

乐为运维管理平台 V1.0

用户手册

2021 年 9 月

目录

乐为运维管理平台 V1.0.....	1
用户手册.....	1
1. 综述.....	1
1.1. 系统概述.....	1
1.2. 系统运行环境.....	1
2. 乐为运维管理平台功能.....	1
2.1. 登录.....	1
2.2. 功能列表.....	2
2.3. 信息资产.....	2
2.4. 安全仿真测试工具.....	14
2.5. 日志管理.....	16
2.6. 系统管理.....	18

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

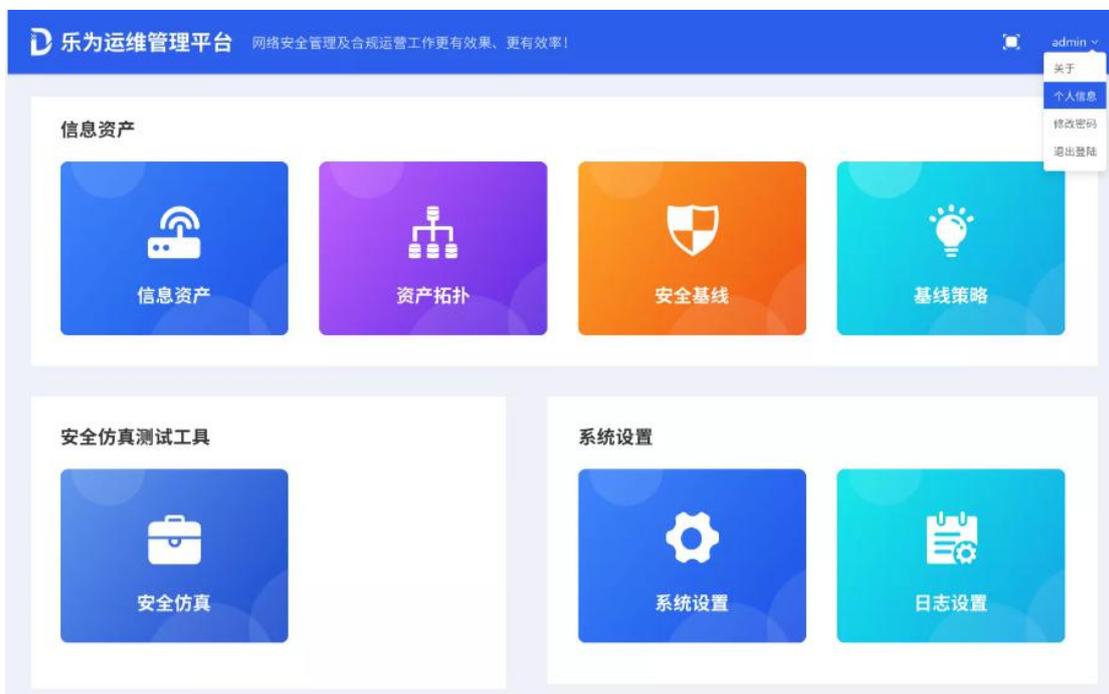
系统采用 BS 架构，在浏览器输入地址后，进入系统登录页（如下图），输入账号、密码，点击登录按钮跳转至管理界面。



