密级：公开

文档编号：AQWY-A-014

版本号：V1.1

安全无忧 MSS 平台

使用手册

快页信息技术有限公司

2025 年 07 月 28 日

文档修改记录

版本号	修改内容描述	修改人	日期	备注
V1.0	新建	陈雨萱	2025-07-28	
V1.1	更新截图	陈雨萱	2025-08-13	

目录

1 前言

本用户手册主要介绍了安全无忧平台的使用和管理。通过阅读本文档，用户可以了解系统的基本组成，并使用系统。

本章内容主要包括：

- 文档目的
- 读者对象
- 文档基本内容
- 约定

1.1 文档目的

通过阅读本文档，使用户能够正确地配置使用系统，实现对设备的日志、事件的综合分析，同时能查看下载已生成的报告，满足合规要求和和业务需求。

1.2 读者对象

本用户手册适用于不具有基本网络知识的用户阅读。

1.3 文档基本内容

本用户手册包含以下章节：

- 第一章“前言”，介绍了本手册目的、读者对象、各章节的基本内容、文档约定和技术支持信息。
- 第二章“系统简介”，介绍了系统的功能点、组成等。
- 第三章“初次使用系统”，介绍了系统登录和角色权限。
- 第四章“系统功能使用”，介绍了所有功能模块的使用方法。

1.4 约定

本文档遵循以下约定：

图形界面操作的描述采用以下约定：

“”表示按钮。

点击（选择）一个菜单项采用如下约定：

点击（选择）高级管理 > 特殊对象 > 用户；

文档中出现的提示、警告、说明、示例等，是关于用户在使用本手册过程中需要特别注意的部分，请用户在明确可能的操作结果后，再进行相关配置。

2 平台介绍

安全无忧运营平台是一个专业的安全运维管理平台，致力于为客户提供高效、可靠的安全事件管理与响应服务。平台通过集中采集防火墙的日志、告警、状态及设备信息，并存储于数据库，帮助运营团队全面掌握网络安全态势。

运营人员可通过平台对各类安全事件进行快速验证与处置，确保威胁得到及时响应。同时，平台支持将二次研判后的精准告警信息实时推送至客户，助力客户迅速采取应对措施。此外，我们还会定期向客户提供详细的服务成果报告，帮助客户持续优化安全防护策略，提升整体安全水平。

安全无忧运营中心，让安全运维更简单、更高效！

3 初次使用系统

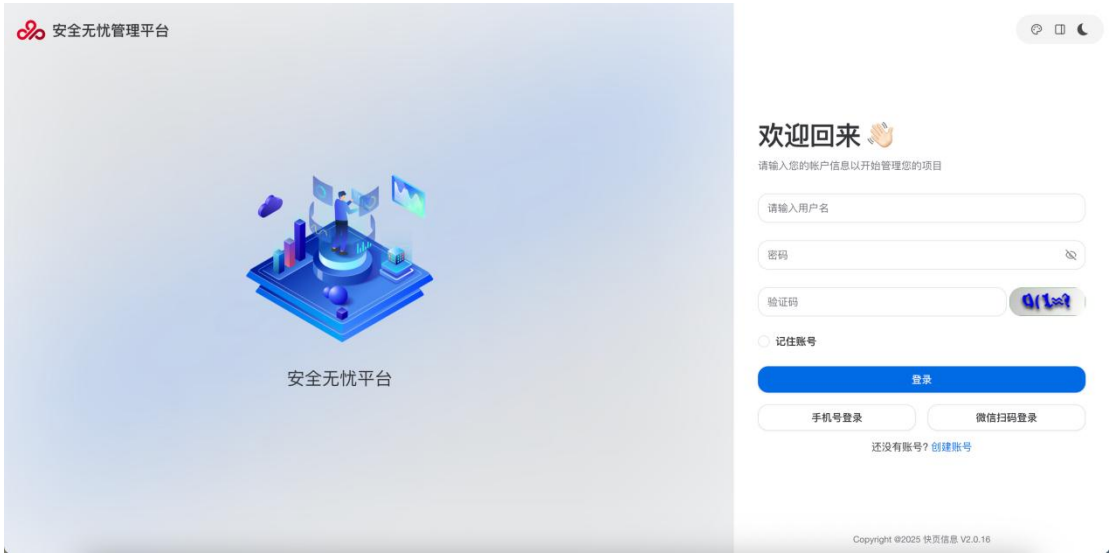

图 3-1 系统登录

Web 管理界面的登录方法：

1）打开浏览器 Google Chrome；（目前推荐浏览器：Google Chrome）

2) 用 HTTP 方式连接 WEB 管理的地址，如：https://mss.wy.link；

3) 回车进入登录页面，输入正确的用户名、密码和验证码（初始账号及密码为问客户经理索要），并单击登录；

4) 登录时连续输入密码错误 5 次后，锁定 15 分钟，支持超级管理员后台密码重置。

4　系统功能使用

4.1　工作台

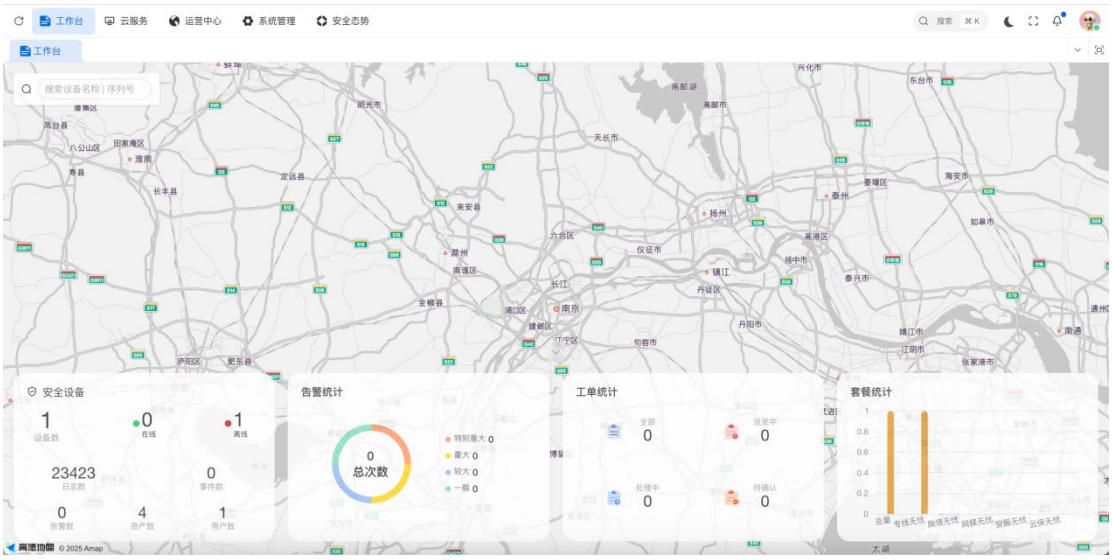

图 4-1 工作台

工作台包含设备地图、设备搜索、安全设备信息、告警统计、工单统计、套餐统计等。

- **设备地图：**地图上以不同颜色的圆圈图标分别标注设备所在地址位置和设备状态，🔴红色表示设备离线、🟢绿色表示设备在线。
- **设备搜索：**可以模糊搜索设备的序列号和设备名称，定位到设备在地图上的地址位置。
- **安全设备：**统计设备数量、在线设备数量、离线设备数量、日志数量、事件数量、告警数量、资产数量和用户数量。
- **告警统计：**针对总告警数量进行统计，以圆环图的形式展现了各个告警级别的占比。
- **工单统计：**统计了全部工单数量、派发中工单数量、处理中工单数量和待确认工单数量。
- **套餐统计：**以柱状图的方式统计了不同类型订单的数量。

