视频安全管控系统

用户操作手册

目　　录

第 一 部 分 **6**

第一章 设备安装 **7**

第 1 节 安全注意事项 7
1.1 通用安全 7
1.2 用电安全 7
1.3 静电安全 7
第 2 节 使用环境要求 8
2.1 温度要求 8
2.2 湿度要求 8
2.3 洁净度要求 9
2.4 抗干扰要求 9
2.5 接地要求 10
2.6 供电要求 10

第二章 系统登录和退出 **10**

第 1 节 启动平台 10
第 2 节 退出平台 11

第 二 部 分 **12**

视频安全管控系统 **13**

第一章 实时查看 **13**

第 1 节 控制监看区窗口的布局 13
第 2 节 选择需要监看的摄像头 14
第 3 节 云台控制操作 14
第 4 节 管理图片 15
第 5 节 声音控制 16
第 6 节 码流设置 16
第 7 节 清除视频窗口显示的视频 17

第二章 录像回放 **17**

第 1 节 检索录像 18
第 2 节 录像抓帧 19
第 3 节 播放控制 19
第 4 节 录像下载 20

第三章 视频防泄密 **20**

第 1 节 终端管理 21
第 2 节 防泄密策略 24
2.1 防泄密配置 24
2.2 客户端配置 25
2.3 点阵水印溯源 26

第 3 节 安全审批 27
第四章 可信管理 28
第 1 节 可信安全度量 28
1.1 全局策略 29
1.2 策略下发 29
第 2 节 可信状态查询 30
第 3 节 可信节点管理 32
3.1 可以节点设置 32
3.2 节点证书 33
3.3 节点状态 33
第五章 准入与防护 34
第 1 节 主页界面介绍 34
第 2 节 系统退出 35
第 3 节 资产档案 35
3.1 归档资产 35
3.2 待录资产 37
3.3 档案配置 39
3.4 资产发现 41
3.5 资产识别 43
3.6 Dfind 引擎 47
3.7 视图配置 49
第 4 节 边界接入 53
4.1 准入配置 53
4.2 病毒防护 54
4.3 漏洞防御 55
4.4 CIPS 引擎 57
4.5 组合准入 61
第 5 节 风险检查 62
5.1 扫描任务 62
5.2 扫描结果 65
5.3 考核结果 67
5.4 扫描记录 68
5.5 Iscan 引擎 70
5.6 Clink 引擎 70
5.7 考核策略库 74
5.8 漏洞策略库 75
5.9 端口策略库 76
5.10 弱口令策略库 78
5.11 边界风险策略库 80
5.12 配置核查策略库 81
第 6 节 应用市场 82
6.1 IP 地址管理 82

6.2 漏洞知识库 83
第 7 节 告警管理 85
7.1 告警事件 85
7.2 告警配置 86
第 8 节 报表统计 88
8.1 资产统计报表 88
8.2 资产在线报表 88
8.3 风险资产报表 89
8.4 漏洞统计报表 89
第 9 节 日志分析 90
9.1 系统操作日志 90
9.2 准入阻断日志 91
9.3 资产变更日志 91
9.4 攻击日志管理 92
9.5 防病毒日志 92
第 10 节 系统配置 93
10.1 基础设置 93
10.2 用户部门 94
10.3 网络配置 97
10.4 性能监控 98
10.5 通知设置 98
10.6 管理工具 99
10.7 自定义页面 100
10.8 设备信息 100
第六章 运维管理 101
第 1 节 查看整体状态 102
第 2 节 查看隐患数据 102
第 3 节 巡检一览 103
第 4 节 视频巡检 104
4.1 视频巡检 104
4.2 巡检结果 105
第 5 节 巡检计划 106
5.1 创建巡检计划 107
第 6 节 人工分析 109
第 7 节 巡检统计 112
第 8 节 告警配置 113
8.1 日间预警规则 113
8.2 夜间预警规则 114
第 9 节 巡检配置 115
9.1 国标编码配置 116
9.2 巡检配置 116
第七章 安全审计 121

第 1 节 选择查询条件 122
第 2 节 日志的查看 122
第八章 用户管理 122
第 1 节 添加用户 122
第 2 节 用户权限设置 123

第 一 部 分

第一章 设备安装

第 1 节 安全注意事项

为了避免对人和设备造成伤害, 请在安装视频安全调阅系统前仔细阅读本节的安全建议。实际情况中包含但不限于以下所有安全建议。

1.1 通用安全

1. 使用安全保护设备（如防静电手腕等），以确保您和系统的安全。
2. 确保您站在合适位置, 并且地板是干燥和平整的, 确保您和地面有很好的摩擦。
3. 保持机箱清洁。
4. 不要将机箱和安装工具放在行走区域内。
5. 不要执行任何可能伤害到您或者设备的操作。
6. 在对设备进行任何操作前，请先确保您已经充分理解将要做的事情，并且在开始之前得到必要的许可。



注意：搬运视频安全调阅系统硬件时，用力要均匀、缓慢，防止坠落或碰撞，否则可能引起设备损坏，甚至伤害到您。

1.2 用电安全

1. 请仔细检查您的工作区域内是否存在潜在的危险，比如电源未接地、电源接地不可靠，地面潮湿等。
2. 安装前，请明确设备所在房间的紧急电源开关位置，当发生意外时，要先切断电源开关。
3. 在移动设备前一定要拔掉所有电源线和外部电缆。
4. 不要进行带电操作。
5. 请不要将设备放置在潮湿的地方，也不要让液体流进设备。

1.3 静电安全

为了避免静电对存储设备的电子器件造成损坏, 除了对安装设备的场所要采取防静电措施外，还要注意在安装设备的各种部件时必须佩戴防静电手腕。防静电手腕的佩戴方法如下：

- 将手伸进防静电手腕。
- 拉紧锁扣，确认防静电手腕与皮肤有良好的接触。
- 将防静电手腕用鳄鱼夹夹在机箱接地线上。
- 确认防静电手腕已良好接地。

第 2 节 使用环境要求

视频安全调阅系统的硬件设备必须在室内使用，为保证设备的正常工作并延长其使用寿命，安装场所应该满足下列要求：

2.1 温度要求

为保证视频安全调阅系统硬件设备的正常工作和使用寿命，机房内需维持一定的温度。工作环境温度要求请参见下表：

项目	要求
工作环境温度	0℃～45℃
推荐环境温度	15℃～25℃
贮存环境温度	-40℃～+70℃

若温度过高，则将加速绝缘材料的老化，使视频安全调阅系统的可靠性大大降低，严重影响其使用寿命。



注意：当设备从低温环境进入高温环境时，若设备上出现冷凝水，请在设备上电前，务必采取一定的措施（如烘干、晾干等），以防设备内部器件发生短路被烧坏。

2.2 湿度要求

为保证视频安全调阅系统硬件设备的正常工作，机房内需维持一定的湿度。工作环境湿度要求请参见下表：

项目	要求
工作环境湿度	20%～80%（非凝露）

贮存环境湿度	10%～90%（非凝露）

若机房内长期湿度过高，易造成绝缘材料绝缘不良甚至漏电，有时也易发生材料机械性能变化、金属部件锈蚀等现象。

若相对湿度过低，绝缘垫片会干缩而引起紧固螺丝松动，同时在干燥的气候环境下，易产生静电，危害设备上的电路。

2.3 洁净度要求

灰尘对视频安全调阅系统的安全运行是一大危害。室内灰尘落在机体上，可以造成静电吸附，使金属接插件或金属接点接触不良。尤其是在室内相对湿度偏低的情况下，更易造成静电吸附，不但会影响设备寿命，而且容易造成设备故障。

对机房内灰尘含量及粒径要求请参见下表：

机械活性物质	**单位**	**含量**
灰尘粒子	粒每立方米	≤3×10^4（3天内桌面无可见灰尘）
注：灰尘粒子直径≥5μm		

除灰尘外，机房内空气中所含的盐、酸、硫化物也有严格的要求。这些有害气体会加速金属的腐蚀和某些部件的老化。机房内应防止有害气体如SO_2、H_2S、NO_2、NH_3、Cl_2等的侵入，其具体限制值如下表所示：

气体	**平均值（mg/m^3）**	**最大值（mg/m^3）**
二氧化硫SO_2	0.3	1.0
硫化氢H_2S	0.1	0.5
二氧化氮NO_2	0.04	0.15
氨NH_3	1.0	3.0
氯气Cl_2	0.1	0.3

2.4 抗干扰要求

视频安全调阅系统的使用中可能存在干扰源。无论是来自应用系统外部，还是

来自设备内部，干扰源都是以电容耦合、电感耦合、电磁波辐射、公共阻抗（包括接地系统）耦合、导线（包括电源线、信号线和输出线等）等多种传导方式对视频安全调阅系统产生影响。因此应注意：

- 对供电系统要采取有效的防电网干扰措施。
- 远离强功率无线电发射台、雷达发射台、高频大电流设备。

说明：必要时，用户可以采取电磁屏蔽的方法进行抗干扰。

2.5 接地要求

良好的接地系统是视频安全调阅系统稳定可靠运行的基础，是视频安全调阅系统防雷击、抗干扰、防静电的重要保障。用户必须为视频安全调阅系统提供良好的接地系统。

2.6 供电要求

供电要求如下表所示：

项目	描述
输入电源	115V～230V AC,50HZ～60HZ

第二章 系统登录和退出

第 1 节 启动平台

浏览器输入地址 https://服务器 IP:10443，弹出系统登录对话框，如下图所示：

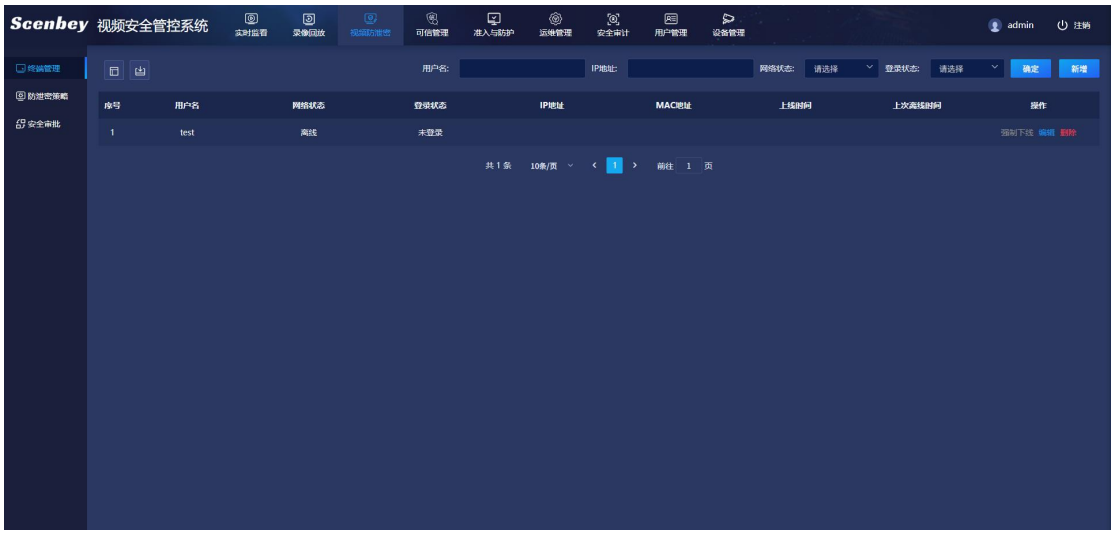


输入账号和密码，点击的登陆菜单即可登

注意：系统默认的管理员账号是 admin,默认的密码是 Dccs12345.。

第 2 节 退出平台

登陆系统后在右上方可以看到登陆的账号和注销按钮，点击注销就平台就会退出到登陆界面。



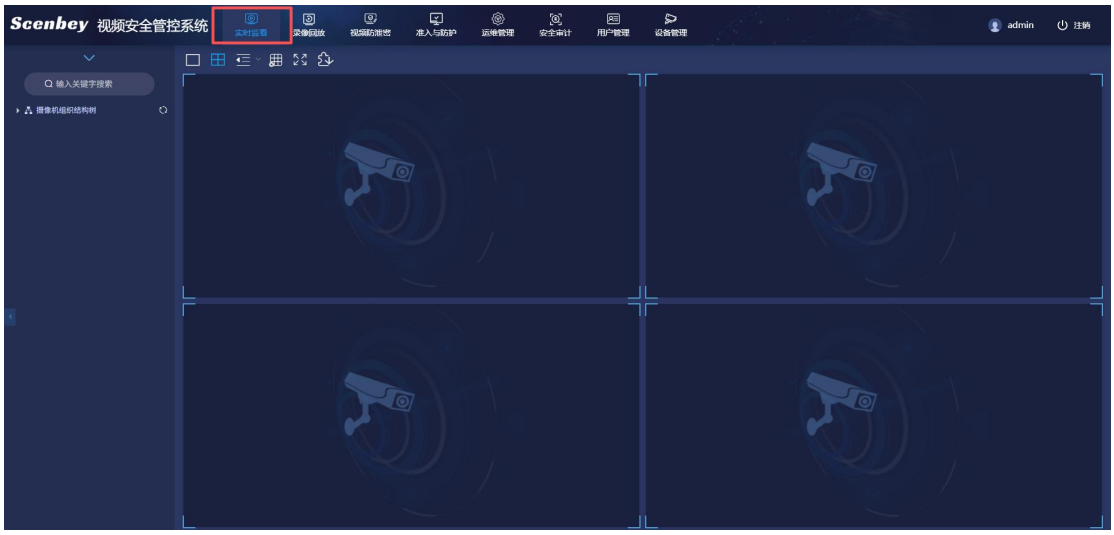
第 二 部 分

视频安全管控系统

第一章 实时查看

在实时视频窗口上可以按多种画面布局实时监看前端送来的视频数据、报警数据，用户能控制图像显示，控制前端设备云台等。

鼠标左键单击快捷工具栏实时查看菜单，进入实时监看主界面，如下图所示：

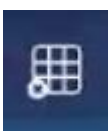


第 1 节 控制监看区窗口的布局

1. 直接点击工具栏区的布局按钮改变监看区的窗口布局。


。如：3/5/7 分屏的走廊模式以及 2 分屏的宽屏模式。

2. 通过工具栏区的全屏按钮  将整个监看区全屏显示。

3. 通过工具栏区的全屏按钮  将整个监看区清屏处理。

4. 可点击“ESC”键或将鼠标移动到窗口上沿，在出现的工具栏上再次点击全屏按钮

退出全屏状态。

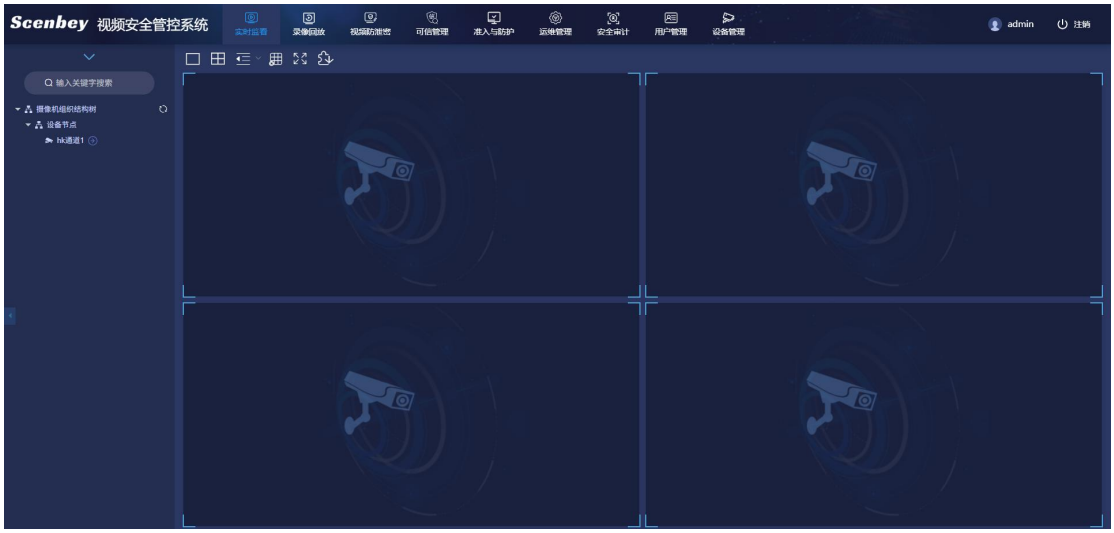
第 2 节 选择需要监看的摄像头

1. 可从资源树中双击摄像即可将该摄像头显示监看窗口中，也可以先选择查看窗口，再双击摄像头就可以控制哪个窗口显示哪路摄像头画面。
2. 也可先选中监看窗口，再双击资源树上摄像头节点实现该摄像头实时视频预览。
3. 点击

，可展开/收拢云台控制区域，且记住用户的选择，在下一次启动时，默认显示。

第 3 节 云台控制操作

对于硬件支持的设备一般情况下可以直接控制，选中摄像头，单机下箭头调出控制菜单。





按箭头所指示方向有：

向上：使云台向上转动；

向下：使云台向下转动；

向左：使云台向左转动；

向右：使云台向右转动；

向左上：使云台向左上转动；

向右上：使云台向右上转动；

向左下：使云台向左下转动；

向右下：使云台向右下转动；

	焦距放大		焦距缩小
	复位		调节转速

第 4 节 管理图片

在实时监控点击相机图标，可将当前图像抓帧，自动下载到浏览器的下载目录里



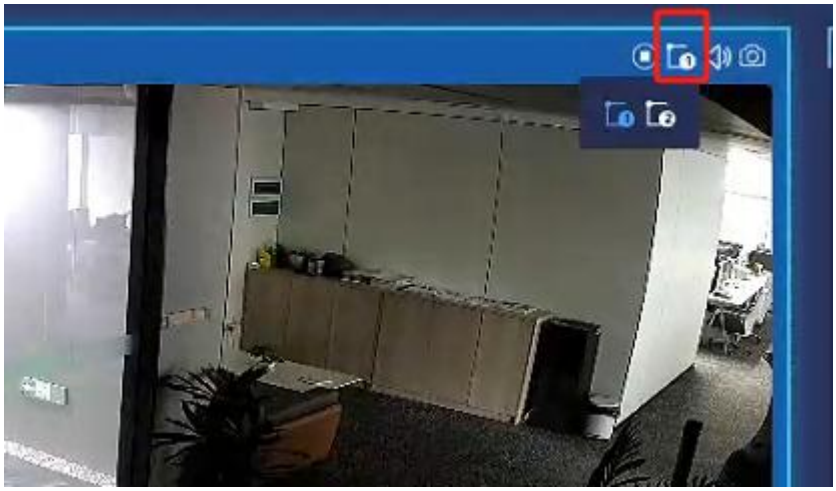
第 5 节 声音控制

点击实时播放的喇叭菜单，可以对监控画面进行声音的大小切换。



第 6 节 码流设置

点击实时监控右上角的码流菜单，可以进行对监控画面进行主码流和子码流进行切换。



第 7 节 清除视频窗口显示的视频

点击实时监控界面的停止菜单，可以清除当前画面的监控视频。



第二章 录像回放

点击实时查看菜单可以切换到实时查看模块。



第 1 节 检索录像

- 在组织结构中勾选要检索的摄像头节点。选择要检索的录像的类型、标签关键字、录像时间等，然后点击查询结果可得到要查询的结果。

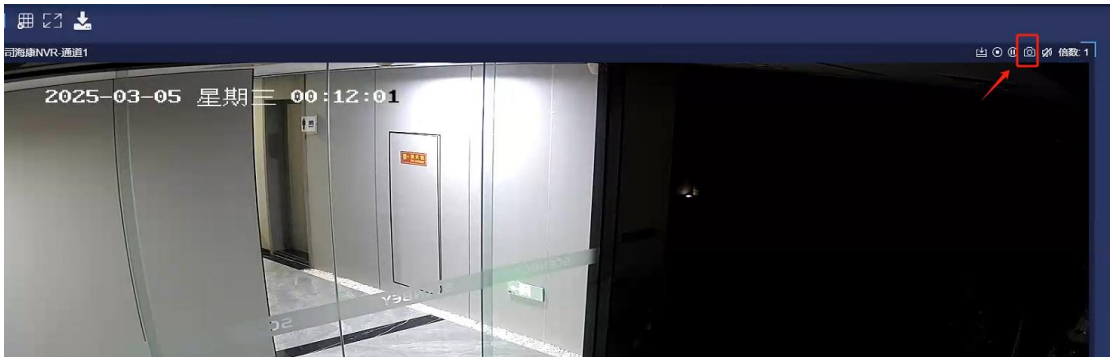




点击操作栏的播放按钮菜单即可在播放窗口播放检索的视频录像。

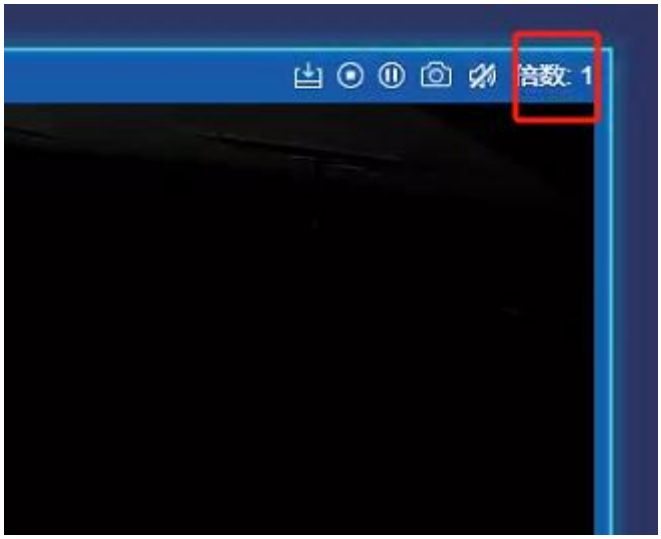
第 2 节 录像抓帧

播放视频录像界面的右上角点击截屏按钮可以进行抓帧。

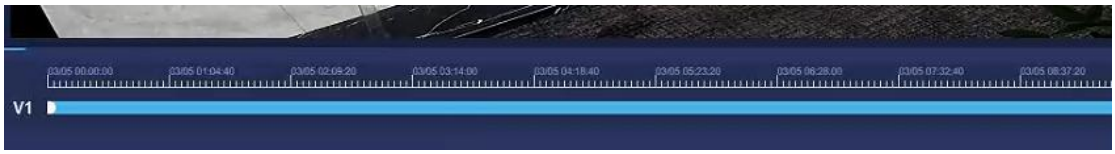


第 3 节 播放控制

1. 在播放视频画面的又上脚可以进行视频倍速播放切换，支持 2 倍、4 倍、8 倍切换



2. 通过播放轨道进行播放控制。



第 4 节 录像下载

1. 视频播放界面右上角菜单进行下载。



2. 界面上方主菜单进行下载。



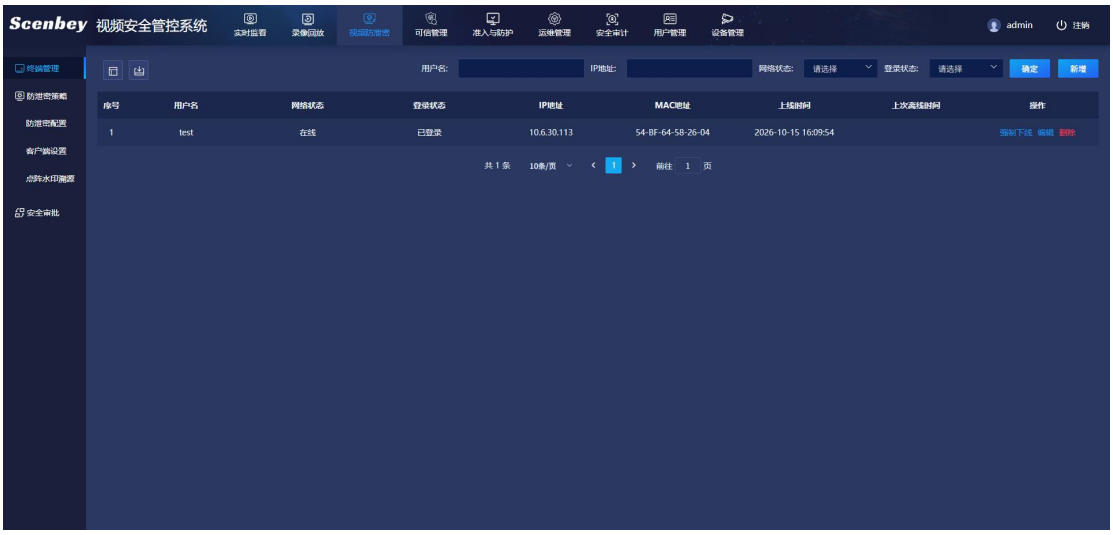
第三章 视频防泄密

鼠标左键单击快捷工具栏视频防泄密菜单，进入实时监看主界面，如下图所示：



第 1 节 终端管理

鼠标点击左侧终端管理菜单，可进入界面查看终端信息。



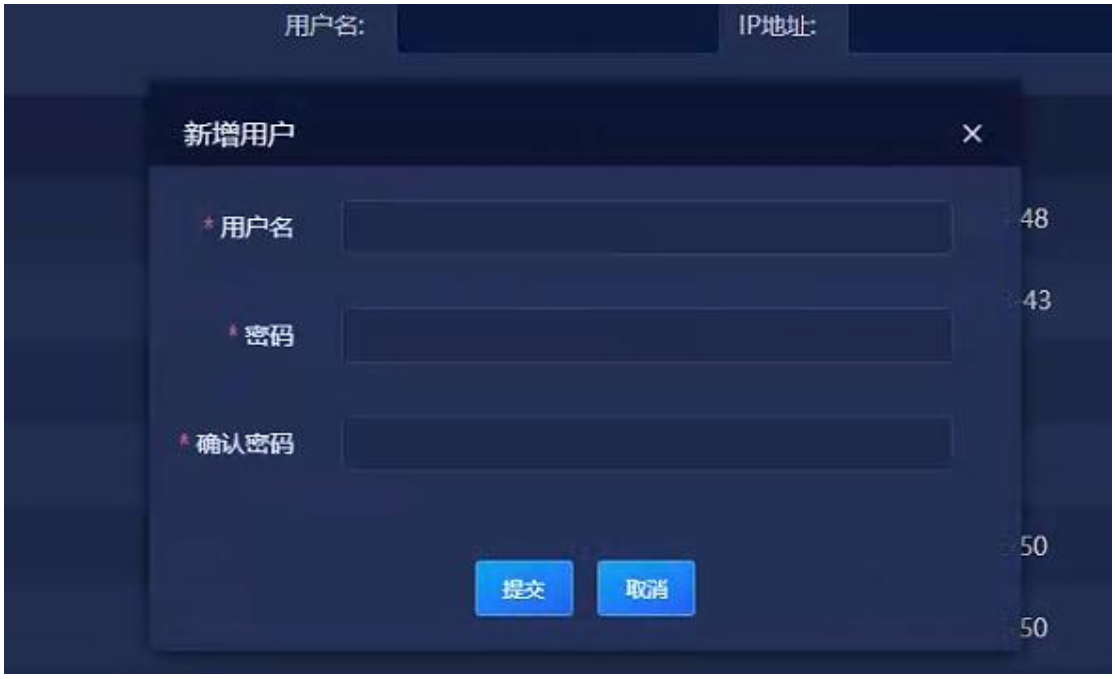
上方可以输入条件点击确认菜单进行筛选操作。



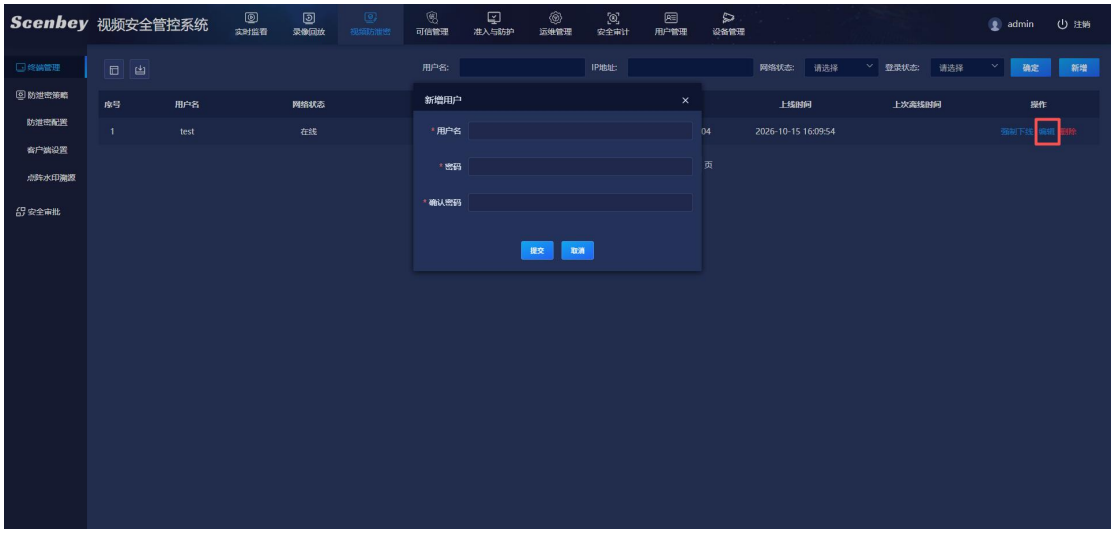
右上角点击新增菜单可以完成对终端的新增操作。



需要输入用户名，密码已经密码二次确认操作后点击提交菜单。



选择用户后可以点击编辑菜单完成对用户的修改操作，包括用户名和密码。



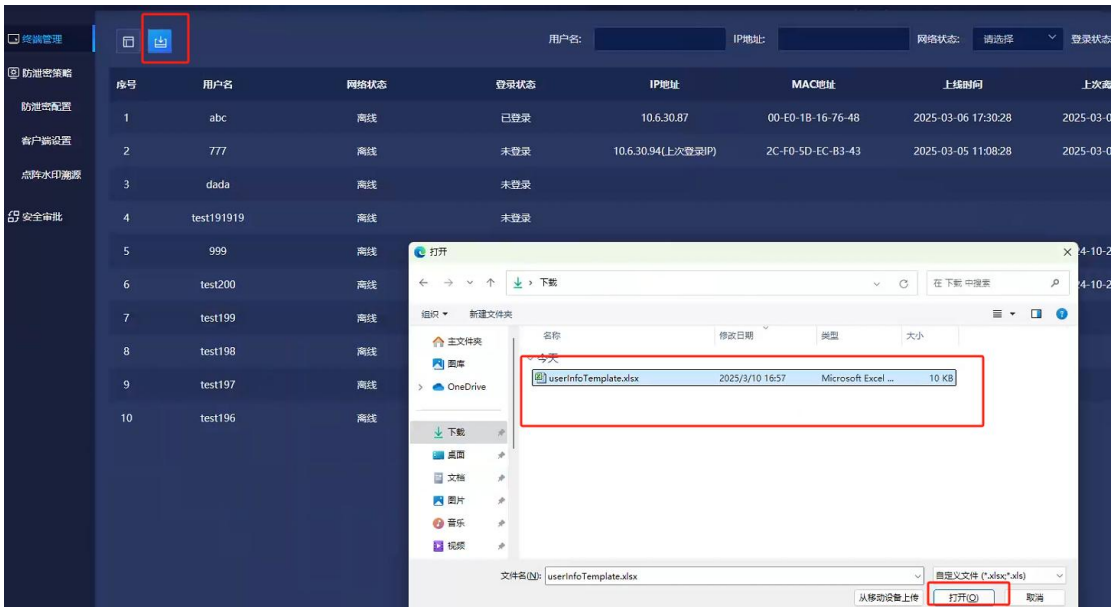
选择用户后可以点击删除菜单完成对用户的删除操作，删除后将无法进行恢复。



用户也可以进行导入操作。点击左上角模板菜单下周模板



输入用户名和密码列。点击导入菜单，选择修改的模板完成对用户的导入操作。



第 2 节 防泄密策略

2.1 防泄密配置

这三个菜单分别是新增，删除，修改菜单。可以完成对策略的新增删除修改操作。

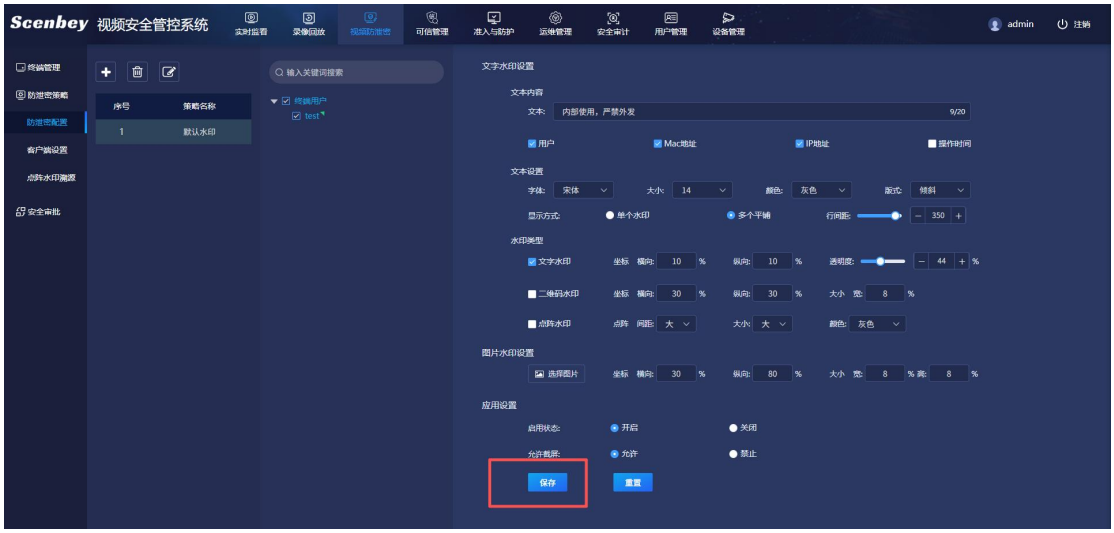


有了策略之后，选择使用该策略的账户，账户可以多选。



选择策略和账户后。可以配置水印的内容，多种方式可以组合配置处理

保存可以使配置的策略生效，也可以点击重置操作完成策略重置。



2.2 客户端配置

点击左侧客户端配置，可以实现对客户端卸载密码，退出密码，修改配置密码等信息的重置。



点击防泄密客户端下载按钮可以完成客户端的下载，适用 windows 系统安装。



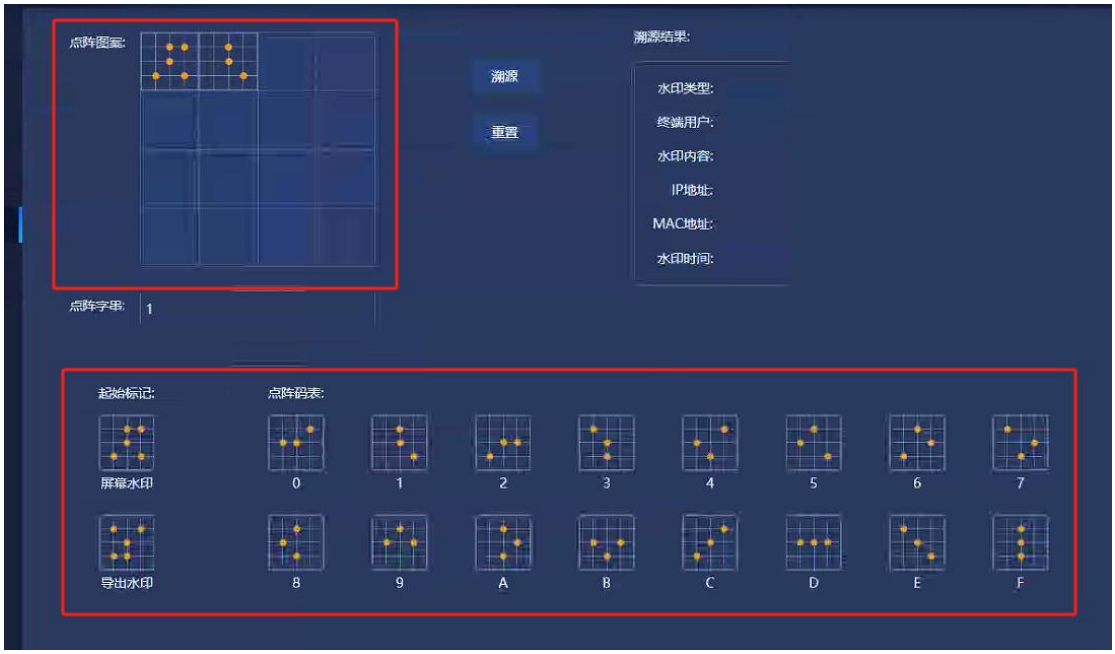
点击防泄密客户端下载按钮可以完成播放器下载，实现隐性水印擦看，适用 windows 系统安装。

