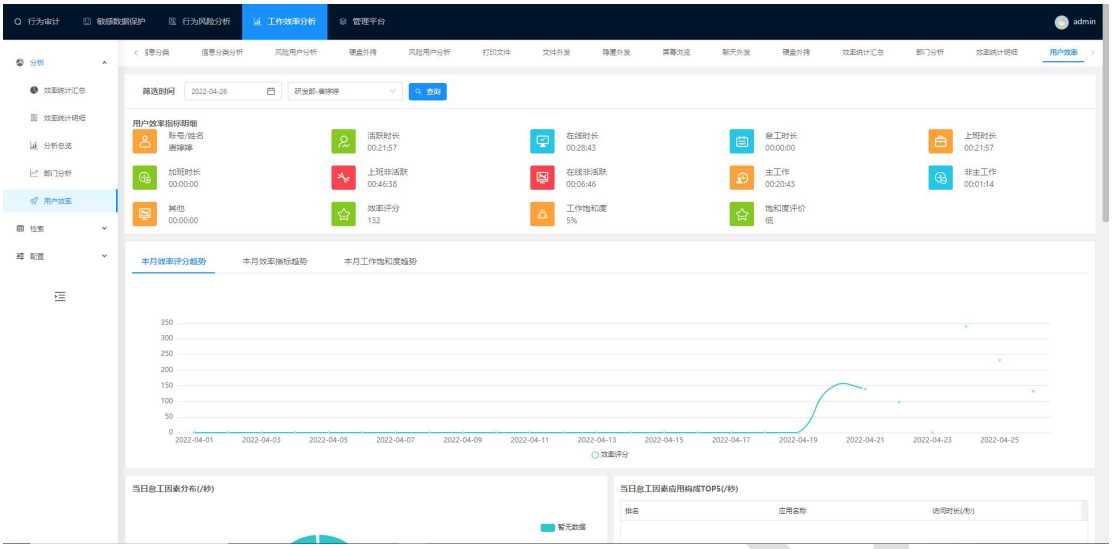
选择“分析>工作效率>部门效率分析”进入部门效率分析界面，如下图所示：



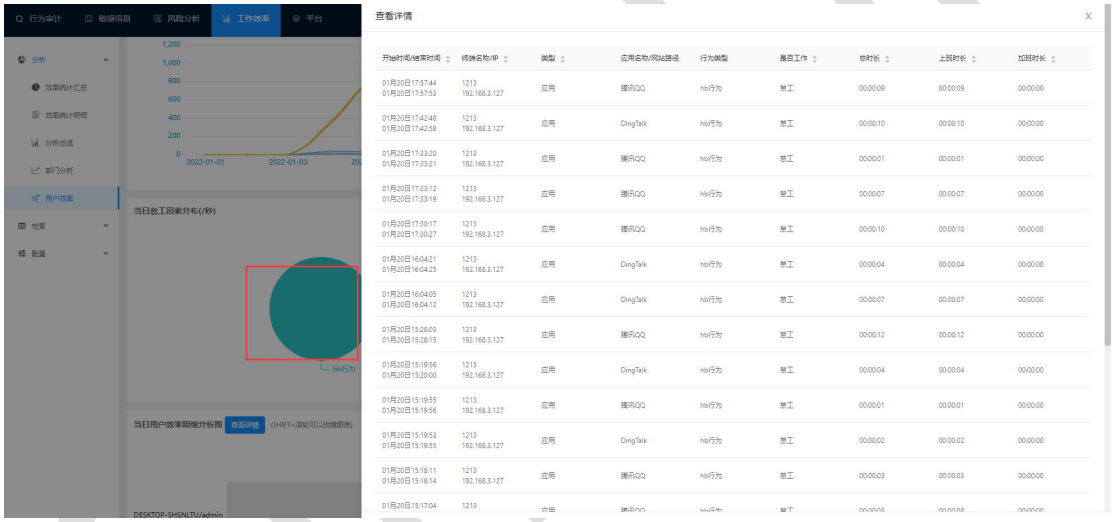
3.3.8 用户效率

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：



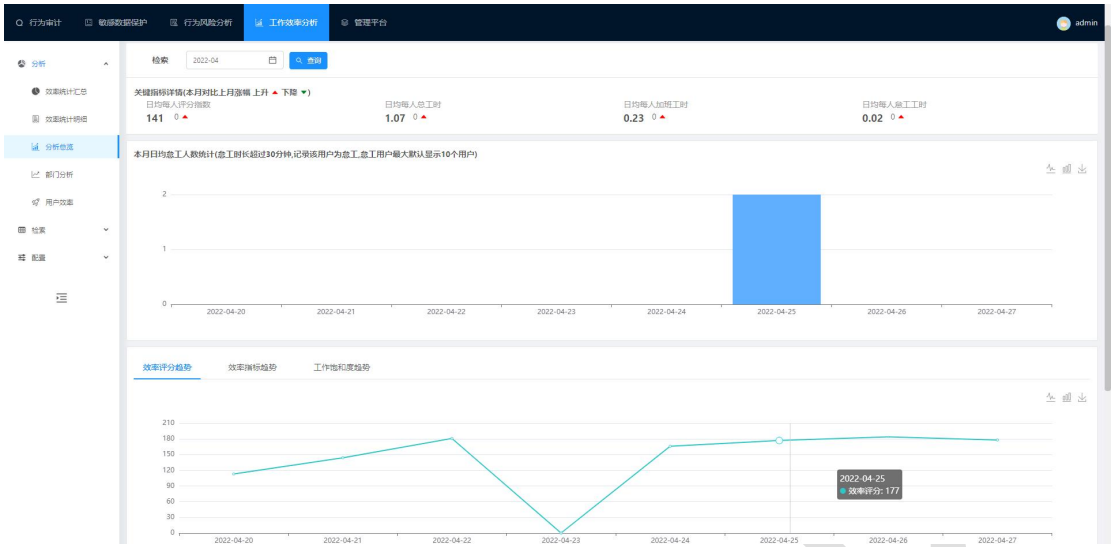
点击相应工时数据可以弹出效率明细详情窗口查看详情；例如：用户行为分类工时分析，点击要查看的行为分类饼图查看详情；如下图所示：



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：

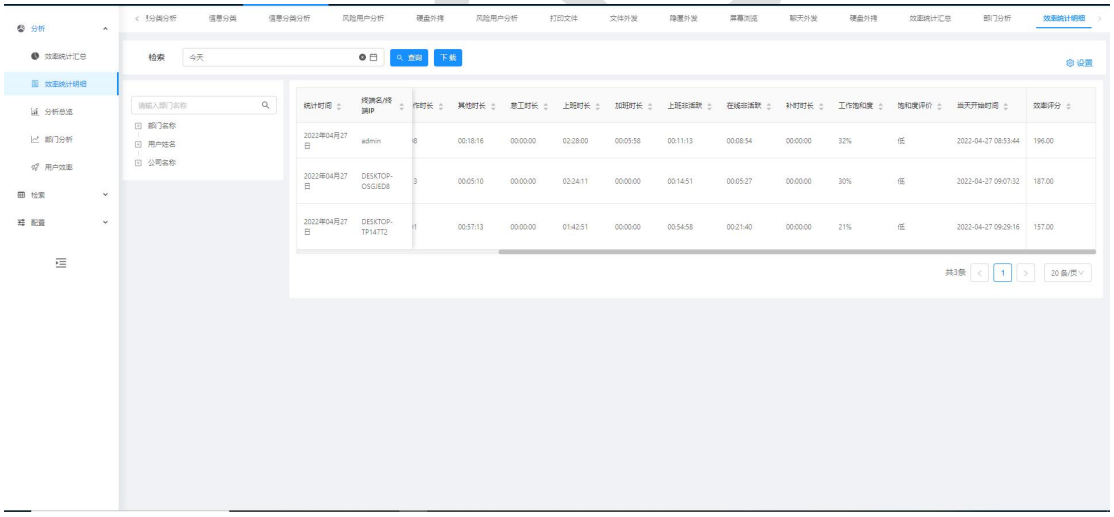


3.3.10 效率统计明细

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：



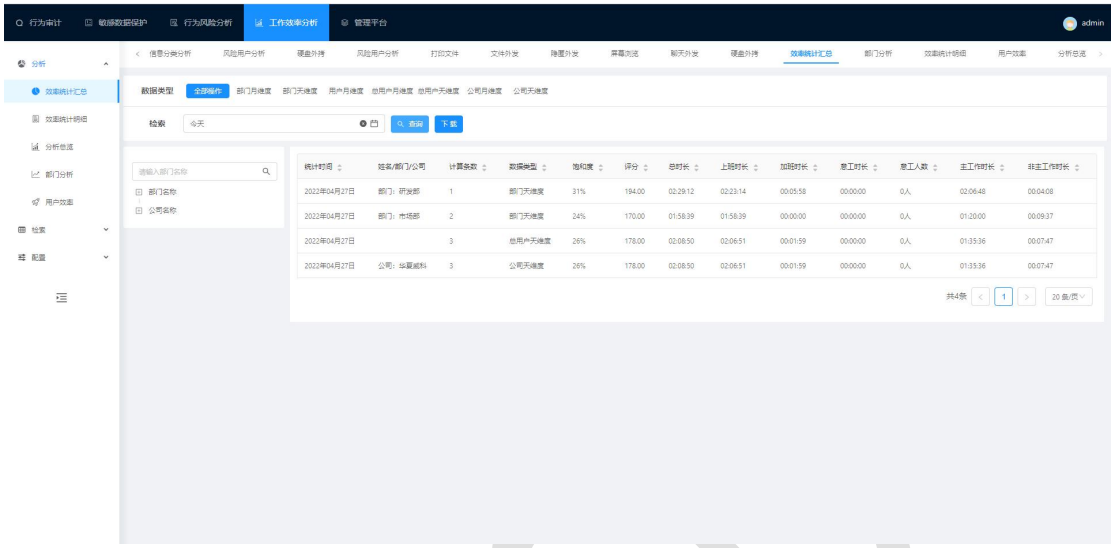
3.3.11 效率明细汇总

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：



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=工作时间配置时间段内离线时长之和。

加班时长=工作时间配置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。

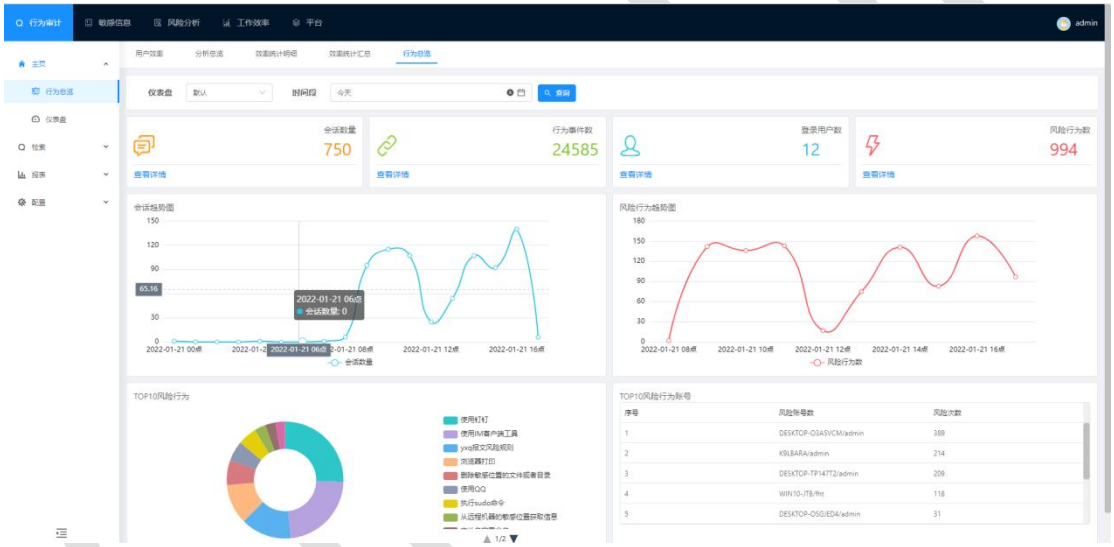
公司天维度：统计公司的当天效率汇总的平均值。

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。

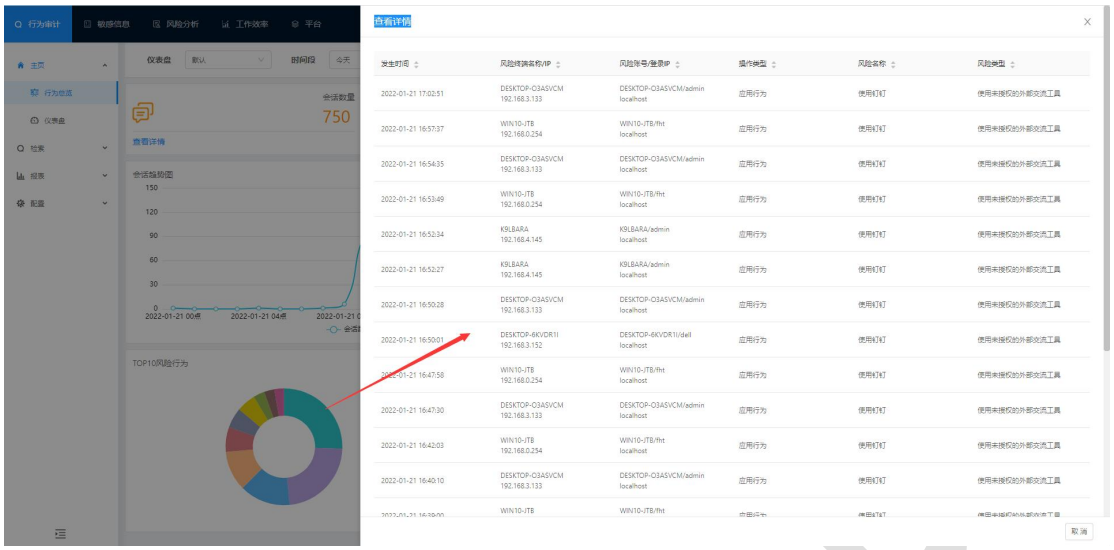
点击“主页”按钮，进入主页查看详情；如下图所示：



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

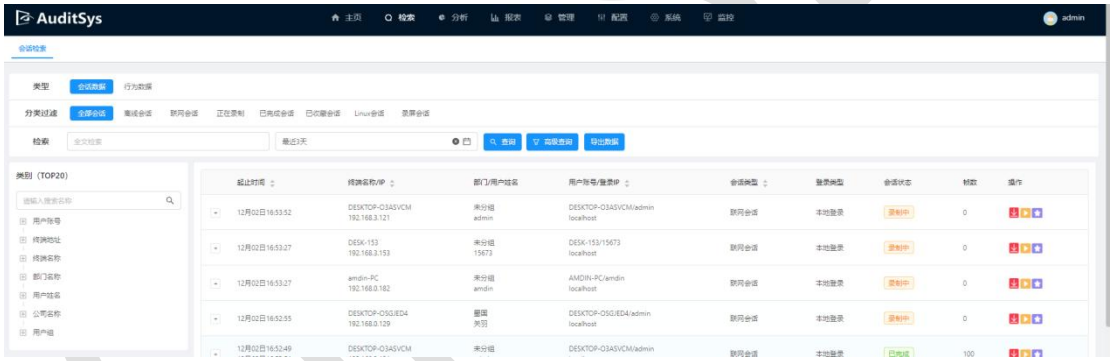
可点击“查看详情”按钮查看对应数据相应；也可以点击趋势图和图表查看数据详情；如下图所示：