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。

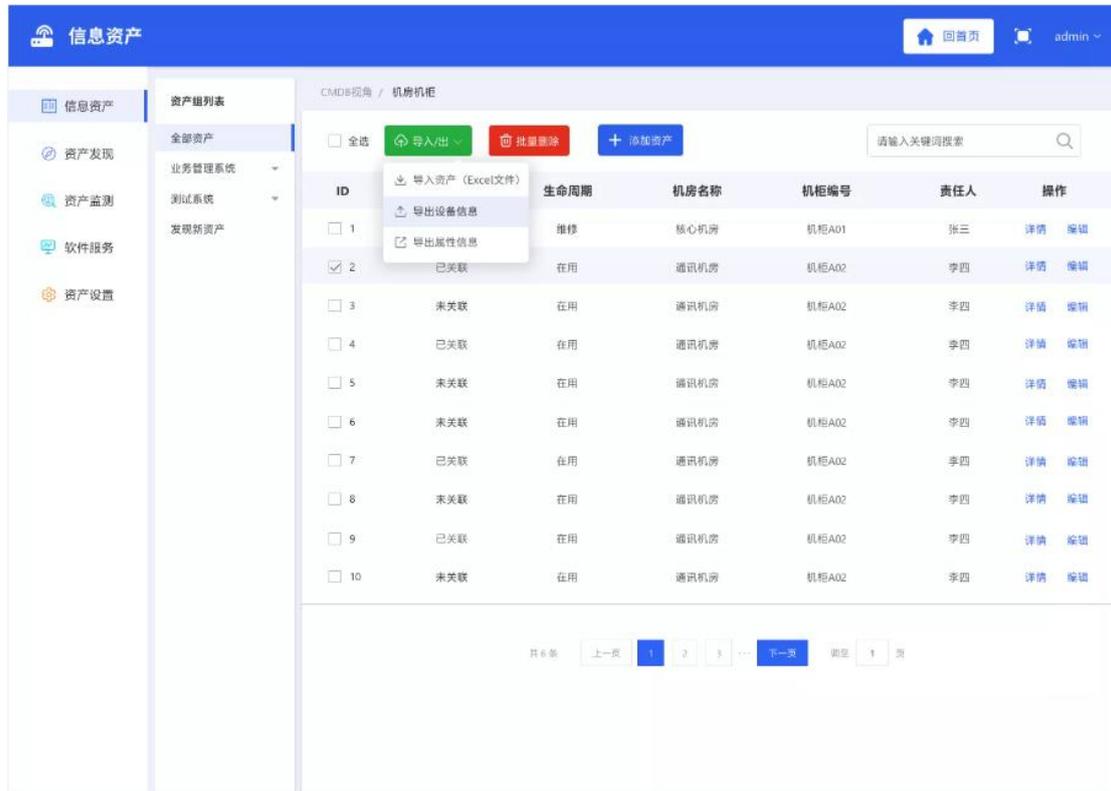


2.3. 信息资产

信息资产主要是提供资产的发现、纳管和基线检查。

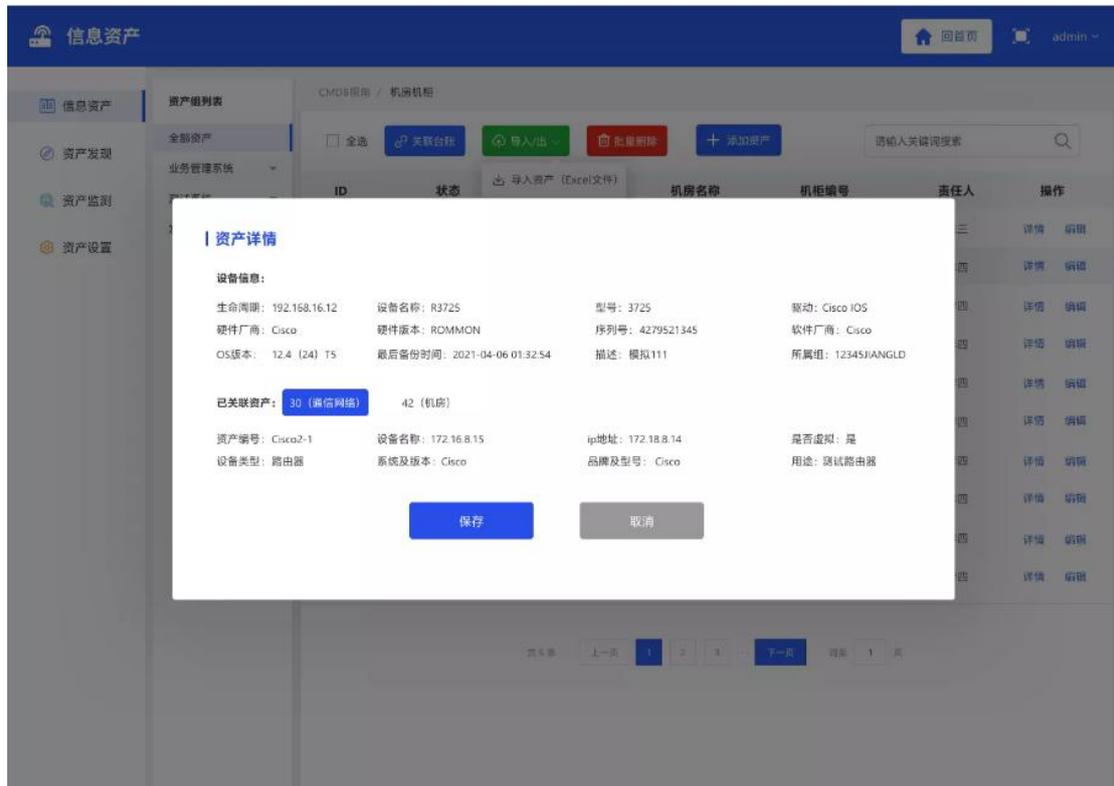
2.3.1. 信息资产

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。

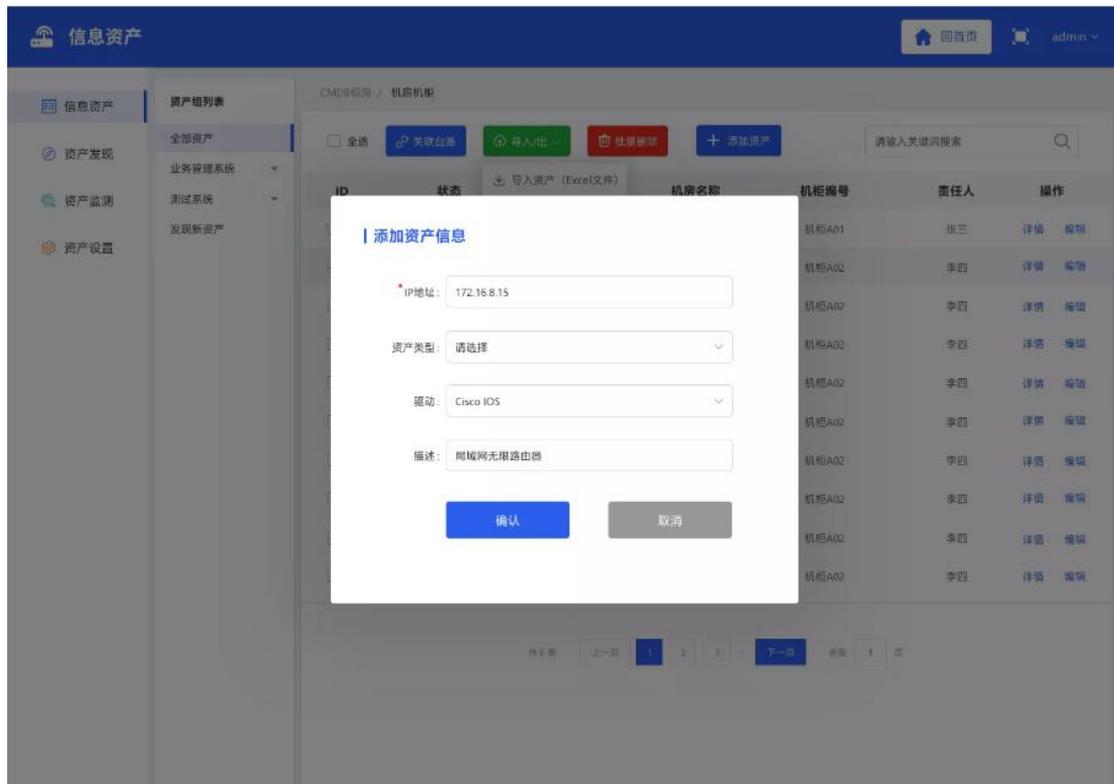


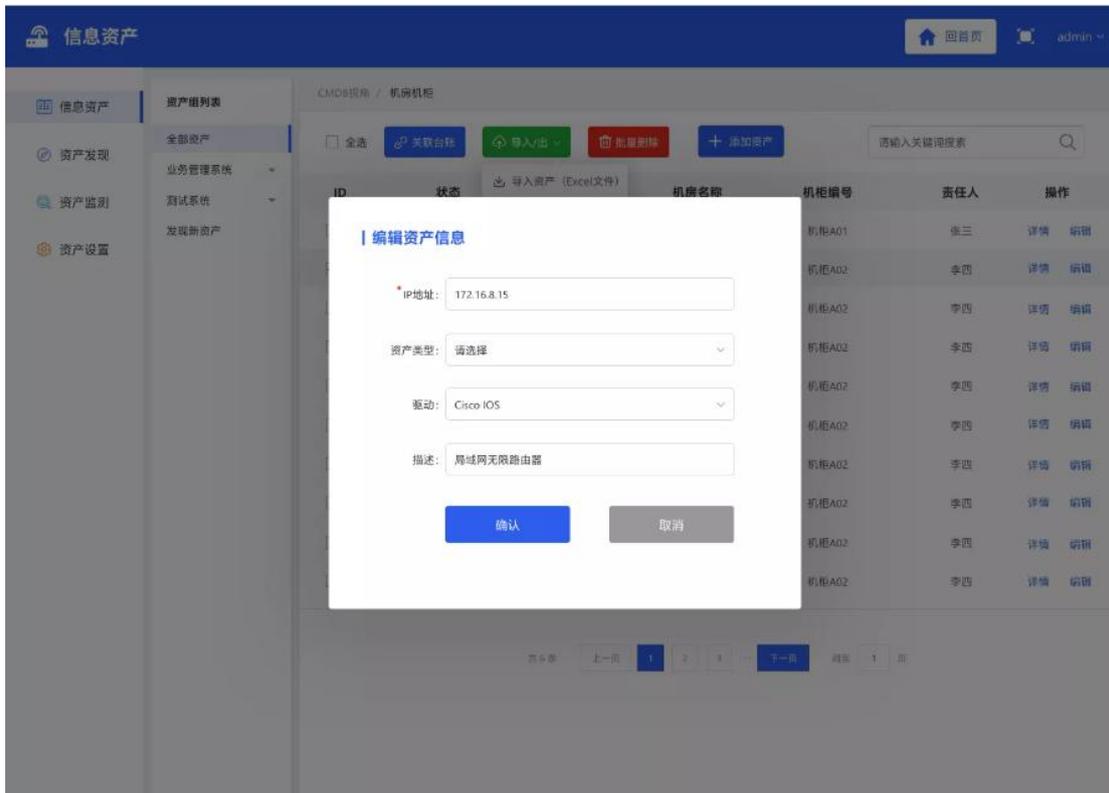
资产列表

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。



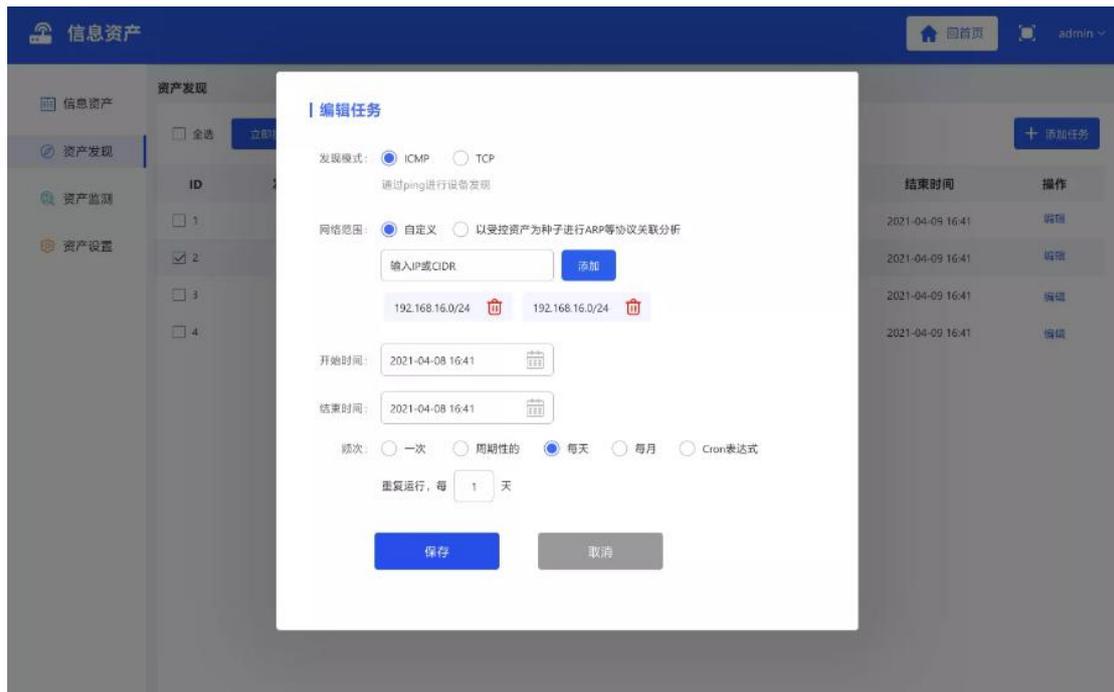


● 资产发现

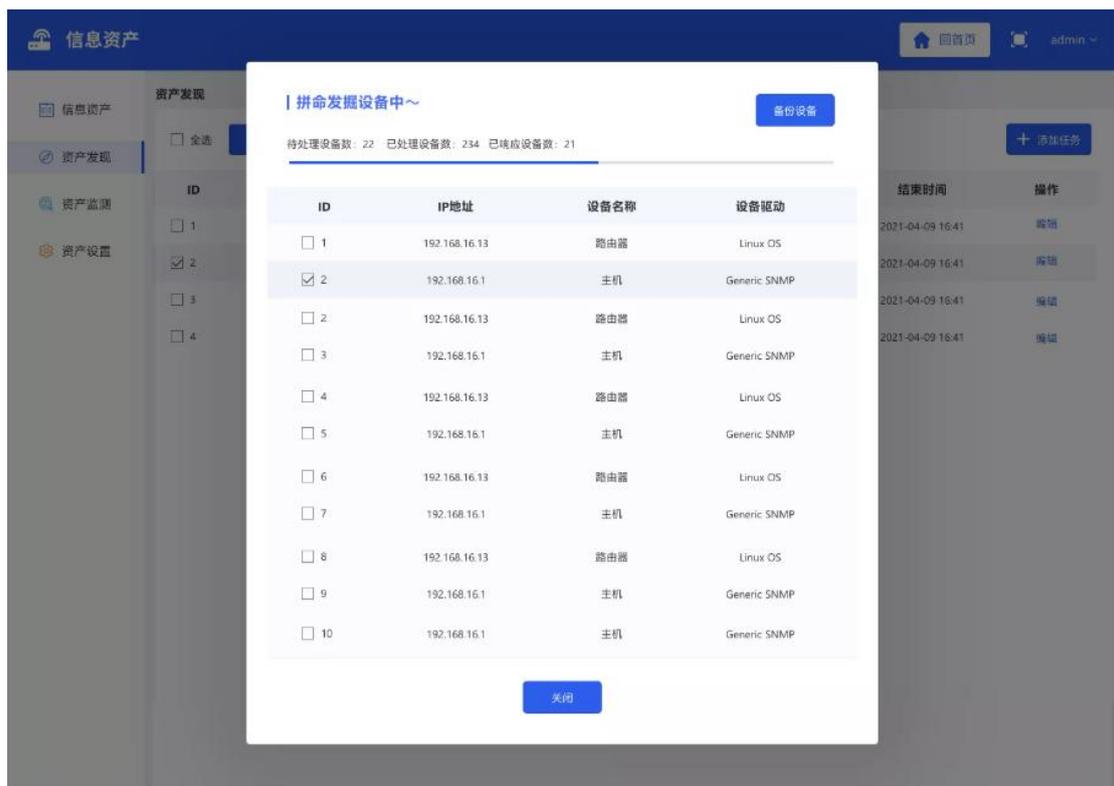
资产发现页面展示所有已经定义发现任务。



可以添加新增自定义发现任务或编辑现有发现任务。

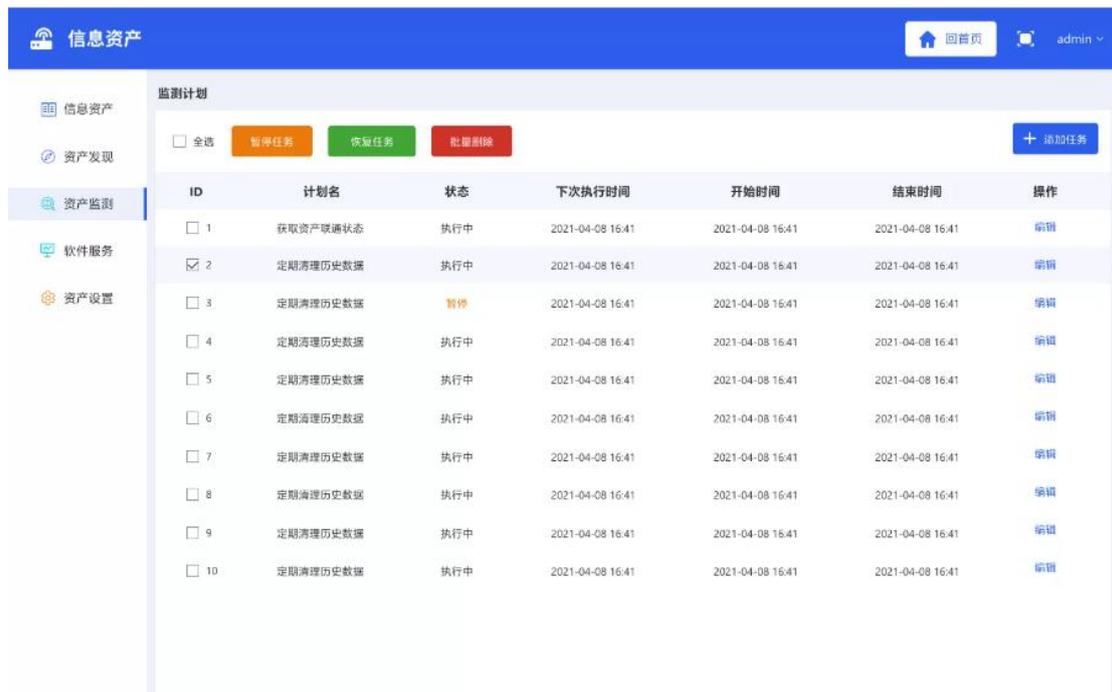


发现的结果通过 Push 方式，将发现的设备信息及时推送到客户端。

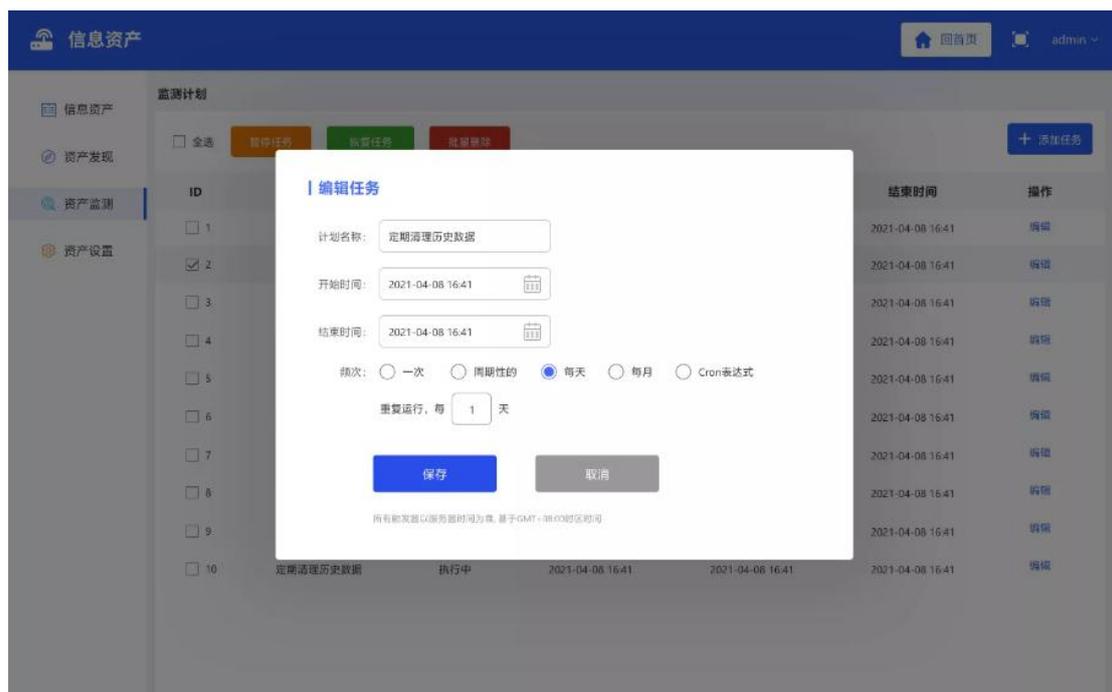