2.3 点阵水印溯源

点击左侧水印溯源菜单，可以对水印进行溯源操作。

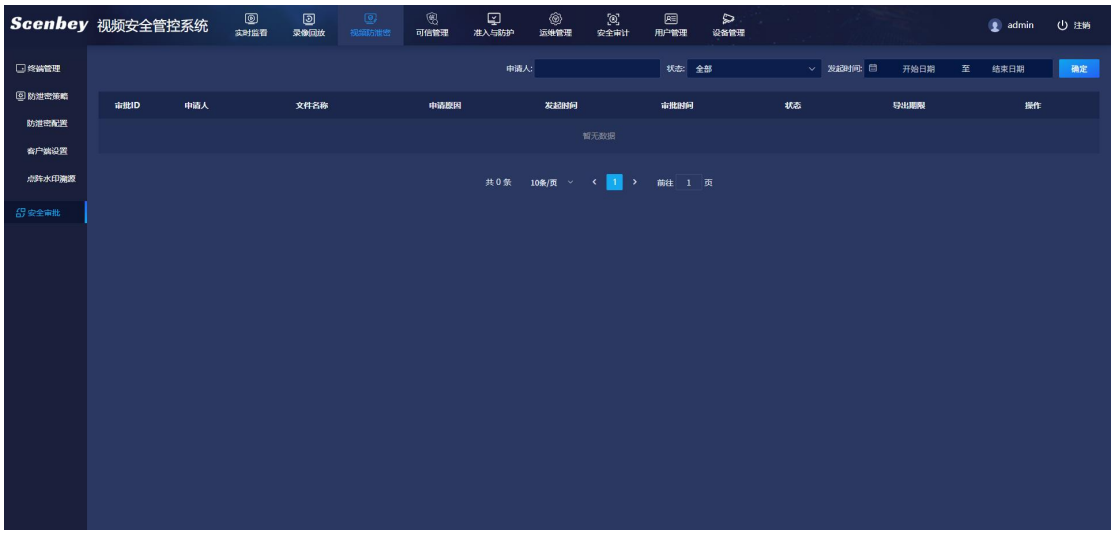


首先选择点图案，图案需要跟视频截图看到的一致，左上方是点阵标记配置区域，下方可以用鼠标选择组成一个整体的图标，点击溯源菜单进行查询，或者点击重置菜单进行重新组合操作。



第 3 节 安全审批

鼠标左键单击安全审批菜单，可以查看审批信息。



通过上方筛选区域可以进行筛选查询。



选择一条审批信息点详情可以查看详细内容。

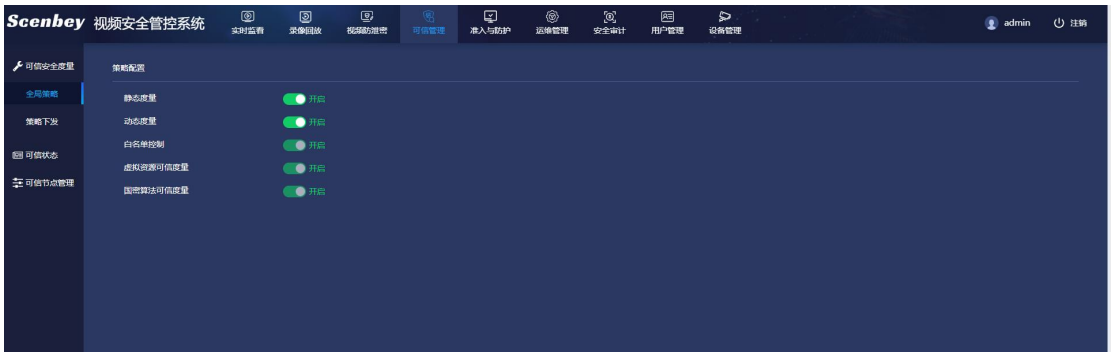


选择一条审批信息点预览首帧可以查看首帧页面。



第四章 可信管理

鼠标左键单击快捷工具可信管理菜单，进入可信管理主界面，如下图所示：



第 1 节 可信安全度量

进入可信管理界面后，点击左侧可信安全度量，如下图所示：



1.1 全局策略

进行策略的配置。点击开启菜单可以实现该策略的开启或关闭。

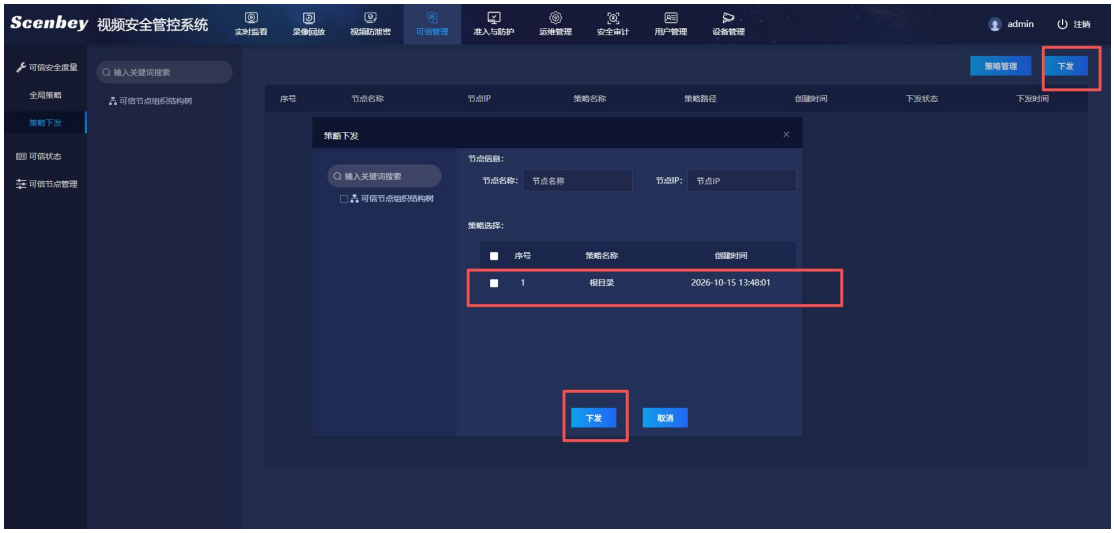


1.2 策略下发

点击策略管理可以完成对策略的创建，需要输入策略名称和路径，然后进行保存。



点击策略下发可以完成对策略的下发操作，需要勾选创建的策略，点下发菜单完成处理。



第 2 节 可信状态查询

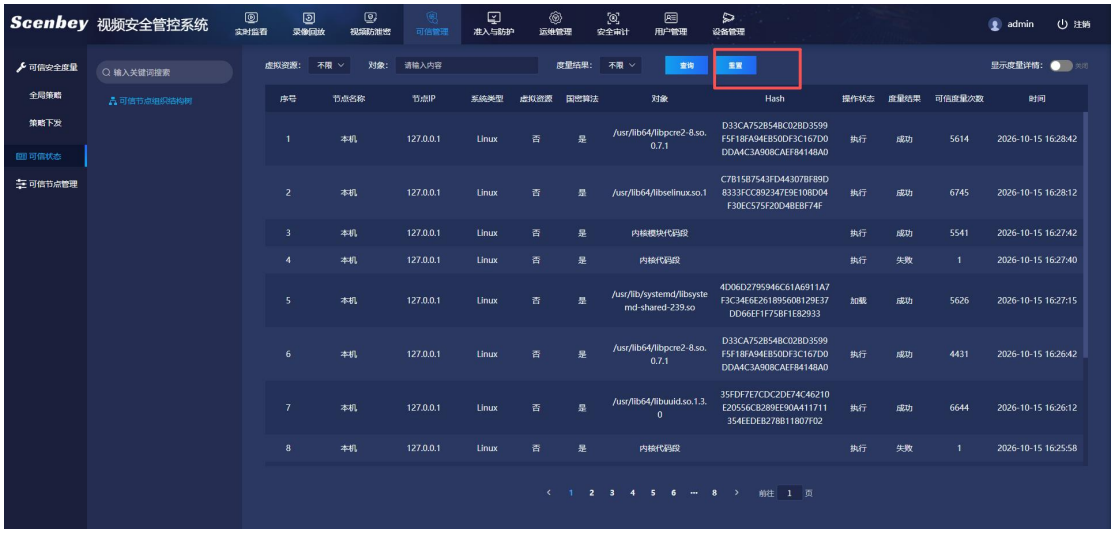
进入可信管理界面后，点击左侧可信状态，如下图所示：



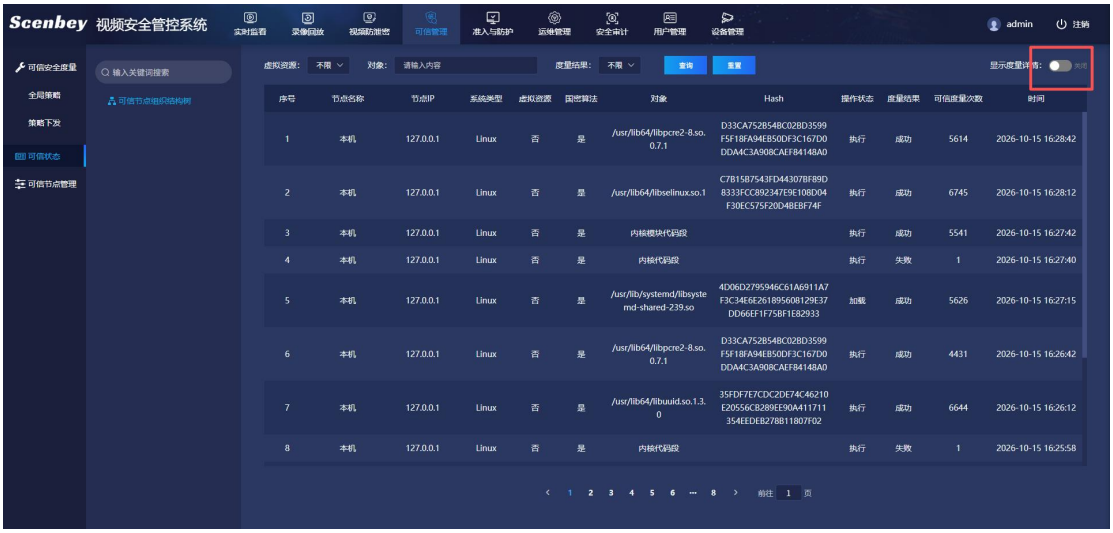
选择组织结构和上方可以输入查询条件进行检索。



查询结果后，点击重置菜单可以对结果进行重置处理。



通过右上角度量详情菜单可以控制详情是否显示。



第 3 节 可信节点管理

3.1 可以节点设置

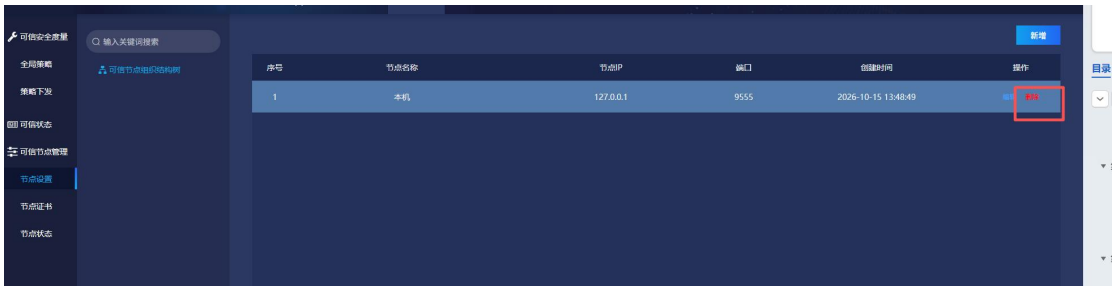
点击新增节点可以完成对新增节点的设置。



输入节点名称，IP，端口号进行保存。



也可以对之前设置的节点进行修改和删除操作。



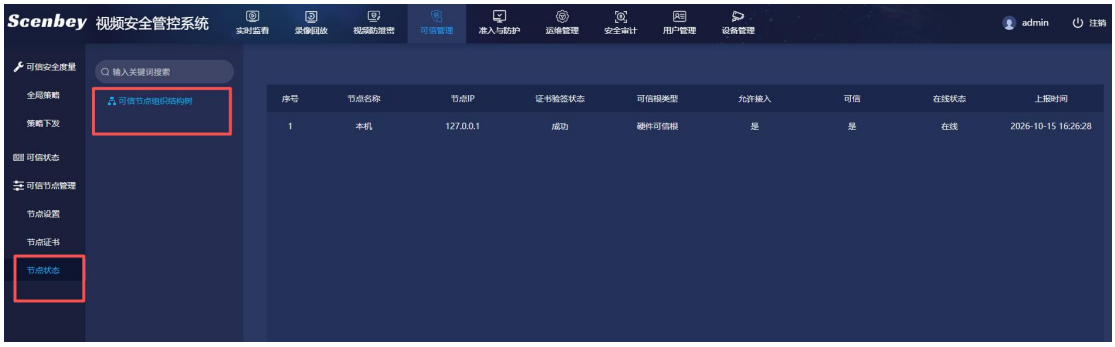
3.2 节点证书

选择节点名称后，点击右上角的签发证书菜单即可完成证书签发。



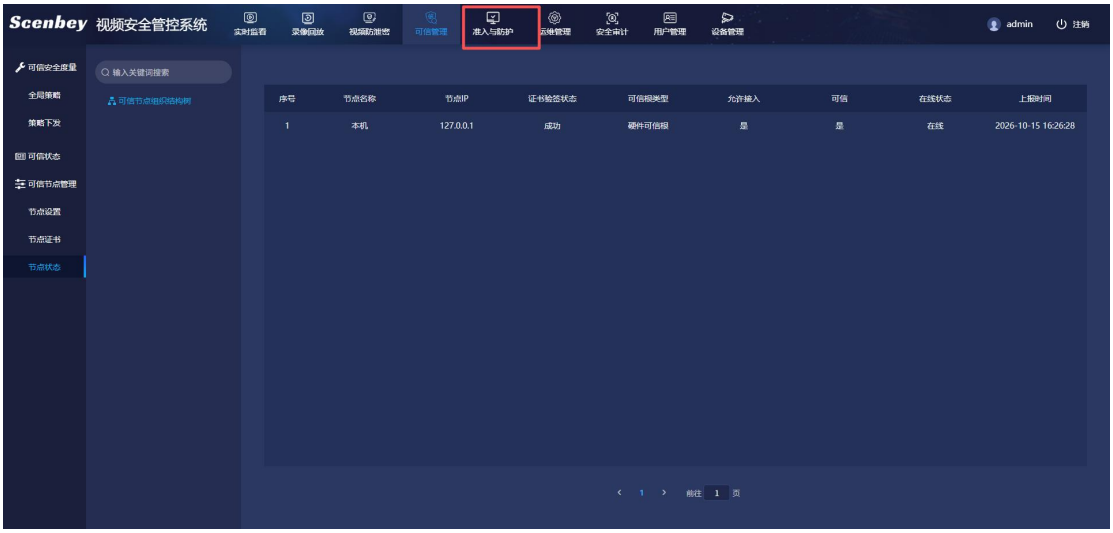
3.3 节点状态

点击节点状态菜单并选择节点名称后即可查看节点的状态。



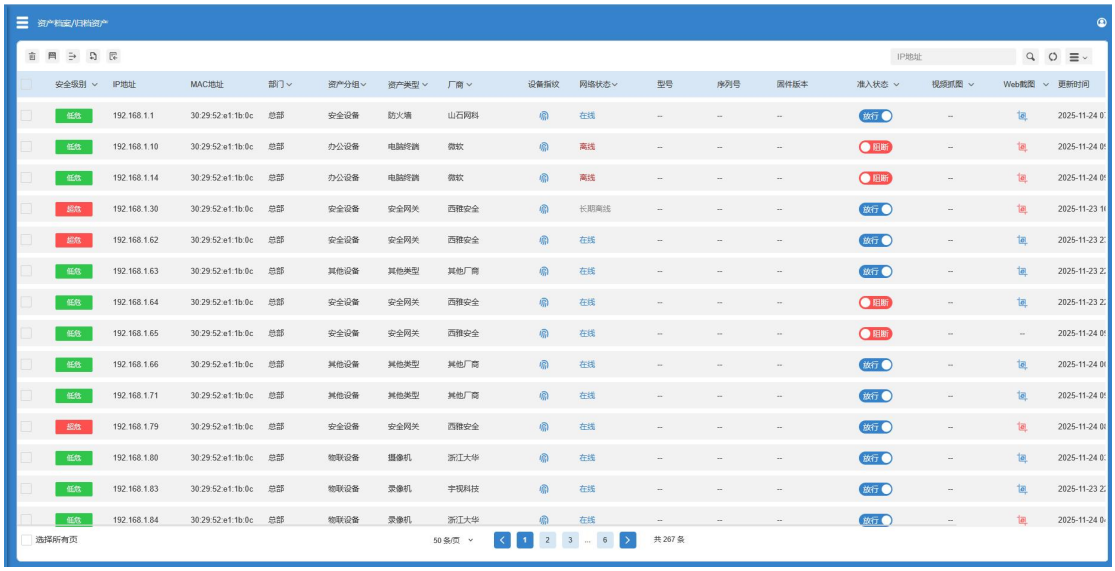
第五章 准入与防护

点击上方安全与准入菜单，输入用户名密码可以登陆安全准入系统。



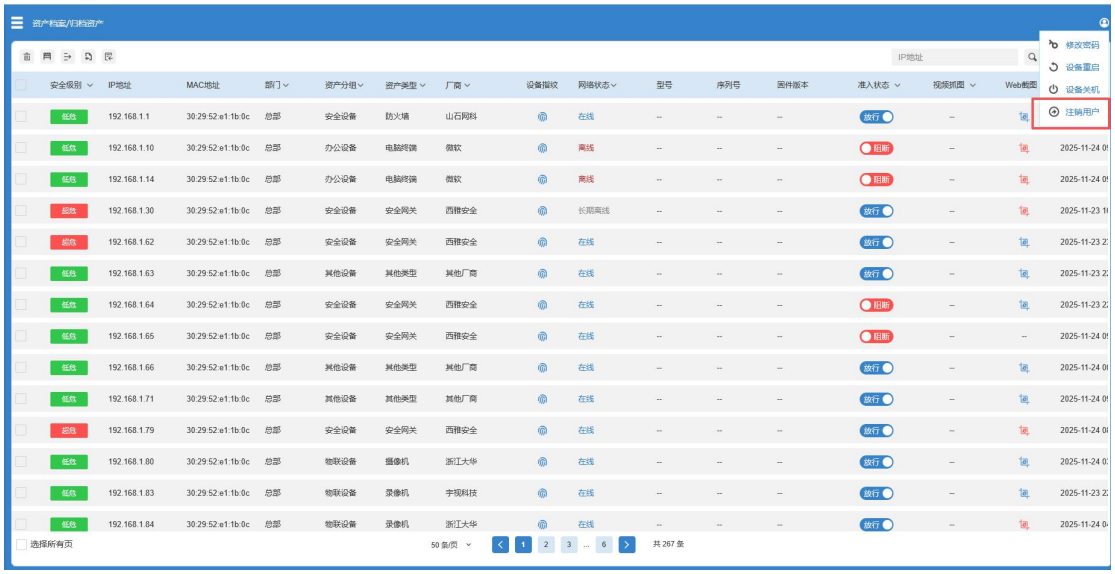
第 1 节 主页界面介绍

当登录视频安全准入系统后，进入资产档案 – 归档资产界面，展示系统中的归档资产信息，如下图所示：



第 2 节 系统退出

使用说明：点击平台右上角【管理员】菜单中的【注销】，即可退出视频安全准入系统，如图 2.3-1 所示，退回到登录页面。

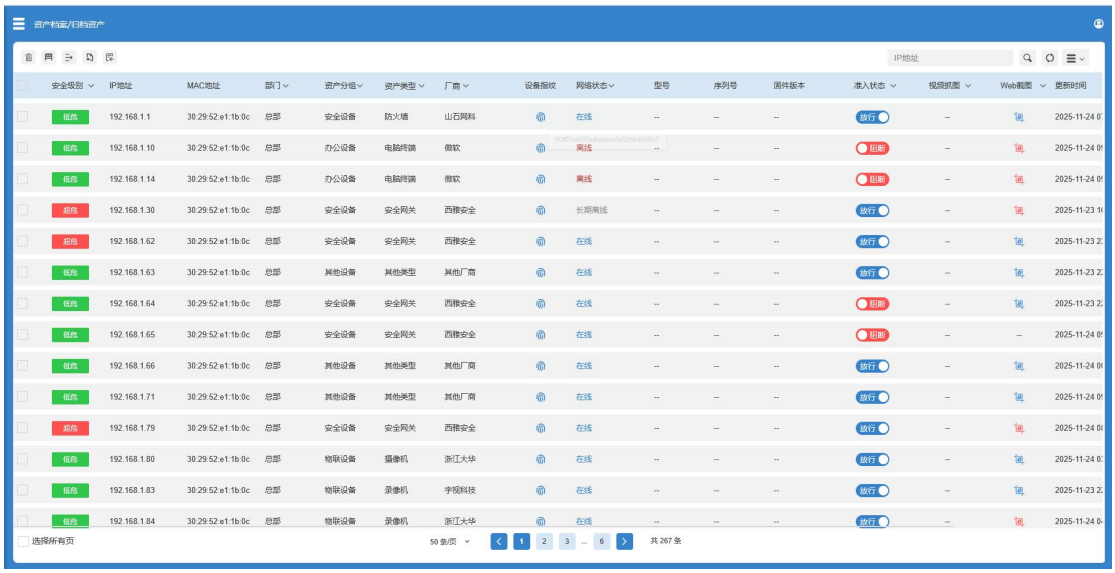


第 3 节 资产档案

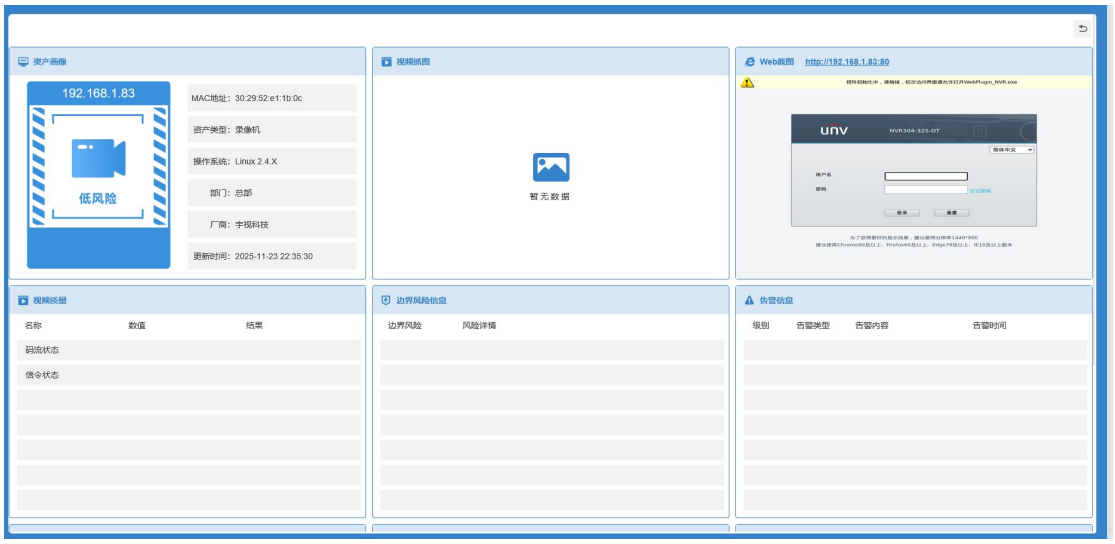
此功能模块主要对资产进行资产信息展示、资产发现、档案配置、资产识别、Dfind 引擎以及视图配置等操作。

3.1 归档资产

点击菜单【资产档案】-【归档资产】，此页面展示资产档案中所有已归档的资产信息，以列表形式展示。如图所示：



1. 资产信息展示：归档资产展示已归档的所有资产，包括：安全等级、IP 地址、名称、MAC 地址各项资产信息全部显示正确，且资产信息以及安全级别等数据符合入档规则配置中的入档规则。
2. 列表信息可根据安全级别、部门、资产类型、厂商、状态、准入状态、数据来源、是否安装客户端进行数据筛选
3. 数据来源：数据来源显示主平台以及所有上报至主平台的子平台名称。
4. 资产画像：点击 IP 地址或点击操作列第一个“资产画像”按钮，进入资产画像页面，如图所示：

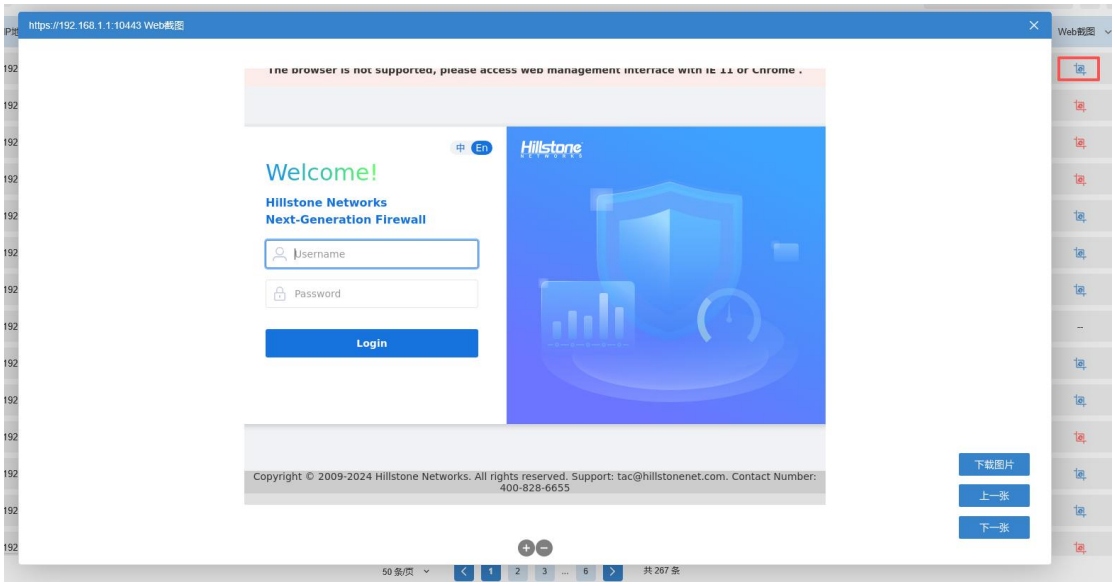


(1) 资产画像页面展示资产的基本信息，包括 mac 地址、资产类型、部门、更新时间等

(2) 展示视频抓图、web 截图（点击截图右侧链接可进入对应环境），视频质量、边界风险信息、告警信息、弱口令信息、端口详情以及漏洞信息。

5. 编辑资产：点击编辑按钮，可编辑本级平台已归档资产，下级平台资产无法进行编辑。

6. 删除资产：点击操作栏删除按钮或选中资产点击上方删除按钮，可成功删除已归档资产。
7. **阻断放行：点击准入状态列开关或选中资产点击上方准入/阻断按钮，可成功对资产进行阻断或放行（包括子平台上报的资产）。**
8. **准入状态：默认新进入资产列表的资产为放行状态，可手动修改，准入状态为阻断时，会对资产进行阻断操作，会导致被阻断的资产无法上网。**
9. 退档：点击操作栏退档按钮或选中资产点击上方退档按钮，可成功将已归档资产退档至待录资产列表中。
10. 批量导出：选择当前页面需要导出的资产或直接点击导出按钮，可成功导出选择的资产，导出文件存放在本地，且导出数据全部正确。
11. 视频抓图：视频抓图列数据是资产根据视图配置页面配置的对接方式、取流地址以及用户名和密码进行抓图，抓图成功，显示蓝色图标，点击图标可查看成功抓取到的截图
12. Web 截图：Dfind 引擎页面开启 web 截图，截图成功则显示蓝色图标，点击蓝色图标显示成功抓取的截图，图片可供下载，如下图所示：
    - 其中点击窗口左上方的链接，可成功跳转至对应页面
    - 存在多张图片时，点击切换按钮，可左右切换
    - 点击下方下载按钮，可将抓取到的图片下载至本地

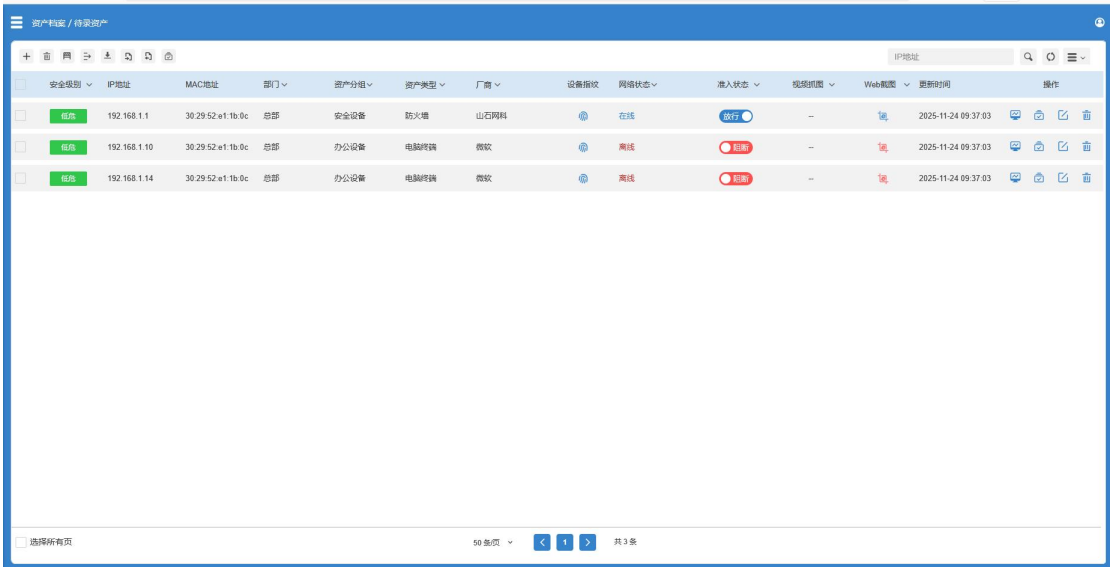


13. 录像完整性、录像点播、录像存储：须在视图配置页面，配置正确的录像机用户名和密码，在视图质量检测配置页面，开启录像质量检测开关，可成功根据检测到数据，获取对应结果。

3.2 待录资产

点击菜单【资产档案】-【待录资产】，此页面展示所有待录资产信息以列表形式展示，

如图所示：



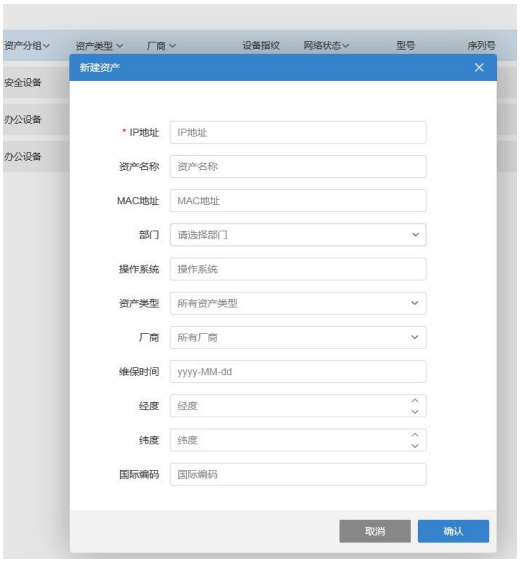
最右侧操作列，用户可对资产进行查看资产画像、归档、编辑、删除操作。

上方按钮区域，用户可进行新增、批量删除、下载模板、批量导入，批量导出、批量归档以及根据资产 IP 地址进行搜索操作以及右上角下拉筛选可设置列表显示内容。

资产列表各列信息数据显示：

- 安全级别：根据告警配置显示资产的安全级别；
- 设备指纹：显示当前资产的设备指纹数据；
- 网络状态：显示当前资产的网络状态（在线/离线/长期离线）；
- 准入状态：显示当前资产的准入状态，配合边界接入中的配置，可对资产进行准入和阻断操作；
- 视频抓图/码流状态/信令状态：显示摄像机类型资产的视频抓图、码流状态以及信令状态，需要先在视图配置页面获取到正确的用户名、密码，才会检测到数据获取结果；
  - Web 截图：Dfind 引擎页面开启 web 截图，截图成功则显示蓝色图标，点击蓝色图标显示成功抓取的截图，图片可供下载。

用户点击页面左上角的“+”号可进行添加资产操作，即可弹出如图 2.4-3 所示页面，其中 IP 地址为必填项，资产名称、MAC 地址、部门、操作系统、资产类型、厂商、维保时间、经度、纬度、国标编码为选填项。



用户输入各项必填信息，点击提交，资产创建成功。

资产归档：选择需要归档的资产，或直接点击操作栏归档按钮，可对资产进行归档，符合入档规则的资产，可直接进入归档资产页面

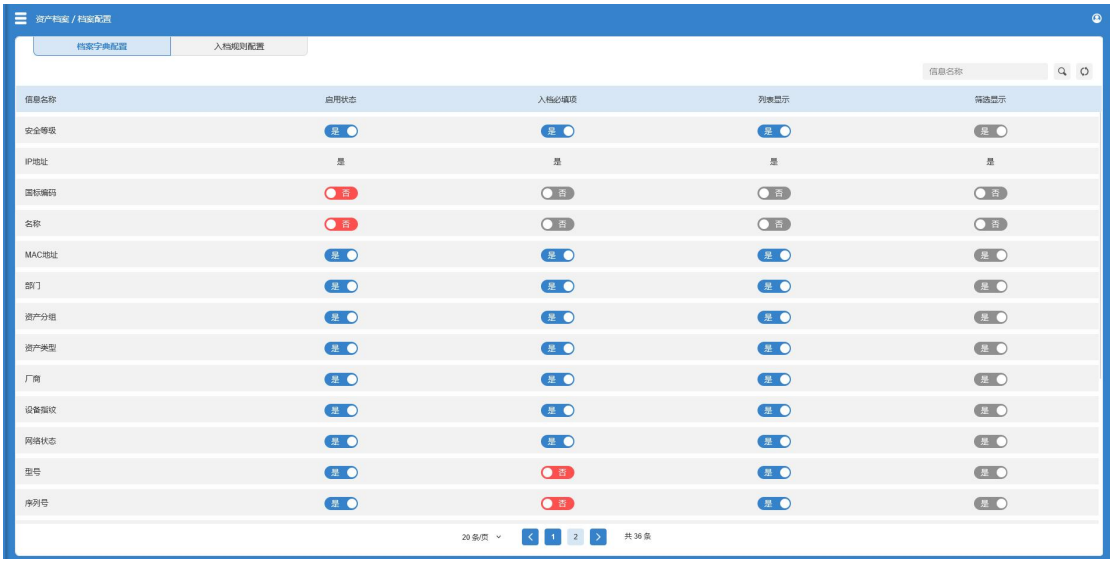
编辑资产：点击编辑按钮，可对已发现的资产进行编辑，注：无法编辑子平台上报的资产信息。

