

# 防爆电子哨兵用户手册

---

V1 202301

## 声明

Kedacom™、TrueSens™、KEDACOM™、摩云视讯™为苏州科达科技股份有限公司的商标，不得擅自使用。苏州科达科技股份有限公司版权所有，保留所有权利。

本手册可能包含技术上不准确的地方、或与产品功能及操作不相符的地方、或印刷错误。我司将根据产品功能的增强而更新本手册的内容，并将定期改进或更新本手册中描述的产品或程序。更新的内容将会在本手册的新版本中加入，恕不另行通知。

此手册的目的是确保用户正确使用本产品，以避免危险或财产损失。在使用产品之前，请认真阅读此手册并妥善保存以备日后参考。如果用户因没有按照以下安全说明，致使设备不能正常使用或损坏等情况，我司恕不负责，感谢您的配合。



使用本设备，应当严格遵守《中华人民共和国个人信息保护法》等有关法律规定，不得违法违规采集他人个人图像信息，不得侵犯他人个人信息权益。

## 安全使用注意事项

请在安装使用设备过程中，严格遵守当地各项电气安全规定。

请使用满足安全电压要求的电源，在设备运行之前检查供电电源是否正确。

请在允许的湿度和温度范围内运输、使用和存储设备。

请勿将设备置于潮湿、多尘、极热、极冷、强电磁辐射或照明条件不稳定等场所。

请在运送设备时，重新以出厂时的包装进行包装，或用同等品质的材质包装。

请勿在运输、存储及安装过程中重压、剧烈震动、浸泡设备。

请勿撞击设备，以免损坏设备。

老人和小孩请在监护下通行。

## 通过互联网访问说明

将本产品接入互联网需自担风险，包括但不限于产品可能遭受的网络攻击、黑客攻击、病毒感染等，本公司不对因此造成的产品工作异常、信息泄露等问题承担责任，本公司将及时为您提供产品相关技术支持。

## 注意

为了提高产品网络使用的安全性，建议您设置高强度密码，密码必须包含 8-16 个字符，且至少由数字、字母或特殊字符中的两种或两种以上类型组合而成。

请您定期更改用户名的密码，建议每 3 个月更新一次。如果设备在较高安全风险的环境中使用，建议每月或每周更新一次。

请妥善保管好您的用户名与密码。

## 环保声明

请遵守有关设备包装材料、耗尽电池和废旧设备处理的本地法规，并支持回收行动。

## 读者对象

防爆电子哨兵安装人员、操作人员。


## 相关手册

《防爆电子哨兵快速安装指南》

## 关于本手册

本手册用于指导用户操作，手册中的界面截图、图表等仅用于解释和说明的目的，与具体产品可能存在差异，请以实际为准。

## 本书约定

图形或格式	约定
	说明、注意：对操作内容描述作必要补充
" "	界面菜单，如点击“保存”
>	多级菜单连接，如 <b>系统配置&gt;基本配置</b>

苏州科达科技股份有限公司

地址:江苏省苏州市高新区金山路 131 号

邮编: 215011

网址: [www.kedacom.com](http://www.kedacom.com)

电话: 0512-68418188

传真: 0512-68412699

客户咨询热线: 400-828-2866

## 目录

<b>1</b>	<b>产品概述</b>	<b>1</b>
<b>2</b>	<b>现场安装说明</b>	<b>2</b>
<b>3</b>	<b>使用前配置</b>	<b>4</b>
3.1	设备激活	4
3.2	快速修改网络参数	7
3.3	客流仪配置	8
3.4	门禁参数配置	10
3.5	防爆箱参数配置	11
3.6	交互配置	12
3.6.1	国标注册	12
3.6.1.1	门禁模块录入	12
3.6.1.2	全景模块录入	17
3.6.2	Web 端协议配置	19
3.6.2.1	门禁模块	19
3.6.2.2	全景模块	21
3.7	WEB 端登录	24
<b>4</b>	<b>门禁模块操作</b>	<b>26</b>
4.1	门禁界面说明	26
4.2	人员查询	27
4.3	通讯配置	27
4.3.1	以太网	27
4.3.2	其他	28
4.4	系统配置	28
4.4.1	基本信息	28
4.4.2	时间配置	30
4.4.3	人脸参数	31
4.4.4	高级配置	31

4.4.5	语言.....	34
4.5	门禁配置.....	34
4.6	管理配置.....	35
4.7	事件查询.....	35
4.8	存储配置.....	35
4.9	功能检测.....	36
4.9.1	声音检测.....	37
4.9.2	读卡器检测.....	37
4.9.3	IO 检测.....	38
4.9.4	网络检测.....	38
4.10	系统信息.....	39
4.10.1	设备信息.....	39
4.10.2	设备日志.....	39
<b>5</b>	<b>通行.....</b>	<b>41</b>
5.1	正常通行.....	41
5.1.1	证件核验.....	41
5.1.1.1	身份证核验.....	41
5.1.1.2	二维码核验.....	42
5.1.1.3	护照核验.....	43
5.1.2	人脸核验.....	43
5.2	异常通行.....	43
<b>6</b>	<b>其他功能.....</b>	<b>45</b>
6.1	一键呼叫.....	45
6.2	全景语音播报.....	45
<b>7</b>	<b>门禁 WEB 客户端.....</b>	<b>46</b>
7.1	开始使用.....	46
7.2	WEB 界面说明.....	46
7.3	实时浏览.....	47
7.4	录像回放.....	49

7.5	图片管理.....	51
7.6	配置.....	52
7.6.1	网络.....	52
7.6.1.1	IP 及端口 .....	52
7.6.1.2	接入协议.....	55
7.6.1.3	其他协议.....	60
7.6.2	门禁.....	64
7.6.2.1	人员管理.....	64
7.6.2.2	参数配置.....	64
7.6.2.3	事件管理.....	67
7.6.2.4	存储状态.....	67
<b>8</b>	<b>全景 WEB 客户端.....</b>	<b>68</b>
8.1	开始使用.....	68
8.2	WEB 界面说明.....	68
8.3	实时浏览.....	69
8.3.1	图像调节.....	70
8.3.2	预览设置.....	70
8.4	录像回放.....	72
8.5	图片管理.....	74
8.6	配置.....	74
8.6.1	网络.....	75
8.6.1.1	IP 及端口 .....	75
8.6.1.2	接入协议.....	77
8.6.1.3	其他协议.....	81
8.6.2	事件.....	85
8.6.2.1	基础智能.....	85
8.6.2.2	报警输入.....	106
8.6.2.3	报警输出.....	106
8.6.2.4	异常联动.....	106

8.6.3	存储.....	107
8.6.3.1	存储管理.....	107
8.6.3.2	录像.....	108
8.6.3.3	抓拍.....	110

## 1 产品概述

防爆电子哨兵（下文统称“防爆哨兵”）是一款具有 AI 客流统计和人证核验功能的防爆智能设备。采用领先的双目立体视觉技术和智能跟踪算法可精确识别客流人数和行走方向。内置的多种证件阅读器，可精准读取国际护照、二代居民身份证、临时出入境证等多种证件信息，并通过人脸匹配技术进行精准的 1:1 人证核验。主要适用于危化品码头人员进出的管控管理。

下图为防爆哨兵外观说明。

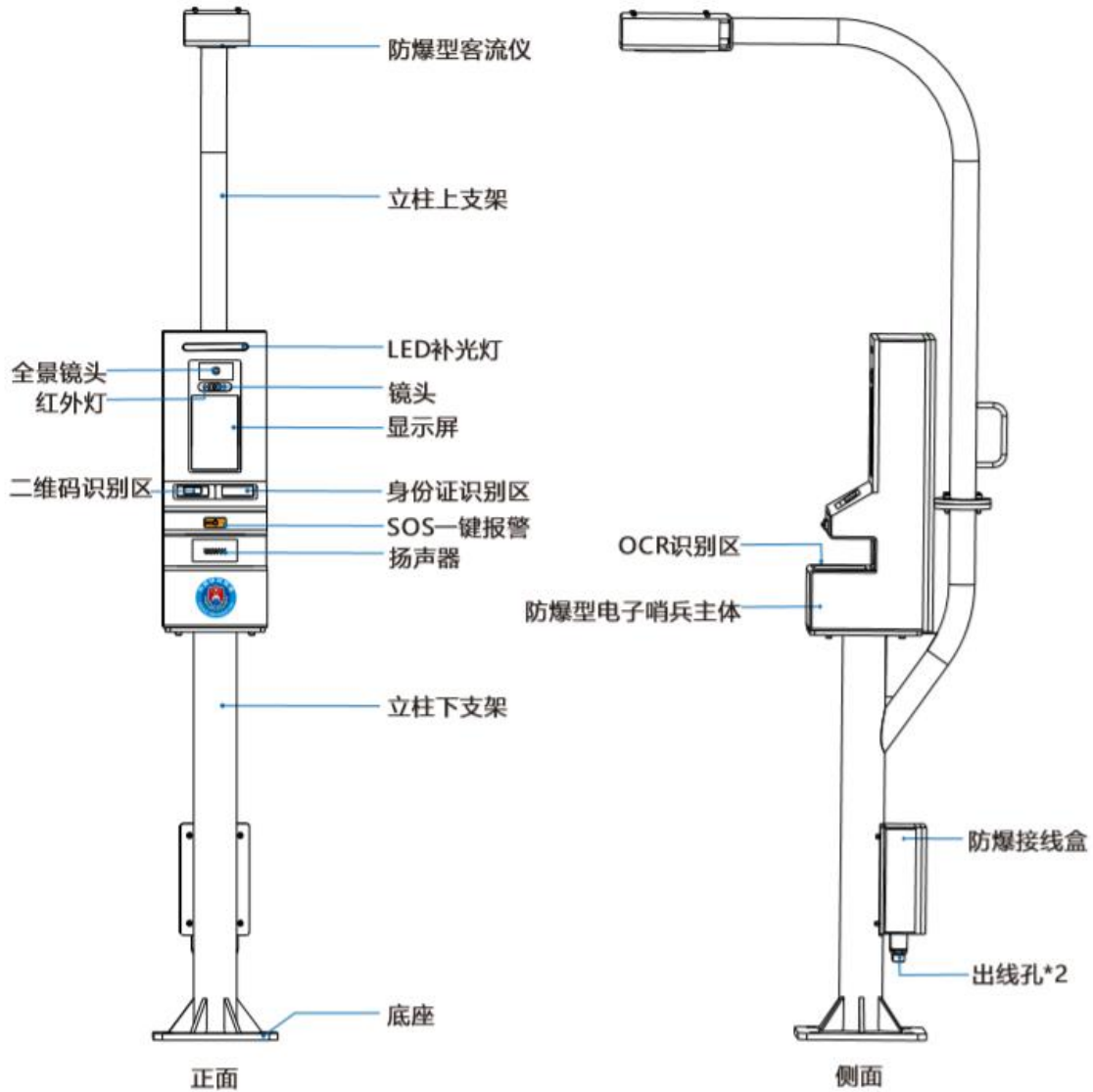


图 1-1 设备外观

## 2 现场安装说明

防爆电子哨兵的现场安装详细请参考《防爆电子哨兵快速安装指南》，本章节主要说明安装时注意事项。

### ➤ 安装点位确定

- 因设备外观限制，安装后不可妨碍大车通行。
- 安装地面尽量为水平面，尽量不要选择有倾斜角度的位置作为安装面。

### ➤ 现场施工需求

- 人脸通行位置和设备安装位置，必须保证在同一水平面上，若有高度差，请提前浇筑。如下图所示。



图 2-1 浇筑水泥墩

- 现场若无适配器或供电机房，或供电机房距离设备超过 30 米，需安装防爆箱，防爆箱的安装及接线详细可参考《防爆电子哨兵快速安装指南》中的相关章节。

### ➤ 设备接线注意事项

- 设备安装接线时，需做好防水处理，线头一定要加防水胶圈和垫片，可参考《防爆电子哨兵快速安装指南》中的相关章节。



图 2-2 防水处理

- 防爆哨兵接线盒中的线缆连接，需严格按照《防爆电子哨兵快速安装指南》。线缆连接错误会导致设备无法正常使用。
- 现场若使用防爆箱，会有两组线缆接入防爆箱内。一组是从防爆哨兵引入防爆箱的线缆，一组是供电机房引入的电源线和网线，这两组线缆接入时也需做好防水处理。两组线缆连接可参考《防爆电子哨兵快速安装指南》中的相关章节。

## 3 使用前配置

### 3.1 设备激活

本设备分三个主模块：全景模块、门禁模块和转接板模块，首次使用时需要激活各模块。

**i** 说明：三个主模块在防爆哨兵中的主要作用如下。

- ◆ 全景模块：主要功能为全景录像并上传平台。
- ◆ 门禁模块：主要功能为人脸核验。
- ◆ 转接板模块：主要功能为证件阅读数据并传送给门禁模块，实现人证核验。

激活方式可分为 Web 界面激活、通过 IPCSearch 激活。

#### ➤ Web 界面激活

- 1) 在 PC 机上打开浏览器，输入设备 IP 地址后单击回车。全景模块默认 IP 为 192.168.1.100；门禁模块默认 IP 为 192.168.1.101:8080；转接板模块默认 IP 为 192.168.1.102:8080；

**i** 说明：若 PC 机与设备不在同一网段，需在 PC 机上增加与设备同网段的 IP 地址。以下操作步骤以 windows7 为例，仅供参考。

- 1) 打开电脑端**开始菜单**，选择**控制面板>网络和 Internet>查看网络状态和任务>本地连接>属性**，弹出如下窗口；

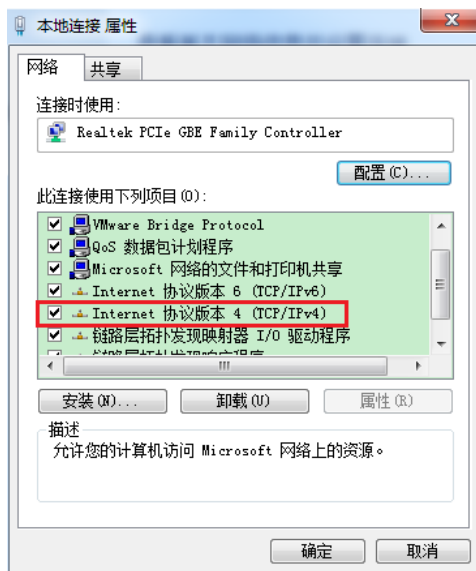


图 3-1 本地连接属性窗口

- 2) 双击 **Internet 协议版本 4 (TCP/IPv4)**，弹出如下窗口；

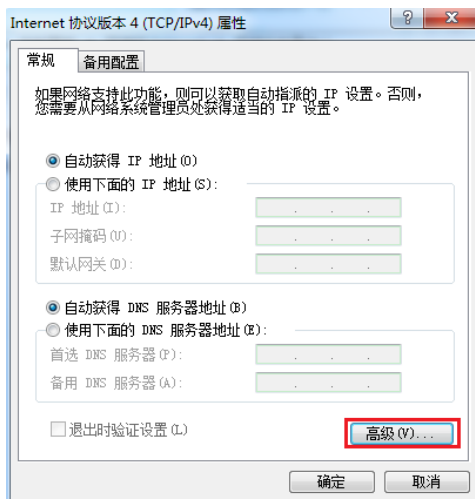


图 3-2 Internet 协议版本 4 (TCP/IPv4) 属性窗口

- 3) 点击**高级 (V) ...**按钮，在弹出的高级 TCP/IP 设置窗口点击**添加**，然后输入 IP 地址和子网掩码，如下图所示，单击**添加**，为 PC 机增加与设备同网段的 IP 地址。

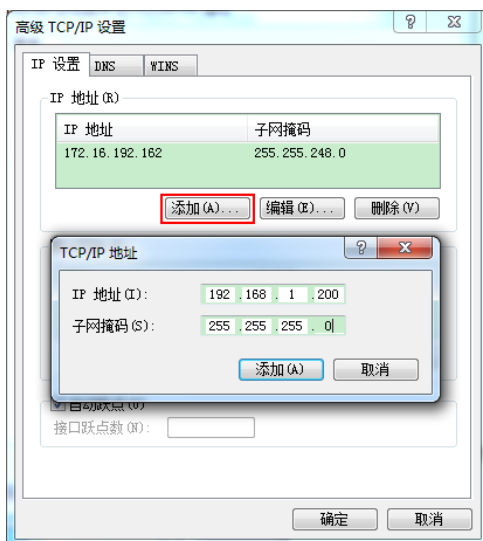


图 3-3 高级设置界面

- 2) 进入网页客户端登录界面，如下图所示；



图 3-4 网页客户端登录界面

3) 设置 admin 用户密码并填写邮箱, 然后点击**激活**按钮激活设备。

**i** 说明:

- ◆ 密码强弱规则: 8-16 位包含字母和数字的密码强度为低; 8-16 位包含字母、数字及一个其他字符的密码强度为中; 8-16 位包含字母、数字及多个其他字符的密码强度为高。
- ◆ 为了提高产品网络使用的安全性, 建议您设置为高强度密码。
- ◆ 请您定期更改用户名的密码, 建议每 3 个月更新一次密码。如果设备在较高安全风险的环境中使用, 建议每月或每周更新一次。

➤ IPCSearch 激活

- 1) 从官网下载 IPCSearch 工具, 根据提示安装 IPCSearch;
- 2) 安装完成后打开 IPCSearch, 系统会自动搜索局域网内的设备, 搜索结果显示在列表中;

**i** 说明: IPCSearch 可同时搜索到三个模块, 其中全景模块默认 IP 地址为 192.168.1.100, 门禁模块默认 IP 地址为 192.168.1.101, 转接板模块 192.168.1.102。

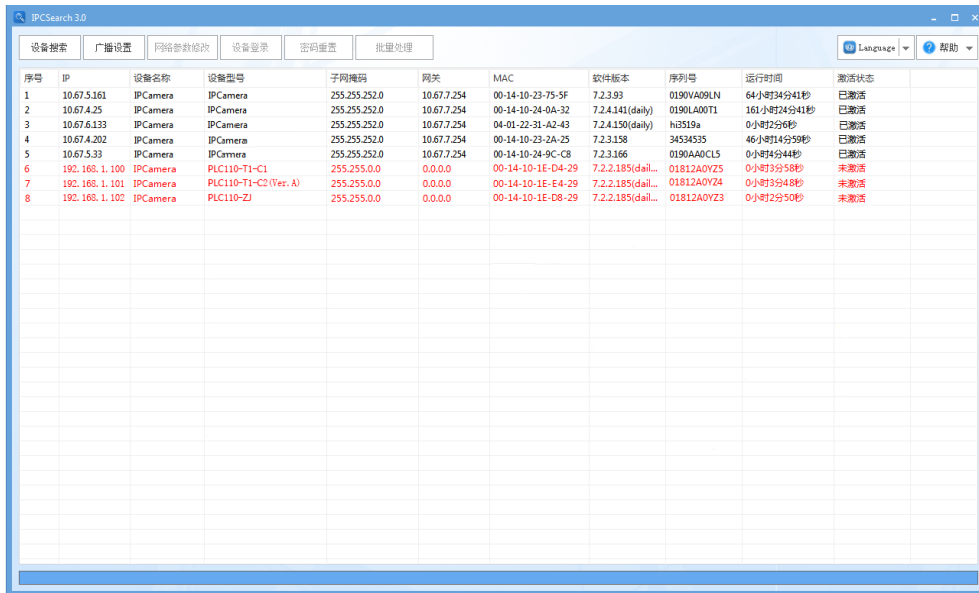


图 3-5 IPCSearch 搜索

- 3) 选择需要激活的设备，单击右键，选择“设备激活”，在弹出的界面中设置 admin 用户的密码和找回密码时需要的邮箱，点击“激活”激活设备；

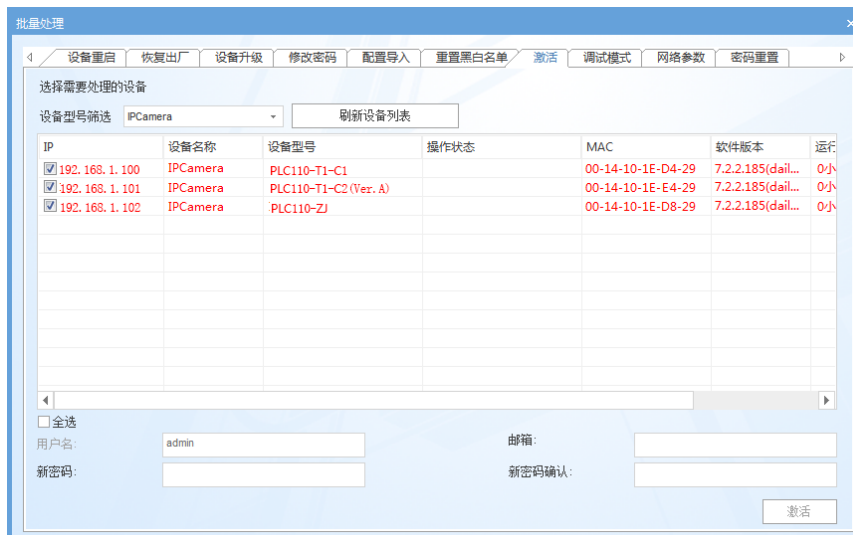


图 3-6 设备激活

### 3.2 快速修改网络参数

设备各模块激活后，可通过 IPCSearch 快速修改各模块的基本网络参数，包括 IP 地址、子网掩码和默认网关等。

因各模块修改网络参数的方法相同，本章节以全景模块为例做说明，其他参考即可。

- 1) 打开 IPCSearch，系统自动搜索局域网内的 IPC 设备，搜索结果显示在列表中；
- 2) 选择修改配置的全景模块，点击“网络参数修改”，或使用鼠标右键菜单，弹出网络参数修改界面。选择“自定义地址”，根据实际场景修改参数配置，填写管理员用户名 (admin) 及激活设备时所设置的密码；



图 3-7 网络修改参数

3) 点击“确认”，弹出如下窗口，点击“确定”，等待设备重启。



图 3-8 设备重启

### 3.3 客流仪配置

工作人员配置客流仪参数时，需通过其的专属配置工具（PassengerFlowClient）完成，配置工具请咨询我司工作人员获取。

1) 运行客流仪配置工具，点击“在线设备搜索”，搜索局域网内的客流仪，双击选择该客流仪；

**i** 说明：客流仪初始 IP 地址默认为 192.168.1.99。



图 3-9 在线搜索设备

- 2) 点击“设备信息”，进入设备信息界面，选择“https 协议”，进入如下窗口，勾选数据推送 1，并修改服务器地址（修改为门禁模块的实际 IP）及端口（默认 5020 即可）；



图 3-10 设备信息

- 3) 点击“修改设备网络参数”，弹出如下窗口，根据实际场景修改网络参数。



图 3-11 修改设备网络参数

### 3.4 门禁参数配置

门禁参数需要配合特定命令及我司特定工具登录门禁 UI 界面后来配置，登录门禁 UI 界面的详细操作可参考 4.1 门禁界面。登录 UI 界面后修改的参数配置如下：

- 1) 通讯配置：在门禁模块菜单界面，进入**通讯配置>其他**界面，修改全景机地址和转接板地址；

**i** 说明：全景机地址和转接板地址均为实际场景地址。

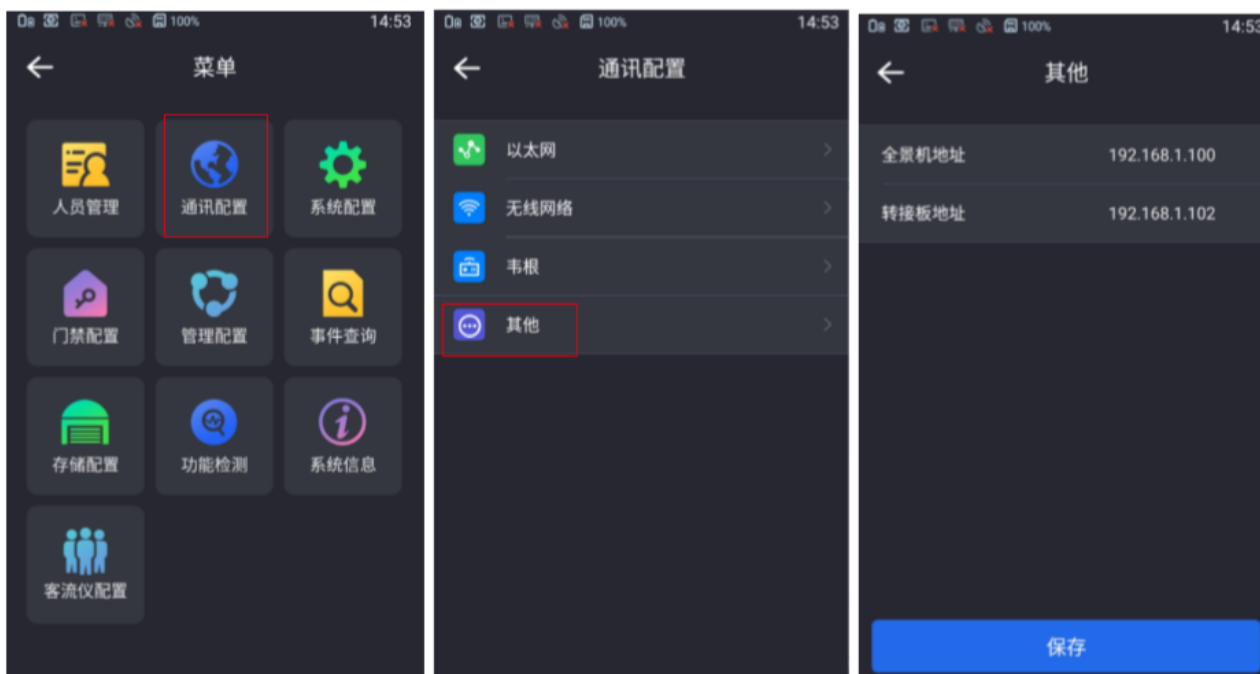


图 3-12 通讯配置

- 2) 客流仪进出方向配置：在门禁模块菜单界面，进入客流仪配置界面，修改客流仪进出方向及通道宽度，点击“保存”完成修改。

**i** 说明：客流仪通道宽度有最窄、默认及最宽三种配置，请用户根据实际通道场景设置。

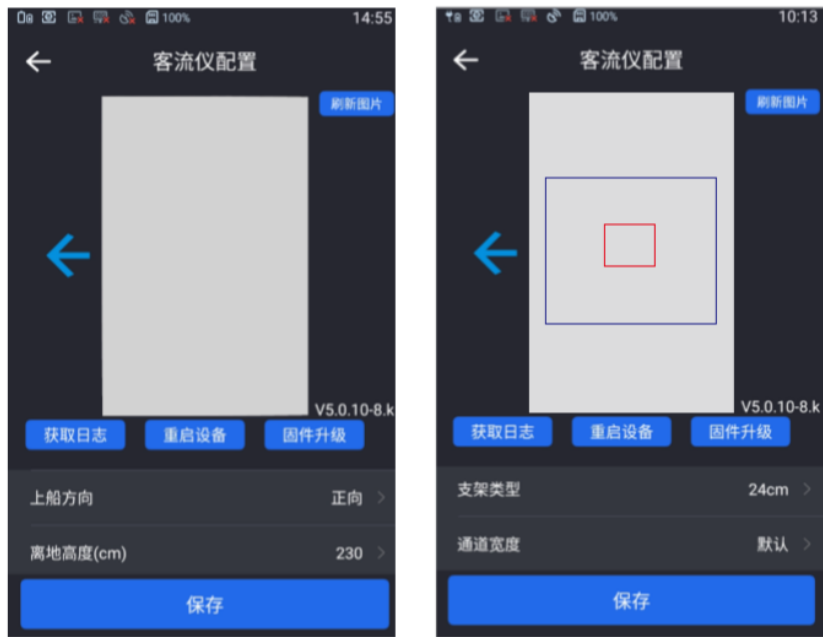


图 3-13 客流仪进出方向配置

### 3.5 防爆箱参数配置

**i** 说明：若现场未安装防爆箱，忽略此章节配置操作。

现场安装了防爆箱，并完成了线缆连接后，用户需要通过 PC 机接入防爆箱的交换机，来修改防爆箱控制器的 IP 地址。修改防爆箱控制器的工具为 USR-M0，请联系我司工作人员获取该工具。