● 资产监测

资产监测主要是监测资产的在线状态。

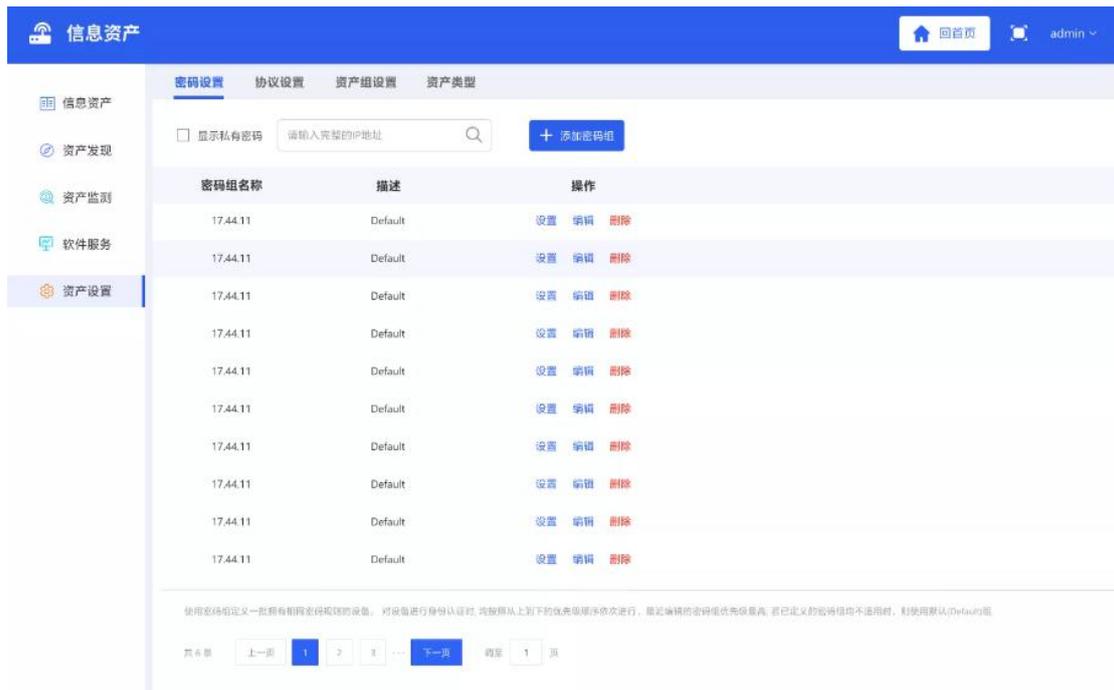


可以定义不同的监测频次任务。

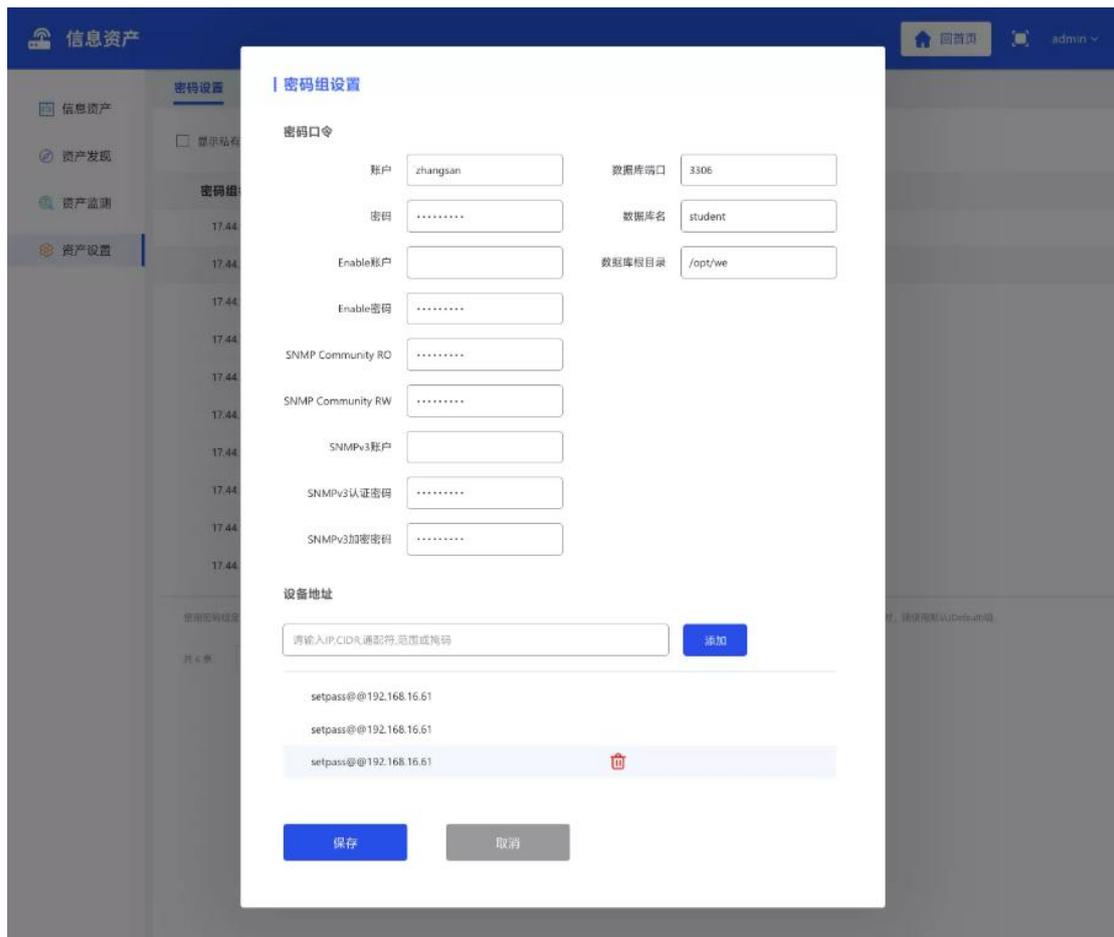


● 资产设置

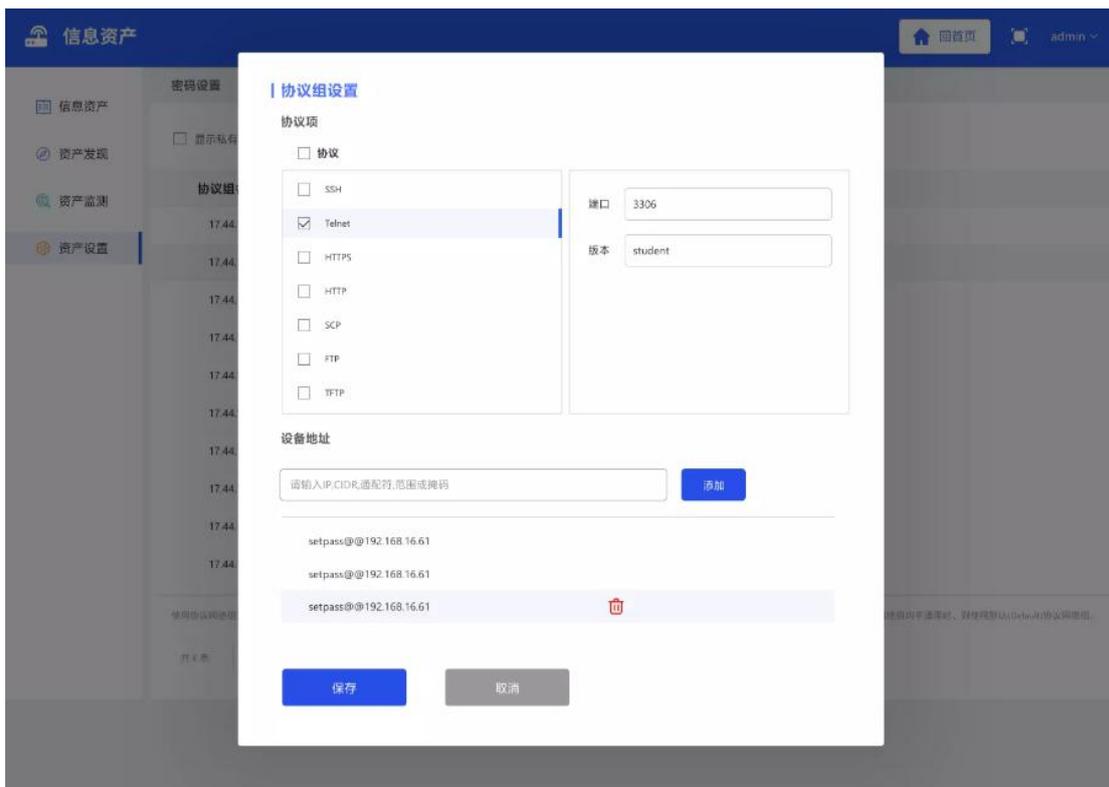
资产设置包括账户口令设置、协议设置、资产类型设置。



账户口令编辑页面：

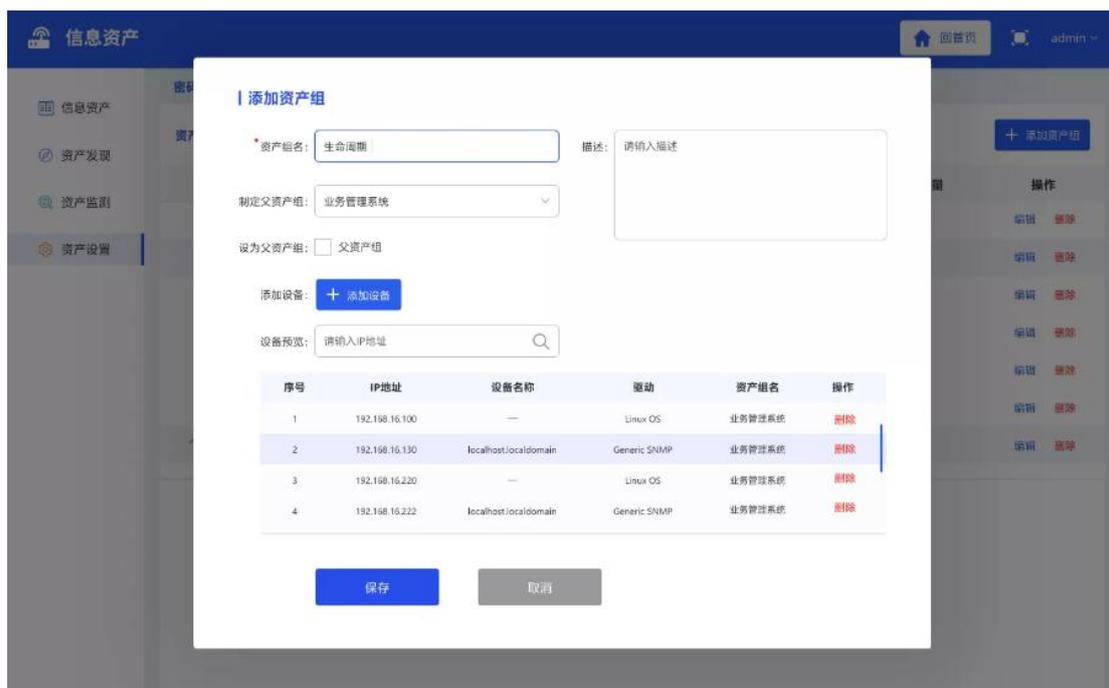


协议编辑页面：



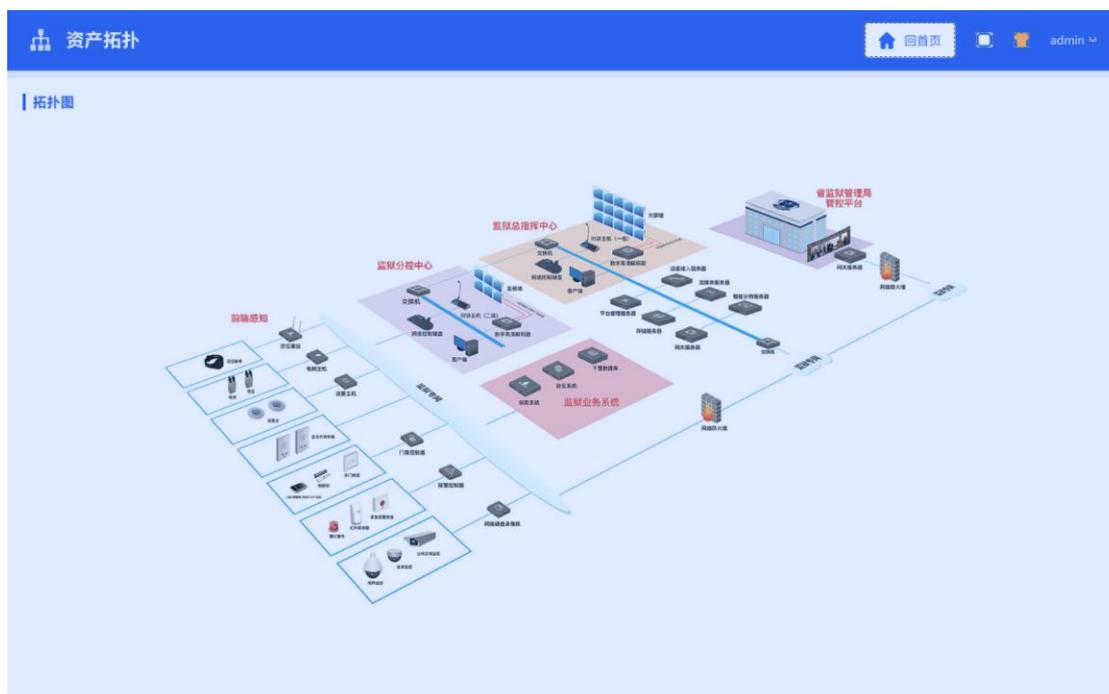
密码和协议定义页面的 IP 地址都支持单个设备、CIDR、通配符、范围等
 资产组可以定义无限级数据，形成资产组管理树。





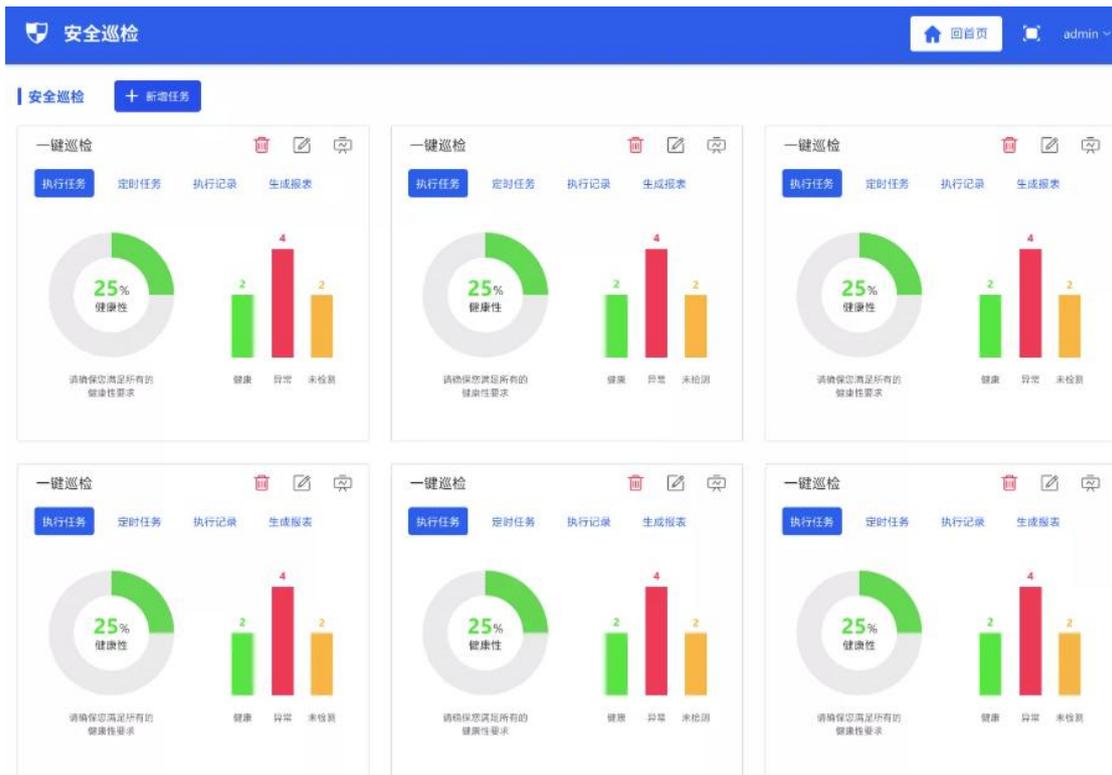
2.3.2. 资产拓扑

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：

安全巡检

添加任务

基本信息

巡检名称: 一键巡检

巡检描述: 2021-04-08 16:41

结果邮件通知

收件人: 12324411@qq.com

设备策略

巡检分类: 请选择

+ 添加设备

ID	IP地址	设备名称	硬件厂商	型号	设备类型	描述	操作
1	192.168.16.13	路由器	Huawei	Linux OS	9.10	华为s5700交换机	配置策略 删除
2	192.168.16.1	主机	Huawei	Generic SNMP	9.10	华为s5700交换机	配置策略 删除
3	192.168.16.13	路由器	Huawei	Linux OS	9.10	华为s5700交换机	配置策略 删除
4	192.168.16.1	主机	Huawei	Generic SNMP	9.10	华为s5700交换机	配置策略 删除

保存 取消

查看单次任务结果：

安全巡检

[返回首页](#)
admin

安全巡检 / 一键巡检

一键巡检

基本信息

任务名称: 一键巡检	开始时间: 2021-08-10 15:56:09	任务类型: Health inspect
任务组: networkinspectSchedule	任务耗时: 1分21秒	执行状态: ✔

设备检查结果

设备选择

序号	IP地址	设备名称	符合数	硬件厂商
1	192.168.16.13	E4-S5700	3	4
2	192.168.16.1	E4-S5700	3	4
3	192.168.16.13	E4-S5700	3	4
4	192.168.16.1	E4-S5700	3	4
5	192.168.16.1	E4-S5700	3	4
6	192.168.16.1	E4-S5700	3	4