4.2　云服务

4.2.1 专线无忧

4.2.1.1　设备管理

设备管理展示所纳管的设备列表，列表项包含：设备名称、设备类型、厂商、状态、版本、设备序列号、套餐状态、坐标、追加信息、备注、注册时间、操作（远程链接、报告历史）。

最上方展示设备总量、在线设备数、离线设备数。

支持按照设备名称、设备序列号、用户名称、注册时间进行组合搜索/筛选。

点击“导出”按钮支持批量导出设备信息。

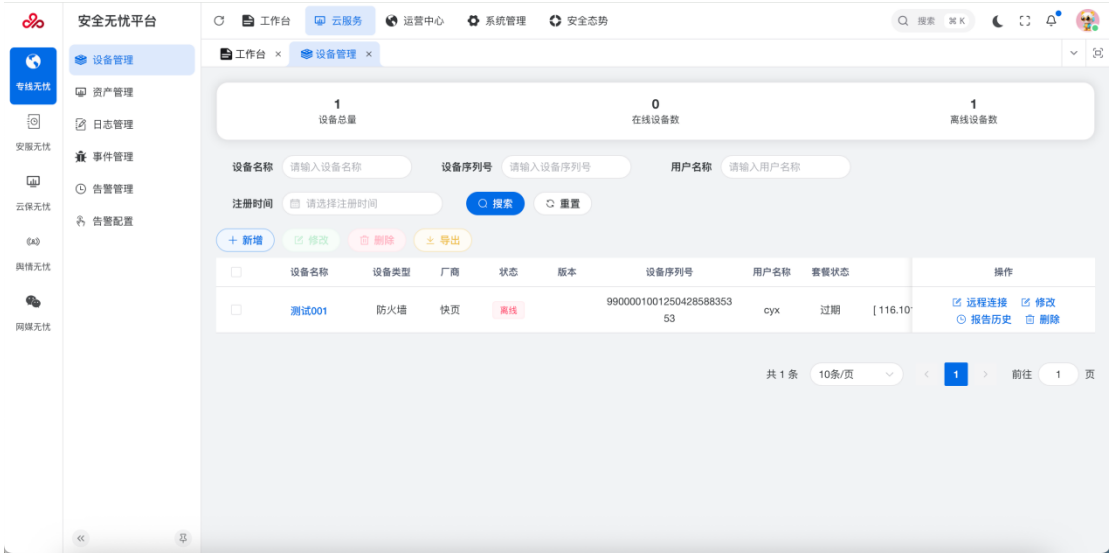

图 4-2 设备管理

点击“设备名称”可以查看设备详情。

图 4-3 设备详情页

点击“远程链接”可以单点登录到设备的管理后台。

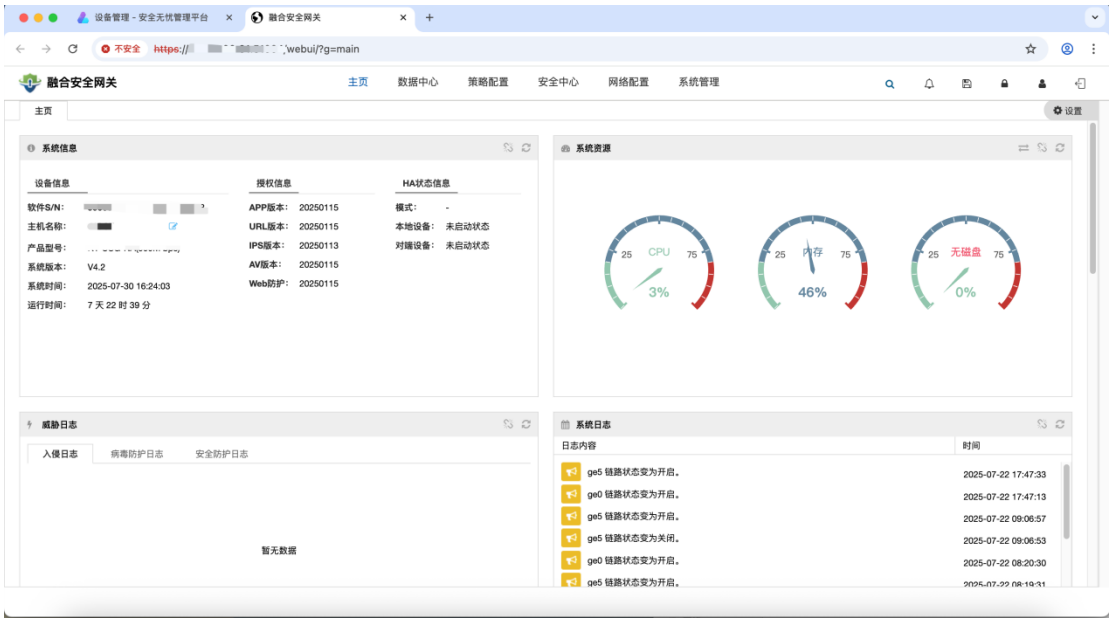

图 4-4 设备后台管理

点击“报告历史”可以查看平台定时生成的周报、月报，可以在线查看，点击“查看报告”可以进行下载和打印的操作。

图 4-5 报告历史

图 4-6 报告详情

4.2.1.2 资产管理

资产管理展示所纳管的资产列表，列表项包含：资产名称、资产类型、资产等级、IP 地址、创建时间、操作（修改、删除）。

支持按照资产名称、资产类型进行组合搜索/筛选。

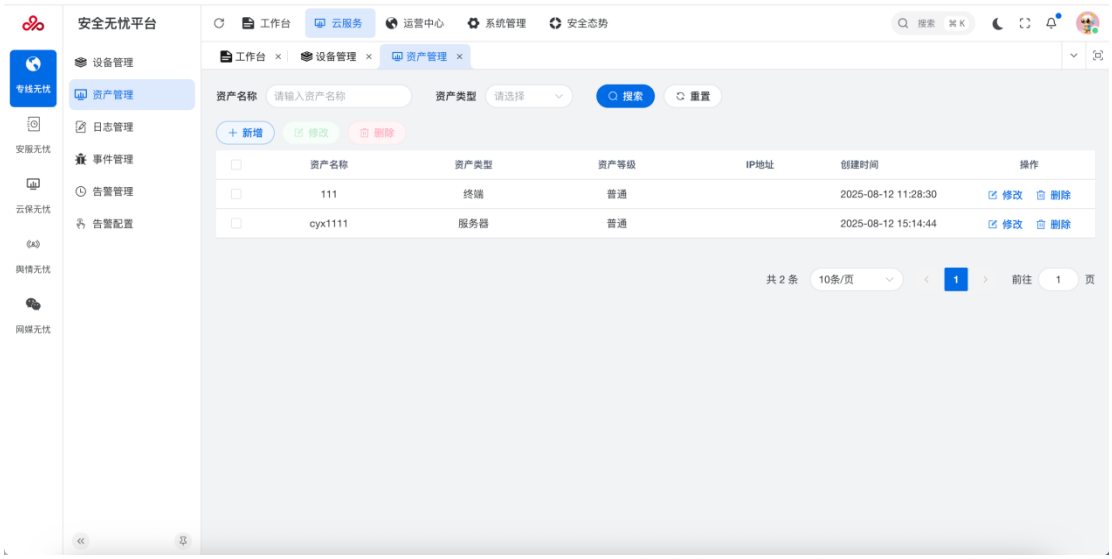

图 4-7 资产管理

点击“新增”按钮可以新增资产，输入对应的资产名称、资产类型、资产等级、设备名称、IP 地址后，点击确认即可成功新增。

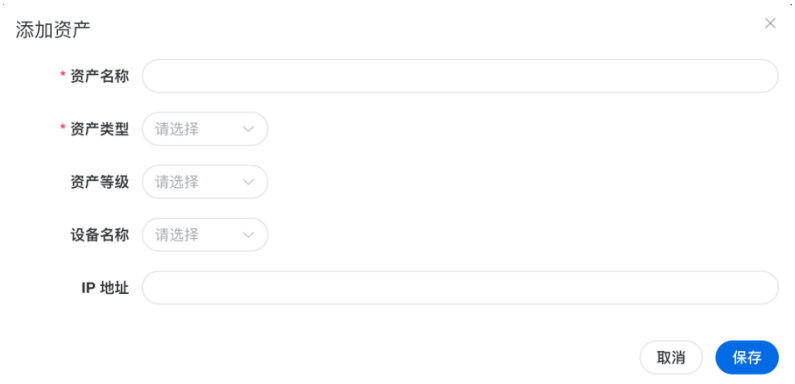

图 4-8 新增资产