4.2 会话检索

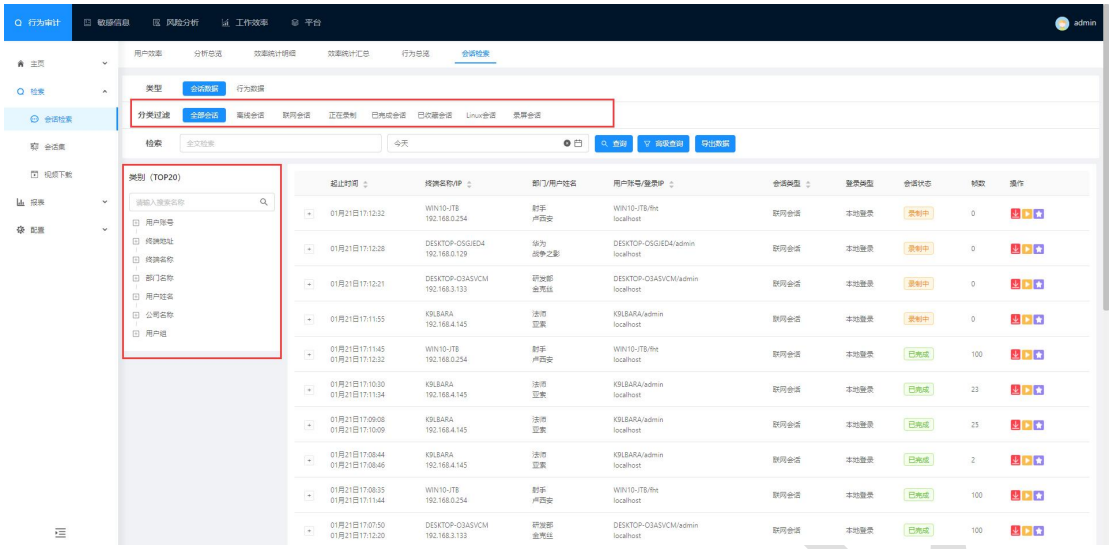
会话检索是录制用户在终端操作行为进行审计记录。

选择“检索>会话检索”进入会话检索界面；如下图所示：

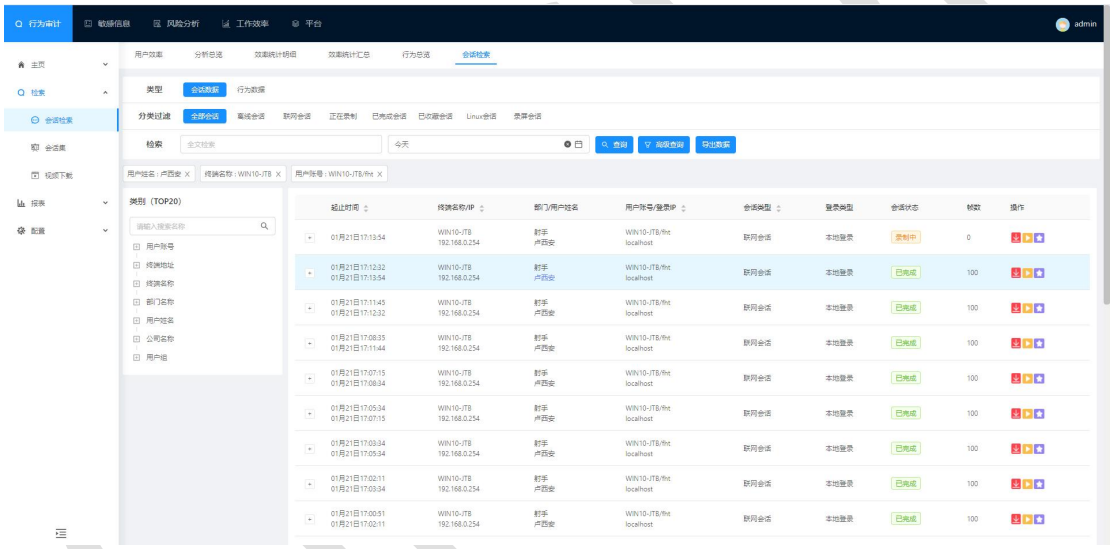


4.2.1 会话查询

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：



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

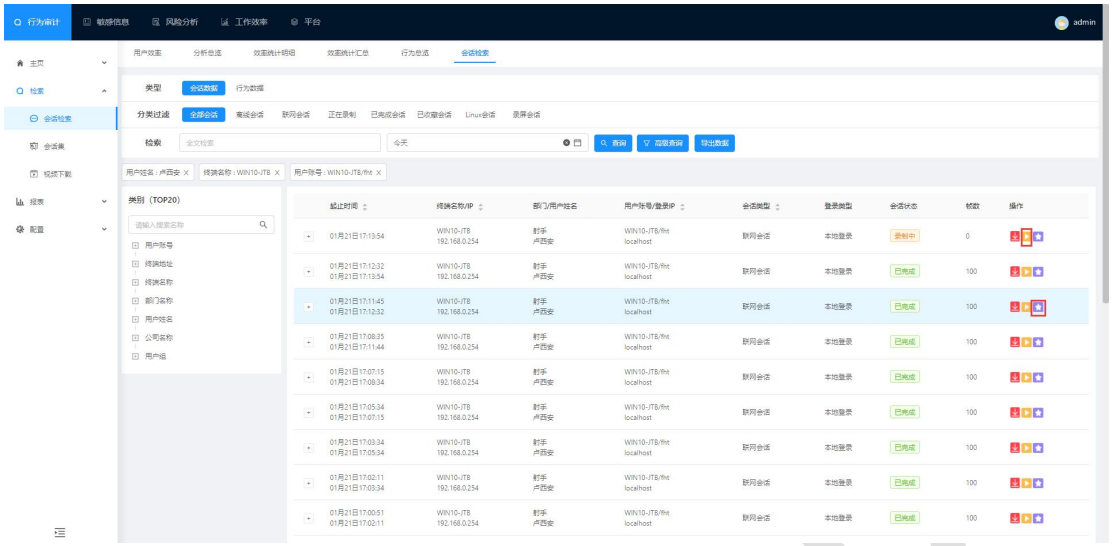


4.2.2 会话播放

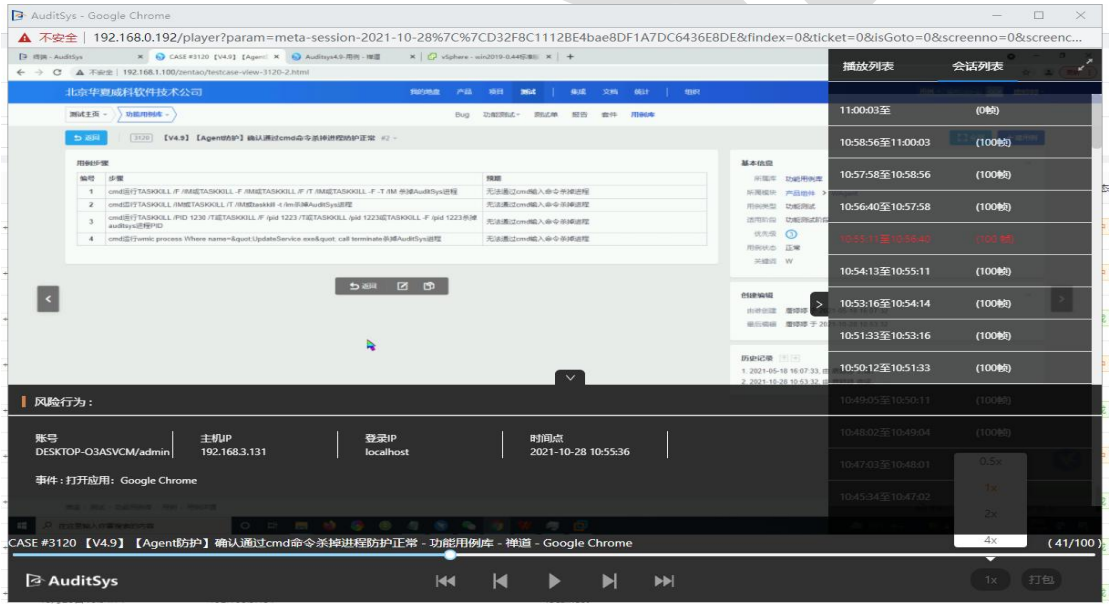
单屏会话：点击“ ”按钮进行播放。

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：

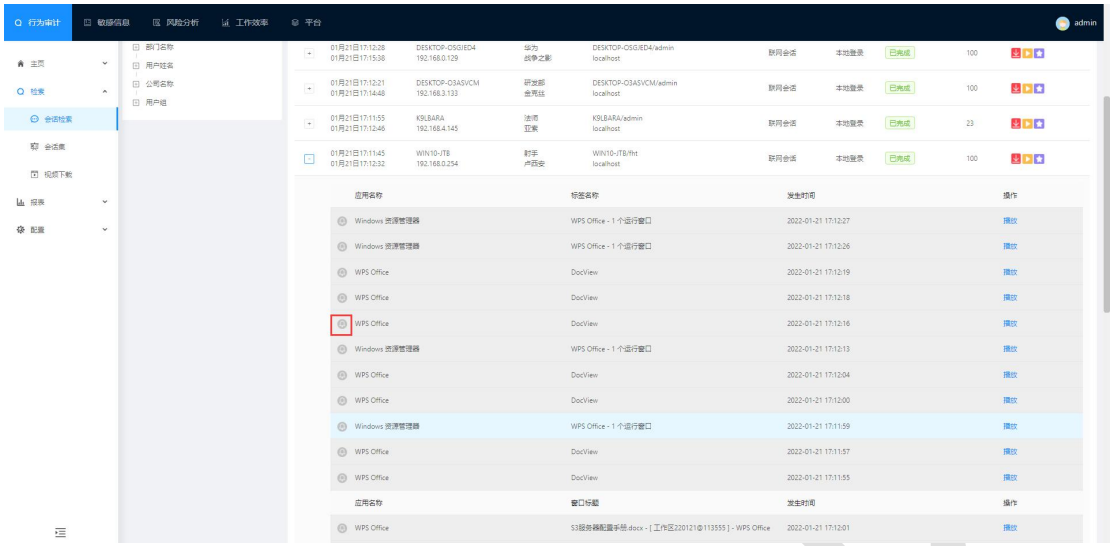


播放画面：点击  可以查看按键事件信息；点击  拉出播放列表信息和会话列表信息，可以选择播放列表信息进行播放，也可以选择会话列表信息进行播放；还可以选择播放倍速；点击  播放上一个会话；点击  播放下一个会话；点击  播放上一帧；点击  播放下一帧；点击  开始播放；点击“打包”按钮可以进行视频下载。如下图所示：



4.2.3 会话明细

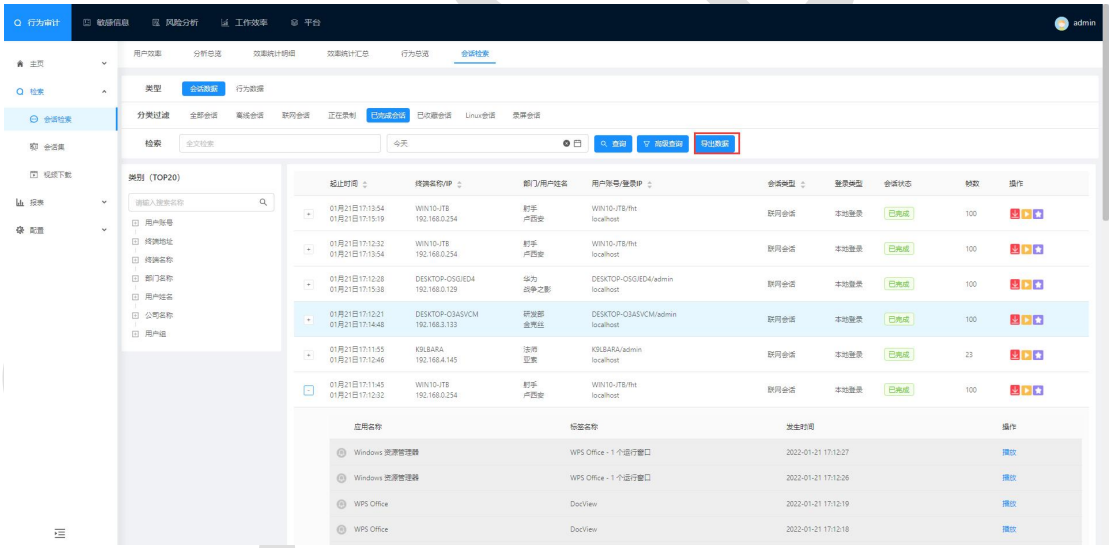
点击“+”按钮可以展开查看会话明细。带“  ”是该会话明细存在风险行为；会话明细中“播放”按钮，可以直接播放到该事件的帧位置画面。如下图所示：



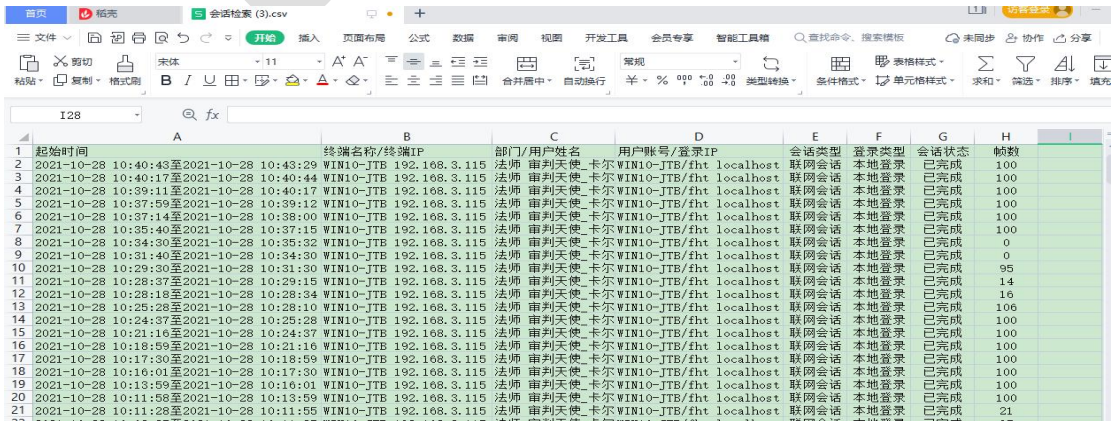
4.2.4 导出数据

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：



导出数据以 excel 文档格式显示，如下图所示：

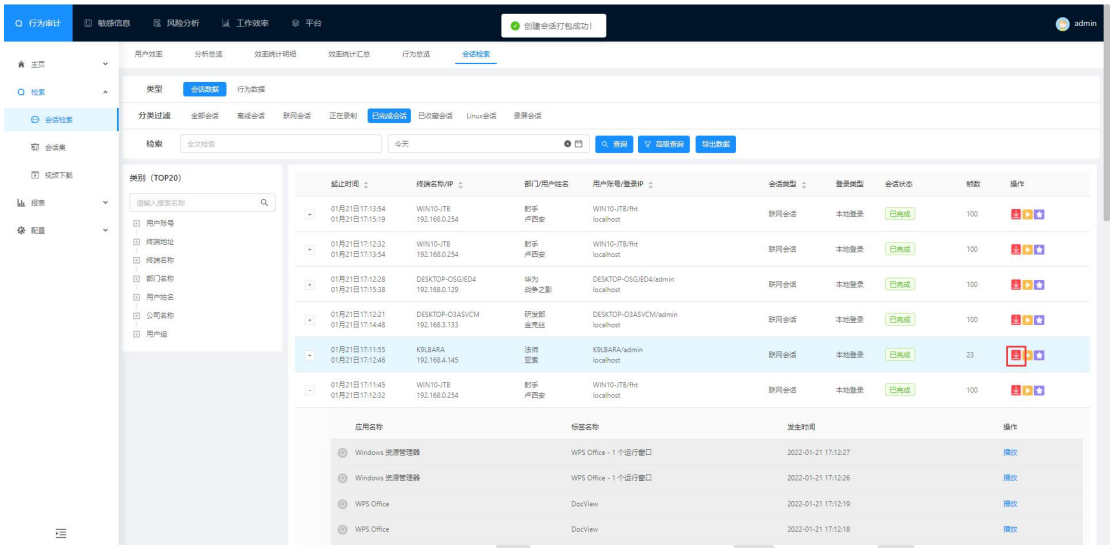


	A	B	C	D	E	F	G	H
1	起始时间	终端名称/终端IP	部门/用户姓名	用户账号/登录IP	会话类型	登录类型	会话状态	帧数
2	2021-10-28 10:40:43至2021-10-28 10:43:29	WIN10-JTB 192.168.3.115	法师 审判天使_卡尔	WIN10-JTB/fht localhost	联网会话	本地登录	已完成	100
3	2021-10-28 10:40:17至2021-10-28 10:40:44	WIN10-JTB 192.168.3.115	法师 审判天使_卡尔	WIN10-JTB/fht localhost	联网会话	本地登录	已完成	100
4	2021-10-28 10:39:11至2021-10-28 10:40:17	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
5	2021-10-28 10:37:59至2021-10-28 10:39:12	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
6	2021-10-28 10:37:14至2021-10-28 10:38:00	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
7	2021-10-28 10:35:40至2021-10-28 10:37:15	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
8	2021-10-28 10:34:30至2021-10-28 10:35:32	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	0
9	2021-10-28 10:31:40至2021-10-28 10:34:30	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	0
10	2021-10-28 10:29:30至2021-10-28 10:31:30	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	95
11	2021-10-28 10:28:37至2021-10-28 10:29:15	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	14
12	2021-10-28 10:28:18至2021-10-28 10:28:34	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	16
13	2021-10-28 10:25:28至2021-10-28 10:28:10	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	106
14	2021-10-28 10:24:37至2021-10-28 10:25:28	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
15	2021-10-28 10:21:16至2021-10-28 10:24:37	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
16	2021-10-28 10:18:59至2021-10-28 10:21:16	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
17	2021-10-28 10:17:30至2021-10-28 10:18:59	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
18	2021-10-28 10:16:01至2021-10-28 10:17:30	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
19	2021-10-28 10:13:59至2021-10-28 10:16:01	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
20	2021-10-28 10:11:58至2021-10-28 10:13:59	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
21	2021-10-28 10:11:28至2021-10-28 10:11:55	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	21