- 1) 双击打开 USR-M0 软件工具，点击“搜索设备”；
- 2) 设备列表中会搜索到防爆箱设备，点击并选择该设备，界面右侧会出现该设备的相关配置项；
- 3) 根据实际场景（客流仪、防爆哨兵的三个模块的 IP 地址）修改模块静态 IP、子网、网关、目标 IP/域名等参数；

**i** 说明：

- ◆ 修改的 IP 地址等信息需和客流仪、防爆哨兵的三个模块在同一个局域网内。
- ◆ “目标 IP/域名”改为服务端的 IP 地址，远程端口为服务端口。

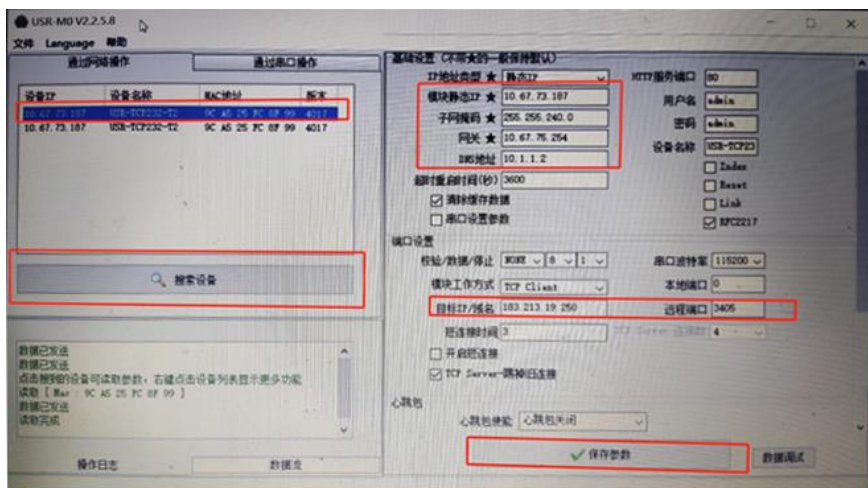


图 3-14 防爆箱参数配置

## 3.6 交互配置

本章节主要介绍完成防爆哨兵与后端平台建立数据交互前的配置。需先完成国标注册，后完成 Web 端部分协议的配置。

### 3.6.1 国标注册

防爆哨兵通过我公司一机一档管理平台录入门禁模块和全景模块。

**i**说明：一机一档管理平台，我公司视频监控业务平台的联网管理客户端，用于对视频设备资源信息进行录入、管理、审核等。详细功能可参考《一机一档管理平台用户手册》。

#### 3.6.1.1 门禁模块录入

门禁模块需分两次录入，一次作为门禁视频通道录入，一次作为门禁录入。

##### ➤ 门禁视频通道录入

门禁录入的步骤如下：

- 1) 登录一机一档管理平台；



图 3-15 登录一机一档

- 2) 登入后，进入主界面，在导航栏中点击“录入设备”，进入设备录入界面；

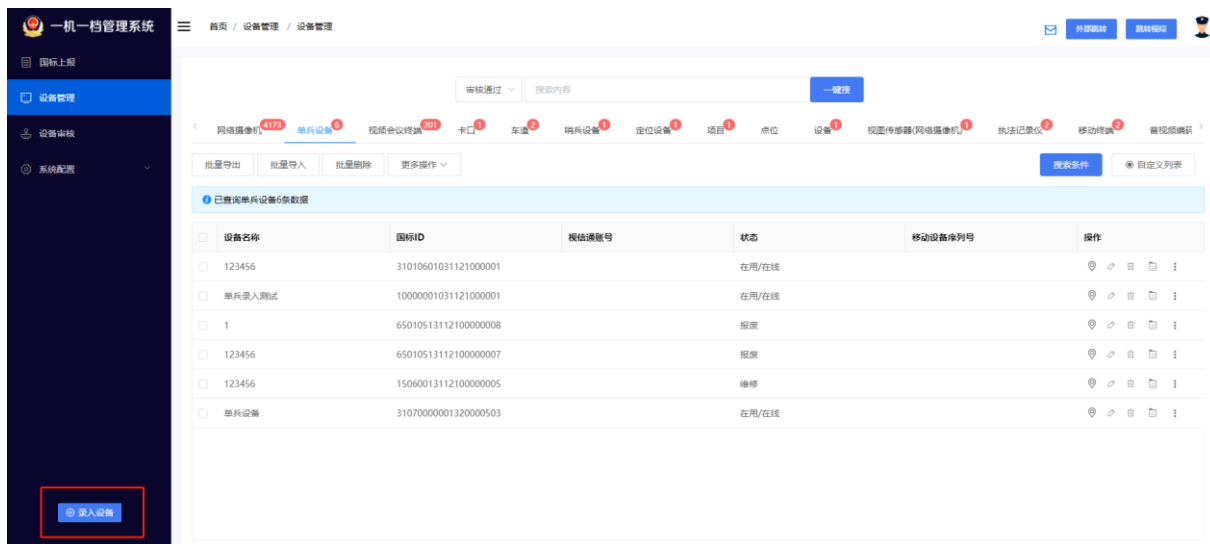


图 3-16 主界面

3) 在设备录入界面，根据实际填写各参数；

**i** 说明：因参数较多，仅以必填项和需要注意的属性作说明，未说明项可根据实际需要填写或不填。

■ 设备类型&设备标签

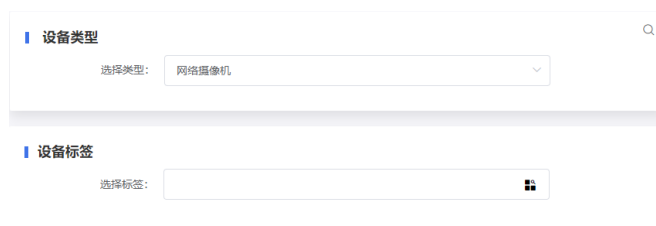


图 3-17 设备类型&设备标签

属性名称	填写说明
设备类型	选择“网络摄像机”
设备标签	根据需要选择已有的标签名 <b>i</b> 说明：若需要自定义标签，需添加新标签名，详细可参考《一机一档用户手册》。

■ 基本属性

基本属性

国标ID:	<input type="text"/>	分辨率:	720P
* 设备名称:	哨兵-门禁模块-视频通道	跟踪方式:	请选择
生命周期:	入网阶段	巡检状态:	请选择
设备厂商:	科达	变焦类型:	请选择
行政区域:	苏州市	备注:	<input type="text"/>
监控点位类型:	一类视频监控点	立杆编号:	<input type="text"/>
设备型号:	<input type="text"/>	拍摄类型:	请选择
点位俗称:	<input type="text"/>	摄像机方向:	请选择
IPV4:	<input type="text"/>	摄像机桩号:	<input type="text"/>
IPV6:	<input type="text"/>	摄像机路段单位名称:	<input type="text"/>
MAC地址:	<input type="text"/>	视频上云网关编号:	<input type="text"/>
* 摄像机类型:	固定枪机	兴趣点名称:	<input type="text"/>
摄像机功能类型:	请选择	组播地址:	<input type="text"/>
补充属性:	请选择	经纬度验证:	请选择
摄像机编码格式:	请选择	兴趣点名称:	<input type="text"/>

图 3-18 基本属性

属性名称	填写说明
国标 ID	自定义包含“132”的 20 位数字 <b>i</b> 说明：该处国标 ID 为视频通道国际 ID，必需是包含“132”的 20 位数字。如“3100000001325001110”。
设备名称	自定义
生命周期	选择“入网阶段”
设备厂商	选择“科达”
行政区域	根据实际选择
监控点位类型	选择“固定枪机”
分辨率	选择“720P”，即 200 万像素
流媒体全局路由信息	如：190/180/155 <b>i</b> 说明：在现场专网中，还会有流媒体全局路由信息。该参数必须配置一个值。因为在现场视频网的新媒体需要和专网的新媒体做级联。

位置属性

位置属性

安装地址: 苏州港

经度: 130.000000

纬度: 30.000000

摄像机位置类型: 车站码头

监控方位: 请选择

所属楼层: 请选择

所属站点编号:

所属站点名称:

监控可视化区域:

位置高度:

图 3-19 位置属性

属性名称	填写说明
经度	手动填写或地图定位 ⓘ 注意：不管是手动填写还是地图定位选择，都需要精确到小数点后六位。
纬度	手动填写或地图定位 ⓘ 注意：不管是手动填写还是地图定位选择，都需要精确到小数点后六位。
摄像机位置类型	根据实际场景选择

管理场景

管理属性

类型编码: 132 社会面监控点位

电信运营商: 1-电信

联网属性: 已联网

安装时间: 选择日期时间

所属辖区公安机关: 江苏边检

管理单位: 江苏边检

管理单位联系人:

管理单位联系方式: 0512-8888888

录像保存天数: 90

设备状态: 在用/在线

所属部门行业: 请选择

所属地铁站点: 请选择

地铁站点层级: 请选择

维保单位:

图 3-20 管理属性

属性名称	填写说明
类型编码	选择“社会面监控点位”
电信运营商	选择“电信”
联网属性	选择“已联网”
管理单位	根据实际情况填写
录像保存天数	90
设备状态	选择“在用/在线”
行业编码	选择“社会治安路面接入”
网络标识	选择“公安信息网”

**i** 说明：因一机一档版本不同，若有设备状态、行业编码、网络标识等必填参数时，参考上表填写即可。

■ 接入属性

**接入属性**

域编号:

\* 新媒体平台:

设备平台:

域ID:

目标网域标识:

用户名:

密码:

登录地址:

视图库平台标识:

连接断开配置:

视图库平台ip:

私有协议服务接入地址:

设备接入协议:

端口号:

\* 媒体流传输模式:

设备接入私有编码:

图 3-21 接入属性

属性名称	填写说明
新媒体平台	填写新媒体平台的 IP
设备接入协议	gb
端口号	5800 <b>i</b> 说明：端口号虽然不是必填项，但此处必须填写，也是由新媒体平台提供。
媒体流传输模式	单播

■ 其他属性

其他

卡口相机编号:

1400ID:

图 3-22 其他

属性名称	填写说明
卡口相机编号	可自定义数字，不冲突即可 <b>i</b> 说明：建议卡口相机编号也填写成国标 ID 号。
1400ID	可不填写，也可填写与卡口相机编号相同编号 <b>i</b> 说明：1400ID 可不填写，保存时自动保存为与基本属性中的国标 ID 相同的 ID 号。

4) 点击“保存”，完成视频通道的录入；

5) 进入设备审核界面，选择待审核的网络摄像机，点击 ，即对新录入的门禁视频通道审核通过。



图 3-23 审核

➤ 门禁录入

门禁录入和门禁视频通道录入相同，详细参考门禁视频通道的录入。

**i**注意：门禁录入时需要注意参数“国标 ID”的不同，门禁录入时的国标 ID，自定义包含“112”的 20 位数字。如“3100000001125001115”。

属性名称	填写说明
国标 ID	自定义包含“112”的 20 位数字

3.6.1.2 全景模块录入

全景模块需分两次录入，一次作为全景视频通道录入，一次作为全景录入。

全景模块录入步骤如下：

1) 请参考门禁模块录入，完成全景和全景视频通道的录入。

**i** 注意：录入全景和录入全景视频通道时，参数填写上分别有以下不同点需要注意。

◆ 全景视频通道录入

属性模块	属性名称	填写说明
设备类型	选择类型	选择“哨兵设备”
其他	子设备列表	选择门禁模块的视频通道和视频通道国标 ID

- 1) 设备类型选择了哨兵设备后，所有属性会有稍许变化，其中需要修改的是，在其他属性模块中的子设备列表。

■ 其他

子设备列表:

图 3-24 子设备列表

- 2) 子设备列表中点击，弹出列表选择框，请选择门禁模块的视频通道（即国标 ID 中含有“132”）作为子设备列表。

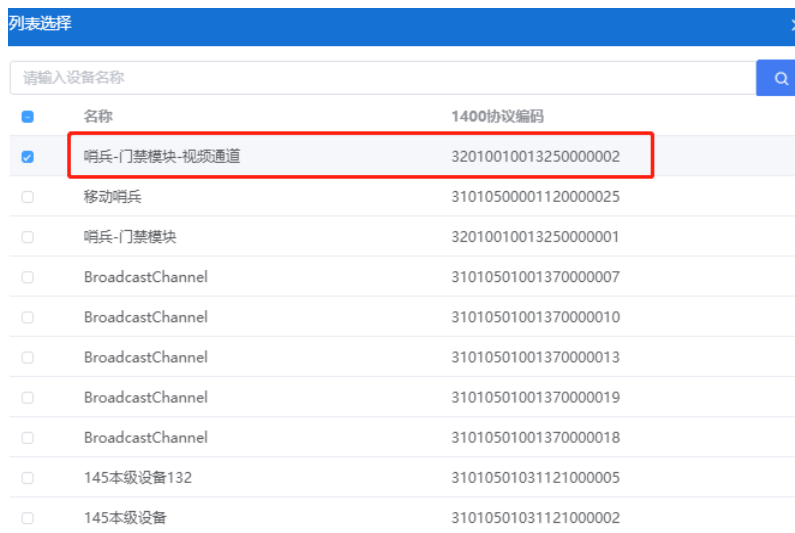


图 3-25 列表选择

◆ 全景录入

属性模块	属性名称	填写说明
设备类型	选择类型	选择“哨兵设备”

- 2) 进入设备审核界面，选择待审核的哨兵设备，点击，即对新录入的全景和全景视频通道审核通过。



图 3-26 审核

**i** 注意：和门禁模块一样，全景视频通道的国标 ID 需含有“132”的 20 位数字，全景国标 ID 需含有“112”的 20 位数字。

### 3.6.2 Web 端协议配置

分别登录门禁模块 Web 端和全景模块 Web 端，进行网络协议的配置。

**i** 说明：全景模块默认 IP 为 192.168.1.100；门禁模块默认 IP 为 192.168.1.101:8080。

#### 3.6.2.1 门禁模块

门禁模块主要配置 SIP 协议、COI 协议、Pigeon Platform 协议、PDNS 协议。

➤ SIP 协议：登录门禁模块 Web 端，进入**配置>网络>接入协议>SIP**界面。

ONVIF SIP DPSS VIID COI Pigeon Platform PDNS

---

注册平台

启用

本地端口  1024-65535

入网ID

设备名称

平台ID

平台地址

平台端口  1024-65535

注册用户名

注册密码

续租时间  (秒) 30~999999

心跳间隔  (秒) 10~1000

设备归属

行政区域

警区

安装地址

GB视频编码通道ID	GB视频编码通道名称	IPC码流类型
31000000001325001110	enc	主码流

告警ID	告警名称	有效性
------	------	-----

国标兼容次序

国家标准->国标扩展(2014)->国标扩展(2016)

扩展配置 <<

可选扩展配置

扩展配置

安全等级

图 3-27 SIP 界面

➤ COI 协议：登录门禁模块 Web 端，进入配置>网络>接入协议>COI 界面。

ONVIF SIP DPSS VIID COI Pigeon Platform PDNS

---

启用

URL

图 3-28 COI 界面

- Pigeon Platform 协议：登录门禁模块 Web 端，进入配置>网络>接入协议>Pigeon Platform 界面。

ONVIF	SIP	DPSS	VIID	COI	Pigeon Platform	PDNS
启用	<input checked="" type="checkbox"/>	平台地址	1.58.29.170		平台端口	8081 0~65535
用户编号	2435		用户名称	4365		
部门编号	24346		部门名称	24345		
SIP						
入网ID	00000000000000000000		注册密码	●●●●●●		
视频通道列表	1	编辑			0~1	
报警通道列表	0	编辑			0~1	
更多参数	配置					
保存						

图 3-29 Pigeon Platform 协议

- PDNS 协议：登录门禁模块 Web 端，进入配置>网络>接入协议>PDNS 界面。

ONVIF	SIP	DPSS	VIID	COI	Pigeon Platform	PDNS
启用	<input checked="" type="checkbox"/>	序列号	42255		名称	name
APPID	appid		APPKEY	●●●●●●		
PDNS地址	1.58.29.170		PDNS端口	4502 1~65535		
连接状态	需要注册PDNS					
保存						

图 3-30 PDNS 协议

### 3.6.2.2 全景模块

全景模块主要配置 SIP 协议、VIID（视图库）协议、Pigeon Platform 协议、PDNS 协议。

- SIP 协议：登录全景模块 Web 端，进入配置>网络>接入协议>SIP 界面。

SIP VID Pigeon Platform PDNS

注册平台 注册平台 1

启用

本地端口 5060 1024-65535

入网ID 3100000001125001116

设备名称 IPCAMERA

平台ID 310200000200000001

平台地址 221.224.163.198

平台端口 5900 1024-65535

注册用户名 3100000001125001116

注册密码 ●●●●●●

续约时间 60 (秒) 30-999999

心跳间隔 30 (秒) 10-1000

设备归属 owner

行政区域

警区

安装地址

添加 修改 删除

GB视频编码通道ID	GB视频编码通道名称	IPC码流类型
3100000001325001111	enc	主码流

添加 修改 删除

告警ID	告警名称	有效性
国标兼容次序		
国标标准->国标扩展(2014)->国标扩展(2016)		
修改国标兼容次序		
扩展配置>>		

保存

图 3-31 SIP

- VIID（视图库）协议：登录全景模块 Web 端，进入配置>网络>接入协议>VIID 界面。

SIP	VIID	Pigeon Platform	PDNS
注册视图库		视图库	
启用		<input checked="" type="checkbox"/>	
入网ID		31000000001325001111	
平台地址		106.14.159.176	
视图库端口		30963	1~65535
注册用户名		admin	
注册密码		•••••	
心跳时间		60	30~300
安装地址		1	
行政区域划分		1	
发送方式		图片集合	(项目不支持该选项的以实际发送为准)
图传优先		<input type="checkbox"/>	
自动校时		<input type="checkbox"/>	
校时时间间隔		60	1~65535
<input type="button" value="保存"/>			

图 3-32 VIID (视图库) 协议

➢ Pigeon Platform 协议：登录全景模块 Web 端，进入配置>网络>接入协议>Pigeon Platform 界面。

SIP	VIID	Pigeon Platform	PDNS
启用		<input checked="" type="checkbox"/>	
平台地址		1.58.29.170	
平台端口		8081	0~65535
用户编号		2435	
用户名称		4365	
部门编号		24346	
部门名称		24345	
<b>SIP</b>			
入网ID		00000000000000000000	
注册密码		••••••••	
视频通道列表		1	<input type="button" value="编辑"/> 0~1
报警通道列表		0	<input type="button" value="编辑"/> 0~1
更多参数		<input type="button" value="配置"/>	
<input type="button" value="保存"/>			

图 3-33 Pigeon Platform 协议

➢ PDNS 协议：登录全景模块 Web 端，进入配置>网络>接入协议>PDNS 界面。

SIP	VIID	Pigeon Platform	PDNS
启用	<input checked="" type="checkbox"/>		
序列号	<input type="text" value="42255"/>		
名称	<input type="text" value="name"/>		
APPID	<input type="text" value="appid"/>		
APPKEY	<input type="password" value="•••••"/>		
PDNS地址	<input type="text" value="1.58.29.170"/>		
PDNS端口	<input type="text" value="4502"/>		1~65535
连接状态	需要注册PDNS		

图 3-34 PDNS 协议

### 3.7 Web 端登录

设备激活完成后将自动重启。待设备重启后，在浏览器地址栏输入防爆哨兵各模块的 IP 地址，进入 Web 客户端登录界面。输入用户名 admin 及激活时设置的密码，进入 Web 客户端。



图 3-35 登录

**i** 说明：若 3 次输入错误的用户名或密码后，设备 IP 将被锁定 10 分钟，此段时间不能登录设备。若忘记密码，可参考如下步骤重置密码。

- 1) 打开 IPCSearch，选择需要重置密码的设备，点击“密码重置”，弹出如下界面；



图 3-36 密码重置

- 2) 点击访问密码重置界面提供的链接或使用移动端扫描图 3-36 中的二维码，并填入序列号和激活时设置的邮箱，如图 3-37。点击“获取安全码”；



重置密码

序列号 7637D72725F90CAACA2C0DD926FFE294E11379F40  
A50C0C08D7C6E7CA57FDA14

邮箱地址 12563@123.com 邮箱地址可用

验证码 37XX

获取安全码

图 3-37 重置密码

- 3) 登录邮箱获取安全码，并将之填入图 3-36 中的安全码栏，点击“确认”。请记住弹出的提示窗中显示的新密码，点击“确认”，设备将自动重启。

## 4 门禁模块操作

防爆型电子哨兵主体即门禁模块，因本设备属于防爆系列，均无法触摸操作，需通过我司 scrcpy 工具在 windows 系统中登录。本章节主要介绍通过 scrcpy 工具来操作门禁模块的说明。



### 4.1 门禁界面说明

登录门禁 UI 界面需要 scrcpy 工具并配合特定的命令来实现，详细操作请咨询我司相关人员。本章节仅介绍登录门禁 UI 界面后的说明。下图为门禁 UI 界面。




图 4-1 主界面

#### ➤ 主界面图标说明

图标	说明	图标	说明
	4G 网络		接入视图库平台
	接入 COI 平台		存储卡

#### ➤ 菜单界面

点击主界面，长按鼠标 3 秒，弹出如下密码登录框，输入激活门禁模块时的密码（门禁模块激活时的密码），进入菜单界面，点击图标，确认后返回主界面。

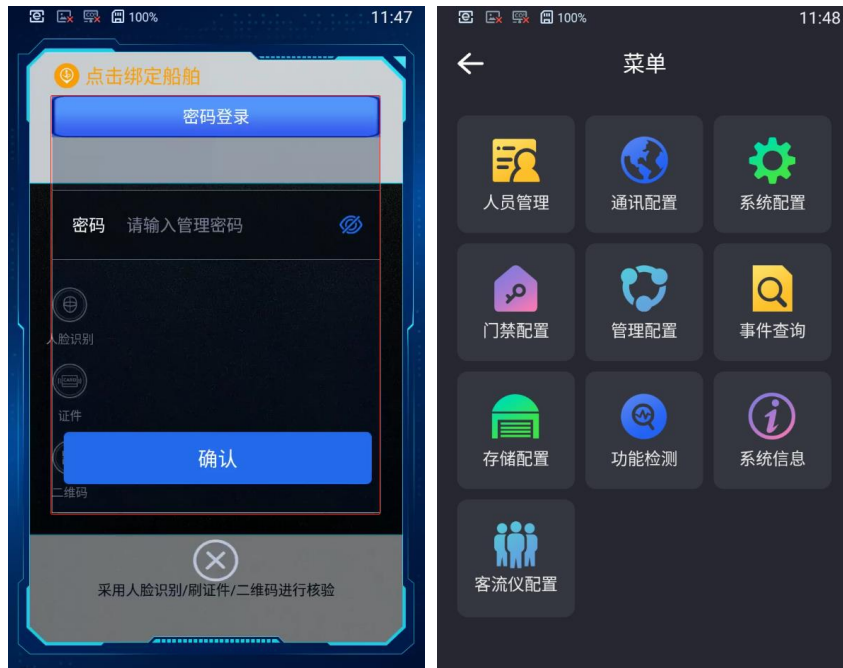


图 4-2 登录菜单界面

## 4.2 人员查询

进入**菜单>人员管理>人员查询**，支持通过姓名或证件号查询平台已下发的人员信息。

**i**说明：

- ◆ 输入姓名或证件号，点击“查询”。完成人员信息搜索。
- ◆ 直接点击“查询”，可查看所有下发至哨兵本地的人员信息以及正常通行是产生的临时人员信息。



图 4-3 人员管理

## 4.3 通讯配置

### 4.3.1 以太网

进入**菜单>通讯配置>以太网**，可查询门禁模块的网络信息。

**i** 说明：该部分配置信息以出厂默认即可，不建议用户手动修改。



图 4-4 以太网

### 4.3.2 其他

进入**菜单>通讯配置>其他**，可查看或修改全景模块和转接板模块的 IP 地址信息。

**i** 说明：全景模块和转接板模块的 IP 地址需根据实际场景来修改。



图 4-5 其他

## 4.4 系统配置

### 4.4.1 基本信息

进入**菜单>系统配置>基本信息**，可根据场景需要修改各项基本参数信息。



图 4-6 基本信息

➤ 语音音量

拖动语音音量滑块，可调节设备语音音量，范围为 0~100，默认为 90。若设置为 0，则不进行语音提示。

➤ 文字提示

- 1) 点击“文字提示”，进入文字提示界面；
- 2) 选择用户在识别时主界面显示的文字提示信息，可选择姓名、证件号、姓名&证件号或关闭；若选择关闭，则识别时主界面将不会显示文字提示信息；
- 3) 点击“隐藏姓名”，可将姓名部分隐藏；
- 4) 点击“保存”，即可完成配置。

➤ 灯光提示

默认绿灯&红灯，即核验成功，绿灯提示；核验失败或未核验，红灯提示。用户可根据现场需要选择红灯、绿灯或关闭。

- 红灯：核验成功无灯光提示，核验失败或未核验红灯提示。
- 绿灯：核验成功绿灯提示，核验失败或未核验无灯光提示。
- 无：任何状态下都无灯光提示。

➤ 白关灯控制

用户可根据现场需要选择低、中、高。

➤ 自动熄屏

点击“自动熄屏”按钮，可开启/关闭自动熄屏功能。开启后，可以设置自动熄屏时间，范围为 10~300s。在相应时间内未对设备进行操作，设备会跳转至待机界面。若关闭该功能，则设备不会自动熄屏。

#### ➤ 返回屏保

点击“返回屏保”按钮，可开启/关闭自动熄屏功能。开启后，可以设置自动熄屏时间，范围为 10~300s。在相应时间内未对设备进行操作，设备会跳转至待机界面。若关闭该功能，则设备不会自动熄屏。

#### ➤ 熄屏检测

点击“熄屏检测”按钮，可开启/关闭熄屏检测功能。开启后，设备在熄屏状态下检测到人脸后，自动显示核验页面。若关闭熄屏检测功能，当设备处于熄屏状态，需点亮屏幕后再进行核验。

#### ➤ 选择屏保

根据现场需要，选择屏保图像。

设置完成后，点击“保存”即可。

### 4.4.2 时间配置

进入**菜单>系统配置>时间配置**，可配置时间格式，修改时间等信息。



图 4-7 时间配置

#### ➤ 时间格式

点击“时间格式”，选择设备显示的时间格式，可选择 MM-dd-yyyy、dd-MM-yyyy 或 yyyy-MM-dd；点击“保存”按钮，即可完成设置。

#### ➤ 时间

点击“时间”，进入时间设置界面，可手动设置系统时间；点击“保存”按钮，即可完成设置。

#### ➤ 夏令时：点击“夏令时”按钮，可开启/关闭夏令时设置，可设置开始时间、结束时间和偏移时间。

- 开始时间：点击“开始时间”，进入开始时间界面，可手动设置夏令时开始时间，默认为四月首个星期日 02 时；点击“保存”按钮，即可完成设置。

- 结束时间：点击“结束时间”，进入结束时间界面，可手动设置夏令时结束时间，默认为十月末个星期日 02 时；点击“保存”按钮，即可完成设置。
- 偏移时间：选择偏移时间，可选择 30 分钟、60 分钟、90 分钟或 120 分钟，默认为 30 分钟。