结果明细-192.168.16.13

序号	策略名称	策略类别	检查结果	查看
1	电源运行状态	常规巡检	✔	源配置 策略信息
2	风扇运行状态	常规巡检	✘	源配置 策略信息
3	CPU温度	常规巡检	✔	源配置 策略信息
4	接口状态	常规巡检	✘	源配置 策略信息
5	CPU使用率	常规巡检	✘	源配置 策略信息
6	内存使用率	常规巡检	✔	源配置 策略信息

查看任务历史执行记录:

安全巡检

[返回首页](#)
admin

安全巡检 / 执行记录

执行记录

全选
导出报告
巡检任务: 任务名称
包含: 值
开始时间: 2021-04-08 16:41
结束时间: 2021-04-08 16:41
搜索

ID	名称	开始时间	结束时间	耗时	执行人员	状态	操作
<input type="checkbox"/> 1	获取资产联通状态	2021-04-08 16:41	2021-04-08 16:41	1分27秒	殷轮亮	不健康: 1	查看结果
<input checked="" type="checkbox"/> 2	定期清理历史数据	2021-04-08 16:41	2021-04-08 16:41	1分27秒	加青	不健康: 1	查看结果
<input type="checkbox"/> 3	定期清理历史数据	2021-04-08 16:41	2021-04-08 16:41	1分27秒	韩素福	不健康: 1	查看结果
<input type="checkbox"/> 4	定期清理历史数据	2021-04-08 16:41	2021-04-08 16:41	1分27秒	宣兴娥	不健康: 1	查看结果
<input type="checkbox"/> 5	定期清理历史数据	2021-04-08 16:41	2021-04-08 16:41	1分27秒	荆研	不健康: 1	查看结果
<input type="checkbox"/> 6	定期清理历史数据	2021-04-08 16:41	2021-04-08 16:41	1分27秒	廖蕊蕊	不健康: 1	查看结果
<input type="checkbox"/> 7	定期清理历史数据	2021-04-08 16:41	2021-04-08 16:41	1分27秒	桑厚	不健康: 1	查看结果
<input type="checkbox"/> 8	定期清理历史数据	2021-04-08 16:41	2021-04-08 16:41	1分27秒	常梦	不健康: 1	查看结果
<input type="checkbox"/> 9	定期清理历史数据	2021-04-08 16:41	2021-04-08 16:41	1分27秒	应静梁	不健康: 1	查看结果
<input type="checkbox"/> 10	定期清理历史数据	2021-04-08 16:41	2021-04-08 16:41	1分27秒	袁蕊竹	不健康: 1	查看结果

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 类别管理

策略组: 常规巡检

ID	策略组名称	类别	描述	操作
<input type="checkbox"/> 1	思科交换路由	常规巡检	思科交换路由	策略 复制 修改 删除
<input checked="" type="checkbox"/> 2	天融信防火墙巡检	数据库巡检	天融信防火墙巡检	策略 复制 修改 删除
<input type="checkbox"/> 3	启明防火墙巡检	启明防火墙巡检	启明防火墙巡检	策略 复制 修改 删除
<input type="checkbox"/> 4	网御防火墙巡检	网御防火墙巡检	网御防火墙巡检	策略 复制 修改 删除
<input type="checkbox"/> 5	RedHat Linux 主机巡检	RedHat Linux 主机巡检	RedHat Linux 主机巡检	策略 复制 修改 删除
<input type="checkbox"/> 6	思科交换路由	常规巡检	思科交换路由	策略 复制 修改 删除
<input type="checkbox"/> 7	天融信防火墙巡检	数据库巡检	天融信防火墙巡检	策略 复制 修改 删除
<input type="checkbox"/> 8	启明防火墙巡检	启明防火墙巡检	启明防火墙巡检	策略 复制 修改 删除
<input type="checkbox"/> 9	网御防火墙巡检	网御防火墙巡检	网御防火墙巡检	策略 复制 修改 删除
<input type="checkbox"/> 10	RedHat Linux 主机巡检	RedHat Linux 主机巡检	RedHat Linux 主机巡检	策略 复制 修改 删除

共 6 条 上一页 1 2 3 ... 下一页 每页 1 页

策略组内的策略:

安全巡检 / 策略组内容

策略组内容

基本信息

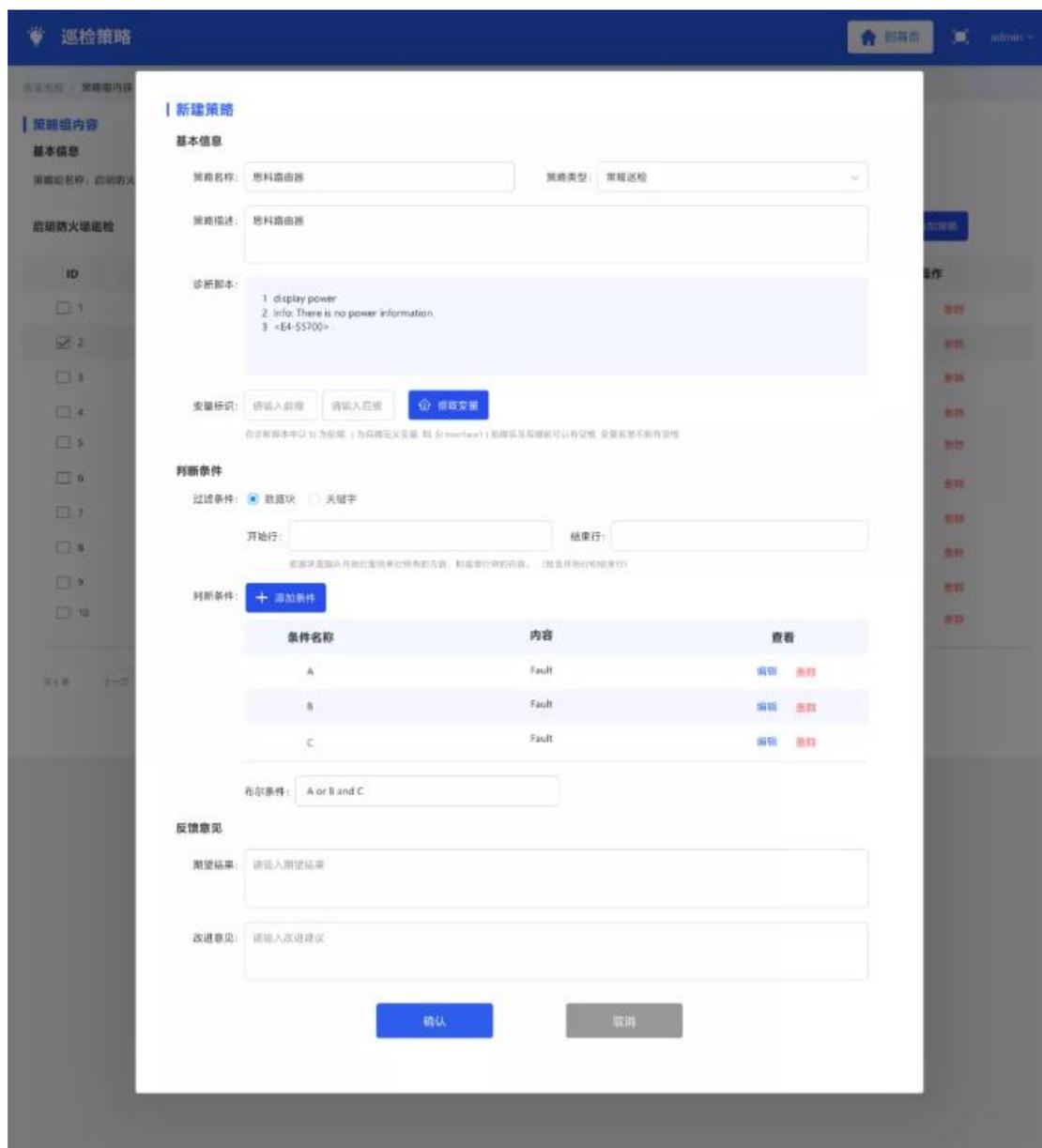
策略组名称: 启明防火墙巡检 检查分类: 常规巡检 设备厂商: 启明 设备类型: 防火墙

启明防火墙巡检

ID	策略名称	策略描述	最后修改时间	状态	操作
<input type="checkbox"/> 1	CPU使用率	CPU使用率需小于50%	2021-04-08 16:41	<input checked="" type="checkbox"/>	编辑 删除
<input checked="" type="checkbox"/> 2	内存使用率	内存使用率需小于50%	2021-04-08 16:41	<input type="checkbox"/>	编辑 删除
<input type="checkbox"/> 3	电源运行状态	接口状态为up	2021-04-08 16:41	<input checked="" type="checkbox"/>	编辑 删除
<input type="checkbox"/> 4	电源运行状态	接口双工模式需要为双工	2021-04-08 16:41	<input type="checkbox"/>	编辑 删除
<input type="checkbox"/> 5	CPU温度	CPU使用率需小于50%	2021-04-08 16:41	<input checked="" type="checkbox"/>	编辑 删除
<input type="checkbox"/> 6	接口状态	内存使用率需小于50%	2021-04-08 16:41	<input type="checkbox"/>	编辑 删除
<input type="checkbox"/> 7	CPU使用率	接口状态为up	2021-04-08 16:41	<input checked="" type="checkbox"/>	编辑 删除
<input type="checkbox"/> 8	内存使用率	接口双工模式需要为双工	2021-04-08 16:41	<input type="checkbox"/>	编辑 删除
<input type="checkbox"/> 9	接口流出差包率	接口状态为up	2021-04-08 16:41	<input checked="" type="checkbox"/>	编辑 删除
<input type="checkbox"/> 10	异常日志信息	接口双工模式需要为双工	2021-04-08 16:41	<input type="checkbox"/>	编辑 删除

共 6 条 上一页 1 2 3 ... 下一页 每页 1 页

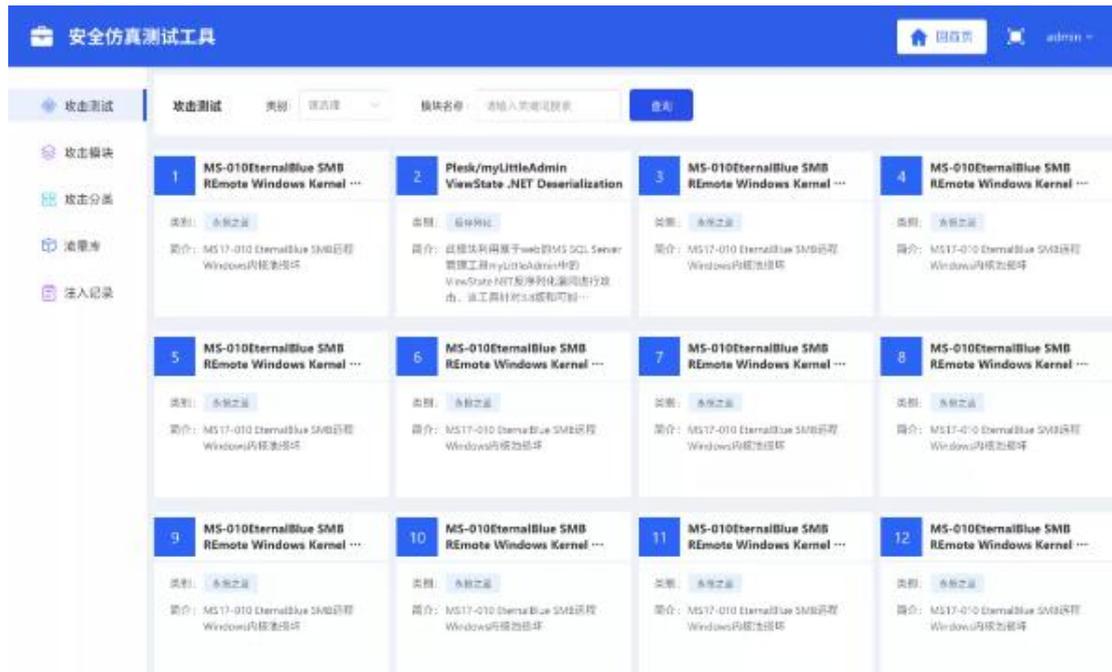
编辑某策略:



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。

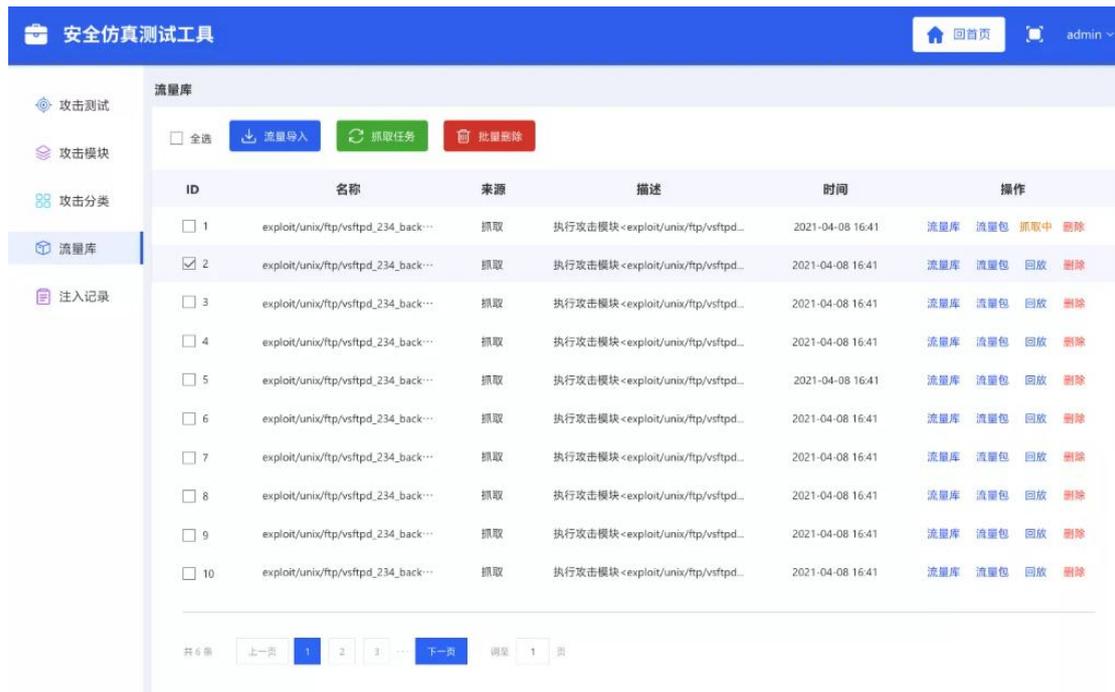
漏洞攻击脚本库:



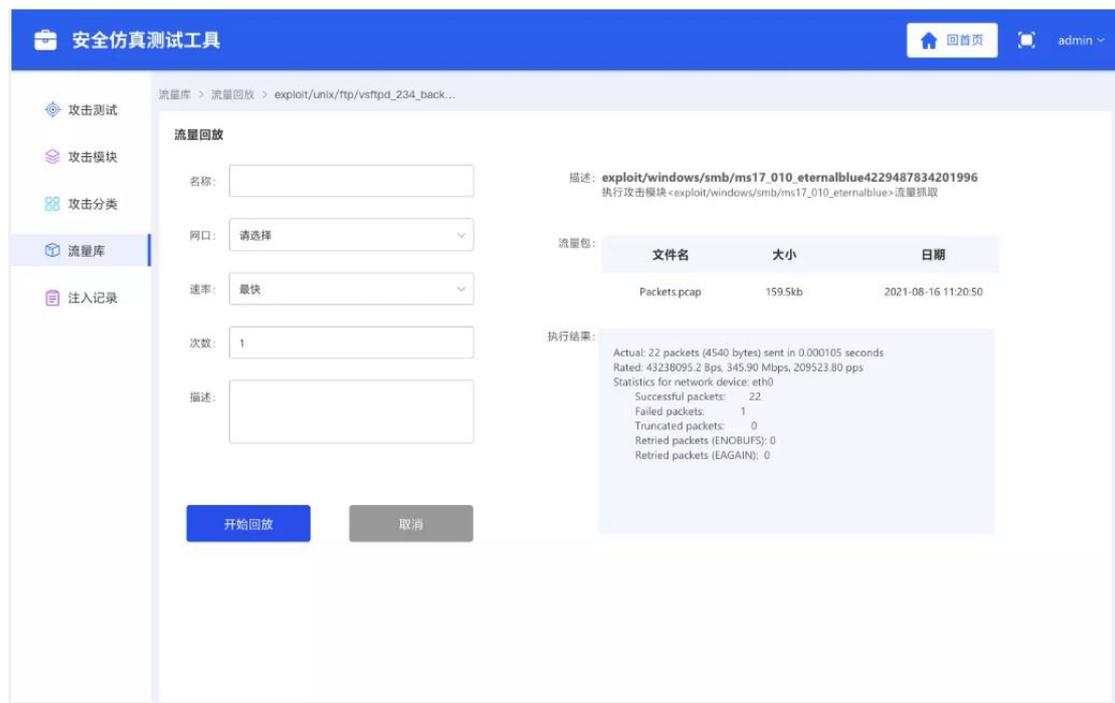
某漏洞攻击脚本执行过程：



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。

日志设置

系统操作日志

用户名: 角色: 包含 时间范围: 操作详情: 搜索 导出

ID	操作时间	用户名	角色	操作详情
1	2021-04-08 16:41	admin	Administrator	设置页面超时时间为: 30
2	2021-04-08 16:41	admin	Administrator	导出登录日志
3	2021-04-08 16:41	admin	Administrator	设置密码更新周期为: 700
4	2021-04-08 16:41	admin	Administrator	删除用户: admin
5	2021-04-08 16:41	admin	Administrator	设置页面超时时间为: 30
6	2021-04-08 16:41	admin	Administrator	导出登录日志
7	2021-04-08 16:41	admin	Administrator	设置密码更新周期为: 700
8	2021-04-08 16:41	admin	Administrator	删除用户: admin
9	2021-04-08 16:41	admin	Administrator	设置密码更新周期为: 700
10	2021-04-08 16:41	admin	Administrator	删除用户: admin

共 6 条 上一页 1 2 3 下一页 1 页

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。

日志设置

登录日志

用户名: IP: 时间范围: 描述: 搜索 导出

ID	状态	用户名	角色	IP地址	登陆时间	描述
1	在线	admin	Administrator	123.116.147.169	2021-04-08 16:41	Normal login!
2	离线	admin	Administrator	123.116.147.169	2021-04-08 16:41	Normal logout!
3	离线	admin	Administrator	123.116.147.169	2021-04-08 16:41	Normal login!
4	离线	admin	Administrator	123.116.147.169	2021-04-08 16:41	Normal logout!
5	离线	admin	Administrator	123.116.147.169	2021-04-08 16:41	Normal login!
6	离线	admin	Administrator	123.116.147.169	2021-04-08 16:41	Normal logout!
7	离线	admin	Administrator	123.116.147.169	2021-04-08 16:41	Normal logout!
8	离线	admin	Administrator	123.116.147.169	2021-04-08 16:41	Normal logout!
9	离线	admin	Administrator	123.116.147.169	2021-04-08 16:41	Normal logout!
10	离线	admin	Administrator	123.116.147.169	2021-04-08 16:41	Normal logout!