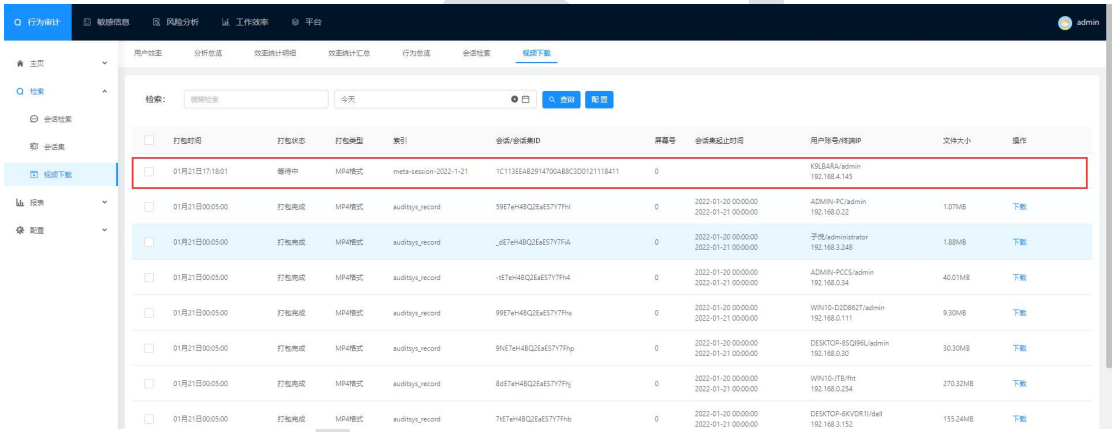
4.3.5 视频下载

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：



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：



4.3 行为数据

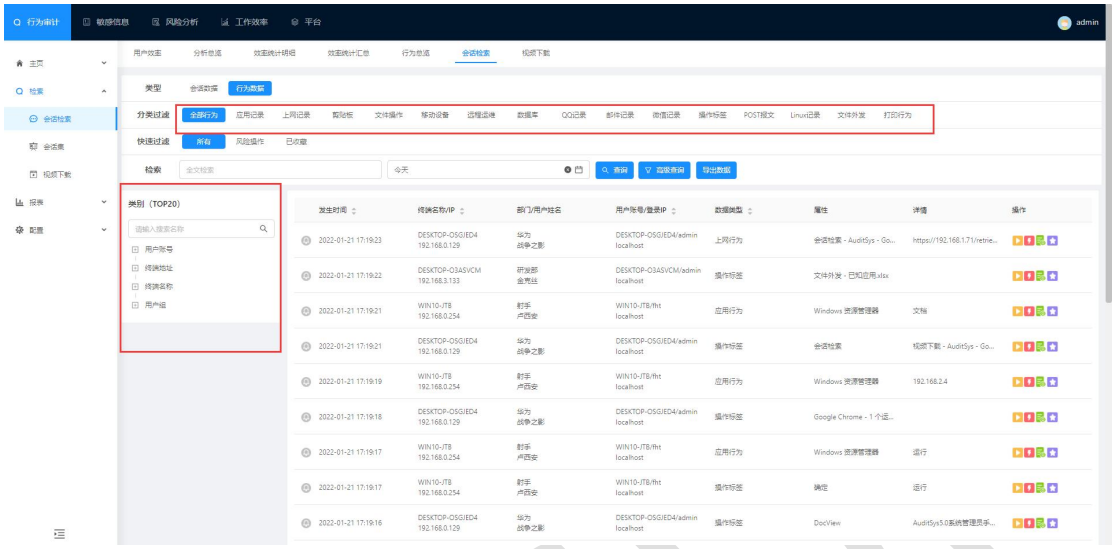
行为数据：对终端的操作所有行为审计记录。

全部行为：对终端的操作所有行为审计记录。

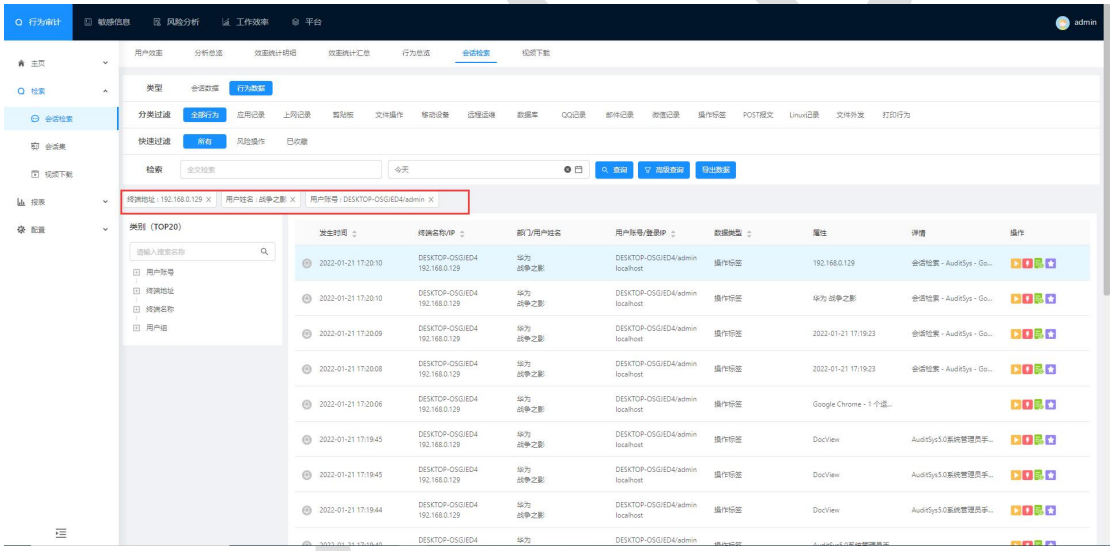
4.3.1 行为数据查询

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：

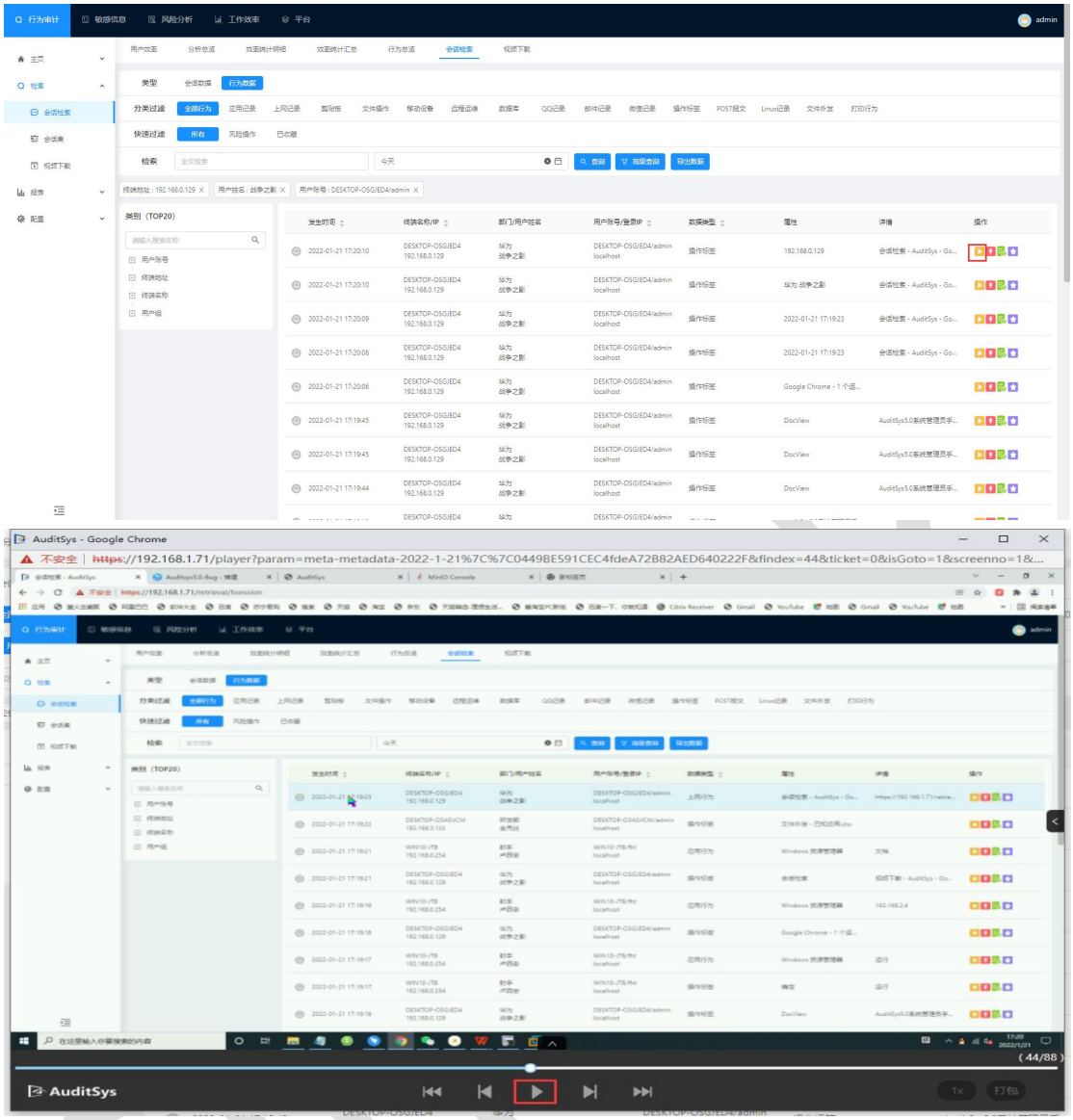


点击会话检索内容的‘终端名称/IP、部门/用户姓名、用户账号/登录 IP’也可以查询；如下图所示：



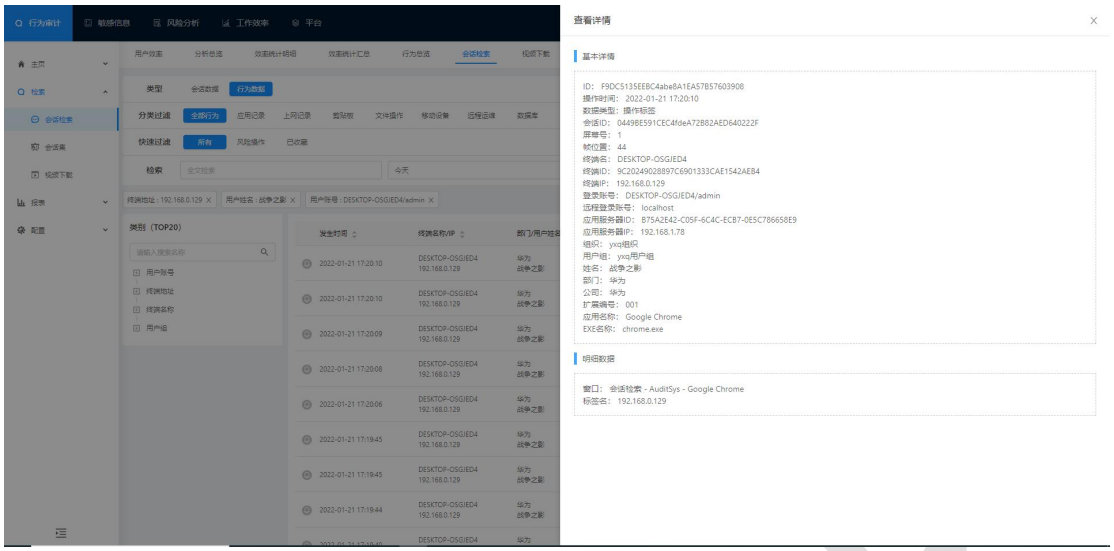
4.3.2 行为数据播放

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：



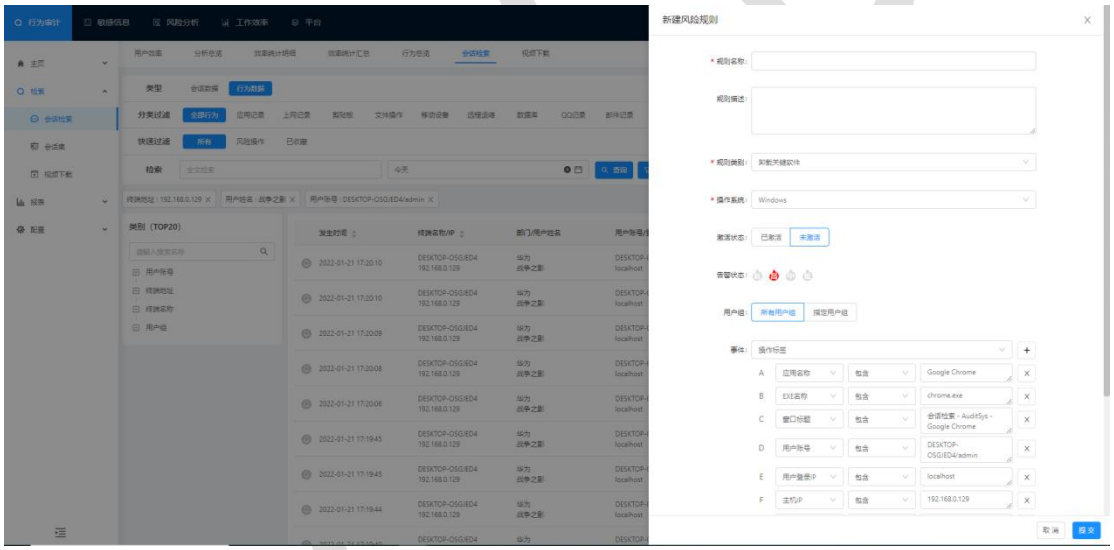
