

网络安全管理平台

用户手册

V1.0.10

杭州奇固科威信息技术有限公司

2024 年 8 月

目 录

1	启动界面.....	3
2	管理员使用界面.....	3
2.1	授权管理.....	4
2.1.1	注册状态.....	4
2.2	用户管理.....	5
2.3	基本配置.....	7
2.4	监控设备管理.....	8
2.4.1	新增通讯参数.....	8
2.4.2	导出平台证书.....	9
2.5	告警设置.....	10
2.5.1	新增告警.....	11
3	操作员使用界面.....	12
3.1	首页.....	13
3.2	网络安全装置管理.....	14
3.2.1	网安切换.....	14
3.2.2	概览.....	14
3.2.3	自诊断.....	15
3.2.3.1	设备诊断.....	15
3.2.4	上传事件.....	15
3.2.4.1	查询.....	16
3.2.5	配置查看.....	17
3.2.5.1	资产更新.....	18
3.2.5.2	资产导出.....	18
3.2.6	监控查看.....	18
3.2.7	特征库配置.....	19
3.2.7.1	新建.....	19
3.2.7.2	搜索.....	20
3.2.7.3	特征库导出.....	20
3.2.7.4	特征库导入.....	20
4	审计员使用界面.....	20
5.1	登录日志.....	21
5.2	操作日志.....	21
5.3	错误日志.....	22

1 启动界面

浏览器（推荐 Google Chrome 浏览器）打开，https://电脑 IP，如本地 IP 为：172.10.11.100，输入 https://172.10.11.100 进入登录界面。



2 管理员使用界面

管理员：用户名 `admin`，密码 `Admin@123456`

进入主界面后如下图所示，该界面主要实现对平台参数的配置，包括用户管理、平台基本配置、授权管理、监控设备管理、告警设置。如下图：

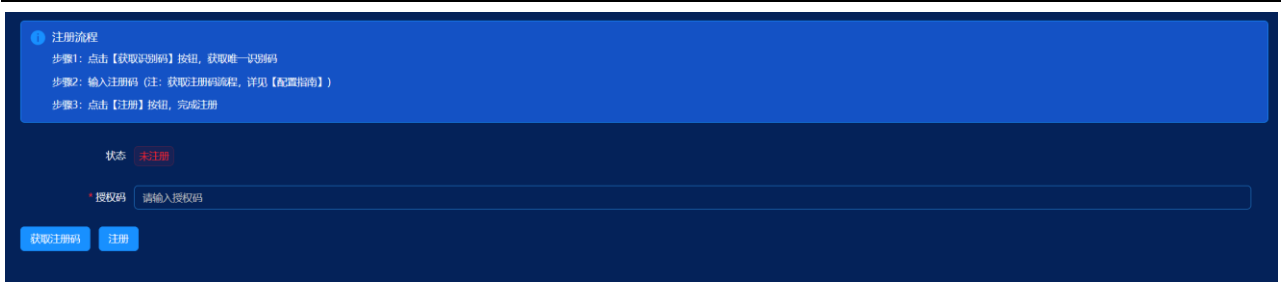


2.1 授权管理

2.1.1 注册状态

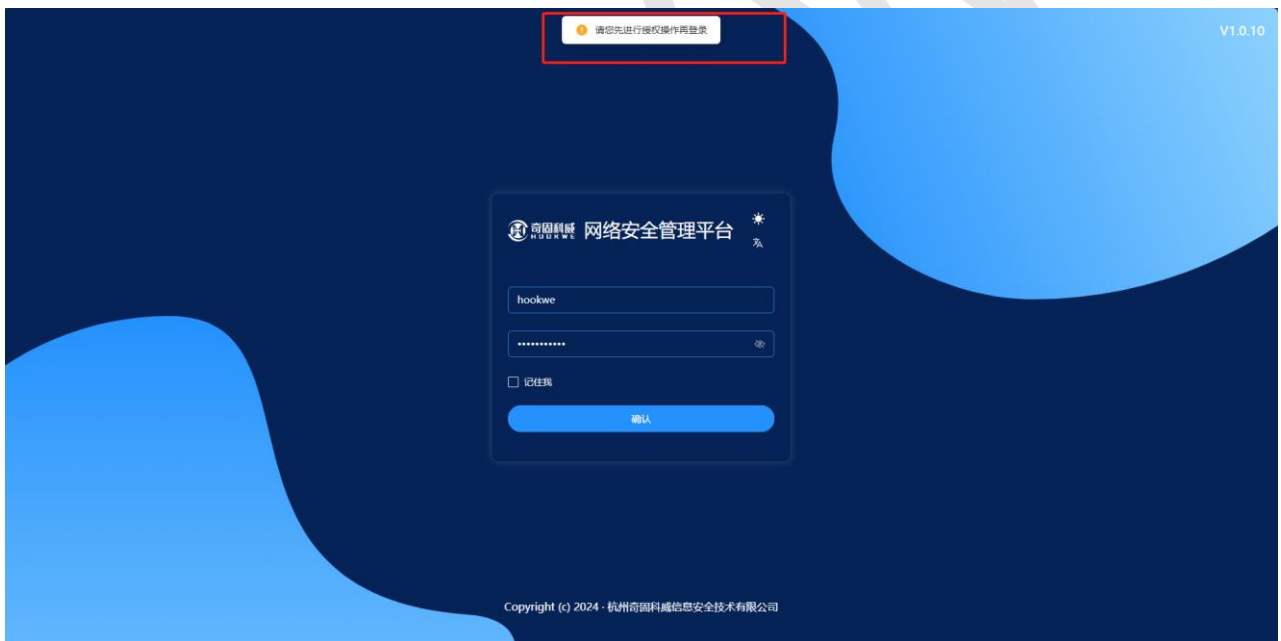
系统会显示注册状态，状态为已注册，说明已经注册成功，其他情况请根据下述步骤进行注册。点击获取注册码，将获得的注册码发给技术人员得到授权码后输入，点击注册即可。