点击“修改”按钮可以修改资产信息，修改对应的资产名称、资产类型、资产等级、设备名称、IP 地址后，点击确认即可成功修改。

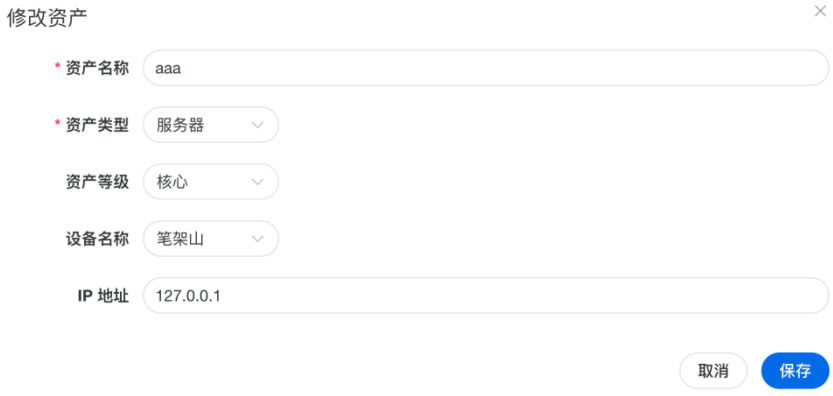

图 4-9 修改资产

点击“删除”按钮，确认后即可成功删除对应资产。

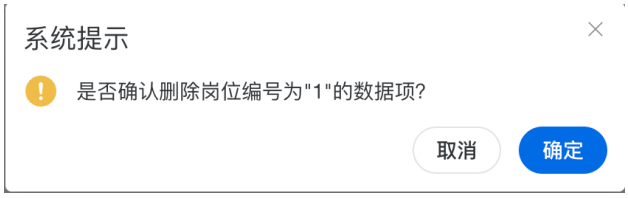

图 4-10 删除资产提示

4.2.1.3 日志管理

日志管理展示所接收到的所有设备原始日志，列表项包含：时间、级别、日志类型、设备序列号、源 IP、源端口、协议、目标位置、目标 IP、目标端口、内容。

支持按照级别、设备序列号、源 IP、源端口、目标 IP、目标端口、日志类型、时间范围进行组合搜索/筛选。

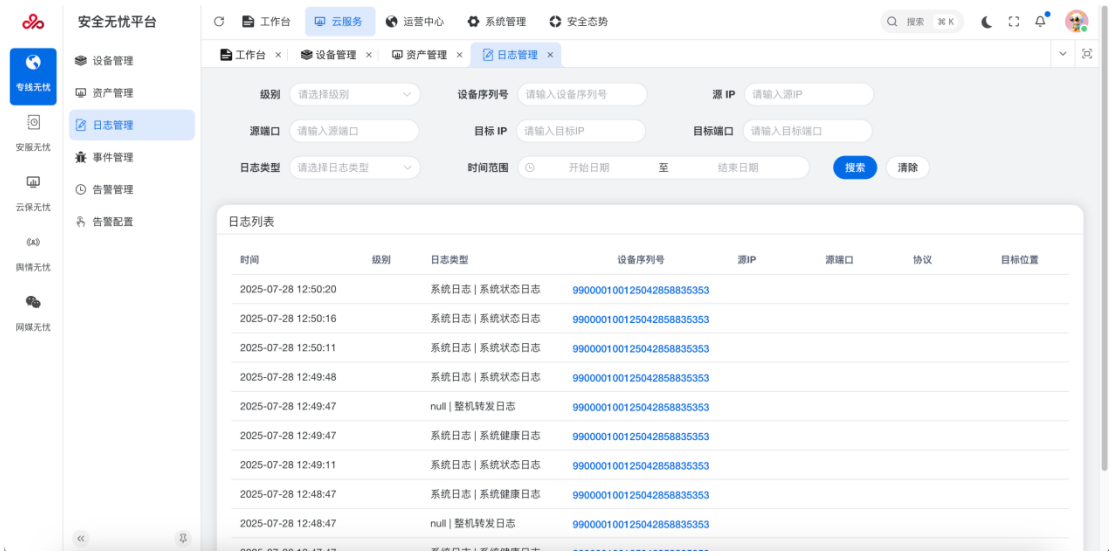

图 4-11 日志管理

点击设备序列号可以查看设备和日志详情信息。

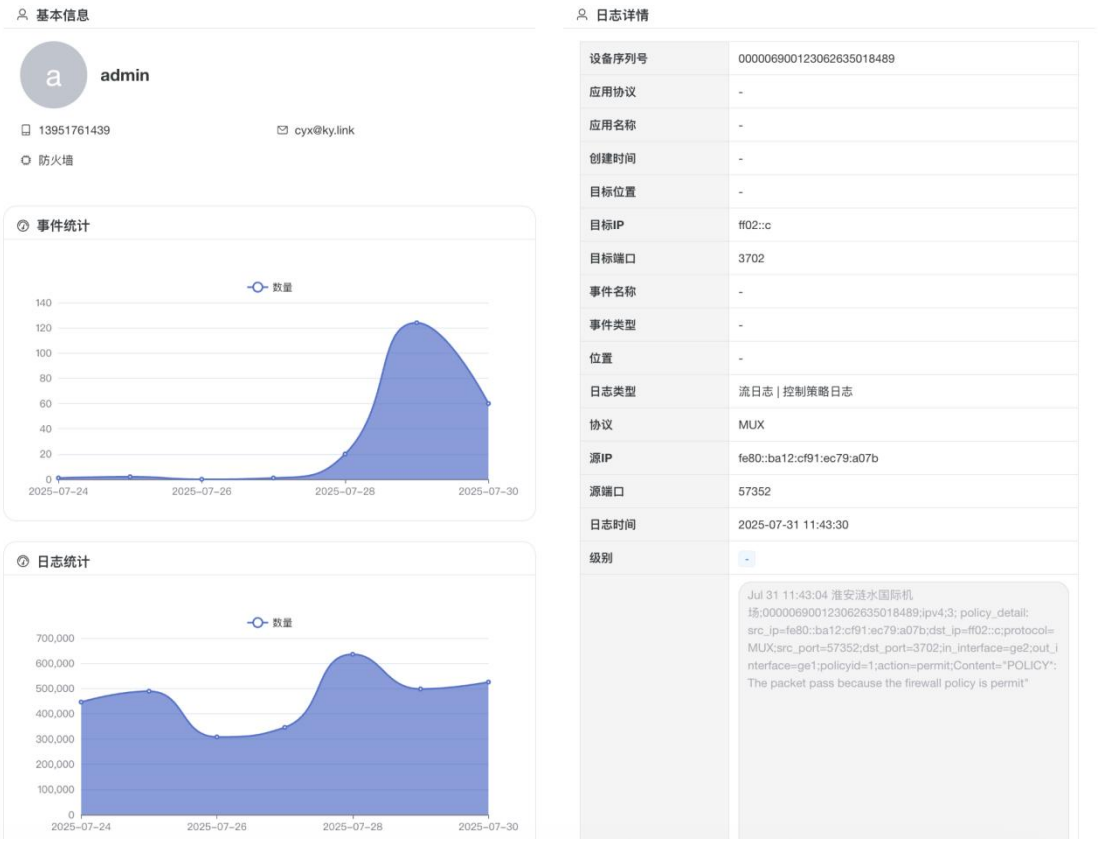

图 4-12 日志详情

4.2.1.4 事件管理

事件管理展示所接收到的所有设备的安全事件，列表项包含：时间、级别、日志类型、设备序列号、源 IP、源端口、协议、目标位置、目标 IP、目标端口、内容。

支持按照级别、设备序列号、源 IP、源端口、目标 IP、目标端口、日志类型、时间范围进行组合搜索/筛选。

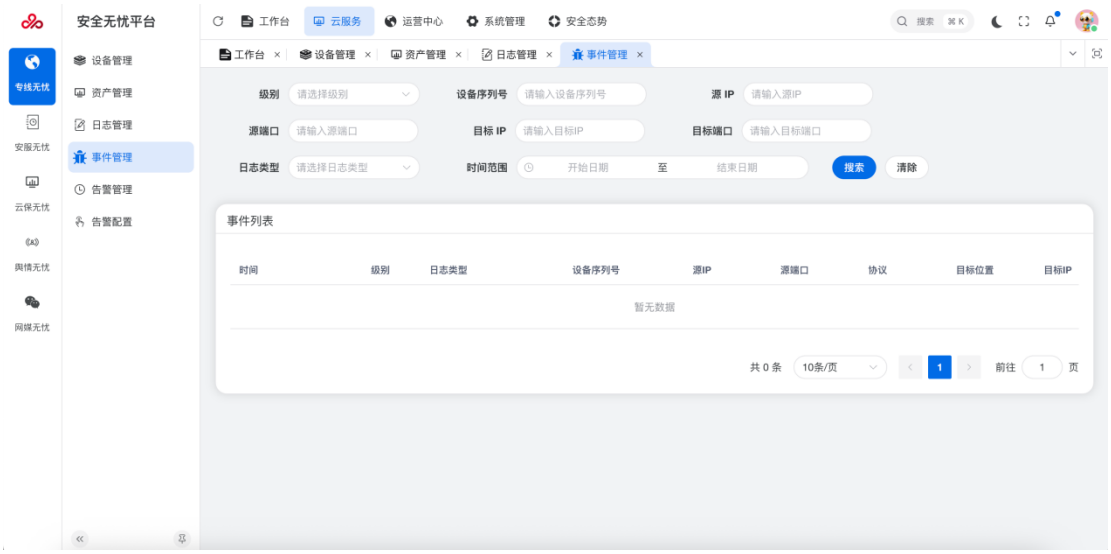

图 4-13 事件管理

4.2.1.5 告警管理

告警管理展示所有匹配到告警规则的安全事件，列表项包含：告警名称、类别、内容、设备序列号、告警状态、告警时间、对应工单 ID、操作（标记状态、创建工单）。