4.3.3 行为数据明细

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：



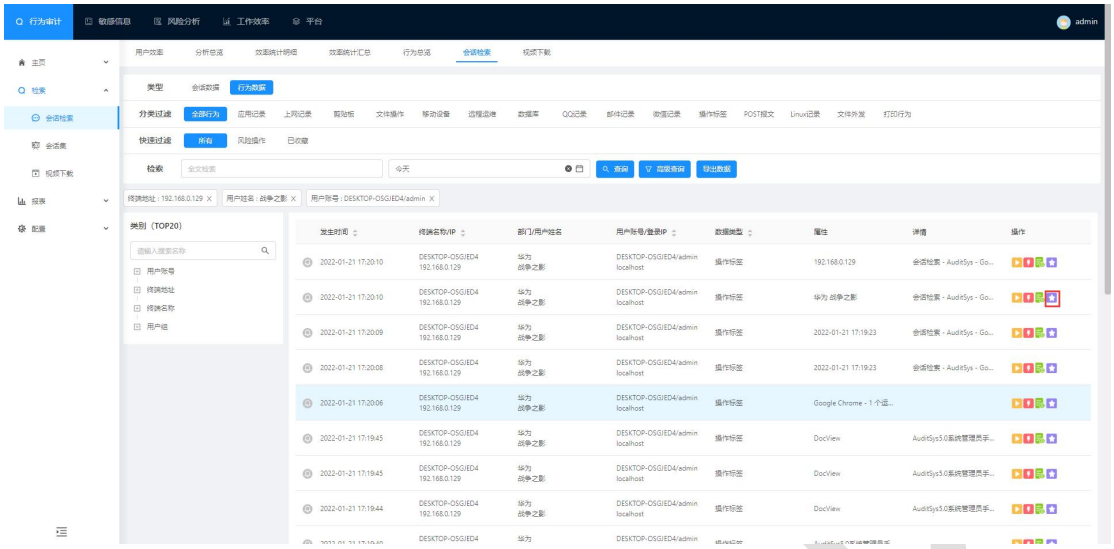
4.3.4 快捷新建风险规则

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

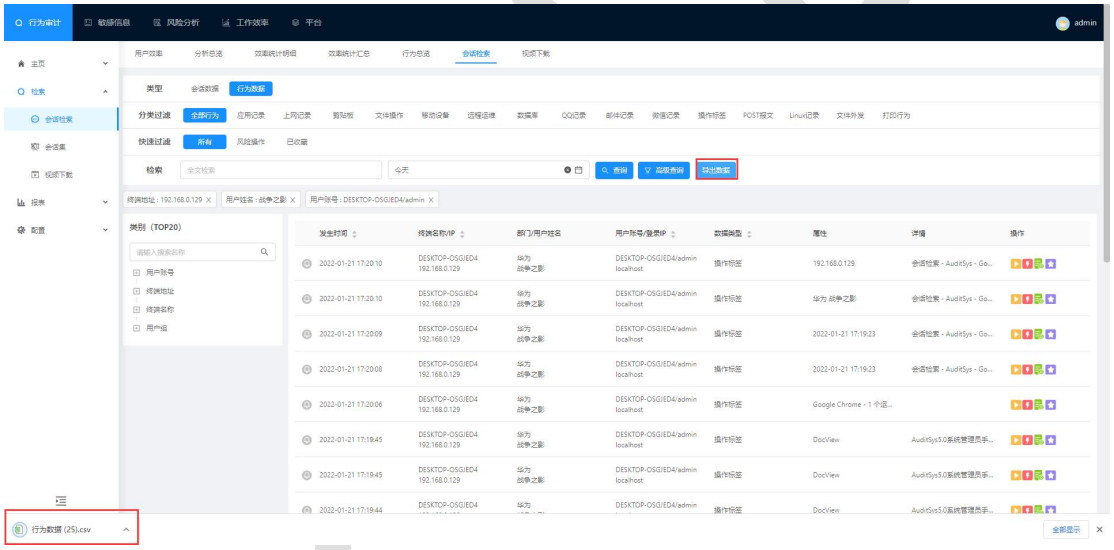
点击‘ ’按钮，可以对此行为数据进行收藏，点击‘ ’按钮取收藏；如下图所示：



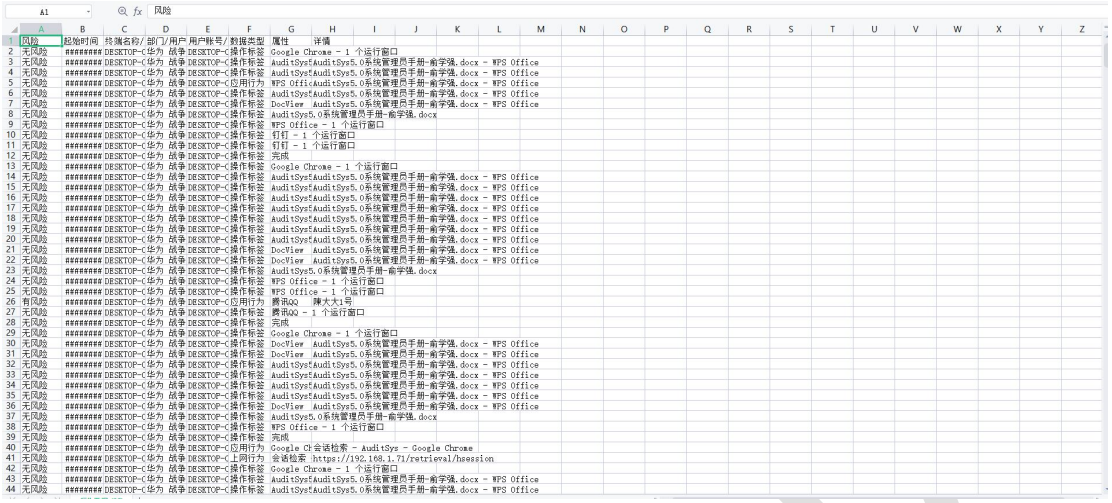
4.3.6 导出数据

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：

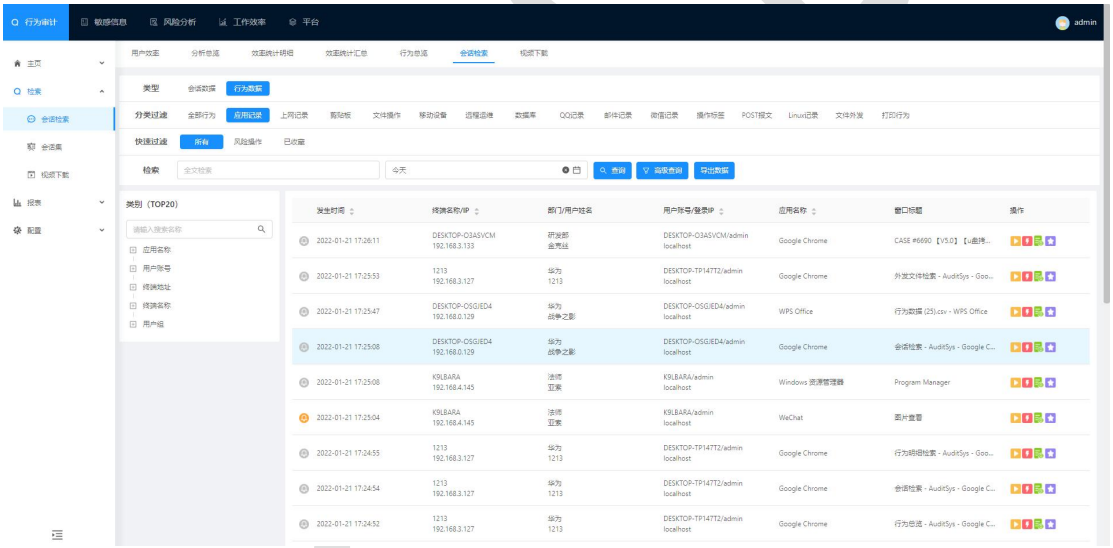


导出数据以 excel 文档格式显示，如下图所示：



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。



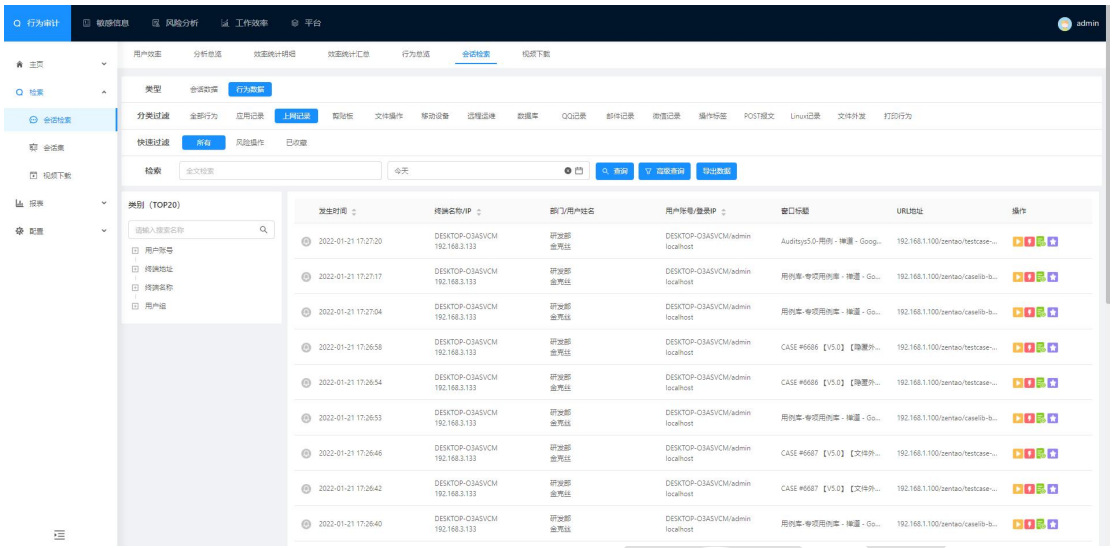
应用记录的查询、播放、创建风险规则、明细、收藏、导出数据等操作请借鉴全部行为步骤4.3.1-->4.3.6。

