乐为运维管理平台 V1.0

用户手册

2021 年 9 月

目录

1. 综述

1.1. 系统概述

乐为运维管理平台是面向 IT 资产的智能化运维管理系统。适应各种平台和运维场景，满足用户实际网络安全运维需求，能将用户个性化的分析方式和处置方式快速实现策略标准化，以期实现用户运维管理标准化和智能化。具有良好的兼容性和扩展性。

平台以资产为核心，使用自动化、智能化技术，实现资产发现、监视和管理资产安全策略状态。针对网络安全设备、数据库等通过预置巡检指标，快速对网络设备、主机系统、数据库和中间件进行健康巡检，实现自动化主动巡防，及早发现安全隐患。系统内置等级保护、行业要求的合规基线，能够手工触发或设置自动化策略，定期执行在线或离线资产的合规评估审计工作，并在评估审计后出具合规报告。

乐为运维管理平台旨在提高网络安全管理和合规运维工作的效率和效果，平台系统完全自主研发，功能模块包括资产管理、基线检查、仿真工具、日志管理和系统管理等。

1.2. 系统运行环境

建议使用谷歌，360，火狐等支持 H5 的浏览器

2. 乐为运维管理平台功能

2.1. 登录

系统采用 BS 架构，在浏览器输入地址后，进入系统登录页（如下图），输入账号、密码，点击登录按钮跳转至管理界面。

登录页

2.2. 功能列表

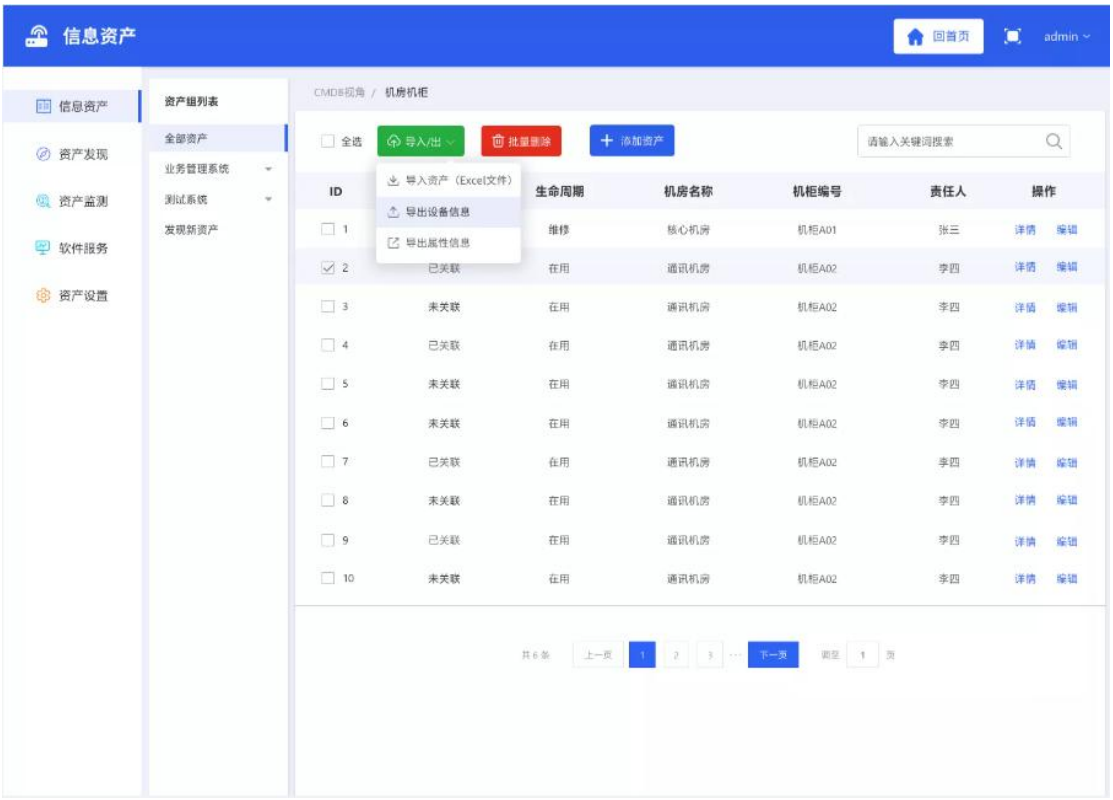
用户登录后默认进入首页，展示该系统的信息资产、安全仿真测试工具、系统设置三个 Banner。