- 1、 合同项目名称：（填写对应的合同或项目名称）
- 2、 厂站名称：（如某某电厂等）
- 3、 地址：（省份-城市）
- 4、 装置名称：网络安全管理平台
- 5、 网安设备套数：（网安本地化模块连接网安的数量，没有则填 0）
- 6、 唯一识别码：（如 269F1F16FDFEBCB61DB058FDD626C9）
- 7、 申请人：
- 8、 联系方式：
- 9、 申请日期：

如果未授权，其他用户无法登录



2.2 用户管理

该模块功能针对用户进行增加、修改、删除操作。

✓ 新增用户

点击新增用户按钮，设置需要新增的用户名，选择角色，创建密码等。点击保存创建成功。如下图：

新增用户 ×

用户名 *

用户类型 *

请选择用户类型 ∨

管理员

操作员

审计员

确认密码 *

✓ 修改用户

点击用户列表中的编辑按钮，可以对用户进行修改操作。

编辑用户 ✕

用户名 *

用户类型 *

管理员密码 *

密码 *

确认密码 *

- ✓ 删除用户
点击用户列表中的删除进行删除。此操作不可逆，点击后直接删除该用户。

2.3 基本配置



配置项	当前值	操作
管理平台名称	网络安全管理平台	
104端口	8080	- +
最大未确认输入数	10	- +
104确认次数	6	- +
历史存储时长	3 年	- +
离线判断周期(分钟)	8	- +
CPU利用率上报阈值(%)	80	- +
内存利用率上报阈值(%)	90	- +