。

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。

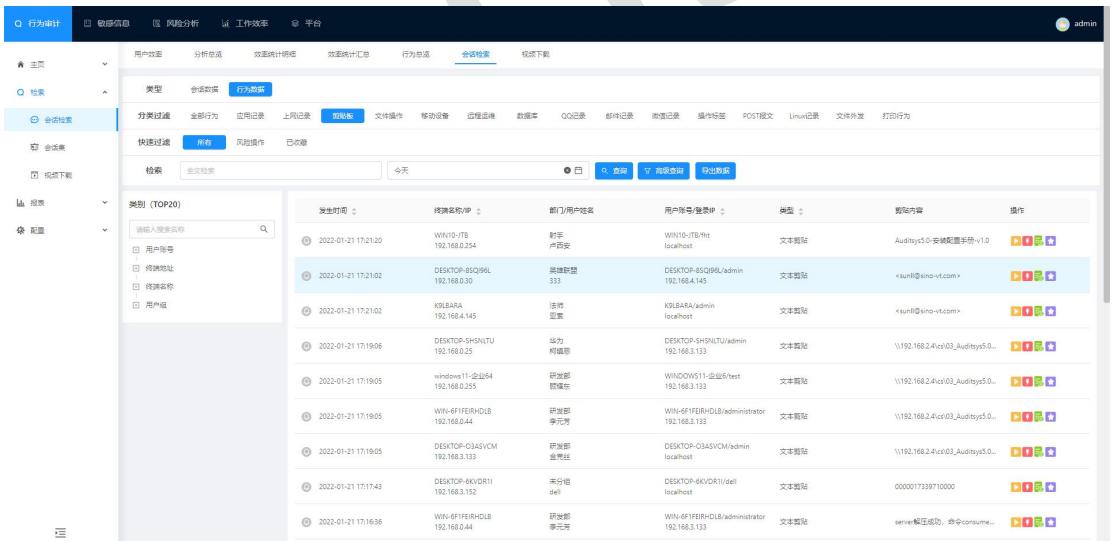


上网记录的查询、播放、创建风险规则、明细、收藏、导出数据等操作请借鉴全部行为步骤 4.3.1-->4.3.6。

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。

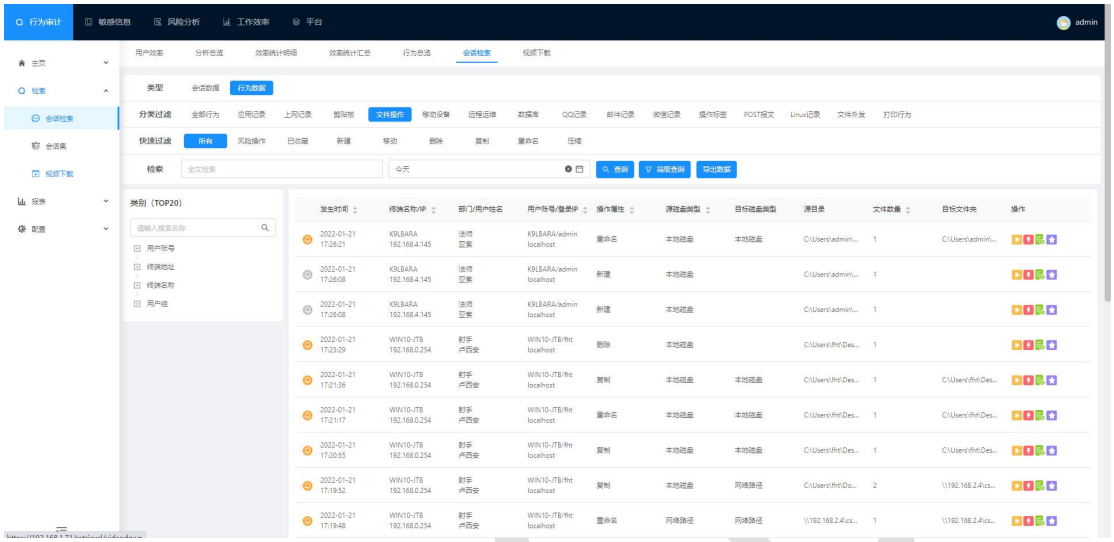


剪切板的查询、播放、创建风险规则、明细、收藏、导出数据等操作请借鉴全部行为步骤 4.3.1-->4.3.6。

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。

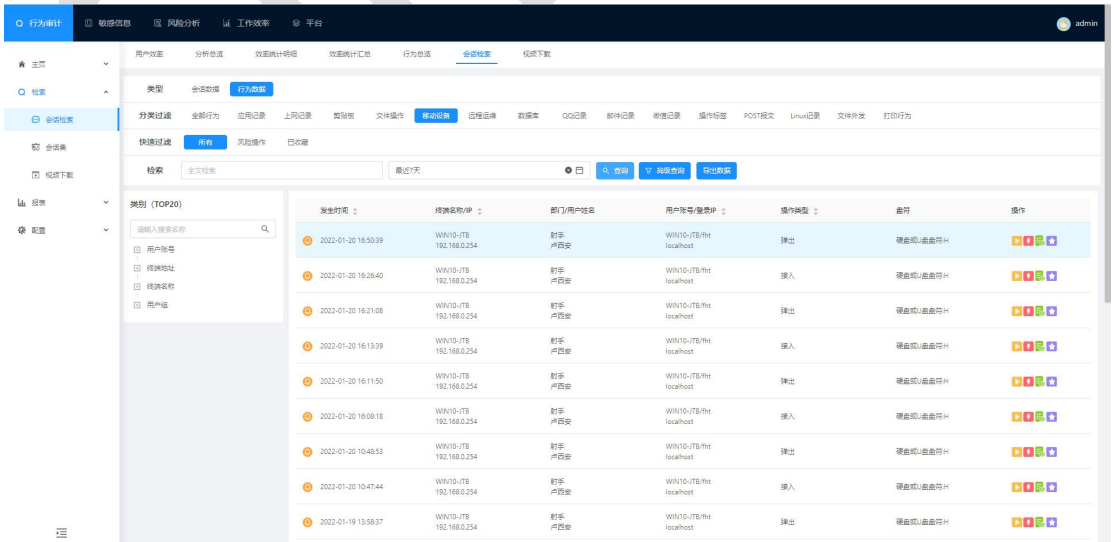


文件操作的查询、播放、创建风险规则、明细、收藏、导出数据等操作请借鉴全部行为步骤 4.3.1-->4.3.6。

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。

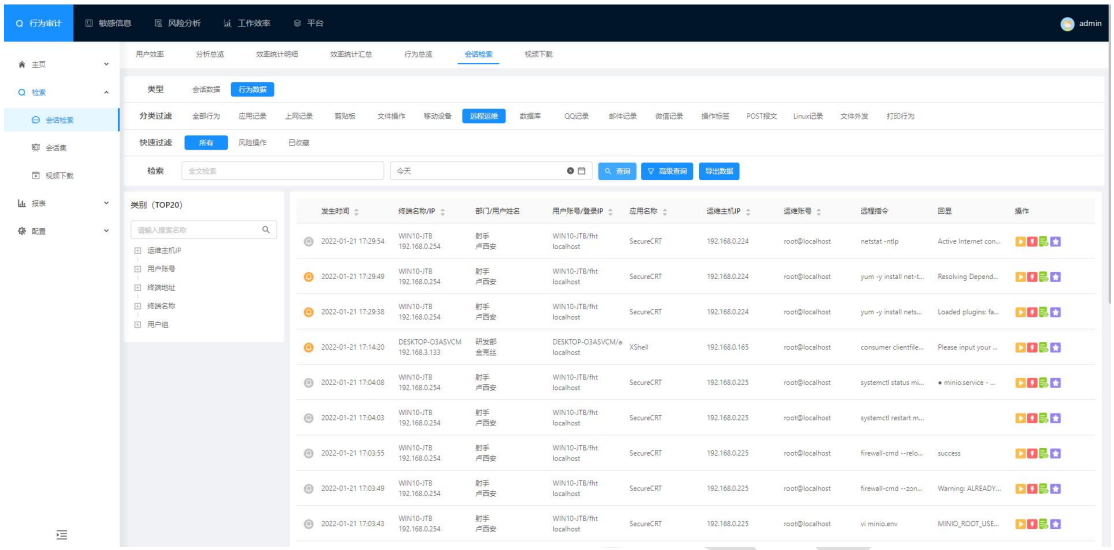


移动设备的查询、播放、创建风险规则、明细、收藏、导出数据等操作请借鉴全部行为步骤 4.3.1-->4.3.6。

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。

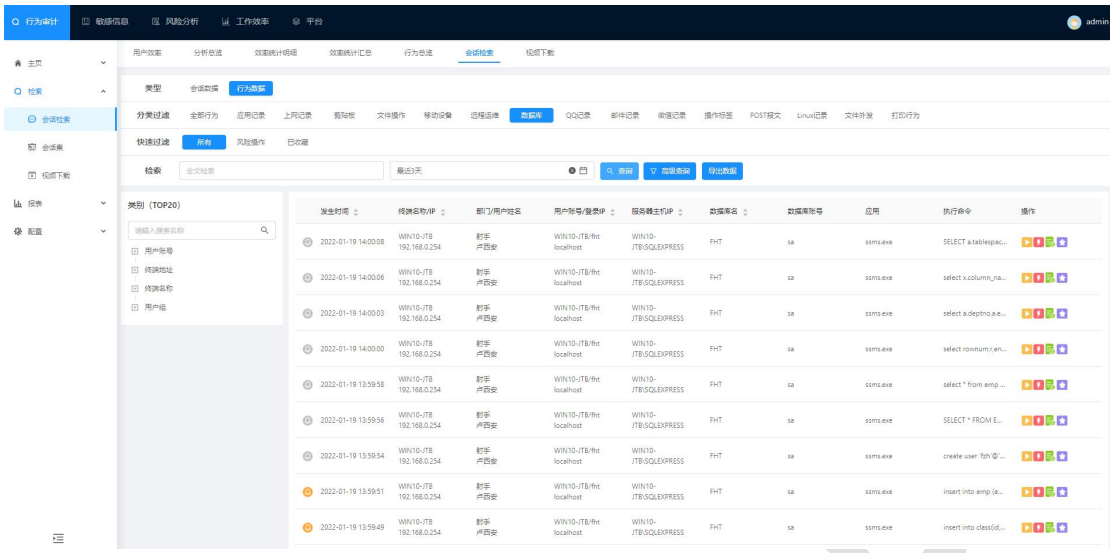


远程运维的查询、播放、创建风险规则、明细、收藏、导出数据等操作请借鉴全部行为步骤 4.3.1-->4.3.6。

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。

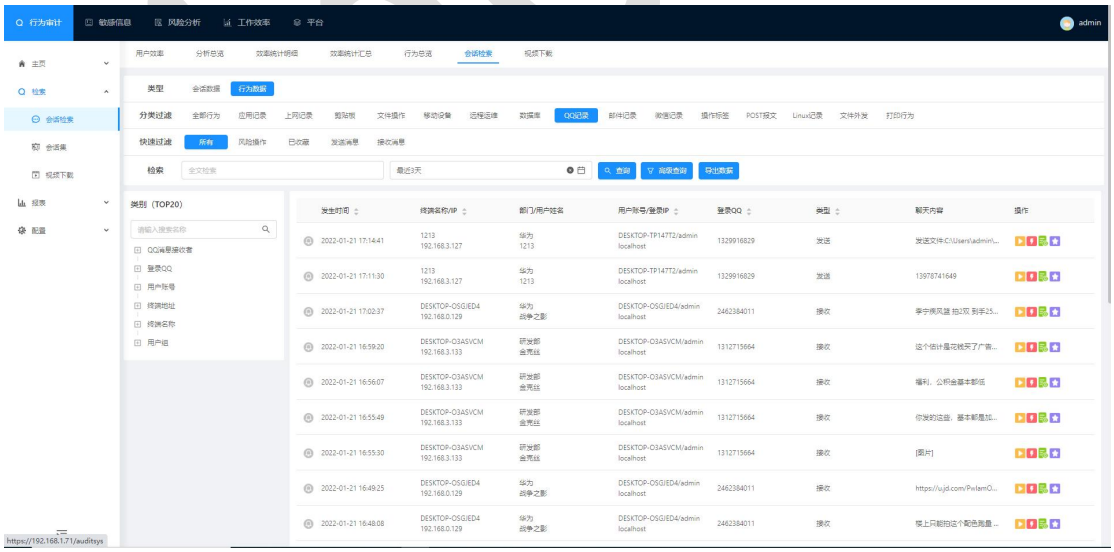


数据库的查询、播放、创建风险规则、明细、收藏、导出数据等操作请借鉴全部行为步骤4.3.1-->4.3.6。

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 记录策略的是否记录 QQ 记录探针才会审计。

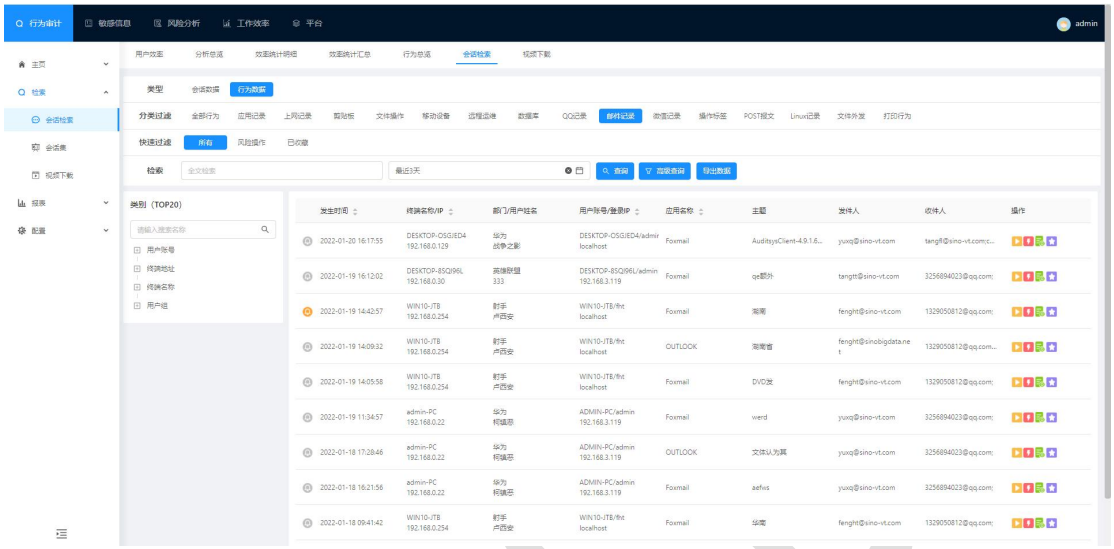


QQ 记录的查询、播放、创建风险规则、明细、收藏、导出数据等操作请借鉴全部行为步骤4.3.1-->4.3.6。

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。

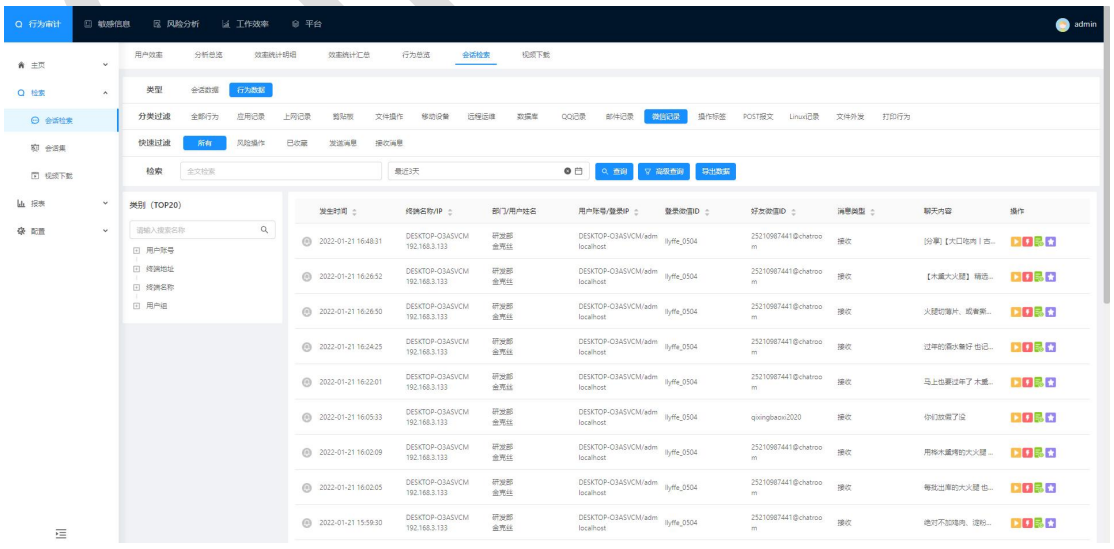


邮件记录的查询、播放、创建风险规则、明细、收藏、导出数据等操作请借鉴全部行为步骤 4.2.1-->4.3.6。

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。



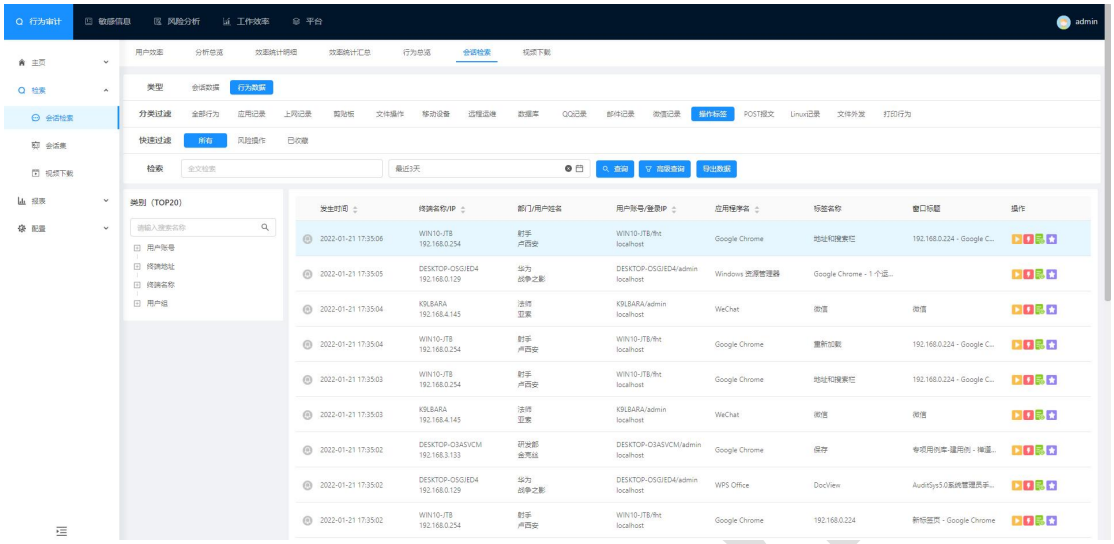
微信记录的查询、播放、创建风险规则、明细、收藏、导出数据等操作请借鉴全部行为步骤