3.3 档案配置

此模块可对入档必填项、待录/归档资产列表显示进行配置，以及针对资产可入档的入档规则进行配置。

3.3.1 档案资产配置

点击菜单【资产档案】-【档案配置】-【档案字典配置】，此页面可对待录/归档资产页面，列表显示、右侧筛选显示，以及入档必填项进行控制。如图所示：



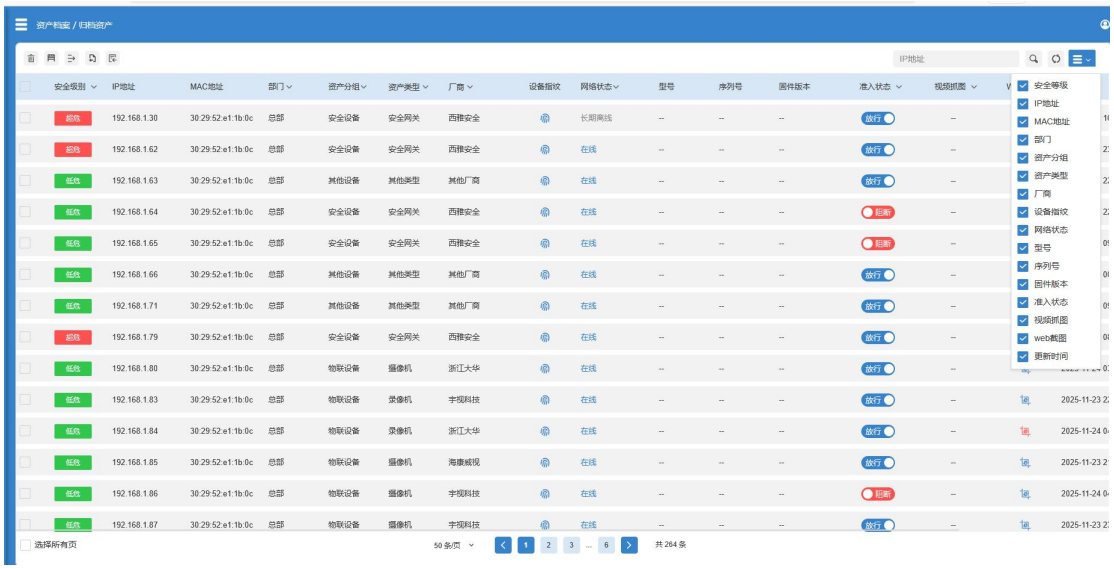
此页面展示待录资产和归档资产列表可显示的资产信息名称（表头名称）。

启用状态：开启此信息的启用状态，可对入档必填项和列表显示列进行开启和关闭操作。

入档必填项：入档必填项选择“是”时，且入档规则“开启入档必填项校验”，资产进行归档时，对开启是的资产信息进行必填项校验。

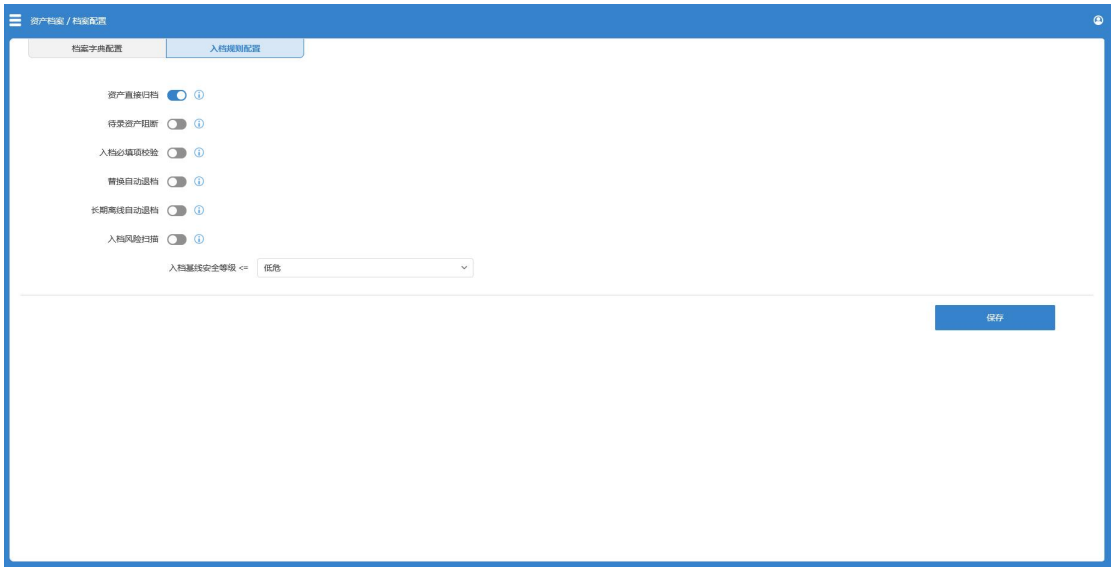
列表显示：列表显示列选择“是”，待录资产/归档资产列表的表头显示所有勾选是的资产信息，列表显示为“否”时，此资产信息不显示在列表中且筛选显示列变为可修改状态。

筛选显示：列表显示为“否”时，筛选显示列可进行修改状态，修改状态为“是”时，待录资产/归档资产列表右侧列表显示中出现此资产信息名称，为“否”时，此资产信息名称不显示在筛选下拉中。如图所示：



3.3.2 入档规则配置

点击菜单【资产档案】-【档案配置】-【入档规则配置】，此页面可对资产入档的规则进行设置，如图所示：



资产直接归档: 开启资产直接归档后, 扫描到资产信息后资产直接进入归档资产列表中, 目录中已存在的资产信息，系统自动归档至归档资产列表中。

待录资产阻断：**开启后，进入待录资产库的所有资产为阻断状态，无法进行放行。**

入档必填项校验：开启后手动入档会按照字典配置进行检测，内容缺失无法入档。

替换自动退档： 归档资产库发现设备有替换冒用告警自动退到待录资产库。

长期离线自动退档：归档资产库发现长期离线告警自动退档至待录资产库。

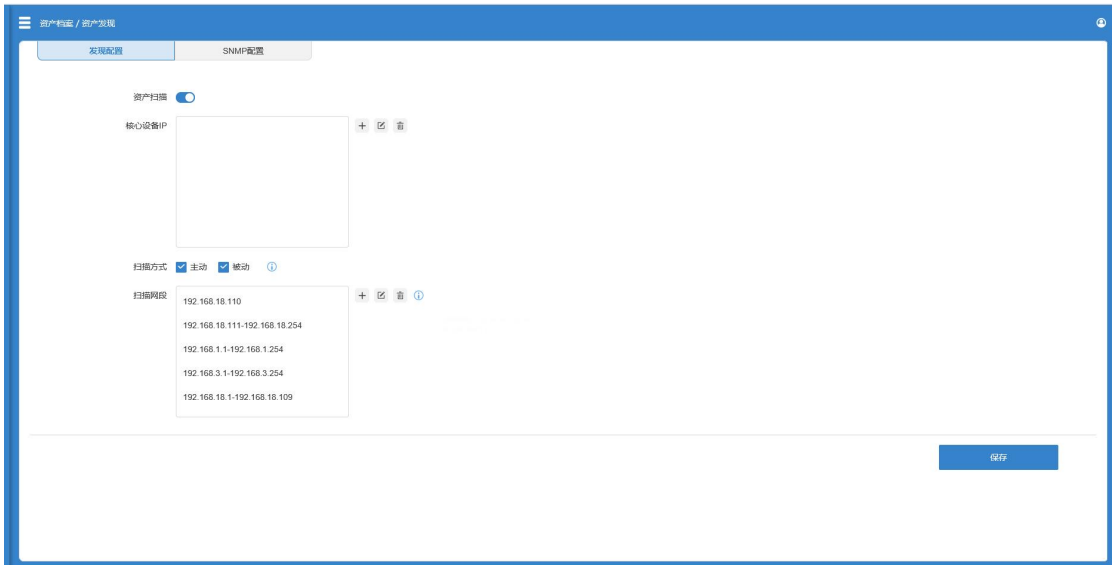
入档风险扫描： 发现新的资产自动加入已创建的扫描任务中，自动进行风险扫描，未扫描完成资产无法进行手动归档，大于入档基线安全等级的资产，不符合入档规则无法进行手动归档。

3.4 资产发现

点击菜单【资产态势】-【资产发现】，此页面可对资产进行发现扫描配置，其中包括发现配置、SNMP 配置两种方式。

3.4.1 发现配置

【资产态势】-【资产发现】-【发现配置】，此界面可以通过设置核心设备 IP、扫描的网段信息、扫描方式等对 IP 地址段内的资产进行扫描，扫描出的结果直接展示在资产列表中。如图 2.4-4 所示，其中核心设备 IP、扫描网段为必填项。



核心设备 IP 地址：为某网段的核心 IP 地址；

扫描网段：为核心设备 IP 地址对应的扫描网段；

扫描方式：分为主动/被动两种。

- **进行资产发现步骤：**

1、开启资产归档开关

2、选择扫描方式如：勾选主动和被动

3、扫描网段处点击【+】添加扫描网段

4、点击保存按钮

5、扫描网段发现成功，资产进入归档资产/待录资产列表中。

6、查看网段内所有资产是否发现完全，当没有发现完全时，可于待录资产列表中手动添加资产进行导入操作。

3.4.2 SNMP 配置

【资产态势】-【资产发现】-【SNMP 配置】，此界面可以通过设置 SNMP 的配置来对相应的资产进行发现，如图 2.4-5 所示。



通过点击左上角“+”进行 SNMP 的新建，弹出界面后选择发现方式、输入只读共同体名称、IP、端口等信息后并提交。



Snmpwalk 测试：点击此按钮可对输入的 IP 地址，进行 snmpwalk 测试，确保添加的 IP 可正常使用

当**存在同一网段下的资产的 mac 地址都一致**时，在此 snmp 配置页面增加对应交换机的 IP，发现方式，只读共同体名等数据，并在资产发现-核心 IP 处增加此 IP 进行，资产发现操作。

等待再次资产发现完，mac 地址发生变化。

3.5 资产识别

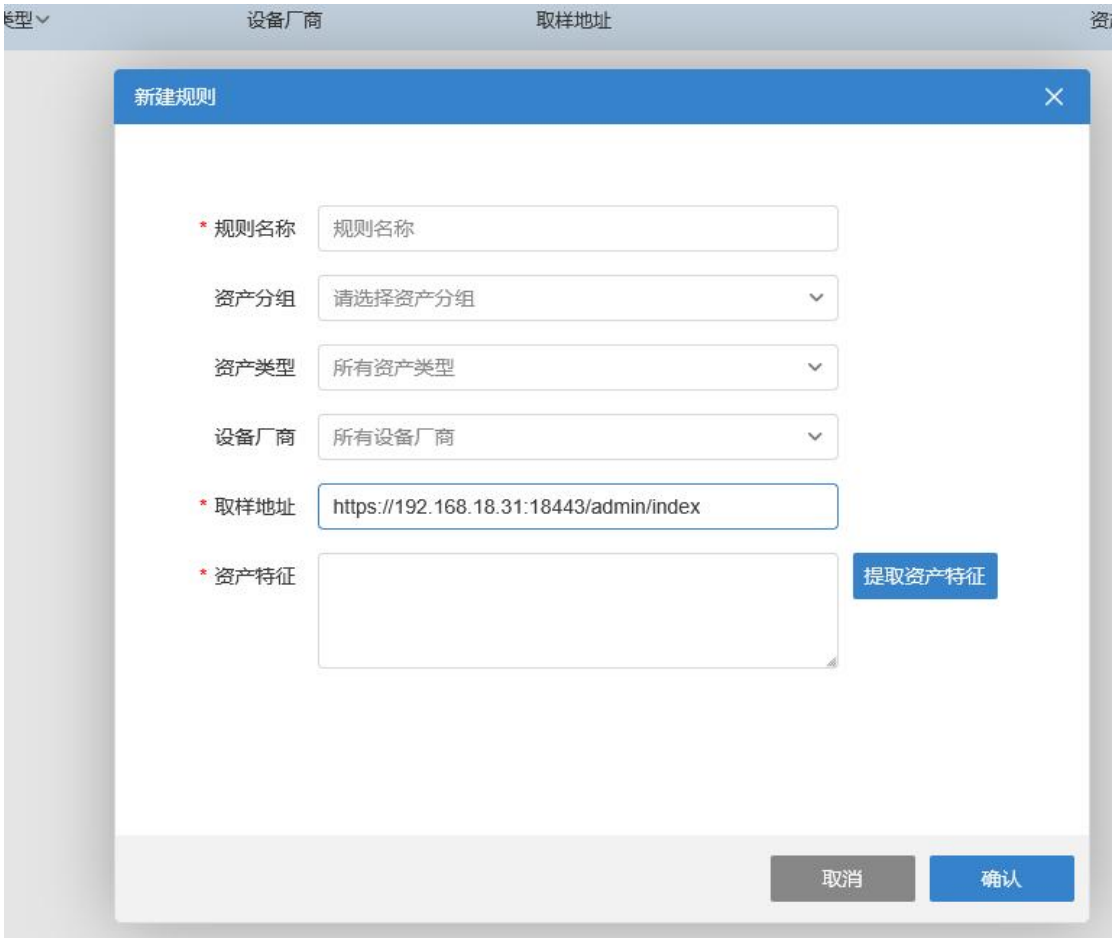
3.5.1 资产特征配置

点击菜单【资产识别】-【资产特征配置】，进入资产特征配置页面，此页面主要针对资产类型、厂商等未正确或未适配的资产进行资产特征配置，以保证在资产识别时可以正确识别。如下图所示：



进入资产特征配置页面，此页面正常显示用户配置的资产特征配置数据，包括规则名称、资产分组、资产类型、厂商、取样地址以及资产特征数据。

点击上方 按钮，进入新增资产配置页面，如下图所示：



输入规则名称，选择资产分组、资产类型、设备厂商、输入需要识别资产的取样地址，如：https://192.168.18.66:18443/admin/index，点击提取资产特征按钮，系统自动根据取样地址提取此地址页面的特征，并回显至资产特征处，点击确定按钮。

资产识别到此资产时，如果未根据系统中内置资产识别规则识别出资产类型以及厂商

时，会根据此配置进行资产识别。

点击页面上方的针筒图标按钮，弹出全量特征提取窗口，如下图所示：

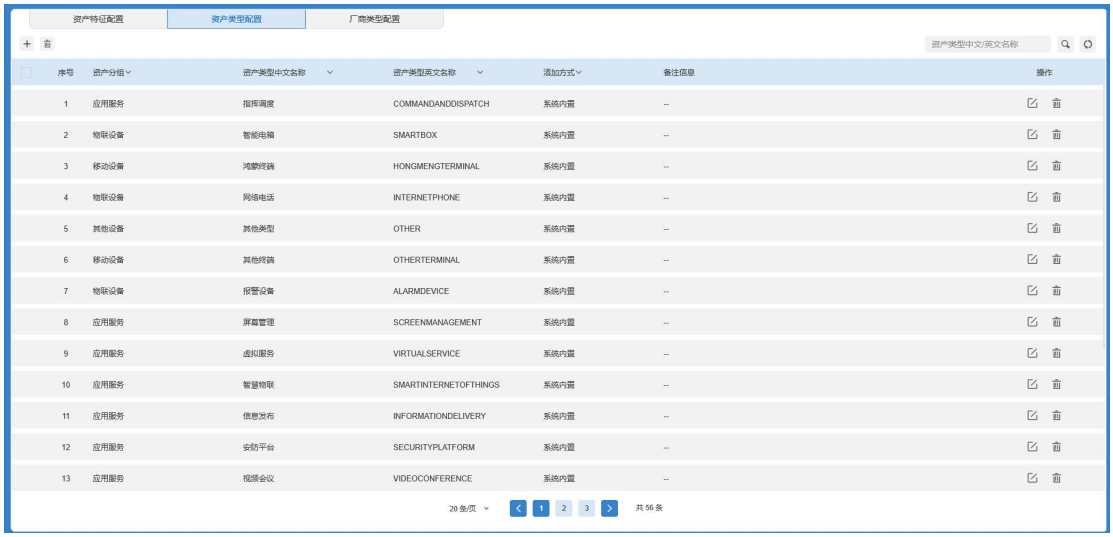


选择资产分组、资产类型，输入设备厂商以及取样地址，点击提取下载按钮。系统会根据取样地址，提取下载由设备厂商、资产类型以及取样地址中的 IP 名称的压缩包至本地，将压缩包提供给开发人员后，开发会根据提取到的数据进行适配。

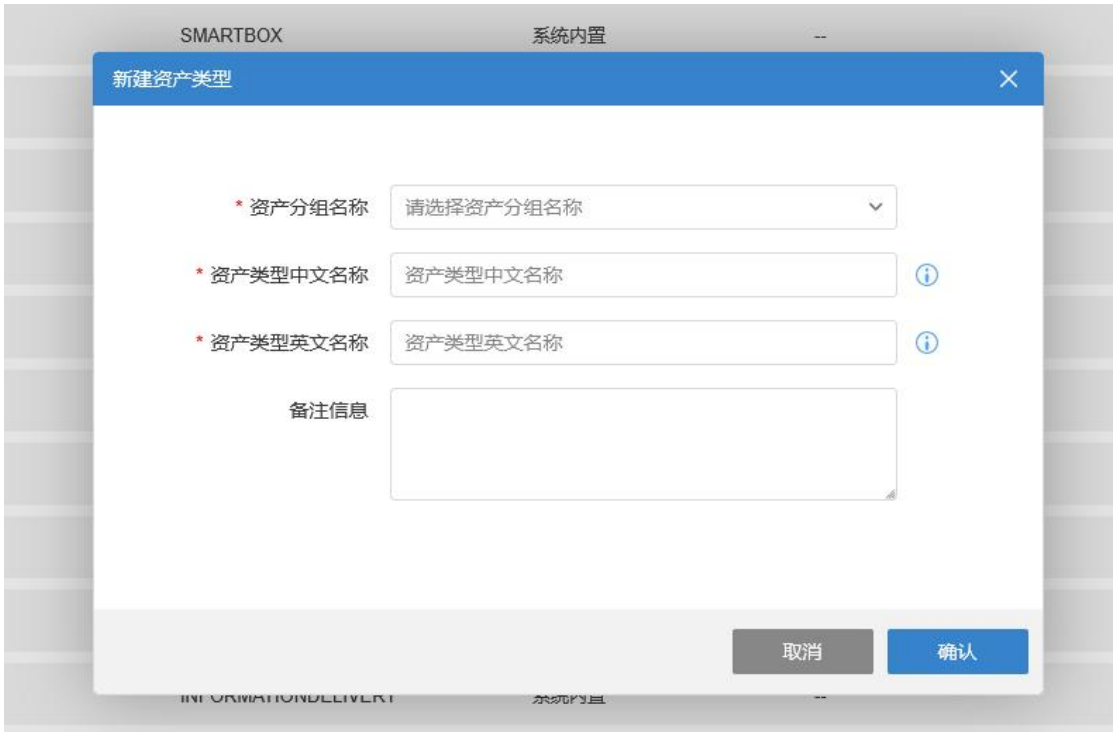


3.5.2 资产类型配置

点击菜单【资产识别】-【资产类型配置】，进入资产类型配置页面，此页面主要显示系统中内置的所有资产类型，以及手动添加的资产类型。如下图所示：



点击上方 按钮，弹窗添加资产类型窗口，如下图所示：

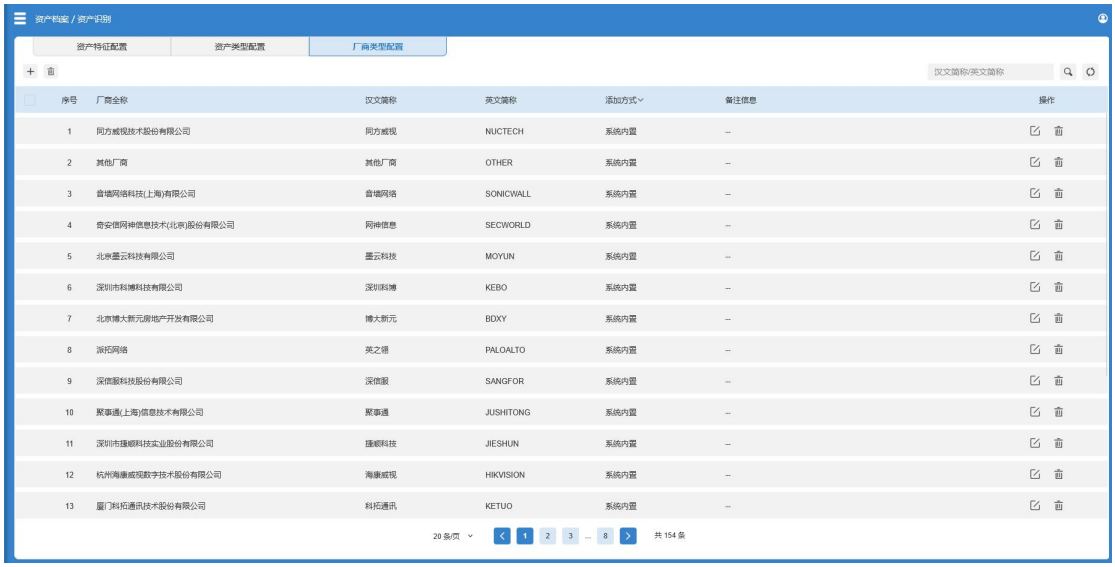


输入必填项：选择资产分组、输入资产类型中文名称、资产类型英文名称，输入备注信息，提交后，此资产类型出现资产类型配置页面，显示在列表最上方。

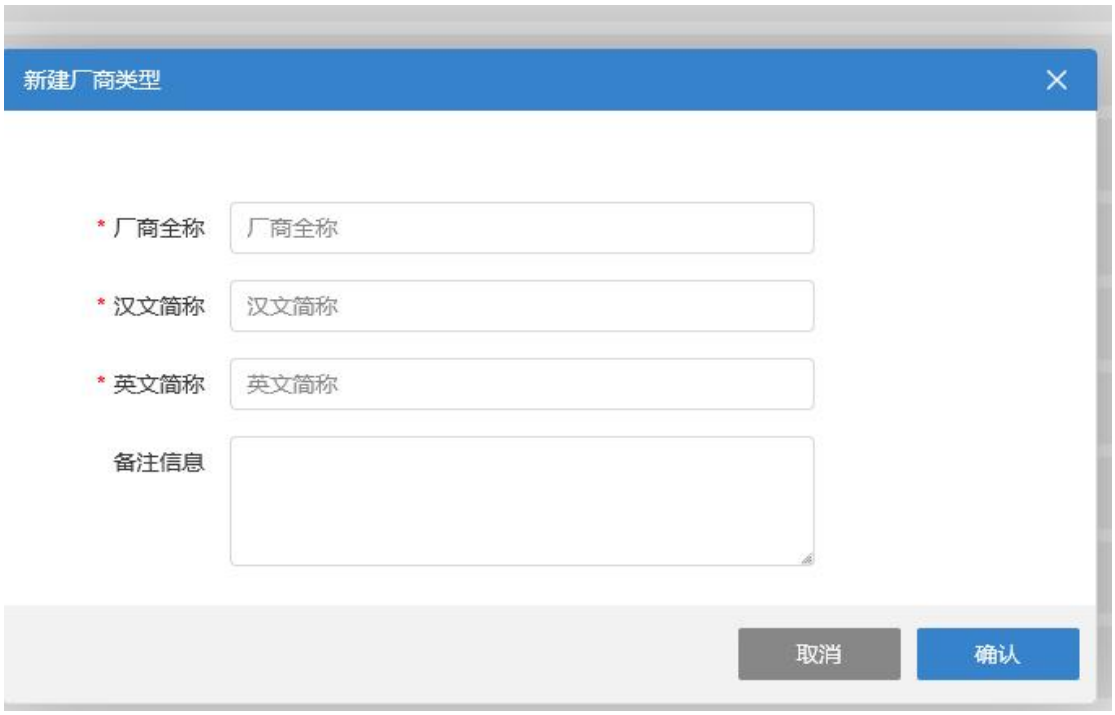
新增的资产类型，会显示正常显示并应用在**资产特征配置页面**的资产类型下拉列表中、待录资产和归档资产的资产类型下拉列表中，并可以成功筛选。

3.5.3 厂商类型配置

点击菜单【资产识别】-【厂商类型配置】，进入厂商配置页面，此页面主要显示系统中内置的所有厂商，以及手动添加的厂商。如下图所示：



点击上方 按钮，弹窗添加厂商窗口，如下图所示：

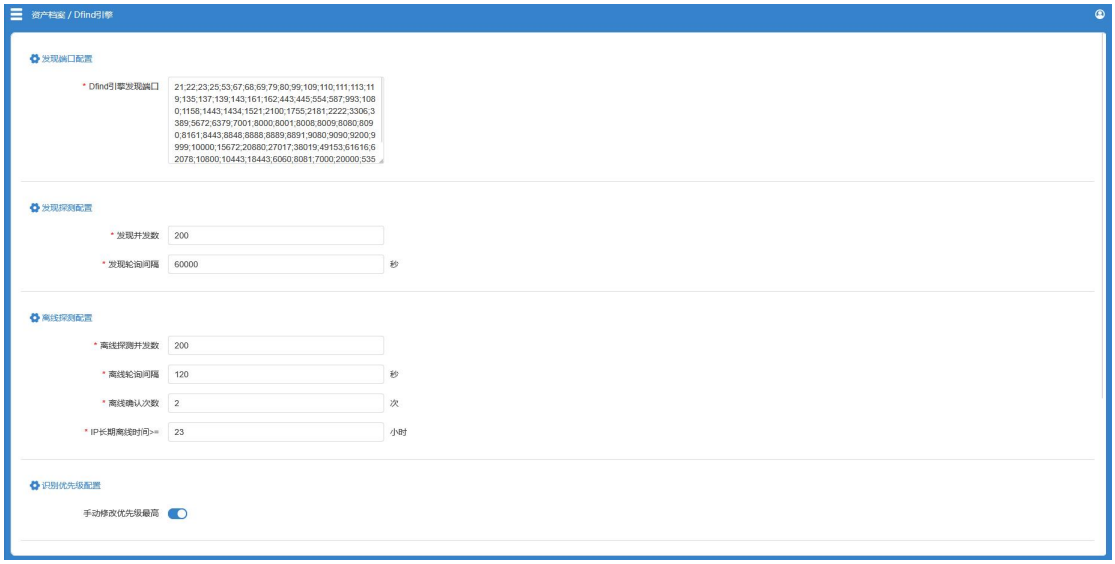


输入必填项：选择资产分组、输入厂商中文名称、厂商英文名称，输入备注信息，提交后，此厂商出现厂商配置页面，显示在列表最上方。

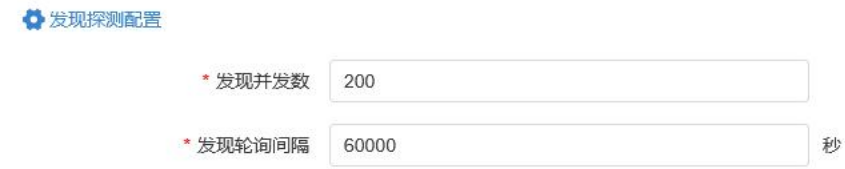
新增的厂商，会显示正常显示以及应用在**资产特征配置**的厂商下拉列表中、待录资产和归档资产的厂商下拉列表中，并可以成功筛选。

3.6 Dfind 引擎

点击【资产档案】-【Dfind 引擎】，进入 Dfind 引擎页面，此页面可以进行发现端口、发现探测、离线探测、识别优先级以及信息采集参数配置。如下图：



Dfind 引擎发现端口：此处配置发现端口，资产发现机制会根据配置的发现网段以及此处的端口进行发现资产。



发现探测配置：此处对发现探测的并发数以及发现轮询间隔进行配置，

发现并发数：同时发现多少 IP 资产

发现轮询间隔：每一轮发现完成后间隔多久再次进行发现。此处时间建议最小不小于 60 秒。



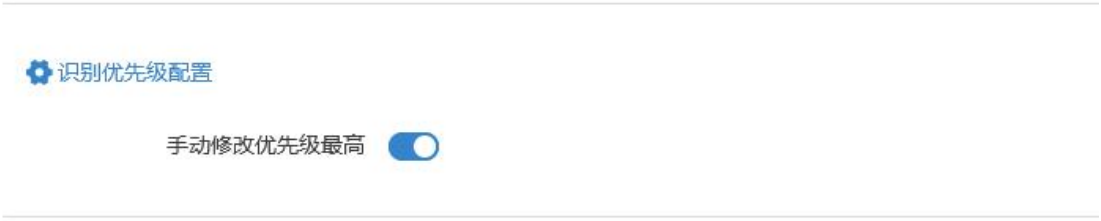
离线探测配置：此处对资产离线在线探测参数进行配置

离线探测并发数：同时探测多少资产是否为离线

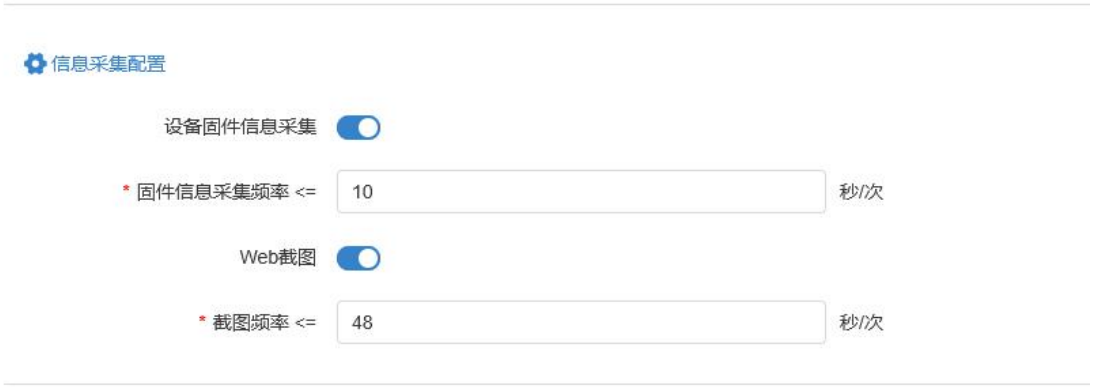
离线轮询间隔：每一轮识别完是否在线离线后间隔多久会再次识别探测。此处建议最小不小于 60 秒

离线确认次数：对一个资产识别为离线多少次时，网络状态置为离线。

IP 长时间离线时间：设置资产类型超过多久时，判定为长期离线的时间。



识别优先级配置：开启手动修改优先级最高时，对于手动修改的资产类型、资产厂商等基础数据置为优先级最高，当资产识别完成的数据与手动修改的数据不一致时，应用手动修改的数据。



设备固件信息采集：开启固件信息采集开关，设置固件信息采集频率时，当资产的用户名和密码准确时，会进行此资产的固件信息采集。

采集结果见资产类型的型号、序列号、固件版本列。注：目前仅支持海康威视厂商数据获取。

Web 截图：开启 web 截图时，会对资产进行 web 截图，截图结果见资产列表中的 web 截图列。

3.7 视图配置

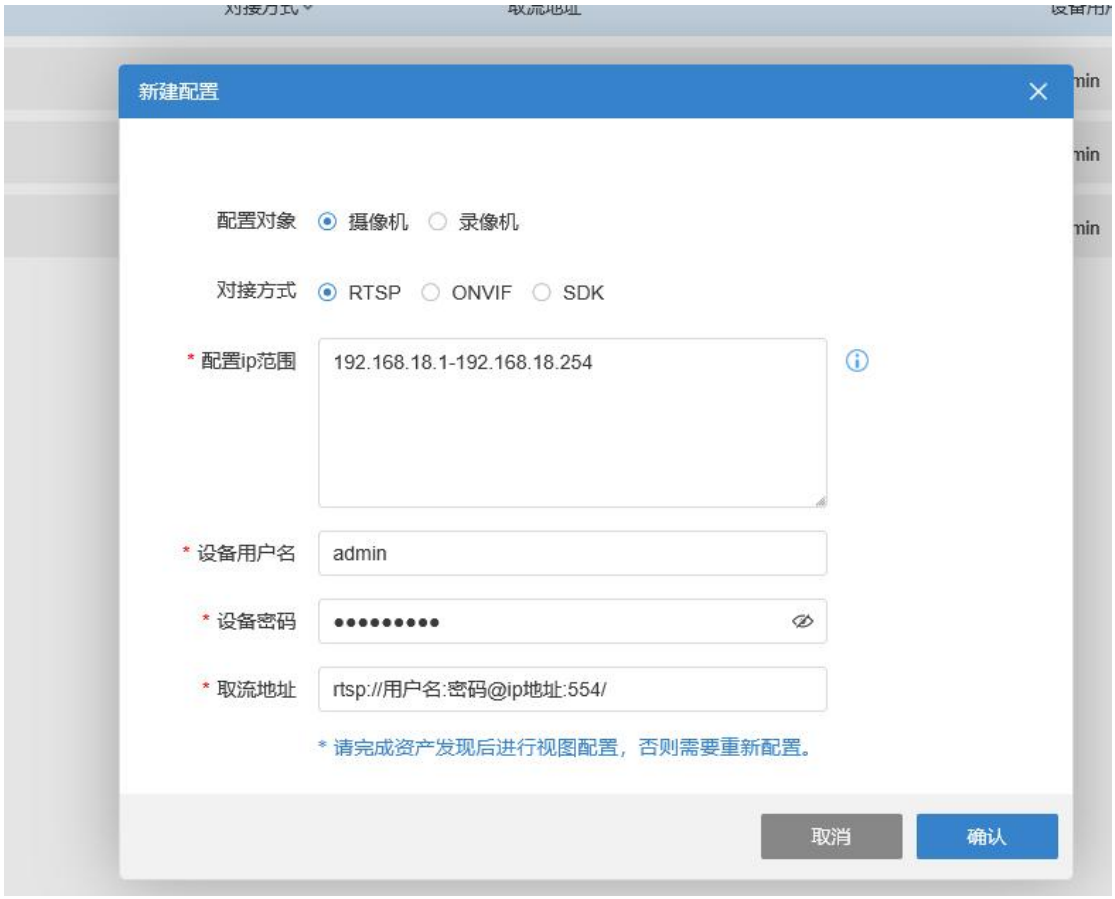
3.7.1 视图设备配置

注：请完成所有资产发现时，再进行视图配置，否则新发现的资产无法应用之前配置的视图配置数据。

点击【资产档案】-【视图配置】，进入视图设备配置页面，此页面展示对摄像机/录像机类型的数据进行对接方式、用户名、密码以及取流地址的配置。如下图：



点击上方　按钮，弹出新建配置页面，如下图：



RTSP/ONVIF 对接方式配置：

- 配置对象选择摄像机
- 选择对接方式-rtsp
- 输入需要识别的资产 IP 地址或者 IP 网段
- 输入网段中设备对应的正确的用户名和设备密码
- RTSP 模式下：点击取流地址，系统自动根据用户名和密码生成取流地址（访问取流地址可成功查看摄像头视频时，此取流地址可用）
- 当系统可根据配置的基本信息访问摄像机并成功取到流时，系统可成功对视频进行抓图，并且资产列表中的视频抓图、用户名和密码列数据会同时同步至列表中。

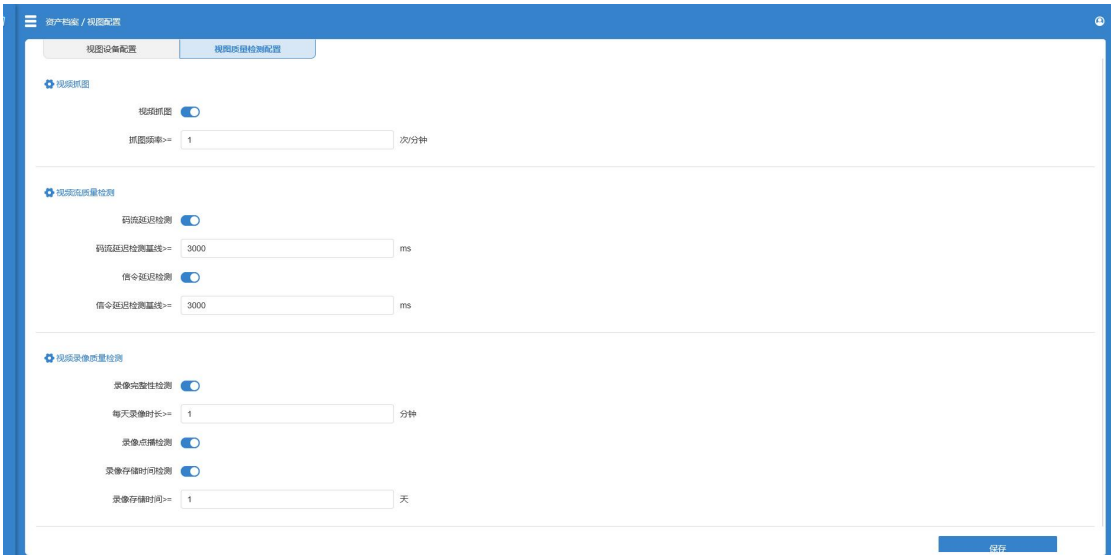
SDK 对接方式：



- 配置对象选择录像机
- 对接方式选择：SDK
- 输入需要识别的资产 IP 地址或者 IP 网段
- 输入网段中设备对应的正确的用户名和设备密码
- 系统可根据 SDK 的对接方式以及正确的用户名和密码对录像机进行检测。
- 根据视图质量检测配置中的视频录像质量检测数据配置，检测此录像机的录像完整性、录像点播、录像储存时间是否都正常，且检测结果成功显示在资产列表的录像完整性、录下点播以及录像存储列中。

3.7.2 视图质量检测配置

点击【资产档案】-【视图配置】-【视图质量检测配置】，进入视图质量检测配置页面，此页面可对视频抓图、视频流质量检测、视频录像质量检测参数进行配置。如下图：



视频抓图：

视频抓图：开启视频抓图，系统可根据视图配置中的数据，对资产进行抓图，抓图结果成功显示在资产列表的视频抓图列。

抓图频率：设置每个资产之间抓图的时间间隔为多久。

视频流质量检测：



码流延迟检测：开启码流延迟检测时，视频抓到图时，会根据抓到图时的码流延迟时间与设置的码流延迟时间进行对比，超过时显示异常，结果显示在资产列表的码流延迟列。

信令延迟检测：开启信令延迟检测时，视频抓到图时，会根据抓到图时的信令延迟时间与设置的信令延迟时间进行对比，超过时显示异常，结果显示在资产列表的信令延迟列。

视频录像质量检测：

当检测时录像机存在多个通道时，将多个通道增加到资产发现网段中，视频录像质量检测结果会一一显示在对应的通道 IP 列。



录像完整性检测：开启录像完整性检测，系统会根据视图配置中 sdk 对接方式的视图配置数据以及视频录像质量检测中设置的每天录像时间，进行录像完整性检测，结果显示在资产列表的录像完整性列。