设置完成后，点击“保存”即可。

#### 4.4.3 人脸参数

进入**菜单>系统设置>人脸参数**界面，可以进行人脸姿态阈值、人脸比对阈值（1：N）、人脸比对阈值（1：1）等设置。



图 4-8 人脸参数

- 人脸姿态阈值：设置人脸识别姿态分阈值，范围为 0~100 分。设备将根据上下俯仰角度、左右水平角度、眼间距等因素对人脸进行姿态评分；若评分低于预设值，则人脸检测不通过，人脸比对或录入失败。
- 人脸比对阈值（1：N）：设置人脸 1：N 比对时的阈值，范围为 0~100 分。阈值越高，则误识率越低，拒认率越高。
- 人脸比对阈值（1：1）：设置人脸 1：1 比对时的阈值，范围为 0~100 分。阈值越高，则误识率越低，拒认率越高。
- 活体检测：点击“活体检测”按钮，可开启/关闭活体检测功能。开启后，设备可判断对象是否为真人本人，可有效甄别照片、换脸、面具、遮挡、屏幕翻拍等欺诈行为；若识别对象不是本人，则人脸比对或录入失败。
- 活体检测安全等级：开启活体检测功能后，可设置活体检测安全等级，可选择普通或高；若选择高，则误识率低，拒认率高。
- 人脸识别距离：拖动滑块可设置人脸识别距离，范围为 0.3~2.5m，默认为 1.5m。

设置完成后，点击“保存”，即可完成配置。

#### 4.4.4 高级配置

进入**菜单>系统设置>高级配置**界面，可进行删除人员数据、删除事件数据、恢复默认设置等操作。



图 4-9 高级配置

➤ 删除人员数据

点击“删除人员数据”，在弹出的提示框中点击“确定”，设备将清除所有人员信息。

➤ 删除事件数据

点击“删除事件数据”，在弹出的提示框中点击“确定”，设备将清除所有事件信息。

➤ 恢复默认设置

点击“恢复默认设置”，在弹出的提示框中点击“确定”，重启后设备将恢复默认设置。

➤ 恢复出厂

点击“恢复出厂”，在弹出的提示框中点击“确定”，重启后设备将恢复出厂状态。

➤ 重启设备

点击“重启设备”，将重新启动门禁模块。

➤ 呼叫求助

点击“呼叫求助”，开启或关闭呼叫求助功能；开启后，主界面将显示呼叫求助。

**i** 说明：该功能需要接入特定的平台，哨兵暂不支持。



图 4-10 呼叫求助

➤ 场景模式

根据设备安装的场景选择相应的模式，可选择室内模式或室外模式。

➤ 设备类型

根据实际场景选择设备类型。

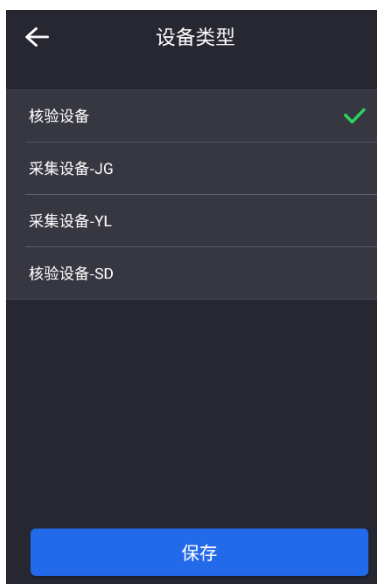


图 4-11 设备类型

➤ 门锁状态恢复：强制恢复门锁状态。

**i** 说明：哨兵暂不支持该功能。

➤ 加热除雾

点击开启全景模块和门禁模块的镜头除雾功能。

➤ RFID 真伪校验

默认不开启该功能，未启用 RFID 真伪校验，设备在解析用户的护照时，仅根据用户图片来解析，开启后，会再次校验护照内的芯片。

#### 4.4.5 语言

进入**菜单>系统配置>语言**界面，可设置门禁模块的语言。

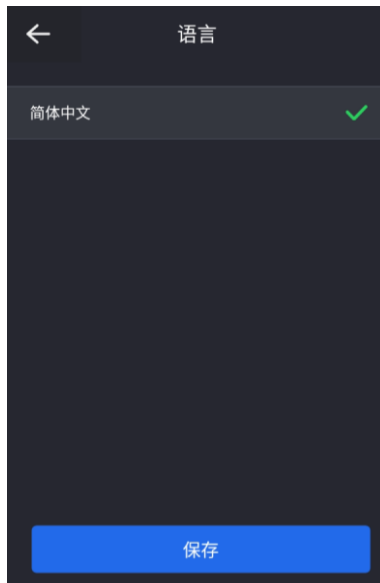


图 4-12 语言

#### 4.5 门禁配置

进入**菜单>门禁配置**界面，可设置门禁默认核验方式、授权方式、识别报警次数等。



图 4-13 门禁配置

各参数说明如下：

- 默认核验方式：点击“默认核验方式”，进入默认核验方式界面。

**i** 注意：核验方式以出厂默认即可，若需修改请联系我司客服人员咨询。

- 授权方式：设置核验方式对应的授权方式。人脸默认前端授权，人证 1:1 默认联网授权。
- 关门延迟时间：根据现场需求设置关门延迟时间。
- 识别报警次数：设置最大识别次数，范围 1~255 次；若连续识别失败次数超过该最大值，则会触发报警。
- 开门信号去重：哨兵暂不支持该功能。
- 待通行人员超时时间：核验成功后的人员未正常通行，在核验区域等待时间超过该处设置时间即警告提示。

## 4.6 管理配置

进入**菜单>管理配置**界面，可以修改 admin 用户的密码。



图 4-14 管理配置

点选用户，进入管理员信息界面；点击“修改密码”，进入修改密码界面；输入原密码和新密码，再输入一遍新密码完成确认；点击“保存”，即可完成密码修改。

### ①说明：

- ◆ 为了提高产品网络使用的安全性，建议您设置为高强度密码，密码长度必须达到 8-16 个字符，且至少由数字和字母或特殊字符中的两种或两种以上类型组合而成。
- ◆ 请您定期更改用户名的密码，建议每 3 个月更新一次密码。如果设备在较高安全风险的环境中使用，建议每月或每周更新一次。
- ◆ 请妥善保管好您的用户名与密码。

## 4.7 事件查询

哨兵暂不支持该功能。

## 4.8 存储配置

进入**菜单>存储配置**界面，可查看存储状态和存储策略。



图 4-15 存储配置

➤ 存储状态：查看该设备的容量状态。



图 4-16 存储状态

➤ 存储策略：设置存储空间不足时的录像策略。

- 覆盖：当存储空间不足时，覆盖最旧录像。
- 存满停止：当存储空间不足时，自动停止录像。

## 4.9 功能检测

进入**菜单>功能检测**界面，可进行声音检测、读卡器检测、IO 检测和网络检测。

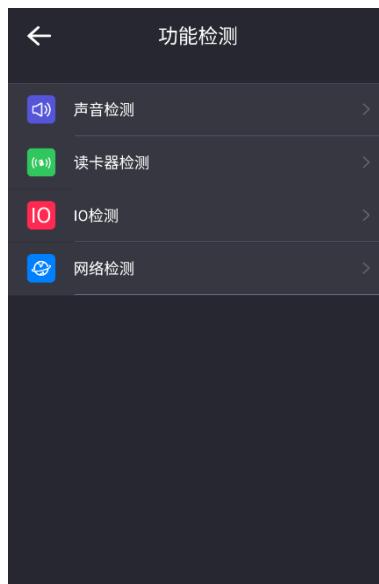


图 4-17 功能检测

#### 4.9.1 声音检测

进入**菜单>功能检测>声音检测**界面，可检测设备声音功能是否正常。

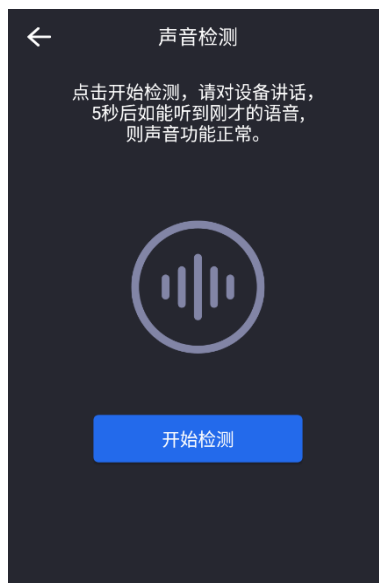


图 4-18 声音检测

点击“开始检测”，对设备讲话，若 5 秒后能正常听到录入的语音，则表示声音功能正常。

#### 4.9.2 读卡器检测

进入**菜单>功能检测>读卡器检测**界面，可检测设备读卡器是否正常。

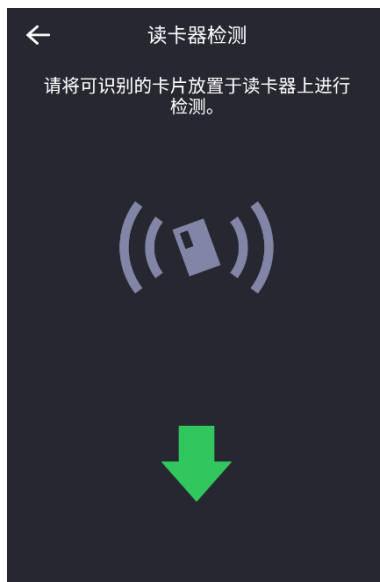


图 4-19 读卡器检测

将可识别的身份证放置于设备身份证阅读区域进行检测，若能正常读取，则表示设备读卡器功能正常。

#### 4.9.3 IO 检测

哨兵暂不支持本功能操作。

#### 4.9.4 网络检测

进入**菜单>功能检测>网络检测**界面，可检测设备是否成功连接到网络。

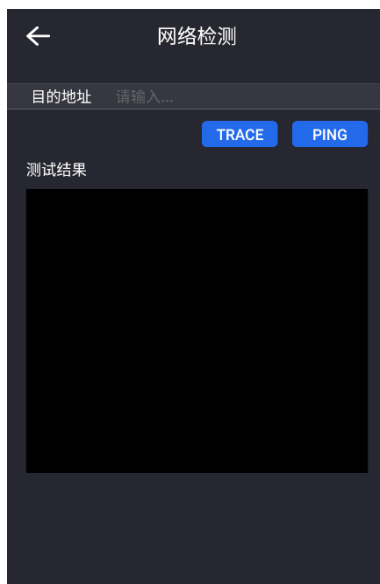


图 4-20 网络检测

- PING: 在“IP 地址”栏中，输入目标设备的 IP 地址，点击“ping”，在测试结果栏中显示访问目标地址的结果，可检测设备与目标设备之间的网络是否连通。
- TRACE: 在“IP 地址”栏中，输入目标设备的 IP 地址，点击“trace”，在测试结果栏中显示访问目标地址的路由条目，可检测设备与目标设备之间的网络路由信息。

## 4.10 系统信息

进入**菜单>系统信息**界面，可查看设备信息和设备日志。

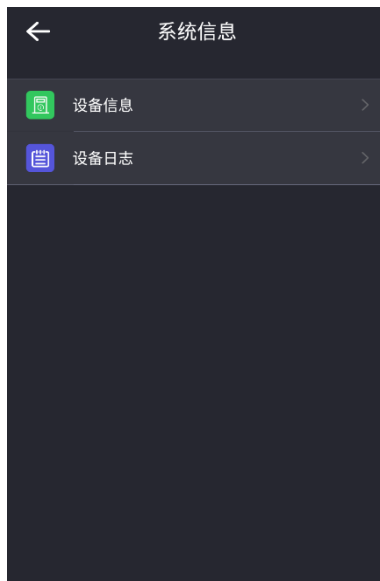


图 4-21 系统信息

### 4.10.1 设备信息

进入**菜单>系统信息>设备信息**界面，可查看设备型号、设备序列号、硬件版本号等设备信息。



图 4-22 设备信息

### 4.10.2 设备日志

进入**菜单>系统信息>设备日志**界面，可进行设备日志设置。

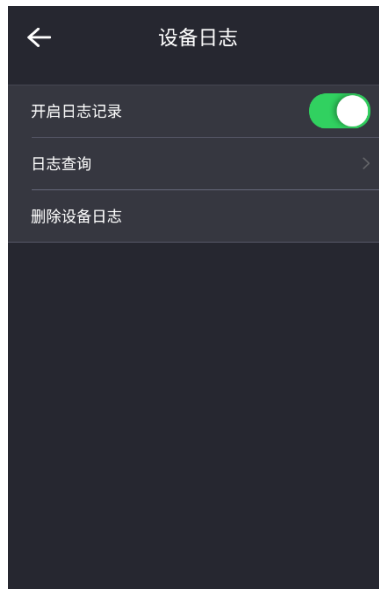


图 4-23 设备日志

➤ 开启日志记录

点击按钮，可开启/关闭设备日志记录功能，设备可记录用户操作、告警信息、系统任务和系统异常日志。

➤ 日志查询

点击“日志查询”，进入日志查询界面，根据日志类型或者日志时间查询日志信息。

➤ 删除设备日志

点击“删除设备日志”，确定后可删除设备日志。

## 5 通行

通行可分为正常通行和异常通行。

### 5.1 正常通行

人员至门禁模块前核验成功且顺利通过客流仪下方，为一次正常通行。

正常通行需至门禁模块前进行核验。核验可分为证件核验和人脸核验，核验成功后，核验人员可正常通行，客流仪会产生进出统计，并发送给后端平台。

**说明：**正常通行人员一般由平台下发，且人员通行记录也需进入精准平台查询。详细可参考《精准平台用户手册》。

通行记录列表

下载当前页

关注	人员姓名	通行时间	通行方向	核验状态	船舶	航次	人员身份	国籍
☆	时强	2021-09-03 16:56:13	下船	核验通过	含信	3282020101053	船员	中国
☆	时强	2021-09-03 16:36:37	下船	核验通过	含信	3282020101053	船员	中国
☆	时强	2021-09-03 16:36:31	上船	核验通过	含信	3282020101053	船员	中国

图 5-1 通行记录

#### 5.1.1 证件核验

防爆哨兵主体部分有身份证核验区域、二维码核验区域和护照核验区域。

**说明：**证件核验前需确认设备已接入 COI。若设备未正常接入网络，则无法进行证件核验，仅可通过人脸核验。

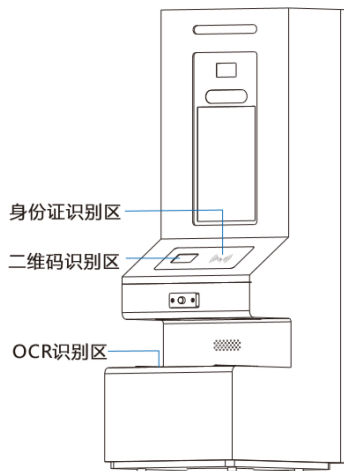


图 5-2 哨兵主体

##### 5.1.1.1 身份证核验

核验步骤如下：

- 1) 将身份证按照下图放置于身份证核验区域；

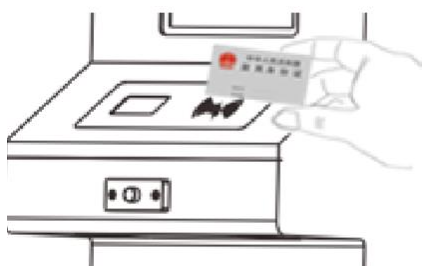


图 5-3 身份证核验

2) 当门禁主界面显示“请正对屏幕”，可以拿开身份证；

**i**说明：若主界面长时间未显示“请正对屏幕”，可能是身份证读取失败。需要拿开身份证，重新放置于核验区域。

3) 核验人员人脸正对镜头。若核验成功，界面显示“核验成功，请通行”。若核验失败，界面显示“核验失败”。

**i**注意：核验过程中，若身份证照片和人脸不符，或者该身份证件未进行后端平台登记，都将导致核验失败。

**i**说明：身份证核验成功后，会将该人员信息录入哨兵人员库。此时登录门禁模块，进行人员查询，可查询到该人员信息。

### 5.1.1.2 二维码核验

核验步骤如下：

1) 将二维码对准扫描区域。如下图；



图 5-4 二维码核验

**i**说明：

- ◆ 若长时间扫描不成功，请重新移动二维码。
- ◆ 若环境下光线较强烈，也会导致扫描不成功，此时需要用手遮挡住强光的照射。

2) 扫描成功后，拿开二维码；

**i**说明：出现以下任一提示即扫描成功：“滴”的提示音、屏幕提示“请正对屏幕”、屏幕提示“请稍后”，即扫描成功。

3) 核验人员人脸正对镜头。若核验成功，界面显示“核验成功，请通行”。若核验失败，界面显示“核验失败”。

**i**注意：核验过程中，若后端登记的二维码人员信息和核验人脸不符，会导致核验失败。

**i**说明：二维码核验成功后，会将该人员信息录入哨兵人员库。此时登录门禁模块，进行人员查询可查询到该人员信息。

### 5.1.1.3 护照核验

核验步骤如下：

1) 将护照人员信息页放置到护照核验区域。如下图；

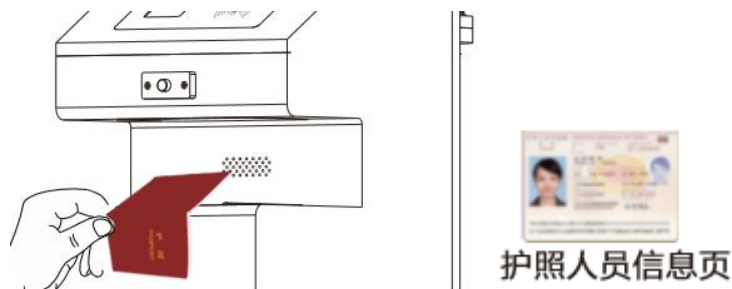


图 5-5 护照核验

2) 核验人员人脸正对镜头。若核验成功，界面显示“核验成功，请通行”。若核验失败，界面显示“核验失败”；

**i**注意：

- ◆ 若人脸未正对镜头，会提示“请正对屏幕”，直到核验成功或者失败的提示。
- ◆ 核验过程中，若护照照片和人脸不符，或者该护照未进行后端平台登记，都将导致核验失败。

3) 核验成功后，取出护照，正常通行。

**i**说明：护照核验成功后，会将该人员信息录入哨兵人员库。此时登录门禁模块，进行人员查询可查询到该人员信息。

### 5.1.2 人脸核验

核验人员走至客流仪下方，正对门禁模块镜头，核验成功后，显示“核验成功，请通行”。若该人员非人员库内人员，将提示“核验失败”。

**i**说明：

- ◆ 人脸核验可在无网络情况下进行，核验成功后的通行记录在恢复网络后，会将该通行记录重新上传至平台。
- ◆ 平台下发至哨兵人员库的白名单人员和证件核验成功后的人员一般均可通过人脸核验。

## 5.2 异常通行

异常通行指人员核验失败后强行通行。异常通行后，设备将产生“请禁止通行”的语音告警。

以下均为异常通行的场景：

- 未经过核验，直接通行；
- 核验失败，直接通行；
- 人脸核验或者证件核验时，未提示“核验成功，请通行”，直接通行；
- 一人核验成功后，同时两人通行；

 说明：此时会产生两条通行记录。

- 未经过核验，直接通行，后期又返回重新核验；
- 核验成功后，在核验区域停留时间较长。

## 6 其他功能

### 6.1 一键呼叫

防爆哨兵主体区域有 SOS 一键呼叫按钮，当有突发状况时，可以通过点按此按钮来呼叫后端平台，并建立和后端的实时语音通话。

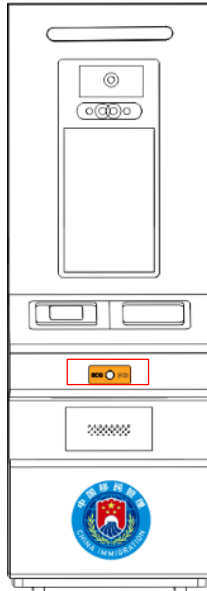


图 6-1 SOS 按钮

### 6.2 全景语音播报

当有人员靠近防爆哨兵时，哨兵将提示“上下船舶，请出示证件”的语音提示。此时该人员可进入核验区进行核验并通行。

## 7 门禁 Web 客户端

登录门禁 Web 端，用户可对该模块进行网络管理、平台接入等功能。

**i** 说明：门禁模块默认 IP 为 192.168.1.101:8080。

### 7.1 开始使用

登录 Web 客户端前需确认设备与电脑已经连接并且网络互通。

**i** 注意：将产品接入互联网需自担风险，包括但不限于产品可能遭受网络攻击、黑客攻击、病毒感染等，本公司不对因此造成的产品工作异常、信息泄露等问题承担责任，但本公司将及时为您提供产品相关技术支持。

电脑配置要求如下：

- 处理器：3.3GHz Intel 酷睿 i3 系列及以上或相同性能的其他处理器
- RAM 内存：4GB 及以上
- 操作系统：Windows7 操作系统或更高版本
- 浏览器：推荐使用 IE 内核浏览器，使用其它内核浏览器会影响客户端部分功能的使用
- DirectX：9.0

### 7.2 Web 界面说明

- 登录 Web 客户端

设备激活完成并修改网络参数后将自动重启。待设备重启后，在浏览器地址栏输入门禁模块 IP 地址 “http://设备的 IP 地址:8080/”，进入 Web 客户端登录界面。输入用户名 admin 及激活时设置的密码，进入客户端。



图 7-1 Web 客户端登录界面

首次成功登录后，请下载插件，按照窗口提示安装插件。安装插件时需要关闭浏览器，安装完成后重新登录。登录成功后界面如下图。

**i** 注意：推荐使用 IE 内核浏览器，使用其他内核浏览器会影响客户端部分功能的使用。

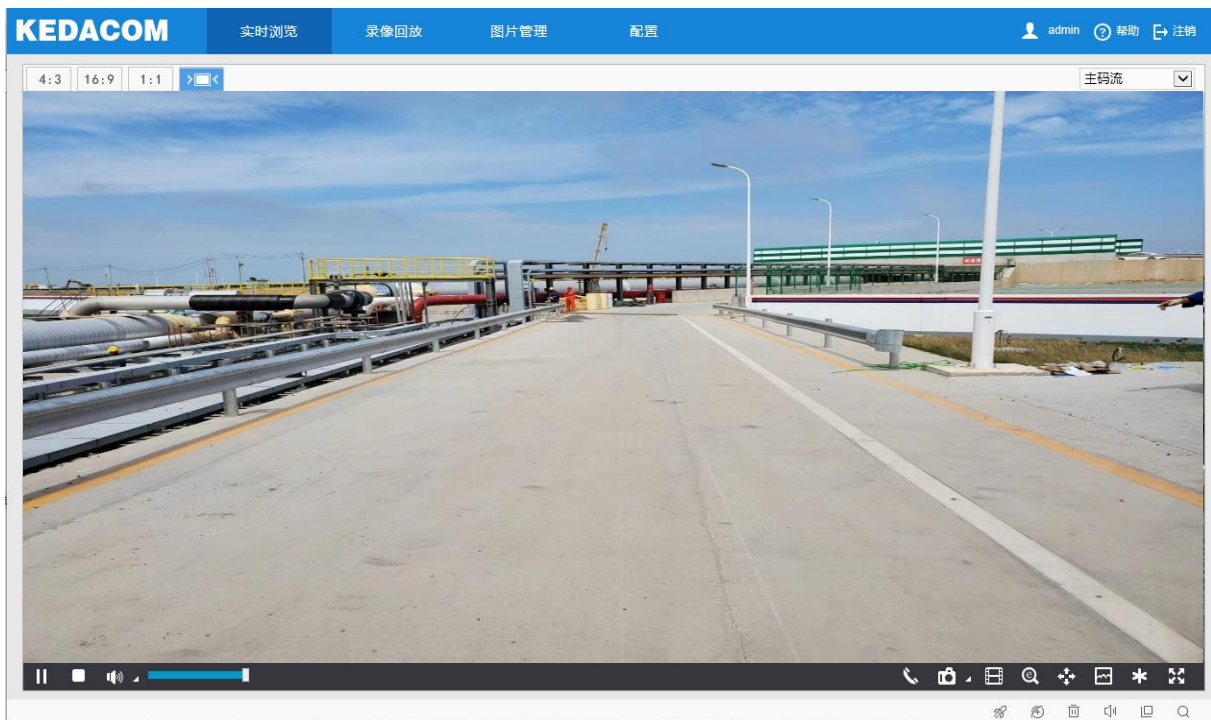


图 7-2 客户端操作界面

#### ➤ 登出 Web 客户端

点击客户端操作界面右上角的 **注销** 按钮，安全退出登录。

#### ➤ 帮助

点击界面右上角的 **帮助** 按钮，弹出联机帮助页面，可查看设备的帮助文档。

#### ➤ 主界面说明

在 Web 客户端主界面，您可以进行实时浏览、录像回放、图片管理、配置等操作。

- 实时浏览：预览门禁模块的实时监控画面并根据需要呼叫、截图、录像等。
- 录像回放：按时间查找录像并进行回放及下载。
- 图片管理：按图片类型查询、查看和下载图片文件。
- 配置：对设备进行参数设置及功能配置。

## 7.3 实时浏览

点击“实时浏览”，进入哨兵门禁模块的浏览界面。

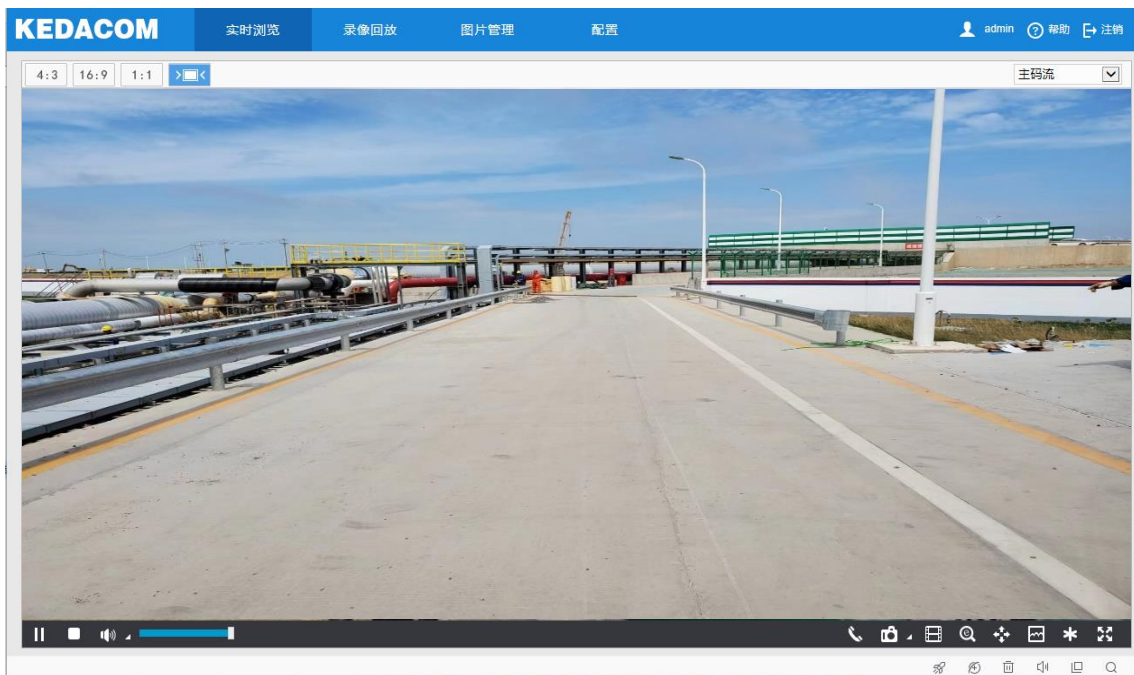





图 7-3 实时浏览

➤ 画面尺寸

图标	功能说明
4:3	表示预览画面以 4 比 3 的比例显示。
16:9	表示预览画面以 16 比 9 的比例显示。
1:1	表示预览画面以 1 比 1 的比例显示。
>◻◀	表示预览画面自适应显示浏览窗口。