2.3. 信息资产

信息资产主要是提供资产的发现、纳管和基线检查。

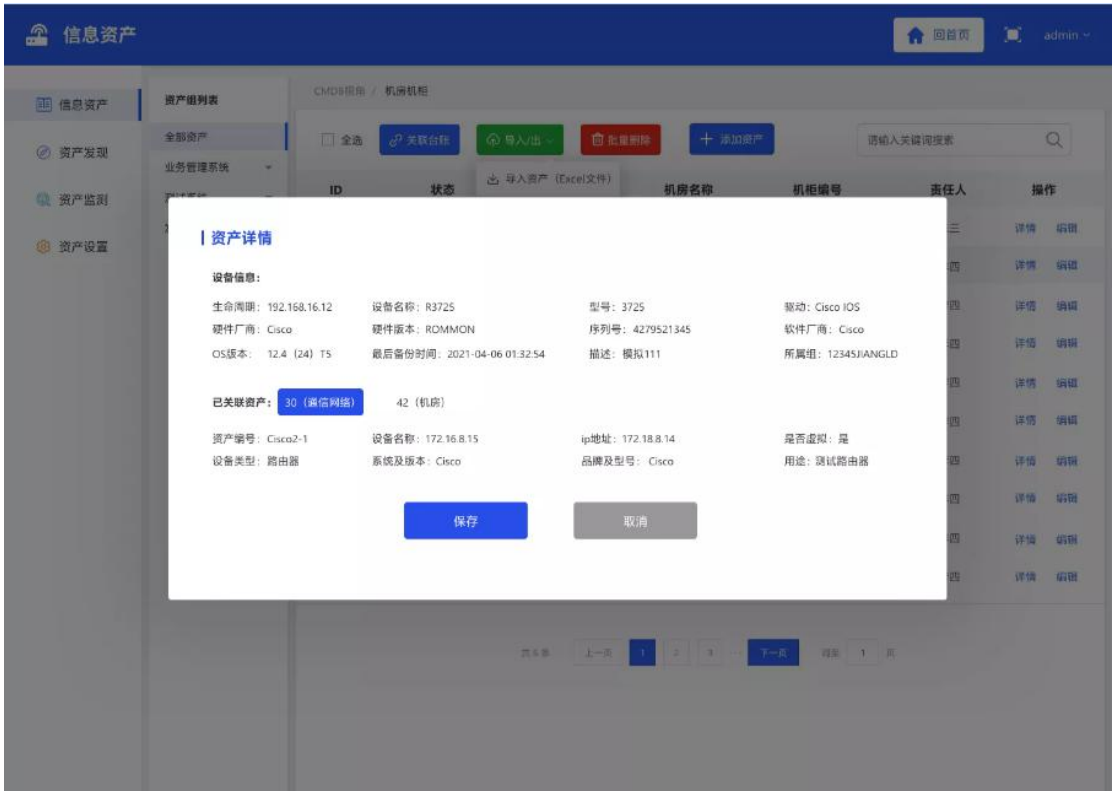
2.3.1. 信息资产

信息资产包括资产列表、资产发现、资产监测、软件服务和资产设置。

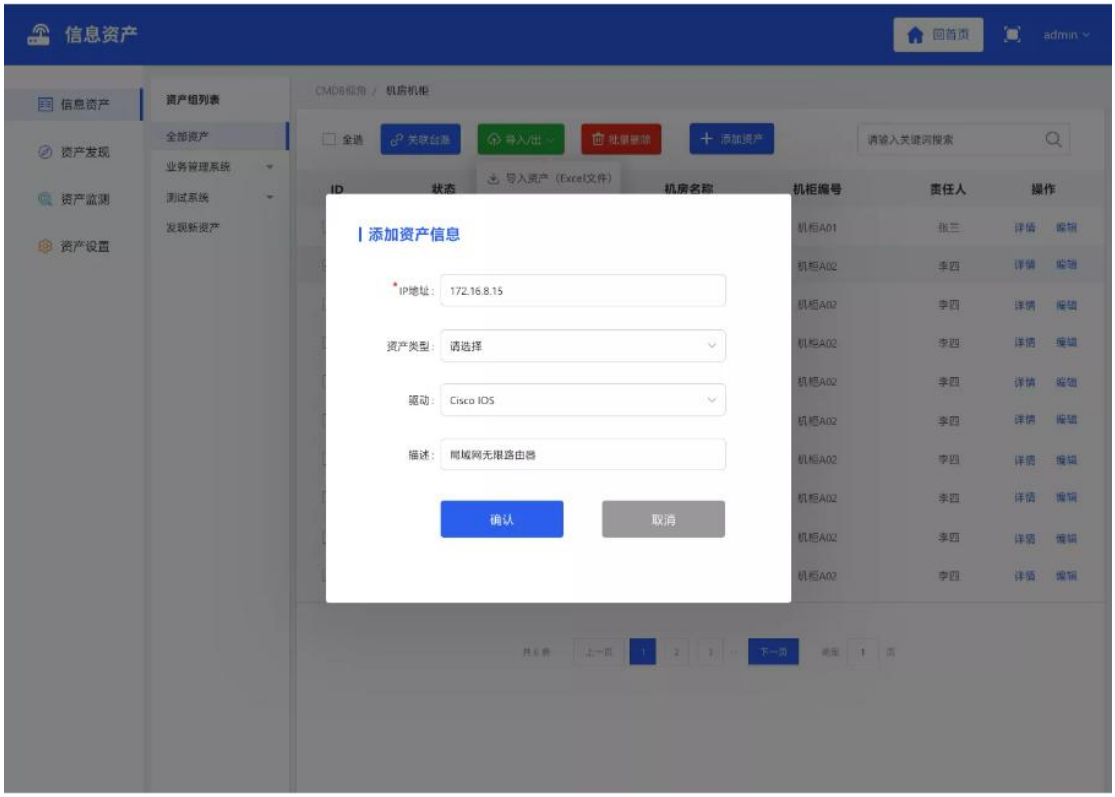


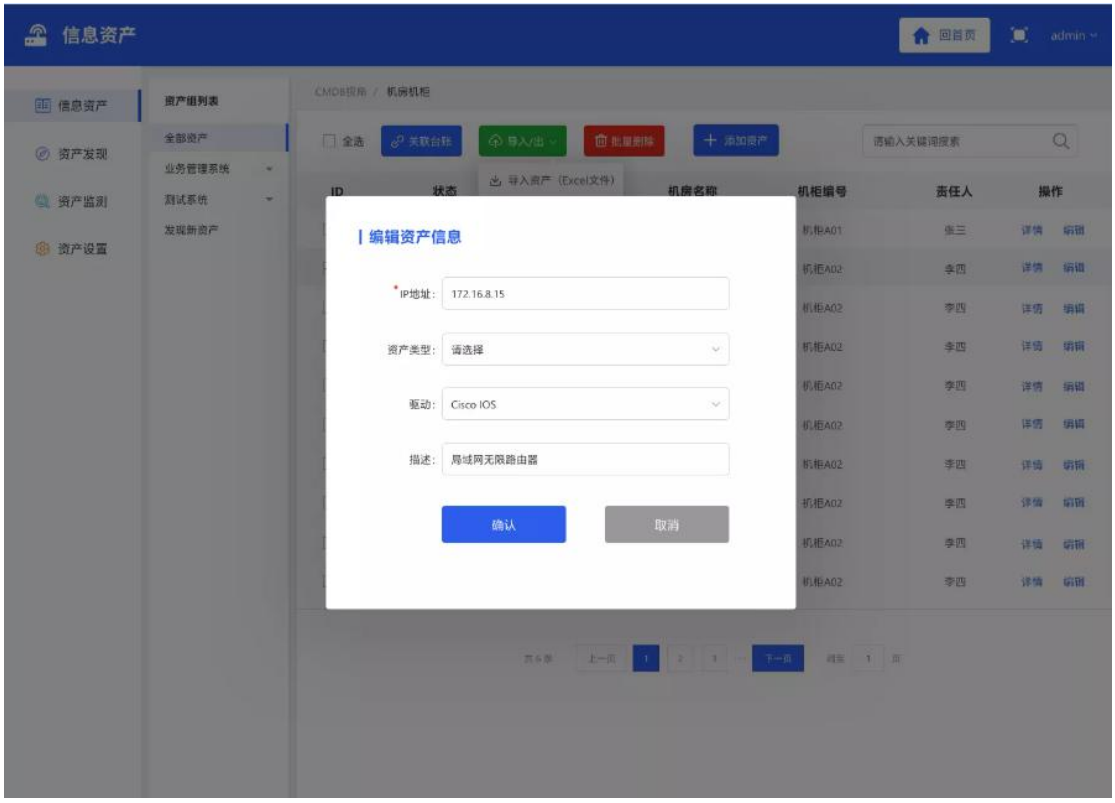
资产列表

双击或者点击“详细”按钮，可以查看资产详情。



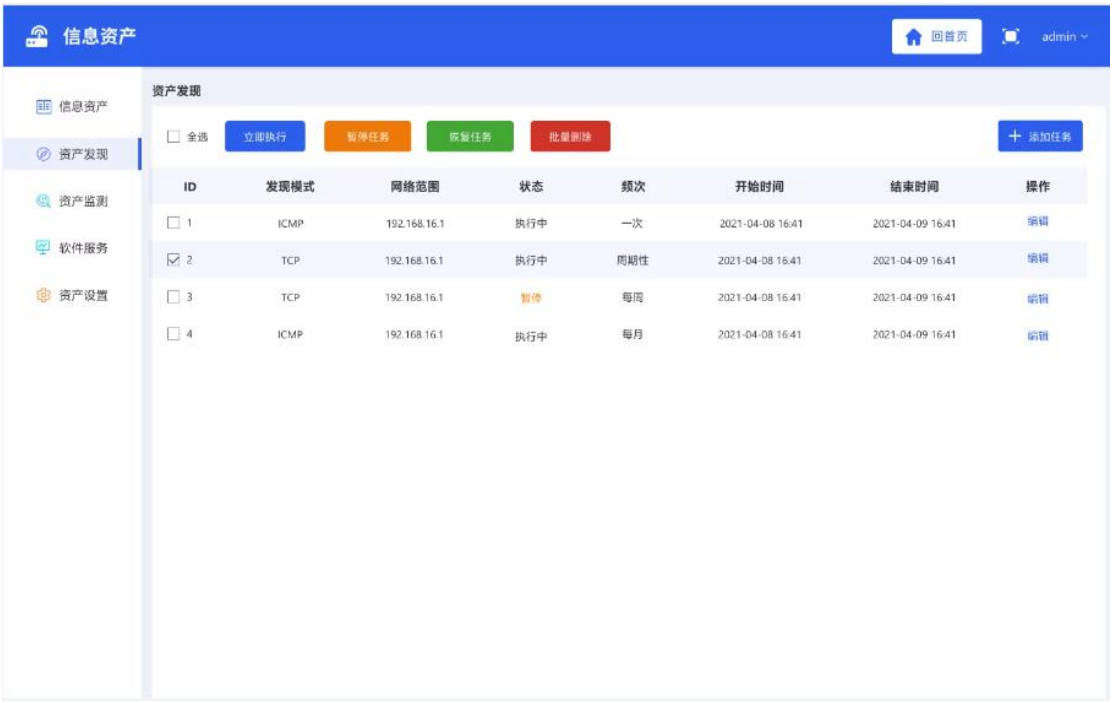
可以手动添加和编辑资产。



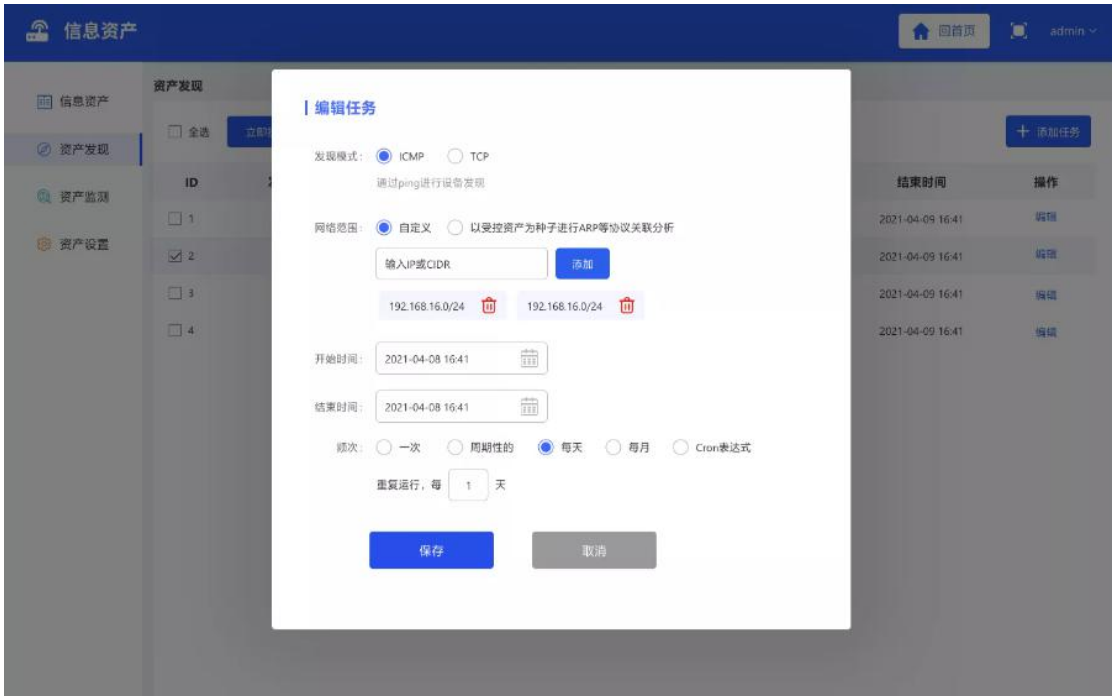


● 资产发现

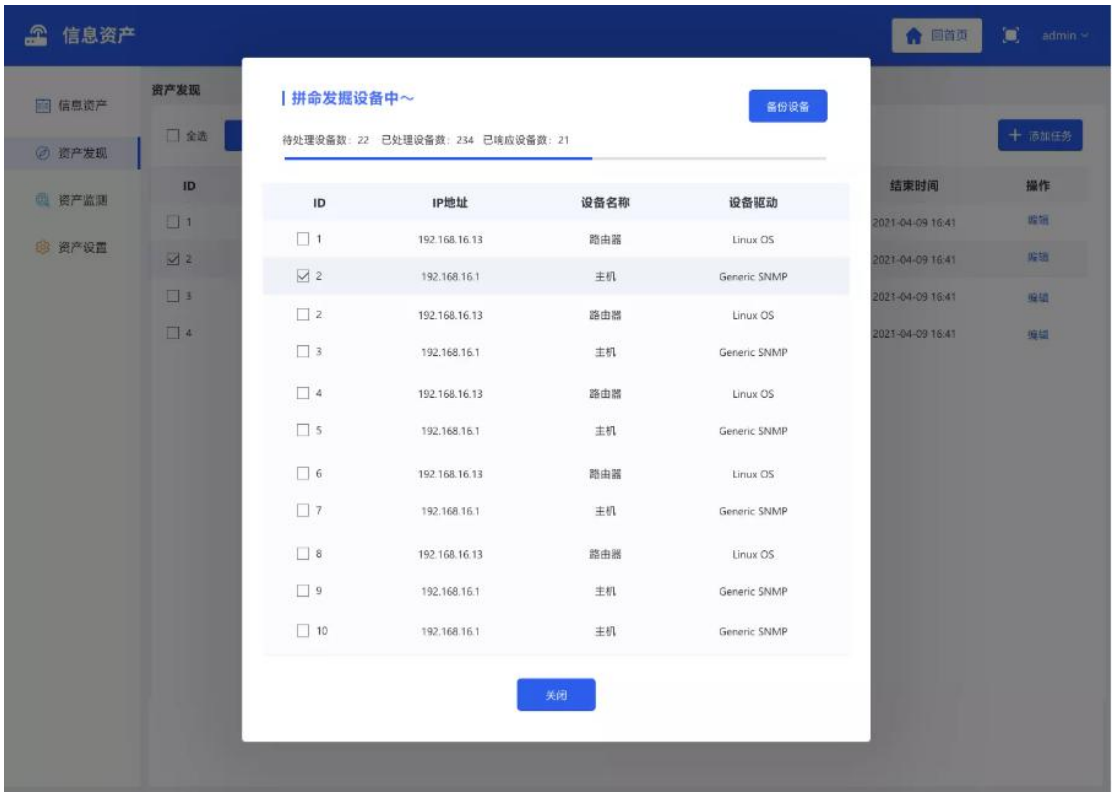