录像点检测：开启录像完整性检测，系统会根据视图配置中 sdk 对接方式的视图配置数据，进行录像点播检测，结果显示在资产列表的录像点播列。

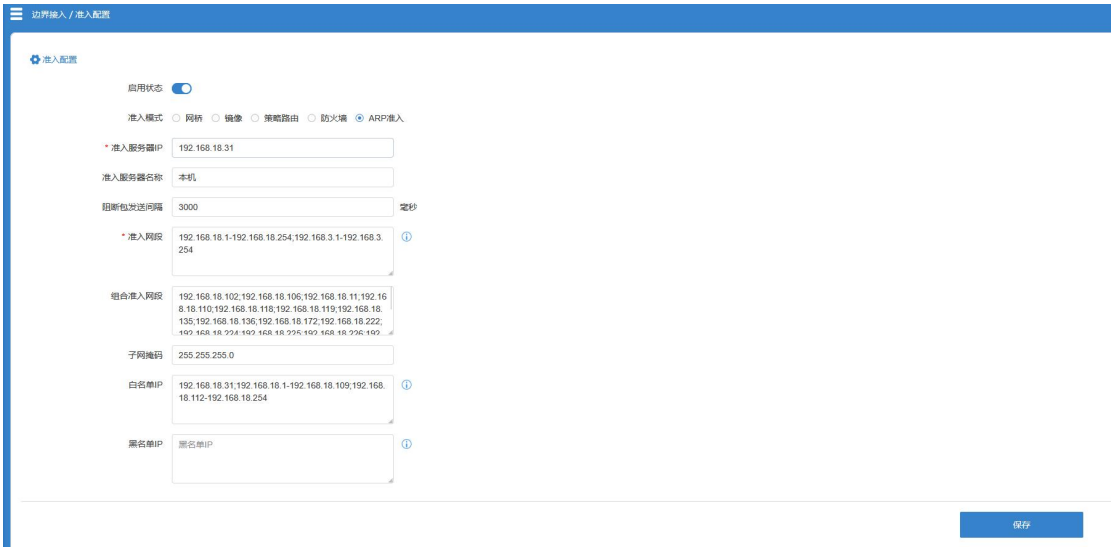
录像存储时间检测：开启录像存储时间检测，系统会根据视图配置中 sdk 对接方式的视图配置数据以及视频录像质量检测中设置的录像存储时间，进行录像存储时间检测，结果显示在资产列表的录像存储列。

第 4 节 边界接入

此功能模块主要进行准入服务器的配置。

4.1 准入配置

点击菜单【边界接入】-【准入配置】，此页面可对准入服务器进行开启、修改准入模式、配置准入网段、白名单等操作。如图 2.5-1 所示：



准入服务器配置完成并启用后可以对准入网段中的资产进行阻断、放行操作。

准入模式：分为网桥、镜像、策略路由、防火墙、ARP 准入五种方式；

具体内容请根据各个方式进行添加，填写完成后点击提交即可。

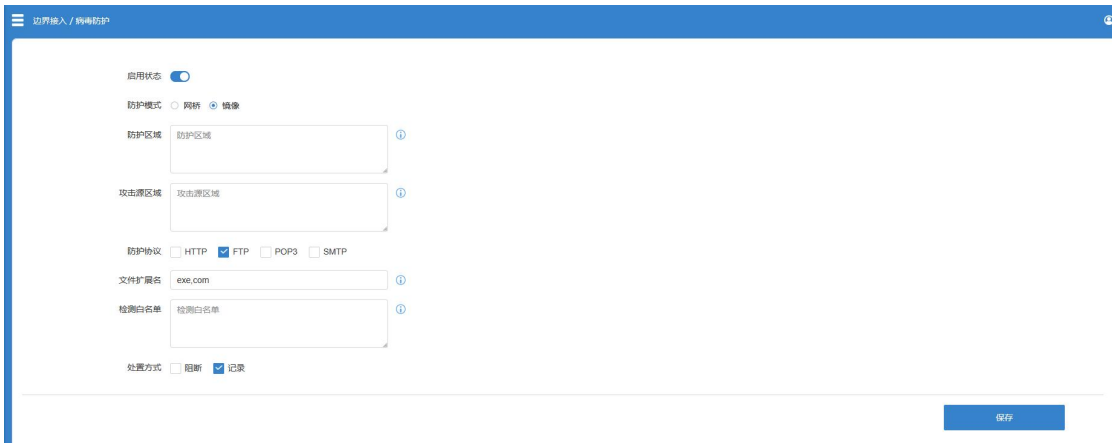
准入网段：此网段内的资产才可进行系统内各功能的阻断和放行控制。**非此网段内的资产且在资产列表中的资产不会被进行阻断控制。**

组合准入网段：此网段为【组合准入】页面中，进行筛选后的准入资产，此数据无需手动添加，为【组合准入】页面的回显数据。**当组合准入开启，且配置组合准入后，准入配置中的准入网段，组合准入网段优先级更高。**

白名单 IP：白名单内填写的 IP 地址，不会被阻断。使用时最好填写几个信任的电脑终端 IP 地址进入白名单 IP 输入框内。注意：开启准入配置之前，一定要把准入系统 IP 地址、宿主机的物理 IP 地址填写进去。

4.2 病毒防护

点击菜单【边界接入】-【病毒防护】，进入病毒防护页面，此页面可对 http、ftp、pop3、smtp 等协议进行流量病毒检测阻断。



- 启用状态：开启启用状态后，系统会对选择的协议进行流量病毒检测，关闭后，不会进行检测
- 防护区域：填写防护区域 IP 或 IP 网段，
  - 防护区域存在数据时，属于防护区域内的 IP 会被检测记录
  - 防护区域为空时，被镜像流量检测到的所有 IP 都会被检测记录
- 攻击源区域：填写 IP 或 IP 网段
  - 攻击源区域存在数据时，属于攻击源区域内的 IP 会被检测记录
  - 防护区域为空时，会对所有的 IP 进行检测记录
- 防护协议：勾选需要检测的防护协议 http、ftp、pop3 以及 SMTP，未勾选的协议不会被检测记录
- 文件扩展名：填写需要检测流量中携带的病毒文件扩展名，未填写的扩展名不会被检测记录
- 检测白名单：填写 IP 或 IP 网段，白名单内的 IP 不会进行流量病毒检测
- 处置方式

- 阻断：勾选阻断后，被检测的攻击源 IP 存在病毒文件时，会对此 IP 进行阻断操作
- 记录：勾选记录时，被检测的攻击源 IP 存在病毒文件时，会对此 IP 进行记录，将日志记录至【日志分析 – 防病毒日志】页面中。

操作步骤：

1、开启启用状态

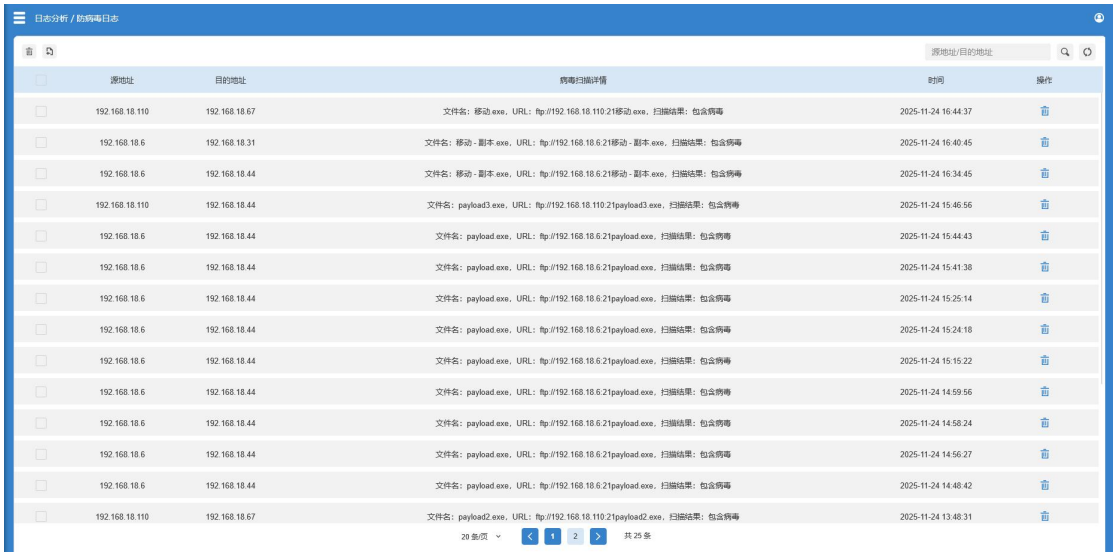
2、设置防护区域和攻击源区域，勾选攻击协议

3、输入文件扩展名如：exe，com

4、勾选处置方式：记录

5、用户于攻击源区域内 IP 根据勾选的协议类型，携带病毒文件后，对防护区域进行攻击，并且被流量检测到。

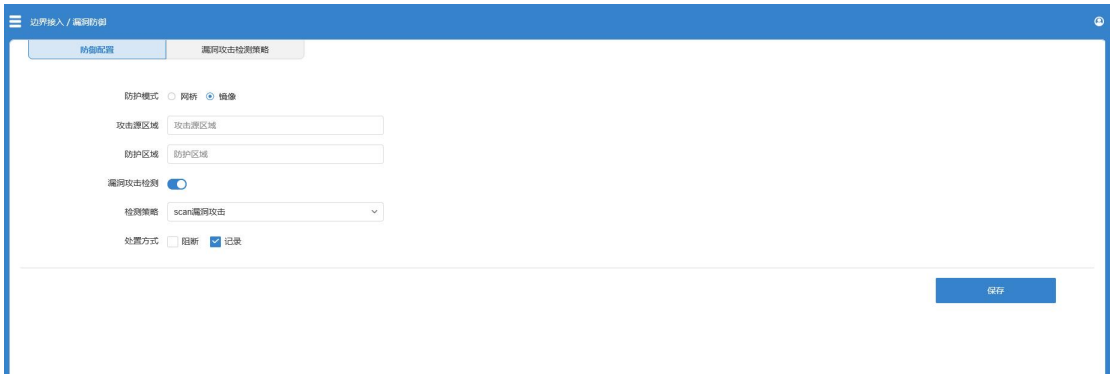
6、攻击日志记录至【日志分析】-【防病毒日志】中。



4.3 漏洞防御

4.3.1 防御配置

点击菜单【边界接入】-【漏洞防御】-【防御配置】，进入漏洞防御页面，此页面根据设置的漏洞检测策略，对漏洞攻击利用进行检测阻断。



操作步骤：

1、选择防护模式：镜像

2、输入攻击源区域 IP/IP 段或为空

3、输入防护区域 IP/IP 段或为空

4、开启漏洞攻击检测开关

5、选择“漏洞攻击检测策略”页面创建的攻击策略

6、选择检测到漏洞攻击后的处置方式：阻断/记录/阻断和记录

7、攻击源区域 IP 地址对防护区域 IP 进行漏洞攻击时，系统根据配置的漏洞攻击策略成功检测到，并对攻击源 ip 进行阻断操作，攻击记录至日志中。

4.3.2 漏洞攻击检测策略

点击菜单【边界接入】-【漏洞防御】-【漏洞攻击检测策略】，进入漏洞攻击检测策略页面，此页面可创建需检测的漏洞攻击策略。



操作步骤：

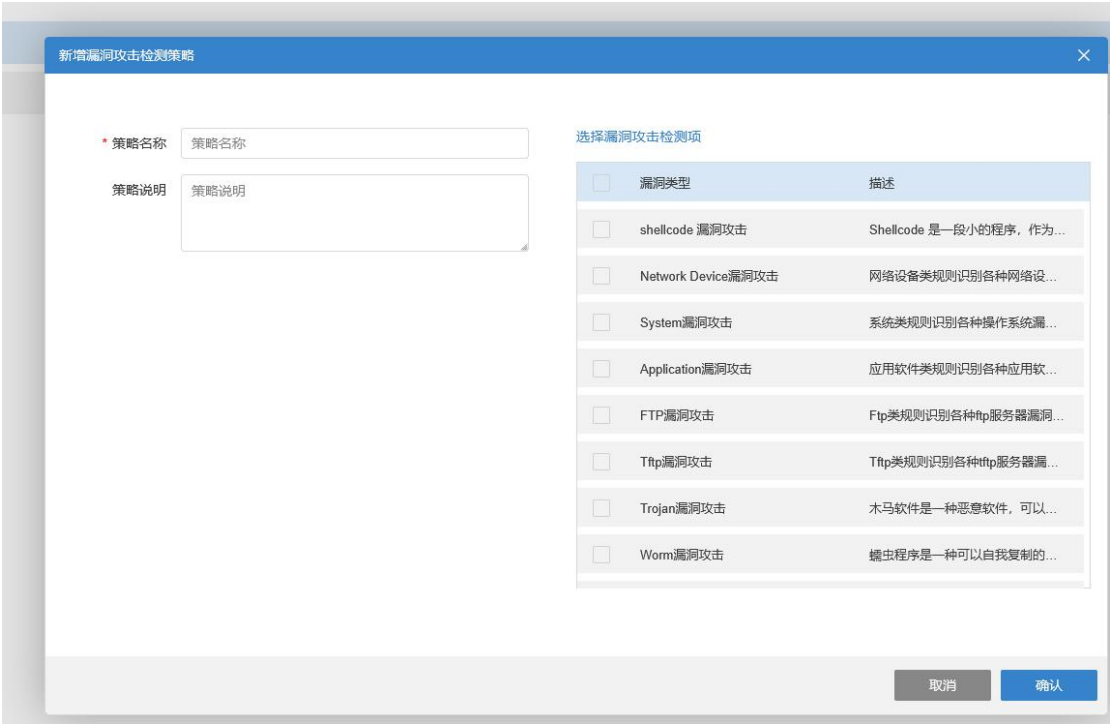
1、点击【+】按钮，弹出新增漏洞攻击检测策略页面

2、输入策略名称和策略说明

3、选择漏洞攻击检测项

4、点击确定按钮，漏洞攻击检测策略创建成功。

5、漏洞攻击检测页面数据显示正常，防御配置页面，漏洞攻击检测策略下拉框数据显示正确。

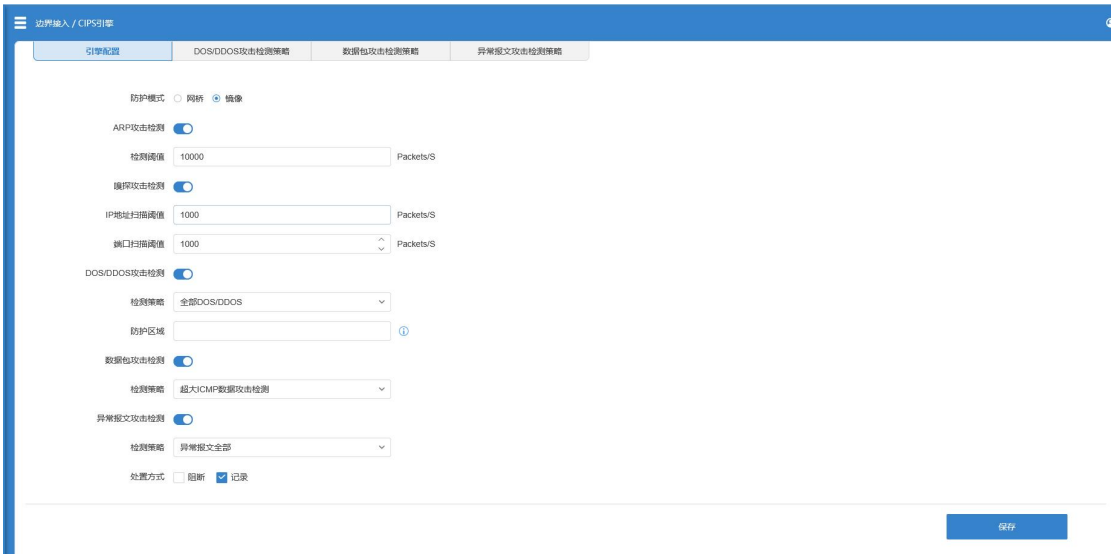


4.4 CIPS 引擎

点击菜单【边界接入】-【CIPS 引擎】，进入 CIPS 引擎页面，此页面包括引擎配置、DOS/DDOS 攻击检测策略、数据包攻击检测策略、异常报文攻击检测策略 4 个页签，可对 CIPS 各类攻击检测设置检测阈值，创建并设置攻击检测策略以及处置方式。

4.4.1 引擎配置

点击菜单【边界接入】-【CIPS 引擎】-【引擎配置】，进入引擎配置页面，此页面可对 CIPS 各类攻击检测设置检测阈值，检测策略以及处置方式。



操作步骤：

1、ARP 攻击检测：开启 ARP 检测开关，设置检测阈值。对系统进行 ARP 攻击，系统自动检测到此行为，超过设置的阈值时，对攻击源 IP 进行阻断以及记录此攻击日志

2、嗅探攻击检测：开启嗅探攻击检测开关，设置 IP 地址扫描阈值和端口扫描阈值。对系统进行检测嗅探攻击，系统自动检测到此行为，超过设置的阈值时，对攻击源 IP 进行阻断以及记录此攻击日志

3、DOS/DDOS 攻击检测：

1) 开启 DOS/DDOS 攻击检测开关，选择检测策略，

2) 输入防护区域，或不输入防护区域（检测所有被镜像到的攻击 IP）

3) 点击保存，

4) 进行 DOS/DDOS 攻击，系统自动检测此攻击，对攻击源 IP 进行阻断以及记录此攻击日志

4、数据包攻击检测：开启数据包攻击检测开关，选择检测策略，点击保存，进行数据包攻击，系统自动检测此攻击，并对攻击源 IP 进行阻断以及记录此攻击日志

5、异常报文攻击检测：开启异常报文攻击检测开关，选择检测策略，点击保存后，进行异常报文攻击，系统自动检测此攻击，并对攻击源 IP 进行阻断以及记录此攻击日志

4.4.2 DOS/DOSS 攻击检测策略

点击菜单【边界接入】-【CIPS 引擎】-【DOS/DDOS 攻击检测策略】，进入 DOS/DDOS 攻击检测策略页面，此页面可创建需检测的 DOS/DDOS 攻击策略。



操作步骤：

- 检测设置

1、点击左上角【 】按钮，弹出检测设置页面

2、查看默认阈值

3、根据需要修改 DOS/DDOS 攻击检测项阈值，点击确定，阈值修改成功。

- 创建 DOS/DDOS 攻击检测策略

1、点击【+】按钮，弹出新增 DOS/DDOS 攻击检测策略页面



2、输入策略名称和策略说明

3、选择 DOS/DDOS 攻击检测项

4、点击确定按钮，DOS/DDOS 攻击检测策略创建成功。

5、DOS/DDOS 攻击检测页面数据显示正常，防御配置页面，DOS/DDOS 攻击检测策略下拉框数据显示正确。

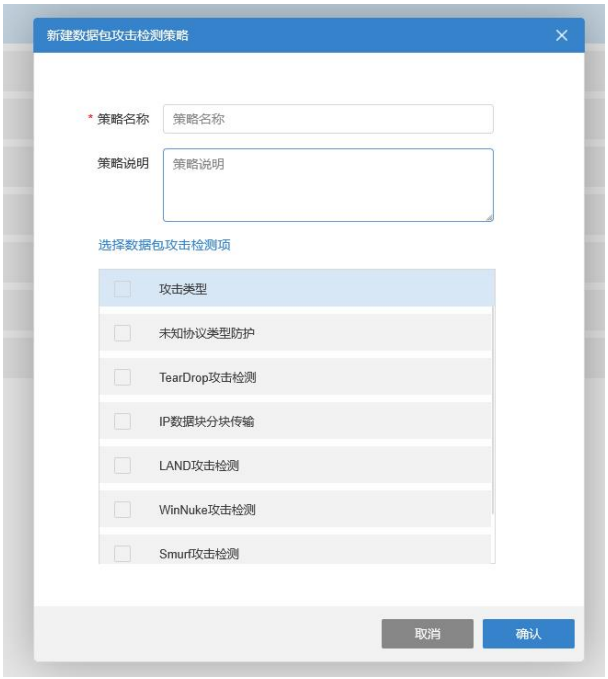
4.4.3 数据包攻击检测策略

点击菜单【边界接入】-【CIPS 引擎】-【数据包攻击检测策略】，进入数据包攻击检测策略页面，此页面可创建需检测的数据包攻击策略。



操作步骤：

1、点击【+】按钮，弹出新增数据包攻击检测策略页面



2、输入策略名称和策略说明

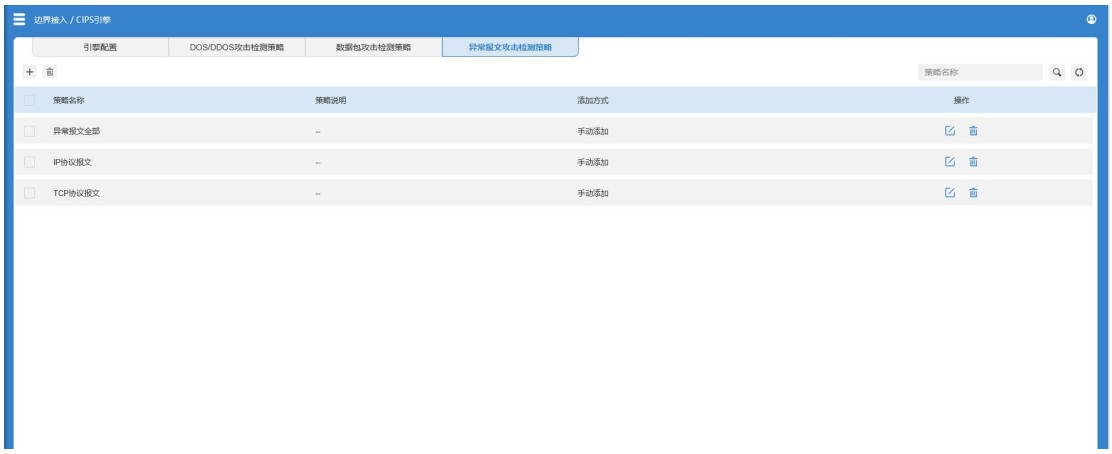
3、选择数据包攻击检测项

4、点击确定按钮，数据包攻击检测策略创建成功。

5、数据包攻击检测页面数据显示正常，防御配置页面，数据包攻击检测策略下拉框数据显示正确。

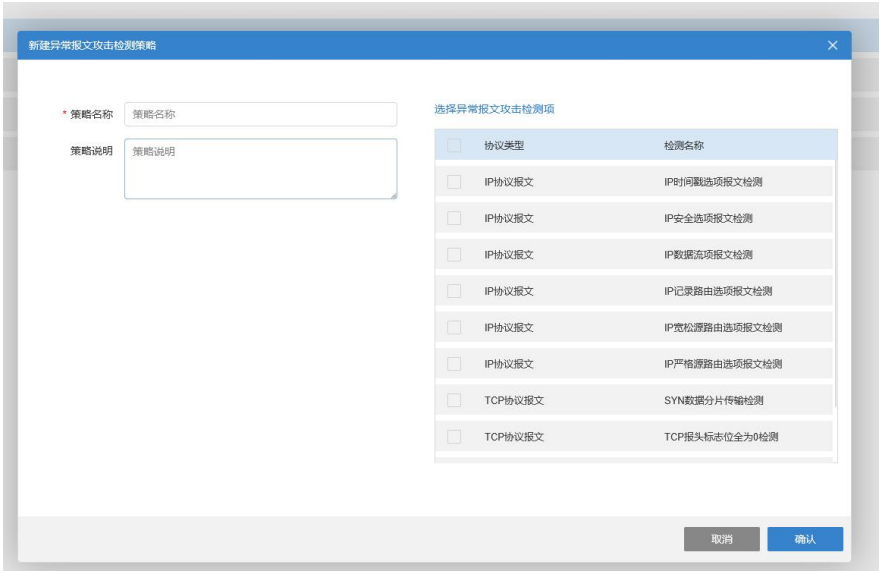
4.4.4 异常报文攻击检测策略

点击菜单【边界接入】-【CIPS 引擎】-【异常报文攻击检测策略】，进入异常报文攻击检测策略页面，此页面可创建需检测的异常报文攻击策略。



操作步骤：

1、点击【+】按钮，弹出新增异常报文攻击检测策略页面



2、输入策略名称和策略说明

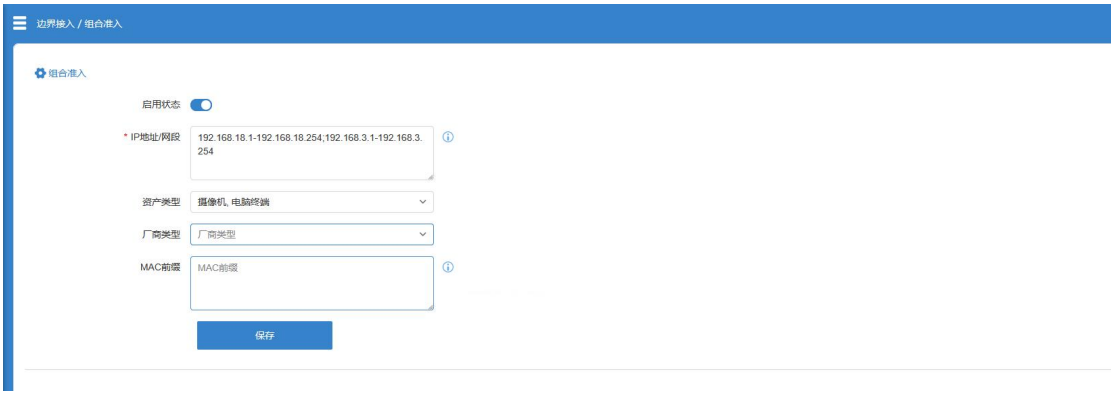
3、选择异常报文攻击检测项

4、点击确定按钮，异常报文攻击检测策略创建成功。

5、异常报文攻击检测页面数据显示正常，防御配置页面，异常报文攻击检测策略下拉框数据显示正确。

4.5 组合准入

此功能模块主要对准入进行组合、单独准入的设置，包括对资产类型、厂商以及 MAC 地址进行组合准入或单独准入。



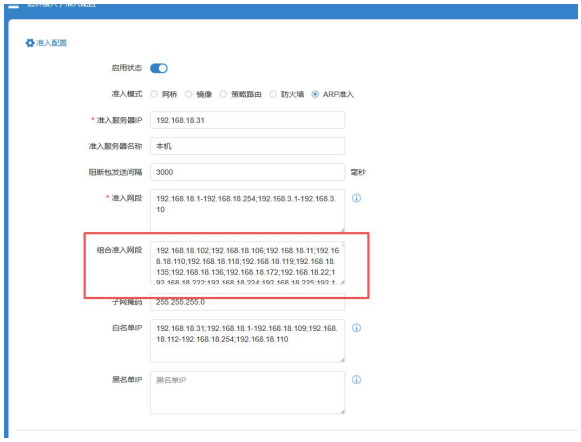
启用状态：开启启用状态后，启用组合准入。

IP 地址/网段：此处填写需要准入的 IP/网段信息，为必填项

资产类型：显示系统中所有的资产类型，可进行多选

厂商类型：显示系统中所有的厂商，可进行多选

Mac 前缀：输入需要进行筛选的 mac 地址的前缀或完整的 mac 地址。



开启组合准入、输入 IP 地址、勾选资产类型、厂商以及输入 mac 地址，点击保存后，被筛选出符合条件的 IP 地址，会回显到【准入配置】页面的“组合准入网段”中，开启准入配置后，以“组合准入网段”为准。

因开启组合准入后，“组合准入网段”优先级高于“准入网段”。

第 5 节 风险检查

此功能模块主要对扫描任务进行创建、启动等操作，对扫描结果和扫描记录进行列表展示，对扫描策略进行创建、展示。

5.1 扫描任务

点击菜单【风险检查】-【扫描任务】，此页面可对扫描任务进行新建、编辑、开启、暂停、终止、删除和导出操作，如图 2.6-1 所示：

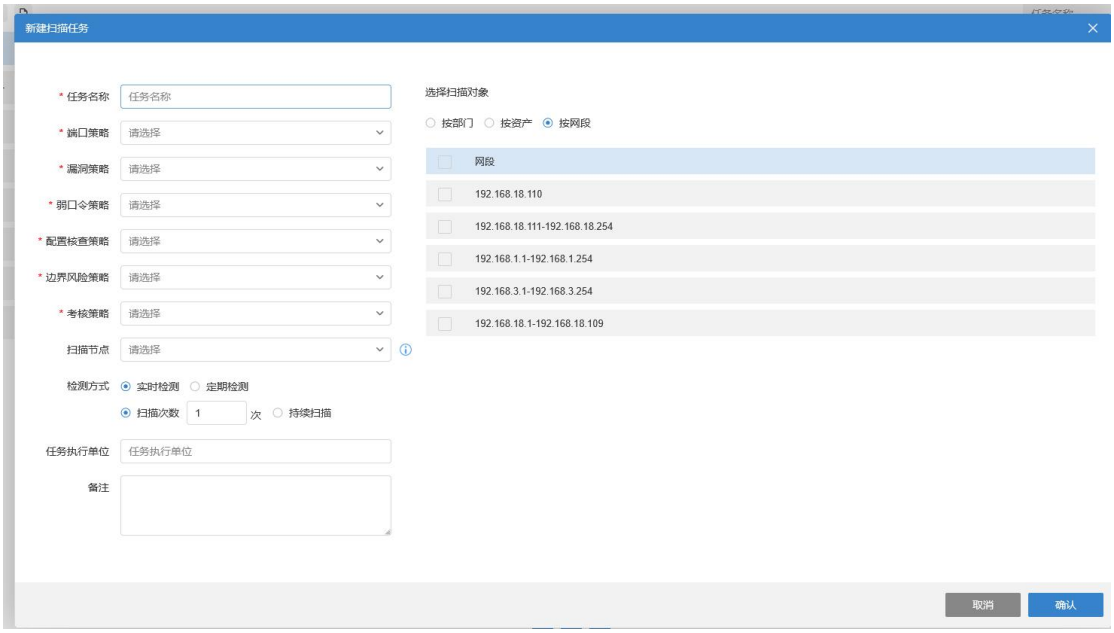


扫描任务页面以列表形式展示任务名称、任务状态、扫描数量、端口策略、漏洞策略、弱口令策略、配置核查策略、边界风险策略、考核策略以及检测方式；

扫描任务页面右侧操作栏可对“非进行中”的扫描任务进行编辑，删除，启动操作；可对“暂停”的任务进行终止操作；可对“进行中”的扫描任务进行暂停和终止的操作；

页面上方操作按钮，可对扫描任务进行新增，批量启动、暂停、终止、删除和导出操作以及右侧搜索框进行模糊查询操作；

用户点击左上角+号，进入【新建扫描任务】页面，如图 2.6-2 所示。此页面任务名称、端口策略、漏洞策略、弱口令策略、配置核查策略、边界风险策略、考核策略、检测方式以及选择扫描对象为必填选项，扫描节点、任务执行单位和备注为选填。



端口策略：端口策略内容以下拉列表形式展示，展示内容为【风险检查】-【端口策略库】中端口策略库列表信息；

漏洞策略：漏洞策略内容以下拉列表形式展示，展示内容为【风险检查】-【漏洞策略库】中漏洞策略库列表信息；

弱口令策略：弱口令策略内容以下拉列表形式展示，展示内容为【风险检查】-【弱口令策略库】中弱口令策略库列表信息；

配置核查策略：配置核查策略内容以下拉列表形式展示，展示内容为【风险检查】-【配置核查策略库】中配置核查策略库列表信息；

边界风险策略：边界风险策略内容以下拉列表形式展示，展示内容为【风险检查】-【边界风险策略库】中边界风险策略库列表信息；

考核策略：考核策略内容以下拉列表形式展示，展示内容为【风险考核】-【考核策略库】中考核策略库列表信息；

扫描节点：当系统于【级联管理】-【平台级联管理】模块开启探针级联时，此扫描节点处显示主平台和所有子平台。

扫描节点选择子平台后，会将此扫描任务下发至子平台进行扫描，扫描完成时，子平台会将扫描结果等数据再次上报至主平台。

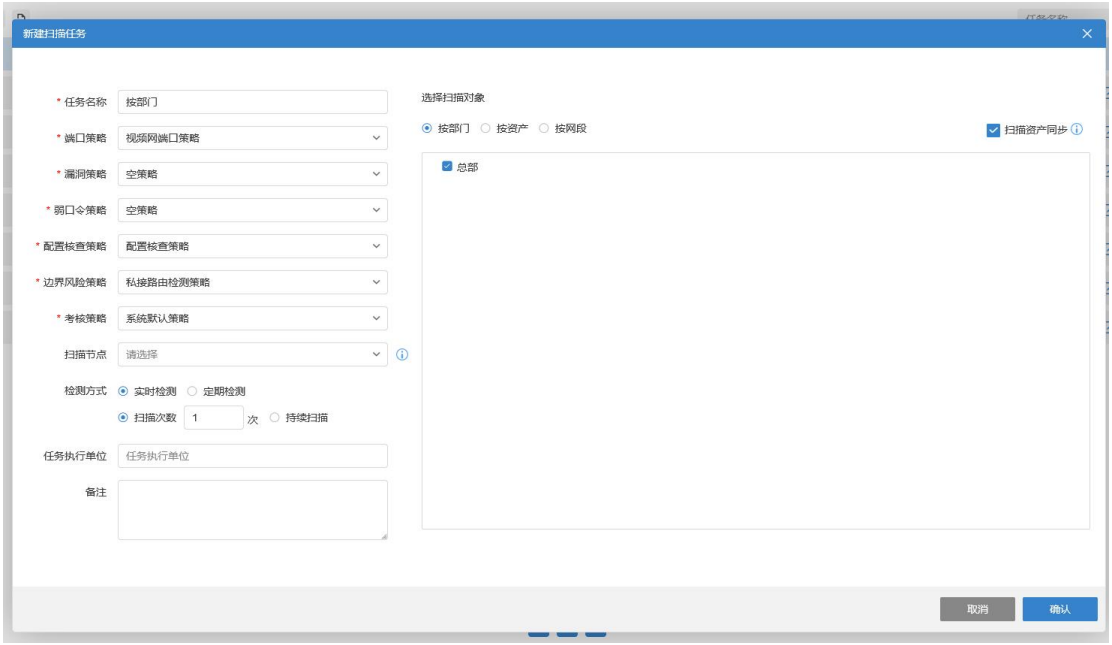
选择对应扫描节点后，扫描对象只允许 – 按资产扫描，且只允许选择此节点下的资产 IP 进行扫描。

扫描方式：包括实时检测和定期检测，



- 实时检测：选择实时检测，
  - 选择扫描次数，任务创建成功，手动点击启动，任务执行扫描，扫描完成后任务自动继续执行检测，直到到达对应次数，任务结束。
  - 持续扫描：任务创建成功，手动点击启动，任务执行扫描，扫描完成后任务自动继续执行检测，直到手动终止此任务，任务结束扫描。
- 定期检测包括：每天、每周、每月和固定日期，到达指定日期时，扫描任务自动启动，开始执行扫描；