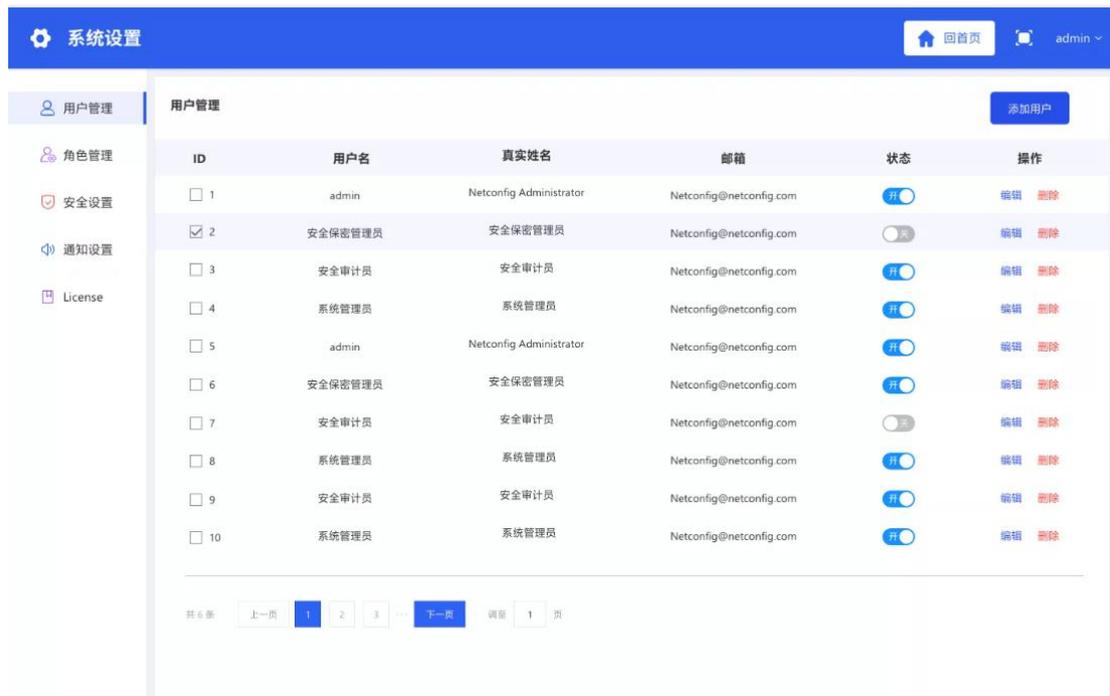
登录日志用于审计用户登录、退出系统的情况。

共 6 条 上一页 1 2 3 下一页 1 页

2.6. 系统管理

2.6.1. 用户管理

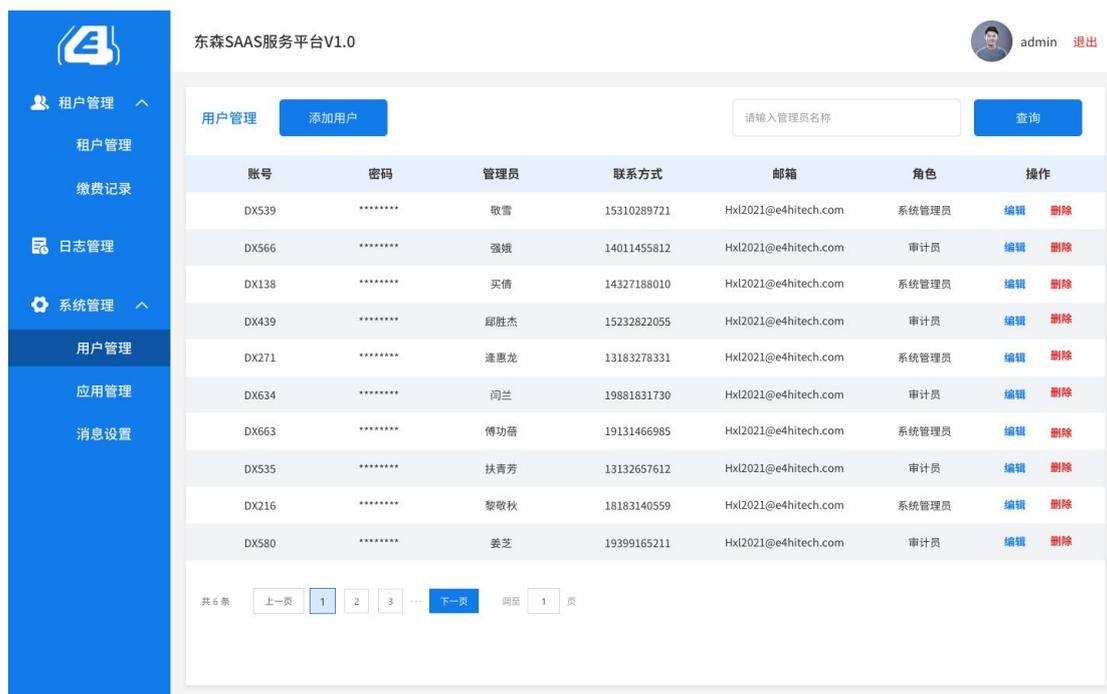
用户管理用于维护平台管理人员。可以进行用户新增、编辑、以及删除操作。系统内置了系统管理员、审计员两个角色。管理员主要负责系统的日常维护。审计员主要负责通过日志对管理员行为进行审计监督工作。



ID	用户名	真实姓名	邮箱	状态	操作
<input type="checkbox"/> 1	admin	Netconfig Administrator	Netconfig@netconfig.com	开	编辑 删除
<input checked="" type="checkbox"/> 2	安全保密管理员	安全保密管理员	Netconfig@netconfig.com	关	编辑 删除
<input type="checkbox"/> 3	安全审计员	安全审计员	Netconfig@netconfig.com	开	编辑 删除
<input type="checkbox"/> 4	系统管理员	系统管理员	Netconfig@netconfig.com	开	编辑 删除
<input type="checkbox"/> 5	admin	Netconfig Administrator	Netconfig@netconfig.com	开	编辑 删除
<input type="checkbox"/> 6	安全保密管理员	安全保密管理员	Netconfig@netconfig.com	开	编辑 删除
<input type="checkbox"/> 7	安全审计员	安全审计员	Netconfig@netconfig.com	关	编辑 删除
<input type="checkbox"/> 8	系统管理员	系统管理员	Netconfig@netconfig.com	开	编辑 删除
<input type="checkbox"/> 9	安全审计员	安全审计员	Netconfig@netconfig.com	开	编辑 删除
<input type="checkbox"/> 10	系统管理员	系统管理员	Netconfig@netconfig.com	开	编辑 删除