刷新 保存

该界面用于配置网络安全管理平台的 104 通讯参数。

2.4 监控设备管理



该界面用于配置网络安全监测装置的 ip，名称，端口号，类型和证书，配置完可以通过状态查看网络安全管理平台 and 网络安全监测装置的通讯状态。

2.4.1 新增通讯参数

点击新增通讯参数按钮，输入网络安全监测装置的 ip，名称，端口号（8801），类型和平台证书，点击确定即可新增。

新增监控设备 ×

监控设备IP地址 *

监控设备名称

端口号 *

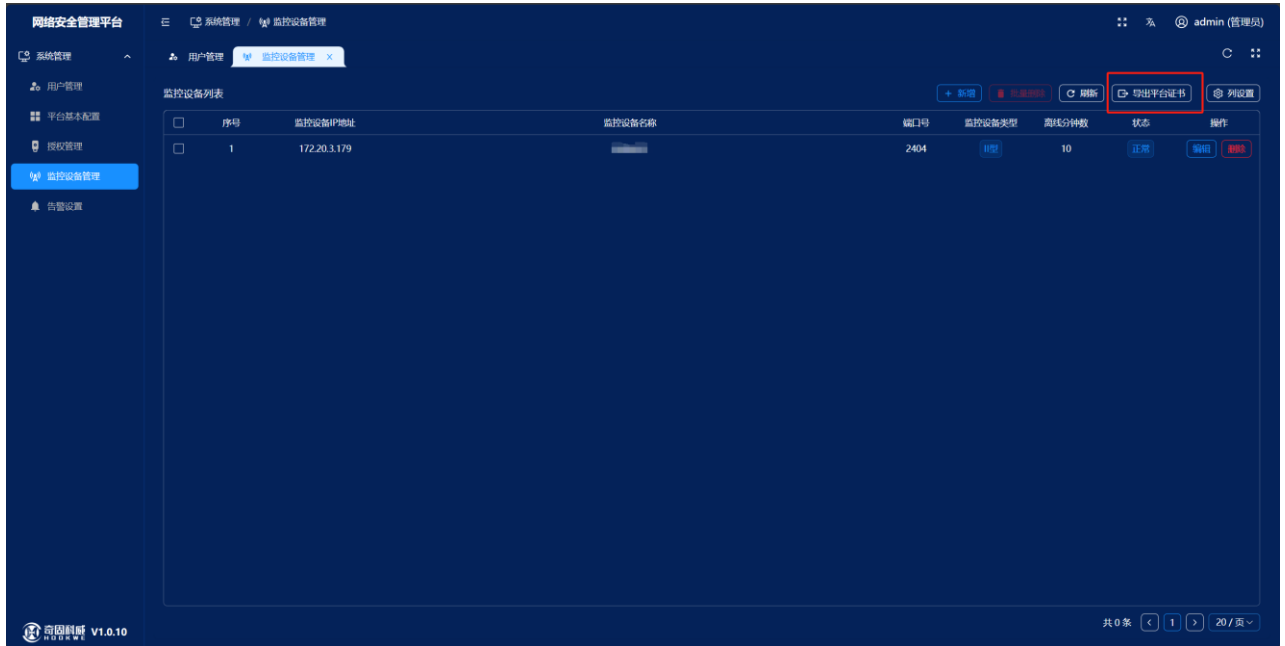
监控设备类型

离线分钟数 *

证书名 *

2.4.2 导出平台证书

点击导出平台证书按钮，可以将本平台的平台证书导出，后续需要将平台证书导入网络安全监测装置，进行通信配置，即可与本平台连接。



2.5 告警设置

该模块功能可以对告警事件等级，设备类型，类型，子类型，内容描述进行设置和过滤。



点击告警配置导出，可以导出配置。

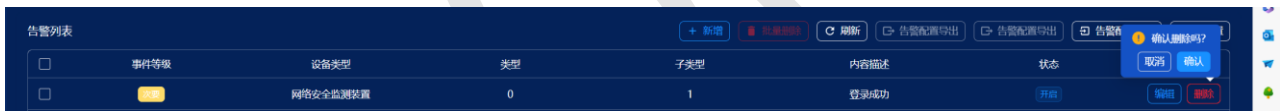
点击告警配置导入，可以导入已有配置。

点击搜索按钮，可以通过设备类型，事件等级和状态对告警进行查询。

点击编辑按钮，可以对单条告警进行配置。



点击删除按钮，可以对告警进行删除。



2.5.1 新增告警

点击新建按钮，可以对告警事件等级，设备类型，类型，子类型，内容描述进行配置，选择开启即为启用，选择关闭可以屏蔽此条告警。



新建告警配置

事件等级 紧急

设备类型 数据库

* 类型 请选择类型

* 子类型 请选择子类型

状态 关闭