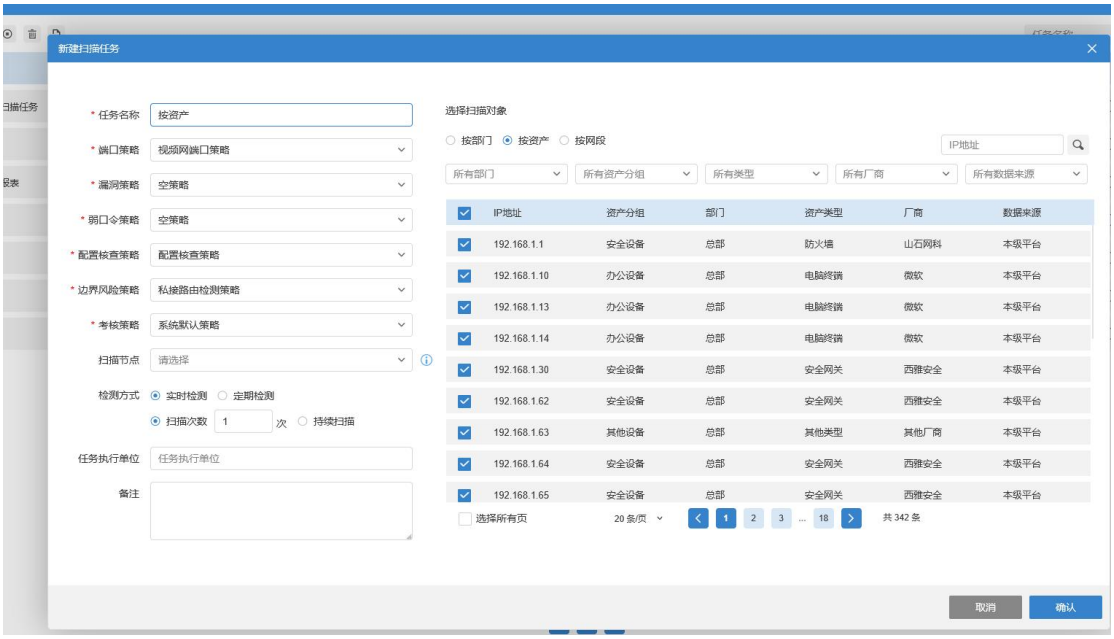
选择扫描对象 – 按部门：如图 2.6-3 所示：



- 此窗口展示【系统设置】-【部门管理】页面中的所有部门，通过复选框进行选择且部门之间相互独立；
- 扫描资产同步：选择扫描对象 – 按部门的窗口处展示“扫描资产同步”复选框，勾选此复选框，在任务开启时可自动同步部门下新增的资产
- 按部门扫描时，被选择的部门中无扫描网段时，无法创建扫描任务。
- 勾选被扫描的部门，输入其他必填信息，创建扫描任务
- 扫描任务可成功被创建，启动以及扫描完成。

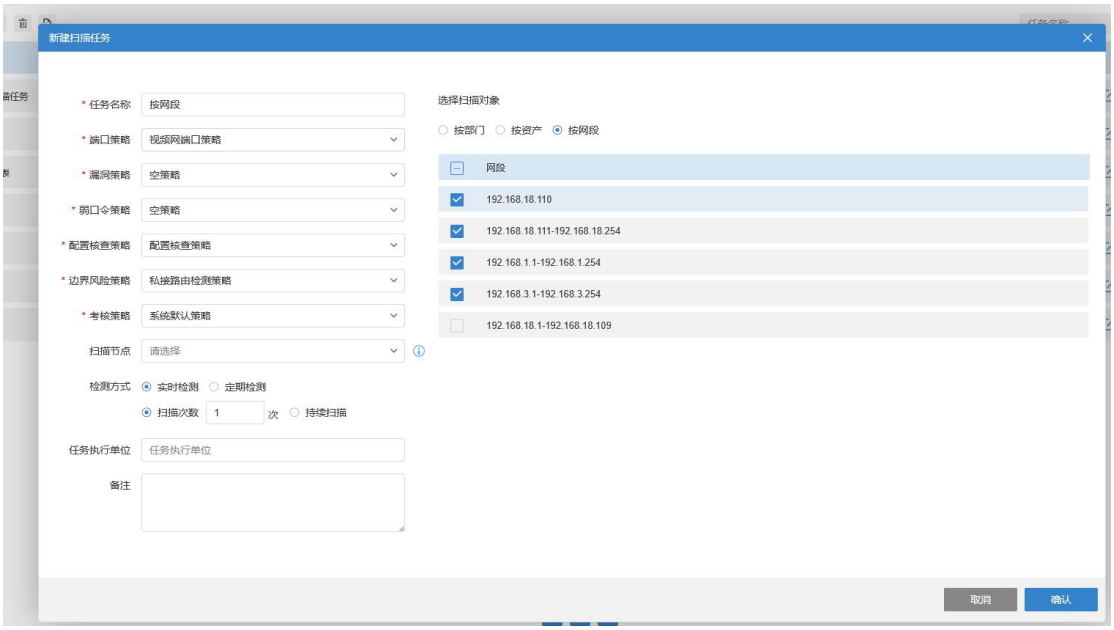
选择扫描对象 – 按资产：

- 此窗口展示【资产档案】-【资产列表】页面中所有的资产信息，通过复选框进行选择。此窗口还提供按照部门、按照资产分组、类型、厂商以及数据来源进行筛选搜索操作，如图 2.6-4 所示：



- 选择所有页：点击此按钮，可同时选择所有页的资产 IP，创建扫描任务
- 勾选被扫描的资产 IP，输入其他必填信息，创建扫描任务
- 扫描任务可成功被创建，启动以及扫描完成。

选择扫描对象 – 按网段：

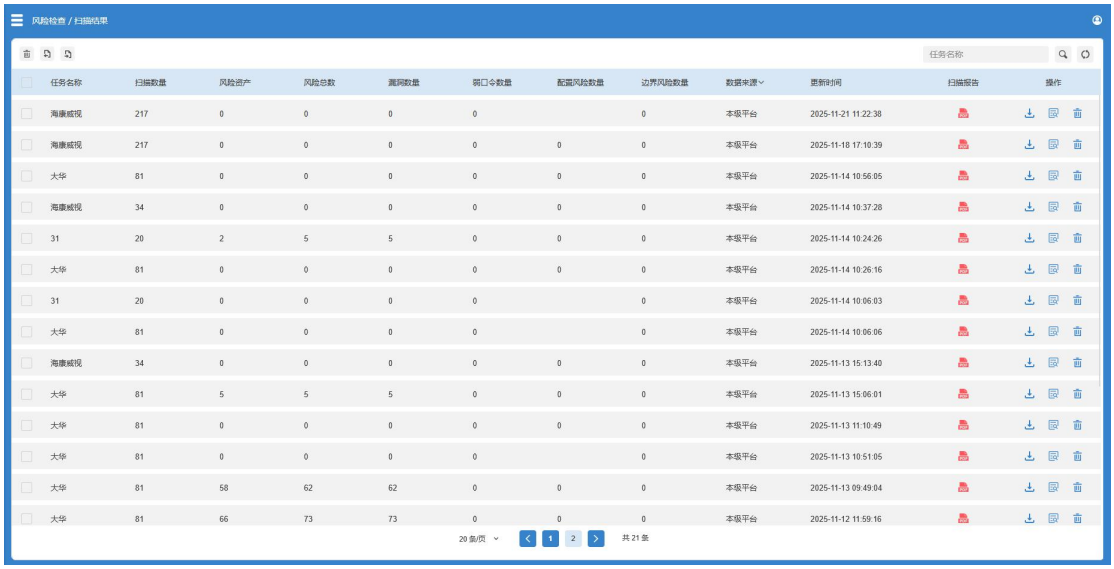


- 此窗口展示【资产发现】 – 扫描网段中的所有网段
- 选择被扫描网段，输入其他必填信息，创建扫描任务
- 扫描任务可成功被创建，启动以及扫描完成。

5.2 扫描结果

点击菜单【扫描结果】-【扫描结果】此页面可查看所有任务已完成状态的扫描结果并

以列表形式展示，如图 2.6-5 所示：



此页面上方按钮区域可对扫描结果进行批量删除、批量导出以及根据任务名称模糊查询操作；

扫描报告列：点击扫描报告 PDF 图标，可对扫描报告进行预览，如图 2.6-6 所示：



操作列可对任务进行扫描报告下载，扫描结果详情查看以及扫描结果进行删除操作；

点击下载按钮，可将扫描报告下载至本地，文件格式为 pdf 格式；

点击详情按钮，进入【扫描结果详情】页面，此页面展示当前任务中的风险详情、漏洞详情、弱口令详情和边界风险详情，如图 2.6-7 所示：



风险详情页面：展示扫描任务的风险资产，包括：IP 地址、资产类型、部门、风险总数、漏洞数和弱口令数，可列表进行导出和搜索操作；

漏洞详情：展示扫描任务中所有的漏洞，包括：IP 地址、资产类型、部门、漏洞级别、漏洞名称和漏洞描述，可对列表进行导出和搜索操作；

弱口令详情：展示扫描任务中的所有弱口令，包括：IP 地址、资产类型、部门、弱口令用户名和弱口令密码，输入账号和密码可查看弱口令密码，点击导出和搜索按钮，对列表进行导出和搜索操作；

配置核查详情：展示扫描任务中所有的配置核查不达标的核查项，包括：IP 地址、资产类型、部门、核查结果、核查详情，可对列表进行导出和搜索操作。

边界风险详情：展示扫描任务中所有的边界风险，包括：IP 地址、资产类型、部门、边界风险类型、风险详情和产生事件，可对列表进行导出和搜索操作。

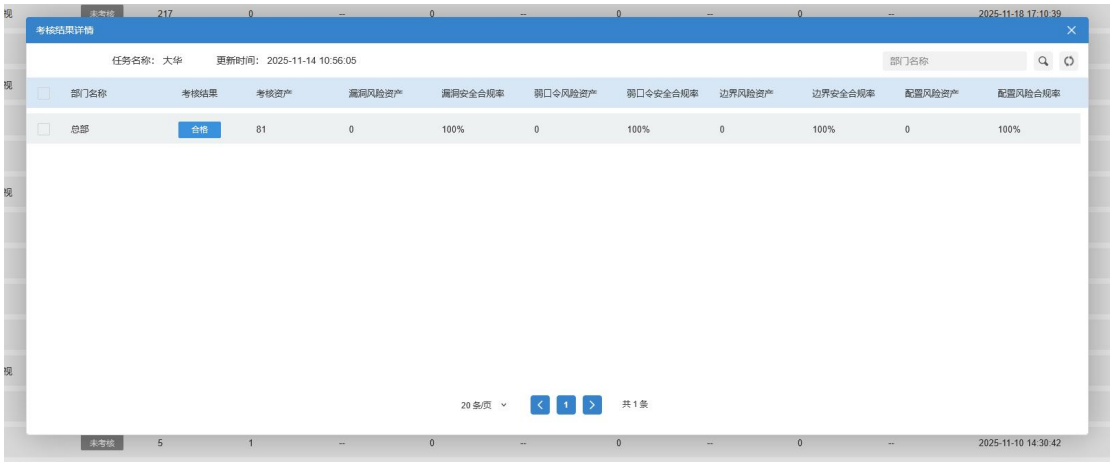
风险变化分析：展示同一扫描任务，扫描 2 次及 2 次以上时，当前任务与上次任务的变化分析。

5.3 考核结果

点击菜单【风险检查】-【考核结果】，此页面可查看已完成状态下，存在考核策略的扫描任务全部的考核结果，包括考核资产、漏洞风险资产、漏洞安全合规率等信息并以列表形式展示，如图所示：



右侧操作列包括详情按钮和删除按钮，点击删除按钮可对当前任务的考核结果进行删除操作，点击详情查看当前任务的考核详情。如图 2.7-2 所示：

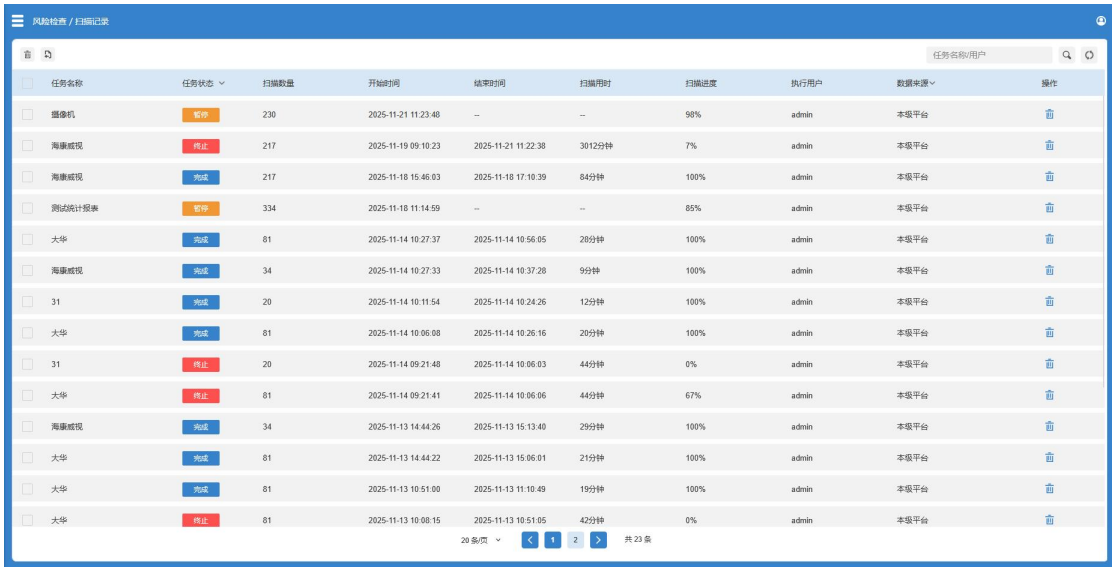


考核结果详情页面：通过部门视角展示当前任务中每个部门的考核结果，包括考核资产、漏洞风险资产、漏洞安全合规率、弱口令风险资产、弱口令安全合规率，边界风险资产、边界安全合规率以及配置核查资产和配置核查合规率以列表形式展示；

5.4 扫描记录

点击菜单【风险检查】-【扫描记录】此页面，展示扫描任务的每次执行记录，包括进行中、暂停、终止和完成状态的任务记录。

扫描记录信息包括：任务的执行状态、扫描数量、开始时间、结束时间，扫描用时，扫描进度、扫描用户以及数据来源并以列表形式展示，如图 2.6-8 所示：



数据来源：根据启动扫描任务时，扫描节点显示此扫描记录是来自本级平台还是子平台。

操作列支持删除扫描记录操作；

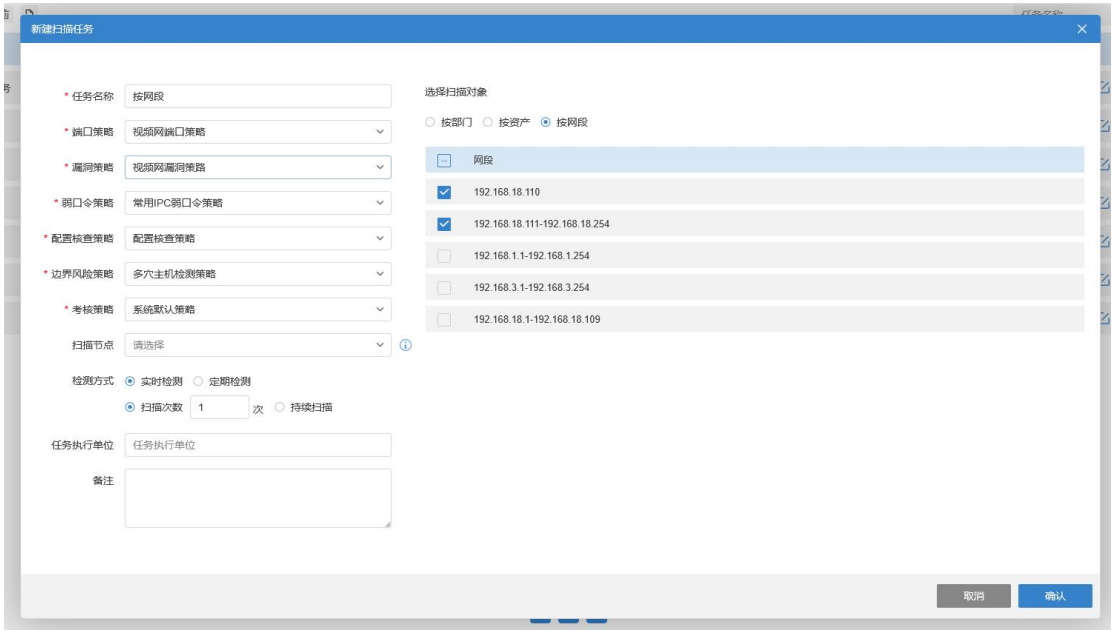
列表上方按钮支持批量删除、批量导出和根据任务名称/用户进行模糊查询操作。

新增扫描任务示例一

1、进入【风险检查】-【扫描任务】页面，点击+按钮，

2、进入【新建扫描任务】页面，输入任务名称、选择端口策略、漏洞策略、弱口令策略、配置核查策略、边界风险策略以及考核策略，

3、选择检测方式 – 实时检测 – 扫描次数 1 次，选择扫描对象 – 按网段，勾选网段，点击提交。



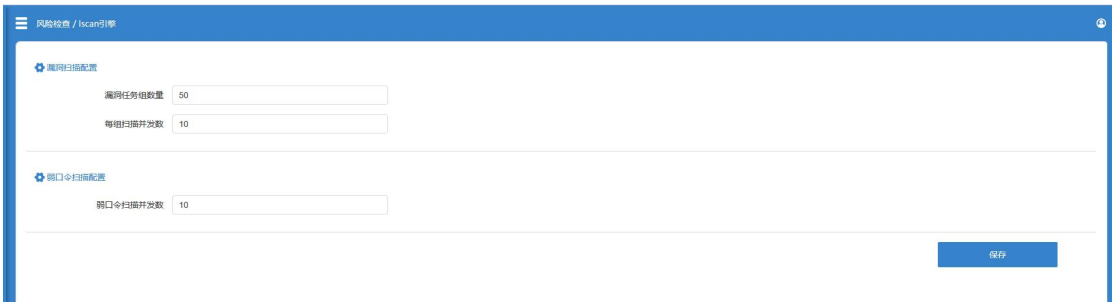
4、进入扫描记录页面，查看此任务的扫描记录

5、任务执行完成，查看此扫描任务状态为完成。

6、进入【扫描结果】页面查看扫描结果和考核结果。

5.5 Iscan 引擎

点击菜单【风险检查】-【Iscan 引擎】进入 Iscan 引擎页面，如下图所示：



漏洞扫描配置：漏洞扫描参数配置

漏洞任务组数量：一个漏洞任务组中分配的 IP 数量，建议数量 50，可根据硬件配置适量修改

每组扫描并发数：同时扫描的任务数量，建议数量 10，可根据硬件配置适量修改

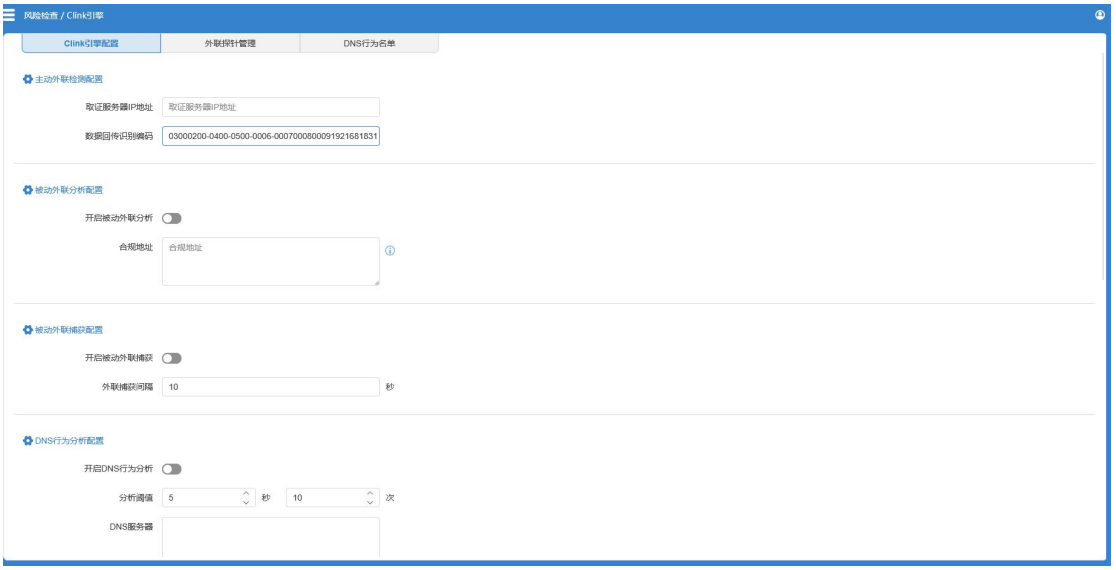
弱口令扫描配置：

弱口令扫描并发数：同时扫描的弱口令数量，建议数量 10-50，可根据硬件配置适量修改，注意：数值过大时，可能会导致弱口令扫描不出来。

5.6 Clink 引擎

5.6.1 Clink 引擎配置

点击【风险检查】-【Clink 引擎】进入 Clink 引擎页面，此页面可以进行主动外联、被动外联、违规 DHCP、私接路由以及双网互联的基础数据配置。如下图：



- 主动外联检测配置：

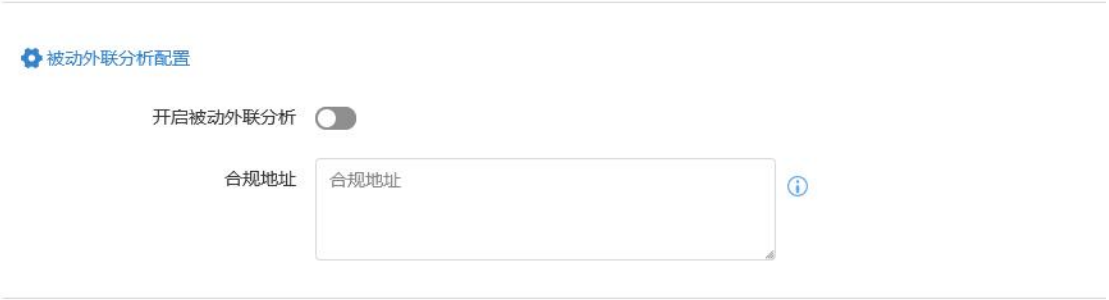


取证服务器 IP 地址：输入取证服务器地址

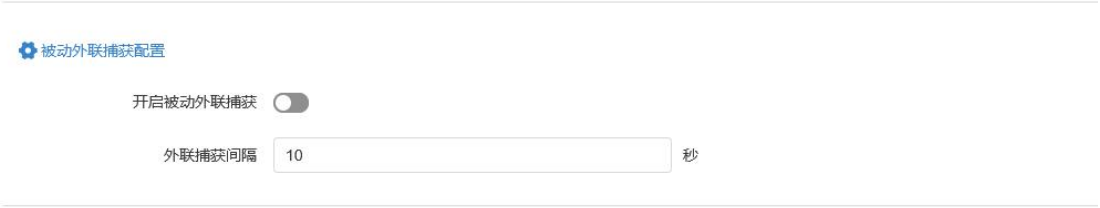
数据回传识别编码：系统自动生成的数据回传编码，具有唯一性，不可修改。将此编码添加至取证平台的【用户管理】－新建用户窗口的设备识别码处。

当系统进行边界风险扫描或客户端所在设备存在违规外联时，可检测到违规外联信息。

- 被动外联分析配置：



-
  - 前提条件需要在【系统配置】-【基础配置】页面配置可以正常应用的镜像采集口以及业务管理网口
  - 开启被动外联分析：当内网环境设备触发 http 或 https，并且流量通过配置的镜像口，则会被检测触发被动违规外联告警
  - 合规地址：设备触发的 http 或 https 的地址为合规地址中配置的 IP，则不会产生告警信息。
- 被动外联捕获配置



  - 开启被动外联捕获：内网环境下设备访问 http 的网址时，会触发被动外联捕获，获取到的违规外联信息会上传至违规外联取证平台
  - 外联捕获间隔：设置每次被动外联捕获之间的捕获间隔
- DNS 外联检测配置



- 开启 DNS 外联检测：开启后会检测内网环境下的设备进行的 dns 请求，不在白名单/黑名单的域名信息会被劫持，并产生违规外联信息。

注：被劫持的 dns 信息会记录到本地的 dns 缓存中，在缓存未更新的时间段中都无法访问此 dns。

- DNS 外联检测间隔：每次进行 dns 的外联检测间隔时间，建议设置 1 小时
- 检测方式：检测方式存在黑名单和白名单，设置域名信息，根据设置黑名单或者白名单，
  - 当域名信息为黑名单时，此域名信息请求会被劫持
  - 当域名信息为白名单时，此域名信息的请求不会被劫持，不在白名单内的都会被劫持

- 违规 DHCP 检测配置：



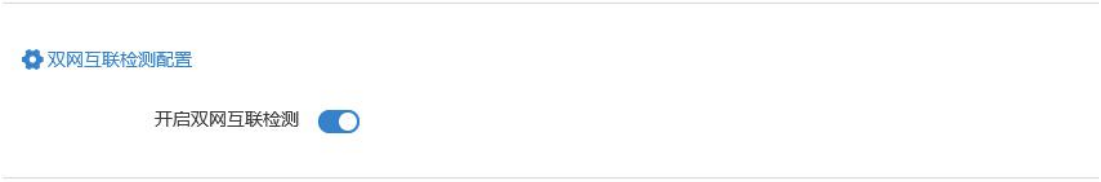
- 设置 DHCP 白名单，当被扫描边界风险策略的资产，开启了 DHCP 服务，且存在 DHCP 白名单中，则不会告警信息，不在白名单内的会产生违规告警信息

- 私接路由检测配置：



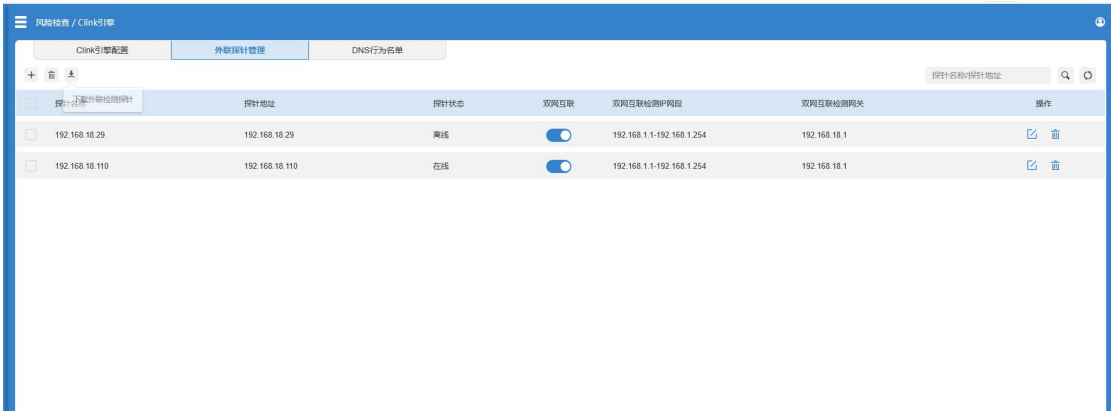
- 设置私接路由白名单，当被扫描边界风险策略的资产，存在路由设备，且此设备 IP 在白名单中的数据，则不会告警信息，不在白名单内的会产生告警信息

- 双网互联检测配置：在外联探针管理中进行外联探针配置，开启双网互联检测，存在双网互联时，会产生告警信息。



5.6.2 外联探针管理

点击菜单【风险检查】-【Clink 引擎】-【外联探针管理】页面，进入外联探针管理页面，此页面进行双网互联-外联探针基础配置，如下图：



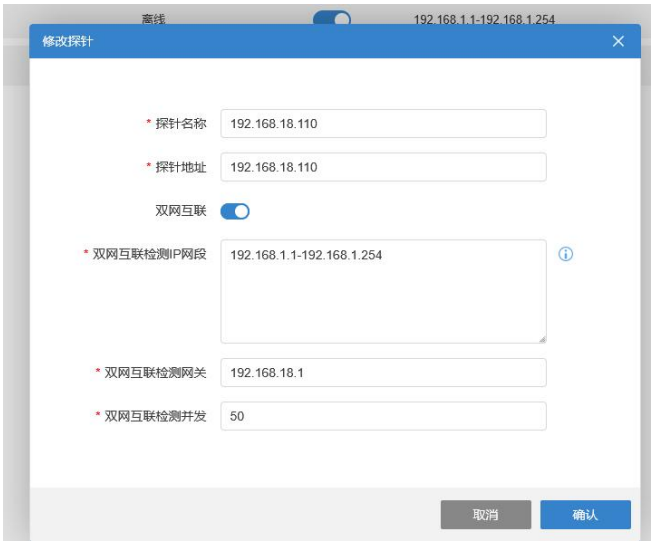
1、点击上方下载按钮，可下载外联探针引擎至本地

2、双击启动外联探针引擎

3、启动完成后，会在此路径下（C:\Program Files\external_insight_engine）生成文件 web.txt

4、进入此文件输入系统的 IP 地址、本机 IP 以及本机 mac 地址。

5、进入外联探针管理页面，点击 + 号按钮，新建外联探针配置



6、创建探针配置

(1) 探针名称：根据需要填写

(2) 探针地址：安装外联洞察引擎的设备 IP 地址

(3) 双网互联检测 IP 网段：需要检测的 IP 网段

(4) 检测网关：探针设备所在网关

(5) 双网互联检测并发：同时检测的 IP 数量。

7、创建完成，等待此配置的探针状态变为在线

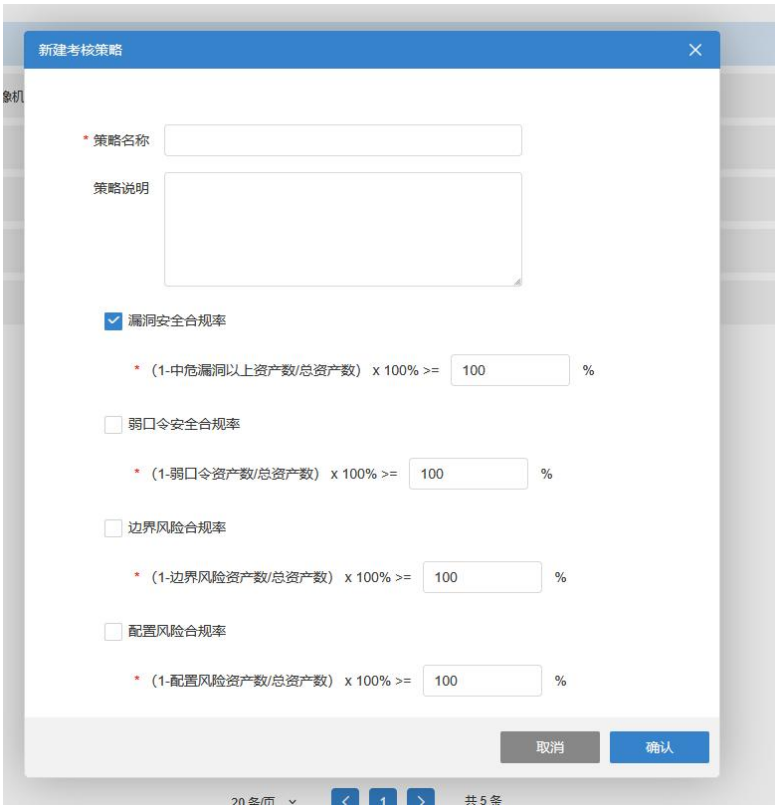
8、探针设备访问 http 的地址，告警事件中会出现告警信息。

5.7 考核策略库

点击菜单【风险考核】-【考核策略库】进入考核策略页面，此页面支持新增自定义配置考核策略并以列表展示系统中所有默认考核策略和自定义策略。如图 2.7-3 所示：



用户点击左上角+号，进入新建考核策略页面，页面内容包括策略名称，漏洞安全合规率、弱口令安全合规率和边界风险合规率，如图 2.7-4 所示：



其中策略名称为必填项，漏洞安全合规率、弱口令安全合规率、边界风险合规率和配置风险合规率为选填项；

用户勾选漏洞、弱口令、边界风险合规率或配置风险合规率时，则对应的合规率考核数值为必填项；

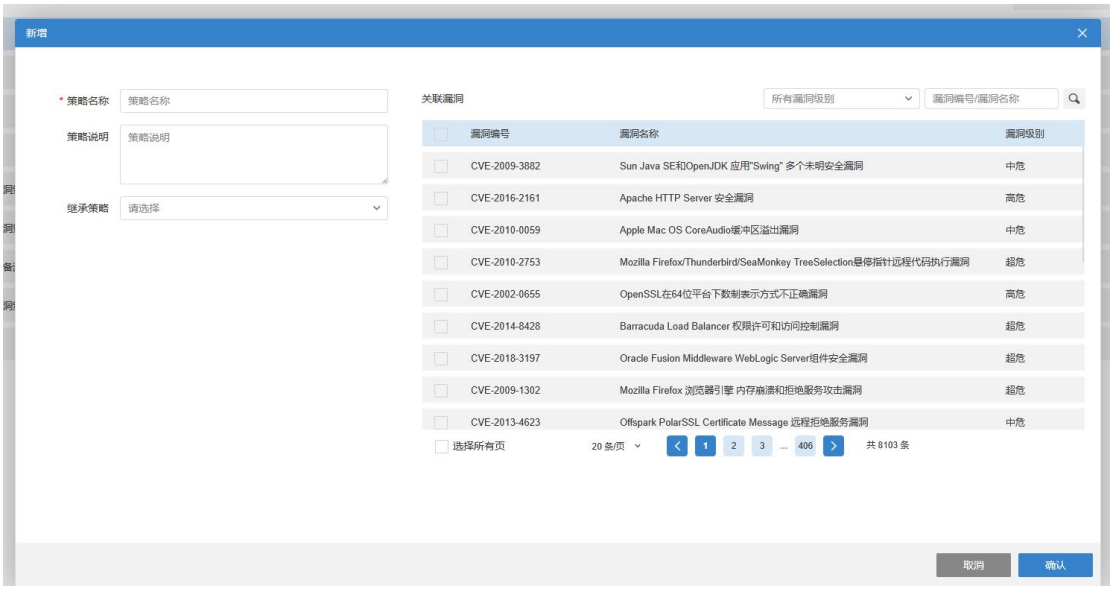
扫描任务选择考核策略时，符合策略中配置的合规率，考核结果则为合格，反之为不合格。

5.8 漏洞策略库

点击菜单【风险检查】-【漏洞策略库】，进入漏洞策略库，此页面展示系统中默认的漏洞策略，如图 2.6-11 所示：



点击　按钮，自定义创建漏洞策略，如下图：



1、输入策略名称

2、选填策略说明

3、选填继承策略，选择继承策略后，关联漏洞处会自动勾选继承策略中的所有漏洞。

4、选择关联漏洞

5、点击确定，漏洞策略创建成功，添加方式为手动添加

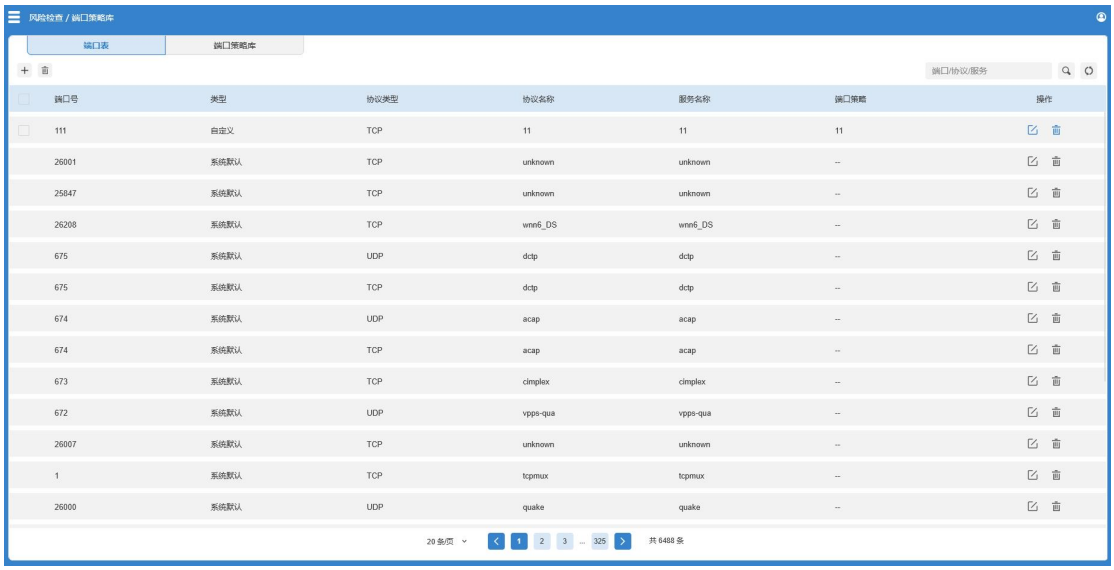
6、创建扫描任务时，选择此策略，会根据选择的漏洞进行漏洞扫描

7、关联扫描任务列存在数据时，此策略不允许删除

5.9 端口策略库

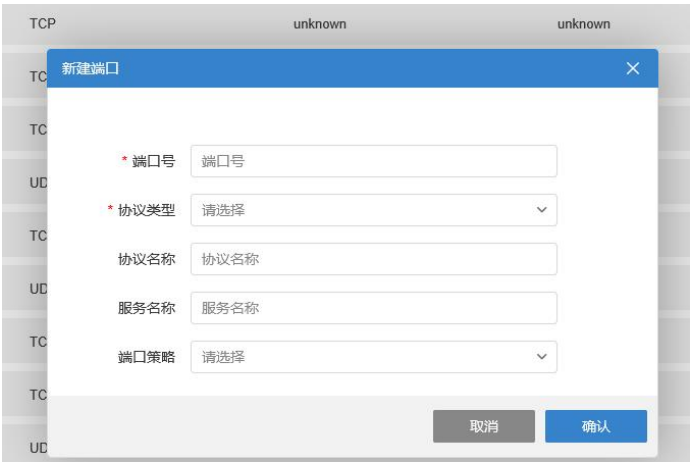
- **端口表**

点击菜单【风险检查】-【端口策略库】-【端口表】，进入端口表页面，此页面展示端口策略中所有的端口号，如图 2.6-12 所示：



点击左上角+按钮，进入新建端口页面，端口号和协议类型为必填项目，协议名称，服务名称和端口策略为选填项目，图 2.6-13 所示；

输入端口号，选择协议类型，输入协议名称，输入服务名称，选择端口策略，其中端口策略展示端口策略库中全部的端口策略，点击提交，端口创建成功。



选择端口策略的端口号，成功进入所选端口策略中对应协议类型的输入框中；

新增的端口号，右侧操作栏支持删除和编辑操作。点击删除按钮，新增端口号可被删除。点击编辑按钮，可编辑端口信息；

新增的端口号，上方按钮支持新增、批量删除、批量导出操作以及根据端口/协议/服务进行模糊查询操作。

- **端口策略库**

点击菜单【风险检查】-【端口策略库】点击端口策略库，进入端口策略库页面，此页面以列表形式展示系统中所有的端口策略包括系统默认策略和自定义策略，如图 2.6-14 所示：