➤ 预览工具栏

图标	功能说明
	开始/暂停，点击该按钮，播放视频浏览画面，再次点击，暂停播放。
	停止，点击该按钮，停止视频浏览。
	音量，本地解码音量。点击  按钮，选择开启或关闭音量；点击 ，选择声道。
	拖动滑块可调节音量大小。
	语音呼叫前端设备，点击开始对讲，再次点击停止对讲。
	抓拍，点击  即可抓拍当前画面。点击  选择浏览抓拍或前端抓拍，浏览抓拍指电脑客户端抓拍图像，前端抓拍指人脸门禁设备抓拍图像。
	开始录像/停止录像，点击按钮开始录像，再次点击停止录像。
	EPTZ，电子放大。单击按钮，按住鼠标左键不放，向右下方框选出某一区域，可以扩大该区域的像素并使该区域铺满画面；按住鼠标左键不放，向左上方框选区域使画面恢复。

图标	功能说明
	状态，点击显示帧率和码率，再次点击，隐藏。该按钮默认不显示，需要时请在配置>本地配置界面勾选状态信息显示。
	视频冻结，点击该按钮，监控画面将显示点击前最后一帧画面，再次点击取消冻结，显示实时画面。
	全屏，点击该按钮，显示全屏画面，在全屏画面中双击鼠标左键或按 Esc 键退出全屏。

## 7.4 录像回放

点击“录像回放”进入录像回放界面，可对保存在存储卡上的录像进行搜索、查看、下载等操作。录像回放界面如下图所示。

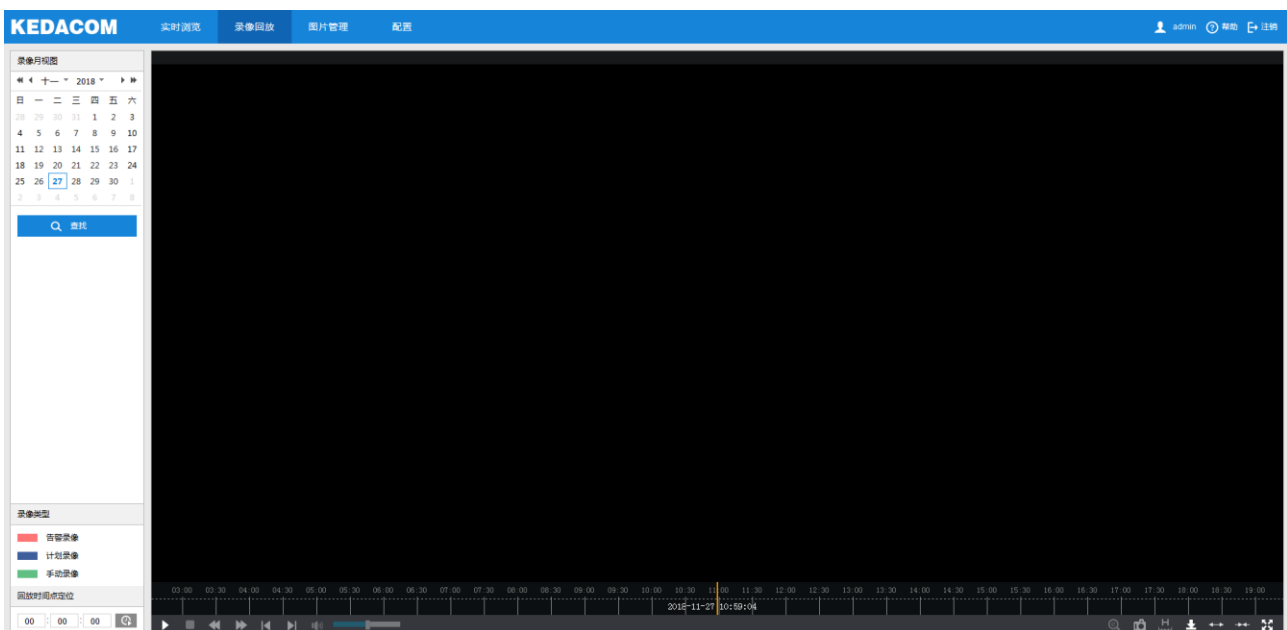


图 7-4 录像回放

具体操作步骤如下：

- 1) 选择录像时间，在录像月视图中选择需要查看录像的日期，如果月视图中的某个日期右下角有蓝色三角标记，则代表该天有监控录像存储；
- 2) 点击“查找”，录像文件显示在时间轴上（时间轴上高亮显示）；














**i** 说明：蓝色表示计划录像，绿色表示手动录像。

- ◆ 计划录像：通过设置设备在某些时间段自动录像。在配置>存储>录像界面进行设置即可。
- ◆ 手动录像：即在门禁设备与平台网络断开的情况下，设备默认开启录像。

- 3) 点击界面下方的播放按钮即可播放录像，在回放录像过程中，可以通过录像回放下方的工具栏对回放的录像进行剪辑、快进、下载等操作；
- 4) 鼠标箭头放在录像时间轴可显示录像时间信息，双击鼠标左键或者按住鼠标左键再左右移动时间轴可进行录像

跳播。也可以通过设置“回放时间点定位”的回放时间，点击  按钮来选择回放时间点。

录像回放界面工具栏按钮说明如下表所示：

图标	功能说明
	播放/暂停，点击按钮播放录像，再次点击暂停播放。
	停止，点击该按钮，停止录像播放。
	减慢播放速度，点击可减慢播放速度，点击一次减慢至 1/2x，再次点击减慢至 1/4x，最低减慢至 1/8x。
	加快播放速度，点击可加快播放速度，点击一次播放速度加快一倍，最高调节到 8x。
	前一片段，点击播放上一个录像片段，可连续点击。连续录像中点击，默认跳播 1 小时。
	后一片段，点击播放下一个录像片段，可连续点击。连续录像中点击，默认跳播 1 小时。
	声音，点击打开声音，再次点击关闭声音，拖动滑块可调节音量。
	EPTZ，电子云台功能。单击按钮，按住鼠标左键不放，向右下方框选出某一区域，可以扩大该区域的像素并使该区域铺满画面；按住鼠标左键不放，向左上方框选区域使画面恢复。
	抓拍，点击即可抓拍当前回放画面。回放抓拍图片的保存路径可在 <b>配置&gt;本地配置</b> 的“回放抓拍保存路径”中设置。
	剪辑，点击即可开始对当前回放录像进行剪辑，再次点击则停止剪辑。回放剪辑录像的保存路径可在 <b>配置&gt;本地配置</b> 的“回放剪辑保存路径”中设置。
	下载，点击该按钮，将弹出下载界面。在弹出的界面设置具体时间和下载录像类型后单击“查询”，符合条件的录像将显示在下方列表中，勾选需要下载的文件，点击“下载”即可下载，表格中下载进度栏可查看相应录像的下载进度。下载录像的保存路径可在 <b>配置&gt;本地配置</b> 界面的“回放下下载保存路径”中设置。
	放大/缩小时间轴，即调整时间轴单位刻度值，点击即可放大或缩小时间轴。时间轴单位刻度值等级为 5 分钟/10 分钟/30 分钟，放大或缩小时间轴不影响当前播放时间点。
	全屏，点击该按钮，显示全屏画面，在全屏画面中双击鼠标左键或者按 Esc 键退出全屏。

## 7.5 图片管理

在菜单栏中点击“图片管理”进入图片管理界面，可以根据需要搜索并下载保存在存储卡中的抓拍图片。

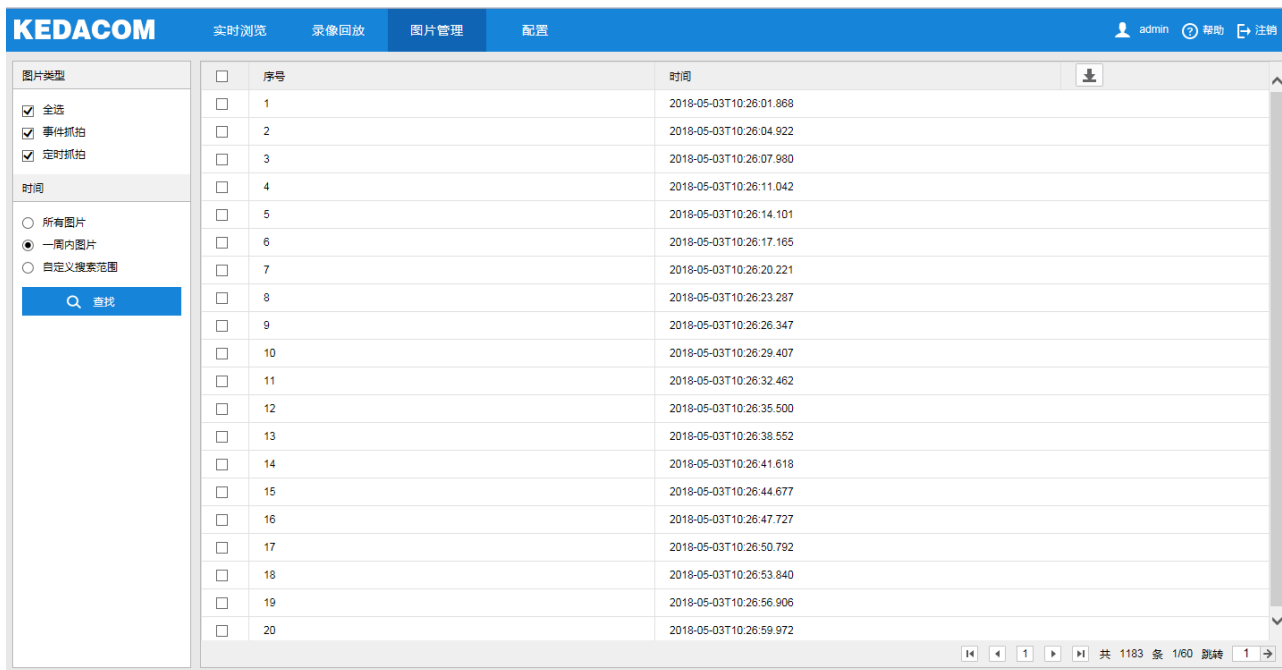



图 7-5 图片管理

图片搜索及下载具体步骤如下：

- 1) 在左侧的图片类型中勾选需要搜索的抓拍图片类型；
- 2) 在时间选项中选择搜索图片的时间范围，选择自定义搜索范围时需设置具体开始时间和结束时间；
- 3) 点击“查找”，搜索结果显示在右方列表中，在列表中可以看到图片序号和图片抓拍时间；
- 4) 勾选图片，点击  按钮，即可下载选中的图片。图片保存路径可在配置>本地配置界面的“前端抓拍保存路径”中设置。

## 7.6 配置

在菜单栏中点击“配置”进入配置界面，可进行本地配置、网络、事件等各项配置。

**i** 说明：本章节介绍哨兵的常用功能配置，其余配置项可点击界面“帮助”，来获取帮助文档，查看对应操作。



图 7-6 配置界面

### 7.6.1 网络

进入**配置>网络**界面，可设置门禁模块的网络参数，包括 IP 及端口、接入协议和其他协议。

#### 7.6.1.1 IP 及端口

##### 7.6.1.1.1 有线网络

进入**配置>网络>IP 及端口>有线网络**界面，配置有线网络参数，包括 IP 地址、子网掩码、默认网关等。

IP地址配置	
网卡	GLAN1
IP版本	IPV4
模式	DHCP
IP地址	10.67.7.86 <span>测试</span>
子网掩码	255.255.252.0
默认网关	10.67.7.254
MAC地址	00-14-1C-2A-2D-1B
MTU	1500 <span>1280~1500</span>
DNS服务器配置	
自动获取DNS	<input type="checkbox"/>
首选DNS服务器	<input type="text"/>
备用DNS服务器	<input type="text"/>
<span>保存</span>	

图 7-7 有线网络

#### ➤ IP 地址配置

IP 版本为 IPV4 时，可选择静态或 DHCP 模式。静态模式下，需根据实际情况输入 IP 地址、子网掩码和默认网关；DHCP 模式下，且所在网络中配置有 DHCP 服务，则设备将自动获取 IP。

**i**说明：填写 IPV4 地址时，可点击“测试”，确定该 IP 地址是否可用。

IP 版本为 IPV6 时，可选择自动获取或手动模式。自动获取模式下，由网络中的服务器、网关下发 IPV6 地址；手动模式下，需根据实际情况输入 IP 地址、子网掩码和默认网关。

“多播地址”即组播地址，门禁模块需要以多播方式被网络内设备发现时，根据实际需求填写即可。

**i**说明：多播是一种数据包传输方式，源主机可以只需要发送一份报文就可以到达组内每个需要接收的主机上，这中间还要取决于路由器对组内关系的维护和选择。

“MTU”项可以设置最大传输单元，指 TCP/UDP 协议网络传输中所通过的最大数据包的大小（以字节为单位），范围 500~1500，默认 1500。

**i**说明：MTU 越大通信效率越高，但传输延时增大。请根据实际需求填写。

#### ➤ DNS 服务器配置

设备需要通过域名访问时，需配置正确的 DNS 服务器地址。可以勾选“自动获取 DNS”或手动填写 DNS 服务器地址；若勾选“自动获取 DNS”，门禁模块将自动从网关获取 DNS 服务器配置参数，无需再手动填写。

设置完成后，点击“保存”即可。

#### 7.6.1.1.2 端口

进入配置>网络>IP 及端口>端口界面，可配置 HTTP 端口、HTTPS 端口、RTSP 端口参数，可根据需要设置相应的端口。

HTTP 端口	<input type="text" value="8080"/>	1~65535 (其中1~1024等端口不可使用)
HTTPS 端口	<input type="text" value="5544"/>	1~65535 (其中1~1024等端口不可使用)
RTSP 端口	<input type="text" value="1554"/>	1~65535 (其中1~1024等端口不可使用)

图 7-8 端口

- HTTP 端口：超文本传输协议端口，使用浏览器登录时需要在地址后面加上修改的端口号。如当 HTTP 端口号修改为 83 时，使用浏览器登录需要输入“http://设备 IP 地址:83”。默认为 80，范围为 1~65535。
- HTTPS 端口：超文本传输安全协议端口，使用浏览器登录时需要在地址后面加上修改的端口号。如当 HTTPS 端口号修改为 5545 时，使用浏览器登录需要输入“https://设备 IP 地址:5545”。默认为 5544，范围为 1~65535。
- RTSP 端口：实时传输协议端口，使用浏览器登录时需要在地址后面加上修改的端口号。如当 RTSP 端口号修改为 555 时，使用浏览器登录需要输入“rtsp://设备 IP 地址:555/id=0 (id=0 播放主流，id=1 播放辅流)”。默认为 554，范围 1~65535。

设置完成后，点击“保存”即可。

### 7.6.1.1.3 无线网络

进入**配置>网络>IP 及端口>无线网络**界面，可查看无线网络状态，配置无线网络连接。



图 7-9 无线网络

操作方法如下：

- 1) 点击模式栏，选择 STA；
- 2) 在热点列表中，选中需要添加的热点名称，点击右侧的添加图标；
- 3) 在弹出的添加连接窗口中输入密码，并勾选高级选项；
- 4) IP 模式默认为 DHCP，若选择静态 IP，还需手动输入 IP 地址、子网掩码、默认网关等信息；
- 5) 点击“保存”，即可连接到指定热点。

**i** 说明：点击“刷新”，可刷新热点列表。

### 7.6.1.1.4 地理定位

进入**配置>网络>IP 及端口>地理定位**界面，可定时将地理定位信息上传至监控中心。

操作方法如下：

- 1) 勾选“启用”；
- 2) 根据实际需求选择定位方式，默认“北斗导航&GPS 导航”；
- 3) 速度单位默认为“公里/小时”；
- 4) 当前状态，显示哨兵的地理定位信息。点击“刷新”，更新最新地理定位信息；
- 5) 点击“保存”即可。

### 7.6.1.1.5 多播

进入**配置>网络>IP 及端口>多播**界面，可根据实际需求设置码流类型、媒体类型、多播地址等多播参数，启用设备多播功能。

**i** 说明：多播是一种数据包传输方式，源主机可以只需要发送一份报文就可以到达组内每个需要接收的主机上，这中间还要取决于路由器对组内关系的维护和选择。

码流类型	主码流	
媒体类型	视频	
多播地址	0.0.0.0	
多播端口	61000	1~65535
发送模式	被动	
TTL	64	0~255

**保存**

图 7-10 多播

- 码流类型：需发送的码流，默认为主码流。
- 媒体类型：需发送码流对应的媒体类型，默认为视频。
- 多播地址：组网发送码流的地址，根据实际情况填写即可。
- 多播端口：多播地址对应的多播端口，范围为 1~65535，默认为 61000。
- 发送模式：可选择主动模式或被动模式。主动模式下，若多播地址正常、有效，则默认向此多播地址发送码流；被动模式下，当且仅当收到组播请求时，才会向多播地址发送码流。若多播地址为 0.0.0.0，则默认向 239.2.2.2 发送码流。
- TTL：即生存时间，范围为 0~255。

**i** 说明：TTL（生存时间）指 IP 数据包在被路由器丢弃前允许通过的最大网段数量，用于避免数据包在网络中无限循环收发，以节省网络资源。

## 7.6.1.2 接入协议

进入**配置>网络>接入协议**界面，可通过配置 SIP、ONVIF、COI 等协议，将设备接入相应的平台。

### 7.6.1.2.1 ONVIF

客户端支持 ONVIF 协议入网后端管理平台，可使不同厂商生产的网络视频产品（包括摄录前端、录像设备等）实现互通。设置方法如下：

- 1) 进入**配置>网络>接入协议>ONVIF**界面；

<b>基本配置</b>	
启用	<input checked="" type="checkbox"/>
服务器地址(URL)	<input type="text" value="http://10.67.73.97:8080/onvif/device_service"/>
<b>鉴权</b>	
鉴权方式	<input type="radio"/> 无 <input checked="" type="radio"/> WS-Username token

**保存**

图 7-11 ONVIF

- 2) 勾选“启用”，开启 ONVIF 协议接入。开启后，设备将自动生成服务器地址（URL），默认端口为 80；
- 3) 设置 ONVIF 登录时的鉴权方式，选择“无”时不需要验证用户名和密码即可登录，选择“WS-Username token”时需验证用户名、密码进行登录；
- 4) 点击“保存”完成配置。

### 7.6.1.2.2 SIP

SIP 接入是指遵循 GB/T28181 的要求，将门禁模块注册到国标平台。设置方法如下：

- 1) 进入配置>网络>接入协议>SIP 界面；

ONVIF
SIP
DPSS
VIID
COI
Pigeon Platform
PDNS

注册平台	<input type="text" value="注册平台 1"/>	
启用	<input checked="" type="checkbox"/>	
本地端口	<input type="text" value="5060"/>	1024~65535
入网ID	<input type="text" value="31000000001125001115"/>	
设备名称	<input type="text" value="IPCAMERA"/>	
平台ID	<input type="text" value="31020000002000000001"/>	
平台地址	<input type="text" value="221.224.163.198"/>	
平台端口	<input type="text" value="5900"/>	1024~65535
注册用户名	<input type="text" value="31000000001125001115"/>	
注册密码	<input type="password" value="••••••••"/>	
续租时间	<input type="text" value="60"/>	(秒) 30~999999
心跳间隔	<input type="text" value="30"/>	(秒) 10~1000
设备归属	<input type="text" value="owner"/>	
行政区域	<input type="text"/>	
警区	<input type="text"/>	
安装地址	<input type="text"/>	

添加
修改
删除

GB视频编码通道ID	GB视频编码通道名称	IPC码流类型
31000000001325001110	enc	主码流

添加
修改
删除

告警ID	告警名称	有效性
国标兼容次序 国家标准->国标扩展(2014)->国标扩展(2016) <input type="button" value="修改国标兼容次序"/>		
<input type="button" value="扩展配置&gt;&gt;"/>		

图 7-12 SIP

- 2) 选择注册平台，设备支持同时接入两个不同国标平台；

- 3) 勾选“启用”，开启 SIP 协议接入；
- 4) 填写入网 ID、平台 ID、平台端口、注册用户名/密码、GB 视频编码通道 ID 等信息；
- 5) 点击“保存”完成配置。

### 7.6.1.2.3 DPSS

门禁模块通过 Wi-Fi 采集无线前端设备（手机等）的 MAC 地址，使用 DPSS 协议将采集到的 MAC 地址传输到后端管理平台。设置方法如下：

- 1) 进入配置>网络>接入协议> DPSS 界面；

图 7-13 DPSS

- 2) 勾选“启用”，开启 DPSS 协议；
- 3) 填写平台地址和平台端口号，端口默认为 50060；
- 4) 填写入网 ID；
- 5) 选择 UUID 类型；
- 6) 点击“保存”完成配置。

### 7.6.1.2.4 VIID（视图库）

门禁模块可将采集到的图片上传至视图库平台，作为后续数据分析和比对的材料。设置方法如下：

- 1) 进入配置>网络>接入协议>视图库界面；

启用	<input checked="" type="checkbox"/>	
入网ID	<input type="text" value="00000000000000000000"/>	
平台地址	<input type="text" value="0.0.0.0"/>	
视图库端口	<input type="text" value="8080"/>	1024-65535
注册用户名	<input type="text" value="admin"/>	
注册密码	<input type="password" value="•••••"/>	
心跳时间	<input type="text" value="60"/>	1-90
安装地址	<input type="text" value="1"/>	
行政区域划分	<input type="text" value="1"/>	
上传类型	<input type="text" value="person"/>	
自动校时	<input type="checkbox"/>	
校时时间间隔	<input type="text" value="60"/>	1-65535

图 7-14 视图库

- 2) 勾选“启用”，开启视图库接入功能；
- 3) 在入网 ID 栏中填写设备入网视图库平台的 ID；
- 4) 在平台地址、视图库端口栏中，分别填入视图库平台的 IP 地址及端口号；
- 5) 在注册用户名、注册密码栏中，分别填入视图库平台的用户名及密码；
- 6) 心跳时间用于检测 TCP 的异常断开。一般采用定时发送简单通讯包的方式，如果在指定时间间隔内未收到对方响应，则判断对方已经断开连接。例如心跳时间为 30 就是 30s 发送一次；
- 7) 根据需要填写安装地址、行政区域划分，便于确定设备位置；
- 8) 点击“保存”完成配置。

### 7.6.1.2.5 COI

门禁模块可连接到后端管理平台，由平台进行统一管理。设置方法如下：

- 1) 进入 **配置>网络>接入协议>COI** 界面；

启用	<input checked="" type="checkbox"/>	
服务器IP	<input type="text" value="0.0.0.0"/>	
服务器端口	<input type="text" value="80"/>	1-65535
URL路径	<input type="text" value="/icmp-ws/entranceSocket"/>	

图 7-15 COI

- 2) 勾选“启用”，开启 COI 接入功能；
- 3) 在服务器 IP、服务器端口栏中，分别填入服务器的 IP 地址及端口号；
- 4) 轮询时间默认为 30s，保持默认即可；

**i** 说明：轮询时间即人脸门禁设备向服务器发送在线消息的间隔时间；如轮询时间为 30s，即人脸门禁设备每隔 30s 向服务器发送一次在线消息。

5) 点击“保存”完成配置。

#### 7.6.1.2.6 Pigeon Platform

Pigeon Platform 即信鸽平台，门禁模块接入信鸽平台后，支持接受信鸽平台下发的安全证书，并对接受到安全证书进行存储和管理；支持接收信鸽平台下发的升级信令，并可按照升级信令中的地址下载版本，执行升级，反馈升级进度等。设置方法如下

1) 进入**配置>网络>接入协议>Pigeon Platform** 界面；

启用	<input checked="" type="checkbox"/>	
平台地址	<input type="text" value="1.58.29.170"/>	
平台端口	<input type="text" value="8081"/>	0~65535
用户编号	<input type="text" value="321"/>	
用户名称	<input type="text" value="321"/>	
部门编号	<input type="text" value="321"/>	
部门名称	<input type="text" value="321"/>	

SIP		
入网ID	<input type="text" value="31000000001125001115"/>	
注册密码	<input type="password" value="••••••••"/>	
视频通道列表	<input type="text" value="1"/>	<input type="button" value="编辑"/> 0~1
报警通道列表	<input type="text" value="0"/>	<input type="button" value="编辑"/> 0~1
更多参数	<input type="button" value="配置"/>	

图 7-16 COI

- 2) 勾选“启用”，开启 Pigeon Platform 接入功能；
- 3) 填写平台地址、平台端口、用户编号、用户名称、部门编号、部门名称；
- 4) 点击“保存”完成配置。

**i** 说明：该处 SIP 配置和 SIP 协议（**配置>网络>接入协议>SIP**）保持同步。详细可参考 [7.6.1.2.2 SIP](#)。

#### 7.6.1.2.7 PDNS

PDNS 即被动 DNS，实现跨 NAT 访问设备的全功能 Web 客户端。设置方法如下

1) 进入**配置>网络>接入协议>PDNS** 界面；

启用	<input checked="" type="checkbox"/>
序列号	<input type="text" value="fjdgfjg"/>
名称	<input type="text" value="name"/>
APPID	<input type="text" value="appid"/>
APPKEY	<input type="text" value="•••••"/>
PDNS地址	<input type="text" value="1.58.29.170"/>
PDNS端口	<input type="text" value="4502"/> 1~65535
连接状态	<input type="text" value=""/>

图 7-17 PDNS

- 2) 勾选“启用”，开启 PDNS 接入功能；
- 3) 填写序列号、APPID、APPKEY、PDNS 地址和 PDNS 端口；
- 4) 点击“保存”完成配置。

### 7.6.1.3 其他协议

#### 7.6.1.3.1 DDNS

DDNS 动态域名服务是通过连接各种类型的服务器，从而达到通过服务器访问该设备的目的。在各服务器网站申请域名，可通过域名直接访问该设备（即使 IP 地址改变也可通过域名访问），可以有效解决公网访问人脸门禁设备的问题。设置方法如下：

- 1) 进入**配置>网络>其他协议>DDNS** 界面；

启用	<input type="checkbox"/>
DDNS类型	<input type="text" value="ORAY"/>
设备域名	<input type="text" value=""/>
用户名	<input type="text" value="admin"/>
密码	<input type="text" value="•••••"/>
状态	<input type="text" value=""/>

图 7-18 DDNS

- 2) 勾选“启用”，开启 DDNS 服务；
- 3) 在 DDNS 类型下拉框中，选择 DDNS 服务类型，可选择“ORAY”、“DYNDS”或“NOIP”。选择 DYNDS 或 NOIP 时，需填写设备域名；
- 4) 根据选择的服务器，填写用户名和密码；
- 5) 点击“保存”完成配置，状态栏中将显示相关连接信息。

#### 7.6.1.3.2 FTP

客户端支持 FTP 协议，可将设备的抓拍图片文件上传到指定的 FTP 服务器上。设置方法如下：

- 1) 进入**配置>网络>其他协议>FTP** 界面；

服务器地址	192.168.1.1	
端口	21	1-65535
用户名	admin	<input type="checkbox"/> 匿名
密码		
目录结构	使用根目录	

图 7-19 FTP

- 2) 填写 FTP 服务器的 IP 地址及对应端口;
- 3) 填写具有上传权限的用户的用户名、密码。若匿名用户也具有上传权限, 也可勾选“匿名”使用匿名方式访问 FTP 服务器;
- 4) 设置目录结构, 即文件的保存路径, 根据实际需求在下拉列表中进行选择, 可选择“使用根目录”、“使用一级目录”、“使用二级目录”;
  - 一级目录可选择“使用设备名”、“使用设备 IP”、“自定义”。
  - 二级目录可选择“使用通道号”、“自定义”。
- 5) 可点击“测试”, 测试当前 FTP 是否可用, 测试结果将显示在弹出的对话框中;
- 6) 点击“保存”完成配置。

#### 7.6.1.3.3 PPPoE

PPPoE 即以太网上的点对点协议, 是通过设置运营商 (电信、联通、移动) 提供的上网账号, 使设备能拨号连接互联网。设置方法如下:

- 1) 进入配置>网络>其他协议>PPPoE 界面;