资产发现页面展示所有已经定义的发现任务。



可以添加新增自定义发现任务或编辑现有发现任务。

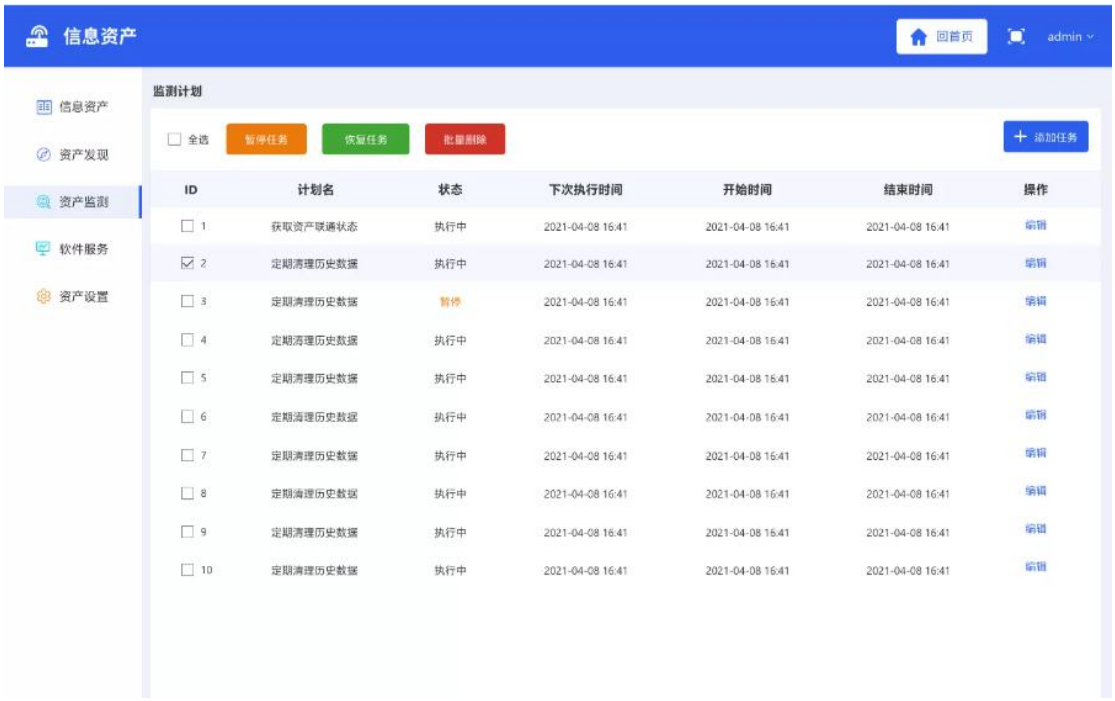


发现的结果通过 Push 方式，将发现的设备信息及时推送到客户端。

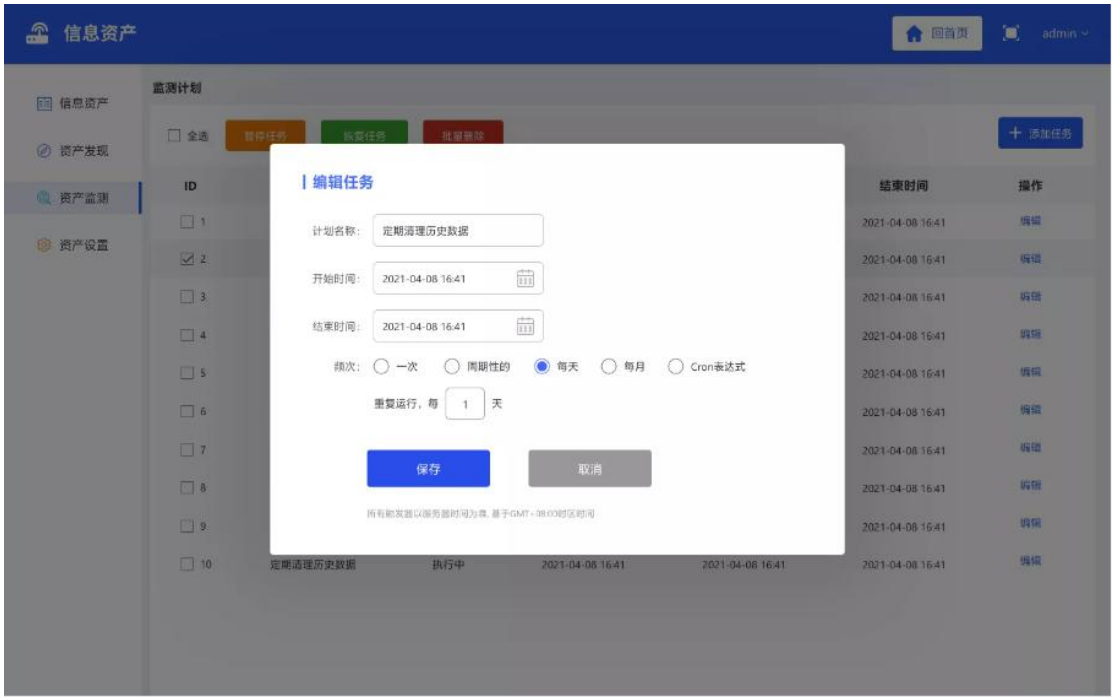


- **资产监测**

资产监测主要是监测资产的在线状态。

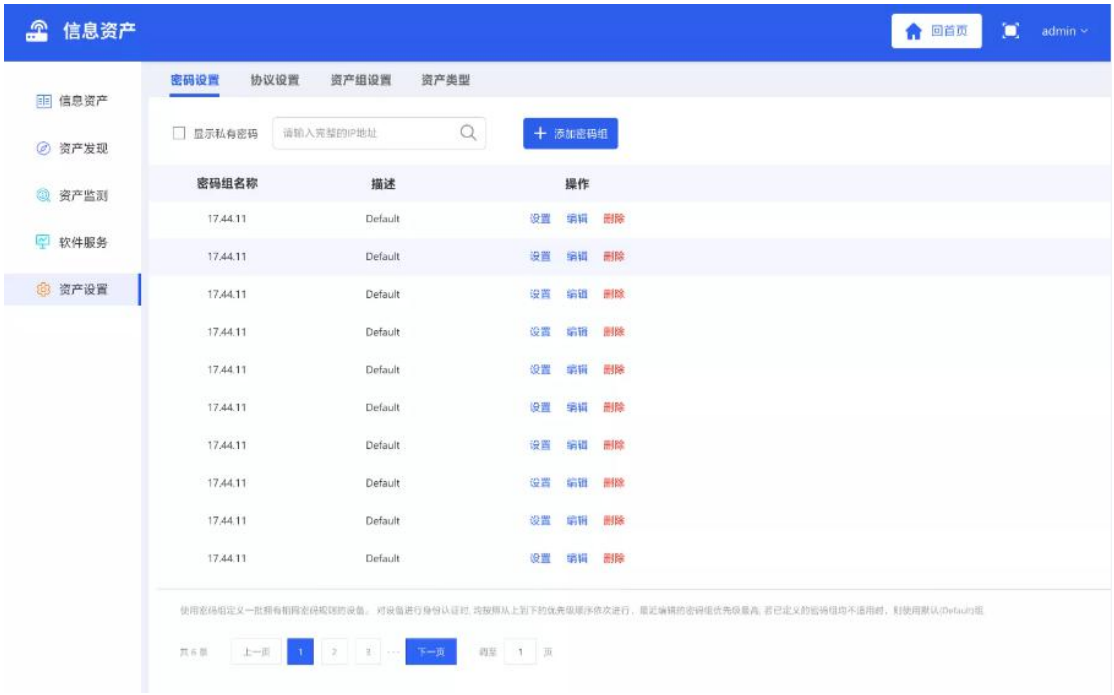


可以定义不同的监测频次任务。

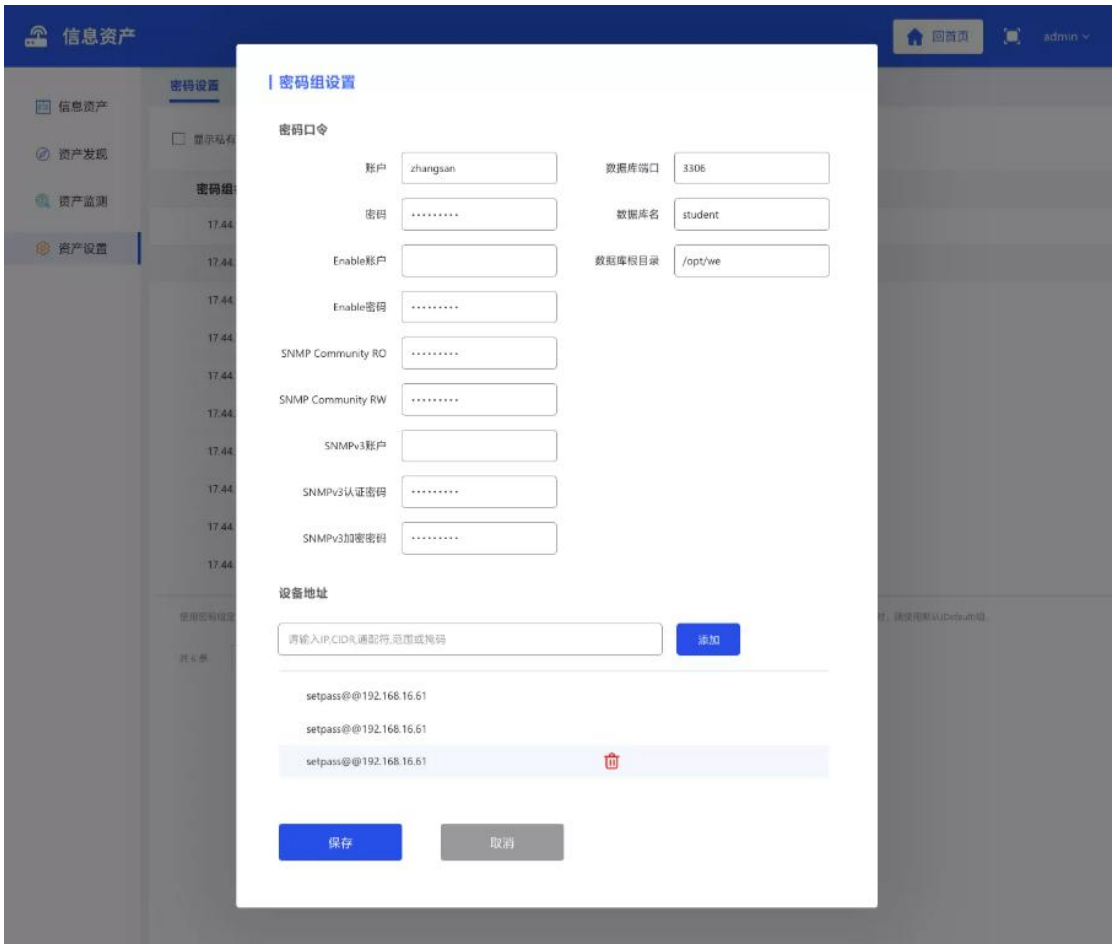


● 资产设置

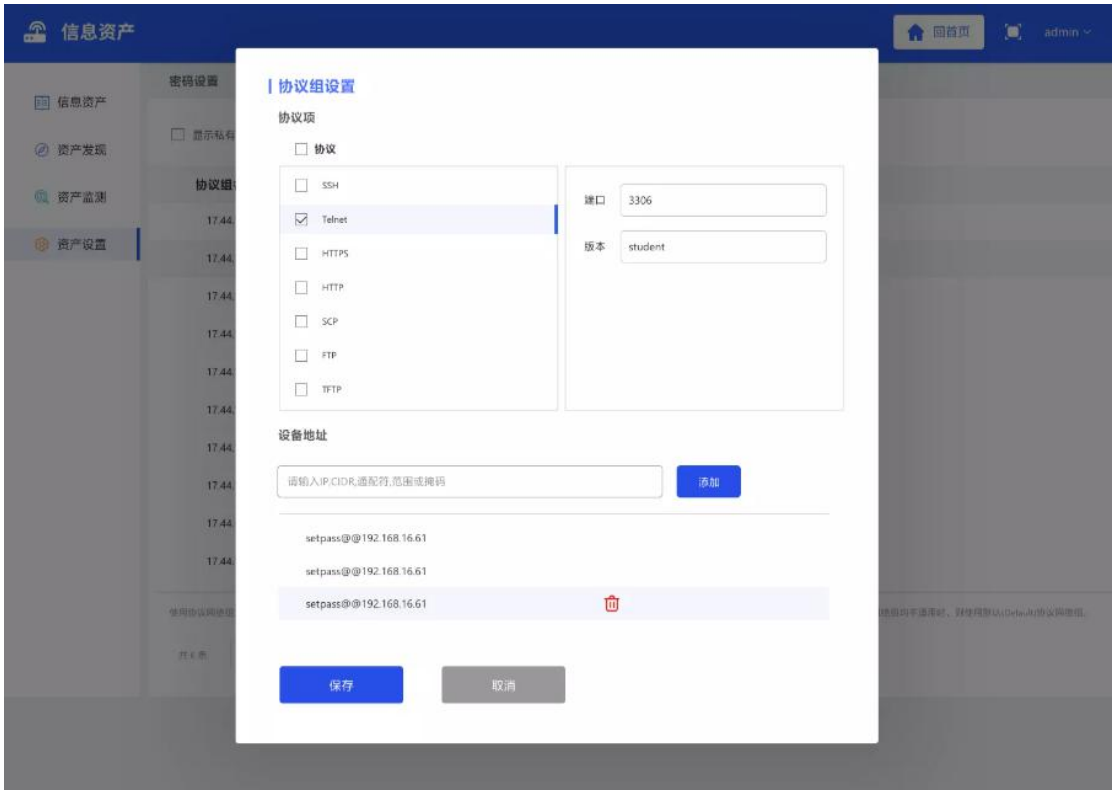
资产设置包括账户口令设置、协议设置、资产类型设置。



账户口令编辑页面：