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。

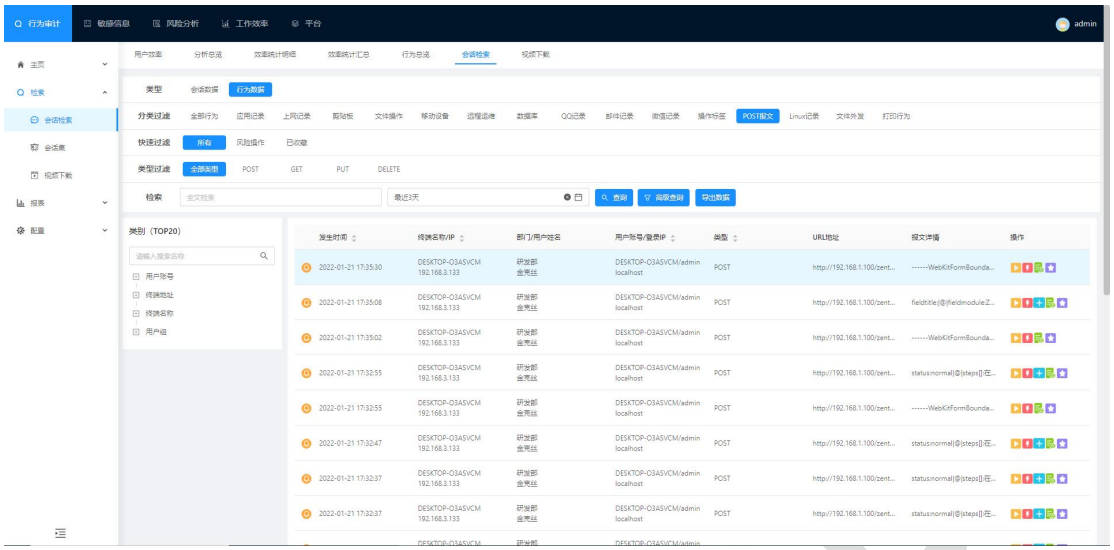


操作标签的查询、播放、创建风险规则、明细、收藏、导出数据等操作请借鉴全部行为步骤 4.2.1-->4.3.6。

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。

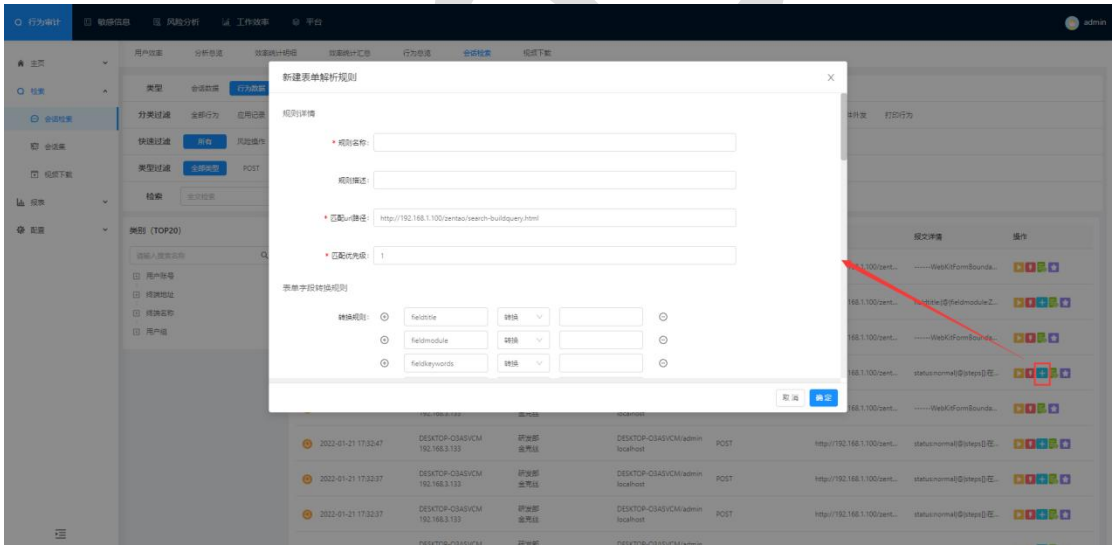
注：需要勾选 Windows 记录策略的是否记录 POST 报文探针才会审计。



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）。

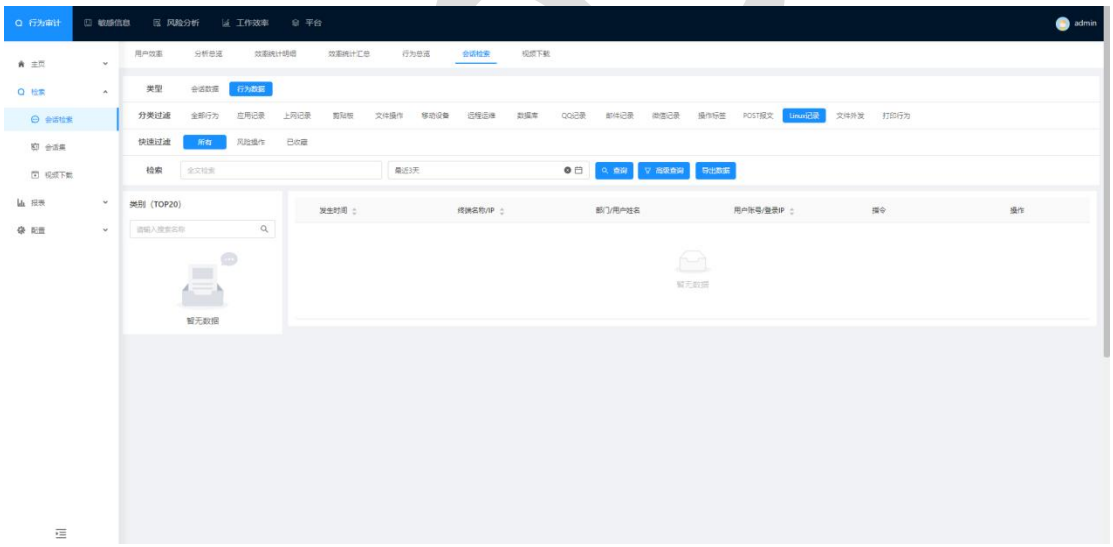
表单字段转换规则：把原本的表单条件名称转换一个自定义表单条件名称显示

（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：

4.3.19Linux 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>



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。

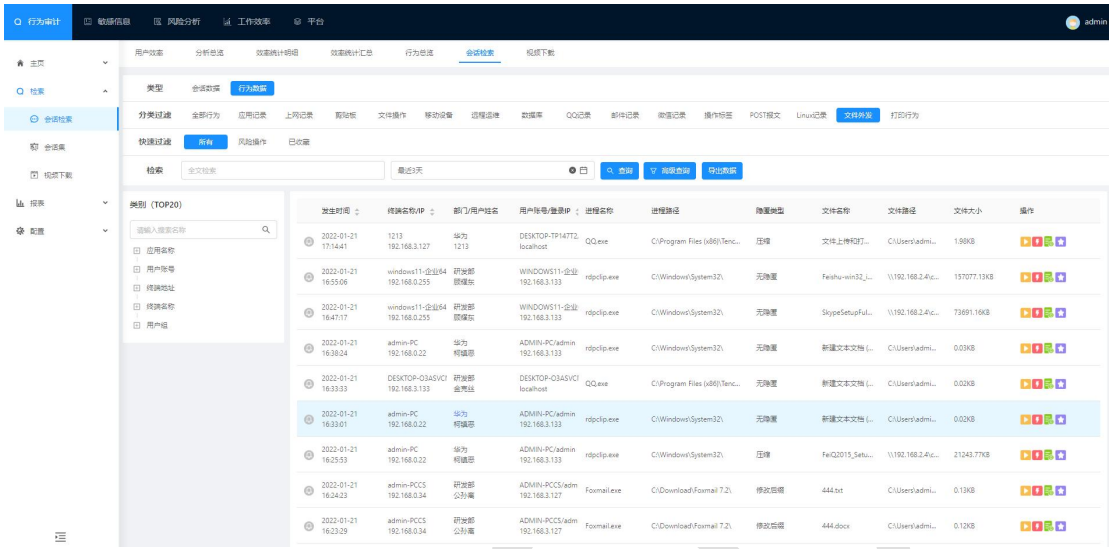
4.3.20 文件外发

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。

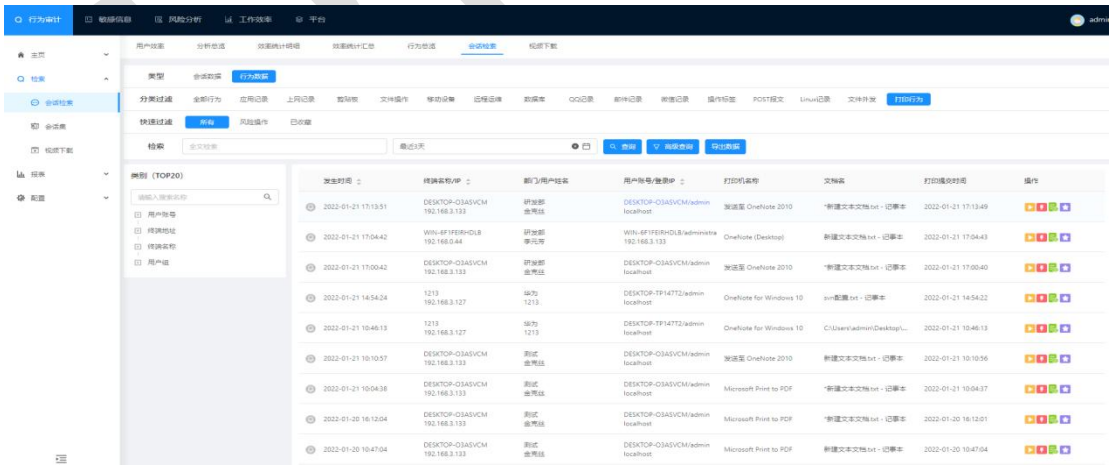
注：目前文件外发还没有支持的 agent 包发布。



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。

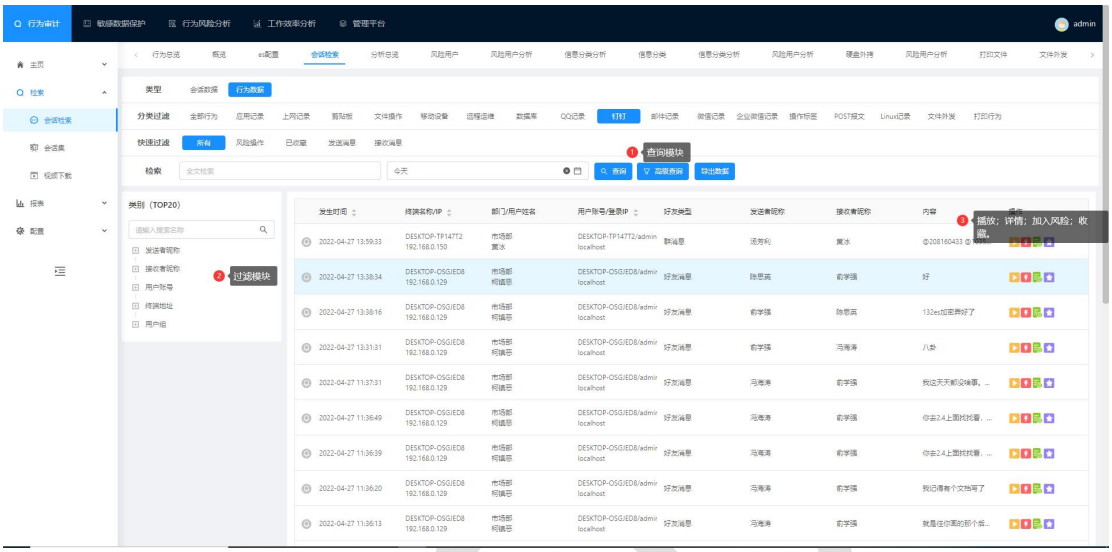


打印行为的查询、播放、创建风险规则、明细、收藏、导出数据等操作请借鉴全部行为步骤 4.2.1-->4.2.6。

=

4.3.22 钉钉记录

记录钉钉应用中消息记录，文件记录等。



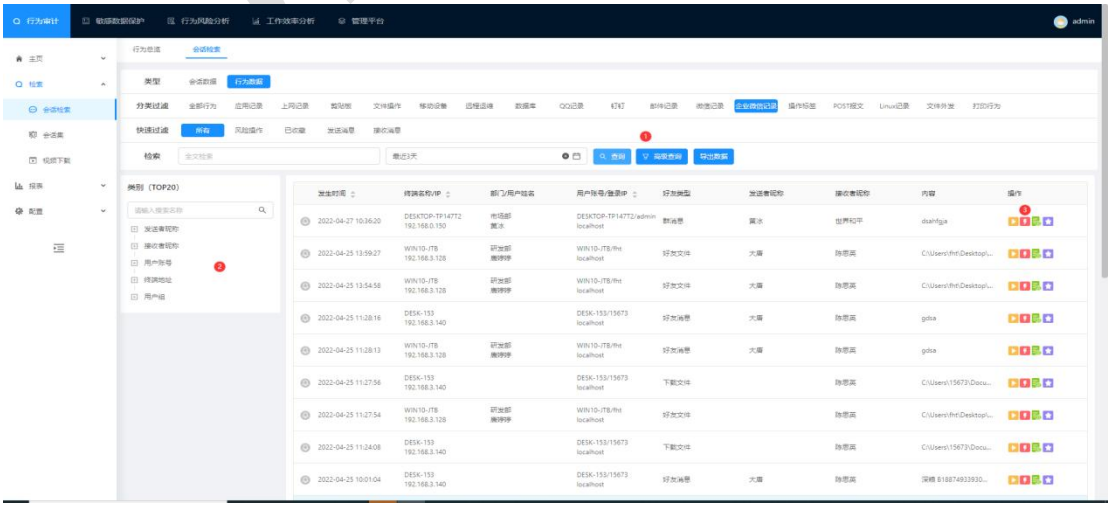
1. 查询模块：模糊查询在搜索框中搜索关键字检索。高级查询可从文档名；好友类型（可分为好友消息；群消息；好友文件；群文件）；接收人/发送人昵称；群备注等检索相应消息记录。

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。

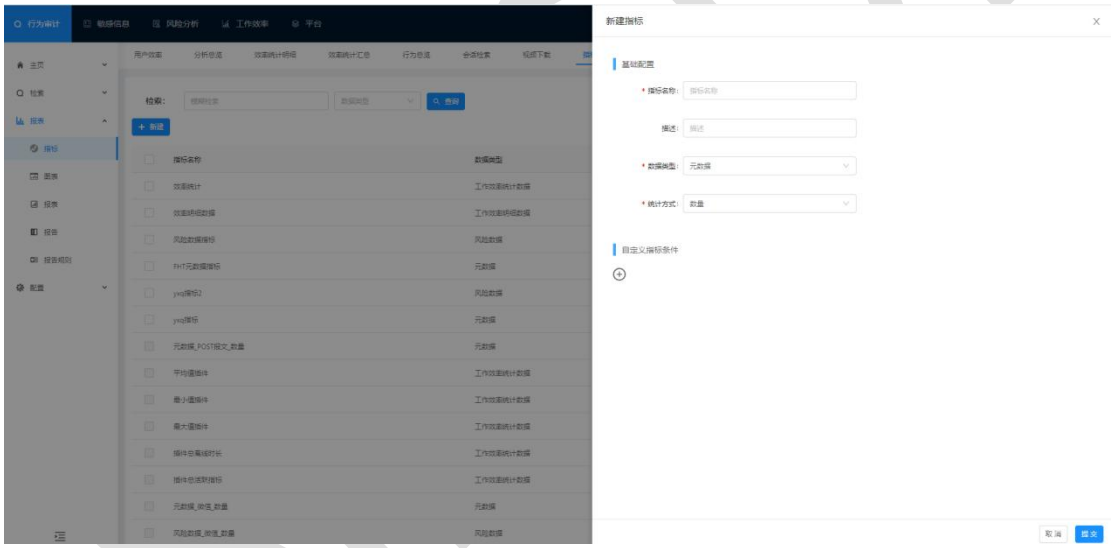


1. 查询模块：模糊查询在搜索框中搜索关键字检索。高级查询可从文档名；好友类型（可分为好友消息；群消息；好友文件；群文件）；接收人/发送人昵称；群备注等检索相应消息记录。
2. 过滤模块：通过过滤模块中的条件过滤。
3. 点击播放视频；点击新建风险，条件自动生成；点击查看消息详情。

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。

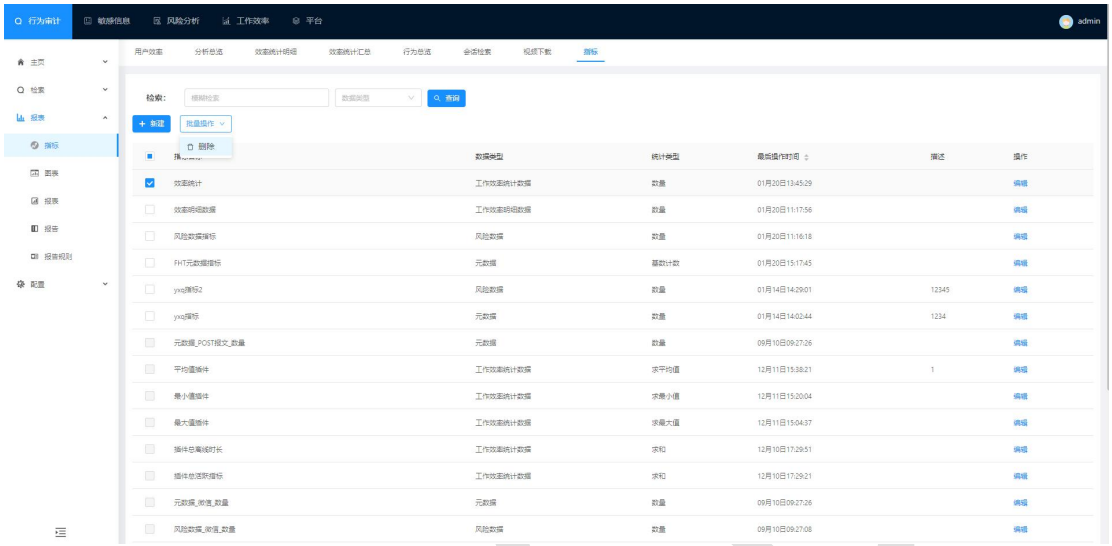
自定义指标条件：自定义需要查询的指标条件；支持‘且’、‘或’、‘非’逻辑关系；多条件需要同时满足才能查询到数据。支持‘精确查找’、‘模糊查找’、‘区间查找’。

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

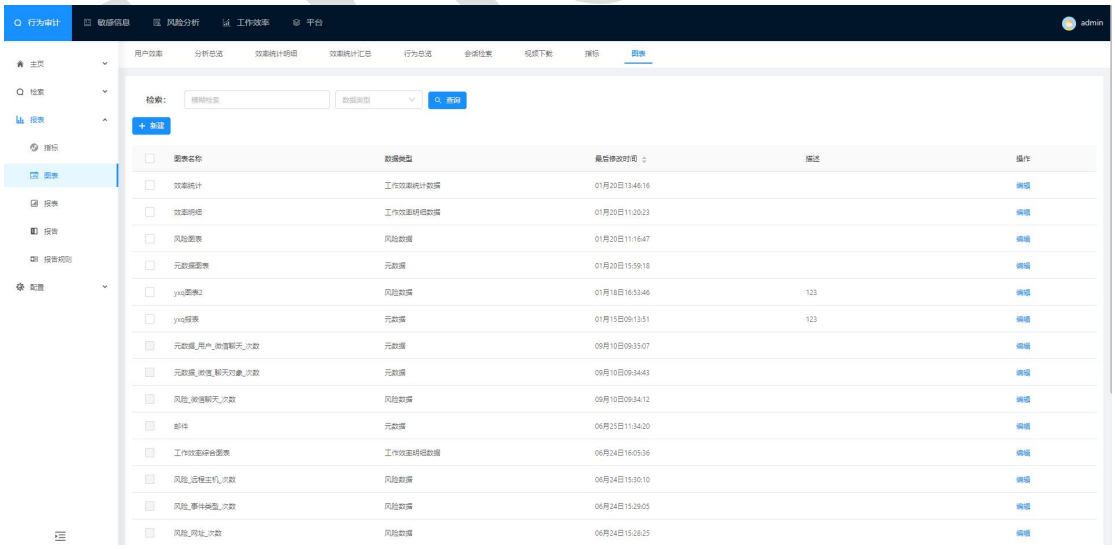
选择要删除的指标，点击“删除”按钮删除指标（提示：默认指标无法被选中删除）。如下图所示：