用户点击左上角+号，弹出新增端口策略页面，如图 2.6-15 所示。其中端口策略名称为必填项，继承策略，TCP 端口和 UDP 端口为选填项目；

继承策略：继承策略以下拉框形式展示所有已创建的端口策略，点击任意一个端口策略，会自动继承此端口策略的 TCP 端口和 UDP 端口；

新增端口策略页面根据需要手动输入 TCP 端口号和 UDP 端口号，此端口号会自动出现在端口表页面，端口策略列默认显示此端口策略名称。



自定义端口策略，右侧操作栏支持删除和编辑操作。点击删除按钮，自定义端口策略可被删除。点击编辑按钮，可编辑端口策略信息；

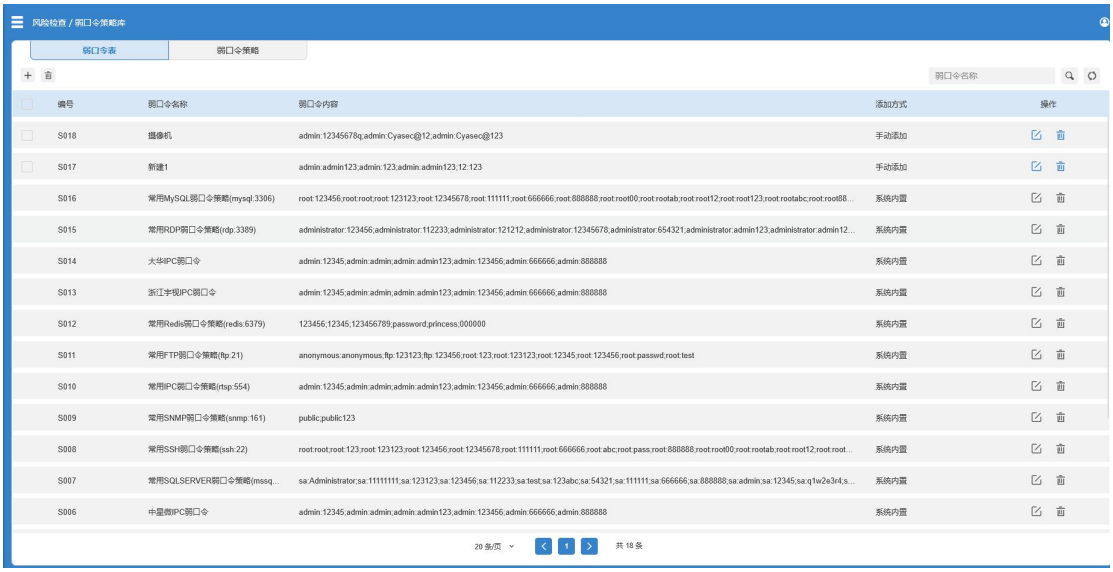
自定义端口策略，上方按钮支持新增、批量删除、批量导出操作以及根据端口策略名称进行模糊查询操作。

关联扫描任务列存在数据时，此策略不允许删除

5.10 弱口令策略库

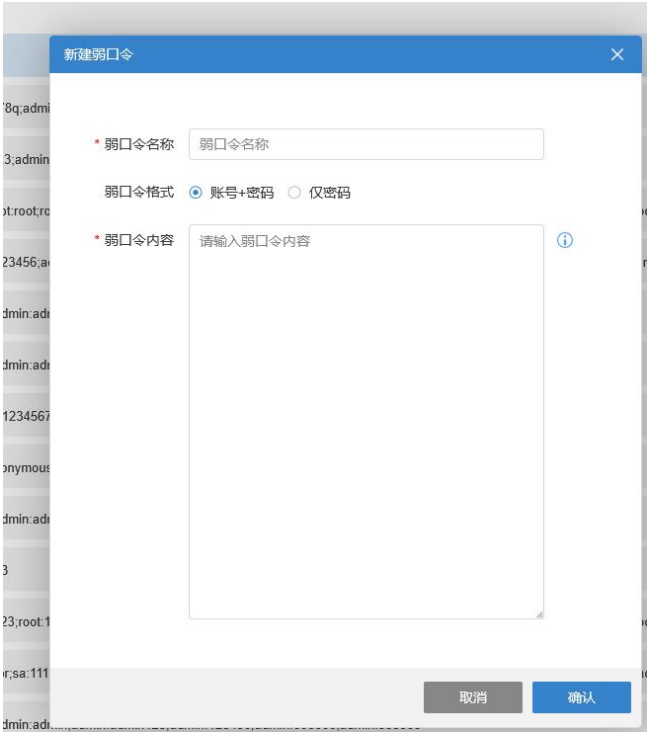
- **弱口令表**

点击菜单【风险检查】-【弱口令策略库】，进入端口表页面，此页面以列表形式展示系统中所有的默认弱口令和自定义弱口令，如图 2.6-16 所示：



点击左上角+按钮，进入新建弱口令页面，弱口令名称和弱口令内容为必填项目，弱口令格式默认选择“账号+密码”可根据需要更改，如图 2.6-17 所示；

输入弱口令名称，选择弱口令格式，根据选择的格式输入弱口令内容，点击提交，弱口令创建成功，进入新增弱口令策略页面，创建的弱口令成功出现在“引用弱口令表”中。



新增的端口号，右侧操作栏支持删除和编辑操作。点击删除按钮，新增端口号可被删除。点击编辑按钮，可编辑端口信息；

新增的端口号，上方按钮支持新增、批量删除、批量导出操作以及根据弱口令名称进行模糊查询操作。

- **弱口令策略**

点击菜单【风险检查】-【弱口令策略库】-【弱口令策略】，进入弱口令策略页面，此页面以列表形式展示系统中所有的弱口令策略包括系统默认策略和自定义策略，如图 2.6-18 所示：



用户点击左上角+号，弹出新增弱口令策略页面，如图 2.6-19 所示。其中弱口令策略名

称和引用弱口令表为必填项，继承策略为选填项目；

继承策略：继承策略以下拉框形式展示所有已创建的弱口令策略，点击任意一个弱口令策略，会自动继承此策略引用的弱口令。



自定义弱口令策略，右侧操作栏支持删除和编辑操作。点击删除按钮，自定义弱口令策略可被删除。点击编辑按钮，可编辑弱口令策略信息；

自定义弱口令策略，上方按钮支持新增、批量删除、批量导出操作以及根据弱口令名称进行模糊查询操作。

关联扫描任务列存在数据时，此策略不允许删除

5.11 边界风险策略库

点击菜单【风险检查】-【边界风险策略库】进入边界风险策略页面，此页面支持新增自定义配置边界风险策略并以列表展示系统中所有默认边界风险策略和自定义策略。如图 2.6-20 所示：



用户点击左上角+号，进入新建边界风险策略页面，页面内容包括策略名称和边界风险检测。如图 2.6-21 所示：



其中策略名称、边界风险检测为必填项；

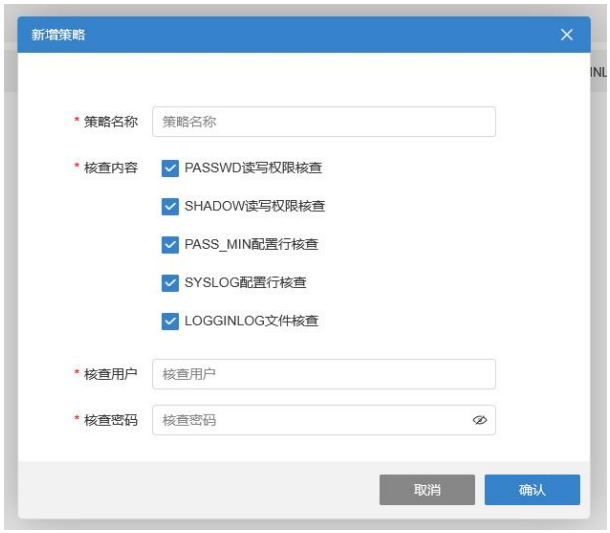
用户勾选边界风险检测方式，支持违规外联、多穴主机、私接路由、违规 DHCP 以及远程工具五种方式检测；

5.12 配置核查策略库

点击菜单【风险检查】-【配置核查策略库】进入配置核查策略页面，此页面支持新增自定义配置配置核查策略并以列表展示系统中所有默认配置核查策略和自定义策略。如图 2.6-20 所示：



用户点击左上角+号，进入新建配置核查策略页面，页面内容包括策略名称和配置核查检测。如图 2.6-21 所示：



其中策略名称、检测内容、核查用户和核查密码为必填项；

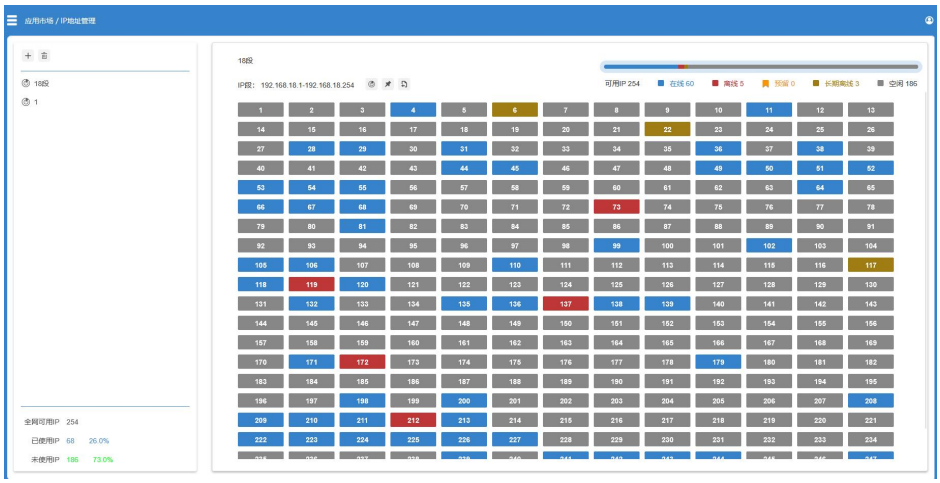
核查用户和核查密码为被检测服务器的用户名和密码；

用户勾选配置核查检测方式，支持 PASSWD 读写权限核查、SHADOW 读写权限核查、PASS_MIN 配置行核查、SYSLOG 配置核查、LOGINLOG 文件核查五项核查内容检测；

第 6 节 应用市场

6.1 IP 地址管理

点击菜单【应用市场】-【IP 地址管理】，进入 IP 地址管理界面，如图 2.11-1 所示，该功能界面可对 IP 地址进行管理，对设置的 IP 地址范围进行扫描，统计出该范围内可用地址、在线地址、离线地址、预留地址、空闲地址、长期离线地址等。



点击页面左上角“+”号，可以新建扫描任务，配置需要扫描的 IP 地址段，如图 2.11-2 所示：

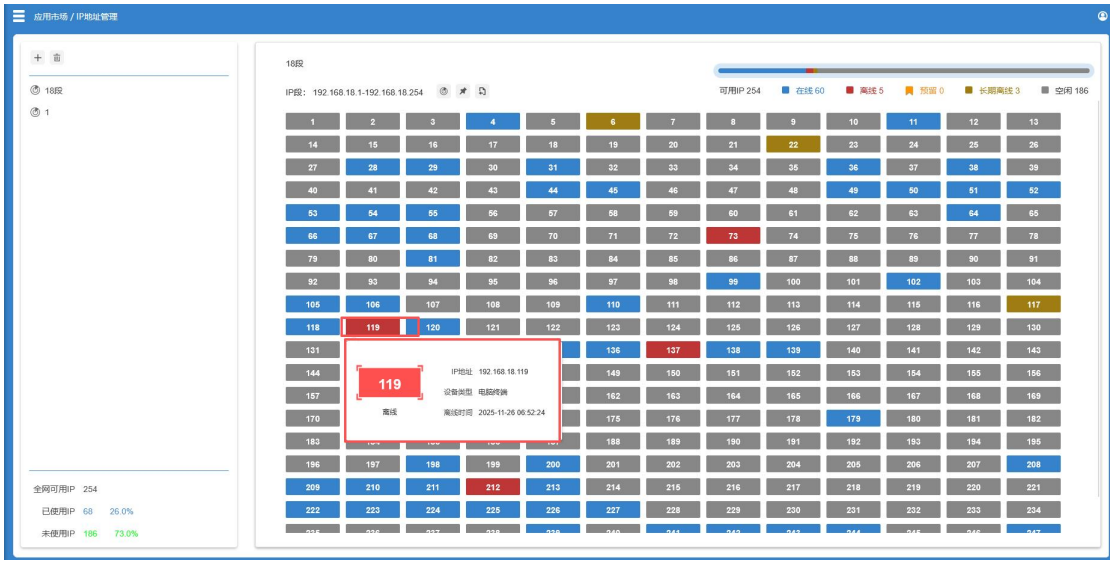


任务创建完成后在右侧展示框内点击扫描按键可以启动扫描任务；

选中 IP 地址，点击预留按键可以标记该地址，将地址设置为预留状态；

点击导出按键，可以将 IP 扫描结果导出，如图 2.11-3 所示：

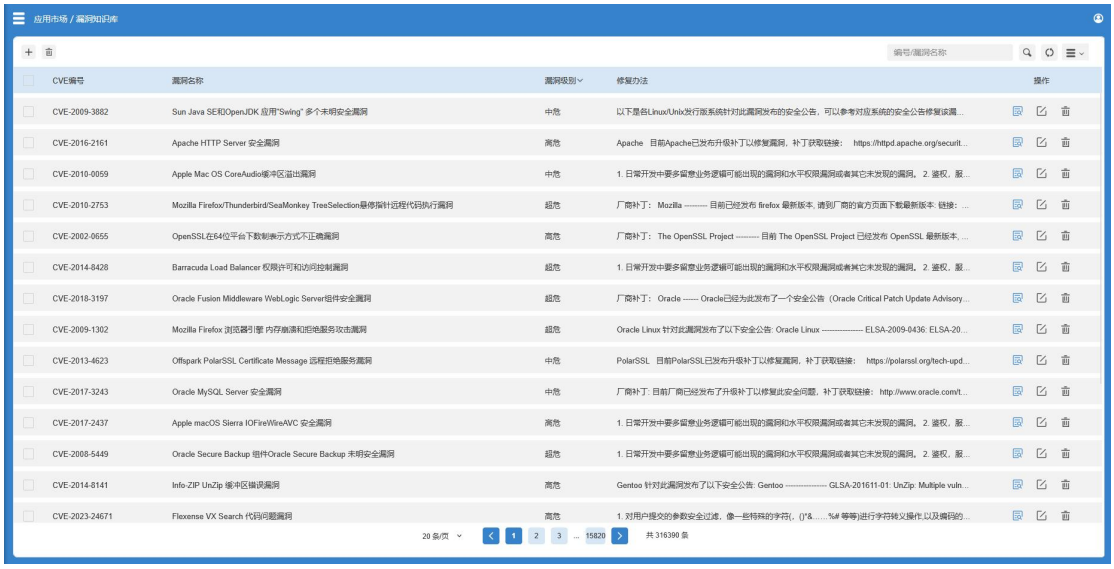
将光标选中在用的 IP 地址，可展示出此 IP 地址、设备类型、离线时间等内容。



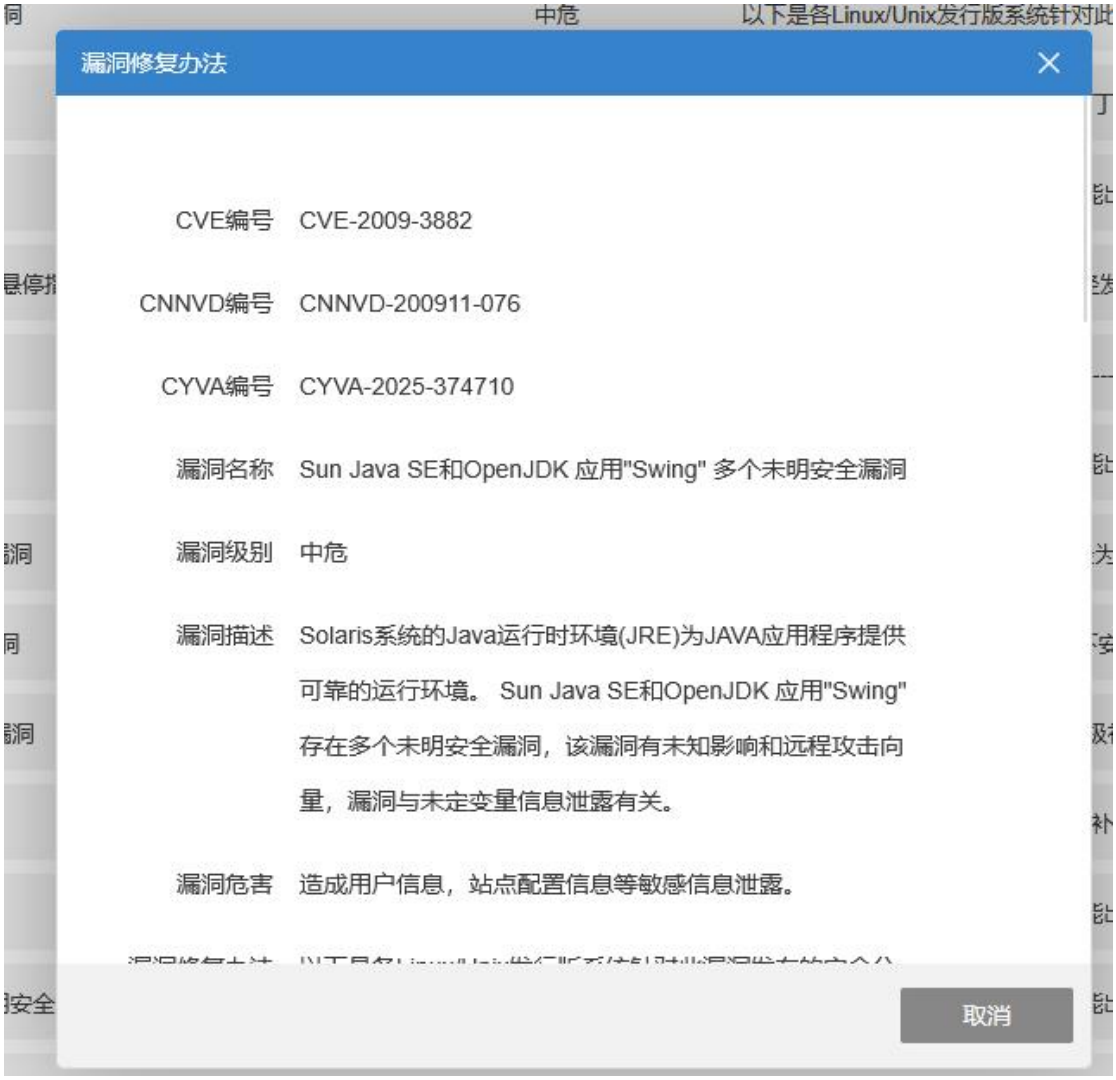
左下角显示：当前网段的下的可用 IP 数量以及已使用 IP 和未使用 IP 的统计结果。

6.2 漏洞知识库

点击菜单【应用市场】-【漏洞知识库】，进入漏洞知识库页面，此页面展示常见的漏洞信息包括漏洞编号，漏洞名称以及漏洞的修复办法。如下图所示。



点击操作列的详情按钮，弹出漏洞修复日志页面，此页面包括漏洞名称以及漏洞修复办法，如下图所示：



点击　按钮，弹出新建漏洞知识库窗口，如下图：



输入 CVE 编号、CNNVD 编号以及 CYVA 编码，输入漏洞名称，以及选填选择漏洞级别、漏洞描述、漏洞危害、漏洞修复办法，创建漏洞。

第 7 节 告警管理

告警管理模块，包括告警配置以及告警事件展示。

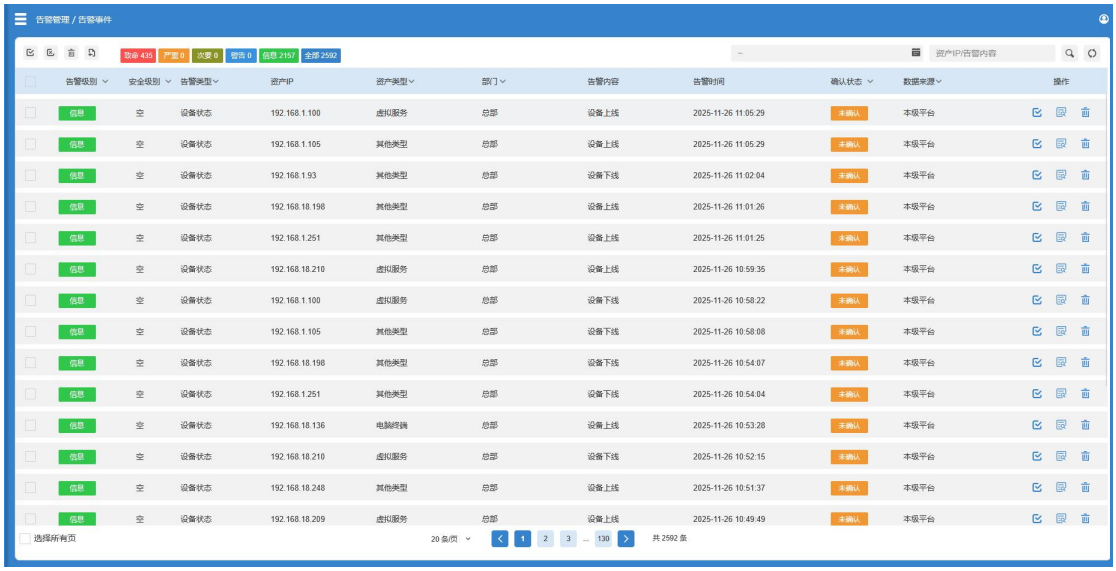
7.1 告警事件

点击菜单【告警管理】-【告警事件】，进入告警事件页面，如图 2.12-1 所示。

告警事件列表展示所有从信息到致命级别的告警事件，包括告警级别、告警类型、资产 IP、资产类型、部门、告警内容、告警时间、确认状态以及数据来源；

列表上方显示各告警级别的事件数量；

列表上方操作按钮可对告警事件进行批量确认，批量取消以及导出的操作，还可根据产生事件、资产 IP，资产名称等关键字进行搜索查询。



操作列提供确认按钮以及详情按钮，点击确认按钮后，告警事件状态由未确认变为已确认；

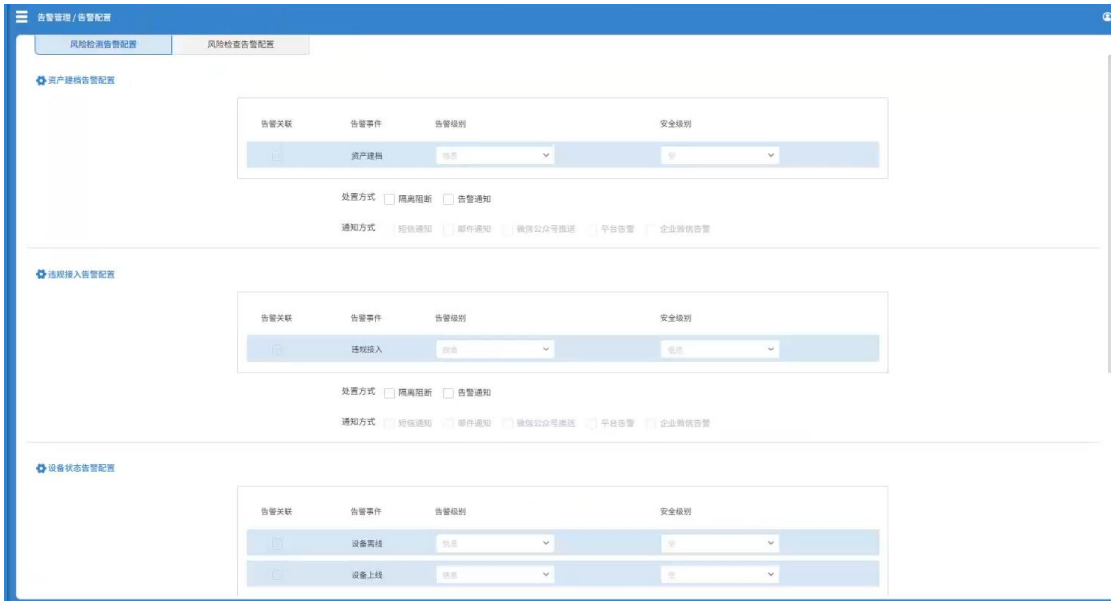
点击详情按钮，进入告警详情页面，展示当前资产下所有的告警信息，如图 2.12-3 所示。告警详情页面左侧展示资产信息包括资产名称，mac 地址，厂商等基础信息，右侧展示资产下所有的告警事件；

告警详情页面支持确认，取消，批量确认，批量取消以及根据事件，资产 IP，名称等关键字进行搜索筛选操作。



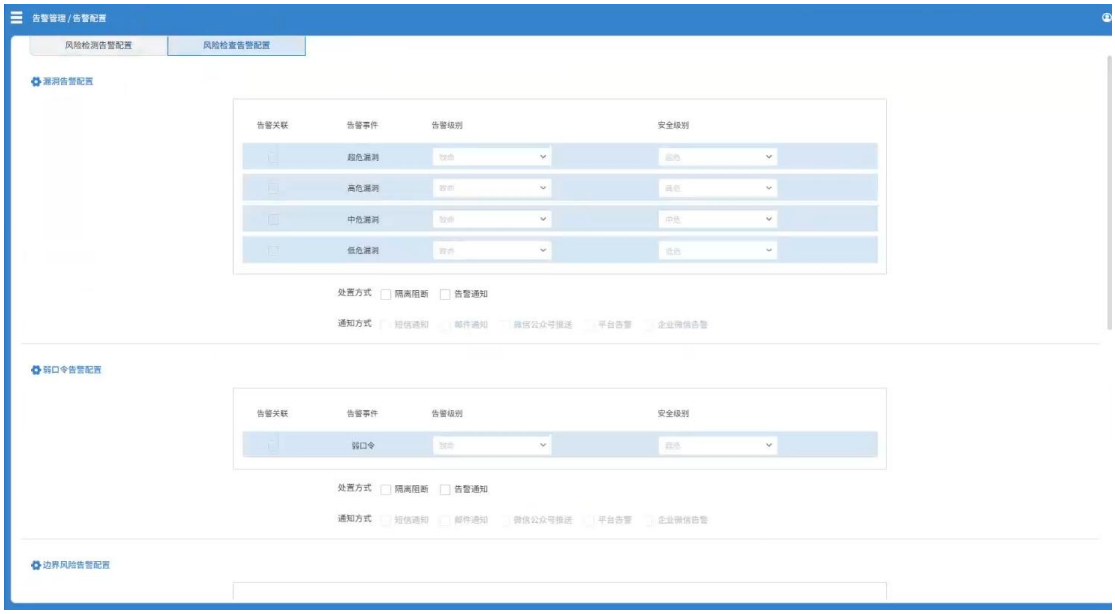
7.2 告警配置

点击菜单【告警管理】-【告警配置】-【风险检测告警配置】，进入告警配置页面，当前页面可对资产建档告警、违规接入告警、设备状态告警、伪冒替换告警进行处置方式以及通知方式配置。如图 2.12-4 所示：



点击菜单【告警管理】-【告警配置】-【风险检查告警配置】，进入告警配置页面，当前页面可对漏洞告警、弱口令告警、边界风险告警进行处置方式以及通知方式配置。如图所示：

扫描任务页面对资产进行风险扫描，可触发此页签的告警事件。



- 处置方式支持隔离阻断和告警通知两种方式；
- 告警设置页面可根据告警事件设置告警级别以及安全级别，达到此告警级别时，根据处置方式，会进行隔离阻断或告警通知；
- 隔离阻断：阻断后此设备无法接入网络，只勾选隔离阻断时，下方的通知方式置灰无法选中，
- 告警通知：勾选告警通知，下方四种通知方式可进行勾选，其中短信通知、邮件通知以及微信公众号通知的设置信息在菜单【系统配置】-【通知设置】中进行配置；
- 设备状态告警配置处置方式只支持告警通知一种；

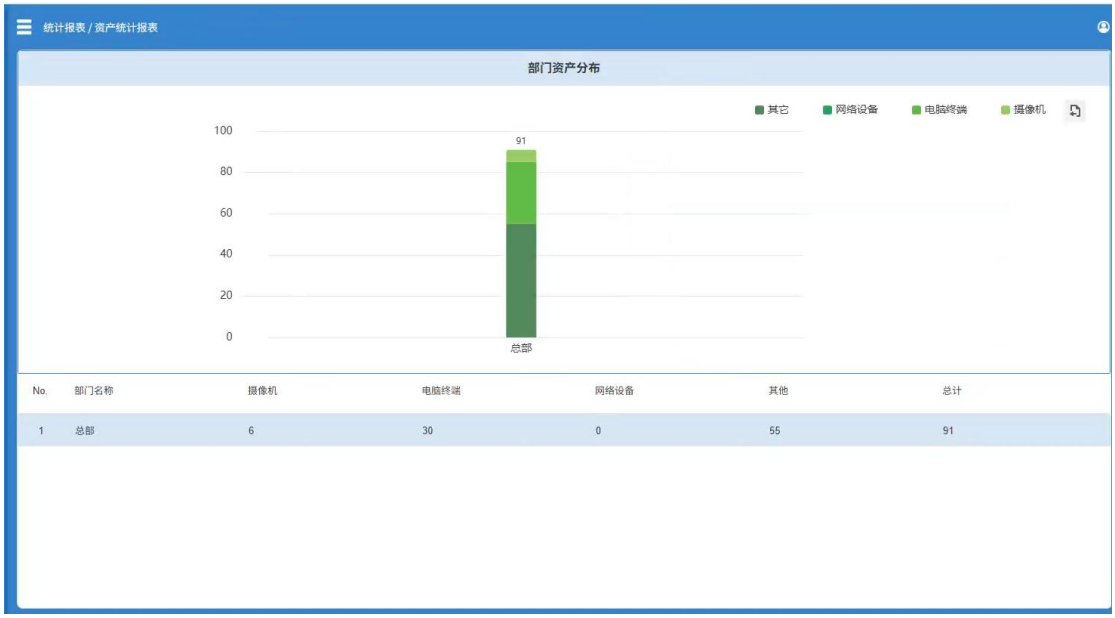
- 平台告警：会将告警信息发送至告警事件页面。

第 8 节 报表统计

该功能模块展示资产、风险、漏洞、AI 反拍照的统计报表。

8.1 资产统计报表

点击菜单【报表统计】-【资产统计报表】，进入资产统计报表界面，如图 2.13-1 所示，界面内展示了部门资产分布柱形图以及部门资产列表，列表包括编号、部门名称、摄像机、电脑终端、网络设备、其他以及总计



点击部门资产分布图右上角的导出按键，可以将报表内容导出。

8.2 资产在线报表

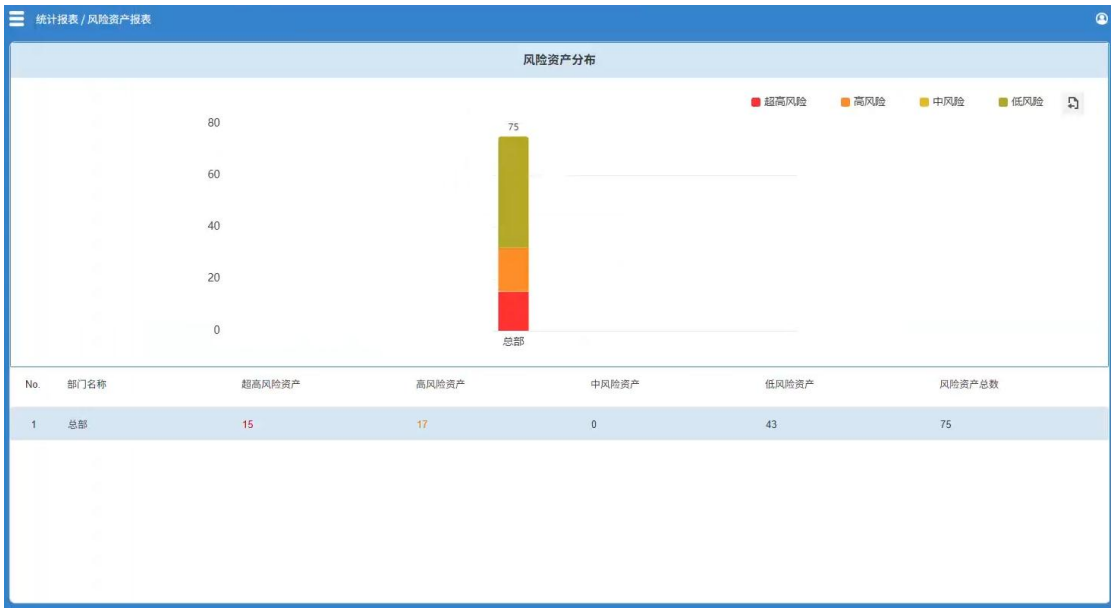
点击菜单【报表统计】-【资产在线报表】，进入资产在线报表界面，如图 2.13-3 所示，界面内展示了全部资产每天在线率的折线图以及资产在线的统计列表，列表包括部门名称、在线资产、离线资产、总资产、资产在线率等内容。



点击资产在线折线图右上角的导出按键，可以将报表内容导出。

8.3 风险资产报表

点击菜单【报表统计】-【风险资产报表】，进入风险资产报表界面，如图 2.13-6 所示，界面内展示了风险资产分布柱形图以及部门的风险资产列表，列表包括编号、部门名称、超高风险资产、高风险资产、中风险资产、低风险资产、风险资产总数等内容。



点击风险资产分布图右上角的导出按键，可以将报表内容导出。

8.4 漏洞统计报表

点击菜单【报表统计】-【漏洞统计报表】，进入漏洞统计报表界面，如图 2.13-8 所示，界面内展示了安全漏洞分布饼状图以及部门的漏洞信息列表，列表包括编号、部门名称、超