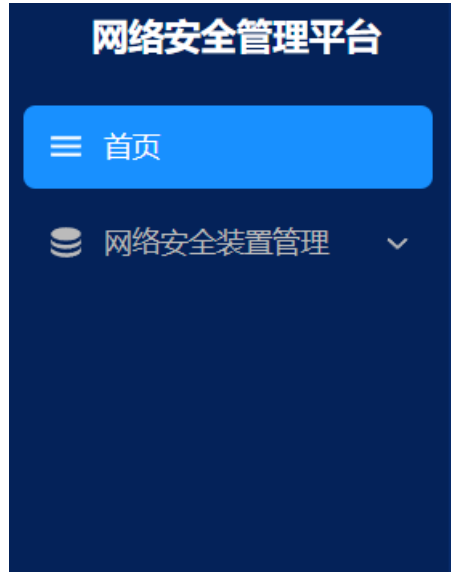
内容描述 请输入内容描述

取消 确认

3 操作员使用界面

操作员：用户名 hookwe，密码 Hookwe@1234

采用操作员用户名和密码进入主界面后如下图所示，该界面主要实现对平台信息查看和统计，包括首页、网安安全装置管理。如下图：



注：操作员首次登录需要优先在网络安全装置管理—配置查看中更新资产，很多展示界面依赖该资产信息。

3.1 首页

该模块功能可以显示网络安全管理装置的信息，如下图：



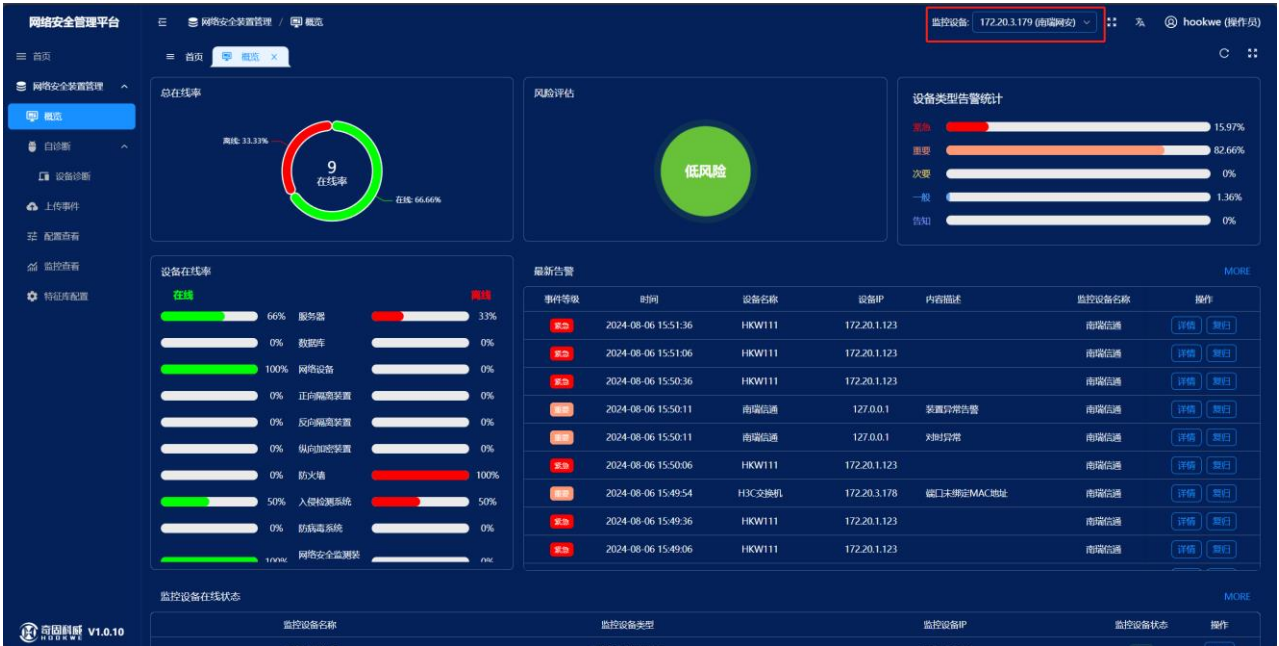
上边显示告警级别统计，实时密通率，资产统计，在线情况和设备类型告警统计。下边最新告警的信息。

3.2 网络安全装置管理

3.2.1 网安切换

该模块功能针对用户切换网安操作。

网安切换在界面右上角功能区中。如下图：



用户可以选择不同网安，查看该网安详细信息。

3.2.2 概览

该模块功能针对用户查看网安整体情况，包括设备总在线率、风险评估、设备在线率、设备类型告警统计、设备告警级别统计、设备在线情况、最新告警信息。

在导航栏中，点击【概览】。如下图：



监控设备在线状态

监控设备名称	监控设备类型	监控设备IP	监控设备状态	操作
南瑞信通	网络安全监测装置	127.0.0.1	在线	详情
联想虚拟机	服务器	172.20.3.181	在线	详情
东软入侵	入侵检测系统	172.20.3.176	离线	详情
linkqi-ubuntu	服务器	172.20.3.119	在线	详情
HKW111	入侵检测系统	172.20.1.123	离线	详情