支持按照告警名称、设备序列号、状态、时间范围进行组合搜索/筛选。

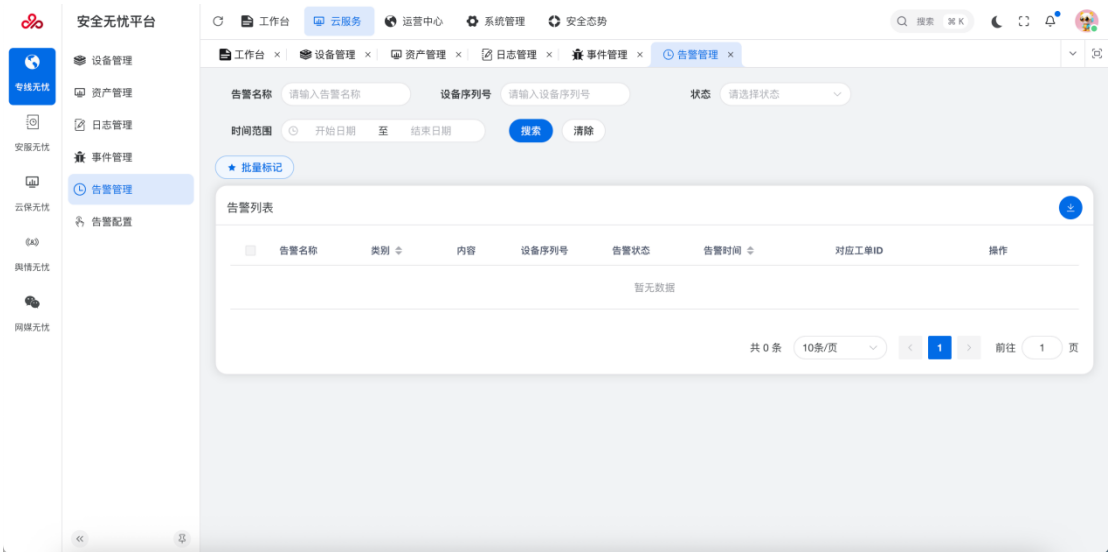

图 4-14 告警管理

点击内容可以查看详细告警详细。

图 4-15 告警详内容

点击操作栏里的“标记状态”按钮可以对该条告警详细进行未处置、已人工处置、忽略三种状态标记，可以进行批量标记操作。

图 4-16 状态标记

点击操作栏里的“创建工单”按钮可以针对该条告警详细进行未处置、已人工处置、忽略三种状态标记。

图 4-17 创建工单

✧ **工单类型：**选择一个工单类型，该工单类型由系统管理员定义。

✧ **工单级别：**输入您认为该工单的紧急级别。

✧ **问题描述：**详细的输入您遇到或需要解决的问题。

✧ **设备序列号：**自动填入。

✧ **套餐名称：**自动填入。

✧ **客户名称：**自动填入。

✧ **开始时间：**选择工单开始时间。

✧ **结束时间：**选择工单结束时间。

✧ **抄送人：**选择工单抄送人。

4.2.1.6 告警配置

告警配置展示所有事件告警规则，列表项包含：预警名称、预警源、预警规则、预警方式、级别、是否内置、创建时间、状态、操作（编辑、删除）。

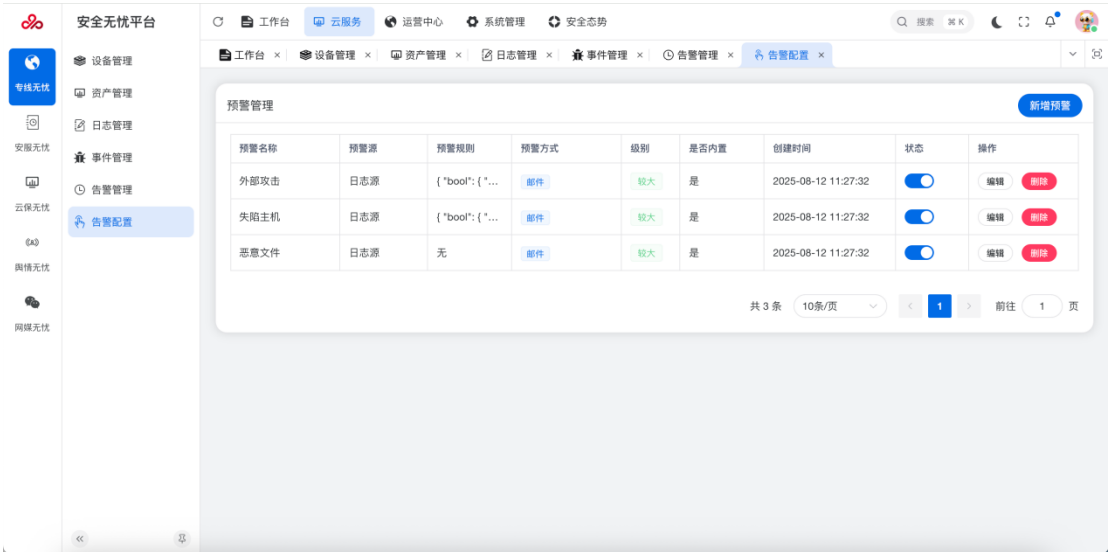

图 4-18 告警配置

点击页面右上角的“新增预警”按钮，填写相关内容点击“确定”后可以创建预警规则。系统默认自带三条预警规则不可删除。

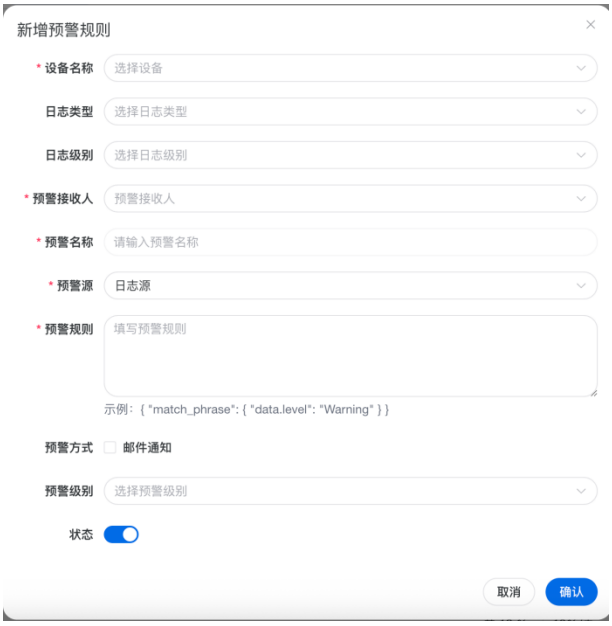