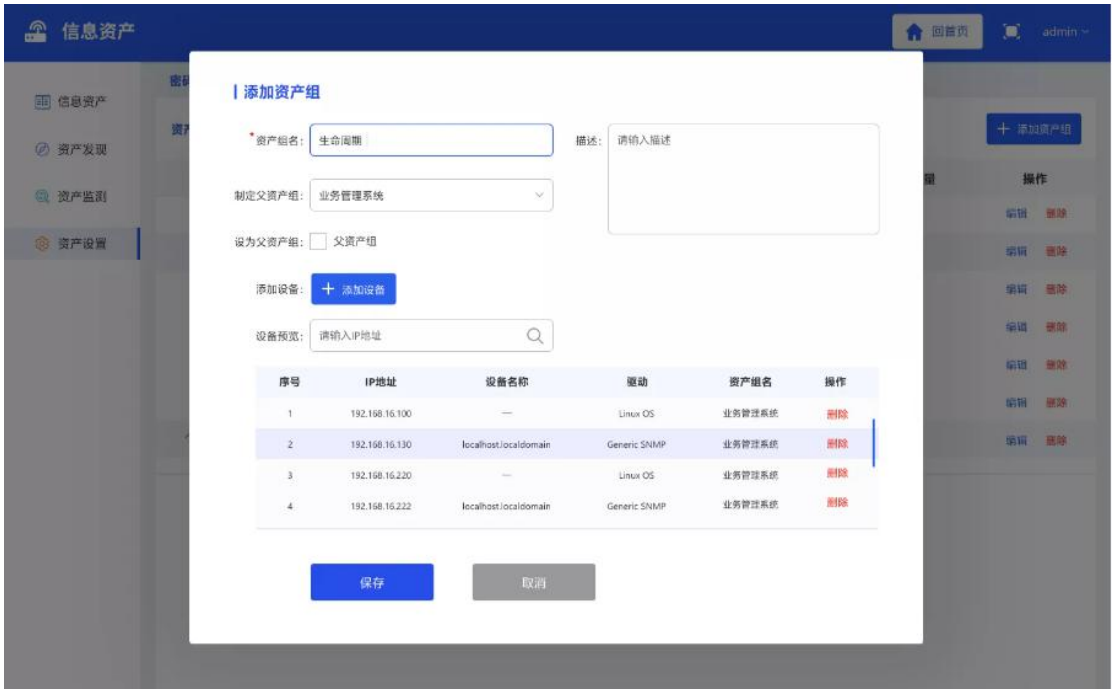


协议编辑页面：



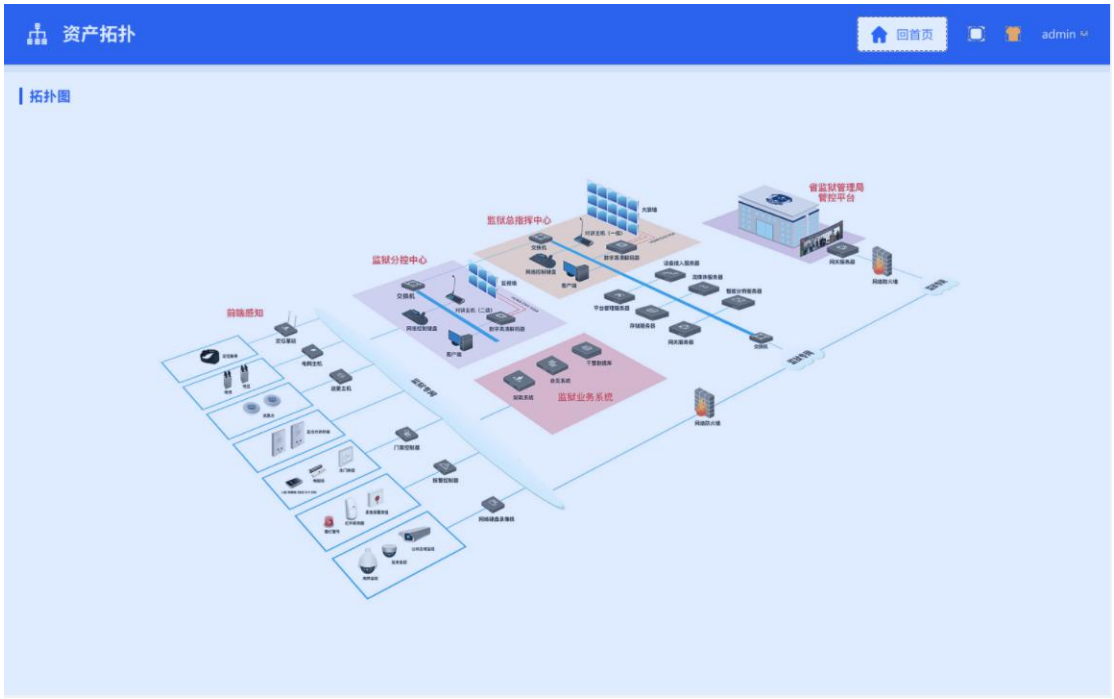
密码和协议定义页面的 IP 地址都支持单个设备、CIDR、通配符、范围等

资产组可以定义无限级数据，形成资产组管理树。



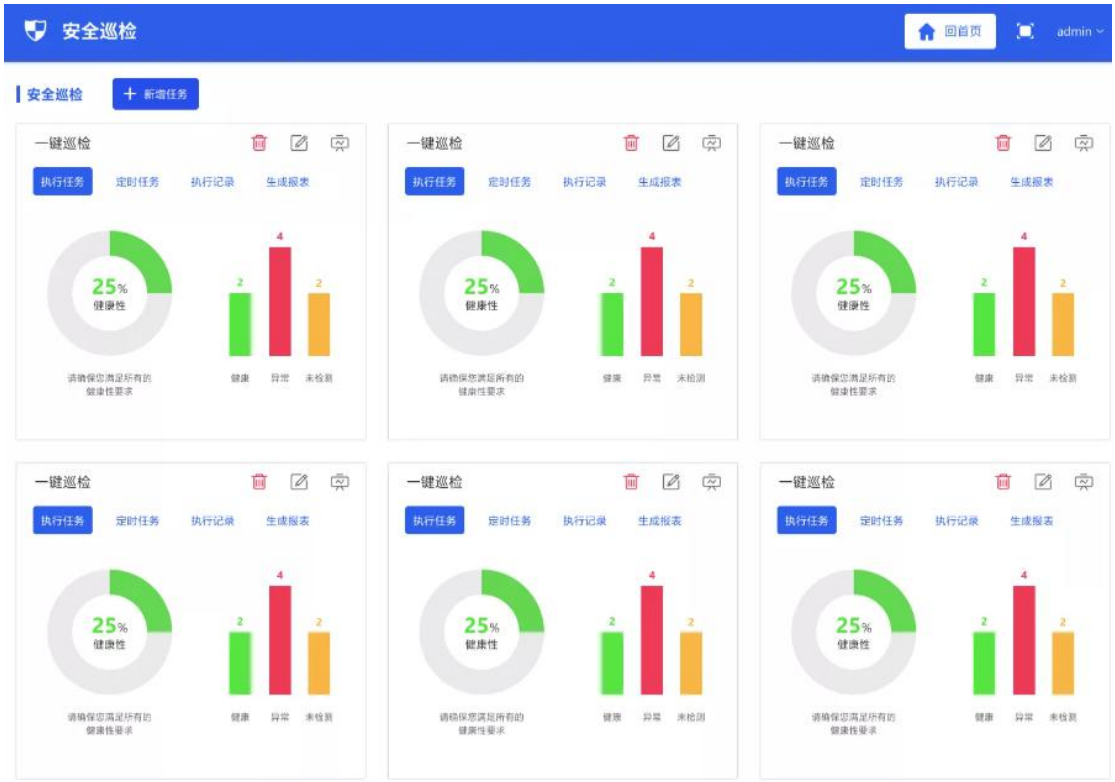
2.3.2. 资产拓扑

系统中支持用户自己绘制多个单个拓扑图，或者多层拓扑图。

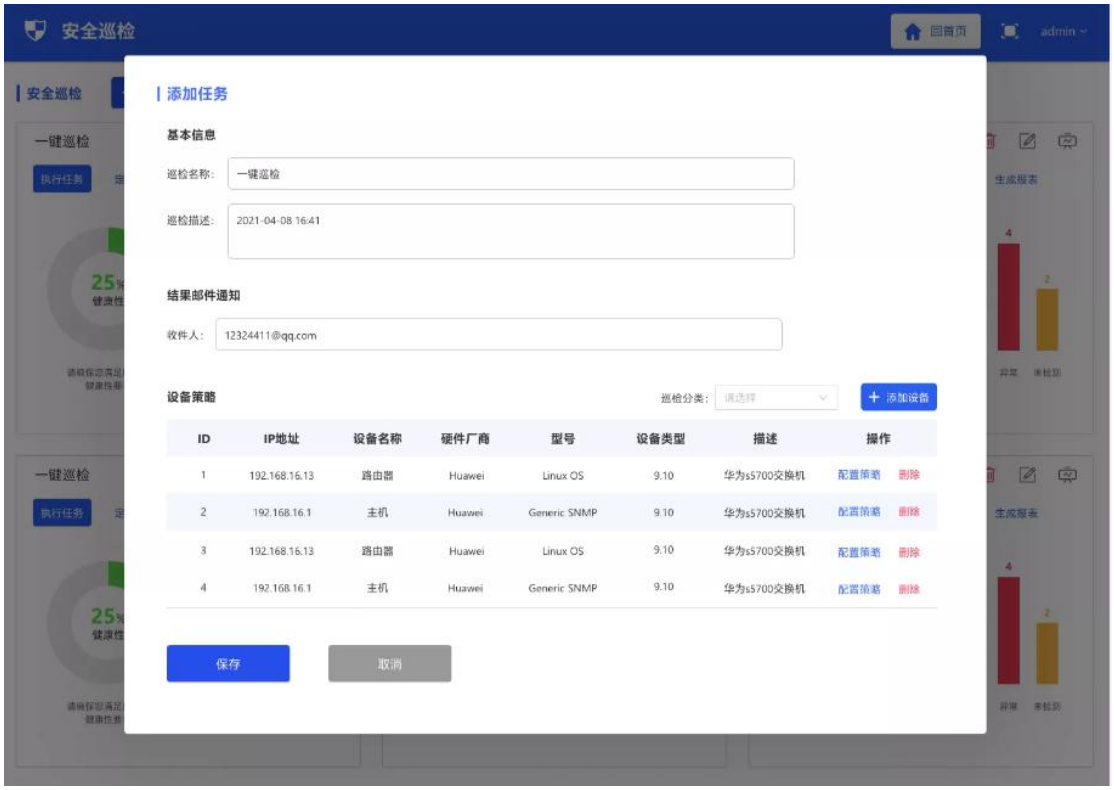


2.3.3. 安全基线

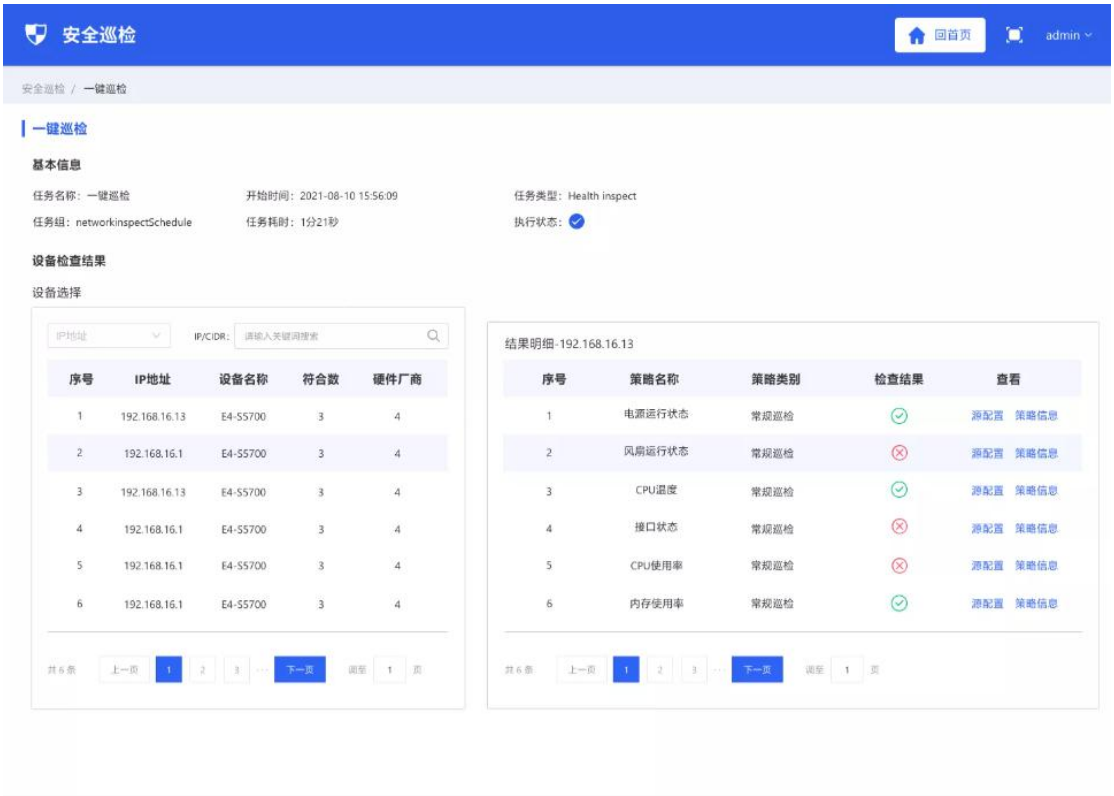
展示全部基线检查任务，并支持编辑和维护任务的信息和状态。对检查结果可以生成报告。