网卡	GLAN1
IP版本	IPV4
启用	<input type="checkbox"/>
动态IP	0.0.0.0
用户名	root
密码	●●●●

根据国家《互联网信息服务管理办法》, 通过80端口提供网页服务都需要ICP备案, 否则无法访问。建议你先修改Web服务端口。

图 7-20 PPPoE

- 2) 勾选“启用”, 开启 PPPoE 拨号功能, 并选择网卡;
- 3) 填写网络运营商 ISP 提供的上网用户名和密码;
- 4) 点击“保存”完成配置, 拨号成功后显示动态 IP。

#### 7.6.1.3.4 K-SNMP

K-SNMP 即科达私有网络管理协议。设置方法如下:

- 1) 进入配置>网络>其他协议>K-SNMP 界面;

网管服务器地址	<input type="text" value="0.0.0.0"/>	
网管服务器端口	<input type="text" value="1727"/>	
设备位置信息	<input type="text" value="0"/>	
CPU利用率阈值	<input type="text" value="100"/>	1~100
内存利用率阈值	<input type="text" value="100"/>	1~100
视频丢包率阈值	<input type="text" value="100"/>	1~100

图 7-21 K-SNMP

- 2) 填写网管服务器地址和设备位置信息;
- 3) 设置 CPU 利用率阈值、内存利用率阈值和视频丢包率阈值, 默认值均为 100, 范围 1~100;
- 4) 点击“保存”完成配置。

#### 7.6.1.3.5 QoS

QoS 即服务质量, 可有效解决网络延迟和网络阻塞问题。设置方法如下:

**i** 说明: QoS 功能需要传输路径上的网络设备 (如路由器、交换机) 支持。

- 1) 进入配置>网络>其他协议>QoS 界面;

启用	<input checked="" type="checkbox"/>	
音视频DSCP	<input type="text" value="0"/>	0~63
管理DSCP	<input type="text" value="0"/>	0~63

图 7-22 QoS

- 2) 勾选“启用”, 开启 QoS 功能;
- 3) 设置音视频 DSCP 和管理 DSCP 值, 范围 0~63;

**i** 说明: DSCP 优先级有 64 个 (0-63), 标识了包的优先级不同, 网络可根据 DSCP 权值来判断数据传输的优先级, 0 优先级最低, 63 优先级最高, 根据包的优先级选择不同的出队列, 不同出队列所占的带宽资源, 拥塞时丢弃比例不同, 从而实现服务质量的的目的。

**i** 注意: 配置时需要在路由器端设置相同值。

- 4) 点击“保存”完成配置。

#### 7.6.1.3.6 UPnP

通过 UPnP 协议在私网与外网间建立映射关系。内部端口为人脸门禁设备端口, 外部端口为路由器端口, 用户访问外部端口时就能访问人脸门禁设备。设置方法如下:

**i** 说明: 对于一台处在内网环境的人脸门禁设备, UPnP 功能可以使网关或路由器做自动端口映射, 将设备监听的端口从网关或路由器映射到内网设备上, 网关或路由器的网络防火墙模块开始对 Internet 上其他电脑开放这个端口。

- 1) 进入配置>网络>其他协议>UPnP 界面;

启用

别名

端口映射

端口映射方式

端口映射表

选择	协议名称	IP	外部端口	状态
<input checked="" type="checkbox"/>	HTTP	0.0.0.0	0	未生效
<input checked="" type="checkbox"/>	RTSP	0.0.0.0	0	未生效
<input checked="" type="checkbox"/>	SDK	0.0.0.0	0	未生效

图 7-23 UPnP

- 勾选“启用”，开启 UPnP 功能；
- 设置别名，设置后，在同一局域网广播域中开启了 UPnP 协议的电脑系统上，用户可以直接在系统的网络中搜索到该别名，双击该图标，即会自动弹出浏览器页面访问设备的当前 IP 地址；
- 选择映射端口方式为手动或自动，选择“手动”时，需填写外部端口；
- 点击“保存”完成配置。

#### 7.6.1.3.7 邮件 (SMTP)

SMTP 即简单邮件传输协议。当产生告警时，设备可通过 SMTP 自动发送告警邮件。设置方法如下：

- 进入配置>网络>其他协议>邮件 (SMTP) 界面；

SMTP服务器

端口  1~65535

发件人

发件人地址

服务器认证

用户名

密码

主题

附件

附件类型

收件人  +

图 7-24 SMTP

- 填写 SMTP 服务器的 IP 地址和端口，端口范围为 1~65535，默认端口为 25；
- 填写发件人的名称和地址；可勾选开启服务器认证，并填写正确的用户名和密码；
- 填写邮件主题；可勾选附件并选择附件类型，勾选后发送的邮件中将附带相关附件；
- 添加收件人邮箱地址，在收件人地址栏输入邮箱地址并点击后面的“+”号，地址保存至下方列表中，选中某一邮

箱地址，点击列表框右下方“-”号即可删除该邮箱；

6) 点击“保存”完成配置。

**i**说明：配置完成，且开启邮件通知后，即可正常发送告警邮件。

## 7.6.2 门禁

### 7.6.2.1 人员管理

进入**配置>门禁>人员管理**界面，可根据姓名、证件号等查询哨兵的人员信息。

**i**说明：直接点击“查询”，可查看所有下发至哨兵本地的人员信息以及正常通行是产生的临时人员信息。

当前人员/最大人员 1/1

姓名

证件号

门禁卡

序号	照片	姓名	证件号	门禁卡
1		png图片测试	9966**88	

图 7-25 人员管理

### 7.6.2.2 参数配置

#### 7.6.2.2.1 基本配置

进入**配置>门禁>参数配置>基本配置**界面，可进行门禁参数配置，包括语音提示、文字提示、隐藏名称等。

语音提示	<input type="text" value="核验成功&amp;失败"/>
文字提示	<input type="text" value="姓名"/>
隐藏名字	<input type="text" value="关闭"/>
灯光提示	<input type="text" value="绿灯&amp;红灯"/>
自动熄屏	<input type="text" value="关闭"/>
自动熄屏时间	<input type="text" value="30"/> (秒) 10~300
自定义核验成功语音	<input type="text"/>
自定义核验失败语音	<input type="text"/>
返回屏保	<input type="text" value="关闭"/>
返回屏保时间	<input type="text" value="20"/> (秒) 10~300
上传屏保	<input type="button" value="上传"/>
熄屏检测	<input type="text" value="关闭"/>

图 7-26 参数配置

- 语音提示：设置人脸门禁设备的语音提示，可选择关闭、验证成功、验证失败等。
- 文字提示：设置核验界面的文字提示，可选择关闭、姓名、证件号或姓名&证件号。
- 隐藏名字：开启后，核验成功时将隐藏人员名称。

- 自动熄屏：开启后，可以设置自动熄屏时间，范围为 10~300s。在相应时间内未对设备进行操作，屏幕会跳转至待机界面。若关闭该功能，则设备不会自动熄屏。
- 自定义核验成功语音：可自定义核验成功时设备播报的语音。
- 自定义核验失败语音：可自定义核验失败时设备播报的语音。
- 返回屏保：开启后，可以设置返回屏保时间，范围 10~300s。在相应时间内未对设备进行操作，屏幕会返回屏保。若关闭该功能，则设备不会自动屏保。
- 上传屏保：点击“上传”，根据需要修改屏保界面。
- 熄屏检测：根据需要开启或关闭熄屏检测。

#### 7.6.2.2.2 门禁配置

进入**配置>门禁>参数配置>门禁配置**界面，可配置默认核验方式和授权方式。

默认核验方式	人证1:1/人脸	▼
授权方式 (人脸)	前端授权	▼
授权方式 (人证1:1)	联网授权	▼
扩展输入	常关	▼
门磁输入	常关	▼
关门延迟时间	5	1~255
开门异常检测时间	60	0~3600
识别报警次数	255	1~255
防拆按钮报警	关闭	▼
开门信号去重	开启	▼
门锁类型	电磁锁	▼

定时开/关门

启用

✕ 删除 🗑️ 清除全部

	0	2	4	6	8	10	12	14	16	18	20	22	24
星期一	[Time slots]												
星期二	[Time slots]												
星期三	[Time slots]												
星期四	[Time slots]												
星期五	[Time slots]												
星期六	[Time slots]												
星期日	[Time slots]												

保存

图 7-27 门禁配置

- 默认核验方式：核验方式以出厂默认即可，若需修改请联系我司客服人员咨询。
- 授权方式 (人脸)：默认前端授权；
- 授权方式 (人证 1:1)：默认联网授权。
- 识别报警次数：设置最大识别次数，范围 1~255 次；若连续识别失败次数超过该最大值，则会触发报警。

**i** 说明：其他参数暂不影响哨兵功能，默认即可。

### 7.6.2.2.3 人脸参数

进入配置>门禁>参数配置>人脸参数界面，可配置人脸参数。

图 7-28 人脸参数

- 人脸姿态阈值：设置人脸识别姿态分阈值，范围为 0~100 分。设备将根据上下俯仰角度、左右水平角度、眼间距等因素对人脸进行姿态评分；若评分低于预设值，则人脸检测不通过，人脸比对或录入失败。
- 人脸比对阈值 (1: N)：设置人脸 1: N 比对时的阈值，范围为 0~100 分。阈值越高，则误识率越低，拒认率越高。
- 人脸比对阈值 (1: 1)：设置人脸 1: 1 比对时的阈值，范围为 0~100 分。阈值越高，则误识率越低，拒认率越高。
- 活体检测：可开启/关闭活体检测功能。开启后，设备可判断对象是否为真人本人，可有效甄别照片、换脸、面具、遮挡、屏幕翻拍等欺诈行为；若识别对象不是本人，则人脸比对或录入失败。
- 活体检测安全等级：开启活体检测功能后，可设置活体检测安全等级，可选择普通或高；若选择高，则误识率低，拒认率高。
- 人脸识别距离：拖动滑块可设置人脸识别距离，范围为 0.3~2.5m，默认为 1.5m。

### 7.6.2.2.4 高级配置

进入配置>门禁>参数配置>高级配置界面。

图 7-29 高级配置

- 删除人员数据：点击“删除”，设备将清除所有人员信息。
- 删除事件数据：点击“删除”，设备将清除所有事件信息。

➤ 呼叫求助：可开启或关闭呼叫求助功能。

**i** 说明：其他参数暂不影响哨兵功能，默认即可。

### 7.6.2.3 事件管理

**i** 说明：防爆哨兵暂不支持事件管理。

### 7.6.2.4 存储状态

进入**配置>门禁>参数配置>存储状态**界面，可查看存储卡存储数据状态。

数量\类型	用户	卡片	指纹	事件
最大数量	50000	0	0	1000000
使用数量	1	0	0	32

图 7-30 存储状态

## 8 全景 Web 客户端

登录全景 Web 端，用户可对该模块进行网络管理、平台接入等功能。

**i** 说明：全景模块默认 IP 为 192.168.1.100。

### 8.1 开始使用

登录 Web 客户端前需确认设备与电脑已经连接并且网络互通。

**i** 注意：将产品接入互联网需自担风险，包括但不限于产品可能遭受网络攻击、黑客攻击、病毒感染等，本公司不对因此造成的产品工作异常、信息泄露等问题承担责任，但本公司将及时为您提供产品相关技术支持。

电脑配置要求如下：

- 处理器：3.3GHz Intel 酷睿 i3 系列及以上或相同性能的其他处理器
- RAM 内存：4GB 及以上
- 操作系统：Windows7 操作系统或更高版本
- 浏览器：推荐使用 IE 内核浏览器，使用其它内核浏览器会影响客户端部分功能的使用
- DirectX：9.0c

### 8.2 Web 界面说明

- 登录 Web 客户端

设备激活完成并修改网络参数后将自动重启。待设备重启后，在浏览器地址栏输入全景模块 IP 地址“http://IP 地址”，进入 Web 客户端登录界面。输入用户名 admin 及激活时设置的密码，进入客户端。



图 8-1 Web 客户端登录界面

首次成功登录后，请下载插件，按照窗口提示安装插件。安装插件时需要关闭浏览器，安装完成后重新登录。登录成功后界面如下图。

**i** 注意：推荐使用 IE 内核浏览器，使用其他内核浏览器会影响客户端部分功能的使用。

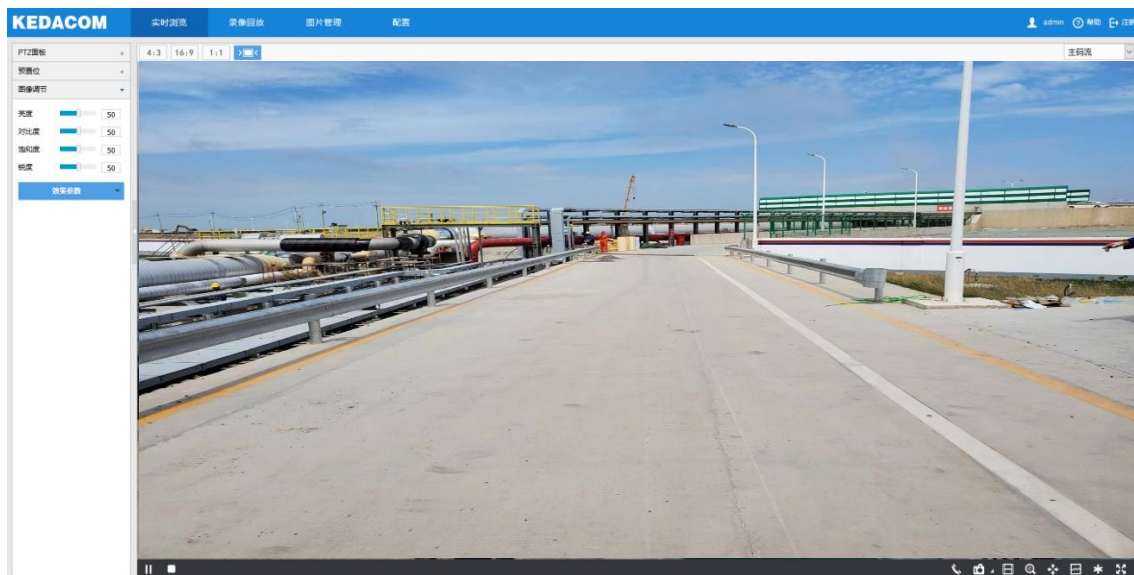


图 8-2 客户端操作界面

### ➤ 登出 Web 客户端

点击客户端操作界面右上角的 **注销** 按钮，安全退出登录。

### ➤ 帮助

点击界面右上角的 **帮助** 按钮，弹出联机帮助页面，可查看设备的帮助文档。

### ➤ 主界面说明

在 Web 客户端主界面，您可以进行实时浏览、录像回放、图片管理、配置等操作。

- 实时浏览：预览门禁模块的实时监控画面并根据需要呼叫、截图、录像等。
- 录像回放：按时间查找录像并进行回放及下载。
- 图片管理：按图片类型查询、查看和下载图片文件。
- 配置：对设备进行参数设置及功能配置。

## 8.3 实时浏览

点击“实时浏览”，进入哨兵全景模块的浏览界面。

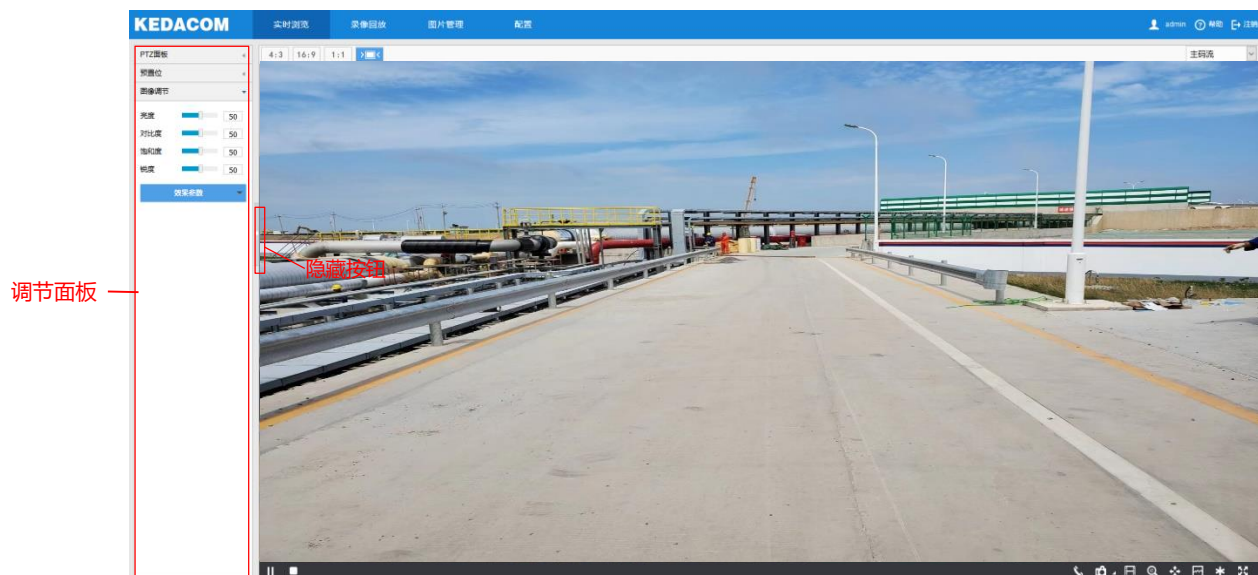


图 8-3 客户端操作界面

**说明:**

- ◆ 点击浏览画面左侧的隐藏按钮，可将图像调节面板隐藏。再次点击，即可展开面板。
- ◆ 实时浏览画面中显示客流统计的进出数量。

**8.3.1 图像调节**

点击 **图像调节** ，将会显示图像调节面板。







图 8-4 图像调节面板

通过拖动滑块调整预览画面的亮度、对比度、饱和度和锐度，也可以设置滑块后面的数值。
















- 亮度：根据实际需求调节当前图像的亮度，亮度越高图像越明亮。
- 对比度：根据实际需求调节当前图像的对比度，对比度越高，图像的明暗对比越清晰。
- 饱和度：根据实际需求调节当前图像饱和度，饱和度越高，图像越鲜艳。
- 锐度：根据实际需求调节当前图像的锐度，锐度越高，图像中物体的轮廓将越清晰。
- 效果参数：根据实际需求调用已设置好的图像参数，可在**配置>摄像机>图像>图像效果**中设置。

**8.3.2 预览设置**

- 画面尺寸

图标	功能说明
	表示预览画面以 4 比 3 的比例显示。
	表示预览画面以 16 比 9 的比例显示。
	表示预览画面以 1 比 1 的比例显示。
	表示预览画面自适应显示浏览窗口。

➤ 预览工具栏

图标	功能说明
	开始/暂停，点击该按钮，播放视频浏览画面，再次点击，暂停播放。
	停止，点击该按钮，停止视频浏览。
	音量，本地解码音量。点击  按钮，选择开启或关闭音量；点击  ，选择声道。
	拖动滑块可调节音量大小。
	语音呼叫前端设备，点击开始对讲，再次点击停止对讲。
	抓拍，点击  即可抓拍当前画面。点击  选择浏览抓拍或前端抓拍，浏览抓拍指电脑客户端抓拍图像，前端抓拍指人脸门禁设备抓拍图像。
	开始录像/停止录像，点击按钮开始录像，再次点击停止录像。
	EPTZ，电子放大。单击按钮，按住鼠标左键不放，向右下方框选出某一区域，可以扩大该区域的像素并使该区域铺满画面；按住鼠标左键不放，向左上方框选区域使画面恢复。
	状态，点击显示帧率和码率，再次点击，隐藏。该按钮默认不显示，需要时请在配置>本地配置界面勾选状态信息显示。
	视频冻结，点击该按钮，监控画面将显示点击前最后一帧画面，再次点击取消冻结，显示实时画面。
	全屏，点击该按钮，显示全屏画面，在全屏画面中双击鼠标左键或按 Esc 键退出全屏。

## 8.4 录像回放

点击“录像回放”进入录像回放界面，可对保存在存储卡上的录像进行搜索、查看、下载等操作。录像回放界面如下图所示。

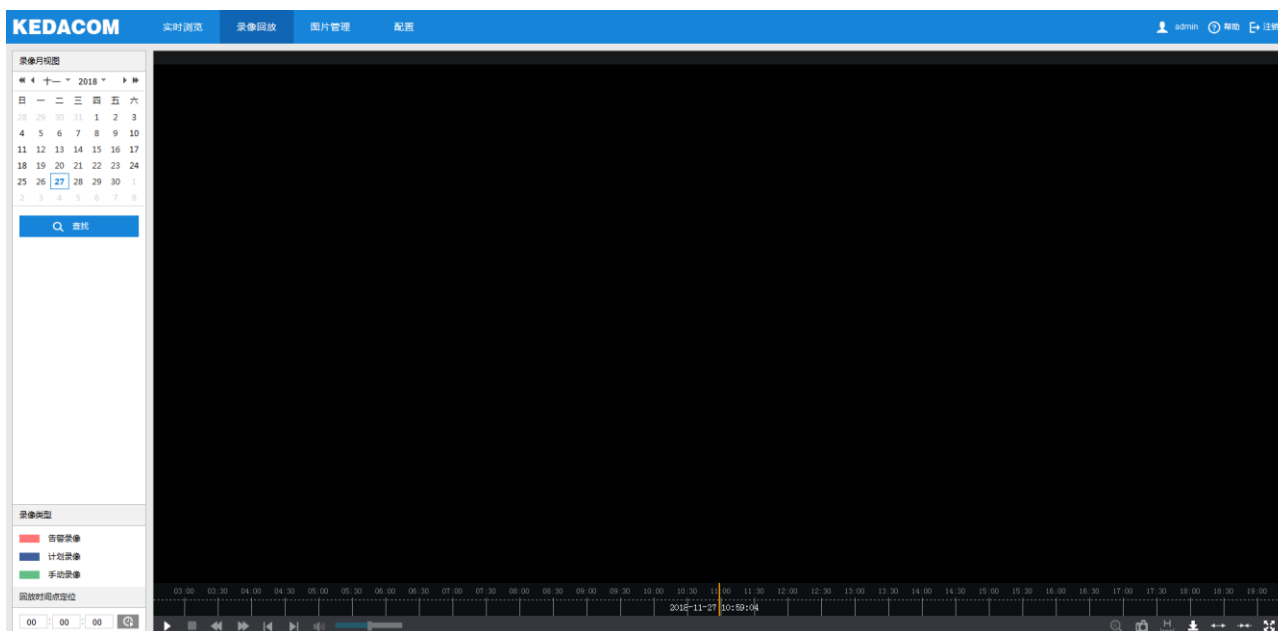



图 8-5 录像回放

具体操作步骤如下：














- 1) 选择录像时间，在录像月视图中选择需要查看录像的日期，如果月视图中的某个日期右下角有蓝色三角标记，则代表该天有监控录像存储；
- 2) 点击“查找”，录像文件显示在时间轴上（时间轴上高亮显示）；

**i** 说明：蓝色表示计划录像，绿色表示手动录像。

- ◆ 计划录像：通过设置设备在某些时间段自动录像。在配置>存储>录像界面进行设置即可。
- ◆ 手动录像：即在门禁设备与平台网络断开的情况下，设备默认开启录像。

- 3) 点击界面下方的播放按钮即可播放录像，在回放录像过程中，可以通过录像回放下方的工具栏对回放的录像进行剪辑、快进、下载等操作；
- 4) 鼠标箭头放在录像时间轴可显示录像时间信息，双击鼠标左键或者按住鼠标左键再左右移动时间轴可进行录像跳播。也可以通过设置“回放时间点定位”的回放时间，点击  按钮来选择回放时间点。

录像回放界面工具栏按钮说明如下表所示：

图标	功能说明
	播放/暂停，点击按钮播放录像，再次点击暂停播放。
	停止，点击该按钮，停止录像播放。
	减慢播放速度，点击可减慢播放速度，点击一次减慢至 1/2x，再次点击减慢至 1/4x，最低减慢至 1/8x。
	加快播放速度，点击可加快播放速度，点击一次播放速度加快一倍，最高调节到 8x。
	前一片段，点击播放上一个录像片段，可连续点击。连续录像中点击，默认跳播 1 小时。
	后一片段，点击播放下一个录像片段，可连续点击。连续录像中点击，默认跳播 1 小时。
	声音，点击打开声音，再次点击关闭声音，拖动滑块可调节音量。
	EPTZ，电子云台功能。单击按钮，按住鼠标左键不放，向右下方框选出某一区域，可以扩大该区域的像素并使该区域铺满画面；按住鼠标左键不放，向左上方框选区域使画面恢复。
	抓拍，点击即可抓拍当前回放画面。回放抓拍图片的保存路径可在 <b>配置&gt;本地配置</b> 的“回放抓拍保存路径”中设置。
	剪辑，点击即可开始对当前回放录像进行剪辑，再次点击则停止剪辑。回放剪辑录像的保存路径可在 <b>配置&gt;本地配置</b> 的“回放剪辑保存路径”中设置。
	下载，点击该按钮，将弹出下载界面。在弹出的界面设置具体时间和下载录像类型后单击“查询”，符合条件的录像将显示在下方列表中，勾选需要下载的文件，点击“下载”即可下载，表格中下载进度栏可查看相应录像的下载进度。下载录像的保存路径可在 <b>配置&gt;本地配置</b> 界面的“回放下下载保存路径”中设置。
	放大/缩小时间轴，即调整时间轴单位刻度值，点击即可放大或缩小时间轴。时间轴单位刻度值等级为 5 分钟/10 分钟/30 分钟，放大或缩小时间轴不影响当前播放时间点。
	全屏，点击该按钮，显示全屏画面，在全屏画面中双击鼠标左键或者按 Esc 键退出全屏。

## 8.5 图片管理

在菜单栏中点击“图片管理”进入图片管理界面，可以根据需要搜索并下载保存在存储卡中的抓拍图片。

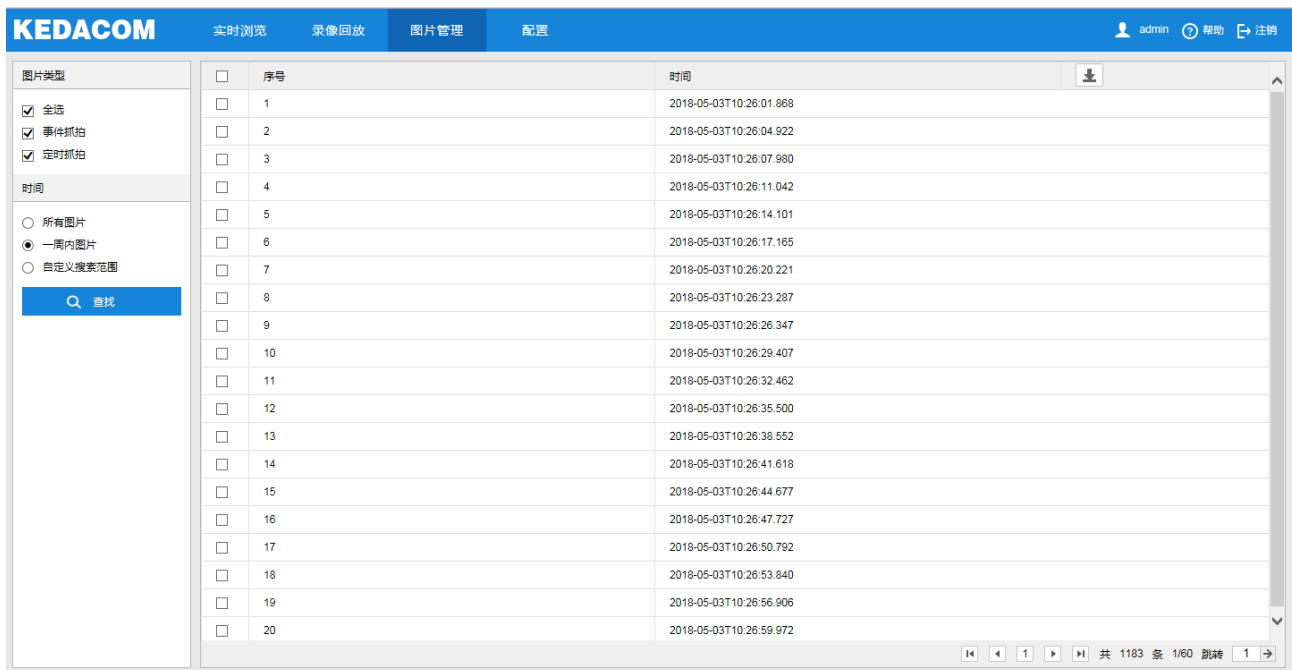



图 8-6 图片管理

图片搜索及下载具体步骤如下：

- 1) 在左侧的图片类型中勾选需要搜索的抓拍图片类型；
- 2) 在时间选项中选择搜索图片的时间范围，选择自定义搜索范围时需设置具体开始时间和结束时间；
- 3) 点击“查找”，搜索结果显示在右方列表中，在列表中可以看到图片序号和图片抓拍时间；
- 4) 勾选图片，点击  按钮，即可下载选中的图片。图片保存路径可在配置>本地配置界面的“前端抓拍保存路径”中设置。