图 4-19 新增预警规则

✧ **设备名称：**选择一个需要预警的设备。

✧ **日志类型：**选择需要预警的日志类型。

✧ **日志级别：**选择需要预警的日志级别。

✧ **预警接收人：**默认是用户自己。

✧ **预警名称：**输入预警名称，如“失陷主机”。

✧ **预警源：**选择需要预警的数据源。

✧ **预警规则：**输入预警规则，如“{ "match_phrase": { "data.level": "Warning" } }”。

✧ **预警方式：**选择预警方式。

✧ **预计级别：**输入预警级别。

✧ **状态：：**选择这条预警规则状态。

4.2.2 安服无忧

如果您订购了安服无忧相关的服务，例如漏扫、渗透、等保等服务，客服会为你开通订单，在这个页面可以看到您所有安服无忧的订单。

列表项包含：服务 ID、用户、服务任务、服务需求、执行时间、执行人员、操作（历史成果）。

支持按照任务名称、执行时间、服务时间进行组合搜索/筛选。

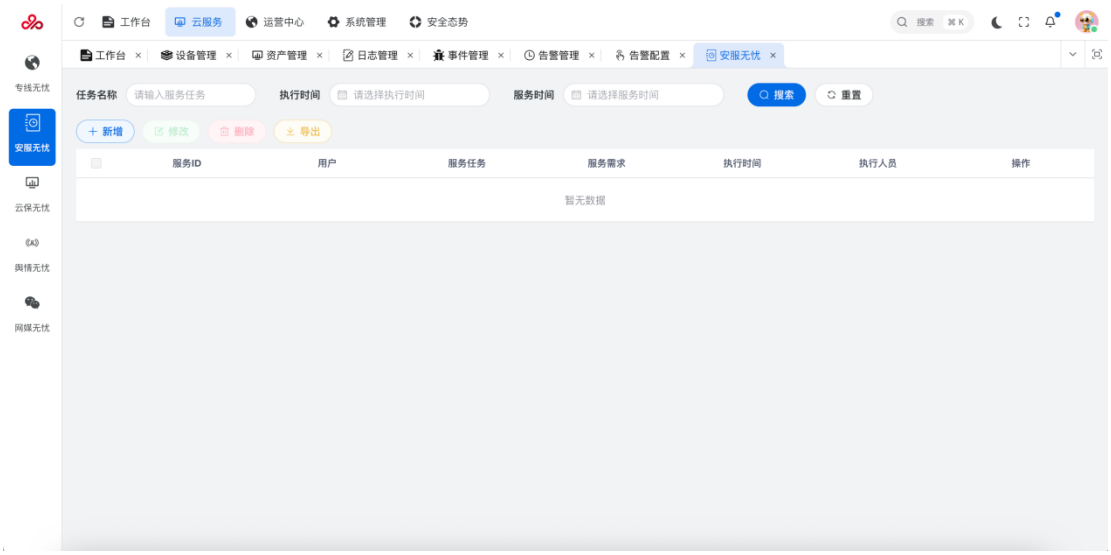

图 4-20 安服无忧

点击操作栏里的“历史成果”，可以看到服务执行人员上传的成果文档。

图 4-21 历史成果

4.2.3 云保无忧

如果您订购了云保无忧相关的服务，点击“云保无忧”可以单点登录到系统里。

图 4-22 云保无忧

4.2.4 舆情无忧

如果您订购了舆情无忧相关的服务，点击“舆情无忧”可以单点登录到系统里。

图 4-23 舆情无忧

4.2.5 网媒无忧

如果您订购了网媒无忧相关的服务，点击“网媒无忧”可以单点登录到系统里。

