# 网络安全管理平台

# 用户手册

# V1.0.10



杭州奇固科威信息安全技术有限公司

2024 年 8 月

# 目 录

# 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

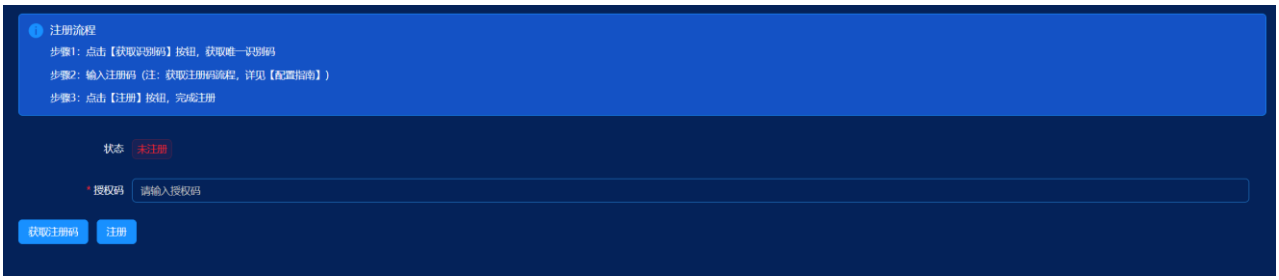
**管理员：用户名 admin，密码 Admin@123456**

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

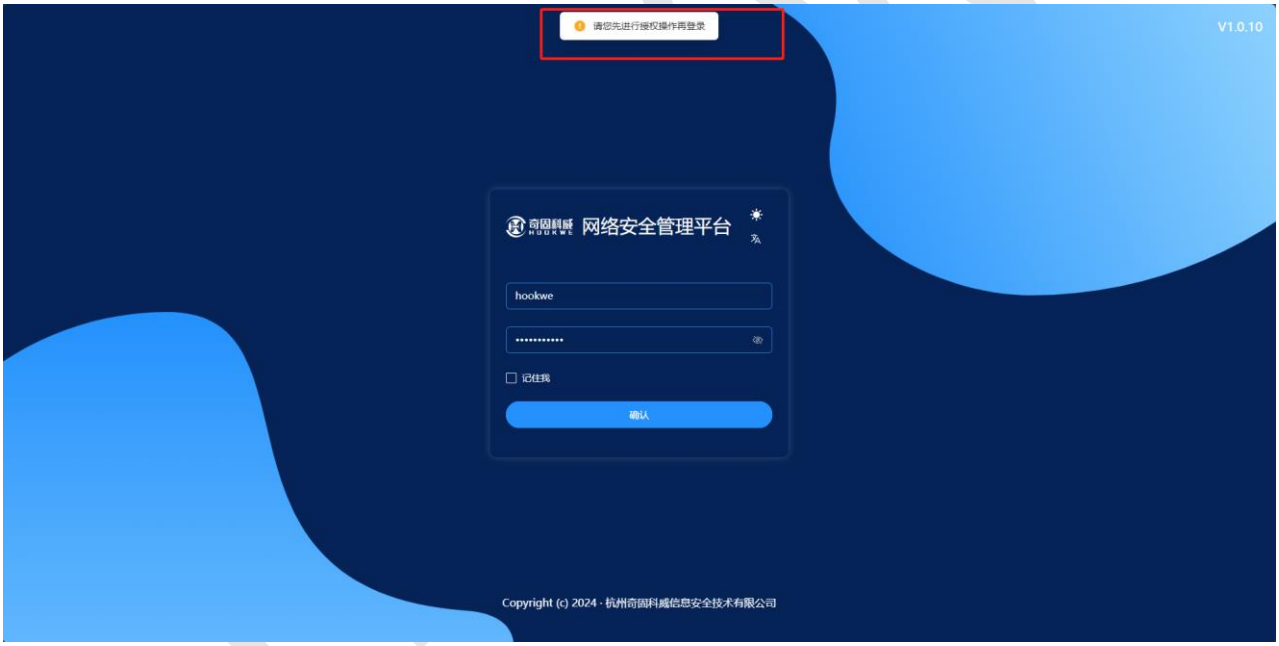
## 2.1.1 注册状态

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：


✓ 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。