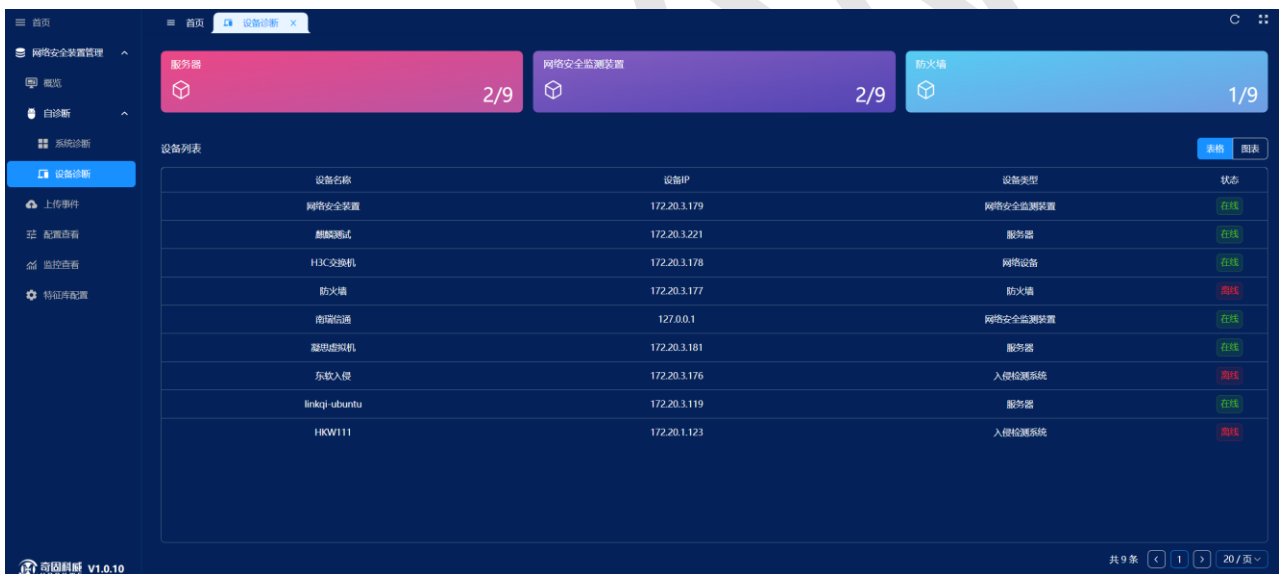
3.2.3 自诊断

该模块功能主要分为系统诊断和设备诊断，用于查看系统状态和设备状态。

3.2.3.1 设备诊断

该模块功能用于查看服务器、横向反向隔离装置、网络安全监测装置、网络设备、防火墙的设备状态，这个需要根据告警信号区分是否在线，在资产更新后需要延迟 3 分钟更新资产状态。

在导航栏中，点击【自诊断】-【设备诊断】。如下图：



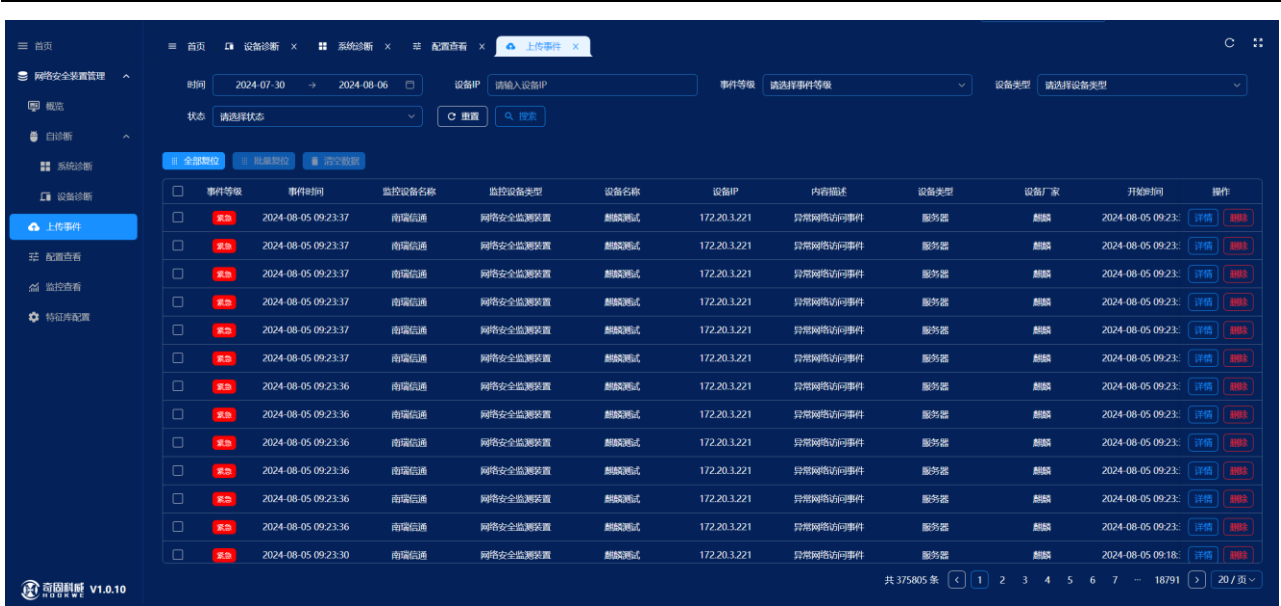
设备列表

设备名称	设备IP	设备类型	状态
网络安全装置	172.20.3.179	网络安全监测装置	在线
麒麟测试	172.20.3.221	服务器	在线
H3C交换机	172.20.3.178	网络设备	在线
防火墙	172.20.3.177	防火墙	离线
南瑞信通	127.0.0.1	网络安全监测装置	在线
联想虚拟机	172.20.3.181	服务器	在线
东软入侵	172.20.3.176	入侵检测系统	离线
linkqi-ubuntu	172.20.3.119	服务器	在线
HKW111	172.20.1.123	入侵检测系统	离线

3.2.4 上传事件

该模块功能将所有采集到的信息，以告警的形式上送至平台。告警信息主要包括非法外联，对时异常，usb 插拔，网口 up/down 等。

在导航栏中，点击【上传事件】。如下图：



3.2.4.1 查询

输入查询条件，点击【查询】按钮。如下图：



点击详情按钮，可以查看具体的告警信息。

详情 ×

事件等级: 一般	事件时间: 2024-07-31 15:38:17	开始时间: 2024-07-31 15:38:17
监控设备名称: 南瑞信通	监控设备类型: 网络安全监测装置	设备名称: 麒麟测试
设备厂家: 麒麟	设备IP: 172.20.3.221	设备类型: 服务器
类型: 5	子类型: 16	状态: 已复位

内容描述:

上报原文:
<4> 2024-07-31 15:38:17 南瑞信通 DCD 2024-07-31 15:38:17 麒麟测试 172.20.3.221 麒麟 SVR 5 16 1 linkqi 172.20.1.102