图 4-24 网媒无忧

4.3 运营中心

4.3.1 订单管理

订单管理展示所有您订购的服务订单，列表项包含：用户、服务类型、设备名称、订单管理、订单类型、创建日期、备注、过期时间、产品组件、产品 URL、三方平台客户 key、产品品牌。

支持按照套餐名称、服务类型、订单号、创建日期进行组合搜索/筛选。

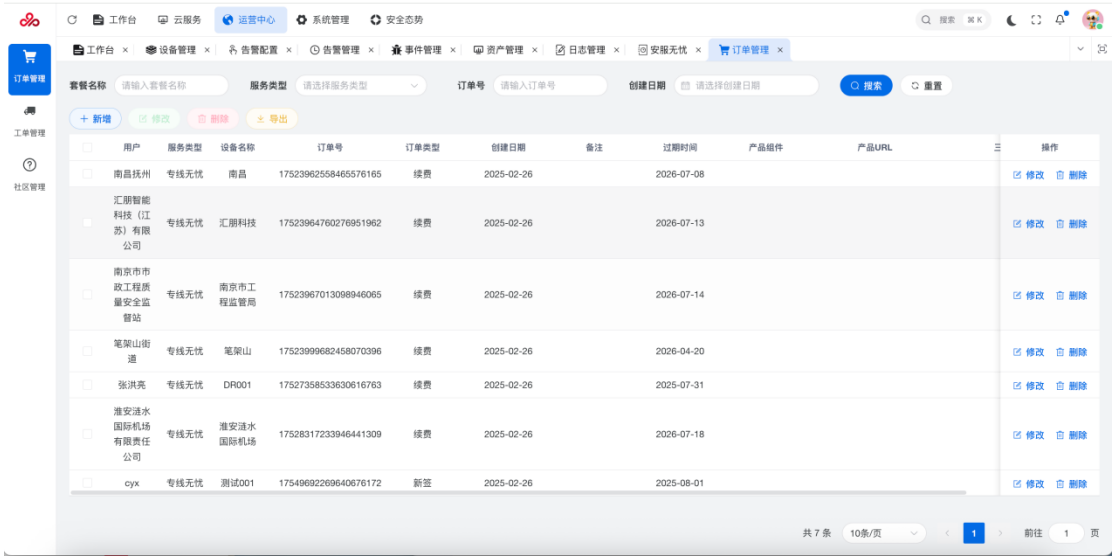

图 4-25 订单管理

4.3.2 工单管理

4.3.2.1 待办

待办展示所有待办的服务工单，列表项包含：序号、ID、流程名称、任务名称、审批人、转办人、未派人、流程状态、激活状态、创建时间。

支持按照任务名称、流程状态、创建时间进行组合搜索/筛选。

图 4-26 待办

4.3.2.2 已办

待办展示所有已办结的服务工单，列表项包含：序号、ID、流程名称、任务名称、审批人、协作类型、协作人、流程状态、审批时间。

支持按照任务名称、流程状态、审批时间进行组合搜索/筛选。

图 4-27 已办

4.3.2.3 抄送

抄送展示所有抄送到你这的服务工单，列表项包含：序号、ID、流程名称、任务名称、抄送人、流程状态、审批时间。

支持按照任务名称、流程状态、抄送人进行组合搜索/筛选。

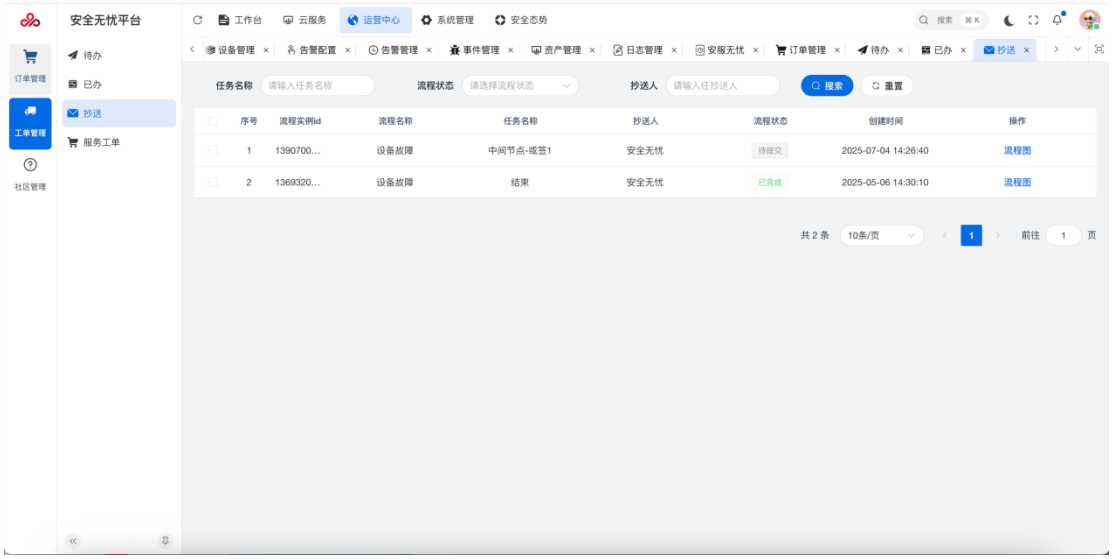

图 4-28 抄送

4.3.2.4 服务工单

服务工单展示所有您新建的服务工单，列表项包含：ID、工单类型、工单级别、问题描述、设备序列号、套餐名称、客户名称、开始时间、结束时间、预估处理时间、流程 ID、节点名称、节点类型、流程状态、操作（新建、删除）。

