秦尉数字一体化安全运营平台
用户手册

文件修改版本控制

序号	版本	更新状态	简要说明（变更内容和范围）	修改人	修改日期	审核人	批准人
1	V1.0	M	修改	闫涵 种瑞平	2024-10-15		
2							
3							
4							
5							
6							

更新状态：用大写字母表示。C——创建，A——增加，M——修改，D——删除

文件审批信息

序号	批准人	角色	批准日期	签字	备注
1					
2					
3					
4					
5					
6					

目录

一、引言

1.1 编写目的

通过清晰的功能说明和操作步骤，帮助用户更快地熟悉产品，快速学习和掌握产品的使用方法，提高用户满意度和产品的易用性。

该文档面向的读者：

系统使用用户：帮助用户快速了解系统功能和使用方法。

技术支持人员：了解软件的所有功能和潜在问题，以便为用户提供帮助和解决方案。

1.2 产品研发背景介绍

秦尉公司凭借多年的深厚经验，在业务重构到数字化实施、业务设计到流程建设与运营等多个领域积累了丰富的实践。我们紧跟时代潮流，抓住 AI 大模型和安全可信技术带来的重构机遇，积极响应国家在数字经济、数字中国建设、数据要素战略上的号召，特别是在一体化安全运营方面，通过深入数字政府安全建设特殊性和需求，为数字政府提供定制化的一体化安全运营解决方案，帮助数字政府提升网络安全治理效率、降低管理难度、提升网络安全能力。依托秦尉 AI 开发平台、操作系统、算力基础设施等独特优势，围绕“11813”体系，构建最懂数据中心的智能安全体系架构，其功能为：“1 套”基础能力支撑、 “1”个安全数据集、“8”个安全应用子系统、“1”个安全运营服务中心、“3”个运营支撑体系。以资产为核心，结合 AI、数据要素独特能力，实现一体化智能安全运营。

1.3 参考资料

《产品需求规则说明书》、《产品技术详细设计文档》

1.4 系统概述

秦尉数字一体化安全运营平台，通过整合多维安全分析能力，贯通安全运营各关键环节，实现一体化安全感知、监测、处置闭环能力。汇聚云、网、数、用、端全面安全数据，横到边、纵到底，覆盖网络、数据、密码、移动应用等多维安全态势，全面掌握安全风险和威胁。解耦探针及应用平台硬关联，统一纳管，消除安全信息孤岛。做到兼容全球主流安全顶尖厂商的业务应用，避免重复投资。利用 AI 智能分析引擎，赋能安全人员，加速威胁研判和处置闭环速度，全流程自动化处置，节省安全运维专家投入，模型泛化能力强，不需要频繁更新，降低系统维护成本。以及灵活的运营属地化+远程服务化模式，快速适配常态化运营、攻防演练、重保等多种运营场景，提供可视的全网监控。最终做到一点感知、全网响应，全网、全域统一策略部署和响应，可复现完整攻击链条，一旦发现威胁，全网实施防御。

1.5 功能简介

No	领域	重点模块
1	安装部署	1、 平台一键部署且服务正常启动
2	数据中台	1、 数据模板 2、 字段管理 3、 对象管理 4、 数据对接 5、 数据检索 6、 数据总线 7、 数仓管理

		8、 对接管理 9、 安全数据资产
3	安全运营工作台	1、 专栏信息 2、 专栏信息管理 3、 知识库管理 4、 知识库信息 5、 个人工作台
4	系统管理	1、 单位管理 2、 权限管理 3、 应用管理 4、 消息管理 5、 登录认证 6、 系统配置 7、 审计中心 8、 个人中心 9、 运维中心
5	安全运营管理	1、 安全运营指标 2、 指挥调度中心

1.6 系统要求

序号	测试环境/工具	型号/版本	规格
1	Nginx 高可用、Visual 前后端服务、运维监控	Taishan2280 V2	8U16G*300G 高速云硬盘
2			
3	分布式集群（nifi、zk、pulsar、es、redis）	Taishan2280 V2	32U64G*500G 告诉云硬盘
4			
5			
6	数据库（DM、MySQL、ActiveNQ）、Foundation、数据总线、数据质量	Taishan2280 V2	
7			

8			8U16G*300G 高速云硬盘
9	运营门户、数据中台	Taishan2280 V2	8U16G*300G 高速云硬盘
10			
11			
12	数据检索（高级检索、QPL）	Taishan2280 V2	32U64G 高速云硬盘
13	浏览器支持	/	Google、Edge

二、安装指南

详见《安全运营支撑平台安装部署指导手册》

三、操作指南

3.1 系统管理

【功能说明】整个平台的系统管理模块，用于维护用户信息，所属单位部门，分配用户权限、设置导航和菜单，系统配置，以及运维监控等等，作为整个平台的基础；

3.1.1 应用管理

3.1.1.1 应用配置

点击【应用配置】菜单，打开应用导航及应用列表展示页面，可以在该菜单实现以下功能

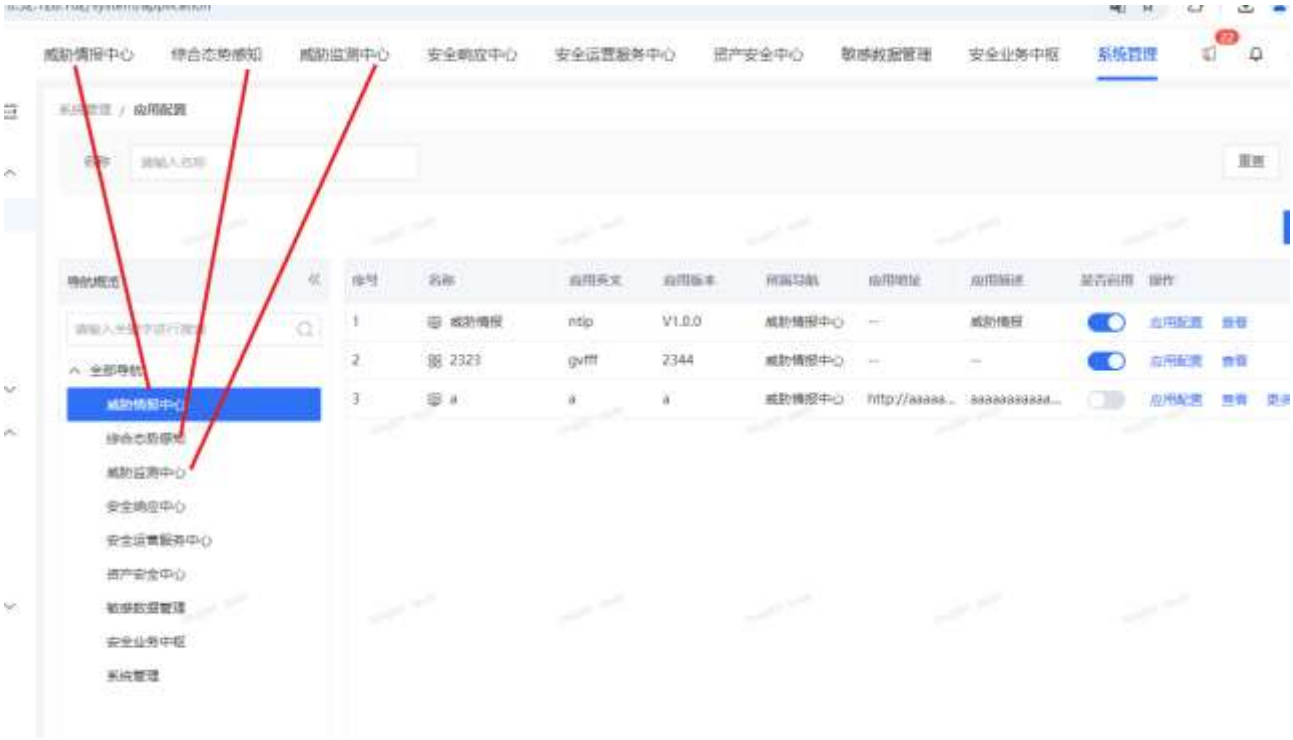
【导航管理】导航新增、修改、删除、排序

【应用信息管理】应用新增、修改、删除、排序

【菜单信息配置】应用新增、修改、删除、排序

3.1.1.1.1 导航管理

【功能说明】配置系统顶部导航信息，导航对应系统顶部菜单展示



3.1.1.1.1.1 导航新增

【功能说明】实现导航新增

3.1.1.1.1.2 导航删除

【功能说明】实现导航新增

3.1.1.1.1.3 导航修改

【功能说明】实现导航修改

3.1.1.1.1.3 导航排序

【功能说明】实现导航排序

操作说明：使用鼠标长按图标上下拖动即可实现排序

3.1.1.1.2 应用信息管理

3.1.1.1.2.1 新增应用

【功能说明】实现应用新增

限制说明：应用英文为应用唯一标识，需要全局唯一

3.1.1.1.2.2 应用停/启用

【功能说明】实现应用停用、启用；应用停用后，相关菜单不再展示

3.1.1.1.2.3 应用修改

【功能说明】实现应用信息编辑（修改应用时，需要先停用应用）

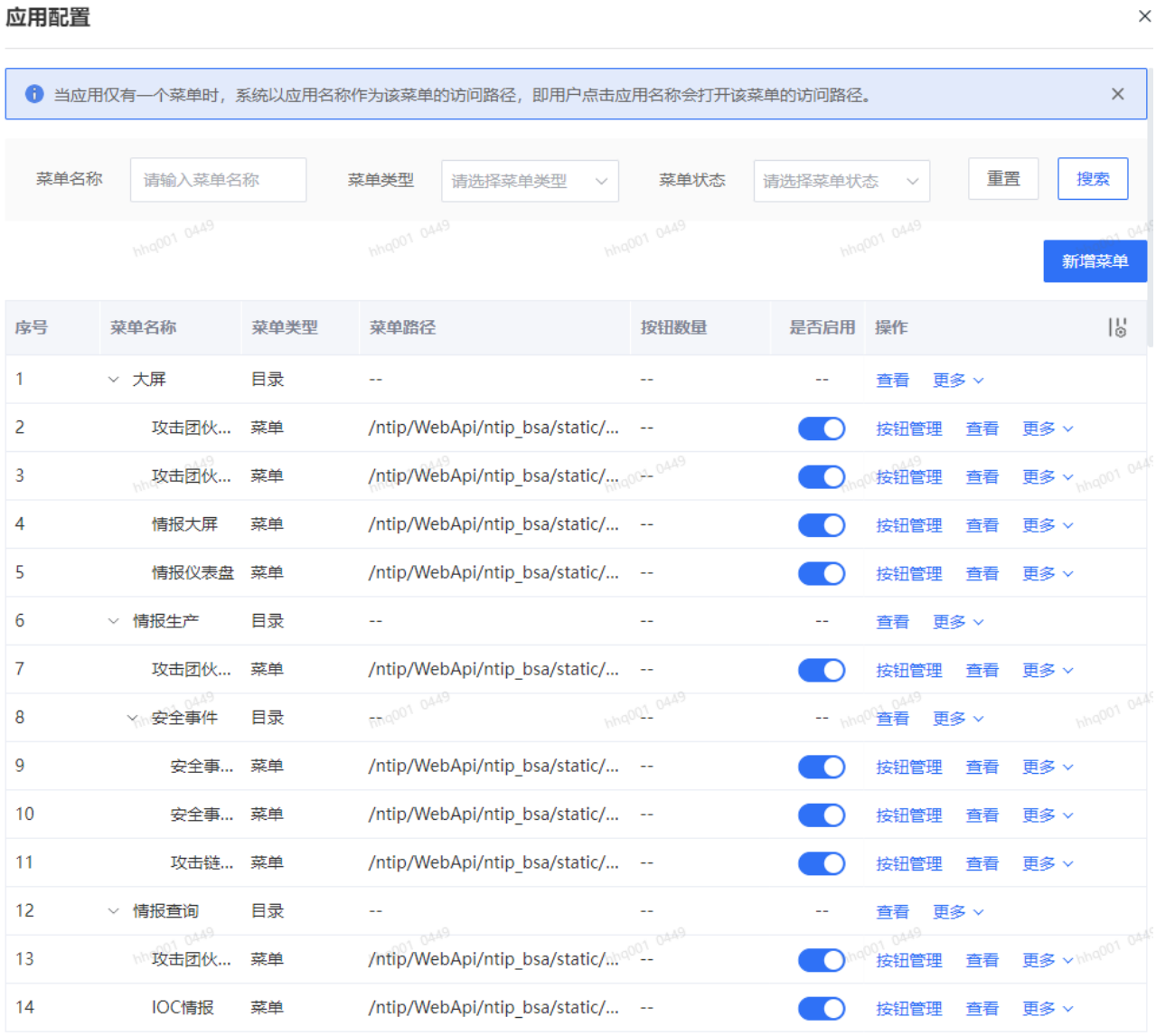
操作限制：应用中英文名称不能被修改

3.1.1.1.2.4 应用删除

【功能说明】实现应用及所属信息删除（删除应用时，需要先停用应用）

3.1.1.1.3 菜单信息管理

【功能说明】维护应用下目录、菜单、按钮信息，点击【应用配置】进入管理页面



3.1.1.1.3.1 目录新增

【功能说明】实现目录信息新增

3.1.1.1.3.2 目录修改

【功能说明】实现目录信息更改

操作说明：鼠标在目录所在行右侧，点击“更多”下面的“编辑”按钮，弹出目录修改页面

操作限制：只能修改目录名称及同级排序

3.1.1.1.3.3 目录删除

【功能说明】删除目录信息

操作限制：若目录下存在菜单，则不能被删除

3.1.1.1.3.4 菜单新增

【功能说明】为系统添加菜单

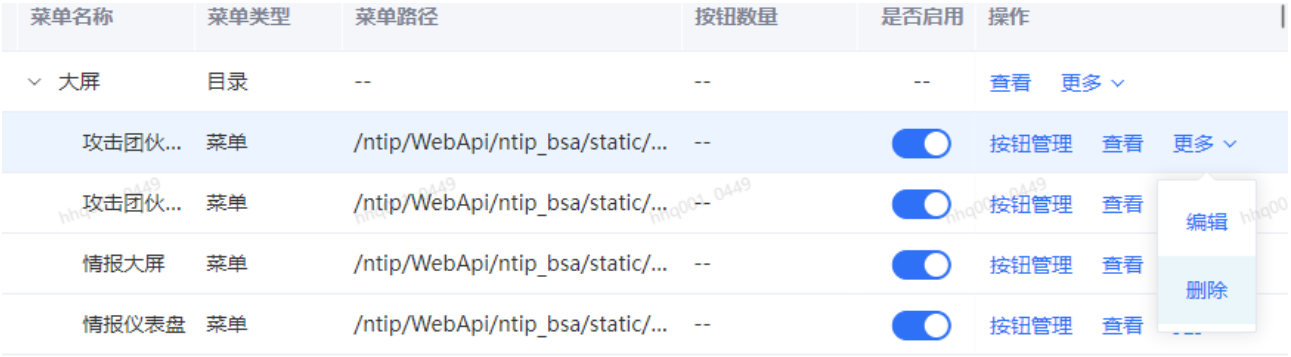
操作限制：权限标识为菜单唯一标识，用于权限管控，全局唯一；鼠标悬浮“？”可查看填写说明。

3.1.1.1.3.5 菜单修改

【功能说明】实现菜单信息修改

3.1.1.1.3.6 菜单删除

【功能说明】删除菜单信息

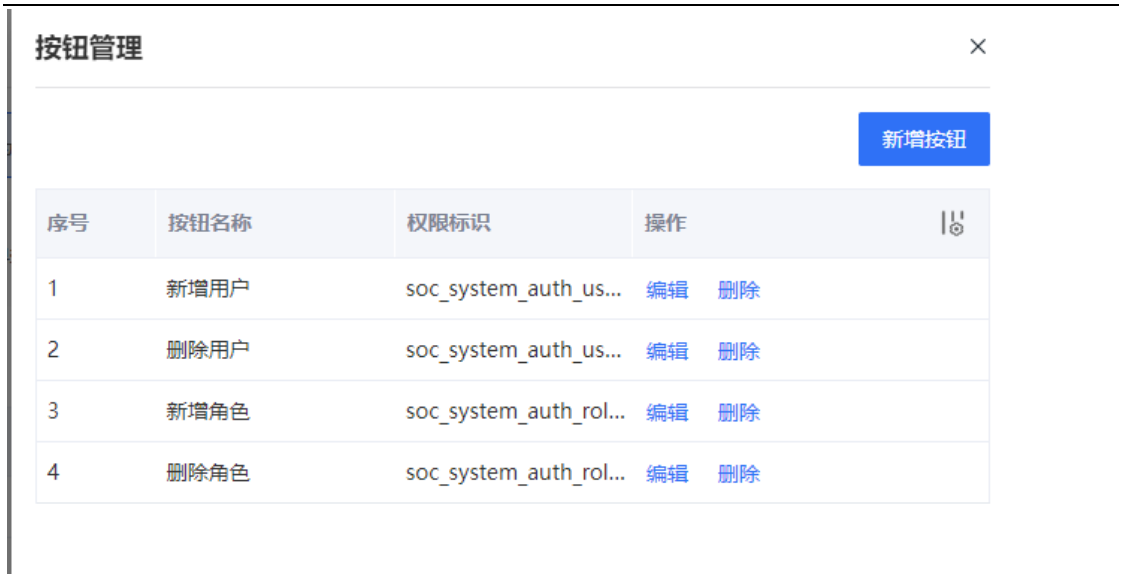


3.1.1.1.3.7 菜单/目录停启用

【功能说明】停用目录/菜单，被停用后，菜单对应功能不再向用户展示

3.1.1.1.3.8 按钮管理

【功能说明】对于涉及敏感操作的按钮，可以添加按钮级权限控制，只有分配相关按钮权限，才会在页面展示【需要定制化开发】



3.1.1.2 应用说明

【功能说明】为各子应用创建使用说明，方便用户使用系统

3.1.1.2.1 应用说明管理

【功能说明】使用富文本或附件形式展示应用功能

3.1.1.2.1.1 应用说明新增

【功能说明】增加应用说明

3.1.1.2.1.2 应用说明修改

【功能说明】修改应用说明信息

3.1.1.2.2 应用说明查看

【功能说明】用户可以查看应用相关说明信息

3.1.1.2.2.1 应用目录检索

【功能说明】用户点击左侧目录树，可快速筛选和应用相关的文章

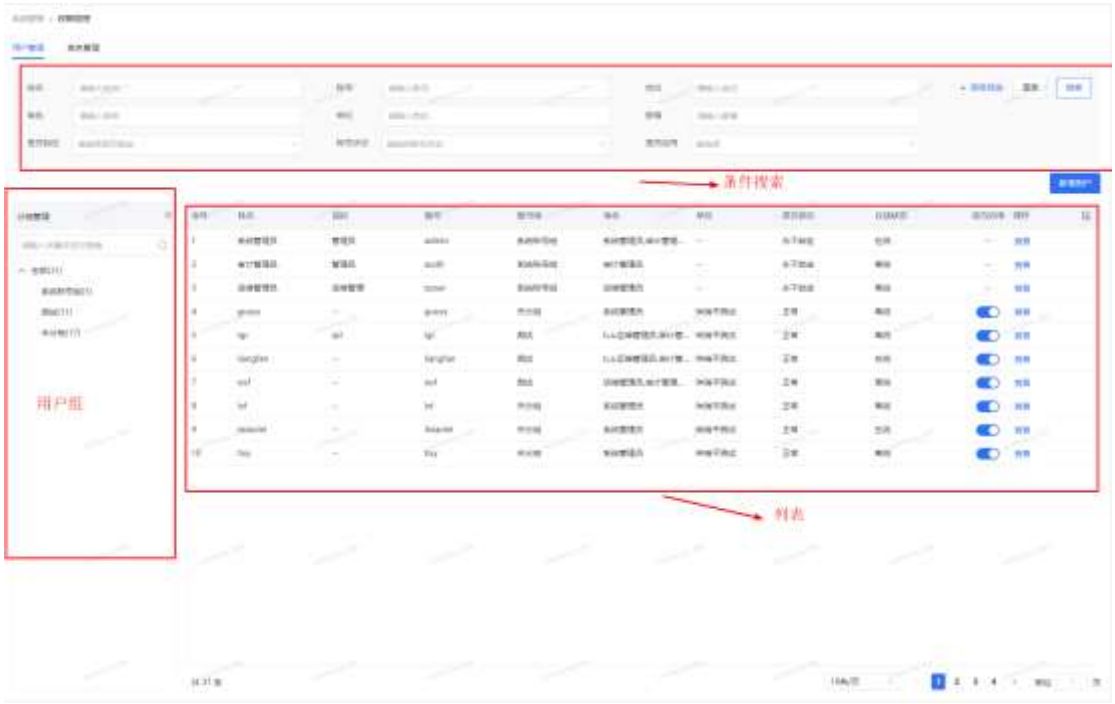
3.1.1.2.2.2 应用说明预览

【功能说明】点击“操作”列查看按钮，以富文本形式展示展示应用说明

3.1.2 权限管理

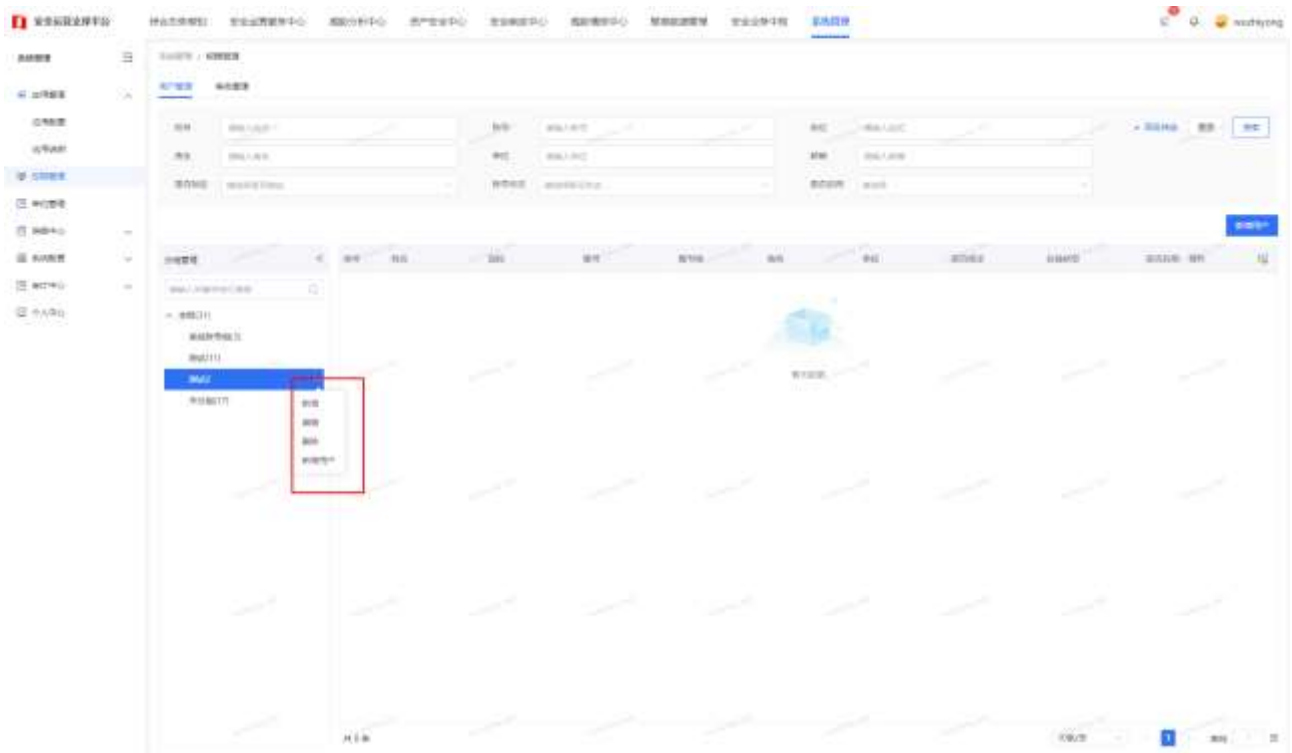
3.1.2.1 用户管理

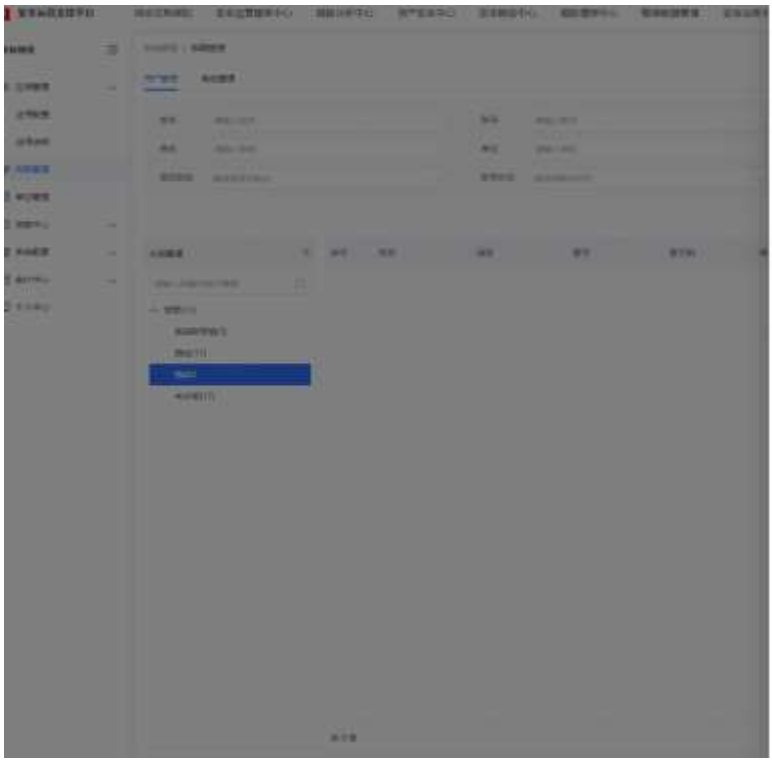
【功能说明】系统内所有用户包括拥有账号和非拥有账号的用户的基本信息新增、修改、删除和查看，以及用户组的维护

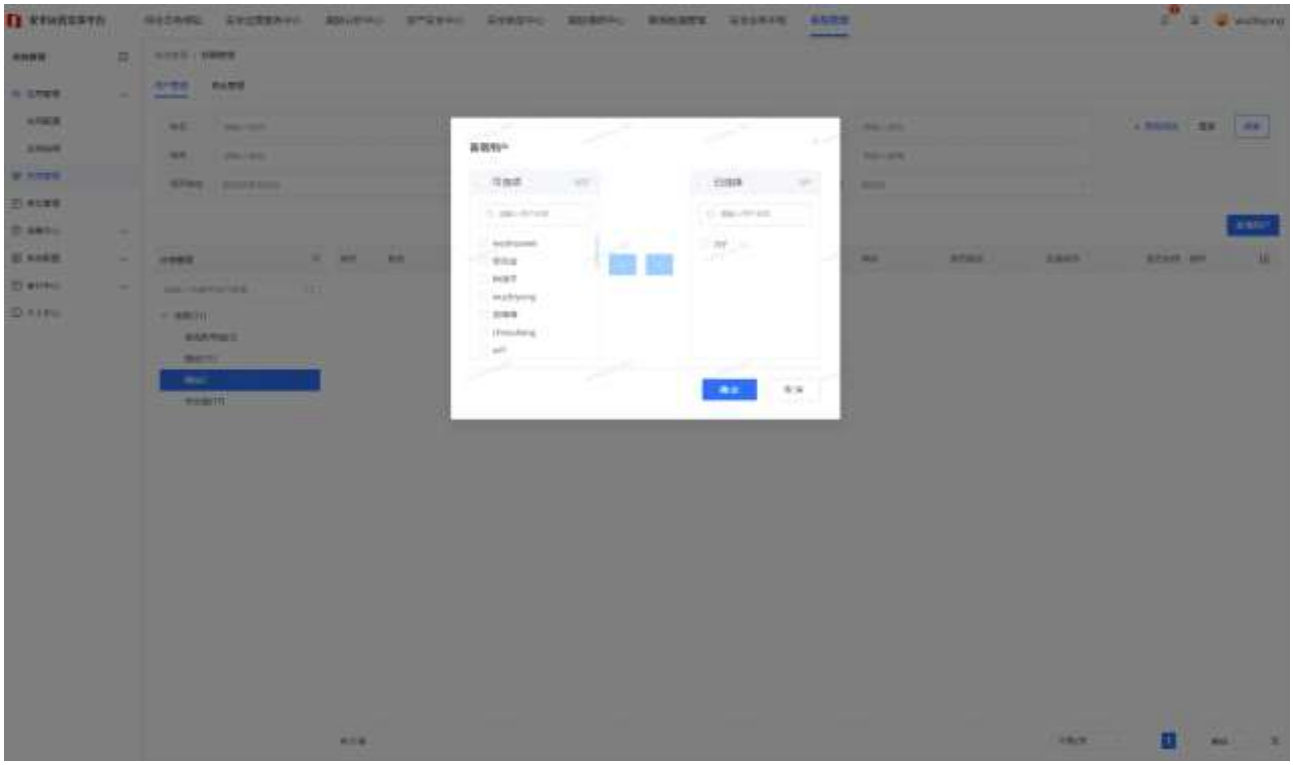


3.1.2.1.1 用户组新增/编辑/删除

【功能说明】对用户组信息进行维护，同时可以对列表展示的用户进行分组

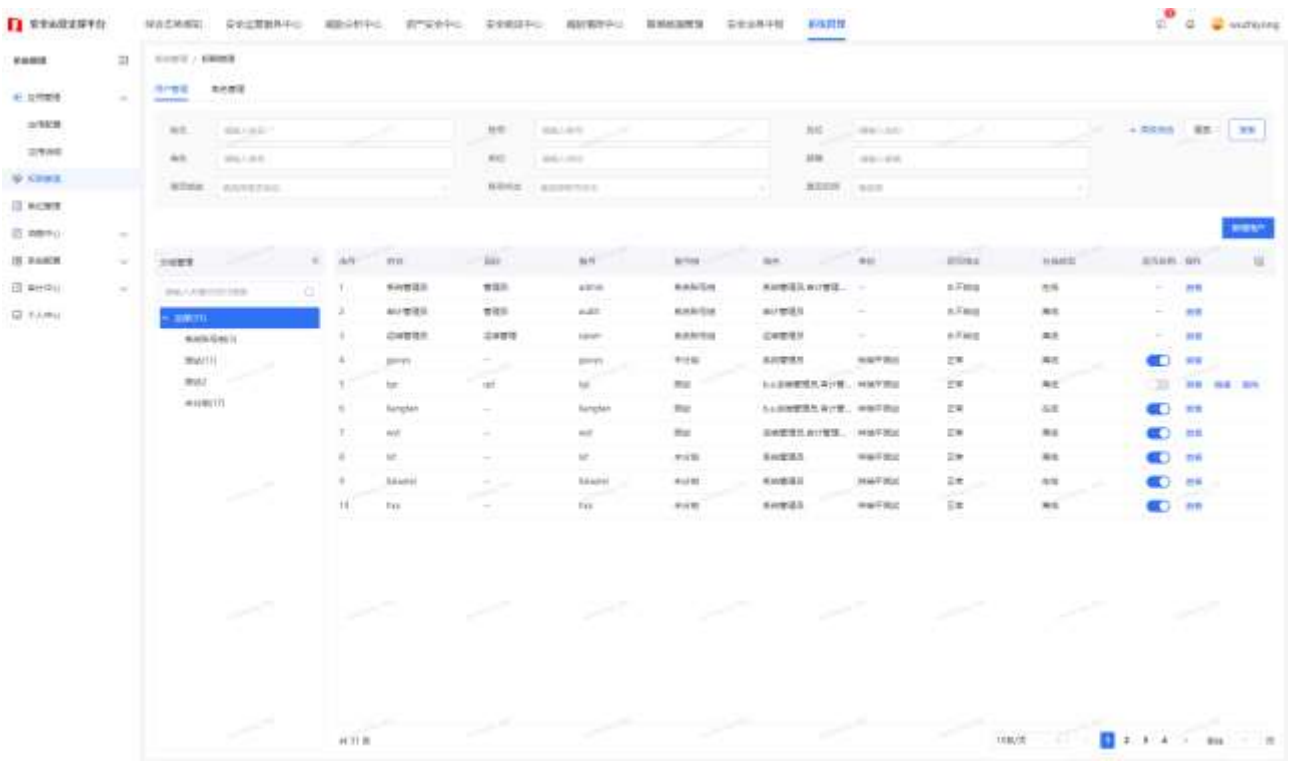


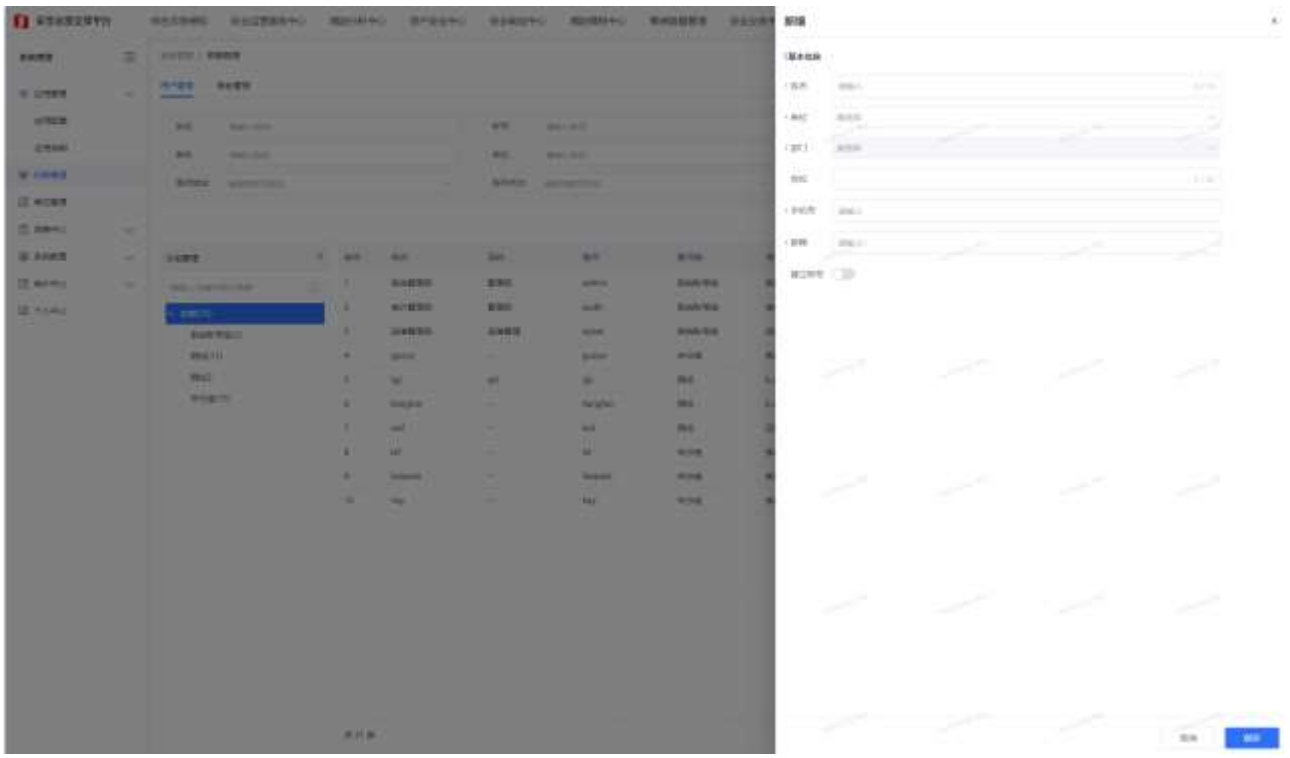


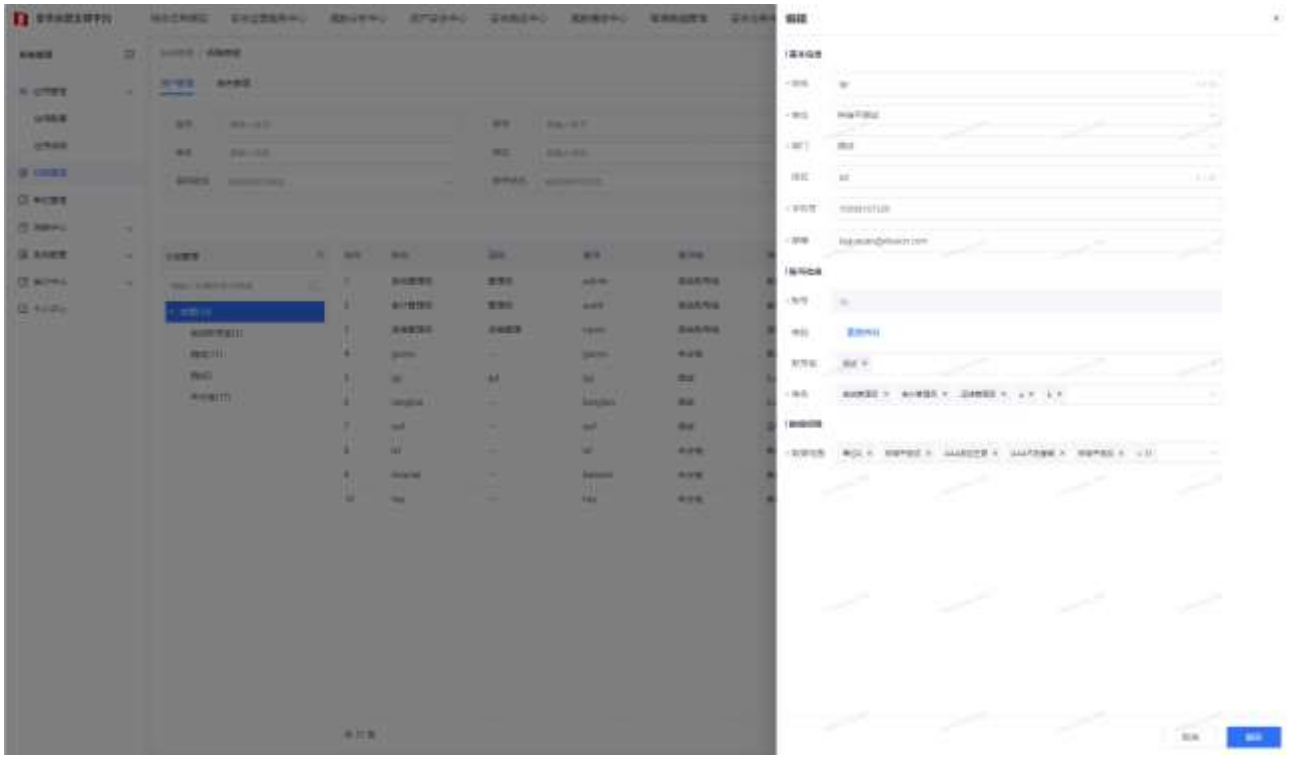


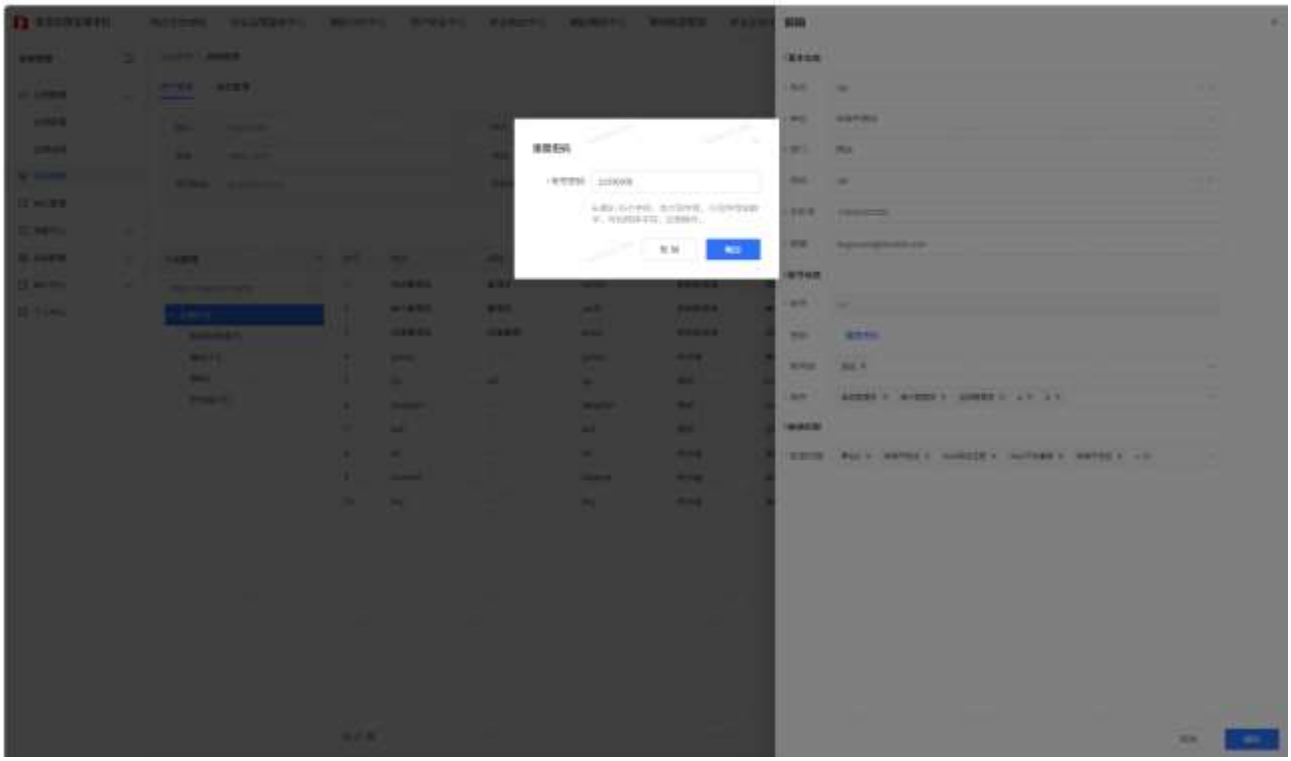
3.1.2.1.2 用户新增/编辑/删除/查看

【功能说明】对用户信息进行基本维护包括有账号和无账号的，只有在用户停用时才能进行编辑和删除操作，以及密码重置；



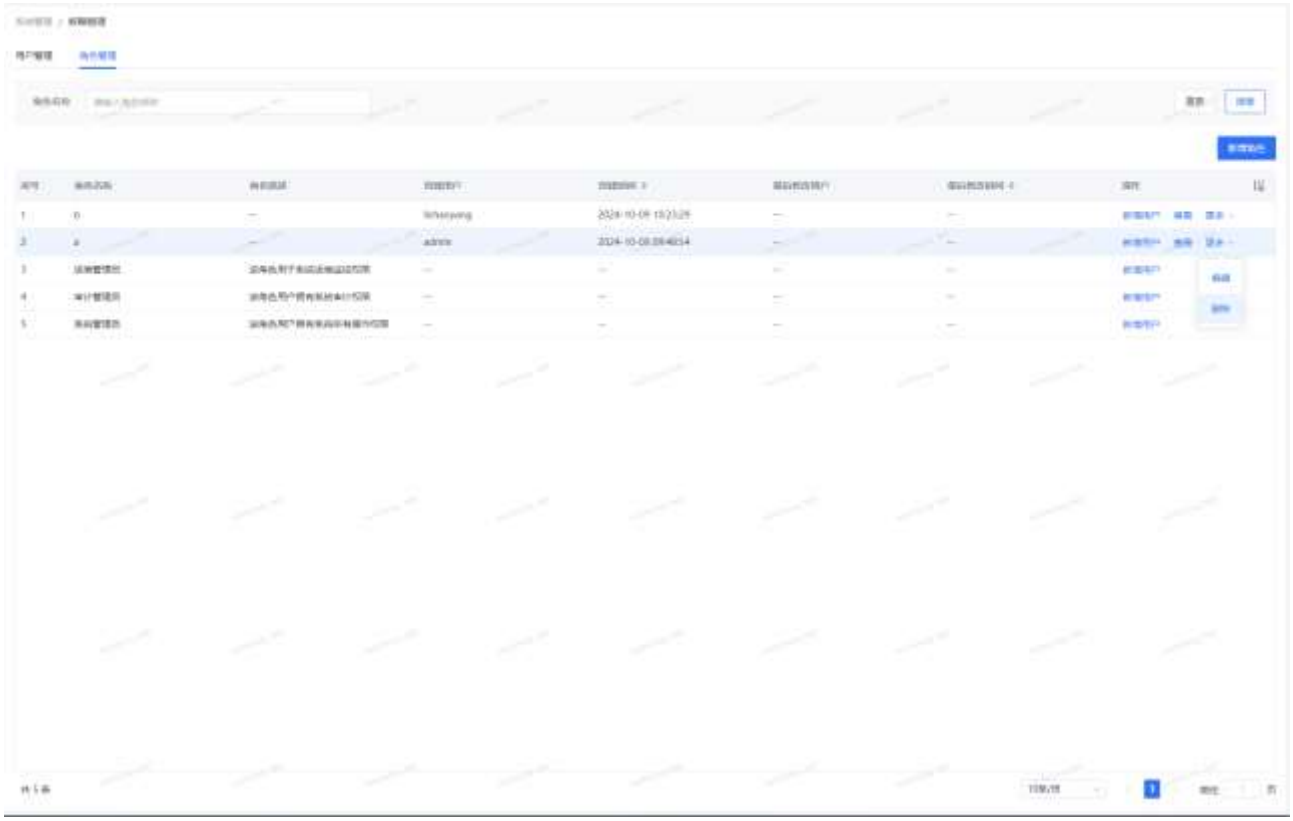






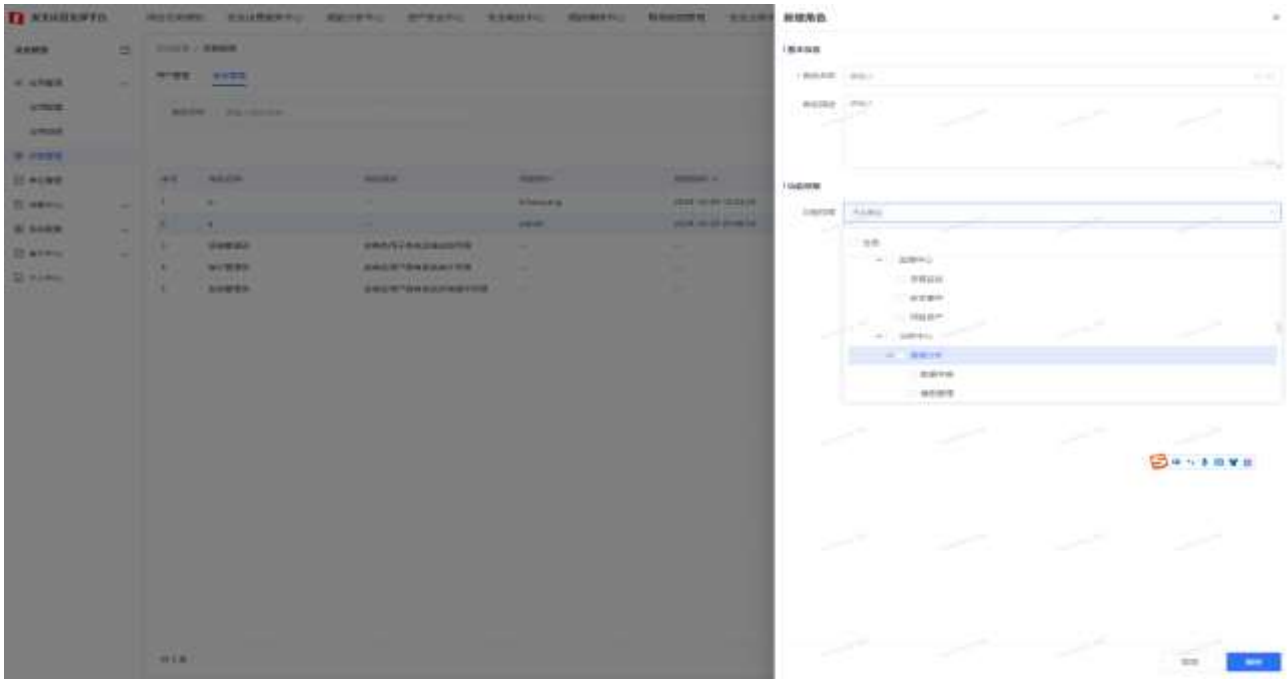
3.1.2.2 角色管理

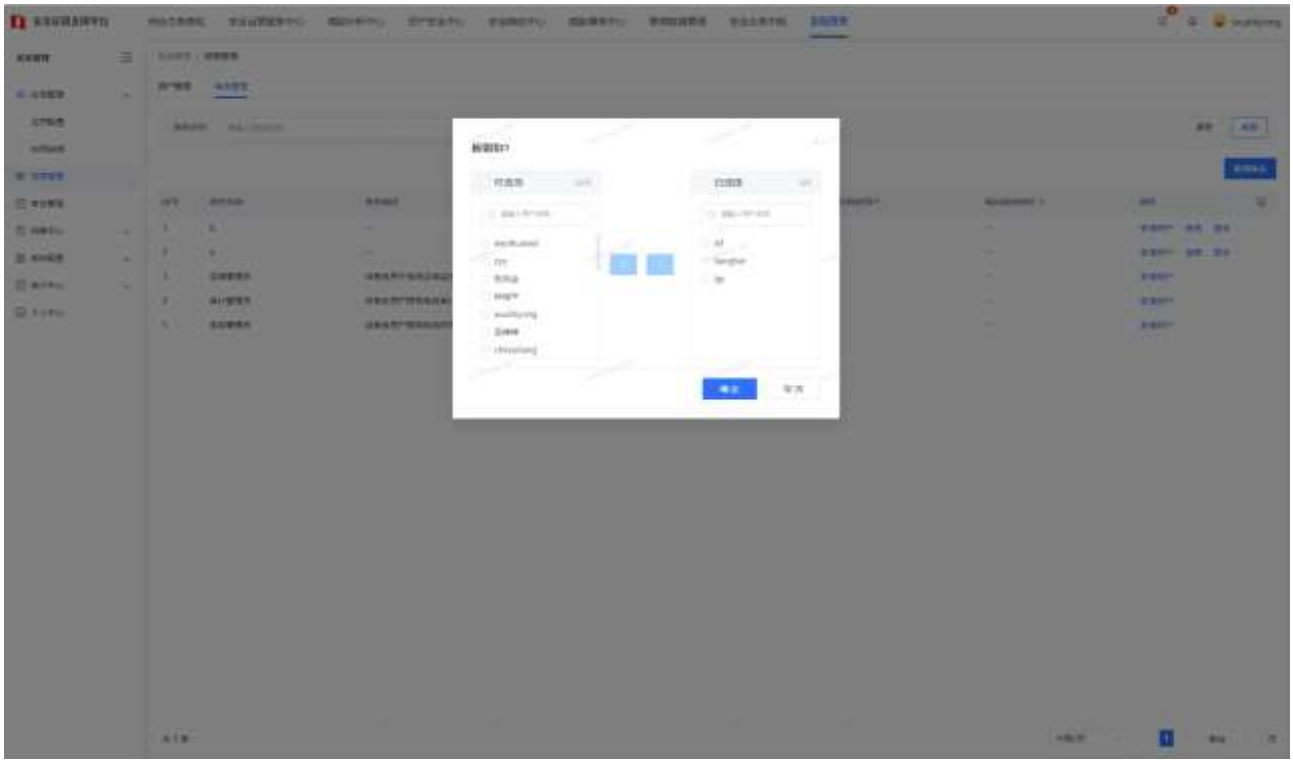
【功能说明】系统角色信息的维护，以及每个角色对应菜单和按钮权限的分配



3.1.2.2.1 用户新增/编辑/删除/查看/角色选择用户

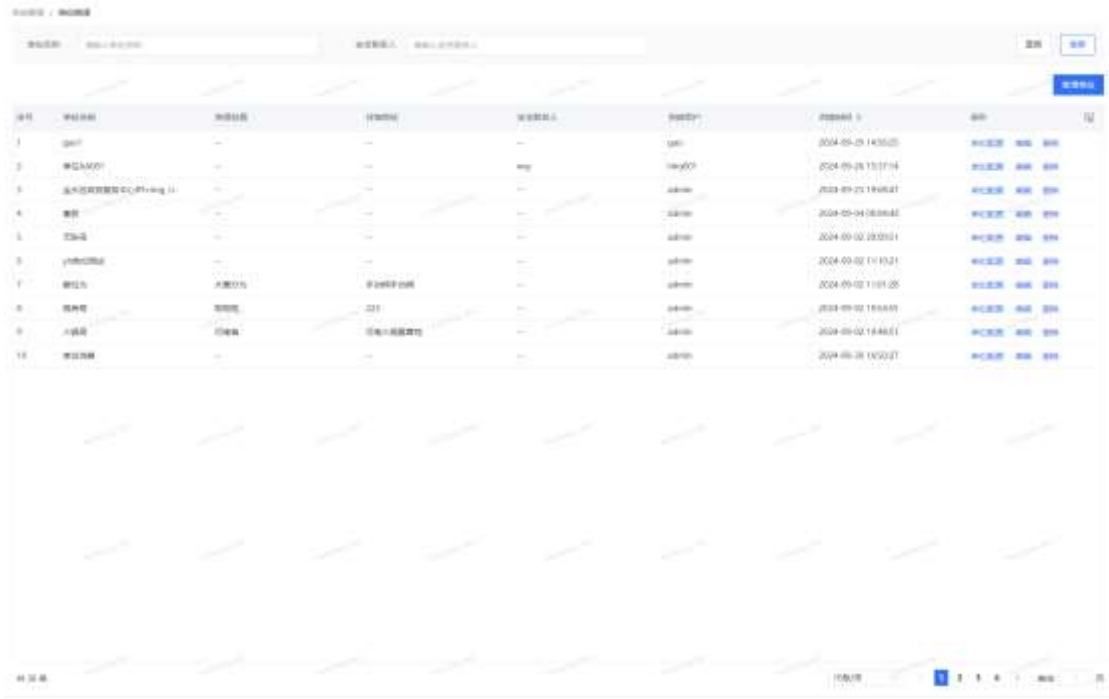
【功能说明】系统角色的新增、修改、删除、查看，以及给角色选择对应的用户，实现用户分配角色；





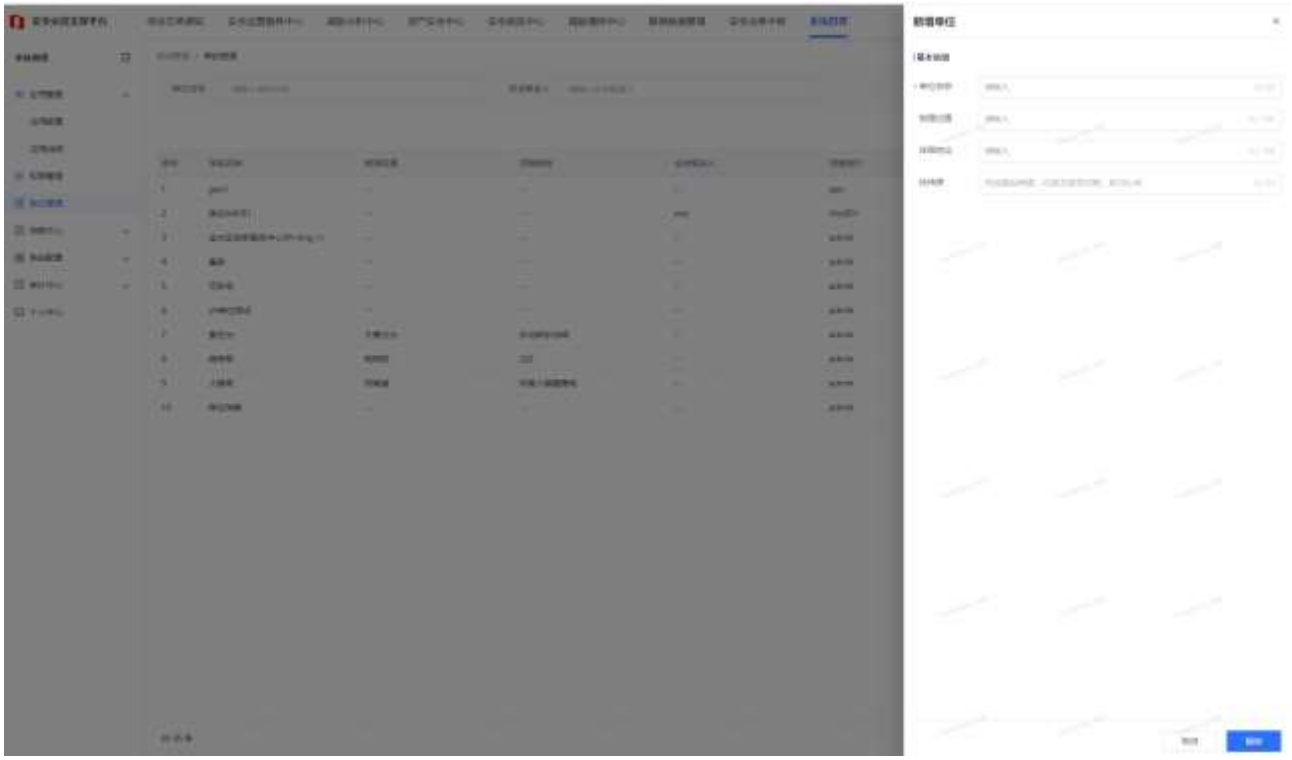
3.1.3 单位管理

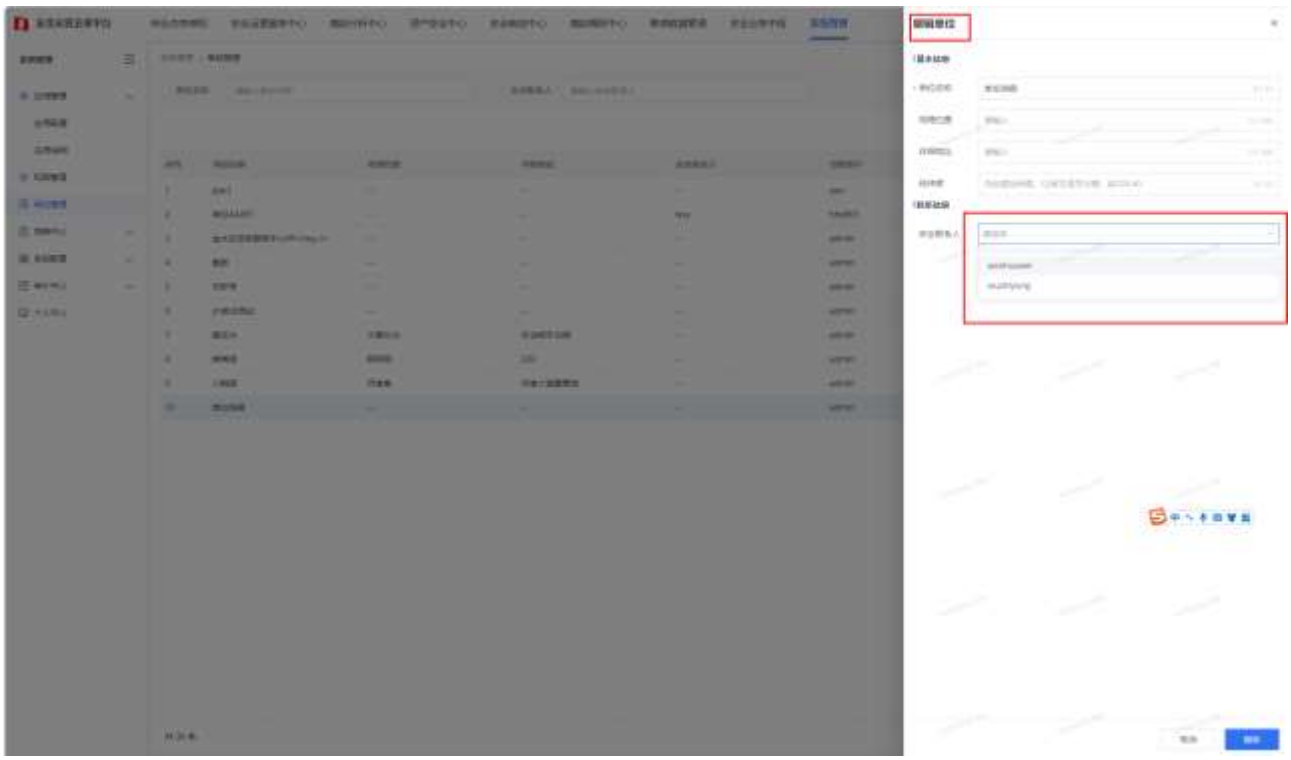
【功能说明】单位基本信息的维护，以及单位包含的部门信息和网络域信息的维护。



3.1.3.1 单位管理新增/修改/删除

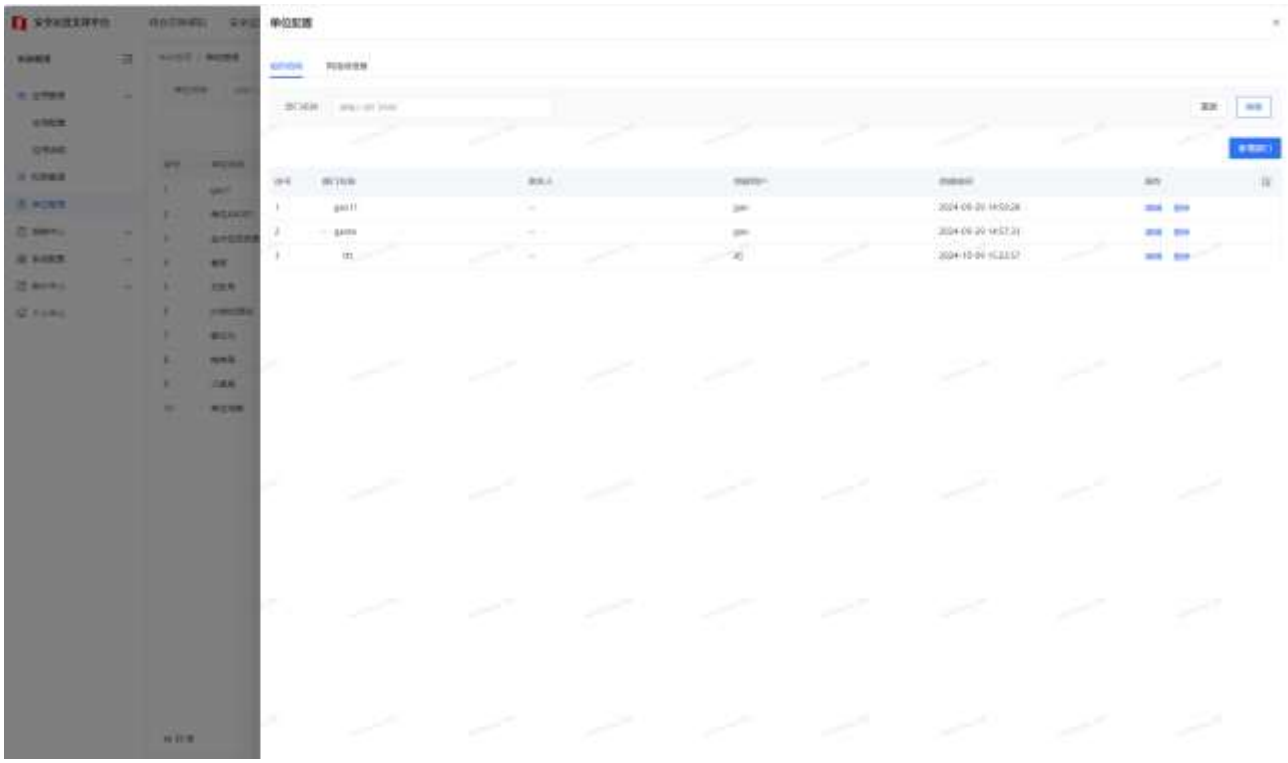
【功能说明】单位基本信息的维护，设置安全联系人

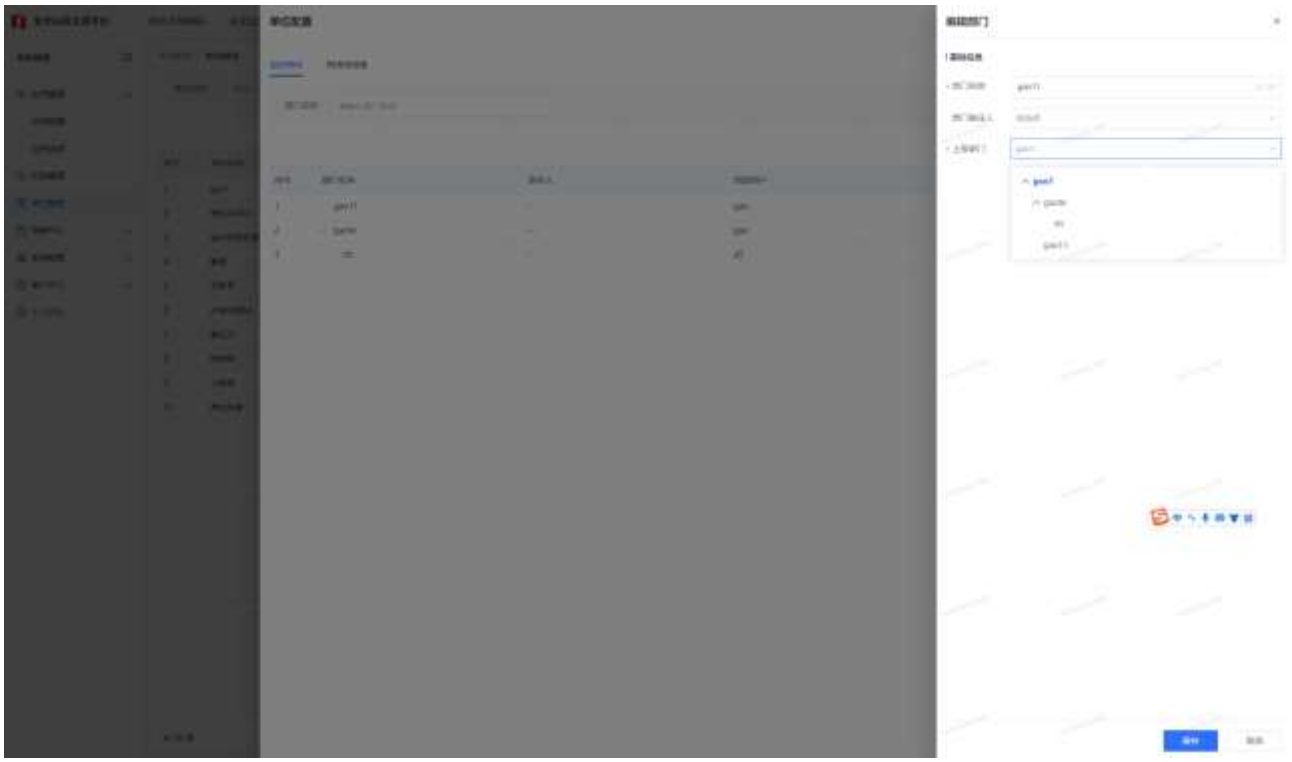




3.1.3.2 组织机构新增/修改/删除

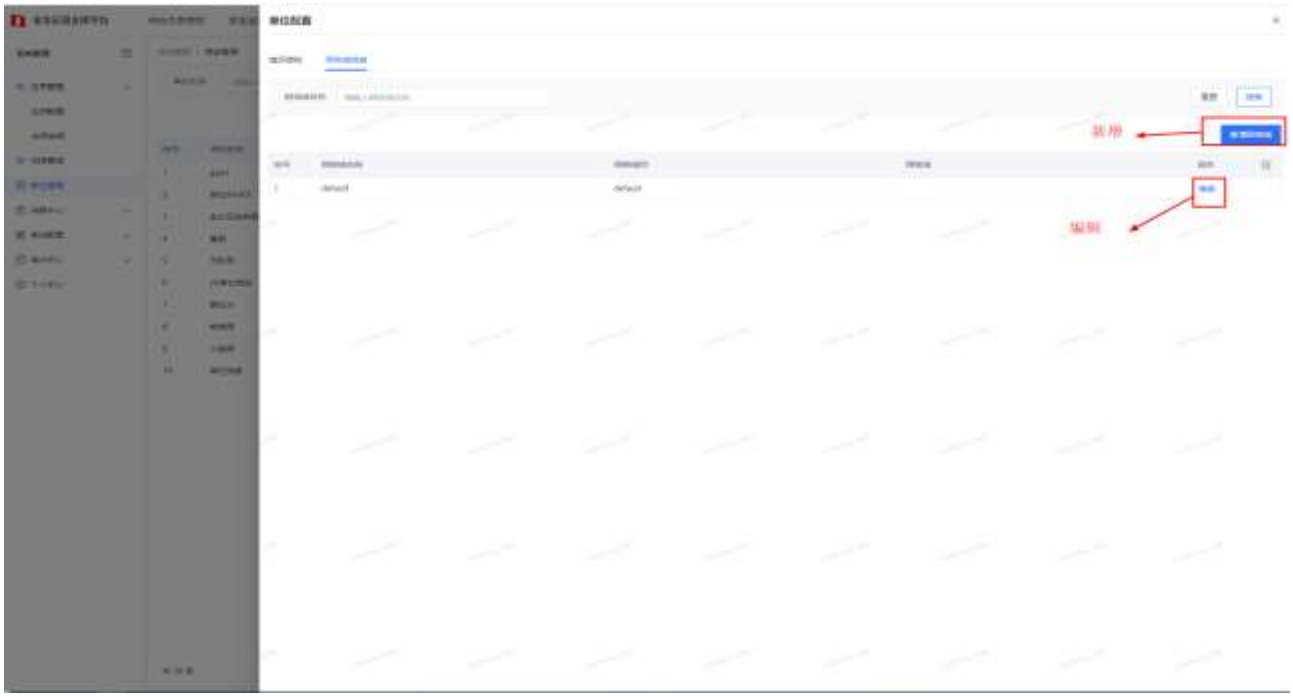
【功能说明】单位下面组织机构树的展示、创建与维护；

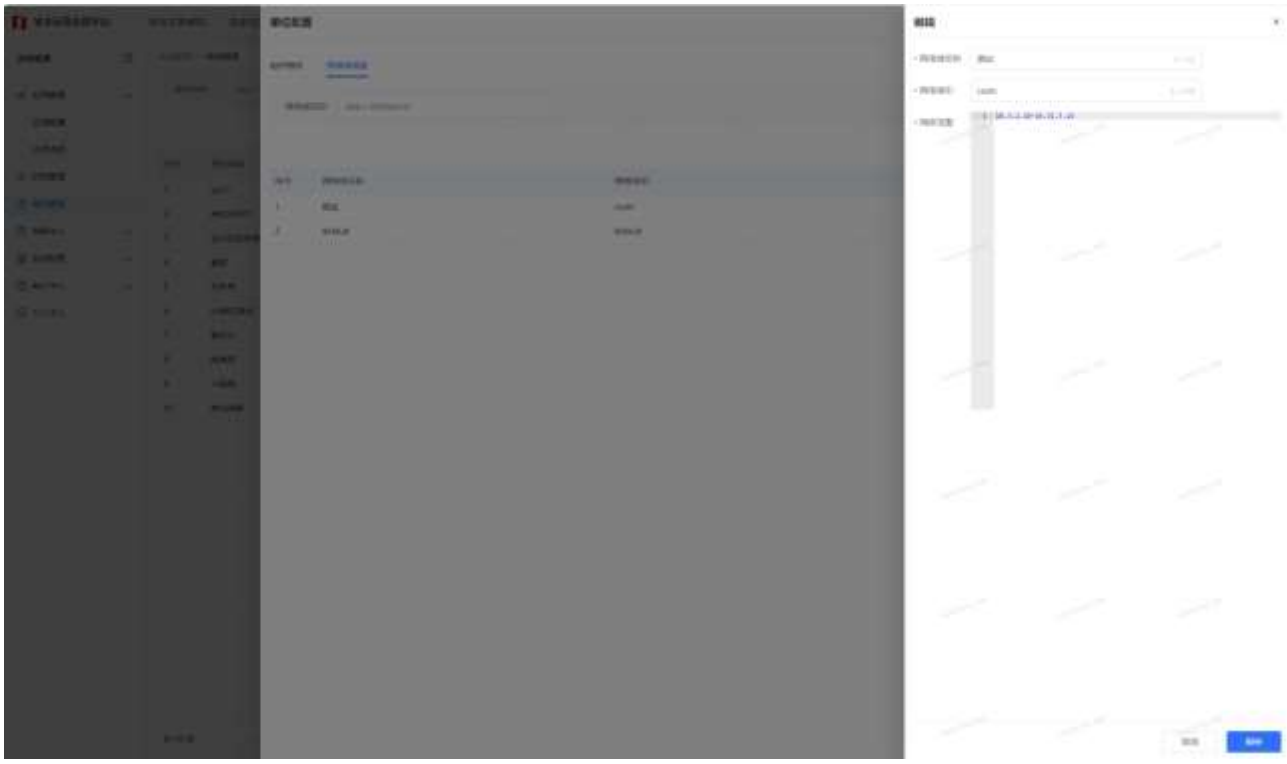




3.1.3.3 网络域信息新增/修改/删除

【功能说明】新增单位时，会初始化一个 default 的网络域，只能编辑不能删除，然后可以新增、修改和删除其他的网络域；



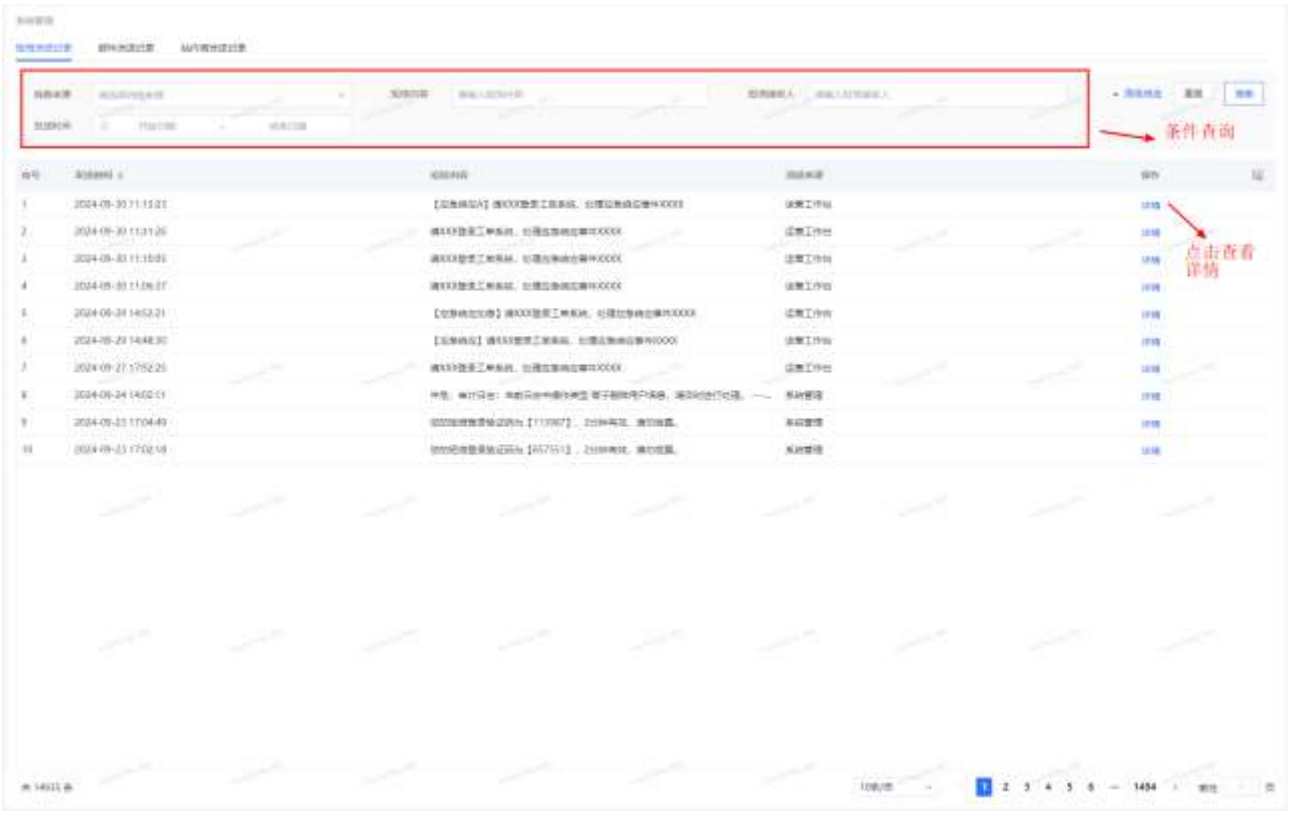


3.1.4 消息中心

3.1.4.1 消息记录

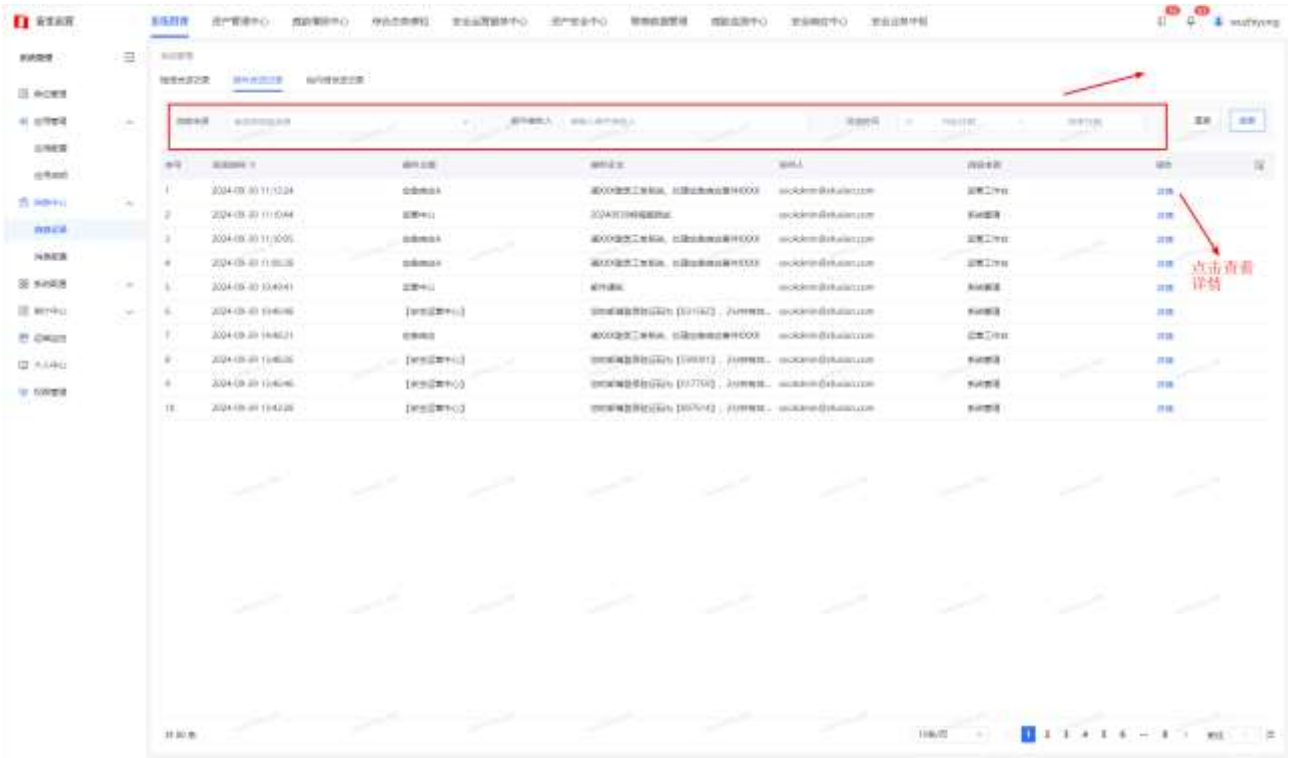
3.1.4.1.1 短信发送记录

【功能说明】系统内所有短信发送记录的查询与展示；



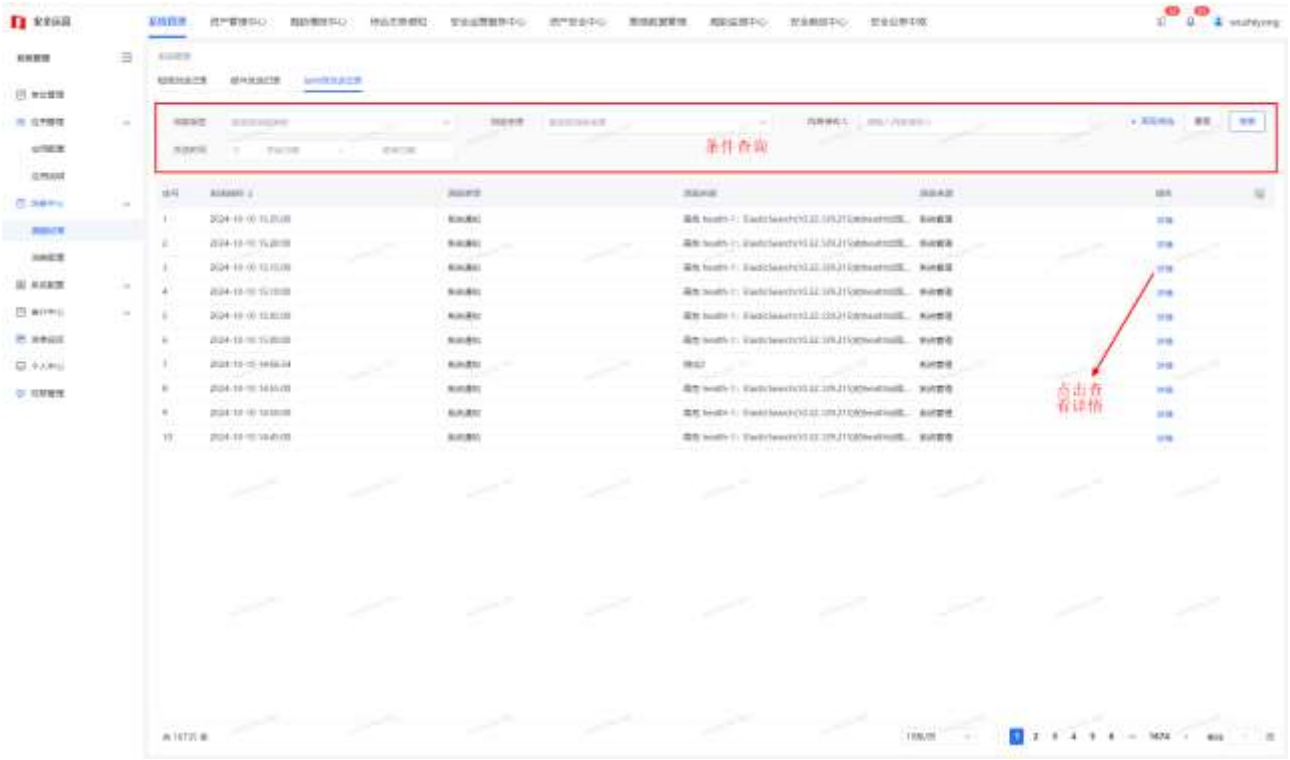
3.1.4.1.2 邮件发送记录

【功能说明】系统内所有进行邮件发送操作的记录查询



3.1.4.1.3 站内信发送记录

【功能说明】系统内所有进行站内信发送操作的记录查询

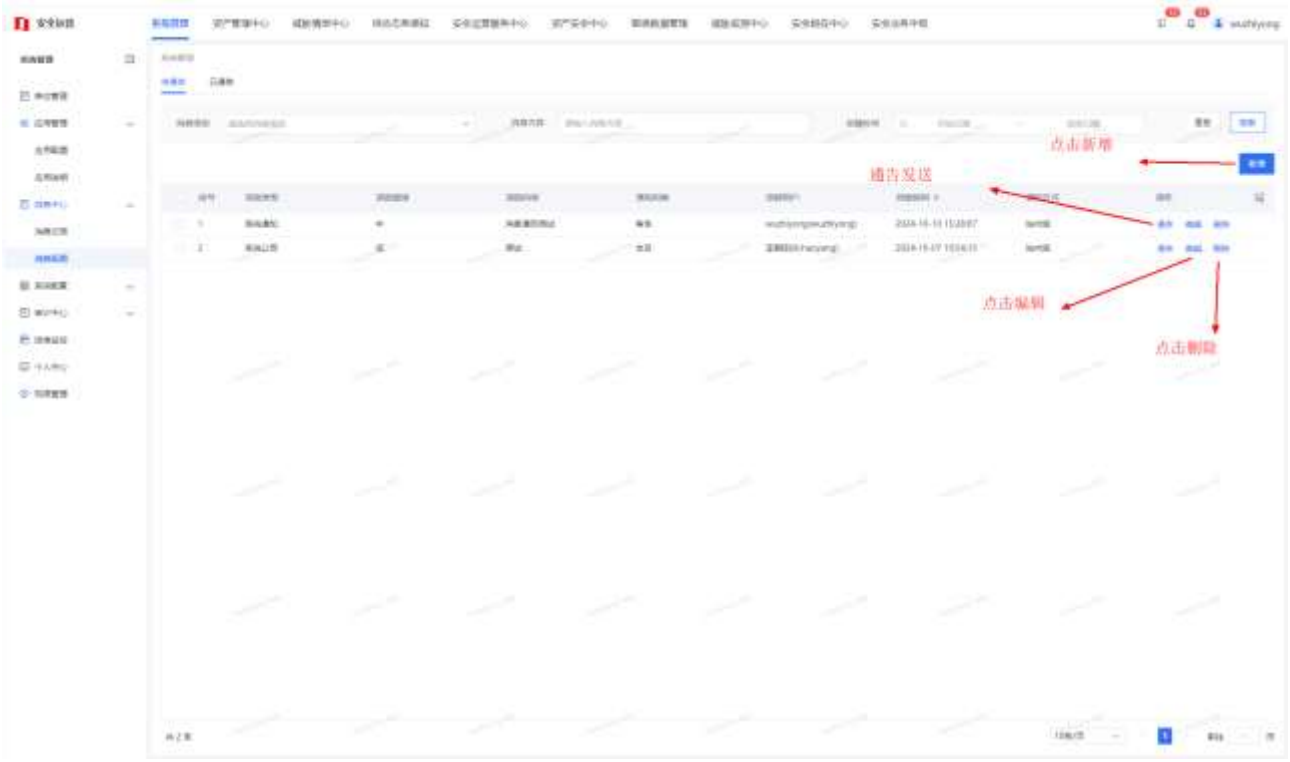


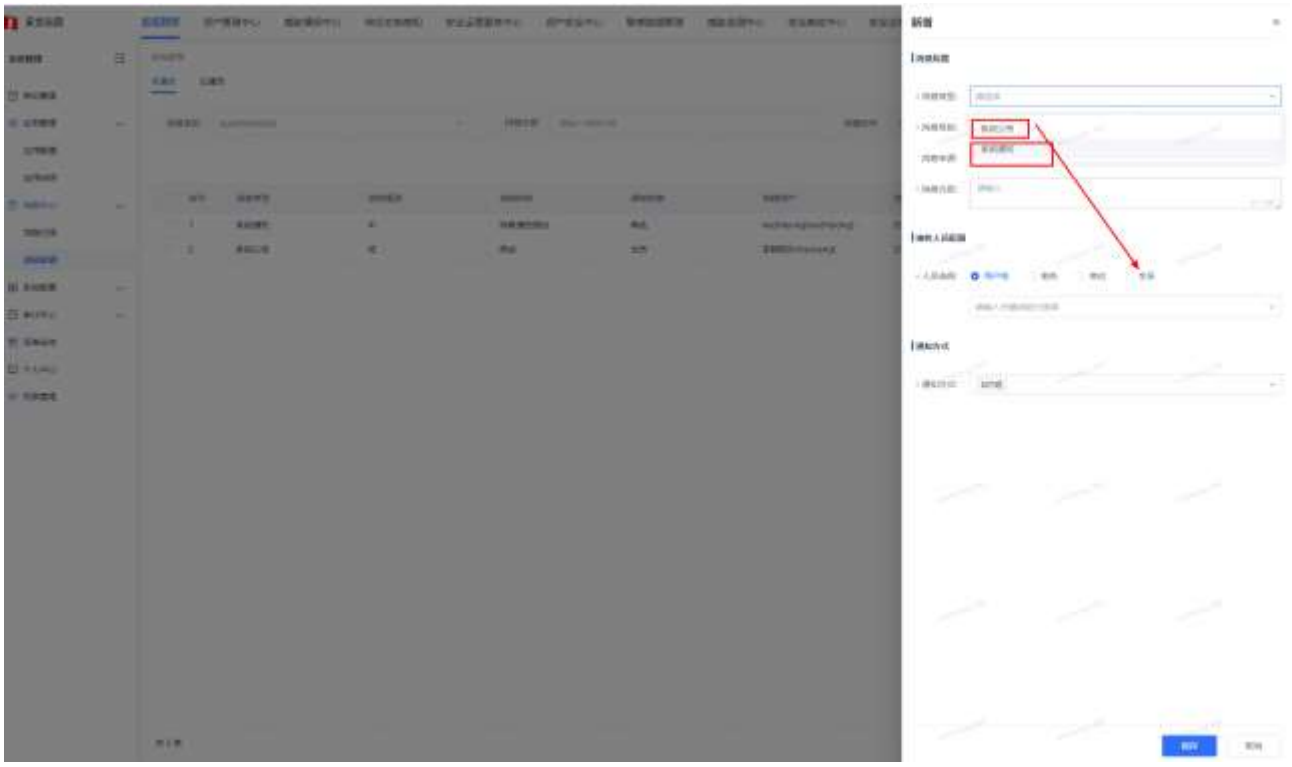
3.1.4.2 消息配置

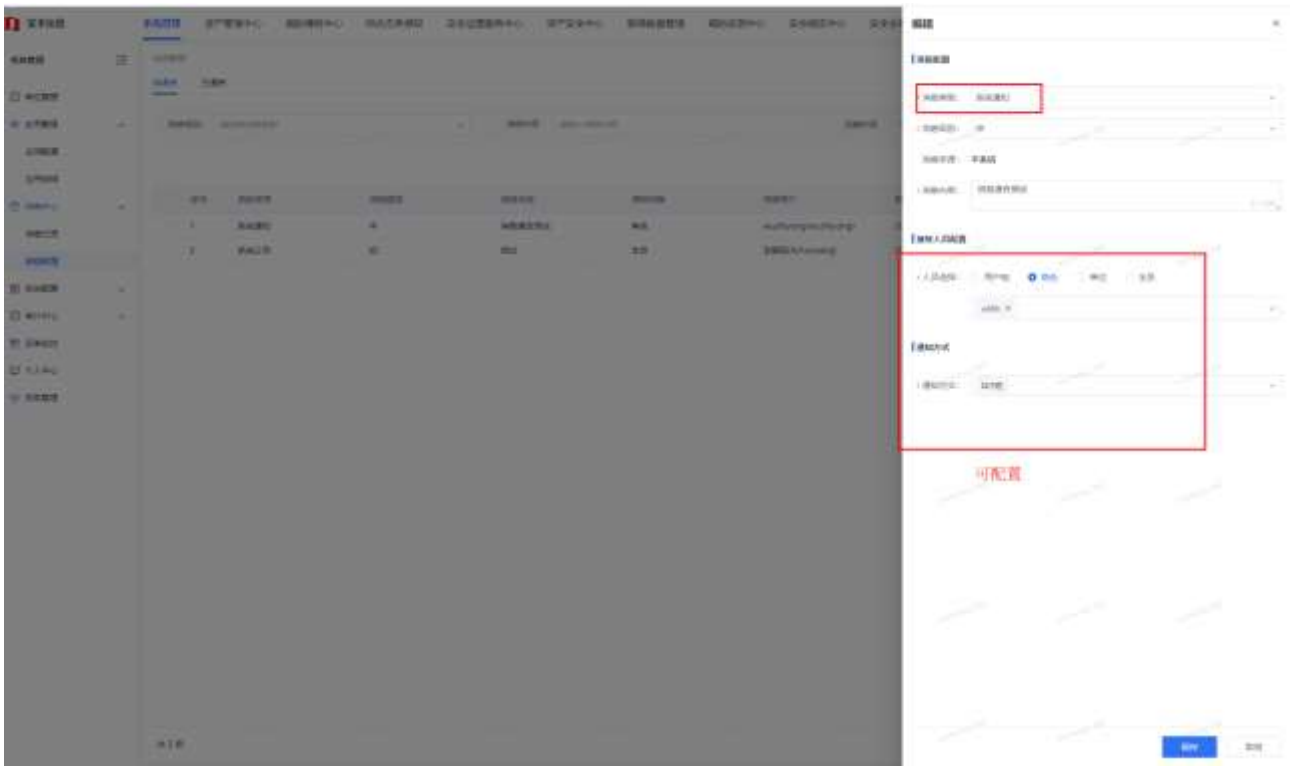
【功能说明】这对于系统通知和系统公告来进行的消息配置，系统通知可以将消息设置为发送给用户组，角色，单位、全员以及个人，同时形式的话可以设置为站内短，邮件，短信等；系统公告的话只能是全员，形式是站内短；