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：



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。

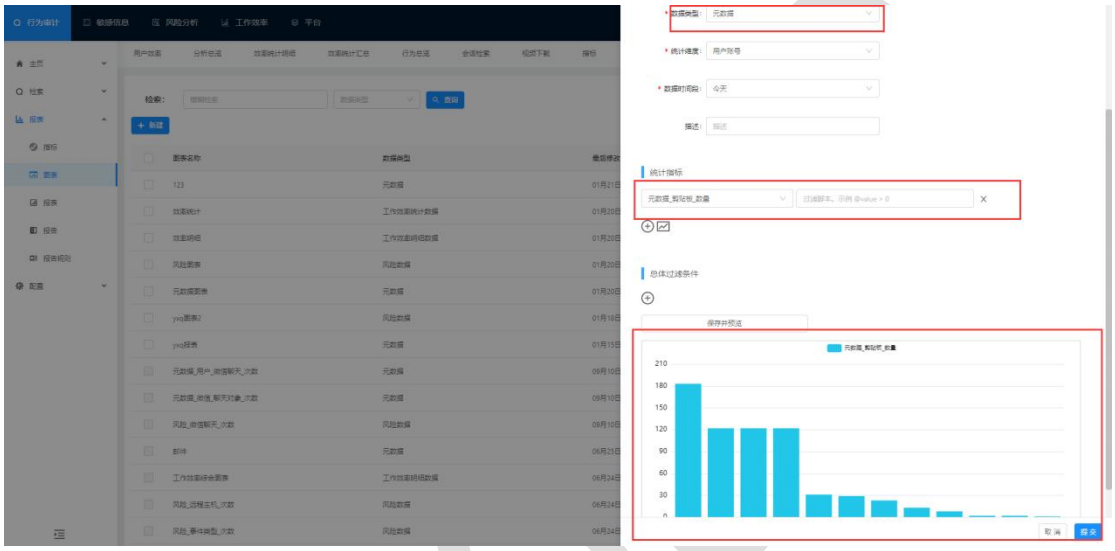
统计维度：可选择按登录用户、时间段、事件类型、终端名称、终端 IP 等维度来统计。

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。

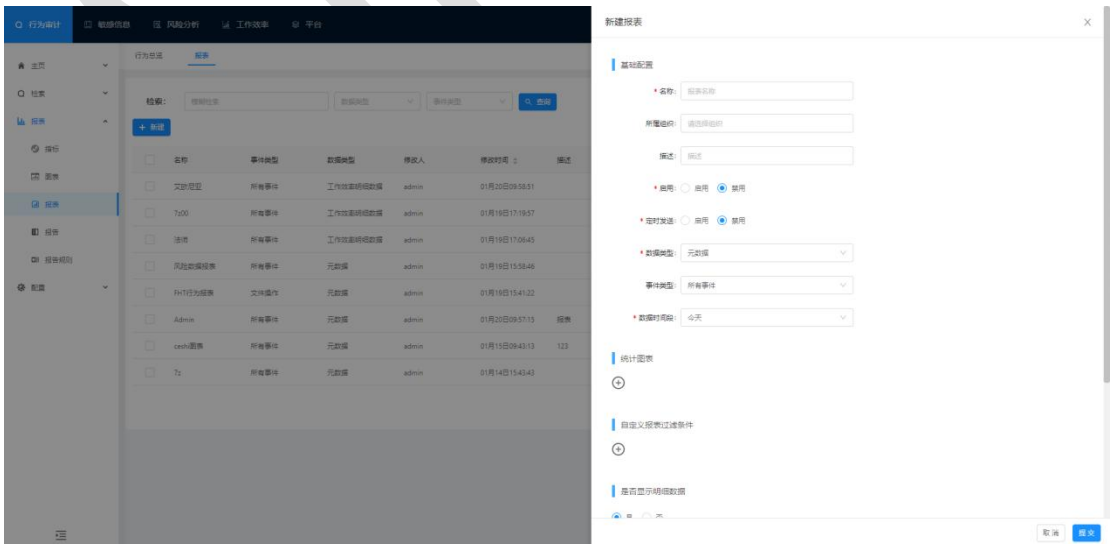
总体过滤条件：输入条件进行查询。

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：



4.21.4 新建报表

点击“新建”按钮进行新建报表；如下图所示：



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。

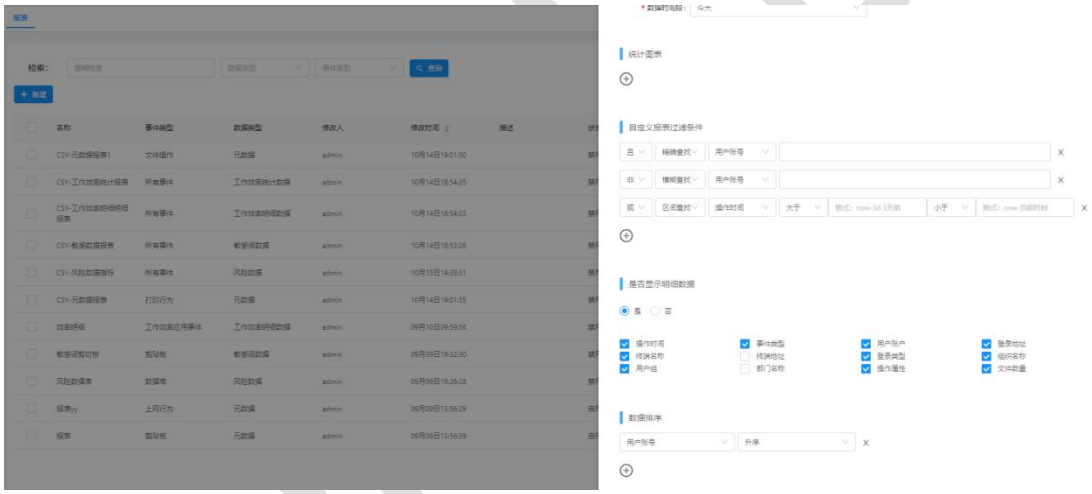
数据类型：选择数据类型。

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。



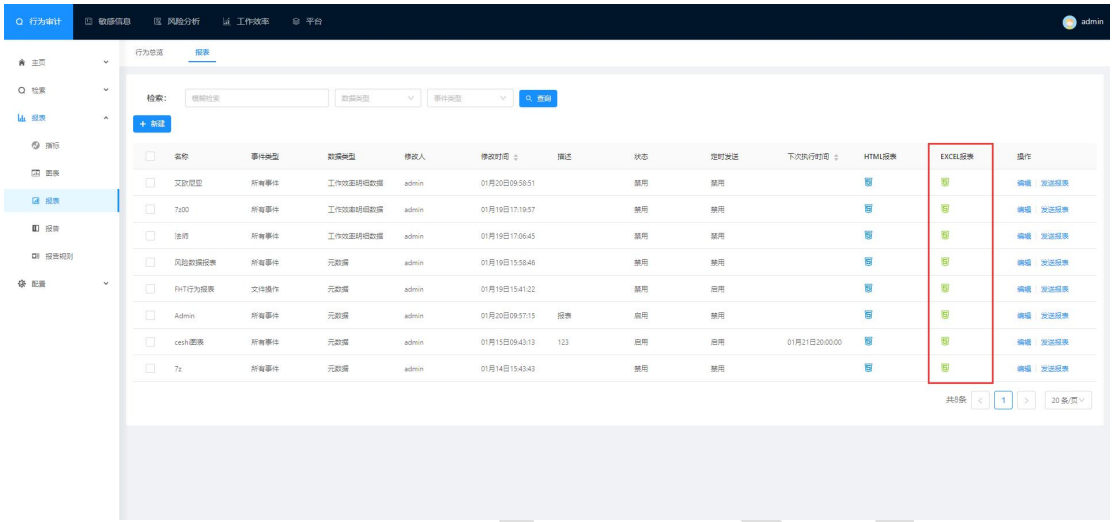
自定义报表过滤条件：自定义需要查询的指标条件；支持‘且’、‘或’、‘非’逻辑关系；多条件需要同时满足才能查询到数据。支持‘精确查找’、‘模糊查找’、‘区间查找’。