✓ 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


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

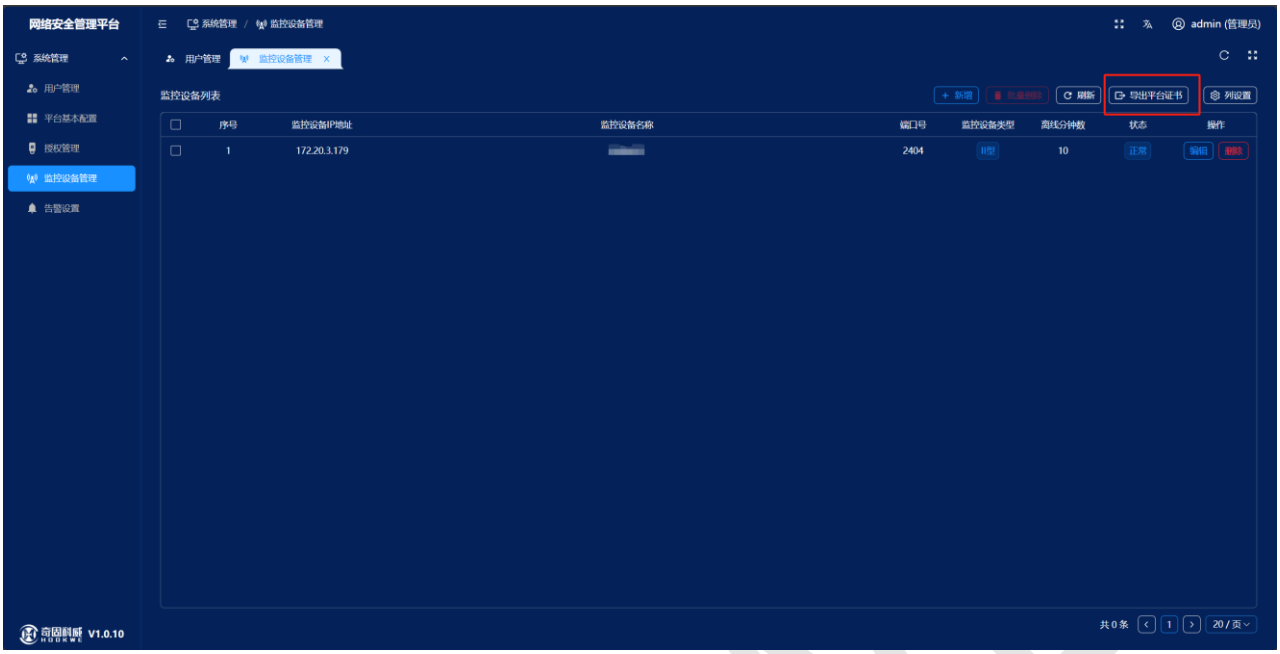

该界面用于配置网络安全监测装置的 ip，名称，端口号，类型和证书，配置完可以通过状态查看网络安全管理平台和网络安全监测装置的通讯状态。

## 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。


## 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。

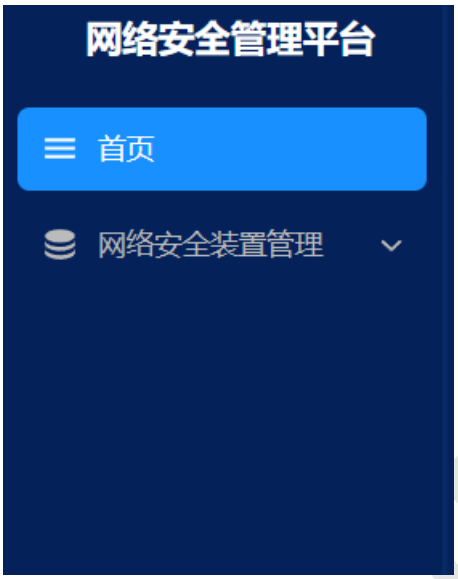