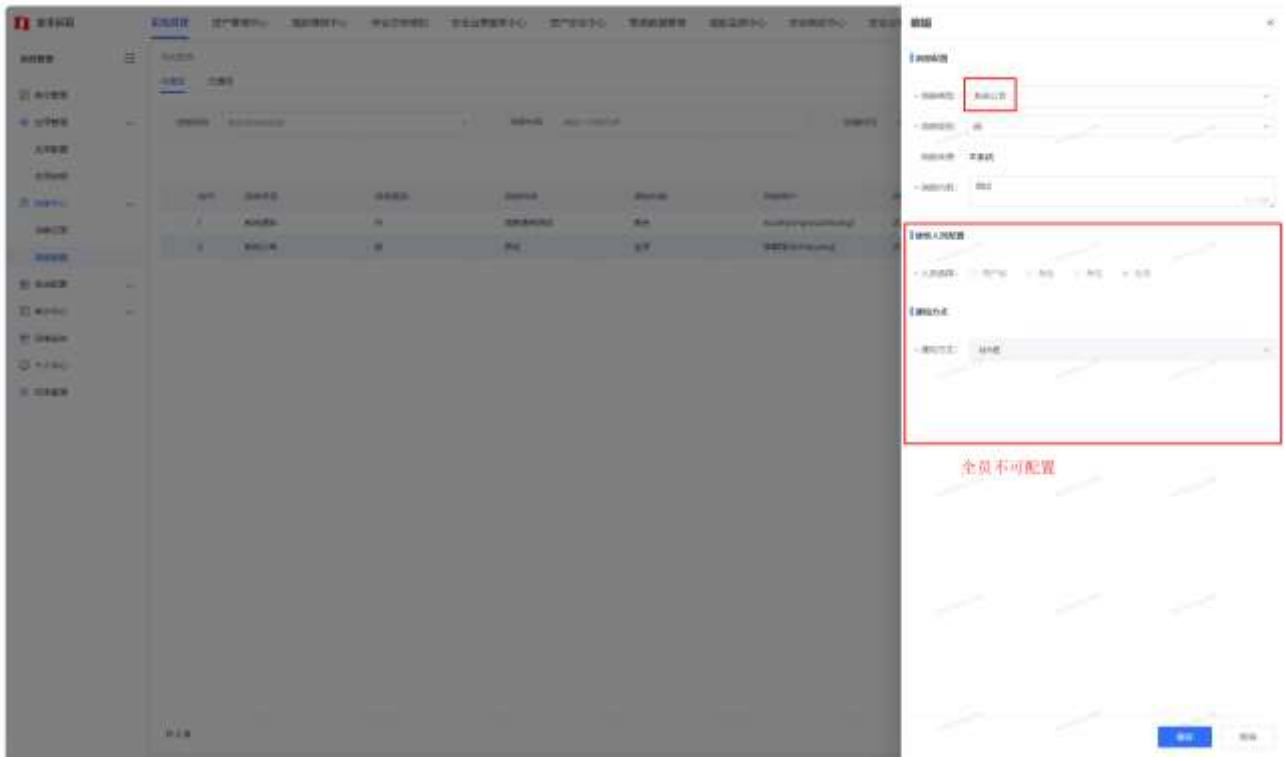
3.1.4.2.1 待通告

【功能说明】待通告中负责消息通告的信息的新增、修改、删除以及发送通告等操作


点击新增
通告发送
点击编辑
点击删除

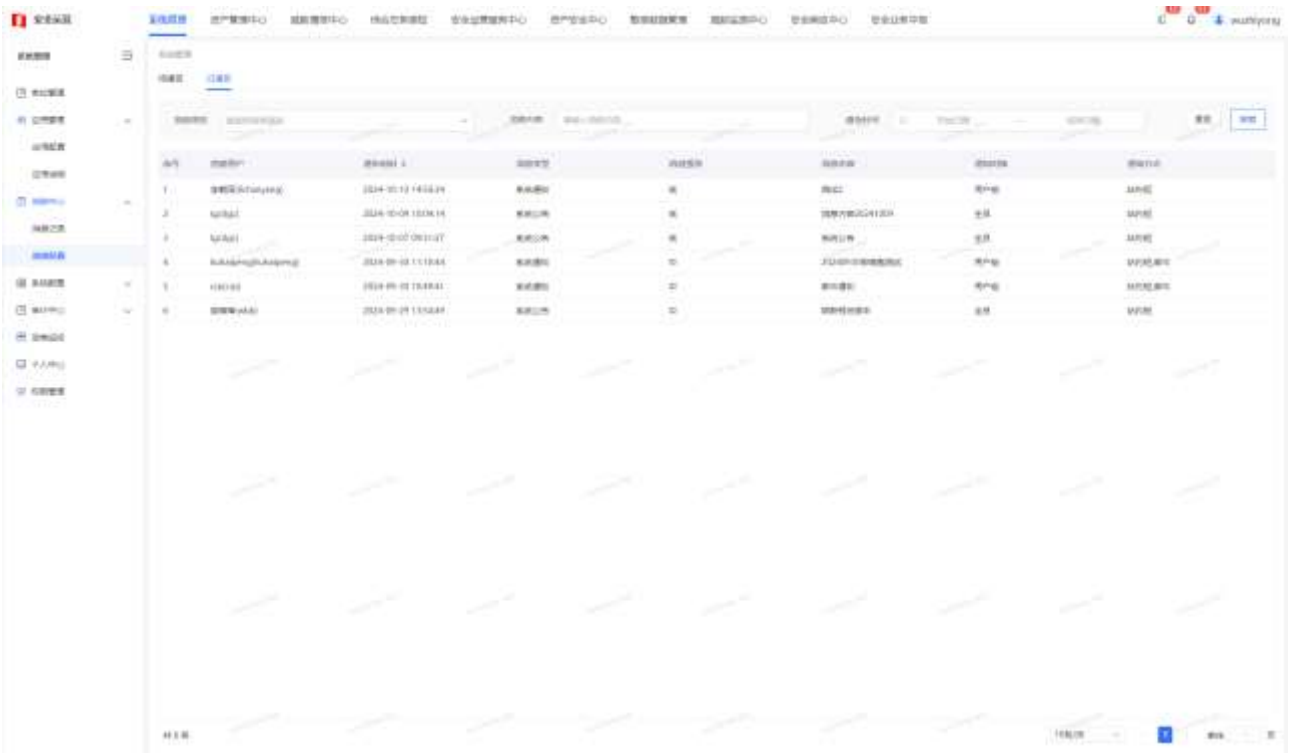






3.1.4.2.2 已通告

【功能说明】已经进行过通告的消息通告的列表查询与展示



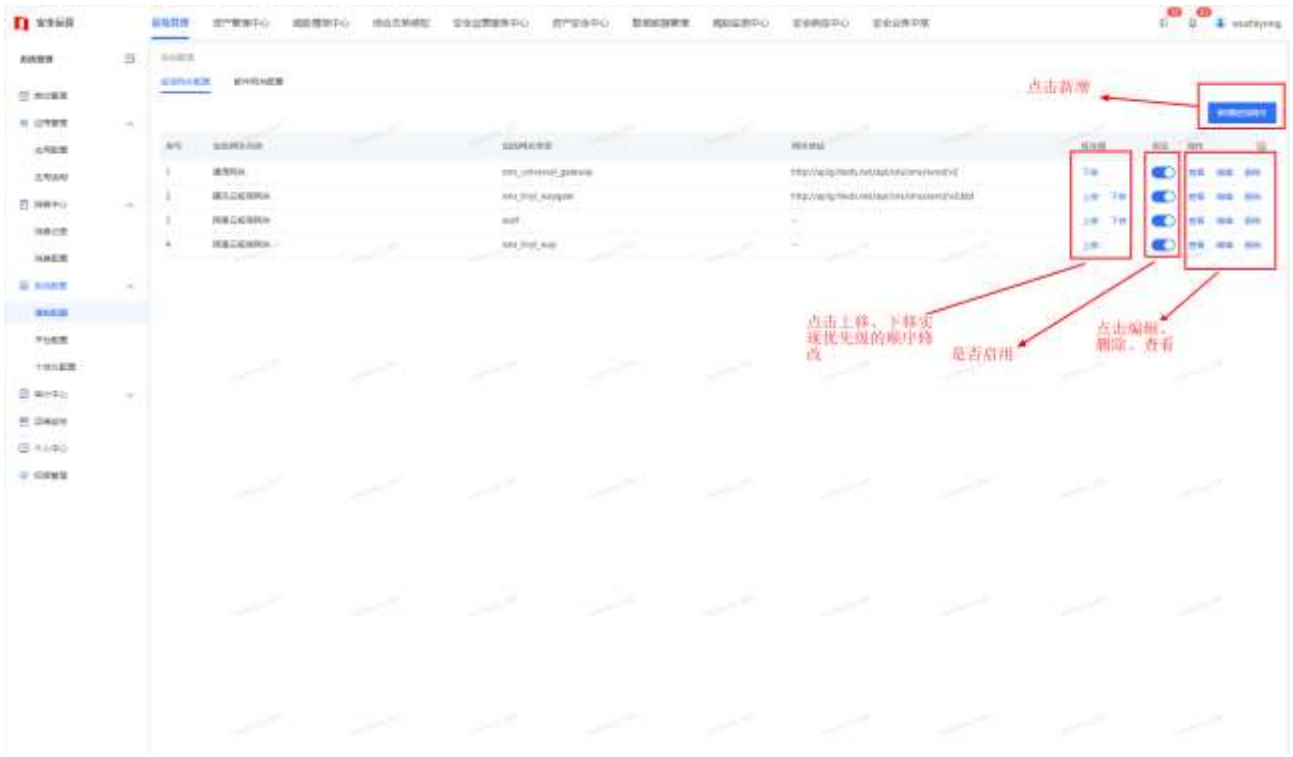
3.1.5 系统配置

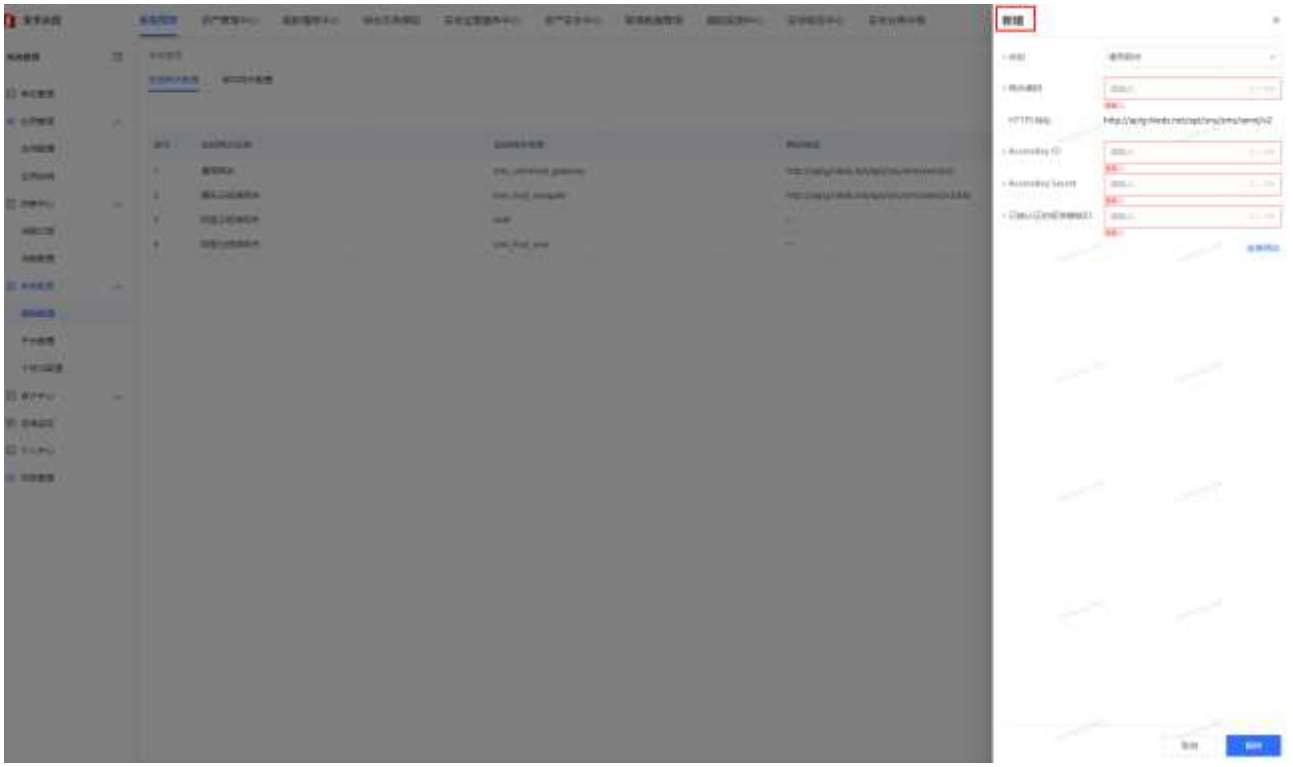
3.1.5.1 通知配置

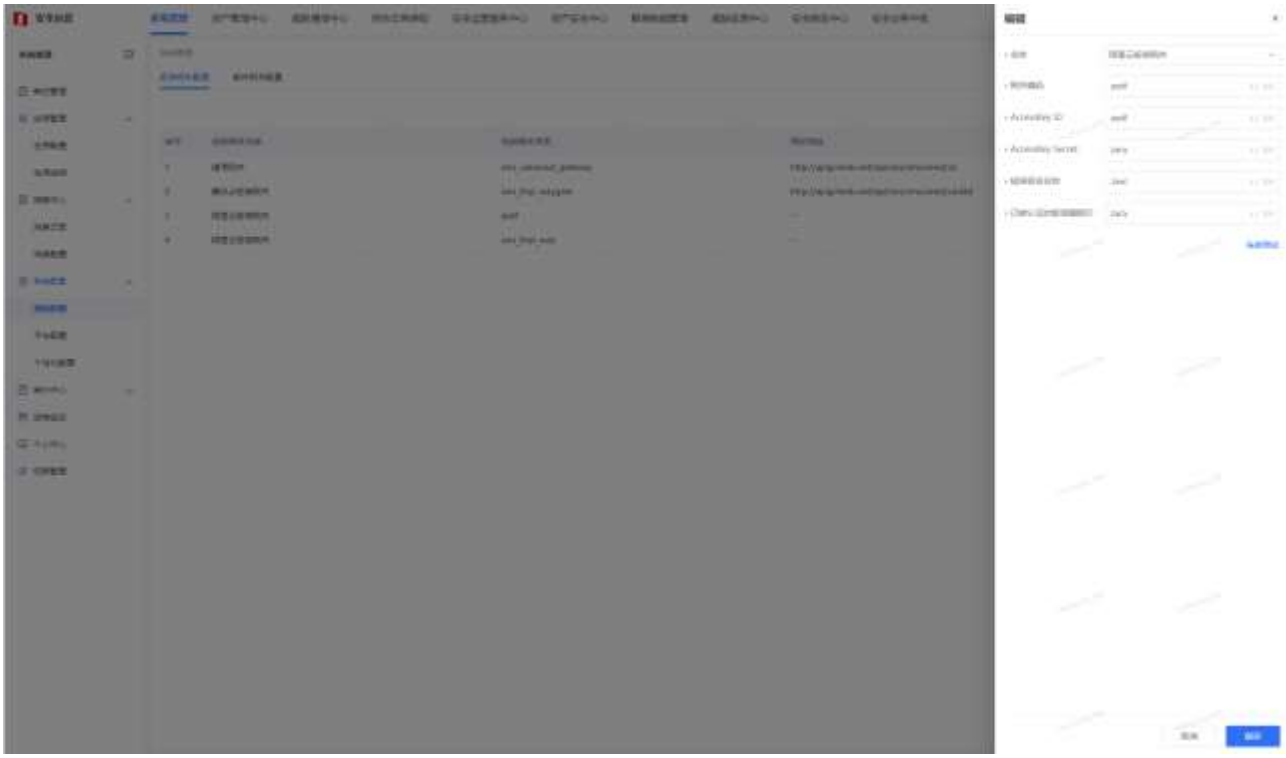
【功能说明】针对于短信网关配置和邮件网关配置的信息维护；

3.1.5.2 短信网关配置

【功能说明】针对发送短信操作进行的不同网关的配置的新增、修改、删除，以及优先级排序，是否启用等；

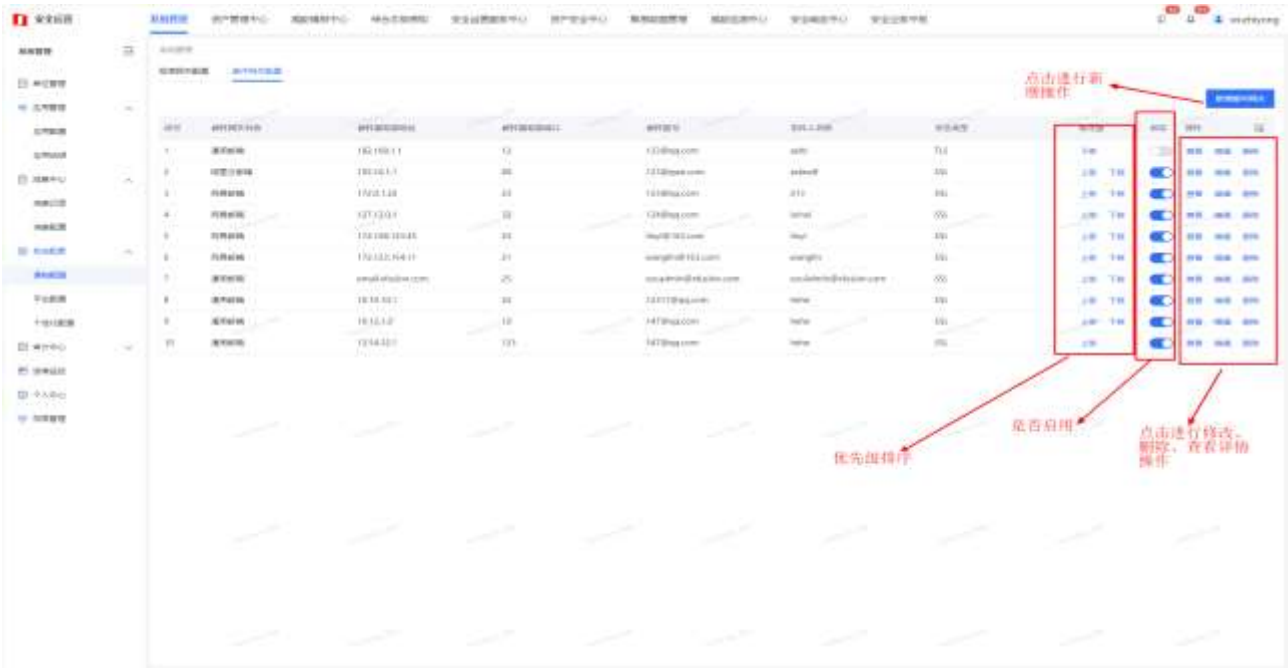

点击新增
点击上移、下移实现优先级的顺序修改
是否启用
点击编辑、删除、查看

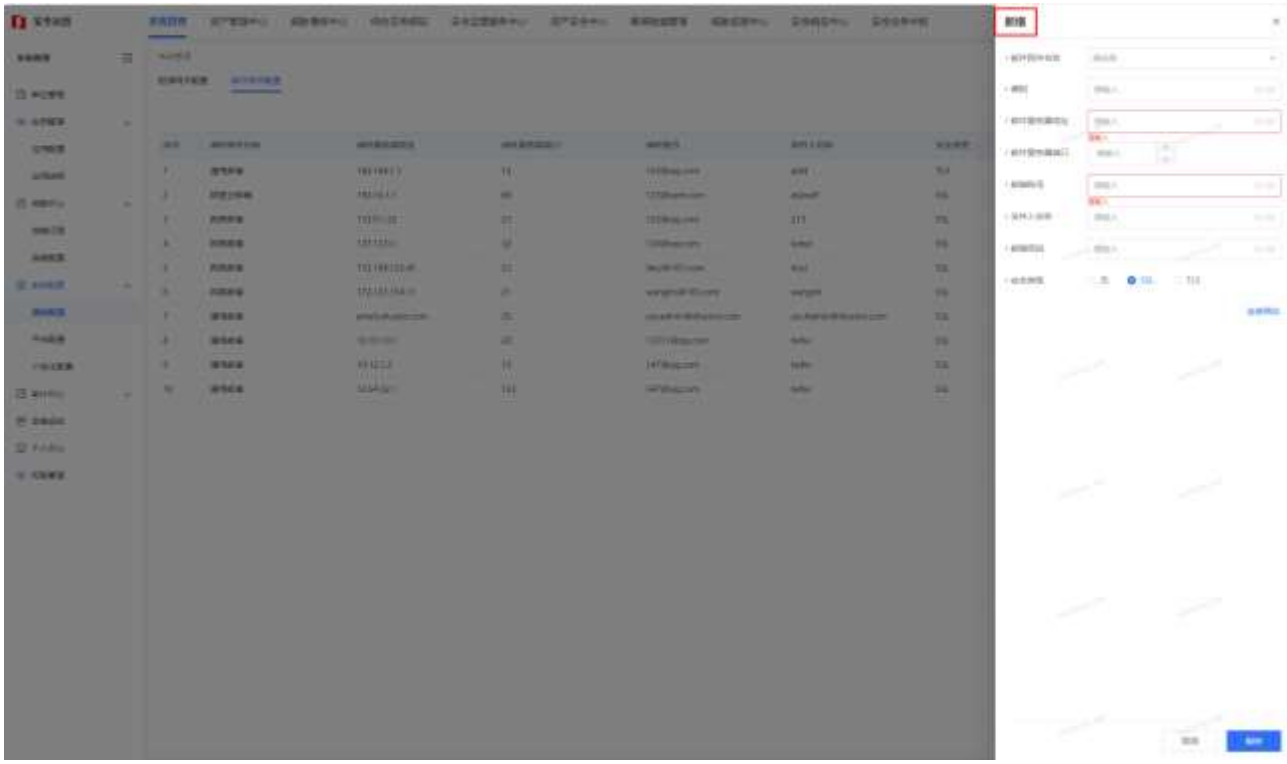


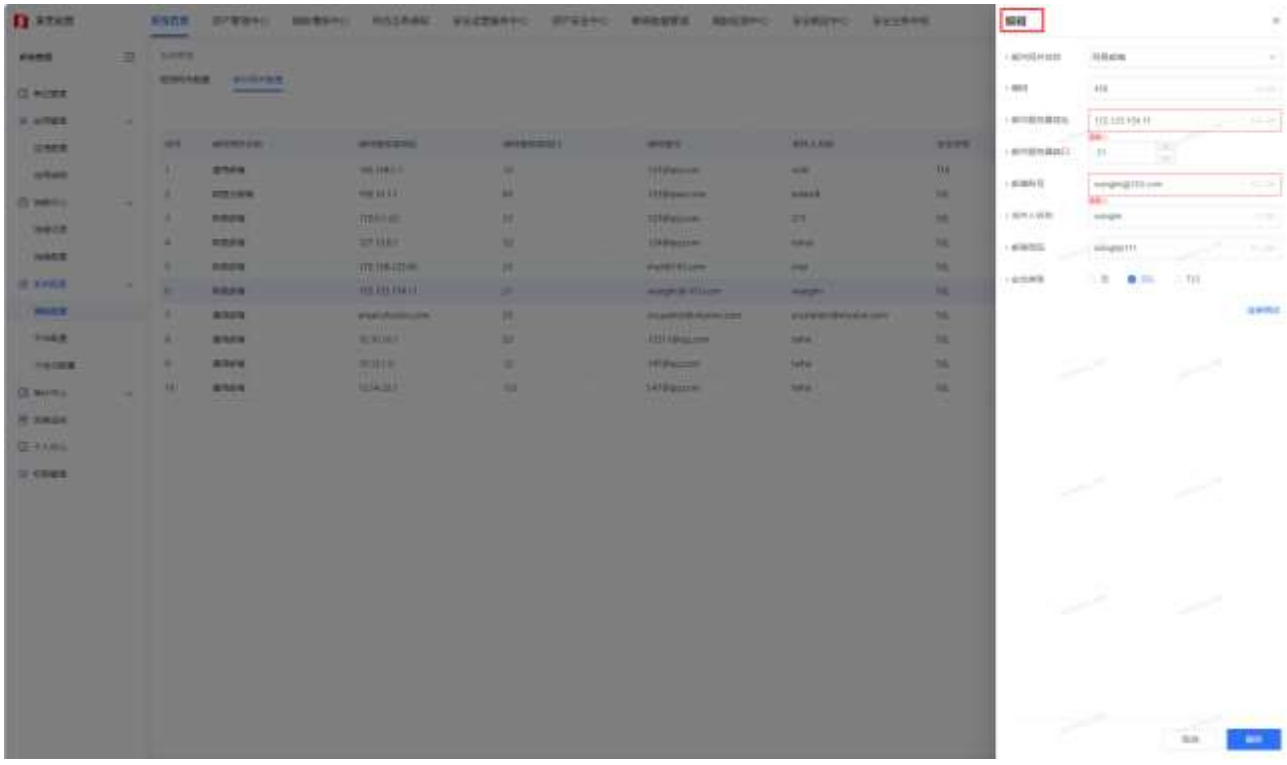


3.1.5.3 邮件网关配置

【功能说明】针对邮件发送的不同的网关配置信息的新增、修改、删除、查看、是否启用以及优先级排序的修改







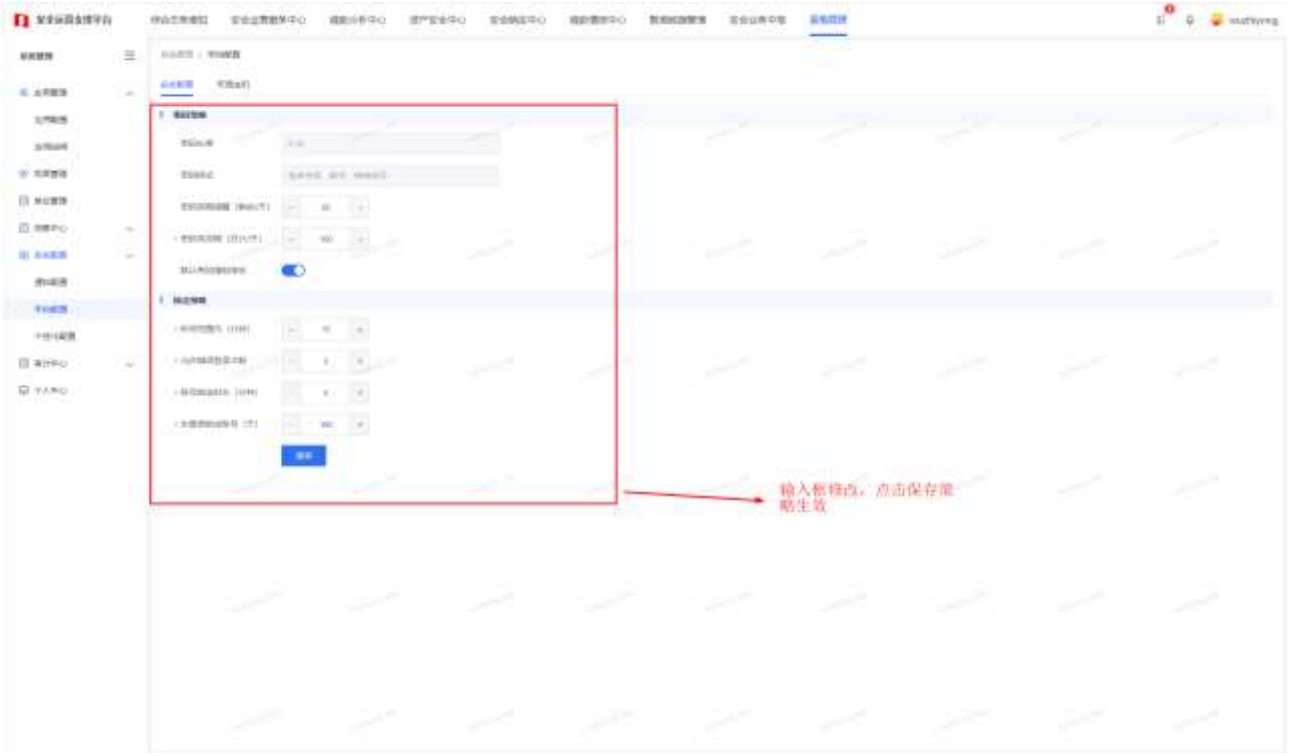
3.1.5.2 平台配置

【功能说明】关于密码策略和账户锁定策略的安全策略的配置，以及可信主机

即安全 ip 白名单的配置功能操作.

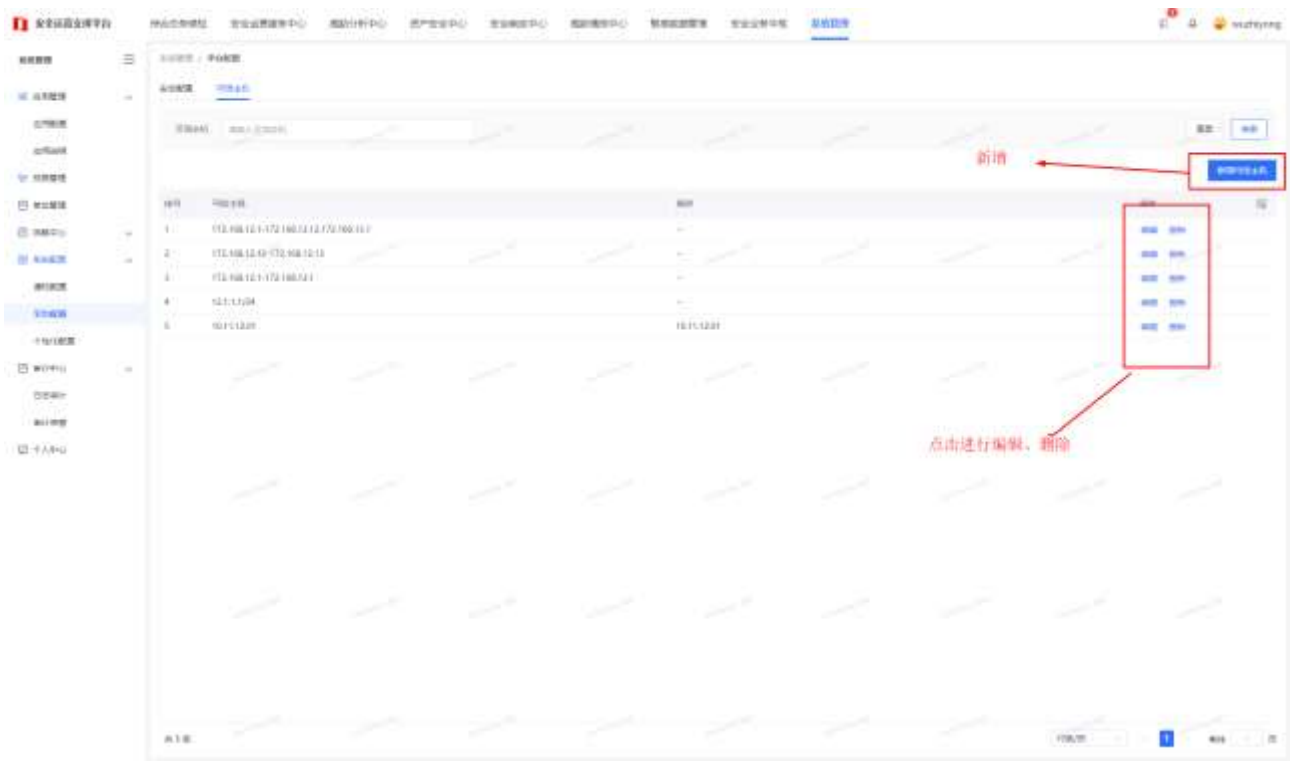
3.1.5.2.1 安全配置

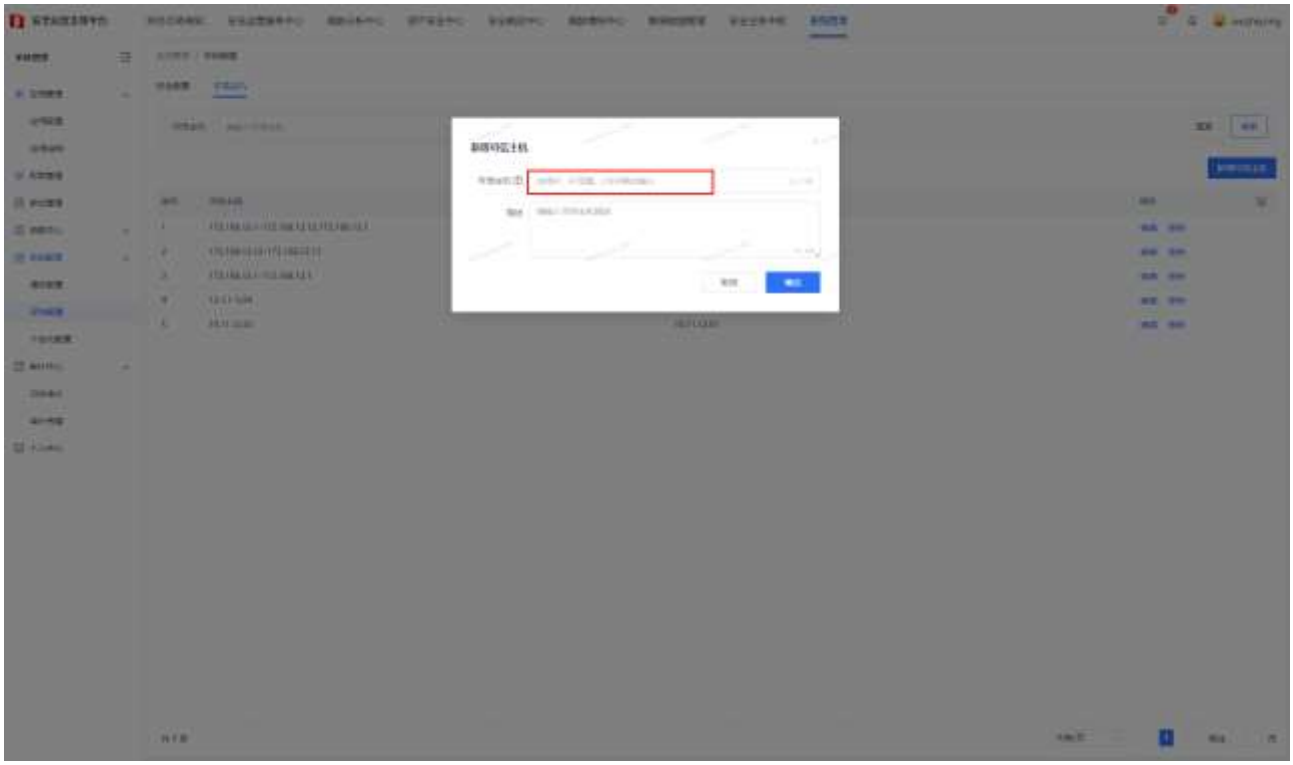
【功能说明】关于系统的密码的长度、格式、到期提醒时间、密码有效期、默认密码强制修改，以及账号的锁定策略的配置信息的维护



3.1.5.2.2 可信主机

【功能说明】可信主机的信息的新增、修改、删除，可以维护 ip、ip 网段、以及 CIDR 的格式，实现对可信主机的限制，保证非可信主机无法访问；





3.1.5.3 个性化配置

【功能说明】关于系统的标题、平台 logo、登录页背景图，以及是否开启水印等的个性化配置；

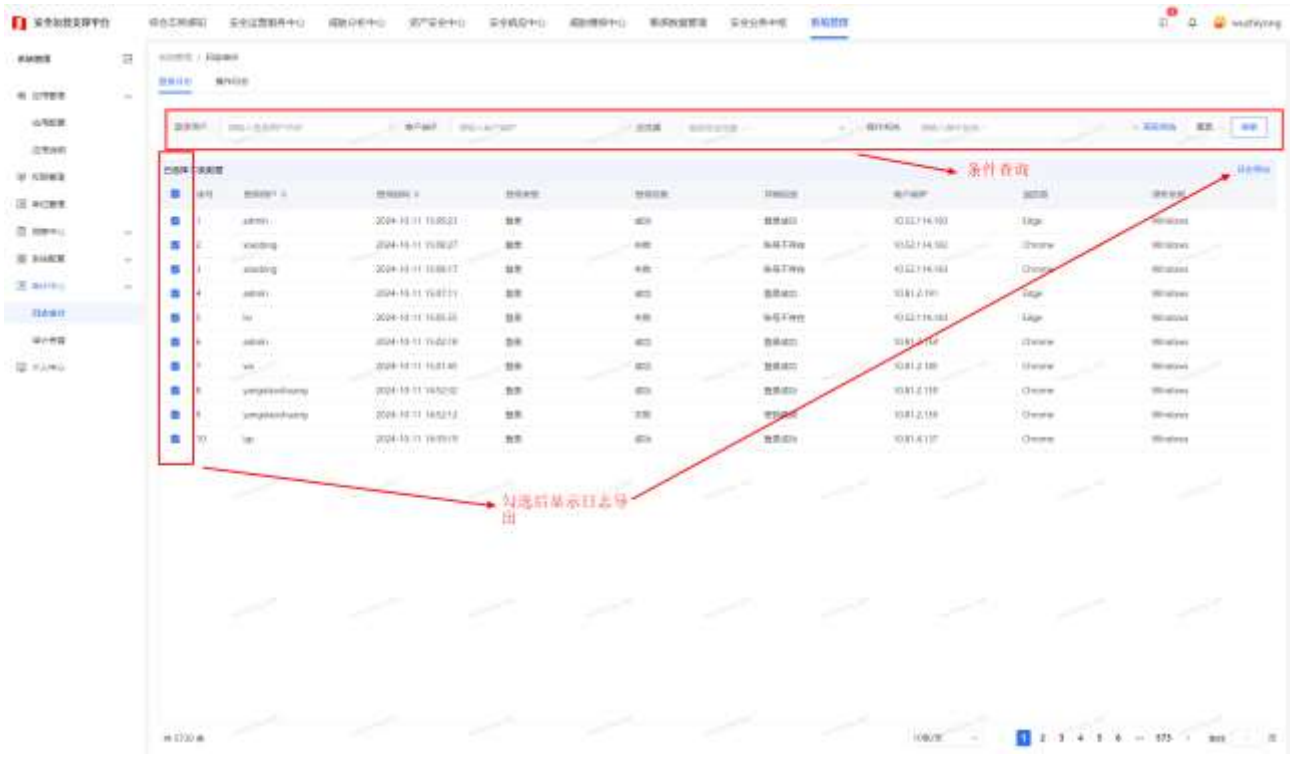
3.1.6 审计中心

3.1.6.1 日志审计

【功能说明】登录和操作日志的日志查询、审计和导出；

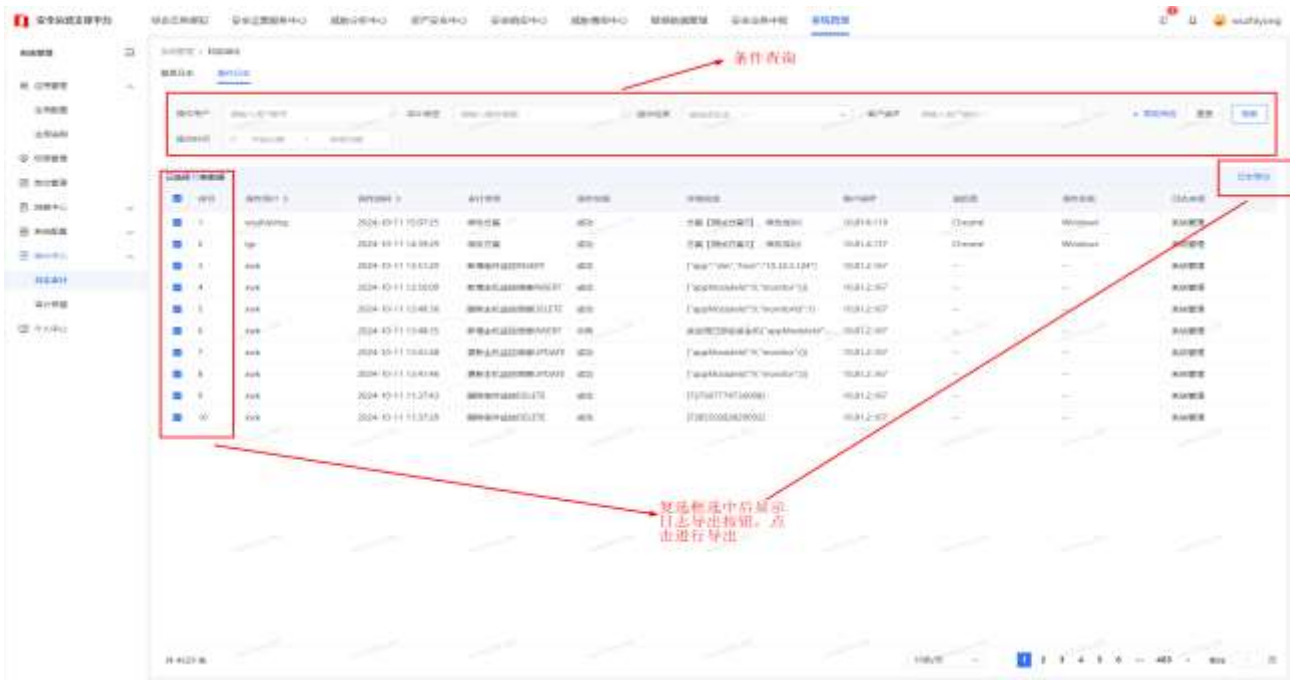
3.1.6.1.1 登录日志

【功能说明】登录日志的查询与导出；



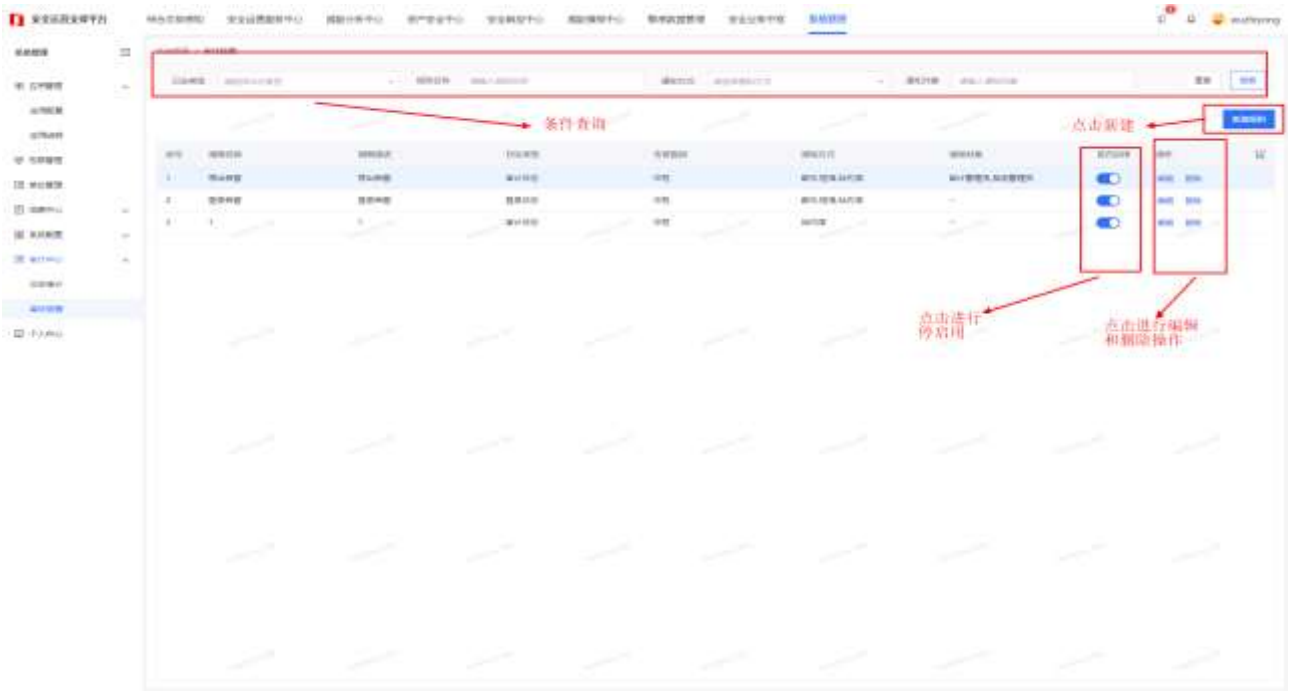
3.1.6.1.2 操作日志

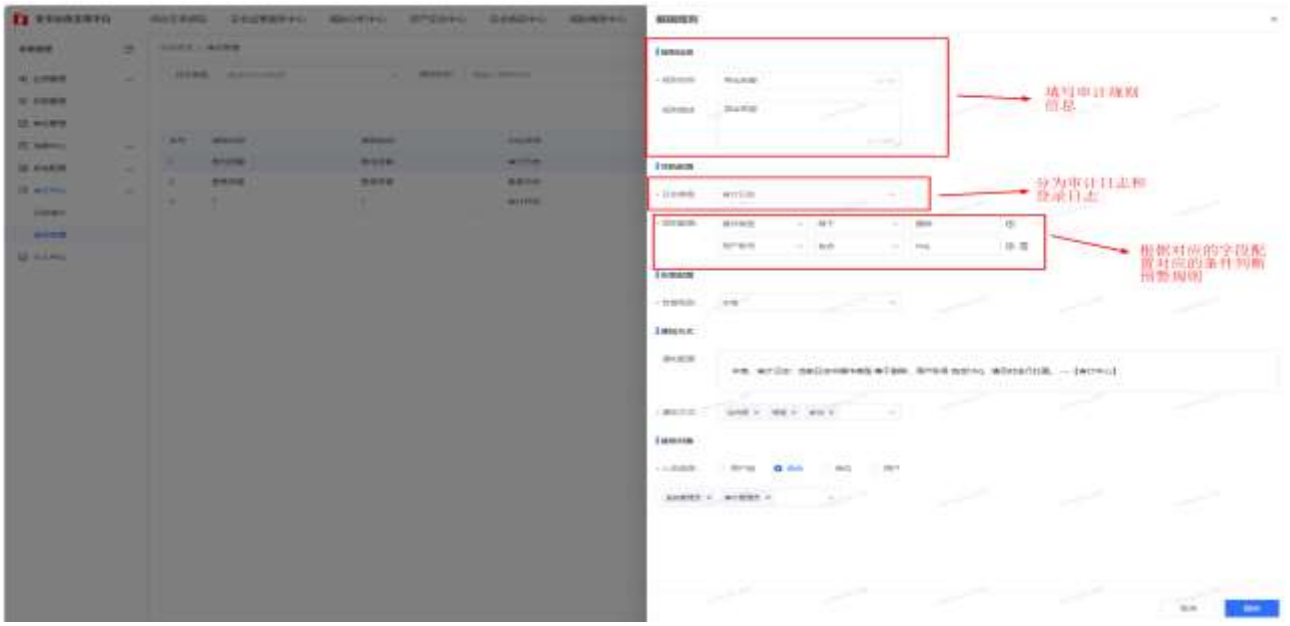
【功能说明】操作日志的日志查询与导出



3.1.6.2 审计告警

【功能说明】审计告警规则配置，用来限定系统中出现哪种操作时会出现日志审计告警，并发送对应级别的日志审计告警，包括对规则的新增、修改、删除操作；





3.1.7 运维监控

3.1.7.1 应用运维监控

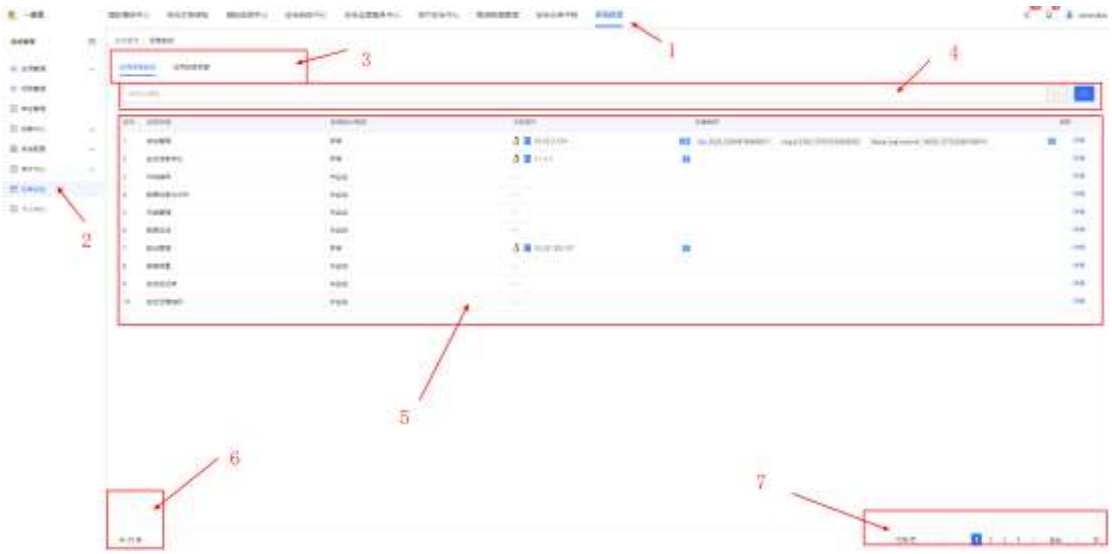
3.1.7.1.1 应用运维监控查询

【功能说明】查看各应用的运行情况，快速管理和查看应用涉及的主机与组件情况。

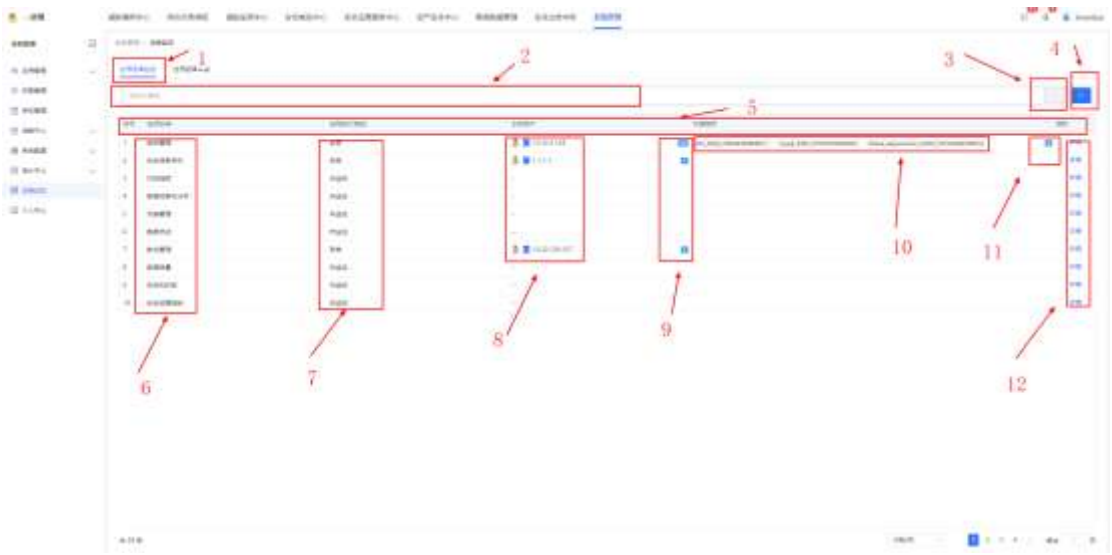
【操作步骤】

1、进入运维监控页面

系统管理 > 运维监控 > 应用运维监控，应用运维监控。

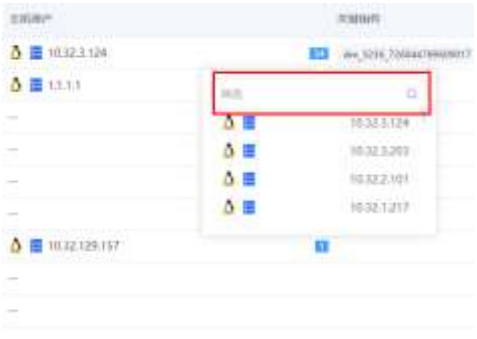


- 点击 1 系统管理，可以进入系统管理菜单，在左侧导航栏可以看到运维监控菜单；
- 点击 2 页面显示运维监控操作页面（如上图：图表 1）；
- 图标记 3 为主要功能分别为：应用运维监控，应用运维告警；
- 图标记 4 为页面自定义筛选框，可以对应用名称进行筛选；
- 图标记 5 为查询信息列表框，对主要信息进行展示；
- 图标记 6 为查询列表总条数；
- 图标记 7 为分页功能，可以选择页面展示 10，20，30，50 条数，可以跳转下一页，和直接输入跳转的页。

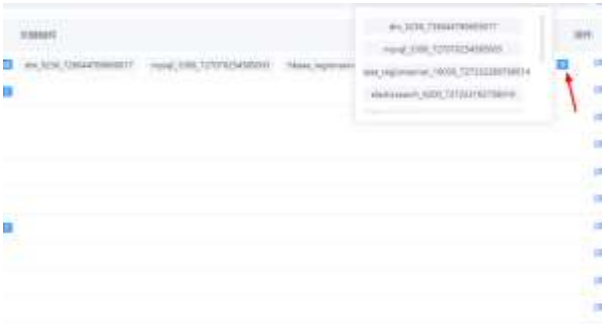


- 页面说明：
- 点击 1 可以进入应用运维监控操作页面；
- 图标记 2 为页面自定义筛选框，可以对应用名称进行筛选；
- 图标记 3 为筛选输入框重置按钮；
- 图标记 4 为搜索按钮对输入框信息进行搜索
- 图标记 5 为列表标头，对列表信息的说明‘
- 图标记 6 为应用名称；
- 图标记 7 为应用运行情况说明，
- 正常：为所有主机资产和关键组件全部正常；
- 异常：为只有其中有主机资产和关键组件中只要有异常就为异常；
- 未监控：为对此应用主机和关键组件没有监控；
- 图标记 8 为主机资产，信息为主机 IP；
- 图标记 9 为主机资产数量，点击数字可以弹出主机资产 IP 列表（如下图）

输入框可以对 IP 进行搜索；



- 图标记 10 为关键组件信息；
- 图标记 11 为关键组件数量，点击数字可以弹出主关键组件列表（如下



图）；

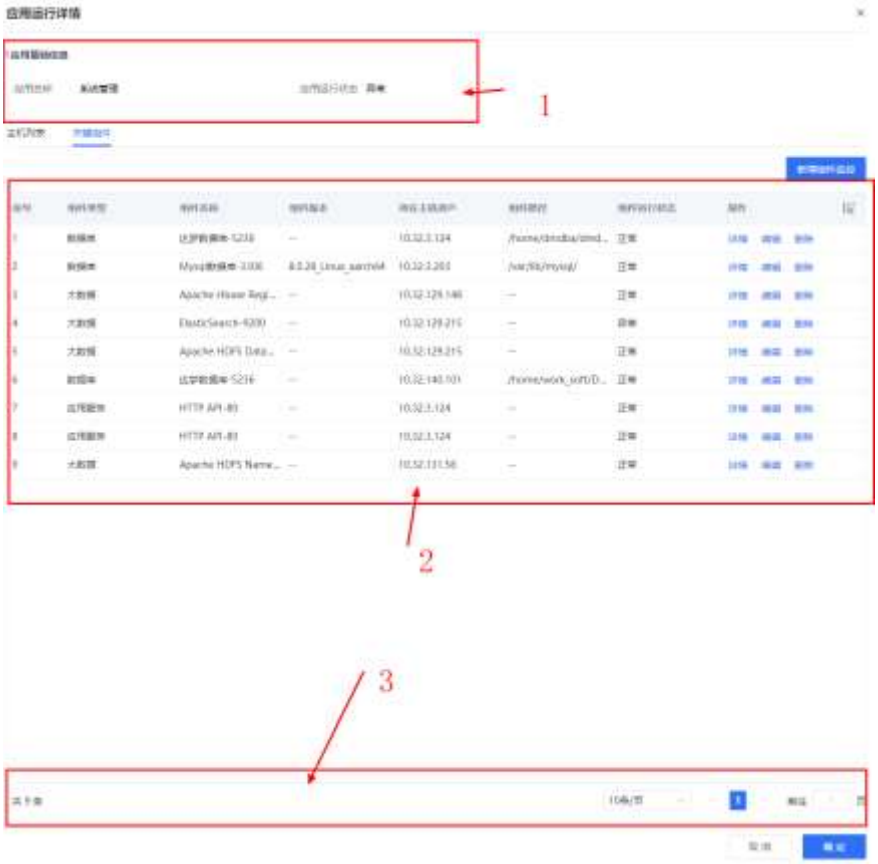
3.1.7.1.2 应用运维监控详情

【功能说明】查看应用的主机运行详情情况，快速管理和查看应用涉及的主机与组件情况。

【操作步骤】

1、进入运维监控页面

- 系统管理 > 运维监控 > 应用运维监控>详情，应用运维监控详情。
- 图标记 1 为应用基础信息；
- 图标记 2 为主机列表和关键组件功能按键；
- 图标记 3 为信息列表，主机状态为：正常，异常和暂停监控；
- 图标记 4 为分页操作；



- 图标记 1 为应用基础信息；
- 图标记 2 为信息列表，组件状态为：正常，异常和暂停监控；
- 图标记 3 为分页操作；

3.1.7.1.2.1 新增主机监控

【功能说明】用户对需要监控的主机进行添加。

【操作步骤】

1、 进入运维监控页面

- 系统管理 > 运维监控 > 应用运维监控 > 详情 > 新增主机监控，新增主机监控。
- 进行表单的填写,有必填项校验
- 填写完成后可进行链接测试
- 点击确定成功添加主机

3.1.7.1.2.2 删除主机监控

【功能说明】前期确定的主机监控，由于业务变化，不再需要主机监控，需删除主机监控。

【操作步骤】

1、 进入运维监控页面

- 系统管理 > 运维监控 > 应用运维监控，进入应用运行详情。
- 点击删除,可进行主机的删除,需要进行管理员密码校验

3.1.7.1.2.3 编辑主机监控

【功能说明】前期确定的主机监控，由于业务变化，需要主机监控。

【操作步骤】

1、 进入运维监控页面

- 系统管理 > 运维监控 > 应用运维监控，进入应用运行详情。
- 进行表单的填写，填写完成后可进行链接测试。

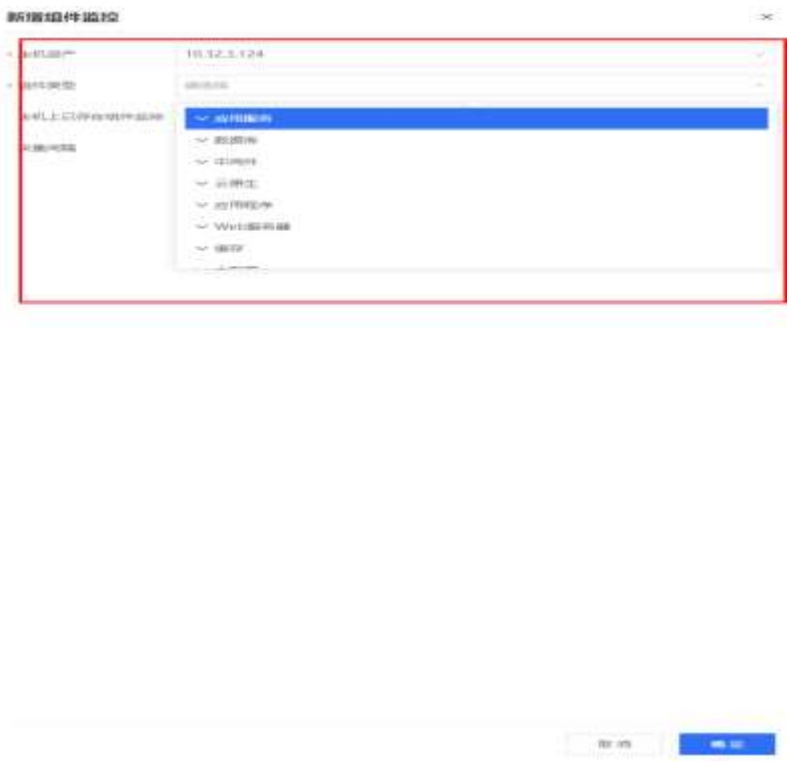
3.1.7.1.2.4 新增组件监控

【功能说明】用户对需要监控主机的组件进行添加

【操作步骤】

1、 进入运维监控页面

- 系统管理 > 运维监控 > 应用运维监控 > 详情 >关键组件详情 > 新增组件监控，新增组件监控。
- 新增组件需要选择主机资产,组件类型,主机上已存在组件监控,采集间隔等信息的填写
- 信息填写完毕点击确定



3.1.7.1.2.5 删除组件监控

【功能说明】前期确定的组件监控，由于业务变化，不再需要主机监控，需删除组件监控。

【操作步骤】

1、 进入运维监控页面

- 系统管理 > 运维监控 > 应用运维监控 > 详情>关键组件，进入关键组件。
- 点击删除,可进行组件的删除,需要进行管理员密码校验

3.1.7.1.2.6 编辑组件监控

【功能说明】前期确定的主机监控，由于业务变化，需要组件监控进行修改。

【操作步骤】

1、 进入运维监控页面

- 系统管理 > 运维监控 > 应用运维监控 > 详情>关键组件，进入关键组件。

3.1.7.2 应用运维告警

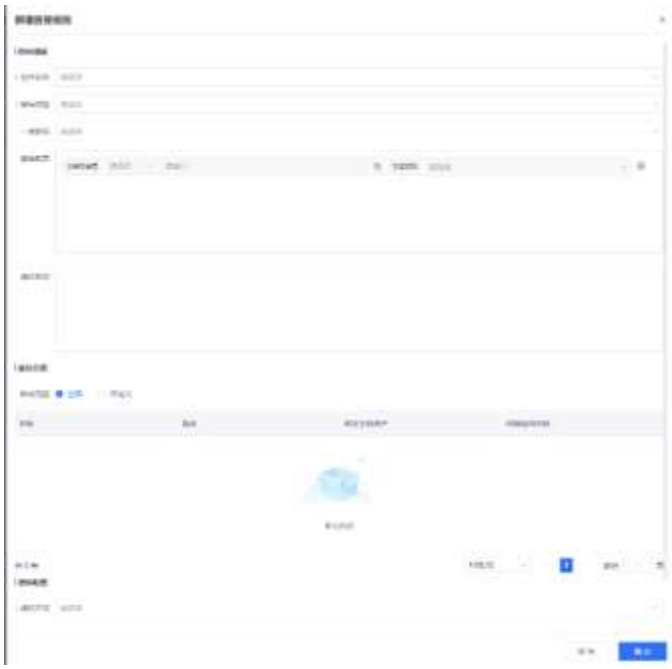
3.1.7.2.1 新增告警规则

【功能说明】用户对需要告警规则进行新增

【操作步骤】

1、 进入运维监控页面

- 系统管理 > 运维监控 > 应用运维告警 > 新增告警规则，进入新增告警规则。
- 新增告警规则需要选择组件名称，指标类型，指标项，阀值配置，通知预览，监控范围等信息的填写
- 信息填写完毕点击确定



3.1.7.2.2 删除告警规则

【功能说明】前期确定的告警规则，由于业务变化，不再需要告警规则，需删除告警规则。

【操作步骤】

1、 进入运维监控页面

- 系统管理 > 运维监控 > 应用运维告警，进入应用运维告警。
- 点击删除,可进行应用运维告警的删除

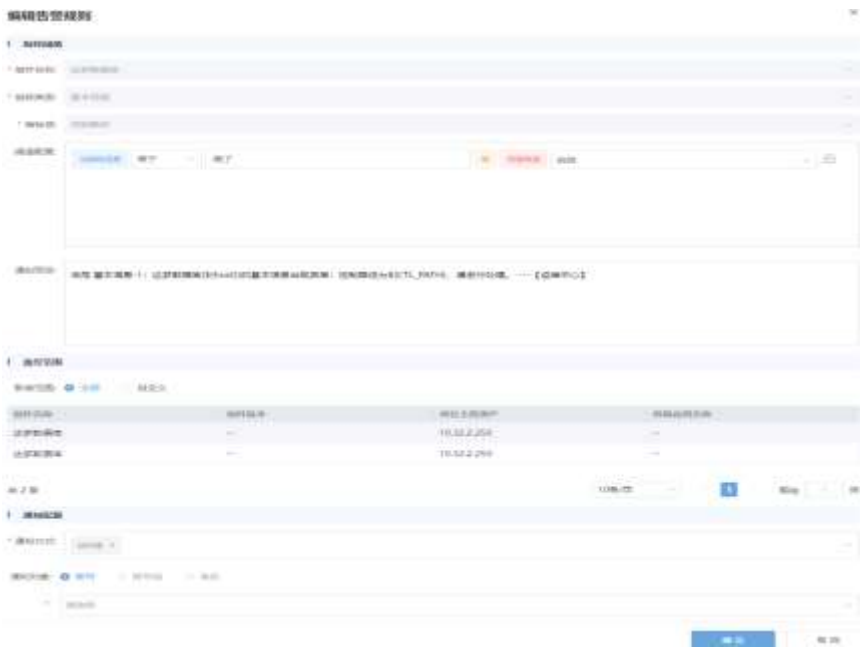
3.1.7.2.2 编辑告警规则

【功能说明】前期确定的主机监控，由于业务变化，需要组件监控进行修改。

【操作步骤】

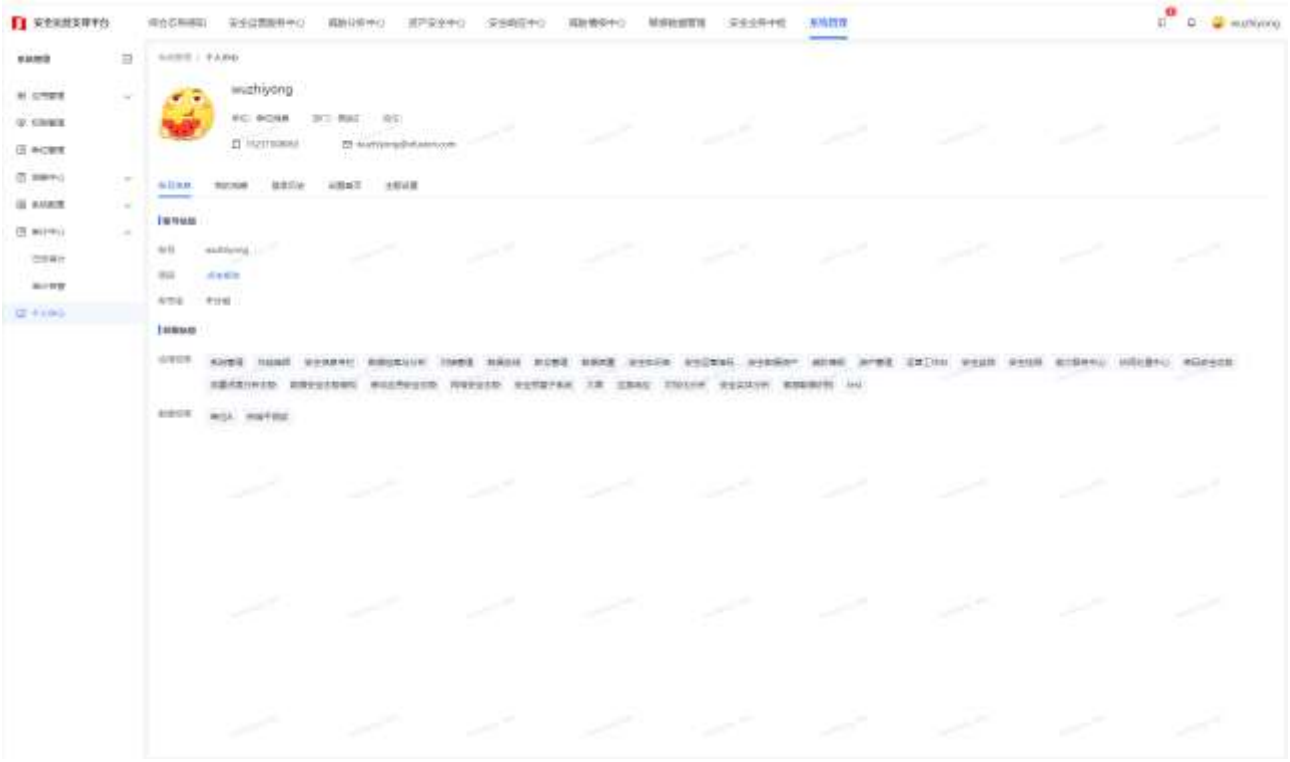
1、 进入运维监控页面

- 系统管理 > 运维监控 > 应用运维告警，进入应用运维告警。
- 只能编辑组件配置信息和采集间隔信息指标阀值：组件名称，指标类型，指标项，阀值配置，通知预览;
- 信息修改完毕点击确定



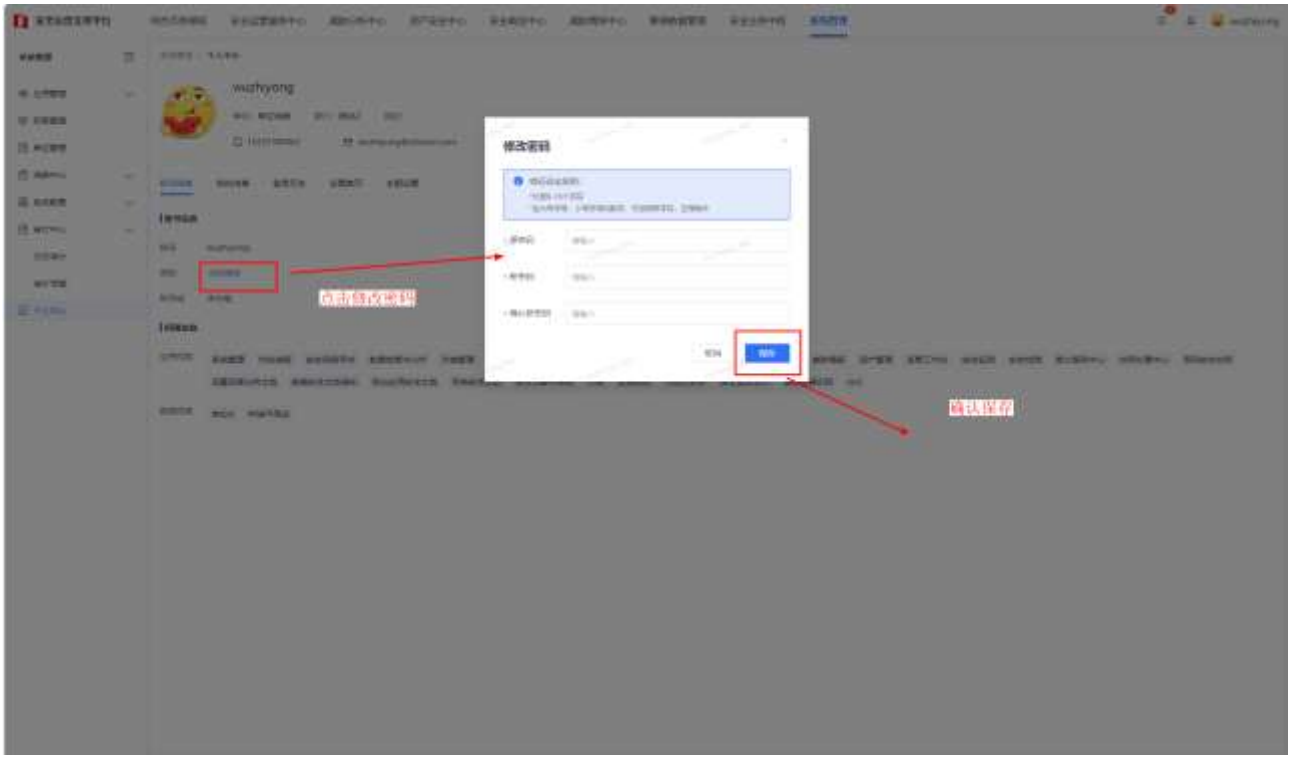
3.1.8 个人中心

【功能说明】关于个人的基本信息，账号信息，我的消息，登录历史，设置首页，以及个性化主题的展示与个人设置;



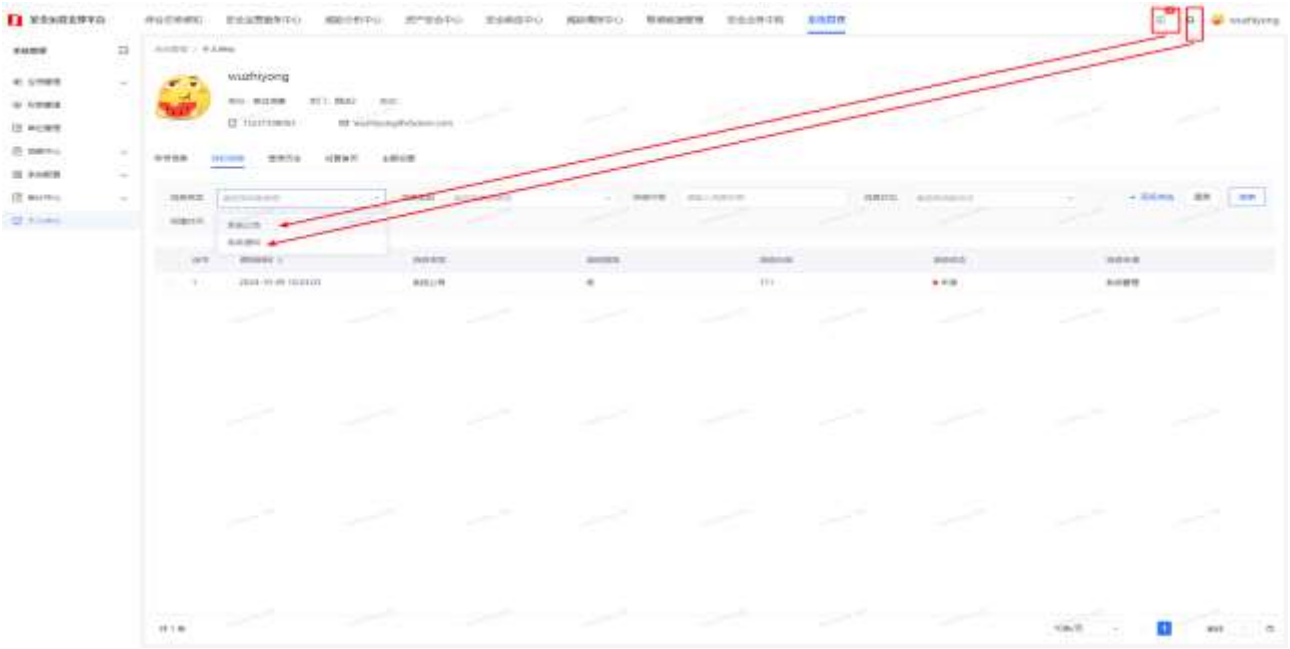
3.1.8.1 账号信息

【功能说明】当前登录人的个人账号的基本信息以及应用权限、数据权限的信息展示，同时可以修改自己的密码；



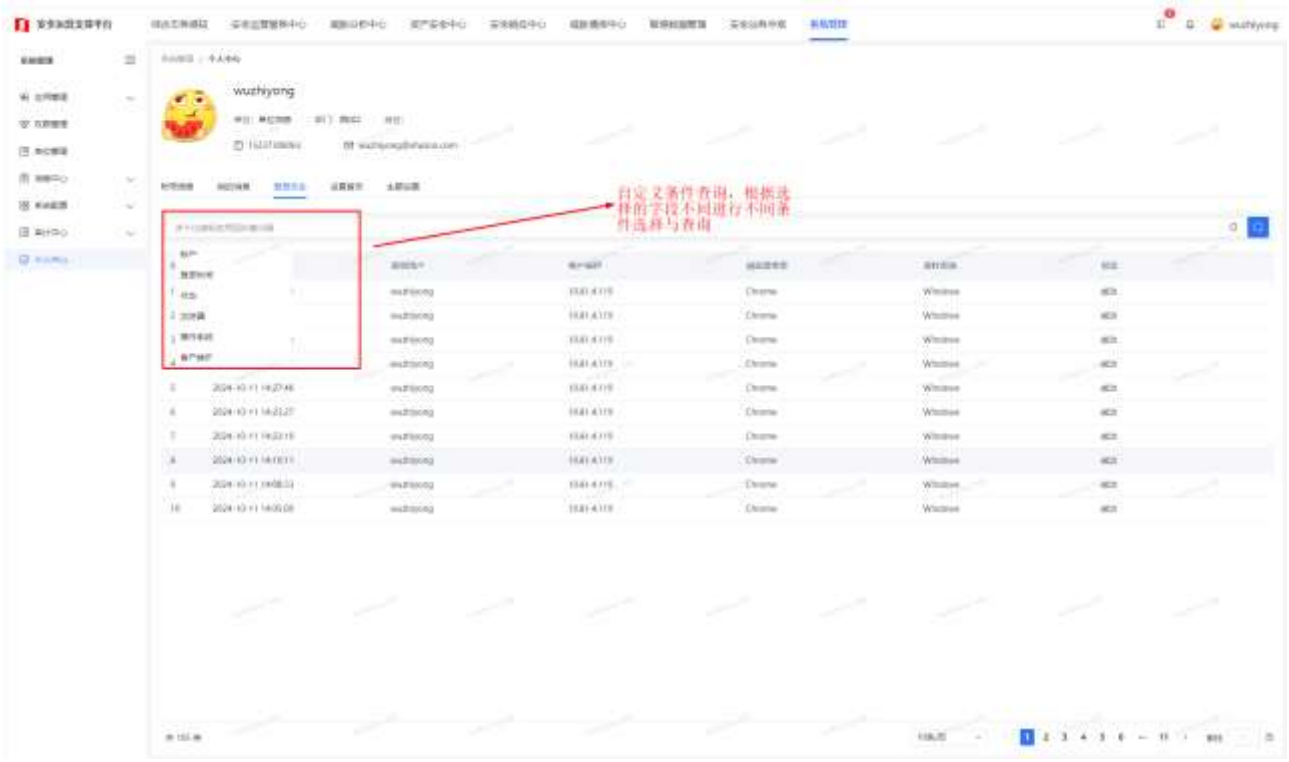
3.1.8.2 我的消息

【功能说明】当前登录人收到的系统公告和系统通知消息的列表展示和查询；



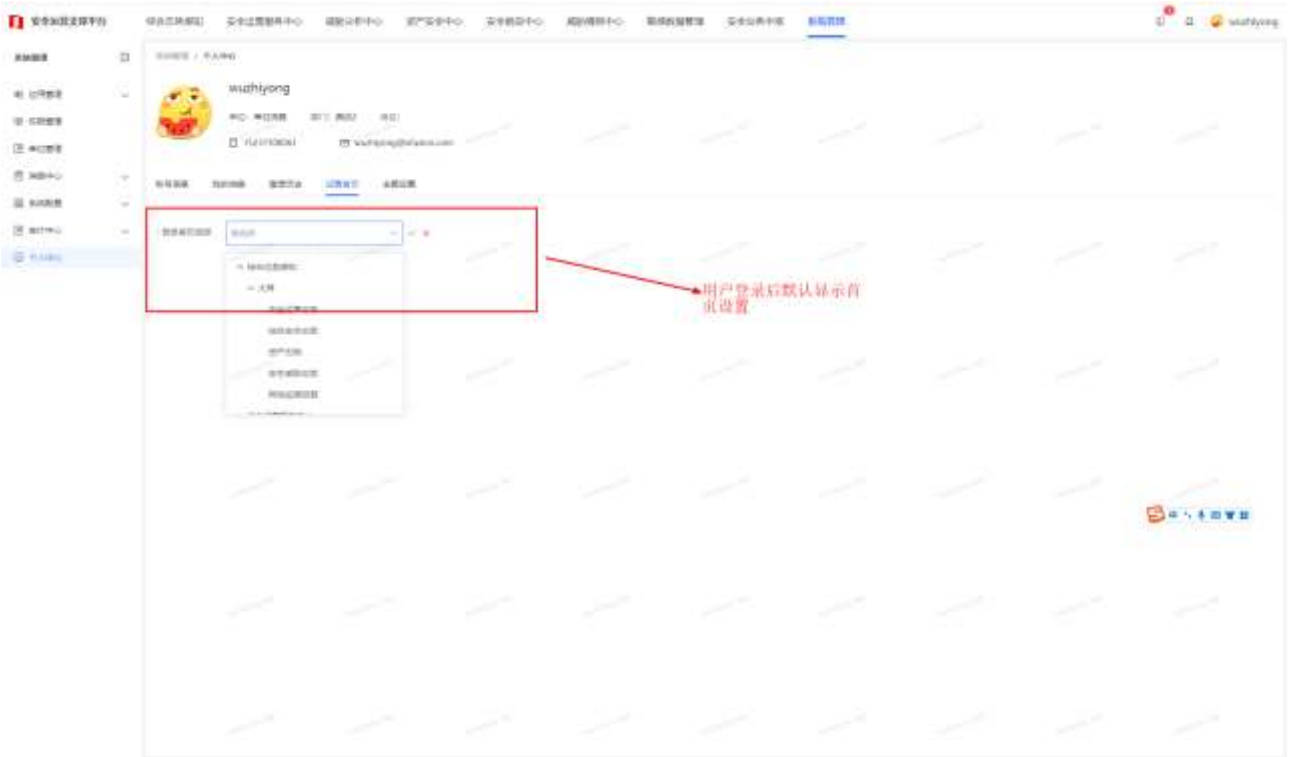
3.1.8.3 登录历史

【功能说明】当前登录人的登录历史记录的列表展示，以及属性字段的自定义查询；



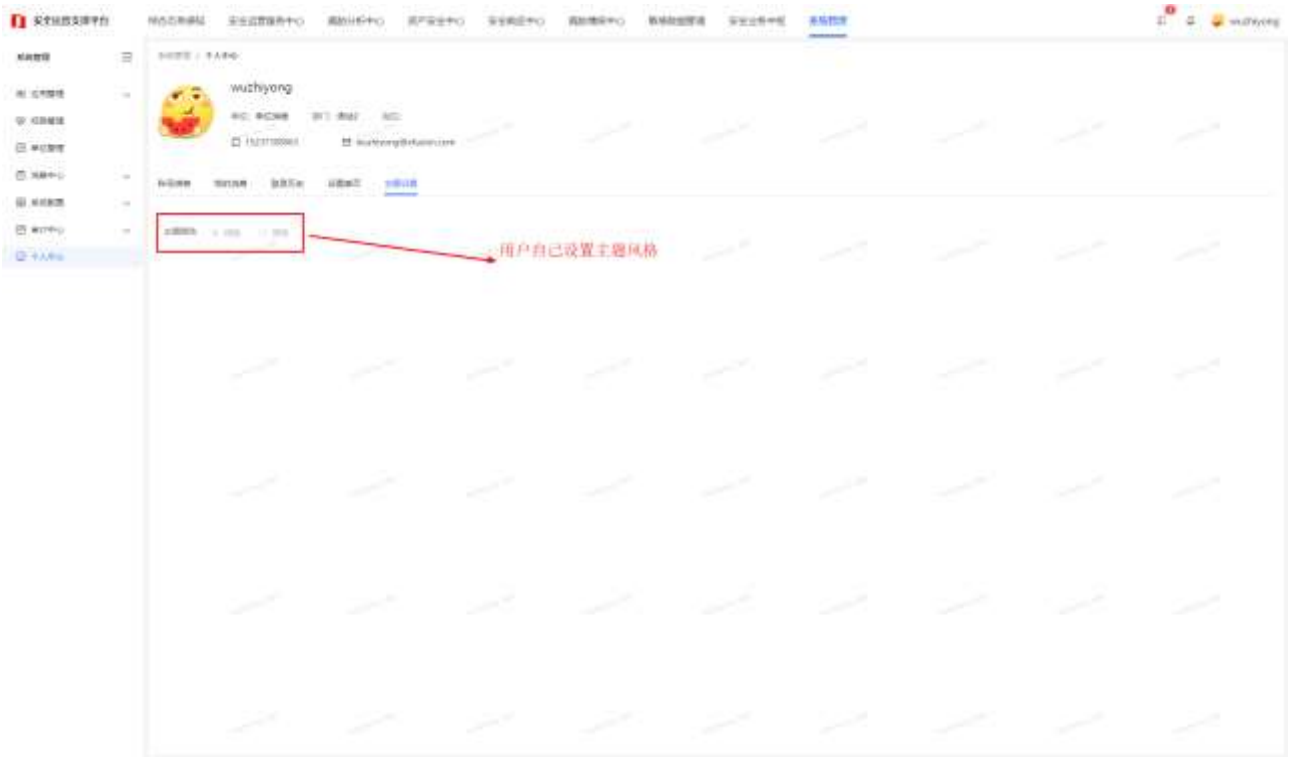
3.1.8.4 设置首页

【功能说明】用于用户登录后显示的默认页面的设置；



3.1.8.5 主题设置

【功能说明】用于用户自己设置自己的页面主题风格，目前只支持浅色和深色；

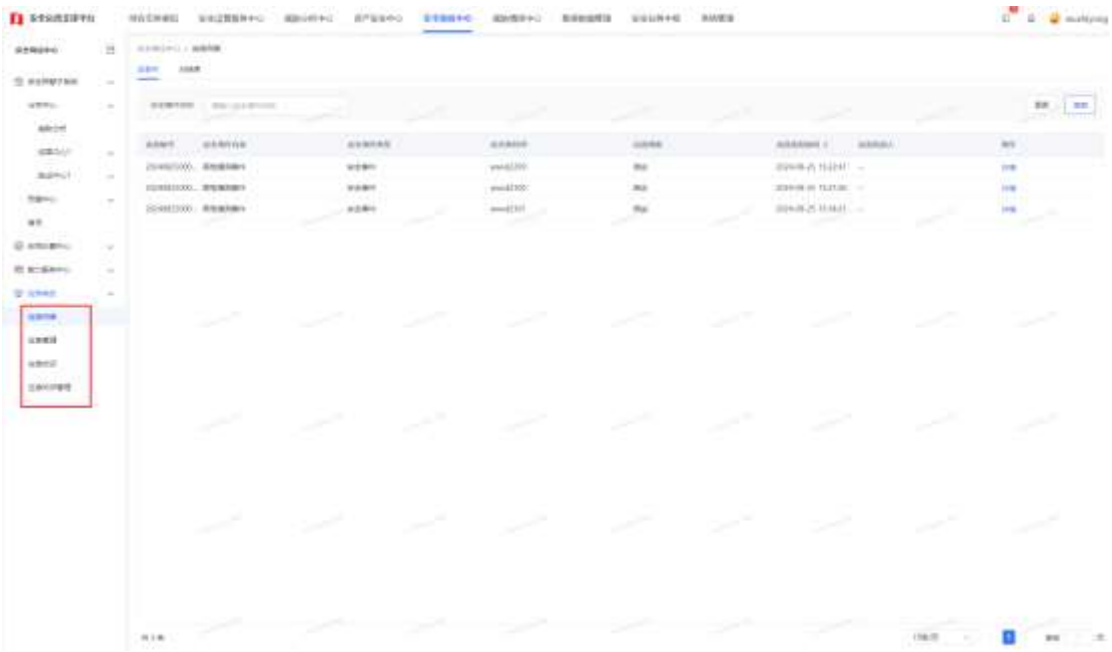


3.2 安全响应中心

【功能说明】主要功能为安全预警、协同处置中心、能力服务中心、以及应急响应，提升应急事件快速响应与处置能力

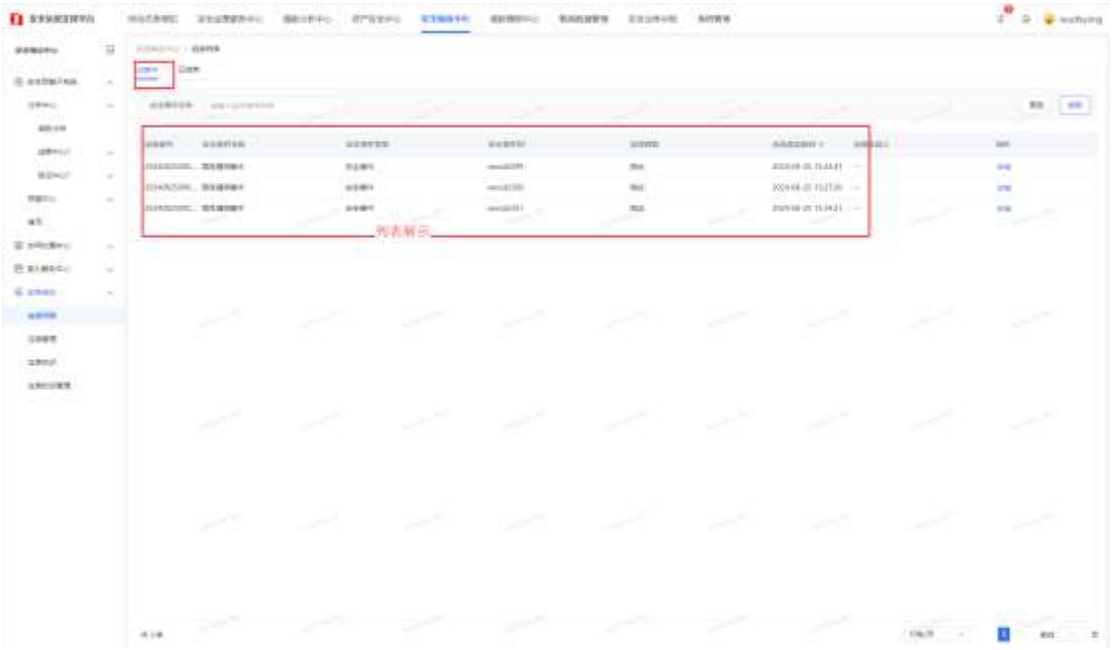
3.2.1 应急响应

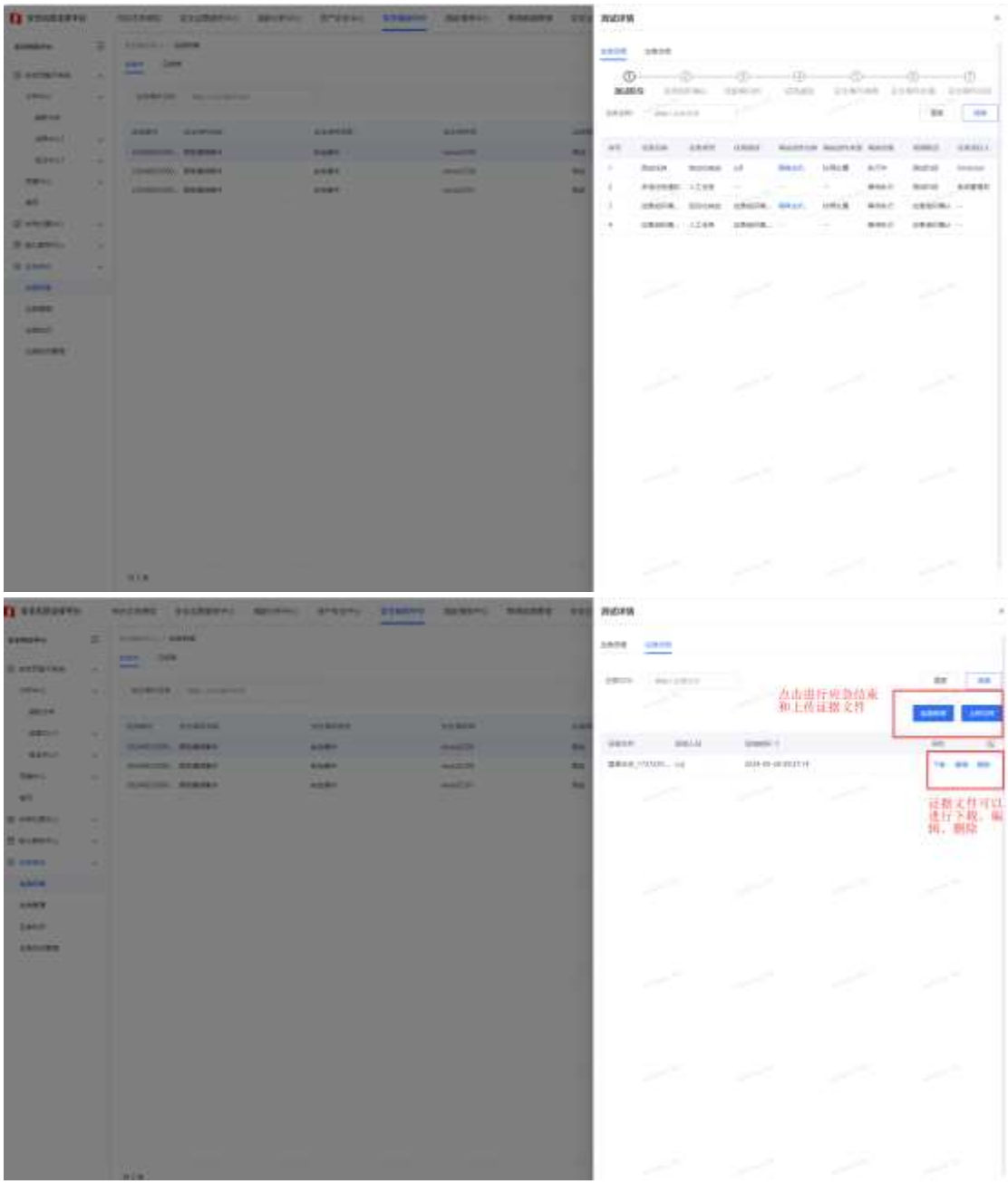
【功能说明】针对应急响应事件的管理与应急响应知识的管理；



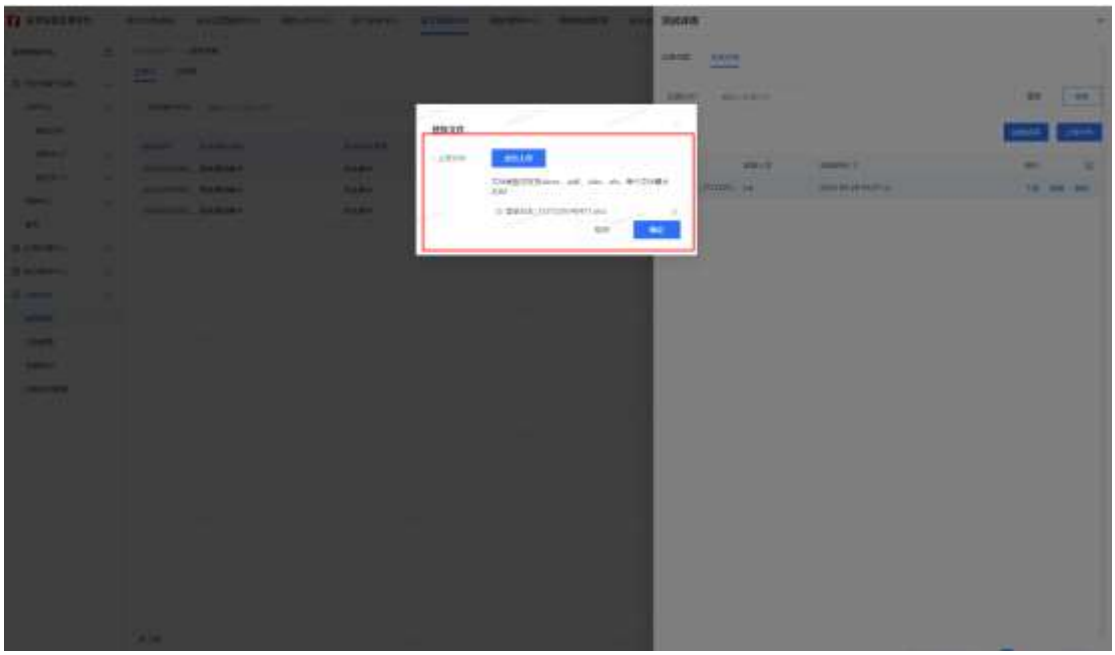
3.2.1.1 应急列表

【功能说明】应急中与已结束的应急管理信息的列表展示



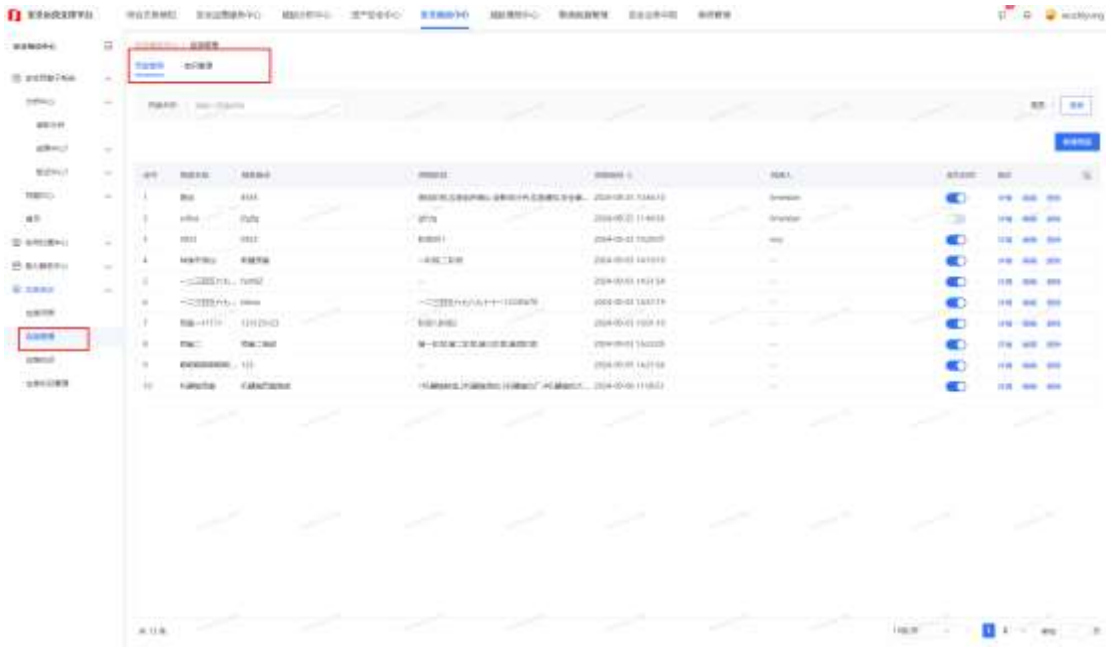


替换文件



3.2.1.2 应急管理

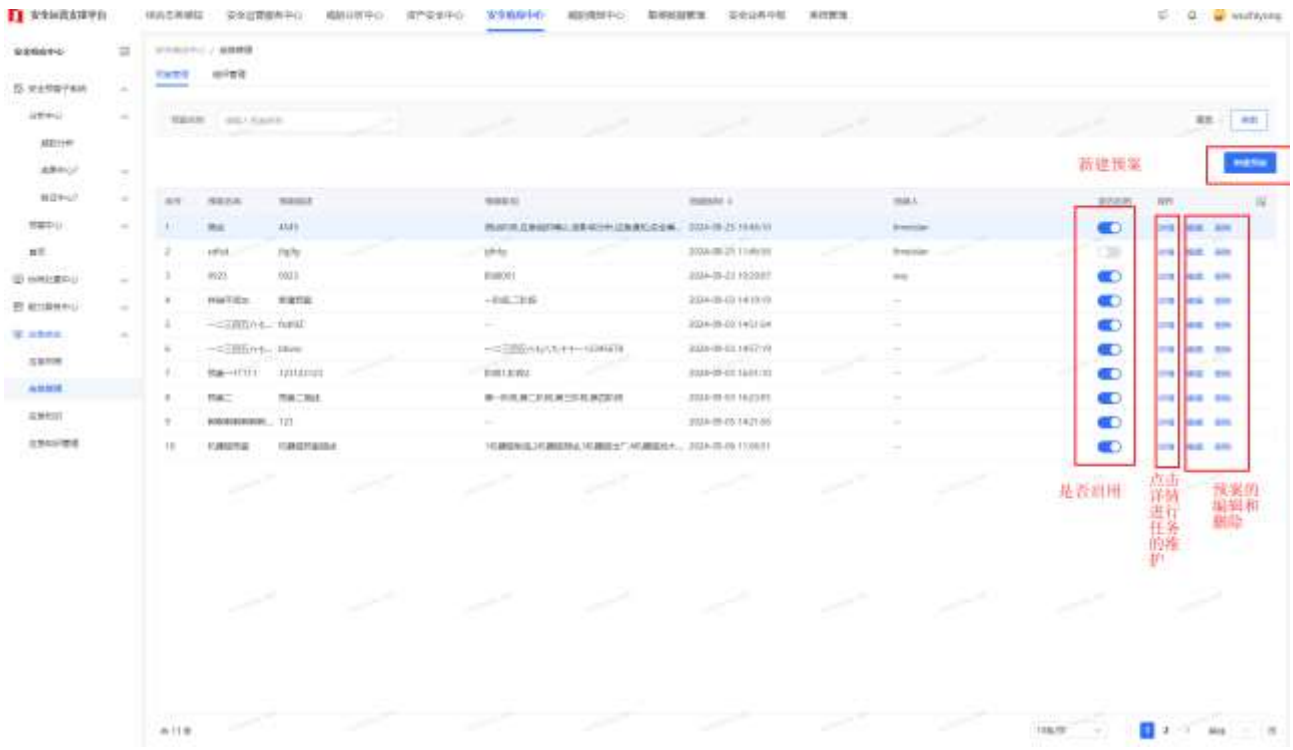
【功能说明】应急响应 -> 应急管理：该功能是针对于应急事件进行应急预案制定，组织管理配置；