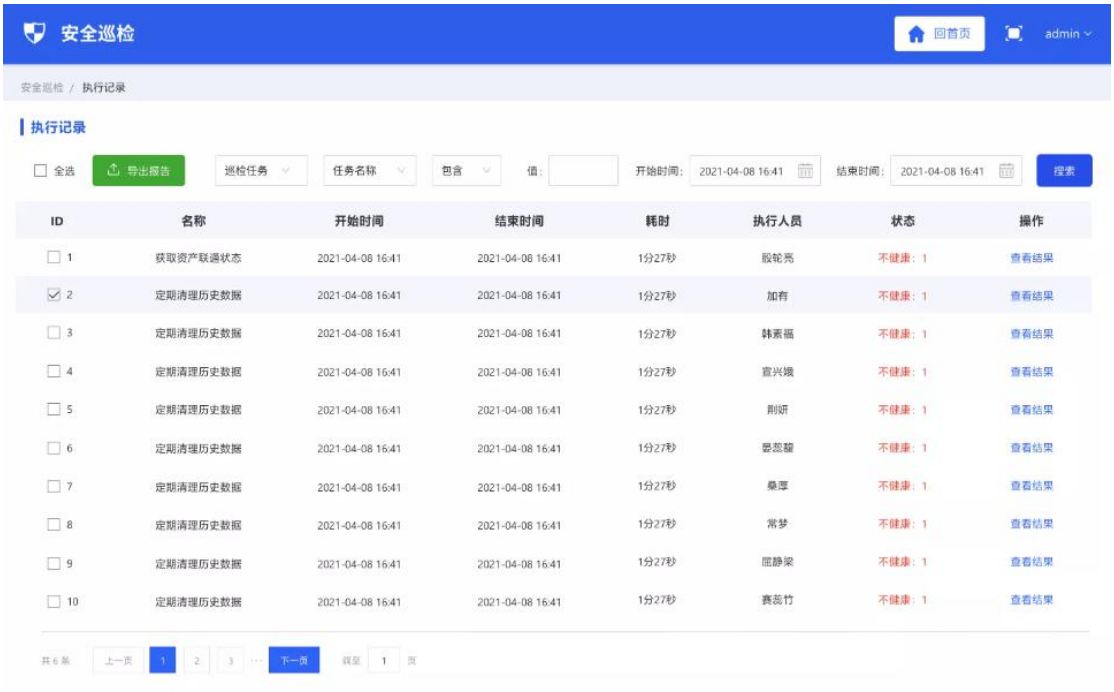
编辑任务：



查看单次任务结果：



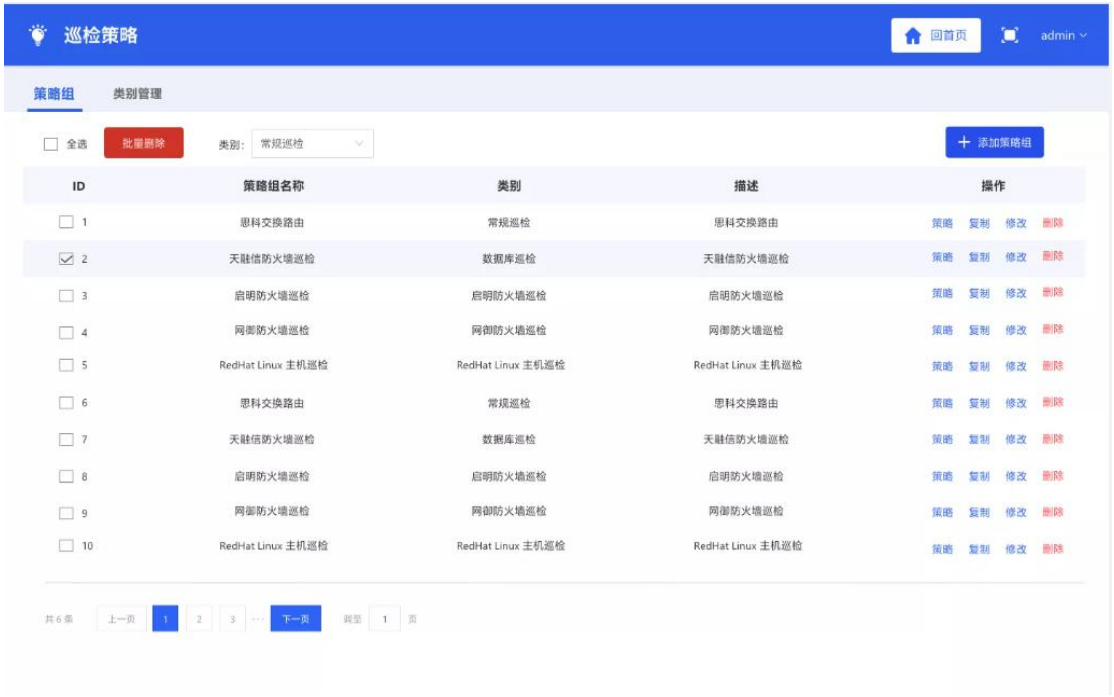
查看任务历史执行记录：



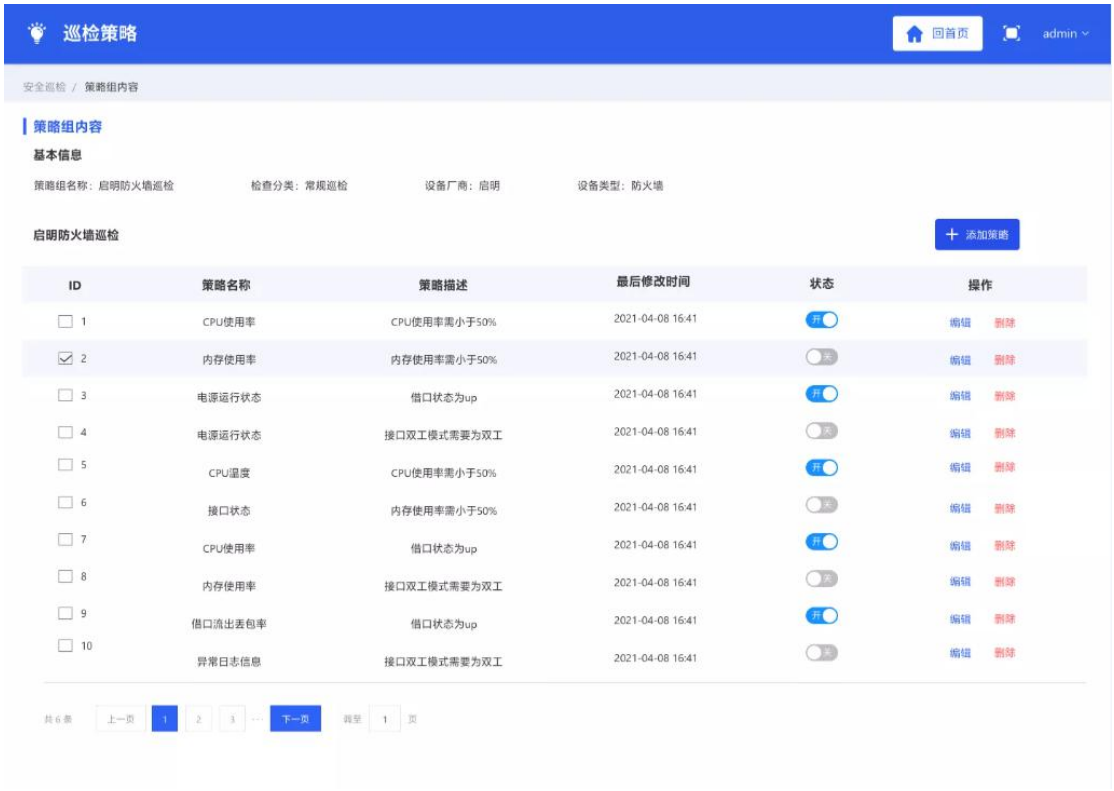
2.3.4. 基线策略

基线策略由三层结构组成：策略类型（标准）-策略组-策略。

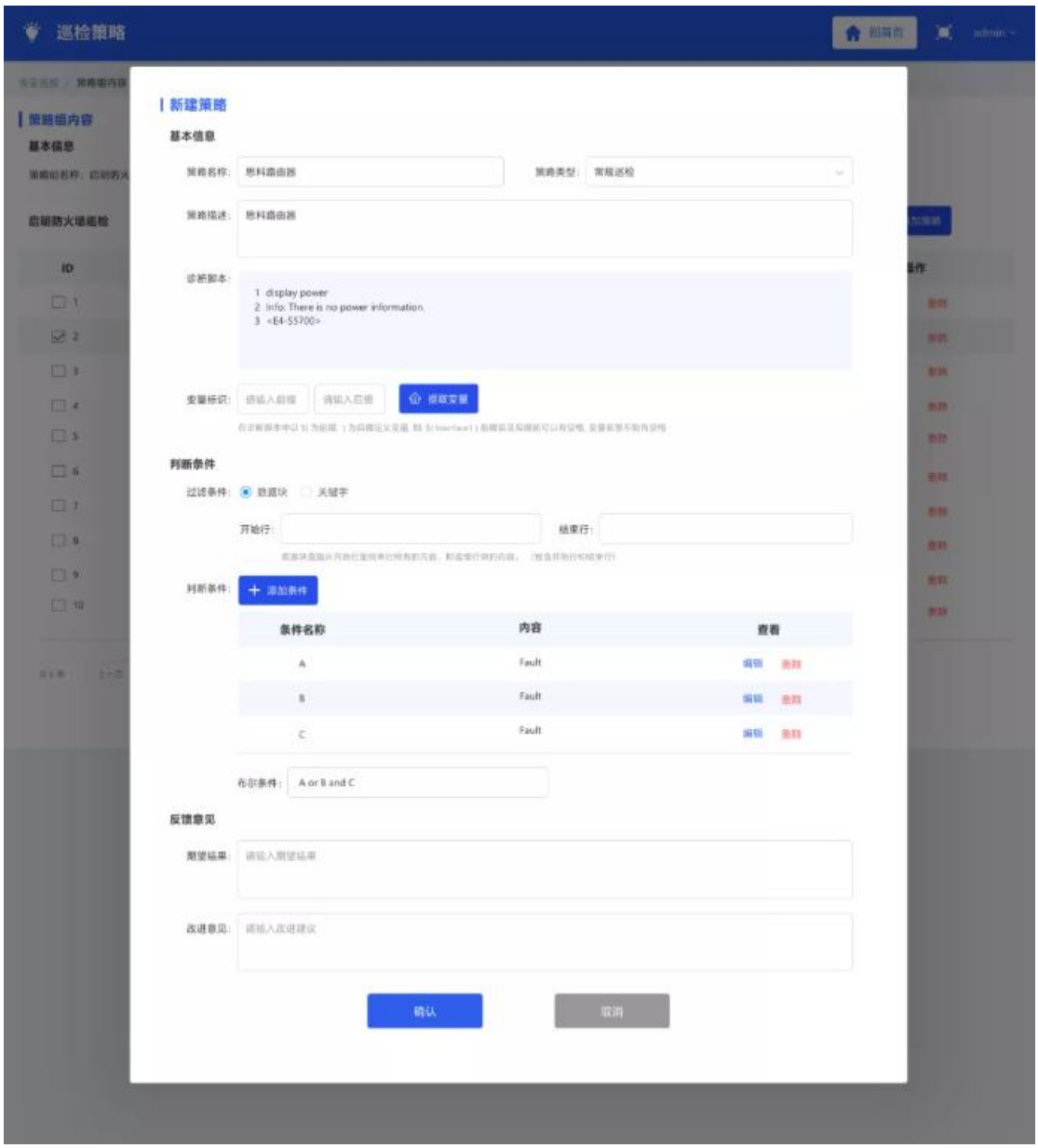
策略组列表：



策略组内的策略：



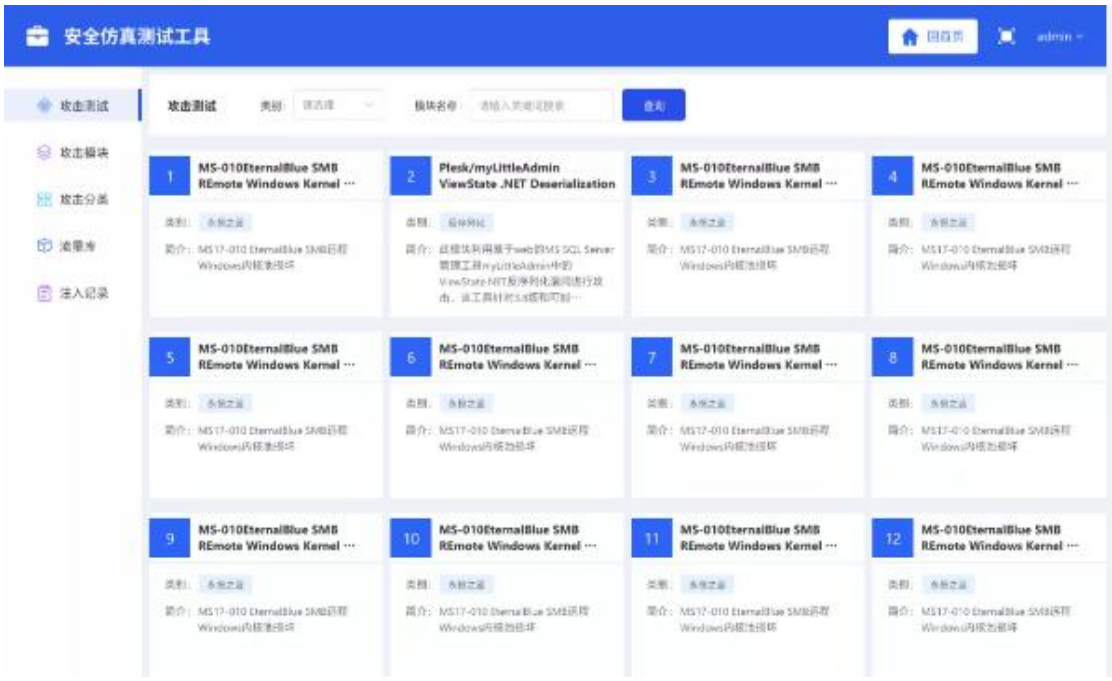
编辑某策略：



2.4. 安全仿真测试工具

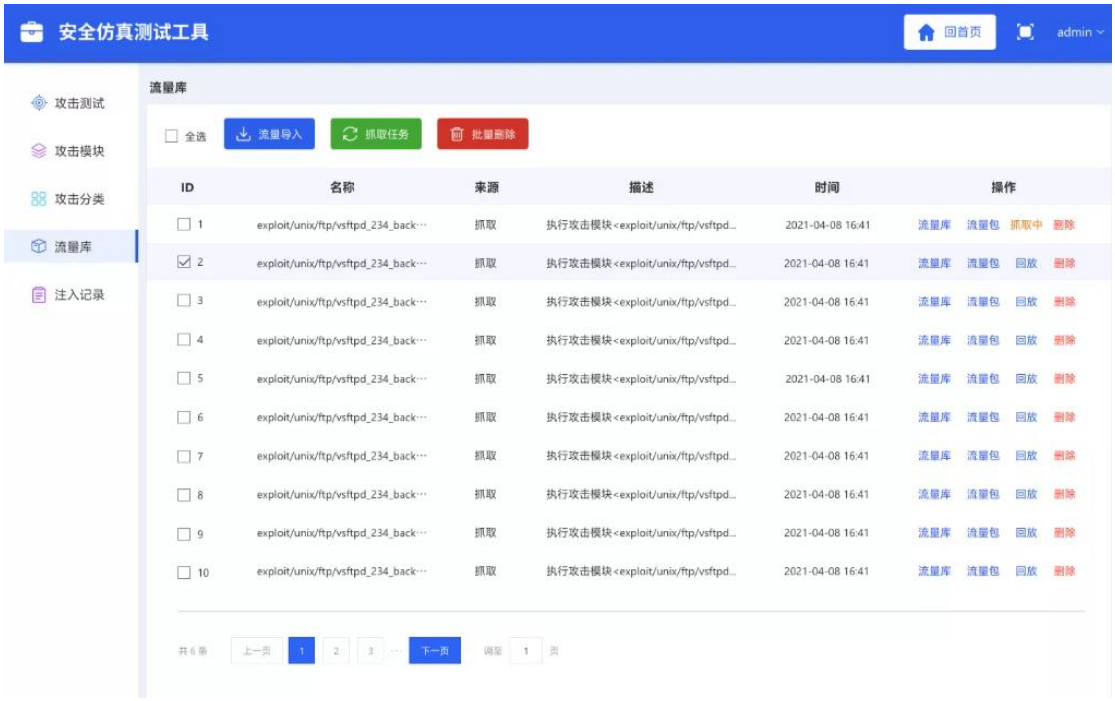
安全仿真测试工具模块是以已知的漏洞攻击脚本或者流量包（网络镜像或者自主生成），对测试网络进行模拟攻击，以便提前发现网络中存在的安全隐患。