建议:

确认

3.2.5 配置查看

该模块功能用于查看当前网安资产详情，包括设备名称、设备 IP、设备 IP2、设备厂商、设备类型、MAC 地址、设备 MAC2、序列号、snmp 版本。

在导航栏中，点击【配置查看】。如下图：



3.2.5.1 资产更新

点击资产更新按钮，可以把网安上新增的资产更新到网络安全管理平台上。

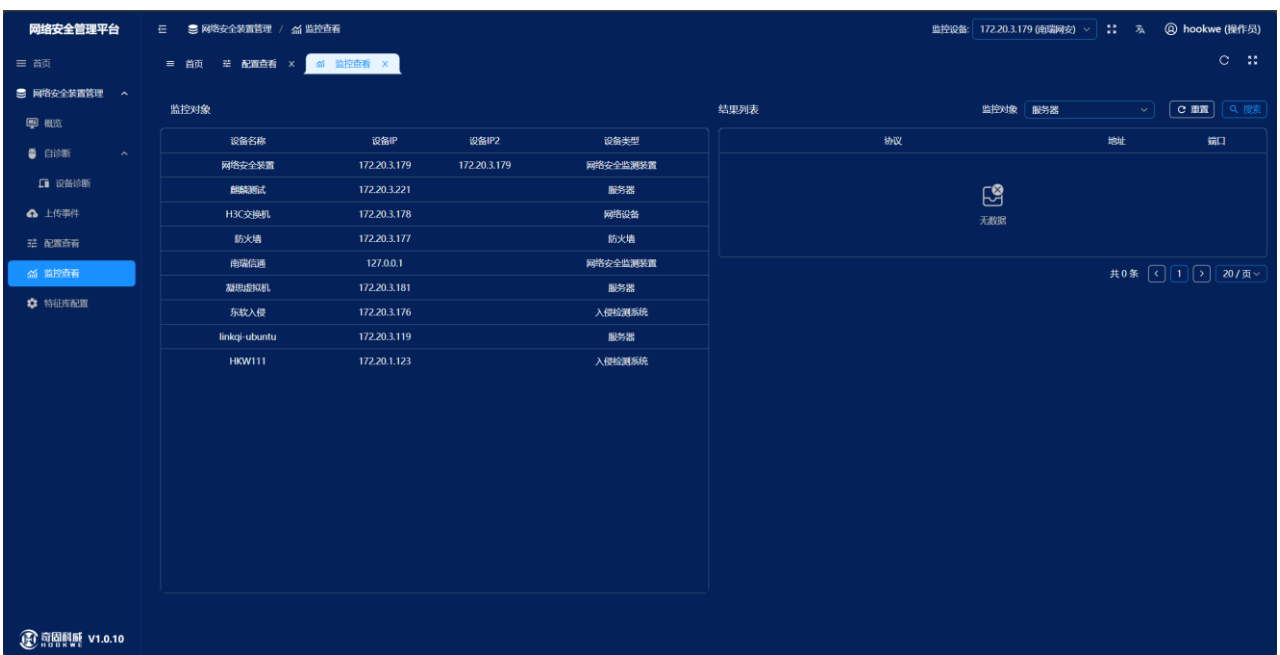
3.2.5.2 资产导出

点击资产导出按钮，可以把网络安全管理平台上的资产导出到本机上。

3.2.6 监控查看

该模块功能用于查看设备的网络连接白名单、服务端口白名单、危险操作定义、关键文件/目录清单、存在光驱设备检测周期、非法端口检测周期。

在导航栏中，点击【监控查看】。如下图：

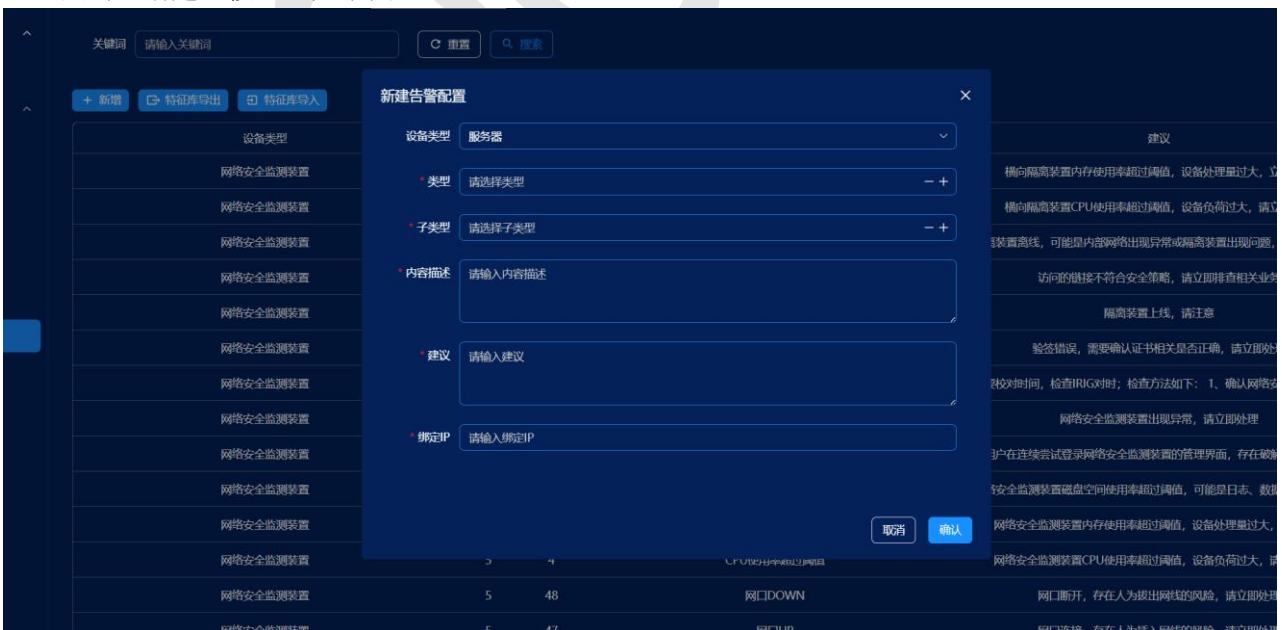


3.2.7 特征库配置

该功能模块用来配置特征库信息。

3.2.7.1 新建

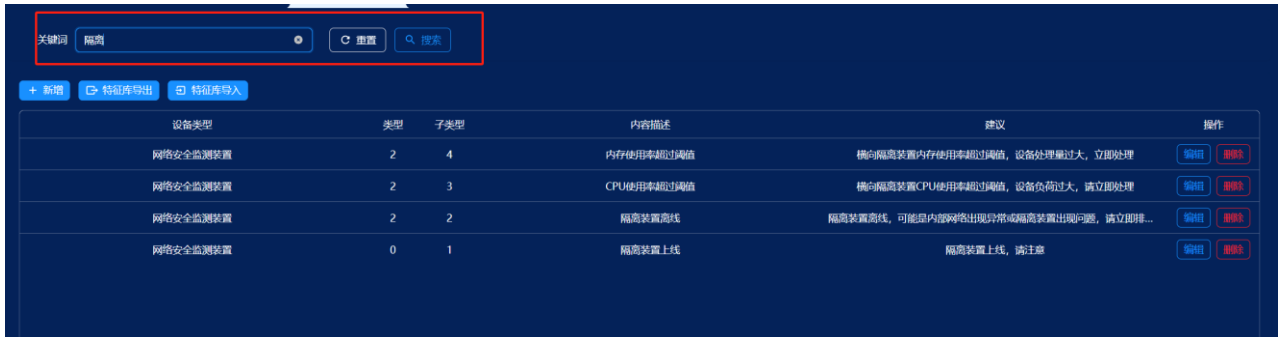
点击【新建】按钮。如下图：



输入设备类型、类型、子类型、内容描述、建议及绑定 IP 后，点击“确定”按钮，进行特征库提交。

3.2.7.2 搜索

输入关键词，点击“搜索”按钮，进行条件查询，如下图：



3.2.7.3 特征库导出

点击“特征库导出”按钮，进行特征库的导出操作。

3.2.7.4 特征库导入

点击“特征库导入”按钮，进行特征库的导入操作。

4 审计员使用界面

审计员：用户名 **auditor**，密码 **Auditor@1234**

5.1 登录日志

网络安全管理平台 日志管理 / 登录日志

用户名: 状态:

登录日志

用户名	操作类型	状态	操作IP	User Agent	创建时间
auditor	登录	成功	172.20.1.161	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36 Edg/126.0.0.0	2024-08-06 15:54:27
auditor	登录	失败	172.20.1.161	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36 Edg/126.0.0.0	2024-08-06 15:54:16
hookwe	登录	成功	172.20.1.161	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36 Edg/126.0.0.0	2024-08-06 15:49:07
hookwe	登录	成功	172.20.1.161	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36	2024-08-06 15:44:11
admin	登录	成功	172.20.1.107	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36	2024-08-06 14:28:55
auditor	登录	成功	172.20.1.107	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36	2024-08-06 14:27:24
admin	登录	成功	172.20.1.107	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36	2024-08-06 14:27:06
auditor	登录	成功	172.20.1.161	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36	2024-08-05 11:40:20
auditor	登录	成功	172.20.1.107	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36	2024-08-05 11:37:46
admin	登录	成功	172.20.1.107	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36	2024-08-05 11:34:21
admin	登录	成功	172.20.1.161	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36 Edg/126.0.0.0	2024-08-05 11:15:40
hookwe	登录	成功	172.20.1.161	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36	2024-08-05 10:59:41
auditor	登录	成功	172.20.1.107	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36	2024-08-05 10:52:16
admin	登录	成功	172.20.1.107	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36	2024-08-05 10:51:00
auditor	登录	成功	172.20.1.161	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36	2024-08-05 08:57:45
admin	登录	成功	172.20.1.161	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36 Edg/126.0.0.0	2024-08-05 08:45:49
admin	登录	成功	172.20.1.161	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36 Edg/126.0.0.0	2024-08-01 15:59:15