## 8.6 配置

在菜单栏中点击“配置”进入配置界面，可进行网络、事件、存储等各项配置。


 说明：本章节介绍防爆哨兵的常用功能配置，其余配置项可点击界面“帮助”，来获取帮助文档，查看对应操作。



图 8-7 配置

## 8.6.1 网络

进入**配置>网络**界面，可设置全景模块的网络参数，包括 IP 及端口、接入协议和其他协议。

### 8.6.1.1 IP 及端口

#### 8.6.1.1.1 有线网络

进入**配置>网络>IP 及端口>有线网络**界面，配置有线网络参数，包括 IP 地址、子网掩码、默认网关等。

IP地址配置	
网卡	GLAN1
IP版本	IPV4
模式	静态
IP地址	10.67.37.253 <span style="float: right;">测试</span>
子网掩码	255.255.240.0
默认网关	10.67.47.254
MAC地址	00-14-10-2D-7C-21
MTU	1500 <span style="float: right;">1280~1500</span>
DNS服务器配置	
自动获取DNS	<input type="checkbox"/>
首选DNS服务器	<input type="text"/>
备用DNS服务器	<input type="text"/>
<span style="background-color: #0070C0; color: white; padding: 5px 10px; border-radius: 3px;">保存</span>	

图 8-8 有线网络

#### ➤ IP 地址配置

IP 版本为 IPV4 时，可选择静态或 DHCP 模式。静态模式下，需根据实际情况输入 IP 地址、子网掩码和默认网关；DHCP 模式下，且所在网络中配置有 DHCP 服务，则设备将自动获取 IP。

**i** 说明：填写 IPV4 地址时，可点击“测试”，确定该 IP 地址是否可用。

IP 版本为 IPV6 时，可选择自动获取或手动模式。自动获取模式下，由网络中的服务器、网关或路由器下发 IPV6 地址；手动模式下，需根据实际情况输入 IP 地址、子网掩码和默认网关。

“多播地址”即组播地址，人脸门禁设备需要以多播方式被网络内设备发现时，根据实际需求填写即可。

**i** 说明：多播是一种数据包传输方式，源主机可以只需要发送一份报文就可以到达组内每个需要接收的主机上，这中间还要取决于路由器对组内关系的维护和选择。

“MTU”项可以设置最大传输单元，指 TCP/UDP 协议网络传输中所通过的最大数据包的大小（以字节为单位），范围 500~1500，默认 1500。

**i** 说明：MTU 越大通信效率越高，但传输延时增大。请根据实际需求填写。

#### ➤ DNS 服务器配置

设备需要通过域名访问时，需配置正确的 DNS 服务器地址。可以勾选“自动获取 DNS”或手动填写 DNS 服务器地址；若勾选“自动获取 DNS”，人脸门禁设备将自动从网关获取 DNS 服务器配置参数，无需再手动填写。

设置完成后，点击“保存”即可。

#### 8.6.1.1.2 端口

进入配置>网络>IP 及端口>端口界面，可配置 HTTP 端口、HTTPS 端口、RTSP 端口参数，可根据需要设置相应的端口。

HTTP端口	80	1~65535
HTTPS端口	5544	1~65535
RTSP端口	554	1~65535

**保存**

图 8-9 端口

- HTTP 端口：超文本传输协议端口，使用浏览器登录时需要在地址后面加上修改的端口号。如当 HTTP 端口号修改为 83 时，使用浏览器登录需要输入“http://设备 IP 地址:83”。默认为 80，范围为 1~65535。
- HTTPS 端口：超文本传输安全协议端口，使用浏览器登录时需要在地址后面加上修改的端口号。如当 HTTPS 端口号修改为 5545 时，使用浏览器登录需要输入“https://设备 IP 地址:5545”。默认为 5544，范围为 1~65535。
- RTSP 端口：实时传输协议端口，使用浏览器登录时需要在地址后面加上修改的端口号。如当 RTSP 端口号修改为 555 时，使用浏览器登录需要输入“rtsp://设备 IP 地址:555/id=0 (id=0 播放主流，id=1 播放辅流)”。默认为 554，范围 1~65535。

设置完成后，点击“保存”即可。

#### 8.6.1.1.3 多播

进入配置>网络>IP 及端口>多播界面，可根据实际需求设置码流类型、媒体类型、多播地址等多播参数，启用设备多播功能。

**i**说明：多播是一种数据包传输方式，源主机可以只需要发送一份报文就可以到达组内每个需要接收的主机上，这中间还要取决于路由器对组内关系的维护和选择。

码流类型	主码流	
媒体类型	视频	
多播地址	0.0.0.0	
多播端口	61000	1~65535
发送模式	被动	
TTL	64	0~255

**保存**

图 8-10 多播

- 码流类型：需发送的码流，默认为主码流。
- 媒体类型：需发送码流对应的媒体类型，默认为视频。
- 多播地址：组网发送码流的地址，根据实际情况填写即可。
- 多播端口：多播地址对应的多播端口，范围为 1~65535，默认为 61000。
- 发送模式：可选择主动模式或被动模式。主动模式下，若多播地址正常、有效，则默认向此多播地址发送码流；被动模式下，当且仅当收到组播请求时，才会向多播地址发送码流。若多播地址为 0.0.0.0，则默认向 239.2.2.2 发送码流。
- TTL：即生存时间，范围为 0~255。

**i**说明：TTL（生存时间）指 IP 数据包在被路由器丢弃前允许通过的最大网段数量，用于避免数据包在网络中无限循环收发，以节省网络资源。

## 8.6.1.2 接入协议

### 8.6.1.2.1 SIP

SIP 接入是指遵循 GB/T28181 的要求，将全景模块注册到国标平台。设置方法如下：

- 1) 进入**配置>网络>接入协议>SIP**界面；

注册平台	注册平台 1	
启用	<input type="checkbox"/>	
本地端口	5060	1024~65535
入网ID	00000000000000000000	
设备名称	IPCAMERA	
平台ID	00000000000000000000	
平台地址	0.0.0.0	
平台端口	5511	1024~65535
注册用户名	00000000000000000000	
注册密码	●●●●●●●●	
续租时间	60	(秒) 30~999999
心跳间隔	30	(秒) 10~1000
设备归属	owner	
行政区域		
警区		
安装地址		

GB视频编码通道ID	GB视频编码通道名称	IPC码流类型
00000000000000000000	enc	主码流

告警ID	告警名称	有效性
国标兼容次序 国标标准->国标扩展(2014)->国标扩展(2016) <input type="button" value="修改国标兼容次序"/>		
<input type="button" value="扩展配置&gt;&gt;"/>		

图 8-11 SIP

- 2) 选择注册平台，设备支持同时接入两个不同国标平台；
- 3) 勾选“启用”，开启 SIP 协议接入；
- 4) 填写入网 ID、平台 ID、平台端口、注册用户名/密码、GB 视频编码通道 ID 等信息；
- 5) 点击“保存”完成配置。

8.6.1.2.2 VIID

全景模块可将采集到的图片上传至视图库平台，作为后续数据分析和比对的材料。设置方法如下：

1) 进入**配置>网络>接入协议>视图库**界面；

注册视图库	视图库	
启用	<input type="checkbox"/>	
入网ID	00000000000000000253	
平台地址	10.67.36.249	
视图库端口	8081	1~65535
注册用户名	admin	
注册密码	●●●●	
心跳时间	60	30~300
安装地址	1	
行政区划划分	1	
发送方式	图片集合	(项目不支持该选项的以实际发送为准)
图传优先	<input type="checkbox"/>	
自动校时	<input type="checkbox"/>	
校时时间间隔	60	1~65535

**保存**

图 8-12 视图库

- 2) 勾选“启用”，开启视图库接入功能；
- 3) 在入网 ID 栏中填写设备入网视图库平台的 ID；
- 4) 在平台地址、视图库端口栏中，分别填入视图库平台的 IP 地址及端口号；
- 5) 在注册用户名、注册密码栏中，分别填入视图库平台的用户名及密码；
- 6) 心跳时间用于检测 TCP 的异常断开。一般采用定时发送简单通讯包的方式，如果在指定时间间隔内未收到对方响应，则判断对方已经断开连接。例如心跳时间为 30 就是 30s 发送一次；
- 7) 根据需要填写安装地址、行政区划划分，便于确定设备位置；
- 8) 根据需要选择发送方式，根据需要勾选图传优先和自动校时，并设置校时时间间隔；
- 9) 点击“保存”完成配置。

### 8.6.1.2.3 Pigeon Platform

Pigeon Platform 即信鸽平台，全景模块接入信鸽平台后，支持接受信鸽平台下发的安全证书，并对接受到安全证书进行存储和管理；支持接收信鸽平台下发的升级信令，并可按照升级信令中的地址下载版本，执行升级，反馈升级进度等。设置方法如下

1) 进入**配置>网络>接入协议>Pigeon Platform** 界面；

启用	<input type="checkbox"/>	
平台地址	<input type="text" value="0.0.0.0"/>	
平台端口	<input type="text" value="0"/>	0~65535
用户编号	<input type="text"/>	
用户名称	<input type="text"/>	
部门编号	<input type="text"/>	
部门名称	<input type="text"/>	

SIP		
入网ID	<input type="text" value="00000000000000000000"/>	
注册密码	<input type="password" value="●●●●●●"/>	
视频通道列表	<input type="text" value="1"/>	<input type="button" value="编辑"/> 0~2
报警通道列表	<input type="text" value="0"/>	<input type="button" value="编辑"/> 0~2
更多参数	<input type="button" value="配置"/>	

图 8-13 COI

- 2) 勾选“启用”，开启 Pigeon Platform 接入功能；
- 3) 填写平台地址、平台端口、用户编号、用户名称、部门编号、部门名称；
- 4) 点击“保存”完成配置。

**i** 说明：该处 SIP 配置和 SIP 协议（配置>网络>接入协议>SIP）保持同步。

#### 8.6.1.2.4 PDNS

PDNS 即被动 DNS，实现跨 NAT 访问设备的全功能 Web 客户端。设置方法如下

- 1) 进入配置>网络>接入协议>PDNS 界面；

启用	<input type="checkbox"/>	
序列号	<input type="text" value="0924y67687"/>	
名称	<input type="text" value="name"/>	
APPID	<input type="text" value="appid"/>	
APPKEY	<input type="password" value="●●●●●"/>	
PDNS地址	<input type="text" value="pdns.bestkunlun.com"/>	
PDNS端口	<input type="text" value="4502"/>	1~65535
连接状态	初始状态	

图 8-14 PDNS

- 2) 勾选“启用”，开启 PDNS 接入功能；

- 3) 填写序列号、APPID、APPKEY、PDNS 地址和 PDNS 端口;
- 4) 点击“保存”完成配置。

### 8.6.1.3 其他协议

#### 8.6.1.3.1 DDNS

DDNS 动态域名服务是通过连接各种类型的服务器，从而达到通过服务器访问该设备的目的。在各服务器网站申请域名，可通过域名直接访问该设备（即使 IP 地址改变也可通过域名访问），可以有效解决公网访问人脸门禁设备的问题。设置方法如下：

- 1) 进入**配置>网络>其他协议>DDNS** 界面；

图 8-15 DDNS

- 2) 勾选“启用”，开启 DDNS 服务；
- 3) 在 DDNS 类型下拉框中，选择 DDNS 服务类型，可选择“ORAY”、“DYNDS”或“NOIP”。选择 DYNDS 或 NOIP 时，需填写设备域名；
- 4) 根据选择的服务器，填写用户名和密码；
- 5) 点击“保存”完成配置，状态栏中将显示相关连接信息。

#### 8.6.1.3.2 FTP

客户端支持 FTP 协议，可将设备的抓拍图片文件上传到指定的 FTP 服务器上。设置方法如下：

- 1) 进入**配置>网络>其他协议>FTP** 界面；

图 8-16 FTP

- 2) 填写 FTP 服务器的 IP 地址及对应端口；
- 3) 填写具有上传权限的用户的用户名、密码。若匿名用户也具有上传权限，也可勾选“匿名”使用匿名方式访问 FTP 服务器；

- 4) 设置目录结构，即文件的保存路径，根据实际需求在下拉列表中进行选择，可选择“使用根目录”、“使用一级目录”、“使用二级目录”；
  - 一级目录可选择“使用设备名”、“使用设备 IP”、“自定义”。
  - 二级目录可选择“使用通道号”、“自定义”。
- 5) 可点击“测试”，测试当前 FTP 是否可用，测试结果将显示在弹出的对话框中；
- 6) 点击“保存”完成配置。

### 8.6.1.3.3 PPPoE

PPPoE 即以太网上的点对点协议，是通过设置运营商（电信、联通、移动）提供的上网账号，使设备能拨号连接互联网。设置方法如下：

- 1) 进入**配置>网络>其他协议>PPPoE** 界面；

网卡	GLAN1
IP版本	IPV4
启用	<input type="checkbox"/>
动态IP	0.0.0.0
用户名	root
密码	●●●●

根据国家《互联网信息服务管理办法》，通过80端口提供网页服务都需要ICP备案，否则无法访问。建议你先修改Web服务端口。

**保存**

图 8-17 PPPoE

- 2) 勾选“启用”，开启 PPPoE 拨号功能，并选择网卡；
- 3) 填写网络运营商 ISP 提供的上网用户名和密码；
- 4) 点击“保存”完成配置，拨号成功后显示动态 IP。

### 8.6.1.3.4 K-SNMP

K-SNMP 即科达私有网络管理协议。设置方法如下：

- 1) 进入**配置>网络>其他协议>K-SNMP** 界面；

网管服务器地址	0.0.0.0	
网管服务器端口	1727	
设备位置信息	0	
CPU利用率阈值	100	1~100
内存利用率阈值	100	1~100
视频丢包率阈值	100	1~100

**保存**

图 8-18 K-SNMP

- 2) 填写网管服务器地址和设备位置信息；
- 3) 设置 CPU 利用率阈值、内存利用率阈值和视频丢包率阈值，默认值均为 100，范围 1~100；

4) 点击“保存”完成配置。

#### 8.6.1.3.5 802.1X

802.1X 即基于端口的访问控制协议。支持用户手动选择认证方式来控制连接到局域网的设备是否能够接入局域网，能够很好的支撑网络的认证、计费、安全和管理要求。设置方法如下：

1) 进入**配置>网络>其他协议>802.1X**界面；

启用	<input type="checkbox"/>
协议类型	EAP-MD5
EAPOL版本	1
用户名	root
密码	....

图 8-19 802.1X

2) 勾选“启用”，开启 802.1x 协议；

3) 协议类型默认为 EAP-MD5；

4) 根据需要在下拉框中选择 EAPOL 版本；

5) 填写用户名和密码；

6) 点击“保存”完成配置。

#### 8.6.1.3.6 QoS

QoS 即服务质量，可有效解决网络延迟和网络阻塞问题。设置方法如下：

**i** 说明：QoS 功能需要传输路径上的网络设备（如路由器、交换机）支持。

1) 进入**配置>网络>其他协议>QoS**界面；

启用	<input checked="" type="checkbox"/>
音视频DSCP	0 0~63
管理DSCP	0 0~63

图 8-20 QoS

2) 勾选“启用”，开启 QoS 功能；

3) 设置音视频 DSCP 和管理 DSCP 值，范围 0~63；

**i** 说明：DSCP 优先级有 64 个（0-63），标识了包的优先级不同，网络可根据 DSCP 权值来判断数据传输的优先级，0 优先级最低，63 优先级最高，根据包的优先级选择不同的出队列，不同出队列所占的带宽资源，拥塞时丢弃比例不同，从而实现服务质量的目的。

**i** 注意：配置时需要在路由器端设置相同值。

4) 点击“保存”完成配置。

### 8.6.1.3.7 UPnP

通过 UPnP 协议在私网与外网间建立映射关系。内部端口为人脸门禁设备端口，外部端口为路由器端口，用户访问外部端口时就能访问人脸门禁设备。设置方法如下：

**i** 说明：对于一台处在内网环境的设备，UPnP 功能可以使网关或路由器做自动端口映射，将设备监听的端口从网关或路由器映射到内网设备上，网关或路由器的网络防火墙模块开始对 Internet 上其他电脑开放这个端口。

1) 进入配置>网络>其他协议>UPnP 界面；

选择	协议名称	IP	外部端口	状态
<input checked="" type="checkbox"/>	HTTP	0.0.0.0	0	未生效
<input checked="" type="checkbox"/>	RTSP	0.0.0.0	0	未生效
<input checked="" type="checkbox"/>	SDK	0.0.0.0	0	未生效

图 8-21 UPnP

2) 勾选“启用”，开启 UPnP 功能；

3) 设置别名，设置后，在同一局域网广播域中开启了 UPnP 协议的电脑系统上，用户可以直接在系统的网络中搜索到该别名，双击该图标，即会自动弹出浏览器页面访问设备的当前 IP 地址；

4) 选择映射端口方式为手动或自动，选择“手动”时，需填写外部端口；

5) 点击“保存”完成配置。

### 8.6.1.3.8 SNMP

通过配置 SNMP 协议可实现对设备参数的获取和接受设备的报警异常信息，设备支持 V1/V2 和 V3 网络管理协议，请根据实际需求选择相应的进行配置。设置方法如下：

**i** 说明：设置 SNMP 参数前，用户需要有 SNMP 服务器并配置好各项参数。

1) 进入配置>网络>其他协议>SNMP 界面；

图 8-22 SNMP

- 2) 选择并勾选 SNMP 对应版本;
- 3) 输入 SNMP 端口, 默认 161, 根据实际情况修改;
- 4) 填写读共同体、写共同体、Trap 地址等信息;
- 5) 填写入网设备 ID;
- 6) 若 SNMP 版本选择了 V3 版本, 还需要填写只读用户名, 选择鉴权方式和加密方式, 设置鉴权密码和加密密码;
- 7) 点击“保存”完成配置。

#### 8.6.1.3.9 邮件 (SMTP)

SMTP 即简单邮件传输协议。当产生告警时, 设备可通过 SMTP 自动发送告警邮件。设置方法如下:

- 1) 进入配置>网络>其他协议>邮件 (SMTP) 界面;

The screenshot shows the configuration page for SMTP. On the left, there are labels for each field: SMTP服务器, 端口, 发件人, 发件人地址, 服务器认证, 用户名, 密码, 主题, 附件, 附件类型, and 收件人. The corresponding input fields are on the right. The '端口' field contains '25' and has a range indicator '1~65535'. The '服务器认证' field has a checked checkbox. The '用户名' field contains 'root'. The '密码' field is masked with dots. The '主题' field contains 'IPCMail'. The '附件' field has an unchecked checkbox. The '附件类型' field is a dropdown menu set to '图片'. The '收件人' field has an input box and a '+' button. Below the recipient list is a '-' button. At the bottom center is a blue '保存' button.

图 8-23 SMTP

- 2) 填写 SMTP 服务器的 IP 地址和端口, 端口范围为 1~65535, 默认端口为 25;
- 3) 填写发件人的名称和地址; 可勾选开启服务器认证, 并填写正确的用户名和密码;
- 4) 填写邮件主题; 可勾选附件并选择附件类型, 勾选后发送的邮件中将附带相关附件;
- 5) 添加收件人邮箱地址, 在收件人地址栏输入邮箱地址并点击后面的“+”号, 地址保存至下方列表中, 选中某一邮箱地址, 点击列表框右下方“-”号即可删除该邮箱;
- 6) 点击“保存”完成配置。

**i** 说明: 配置完成, 且开启邮件通知后, 即可正常发送告警邮件。

## 8.6.2 事件

### 8.6.2.1 基础智能

### 8.6.2.1.1 移动侦测

移动侦测功能用来侦测某段时间内，侦测区域内是否有移动的物体。当有移动的物体时，全景模块的摄像机将根据设置的联动方式进行自动录像、报警等操作。设置方法如下：

1) 进入**配置>事件>基础智能>移动侦测**界面；



图 8-24 移动侦测

- 2) 勾选“启用”，开启移动侦测功能；
- 3) 设置移动侦测区域，默认为全画面侦测，点击“清除全部”，取消全画面侦测。点击“开始绘制”，视频图像被划分成 16 列 12 行的小区域，按住鼠标左键向右下方画出一个被侦测区域，该区域呈紫红色，IPC 设备最多可同时支持 4 个区域的移动侦测功能；按住鼠标左键向左上方画出一个区域或单击小方格取消区域，点击“停止绘制”，完成移动侦测区域的绘制；
- 4) 拖动灵敏度滑块调整移动侦测灵敏度，灵敏度越高，越容易触发告警；

- 5) 选择检测目标，可勾选人、机动车、非机动车。即在侦测区域内检测所选择的目标；
- 6) 勾选联动方式，即移动侦测区域检测到异常情况触发告警的联动方式；

**i** 说明：本设备暂不支持报警输出。

- 7) 设置布防时间，默认布防时间为全天 24 小时，高亮显示，可自定义时间段。一天内最多可设置 10 个时间段，不同的时间段不能重合；

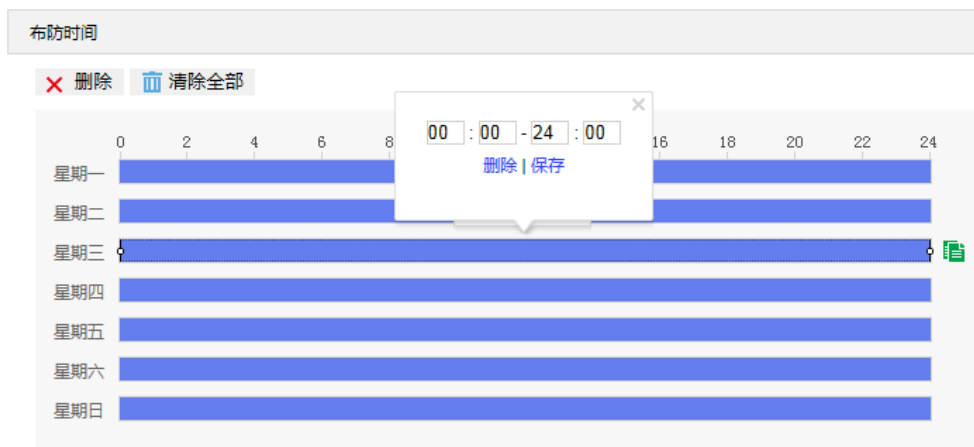



图 8-25 布防时间

- 设置时间：根据需要设置布防时间。
  - 单击高亮长方形会弹出编辑窗口，可设置时间段的具体开始时间和结束时间，点击该窗口“保存”即可生效。
  - 单击高亮长方形，两端会出现白色方块。鼠标拖动白色方块，可设置开始时间和结束时间。
  - 选定某一天的时间轴，删除默认高亮时间段，按住鼠标左键在时间轴上从左向右拉出一个高亮长方形，长方形两端上方会显示开始时间和结束时间。
- 复制时间：点击时间轴后面的  图标可将该天的布防时间复制到其余一个或多个日期当中。
- 删除时间：点击时间轴上方“清除全部”可删除全部时间段；单击某一时间段，点击弹出的编辑窗口“删除”或时间轴上方“删除”均可删除时间段。

**i** 说明：鼠标点击选中时间段，可在不改变录像时长的情况下在时间轴上拖动时间段改变录像时间的起始结束位置。

- 8) 点击“保存”完成配置。

#### 8.6.2.1.2 遮挡报警

遮挡报警是指当设置的遮挡报警区域被遮挡，致使无法对该区域进行正常的画面监控时产生的报警。当遮挡报警产生后，可以迅速排查遮挡报警产生的原因，还原监控画面。设置方法如下：

- 1) 进入配置>事件>基础智能>遮挡报警界面；



图 8-26 遮挡报警

- 2) 勾选“启用”，开启遮挡报警功能；
- 3) 设置遮挡报警区域，默认为全画面侦测，点击“清除全部”，取消全画面侦测。点击“开始绘制”，视频图像被划分成 16 列 12 行的小区域，按住鼠标左键向右下方画出一个区域，该区域呈紫红色，IPC 设备最大支持 1 个区域的遮挡报警功能；点击“清除全部”，取消区域；点击“停止绘制”，完成区域设置；
- 4) 拖动灵敏度滑块调整遮挡报警灵敏度，灵敏度越高，越容易触发告警；
- 5) 勾选联动方式，即遮挡报警区域检测到异常情况触发告警的联动方式；

**i 说明：**本设备暂不支持报警输出。

- 5) 设置布防时间，默认布防时间为全天 24 小时，高亮显示，可自定义时间段。一天内最多可设置 10 个时间段，不同的时间段不能重合；

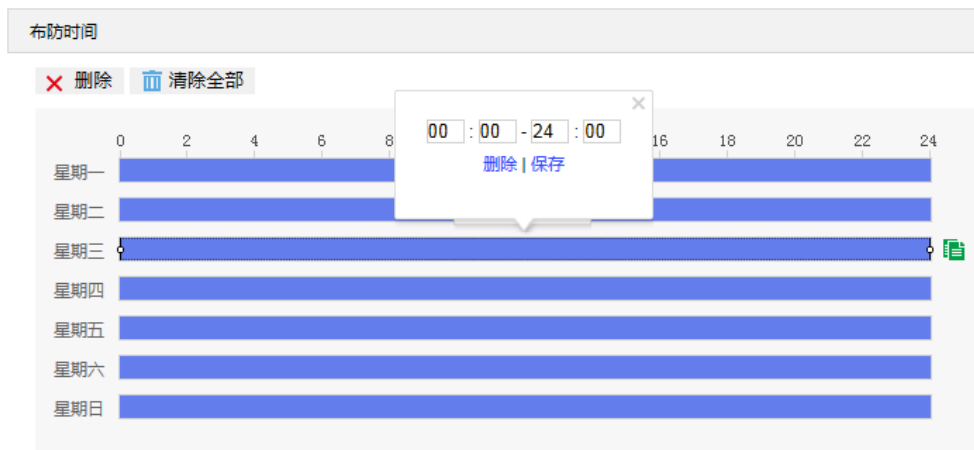



图 8-27 布防时间

- 设置时间：根据需要设置布防时间。
  - 单击高亮长方形会弹出编辑窗口，可设置时间段的具体开始时间和结束时间，点击该窗口“保存”即可生效。
  - 单击高亮长方形，两端会出现白色方块。鼠标拖动白色方块，可设置开始时间和结束时间。
  - 选定某一天的时间轴，删除默认高亮时间段，按住鼠标左键在时间轴上从左向右拉出一个高亮长方形，长方形两端上方会显示开始时间和结束时间。
- 复制时间：点击时间轴后面的  图标可将该天的布防时间复制到其余一个或多个日期当中。
- 删除时间：点击时间轴上方“清除全部”可删除全部时间段；单击某一时间段，点击弹出的编辑窗口“删除”或时间轴上方“删除”均可删除时间段。