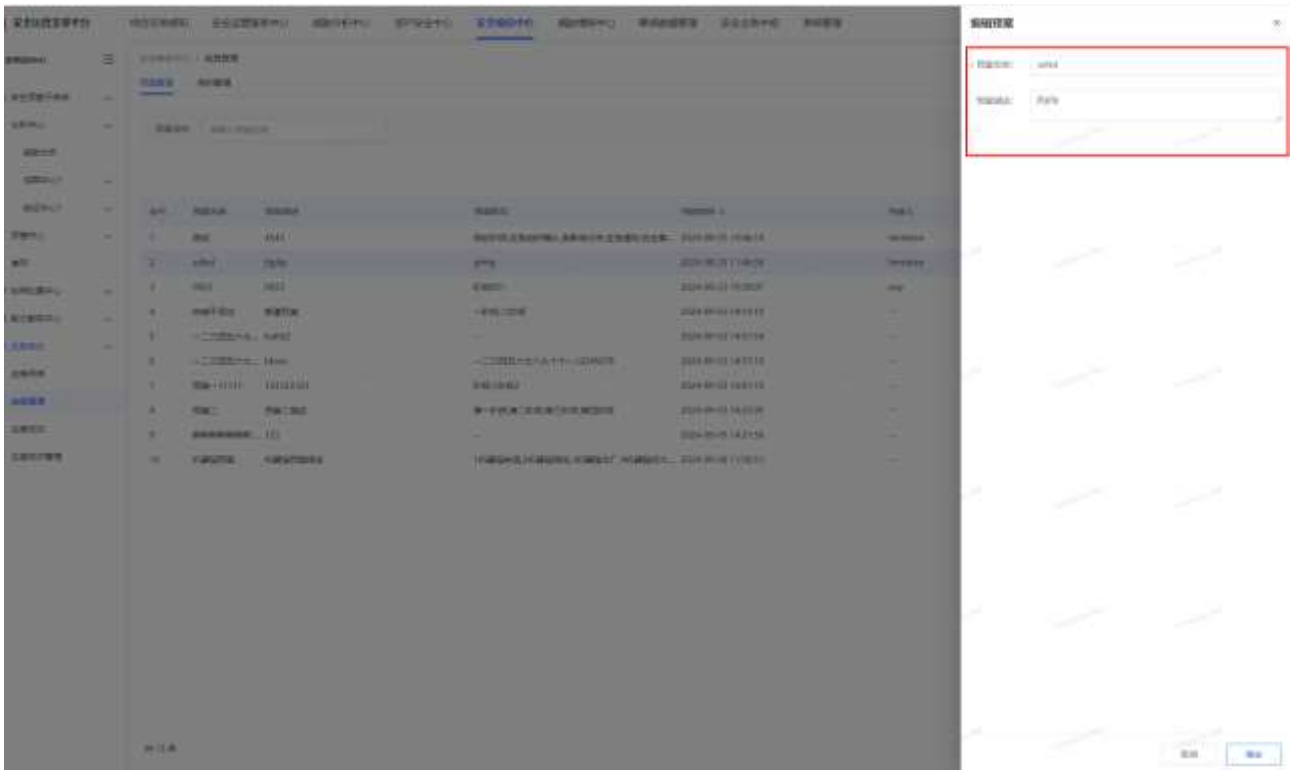


3.2.1.2.1 预案管理

【功能说明】应急管理 -> 预案管理（tab 页）：该功能用户预案的制定，编

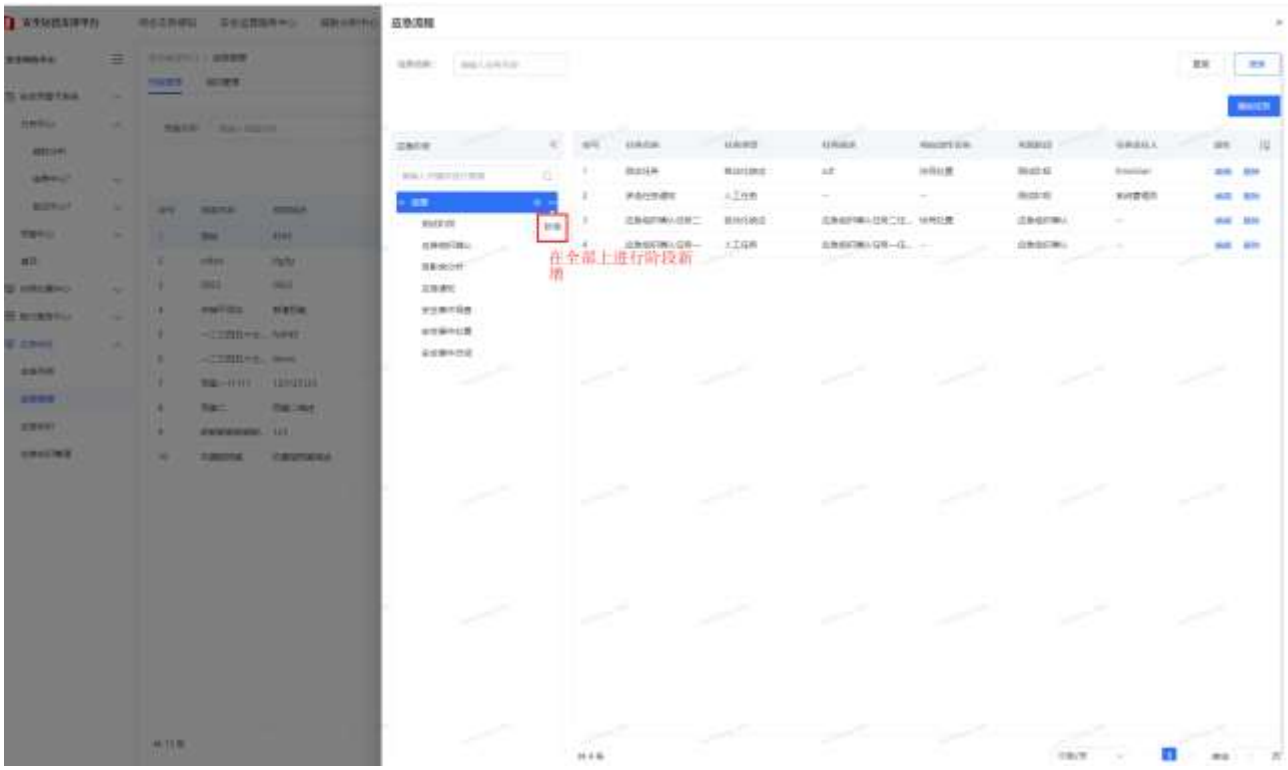
辑、删除以及任务的新增、修改、删除；

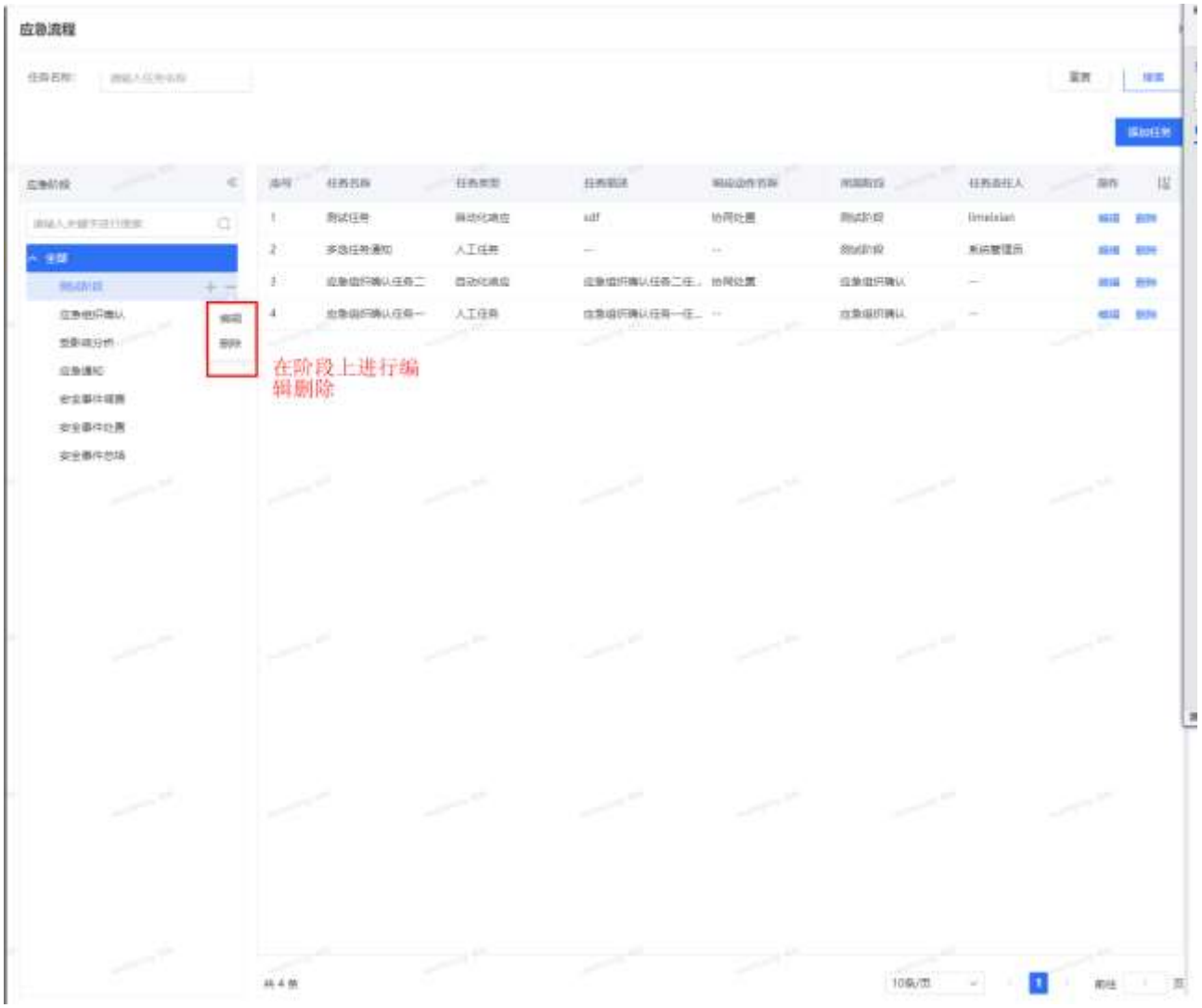


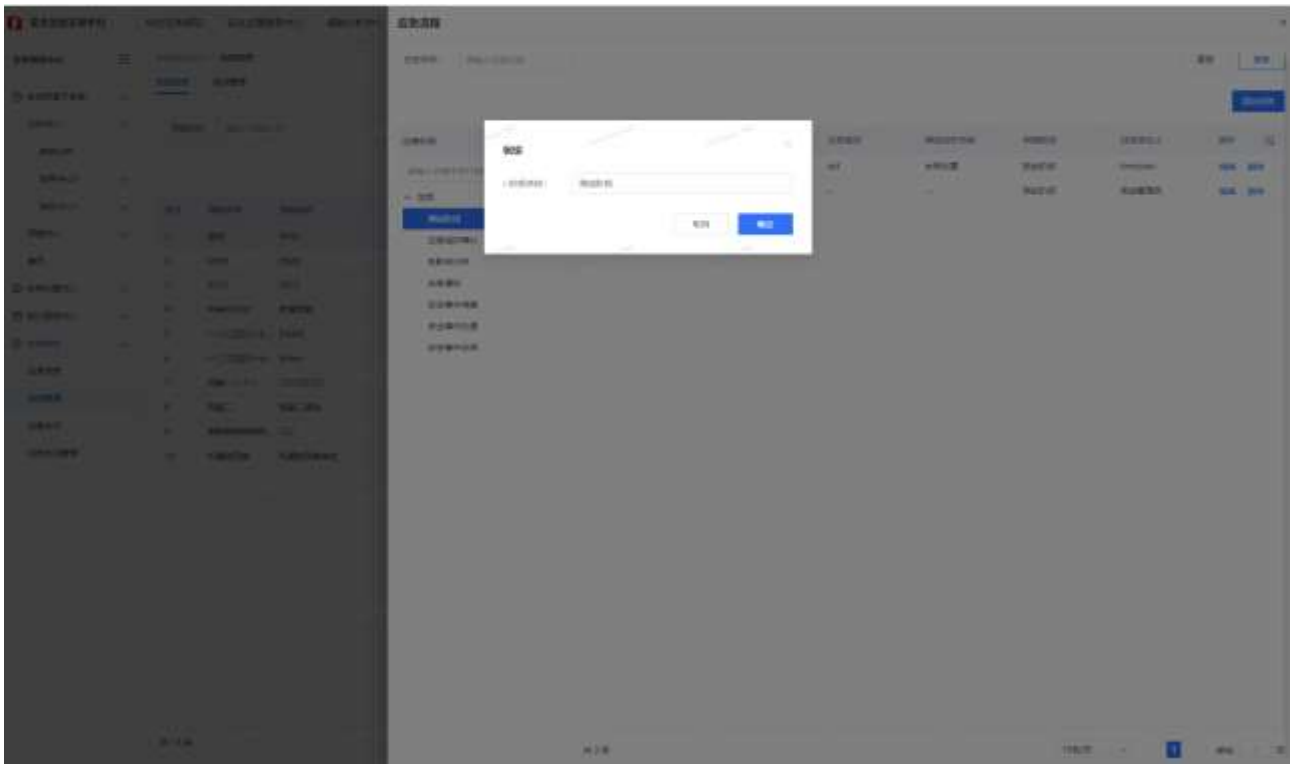


详情-> 应急阶段管理和任务管理

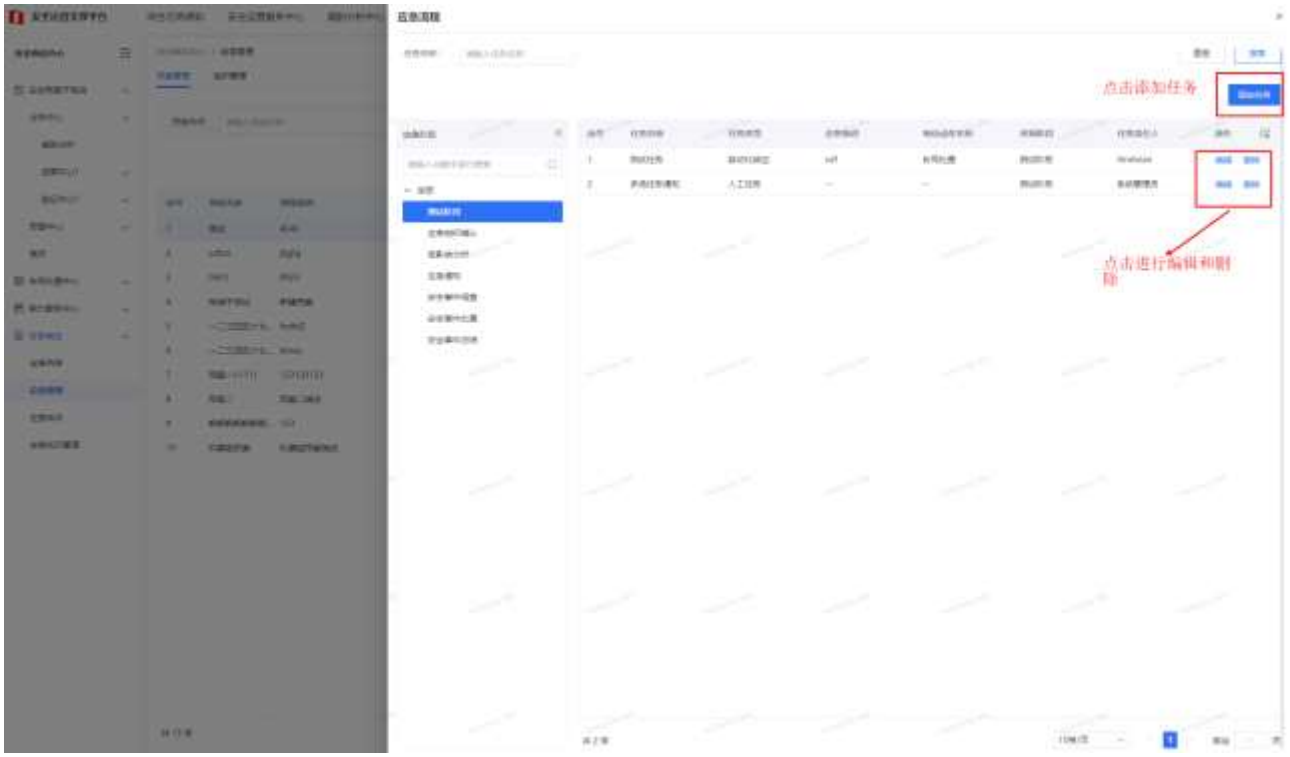
应急阶段管理


在全部上进行阶段新增

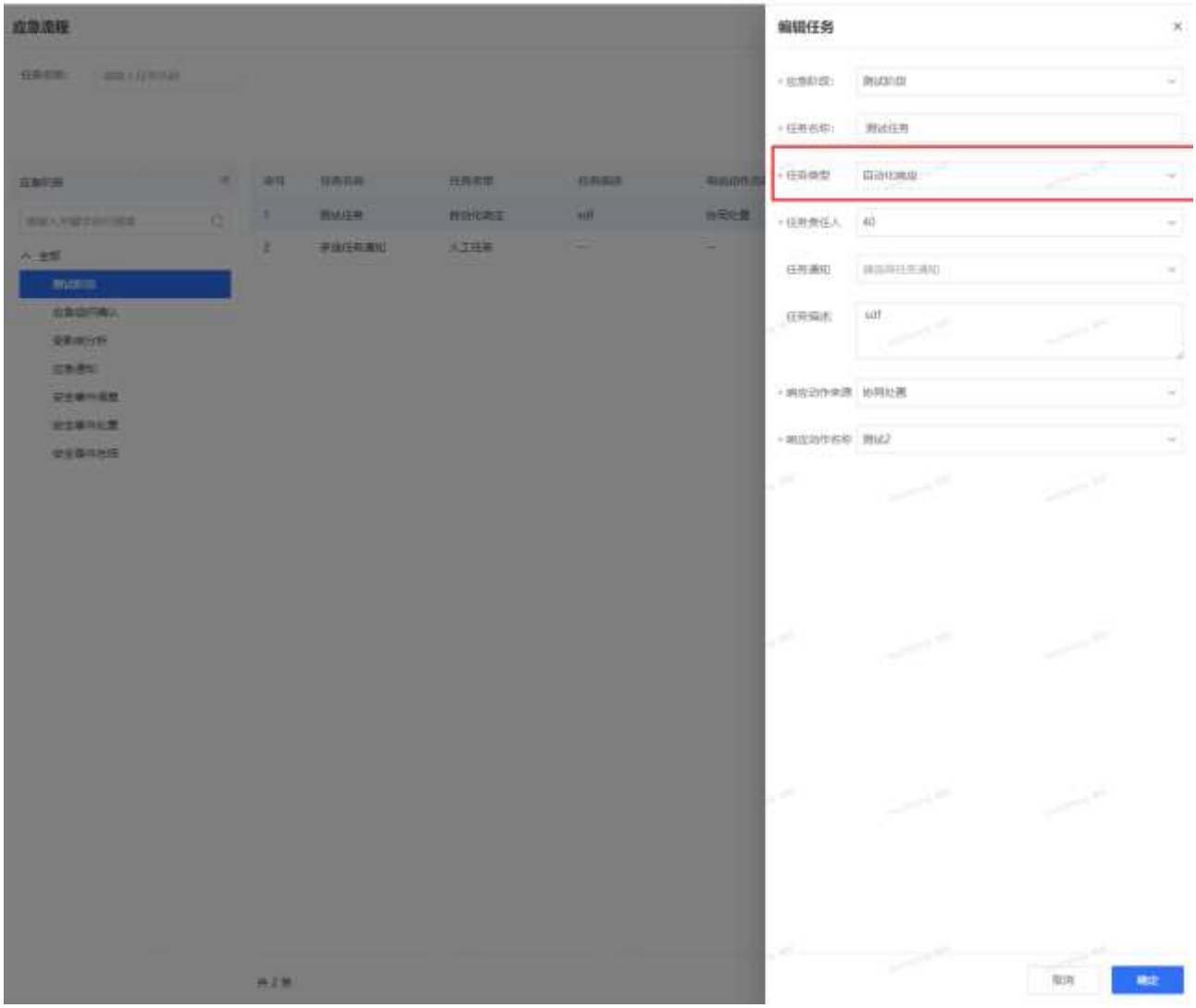

应急流程
在阶段上进行编辑删除



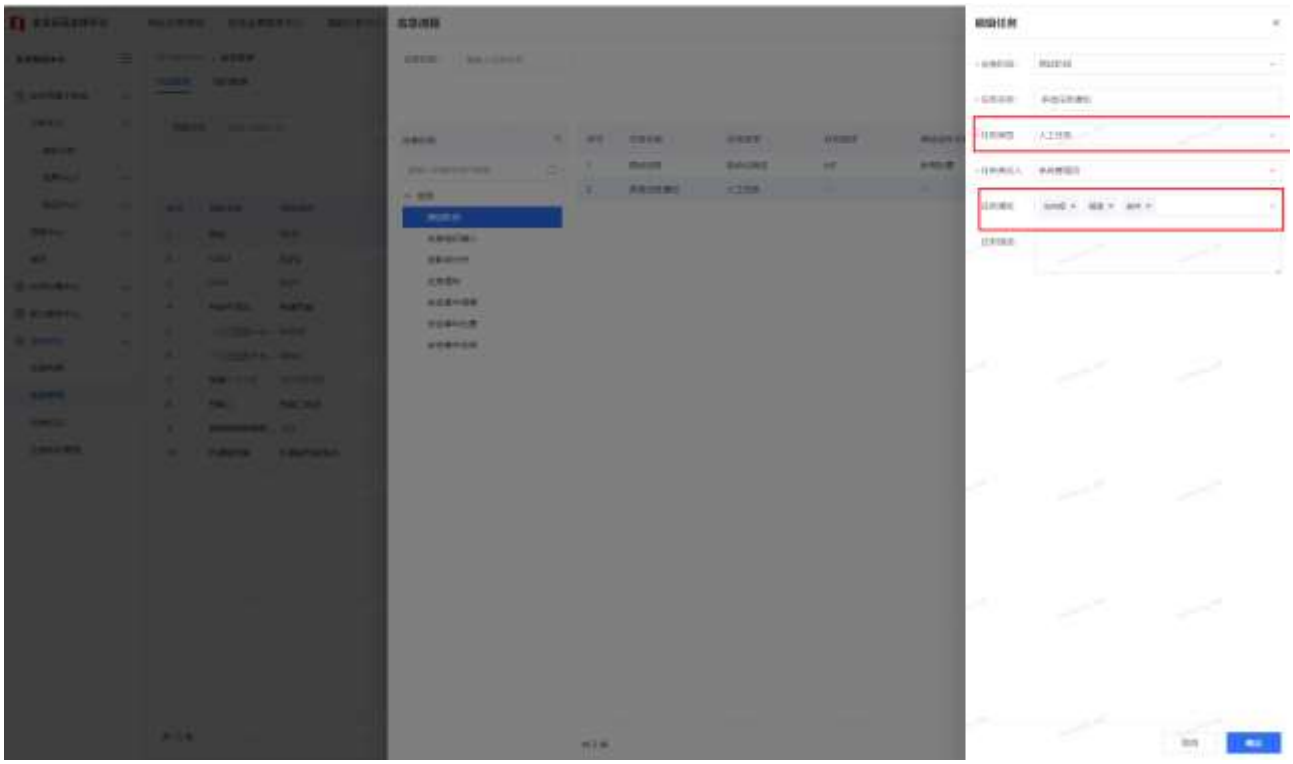
应急任务管理



任务类型为自动化响应


应急流程
编辑任务
任务类型
自动化响应
任务责任人
admin
任务描述
sdf
响应动作来源
协同处置
响应动作名称
测试2
取消
确定

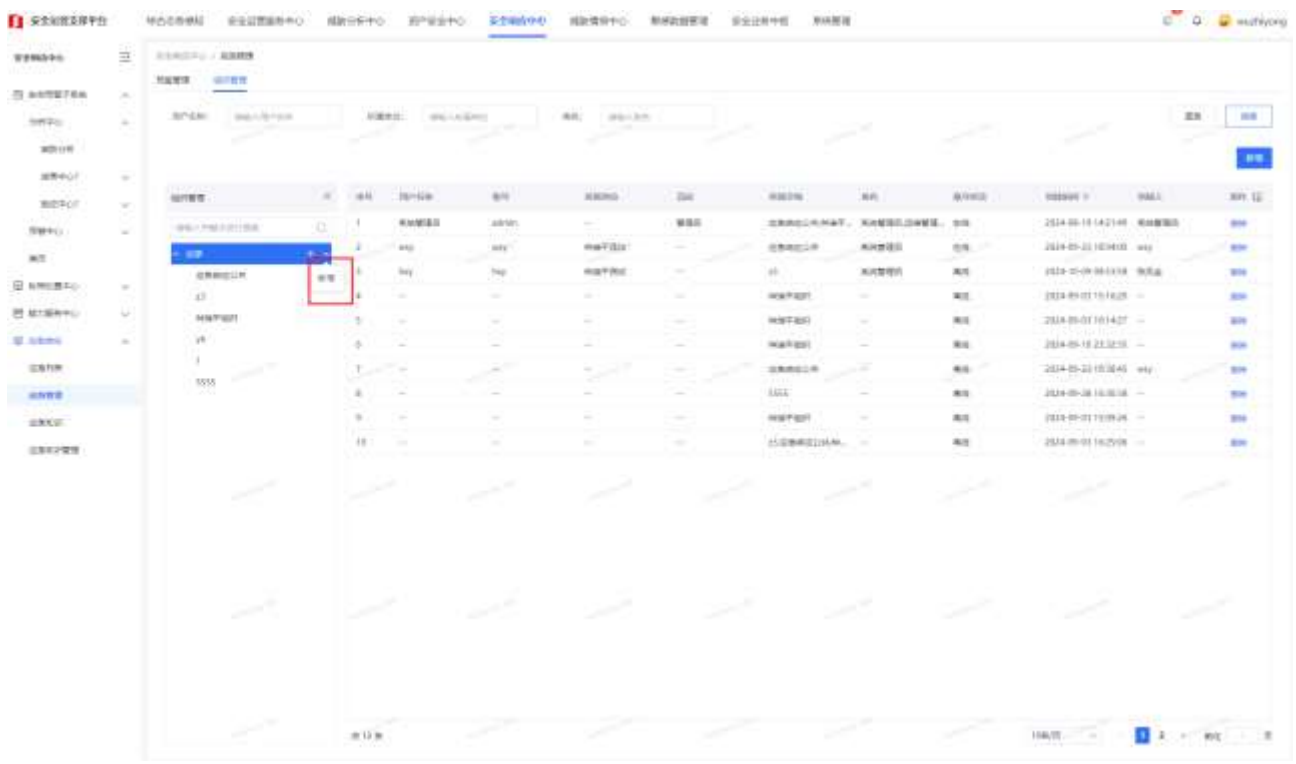
任务类型为人工任务

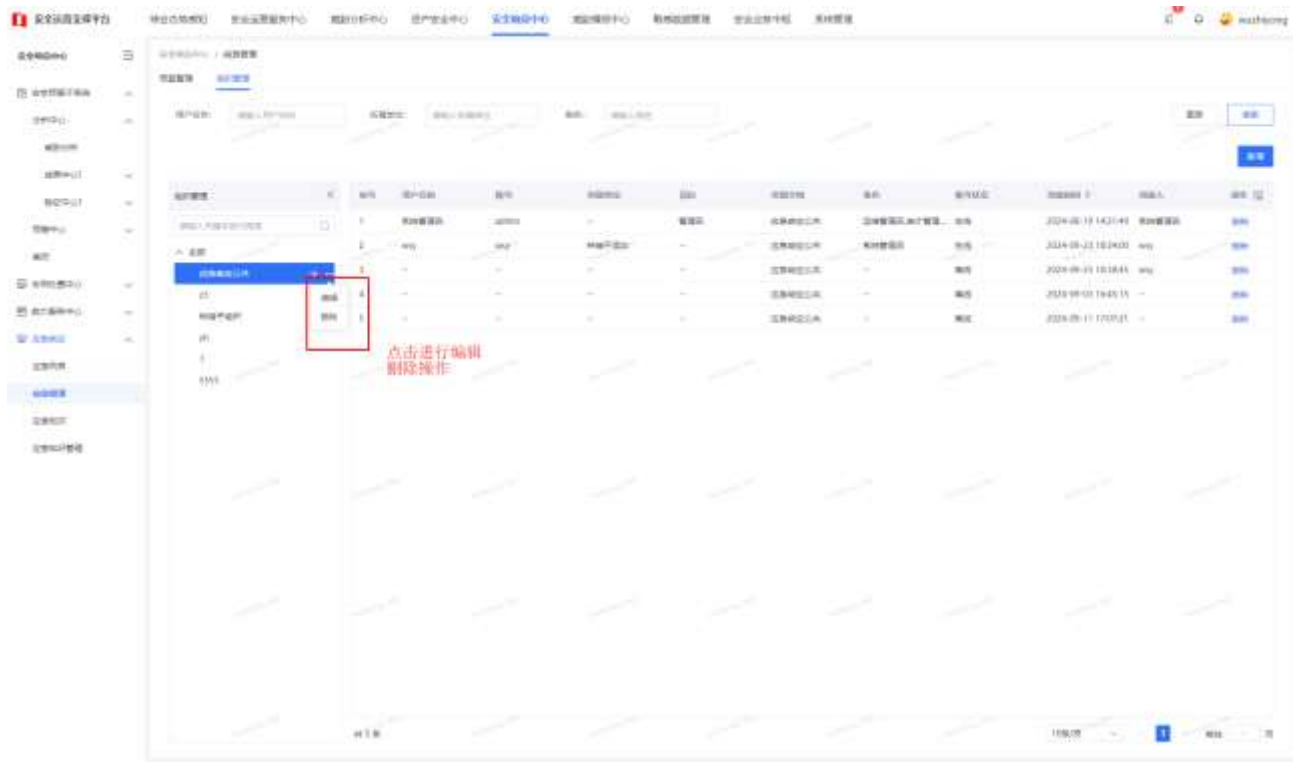


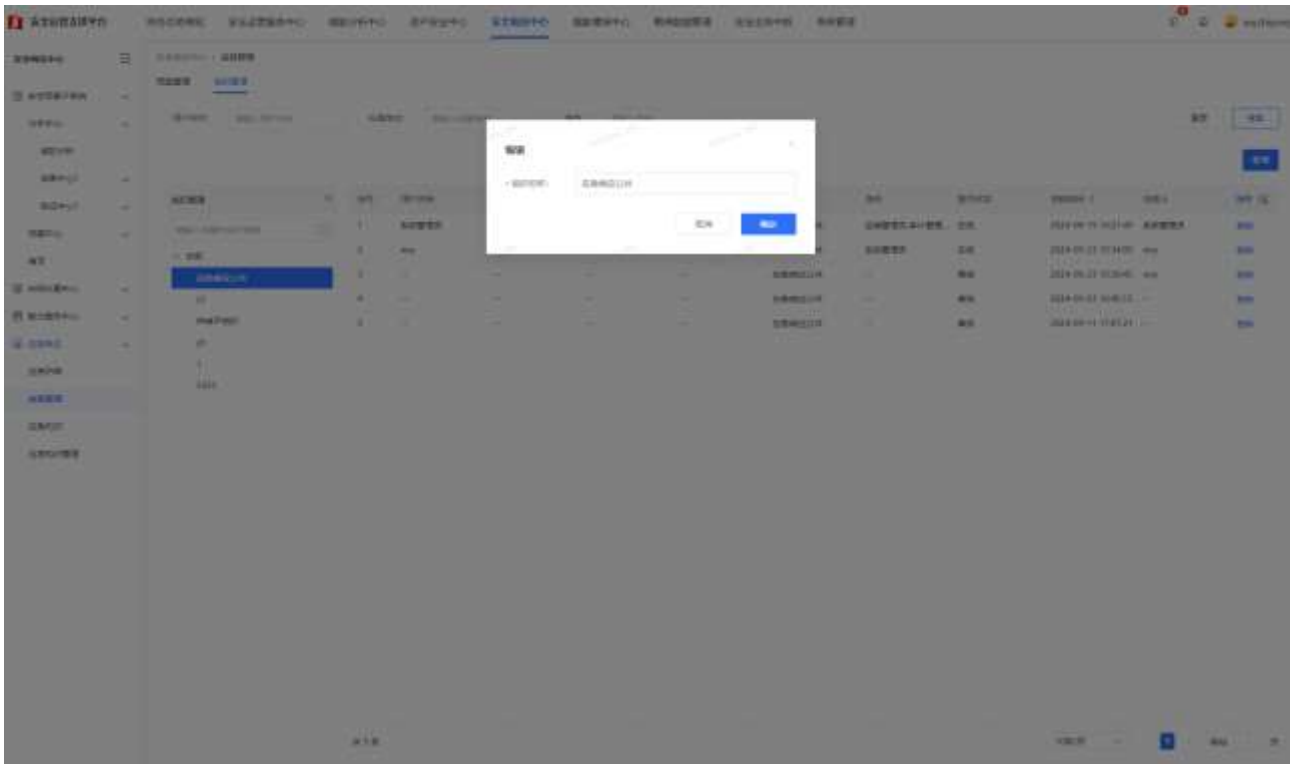
3.2.1.2.2 组织管理

【功能说明】【功能说明】应急管理 -> 组织管理（tab 页）：该功能用于应急响应小组管理以及小组成员的管理

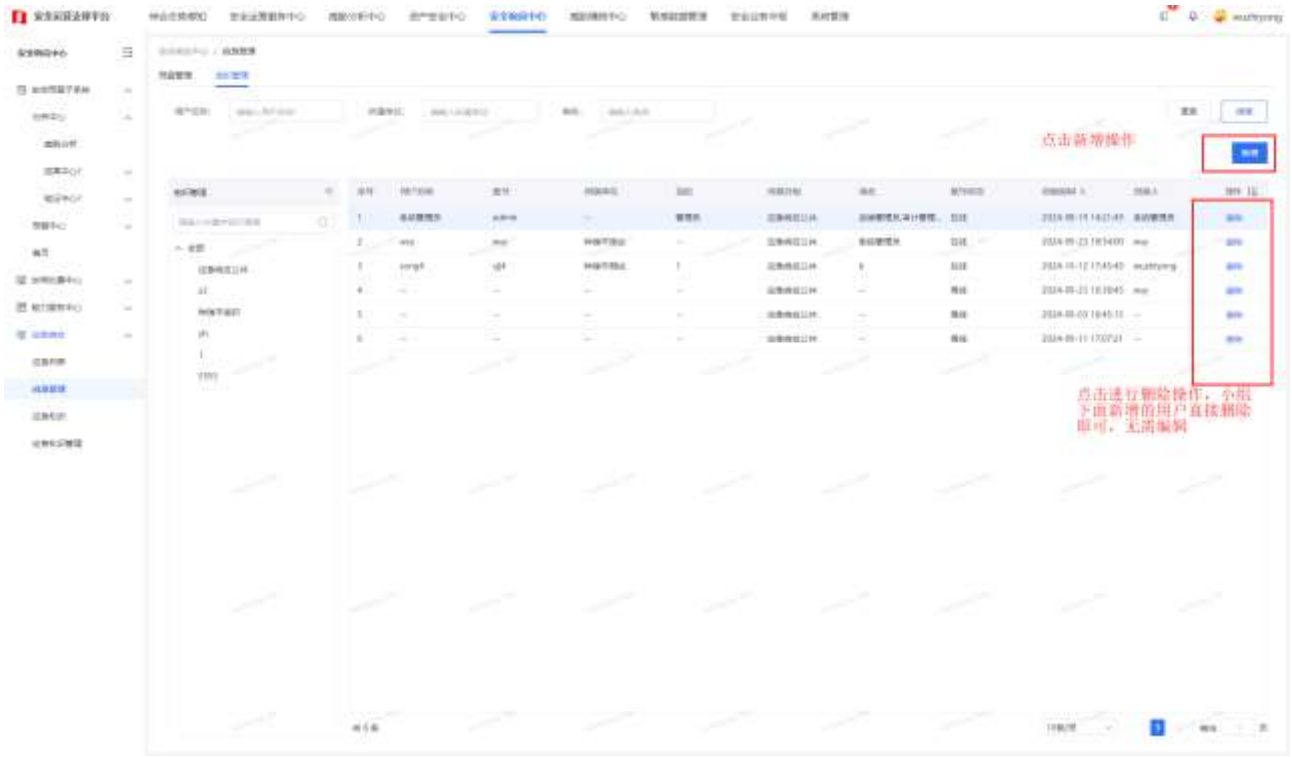
应急小组管理




点击进行编辑
删除操作

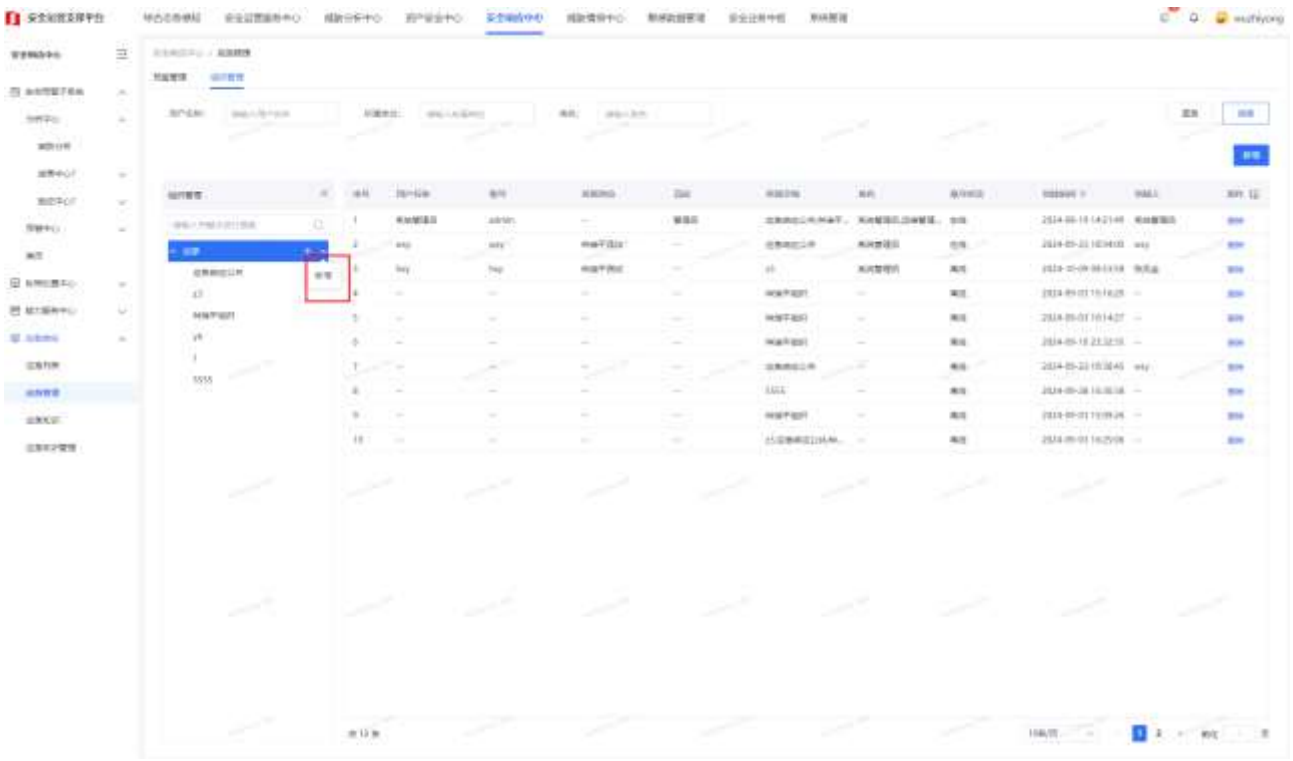


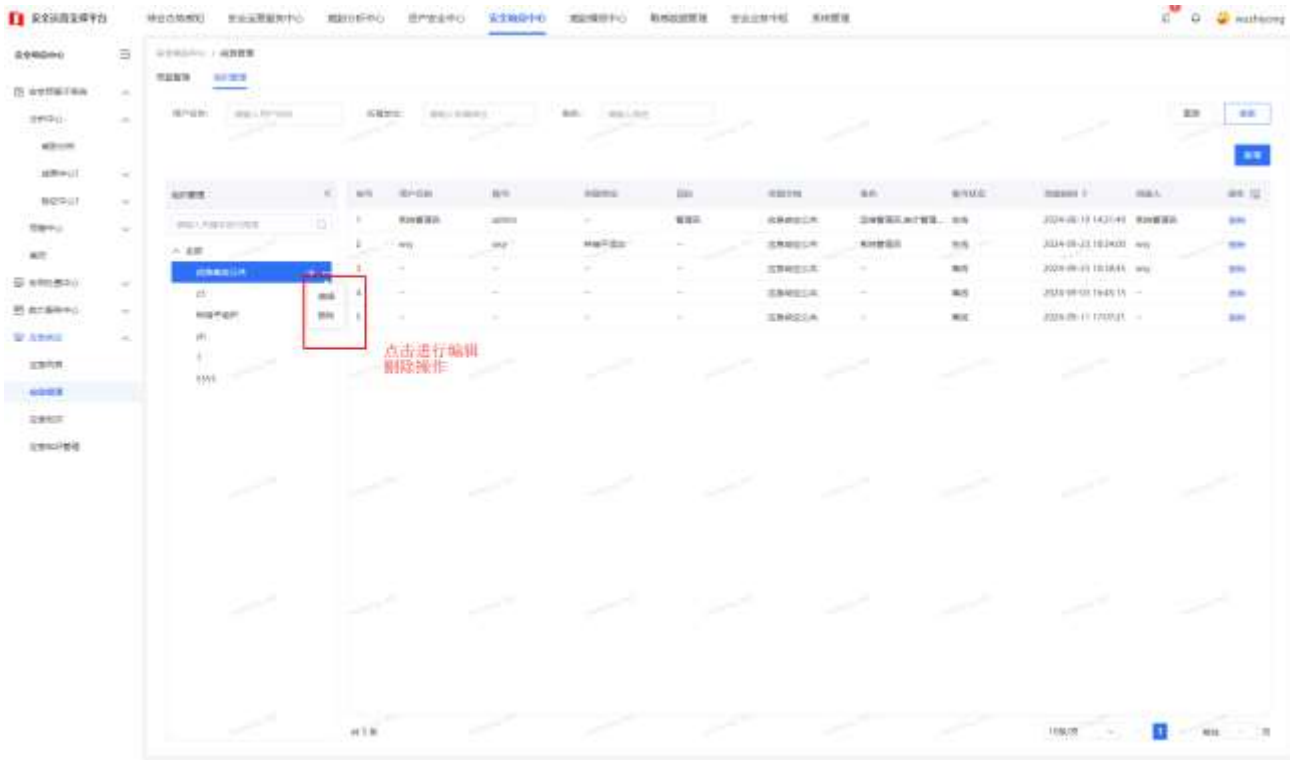
小组成员管理

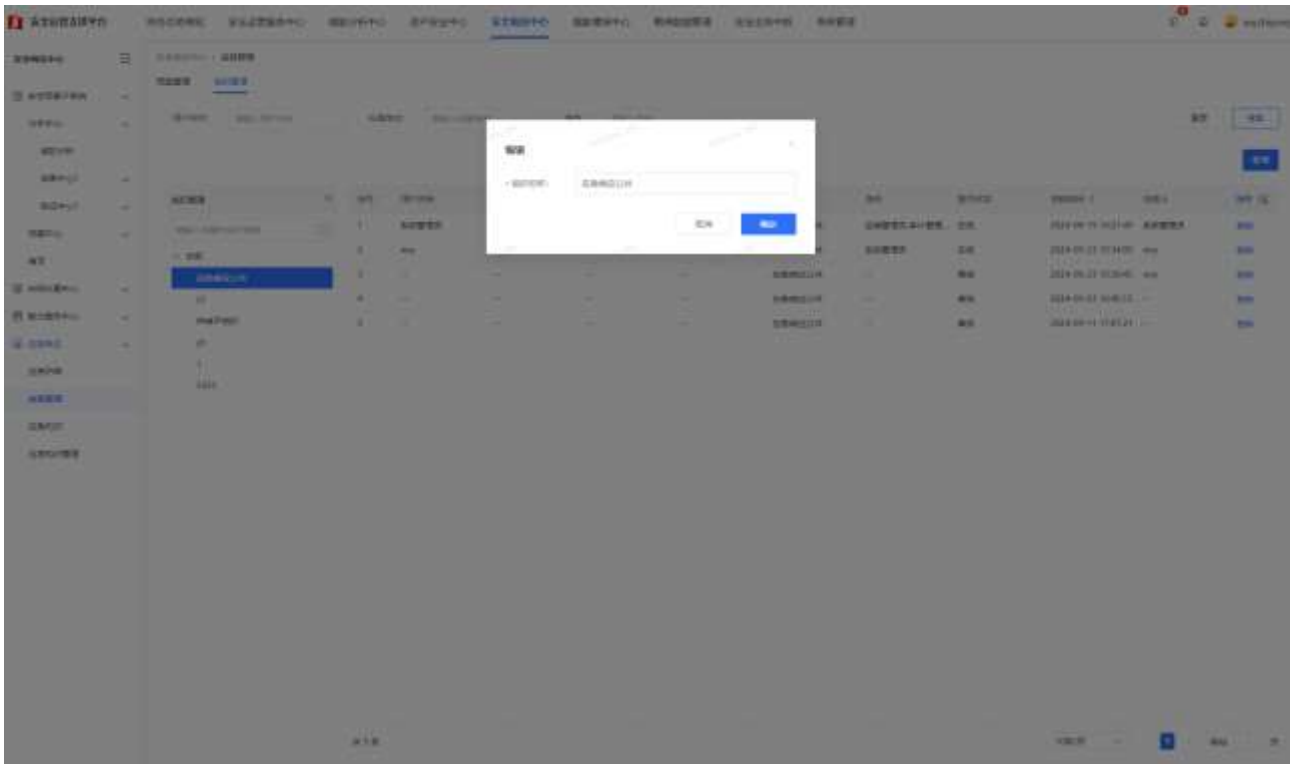


【功能说明】【功能说明】应急管理 -> 组织管理（tab 页）：该功能用于应急响应小组管理以及小组成员的管理

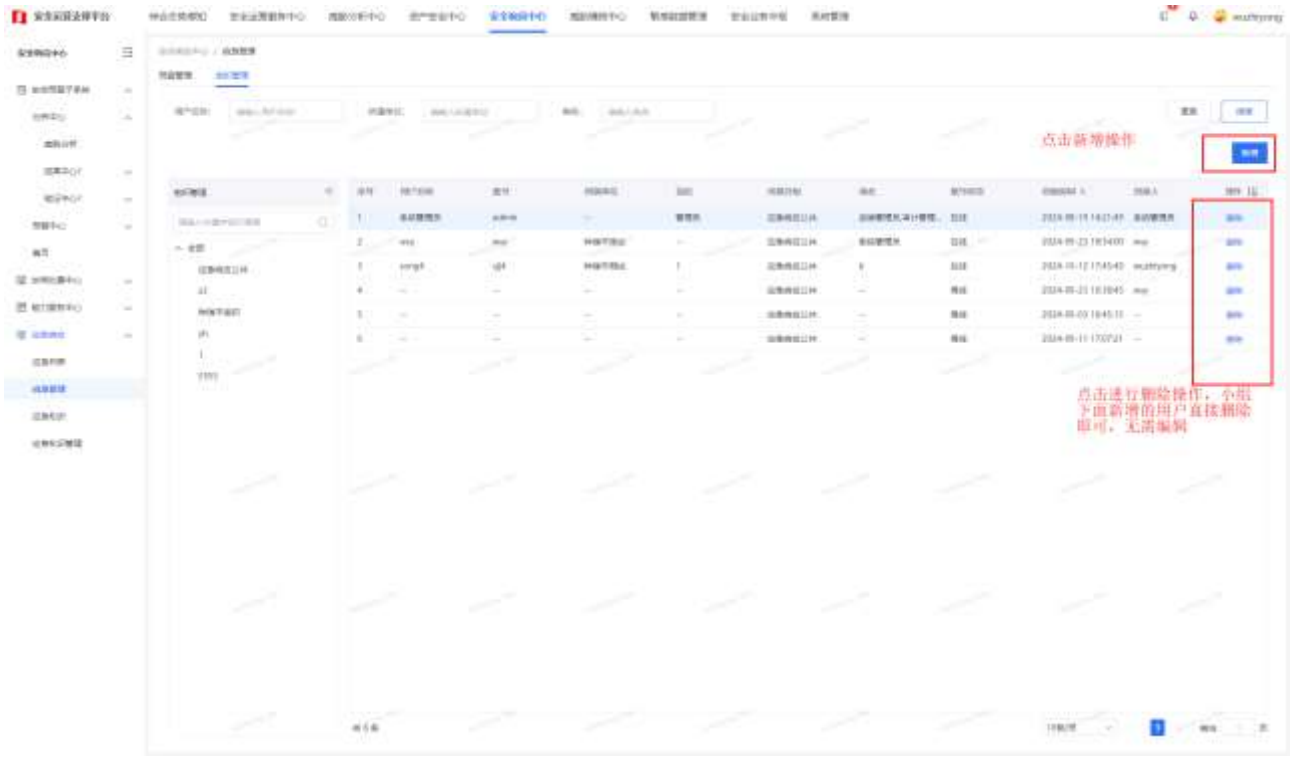
应急小组管理

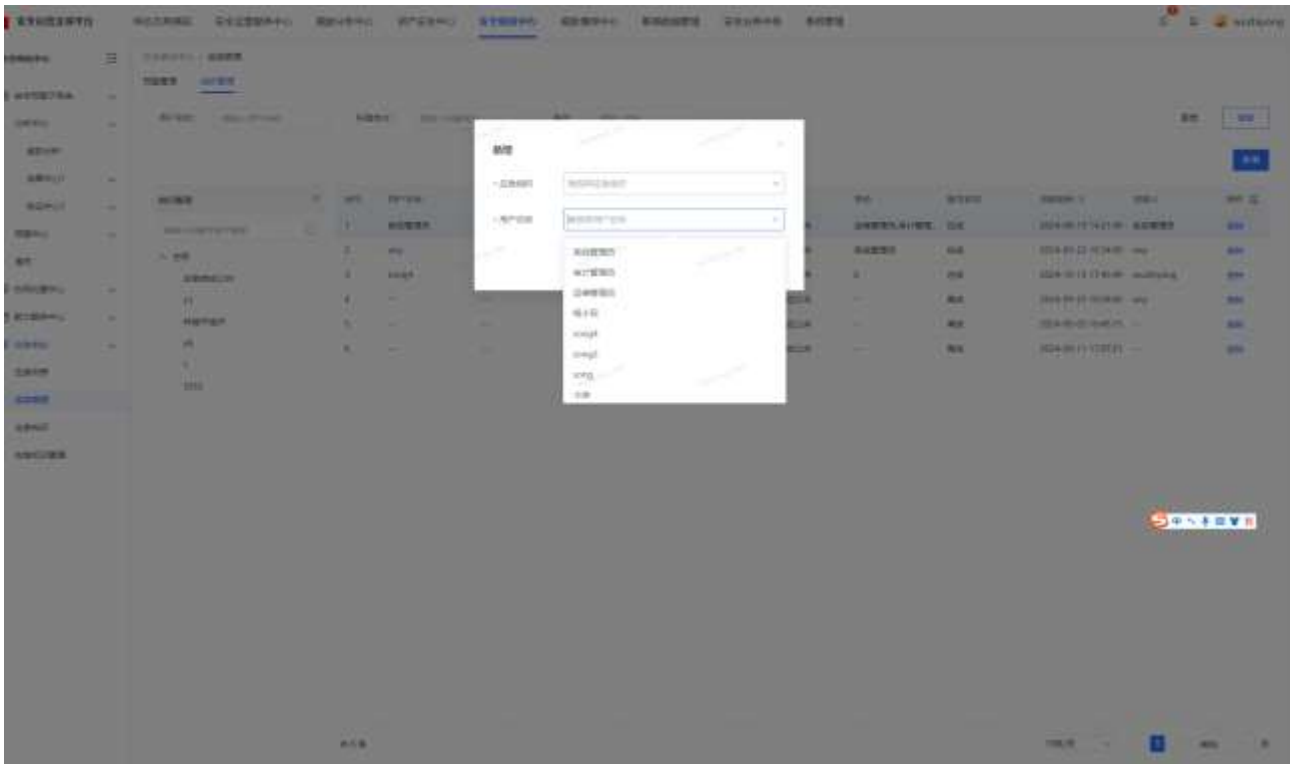






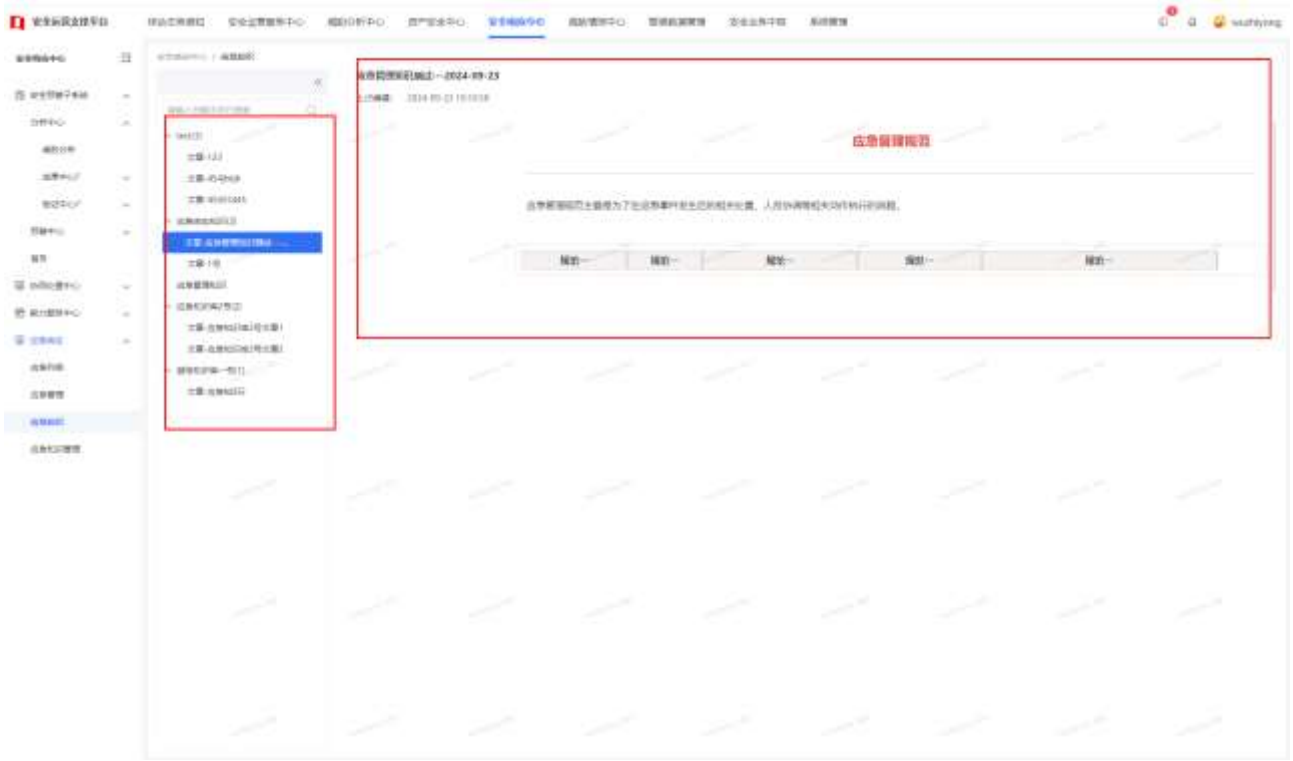
小组成员管理





3.2.1.3 应急知识

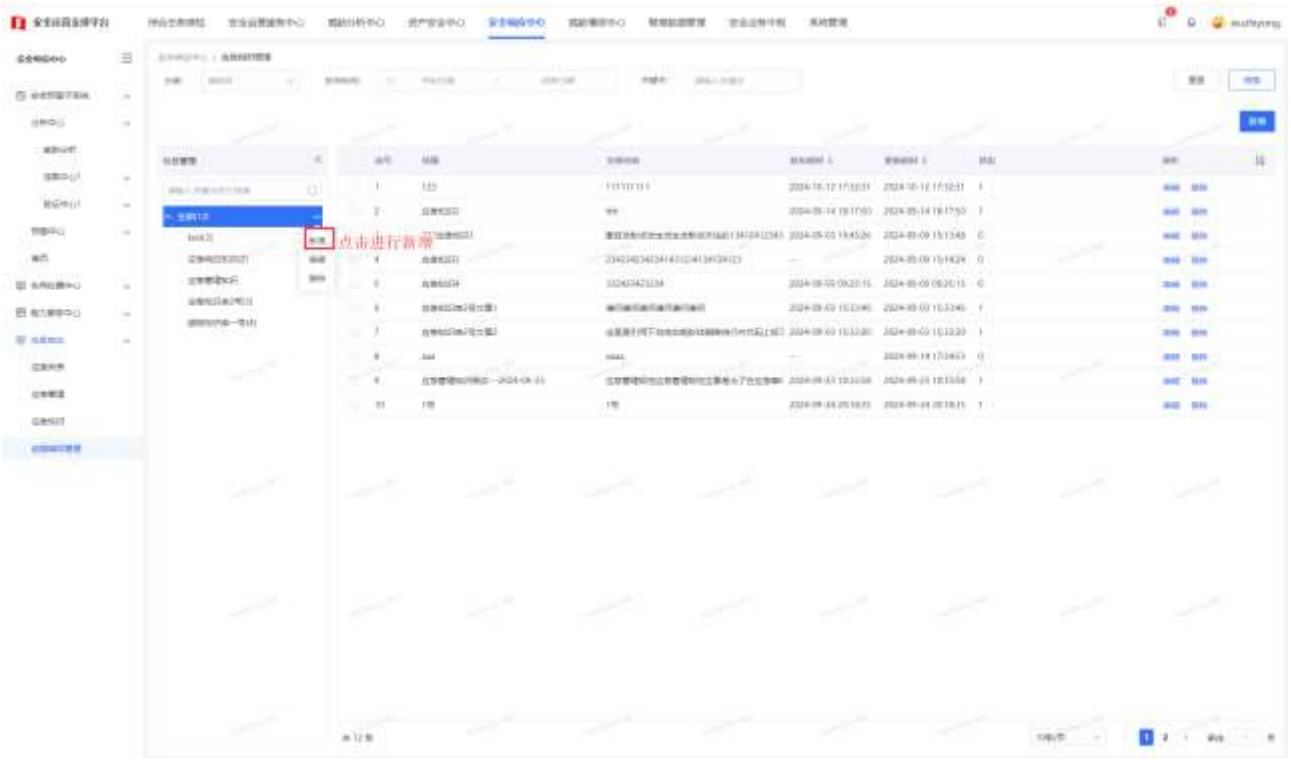
【功能说明】应急知识的集中展示；

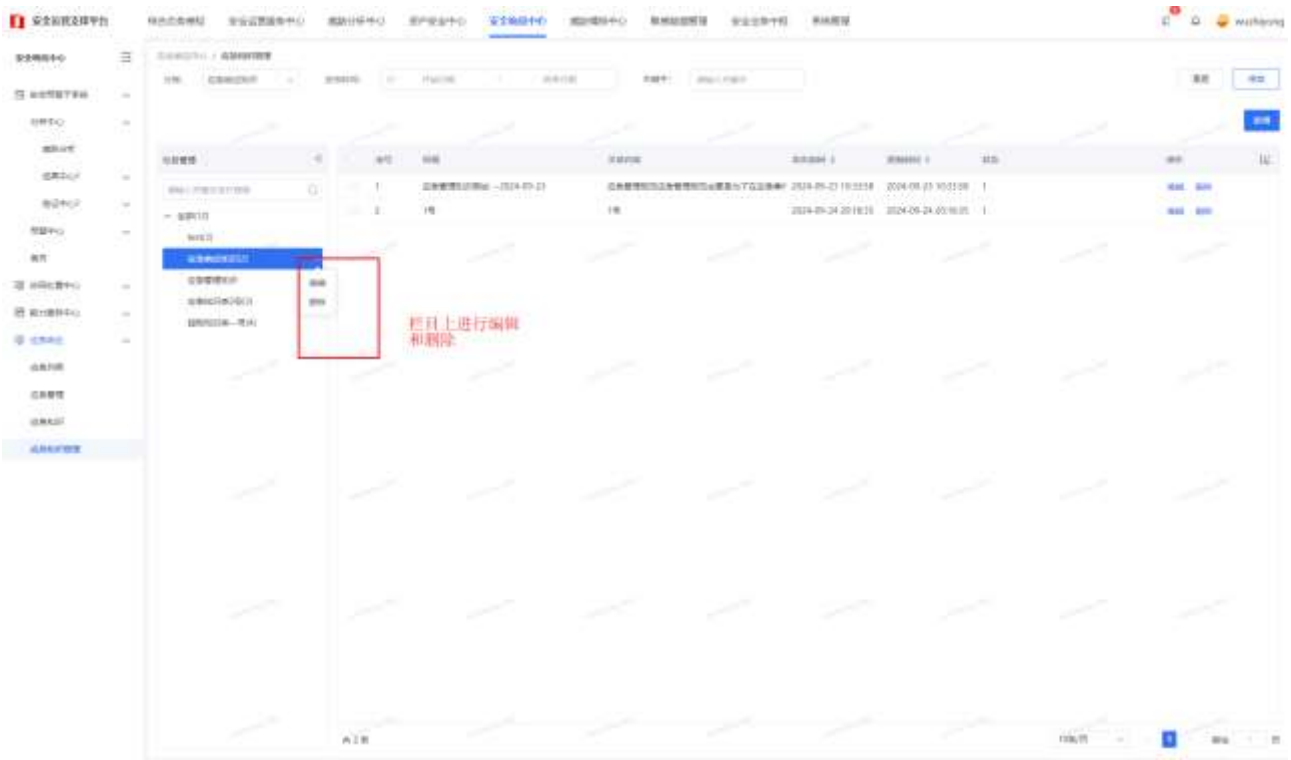


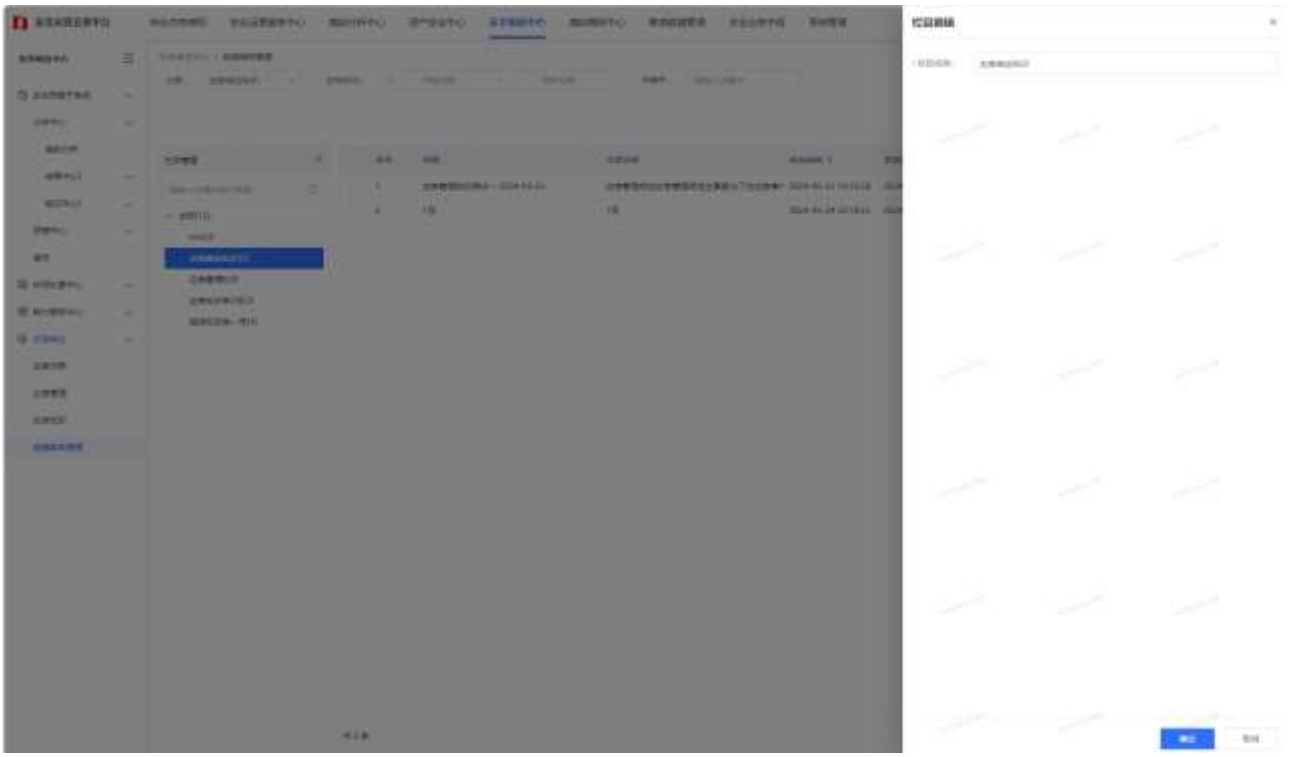
3.2.1.4 应急知识管理

【功能说明】该功能为应急知识的管理，包含栏目管理和知识管理

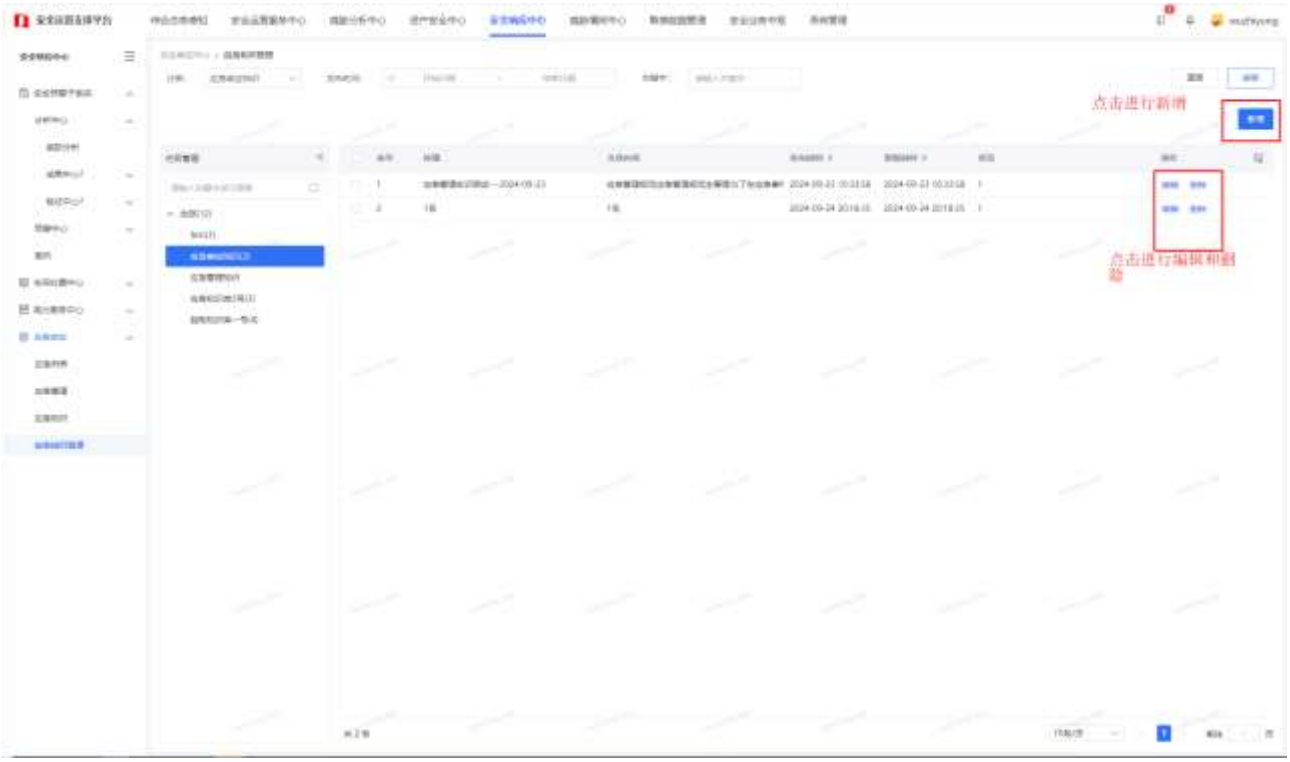
栏目管理

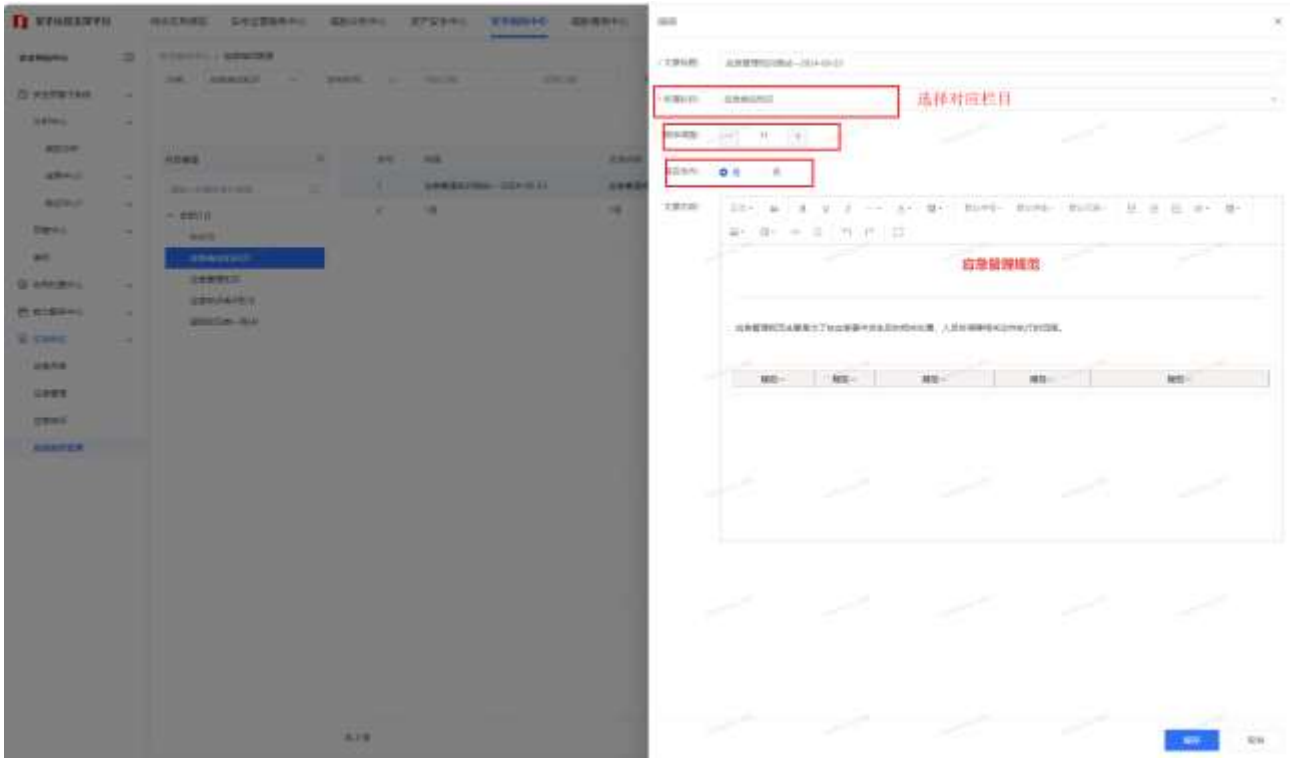


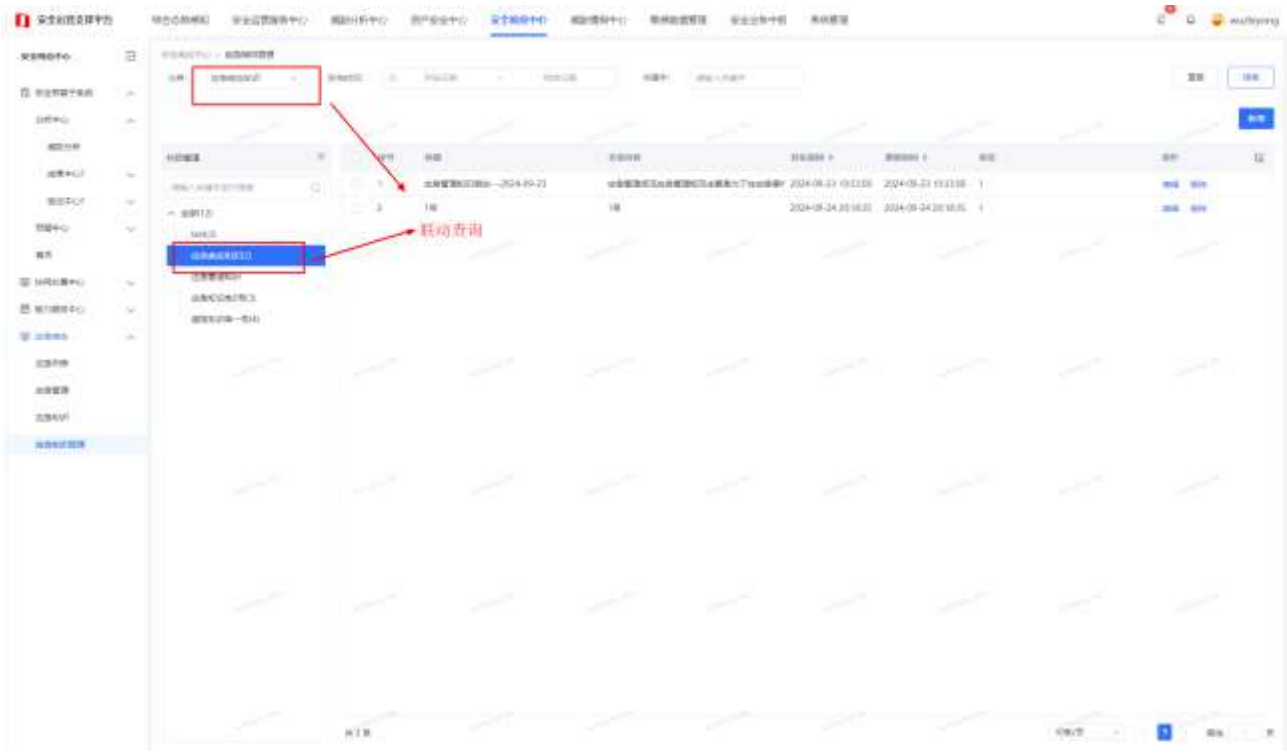




知识管理：针对应急知识的增加、修改、删除




选择对应栏目
应急管理规范


联动查询

3.3 安全运营服务中心

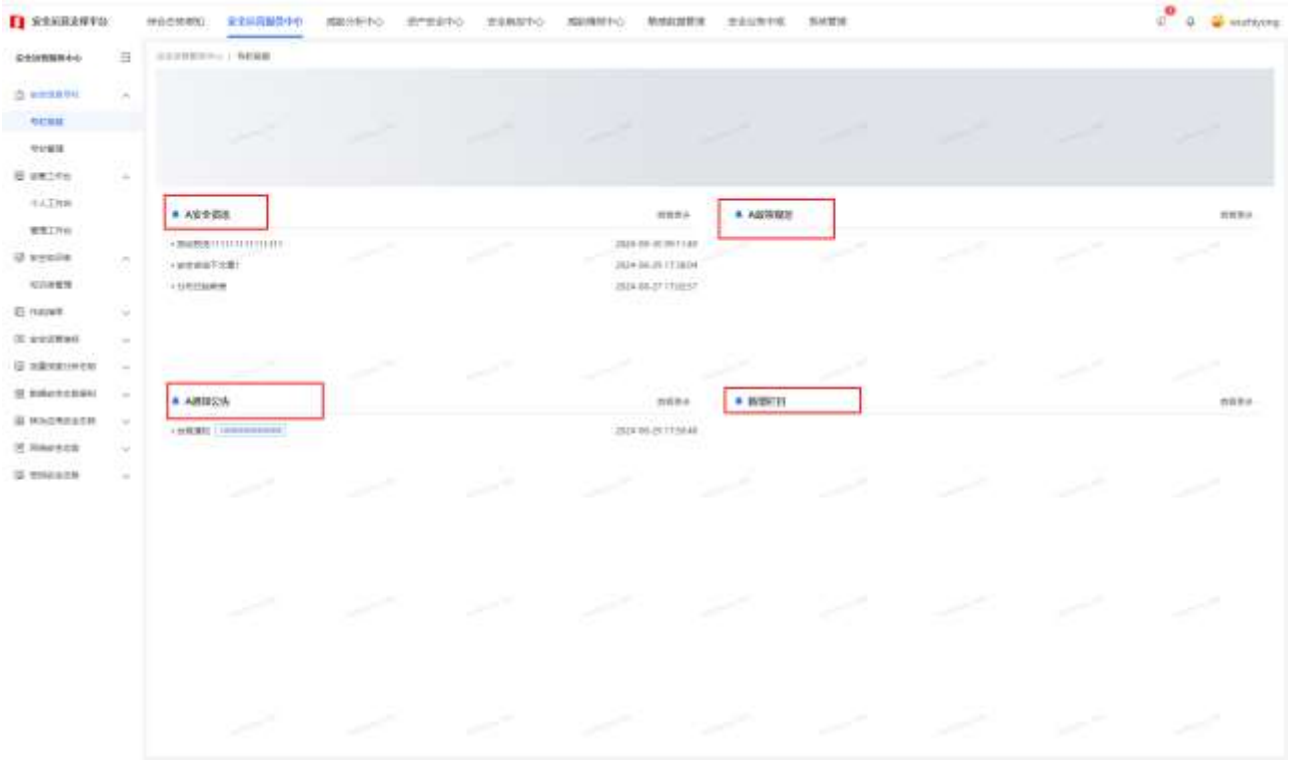
【功能说明】该模块用于提供安全运营服务，为系统的安全运营提供支撑；包括安全信息专栏、运营工作台、安全知识库、指挥调度、安全运营指标以及安全运营态势感知与分析等等；

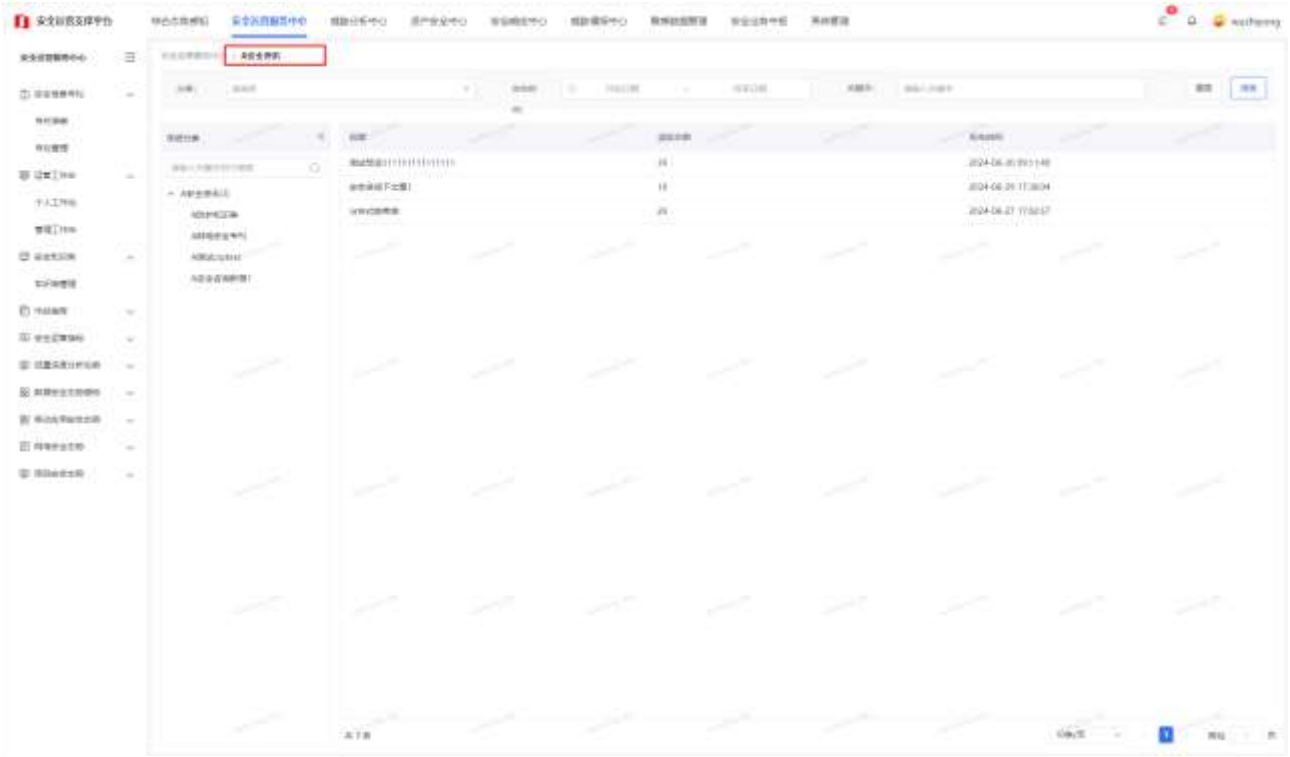
3.3.1 安全信息专栏

【功能说明】包括安全信息的专栏管理，文章管理，以及对外发布的专栏信息的页面展示；

3.3.1.1 专栏信息

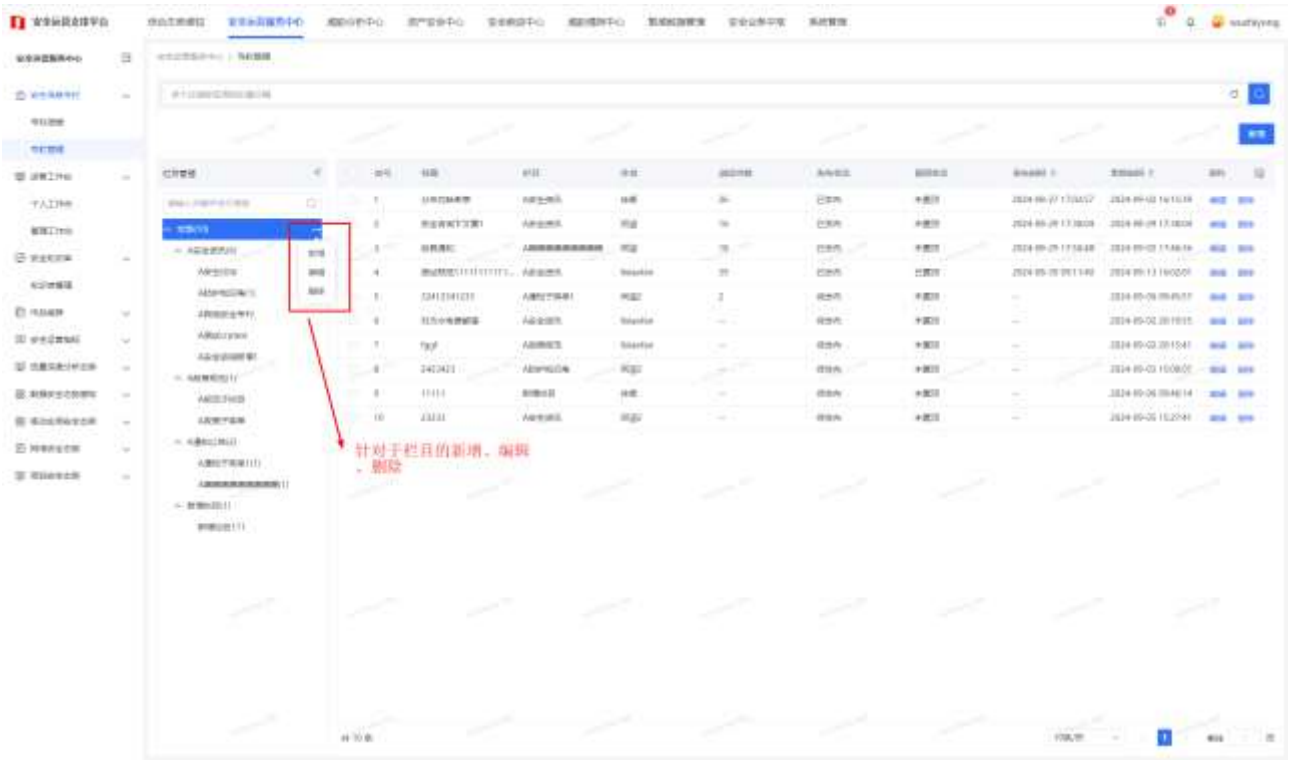
【功能说明】专栏信息不同栏目的整体布局查看与展示；

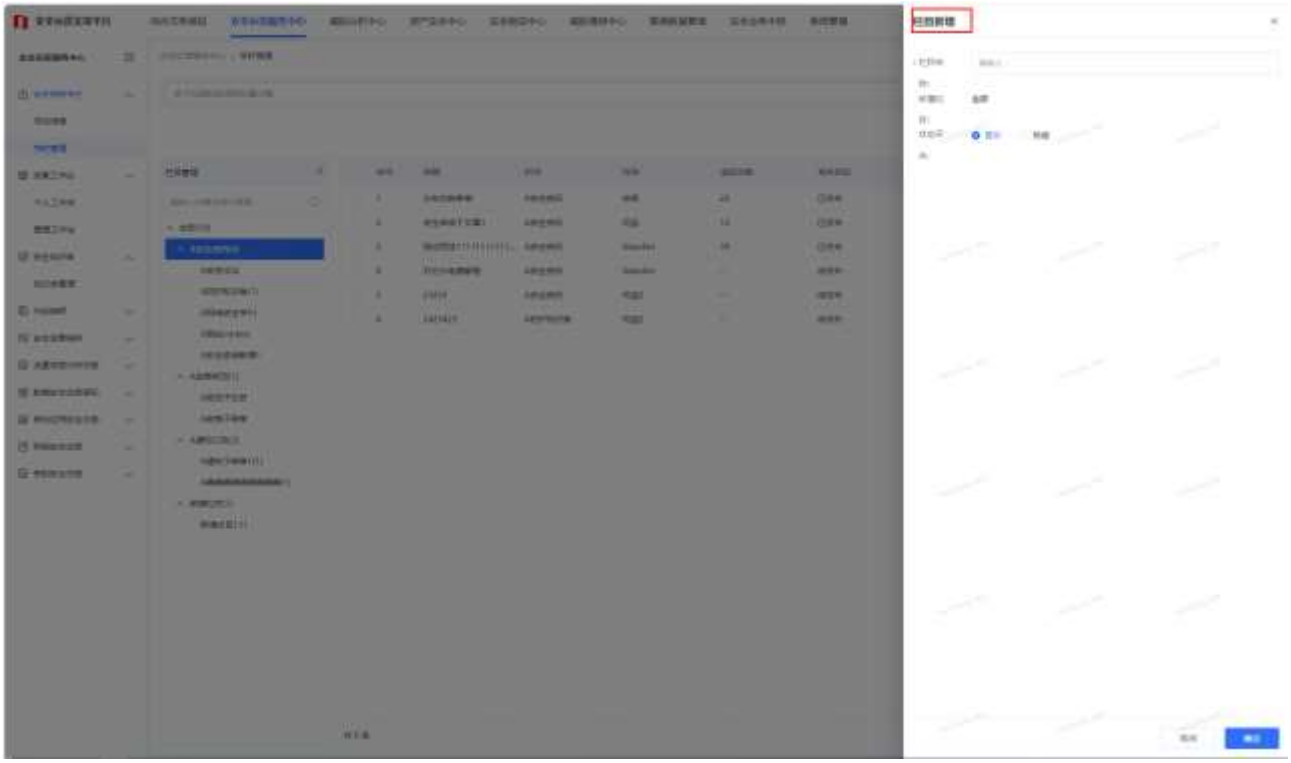


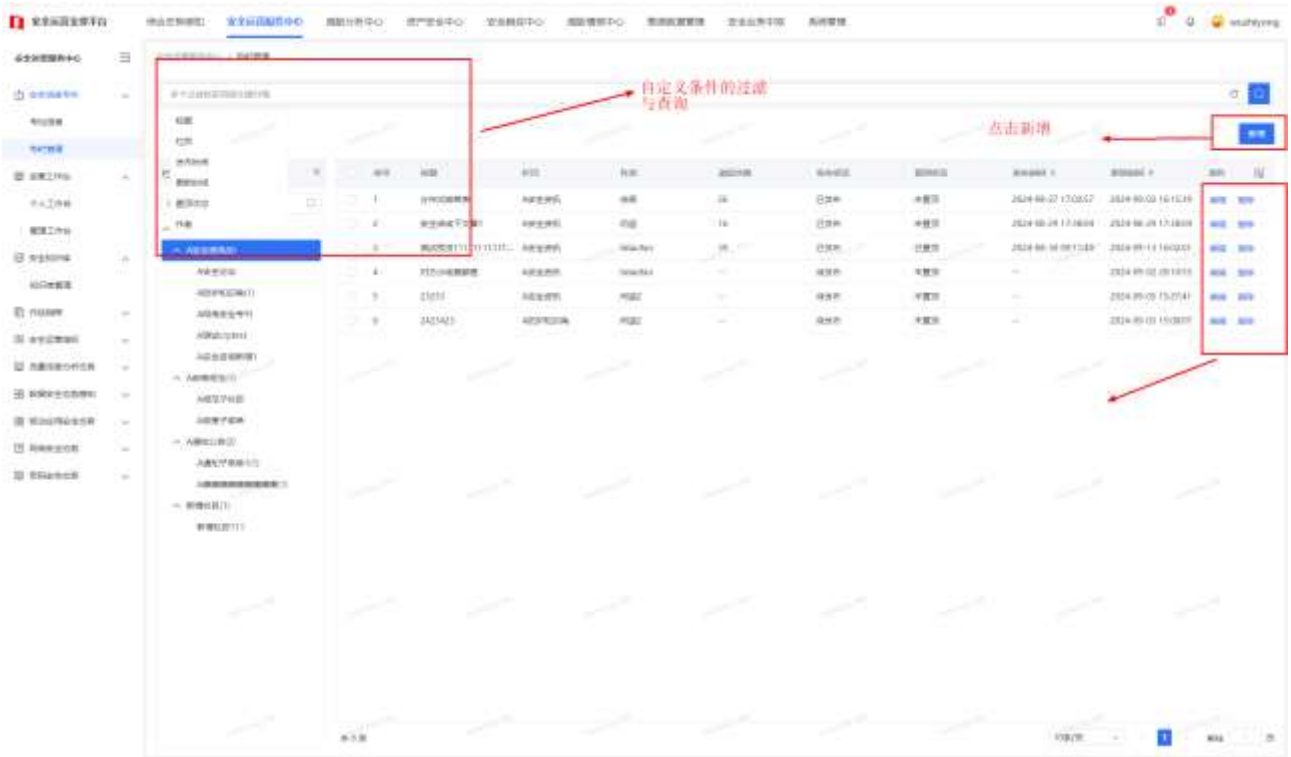


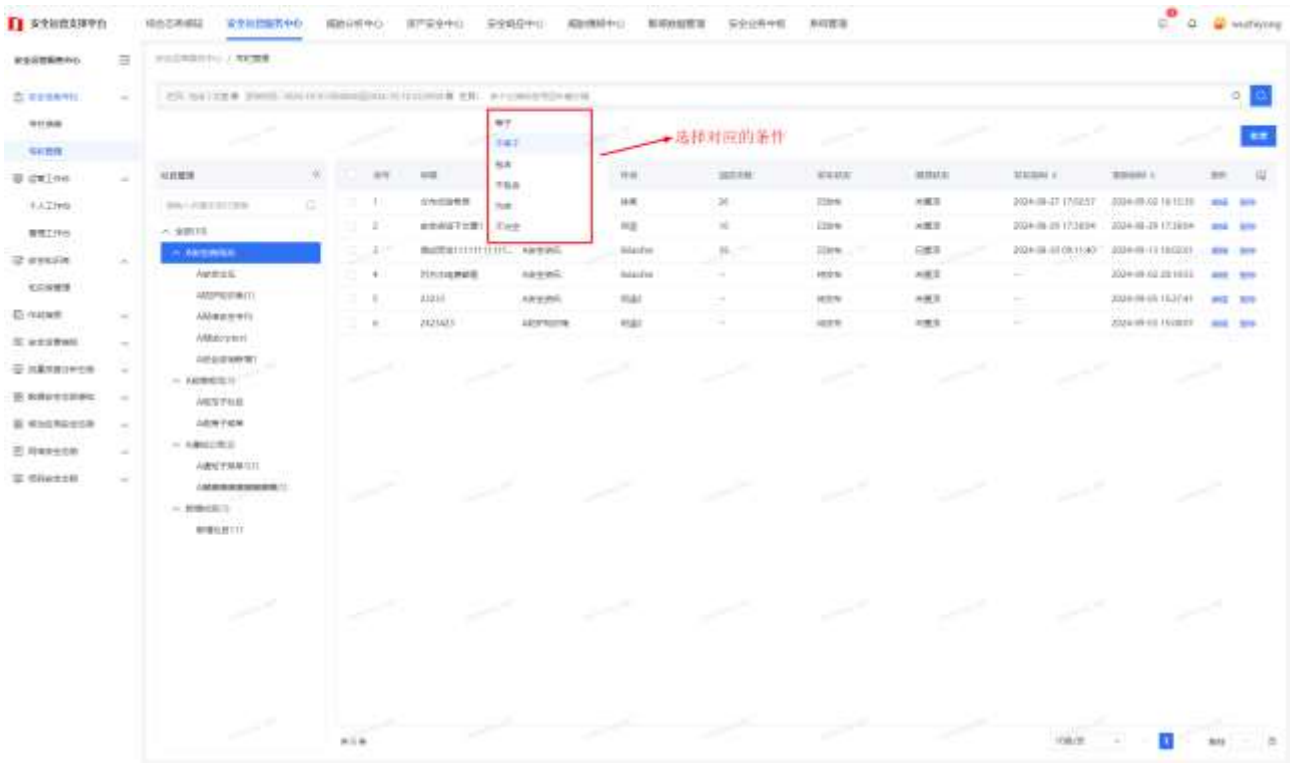
3.3.1.2 专栏管理

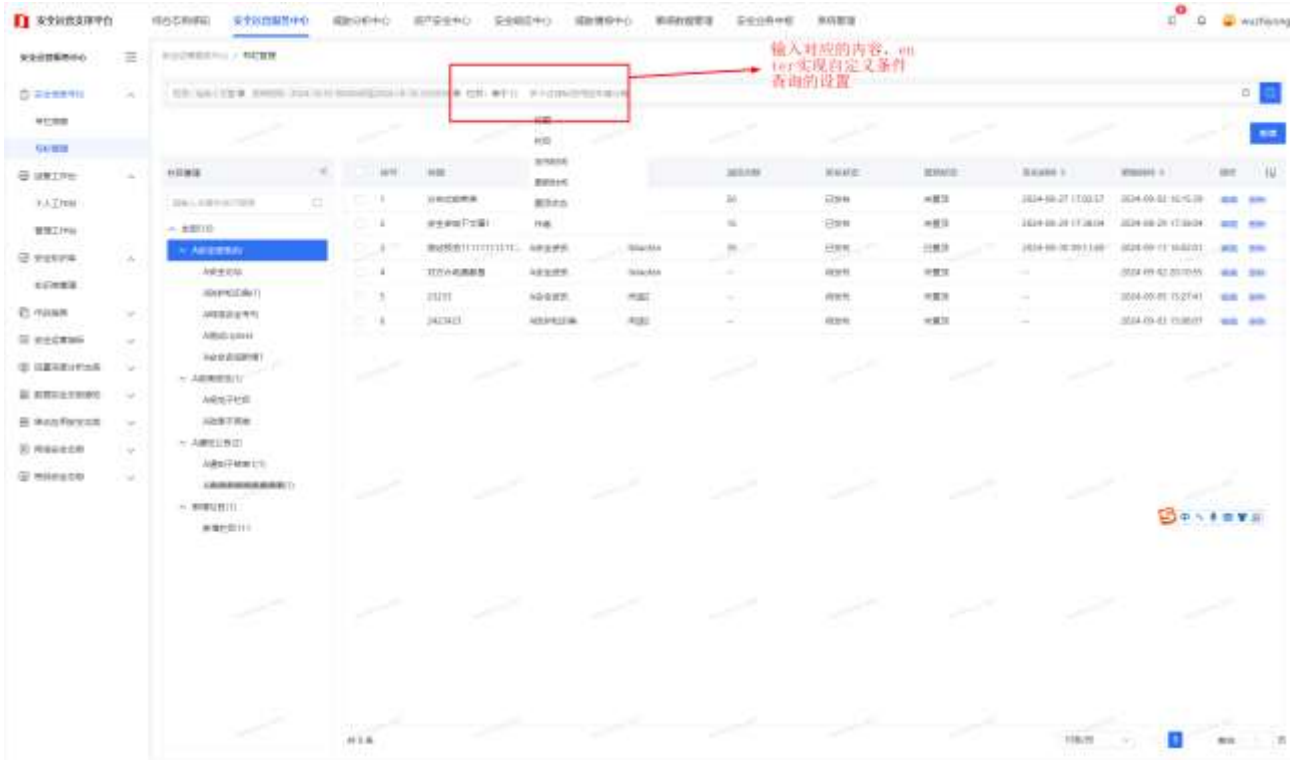
【功能说明】针对于信息专栏的增加、编辑、删除的维护，以及专栏下信息的增加、编辑、删除的维护；

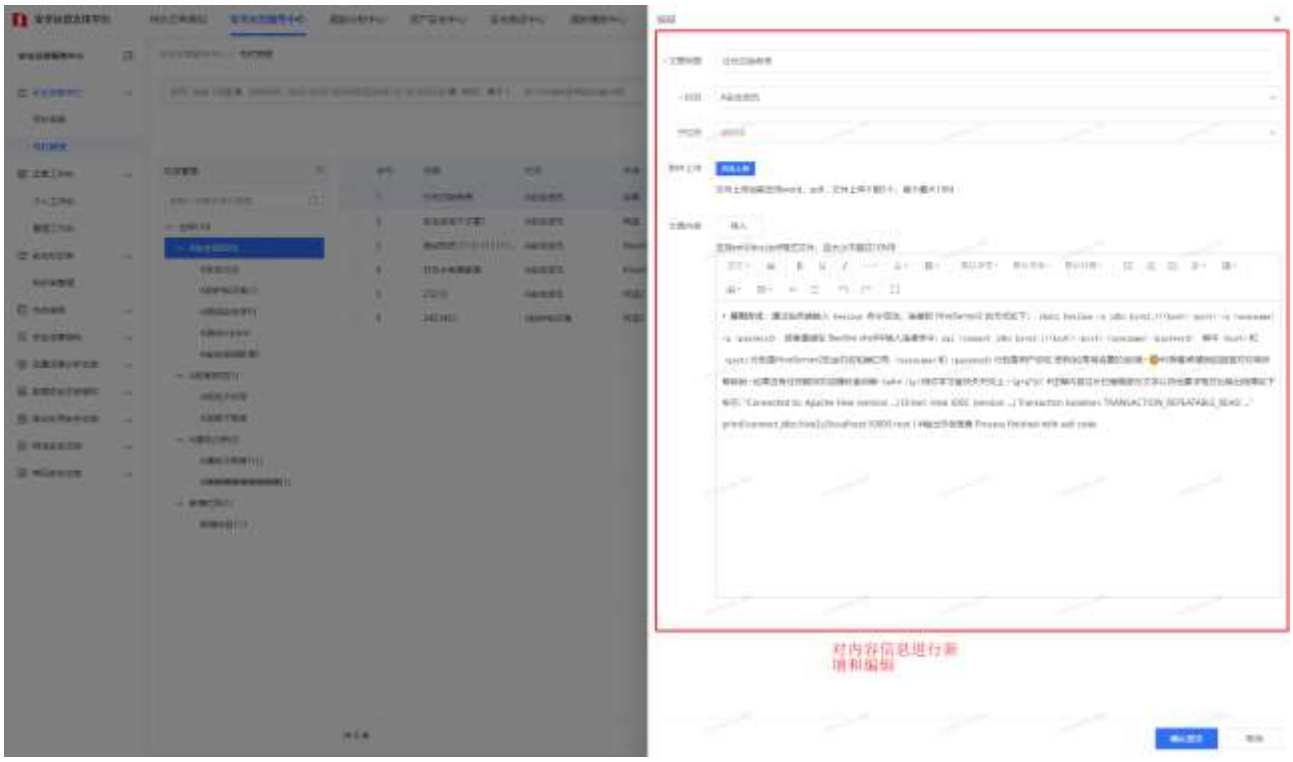





自定义条件的过滤
与查询
点击新增


选择对应的条件


输入对应的内容，enter实现自定义条件查询的设置

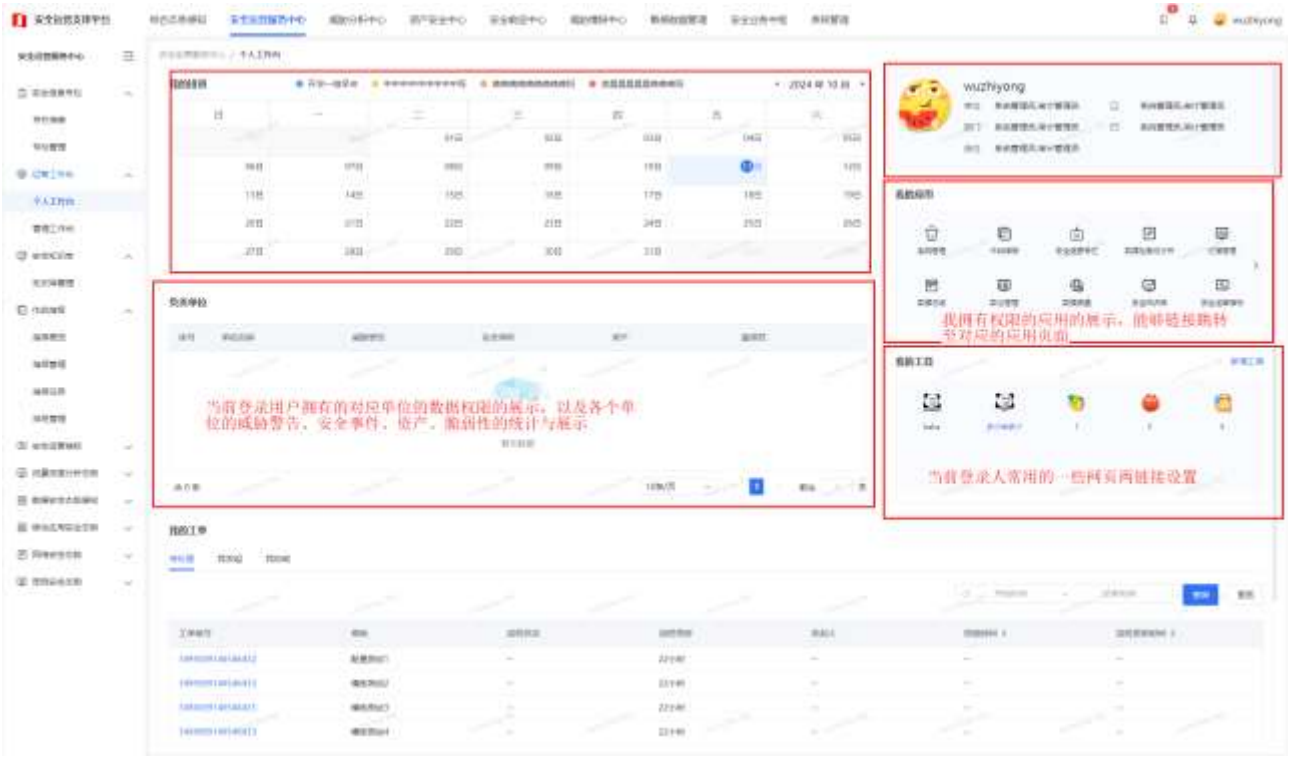


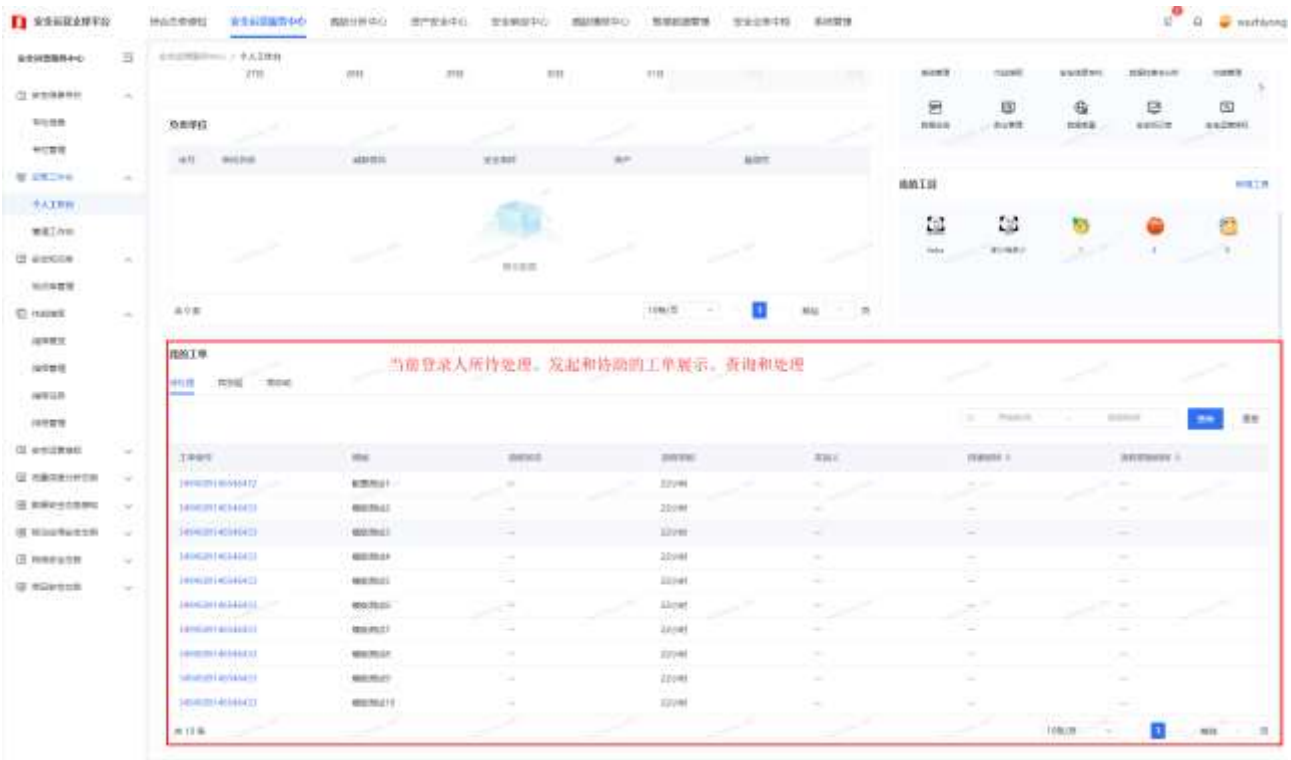
3.3.2 运营工作台

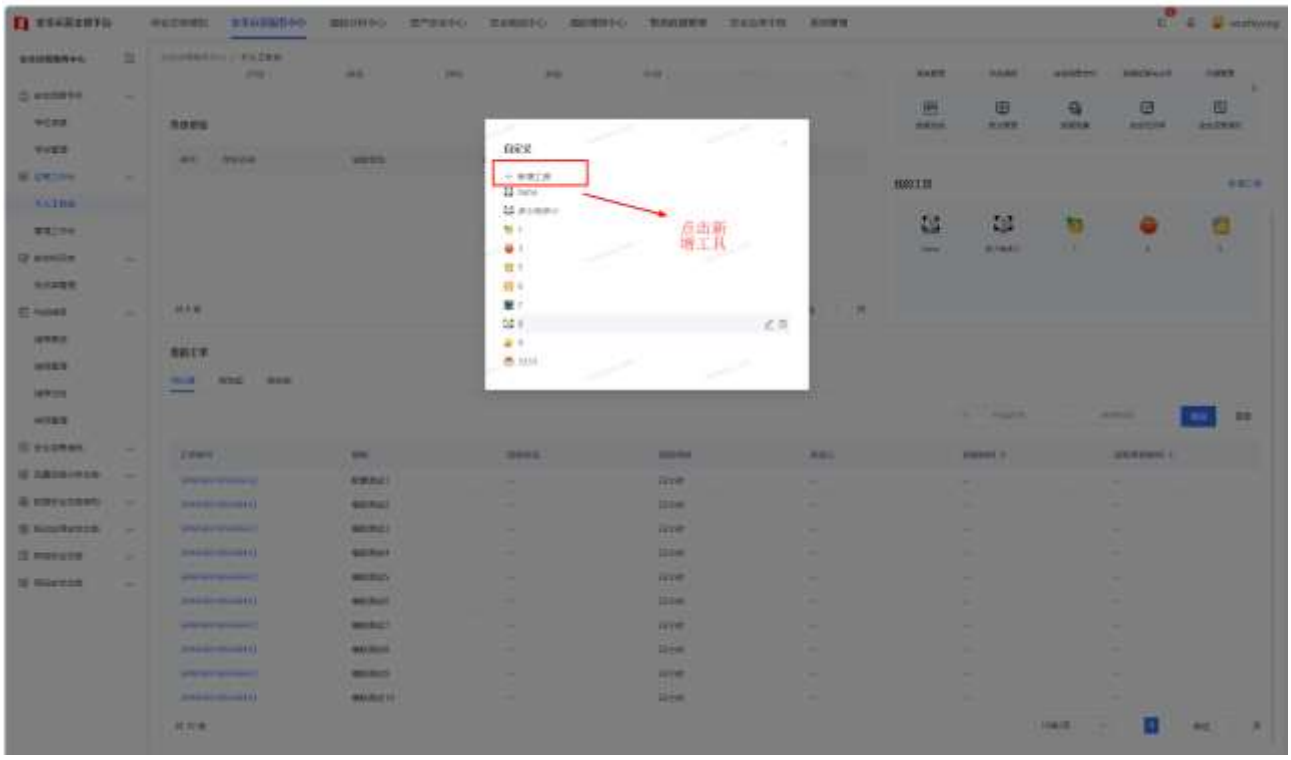
【功能说明】该功能用于个人工作台的运营基本信息展示，以及管理工作台不同视角的运营指标的统计与展示；