共 376 条 / 页

5.2 操作日志

网络安全管理平台 日志管理 / 操作日志

状态:

操作日志

用户名	用户操作	请求URL	请求方式	请求参数	请求时长	状态	操作IP	User Agent	创建时间
auditor	导入	/networkSecurity/fil...	POST	["bytes":"0M8R4...	40	成功	172.20.1.161	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, li...	2024-08-05 14:21:10
auditor	导入	/networkSecurity/fil...	POST	["bytes":"0M8R4...	51	成功	172.20.1.161	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, li...	2024-08-05 14:20:43
auditor	导入	/networkSecurity/fil...	POST	["bytes":"0M8R4...	43	成功	172.20.1.161	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, li...	2024-08-05 14:20:06
admin	修改	/networkSecurity/c...	PUT	[{"cer":"172.20.3...	3	成功	172.20.1.161	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, li...	2024-08-05 11:27:57
admin	修改	/networkSecurity/c...	PUT	[{"cer":"172.20.3...	42	成功	172.20.1.161	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, li...	2024-08-05 11:27:33
admin	修改	/networkSecurity/c...	PUT	[{"cer":"172.20.3...	3	成功	172.20.1.161	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, li...	2024-08-05 11:27:12
admin	证书文件上传	/networkSecurity/fil...	POST	"172.20.3.179.cer"	1	成功	172.20.1.161	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, li...	2024-08-05 11:26:53
admin	修改	/networkSecurity/c...	PUT	[{"cer":"172.20.3...	2	成功	172.20.1.161	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, li...	2024-08-05 11:26:32
admin	文件下载	/networkSecurity/fil...	POST		0	成功	172.20.1.161	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, li...	2024-08-05 11:25:23
admin	文件下载	/networkSecurity/fil...	POST		5	成功	172.20.1.161	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, li...	2024-08-05 11:25:08
auditor	导入	/networkSecurity/fil...	POST	["bytes":"UEsDB...	28	失败	172.20.1.107	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, li...	2024-08-05 11:05:17
auditor	导入	/networkSecurity/fil...	POST	["bytes":"0M8R4...	37	成功	172.20.1.161	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, li...	2024-08-05 09:46:31
auditor	导入	/networkSecurity/fil...	POST	["bytes":"0M8R4...	53	成功	172.20.1.161	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, li...	2024-08-05 09:40:48
auditor	导入	/networkSecurity/fil...	POST	["bytes":"0M8R4...	25	成功	172.20.1.161	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, li...	2024-08-05 09:34:15
auditor	导入	/networkSecurity/fil...	POST	["bytes":"0M8R4...	186	成功	172.20.1.161	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, li...	2024-08-05 09:33:50
admin	删除	/networkSecurity/al...	DELETE	[15]	4	成功	172.20.1.161	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, li...	2024-08-01 16:28:34
admin	新增	/networkSecurity/al...	POST	[{"adesc":"","alar...	6	成功	172.20.1.161	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, li...	2024-08-01 16:28:28

共 213 条 / 页

5.3 错误日志

The screenshot displays the 'Error Log' (错误日志) section of the Hookwe Network Security Management Platform. The interface includes a sidebar with navigation options like '日志管理' (Log Management) and '错误日志' (Error Log). The main area shows a table of error records. Each record contains the following information:

- 请求URL (Request URL): /networkSecurity/...
- 请求方式 (Request Method): POST or GET
- 请求参数 (Request Parameters): ["ip": "172.20.3.1...", ["id": "687156"]]
- 操作IP (Operation IP): 172.20.1.107 or 172.20.1.161
- User Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36
- 创建时间 (Creation Time): 2024-08-05 11:05:17, 2024-08-05 09:23:10, 2024-08-05 09:22:35, 2024-08-05 09:22:24, 2024-08-05 09:22:12, 2024-08-05 09:22:09, 2024-08-01 16:11:47, 2024-08-01 16:10:13, 2024-08-01 16:07:48, 2024-08-01 16:05:08, 2024-08-01 16:04:46, 2024-08-01 16:02:06, 2024-08-01 16:00:14, 2024-08-01 15:59:05, 2024-08-01 15:45:32
- 操作 (Action): 异常信息 (Abnormal Information)

At the bottom of the page, there is a footer with the Hookwe logo and version 'V1.0.10', and a pagination bar showing '共 131 条' (Total 131 items) and page numbers 1 through 7.