**i** 说明：鼠标点击选中时间段，可在不改变录像时长的情况下在时间轴上拖动时间段改变录像时间的起始结束位置。

6) 点击“保存”完成配置。

#### 8.6.2.1.3 警戒线

警戒线功能是指侦测是否有物体按照设置的移动方向跨越设置的警戒线，全景模块的摄像机将根据判断结果联动报警。设置方法如下：

- 1) 进入 **配置>事件>基础智能>警戒线** 界面；



图 8-28 警戒线

- 2) 勾选“启用”，开启警戒线功能；
- 3) 在警戒线方向下拉列表中选择警戒线方向，可选择“A->B”、“B->A”、“A<-> B”。“A->B”是指移动物体由 A 到 B 移动时将触发报警，“B->A”是指移动物体由 B 到 A 移动时将触发报警，“A<-> B”是指移动物体双向移动时将触发报警；
- 4) 目标过滤，即设置目标区域。点击“开始绘制”，在画面中拖动鼠标绘制出矩形区域，绘制完成后点击“停止绘制”，然后拖动下方的最大、最小目标比例滑块设置目标比例（默认为 1%），目标比例设置后，超过最大目标或小于最小目标的移动物体跨越警戒线均不会触发告警；
- 5) 区域设置，即规划警戒线。点击“开始绘制”，在画面中拖动鼠标绘制一条警戒线，警戒线绘制完成后，可拖动其起点或终点调节警戒线长度和角度，点击“停止绘制”停止绘制；
- 6) 拖动灵敏度滑块调整警戒线告警灵敏度，灵敏度越高，越容易触发告警；

- 7) 选择检测目标，可勾选人、机动车、非机动车。即在侦测区域内检测所选择的目标。
- 8) 勾选联动方式，即警戒线检测到异常情况触发告警的联动方式；

**i** 说明：本设备暂不支持报警输出。

- 9) 设置布防时间，默认布防时间为全天 24 小时，高亮显示，可自定义时间段。一天内最多可设置 10 个时间段，不同的时间段不能重合；

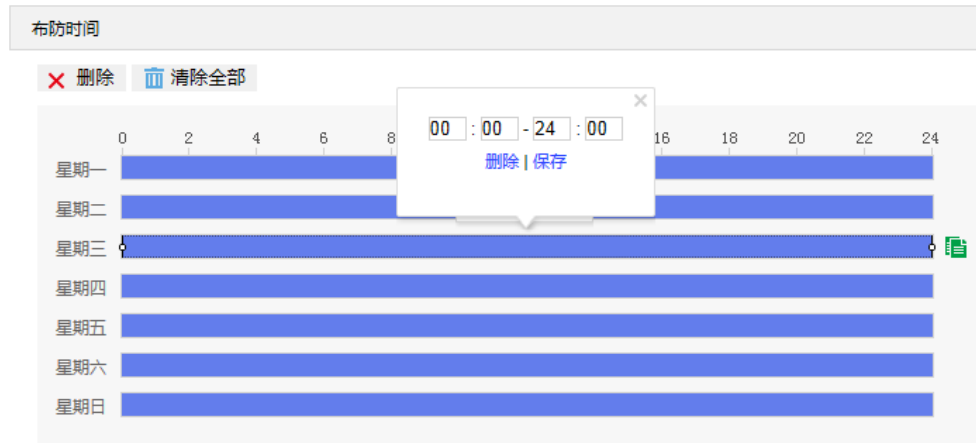



图 8-29 布防时间

- 设置时间：根据需要设置布防时间。
  - 单击高亮长方形会弹出编辑窗口，可设置时间段的具体开始时间和结束时间，点击该窗口“保存”即可生效。
  - 单击高亮长方形，两端会出现白色方块。鼠标拖动白色方块，可设置开始时间和结束时间。
  - 选定某一天的时间轴，删除默认高亮时间段，按住鼠标左键在时间轴上从左向右拉出一个高亮长方形，长方形两端上方会显示开始时间和结束时间。
- 复制时间：点击时间轴后面的  图标可将该天的布防时间复制到其余一个或多个日期当中。
- 删除时间：点击时间轴上方“清除全部”可删除全部时间段；单击某一时间段，点击弹出的编辑窗口“删除”或时间轴上方“删除”均可删除时间段。

**i** 说明：鼠标点击选中时间段，可在不改变录像时长的情况下在时间轴上拖动时间段改变录像时间的起始结束位置。

- 10) 点击“保存”完成配置。

#### 8.6.2.1.4 虚焦检测

虚焦检测功能是指检测监控图像是否存在不清晰的情况，全景模块的摄像机将根据判断结果联动报警。设置方法如下：

- 1) 进入**配置>事件>基础智能>虚焦检测**界面；

启用

灵敏度

联动方式(常规联动)

上传中心

上传COI

显示字幕

邮件通知

联动方式(其他联动)

报警输出  报警输出1

保存

图 8-30 虚焦检测

- 勾选“启用”，开启虚焦检测功能；
- 拖动灵敏度滑块设置虚焦检测灵敏度，灵敏度越高，越容易触发告警；
- 勾选联动方式，即检测到异常情况触发告警的联动方式；

**i** 说明：本设备暂不支持报警输出。

- 点击“保存”完成配置。

#### 8.6.2.1.5 场景变更

场景变更功能是指检测监控场景是否发生变更，全景模块的摄像机将根据判断结果联动报警。设置方法如下：

- 进入配置>事件>基础智能>场景变更界面；

启用  
 检测模式 软件检测  
 灵敏度 1

联动方式(常规联动)

上传中心  
 上传COI  
 显示字幕  
 录像联动  
 抓拍  
 邮件通知

联动方式(其他联动)

报警输出  报警输出1

布防时间

	0	2	4	6	8	10	12	14	16	18	20	22	24
星期一	[高亮显示]												
星期二	[高亮显示]												
星期三	[高亮显示]												
星期四	[高亮显示]												
星期五	[高亮显示]												
星期六	[高亮显示]												
星期日	[高亮显示]												

图 8-31 场景变更

- 2) 勾选“启用”，开启场景变更侦测功能；
- 3) 在下拉列表中选择检测模式并拖动灵敏度滑块设置场景变更侦测灵敏度，灵敏度越高，越容易触发告警；
- 4) 勾选联动方式，即检测到异常情况触发告警的联动方式；

**i** 说明：本设备暂不支持报警输出。

- 5) 设置布防时间，默认布防时间为全天 24 小时，高亮显示，可自定义时间段。一天内最多可设置 10 个时间段，不同的时间段不能重合；

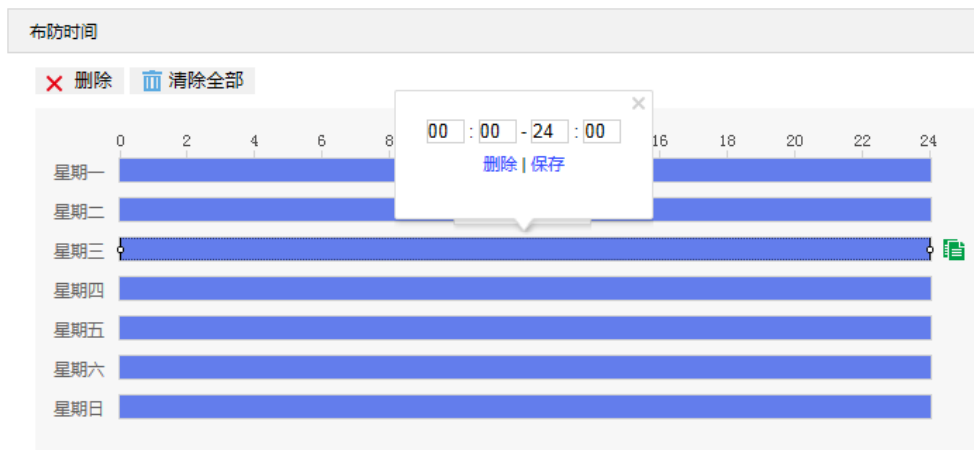



图 8-32 布防时间

- 设置时间：根据需要设置布防时间。
  - 单击高亮长方形会弹出编辑窗口，可设置时间段的具体开始时间和结束时间，点击该窗口“保存”即可生效。
  - 单击高亮长方形，两端会出现白色方块。鼠标拖动白色方块，可设置开始时间和结束时间。
  - 选定某一天的时间轴，删除默认高亮时间段，按住鼠标左键在时间轴上从左向右拉出一个高亮长方形，长方形两端上方会显示开始时间和结束时间。
- 复制时间：点击时间轴后面的  图标可将该天的布防时间复制到其余一个或多个日期当中。
- 删除时间：点击时间轴上方“清除全部”可删除全部时间段；单击某一时间段，点击弹出的编辑窗口“删除”或时间轴上方“删除”均可删除时间段。

**i** 说明：鼠标点击选中时间段，可在不改变布防时长的情况下在时间轴上拖动时间段改变布防时间的起始结束位置。

6) 点击“保存”完成配置。

#### 8.6.2.1.6 区域进入

区域进入功能是指侦测是否有物体进入设置的警戒区域，全景模块的摄像机将根据判断结果联动报警。设置方法如下：

- 1) 进入 **配置>事件>基础智能>区域进入**界面；

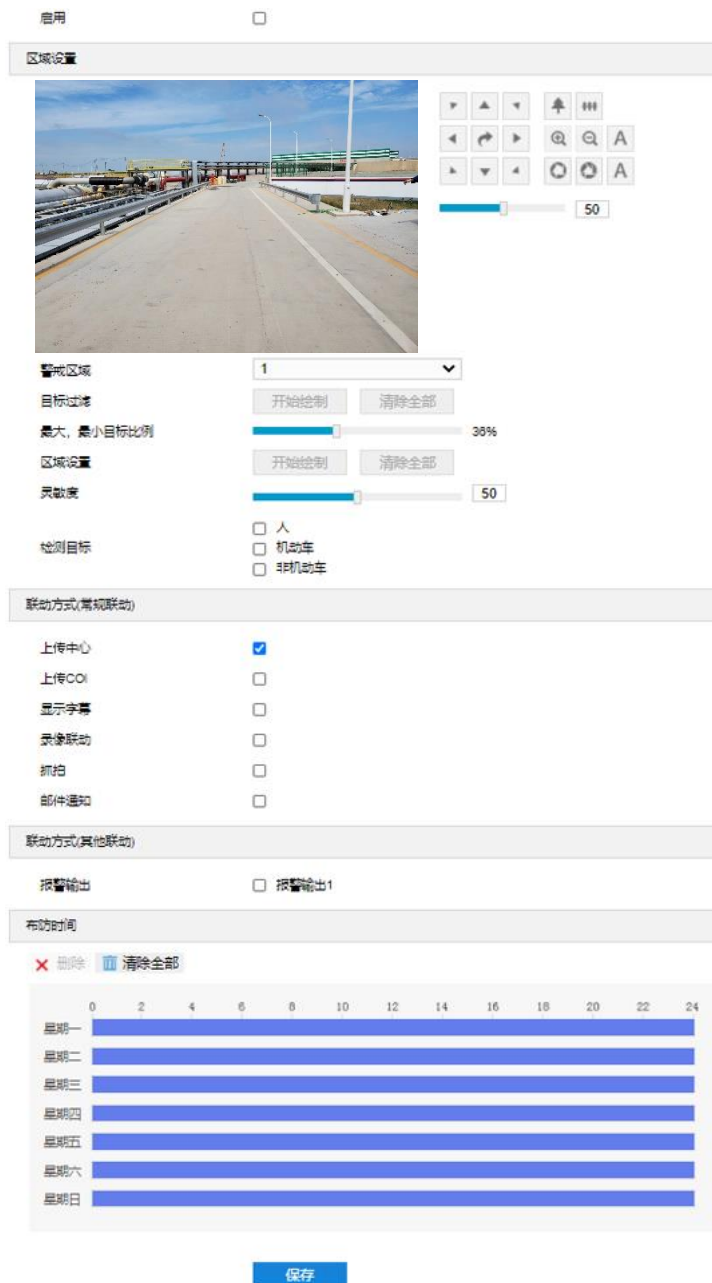


图 8-33 区域进入

- 2) 勾选“启用”，开启区域进入侦测功能；
- 3) 目标过滤，即设置目标区域。点击“开始绘制”，在画面中拖动鼠标绘制出矩形区域，绘制完成后点击“停止绘制”，然后拖动下方的最大、最小目标比例滑块设置目标比例（默认为 1%），目标比例设置后，超过最大目标或小于最小目标的移动物体进入区域均不会触发告警；
- 4) 区域设置，即设置警戒区域。点击“开始绘制”，在画面中依次点击鼠标绘制 3~6 个点的封闭区域，单击鼠标右键或点击起始点封闭区域，点击“停止绘制”停止绘制；
- 5) 拖动灵敏度滑块调整区域进入告警灵敏度，灵敏度越高，越容易触发告警；
- 6) 选择检测目标，可勾选人、机动车、非机动车。即在侦测区域内检测所选择的目标；
- 7) 勾选联动方式，即警戒区域检测到异常情况触发告警的联动方式；

**i** 说明：本设备暂不支持报警输出。

- 8) 设置布防时间，默认布防时间为全天 24 小时，高亮显示，可自定义时间段。一天内最多可设置 10 个时间段，不同的时间段不能重合；

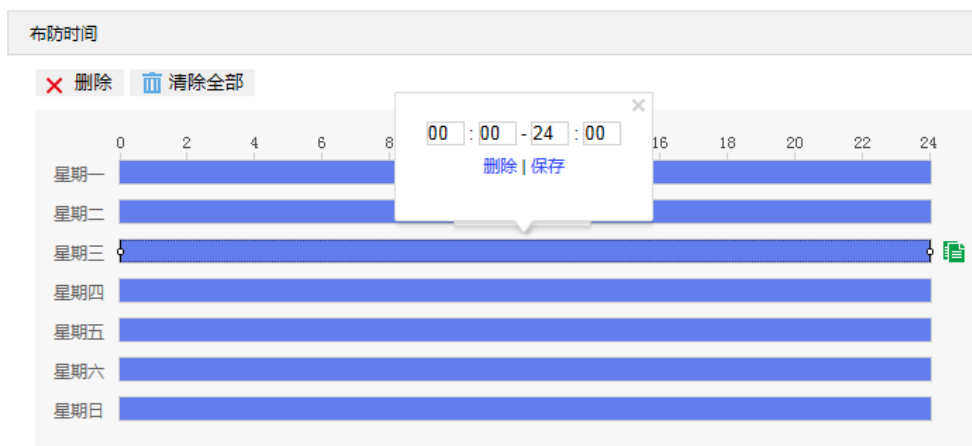



图 8-34 布防时间

- 设置时间：根据需要设置布防时间。
  - 单击高亮长方形会弹出编辑窗口，可设置时间段的具体开始时间和结束时间，点击该窗口“保存”即可生效。
  - 单击高亮长方形，两端会出现白色方块。鼠标拖动白色方块，可设置开始时间和结束时间。
  - 选定某一天的时间轴，删除默认高亮时间段，按住鼠标左键在时间轴上从左向右拉出一个高亮长方形，长方形两端上方会显示开始时间和结束时间。
- 复制时间：点击时间轴后面的  图标可将该天的布防时间复制到其余一个或多个日期当中。
- 删除时间：点击时间轴上方“清除全部”可删除全部时间段；单击某一时间段，点击弹出的编辑窗口“删除”或时间轴上方“删除”均可删除时间段。

**i** 说明：鼠标点击选中时间段，可在不改变录像时长的情况下在时间轴上拖动时间段改变录像时间的起始结束位置。

- 9) 点击“保存”完成配置。

#### 8.6.2.1.7 区域离开

区域离开功能是指侦测是否有物体离开设置的警戒区域，全景模块的摄像机将根据判断结果联动报警。设置方法如下：

- 1) 进入配置>事件>基础智能>区域离开界面；

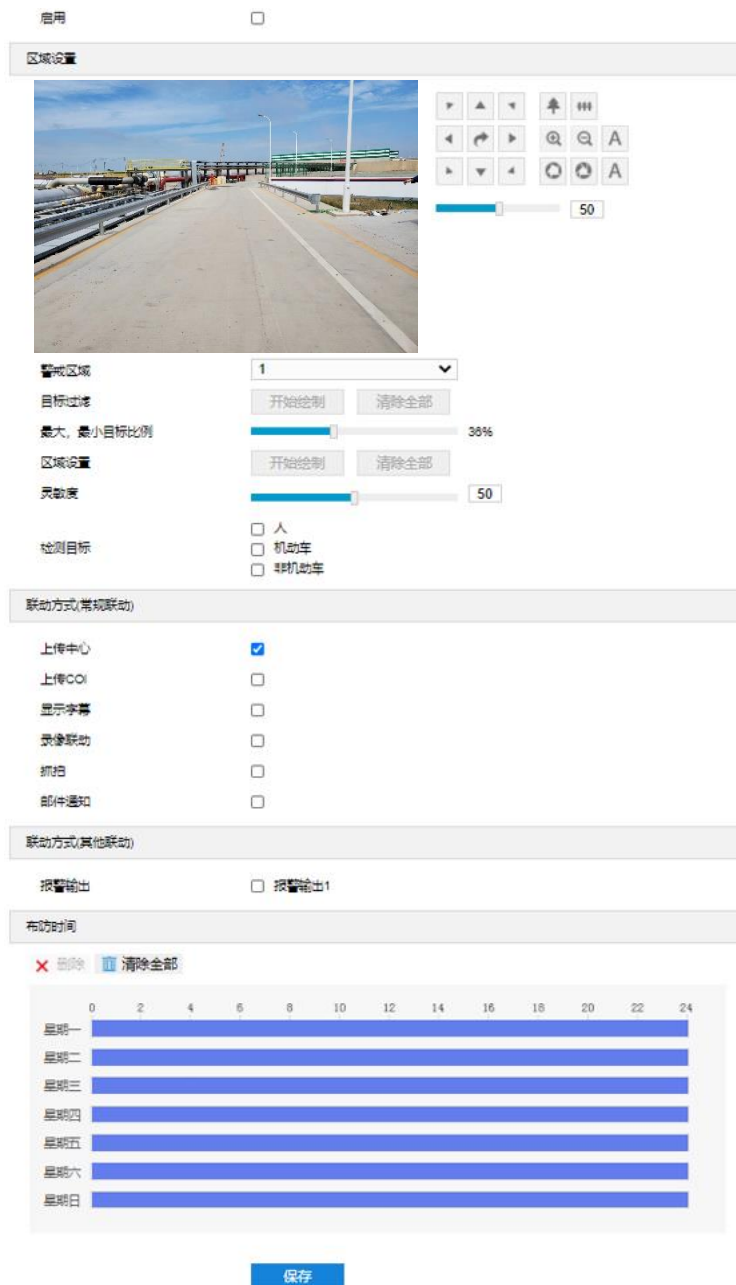


图 8-35 区域离开

- 2) 勾选“启用”，开启区域离开侦测功能；
- 3) 目标过滤，即设置目标区域。点击“开始绘制”，在画面中拖动鼠标绘制出矩形区域，绘制完成后点击“停止绘制”，然后拖动下方的最大、最小目标比例滑块设置目标比例（默认为 1%），目标比例设置后，超过最大目标或小于最小目标的移动物体离开区域均不会触发告警；
- 4) 区域设置，即设置警戒区域。点击“开始绘制”，在画面中依次点击鼠标绘制 3~6 个点的封闭区域，单击鼠标右键或点击起始点封闭区域，点击“停止绘制”停止绘制；
- 5) 拖动灵敏度滑块调整区域离开告警灵敏度，灵敏度越高，越容易触发告警；
- 6) 选择检测目标，可勾选人、机动车、非机动车。即在侦测区域内检测所选择的目标。
- 7) 勾选联动方式，即警戒区域检测到异常情况触发告警的联动方式；

**i** 说明：本设备暂不支持报警输出。

- 8) 设置布防时间，默认布防时间为全天 24 小时，高亮显示，可自定义时间段。一天内最多可设置 10 个时间段，不同的时间段不能重合；

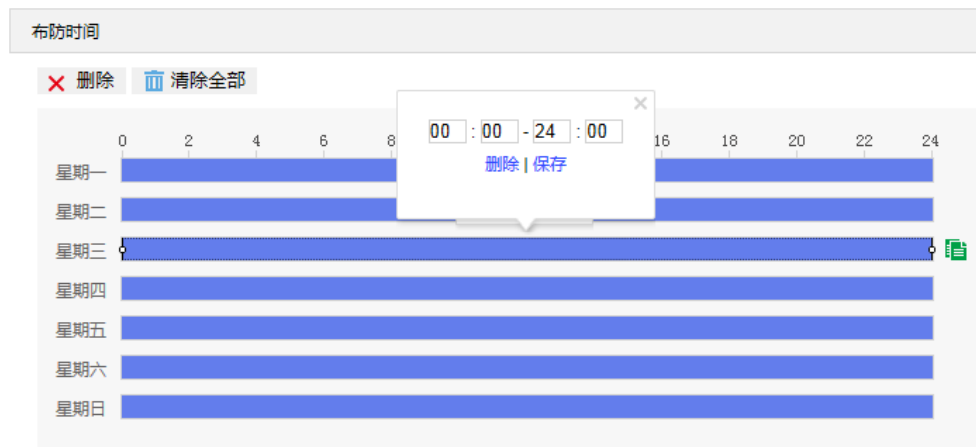



图 8-36 布防时间

- 设置时间：根据需要设置布防时间。
  - 单击高亮长方形会弹出编辑窗口，可设置时间段的具体开始时间和结束时间，点击该窗口“保存”即可生效。
  - 单击高亮长方形，两端会出现白色方块。鼠标拖动白色方块，可设置开始时间和结束时间。
  - 选定某一天的时间轴，删除默认高亮时间段，按住鼠标左键在时间轴上从左向右拉出一个高亮长方形，长方形两端上方会显示开始时间和结束时间。
- 复制时间：点击时间轴后面的  图标可将该天的布防时间复制到其余一个或多个日期当中。
- 删除时间：点击时间轴上方“清除全部”可删除全部时间段；单击某一时间段，点击弹出的编辑窗口“删除”或时间轴上方“删除”均可删除时间段。

**i** 说明：鼠标点击选中时间段，可在不改变录像时长的情况下在时间轴上拖动时间段改变录像时间的起始结束位置。

- 9) 点击“保存”完成配置。

#### 8.6.2.1.8 区域入侵

区域入侵功能是指侦测是否有物体入侵设置的警戒区域，并在该警戒区域停留时间达到设置的时间阈值，全景模块的摄像机将根据判断结果联动报警。设置方法如下：

- 1) 进入配置>事件>基础智能>区域入侵界面；

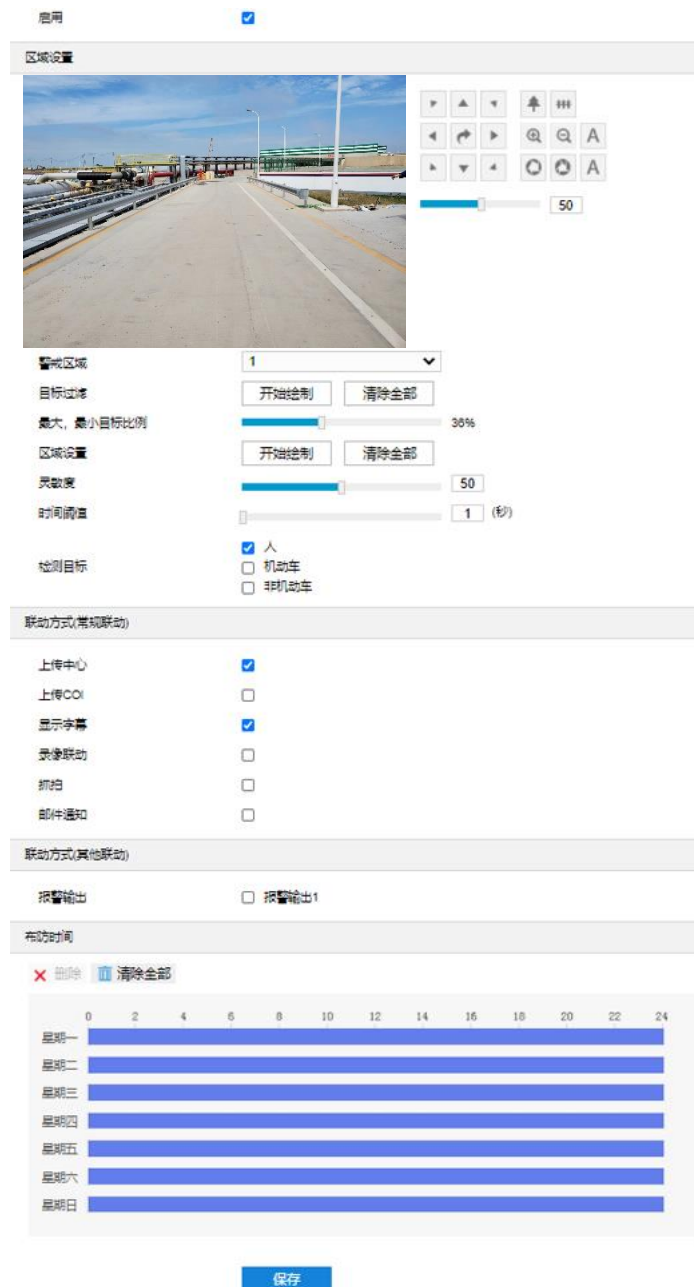


图 8-37 区域入侵

- 2) 勾选“启用”，开启区域入侵侦测功能；
- 3) 目标过滤，即设置目标区域。点击“开始绘制”，在画面中拖动鼠标绘制出矩形区域，绘制完成后点击“停止绘制”，然后拖动下方的最大、最小目标比例滑块设置目标比例（默认为 1%），目标比例设置后，超过最大目标或小于最小目标的移动物体进入区域均不会触发告警；
- 4) 区域设置，即设置警戒区域。点击“开始绘制”，在画面中依次点击鼠标绘制 3~6 个点的封闭区域，单击鼠标右键或点击起始点封闭区域，点击“停止绘制”停止；
- 5) 拖动灵敏度滑块调整区域入侵告警灵敏度，灵敏度越高，越容易触发告警；
- 6) 拖动时间阈值滑块调节时间阈值，即物体持续停留的最大时间。例如设置为 5 秒，则物体入侵警戒区域内停留 5 秒后触发告警；

- 7) 选择检测目标，可勾选人、机动车、非机动车。即在侦测区域内检测所选择的目标。
- 8) 勾选联动方式，即警戒区域在布防时间内检测到异常情况触发告警的联动方式；

**i** 说明：本设备暂不支持报警输出。

- 9) 设置布防时间，默认布防时间为全天 24 小时，高亮显示，可自定义时间段。一天内最多可设置 10 个时间段，不同的时间段不能重合；

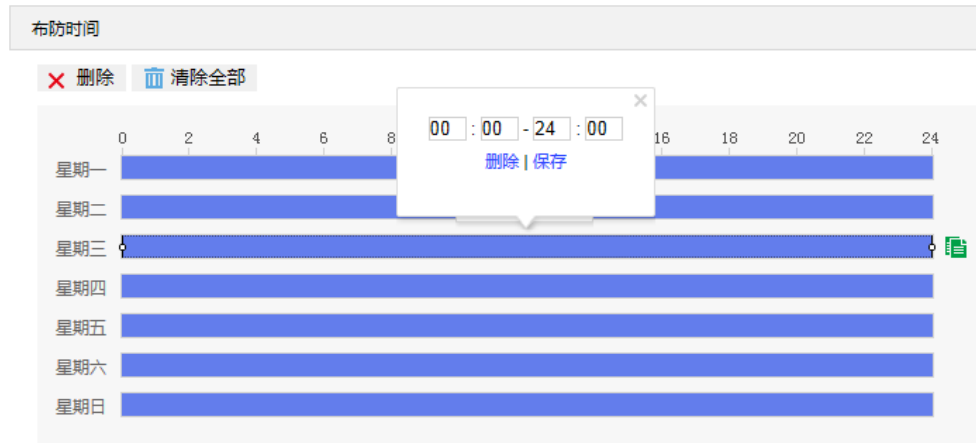



图 8-38 布防时间

- 设置时间：根据需要设置布防时间。
  - 单击高亮长方形会弹出编辑窗口，可设置时间段的具体开始时间和结束时间，点击该窗口“保存”即可生效。
  - 单击高亮长方形，两端会出现白色方块。鼠标拖动白色方块，可设置开始时间和结束时间。
  - 选定某一天的时间轴，删除默认高亮时间段，按住鼠标左键在时间轴上从左向右拉出一个高亮长方形，长方形两端上方会显示开始时间和结束时间。
- 复制时间：点击时间轴后面的  图标可将该天的布防时间复制到其余一个或多个日期当中。
- 删除时间：点击时间轴上方“清除全部”可删除全部时间段；单击某一时间段，点击弹出的编辑窗口“删除”或时间轴上方“删除”均可删除时间段。