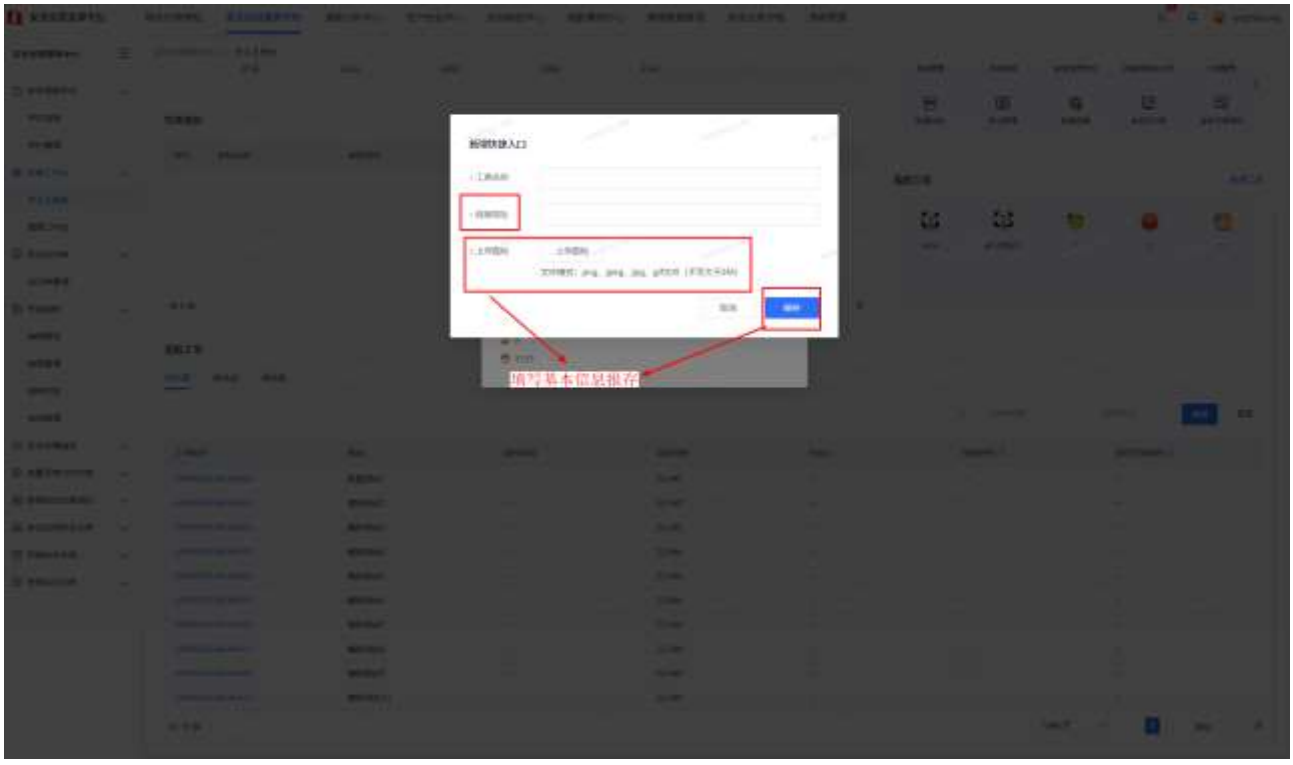
3.3.2.1 个人工作台

【功能说明】用于当前登录人的当前运营工作的信息与功能的展示，包括我的排班、个人信息、所负责的单位、所拥有的应用、个人常用的工具以及对应的需要处理的工单信息等；


wuzhiyong
我拥有权限的应用的展示，能够链接跳转至对应的应用页面
当前登录用户拥有的对应单位的数据权限的展示，以及各个单位的威胁警告、安全事件、资产、脆弱性的统计与展示
当前登录人常用的一些网页两链接设置


当前登录人所待处理、发起和协助的工单展示，查询和处理





3.3.2.2 管理工作台

【功能说明】该功能用于通过不同的视角实现对安全事件的统计与展示，目前

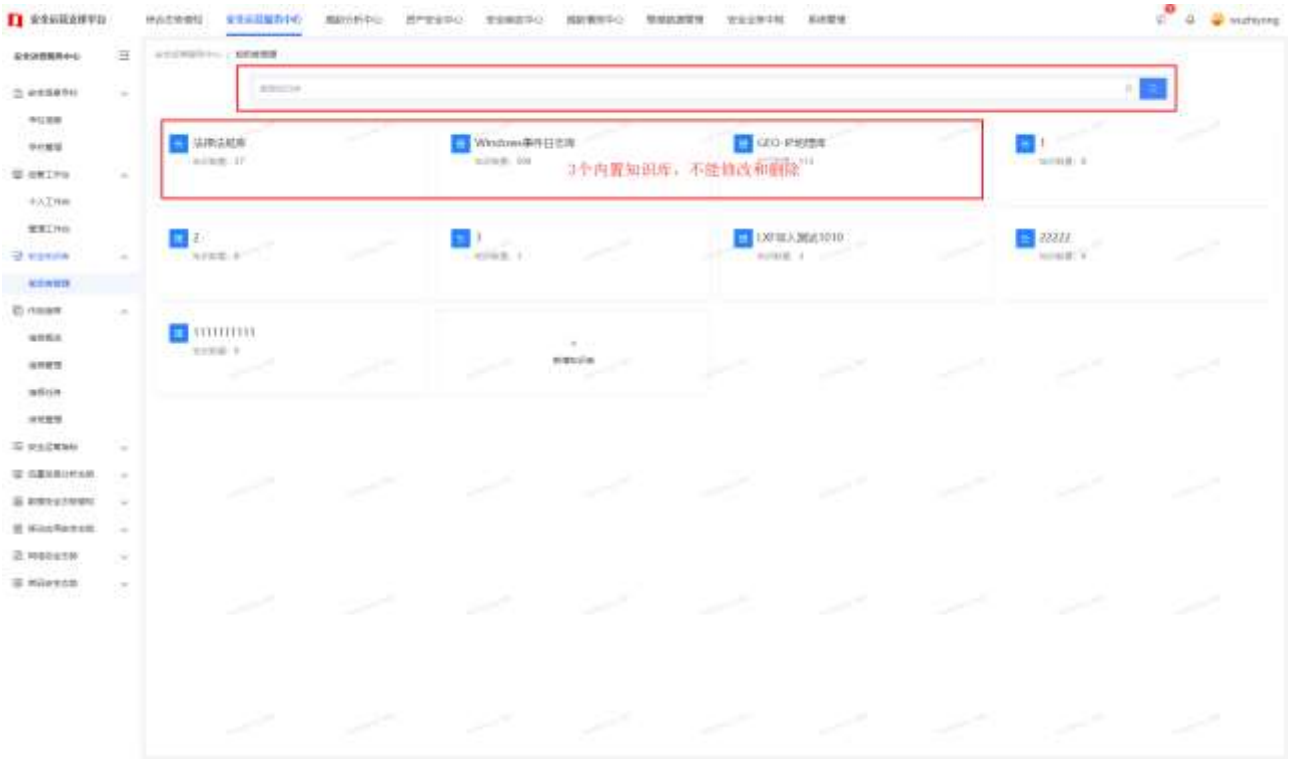
主要为单位视角和人员视角；

3.3.3 安全知识库

【功能说明】点击【安全知识库】-【知识库管理】进入知识库管理页面，该功能实现了对内置知识库与自定义知识库的管理，同时实现了对各知识库中知识内容的管理；

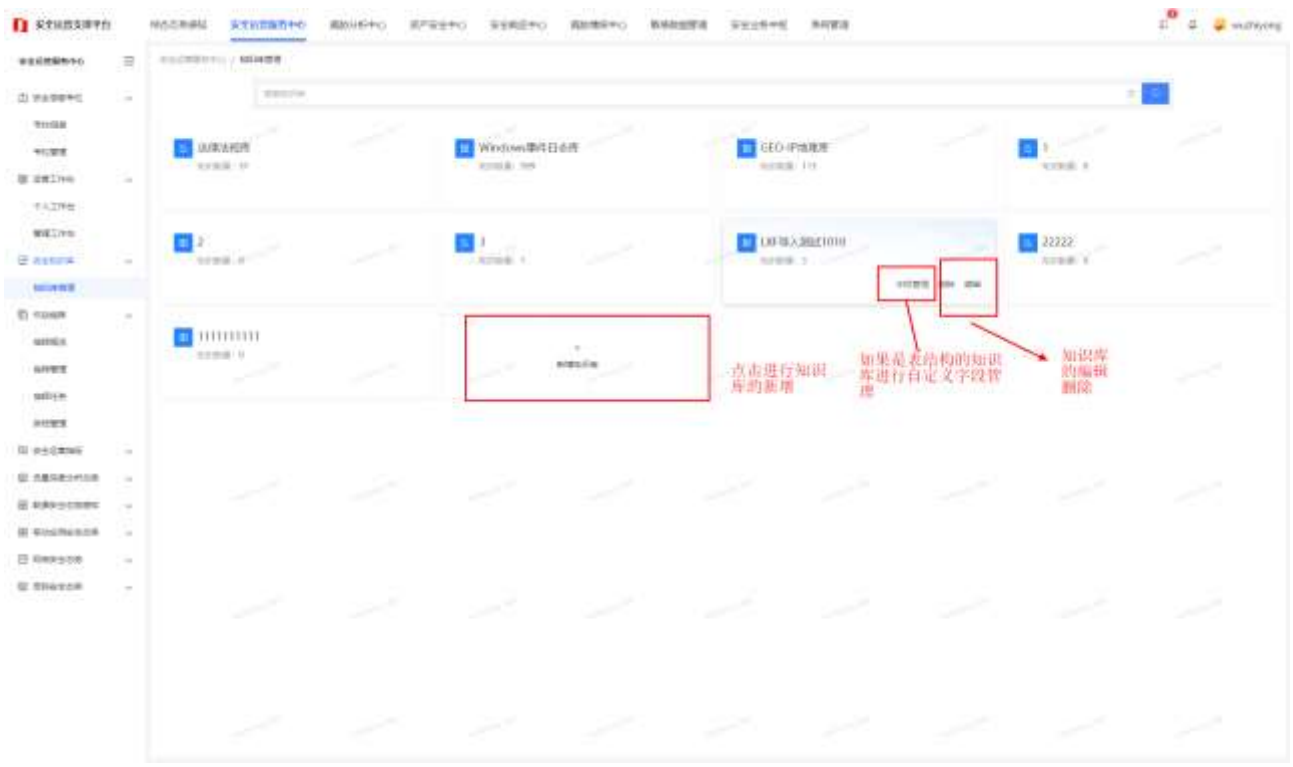
3.3.3.1 知识库管理

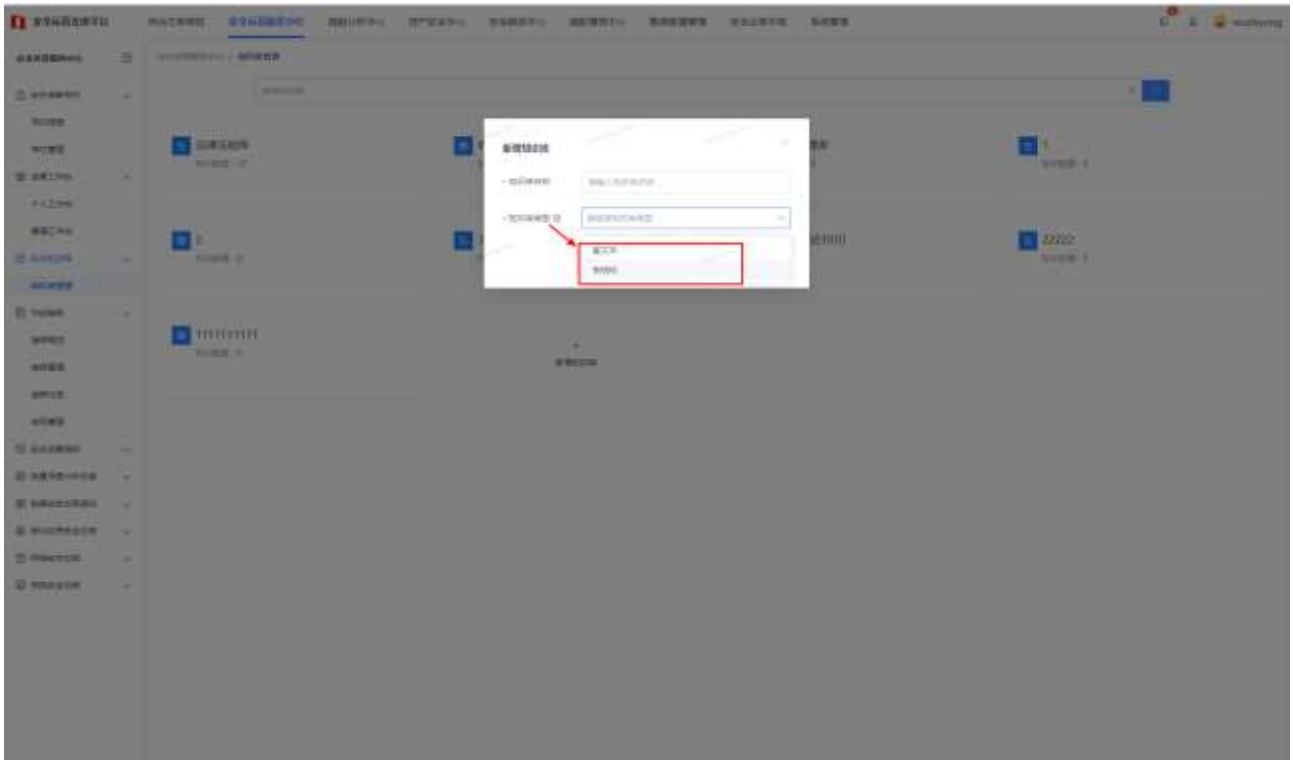
【功能说明】针对于不同类型知识库的新增修改、编辑和删除，以及不同类型知识库的内容的新增、修改、删除；

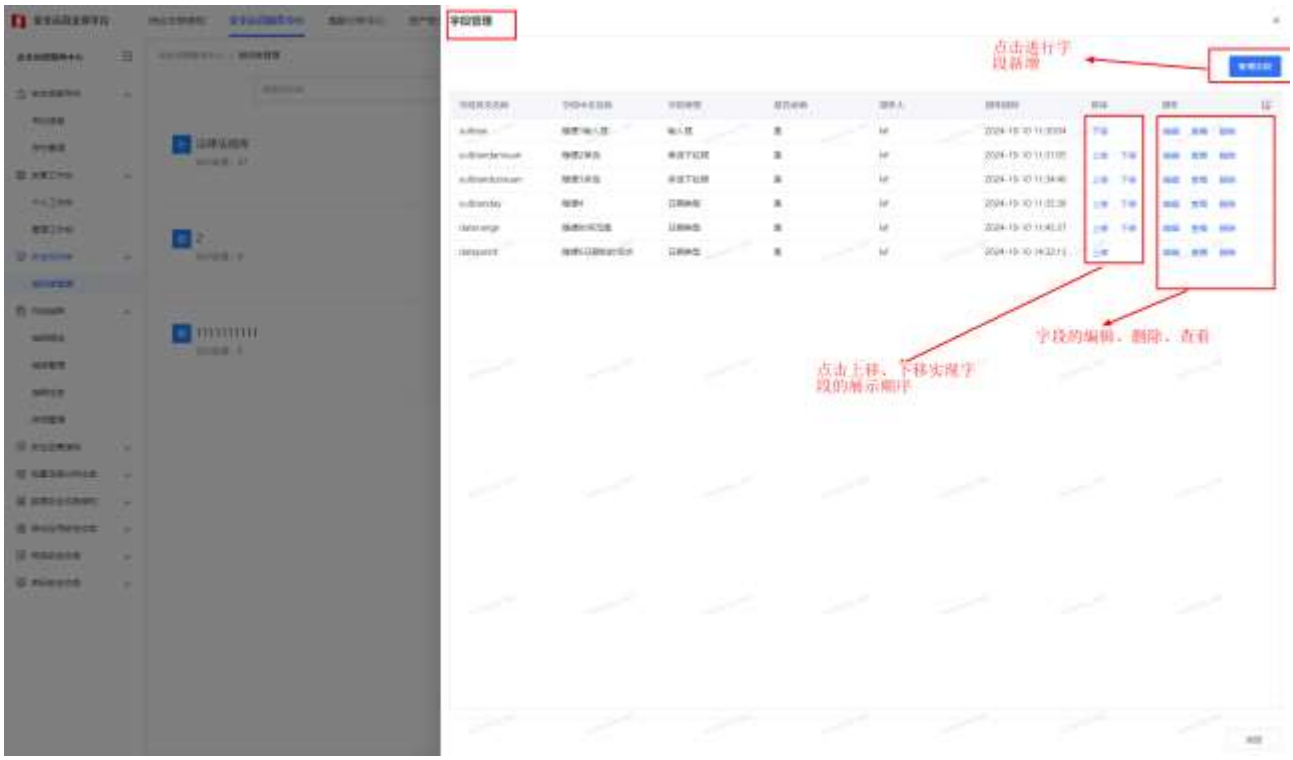


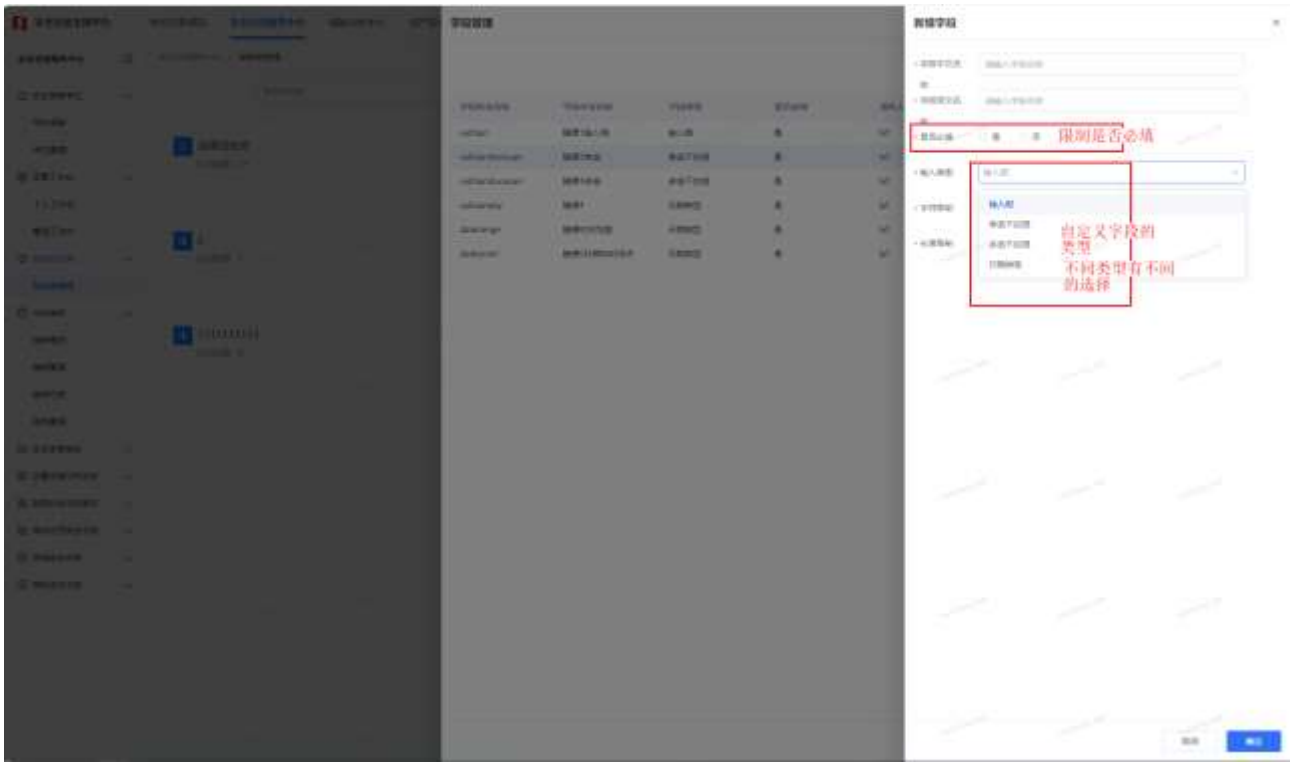
3.3.3.1.1 知识库管理

【功能说明】点击【知识库管理】菜单进入知识库管理展示页面，该功能实现了内置知识库的展示，自定义知识库的增加、修改、删除，如果类型为表结构的实现了知识库的自定义字段；


点击进行知识库的新增
如果是表结构的知识库进行自定义字段管理
知识库的编辑删除




字段管理
点击进行字段新增
字段的编辑、删除、查看
点击上移、下移实现字段的展示顺序


限制是否必填
自定义字段的类型
不同类型有不同的选择

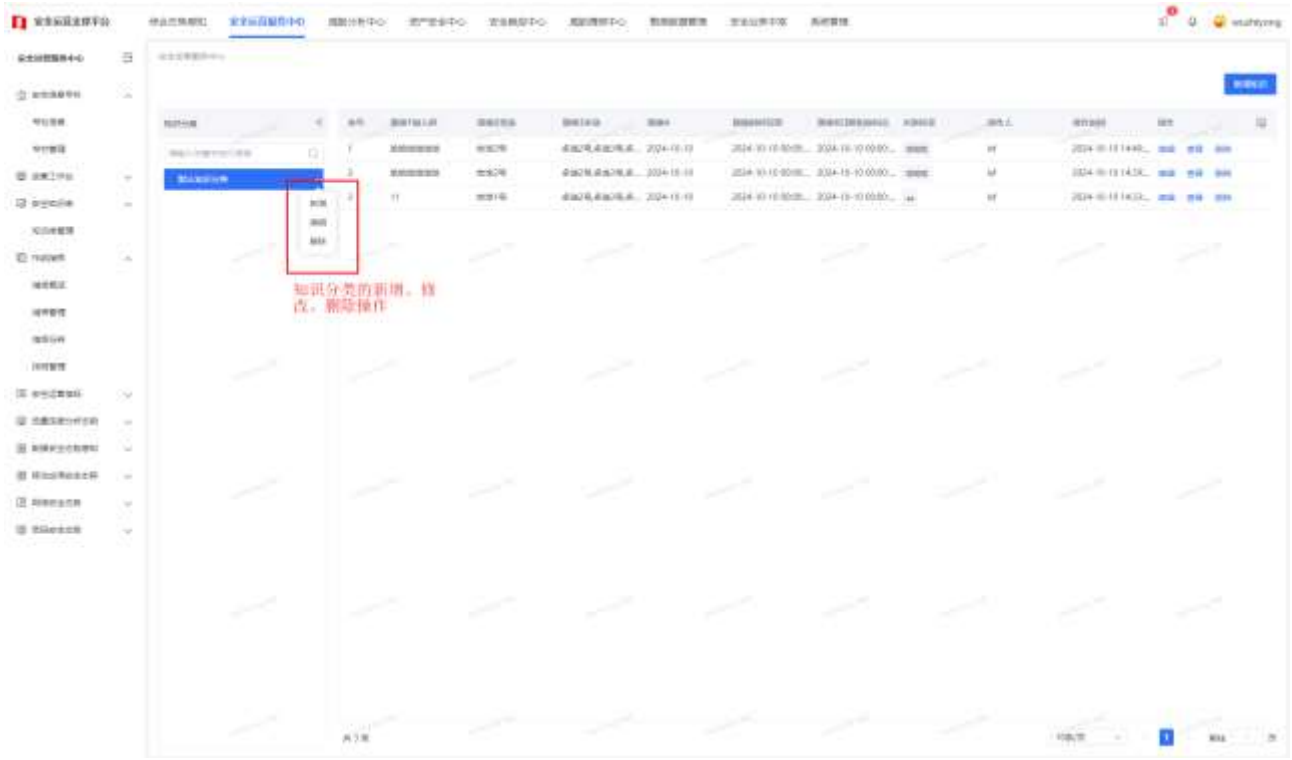

字段管理
新增字段
中文
英文
数字
特殊字符


字段管理
新增字段
必须属性填完后
才能新增枚举值

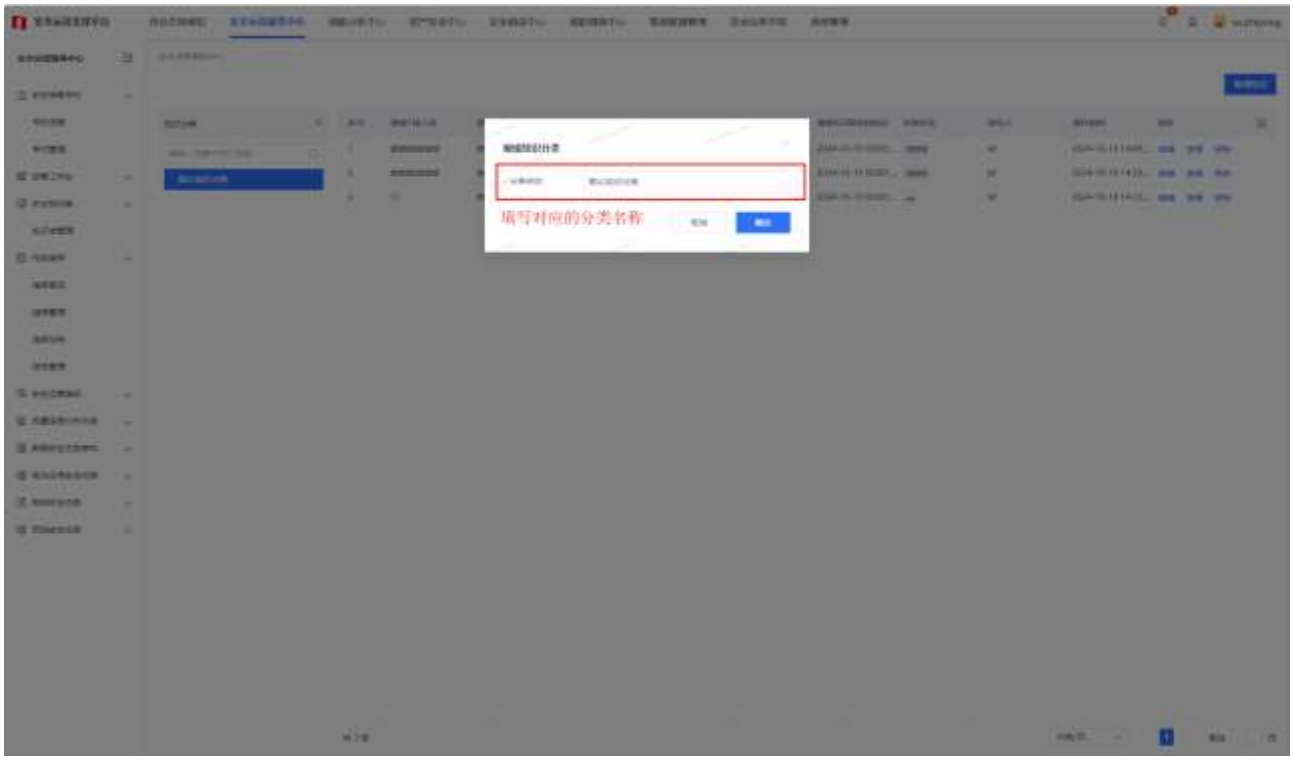

字段管理
新增字段

3.3.3.1.2 知识库内容管理

【功能说明】点击对应的知识库进入对应的知识库内容管理页面，实现知识库内容的新增、修改、删除、查看操作，以及知识分类管理操作；

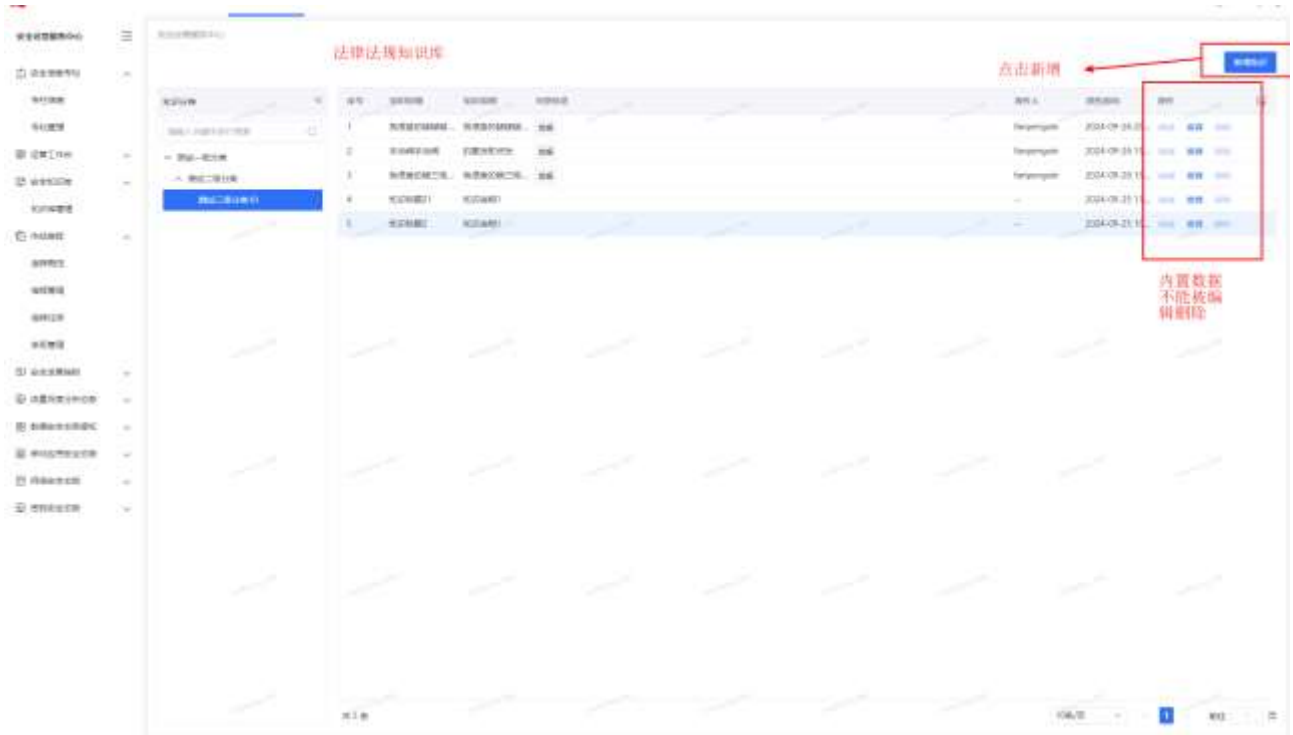


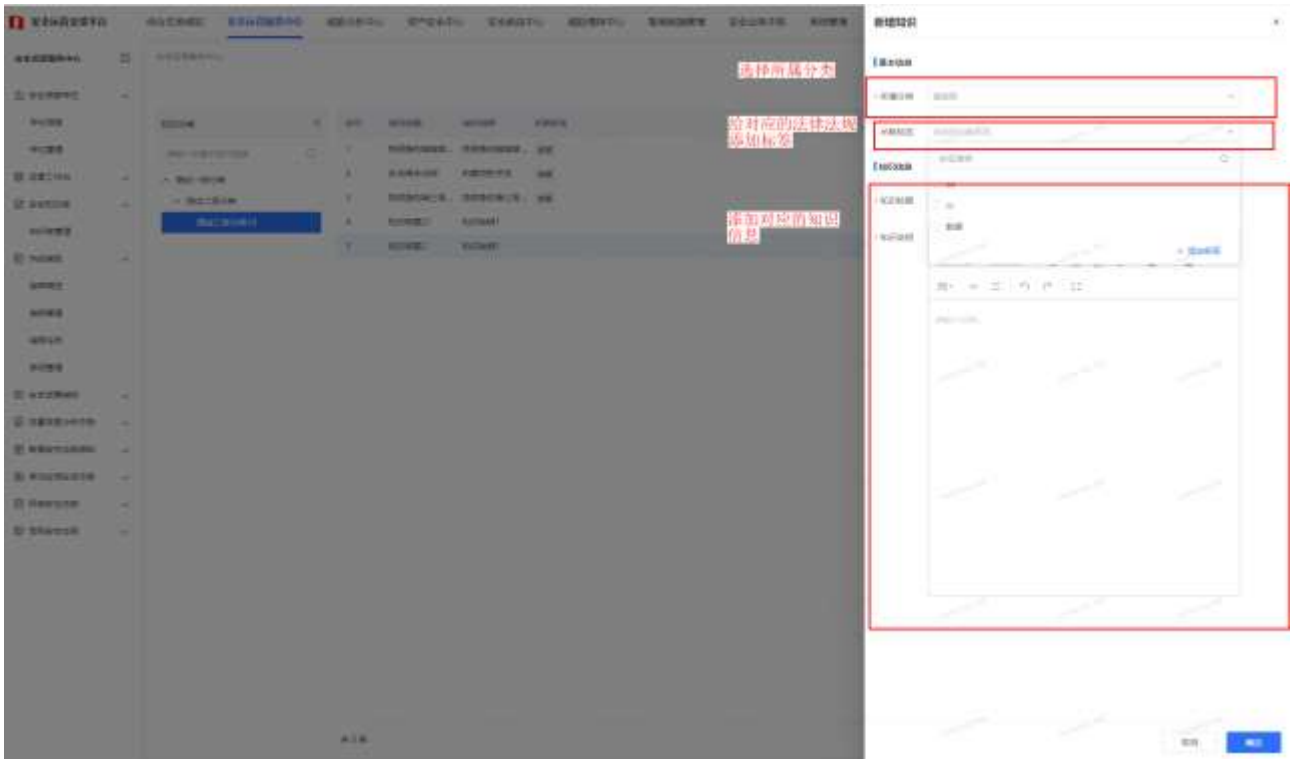
知识分类的新增、修改

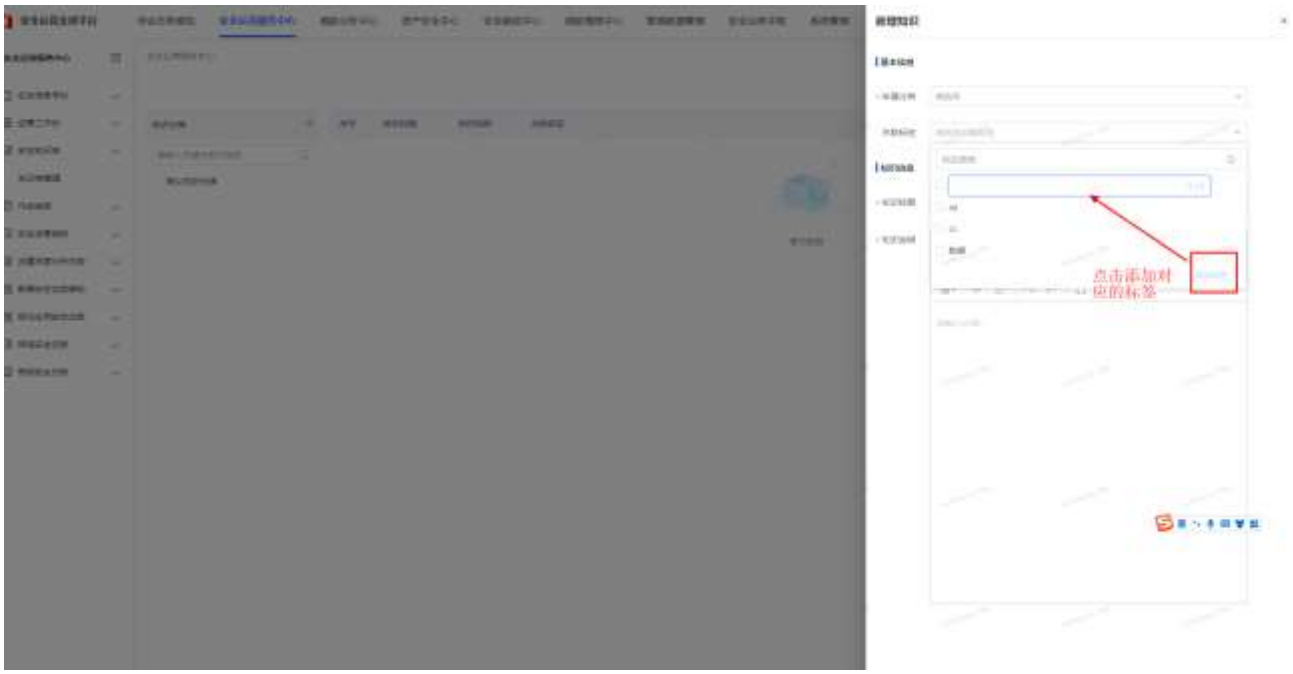


知识内容的维护

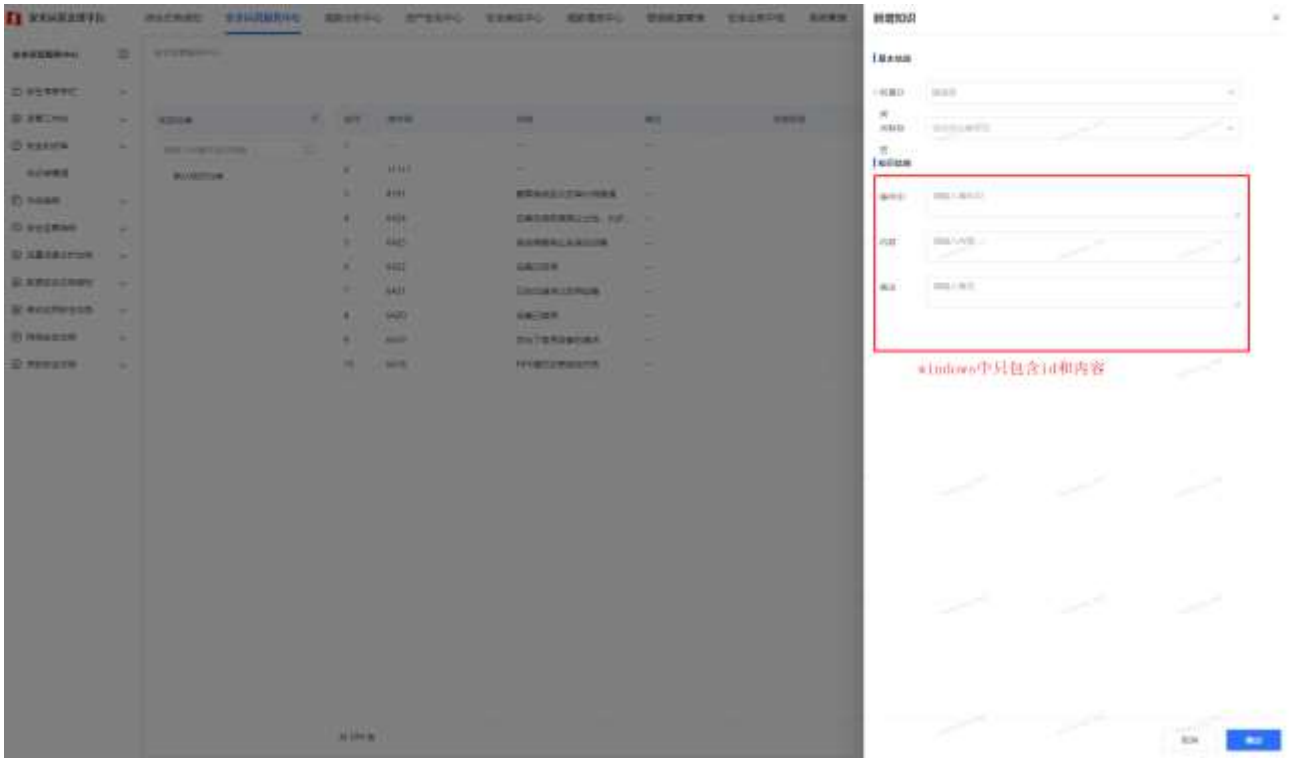
内置知识库 -> 法律法规知识库：网络安全相关的法律法规知识的新增、修改、删除，内置知识不能编辑和删除



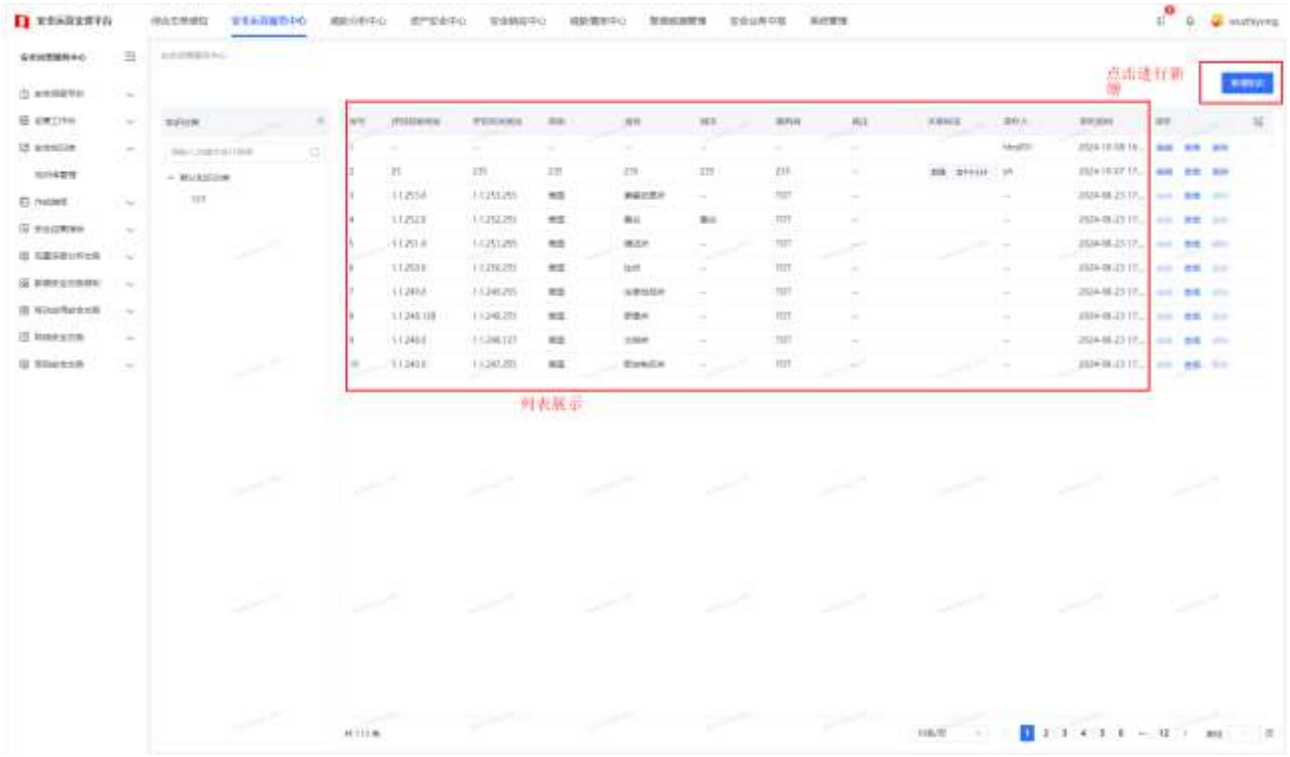


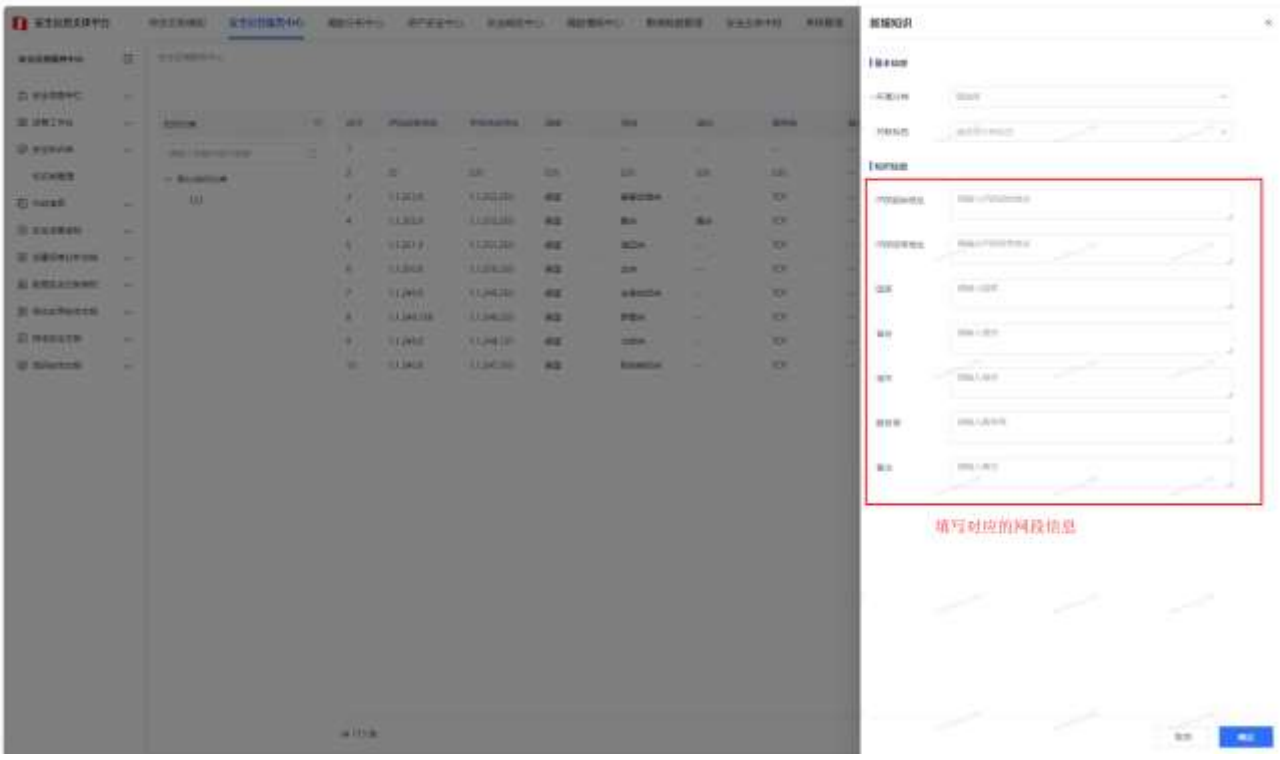


内置知识库 -> windows 安全事件日志知识库 是指 windows 系统中出现的安全日志的类型；存在内置数据，不可修改和删除，同时用户也可以新增知识，也可以对新增的知识进行修改和删除；

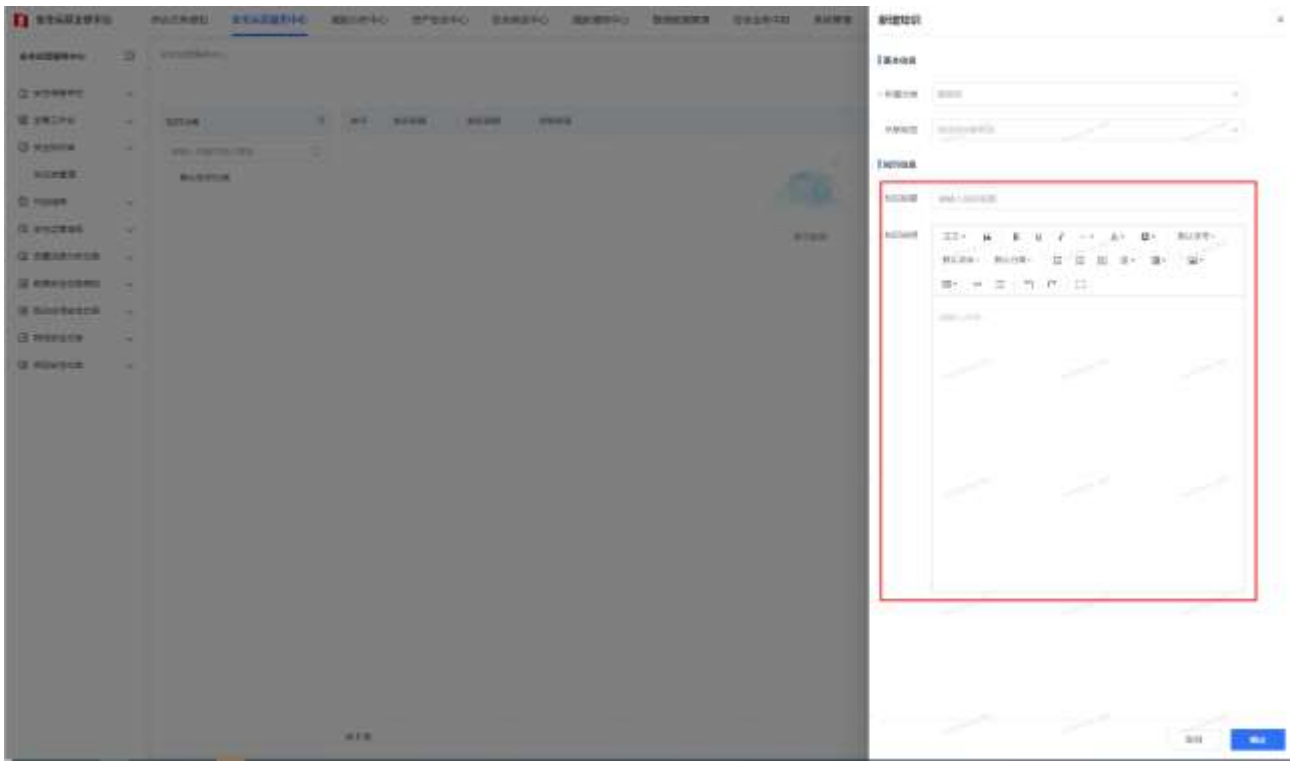


内置数据库 -> GEO-IP 地理库：全球各个地区分配的 ip 网段信息，同样包括内置数据，不能编辑和删除，也可以自己新增；

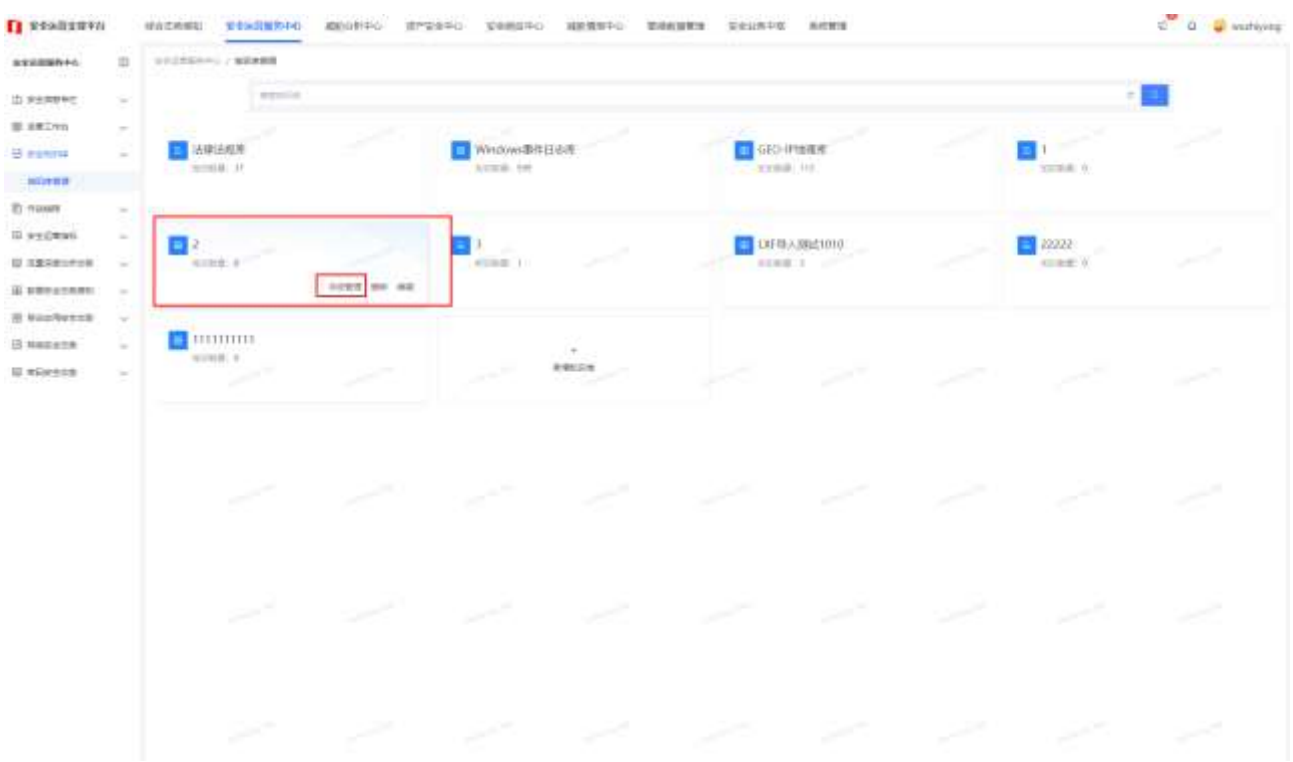




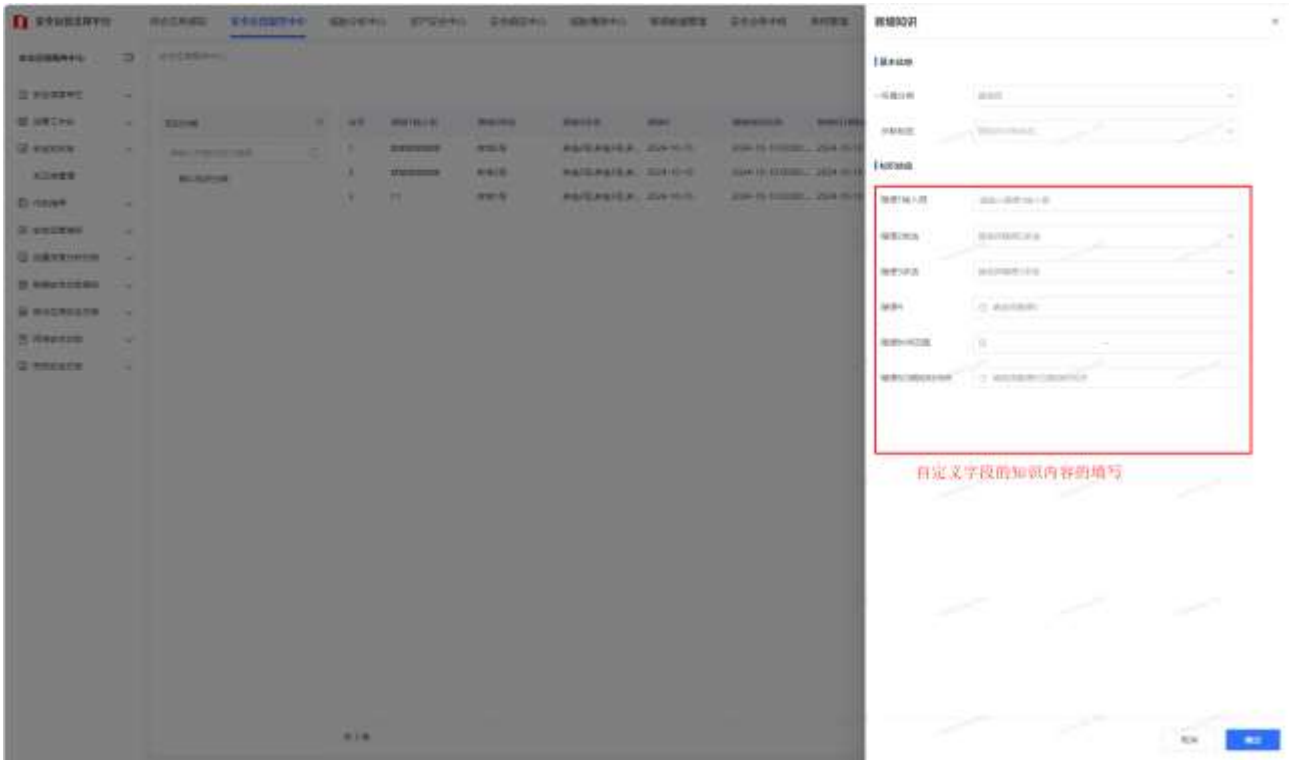
富文本类型知识库：用户自定义富文本类型知识库，和法律法规知识库类似



表结构类型知识库：用户通过设置自定义字段，实现知识库的属性配置，然后根据自定义字段填写相关内容

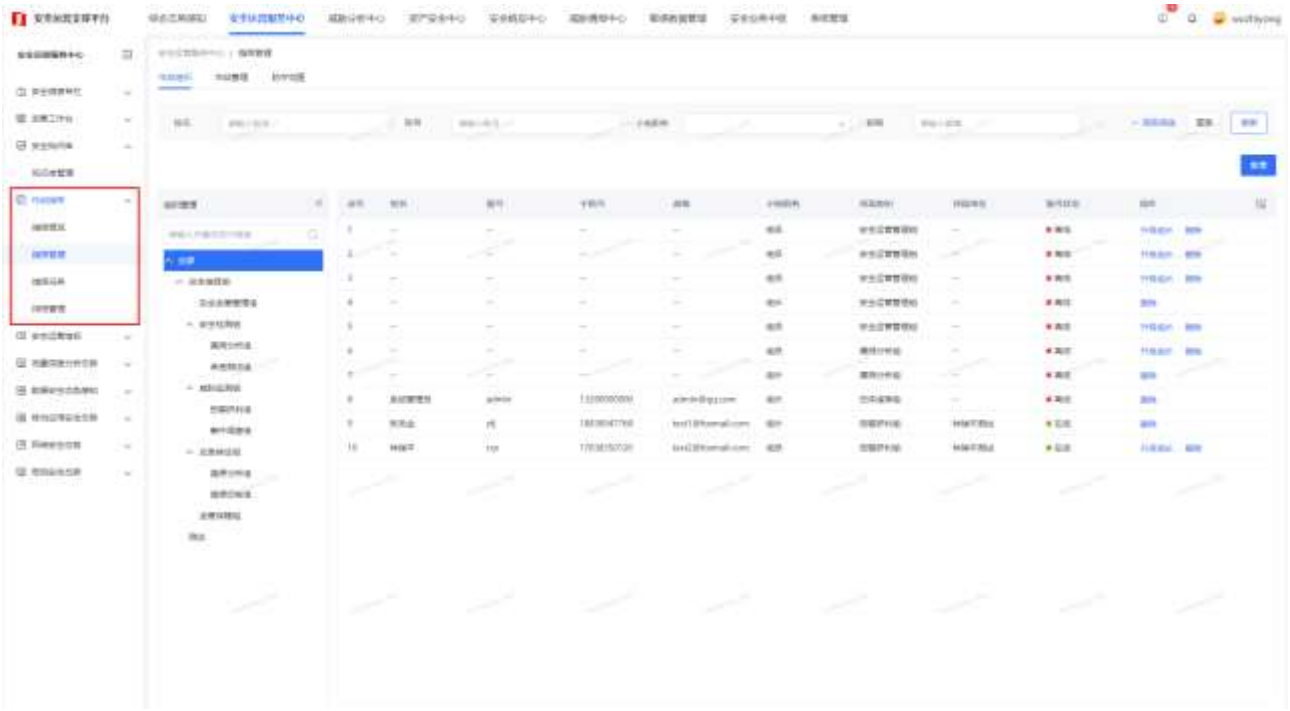



自定义字段动态展示
点击进行新增操作
点击进行编辑，删除，查看操作


自定义字段的知识内容的填写

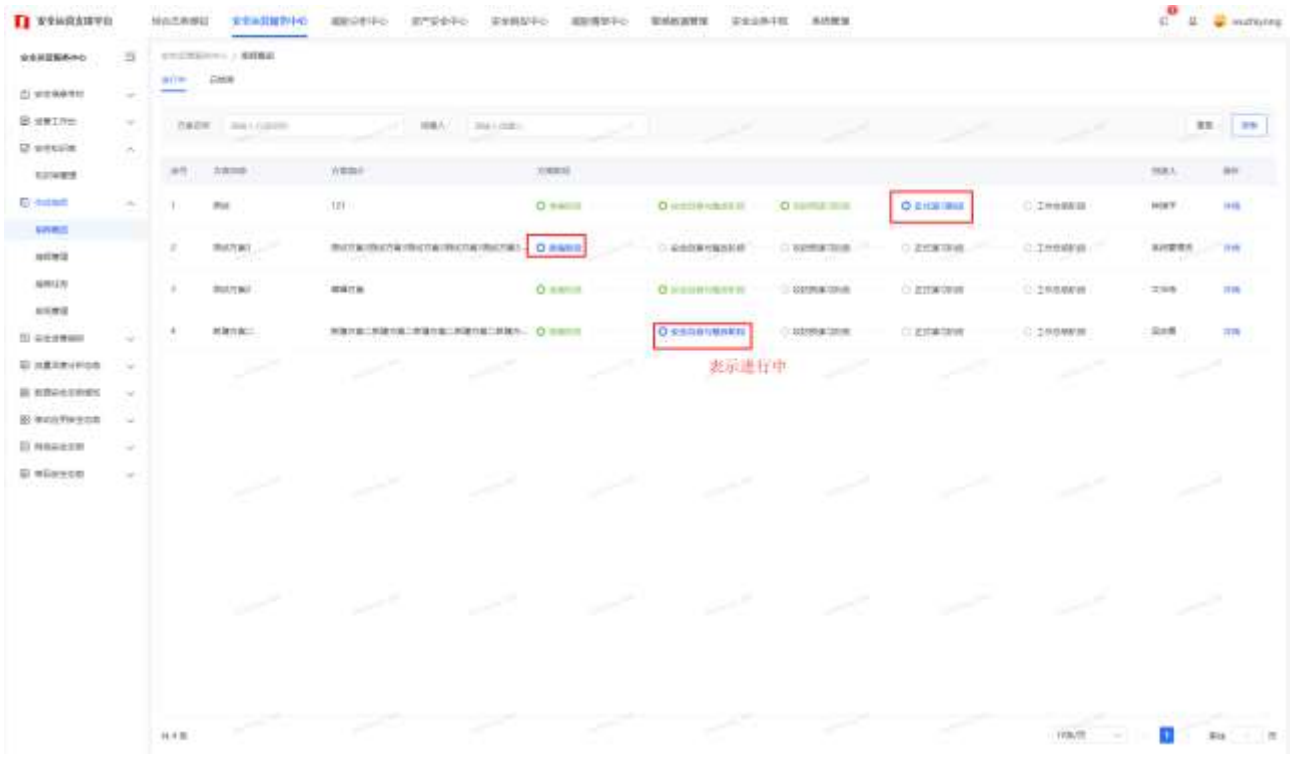
3.3.4 作战指挥

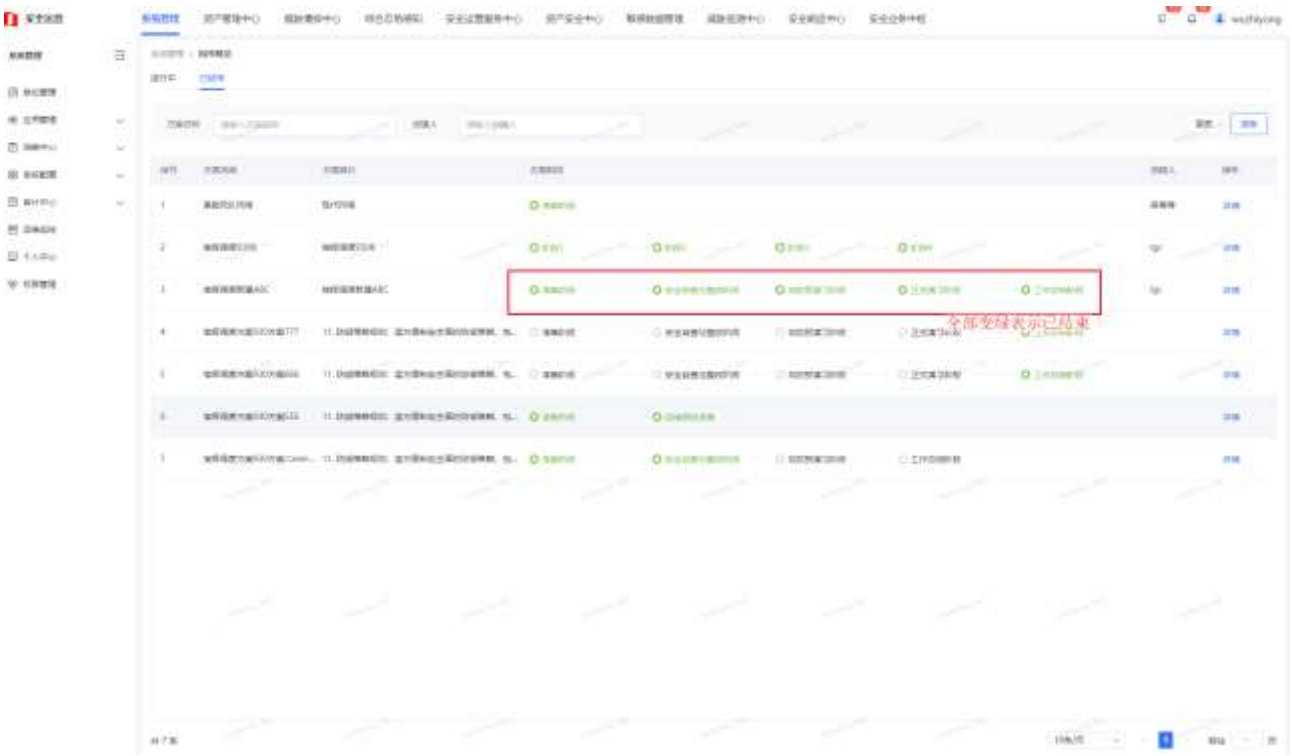
【功能说明】通过指挥管理进行指挥调度的实现，通过指挥任务实现分配调度工作任务的材料收集，指挥概览实现指挥调度整体信息的展示；



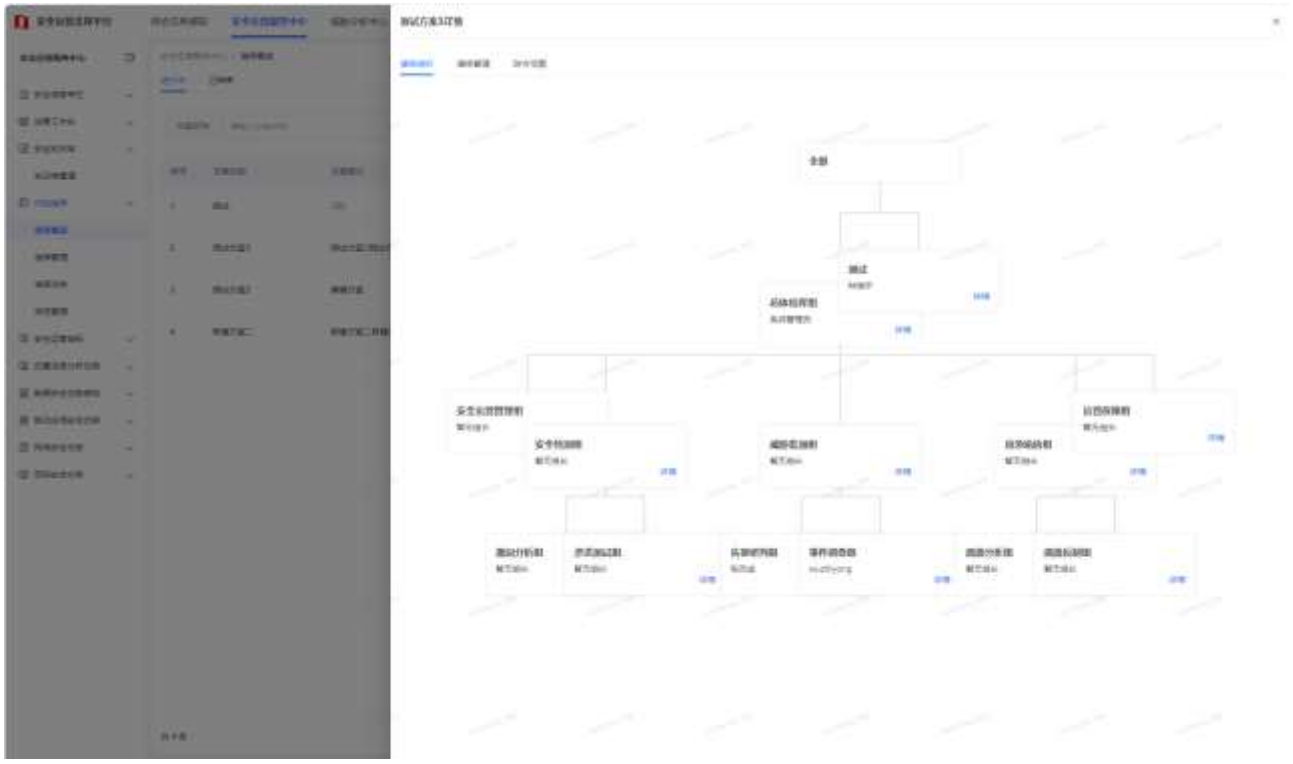
3.3.4.1 指挥概览

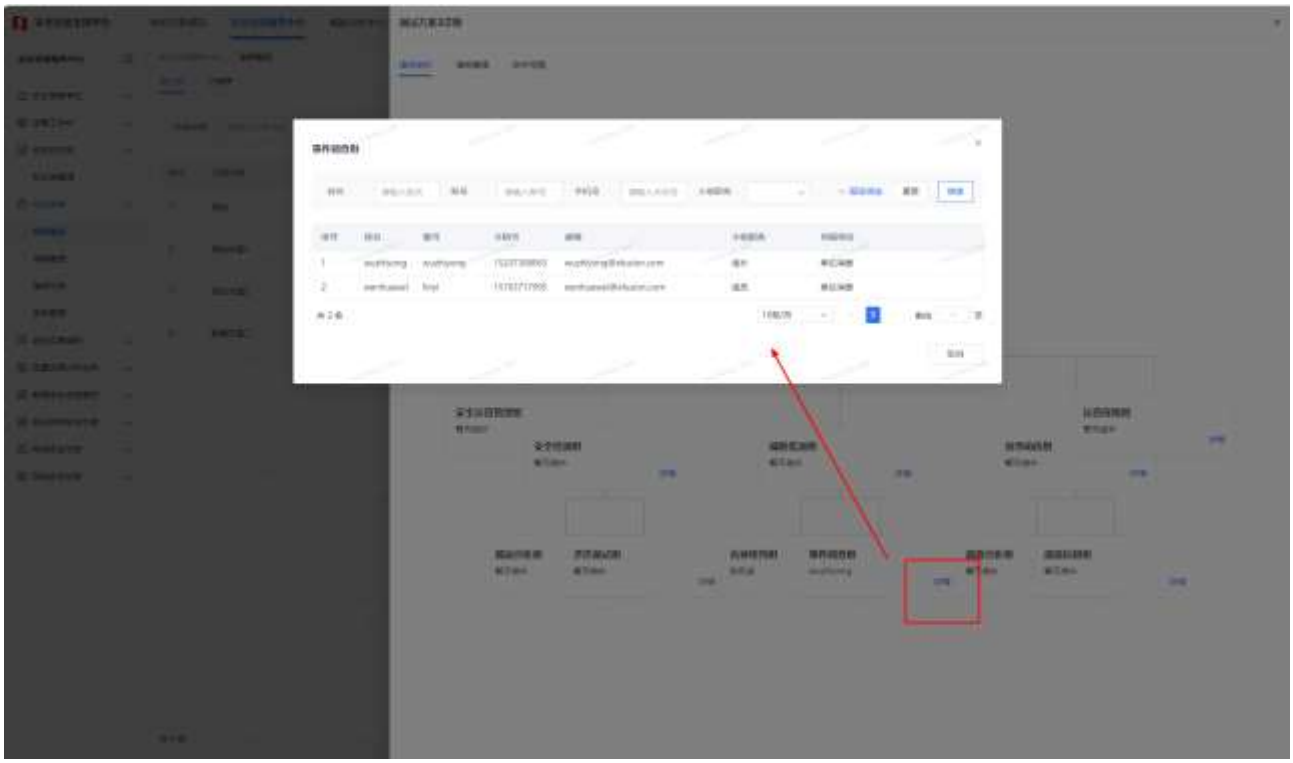
【功能说明】点击【指挥调度】-【指挥概览】进入概览列表页，实现指挥调度信息的全量展示，为整体指挥调度提供支撑；列表页将所有方案分为进行中和已结束；当前时间处于该方案的整体的时间段内或之前，就为进行中，当前时间晚于方案的最后阶段的结束时间，就为已结束；



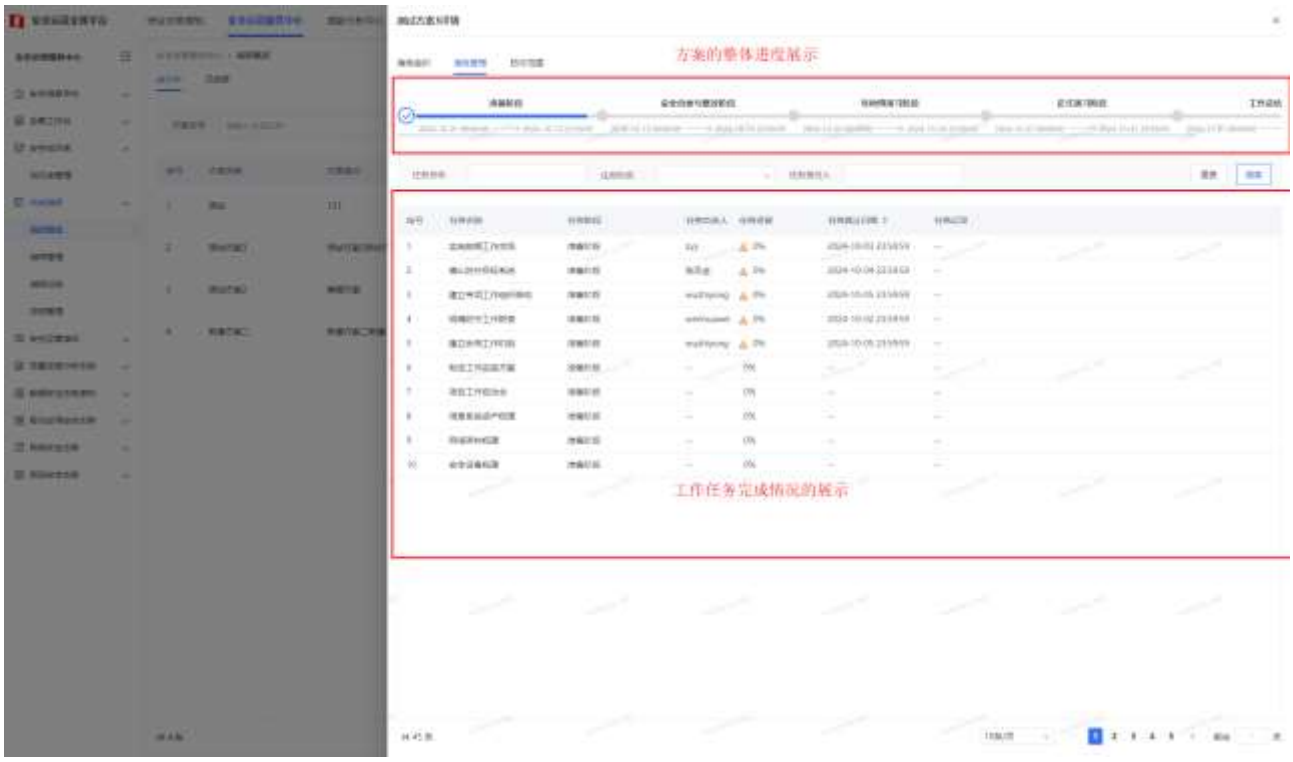


演练组织概览：【指挥概览】列表页点击操作列详情按钮。进入详情页面，第一个展示演练组织，展示的是所有参与演练的小组用户；点击详情进入小组成员列表页

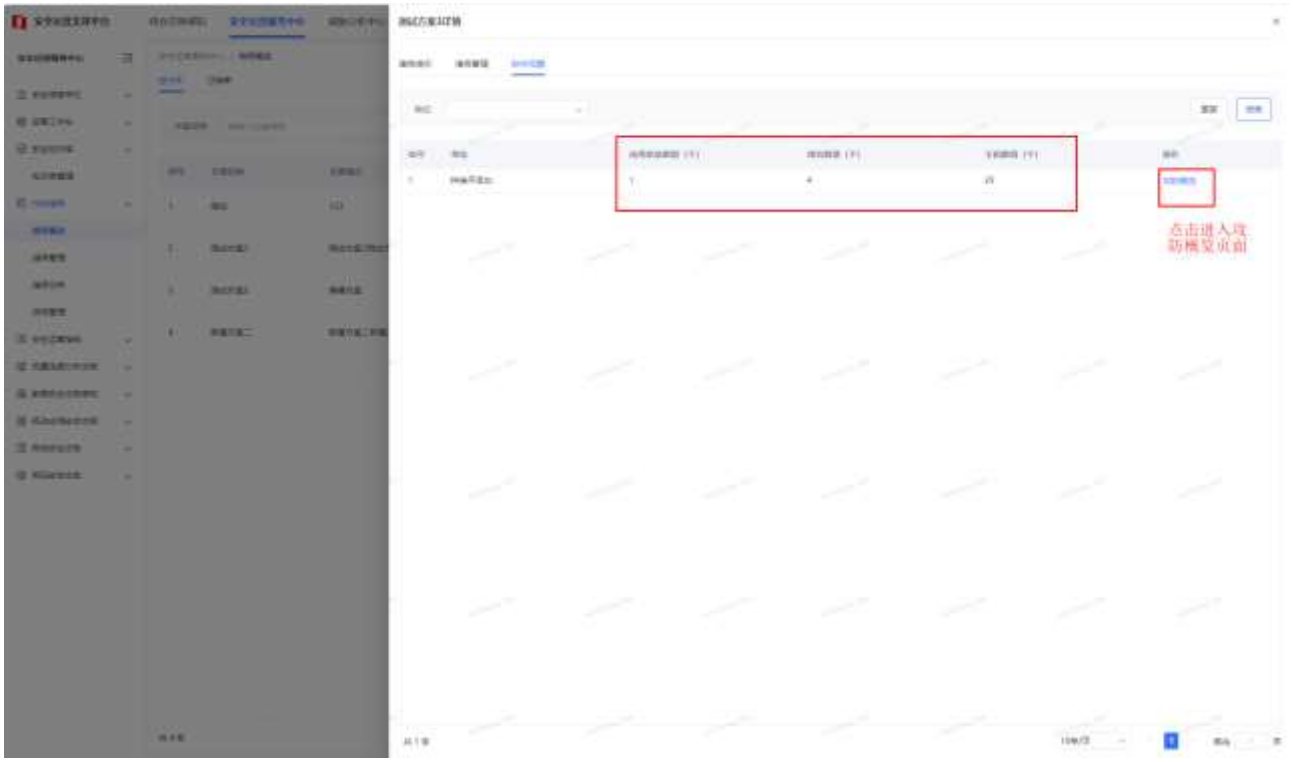


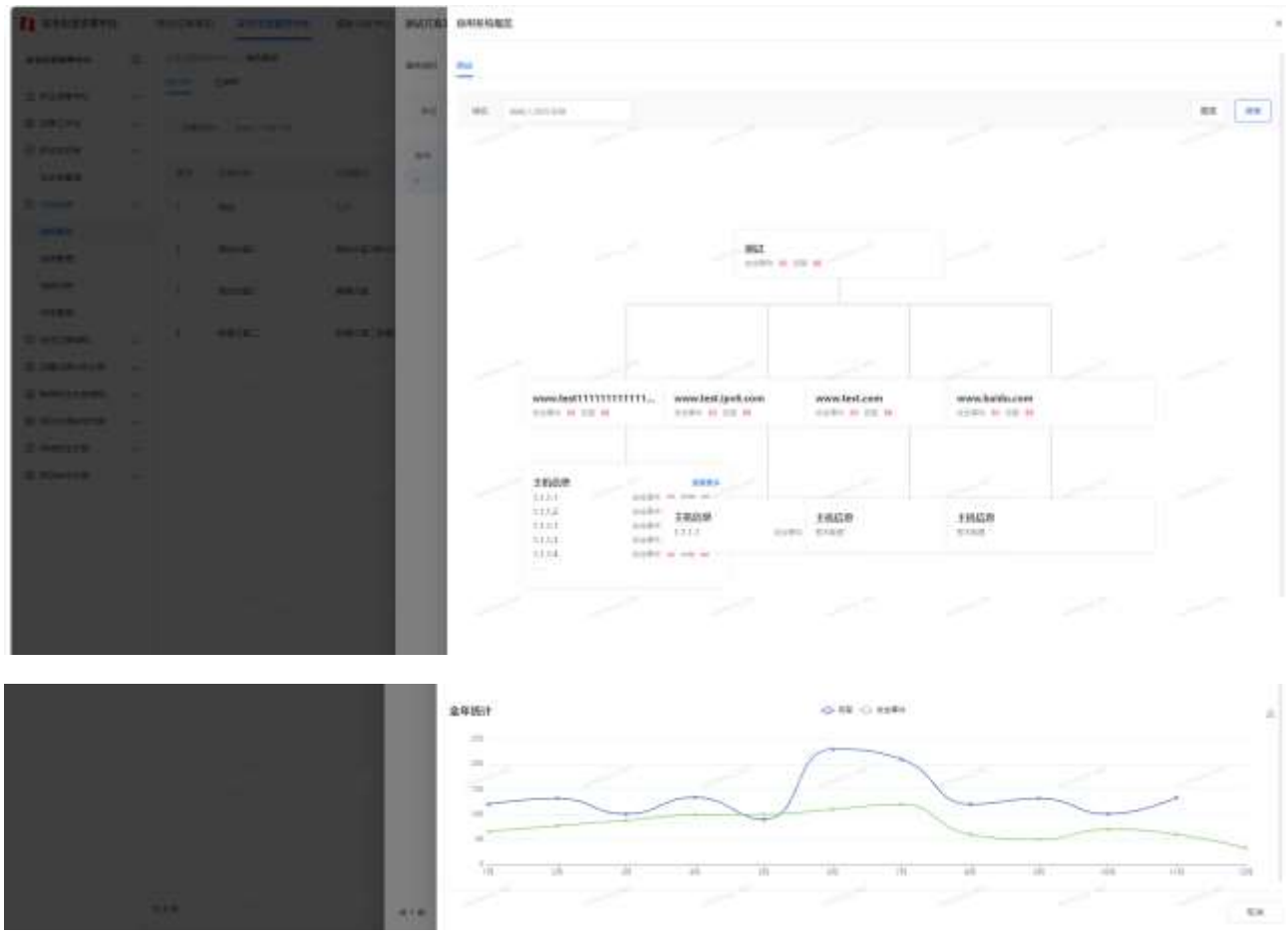


演练管理概览:【指挥概览】详情页，切换 tab 页，进入演练管理的展示，包括方案的阶段进度展示，以及工作任务的完成情况展示



防守范围概览:【指挥概览】详情页，切换 tab 页，进入防守范围展示，主要包括该方案的所有防护单位的应用系统的数量、相关域名数量以及主机个数等，点击操作列攻防概览可以预览防护范围整体的树状图





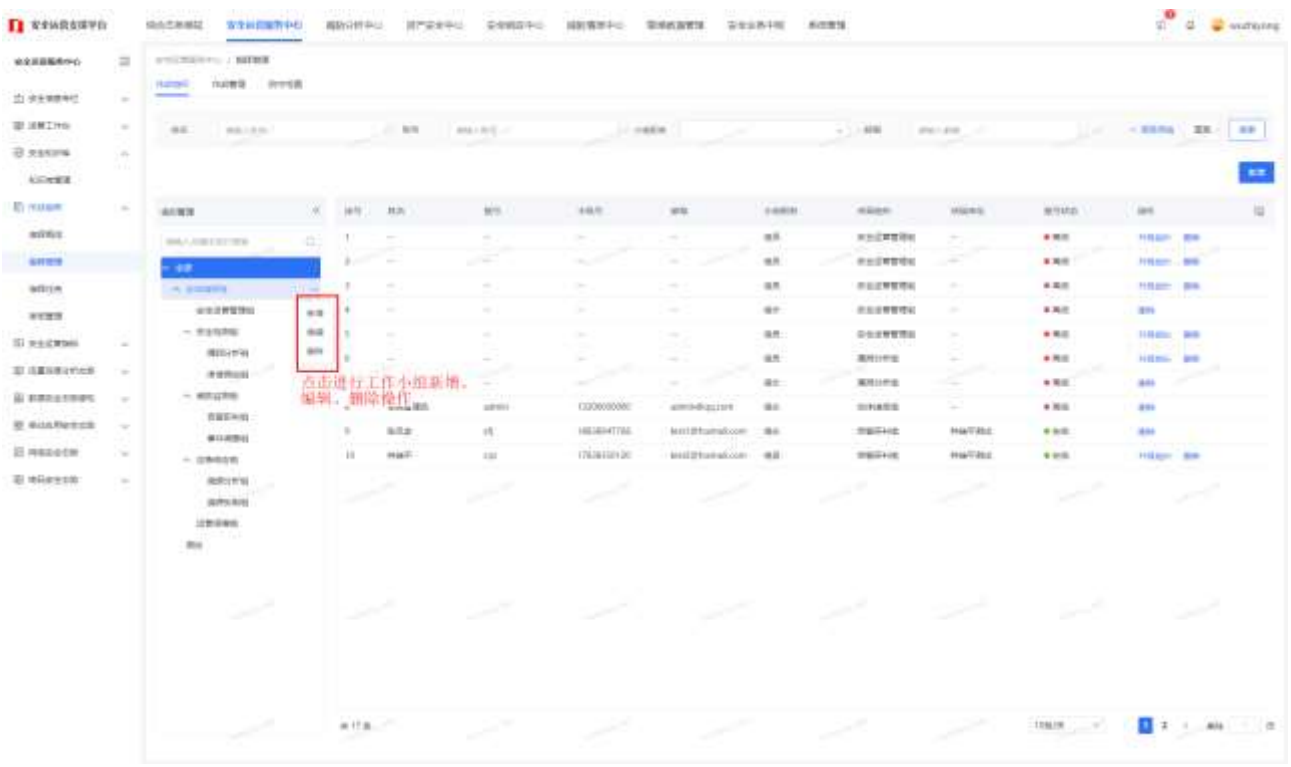
3.3.4.2 指挥管理

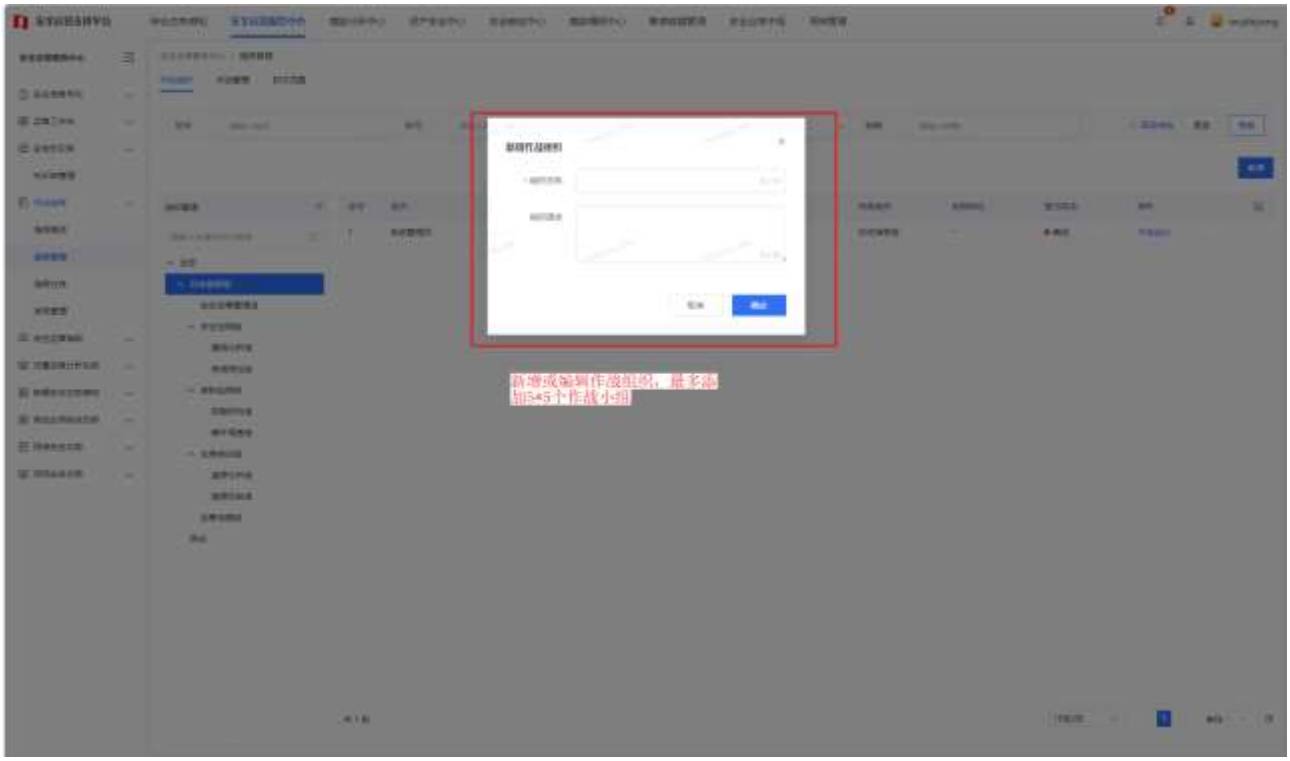
【功能说明】【指挥调度】-> 【指挥管理】进入指挥管理的列表展示页，主要包括作战组织的小组和人员设置，作战管理即方案的制定，防守范围的设置即设置所有单位的应用系统，以及所有域名和主机；

3.3.4.2.1 作战组织

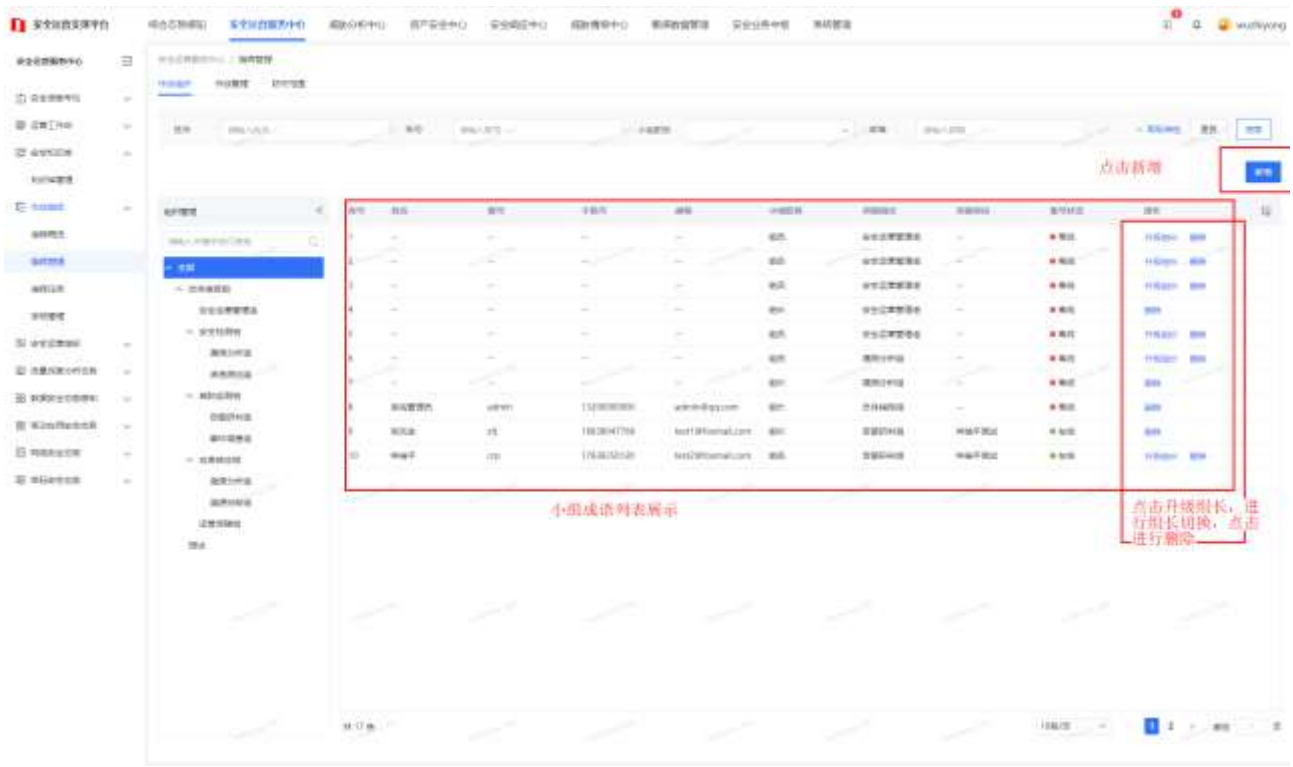
【功能说明】【指挥调度】-> 【指挥管理】-> 【作战组织】（tab 页）主要包括作战组织的工作小组和工作人员的设置；实现工作小组和工作人员的增加、修改、和删除；