支持按照工单类型、设备序列号、套餐名称、客户名称、开始时间、结束时间进行组合搜索/筛选。

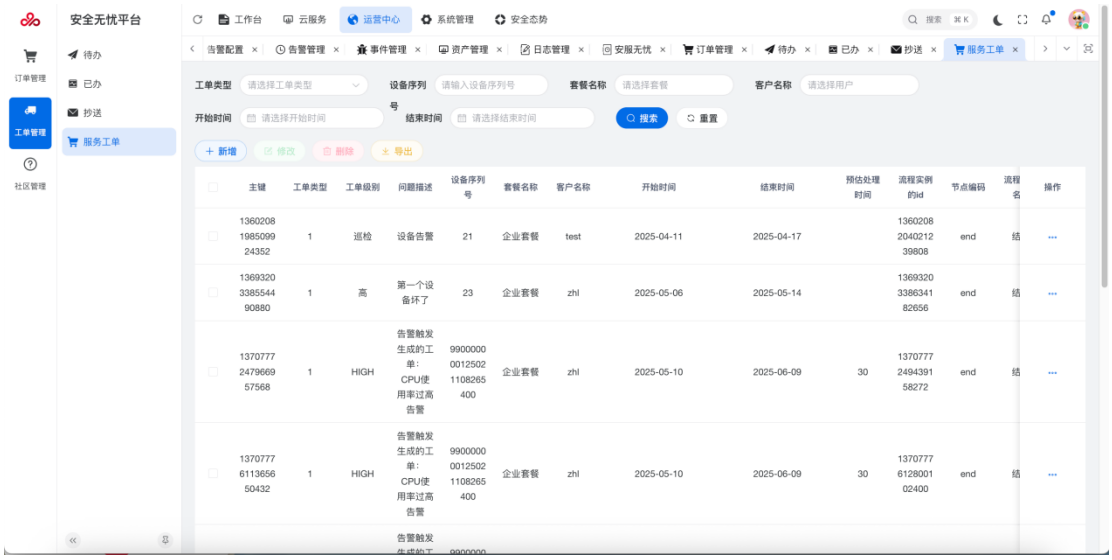

图 4-29 服务工单

点击“新建”按钮，填写相关信息后点击“确认”，即可创建一条服务工单。

图 4-30 新建服务工单

- ✧ **工单类型：**选择工单类型，不同类型的工单对应不同的工单流程。
- ✧ **工单级别：**填写工单级别。
- ✧ **问题描述：**输入您需要解决的问题。
- ✧ **设备序列号：**选择发生问题的设备。
- ✧ **套餐名称：**自动填入。
- ✧ **客户名称：**自动填入。
- ✧ **开始时间：**选择工单开始时间。
- ✧ **结束时间：**选择工单结束时间。
- ✧ **抄送人：**选择工单抄送人。

4.3.3 社区管理

社区管理展示自己所有发帖信息，列表项包含：帖子 ID、帖子标题、作者 ID、用户昵称、分类 ID、状态、备注、操作（修改、删除）。

支持按照帖子标题、作者 ID、用户昵称、分类 ID 进行组合搜索/筛选。

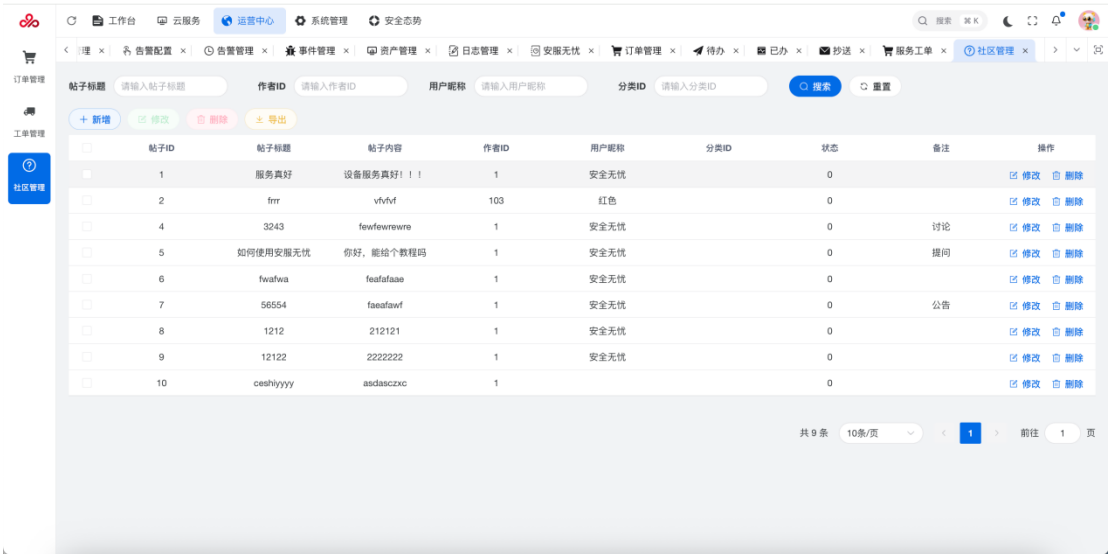

图 4-31 社区管理

点击“新建”按钮，填写相关信息后点击“确认”，即可创建一条帖子。

图 4-32 添加社区帖子

- ✧ **帖子标题：**输入帖子标题。
- ✧ **帖子内容：**输入发帖内容。
- ✧ **作者 ID：**自动填入。
- ✧ **分类 ID：**输入分类。
- ✧ **备注：**输入备注内容。