危漏洞、高危漏洞、中危漏洞、低危漏洞、漏洞总数等内容。



点击安全漏洞分布图右上角的导出按键，可以将报表内容导出。

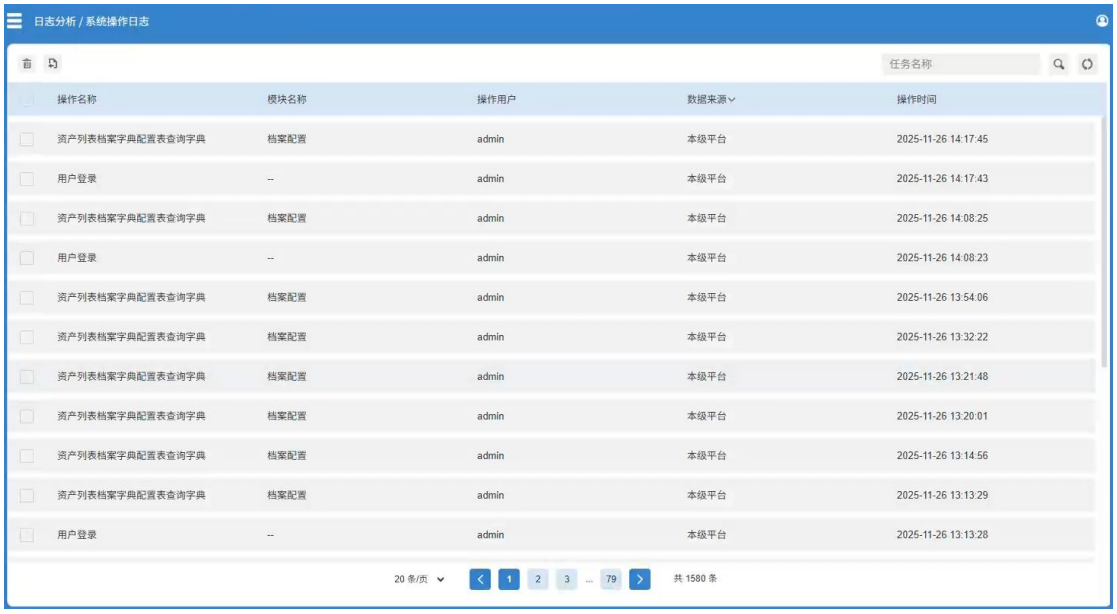
第 9 节 日志分析

此功能模块主要对各模块的日志进行记录、分析，其中包括终端登录日志、系统操作日志、终端操作日志、终端解密日志、终端外发日志、准入阻断日志等。

注：系统默认非系统管理员、超级管理员、管理员角色的用户，无法删除日志信息。

9.1 系统操作日志

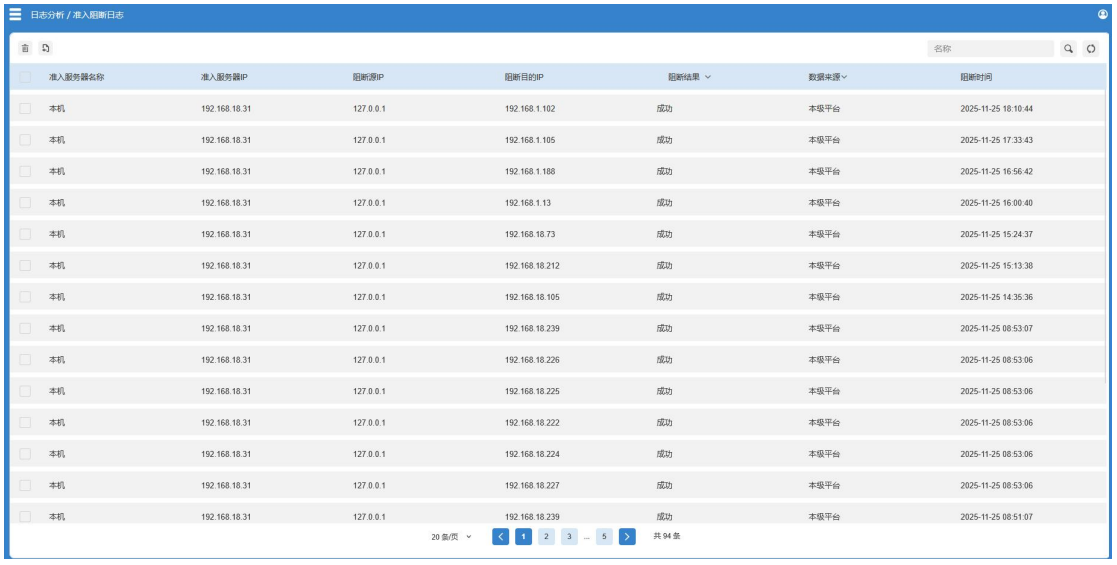
点击菜单【日志分析】-【系统操作日志】，进入系统操作日志界面，如图 2.14-2 所示，界面内展示了系统操作的信息列表，列表包括操作名称、模块名称、操作用户、数据来源、操作时间等内容。



在界面左上角可以点击删除按键删除日志以及通过导出按键将日志导出；

9.2 准入阻断日志

点击菜单【日志分析】-【准入阻断日志】，进入准入阻断日志界面，如图 2.14-6 所示，界面内展示了准入阻断的信息列表，列表包括准入服务器名称、准入服务器 IP、阻断源 IP、阻断目的 IP、阻断结果、阻断时间等内容。

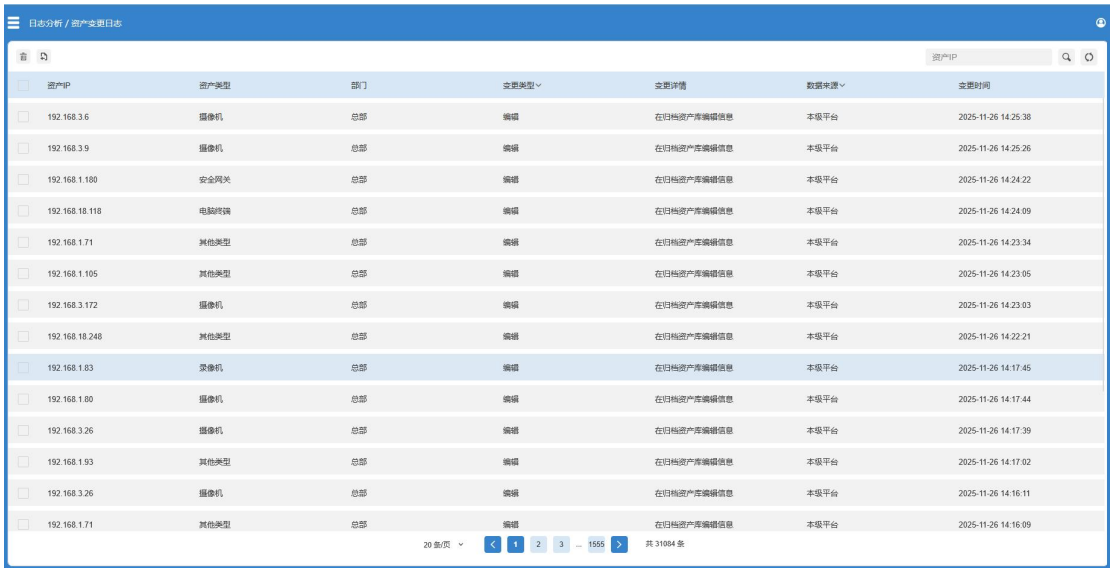


在界面左上角可以点击删除按键删除日志以及通过导出按键将日志导出；

在界面右上角可以通过输入日志名称进行搜索查询。

9.3 资产变更日志

点击菜单【日志分析】-【资产变更日志】，进入资产变更日志界面，如图所示，界面内展示了待录资产和归档资产库中资产变更的信息列表，列表包括资产 IP、资产名称、国标编码、变更类型、变更详情、数据来源以及变更时间等内容。

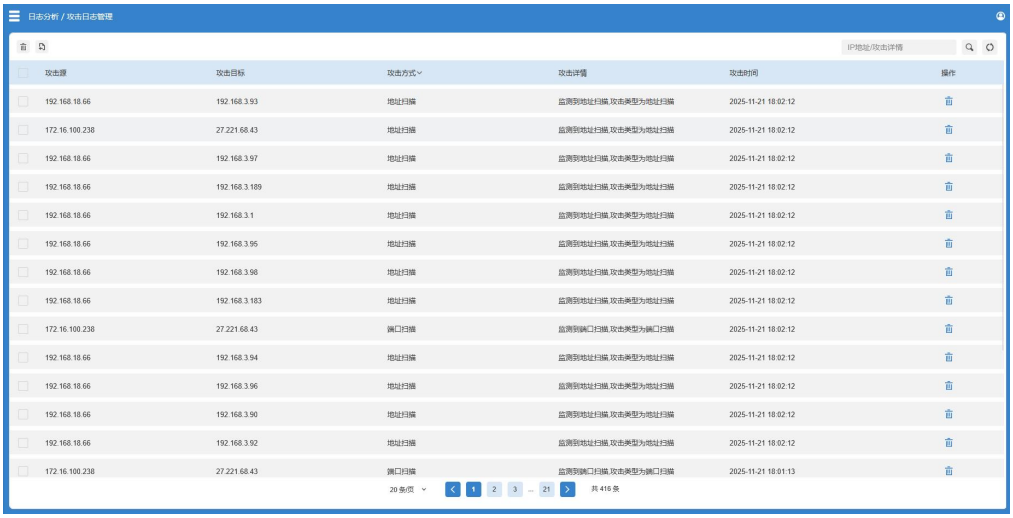


在界面左上角可以点击删除按键删除日志以及通过导出按键将日志导出；

在界面右上角可以通过输入资产 IP 进行搜索匹配查询日志；

9.4 攻击日志管理

点击菜单【日志分析】-【攻击日志管理】，进入攻击日志管理页面。此页面展示【漏洞防御】和【CIPS 引擎】中记录到的所有攻击日志信息。



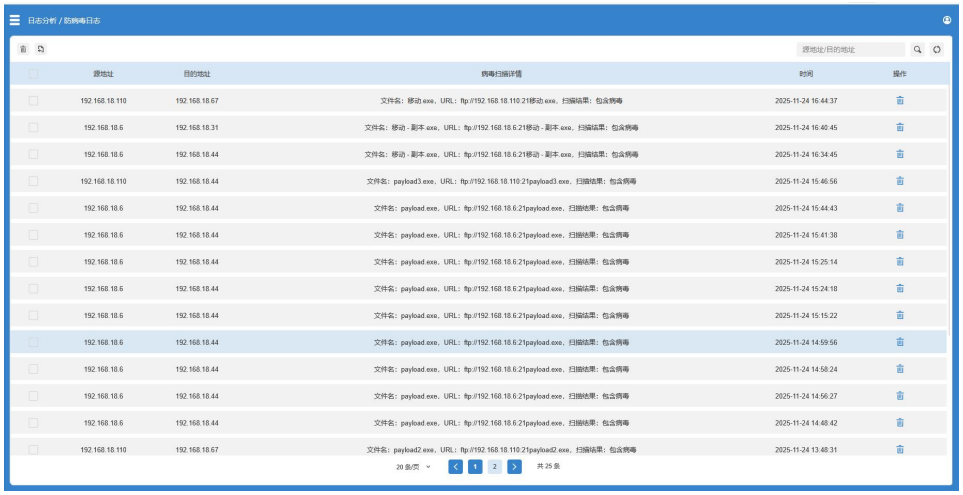
点击攻击方式可以根据攻击方式进行下拉筛选。

在页面左上角可以点击删除按键删除日志以及通过导出按键将日志导出；

在页面右上角可以通过输入 IP 地址以及攻击详情进行搜索匹配查询日志；

9.5 防病毒日志

点击菜单【日志分析】-【防病毒日志】，进入防病毒日志页面。此页面展示【病毒防护】中记录到的所有被检测到的攻击日志信息。



在页面左上角可以点击删除按键删除日志以及通过导出按键将日志导出；

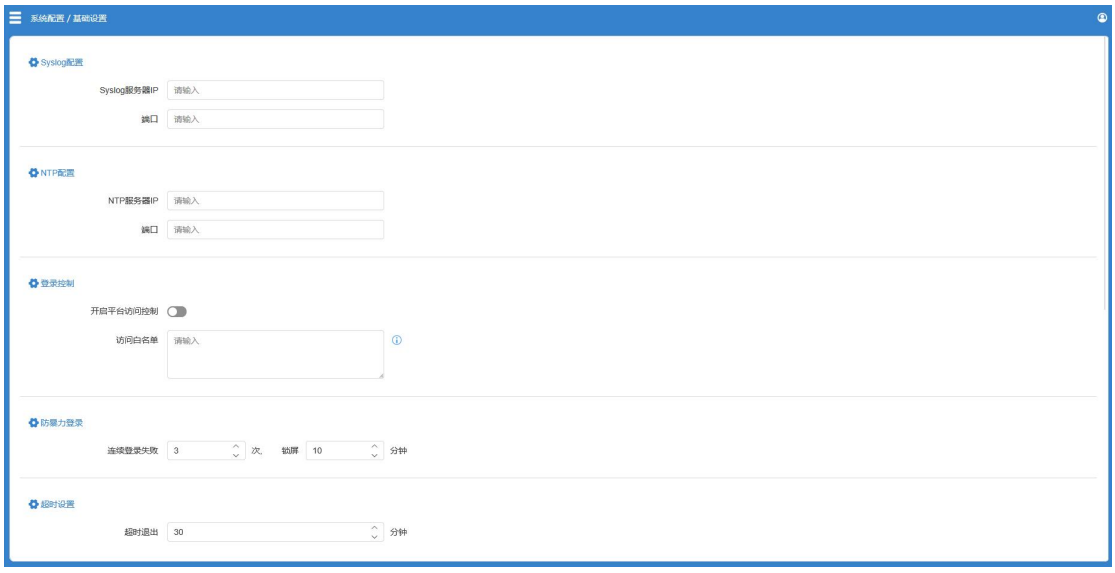
在页面右上角可以通过输入源 IP 地址以及目的地址进行搜索匹配查询日志；

第 10 节 系统配置

系统管理模块，包含基础设置、应用设置、用户部门、网络配置、通知设置、自定义页面、设备信息等。

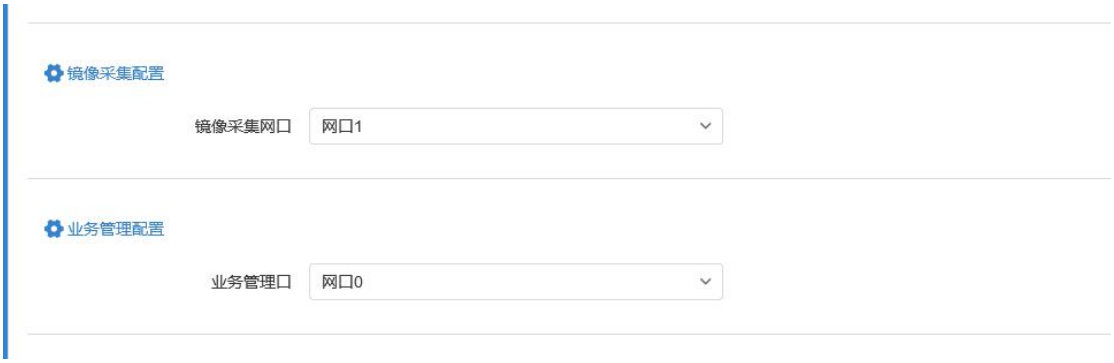
10.1 基础设置

点击菜单【系统配置】-【基础设置】，进入基础设置界面，该功能界面可以对 Syslog、NTP、登录控制、防爆力登录、超时设置、日志保存设置、镜像采集配置等功能进行配置，



镜像采集配置：当功能需要使用镜像时，需要在此镜像采集网口选择镜像网口。

业务管理口：在此处选择业务口



级联鉴权码：此处填写主级平台的级联鉴权码，主级平台与子级平台鉴权码匹配上后，可上报下发级联数据。

注意：保存基础配置，系统会重启。

10.2 用户部门

该功能模块可以对用户、角色、部门等模块进行配置；

10.2.1 用户管理

点击菜单【系统配置】-【用户部门】-【用户管理】，进入用户管理页面，用户列表包含昵称、登录名称和操作，最右侧操作栏，可对除管理员以及当前登录用户外的其他用户进行编辑或删除，如图 2.15-3 所示：



点击页面左上角“+”号，可新增用户。输入登录名称、昵称、用户密码，选择用户所属角色，点击提交，即可创建完成，如图 2.15-4 所示：



点击最右侧操作栏的”锁“图标，进入修改密码页面，可对用户进行修改登录密码和确认密码的操作。图 2.15-5 所示：



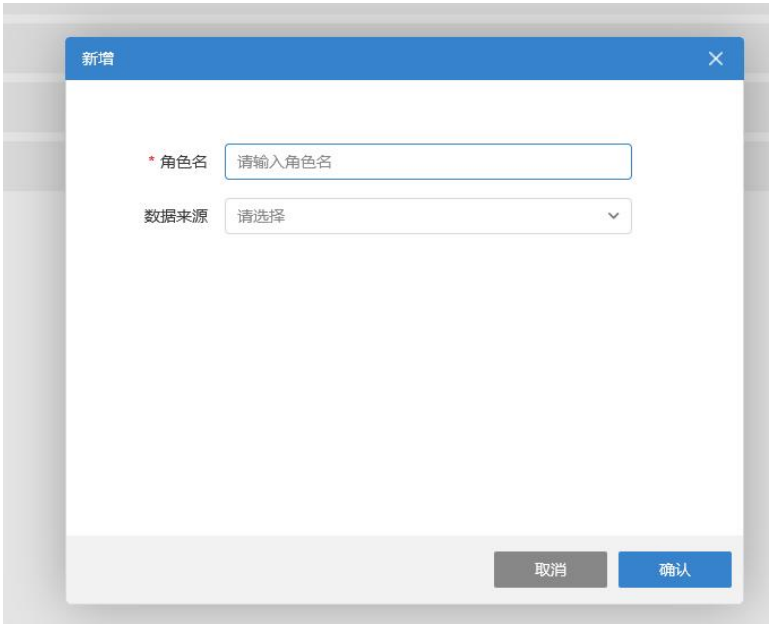
列表上方按钮可支持新增、删除、导出以及根据登录名称/昵称进行模糊查询操作。

10.2.2 角色管理

点击菜单【系统配置】-【用户部门】-【角色管理】，进入角色管理页面，列表包含角色名以及操作，最右侧操作栏，可对管理员普通用户进行编辑、授权、删除，如图 2.15-6 所示：



点击页面左上角“+”号，可新增角色。输入角色名称，点击确定，即可创建完成，如图 2.15-7 所示：



点击操作列中间授权图标，即可对角色设置相应的权限，系统默认角色不允许修改授权信息。

点击编辑按钮，可对新建角色进行修改名称操作；

点击删除按钮，可对角色进行删除操作；

10.2.3 部门管理

点击菜单【系统配置】-【用户部门】-【部门管理】，进入部门管理页面，部门列表包含部门名称、部门负责人、电话、邮箱、排序等信息，最右侧操作栏，可对部门进行编辑或删除操作，如图 2.15-8 所示：



点击左上角”+“号，可新增部门，部门名称为必填项，父级、部门负责人、电话、邮

箱、排序、部门资源网段为选填项。输入部门名称，点击提交，部门创建成功，如图 2.15-9 所示：



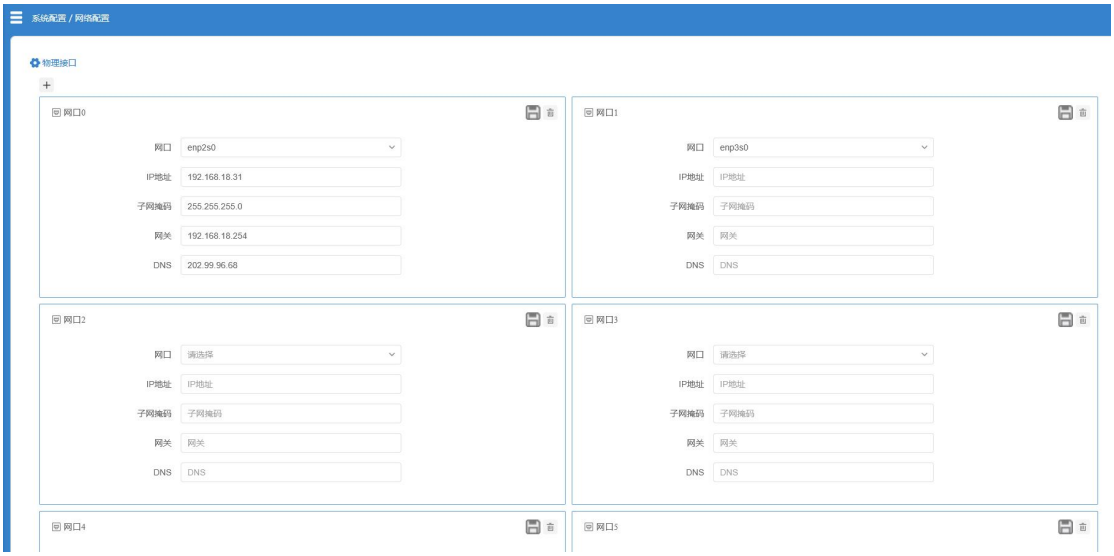
父级：父级下拉列表内容为所有已创建的部门，新增部门选择父级时，创建的新部门会成为此部门的子级；父级部门为空时，则创建的部门为一级部门。

点击右侧操作列表可对部门进行编辑和删除操作，点击左上角删除按钮，可进行批量删除操作。

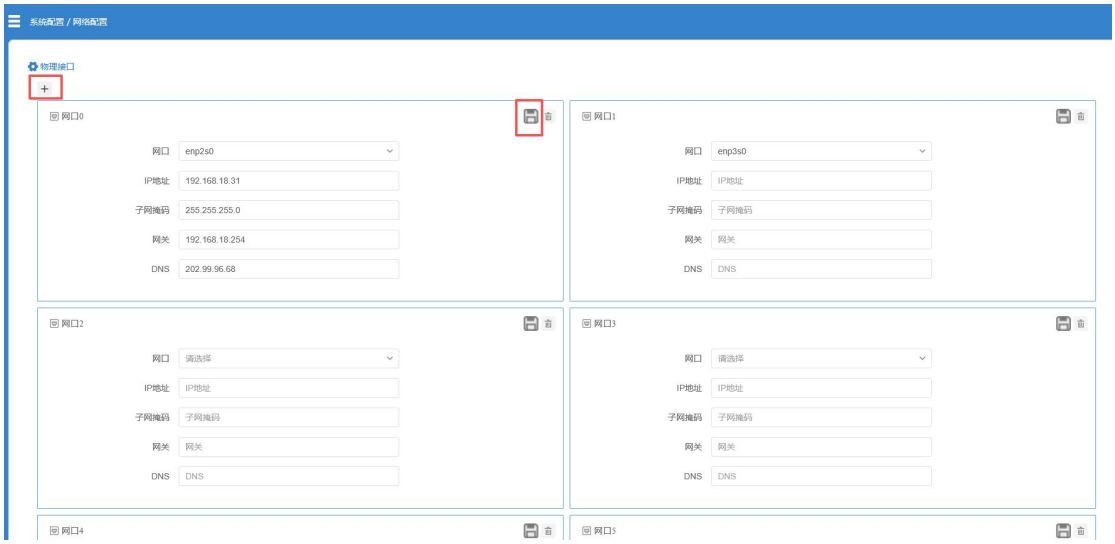
右上角输入部门名称，可根据名称进行搜索。

10.3 网络配置

点击菜单【系统配置】-【网络配置】，进入网络配置页面，该功能界面可以对物理接口、端口聚合、网桥管理等进行网络配置，如图 2.15-10 所示：



点击各模块左上角“+”按键可以新增物理接口、聚合口、网桥接口，根据内容配置 IP、掩码、网关、DNS 后点击右上角的“保存”按键即可，如图 2.15-11 所示：



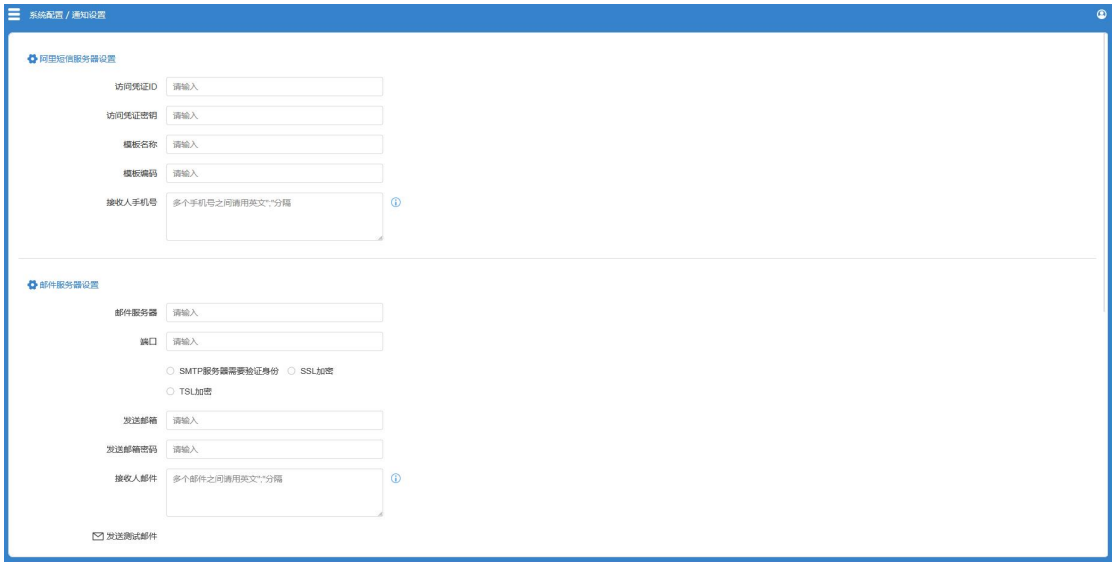
10.4 性能监控

点击菜单【系统配置】-【性能监控】，进入性能监控页面，该功能页面展示当前系统CPU/内存利用率、磁盘/算卡利用率、网卡上行流量以及网卡下行流量。如图所示：



10.5 通知设置

点击菜单【系统配置】-【通知设置】，进入通知设置页面，该功能界面可以对短信服务器、邮件服务器等进行配置，如图 2.15-12 所示：



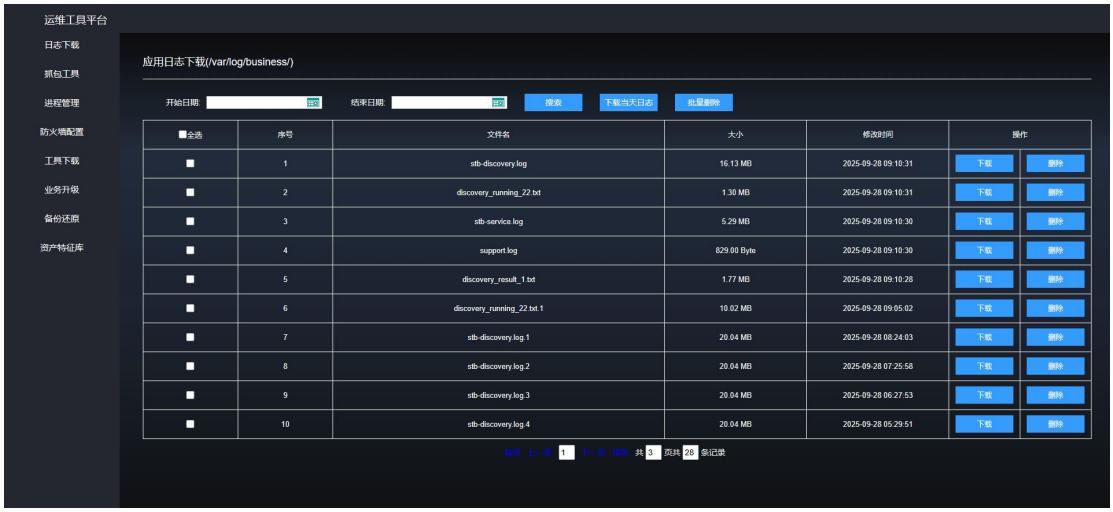
根据短信服务器、邮件服务器的配置内容输入并保存即可。

10.6 管理工具

点击菜单【管理工具】-【管理工具】，进入管理工具页面，该功能页面展示运维工具平台的跳转连接，如下图所示：

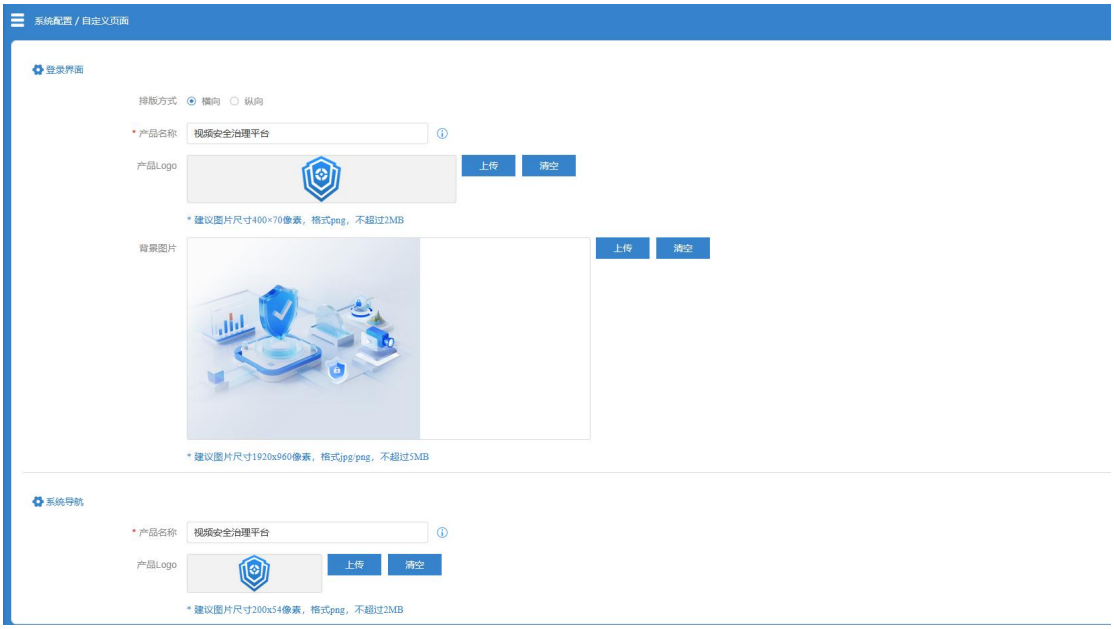


点击【运维工具平台】可跳转至【运维工具平台】系统中，可对系统进行日志下载、业务升级、备份还原等操作。



10.7 自定义页面

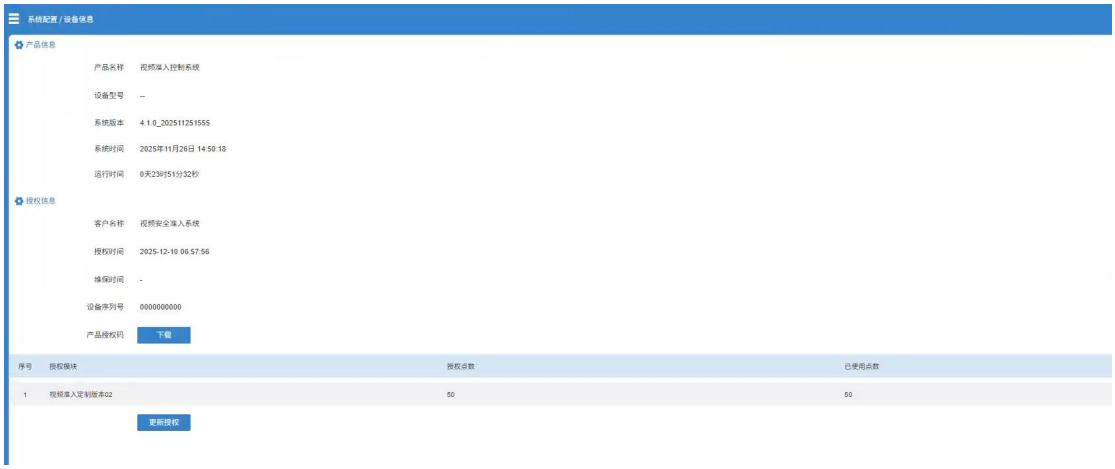
点击菜单【系统配置】-【自定义页面】，进入自定义页面，该功能界面可以对登录界面、系统导航、浏览器页签进行产品名称、Logo、背景图片、图标等进行修改及配置，如图 2.15-13 所示：



根据各模块信息的内容提示输入以及上传图片、图标后保存即可，保存后重新登录界面，配置更新。如未更新成功则清理浏览器缓存。

10.8 设备信息

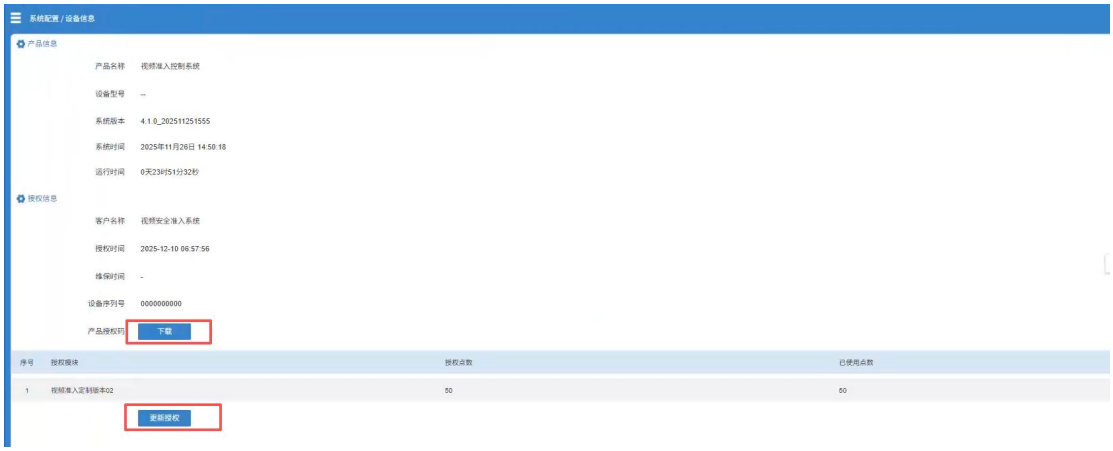
点击菜单【系统配置】-【设备信息】，进入设备信息页面，该功能界面展示产品信息、授权信息等内容，如图 2.15-14 所示：



产品信息模块包括产品名称、设备型号、系统版本、系统时间、系统运行时间等内容；

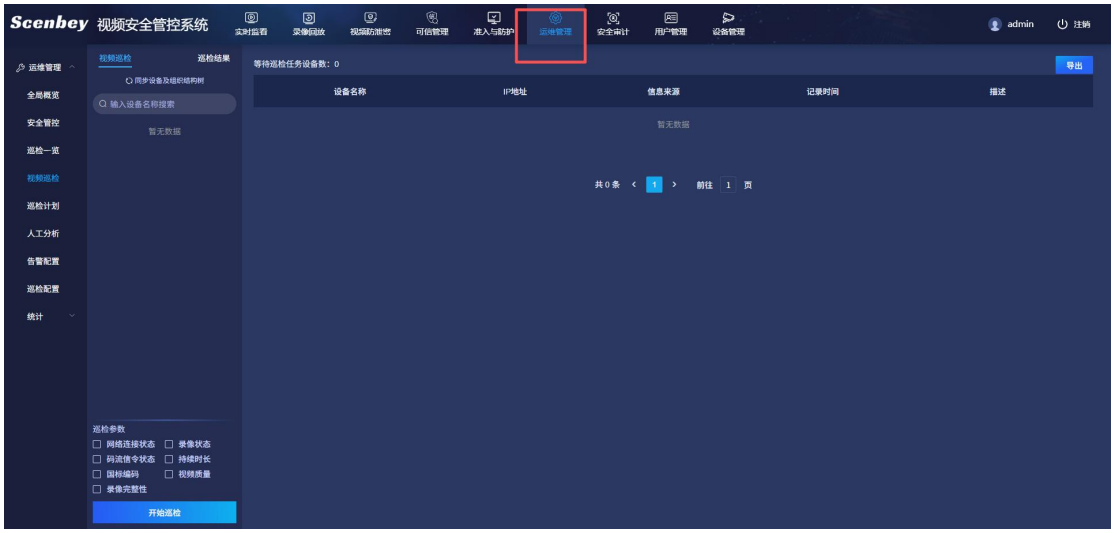
授权信息模块包括客户名称、授权时间、设备序列号、产品授权码，授权信息列表等内容；

授权更新：点击授权信息模块下的产品授权码旁边的下载按键，下载机器码，将机器码提供给我司技术工程师，得到授权码，获取授权码后点击更新授权选择授权码文件后即可更新完成，如图 2.15-15 所示：