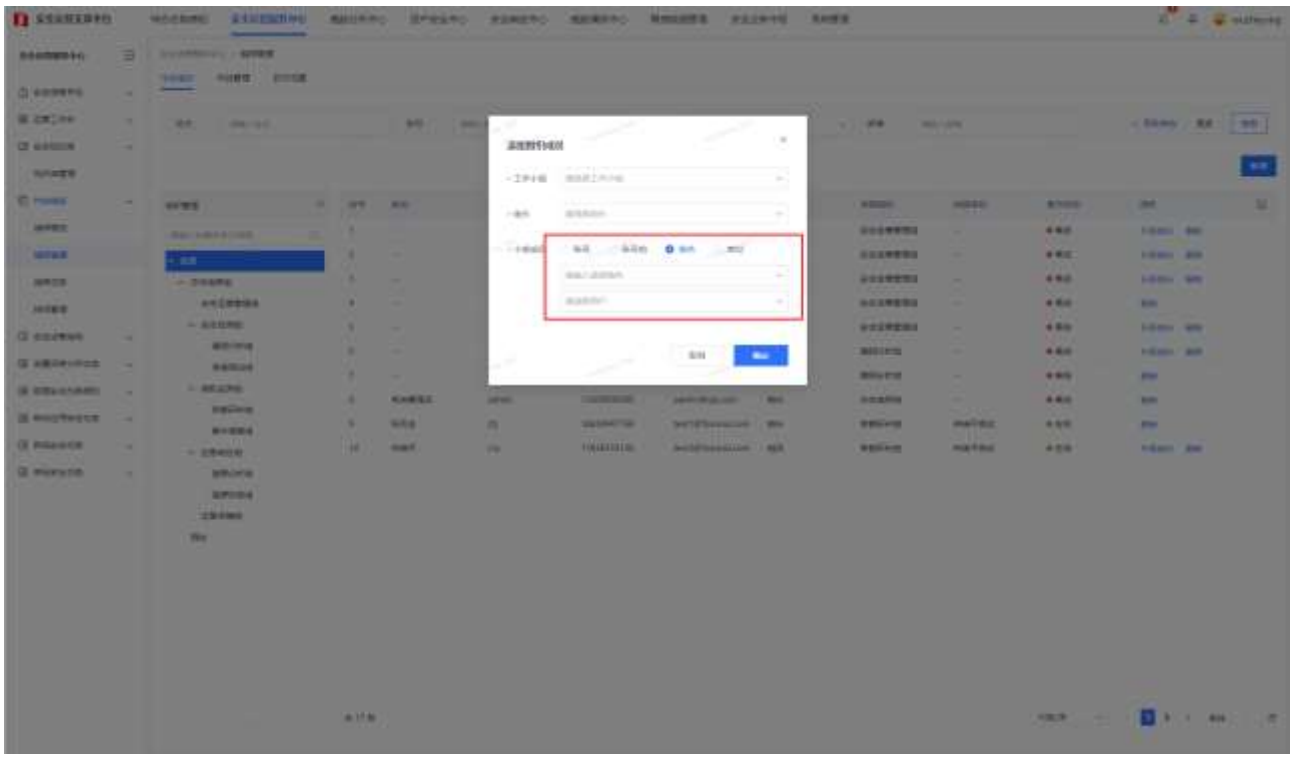
工作小组的设置：





小组成员设置，在新增时作战组织选择，组长设置，以及根据 账号、用户组、角色、单位等类型，进行人员的选择；

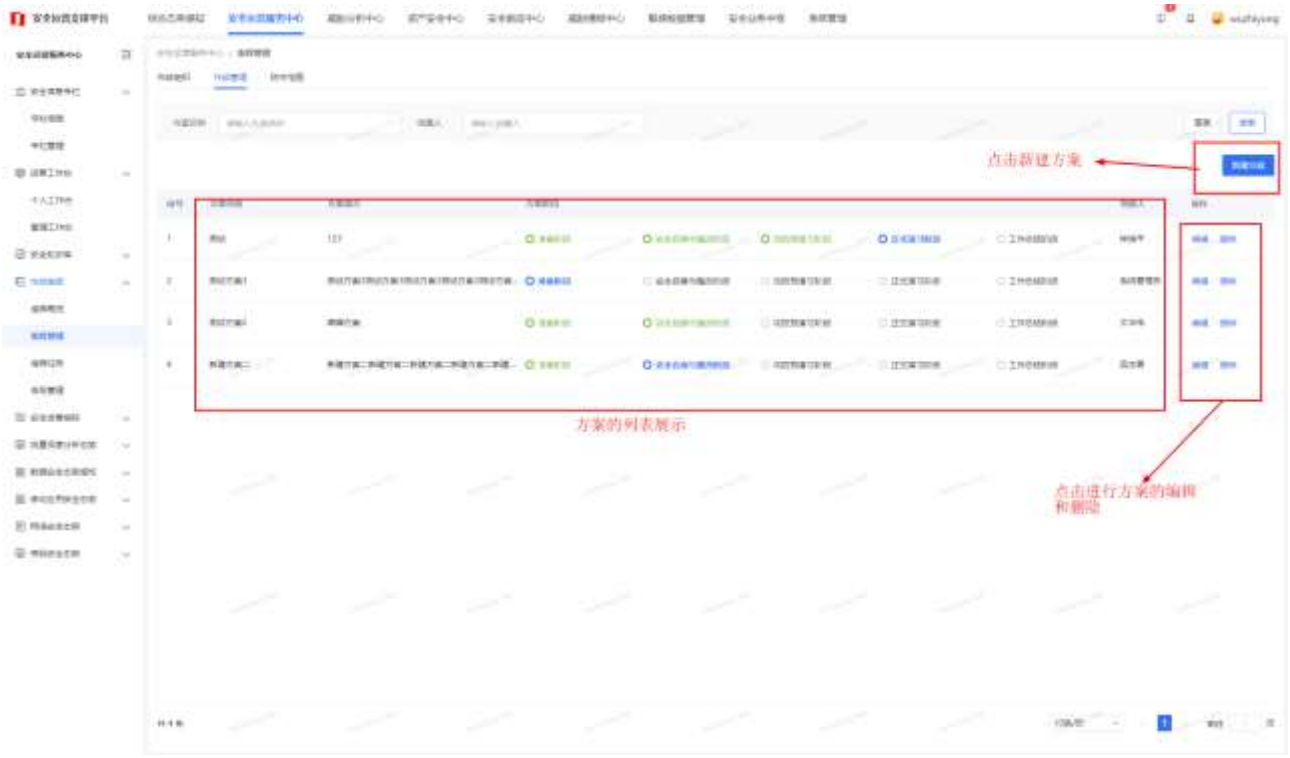




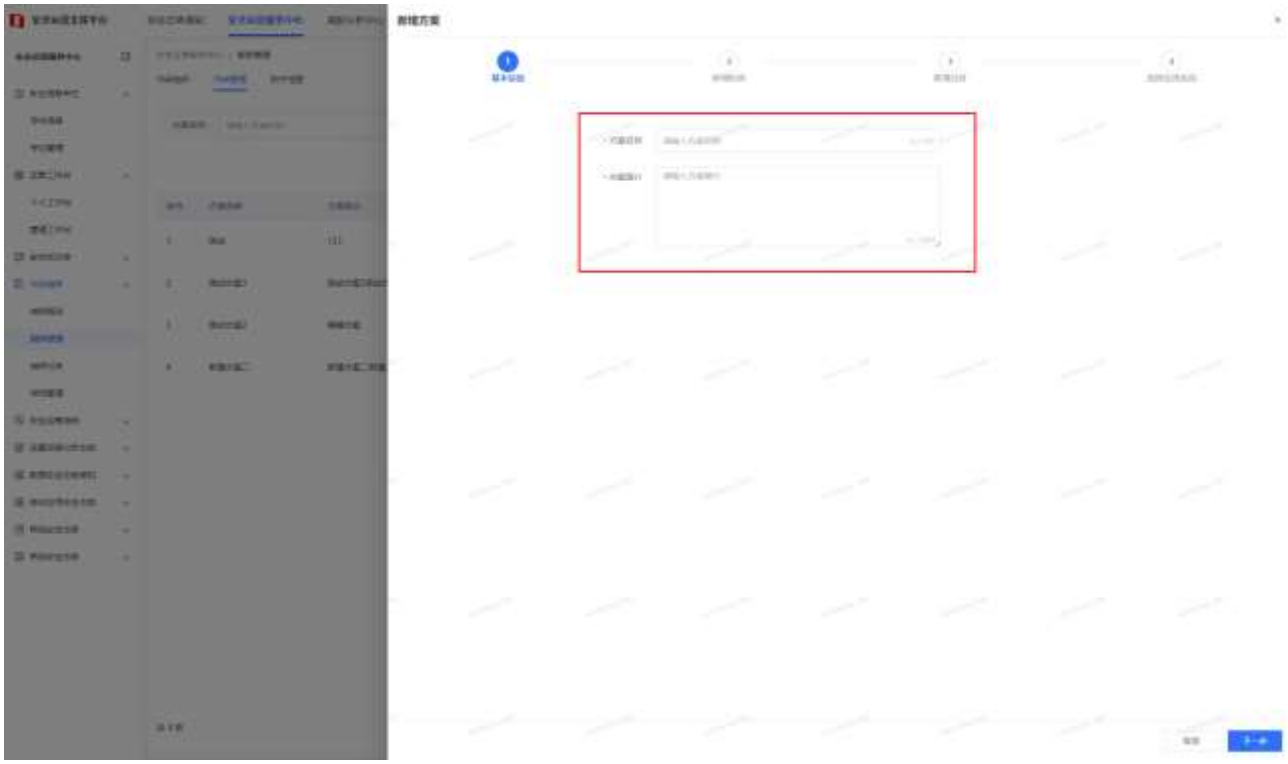
3.3.4.2.2 作战管理

【功能说明】【指挥调度】-> 【指挥管理】-> 【作战管理】（tab 页）主要功

能为整个方案的制定，包括方案的基本信息，方案的工作阶段，以及每个阶段的任务管理，选择对应防护范围；

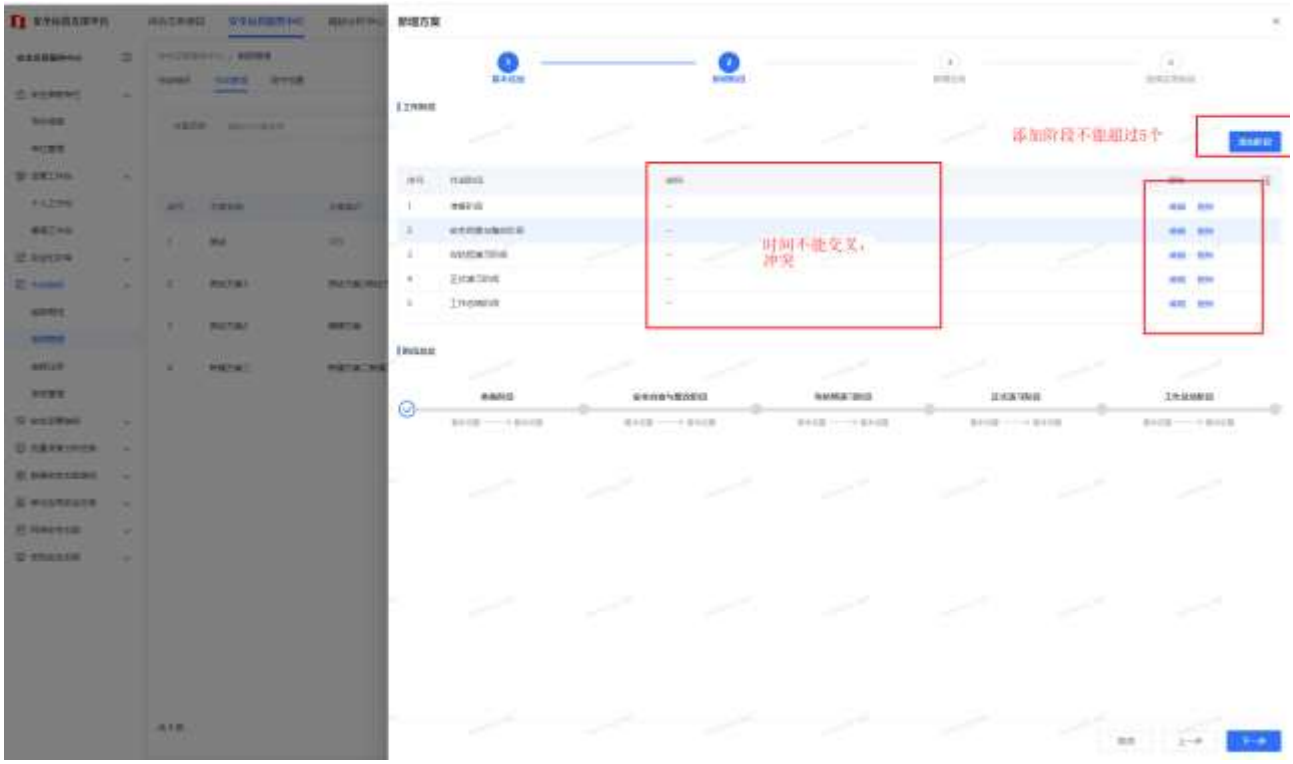


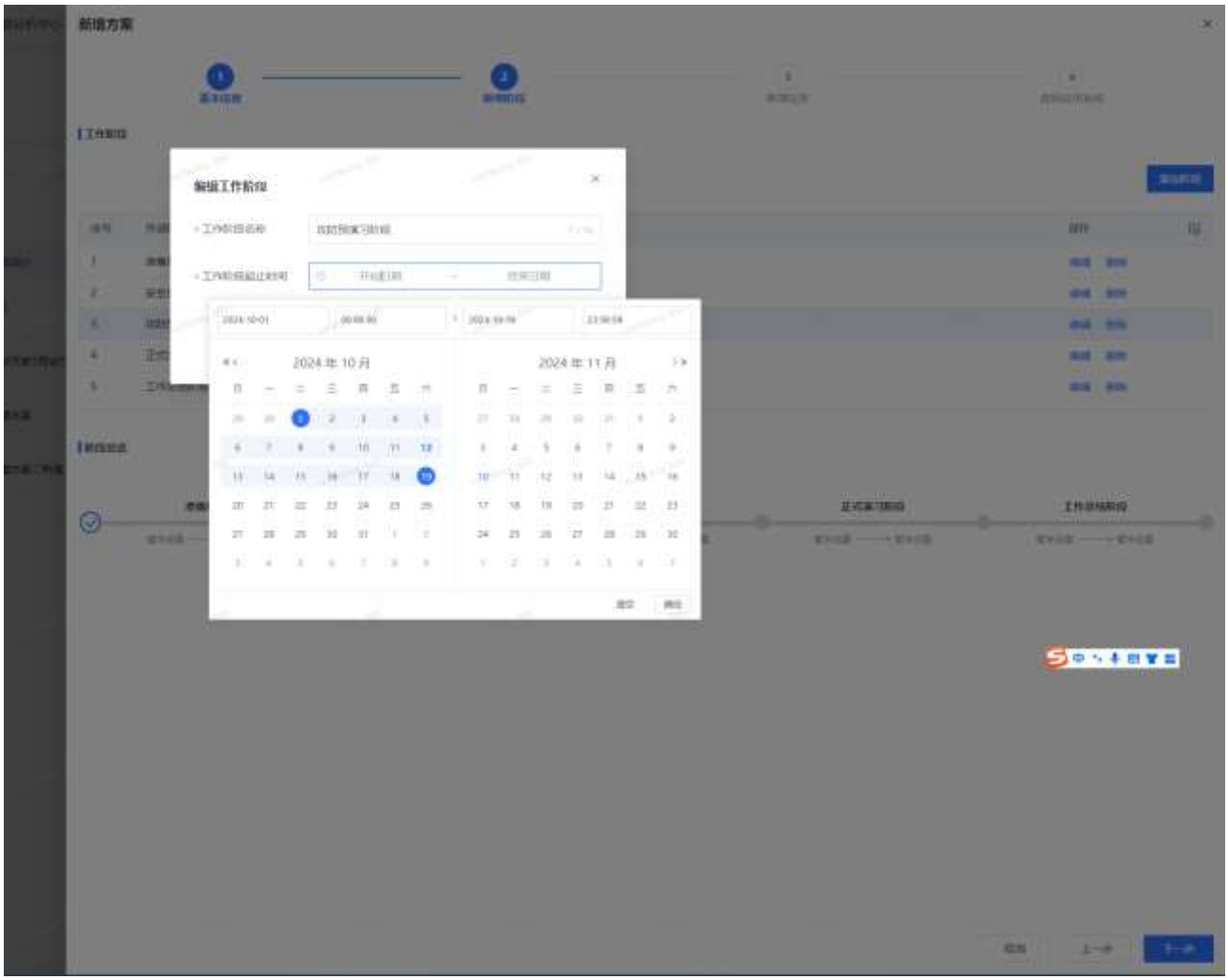
方案的基本信息：点击下一步进行了方案基本信息的保存



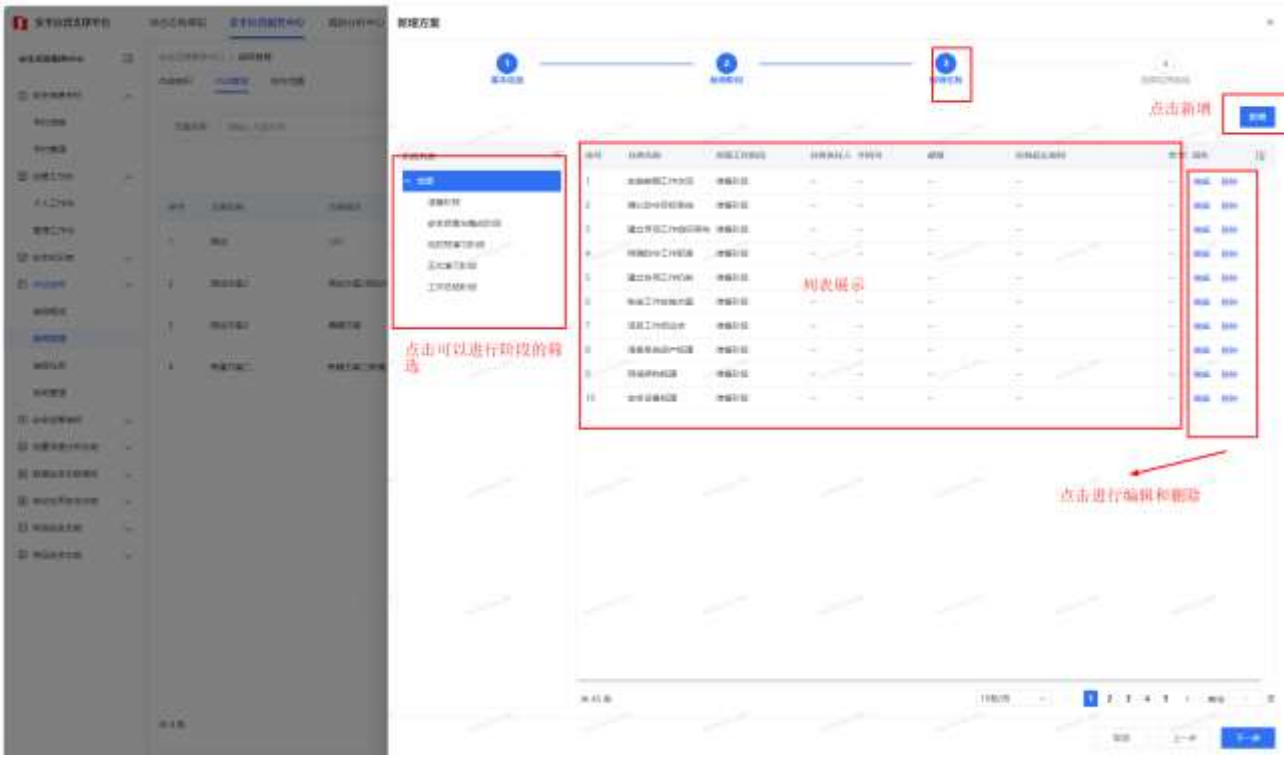
方案的工作阶段维护：创建方案基本信息时，将对应的工作阶段进行了初始

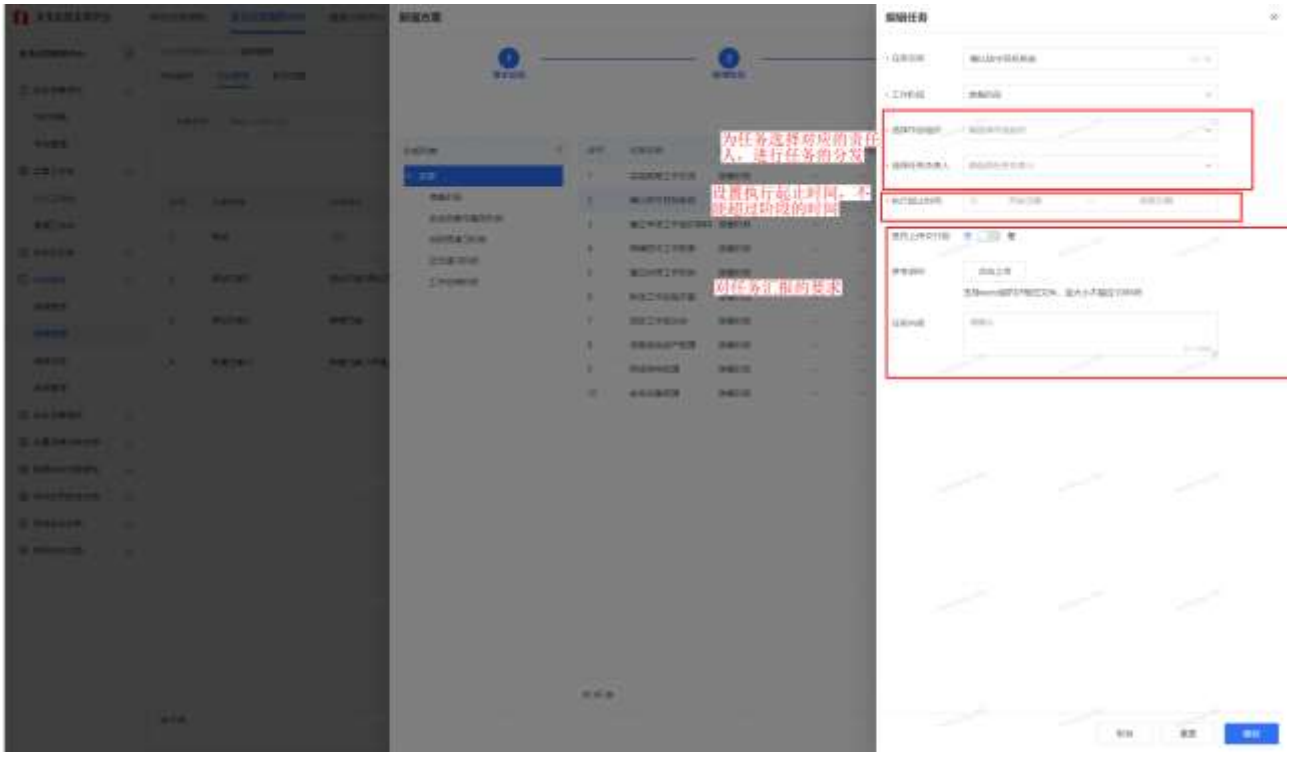
化，用户可以对初始化的数据进行修改和删除，阶段最多不能超过 5 个，各个阶段时间不能交叉和冲突，各个阶段的时间为必填项，所有时间填完才能进行下一步；



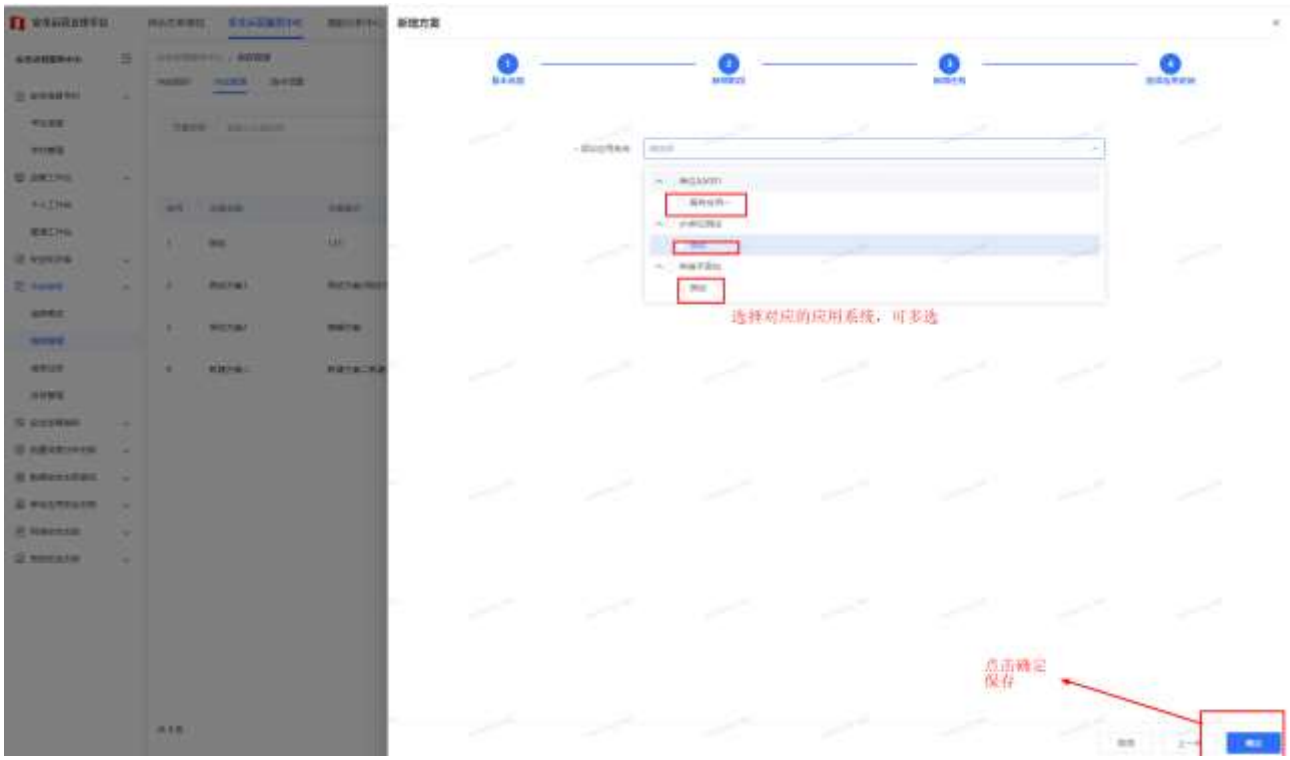


方案的工作任务：创建方案基本信息时同步将内置的工作任务初始化了一份放入本方案中，用户可以针对这些任务进行修改和删除，同时能够添加新的任务，完善任务时，各阶段的任务时间不能超出每个阶段的时间区间；





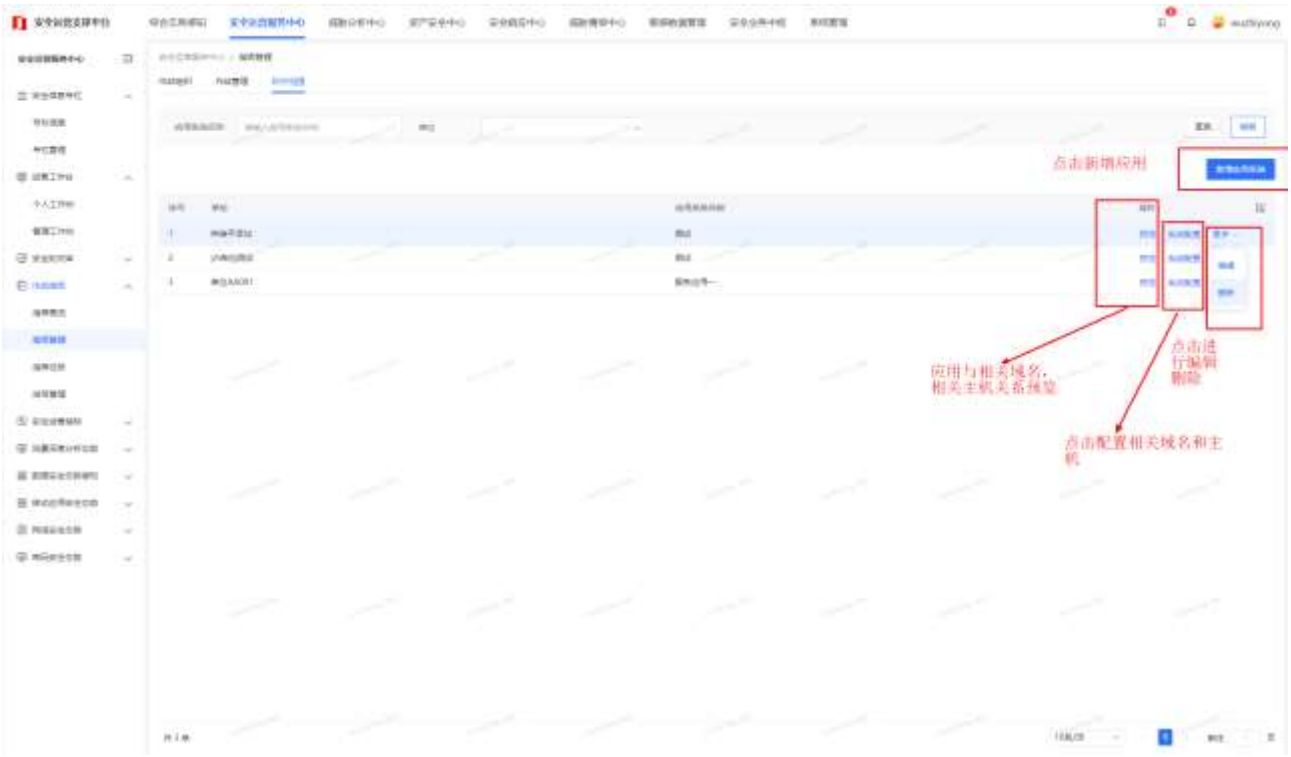
选择应用系统：根据防守范围中创建的各个单位的应用进行选择本次方案防守时需要防守的范围；

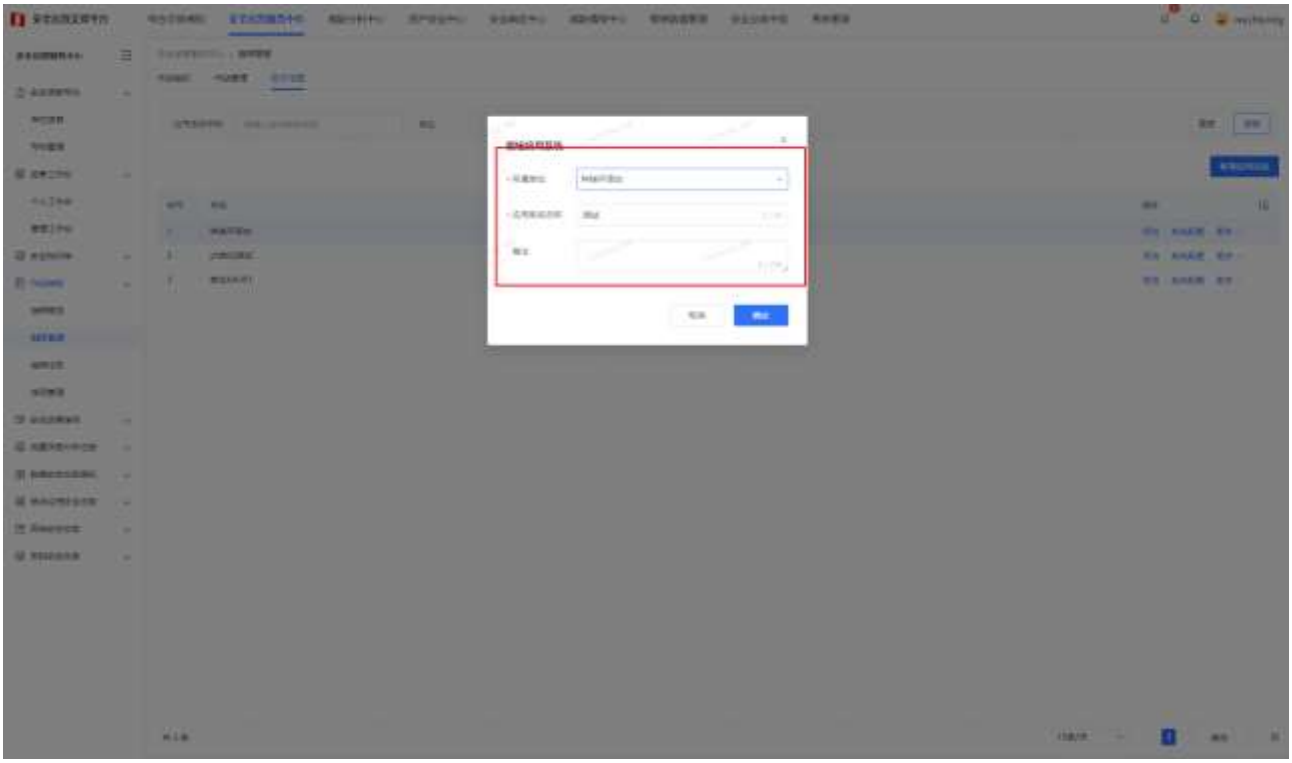


3.3.4.2.3 防守范围

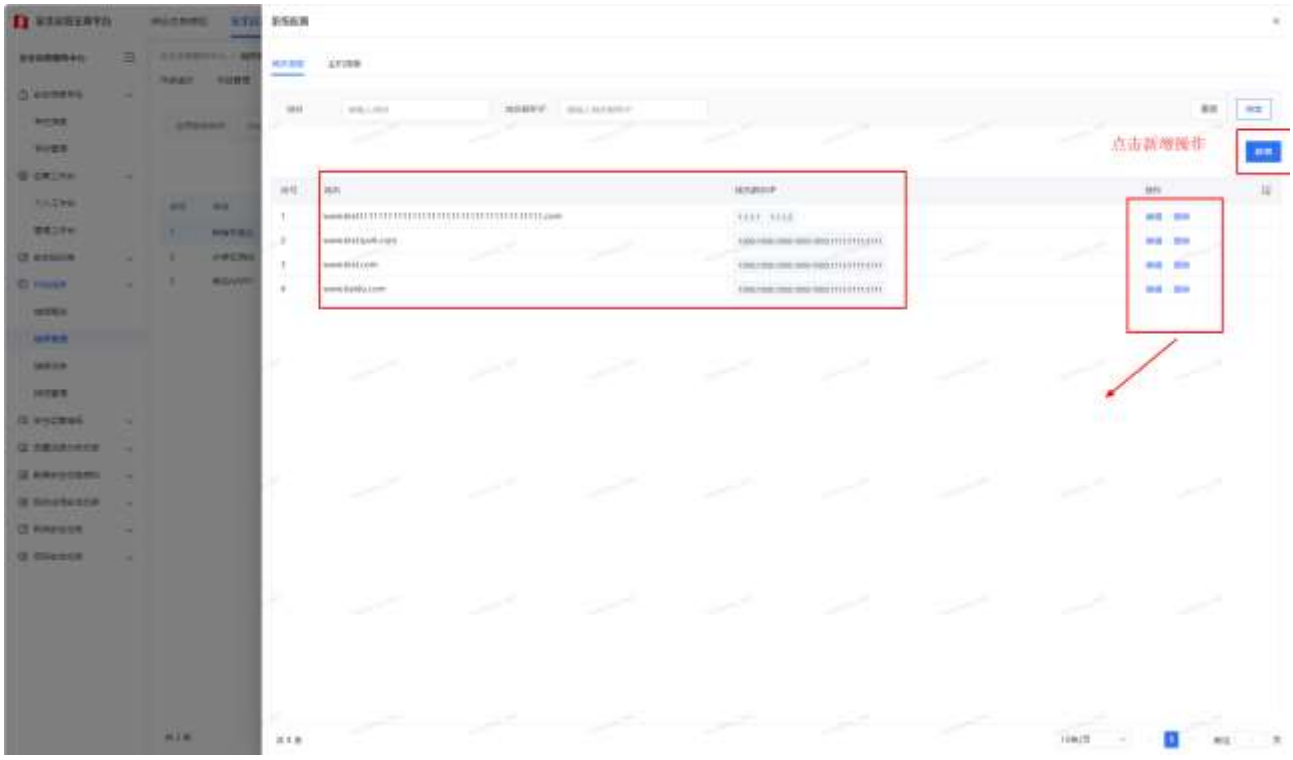
【功能说明】 【指挥调度】-> 【指挥管理】-> 【防守范围】（tab 页）该功能实现了各单位的应用系统的配置，以及对应的相关域名和相关主机的维护，用来确定该单位应用的防守范围

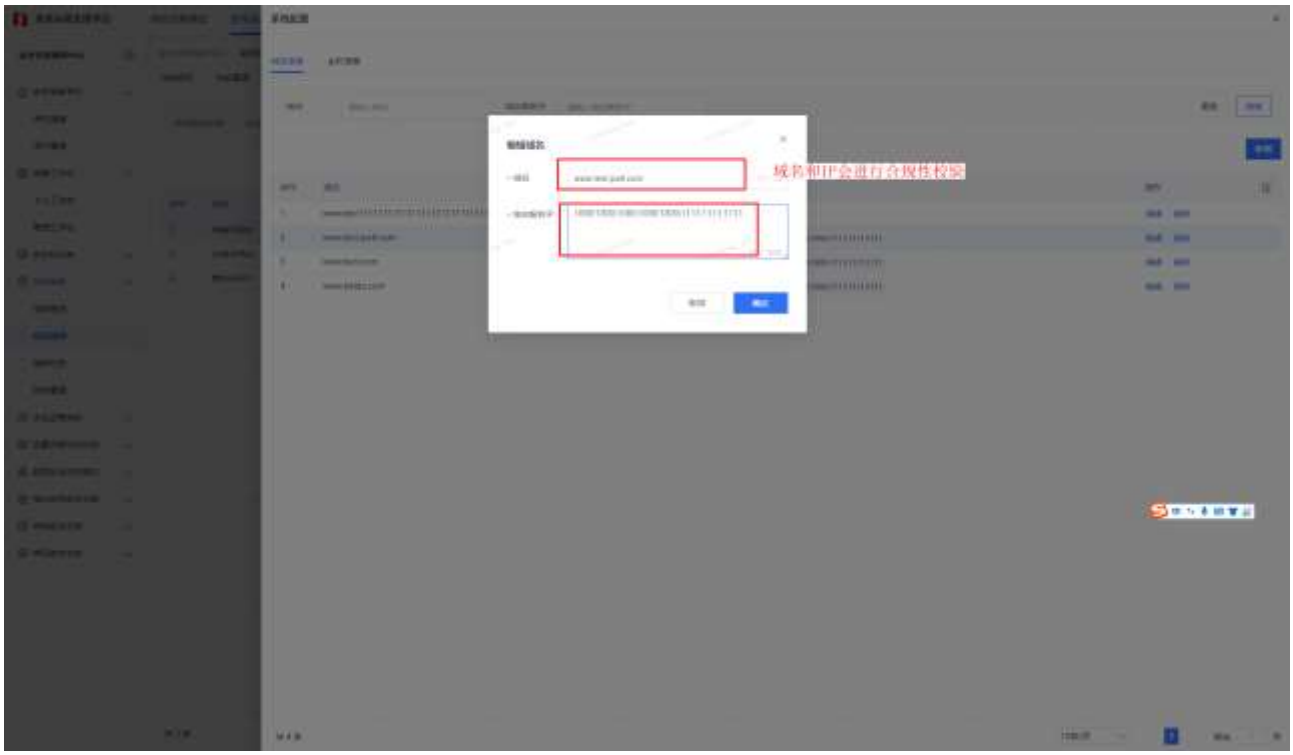
应用系统 ：应用系统的增加、修改、删除；应用系统与相关域名、相关主机关系的预览；系统配置，配置相关域名和主机



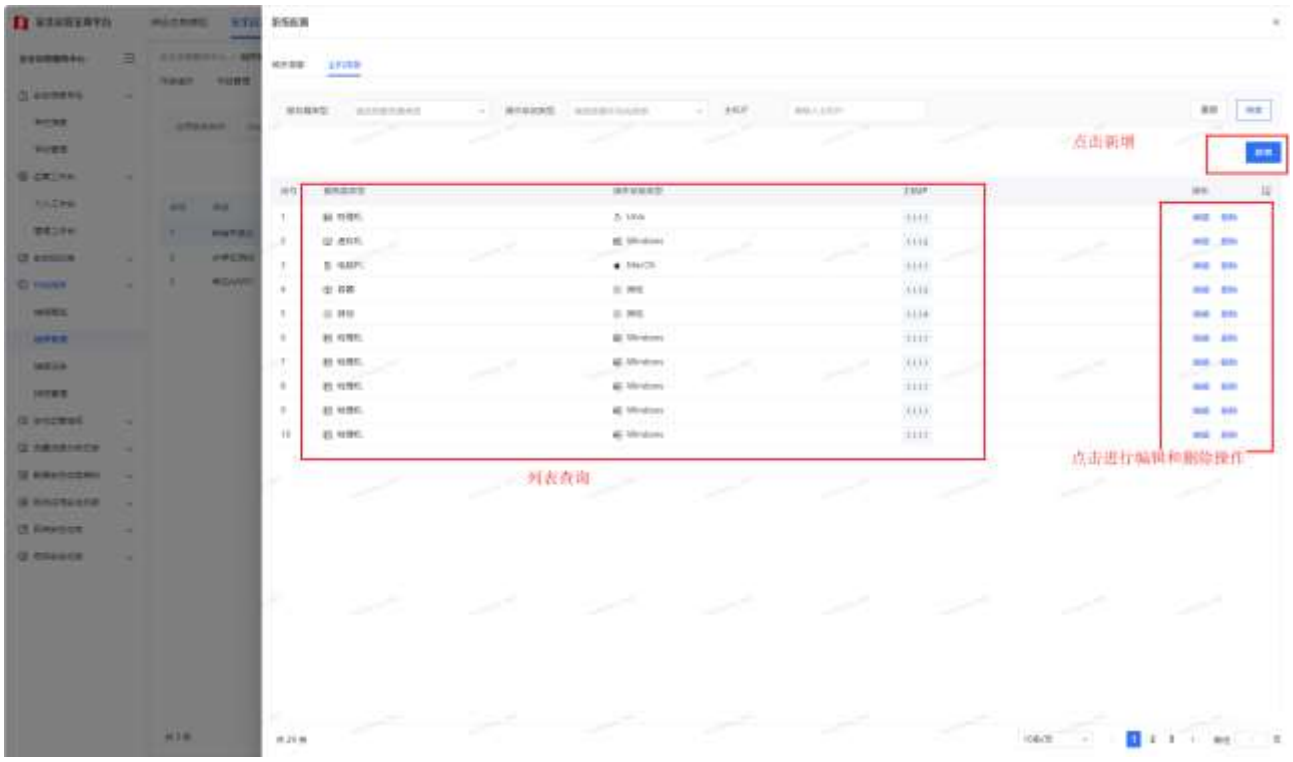


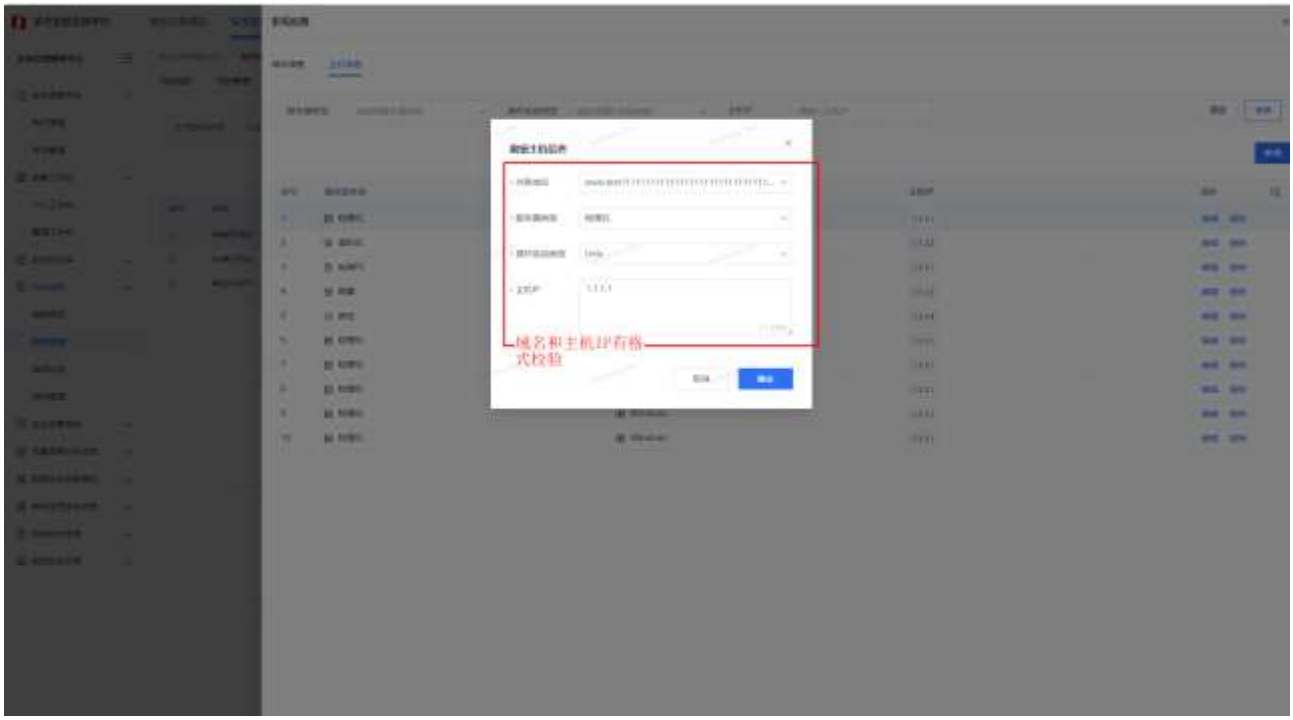
域名信息配置：防守范围 -> 系统配置 -> 域名信息 主要功能为域名信息的增加、修改、删除；





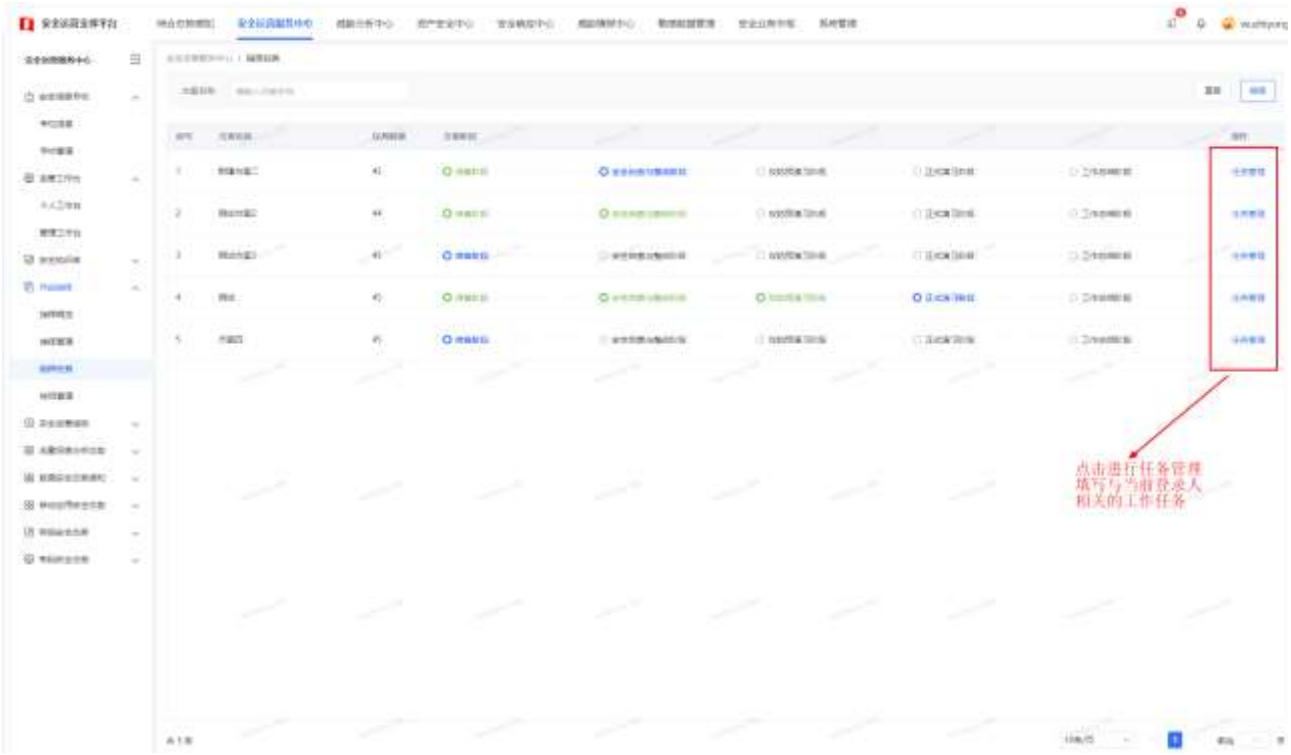
相关主机配置：防守范围 -> 系统配置 -> 相关主机 主要功能为域名信息的增加、修改、删除；

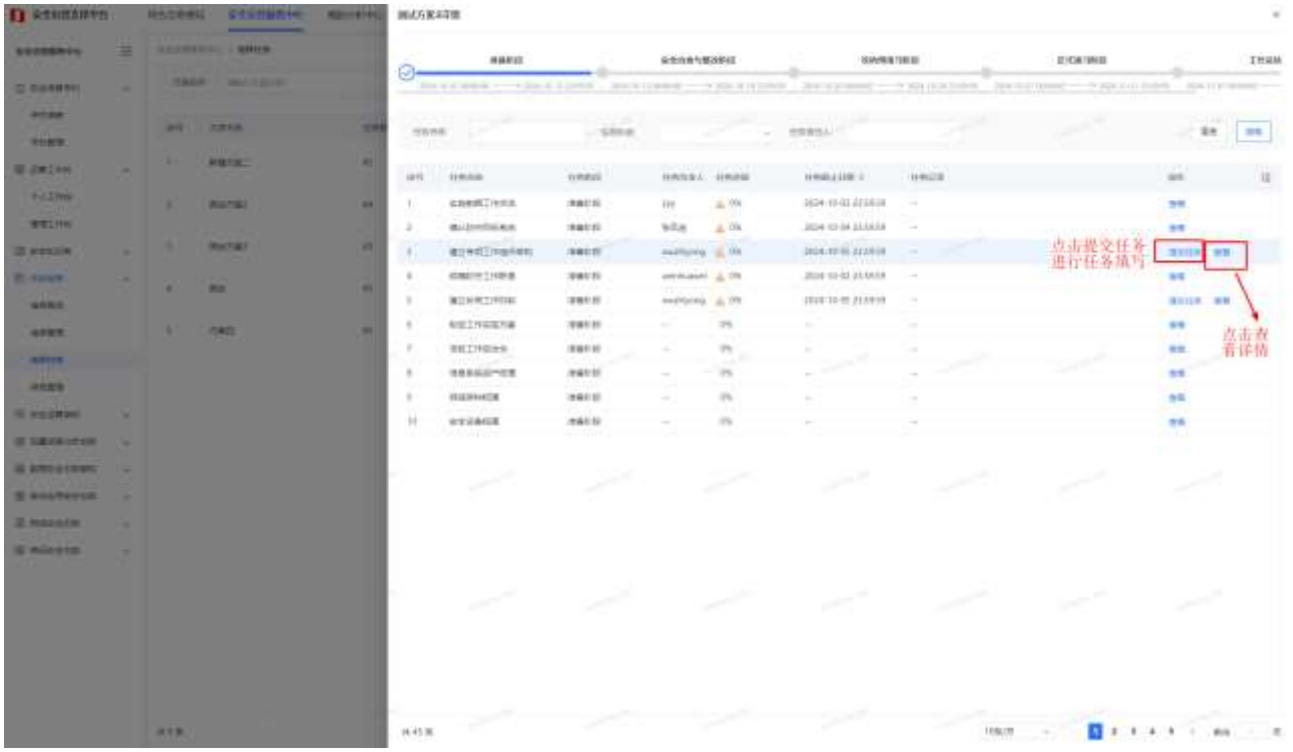


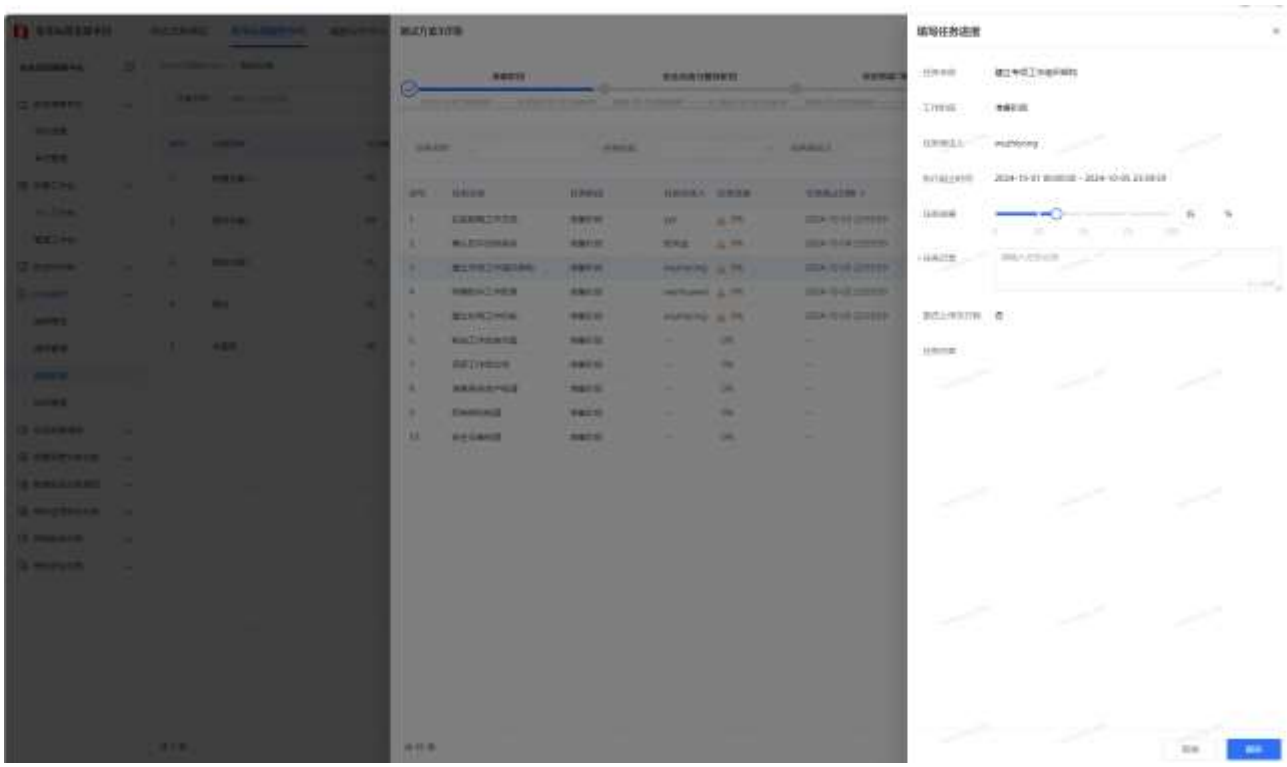


3.3.4.3 指挥任务

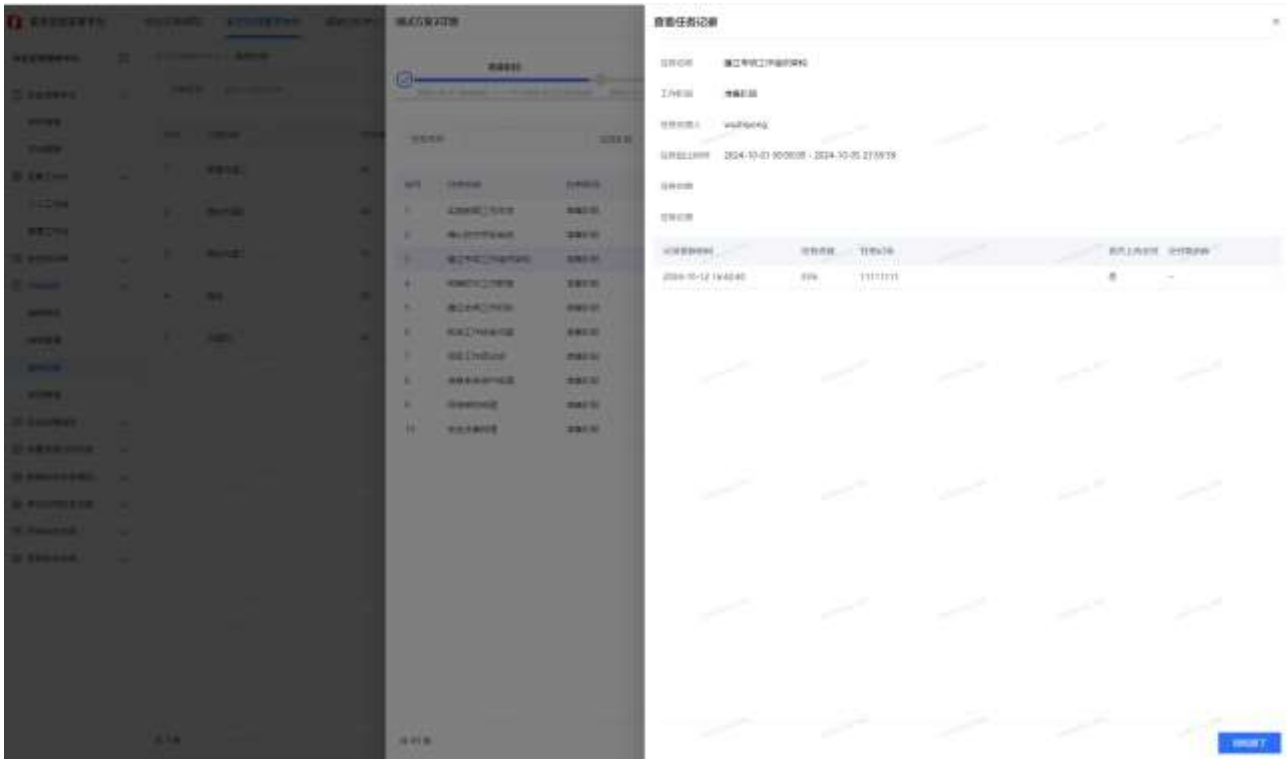
【功能说明】分配给各个责任人的任务进展记录与材料的提交；


点击进行任务管理
填写与当前登录人
相关的工作任务


点击提交任务
进行任务填写
点击查
看详情

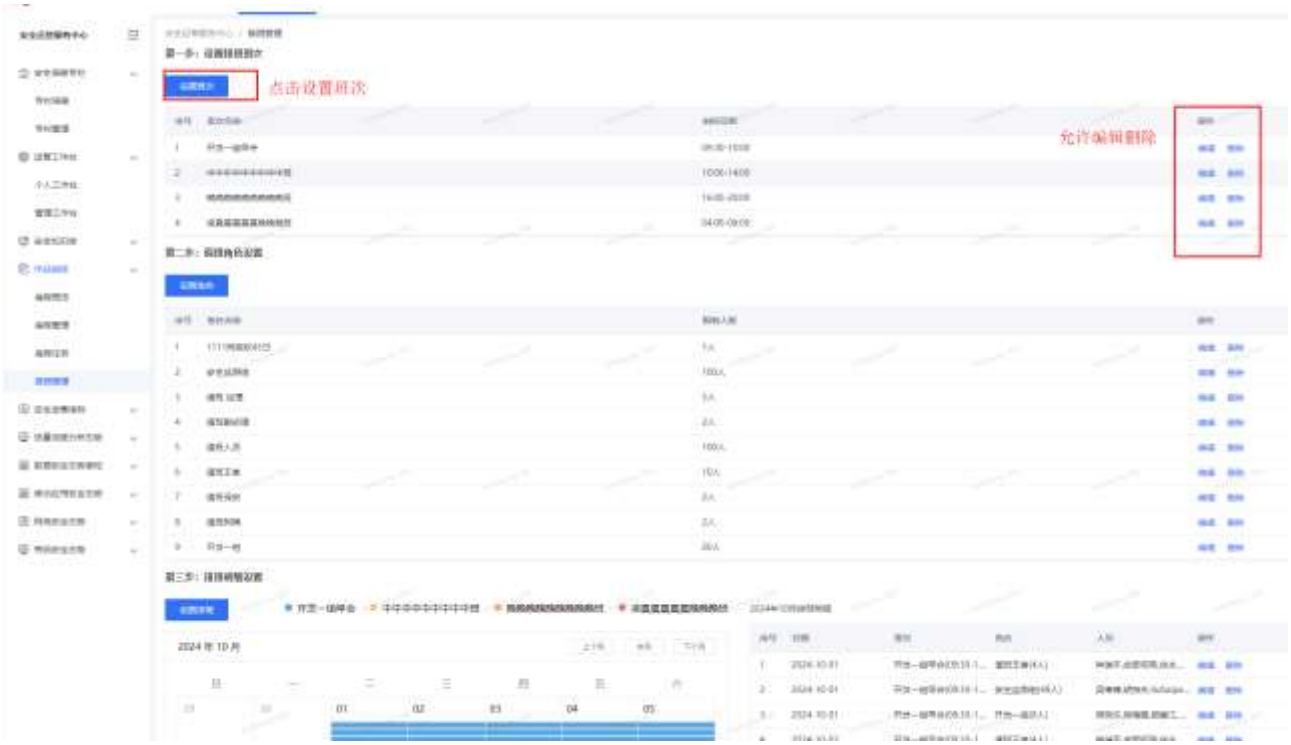


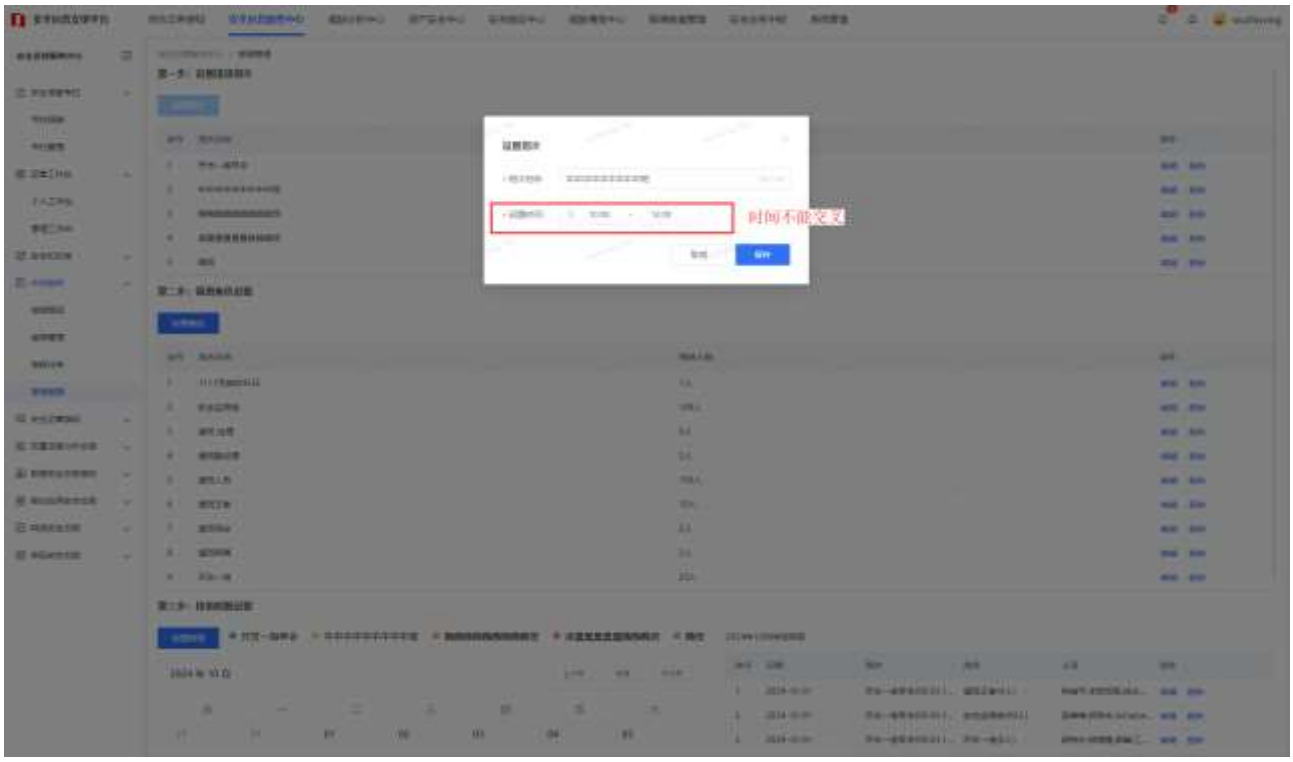
点击详情按钮，查看详情



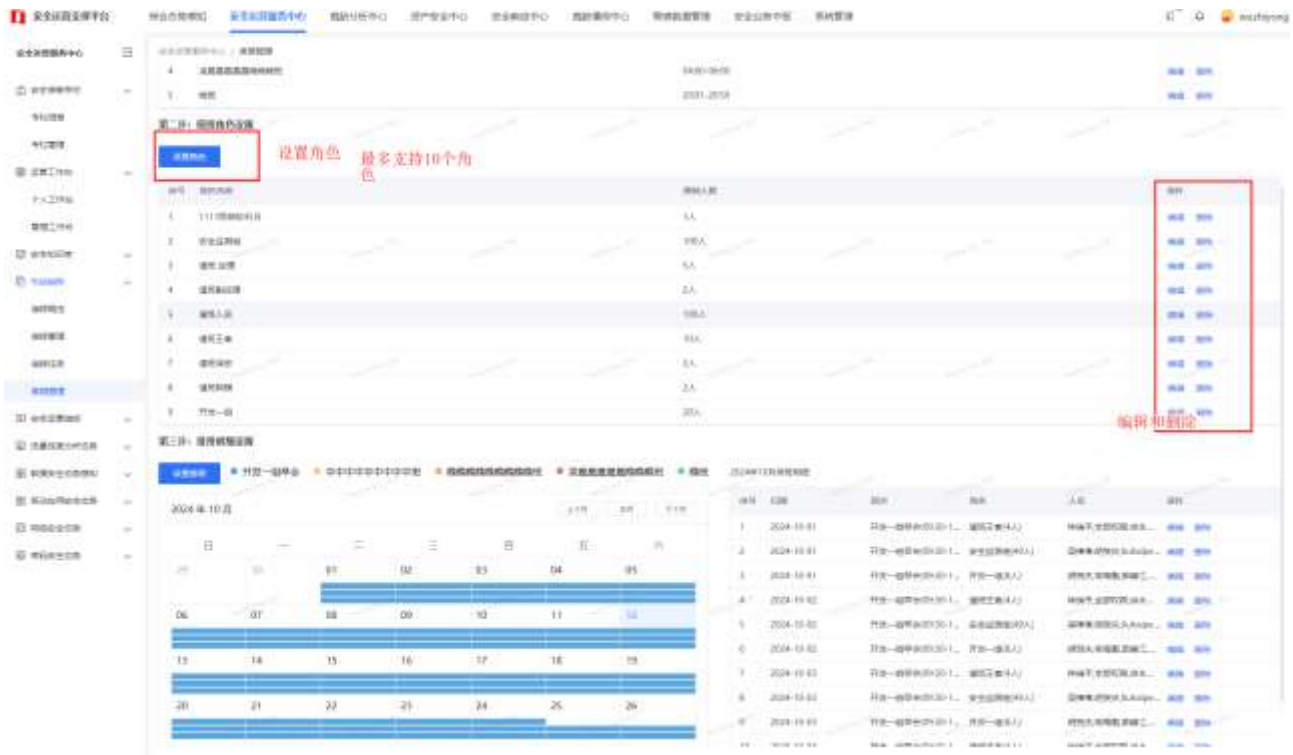
3.3.4.4 排班管理

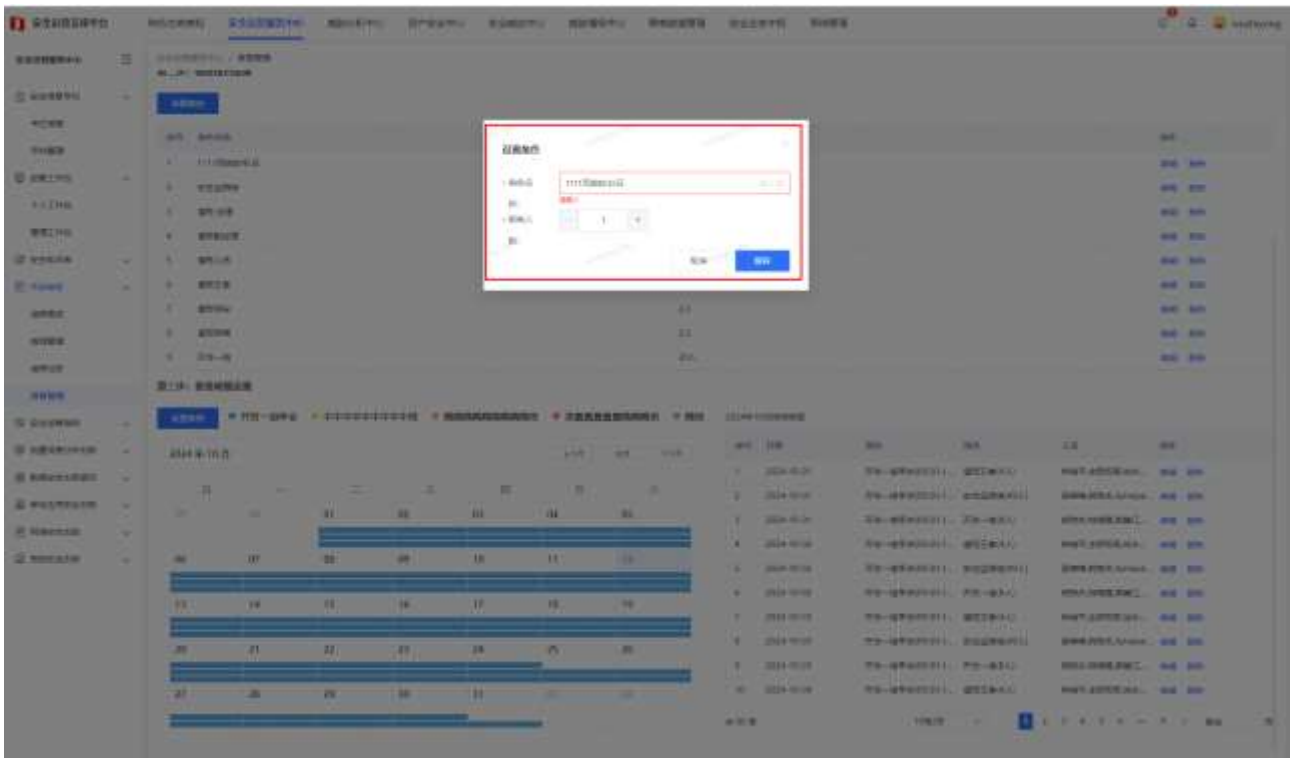
【功能说明】【指挥调度】-> 【排班管理】针对所有用户进行整体的排班管理，需要先进行班次设置，设置值班班次，最多支持 5 个班次





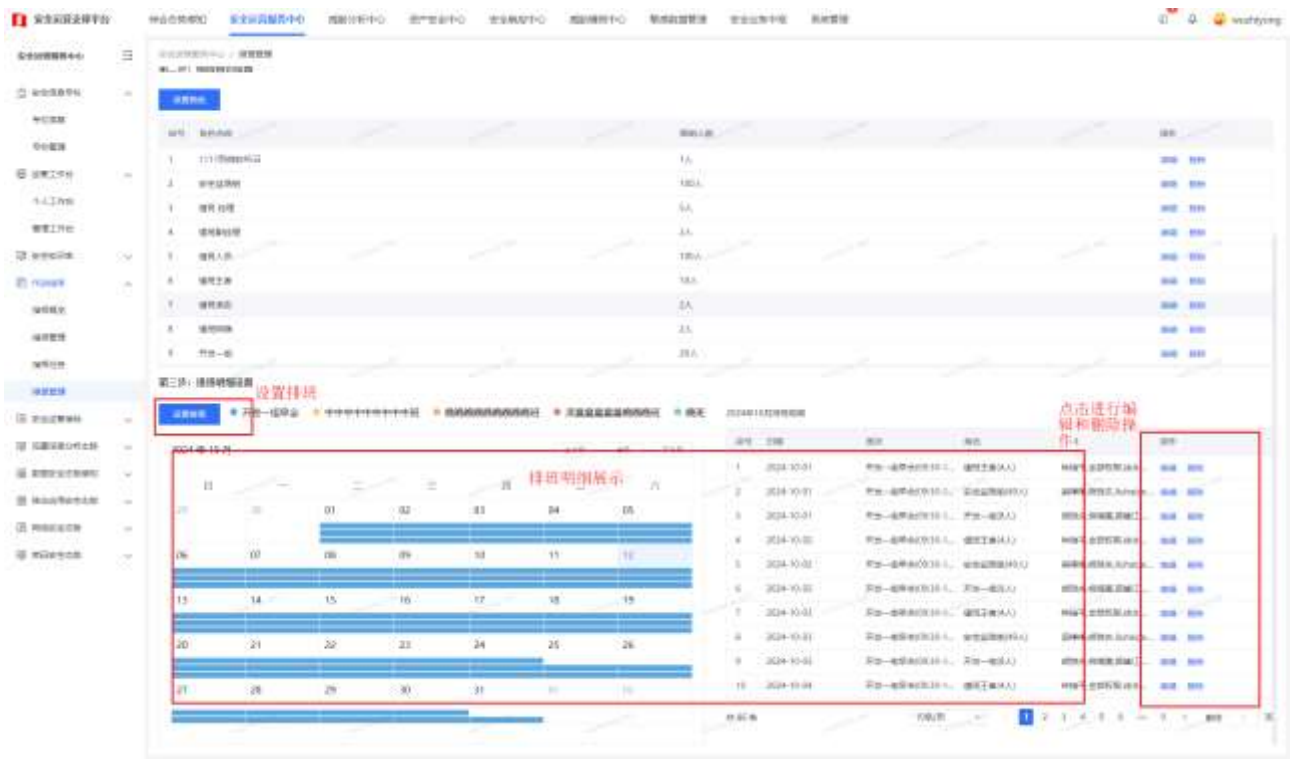
值班角色设置，最多支持 10 个角色设置；

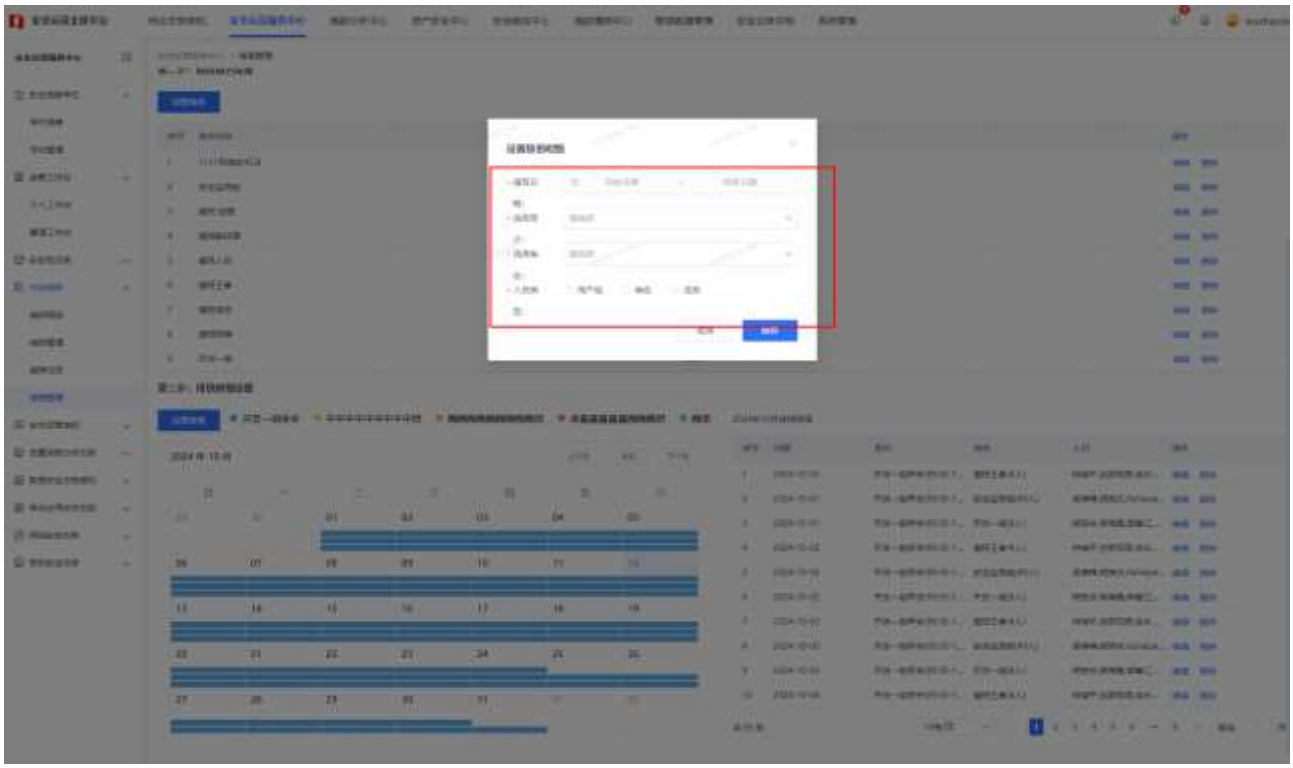




值班排班明细设置：根据前面两步的设置进行配置班次，角色、然后选择值班

人；





3.4 安全业务中枢

3.4.1 可视化分析

进入安全业务中枢主页后,点击左侧可视化分析按钮,展开下拉

图表管理

3.4.1.1 图表管理

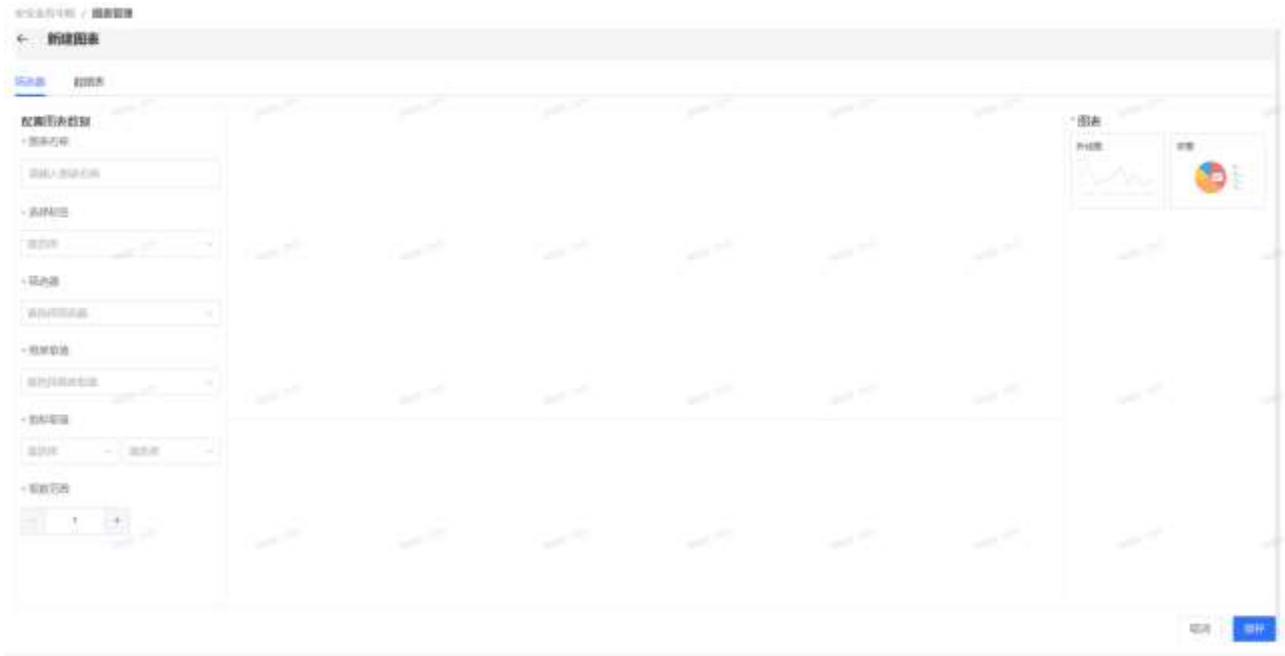
3.4.1.1.1 用户点击图表管理进入图表列表页面

页面展示内容分别为图表标签列表,右侧主体部分为图表的列表;

顶部可进行条件填写进行条件查询,同时图表的创建是根据标签创建的,同时左侧的标签的点击也可进行关联查询图表;

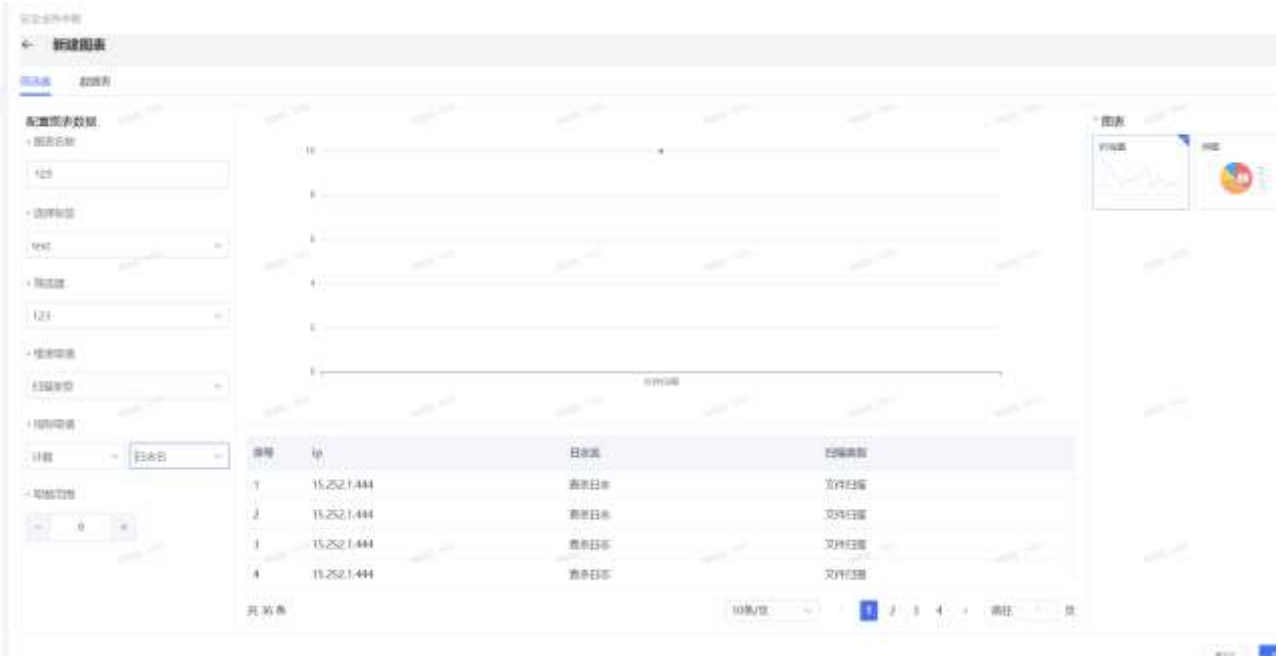
3.4.1.1.2 新建图表

1、创建图表：点击新建图表按钮进入新建图表页面， 可进行相关图表的数据配置.



2、分为筛选器,数据表数据来源:可进行键入图表名称,选择标签,选择筛选器,以及维度取值,指标取值取数范围和图表样式后展示对应的图表数据。

3、正常获取的数据，会生成图表,以及关联的数据表表格。



4、可进行保存,后续可在列表查询页面进行查看详情以及编辑。

3.4.2 数据检索与分析

3.4.2.1 数据检索

3.4.2.1.1 默认检索

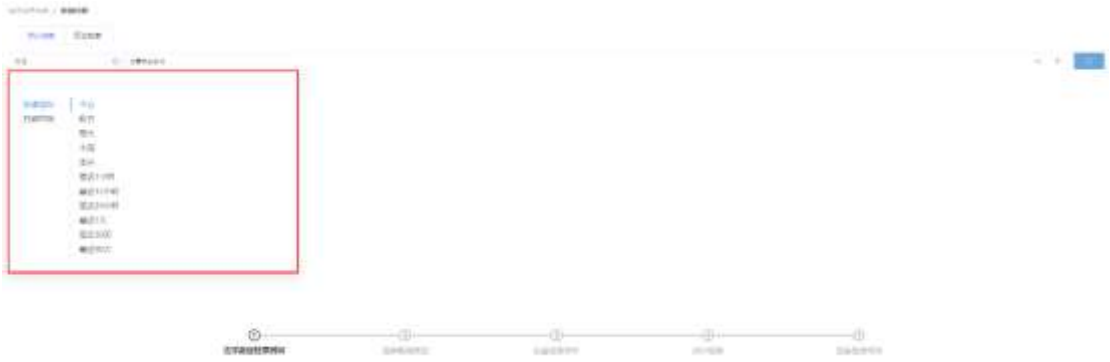
【应用场景】

添加数据源维护数据表之后，还需要数据源,数据表开启检索。一般来说，基本的检索语句可以自动生成。

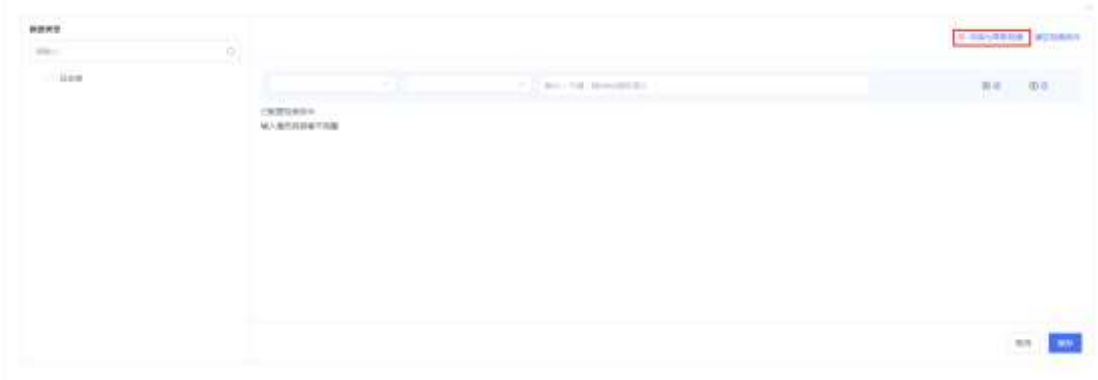
【操作步骤】

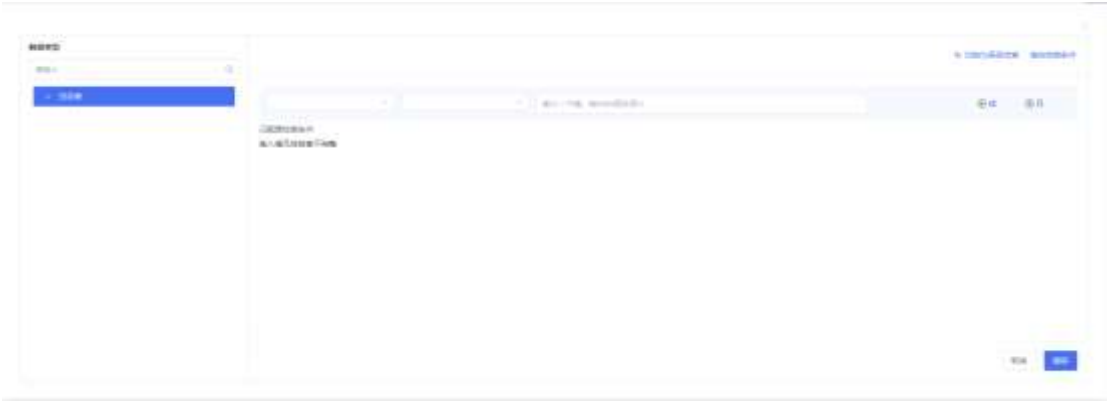
数据检索与分析>数据检索

1、 选择数据检索时间



2、 可以切换检索方式（快速检索，高级检索）选择数据类型

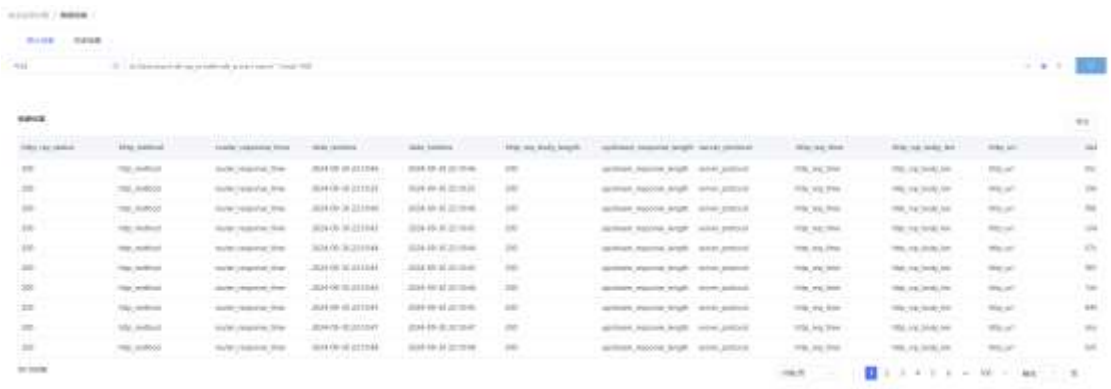




3、 设置检索条件

4、 执行检索

5、查看检索结果



3.4.2.1.2 保存筛选器

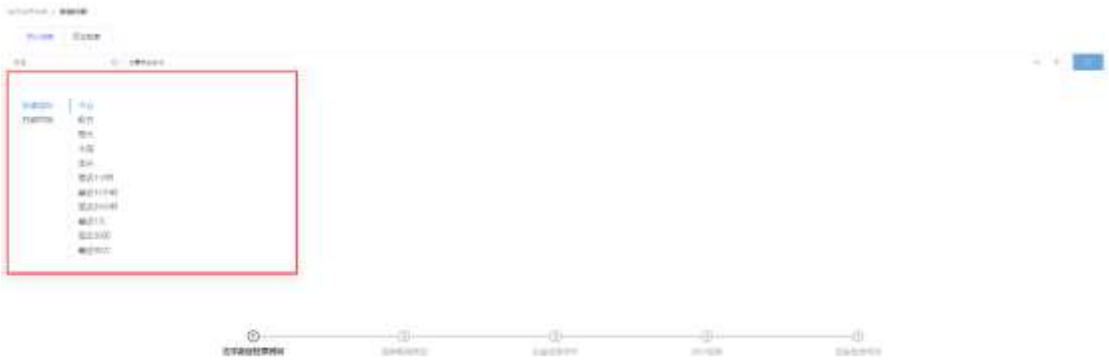
【应用场景】

设置检索条件可以保存筛选器。

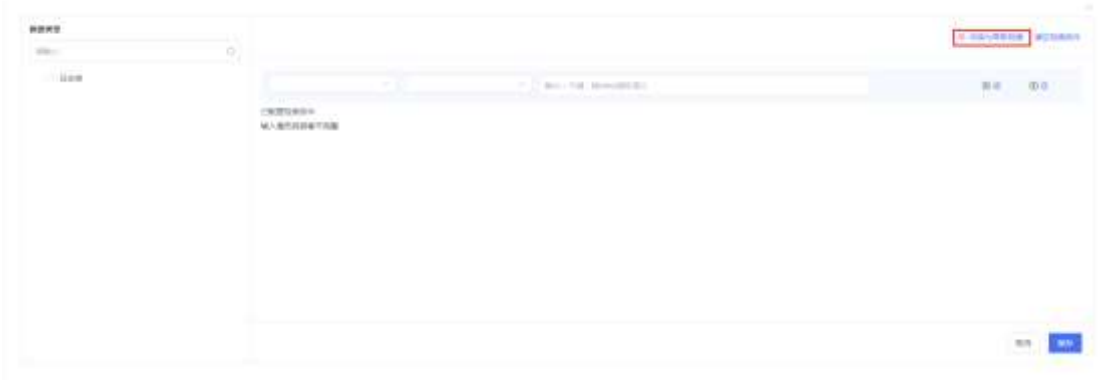
【操作步骤】

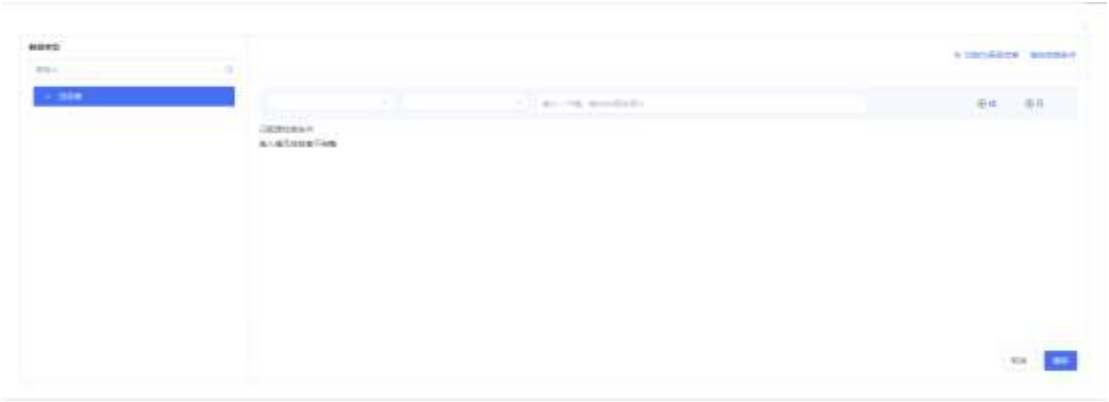
数据检索与分析>数据检索

1、 选择数据检索时间



2、 可以切换检索方式（快速检索，高级检索）选择数据类型





3、 设置检索条件

4、输入筛选器名称保存筛选器

3.4.2.1.3 筛选器

【应用场景】

通过筛选器，快速填写检索语句。

【操作步骤】

数据检索与分析>数据检索

1、 默认检索查看筛选器。

2、 筛选器检索

3、删除筛选器

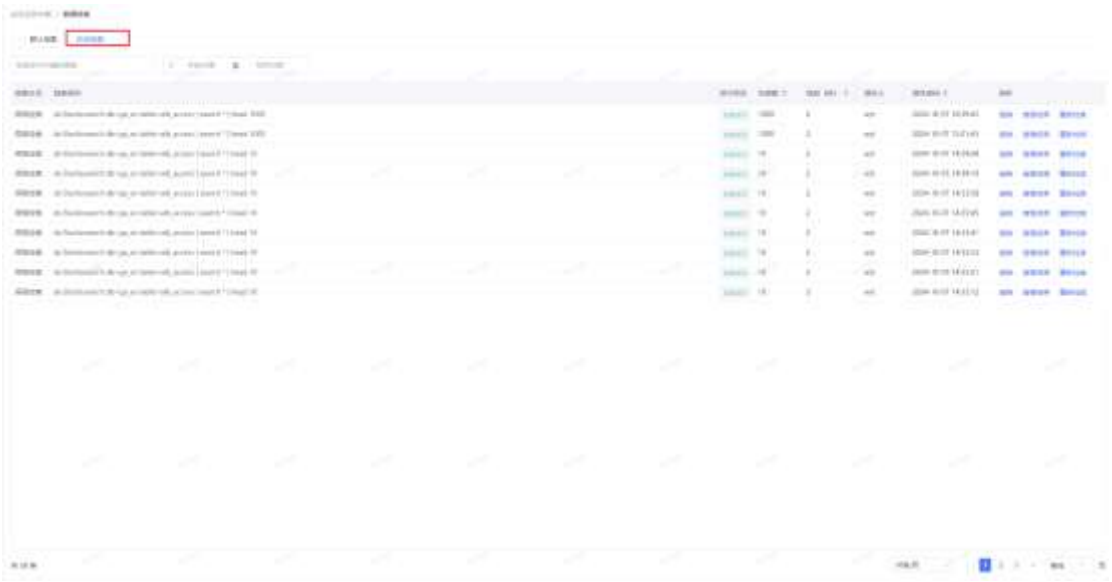
3.4.2.1.4 历史检索

【应用场景】

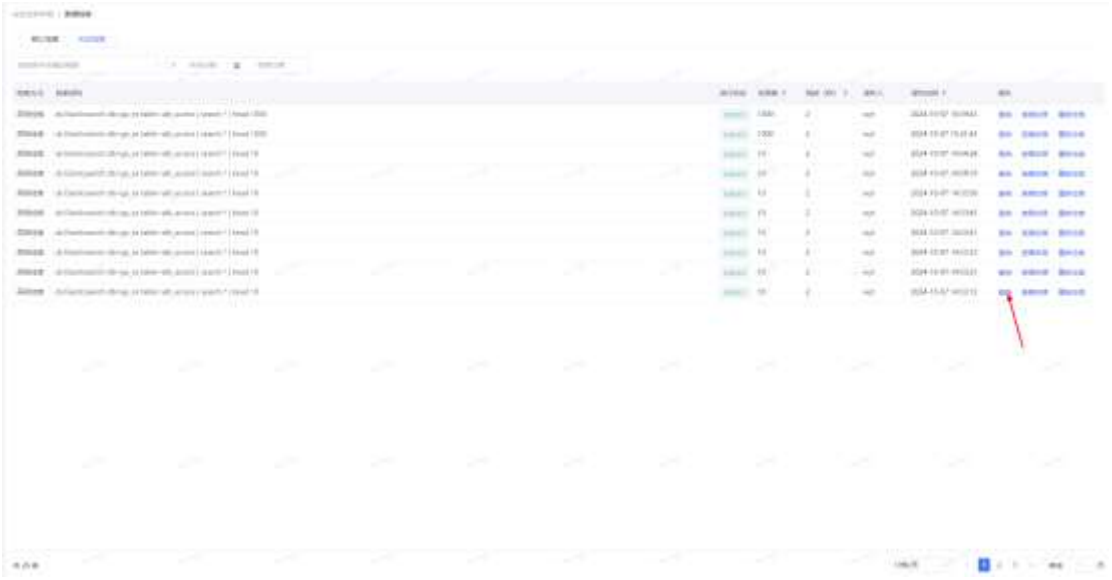
每一次检索后的检索语句都保存历史检索。通过历史检索快速重新访问之前查找过的检索结果，无需重新输入检索语句。

【操作步骤】

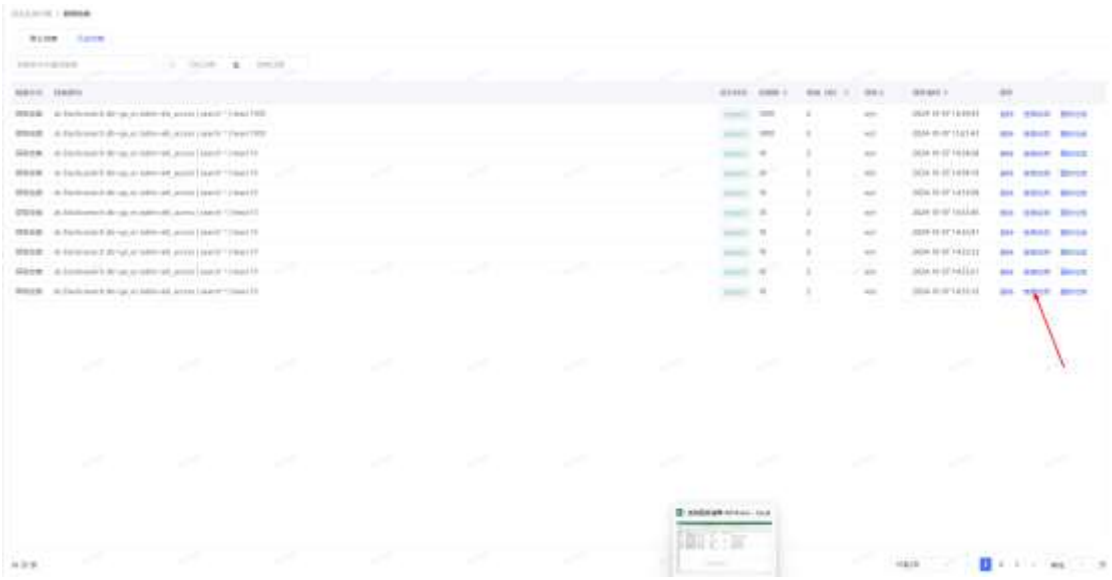
1、 历史检索列表。



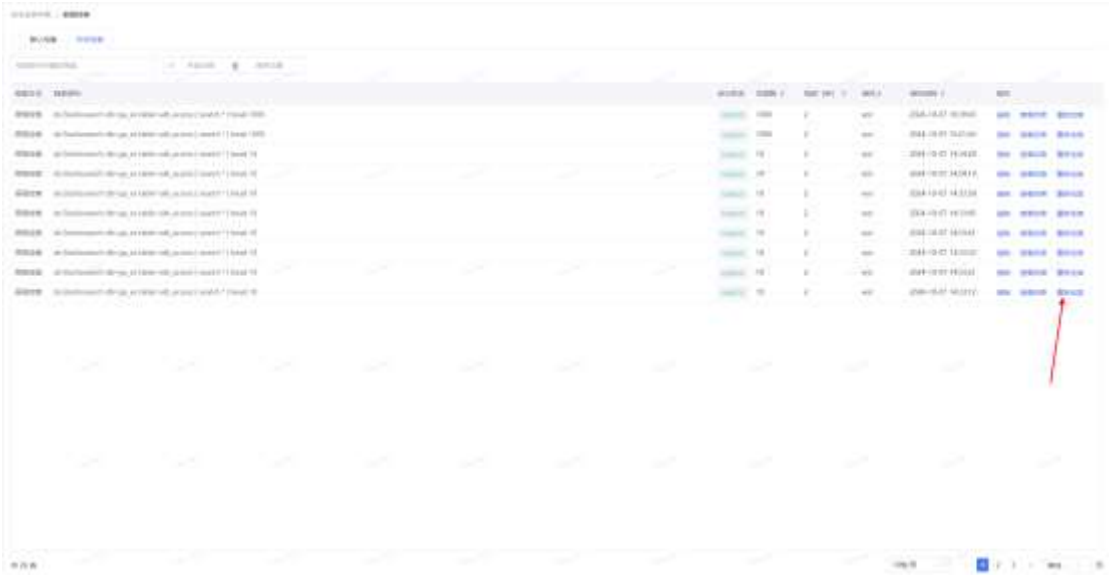
2、 删除历史检索。



3、 历史检索查看结果。

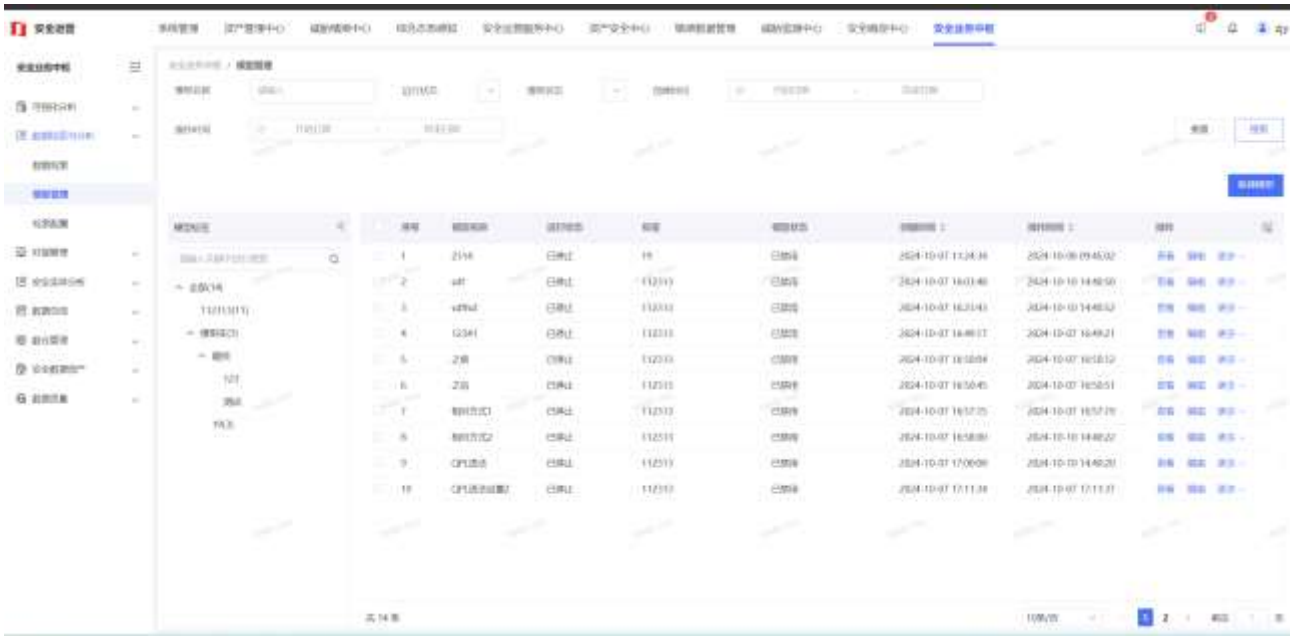


4、历史检索重新检索。



3.4.2.2 模型管理

3.4.2.2.1 用户点击模型管理进入模型列表页面



页面展示内容分别为模型标签列表,右侧主体部分为模型的列表

顶部可进行条件填写进行条件查询,同时模型的创建是根据标签创建的,同时左侧的标签的点击也可进行关联查询模型;

3.4.2.2.2 新建模型

点击新建模型进入模型创建页面,

基本信息:可以填充基础信息,模型名称,关联标签,添加模型描述.

运行配置:分为查询时间范围部分,模型运行周期,查询的结果的保留时间

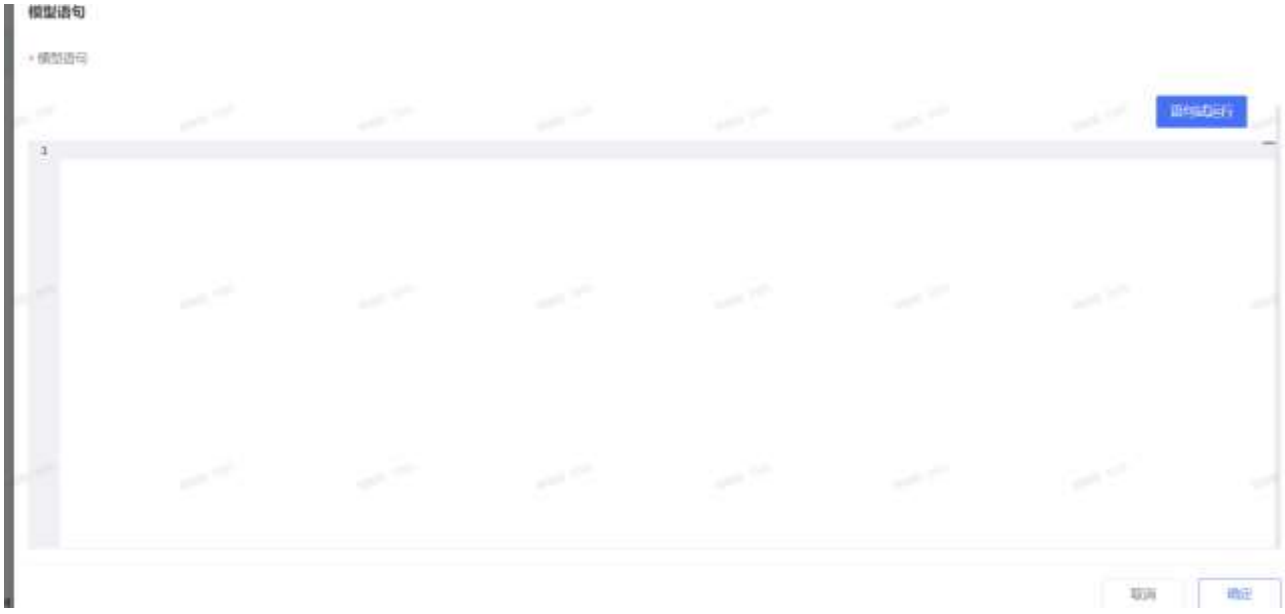
查询时间范围:分为日期时间范围,相对时间范围,qpl 语法设置;可进行固定时间范围以及相对时间范围的填写,以及通过 qpl 的语法时间表达进行类似于相对时间范围的填写

模型运行周期:可以设置简易的:每多少分钟或者多少小时多少天进行执行该模型;也可以通过简易的 cron 表达式进行特殊的运行周期设置;

保留时间:可进行相关设置,查询出的数据会按照模型设置的保留时间进行定时

删除;

接下来为具体的模型执行语句:按照 qpl 语法说明进行查询相关的表以及拼接相应的条件,填写完成后,可以点击语句试运行按钮,查看当前的语句是否能够成功执行.