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。

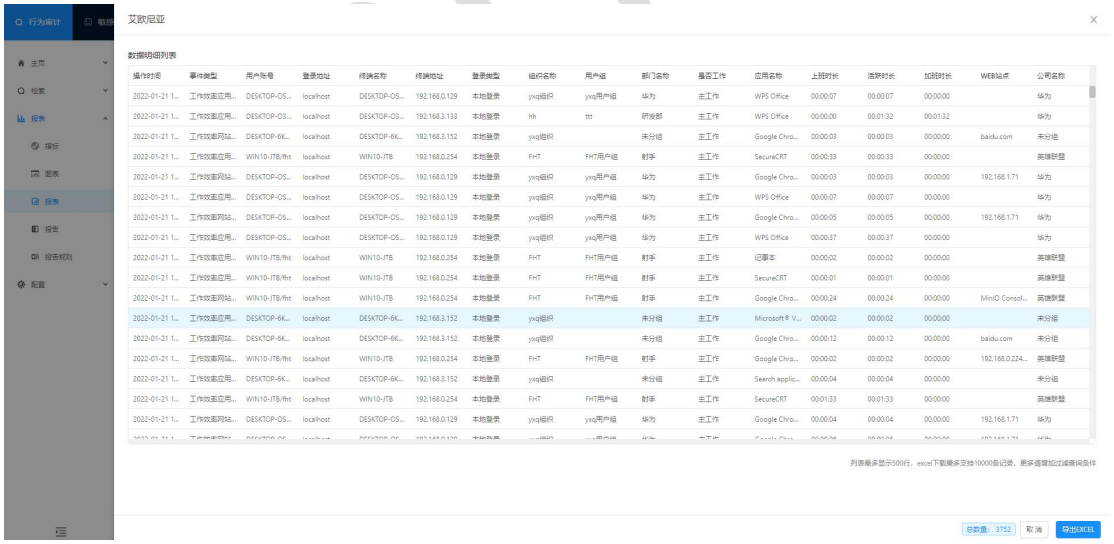
4.21.5 excel 报表

点击“ ”导出 Execl 报表。或者先点击“ ”生成 HTML 报表，再在 HTML 界面，在点击“导出 EXECL”导出 execl。



4.21.6html 报表

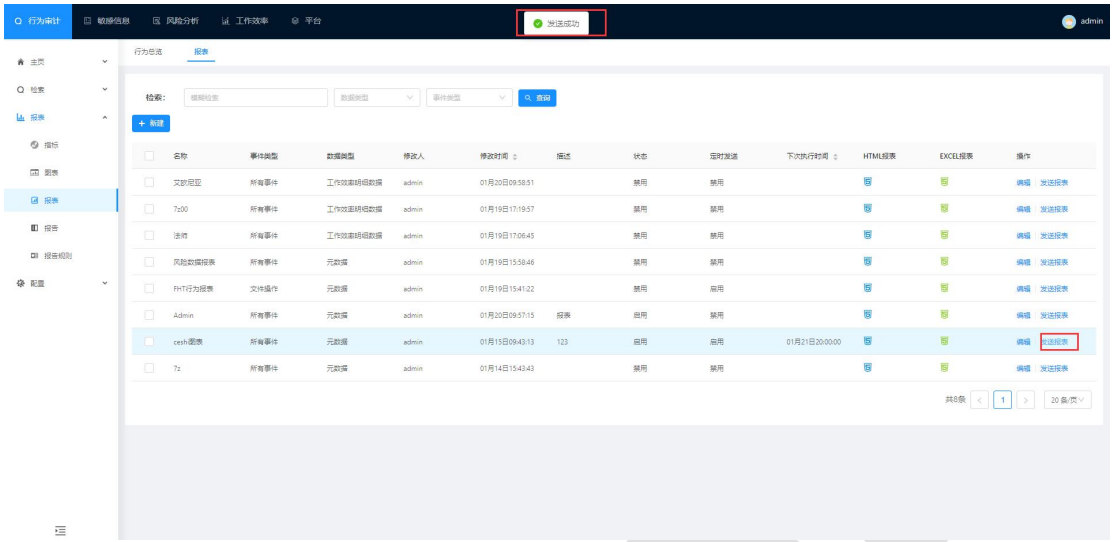
点击“ ”按钮生成 HTML 报表；如下图所示：



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。



4.21.8 仪表盘

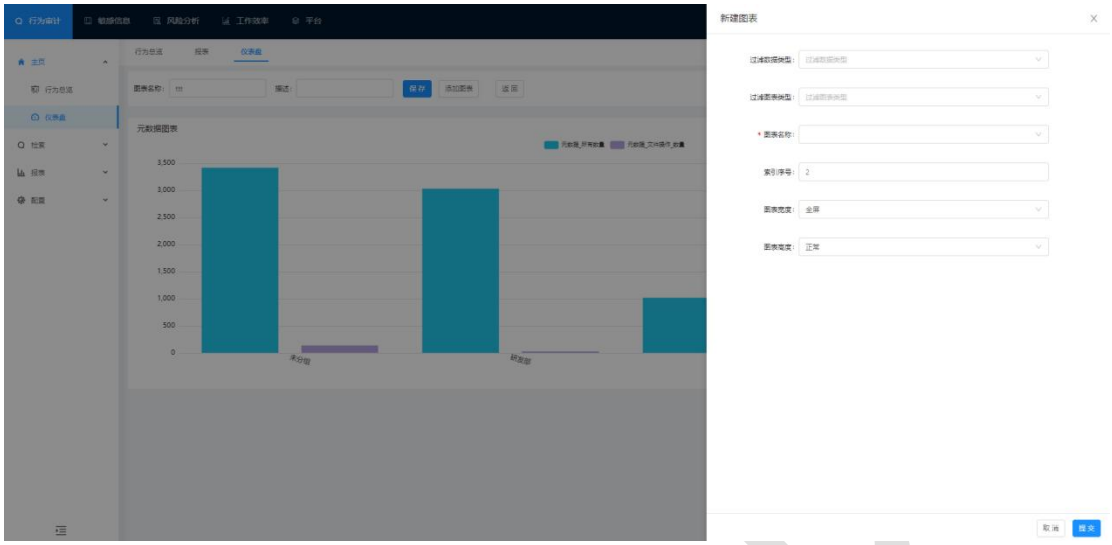
仪表盘是用来展示图表统计数据。

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：

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。

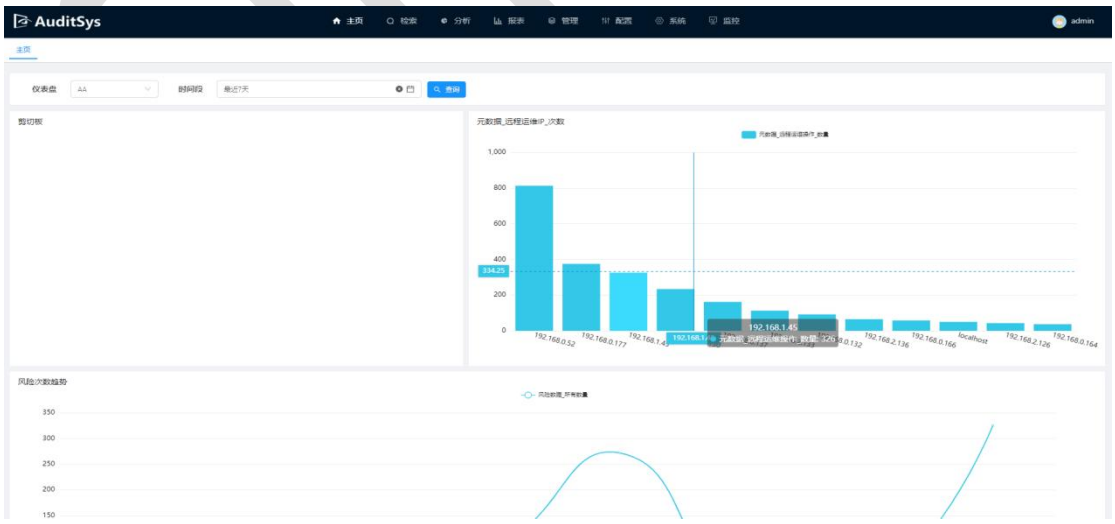
索引序号：在仪表盘添加的第几个图表。

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

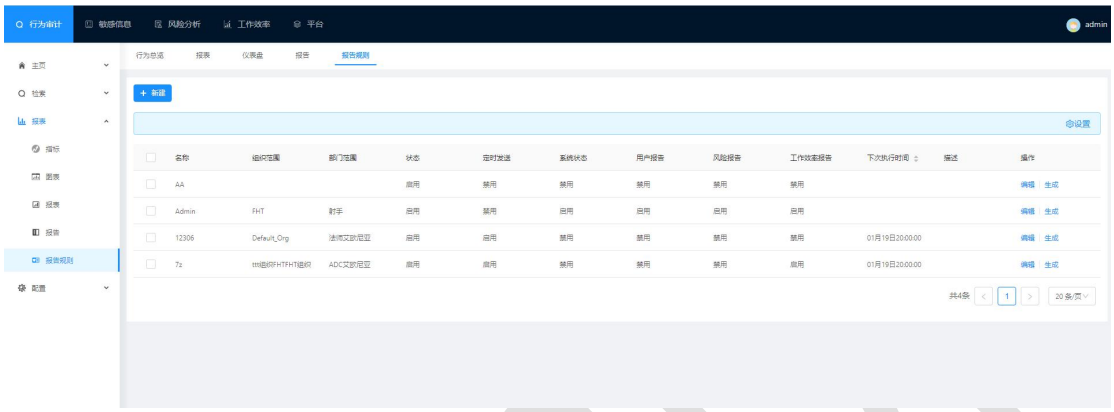
可在主页选择仪表盘展示；选择仪表盘后，不同的管理员再次登录可以展示不同仪表盘数据；仪表盘展示的时间默认是 7 天。



4.21.9 报告规则

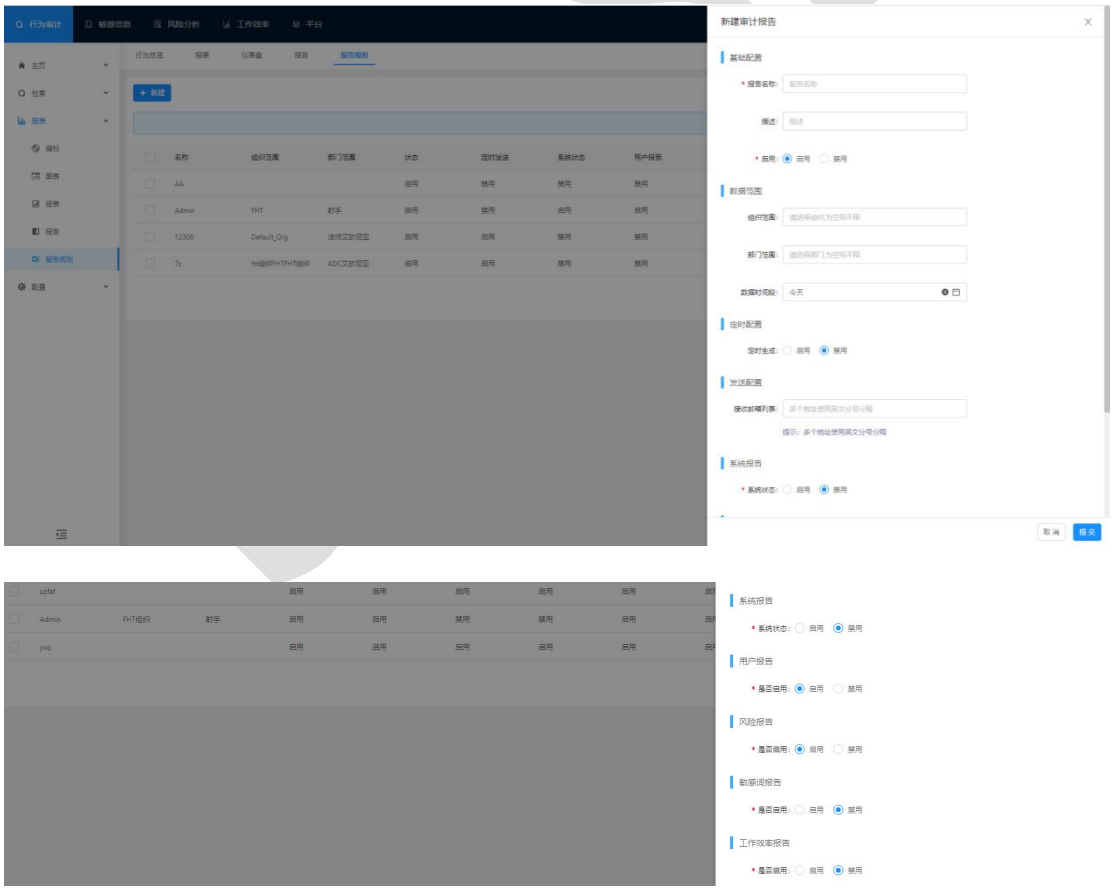
报告规则是自定义选择时间范围从多个维度（系统报告、风险报告、敏感词报告、工作效率报告）制定规则生成报告。

点击“报表>报告规则”进入报告规则界面；如下图所示：



新建报告规则

点击“新建”新建报告规则；如下图所示：



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。

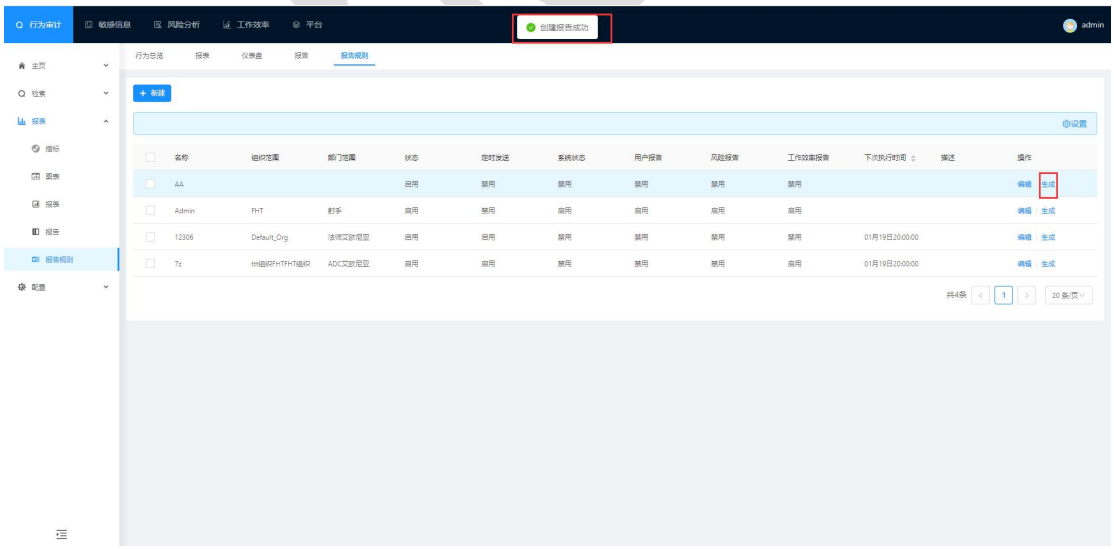
风险报告：勾选启用，则统计显示用户的风险行为数据信息报告。

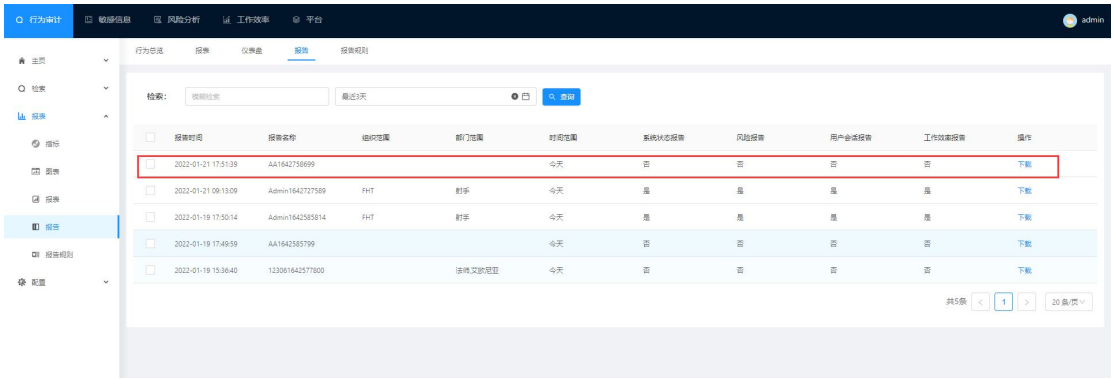
敏感词报告：勾选启用，则统计显示用户的敏感行为数据信息报告。

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：

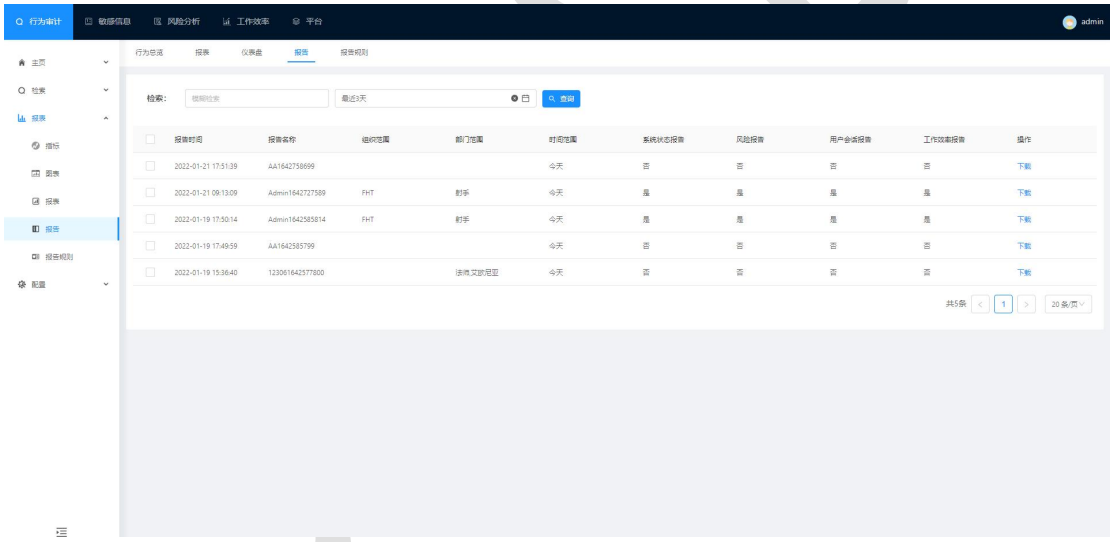




4.21.11 报告

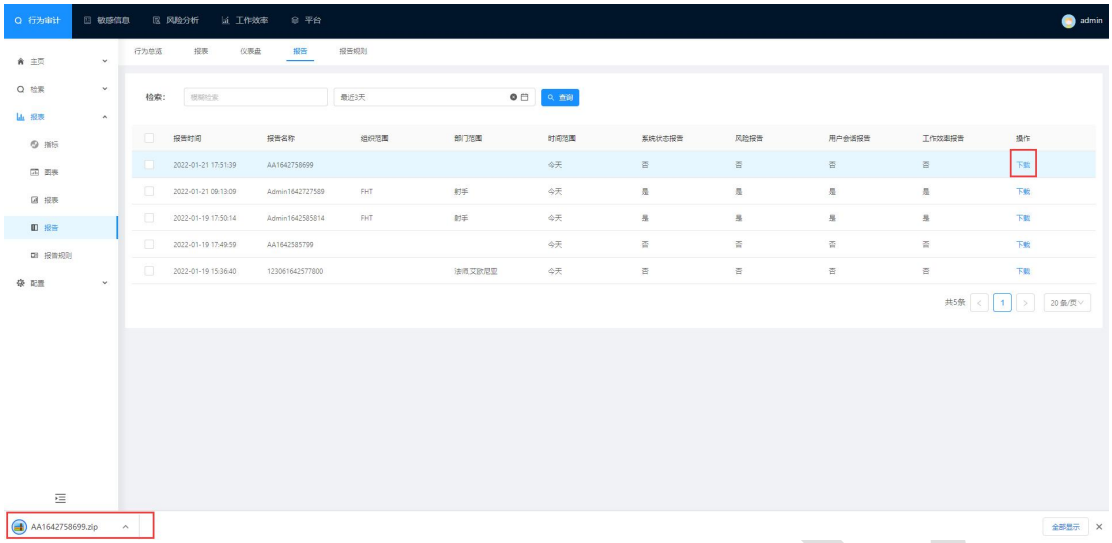
报告是对多个维度（系统状态、用户行为、风险行为、敏感行为、工作效率分析）数据统计生成运行报告。

点击“报表>报告”进入报告界面；如下图所示：

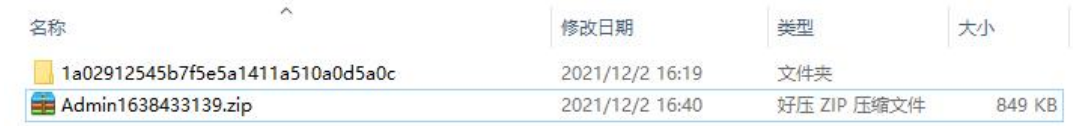


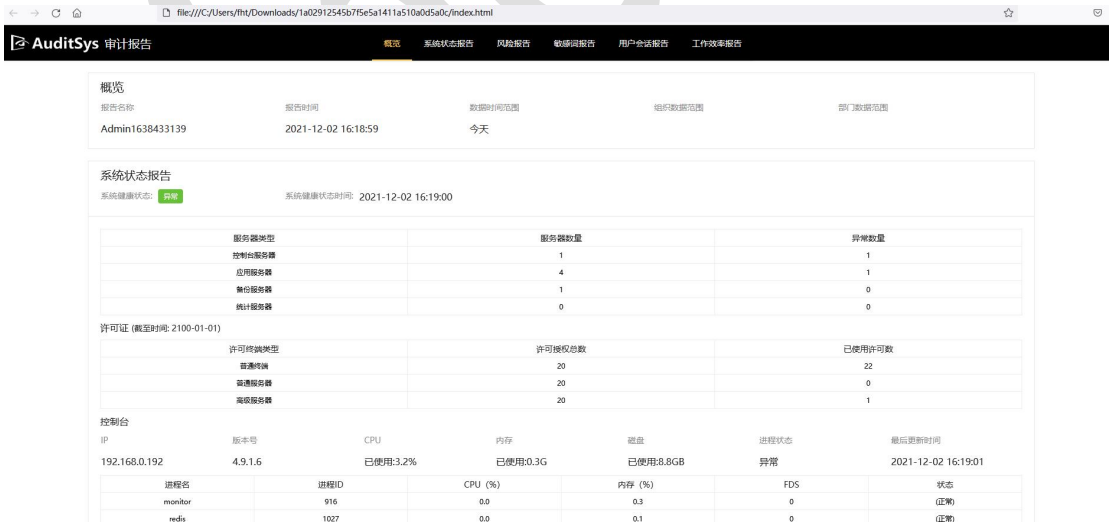
4.21.12 报告下载

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：



对下载的报告进行解压；打开 index.html 文件查看报告统计详情；





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：