第六章 运维管理

点击上方运维管理菜单，可进入运维管理界面。



第 1 节 查看整体状态

点击左侧全局概览菜单，可进入全局概览界面，查看整体信息。



第 2 节 查看隐患数据

点击左侧安全管控菜单，可进入安全管控界面，查看整体信息。

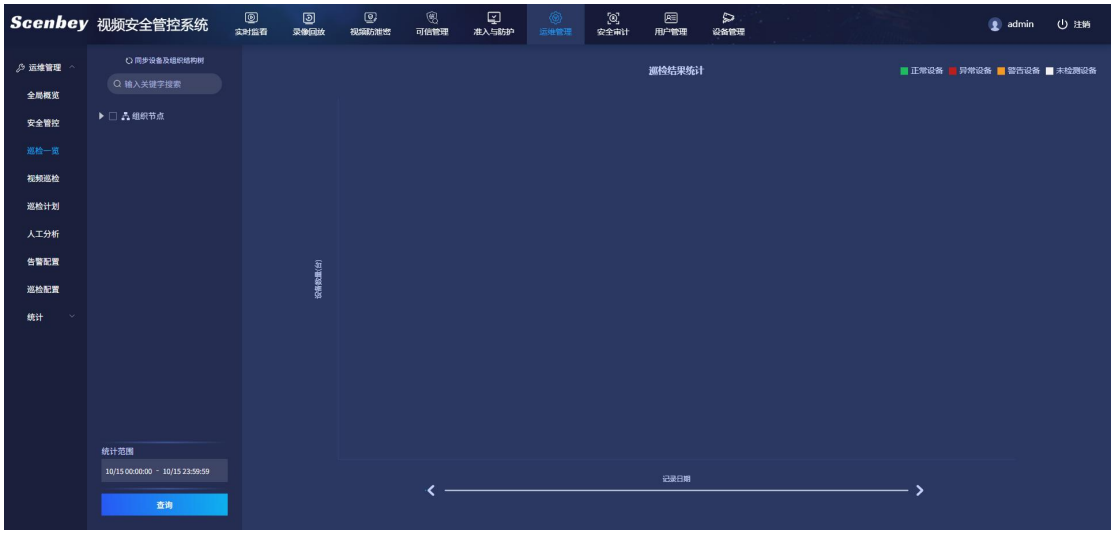


通过点击右上角齿轮菜单，可以查看配置信息。



第 3 节 巡检一览

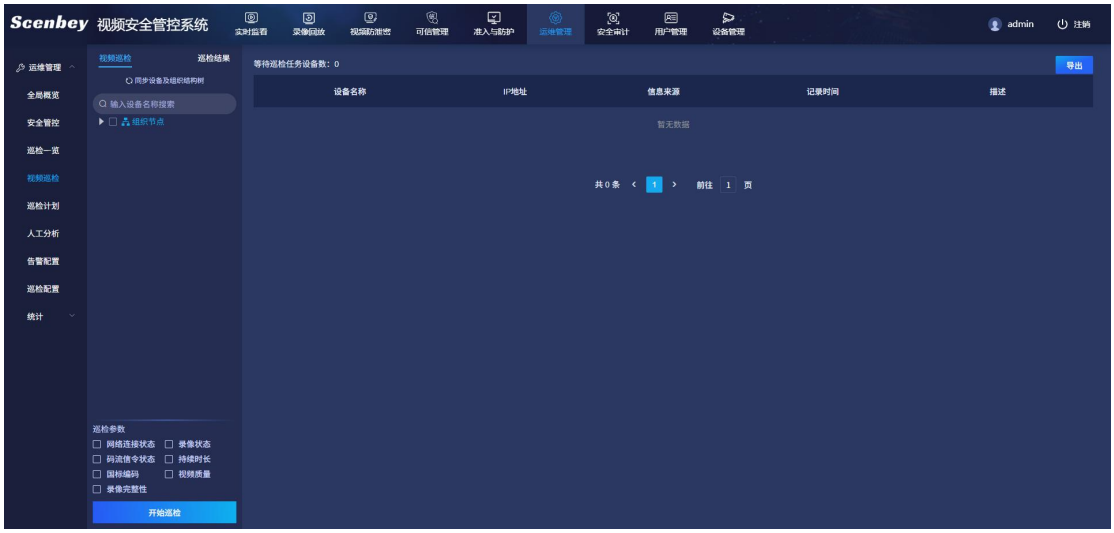
点击左侧巡检一览菜单，选择摄像头和日期范围，点击查询就能查看结果。



第 4 节 视频巡检

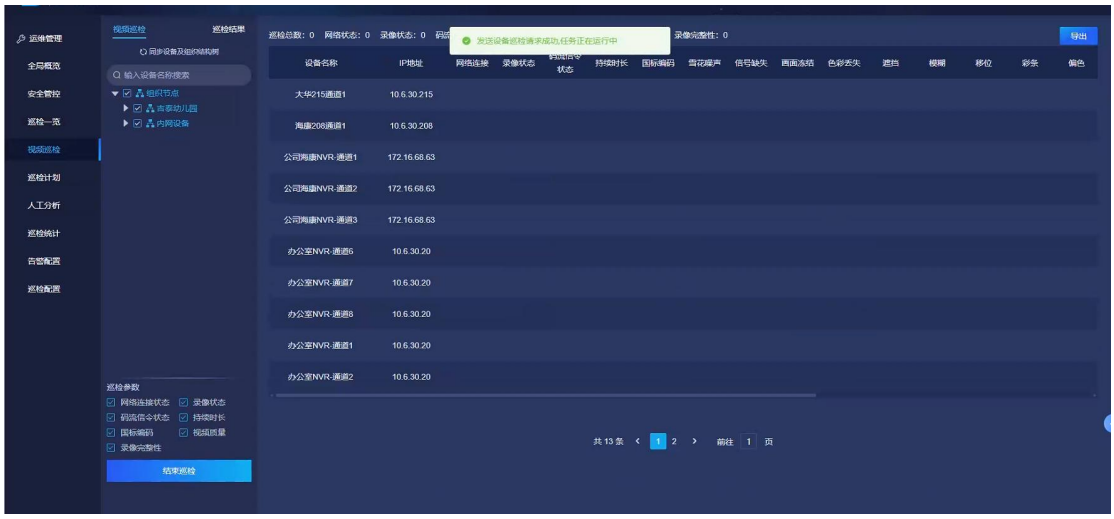
4.1 视频巡检

进入运维管理主界面后，点击左侧视频巡检菜单，进入视频巡检模块，如下图所示：



1、搜索：展开左侧组织结构树，点击复选框勾选需要巡检的设备，或在组织结构树上方输入框输入关键字进行搜索。

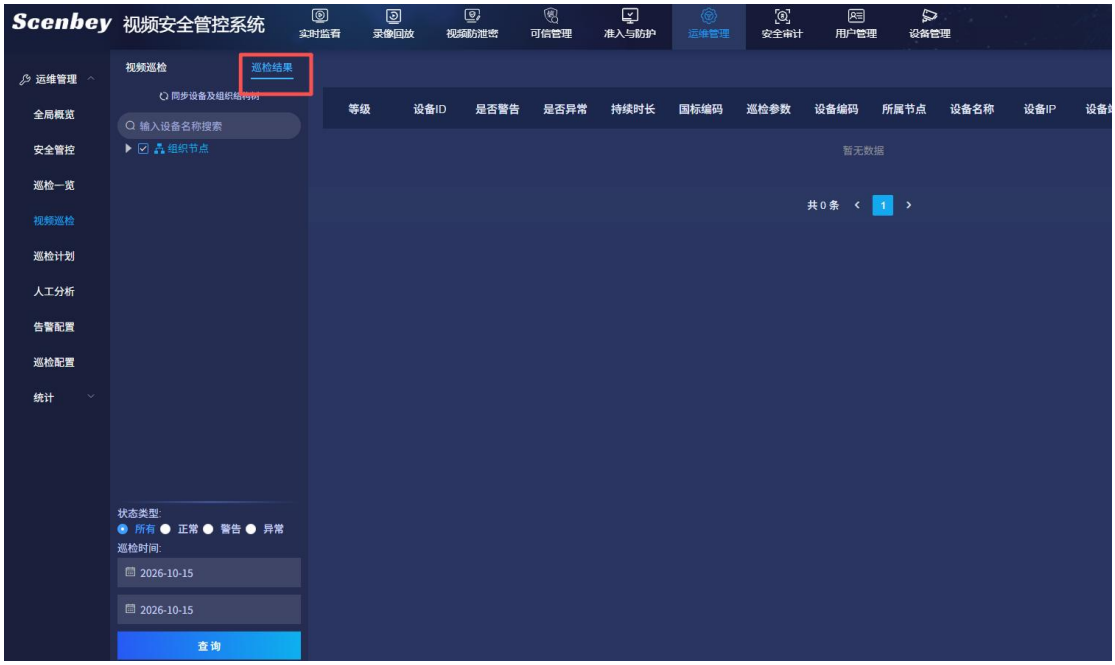
2、巡检参数：勾选左侧组织结构树下方需要巡检的参数，完成后点击开始巡检按钮，巡检完成后在右侧列表展示巡检结果，如下图：



点击导出按钮，即可导出所有巡检结果为 excel 表格格式

4.2 巡检结果

点击左侧上方巡检结果菜单，可查看设备的详细信息，如下图：



默认勾选视频巡检选择的设备，状态类型默认勾选所有，支持自定义状态类型，选择巡检类型和巡检时间段，



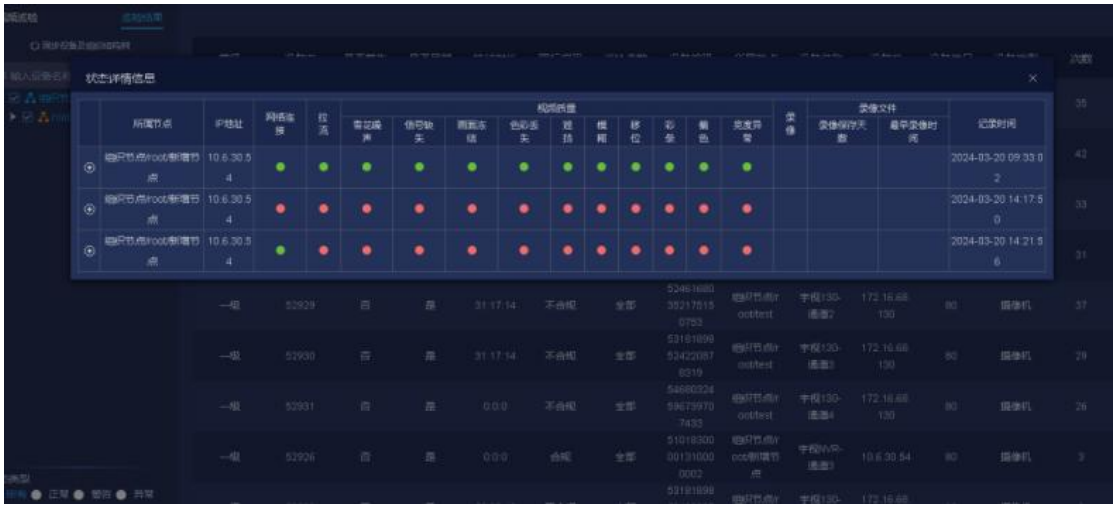
，点击

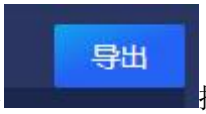


按钮，巡检结果如下图：



点击列表操作栏中详情按钮，可查看该设备的详情，如下图：



点击导出

按钮，即可导出所有巡检结果为 excel 表格格式

第 5 节 巡检计划

进入运维管理主界面后，点击左侧巡检计划，进入巡检计划模块，如下图所示：

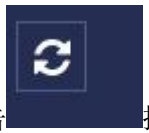


界面左侧为计划的增新增、编辑、删除、刷新区域

新增：点击按钮，即可创建一个新任务；

编辑：选中下方任务列表某一个任务后，点击按钮，即可修改该任务名称；

删除：选中下方任务列表某一个任务后，点击按钮，即可删除该任务；

刷新：点击按钮，刷新页面

5.1 创建巡检计划

点击按钮，创建一个新任务后，在界面中间组织结构树勾选需要创建巡检的

设备

，设备过多时可在输入框输入设备名称进行搜索

完成后在界面右侧配置巡检时间，支持自定义巡检时间、按周巡检或者按月巡检，如下图：



巡检时间选择配置完成后再对巡检参数进行配置，包含：网络连接状态、录像状态、码流信令状态、视频质量、持续时长、国标编码、录像完整性等，如图：



完成后点击

按钮，新增计划成功。

第 6 节 人工分析

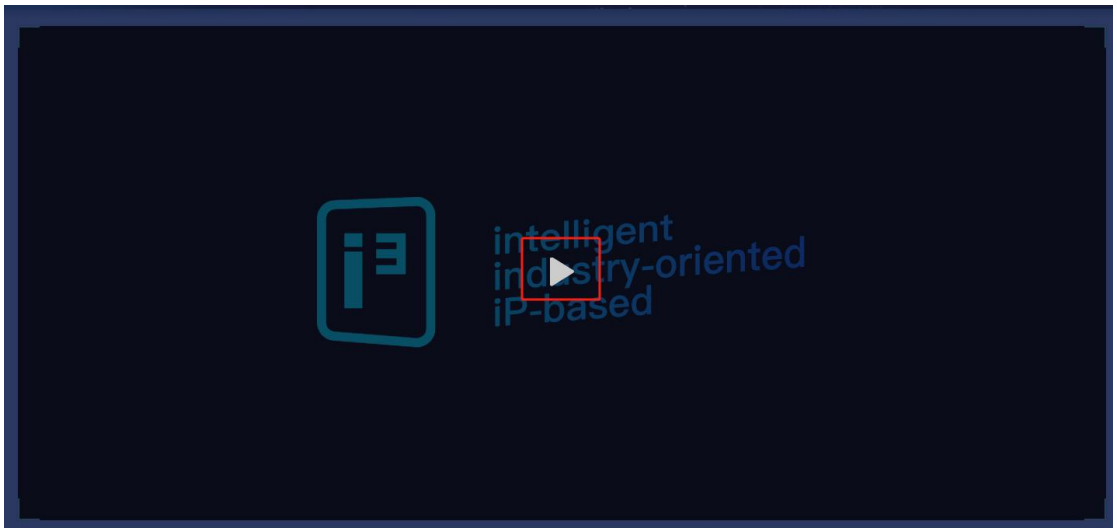
进入运维管理面后，点击左侧人工分析，进入人工分析模块，如下图所示：

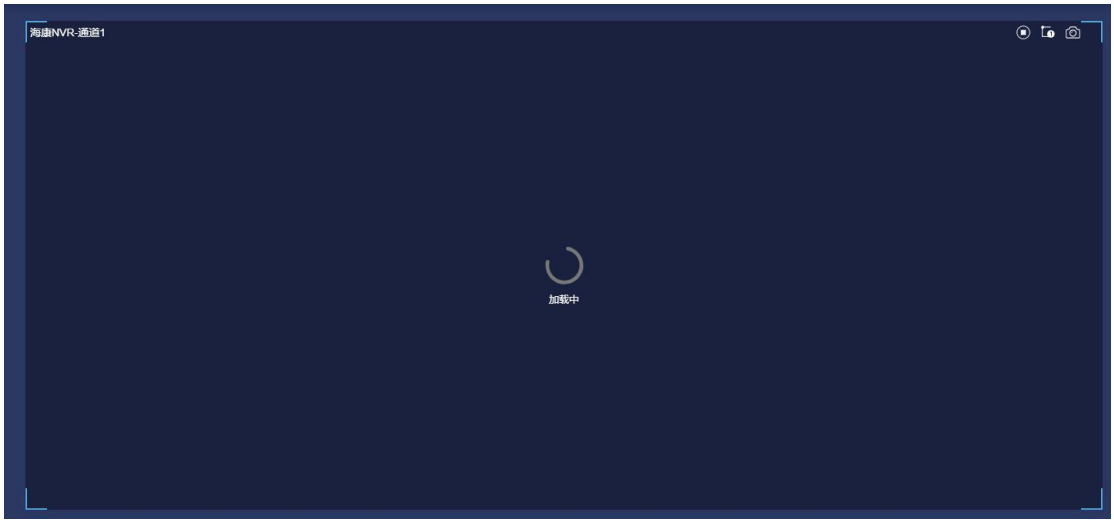


勾选左侧组织结构树需要进行分析的设备，



鼠标悬浮到播放窗口，点击播放按钮，即可从组织结构树勾选的设备依次播放





点击播放窗口上图标停止播放视频，点击可切换主码流或者子码流

，点击图标可截屏抓帧保存到本地。

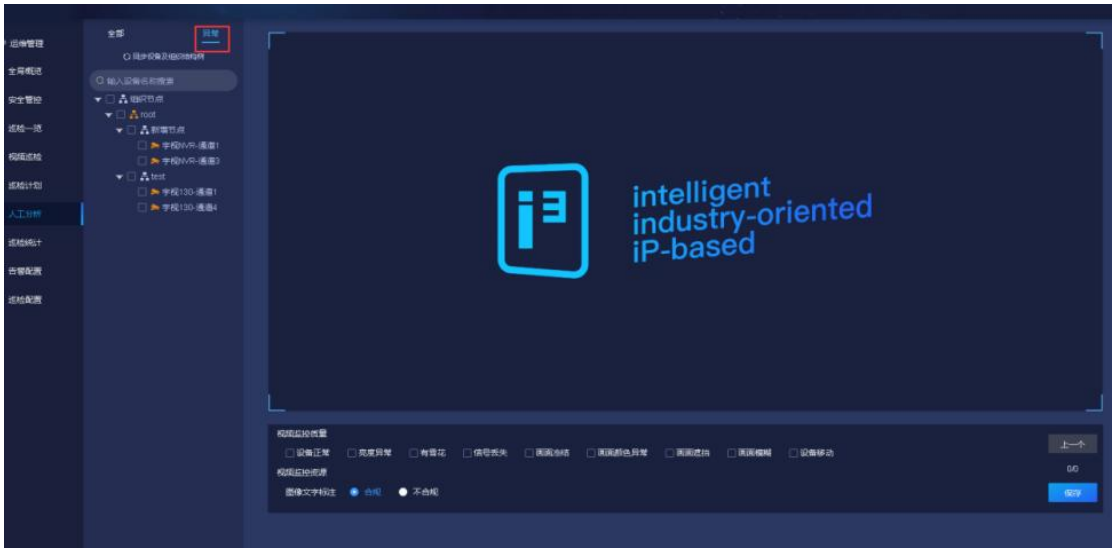
可在下方对该设备视频监控质量和视频监控资源图像文字标注是否合规进行标注，图像文字不合规标注后组织结构树上图标变黄

，如下图：



完成后点击下一个，自动保存上一个的标注信息。

点击左侧上方 tab“异常”，进入异常界面，可查看已标注为异常的设备信息，能对已标注为异常的重新进行标注，标注为正常后，则不在该页面进行展示，如下图：



其余所有操作与“全部”的界面操作一致。

第 7 节 巡检统计

进入运维管理主界面后，点击左侧巡检统计，进入巡检统计模块，如下图所示：



默认统计所有节点，可勾选单个组织节点进行查询，勾选组织结构树节点



，点击 

按

钮，即可查询该节点的在线信息、出图信息、合规信息等

第 8 节 告警配置

进入运维主界面后，点击左侧告警配置，进入告警配置模块，如下图所示：

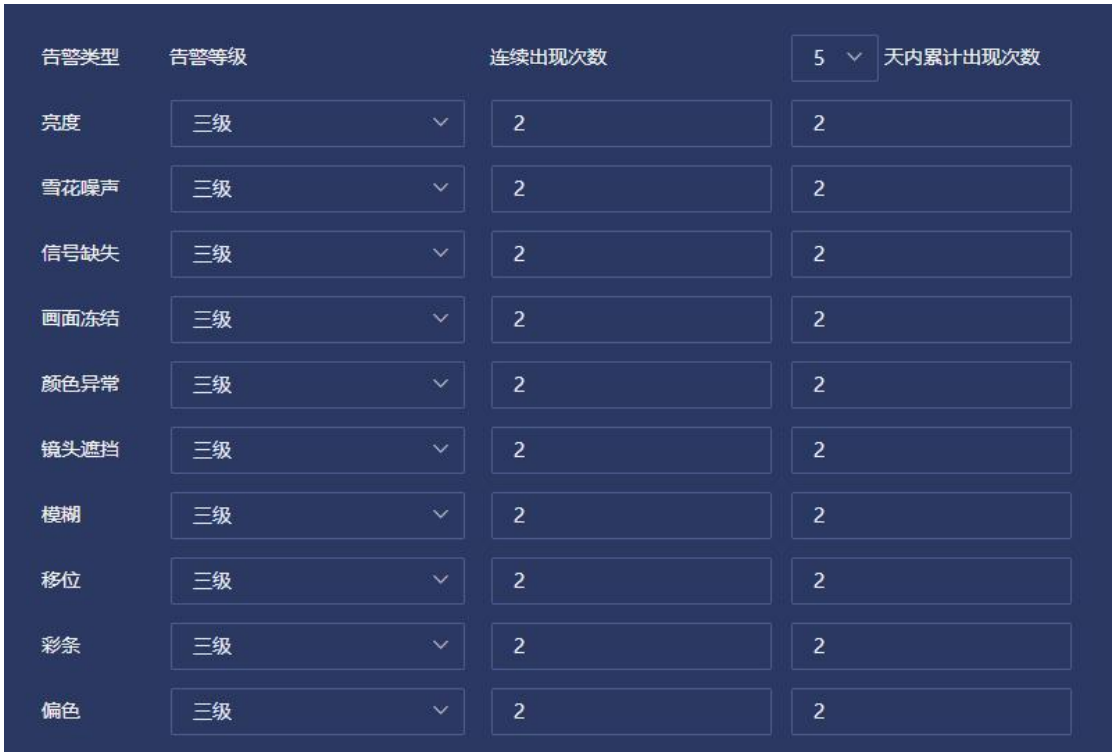


8.1 日间预警规则

支持配置日间预警规则，日间预警规则告警时间段默认早八到晚八，可选择文本框自定义告警时间段



选择告警类型，告警等级、连续出现次数、多少天内累计出现多少次等，如下图：



勾选启用状态

，勾选

，则启用该规则，勾选

，则关闭该规则，完成后点击

按钮，保存以上操作，点击

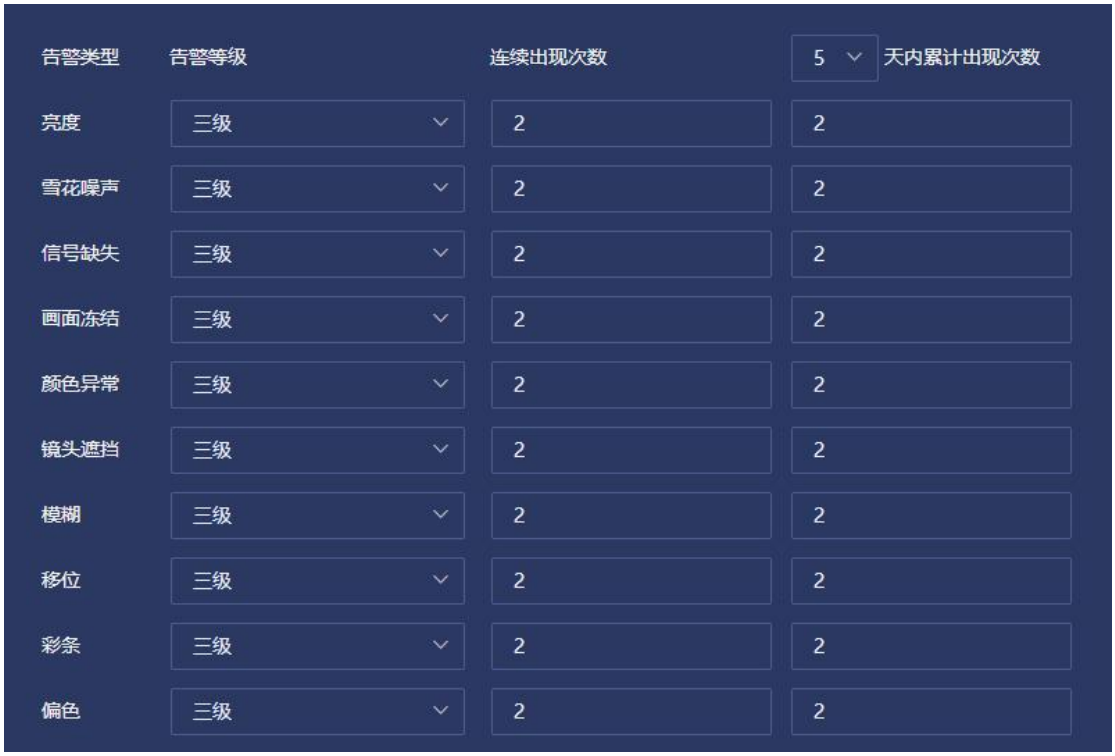
按钮，恢复至初始状态

8.2 夜间预警规则

支持配置夜间预警规则，点击上方 tab“夜间预警规则”进入该界面，夜间预警规则告警时间段默认晚八到早八，可选择文本框自定义告警时间段



选择告警类型，告警等级、连续出现次数、多少天内累计出现多少次等，如下图:



勾选启用状态

，勾选

，则启用该规则，勾选

，则关闭该规则，完成后点击

按钮，保存以上操作，点击

按钮，恢复至初始状态

第 9 节 巡检配置

进入运维主界面后，点击左侧巡检配置，进入巡检配置模块，如下图所示：

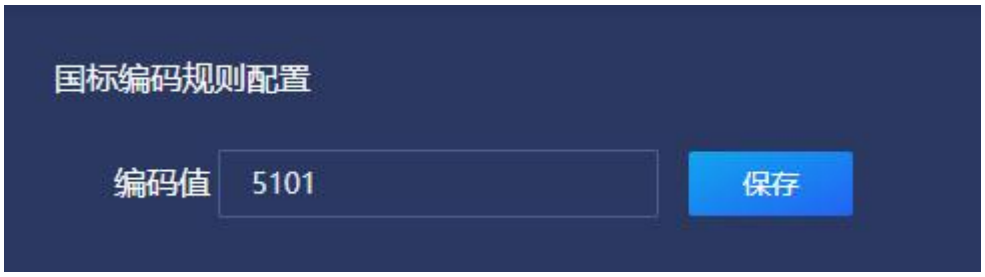


9.1 国标编码配置

界面上方可配置国标编码规则，在输入框内输入限定值，如：四川成都编码为 5101，国标编码一般以 5101 开头，设备未以 5101 开头的则为不合规，规则定义完成后点击保存



按钮，则保存该配置。如图：



9.2 巡检配置

该模块用于配置服务器和设备，如图：



点击设备上方详情按钮，可查看配置的设备详情，如图：

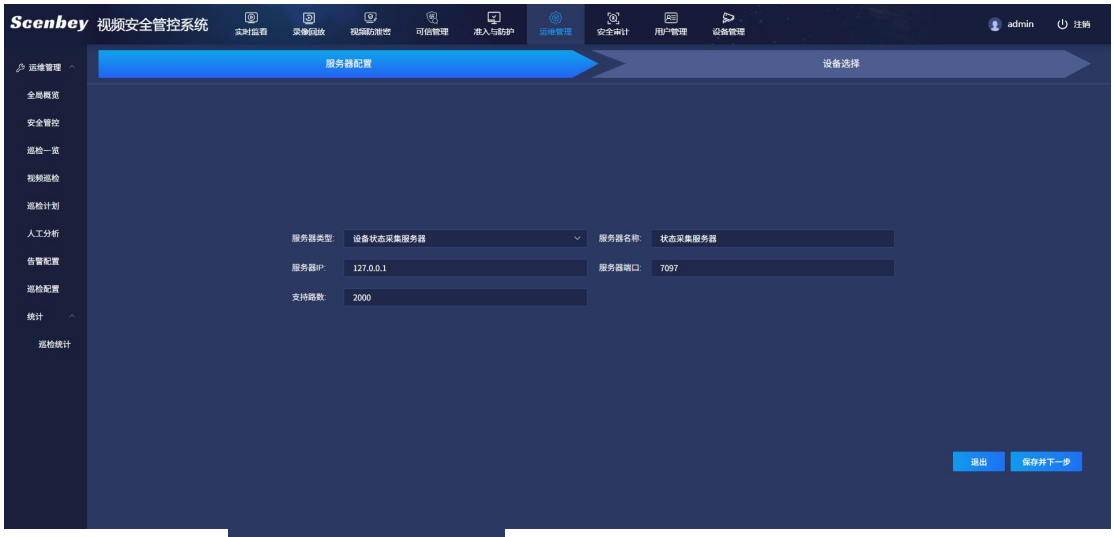


设备列表支持输入设备名称进行搜索



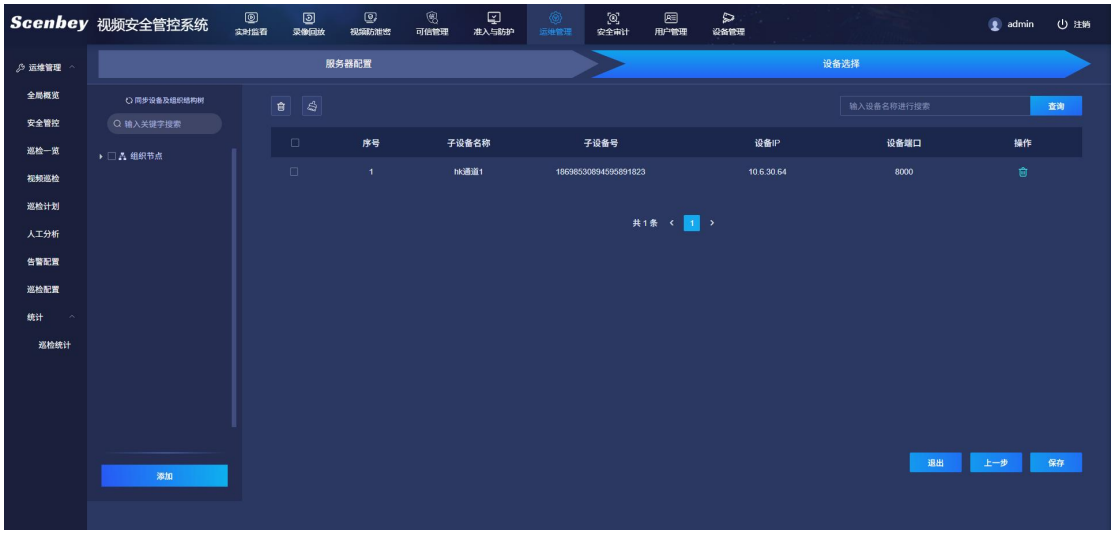
编辑：点击

服务器信息下方的编辑按钮可对已经配置完成的服务器信息进行编辑，点击编辑，进入服务器配置界面，如图：



配置完成后对点击

可进入设备选择界面，如图：



勾选左侧组织结构树设备，点击下方

按钮，即可将该设备添加至该服务器下

可多选点击按钮批量删除或点击按钮删除单个设备

完成后点击

退出该操作，点击

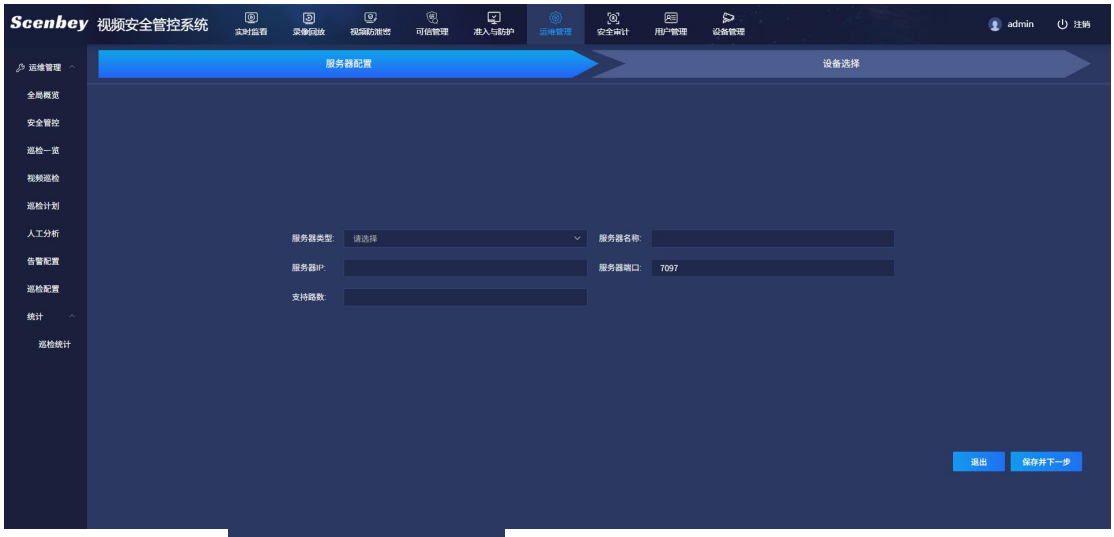
返回服务器配置界面，点击

按钮保存以上配置。

添加巡检配置：点击添加巡检配置按钮



进入服务器配置界面，如图：



配置完成后对点击  可进入设备选择界面，如图：



勾选左侧组织结构树设备，点击下方

按钮，即可将该设备添加至该服务器下

可多选点击按钮批量删除或点击按钮删除单个设备

完成后点击

退出该操作，点击

返回服务器配置界面，点击

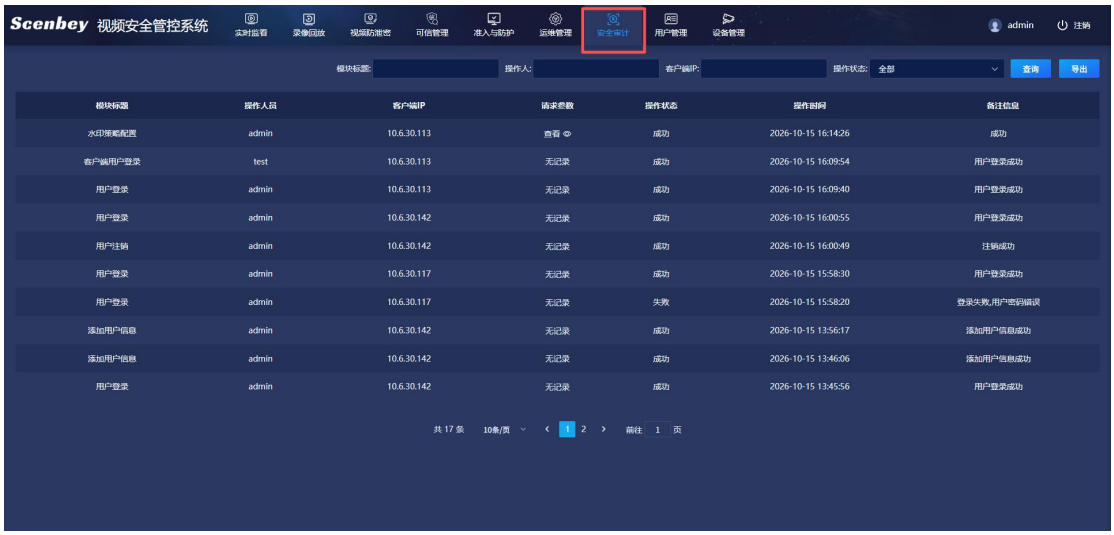
按钮保存以上配置。



删除：点击按钮，删除该服务器的配置信息。

第七章 安全审计

点击上方安全审计菜单，可以进入安全审计界面。



第 1 节 选择查询条件

日志的查询条件共有四个约束条件：模块标题、操作人、客户端 IP、操作状态四个条件，可以输入关键字点击确定才按进行组合查询，默认显示所有信息。



第 2 节 日志的查看

模块标题：操作了哪些模块
操作人员：登陆者的账号
客户端 IP：登陆这登陆账号电脑的 ip 地址
请求参数：登陆者做了哪些操作
操作状态：分为成功失败，分别代表用户对当前操作的修改是否成功
操作时间：登陆者对系统进行修改的时间
执行时长：登陆者对每项请求花费了多长时间

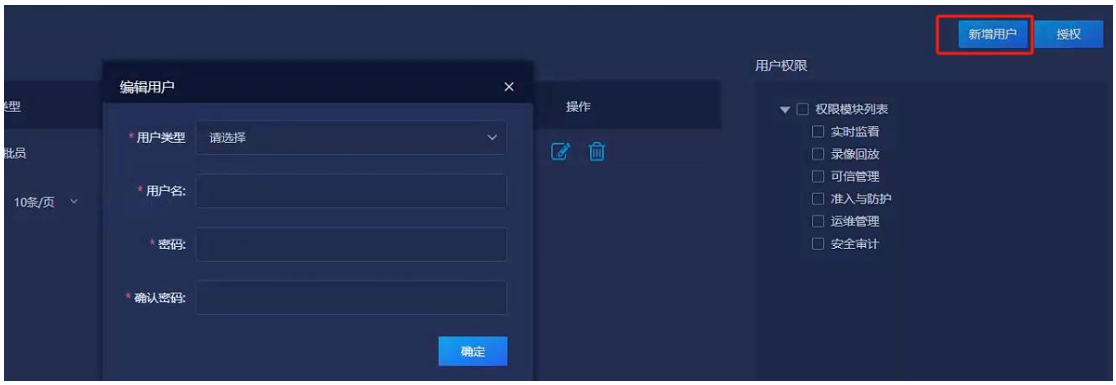
第八章 用户管理

点击用户管理菜单可以切换到用户管理界面。



第 1 节 添加用户

点击新增用户在弹出用户信息输入对话框：



在用户信息对话框中输入用户类型、用户名称、密码，密码要二次确认才能保存成功，

第 2 节 用户权限设置

鼠标左键单击用户资源，右侧选择分配的权限，点击授权菜单完成授权操作。