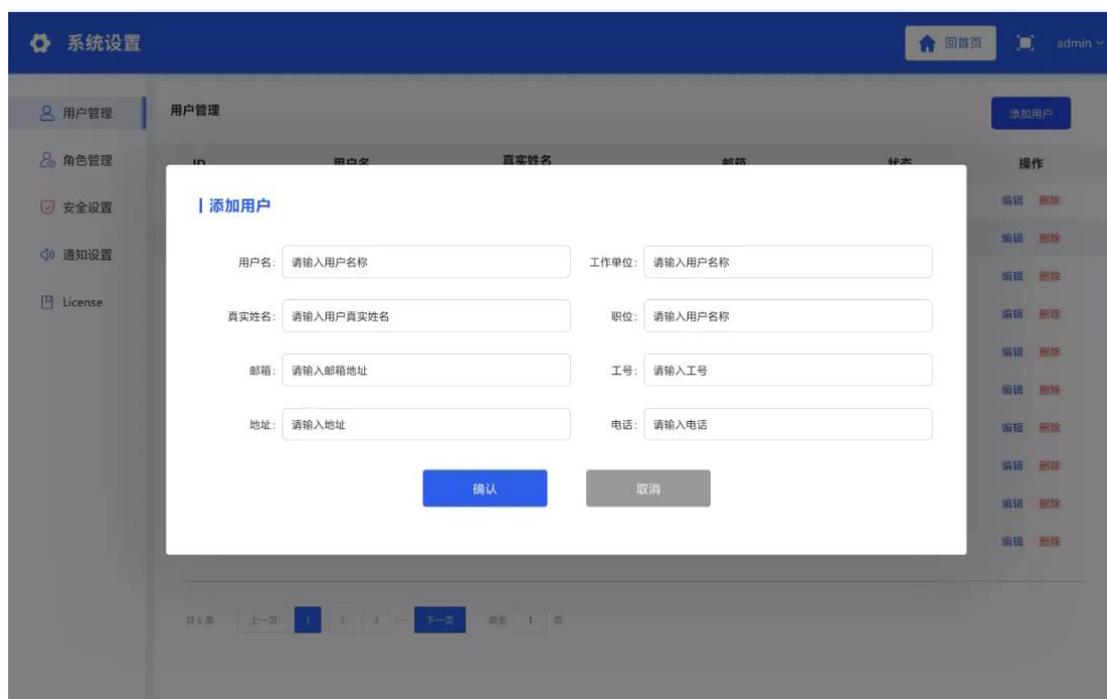
查询

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。



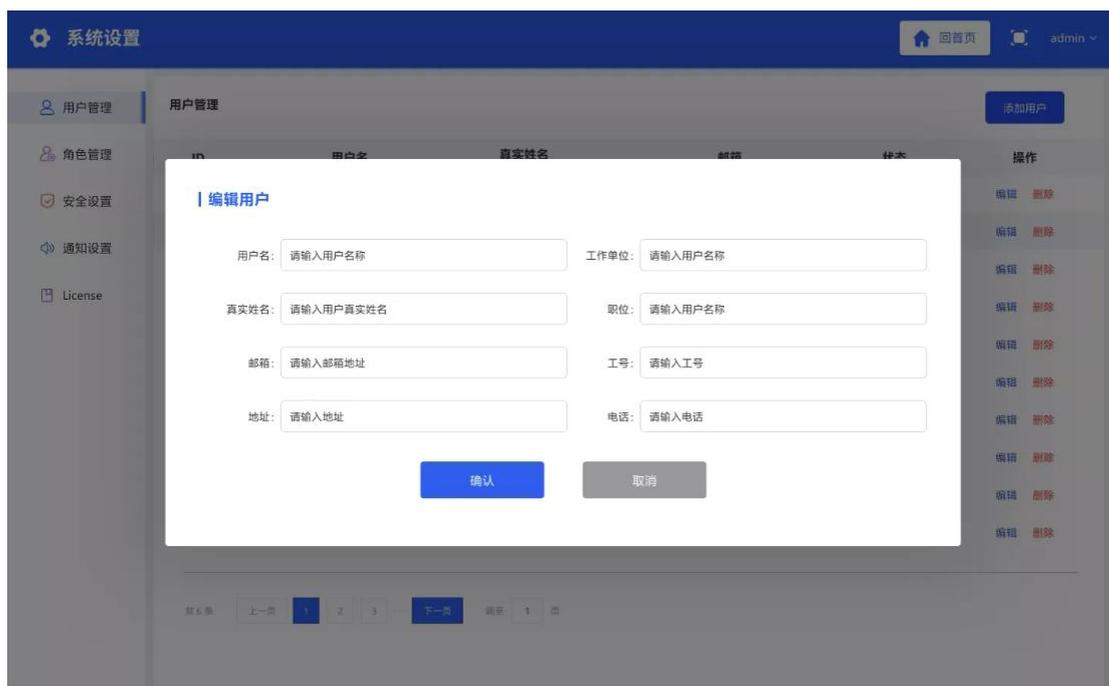
新增

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。



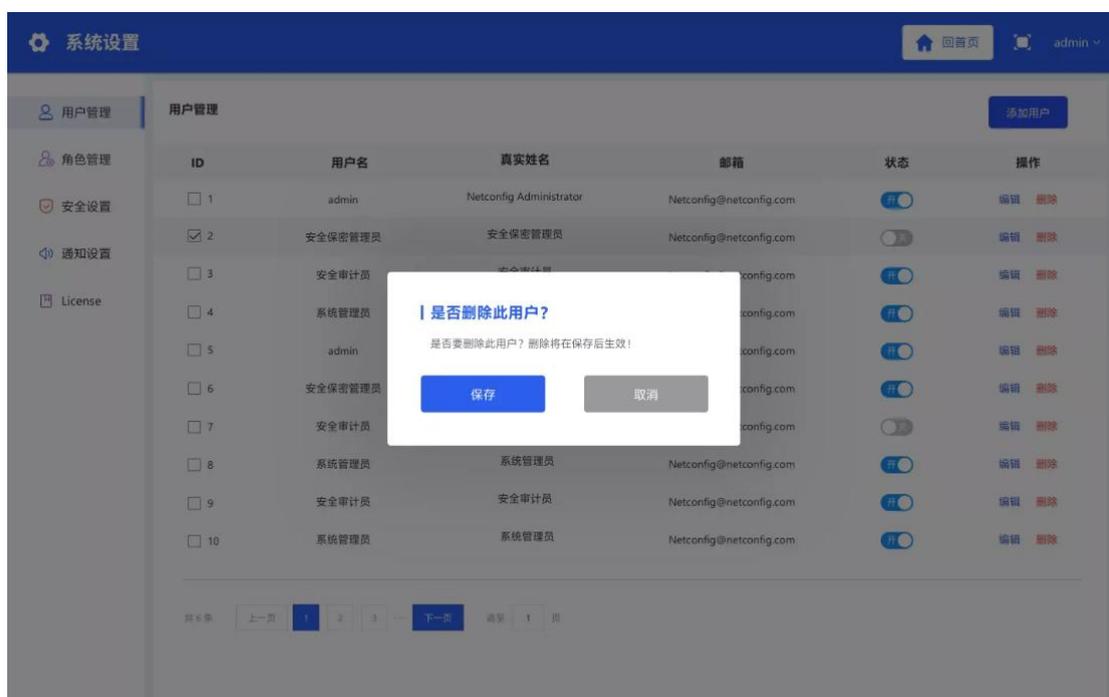
编辑

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。



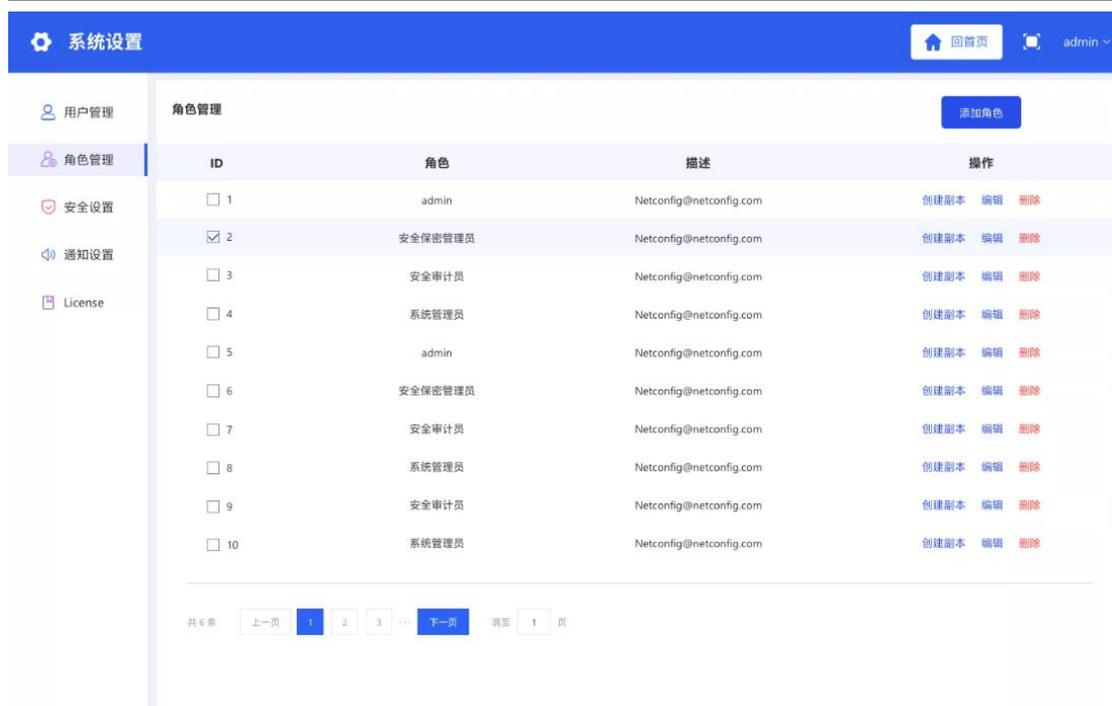
删除

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。



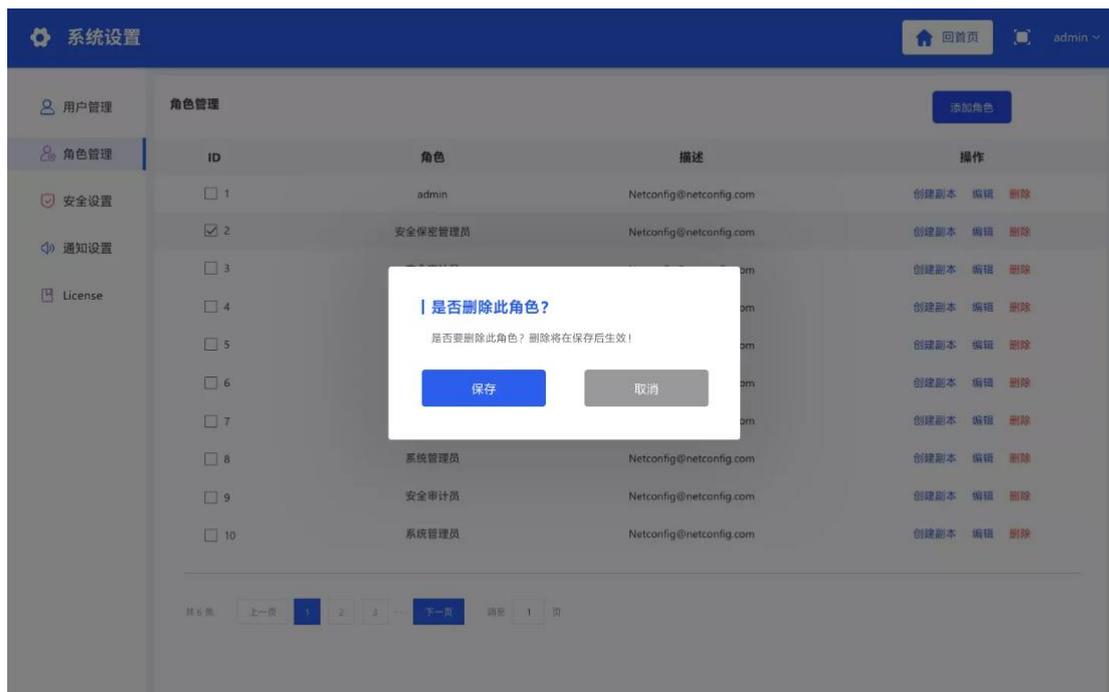
编辑

选择一条角色，点击编辑按钮，弹出此角色信息。



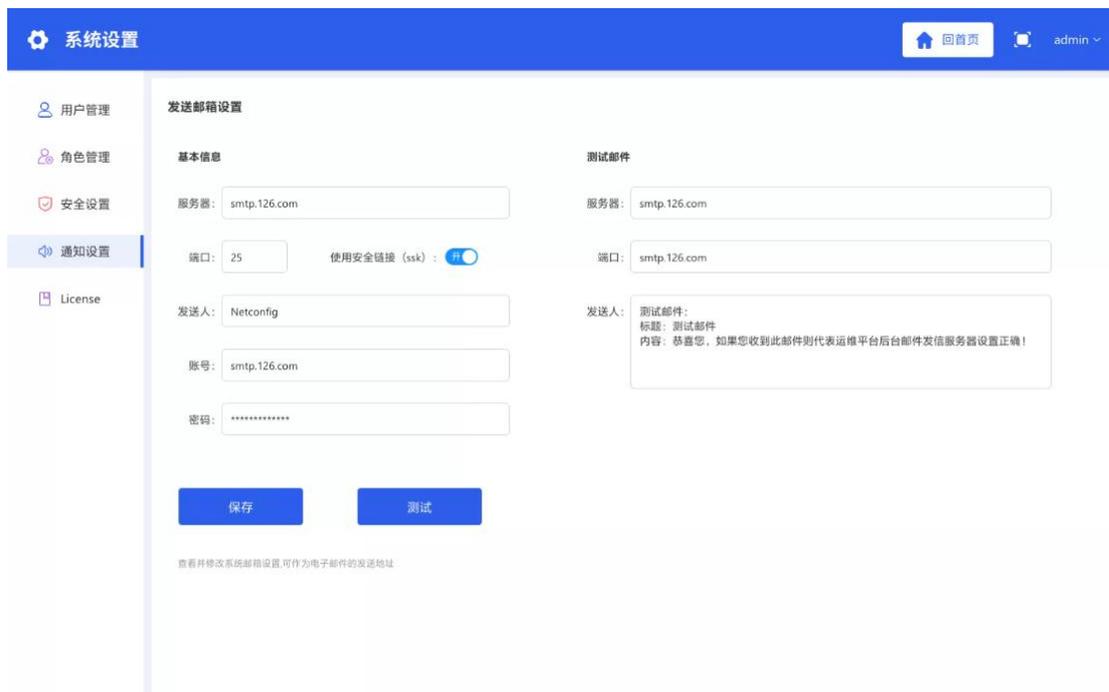
删除

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。



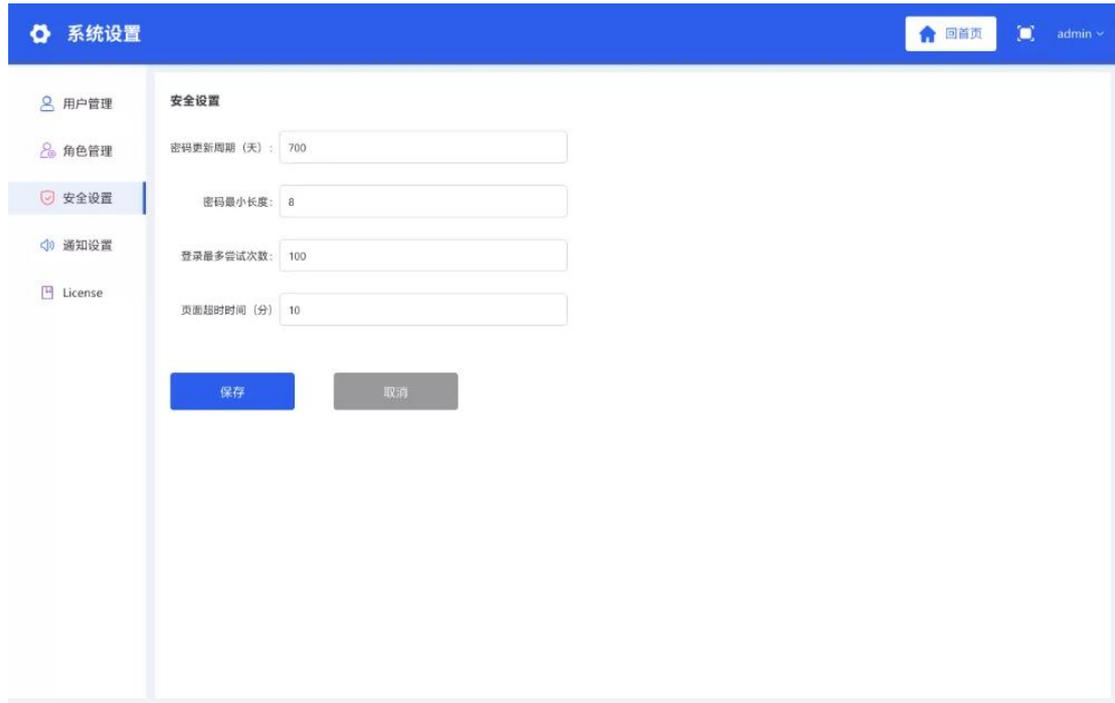
2.6.3. 通知设置

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。