保存成功后模型自动运行,可进行启用禁用以及编辑.

3.4.2.2.3 模型查看

点击查看按钮进入对应模型的详情页面.

页面中展示执行的周期数以及成功次数和失败次数,每页会固定展示五个周期的数据,展示当前的运行版本.

3.4.2.3 检索配置

3.4.2.3.1 数据源管理

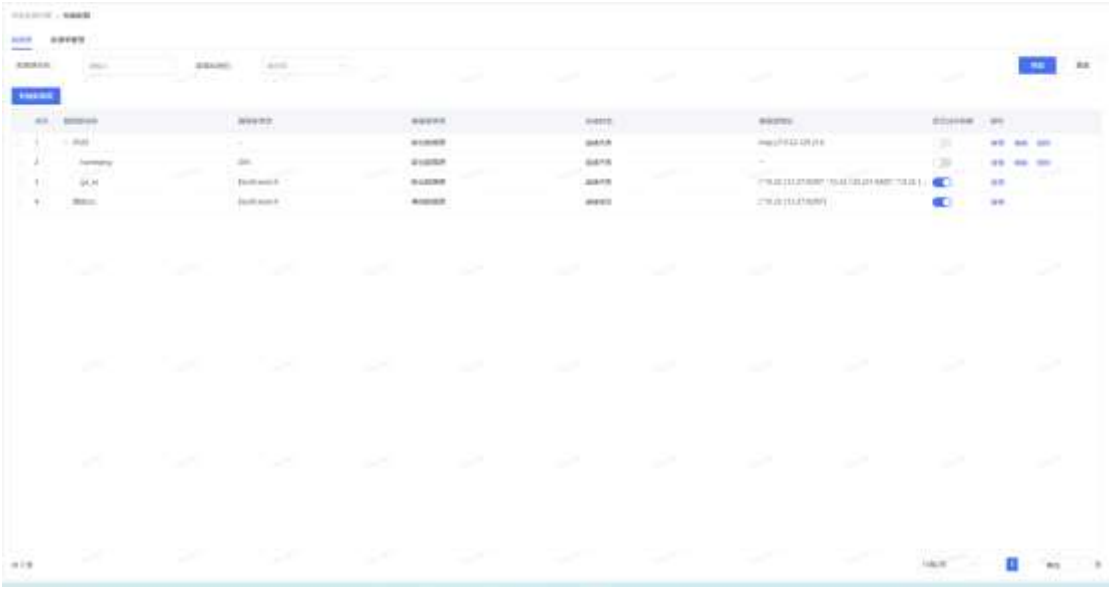
【应用场景】

数据源管理是数据检索的基础，它涉及数据的采集、整合、存储、分析和利用等多个环节。

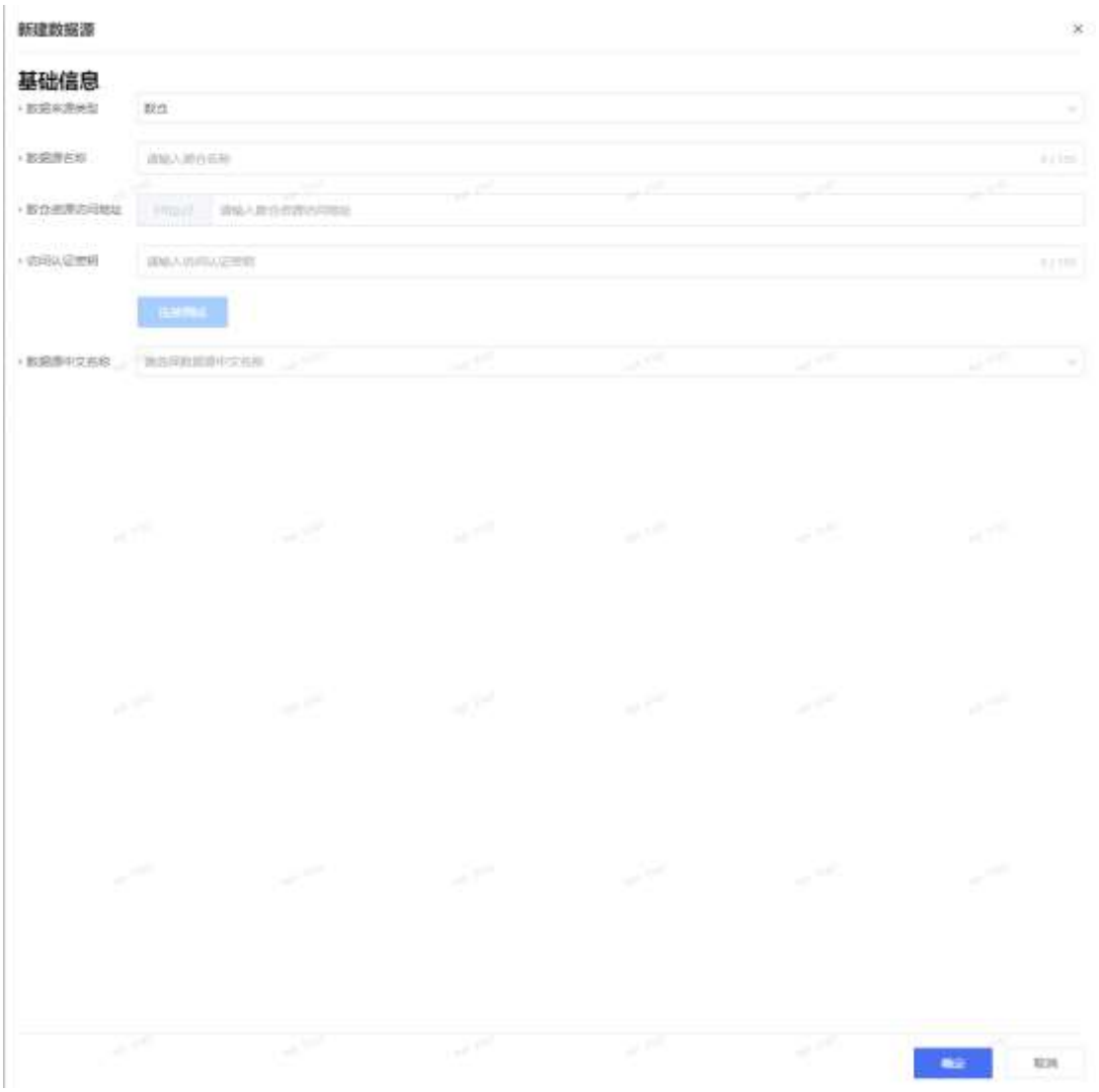
【操作步骤】

数据检索与分析>检索配置> 数据源

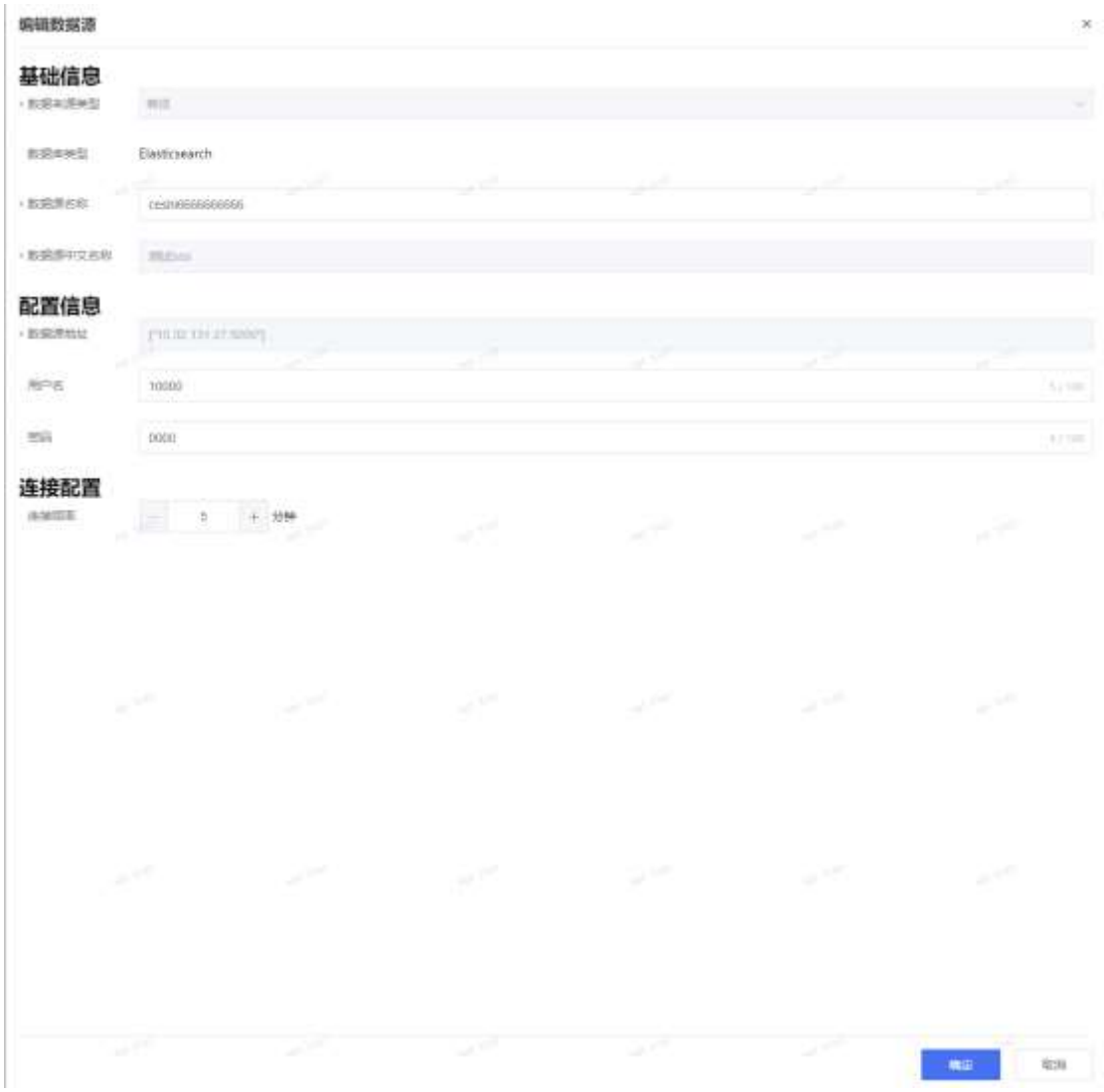
1、 数据源列表

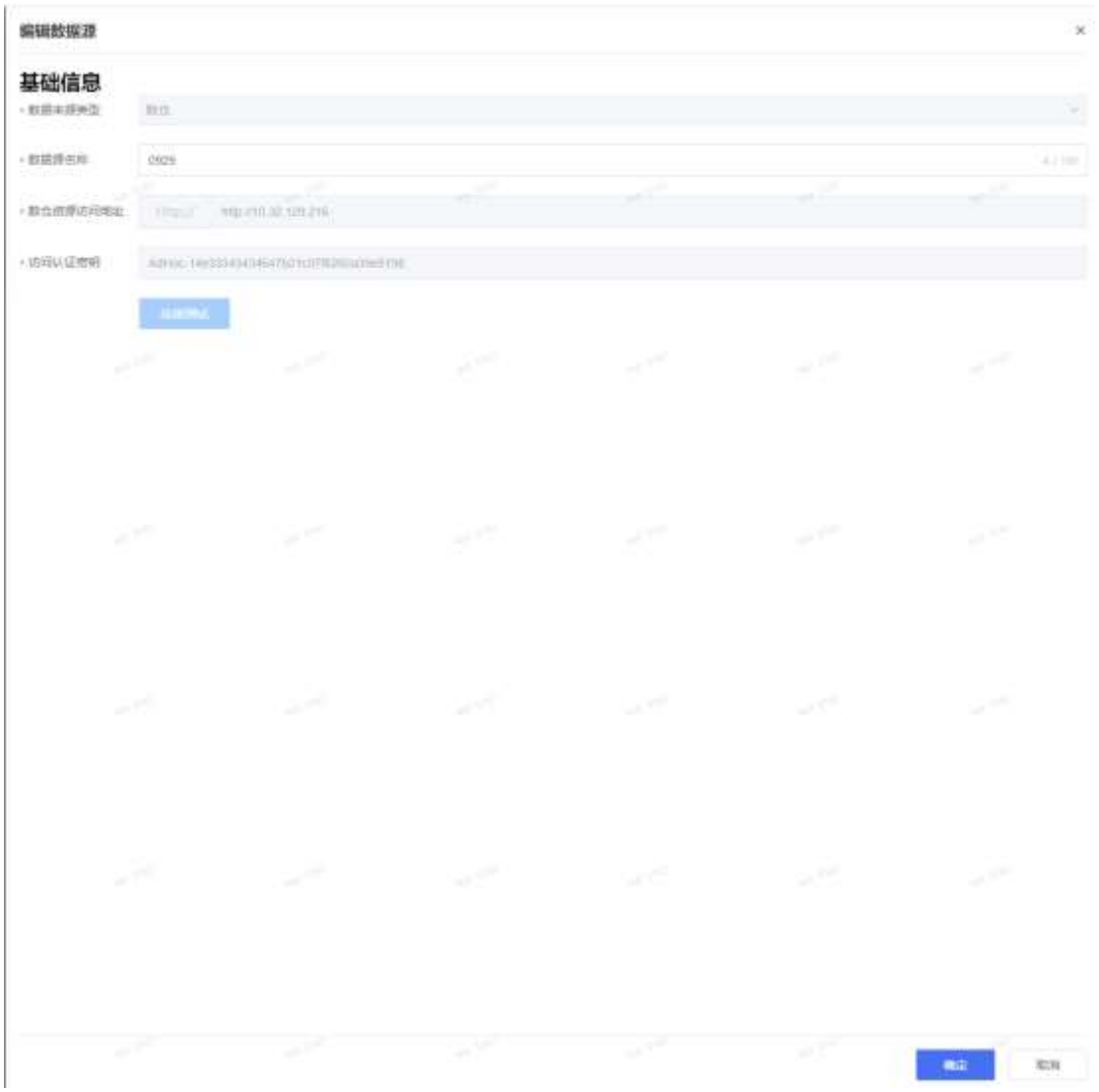


2、新建数据源

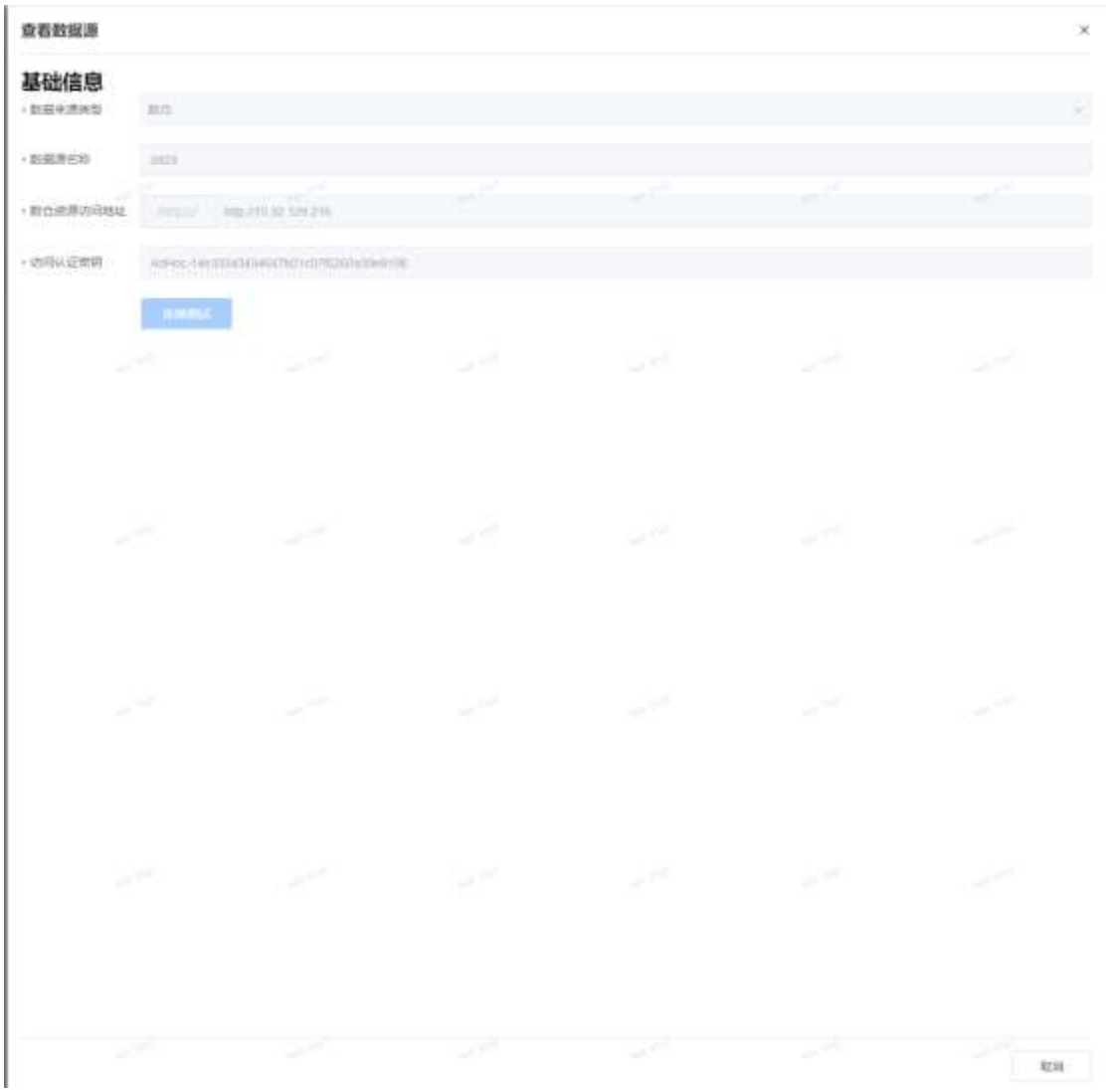


3、 编辑数据源

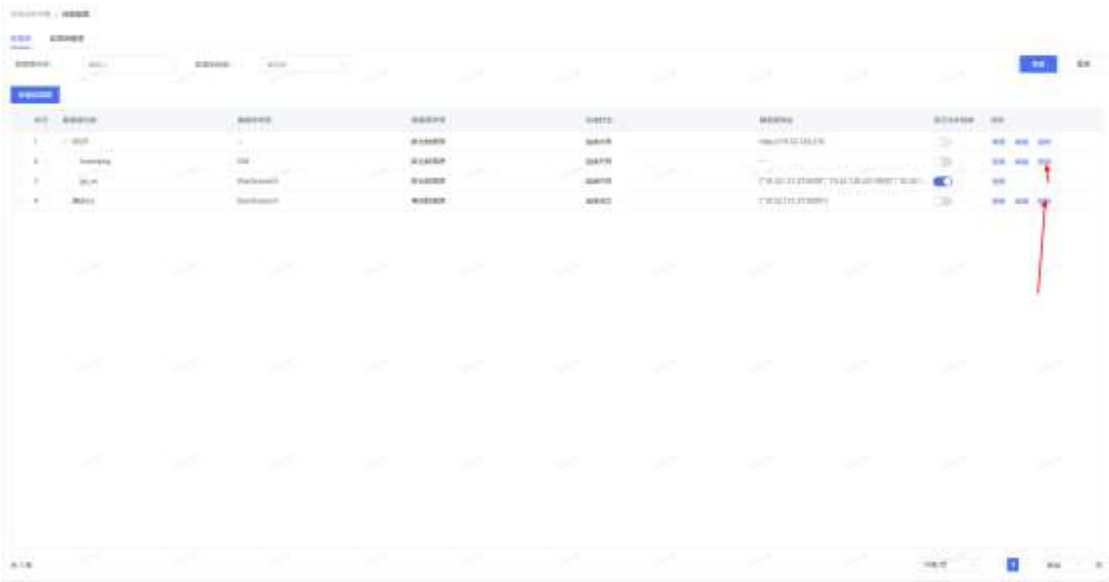


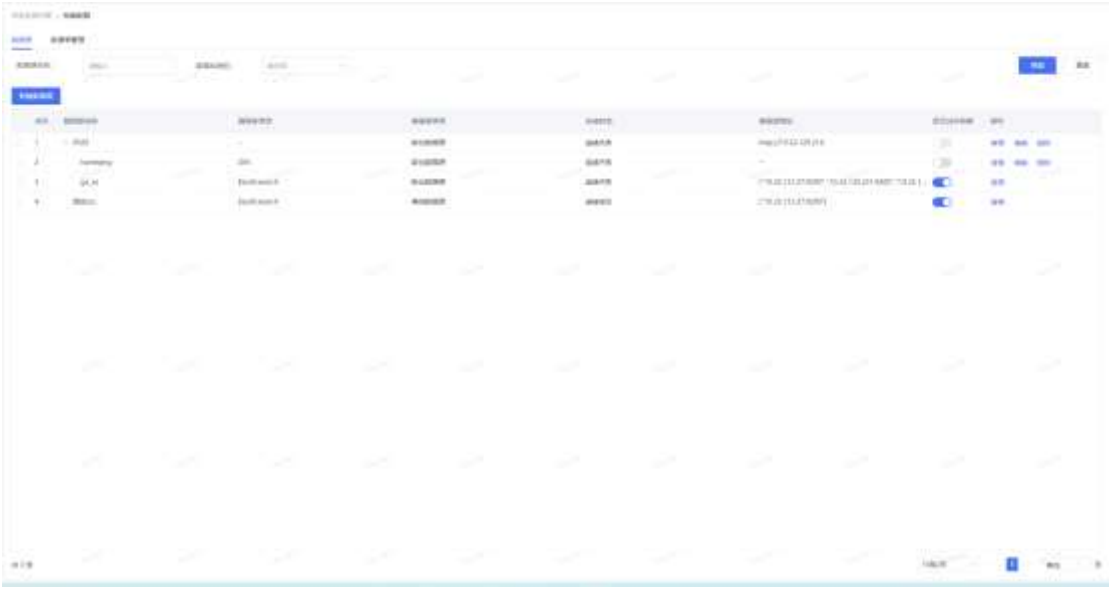


4、 查看数据源


查看数据源
基础信息

5、删除数据源





3.4.2.3.2 数据表管理

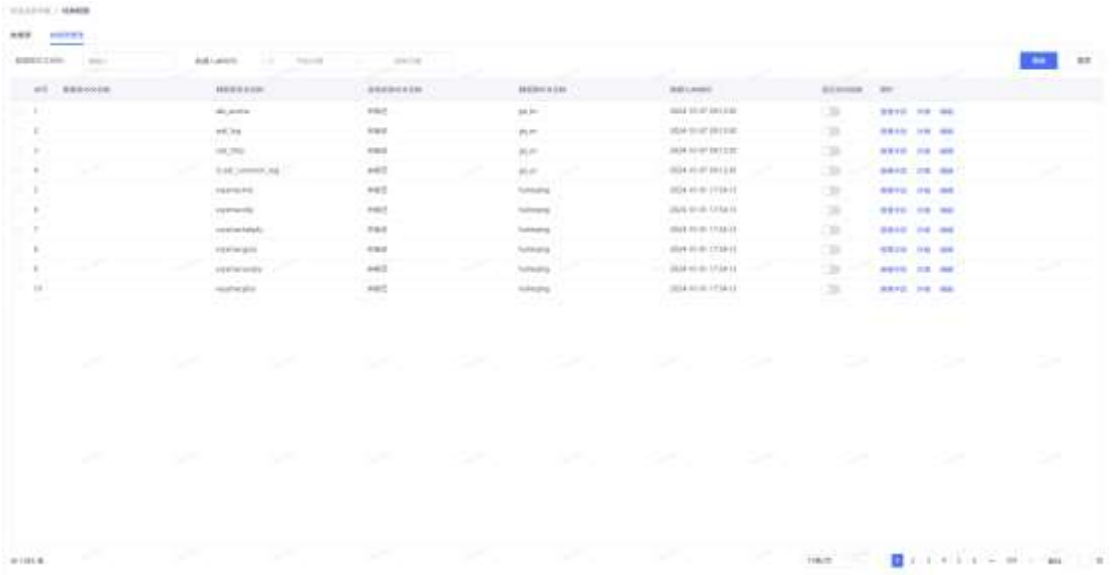
【应用场景】

数据表管理是数据源管理的重要组成，它涉及数据的采集、整合、存储、分析和利用等多个环节的基础。

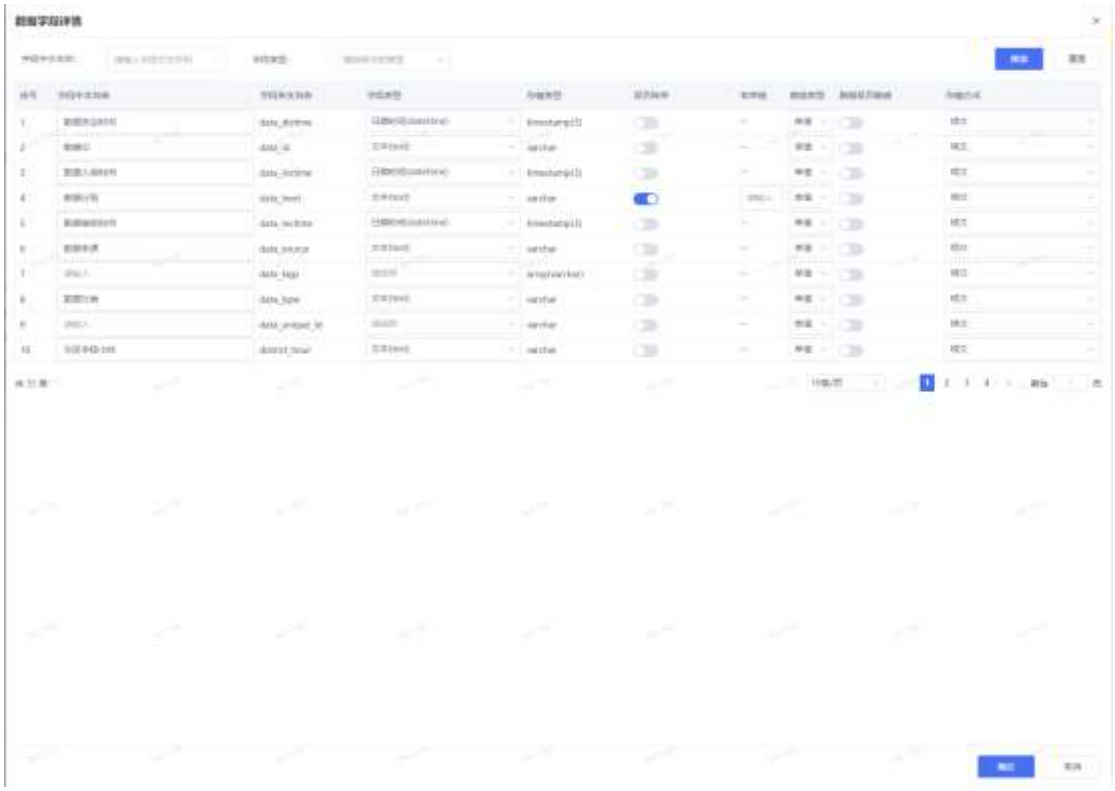
【操作步骤】

数据检索与分析>检索配置> 数据表

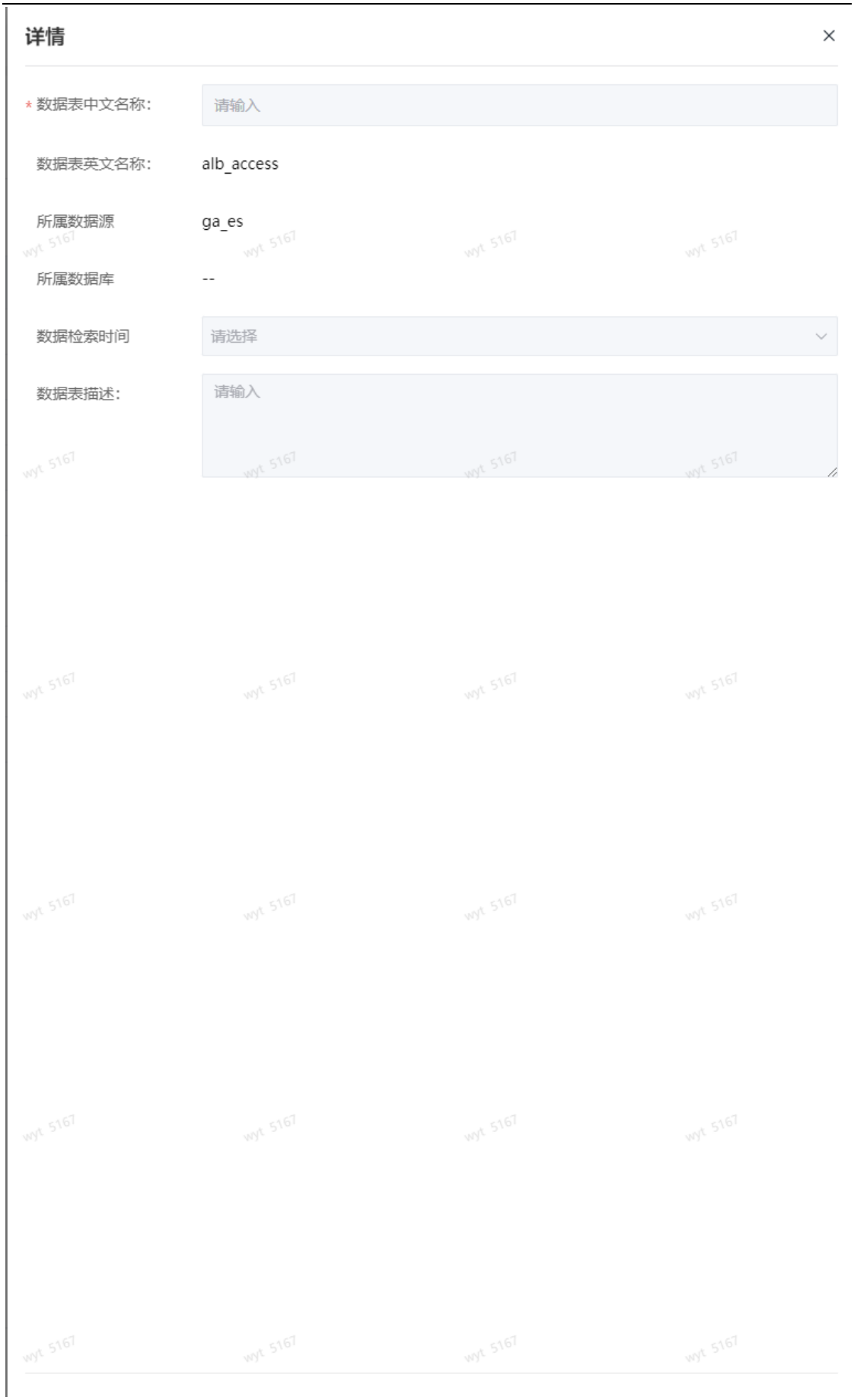
1、 数据表列表



2、 查看字段



3、 数据表详情


详情
* 数据表中文名称:
请输入
数据表英文名称:
alb_access
所属数据源
ga_es
所属数据库
--
数据检索时间
请选择
数据表描述:
请输入

4、编辑数据表


编辑数据表
* 数据表中文名称：
请输入
0 / 100
数据表英文名称：
alb_access
所属数据源
ga_es
所属数据库
--
数据检索时间
请选择
数据表描述：
请输入
0 / 1000
确定
取消

3.4.3 对接管理

3.4.3.1 对接插件

3.4.3.1.1 数据对接插件

3.4.3.1.1.1 新增数据对接插件

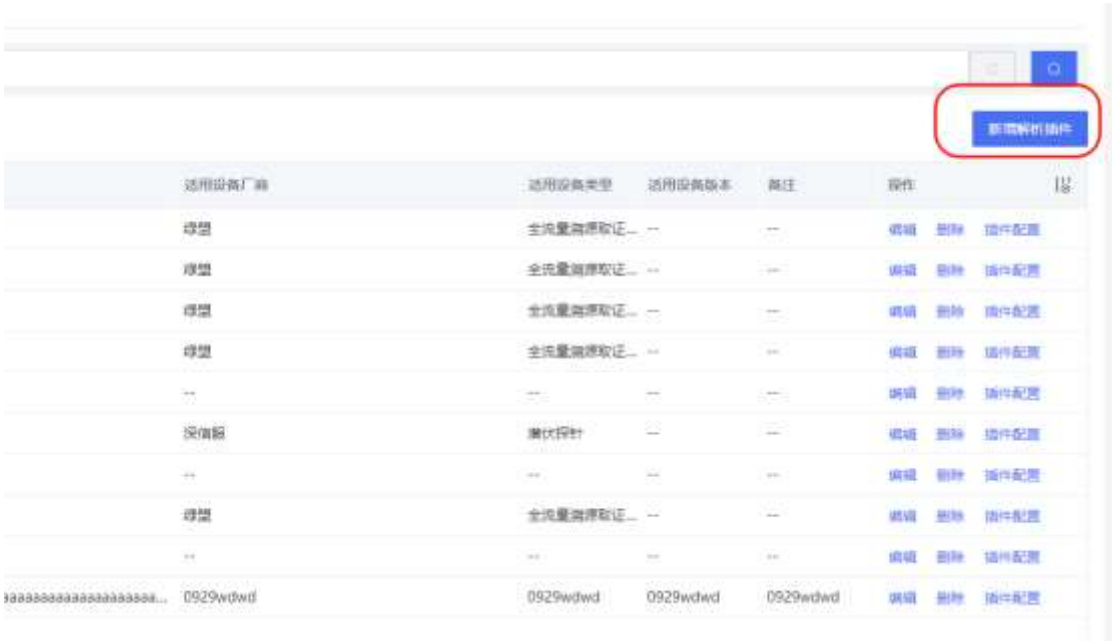
【应用场景】

新增一个对接插件供设备对接使用。

【操作角色】

【操作步骤】

1、 点击新增解析插件按钮



2、 根据列名填写内容

3、点击保存按钮保存插件，插件名称已存在则不能保存

3.4.3.1.1.2 删除数据对接插件

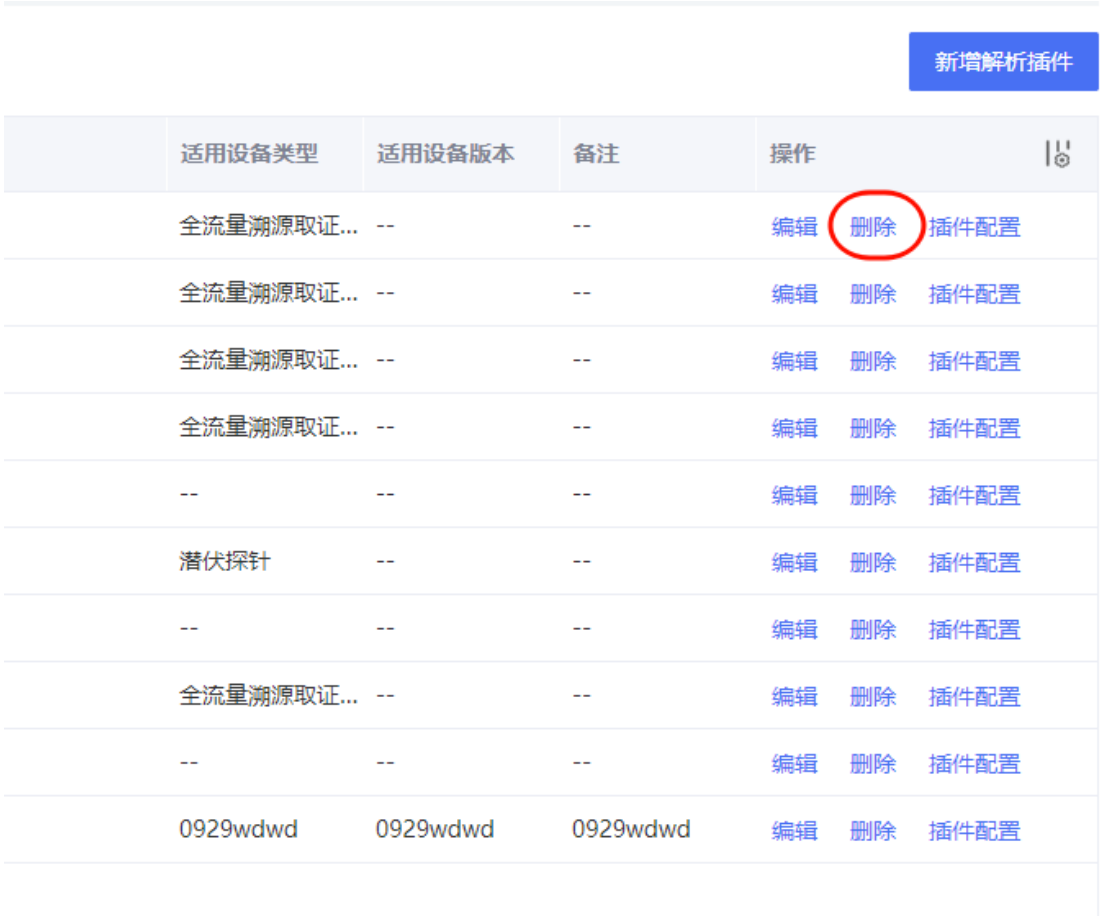
【应用场景】

删除多余的或者废弃的对接插件。

【操作角色】

【操作步骤】

1、 点击删除按钮删除对接插件



2、如果插件已被调用，则不可删除，需要先删除调用的设备对接

3.4.3.1.1.3 修改数据对接插件

【应用场景】

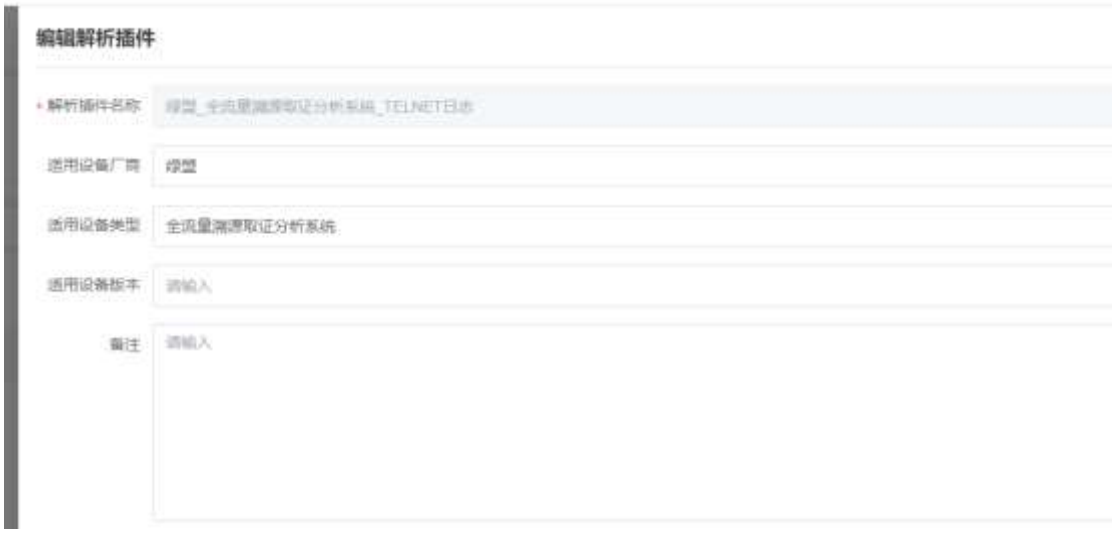
对已存在的插件内容做修改。

【操作角色】

【操作步骤】

1、点击编辑按钮

2、修改插件的信息，插件名称不可修改



3、保存插件

3.4.3.1.1.4 查询数据对接插件

【应用场景】

对现有的对接插件进行检索，默认全量分页检索，可以对插件名称做模糊匹配检索。

【操作角色】

【操作步骤】

1、 直接点击对接插件菜单，默认是全量分页检索

2、输入解析插件名称模糊检索

3.4.3.1.1.5 数据对接插件配置

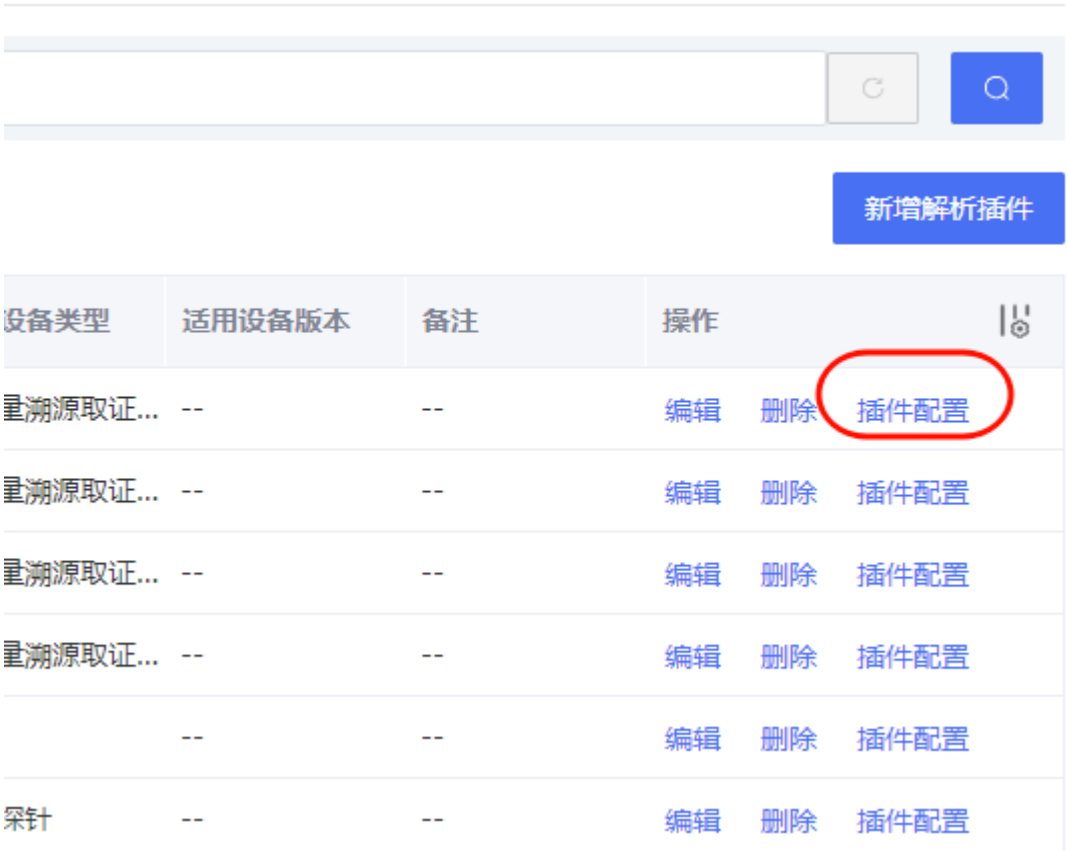
【应用场景】

对数据对接插件进行配置，生成 NIFI 插件模板。

【操作角色】

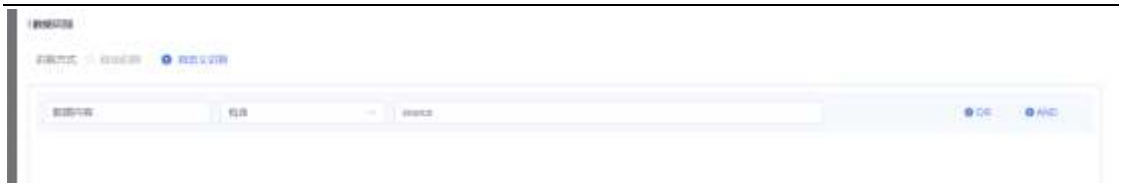
【操作步骤】

1、 点击插件配置

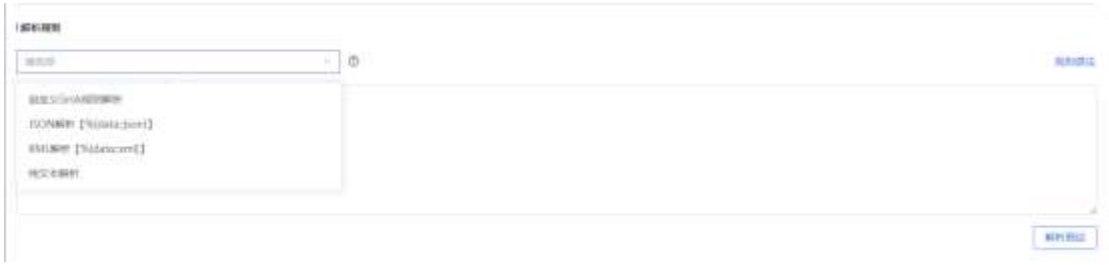


2、 填写日志样例

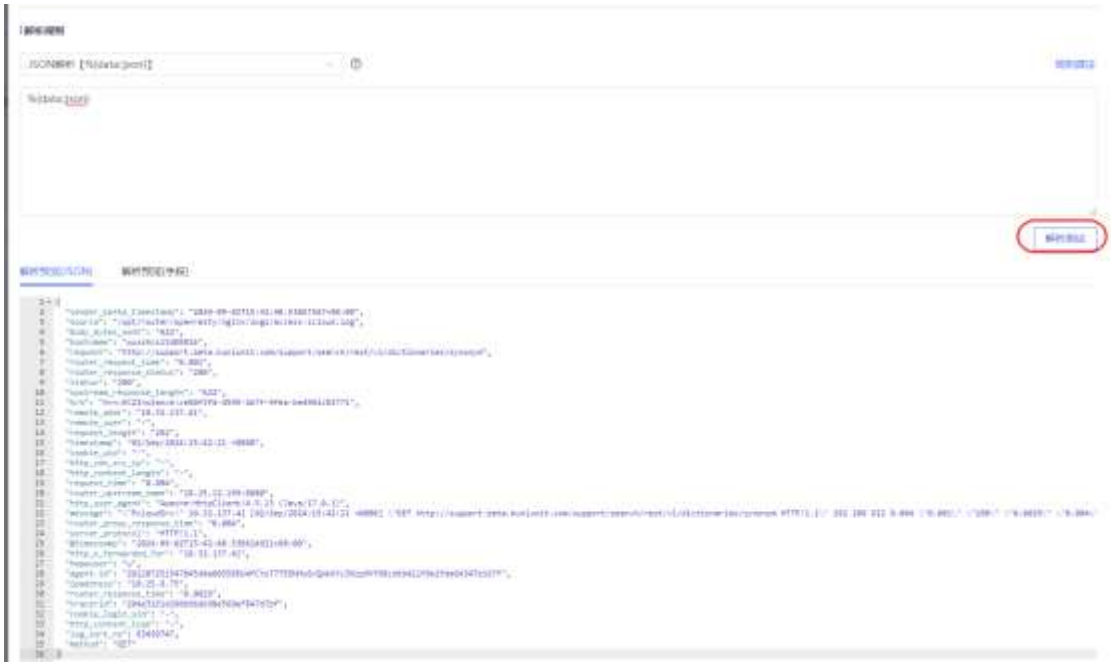
3、设置数据识别：第一个输入框输入固定值【数据内容】；第二个下拉框是选择匹配的方式，又包含和正则两种方式；第三个输入框是写值，如果第二个输入框选择的是包含，则输入日志中的某一个 key，选择的是正则匹配则需要输入正则表达式；可以用 OR 连接或者是 AND 连接，但是 AND 和 OR 不能混用，目的是为了判别是哪种数据类型。



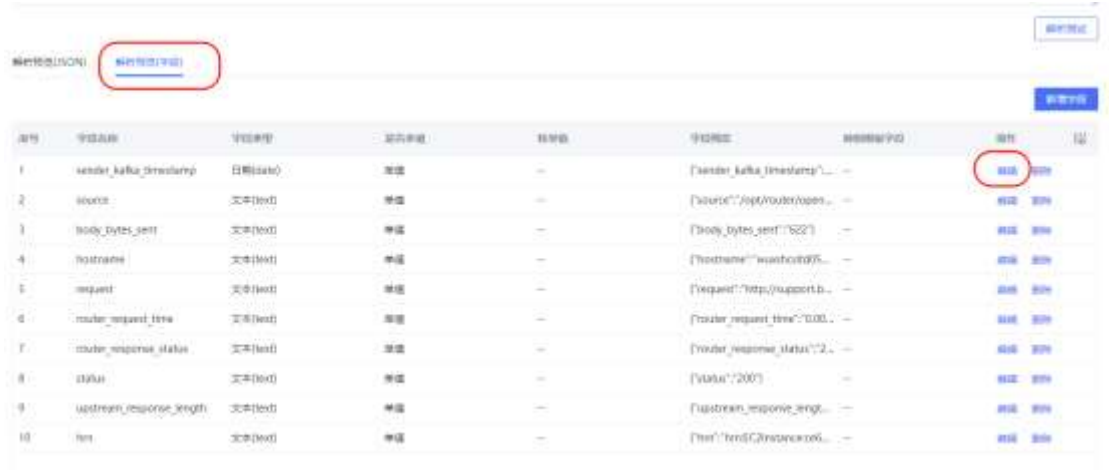
4、解析规则：可以选择以下四种，根据第一步的日志样例进行选择合适的解析规则



5、 点击解析测试，解析出日志中包含的字段，用于第二步赋值使用



6、 切换到解析预览(字段)，对解析出的字段进行配置



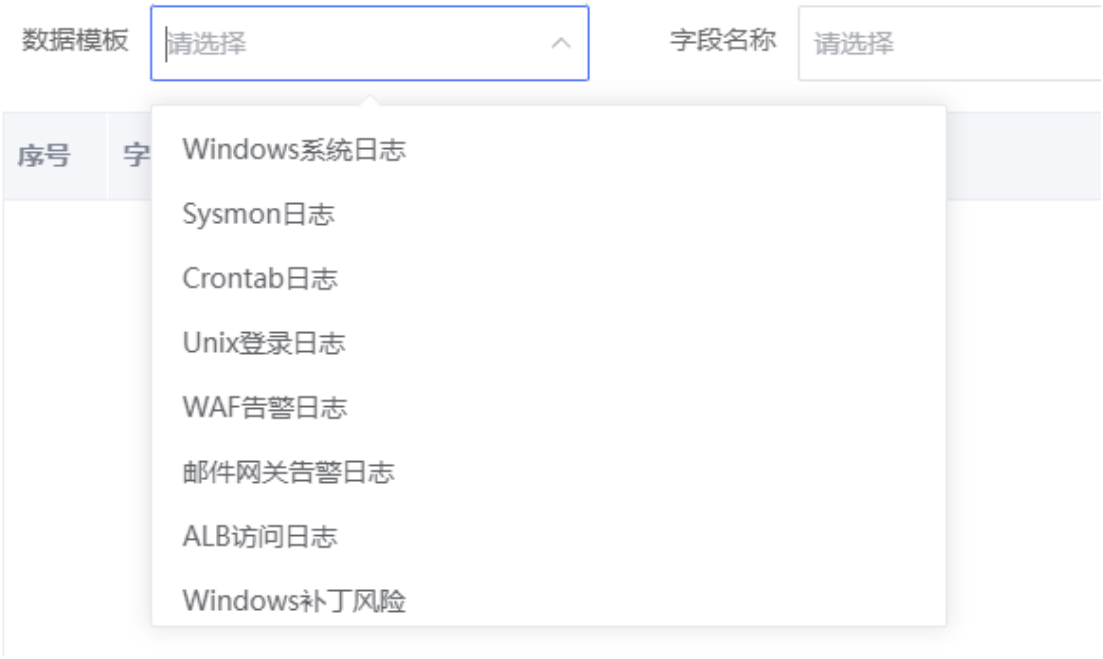
7、 点击编辑对解析出的字段做赋值操作

字段取值支持字段拼接，赋值样例：
#java#$alert_type$#shell#$attack_type$，#中间包括的是常量，$中间包括的是变量

9、 配置字段解析后即可保存

10、 点击下一步或者确定都可以保存当前步骤的数据

11、 选择合适的数据模板对数据做归一化处理



12、选择模板后可以对改模板的字段名称，字段英文，字段类型做筛选，默认是查该模板的全部字段

13、对模板的字段进行赋值操作

a) 选取解析字段赋值：选择的是第 5 步解析出来的数据

b) 自定义赋值：手动输入的固定值

c) 枚举映射：将日志中的枚举值做转换

1 所有的字段配置完毕后点击确定保存，即可根据配置生成 NIFI 模板(页面不可见)

3.4.3.1.2 指令对接插件

3.4.3.1.2.1 新增指令对接插件

【应用场景】

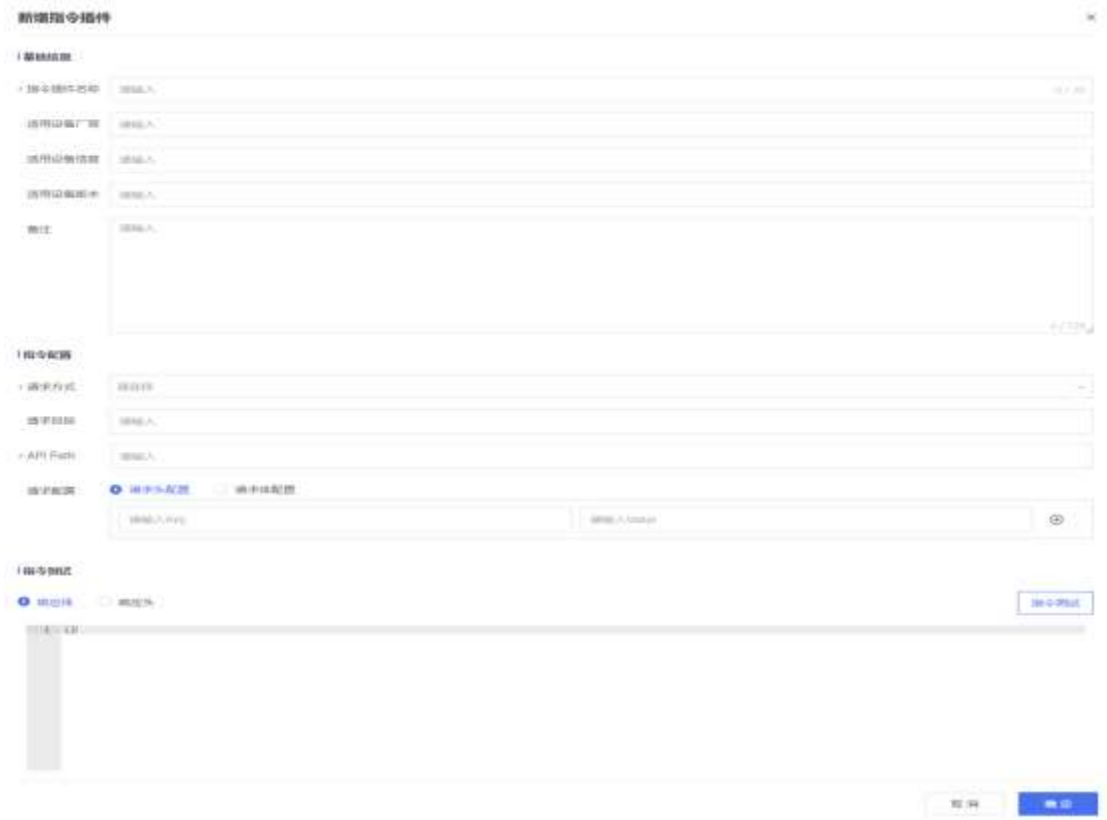
新添加一个指令对接插件。

【操作角色】

【操作步骤】

1、 点击新增指令插件按钮

2、根据列名填写信息



3.4.3.1.2.2 删除指令对接插件

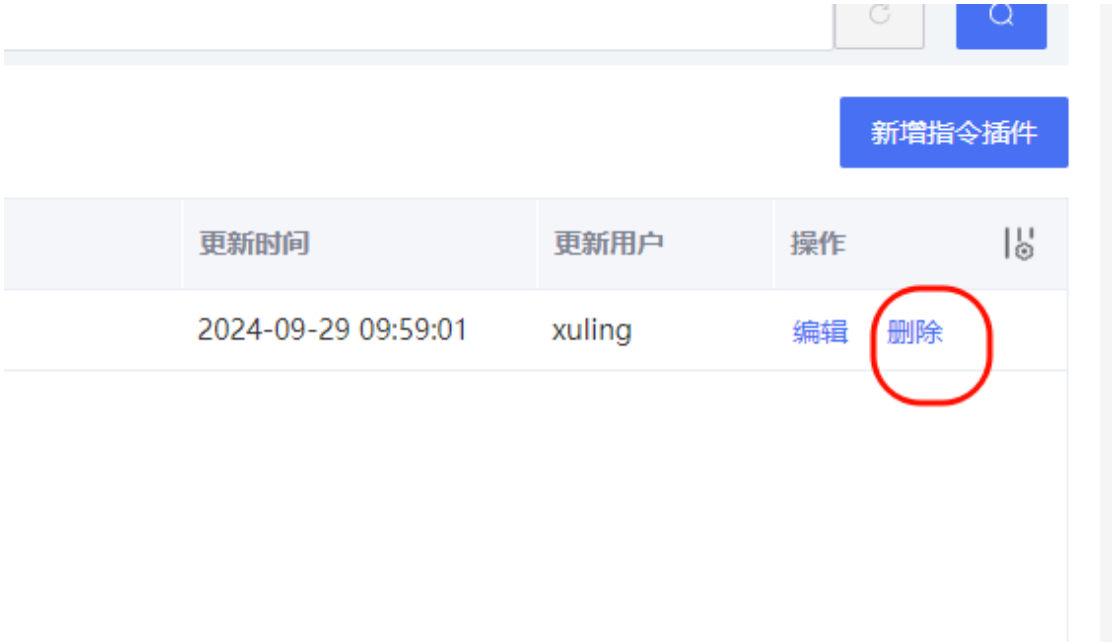
【应用场景】

删除废弃的指令对接插件。

【操作角色】

【操作步骤】

1、 点击页面删除按钮



2、被调用指令对接插件不可删除

3.4.3.1.2.3 修改指令对接插件

【应用场景】

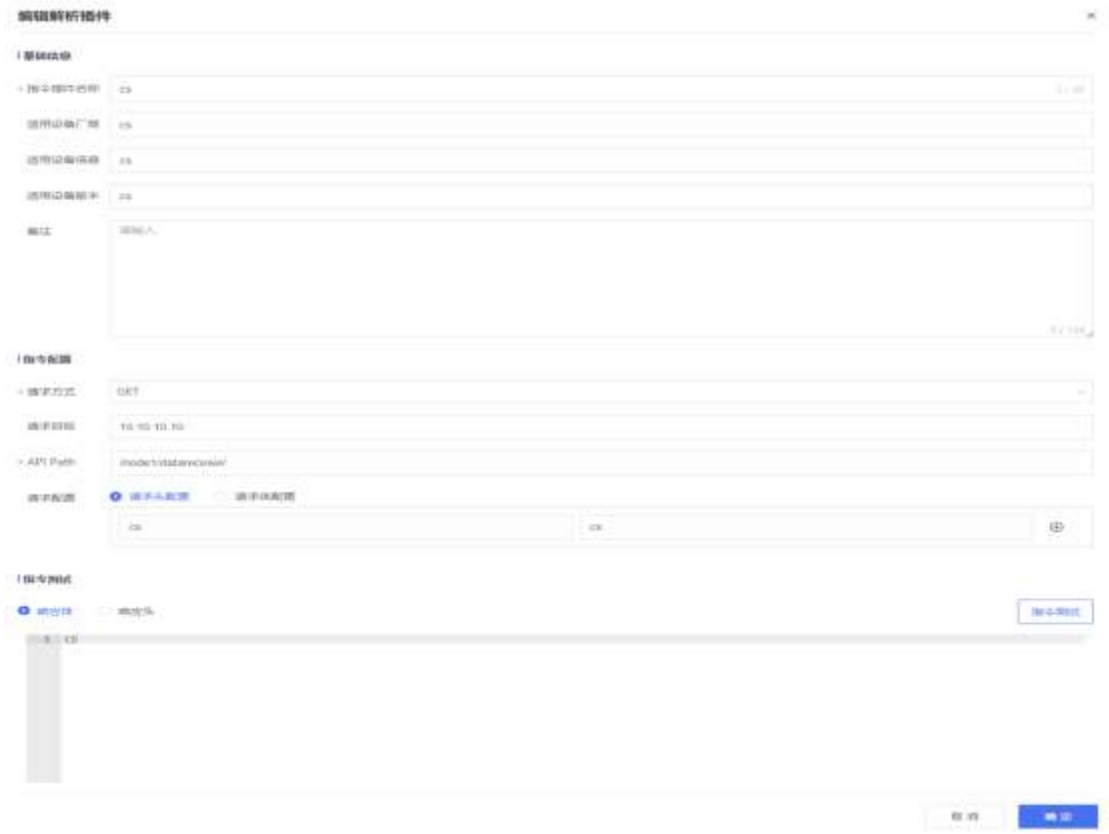
对已存在的指令对接插件做修改。

【操作角色】

【操作步骤】

1、 点击页面编辑按钮

2、修改指令对接插件内容



3.4.3.1.2.4 查询指令对接插件

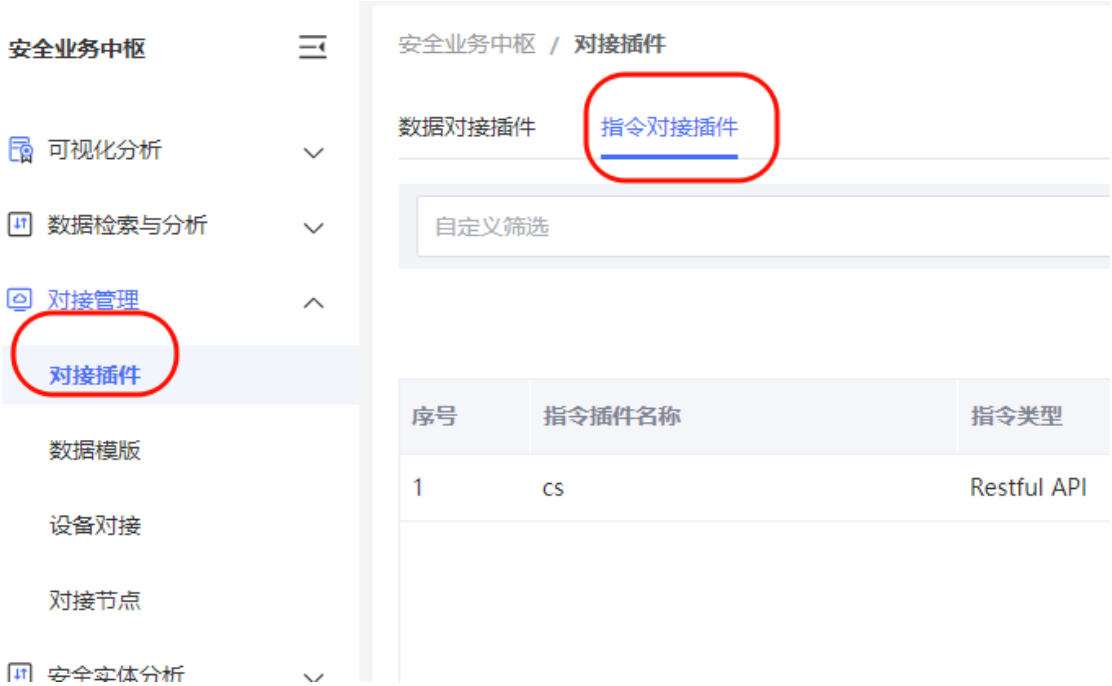
【应用场景】

检索指令对接插件，默认是全量分页检索，可以根据插件名称做模糊匹配检索。

【操作角色】

【操作步骤】

1、 点击对接插件，切换到指令对接插件 TAB 页



2、检索输入框输入插件名称模糊查询

3.4.3.2 数据模版

3.4.3.2.1 字段管理

3.4.3.2.1.1 新增字段

【应用场景】

创建数据模板字段。

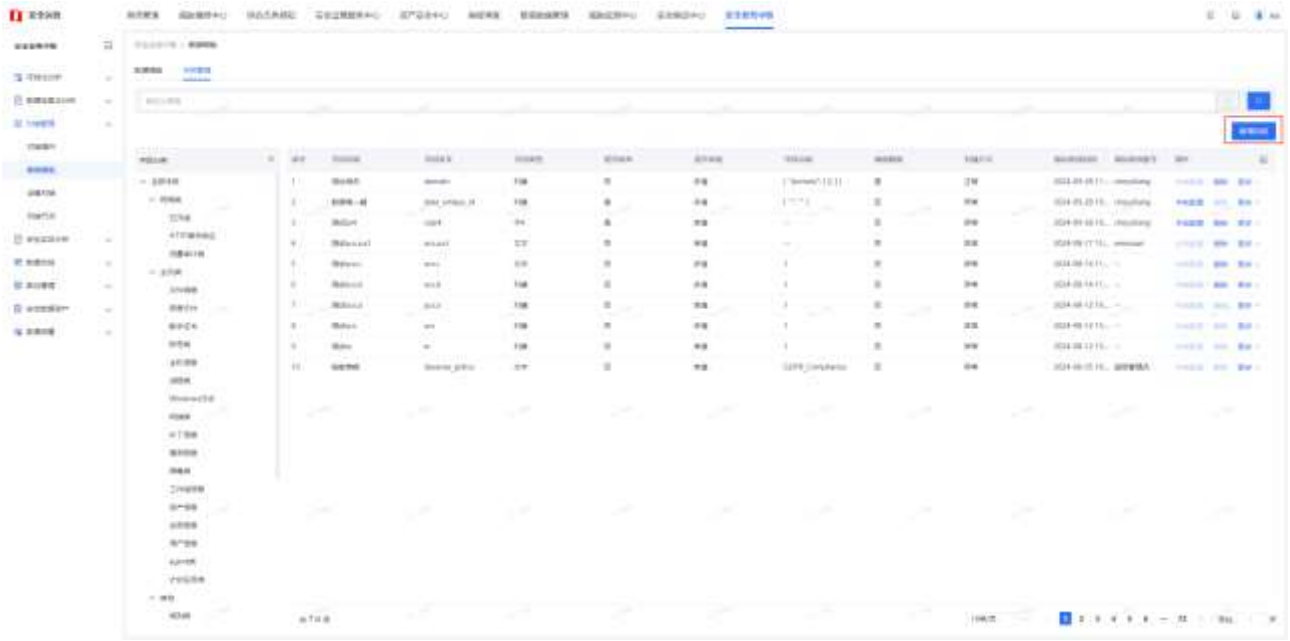
【操作角色】

1、进入字段创建界面

- 对接管理菜单下的数据模板子菜单，点击“字段管理”切换到字段管理界

面。

- 点击“新增字段”进入字段编辑界面。

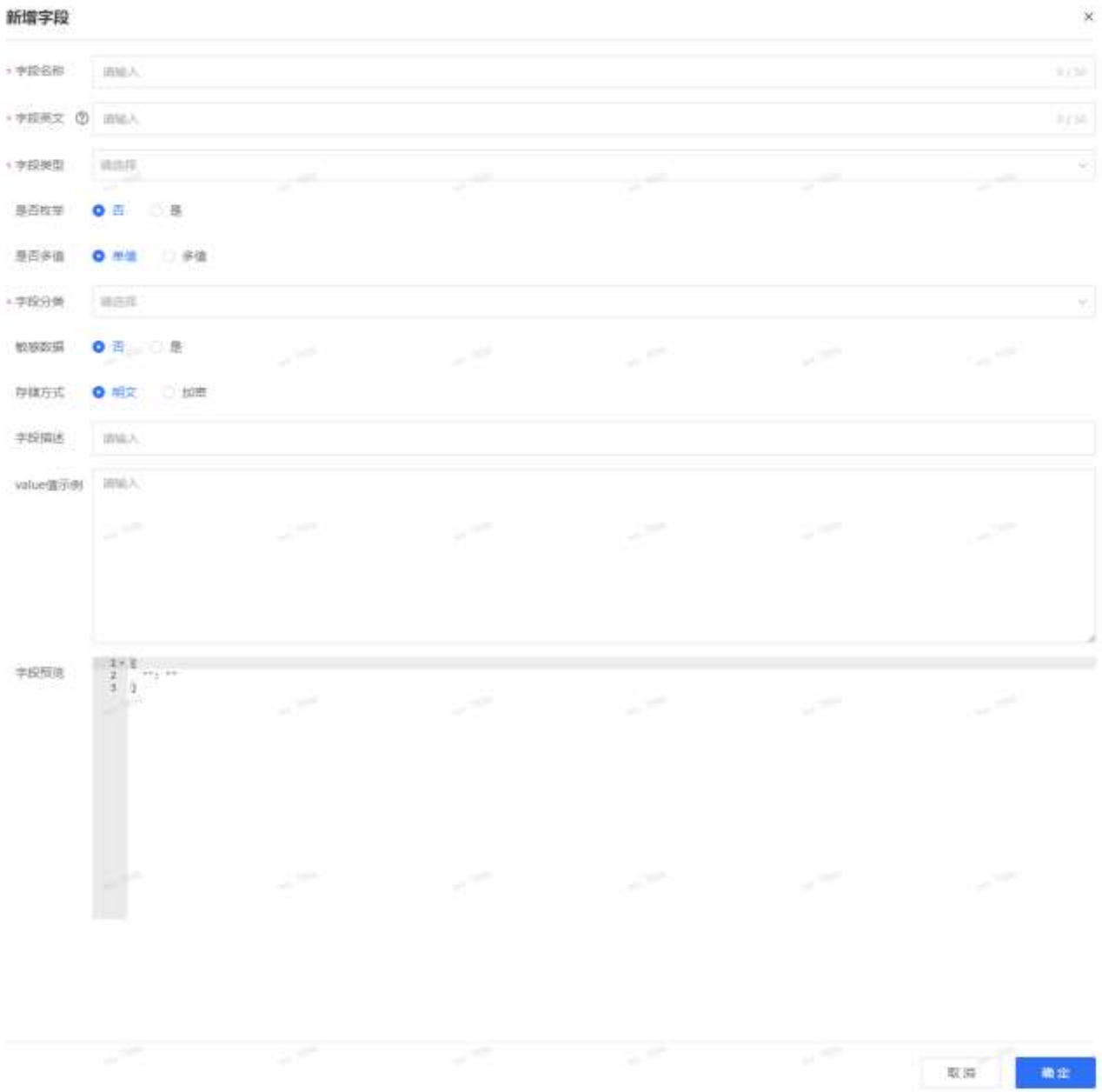


2、录入字段信息

1） 填写设备信息

- 字段名称：填写字段的中文名称。
- 字段英文：填写字段英文名称，当输入字段名.字段名时，则自动将其拆分成对象，如输入 file.name，自动拆分成{"file":{"name":""}}。
- 字段类型：选择字段类型
- 是否枚举：选择字段是否是枚举
- 是否多值：选择字段是否多值
- 字段分类：选择字段分类
- 敏感数据：选择字段是否敏感数据
- 存储方式：选择字段存储方式
- 字段描述：填写字段描述
- Value 值示例：填写字段 value 值示例

2） 点击“确定”按钮，完成字段的录入。



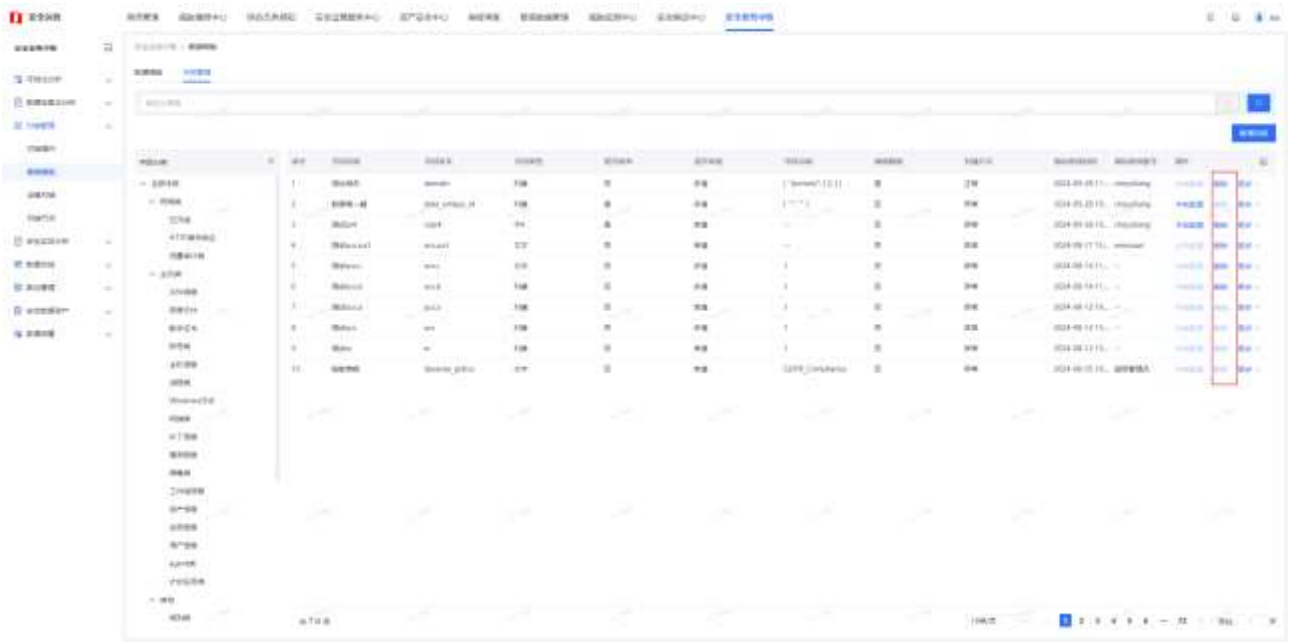
3.4.3.2.1.2 删除字段

【应用场景】

录入的字段不再需要，要进行删除。

【操作角色】

1、 如果字段添加之后，未被模板引用。点击“删除”按钮，直接删除。



2、如果字段添加之后，已被模板引用，不支持删除。

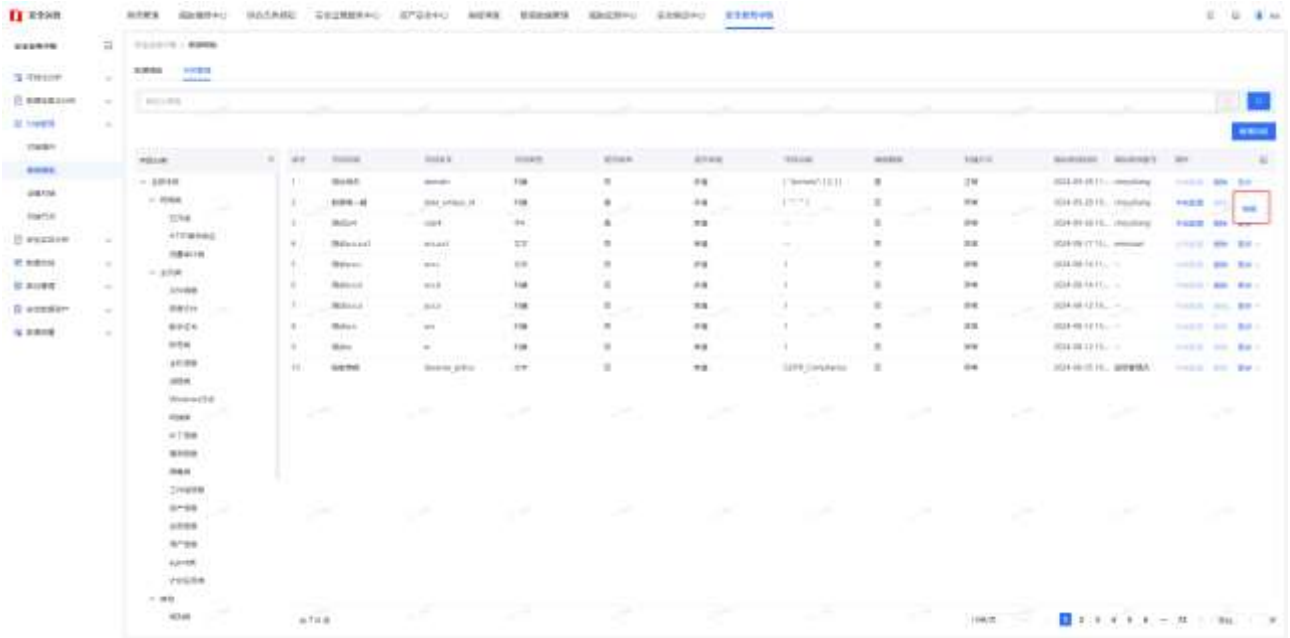
3.4.3.2.1.3 修改字段

【应用场景】

录入的字段信息，需要修改。

【操作角色】

1、 如果字段信息添加后，未被模板引用。点击“编辑”按钮，可以直接修改



2、如果字段添加之后，已被模板引用，不支持修改，只能查看。

3.4.3.2.1.4 查询字段

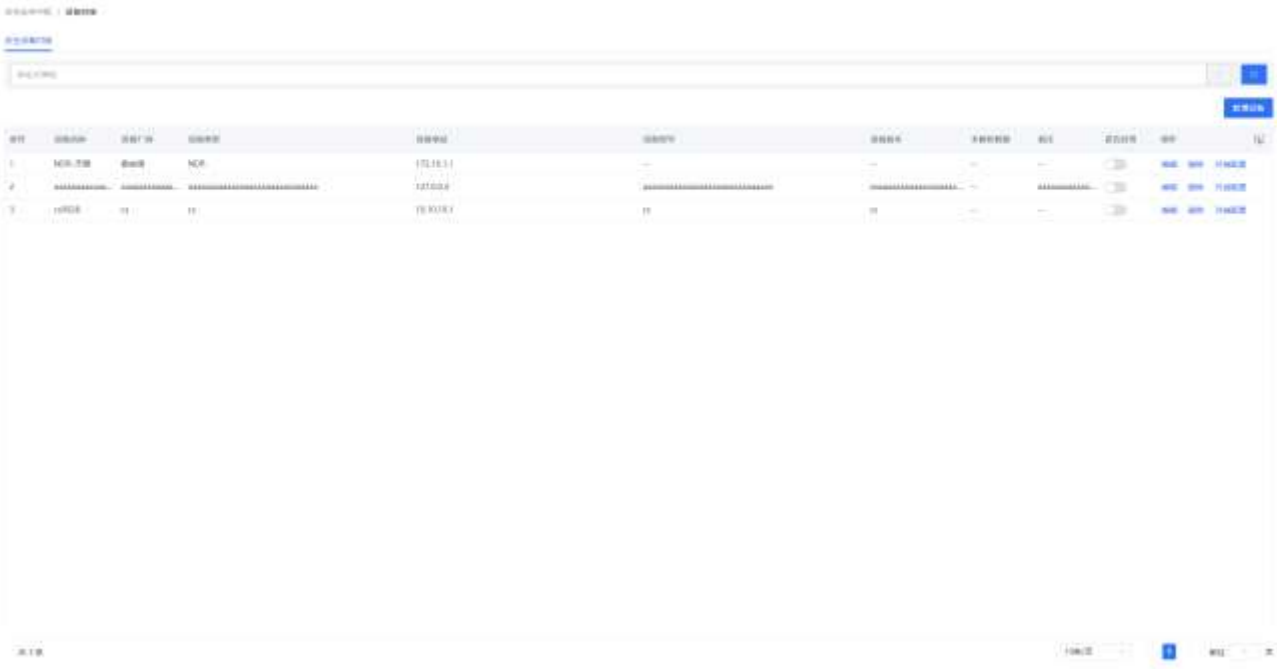
【应用场景】

查询字段信息。

【操作角色】

1、 查询列表

- 对接管理菜单下的数据模板子菜单，点击“字段管理”进入查询界面。
- 按照字段分类，展现字段名称、字段类型等数据。



3.4.3.2.1.5 新增字段分类

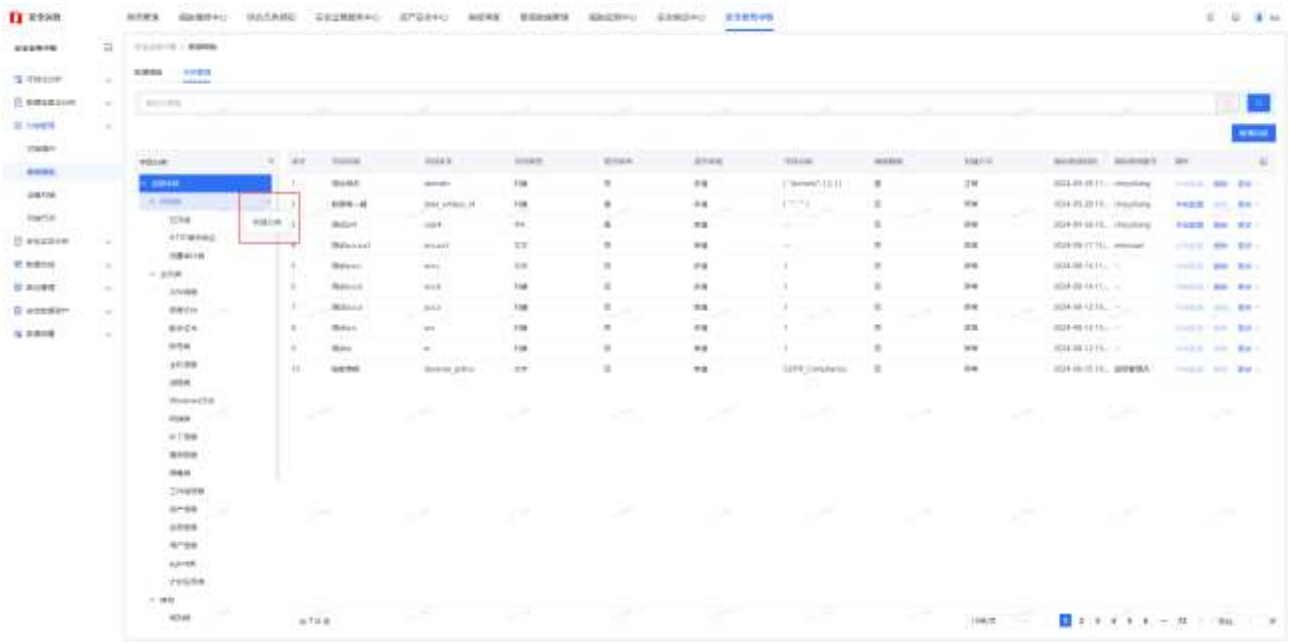
【应用场景】

创建字段分类。

【操作角色】

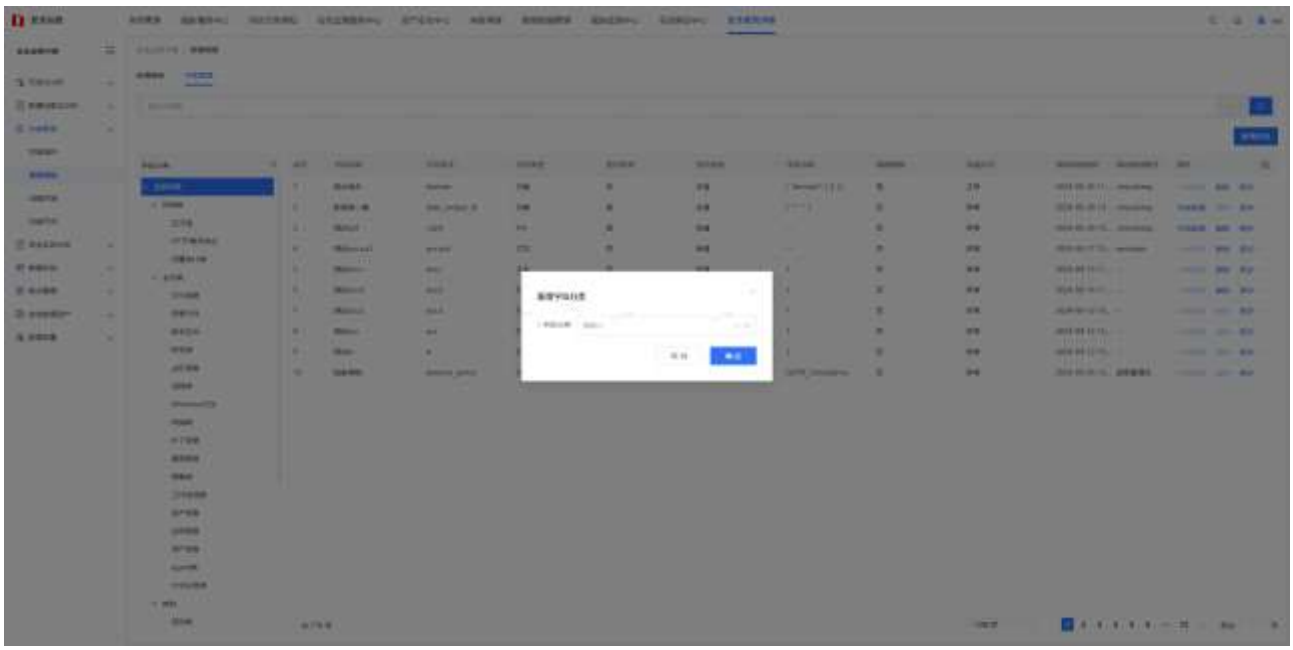
1、 字段分类展示

- 对接管理菜单下的数据模板子菜单，点击“字段管理”进入字段管理界面。
- 点击左侧字段分类下相应分类后面的“…”，在弹出的下拉列表中点击“新建分类”，进入字段分类编辑界面。



2、字段分类编辑

- 在新增字段分类界面，输入字段分类名称，点击“确定”按钮，完成字段分类的录入



3.4.3.2.1.6 内置字段查看

【应用场景】

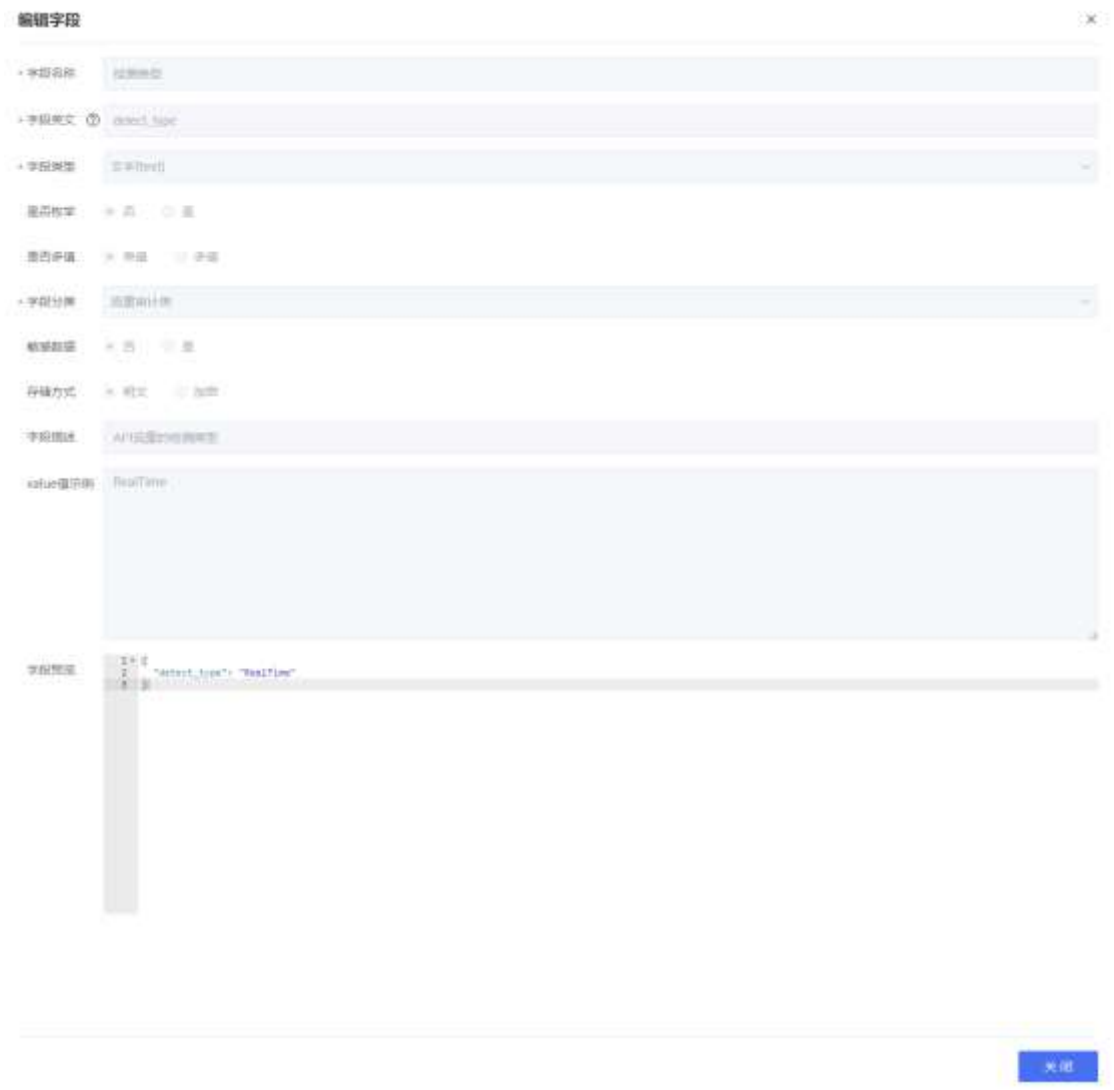
内置字段不可编辑，删除，但可以进行查看操作

【操作角色】

【操作步骤】

1、 点击更多，选择查看

2、查看内置字段配置



3.4.3.2.1.7 枚举值类型字段字典配置

同字典配置菜单

3.4.3.2.2 数据模版

3.4.3.2.2.1 新增数据模板

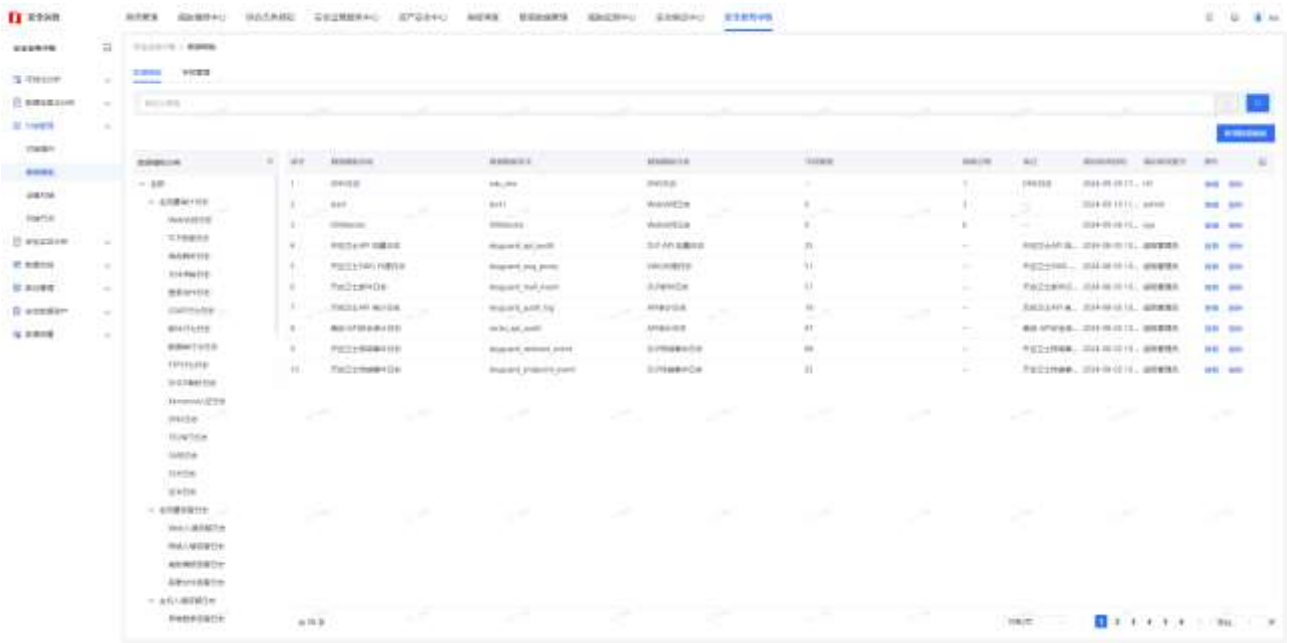
【应用场景】

创建数据模板。

【操作角色】

1、 进入数据模板创建界面

- 对接管理菜单下的数据模板子菜单，进入数据模板管理界面。
- 点击“新增数据模板”进入数据模板编辑界面。



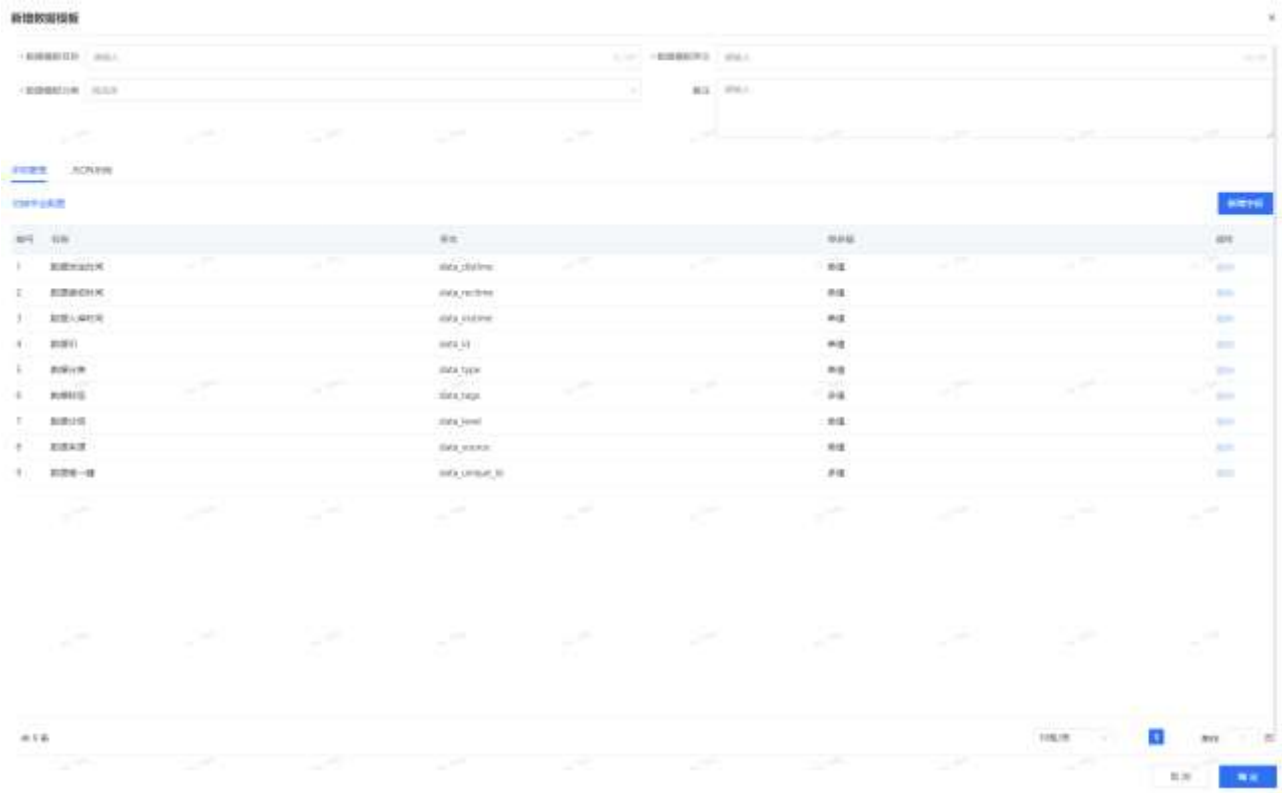
2、录入数据模板信息

1） 填写设备信息

- 数据模板名称：填写数据模板的中文名称。
- 数据模板英文：填写数据模板英文名称。
- 数据模板分类：选择数据模板分类
- 备注：填写备注

- 字段管理：选择数据模板包含的字段，内置字段不可删除，可切换至专业模式，专业模式下，可灵活根据业务场景需要创建数据模板
- JSON 示例：展示数据模板的 JSON 示例