## 2.5.1 新增告警

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。


# 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。

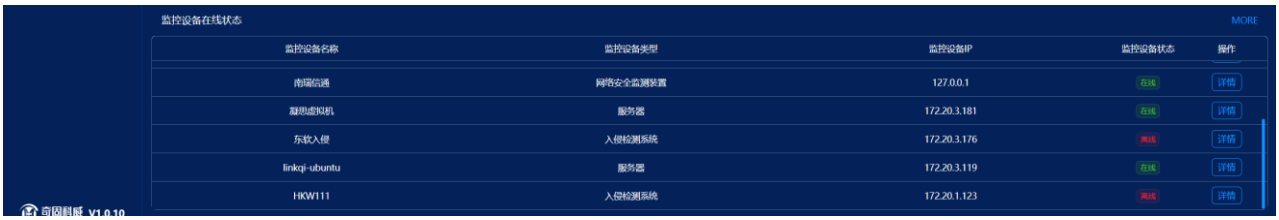
网安切换在界面右上角功能区中。如下图：


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：




## 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

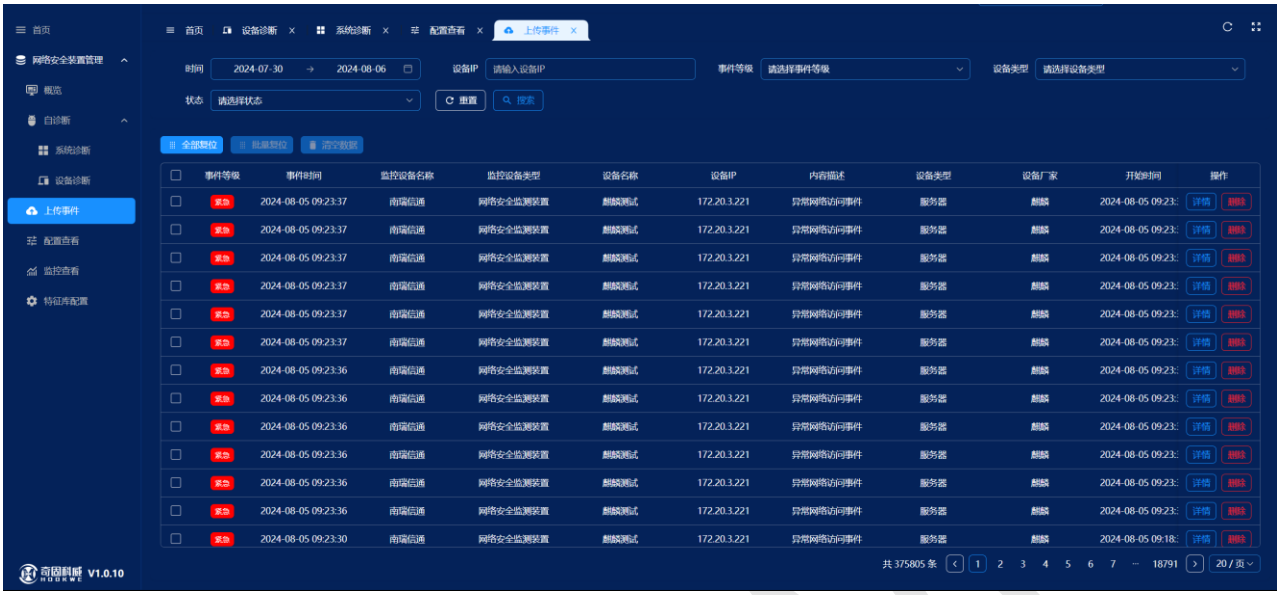
该模块功能用于查看服务器、横向反向隔离装置、网络安全监测装置、网络设备、防火墙的设备状态，这个需要根据告警信号区分是否在线，在资产更新后需要延迟 3 分钟更新资产状态。