漏洞攻击脚本库：

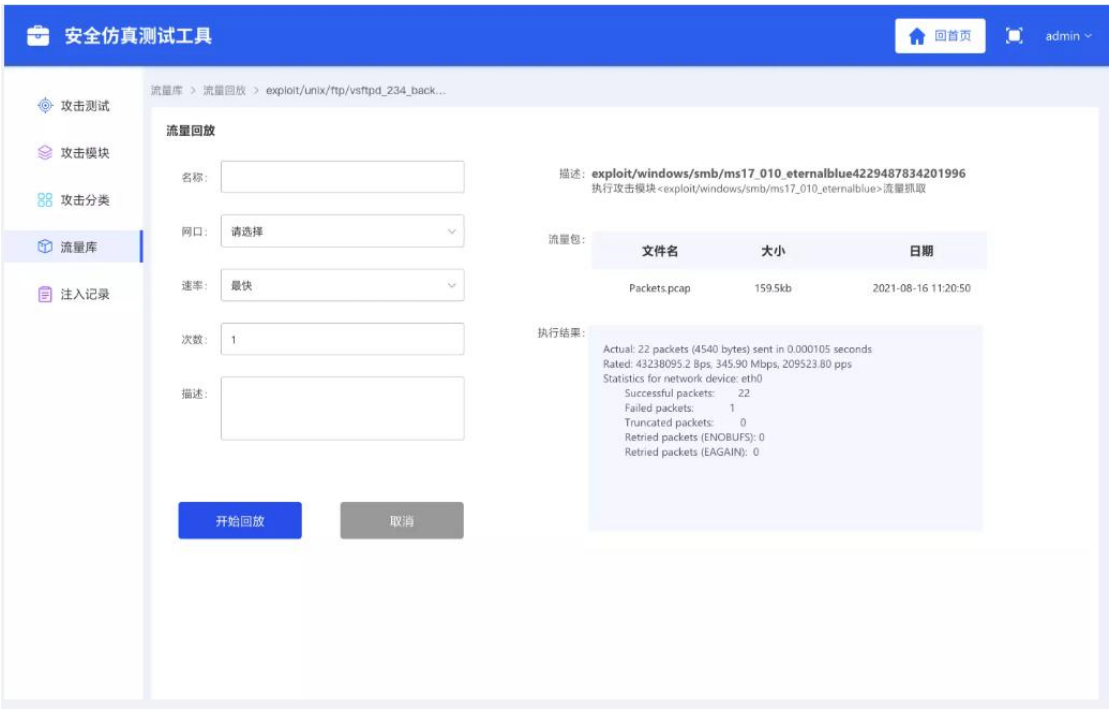


某漏洞攻击脚本执行过程：

流量库：



流量包回放规则设置：



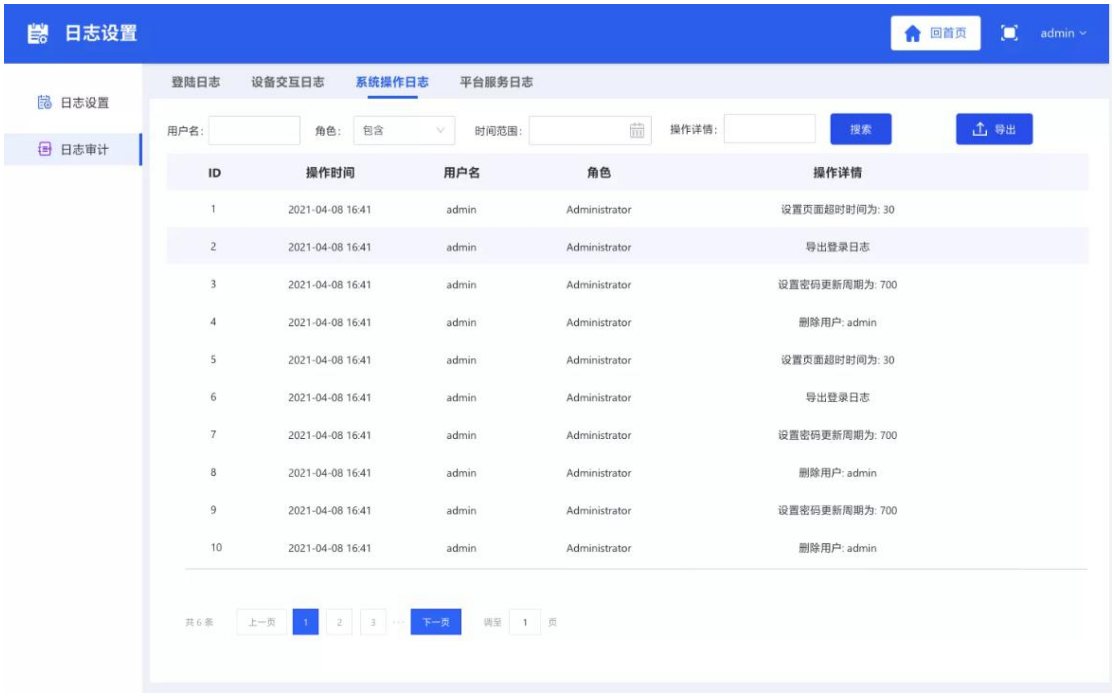
2.5. 日志管理

日志管理是平台管理人员操作以及登录日志记录。

操作日志

点击操作日志，系统跳转至操作日志界面，显示内容为运营管理人员在服务平台的操作日志。

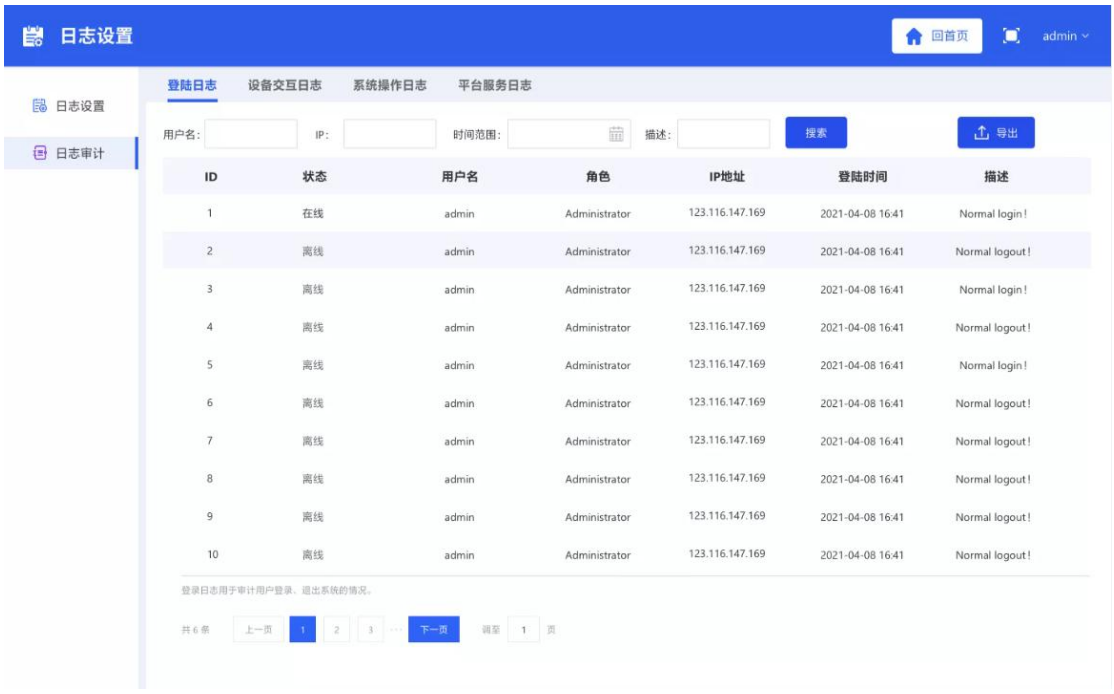
查询：输入操作人员名称点击查询按钮，页面刷新显示查询后的日志列表。



登录日志

点击登录日志，系统跳转至登录日志界面，显示内容为运营管理人员登录日志信息。

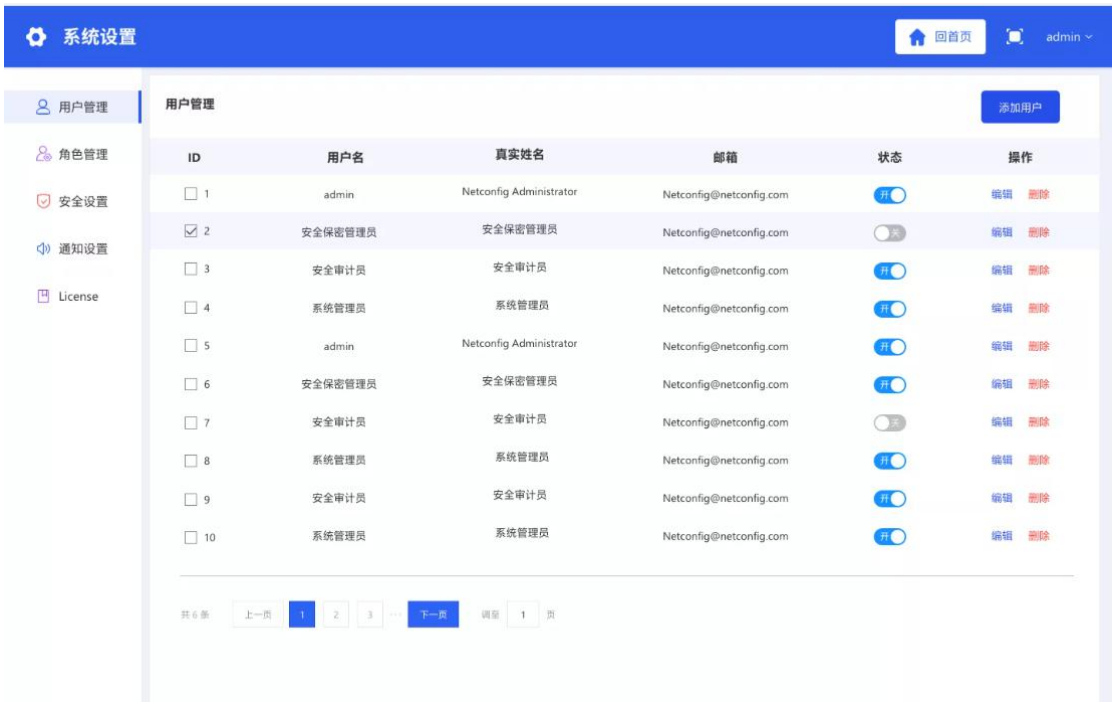
查询：输入管理人员名称，点击查询按钮，页面刷新后显示过滤后的日志信息。



2.6. 系统管理

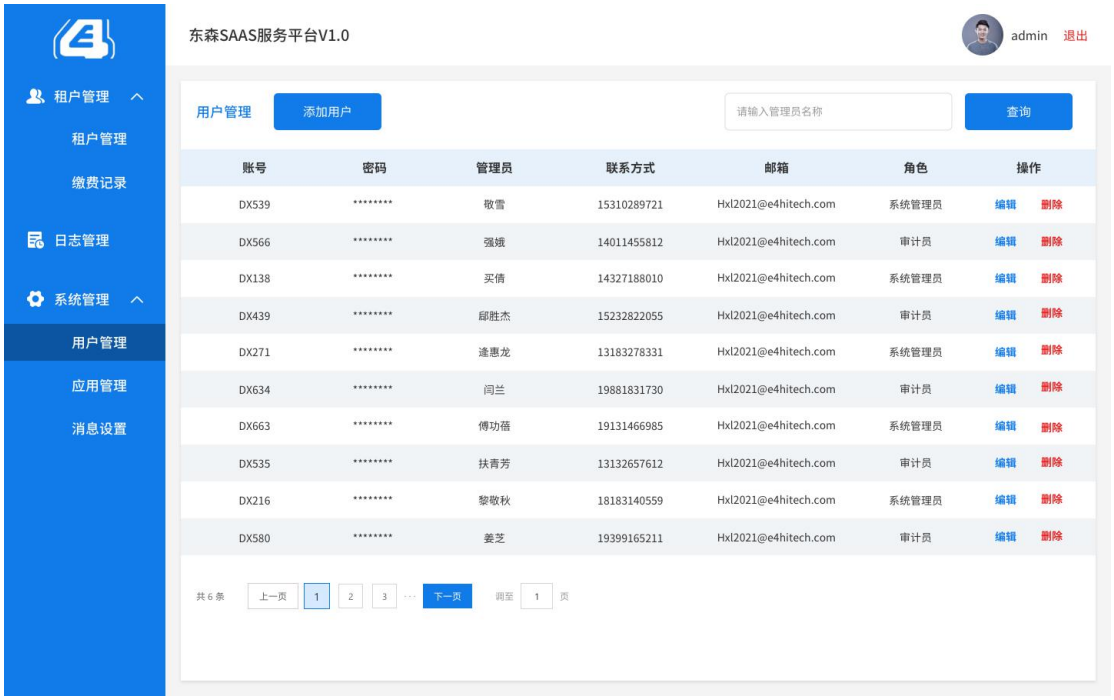
2.6.1. 用户管理

用户管理用于维护平台管理人员。可以进行用户新增、编辑、以及删除操作。系统内置了系统管理员、审计员两个角色。管理员主要负责系统的日常维护。审计员主要负责通过日志对管理员行为进行审计监督工作。