2） 点击“确定”按钮，完成数据模板的录入。



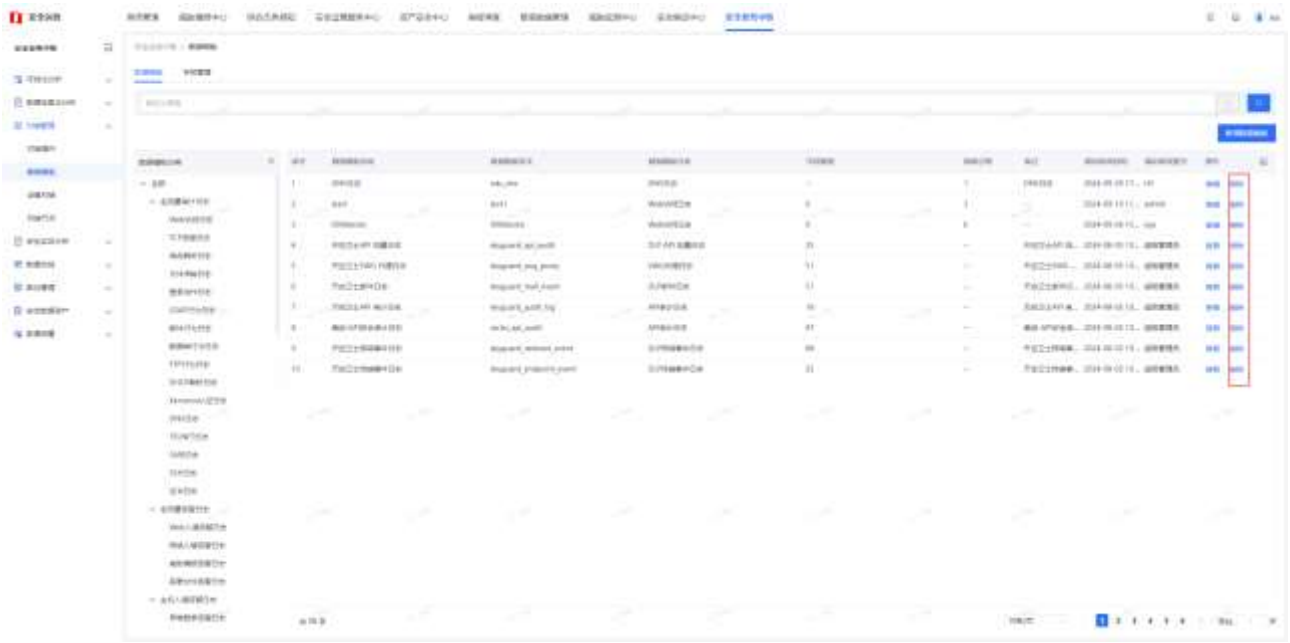
3.4.3.2.2.2 删除数据模板

【应用场景】

录入的数据模板不再需要，要进行删除。

【操作角色】

1、 如果数据模板添加之后，未被对接插件引用。点击“删除”按钮，直接删除。



2、如果数据模板添加之后，已被对接插件引用，不支持删除。

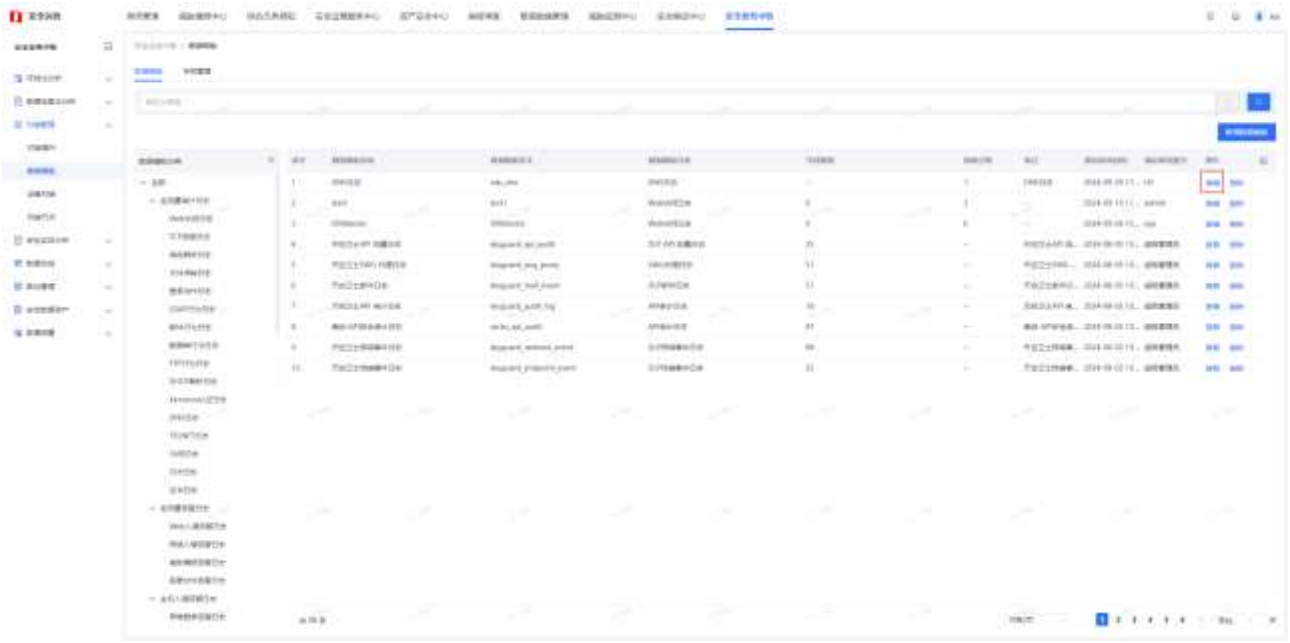
3.4.3.2.2.3 修改数据模板

【应用场景】

录入的数据模板信息，需要修改。

【操作角色】

1、 如果数据模板信息添加后，未被模板引用。点击“编辑”按钮，可以直接修改



2、如果数据模板添加之后，已被模板引用，不支持修改，只能查看。

3.4.3.2.2.4 查询数据模板

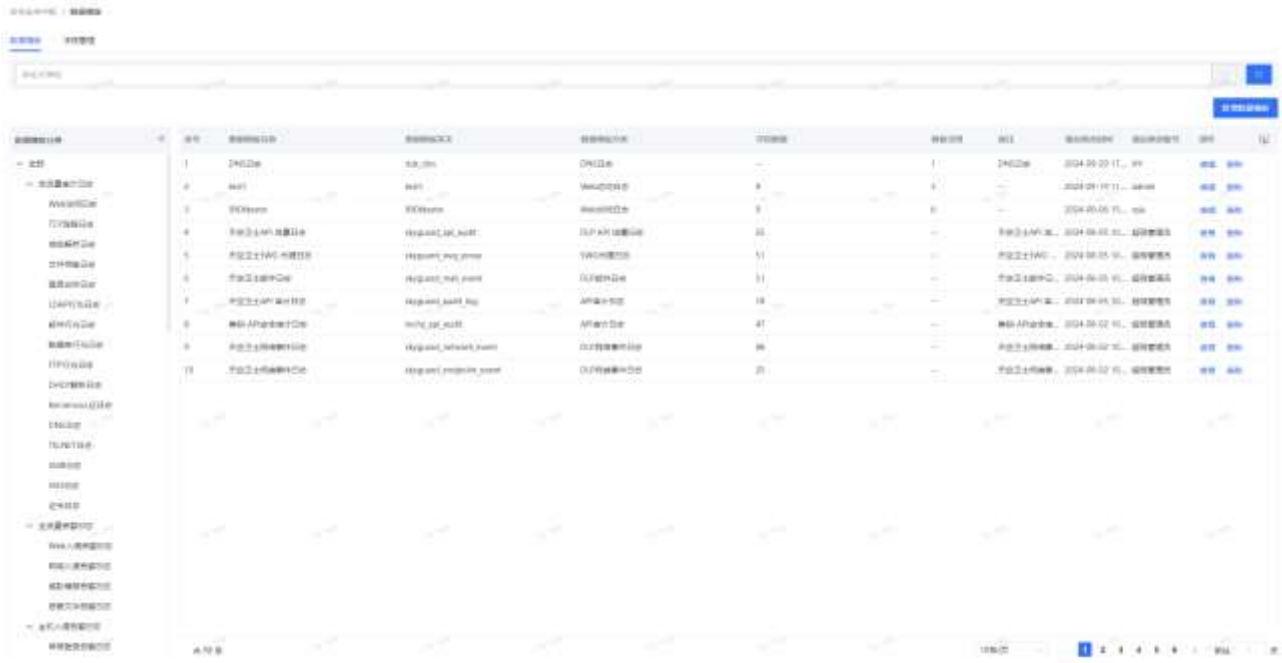
【应用场景】

查询数据模板信息。

【操作角色】

1、 查询列表

- 对接管理菜单下的数据模板子菜单进入数据模板查询界面。
- 按照数据模板分类，展现数据模板名称、数据模板分类等数据。



3.4.3.2.2.5 新增数据模板分类

【应用场景】

创建数据模板分类。

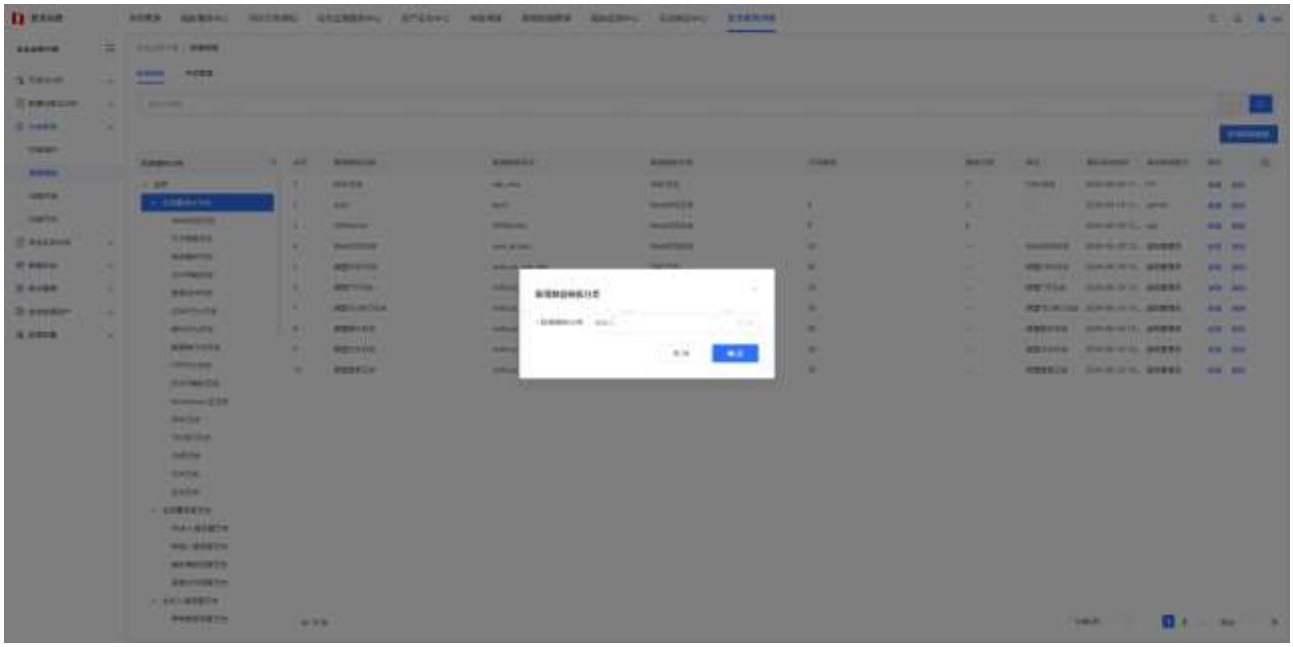
【操作角色】wx

1、 数据模板分类展示

- 对接管理菜单下的数据模板子菜单进入数据模板管理界面。
- 点击左侧数据模板分类下相应分类后面的“…”，在弹出的下拉列表中点击“新建分类”，进入数据模板分类编辑界面。

2、数据模板分类编辑

- 在新增数据模板分类界面，输入数据模板分类名称，点击“确定”按钮，完成数据模板分类的录入



3.4.3.3 设备对接

3.4.3.3.1 新增设备

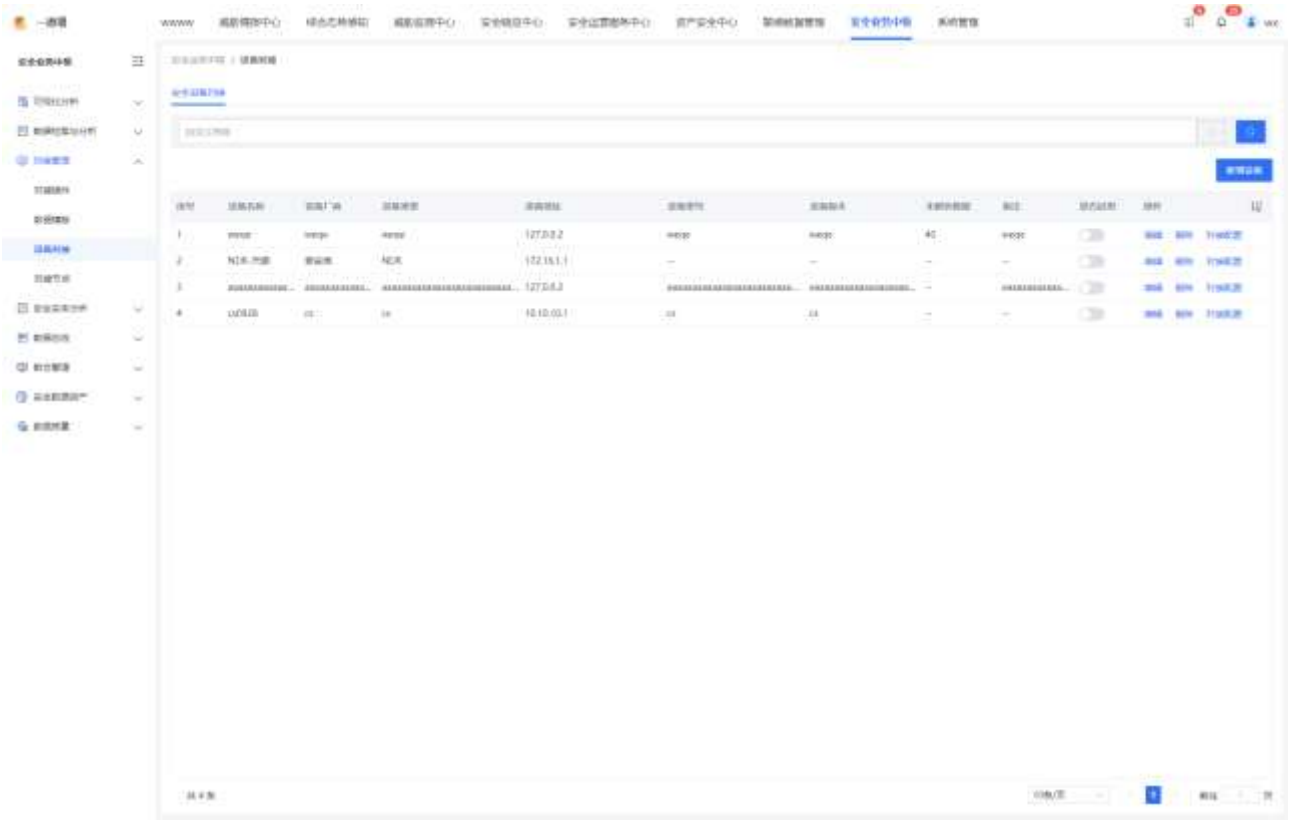
【应用场景】

对接插件和对接节点创建后，创建安全设备。

【操作角色】

1、 进入安全设备创建界面

- 对接管理菜单下的设备对接子菜单，进入查询界面。
- 点击“新增设备”进入安全设备编辑界面。



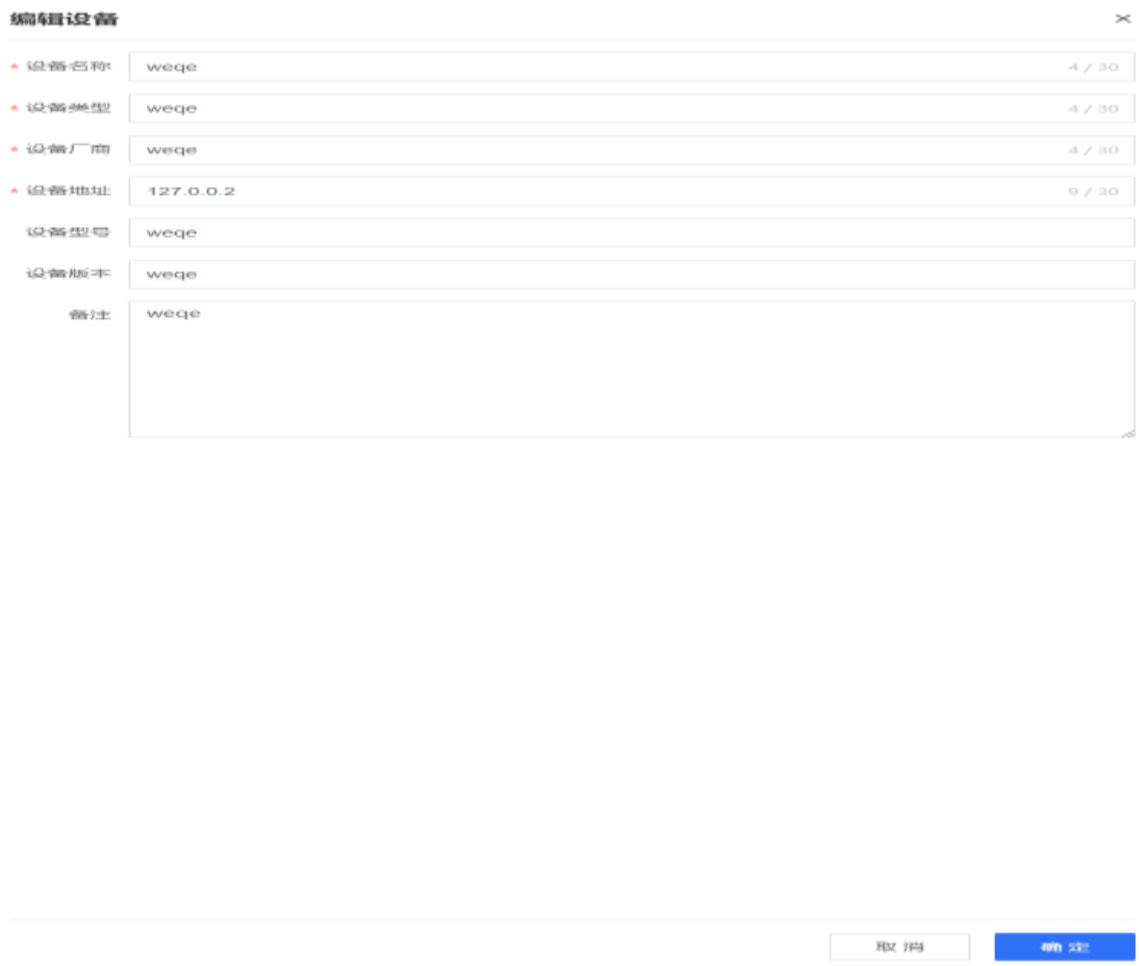
2、录入安全设备信息

1） 填写设备信息

- 设备名称：填写对应安全设备的名称。
- 设备类型：填写对应设备类型。
- 设备厂商：填写对应设备厂商
- 设备地址：填写对应设备地址

- 设备型号：填写对应设备型号
- 设备版本：填写对应设备版本
- 备注：填写备注

2） 点击“确定”按钮，完成设备的录入。



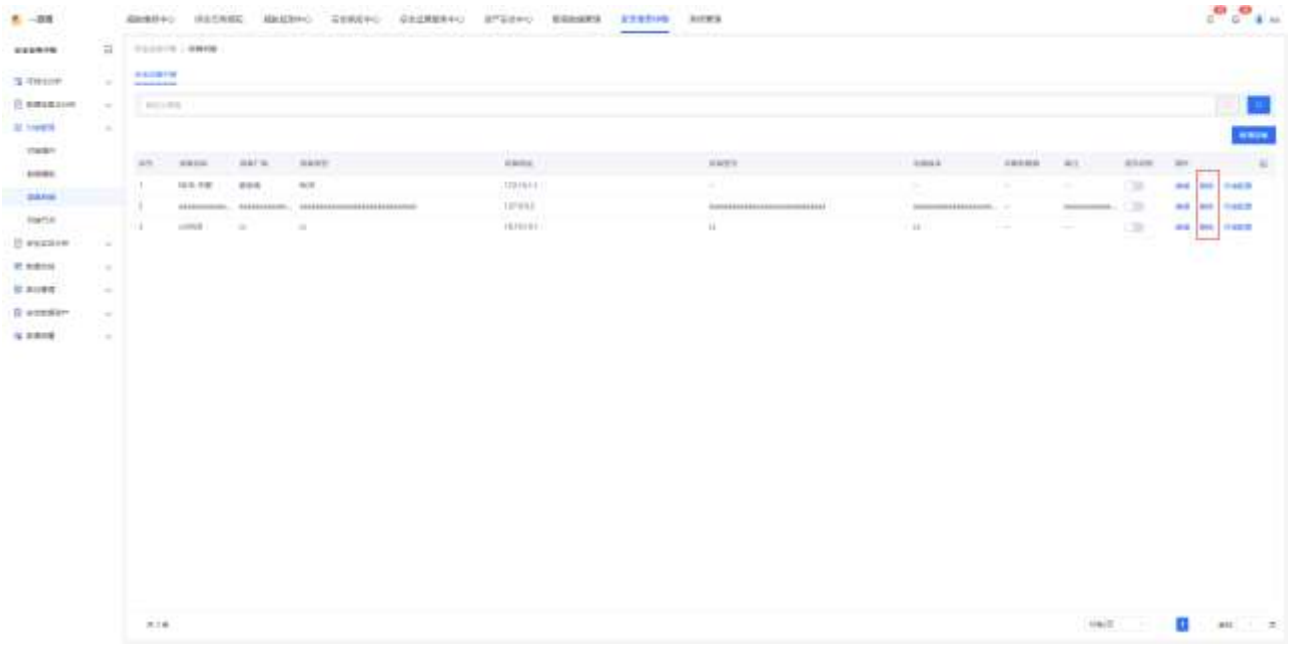
3.4.3.3.2 删除设备

【应用场景】

录入的设备不再需要，要进行删除。

【操作角色】

1、 如果设备添加之后，未启用设备。点击“删除”按钮，直接删除。



2、如果设备添加之后，已启用设备，不支持删除。

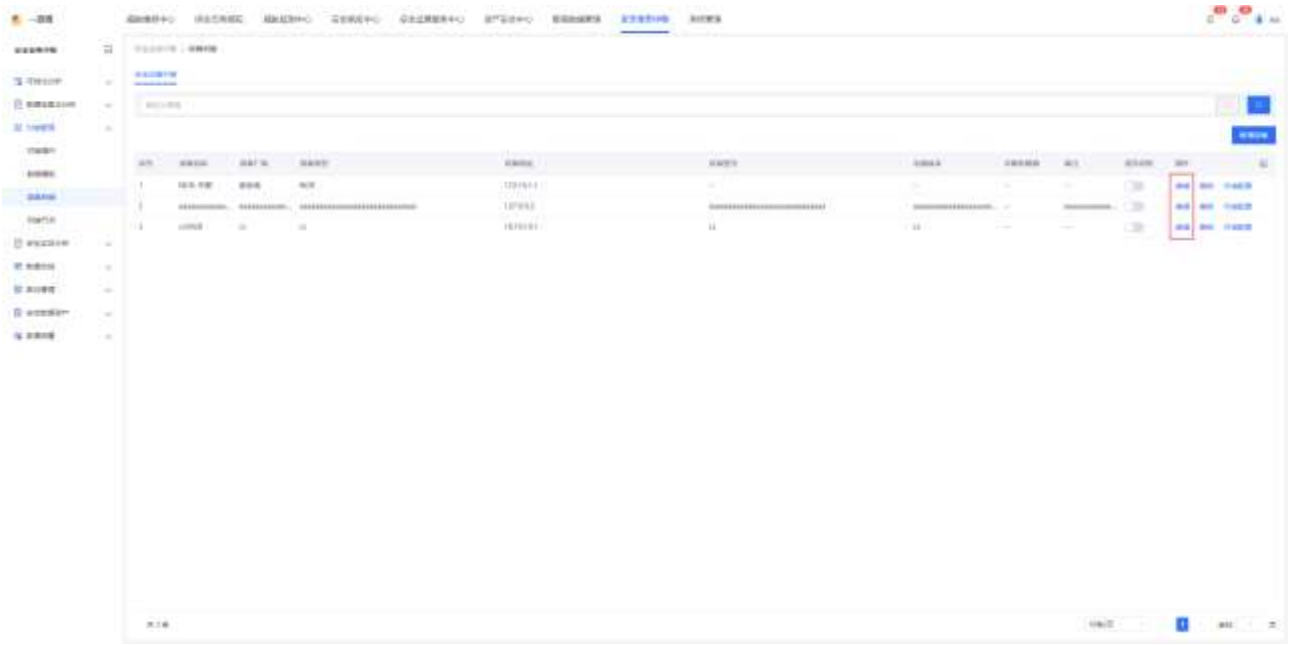
3.4.3.3.3 修改设备

【应用场景】

录入的安全设备信息，需要修改。

【操作角色】

1、 如果安全设备信息添加后，未启用。点击“编辑”按钮，可以直接修改



2、如果设备添加之后，已启用设备，不支持修改。

3.4.3.3.4 查询设备

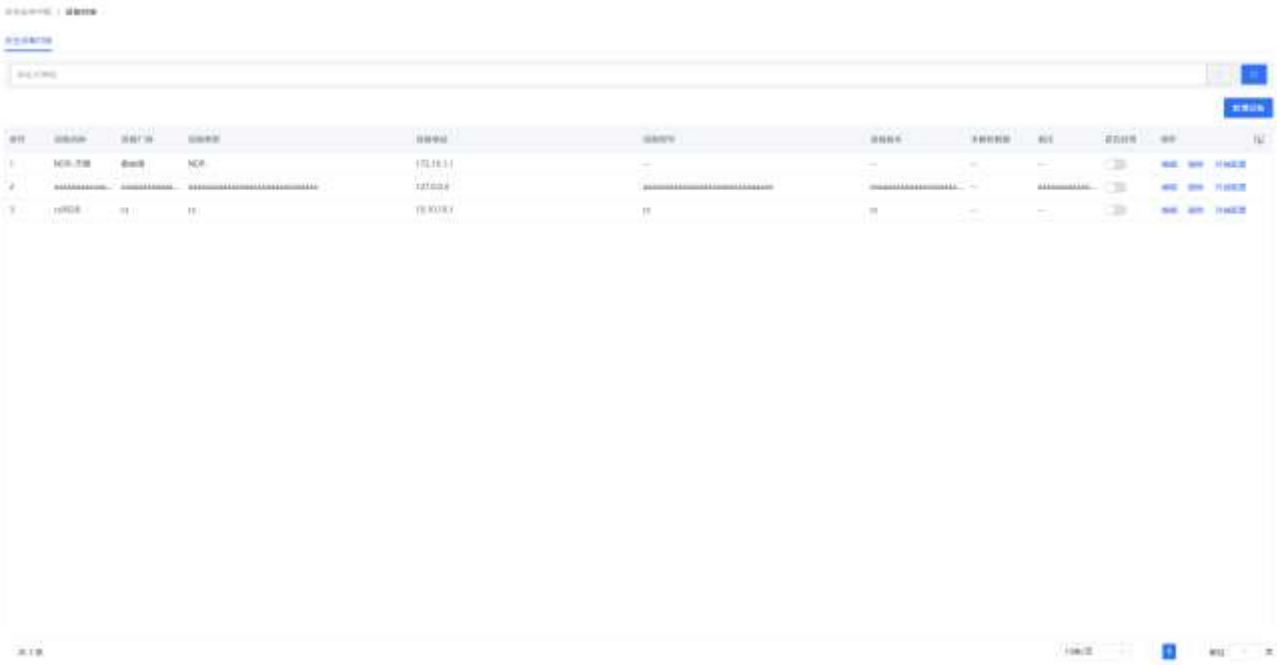
【应用场景】

查询安全设备信息。

【操作角色】

1、 查询列表

- 对接管理菜单下的设备对接子菜单，进入查询界面。
- 按照设备名称，展现设备名称、设备厂商等数据。



3.4.3.3.5 启用/关闭设备

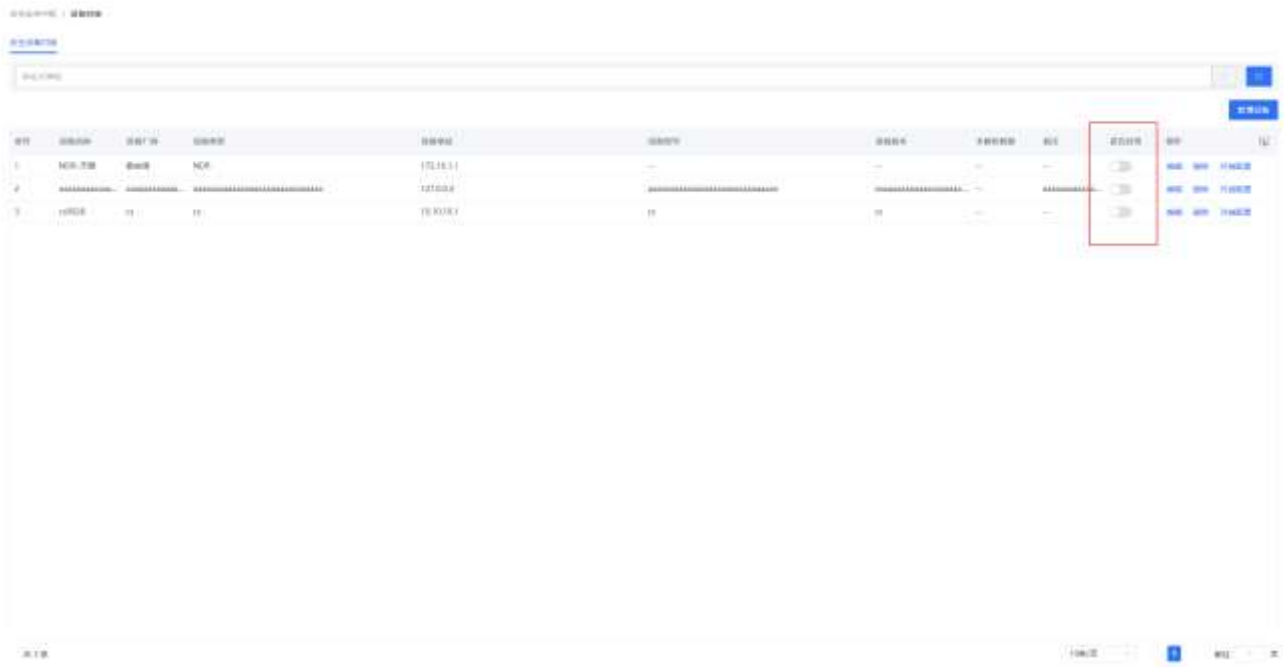
【应用场景】

启用/关闭安全设备。

【操作角色】

1、 启用/关闭

- 对接管理菜单下的设备对接子菜单，进入查询界面。
- 点击设备后面的滑动按钮对安全设备进行启动/关闭操作。



3.4.3.3.6 新增数据对接

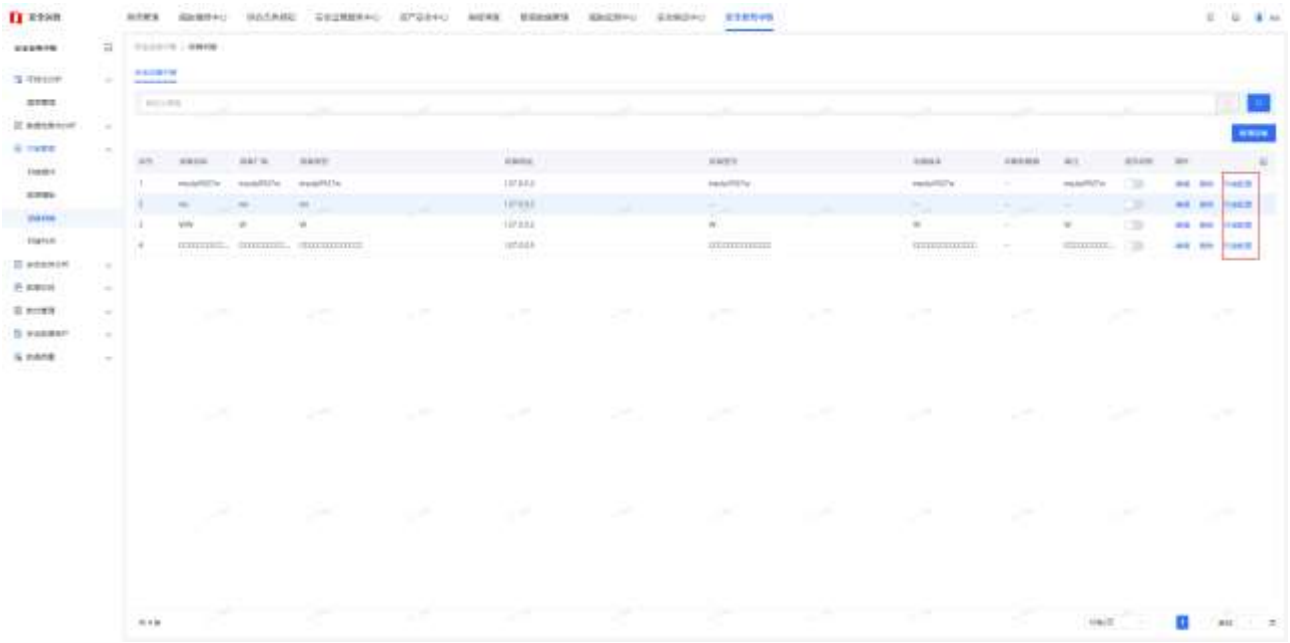
【应用场景】

设备创建完成后，创建数据对接。

【操作角色】

1、 查询设备

- 对接管理菜单下的设备对接子菜单，进入查询界面。
- 选择相应的设备，点击“对接配置”按钮，进入对接配置列表界面。



2、对接配置

在对接配置列表界面，点击“新增数据对接”进入数据对接编辑界面

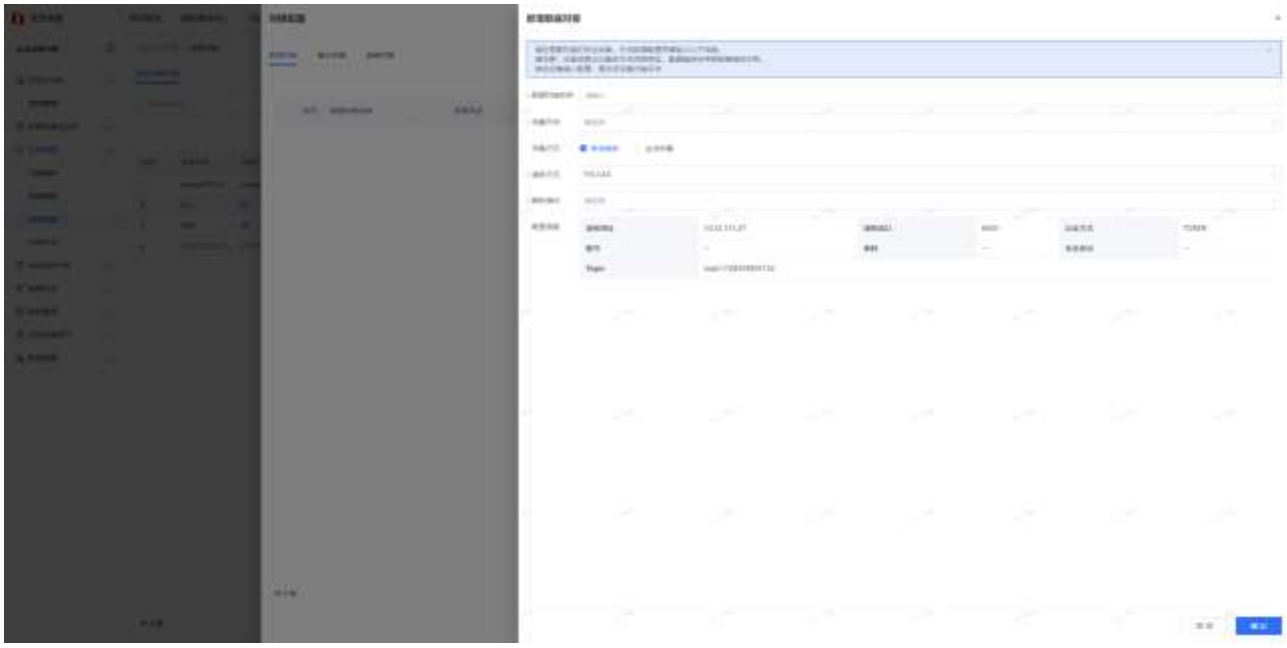
3、编辑数据对接

1） 填写设备对接信息

- 数据对接名称：填写数据对接的名称。
- 采集节点：选择对接节点。
- 采集方式：选择采集方式。
- 接收方式：选择数据接收方式。

- 解析插件：选择数据解析插件。
- 配置信息：数据接收的配置信息，当采集方式为被动接收时，配置信息为默认的接收地址，当采集方式为主动采集时，需按照接收方式配置相应的中间件地址等。

2） 点击“确定”按钮，完成设备对接的录入。



3.4.3.3.7 修改数据对接

【应用场景】录入的数据对接，需要修改。

【操作角色】

1、如果数据对接添加后，未启用。点击“编辑”按钮，可以直接修改

2、如果数据对接添加之后，已启用，不支持修改。

3.4.3.3.8 删除数据对接

【应用场景】录入的数据对接不再需要，要进行删除。

【操作角色】

1、 如果数据对接添加之后，未启用。点击“删除”按钮，直接删除。

如果数据对接添加之后，已启用，不支持删除。

3.4.3.3.9 启用/关闭数据对接

【应用场景】

启用/关闭数据对接。

【操作角色】wx

1、启用/关闭

- 对接管理菜单下的设备对接子菜单，进入查询界面。
- 选择相应的设备，点击“对接配置”按钮，进入对接配置列表界面。
- 点击数据对接后面的滑动按钮对数据对接进行启动/关闭操作。

3.4.3.3.10 未解析数据处理

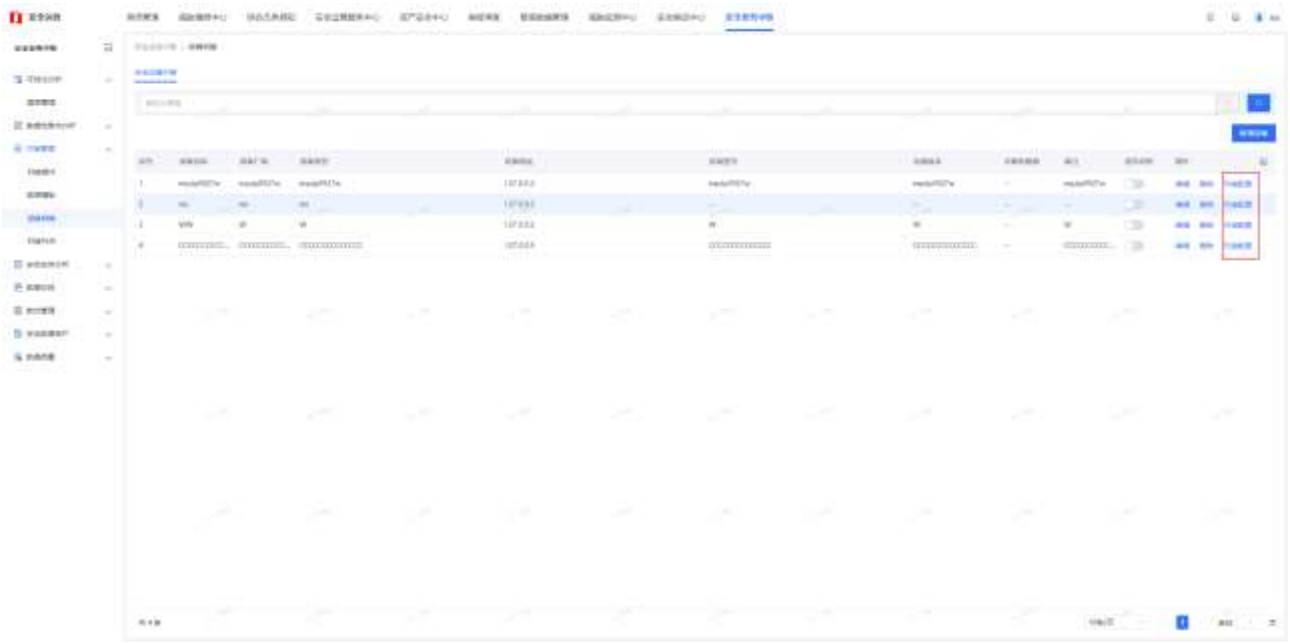
【应用场景】

查询安全设备信息。

【操作角色】

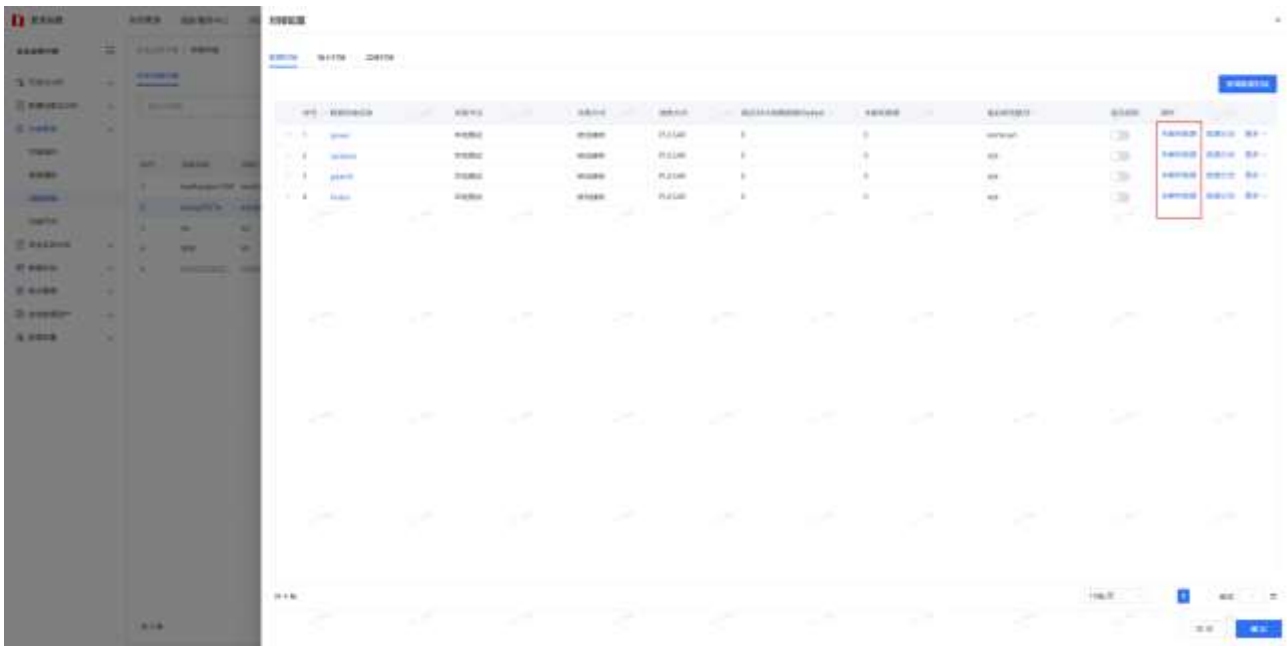
2、查询列表

- 对接管理菜单下的设备对接子菜单，进入查询界面。
- 选择相应的设备，点击“对接配置”按钮，进入对接配置列表界面。



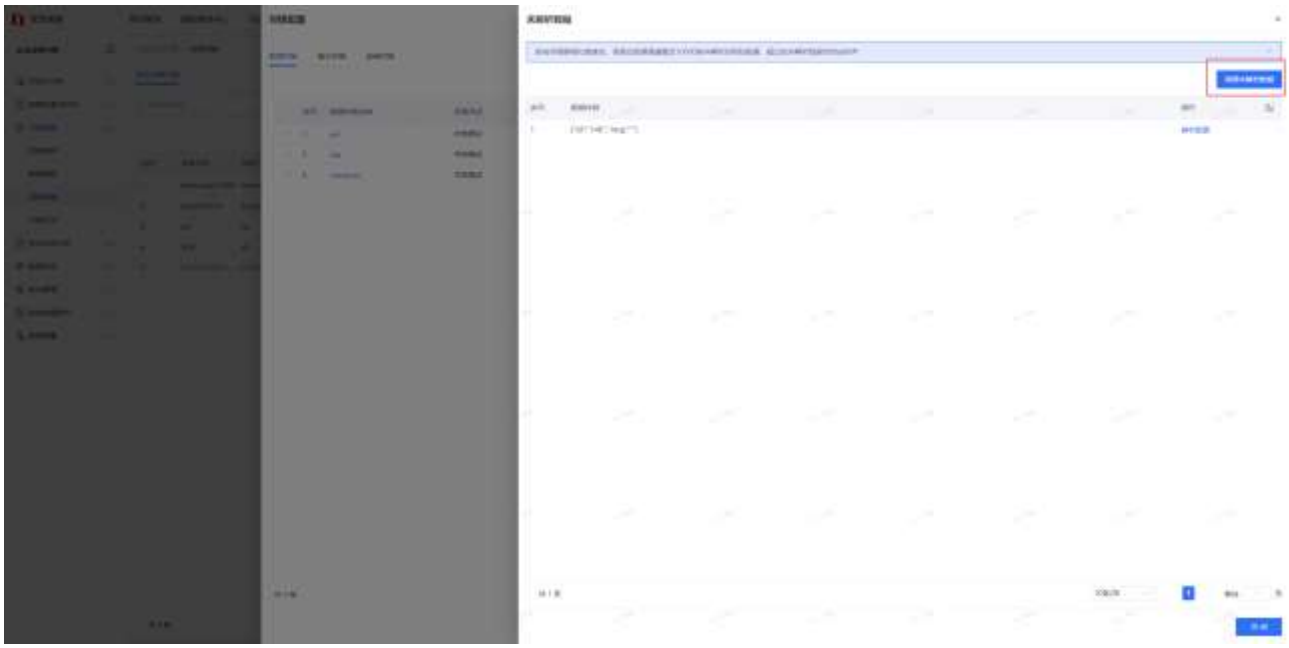
3、 对接配置

- 在对接配置列表界面，选择相应的数据对接，点击“未解析数据”按钮，进入未解析数据处理界面

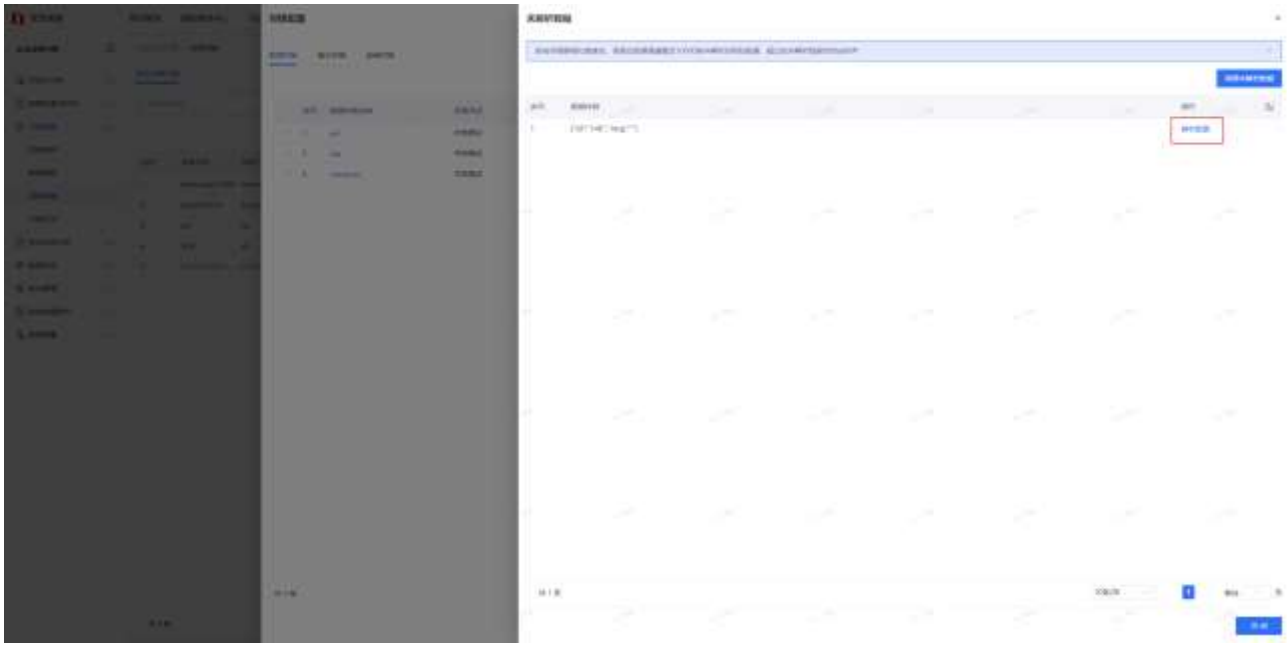


4、 未解析数据处理

- 在未解析数据处理界面，点击“清理未解析数据”按钮，可将未解析数据进行清理



- 点击“解析配置”按钮可对未解析数据重新配置



3.4.3.3.11 新增数据分发任务

【应用场景】

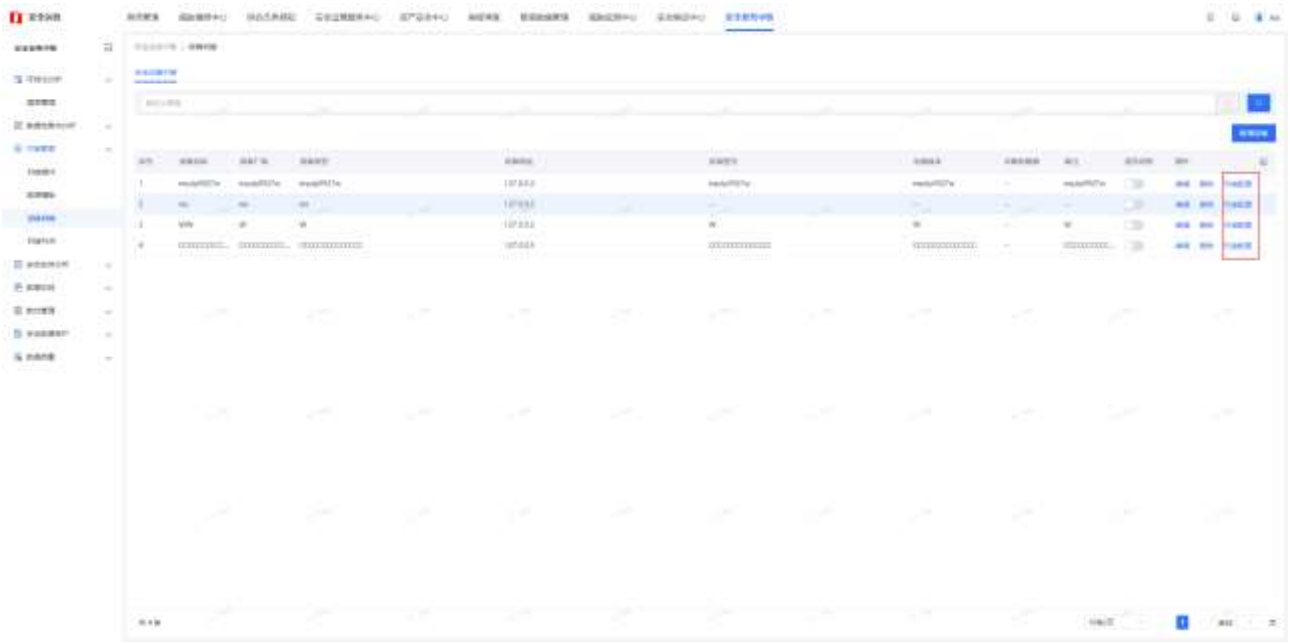
设备创建完成后，创建数据对接。

【操作角色】wx

1、查询设备

- 对接管理菜单下的设备对接子菜单，进入查询界面。

- 选择相应的设备，点击“对接配置”按钮，进入对接配置列表界面。

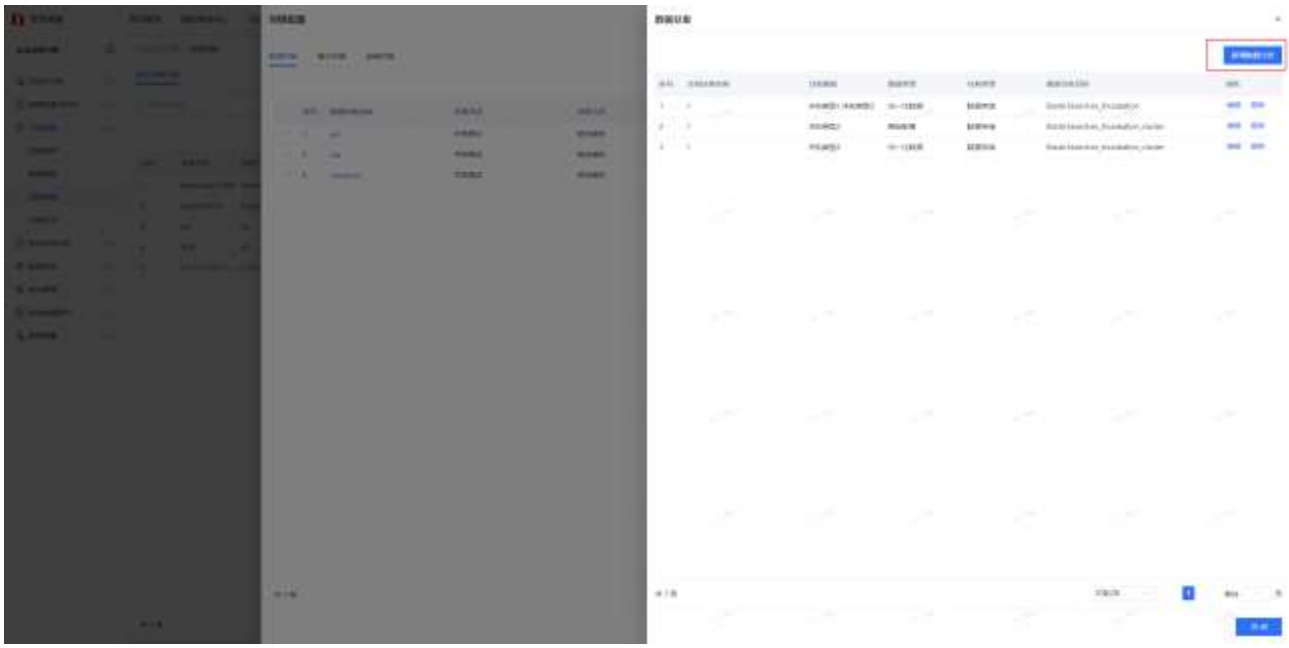


2、对接配置

- 在对接配置列表界面，点击“数据分发”进入数据分发任务列表界面

3、数据分发配置

- 在数据分发任务列表界面，点击“新增数据分发”按钮进入数据分发任务编辑界面

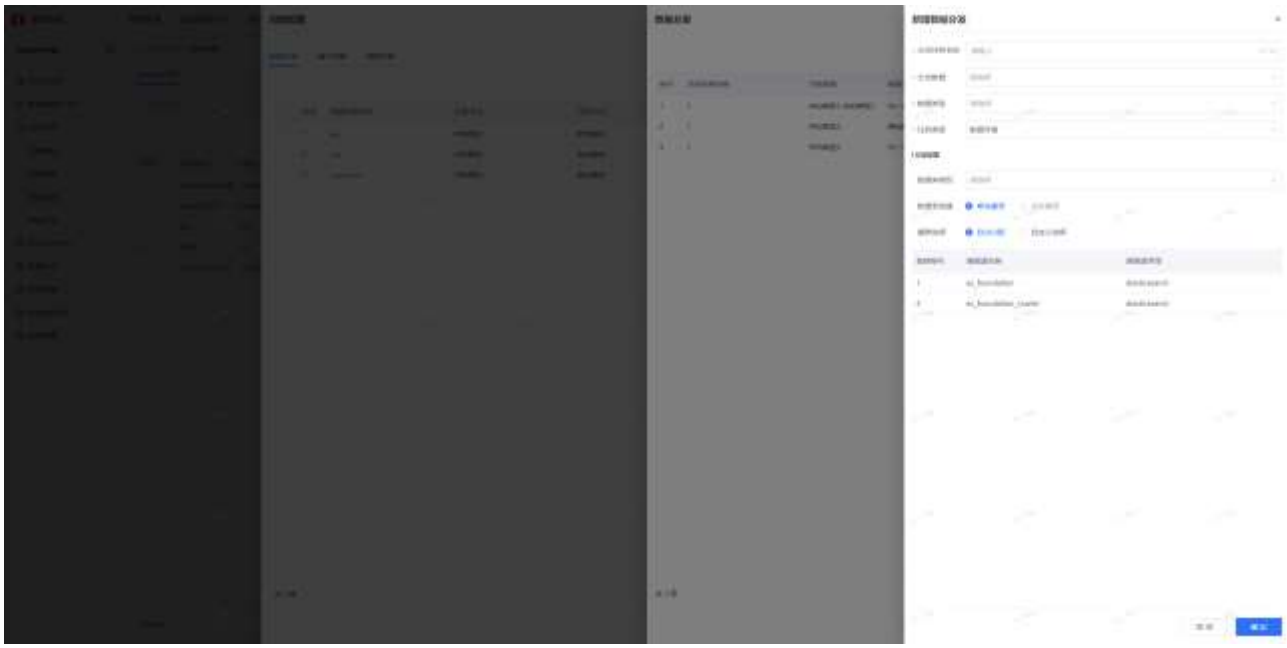


4、编辑数据分发任务

1） 填写数据分发任务信息

- 分发任务名称：填写数据分发任务的名称。
- 分发数据：选择该任务处理的数据。
- 数据类型：选择该任务处理的数据类型。
- 任务类型：选择该任务的类型，包括数据存储和数据转发。
- 任务配置：数据分发任务的配置信息，当任务类型为数据存储时，配置信息为默认的 elasticsearch 数据库，可选择指定或自动分配数据源，当任务类型为数据转发时，若转发方式为被动发送，配置信息为默认的 PULSAR 接收地址，若转发方式为被动发送，需配置对应的 kafka 地址等信息。

2） 点击“确定”按钮，完成数据分发任务的录入。

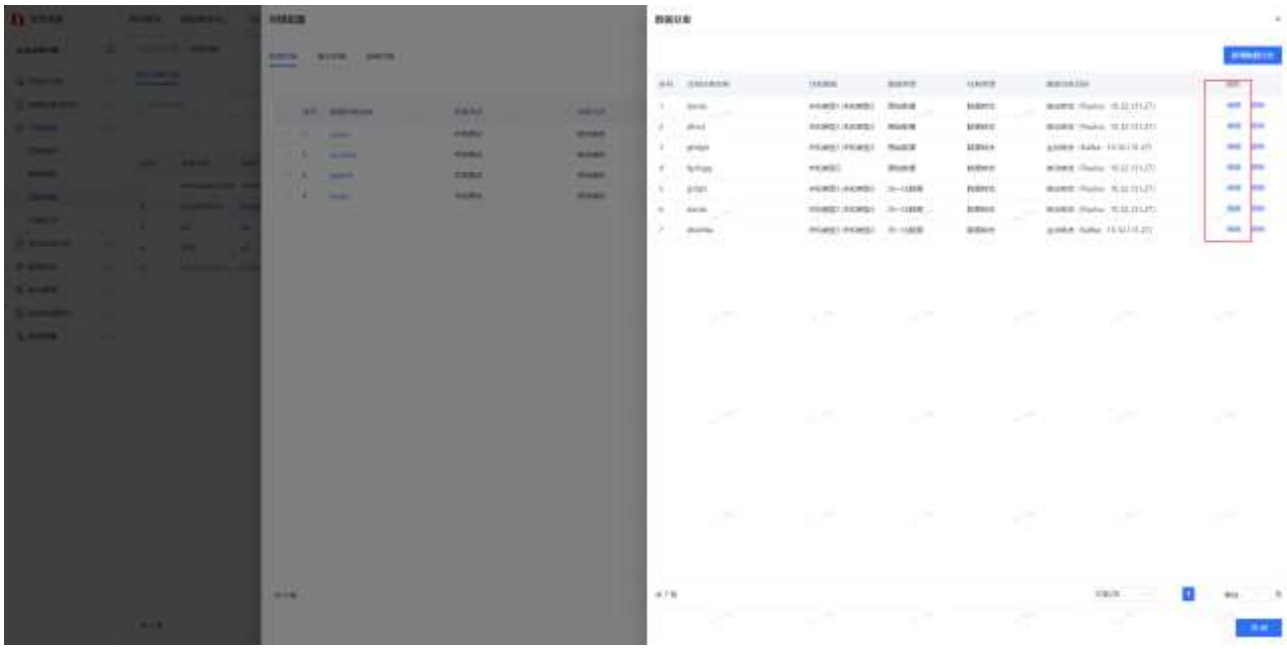


3.4.3.3.12 修改数据分发任务

【应用场景】录入的数据分发任务，需要修改。

【操作角色】wx

1、如果数据分发任务添加后，点击“编辑”按钮，可以直接修改

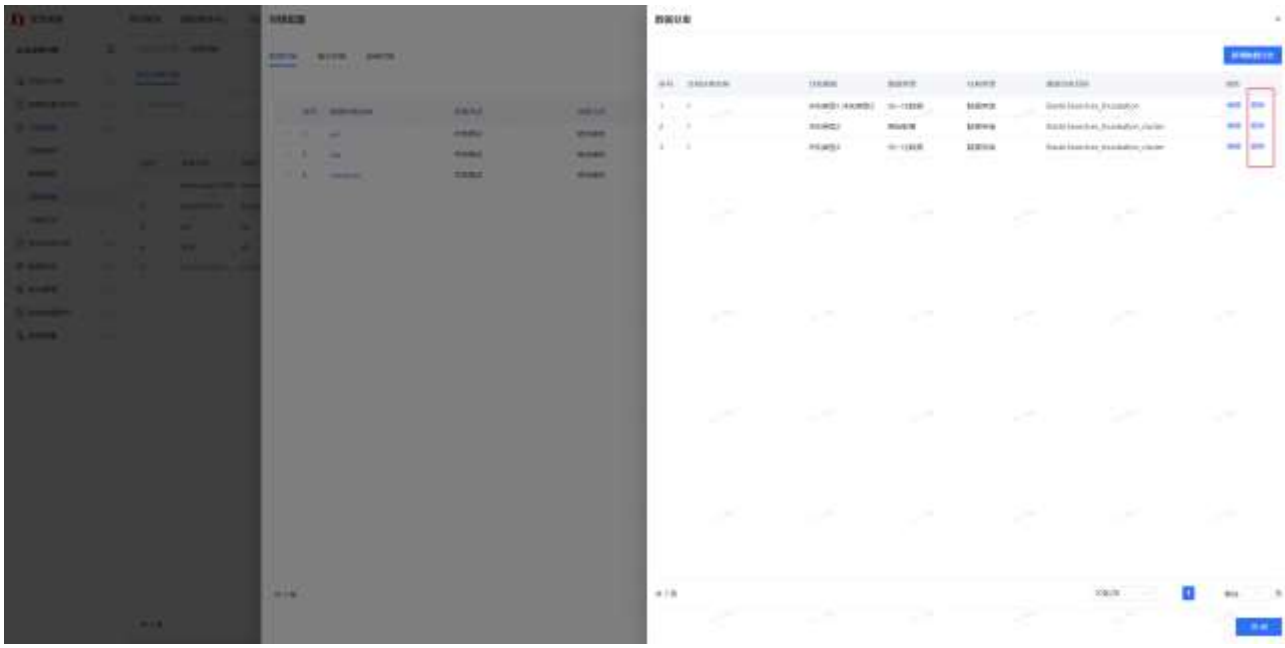


3.4.3.3.13 删除数据分发任务

【应用场景】录入的数据分发任务不再需要，要进行删除。

【操作角色】

1、数据分发任务添加之后，点击“删除”按钮，直接删除。



3.4.3.4 对接节点

3.4.3.4.1 新增对接节点

【应用场景】

在对接节点中新增对接节点信息。

【操作角色】系统自动

1、进入安全业务中枢对接节点界面

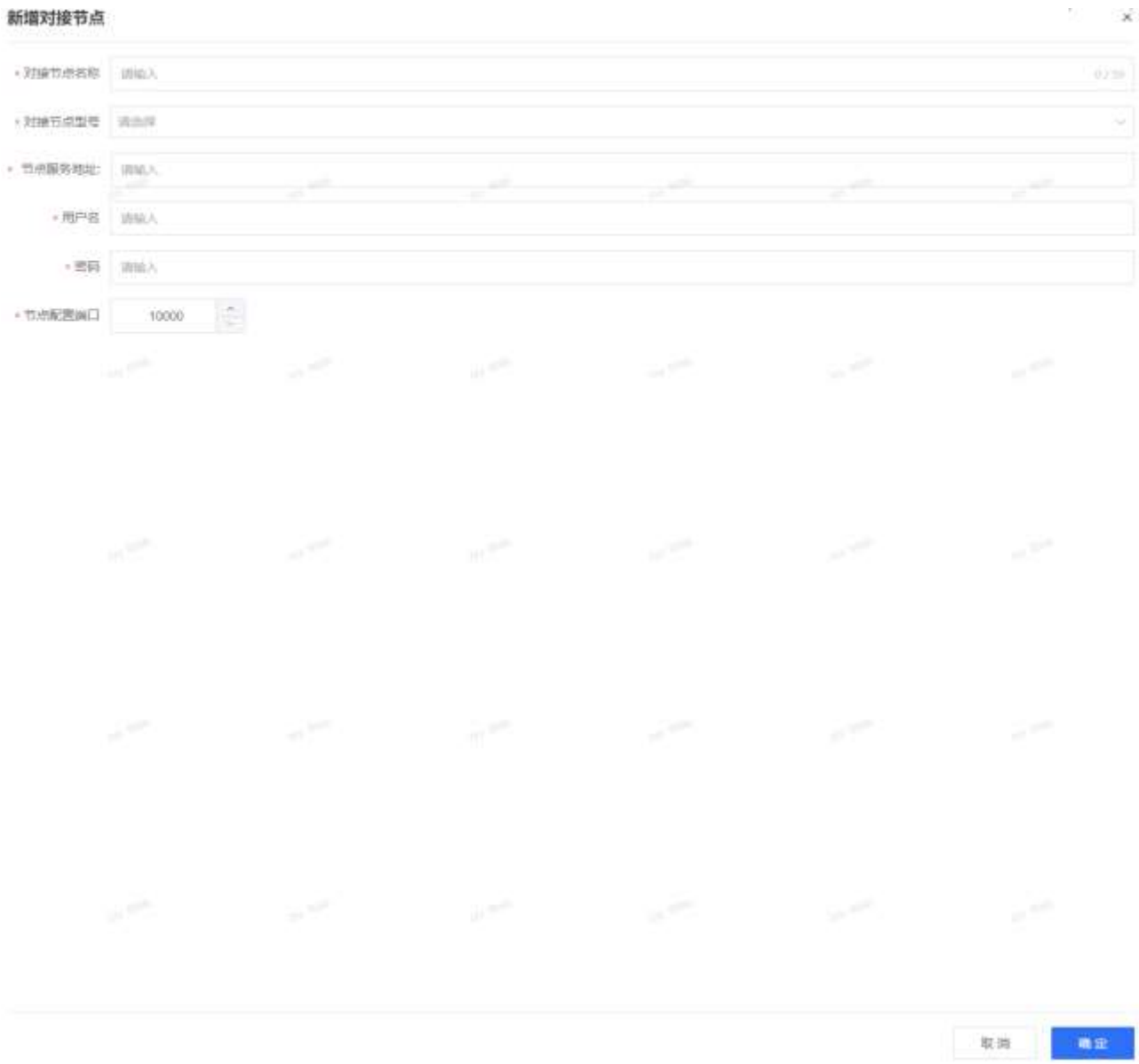
- 对接节点菜单，进入查询界面。
- 点击“新增”进入对接节点编辑界面。

2、录入对接节点

3） 填写节点信息

- 对接节点名称：填写对接节点名称。
- 对接节点型号：选择对接节点型号。
- 节点服务地址：填写节点服务地址。
- 用户名：填写用户名。
- 密码：填写密码。
- 节点配置端口：填写节点配置端口。

4） 点击“确定”按钮，完成对接节点的录入。



5） 点击“确定”按钮，完成对接节点的录入。

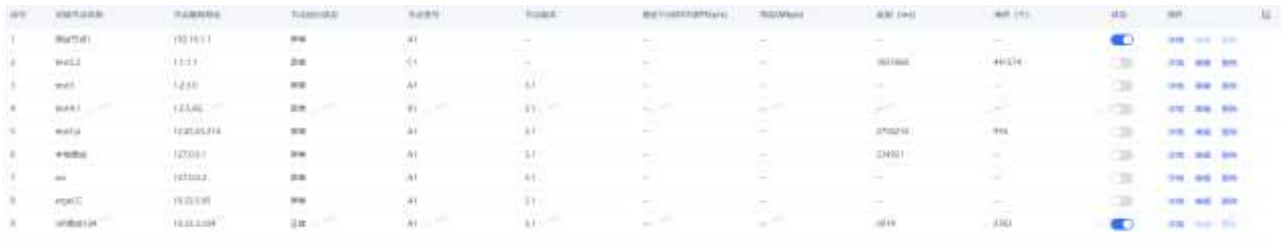
3.4.3.4.2 删除稽查问题

【应用场景】

录入的对接节点不再需要，要进行删除。

【操作角色】系统自动

1、 如果对接节点记录之后，状态未启用。点击“删除”按钮，直接删除。



2、如果对接节点已经录入，状态为启用，不支持删除。

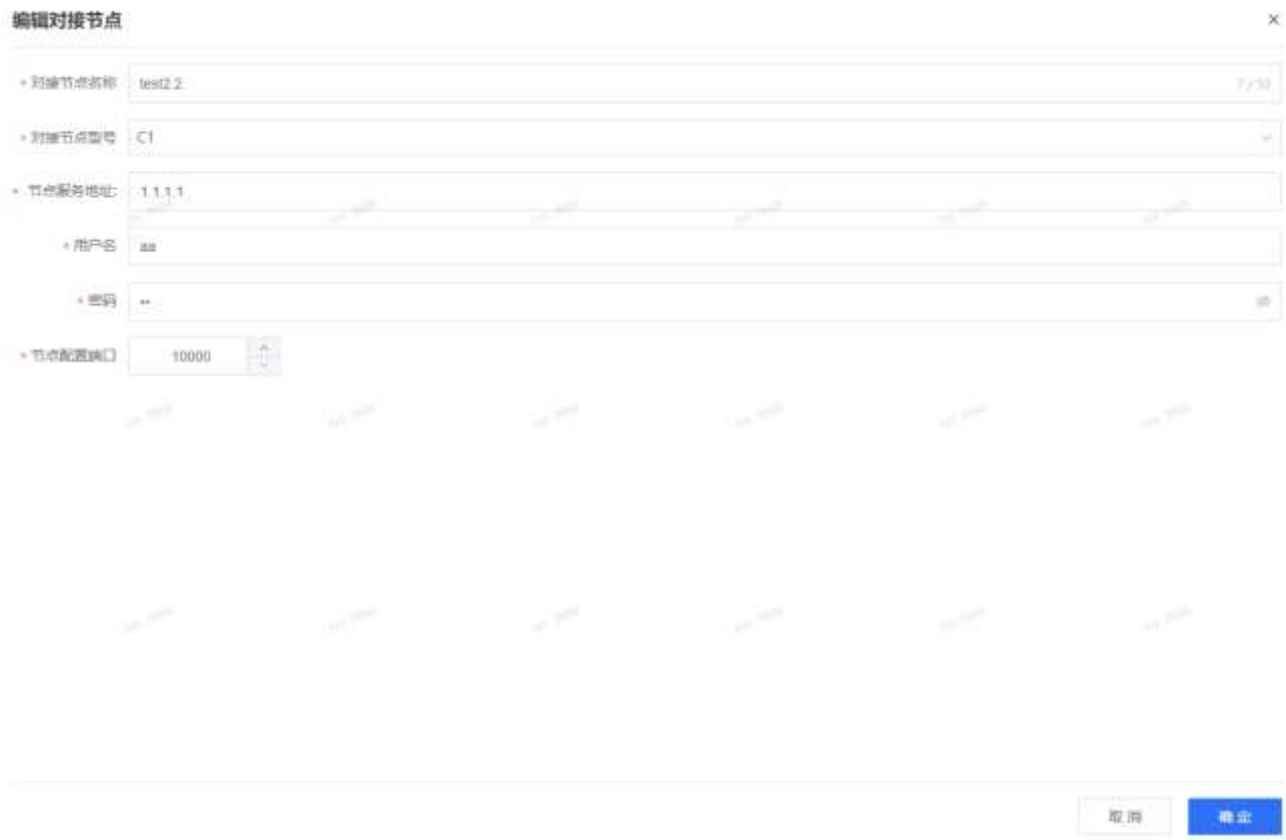
3.4.3.4.3 修改对接节点

【应用场景】

录入的对接节点，需要修改。

【操作角色】系统自动

1、如果对接节点记录之后，状态未启用。点击“编辑”按钮，可以直接修改



2、如果对接节点已经录入，状态为启用，不支持修改。

3.4.3.4.4 查询对接节点

【应用场景】

查询对接节点信息，了解对接节点跟踪情况。

【操作角色】系统自动

1、 查询列表

- 通过对接节点菜单，进入查询界面。
- 按照对接节点的颗粒度，展现节点信息等数据。
- 用户可以使用自定义筛选，按照对接节点名称进行模糊查询。

3.4.3.4.5 查询对接节点详情

【应用场景】

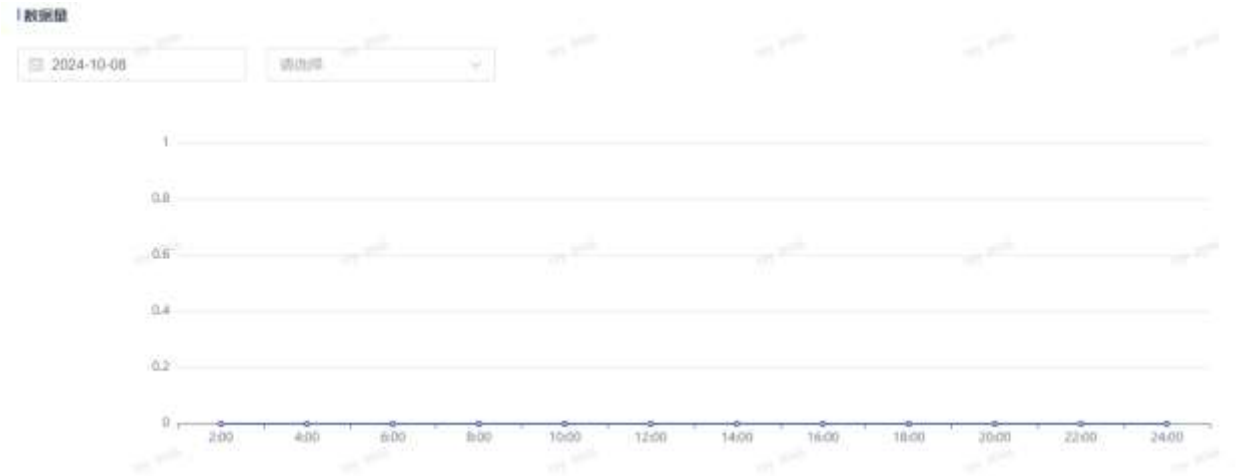
查询对接节点信息，了解对接节点跟踪情况。

【操作角色】系统自动

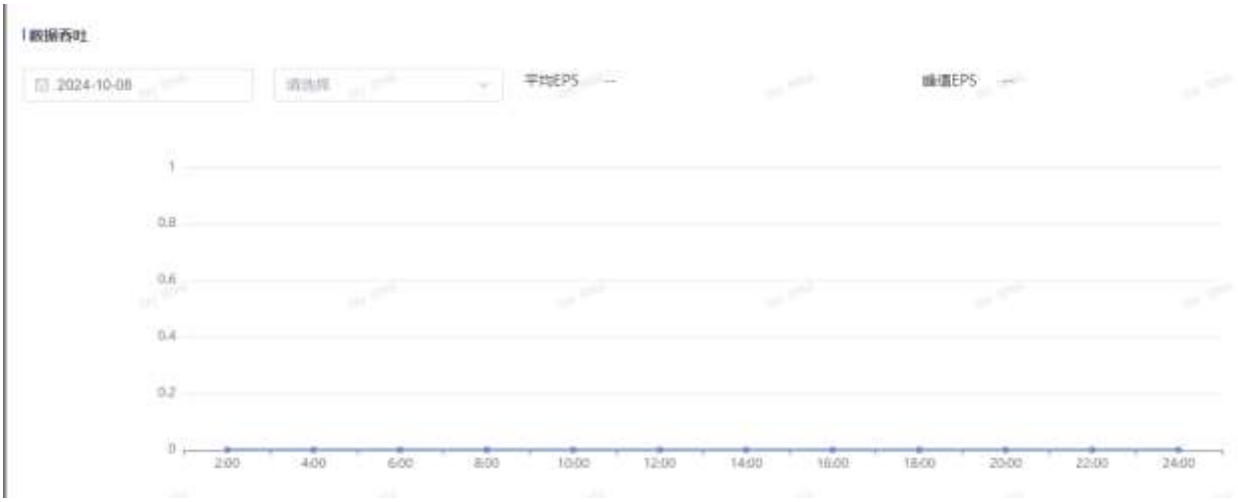
1、查询详情

1） 对接节点菜单，点击状态“详情”按钮，进入节点详情界面。

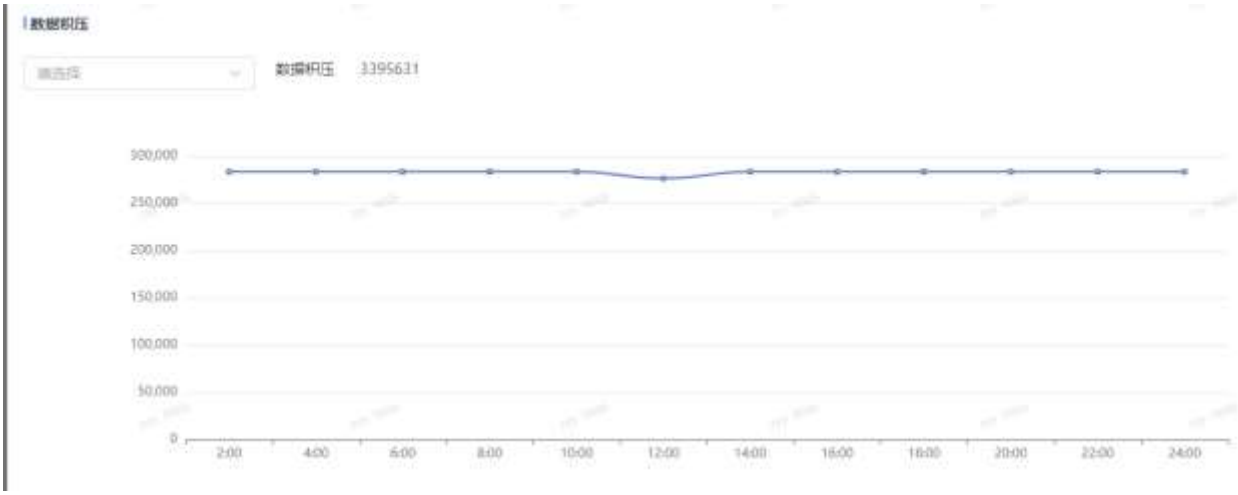
2） 数据对接选择起始日期进行数据量查询。



3） 数据对接选择起始日期进行数据吞吐查询。



4） 数据对接选择类型进行数据积压查询。



5） 点击异常记录，进行异常记录的查询操作，点击清理积压按钮可以清除数

据积压。

3.4.3.4.6 异常通知配置

【应用场景】

进行异常通知配置，了解对接节点异常情况并进行通知。

【操作角色】系统自动

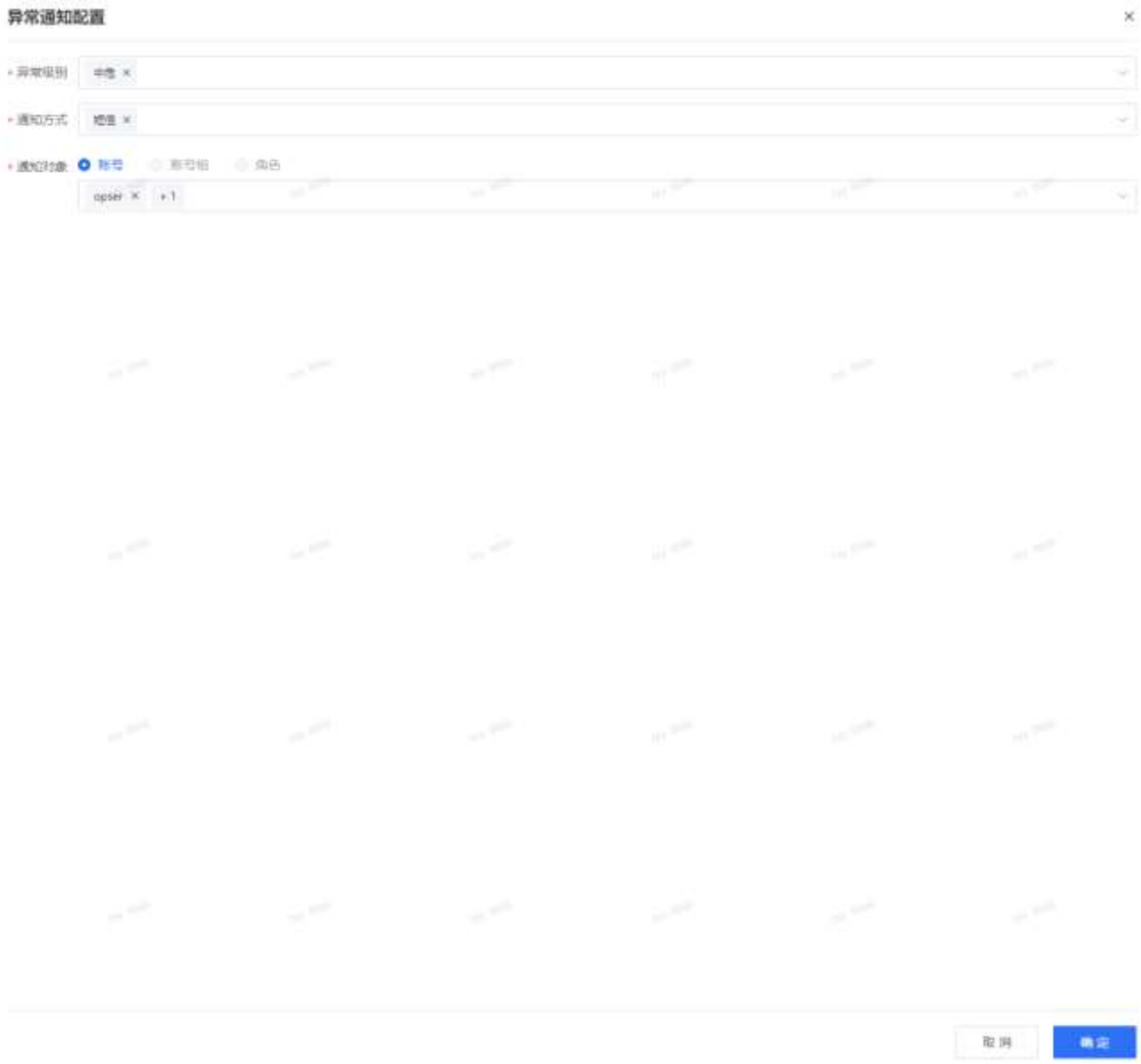
1、异常通知配置

1） 填写异常通知配置信息

异常级别：选择异常级别。

通知方式：选择通知方式。

通知对象：选择通知对象。



2） 点击“确定”按钮，完成异常通知配置的录入。

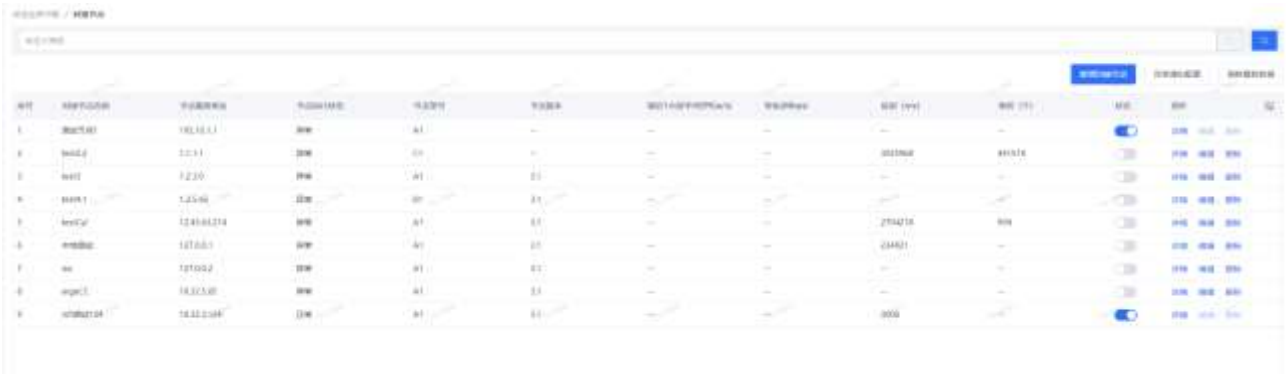
3.4.3.4.7 刷新最新数据

【应用场景】

刷新对接节点信息，获取最新对接节点跟踪情况。

【操作角色】系统自动

1、点击“刷新最新数据”按钮获取最新对接节点信息



3.4.3.4.8 对接节点启用

【应用场景】

启用对接节点。

【操作角色】系统自动

1、点击状态下面的按钮“按钮启用对接节点

3.4.3.5 字典配置

3.4.3.5.1 数据字典配置新增

【应用场景】

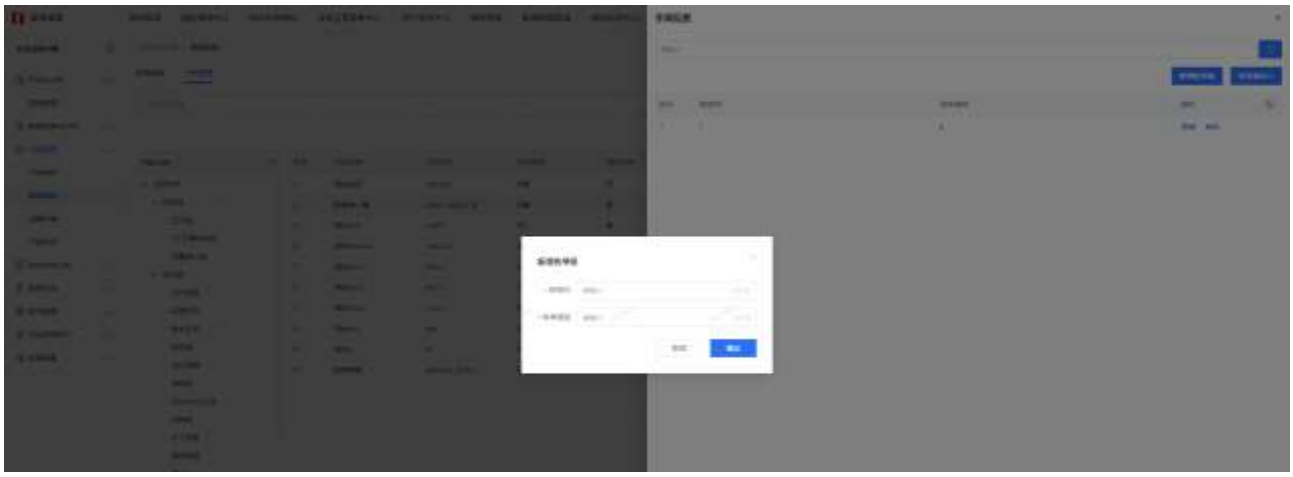
在数据模板的字段管理（字段是枚举）点击字典配置进行新增字典值。

【操作角色】系统自动

1、进入安全业务中枢数据模板界面

- 字段管理菜单，点击字典配置按钮。

- 点击“新增枚举值”进入新增界面。



2、录入枚举值

1） 填写节点信息

- 枚举 ID：填写枚举 ID。
- 枚举描述：填写枚举描述。

2） 点击“确定”按钮，完成字典值的录入。

3.4.3.5.2 数据字典配置导入模版下载

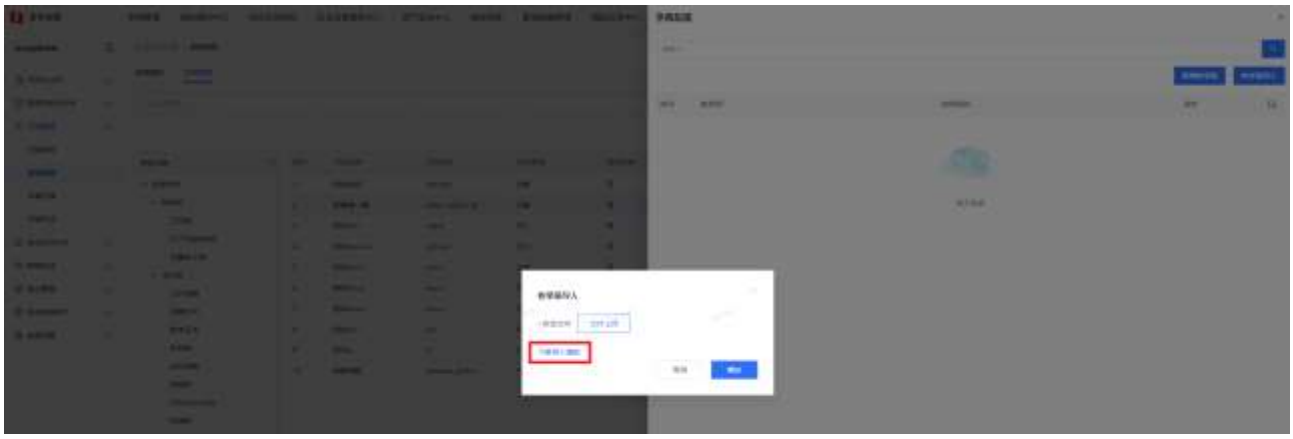
【应用场景】

在数据模板的字段管理（字段是枚举）点击字典配置进行导入模版下载。

【操作角色】系统自动

1、进入安全业务中枢数据模板界面

- 字段管理菜单，点击字典配置按钮。
- 点击“枚举值导入”进入导入界面。
- 点击“下载导入模版”按钮下载模版。



3.4.3.5.3 数据字典配置导入

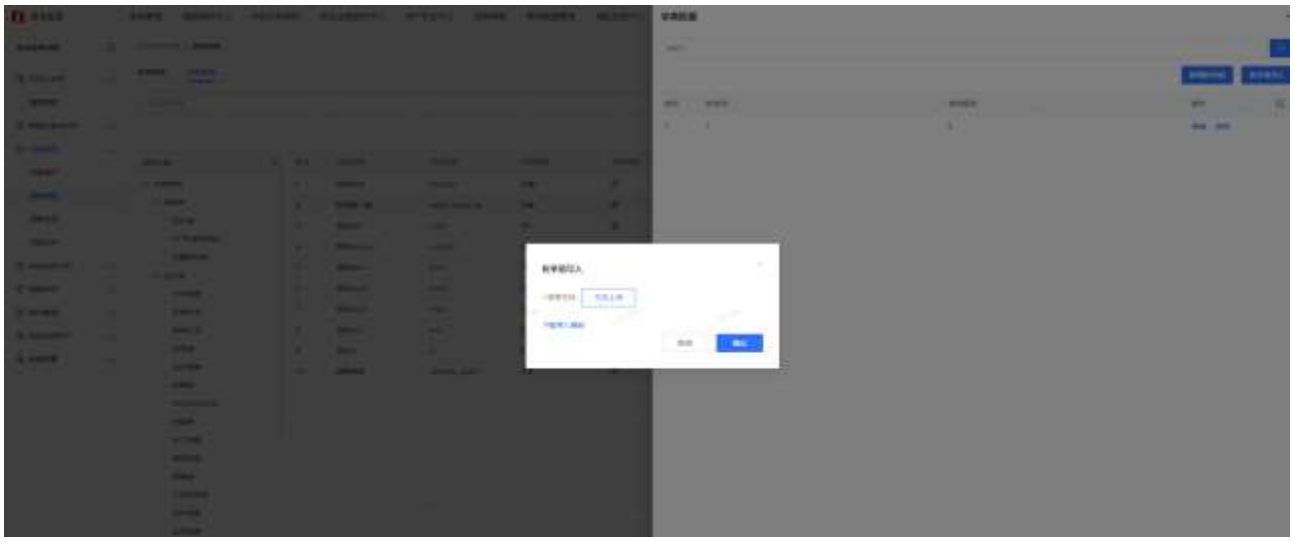
【应用场景】

在数据模板的字段管理（字段是枚举）点击字典配置进行字典值导入。

【操作角色】系统自动

1、进入安全业务中枢数据模板界面

- 字段管理菜单，点击字典配置按钮。
- 点击“枚举值导入”进入导入界面。



2、点击文件上传按钮，上传已经下载并编辑好的导入模版。

3.4.3.5.4 数据字典配置查询

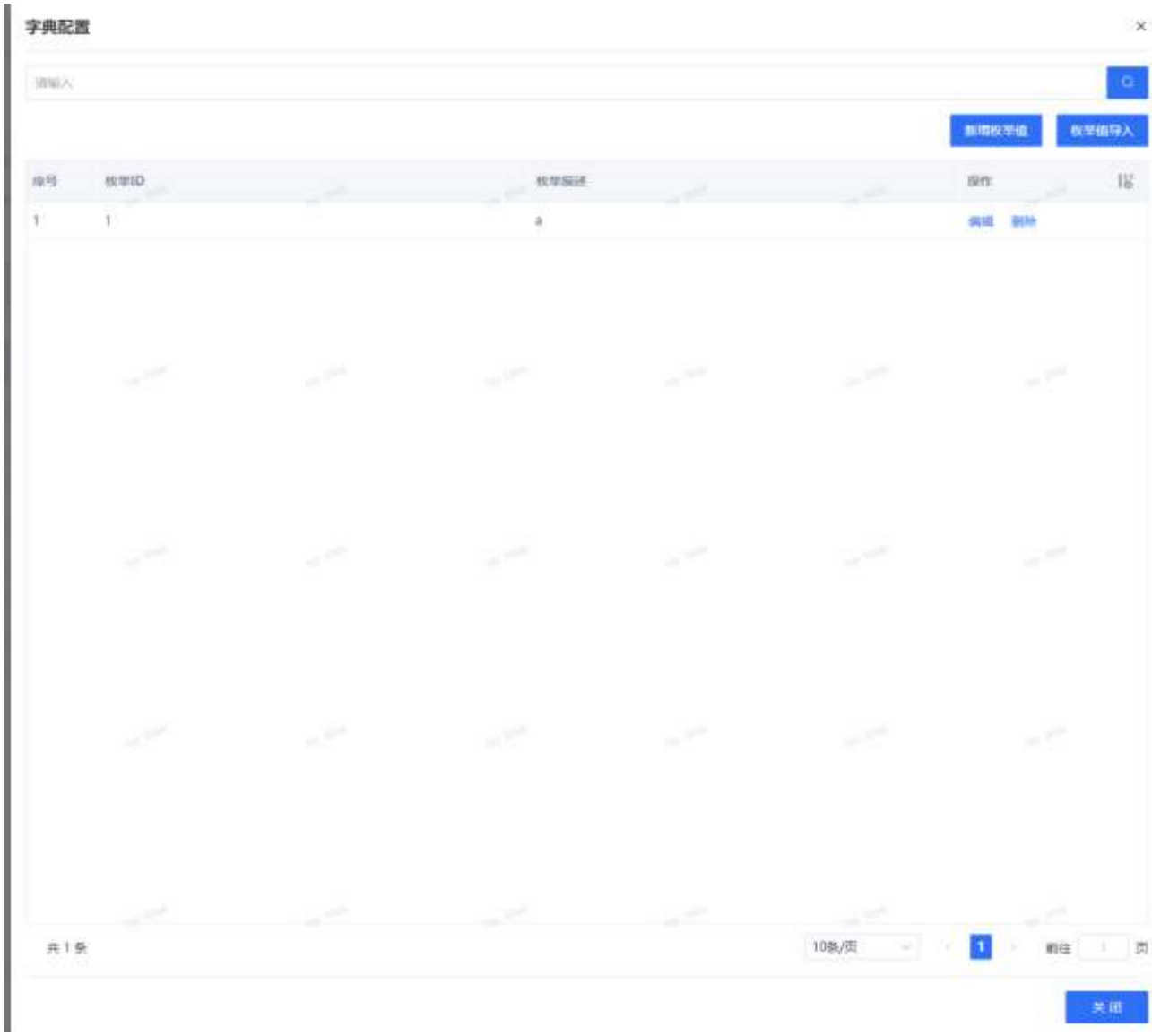
【应用场景】

在数据模板的字段管理（字段是枚举）点击字典配置进行字典值查询。

【操作角色】系统自动

1、进入安全业务中枢数据模板界面

- 字段管理菜单，点击字典配置按钮。
- 输入枚举 ID 或者枚举描述进行查询



3.4.3.5.5 数据字典配置编辑

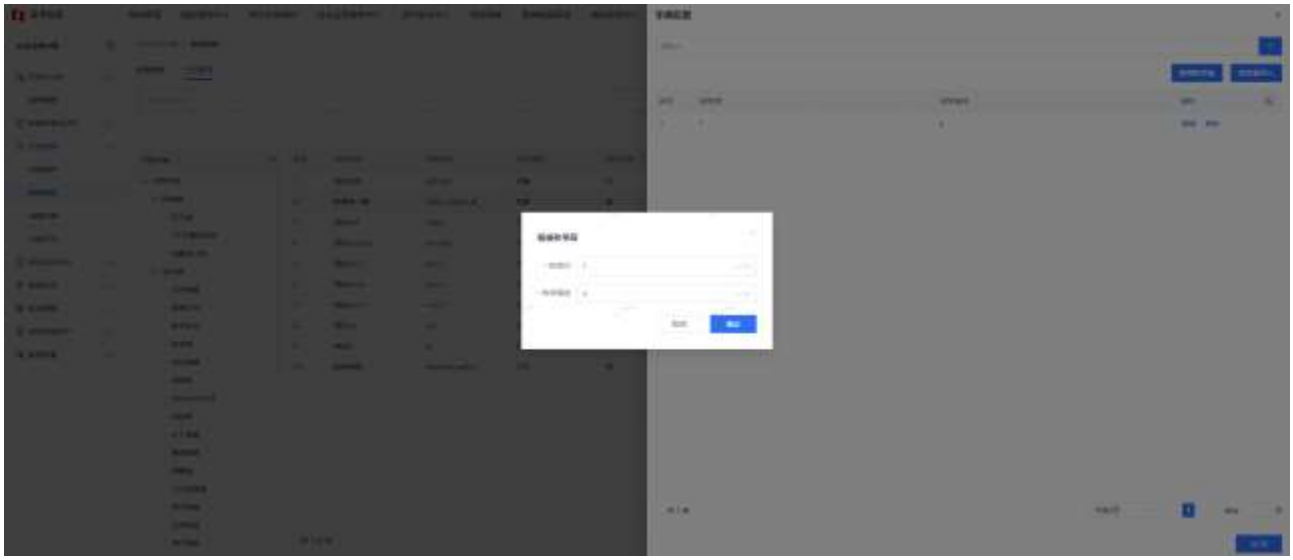
【应用场景】

在数据模板的字段管理（字段是枚举）点击字典配置进行修改字典值。

【操作角色】系统自动

1、进入安全业务中枢数据模板界面

- 字段管理菜单，点击字典配置按钮。
- 查询出来的字典值列表中，点击字典值后面的“编辑”按钮进入修改界面。



2、点击“确定”按钮，完成字典值的修改。

3.4.3.5.6 数据字典配置删除

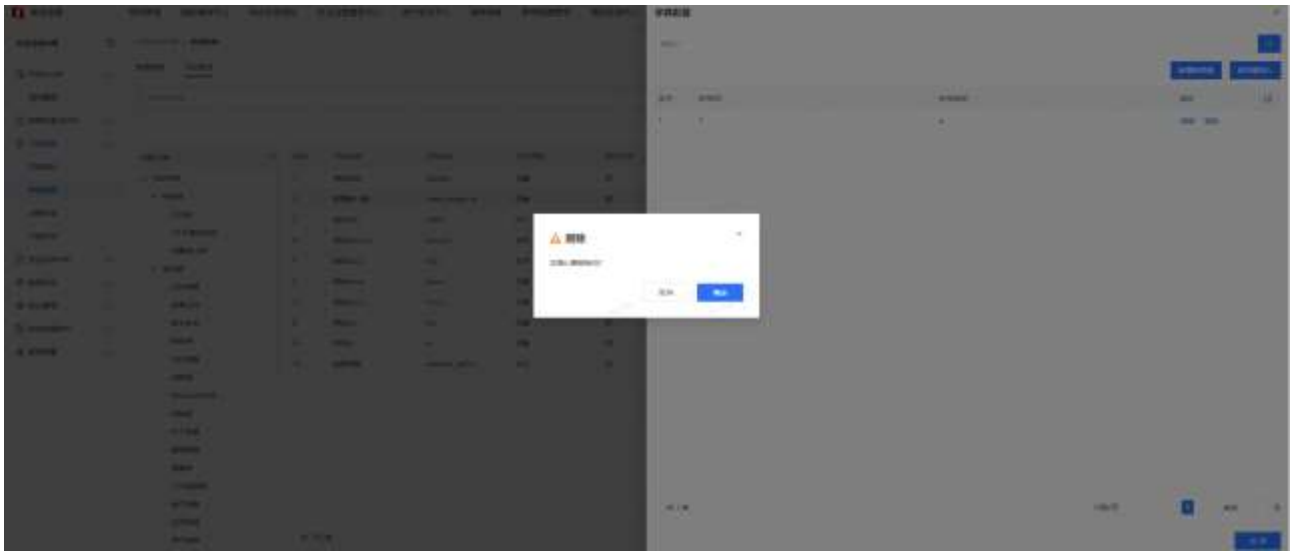
【应用场景】

在数据模板的字段管理（字段是枚举）点击字典配置进行删除字典值。

【操作角色】系统自动

1、进入安全业务中枢数据模板界面

- 字段管理菜单，点击字典配置按钮。
- 查询出来的字典值列表中，点击字典值后面的“删除”按钮。



点击“确定”按钮，完成枚举值的删除。

3.4.4 安全实体分析

模块（菜单）	主要功能
安全业务中枢>安全实体分析>安全实体模板	IP、域名实体对应的实体属性配置、实体关系配置及过滤配置(实体计算黑名单)。
安全业务中枢>安全实体分析>实体分析	查询实体列表信息、实体关联关系和相关 IP、相关域名等信息。
安全业务中枢>对接管理	配置实体对应的数据模板、对接插件、对接设备等信息

3.4.4.1 安全实体模板

3.4.4.1.1 实体配置-属性

【功能说明】系统在初始的时候会内置一些实体配置信息。

内置的 IP 实体属性信息：

实体属性　实体关系　过滤配置

实体类型：IP实体

唯一键：ip

序号	字段名称	字段英文名	字段类型	是否多值	示例
1	IP	entity_ip	单值ip	多值	172.16.1.1
2	网络域	vpc_id	多值text	多值	"vpc_id":"hnnswjw3...
3	端口	port	数字num	多值	"port":["21","22","23"]
4	实体信息来源	entity_source	对象object	多值	"entity_source.db":"...
5	实体来源库	entity_source.db	多值text	多值	"entity_source.db":"...
6	实体来源表	entity_source.table	多值text	多值	"entity_source.table...
7	实体来源数据ID	entity_source.dataid	多值text	多值	"entity_source.datai...
8	实体来源字段	entity_source.field	多值text	多值	"entity_source.field"...
9	实体发现时间	entity_dis_time	多值text	多值	"entity_dis_time":"2...