4.4　系统管理

4.4.1 日志审计

4.4.1.1　平台登陆日志

平台登陆日志展示平台登录信息，列表项包含：访问编号、用户名、地址、登录地点、操作系统、浏览器、登录状态、描述、访问时间。

支持按照登录地址、用户名称、状态、登录时间进行组合搜索/筛选。

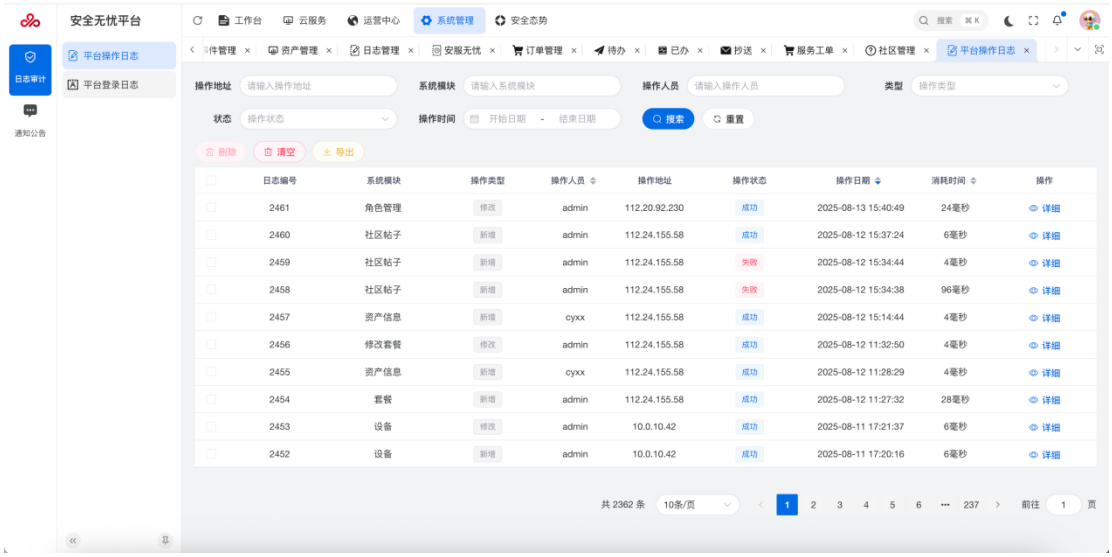

图 4-33 平台登录日志

4.4.1.2　平台操作日志

平台操作日志展示平台操作信息，列表项包含：日志编号、系统模块、操作类型、操作人员、操作地址、操作状态、操作日志、消耗时间。

支持按照操作地址、系统模块、操作人员、类型、状态、操作时间进行组合搜索/筛选。

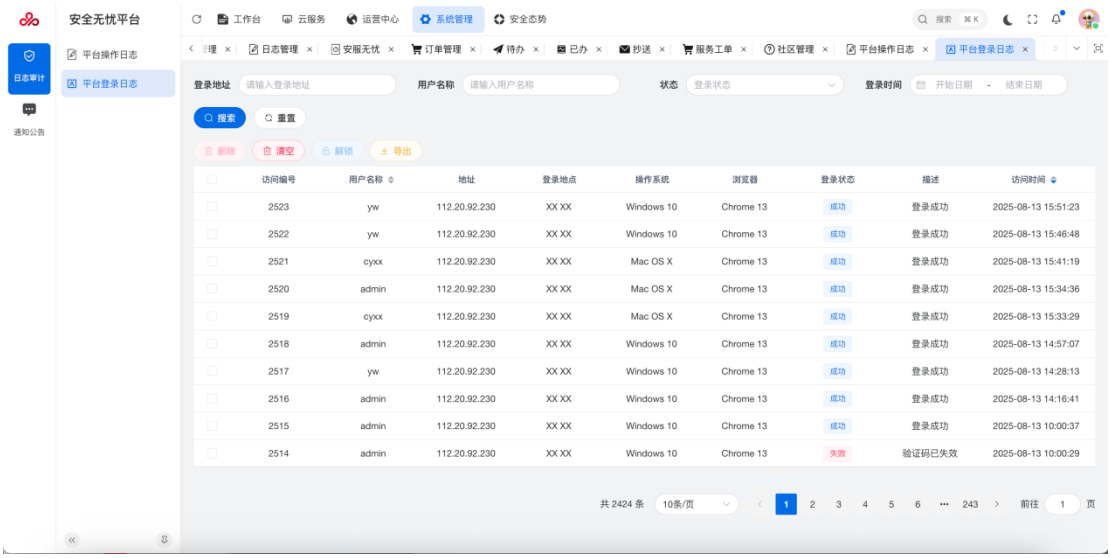

图 4-34 平台操作日志

4.4.2 通知管理

通知管理展示平台通知信息，列表项包含：序号、公告标题、公告类型、状态、创建者、创建时间。

支持按照公告标题、操作人员、类型进行组合搜索/筛选。

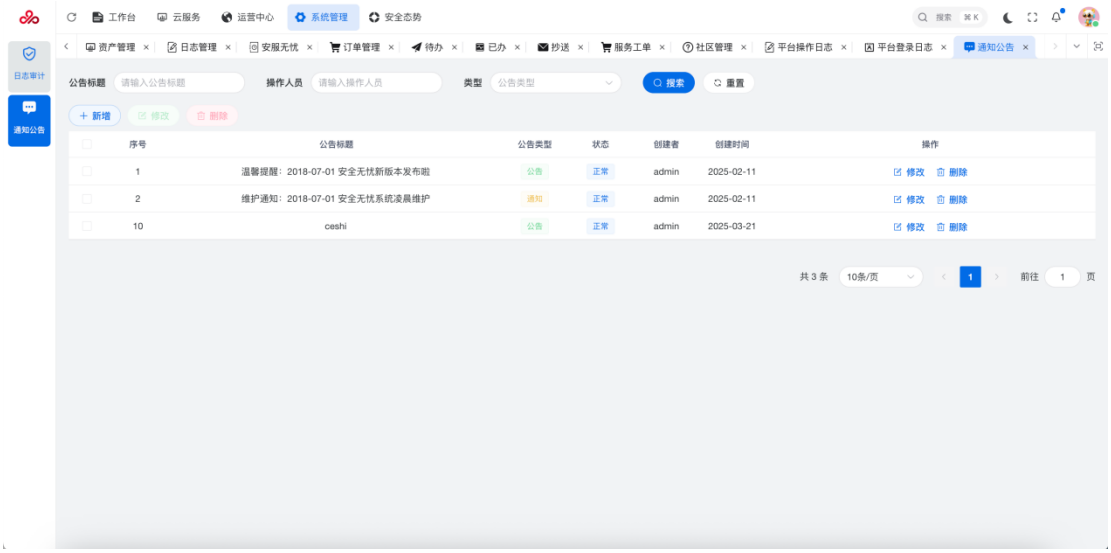

图 4-35 通知管理

4.5 安全态势

安全态势是平台的态势大屏，模块包含：事件类别、事件趋势、事件级别、工单、最近时间、告警级别、告警趋势、告警类别。


工作台
云服务
运营中心
系统管理
安全态势
事件类别
其他
内部威胁
网络攻击
恶意软件
数据泄露
安全
34,272
日志
10,969
事件
24,363
告警
告警类别
其他告警
权限滥用
网络攻击
数据泄露
恶意软件
异常登录
事件趋势
告警趋势
事件级别
信息
紧急
低危
高危
中危
工单
最近事件
事件名称
源IP
目的IP
最近攻击时间
DDoS攻击
112.104.18...
33.255.53.165
2004-03-08...
端口扫描
189.224.18...
52.72.81.226
1989-10-24...
端口扫描
32.94.194.225
69.107.15.112
2022-10-30...
告警级别
提示
紧急
高危
中危
低危

图 4-36 安全态势