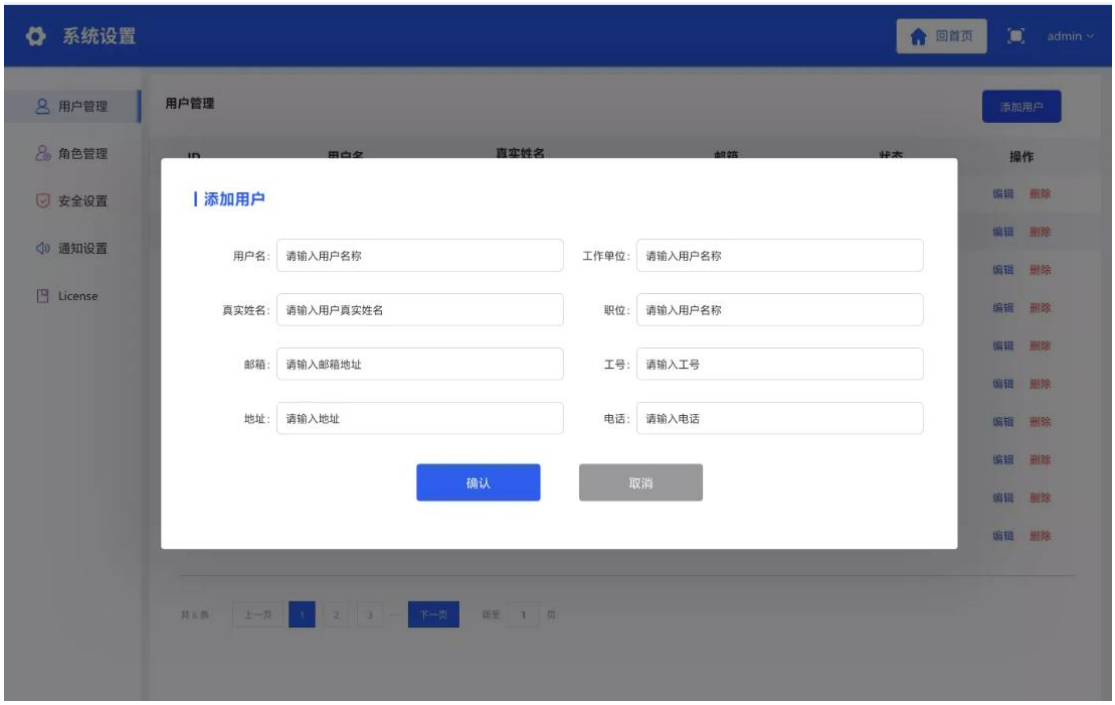
查询

输入框内填写需要查询的管理员的信息，点击查询按钮，页面刷新后显示过滤后的用户信息。



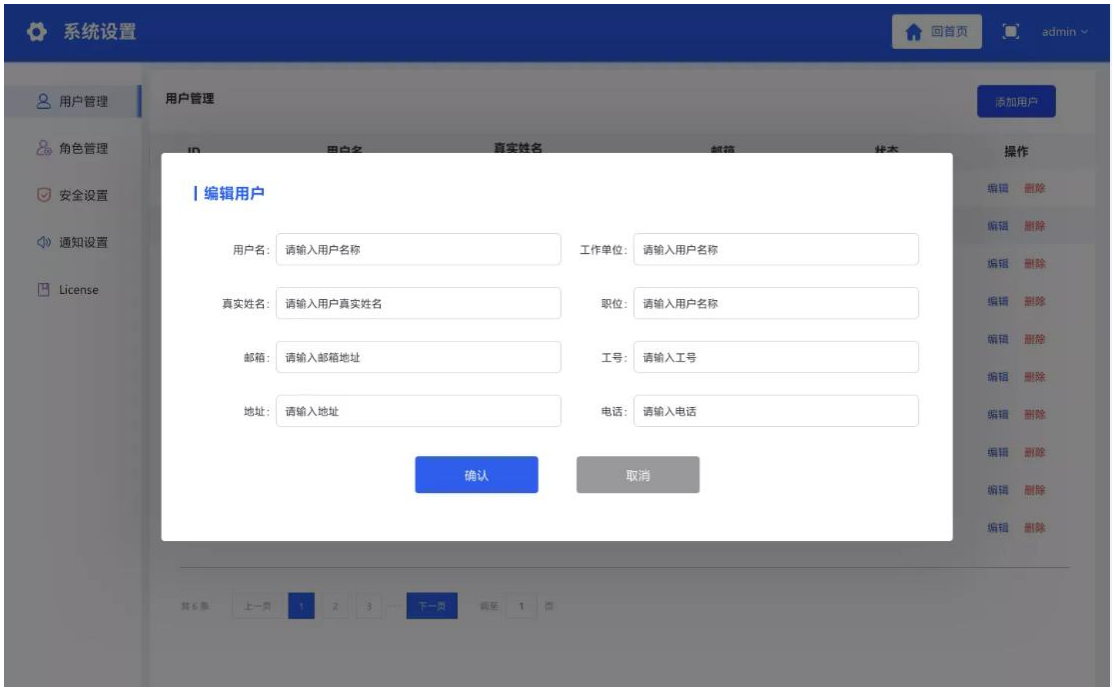
新增

点击添加用户按钮，弹出用户编辑界面、输入用户账号、用户密码、联系方式、邮箱、勾选角色，点击确认保存。



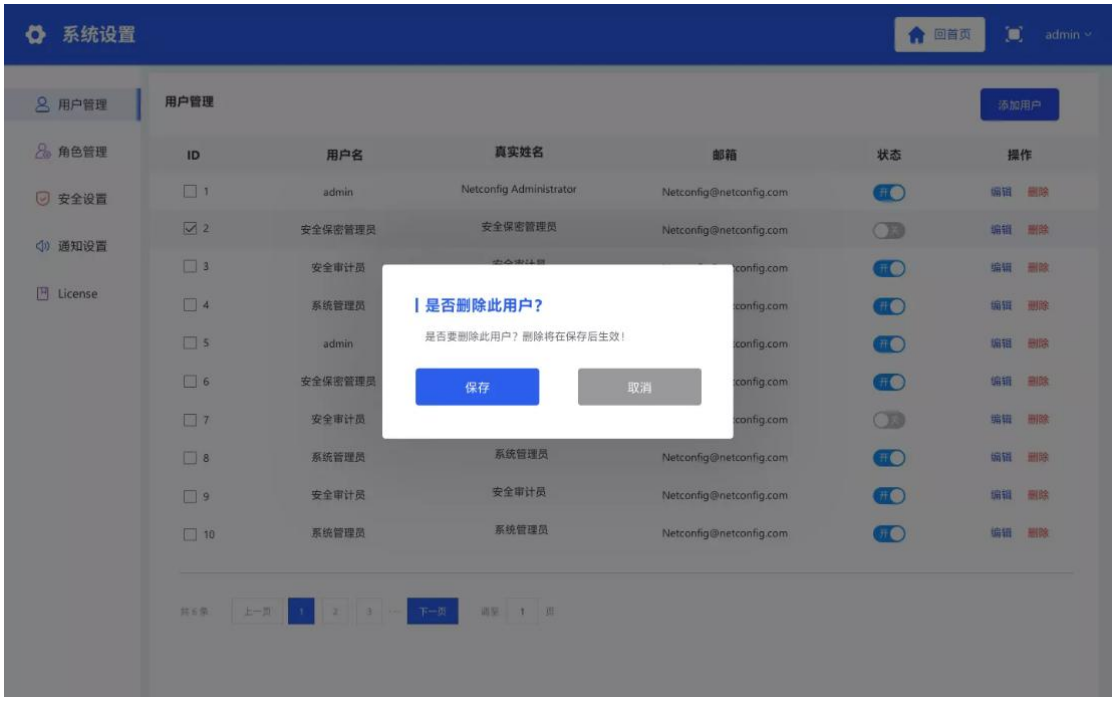
编辑

选择一条用户信息的，点击编辑按钮后弹出编辑界面，界面内自动回显用户信息，修改后点击确认，进行保存。



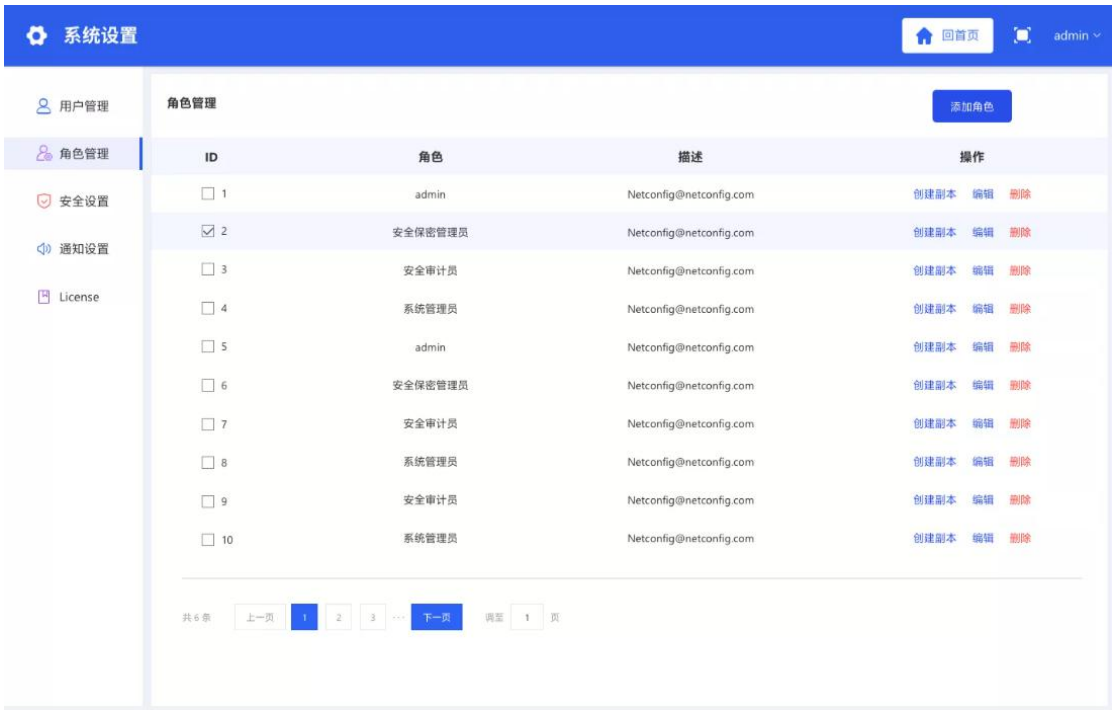
删除

选择一条用户信息，点击删除按钮，弹出是否删除确认的弹出框，点击确认系统删除用户，并且关闭弹窗，重新刷新用户列表。



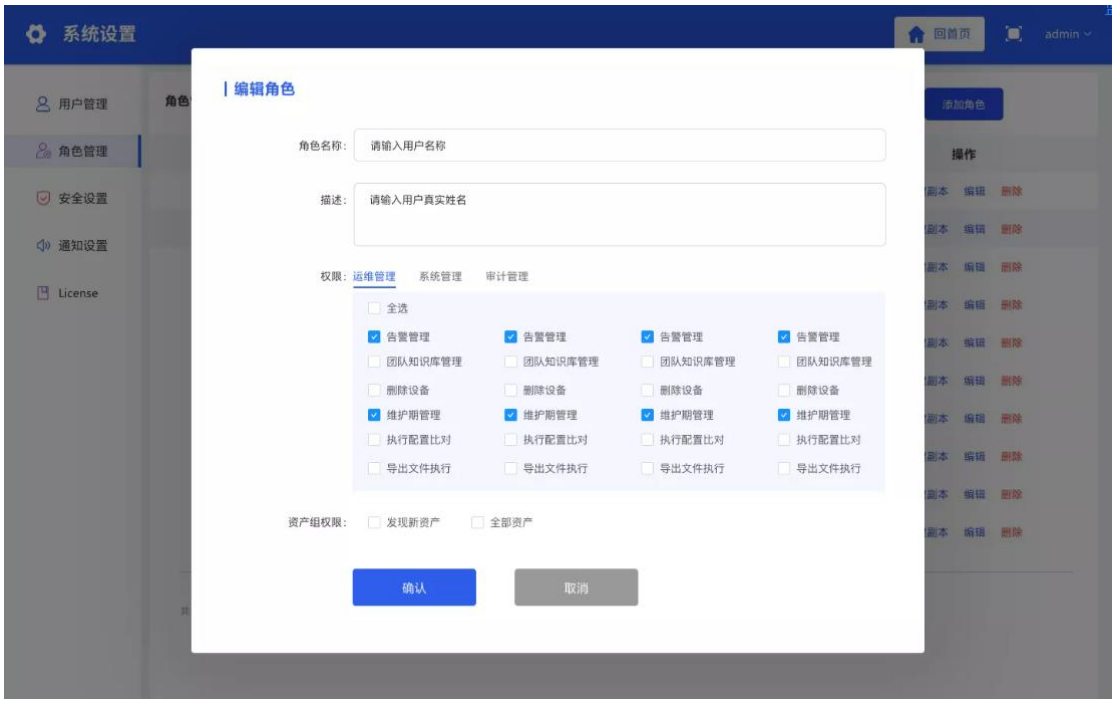