内置的域名属性信息：

实体属性　实体关系　过滤配置

实体类型：域名实体

唯一键：domain

序号	字段名称	字段英文名	字段类型	是否多值	示例
1	IP	entity_ip	单值ip	多值	172.16.1.1
2	实体信息来源	entity_source	对象object	多值	"entity_source":"es:1...
3	实体来源库	entity_source.db	多值text	多值	"entity_source.db":"...
4	实体来源表	entity_source.table	多值text	多值	"entity_source.table...
5	实体来源数据ID	entity_source.dataid	多值text	多值	"entity_source.datai...
6	实体来源字段	entity_source.field	多值text	多值	"entity_source.field"...
7	实体发现时间	entity_dis_time	多值text	多值	"entity_dis_time":"2...
8	域名	entity_domain	多值text	单值	www.qinwei.com

3.4.4.1.2 实体配置-关系

【功能说明】系统在初始的时候会内置一些实体关系信息。

内置的 IP 实体关系信息：

实体属性　实体关系　过滤配置

序号	实体类型	实体关系类型	实体关系别名	实体关系图
1	IP	连接	网络连接	IP —网络连接→ IP
2	IP	连接	DNAT映射	IP —DNAT映射→ IP
3	IP	连接	SNAT映射	IP —SNAT映射→ IP
4	IP	连接	DNS请求	IP —DNS请求→ IP
5	IP	连接	域名请求	IP —域名请求→ 域名

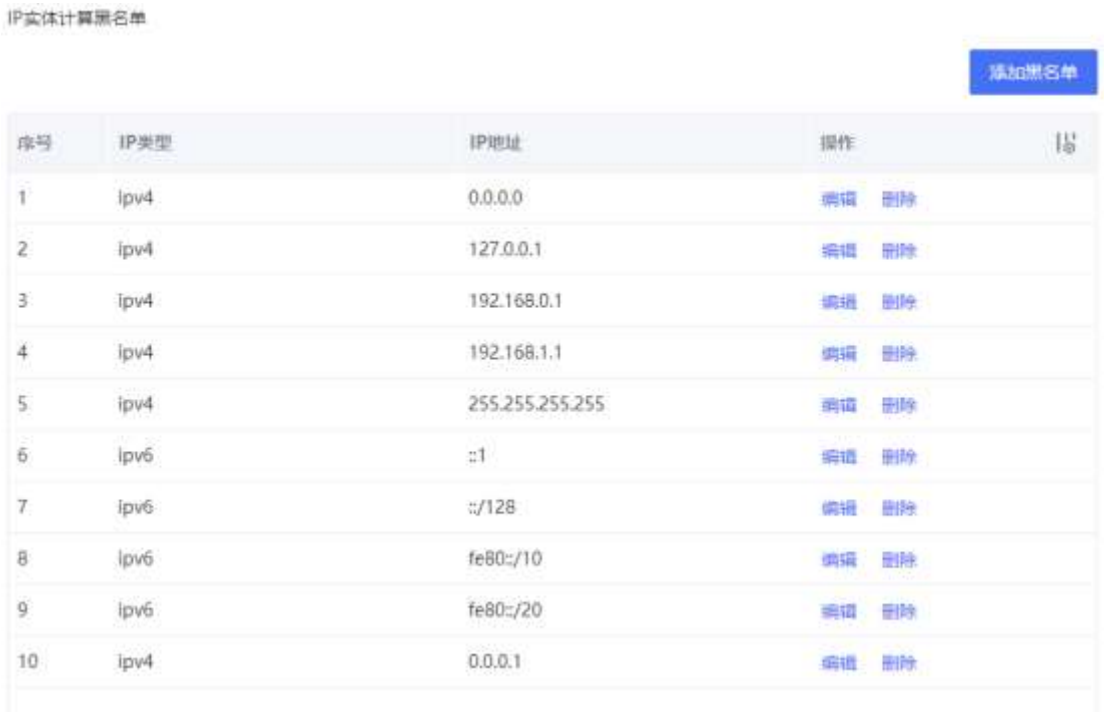
内置的域名实体关系信息：

实体属性　实体关系　过滤配置

序号	实体类型	实体关系类型	实体关系别名	实体关系图
1	域名	连接	域名解析	域名 —域名解析→ IP
2	域名	包含	域名包含	域名 —域名包含→ 域名
3	域名	连接	域名解析	域名 —域名解析→ 域名

3.4.4.1.3 实体配置-过滤配置

【功能说明】IP 实体对应的过滤配置信息



3.4.4.1.3.1 IP 实体过滤配置新增

【功能说明】选择 IPv4/IPv6；并填写对应 IP 地址范围

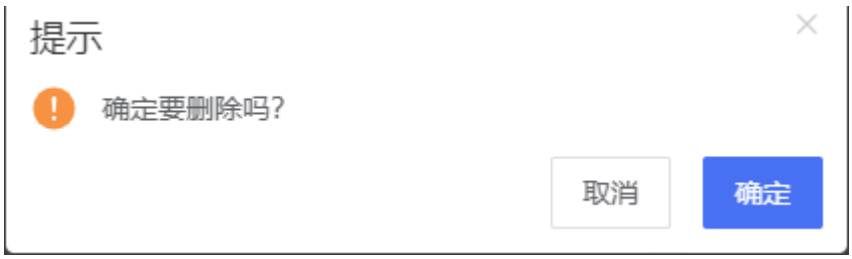
3.4.4.1.3.2 IP 实体过滤配置编辑

【功能说明】编辑已存在的过滤配置信息

保存成功

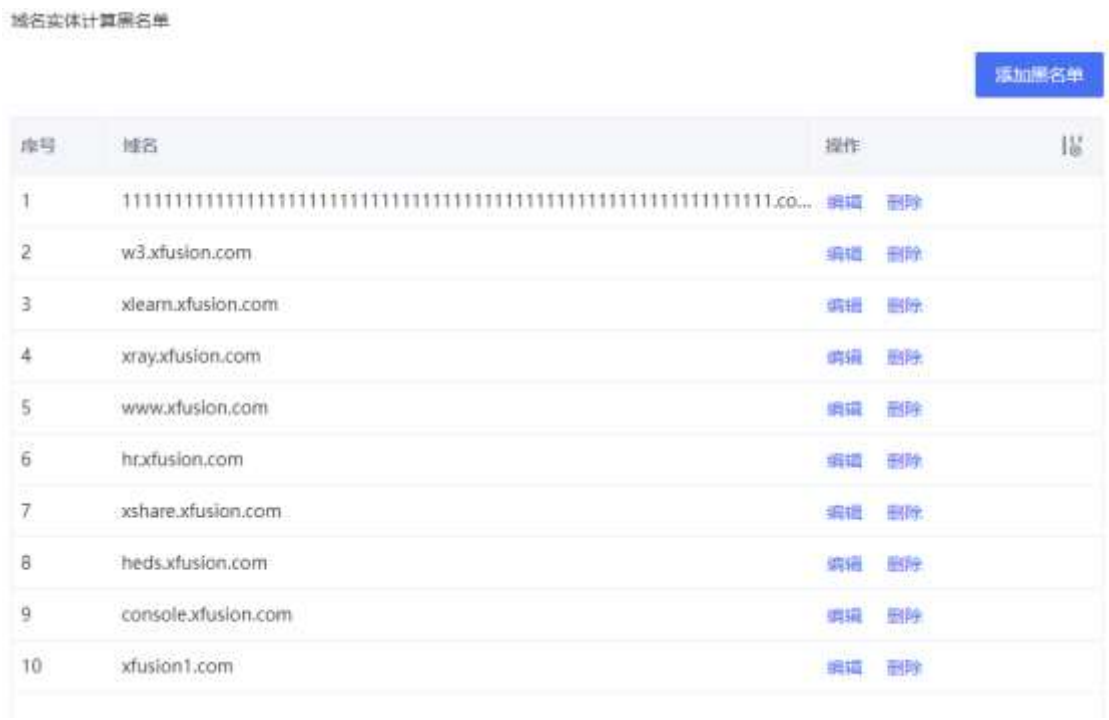
3.4.4.1.3.3 IP 实体过滤配置删除

【功能说明】点击删除



点击确定删除成功

域名实体的过滤配置信息：

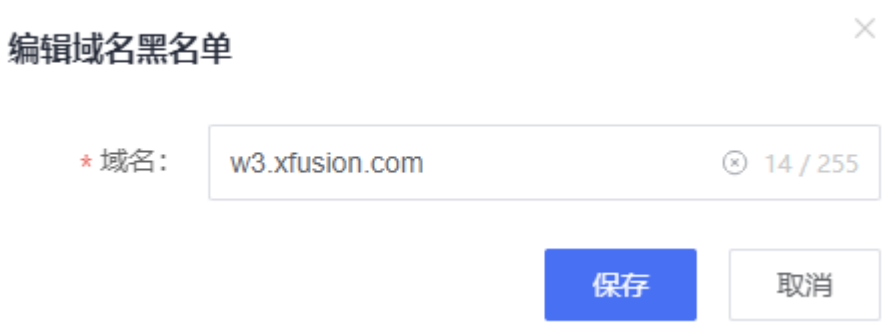


3.4.4.1.3.4 域名实体过滤配置新增

【功能说明】新增域名实体过滤配置，支持模糊匹配：

3.4.4.1.3.5 域名实体过滤配置编辑

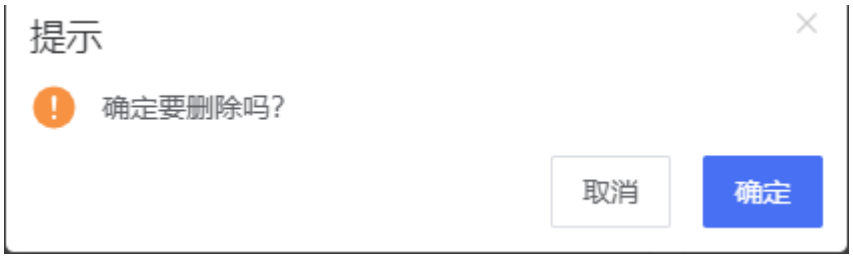
【功能说明】编辑域名实体过滤配置，支持模糊匹配：



保存成功

3.4.4.1.3.6 域名实体过滤配置删除

【功能说明】点击删除



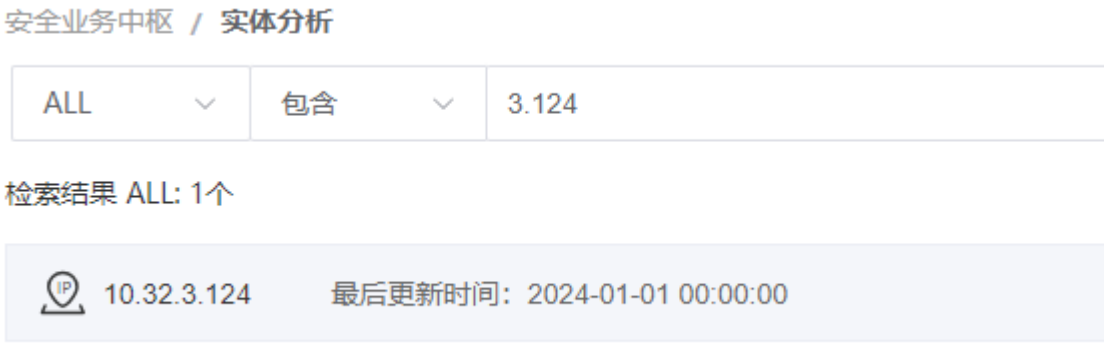
点击确定删除成功

3.4.4.2 实体分析

3.4.4.2.1 实体分析信息查询

【功能说明】可以选择 IP/域名/ALL，关系为包含/等于进行查询

如：



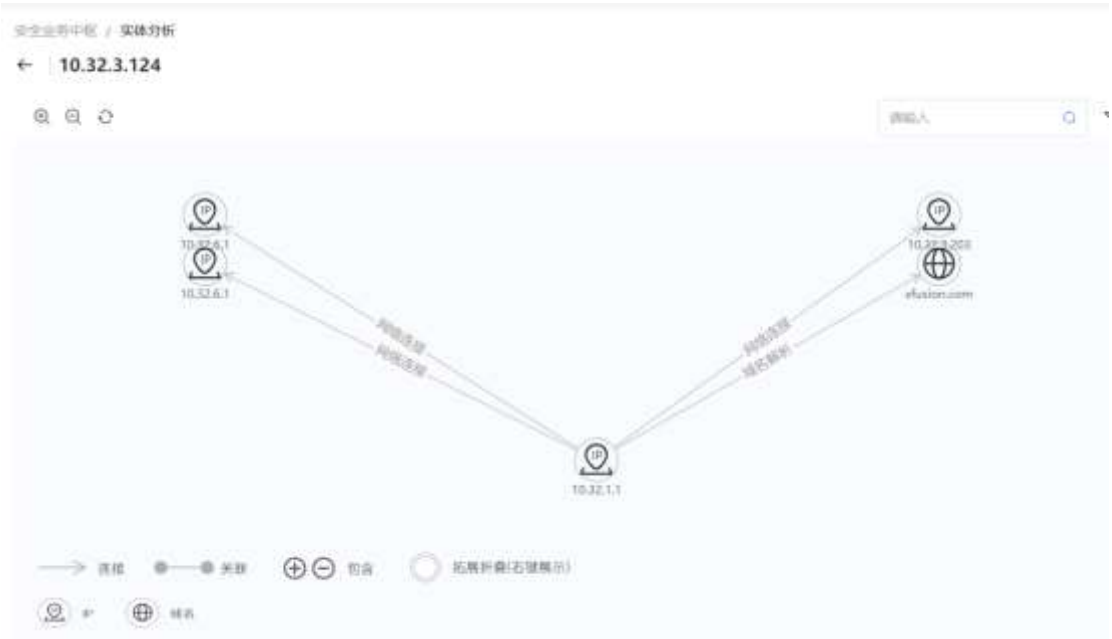
3.4.4.2.2 实体分析信息详情

【功能说明】点击按钮查看详情

展示相关 IP、域名等信息

点击品字按钮可以查看实体关系图示：

展示实体关系信息



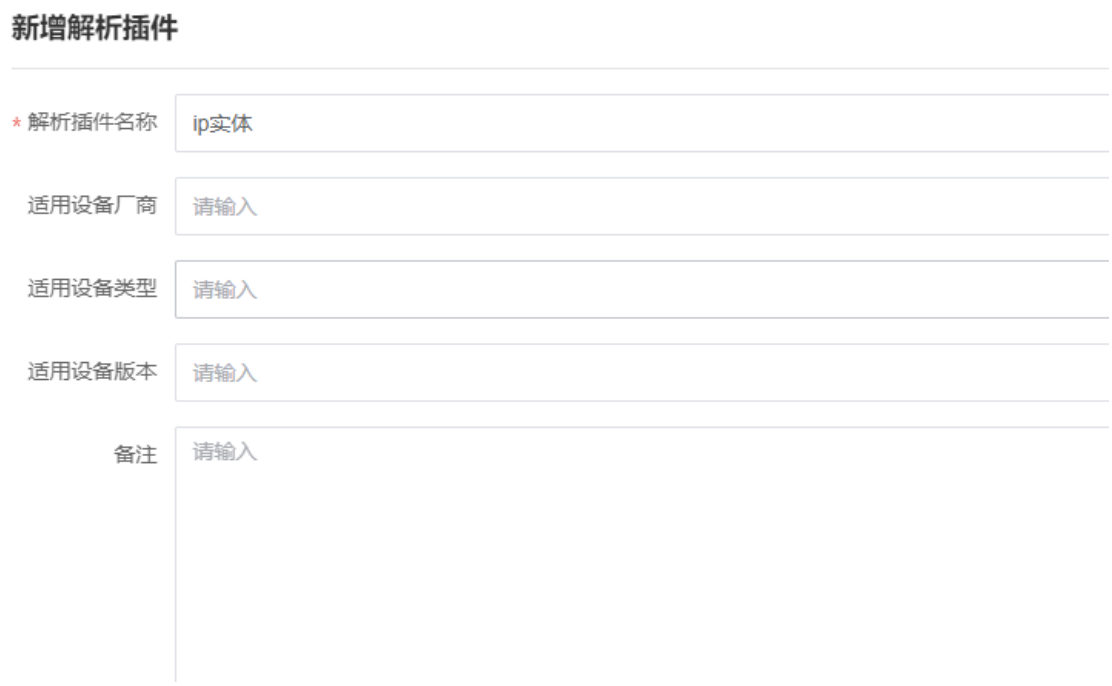
3.4.4.3 实体分析数据生成

3.4.4.3.1 对接管理模块配置实体分析数据来源信息

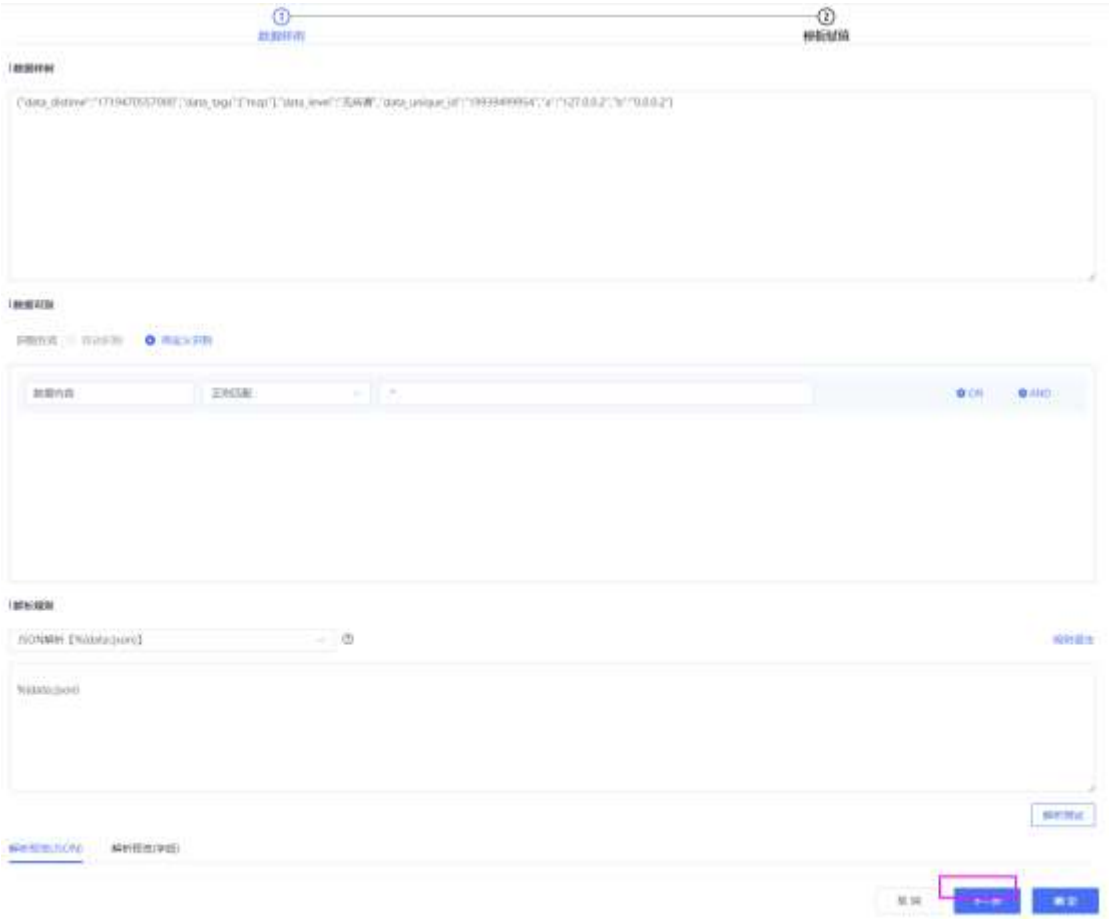
1、 首先在安全业务中枢>对接管理>数据模板中新建 IP/域名对应的模板信息

2、在安全业务中枢>对接管理>对接插件

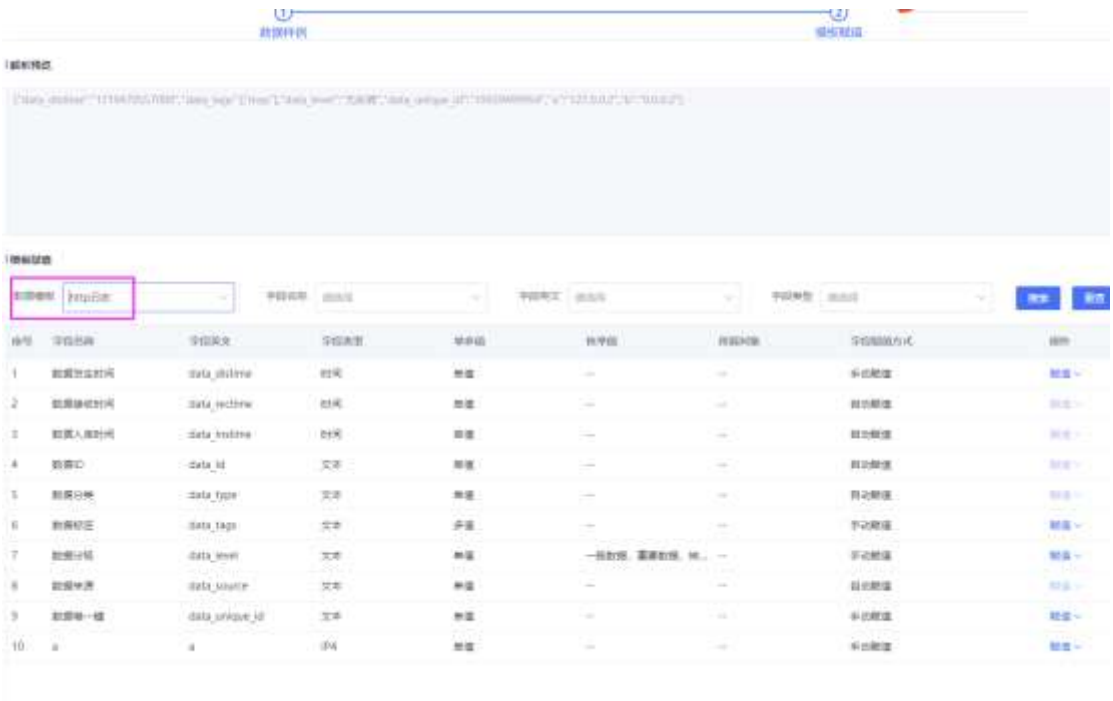
新建插件，并设置数据样例和模板赋值



插件配置—数据样例

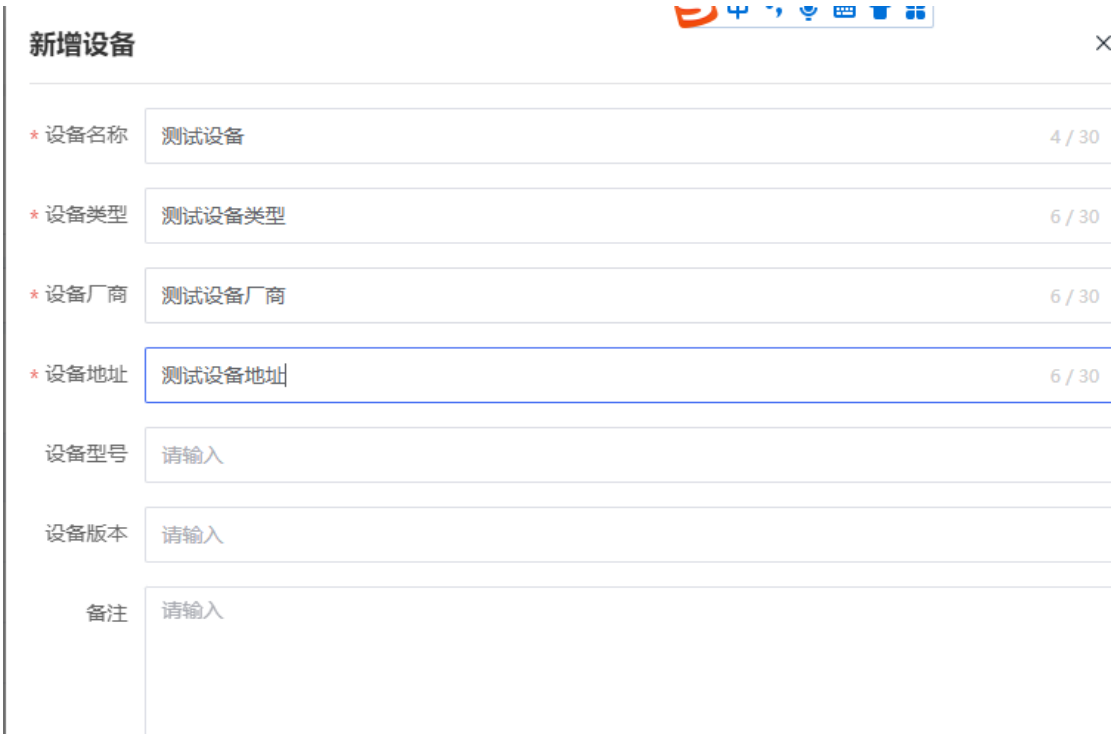


2、 下一步—模板赋值，选择对应的模板



3、在安全业务中枢>对接管理>设备对接

新建设备对接



4、点击—对接关系，新增数据对接信息

点击启用数据对接

5、厂商根据配置的数据对接信息将 IP 实体模板信息传入对应的接收地址

如上图中，厂商可有将需要对接的 IP 实体模板信息传入对应的 pulsar 地址

6、实体分析接收数据后显示

3.4.5 数据中台

3.4.5.1 登录

测试环境登录地址：http://xsee2.0.beta.xfusion.com/xsee/login

【登录说明】需要平台管理员用户优先创建用户账号，员工通过登录账号和密码登录系统

3.4.5.1.1 首页

3.4.5.1.1.1 首页-普通用户

普通用户登录系统首页可查看当前用户已加入的工作空间，已加入工作空间可通过点击服务标签，进入对应的服务功能模块；未加入空间不支持该操作，可联系空间管理员将用户添加至工作空间。

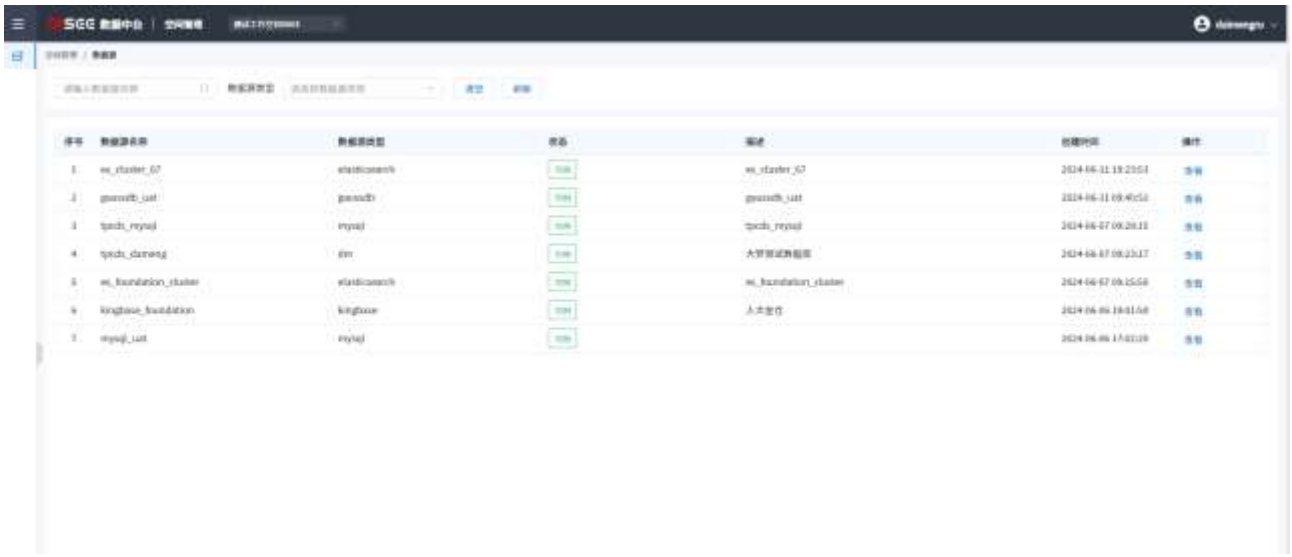
3.4.5.1.1.2 首页-空间管理员

空间管理员用户登录系统进入首页，默认可查看用户已加入和未加入的全部工作空间信息，已加入空间支持用户进入空间下的服务模块，切换至【我管理的工作

空间】标签下，可查看当前用户管理的工作空间信息：

在我管理的工作空间下，工作空间管理员可对空间成员进行管理，空间管理员用户默认添加为空间成员，且不支持移除：

点击空间管理标签可进入当前工作空间管理模块，空间管理模块当前包含数据源菜单，支持查看当前工作空间下已授权数据源：



3.4.6 数据总线

3.4.6.1API 开发

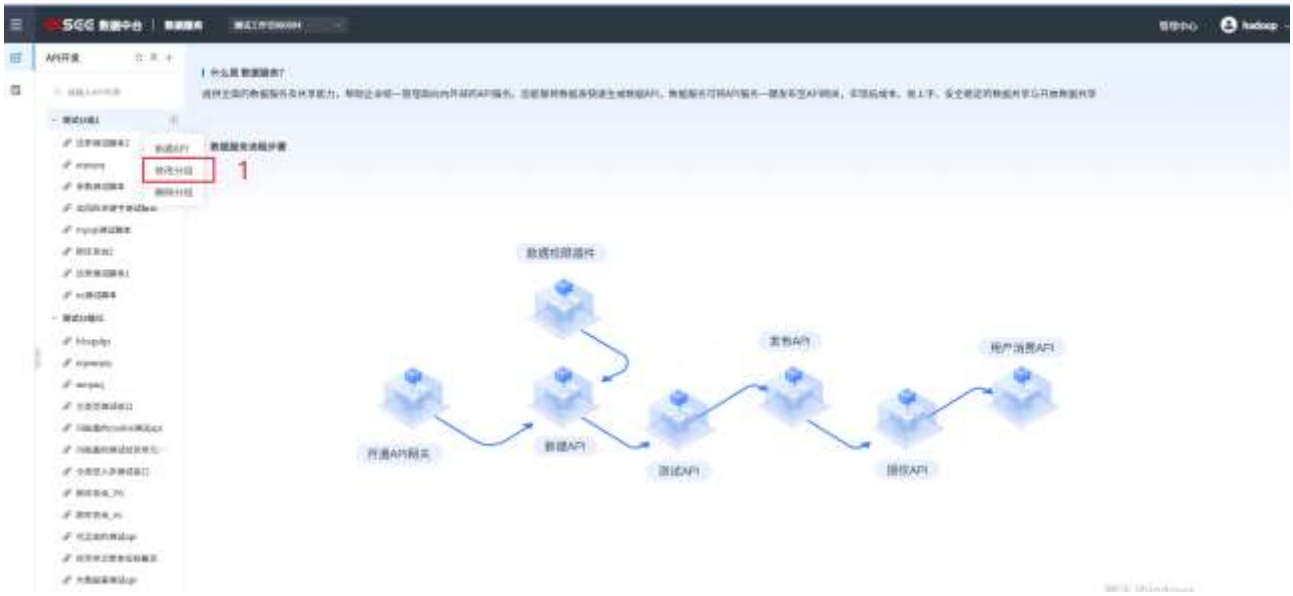
3.4.6.1.1 新增分组

操作步骤：进入 API 开发界面，点击新建分组按钮，设置分组名称和描述信息，点击保存，分组创建成功。

功能说明：通过分组对 API 归类管理，同一空间下分组名称不能重复

3.4.6.1.2 修改分组

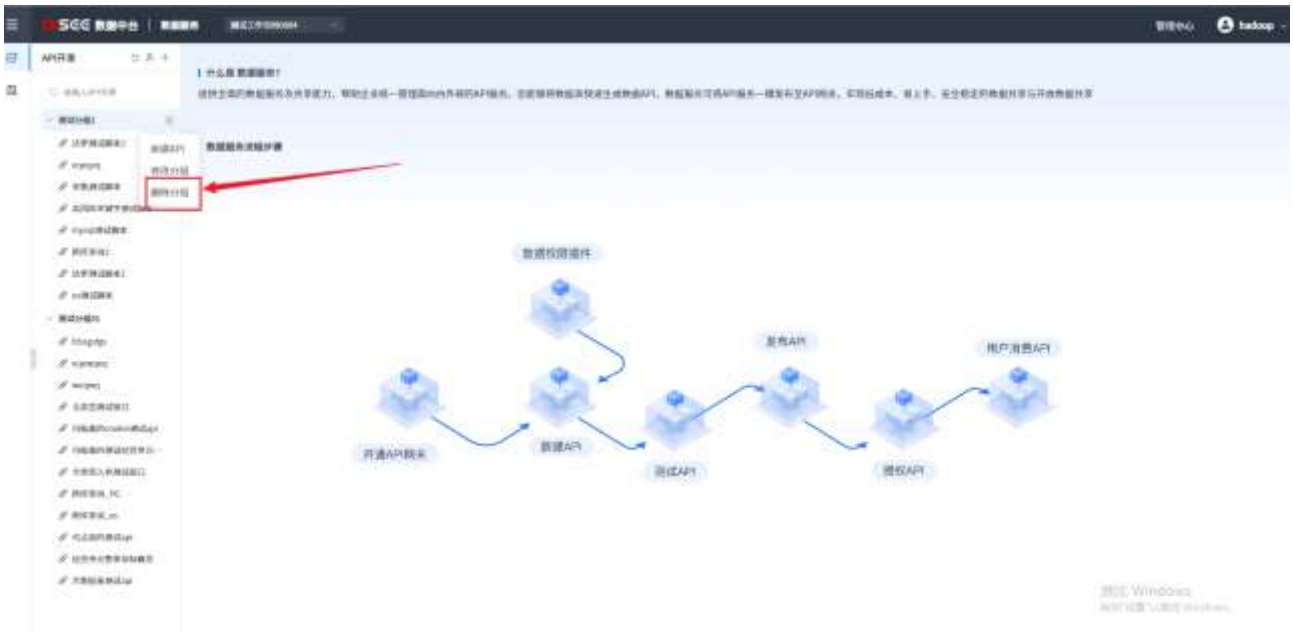
光标悬浮至分组名称上方，右侧显示操作按钮，点击修改分组，支持修改分组名称和描述内容。



3.4.6.1.3 删除分组

操作步骤：进入 API 开发界面，选择待删除分组，点击删除分组，点击二次确认弹窗中确定按钮，分组删除成功。

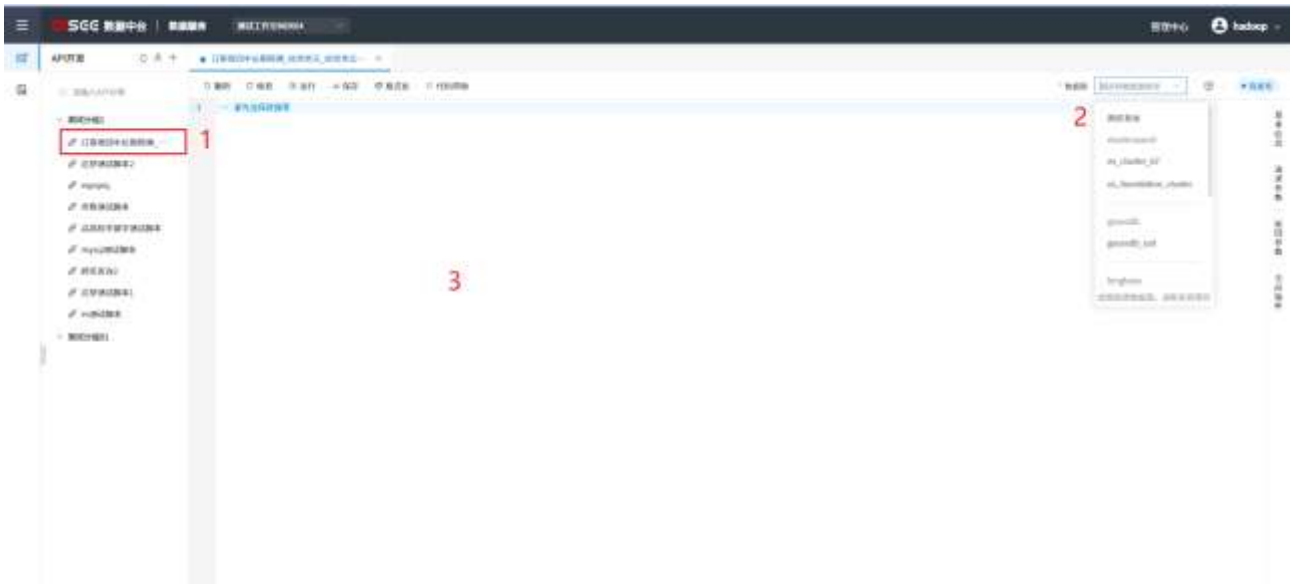
功能说明：删除分组需保证分组下未包含 API

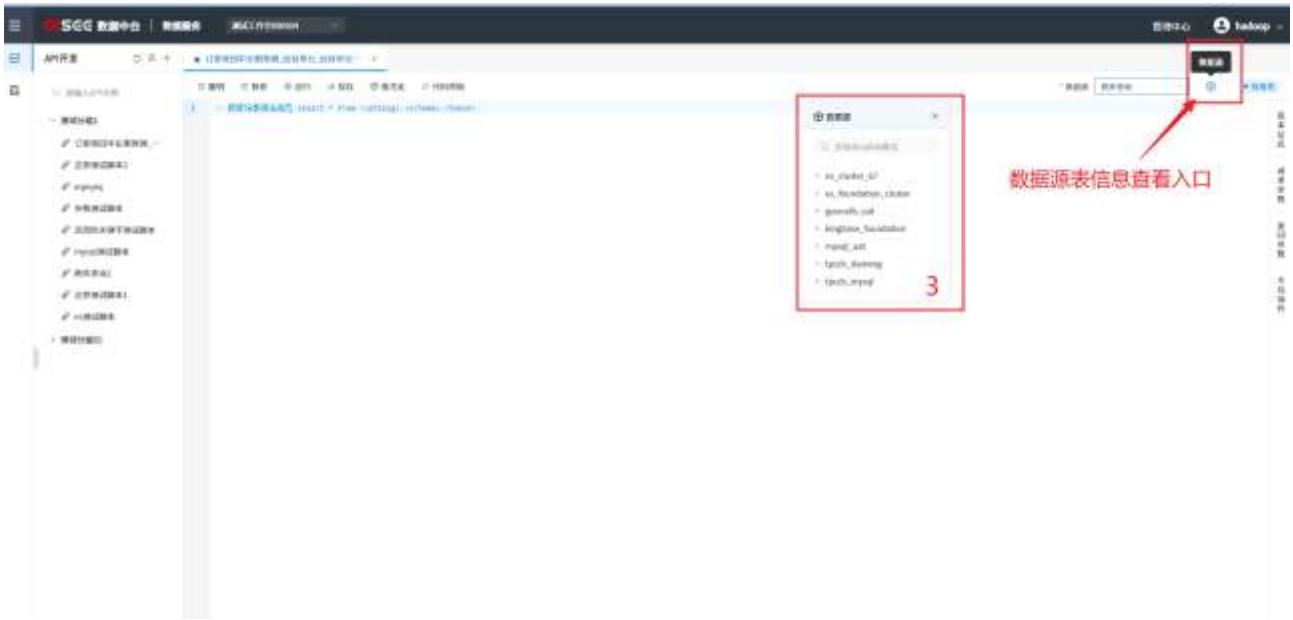


3.4.6.1.4 新建 API

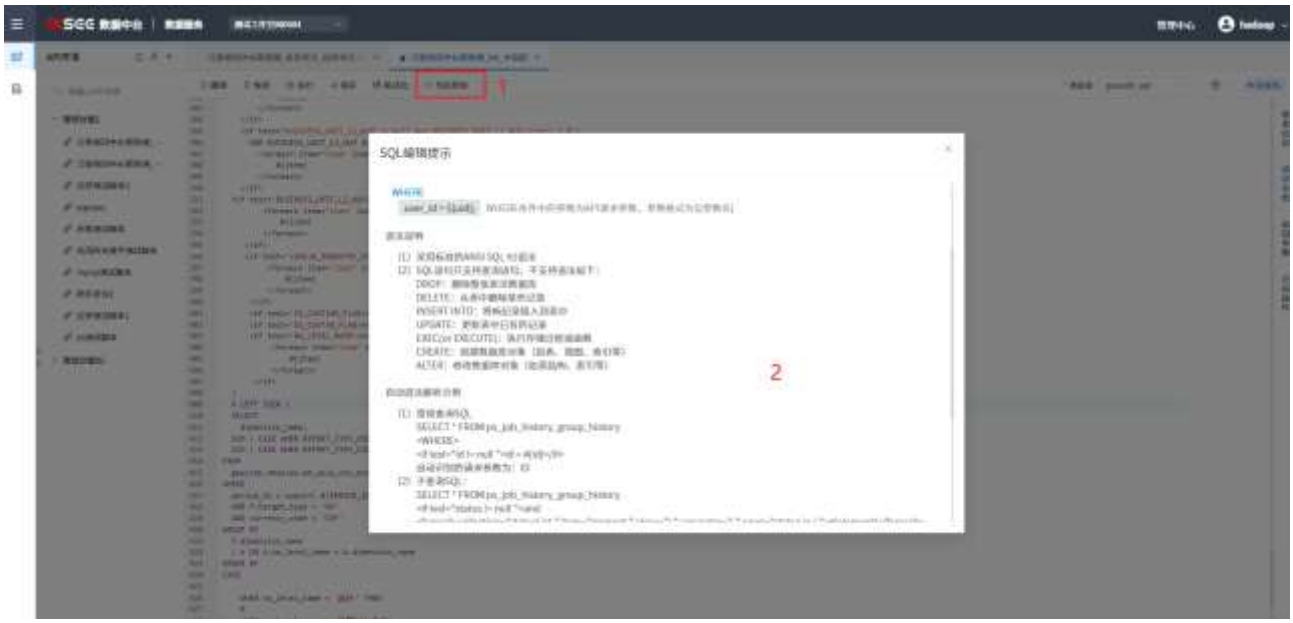
步骤一：进入 API 开发界面，点击新建 API 按钮或点击分组下的新建 API，设置 API 基本信息，点击确定，API 创建成功。

步骤二：双击新建 API 名称，打开 API 标签，进入 API 编辑模式，编写脚本之前需按照脚本内容选择数据源，支持跨库查询和单库查询，根据脚本使用场景选择，选中数据源后编辑区域会自动弹出数据源详细列表弹窗，支持查看数据源下表信息：

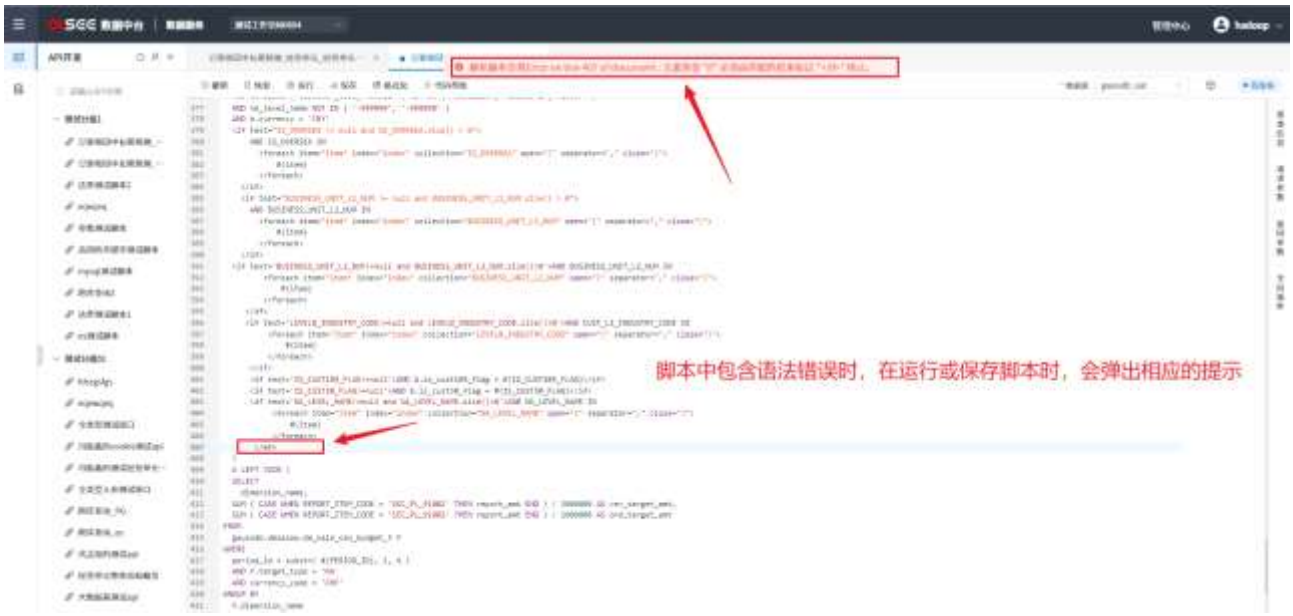




步骤三：编写 API 脚本，根据选中数据源编写脚本内容，数据源选择跨库查询时，脚本内容统一按照 Trino 语法编写，选择单库查询时，脚本内容按照该数据源语法编写，脚本中包含的请求参数信息均需要按照 Mybatis 动态 SQL 语法编写，详细的 SQL 编写原则可参考【代码帮助】中的说明：

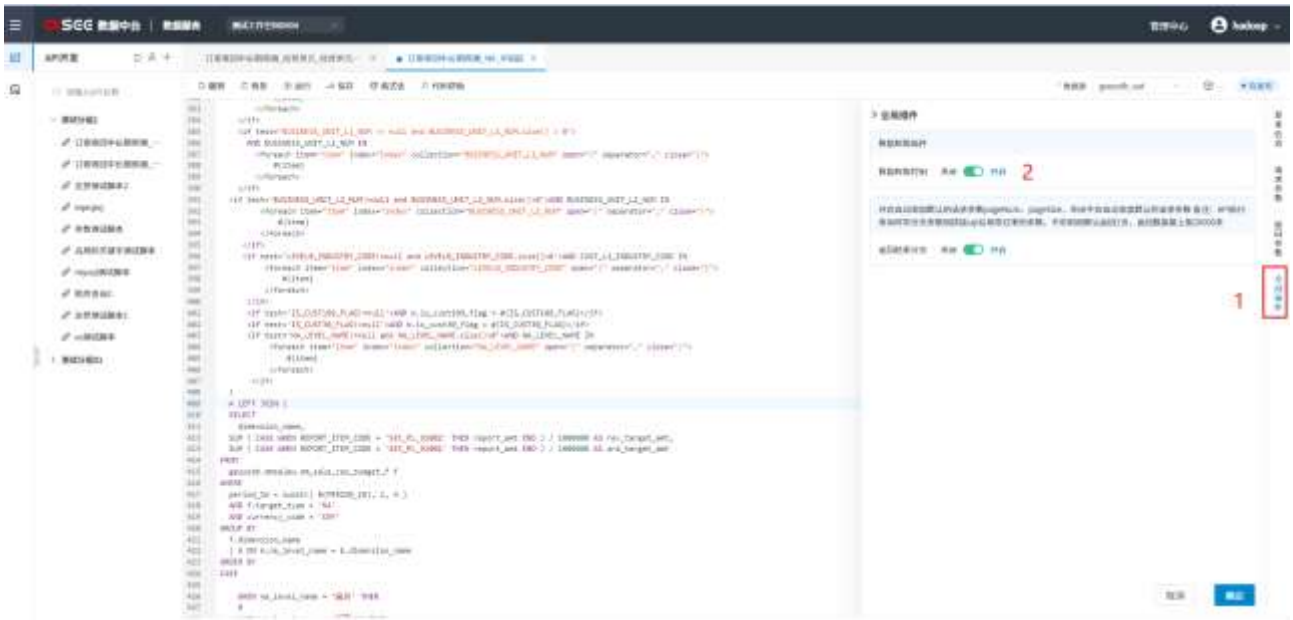


编写的脚本内容中包含语法错误时，操作保存或运行脚本时，会弹出相应的提示信息：

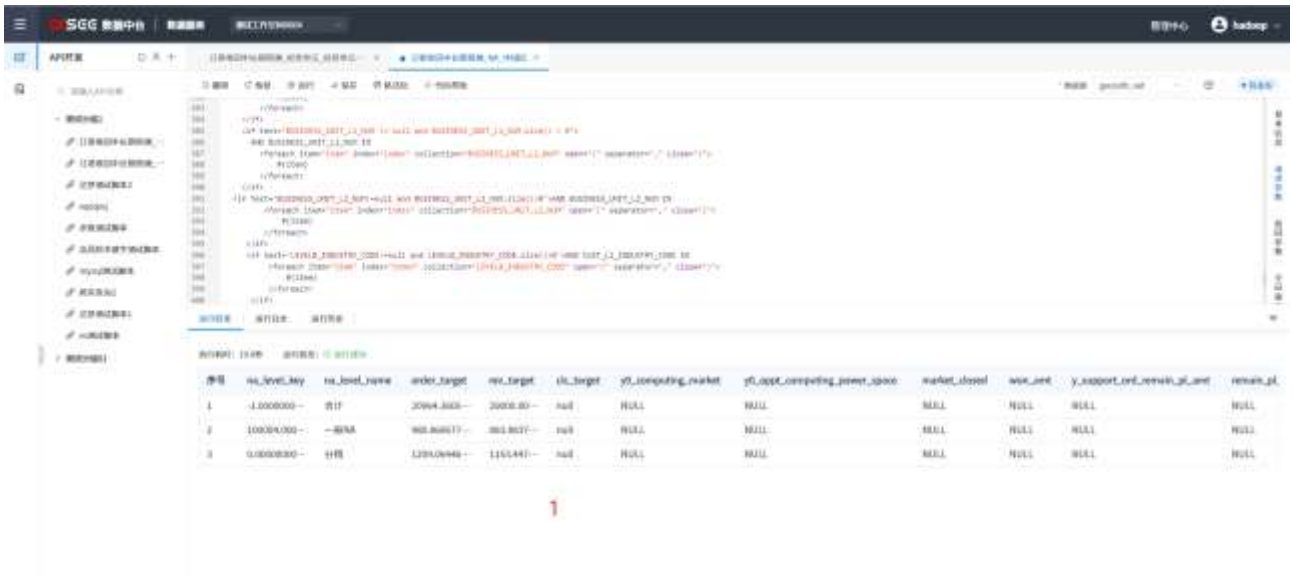


步骤四：系统根据编写的脚本内容自动识别请求参数，支持用户手动调整请求参数类型和参数值：

步骤五：点击全局插件按钮，可设置 API 插件信息，用于控制脚本执行返回内容数据权限，以及请求参数、返回参数分页信息：



步骤六：设置必填请求参数默认值后，点击运行按钮，脚本运行成功，可查看运行结果和运行日志内容：



补充说明：脚本编写过程支持以下快捷键操作：

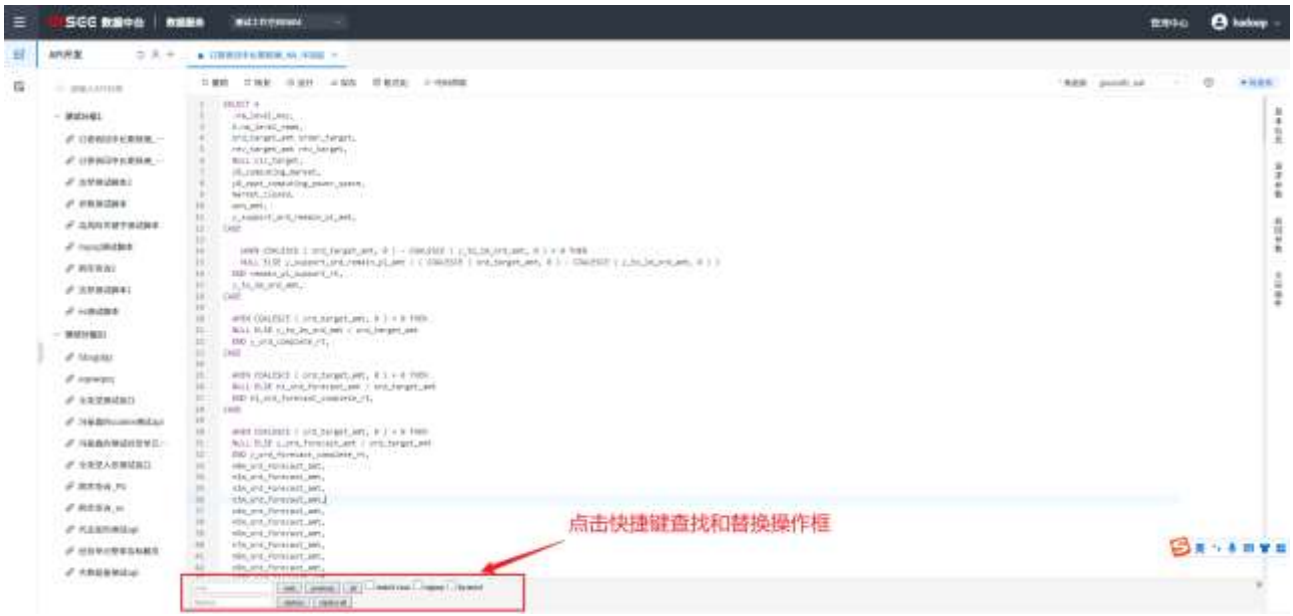
（1）保存 - Ctrl+S / Cmd+S

（2）撤销 - Ctrl+Z / Cmd+Z

（3）恢复 - Ctrl+Y / Cmd+Y

（4）查找 - Ctrl+F / Cmd+F

（5）替换 - Ctrl+Shift+F / Cmd+Shift+F

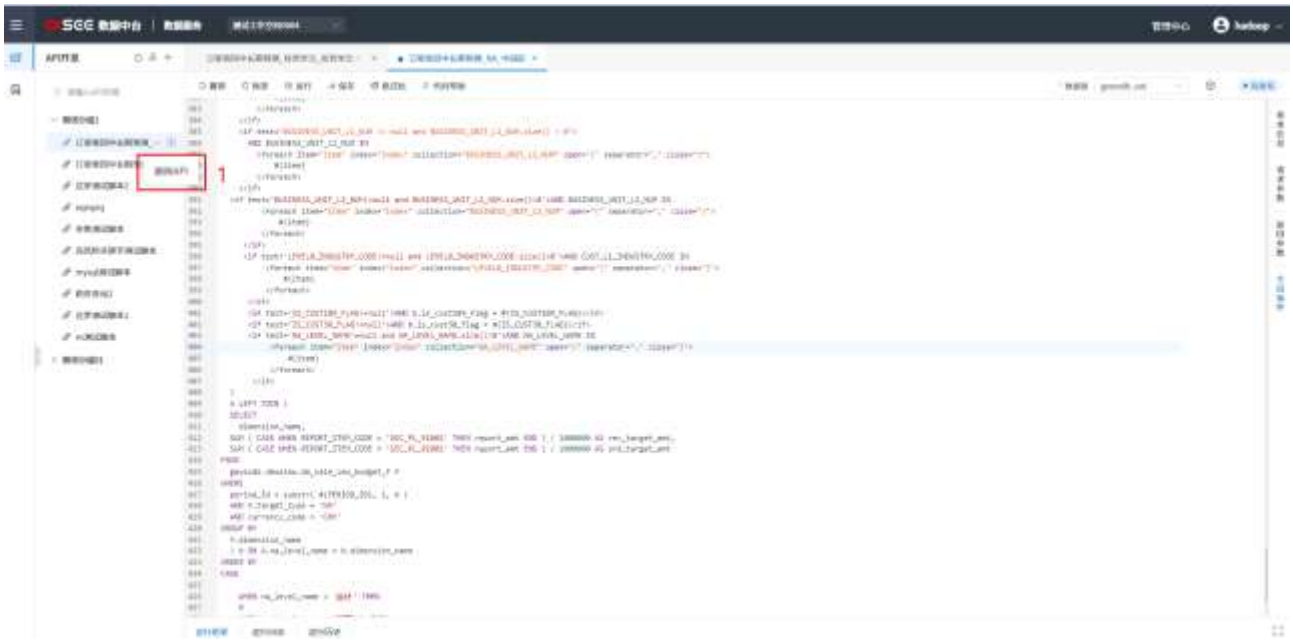


3.4.6.1.5 删除 API

操作步骤：选中待删除 API，点击删除 API 二次确认弹窗中确定按钮，API 删除

成功。

功能说明：仅支持删除待发布和已下线状态 API

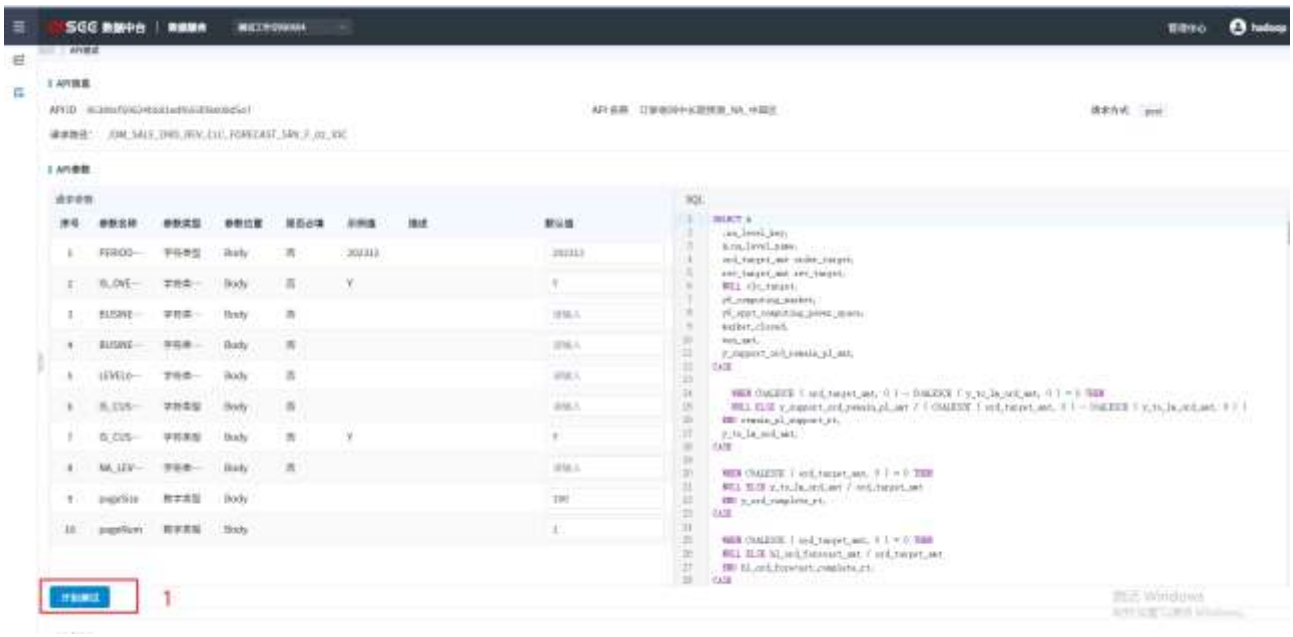


3.4.6.2 API 管理-API 列表

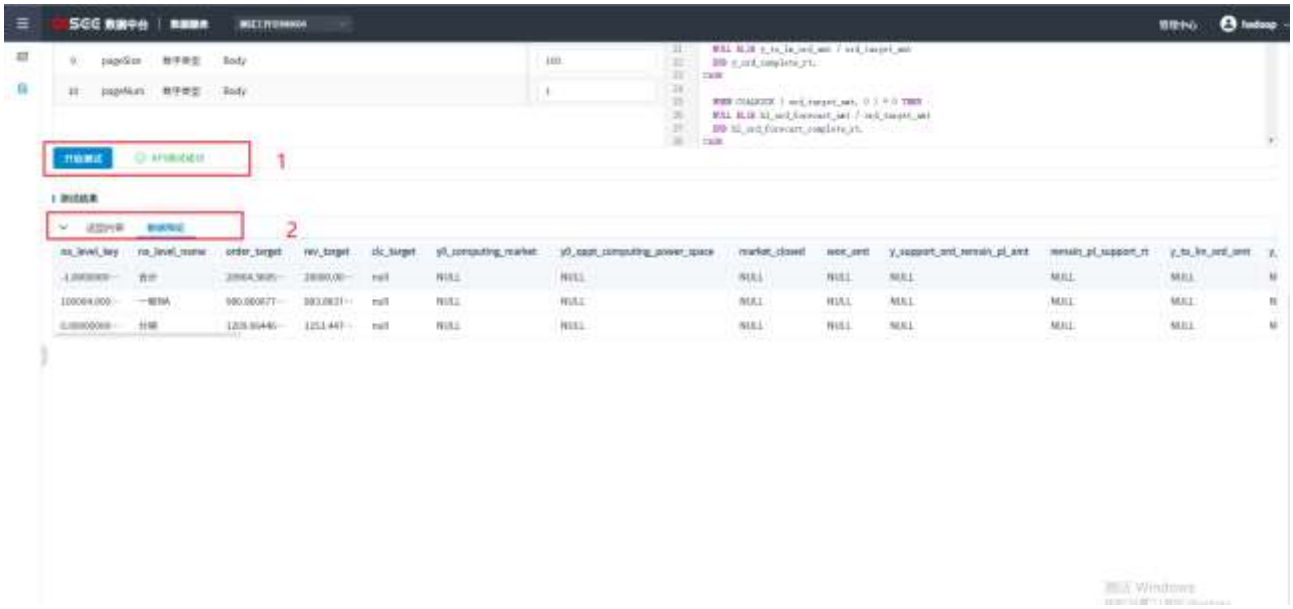
API 列表包含当前空间下所有 API，支持 API 测试、发布、授权、查看和删除等功能。

3.4.6.2.1 API 测试

操作步骤：点击操作列测试按钮，进入 API 测试界面，点击开始测试 API 进入测试中状态，根据脚本执行情况返回 API 运行结果：

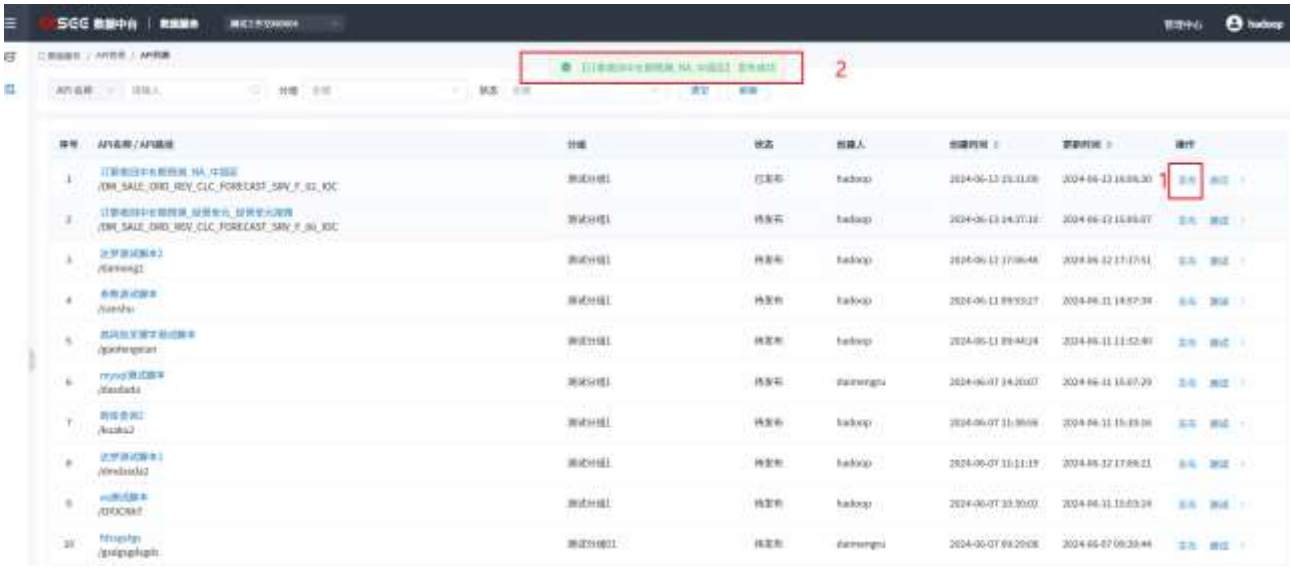


测试成功 API 支持查看 API 返回内容和数据预览信息：



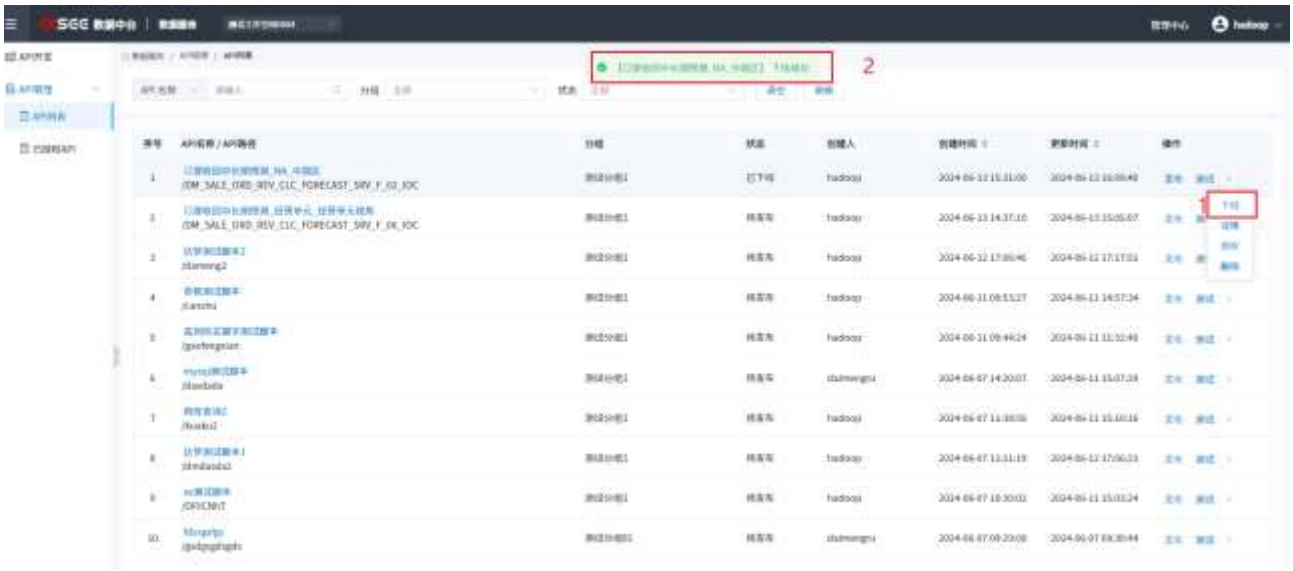
3.4.6.2.2 发布 API

仅支持发布已测试通过 API，选择测试成功 API，点击发布按钮，API 发布成功：



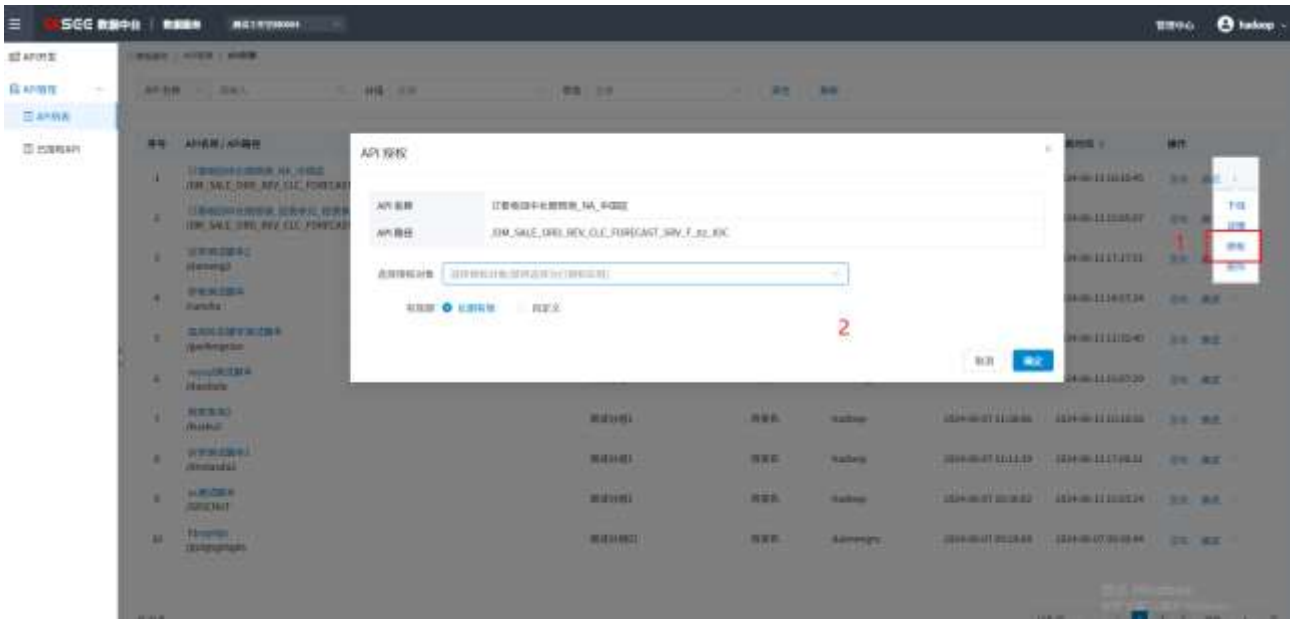
3.4.6.2.3 API 下线

当已发布 API 下没有已授权应用时，支持操作下线，点击下线按钮，API 下线成功，已下线 API 不支持操作授权：



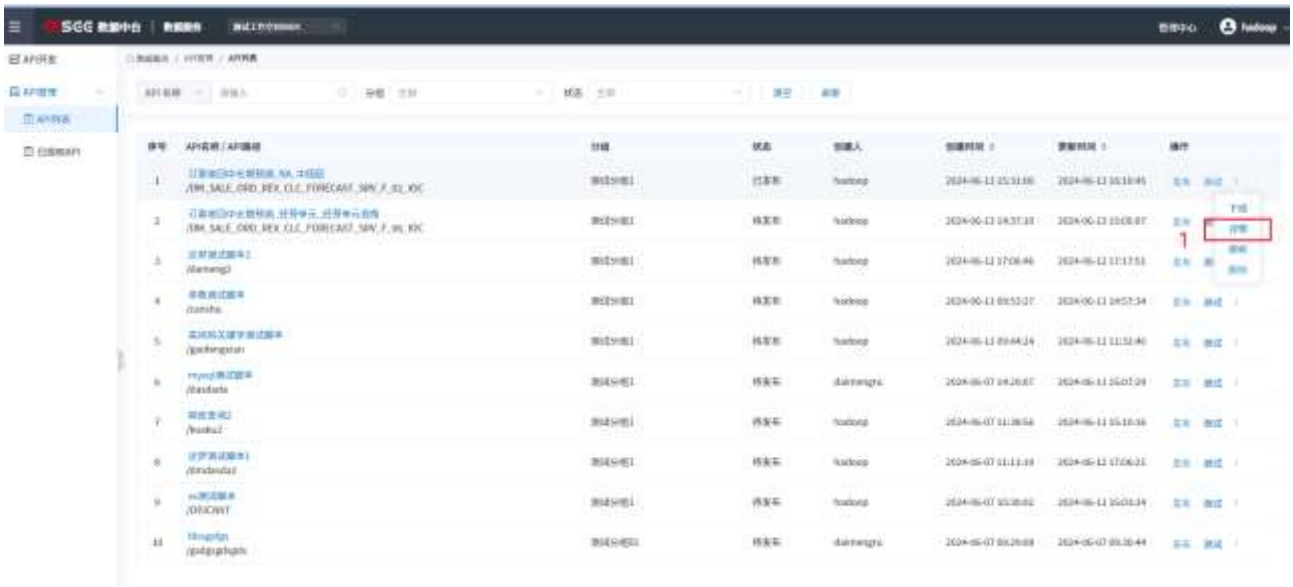
3.4.6.2.4 API 授权

操作步骤：仅支持对已发布 API 操作授权，点击授权按钮，弹出授权设置界面，选择授权应用对象（支持批量选择），设置授权有效期，默认长期有效，支持自定义时间区间，点击确定按钮，授权成功，已授权应用可在 API 授权列表查看：



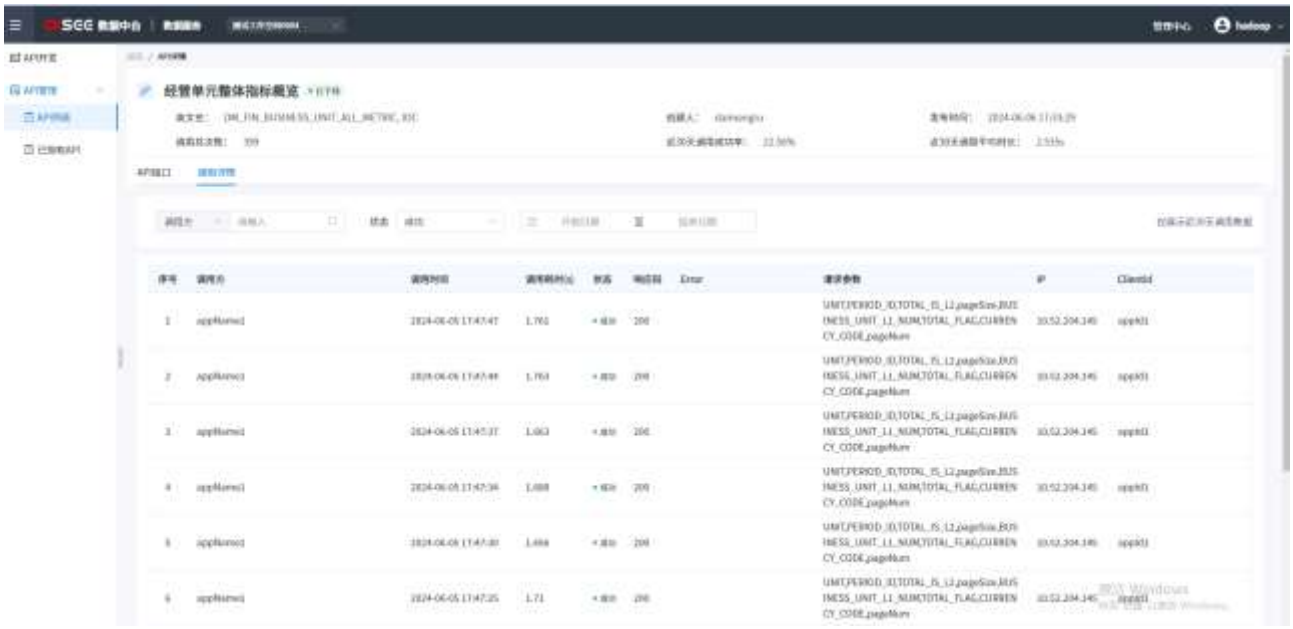
3.4.6.2.5 查看 API 详情

操作步骤：点击 API 详情按钮，跳转至 API 详情页面，详情页面包含 API 基本信息和调用详情：



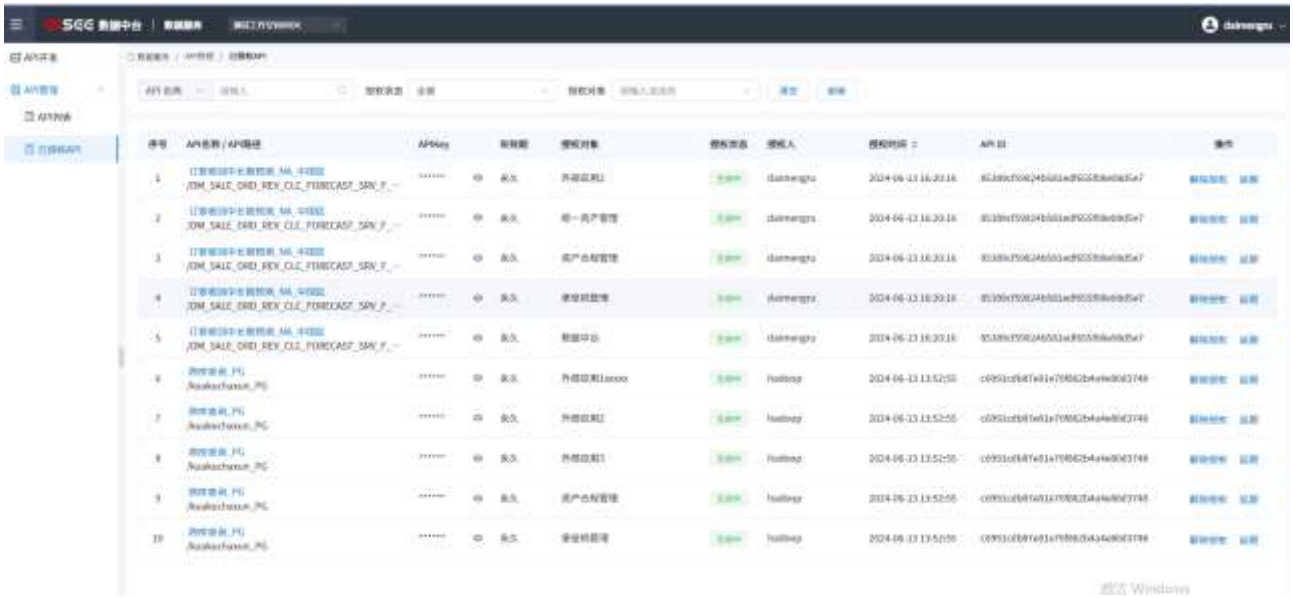
基本信息页面包含 API 调用内容、脚本信息和参数请求返回示例：

调用详情页面可查看所有应用对 API 的调用情况，用于监控 API 调用分布和请求结果

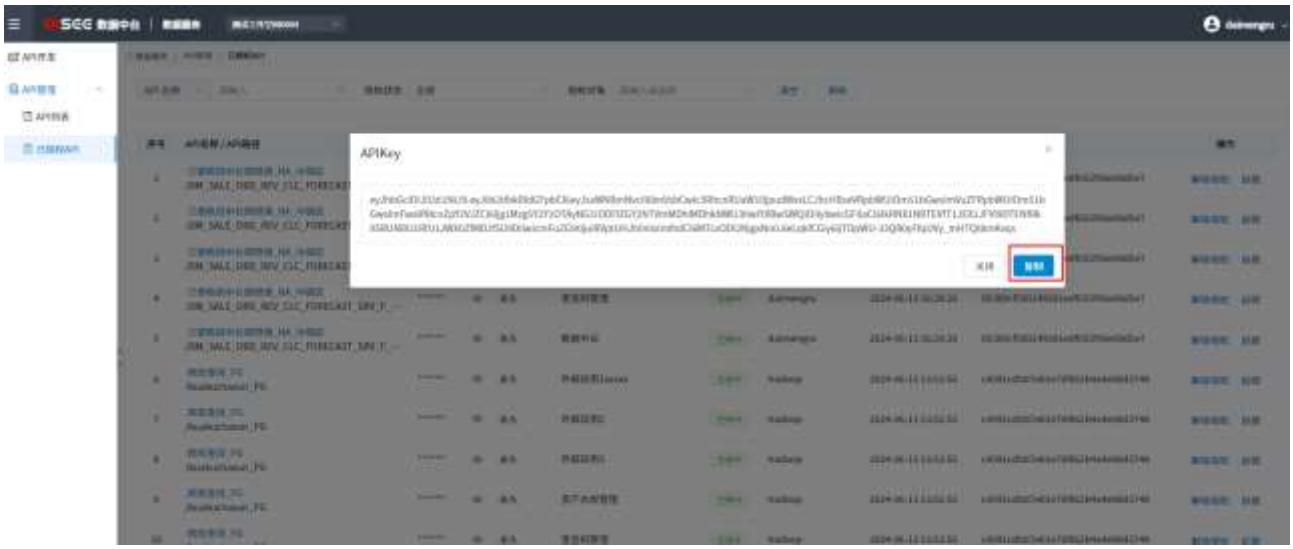


3.4.6.3 API 管理-已授权 API

已授权 API 列表包含所有应用已授权 API 信息，支持查看已授权 API 鉴权值 APIKey，可对已授权 API 操作解除授权和延期：



点击列表 APIKey 查看 icon，弹出 APIKey 查看弹窗，支持一键复制内容：

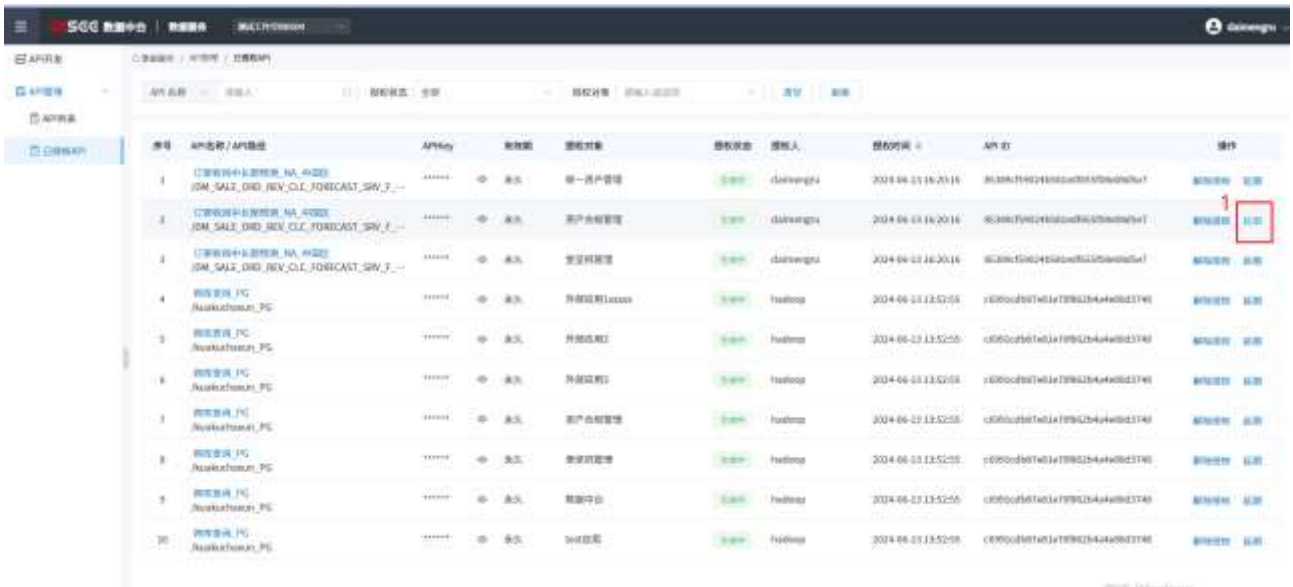


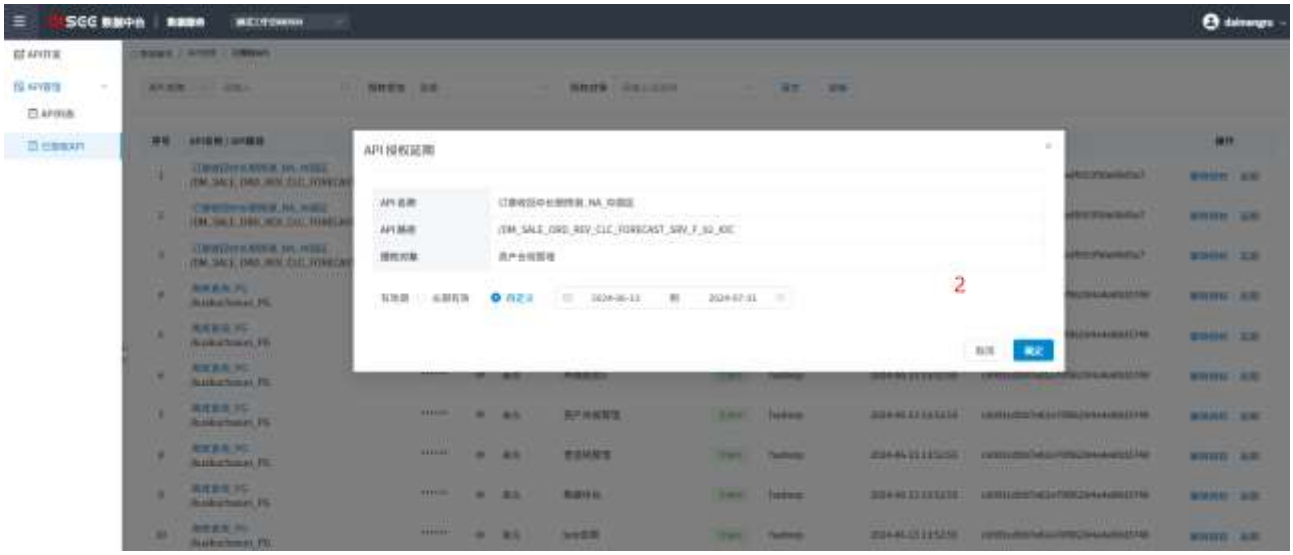
3.4.6.3.1 API 解除授权

选择需要解除授权的应用信息，点击解除授权按钮，API 解除授权成功，已解除授权的应用无法再次调用该 API：

3.4.6.3.2 授权延期

操作步骤：选择需要延期授权的应用信息，点击延期按钮，弹出 API 授权延期弹窗，重新设置 API 授权有效期，点击确定按钮，API 延期授权设置成功，应用系统将按照最新的授权区间调用 API：





3.4.6.4 API 调用

所有已授权的 API 均支持通过三方平台调用，以已授权 API 为例，API 参数设置：

API 请求地址：http://xdataservice-sit.beta.xfusion.com/req/xdservice/api/execute/DM_SALE_REQ_FCT_CM_SUM_F_BUSI_02_IOC6

请求协议：HTTP

请求方式：post

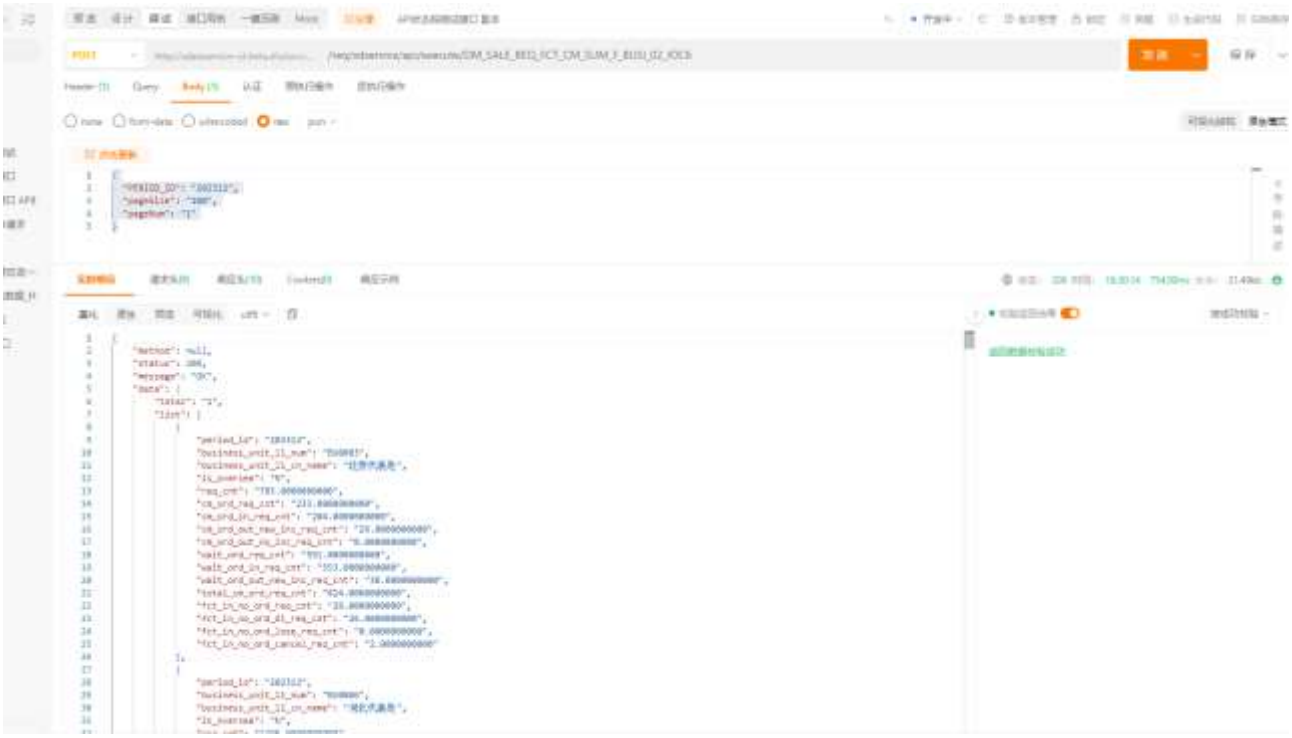
请求 header 增加参数 apikey，参数值取已授权列表中 APIKey：

eyJhbGciOiJIUzI1NiJ9.eyJ0b2tlbkRldGFpbCI6eyJsaWNlbnNvciI6bnVsbCwic3RhcnRUaW1lIjpudWxsLCJhcHBseVRpbWUiOm51bGwsImVuZFRpbWUiOm51bGwsImFwaVNlcnZpY2VJZCI6ImY4MTUyOWY2NWVhYzE5NjIzYWZkYTY3MmNhYWIyZDY2IiwiYXBwSWQiOiJhcHBJZCIsInBhdGgiOiJETV9TQUxFX1JFUV9GQ1RfQ01fU1VNXOZfQlVTSV8wM19JTOM2IiwicmFuZG9tIjoiUlBmWThUInOsImlhdCI6MTcxNzY2MTIxMXO.-HRAM5JCvcBvxIweWOlf14juOhAy4U3RFmrau_4zpn4

Body 请求参数可参考 API 详情页面中的请求示例，取值如下：

```
{
   "PERIOD_ID": "202312",
   "pageSize": "100",
   "pageNum": "1"
}
```

发送请求，API 调用成功，查看运行结果：



3.4.7 数仓管理

3.4.8 安全数据资产

3.4.9 数据质量

3.5 敏感数据管理

3.5.1 敏感数据识别

功能配置：在系统管理/应用管理/应用配置功能下，可以配置敏感数据管理的菜单顺序以及是否启用。

3.5.1.1 敏感数据管理

3.5.1.1.1 规则配置

3.5.1.1.1.1 查询规则

【功能说明】列表为分页列表每页展示数量可以自由选择。列表上方可以对规则进行高级筛选，筛选条件有 规则名称，规则类型（关键字，正则表达式），是否内置，创建时间。重置按钮可以清除查询条件。

列表的左侧是规则的分组和右侧的列表内容联动 左侧规则组支持按关键字进行模糊搜索

3.5.1.1.1.2 新增规则

【功能说明】点击列表上方的新增按钮，右侧弹出新增输入框，可以新增规则，输入 规则名称，所属分组，规则类型，规则定义，样例验证后点击确定安全完成新增操作，点击取消，取消此次的新增操作。

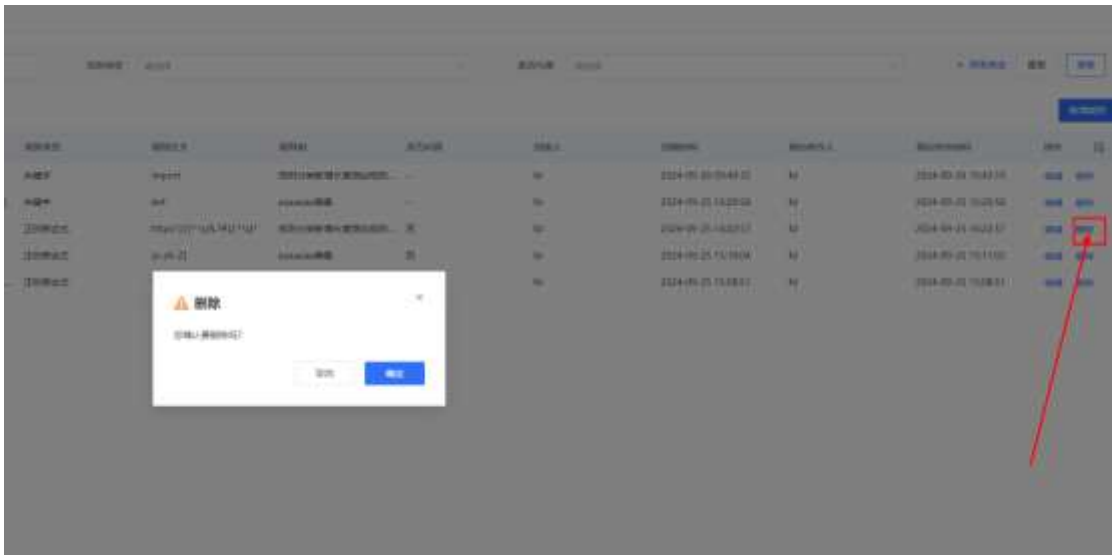
3.5.1.1.1.3 编辑规则

【功能说明】点击编辑按钮屏幕右侧出现弹框可以对规则名称，所属分组，规则类型，规则定义，样例验证进行编辑，点击下方确认按钮完成编辑操作，点击取消，取消编辑操作数据没有变化。

3.5.1.1.1.4 删除规则

功能说明：点击操作列的删除按钮可以对当前行数据进行删除操作。点击完删除按钮，弹出确认删除弹框，点击确定之后删除数据，点击取消，取消删除操

作。



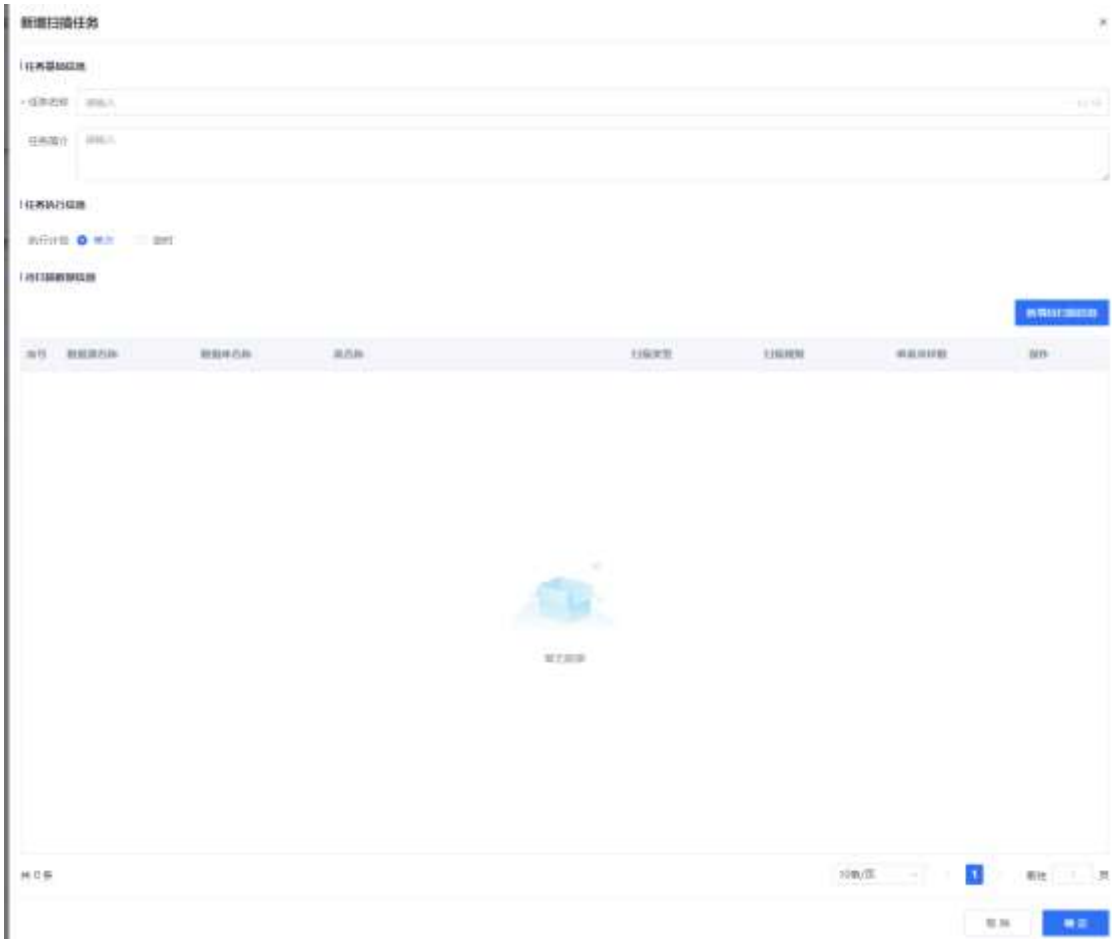
3.5.1.1.2 敏感资产扫描

3.5.1.1.2.1 任务列表查询

【功能说明】输入任务名称，执行次数，任务状态（未开始，已完成，进行中，已中止）进行任务的筛选搜索，点击重置对搜索条件进行清除。

3.5.1.1.2.2 新增任务

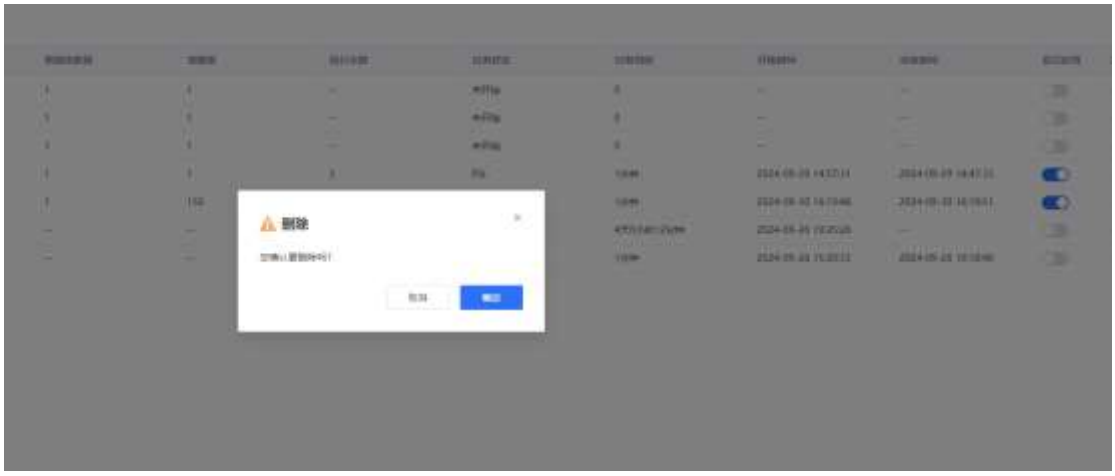
【功能说明】新增点击新增任务按钮可以新增扫描任务，输入任务名称，任务简介，任务的执行计划，



任务创建的同时也要指定待扫描的信息，待扫描的任务针对需要扫描的数据源信息进行配置。需要添加数据源名称，数据库名称，表名称（可以部分指定或者选择数据库中所有的表），扫描类型可以按规则组分配或者指定具体的某一个规则。最后配置一下单表的采样数。

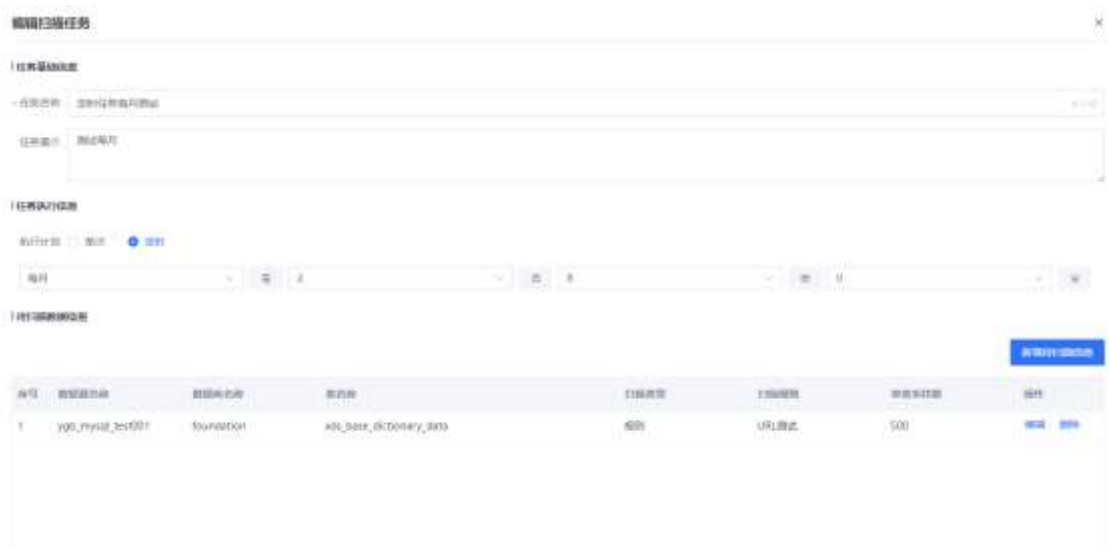
3.5.1.1.2.3 删除任务

【功能说明】点击操作列的删除按钮可以删除某行数据，弹出二次确认框 ，点击确认完成删除操作，点击取消撤销此次删除操作。



3.5.1.1.2.4 编辑任务

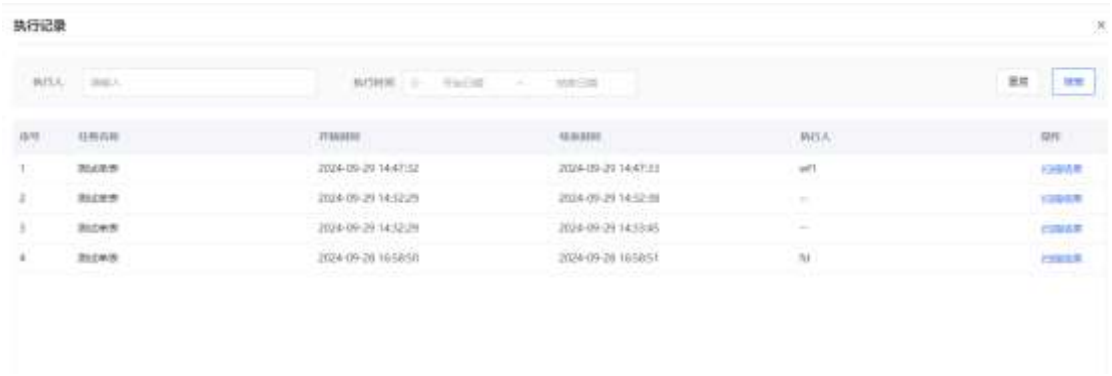
【功能说明】点击编辑按钮，可以对当前任务的基本信息以及扫描对象进行编辑操作，点击确认按钮保存修改信息生效。



操作列的执行按钮点击执行立即执行一次任务。

操作列详情功能是一个分页展示主要展示一下信息包括数据源的名称，数据库的名称，表名称，扫描规则，和扫描进度。并且提供了三个筛选条件：数据源名称，数据库名称，表名称，可以对列表内容进行查询过滤。

操作列的执行记录功能：分页展示任务的名称以及开始时间，结束时间，执行人，以及扫描结果。并且在列表上方提供了两个过滤的查询条件：执行人，执行时间。可以对列表内容进行筛选。重置按钮可以清空删选条件。



3.5.1.2 敏感数据展示

【功能说明】敏感数据扫描任务的执行结果会在此页面进行展示。

3.5.1.2.1 敏感数据源树形展示

【功能说明】左侧树形结构为 敏感数据源的树形展示包括数据源的表结构信息

3.5.1.2.2 页面信息查询

【功能说明】分页查询搜索条件有所属任务，字段名称，重置按钮可以清空搜索条件。列表展示内容有，表结构的字段名称，敏感标签，数据类型，样例数据，所属数据库，所属数据表，所属数据源，最后发现时间。