在导航栏中，点击【自诊断】-【设备诊断】。如下图：


## 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。


## 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。

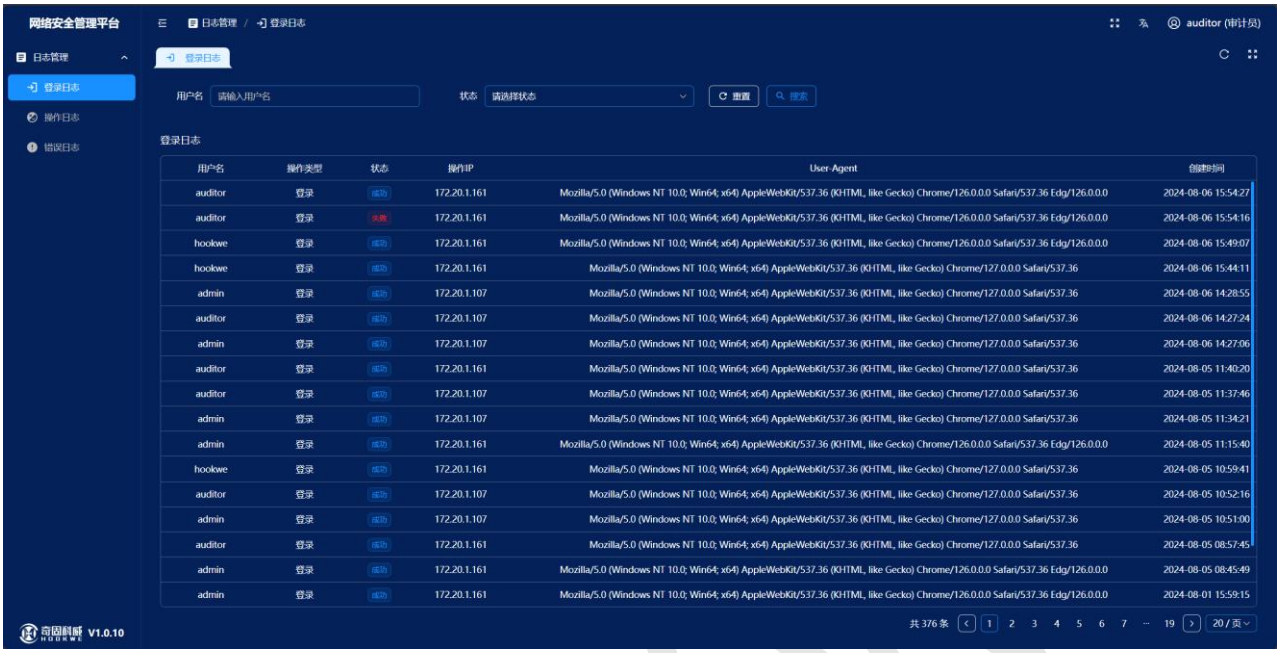
### 3.2.7.4 特征库导入

点击“特征库导入”按钮，进行特征库的导入操作。

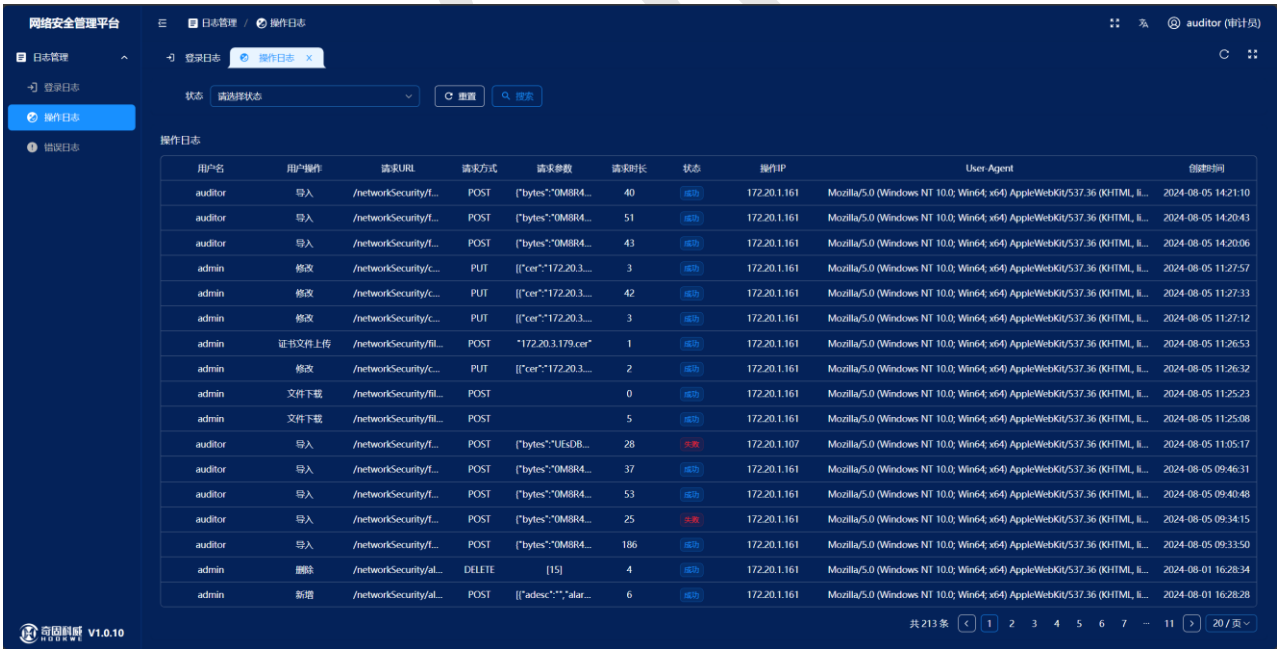
# 4 审计员使用界面

**审计员：用户名 auditor，密码 Auditor@1234**

# 5.1 登录日志




# 5.2 操作日志



# 5.3 错误日志