2.6.2. 角色管理

角色管理主要用于管理人员对使用平台的用户进行分组赋权。



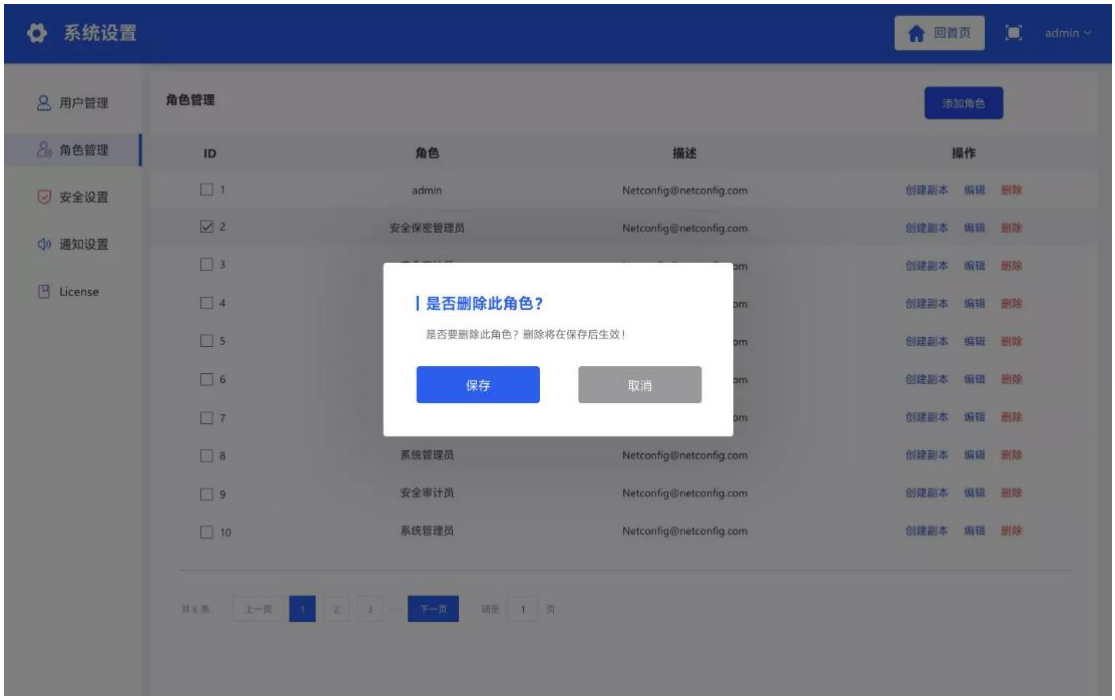
编辑

选择一条角色，点击编辑按钮，弹出此角色信息。



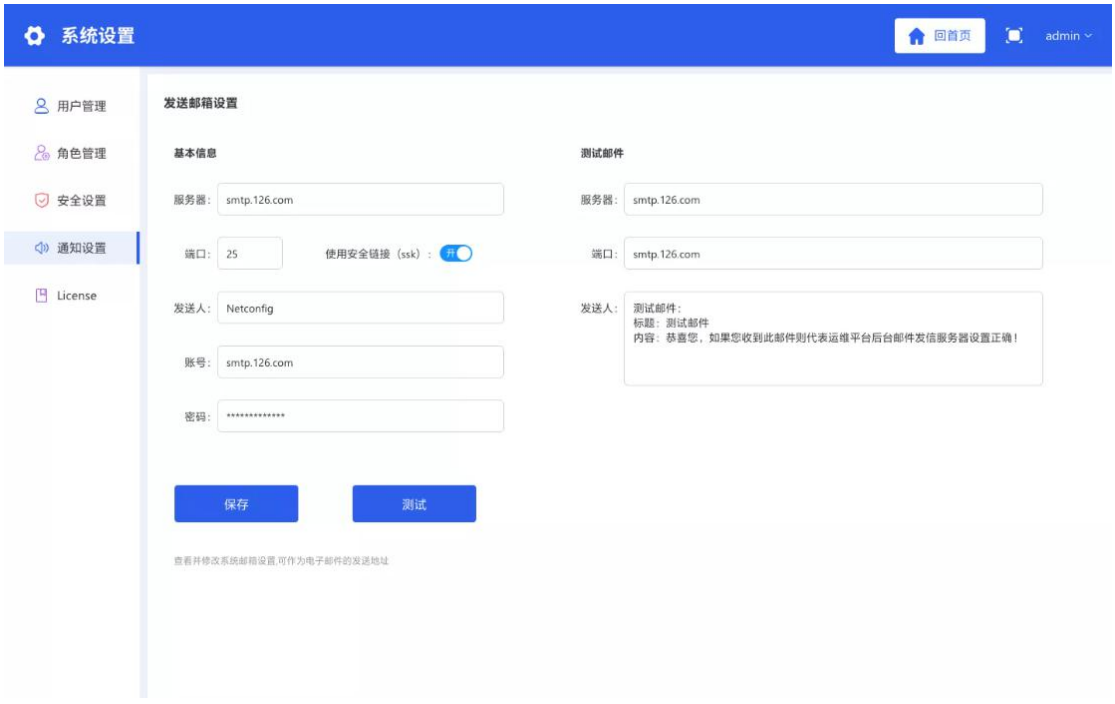
删除

选择一条角色，点击删除按钮，弹出是否删除的确认弹出框，点击确认，系统页面自动刷新，并且关闭弹出框。



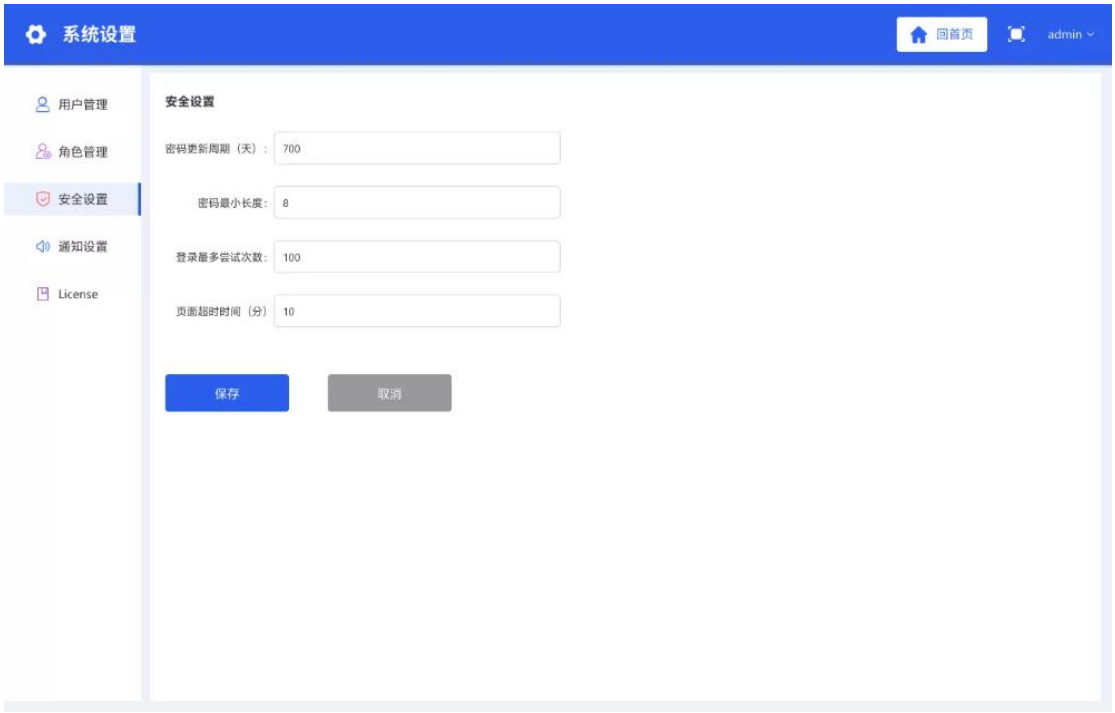
2.6.3. 通知设置

通知设置就是对系统中发件箱的设置，包括测试功能。



2.6.4. 安全设置

安全设置包括密码长度、有效期的设置，以及页面超时时间、失败重试次数的设置。



2.6.5. License 管理

平台 license 包括两部分内容的限制：信息资产数和服务有效期。