**i** 说明：鼠标点击选中时间段，可在不改变录像时长的情况下在时间轴上拖动时间段改变录像时间的起始结束位置。

- 10) 点击“保存”完成配置。

#### 8.6.2.1.9 物品遗留

物品遗留功能是指侦测是否有物体滞留在设置的警戒区域内，并在该警戒区域停留时间达到设置的时间阈值，全景模块的摄像机将根据判断结果联动报警。设置方法如下：

- 1) 进入**配置>事件>基础智能>物品遗留**界面；

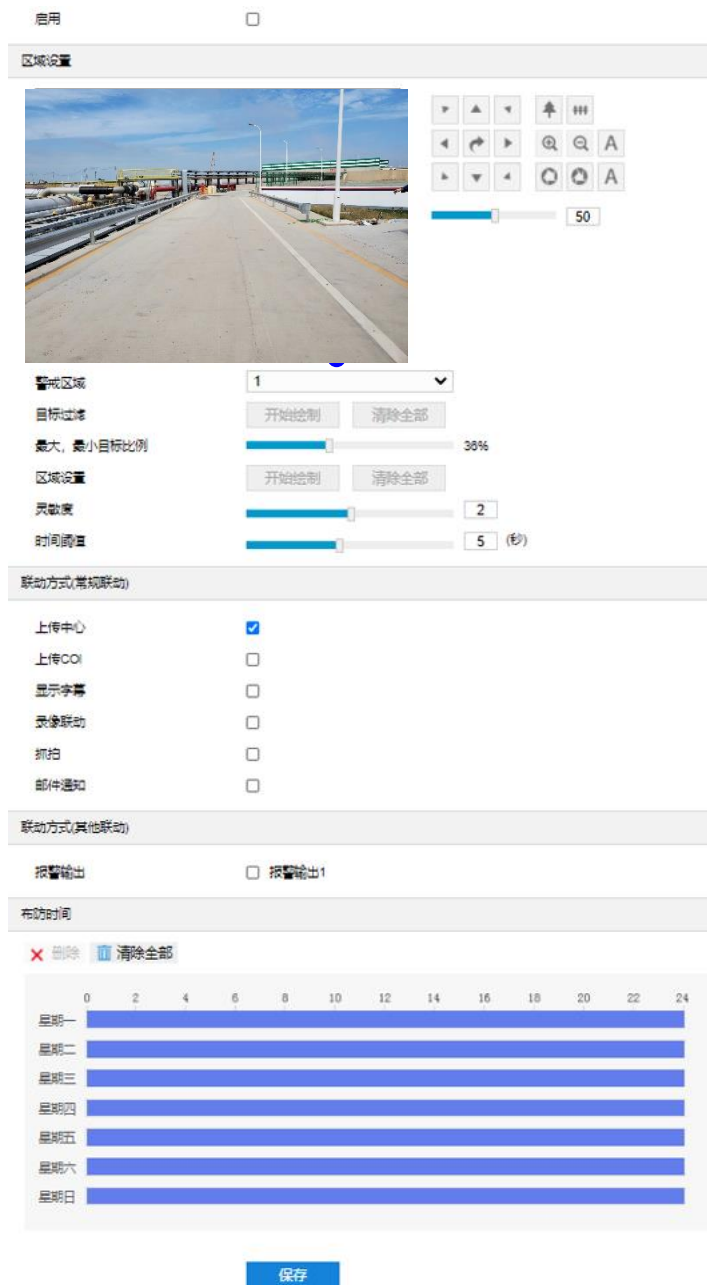


图 8-39 物品遗留

- 2) 勾选“启用”，开启物品遗留侦测功能；
- 3) 在警戒区域下拉列表中选择警戒区域，一次只能设置一个警戒区域，保存后方可设置其他警戒区域，最多可设置四个警戒区域；
- 4) 目标过滤，即设置目标区域。点击“开始绘制”，在画面中拖动鼠标绘制出矩形区域，绘制完成后点击“停止绘制”，然后拖动下方的最大、最小目标比例滑块设置目标比例（默认为 1%），目标比例设置后，超过最大目标或小于最小目标的物体遗留在区域内均不会触发告警；
- 5) 区域设置，即设置警戒区域。点击“开始绘制”，在画面中依次点击鼠标绘制 3~6 个点的封闭区域，单击鼠标右键或点击起始点封闭区域，点击“停止绘制”停止绘制；
- 6) 拖动灵敏度滑块调整物品遗留告警灵敏度，灵敏度越高，越容易触发告警；

- 7) 拖动时间阈值滑块调节时间阈值，即物体滞留的最大时间。例如设置为 5 秒，则物体在警戒区域内滞留 5 秒后触发告警；
- 8) 勾选联动方式，即警戒区域检测到异常情况后触发告警的联动方式；

**i** 说明：本设备暂不支持报警输出。

- 9) 设置布防时间，默认布防时间为全天 24 小时，高亮显示，可自定义时间段。一天内最多可设置 10 个时间段，不同的时间段不能重合；

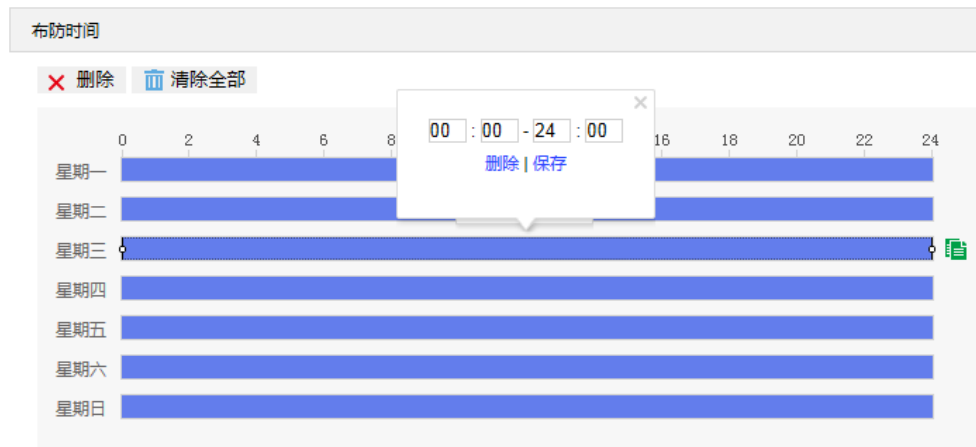



图 8-40 布防时间

- 设置时间：根据需要设置布防时间。
  - 单击高亮长方形会弹出编辑窗口，可设置时间段的具体开始时间和结束时间，点击该窗口“保存”即可生效。
  - 单击高亮长方形，两端会出现白色方块。鼠标拖动白色方块，可设置开始时间和结束时间。
  - 选定某一天的时间轴，删除默认高亮时间段，按住鼠标左键在时间轴上从左向右拉出一个高亮长方形，长方形两端上方会显示开始时间和结束时间。
- 复制时间：点击时间轴后面的  图标可将该天的布防时间复制到其余一个或多个日期当中。
- 删除时间：点击时间轴上方“清除全部”可删除全部时间段；单击某一时间段，点击弹出的编辑窗口“删除”或时间轴上方“删除”均可删除时间段。

**i** 说明：鼠标点击选中时间段，可在不改变布防时长的情况下在时间轴上拖动时间段改变布防时间的起始结束位置。

- 10) 点击“保存”完成配置。

#### 8.6.2.1.10 物品拿取

物品拿去功能是指侦测是否有物体从设置的警戒区域内消失，且消失时间达到设置的时间阈值，全景模块的摄像机将根据判断结果联动报警。设置方法如下：

- 1) 进入 **配置>事件>基础智能>物品拿取** 界面；



图 8-41 物品拿取

- 2) 勾选“启用”，开启物品拿取侦测功能；
- 3) 在警戒区域下拉列表中选择警戒区域，一次只能设置一个警戒区域，保存后方可设置其他警戒区域，最多可设置四个警戒区域；
- 4) 目标过滤，即设置目标区域。点击“开始绘制”，在画面中拖动鼠标绘制出矩形区域，绘制完成后点击“停止绘制”，然后拖动下方的最大、最小目标比例滑块设置目标比例（默认为 1%），目标比例设置后，超过最大目标或小于最小目标的物体从区域中消失均不会触发告警；
- 5) 区域设置，即设置警戒区域。点击“开始绘制”，在画面中依次点击鼠标绘制 3~6 个点的封闭区域，单击鼠标右键或点击起始点封闭区域，点击“停止绘制”停止绘制；
- 6) 拖动灵敏度滑块调整物品拿取告警灵敏度，灵敏度越高，越容易触发告警；

7) 拖动时间阈值滑块调节时间阈值，即物体消失的最大时间。例如设置为 5 秒，则物体从警戒区域内消失 5 秒后触发告警；

8) 勾选联动方式，即警戒区域检测到异常情况后触发告警的联动方式；

**i** 说明：本设备暂不支持报警输出。

9) 设置布防时间，默认布防时间为全天 24 小时，高亮显示，可自定义时间段。一天内最多可设置 10 个时间段，不同的时间段不能重合；

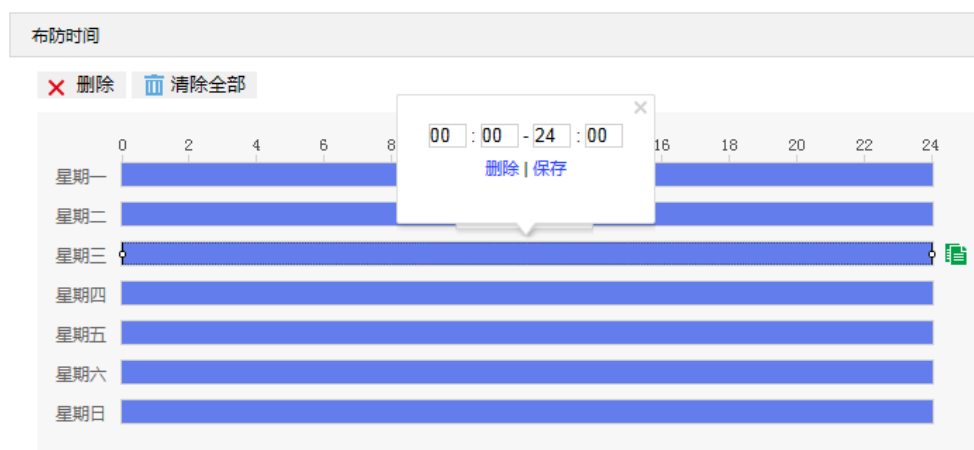



图 8-42 布防时间

➤ 设置时间：根据需要设置布防时间。

- 单击高亮长方形会弹出编辑窗口，可设置时间段的具体开始时间和结束时间，点击该窗口“保存”即可生效。
- 单击高亮长方形，两端会出现白色方块。鼠标拖动白色方块，可设置开始时间和结束时间。
- 选定某一天的时间轴，删除默认高亮时间段，按住鼠标左键在时间轴上从左向右拉出一个高亮长方形，长方形两端上方会显示开始时间和结束时间。

➤ 复制时间：点击时间轴后面的  图标可将该天的布防时间复制到其余一个或多个日期当中。

➤ 删除时间：点击时间轴上方“清除全部”可删除全部时间段；单击某一时间段，点击弹出的编辑窗口“删除”或时间轴上方“删除”均可删除时间段。

**i** 说明：鼠标点击选中时间段，可在不改变录像时长的情况下在时间轴上拖动时间段改变录像时间的起始结束位置。

10) 点击“保存”完成配置。

#### 8.6.2.1.11 人员聚集

人员聚集功能是指侦测设置的警戒区域内，人员密度占比是否超过设置的占比，全景模块的摄像机将根据判断结果联动报警。如规划区域后，设置占比为 50%，则在该区域中的人员覆盖超过 50%的区域即触发告警。设置方法如下：

1) 进入配置>事件>基础智能>人员聚集界面；

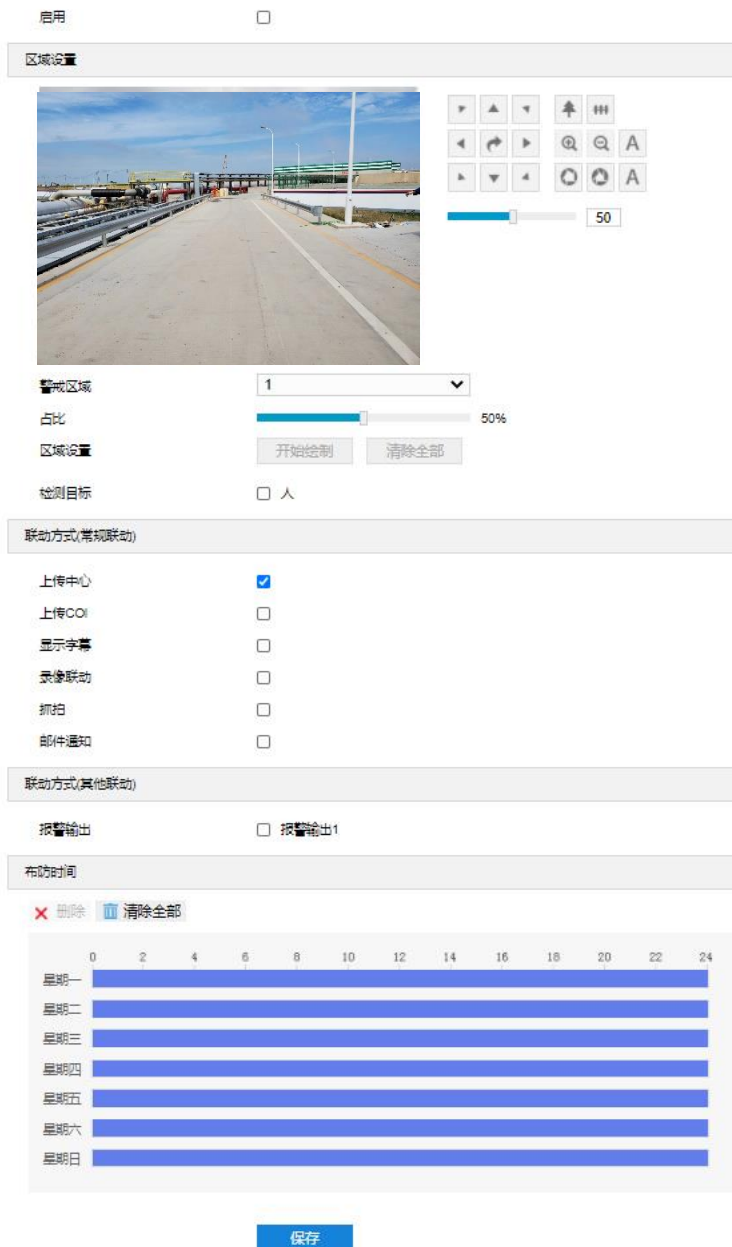


图 8-43 人员聚集

- 2) 勾选“启用”，开启人员聚集侦测功能；
- 3) 设置占比，即在警戒区域中人员覆盖所占的比例，拖动占比滑块设置占比值；
- 4) 区域设置，即设置警戒区域。点击“开始绘制”，在画面中依次点击鼠标绘制 3~6 个点的封闭区域，单击鼠标右键或点击起始点封闭区域，点击“停止绘制”停止绘制；
- 5) 设置检测目标，可勾选为人；
- 6) 勾选联动方式，即警戒区域检测到异常情况后触发告警的联动方式；

**i** 说明：本设备暂不支持报警输出。

- 7) 设置布防时间，默认布防时间为全天 24 小时，高亮显示，可自定义时间段。一天内最多可设置 10 个时间段，不同的时间段不能重合；

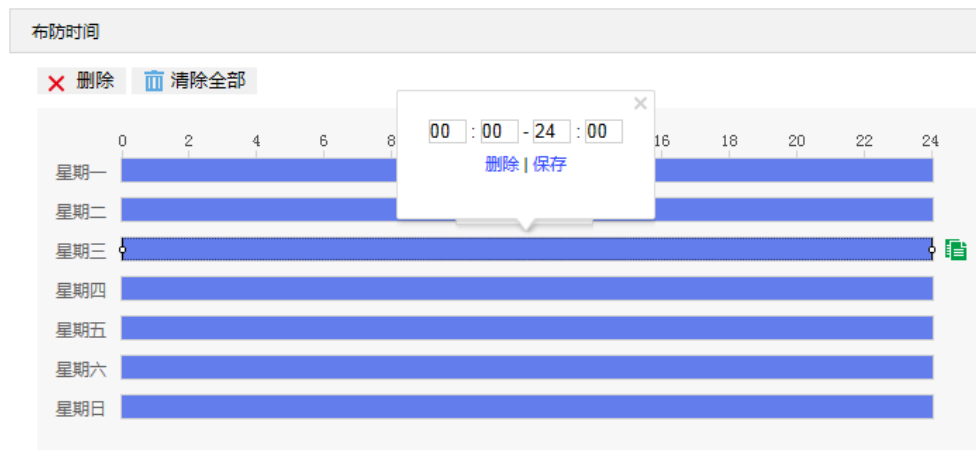



图 8-44 布防时间

- 设置时间：根据需要设置布防时间。
    - 单击高亮长方形会弹出编辑窗口，可设置时间段的具体开始时间和结束时间，点击该窗口“保存”即可生效。
    - 单击高亮长方形，两端会出现白色方块。鼠标拖动白色方块，可设置开始时间和结束时间。
    - 选定某一天的时间轴，删除默认高亮时间段，按住鼠标左键在时间轴上从左向右拉出一个高亮长方形，长方形两端上方会显示开始时间和结束时间。
  - 复制时间：点击时间轴后面的  图标可将该天的布防时间复制到其余一个或多个日期当中。
  - 删除时间：点击时间轴上方“清除全部”可删除全部时间段；单击某一时间段，点击弹出的编辑窗口“删除”或时间轴上方“删除”均可删除时间段。
- i** 说明：鼠标点击选中时间段，可在不改变录像时长的情况下在时间轴上拖动时间段改变录像时间的起始结束位置。

8) 点击“保存”完成配置。

### 8.6.2.2 报警输入

本设备暂不支持该功能。

### 8.6.2.3 报警输出

本设备暂不支持该功能。

### 8.6.2.4 异常联动

配置异常联动参数，当发生异常时，全景模块将根据判断结果联动报警。设置方法如下：

- 1) 进入**配置>事件>异常联动**界面；

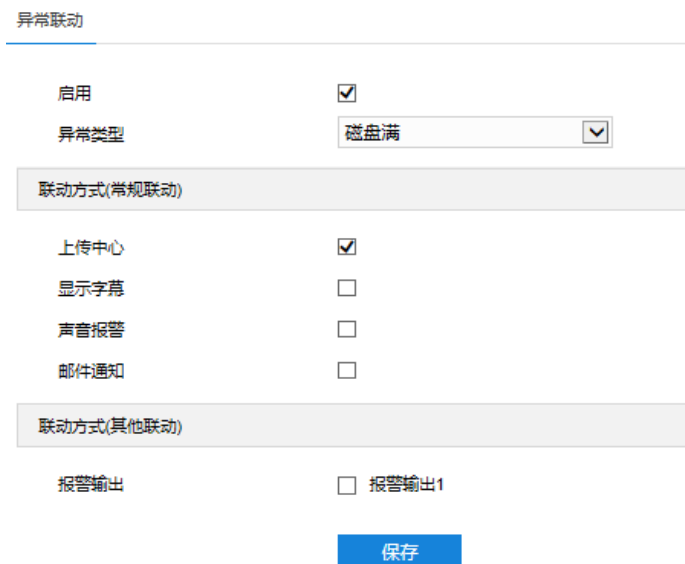


图 8-45 异常联动

- 2) 勾选“启用”，开启异常联动功能；
- 3) 在异常类型下拉列表中选择异常类型；

**i** 说明：

- ◆ 磁盘满：磁盘存储空间不足。
- ◆ 磁盘错误：磁盘不能被识别。
- ◆ 网络断开：设备没有正常联网。

- 4) 点击“保存”完成配置。

**i** 说明：本设备暂不支持报警输出。

### 8.6.3 存储

#### 8.6.3.1 存储管理

进入配置>存储>存储管理界面，可设置磁盘满策略；查看存储设备列表，格式化存储卡；设置抓拍图片的存储位置。

**i** 说明：当设备安装有存储卡且工作正常时，可配置录像计划及抓拍计划。



图 8-46 存储管理

➤ 磁盘满策略：设置磁盘空间不足时的录像策略。

- 覆盖：当存储空间不足时，覆盖最旧录像。
- 停止：当存储空间不足时，自动停止录像。

可以在**配置>事件>异常联动**中设置“异常类型”为磁盘满时触发的告警形式，提示用户本地存储已停止。

➤ 存储设备列表：显示所有存储设备的状态、容量、进度等信息。

- 磁盘号：显示存储设备的序号。
- 容量：显示存储设备的存储容量。
- 剩余空间：显示存储设备的剩余存储空间。
- 状态：显示存储设备的状态信息，如正常（即有存储卡且正常读写）、不存在（即没有存储卡）、未格式化（第一次插入存储卡需要格式化）等；
- 类型：显示存储设备的安装形式。
- 属性：显示存储设备的读写属性，只读、只写或者读写。
- 进度：以百分比形式显示存储卡格式化的进度。选中磁盘，点击“格式化”，即可对选中磁盘进行格式化。

➤ 抓拍：设置抓拍图片的存储位置，根据实际需求选择定时抓拍图片和报警抓拍图片存储在本地或 FTP 服务器。

 **说明：**存储卡出厂时已安装在设备内部，首次使用时，请先点击“格式化”对磁盘进行格式化。

### 8.6.3.2 录像

配置录像计划后，设备将自动在配置的时间内执行不同的录像任务并将该录像保存在存储卡中。设置方法如下：

- 1) 进入**配置>存储>存储管理**界面，设置磁盘满策略并对设备识别到的存储卡进行格式化，如果格式化成功，状态“正常”，表明存储卡可以正常使用；
- 2) 进入**配置>存储>录像**界面，进行录像配置；
  - 录像类型：即选择具体录像的码流。如果对应码流未启用，将无法进行录像。
  - 码流打包格式：根据接入协议的类型选择录像打包格式。
  - 预录方式：即预录时间，为录像开始时间点前的预先录像时间。固定为 30 秒。
  - 录像延时：即录像的延时时间，即在设置的录像时间结束后继续录像的时间。



图 8-47 录像计划

- 3) 勾选“启用”，启用计划录像；
- 4) 设置布防时间，默认时间为全天 24 小时，高亮显示，可自定义时间段。一天内最多可设置 4 个时间段，不同的时间段不能重合。

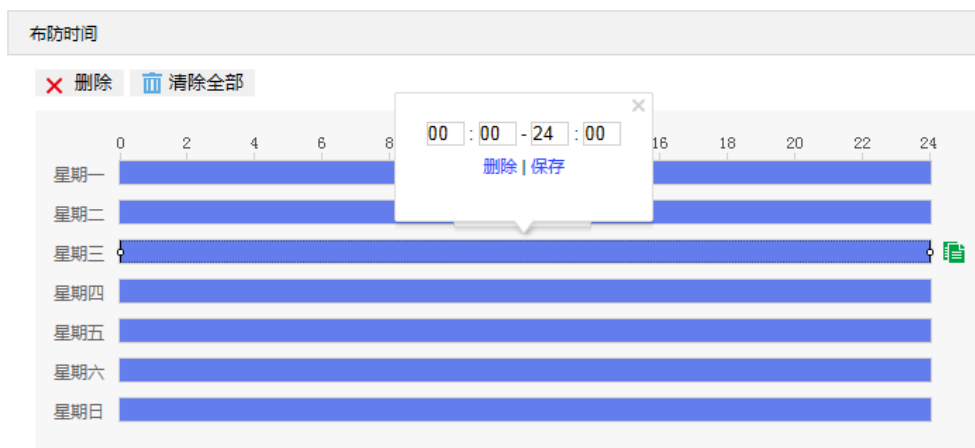



图 8-48 布防时间

- 设置时间：根据需要设置录像时间。
  - 单击高亮长方形会弹出编辑窗口，可设置时间段的具体开始时间和结束时间，点击该窗口“保存”即可生效。

- 单击高亮长方形，两端会出现白色方块。鼠标拖动白色方块，可设置开始时间和结束时间。
  - 选定某一天的时间轴，删除默认高亮时间段，按住鼠标左键在时间轴上从左向右拉出一个高亮长方形，长方形两端上方会显示开始时间和结束时间。
  - 复制时间：点击时间轴后面的图标可将该天的布防时间复制到其余一个或多个日期当中。
  - 删除时间：点击时间轴上方“清除全部”可删除全部时间段；单击某一时间段，点击弹出的编辑窗口“删除”或时间轴上方“删除”均可删除时间段。
- i** 说明：鼠标点击选中时间段，可在不改变录像时长的情况下在时间轴上拖动时间段改变录像时间的起始结束位置。

5) 点击“保存”完成配置。

### 8.6.3.3 抓拍

配置抓拍计划后，设备将自动在配置的时间内执行不同的抓拍任务并将抓拍图片保存在存储卡中。设置方法如下：

- 1) 进入**配置>存储>存储管理**界面，设置磁盘满策略并对设备识别到的存储卡进行格式化，如果格式化成功，状态“正常”，表明存储卡可以正常使用；
- 2) 进入**配置>存储>抓拍**界面，设置抓拍图片参数；
  - 图片格式：只支持 jpeg 格式。
  - 图片分辨率：与主码流当前设置的分辨率一致。
  - 图片质量：设置抓拍图片的质量。

图片格式    
 图片分辨率    
 图片质量

**存储设备列表**

磁盘号	容量	剩余空间	状态	类型	属性
1	30550M	1524M	正常	本地外置	读写

**定时抓拍**

启用    
 抓拍类型    
 时间间隔  (秒) 1~3600

**事件抓拍**

启用    
 时间间隔  (秒) 1~3600   
 抓拍数量  1~65535


图 8-49 抓拍计划

3) 设置定时抓拍参数:

- a) 勾选“启用”，开启定时抓拍;
- b) 选择按时间抓拍或者按数量抓拍，选择按数量抓拍，除设置时间间隔外还需设置抓拍数量;
- c) 设置抓拍的时间间隔;
- d) 设置定时抓拍时间，默认时间为全天 24 小时，高亮显示，可自定义时间段;

➢ 设置时间：根据需要设置录像时间。

- 单击高亮长方形会弹出编辑窗口，可设置时间段的具体开始时间和结束时间，点击该窗口“保存”即可生效。
- 单击高亮长方形，两端会出现白色方块。鼠标拖动白色方块，可设置开始时间和结束时间。
- 选定某一天的时间轴，删除默认高亮时间段，按住鼠标左键在时间轴上从左向右拉出一个高亮长方形，长方形两端上方会显示开始时间和结束时间。

➢ 复制时间：点击时间轴后面的  图标可将该天的布防时间复制到其余一个或多个日期当中。

➤ 删除时间：点击时间轴上方“清除全部”可删除全部时间段；单击某一时间段，点击弹出的编辑窗口“删除”或时间轴上方“删除”均可删除时间段。

**i** 说明：鼠标点击选中时间段，可在不改变录像时长的情况下在时间轴上拖动时间段改变录像时间的起始结束位置。

4) 设置事件抓拍参数：

- a) 勾选“启用”，开启事件抓拍；
- b) 设置抓拍的时间间隔；
- c) 设置每次抓拍的图片数量。

5) 点击“保存”完成配置。