隔爆型制冷型红外光谱成像探测器

[VOCs 气云成像遥测仪]

HS-EX570HD-GLT-CL

用户手册

[

规范使用视频产品的倡议

感谢您选择海是智能的产品。

随着科技进步，技术应用的影响涉及到我们生活的方方面面。作为一家高科技公司，我们日益深刻地认识到科技在提升效率、改善生活品质方面的贡献，同时也认识到科技被不当使用也会带来伤害。例如视频监控产品，因其能够录制真实、完整、清晰的影像，在回溯和还原事实方面具有突出的价值，然而对影像记录的不当传播、不当使用和不当加工等也可能产生侵犯他人合法权益的问题。为了不断推进科技向善，海是智能倡议每一位用户善用科技、善用视频产品，不仅遵循法律法规等规范要求，也遵循道德风俗的约束，共同建立和维护我们良好的社会环境和氛围。

请您仔细阅读如下倡议：

1. 每个人都拥有合理的隐私期待，视频类产品的安装不应违背一个正常人的合理隐私期待。在公共场所安装视频监控类产品时，应当以合理有效的方式做出提示，明确监控区域；在非公共场所安装视频类产品时，不应当侵犯他人的权利和利益，包括但不限于不应当在未经利害关系人同意的情况下安装视频监控类产品、安装高隐蔽性的视频监控类产品。

2. 视频类产品使用期间，将在特定的条件下，对特定的时间和空间范围内真实活动进行记录，用户应当对自身在该特定范围内享有的权利进行合理界定，避免侵犯他人肖像、隐私或其他合法权利。

3. 视频类产品使用期间，将持续产生源于真实场景的视频影像数据，包括产生大量生物数据（如人脸数据），数据可被应用或再加工应用等。视频类产品本身并不能对数据使用做出好坏善恶的识别和区分，数据使用的结果取决于数据控制者的使用方式、使用目的，数据控制者不仅应当遵循法律法规等规范性要求，也应当尊重国际惯例及本地常规、社会道德、公序良俗等非强制性要求，尊重个人的隐私、肖像及其他权利。

4. 鉴于视频类产品持续产生的视频影像数据承担有各利益相关方的权利保护要求、价值主张或其他诉求，保护产品不受侵入、保护数据的安全是至关重要的。产品使用者、数据控制者应当采取合理必要的举措，从而保证数据安全，避免数据泄露、不当披露和使用，包括但不限于合理分配产品的使用与管理权限，结合产品的使用场景建立并不断优化产品所接入的互联网、局域网等各类网络的安全体系等。

5. 视频类产品已经为社会安全的提升做出了很大的贡献，我们相信这些产品还将在社会生活的更多方面发挥积极作用。任何将这些产品用于侵犯人权或违法犯罪的行为，都是违背技术创新和产品研发本意的。为此，海是智能鼓励每一位用户建立评估与跟踪机制，确保产品被正当、合理与善意地使用。

法律声明

版权所有©浙江海是智能科技有限公司　　2022。保留一切权利。

本手册的任何部分，包括文字、图片、图形等均归属于浙江海是智能科技有限公司 或其关联公司（以下简称“海是智能”）。未经书面许可，任何单位或个人不得以任何方式摘录、复制、翻译、修改本手册的全部或部分。除非另有约定，海是智能不对本手册提供任何明示或默示的声明或保证。

关于本产品

本手册描述的产品仅供中国大陆地区销售和使用。本产品只能在购买地所在国家或地区享受售后服务及维保方案。

关于本手册

本手册仅作为相关产品的指导说明，可能与实际产品存在差异，请以实物为准。因产品版本升级或其他需要，海是智能可能对本手册进行更新，如您需要最新版手册，请您登录海是智能官网查阅（***http://www.HIOTSE.com***）。

海是智能建议您在专业人员的指导下使用本手册。

商标声明

- HIOTSE 海是智能 为海是智能的注册商标。

6. 本手册涉及的其他商标由其所有人各自拥有。

责任声明

7. 在法律允许的最大范围内，本手册以及所描述的产品（包含其硬件、软件、固件等）均“按照现状”提供，可能存在瑕疵或错误。海是智能不提供任何形式的明示或默示保证，包括但不限于适销性、质量满意度、适合特定目的等保证；亦不对使用本手册或使用海是智能产品导致的任何特殊、附带、偶然或间接的损害进行赔偿，包括但不限于商业利润损失、系统故障、数据或文档丢失产生的损失。

8. 您知悉互联网的开放性特点，您将产品接入互联网可能存在网络攻击、黑客攻击、病毒感染等风险，海是智能不对因此造成的产品工作异常、信息泄露等问题承担责任，但海是智能将及时为您提供产品相关技术支持。

9. 使用本产品时，请您严格遵循适用的法律法规，避免侵犯第三方权利，包括但不限于公开权、知识产权、数据权利或其他隐私权。您亦不得将本产品用于大规模杀伤性武器、生化武器、核爆炸或任何不安全的核能利用或侵犯人权的用途。

10.　如本手册内容与适用的法律相冲突，则以法律规定为准。

前言

本节内容的目的是确保用户通过本手册能够正确使用产品，以避免操作中的危险或财产损失。在使用此产品之前，请认真阅读产品手册并妥善保存以备日后参考。

符号约定

对于文档中出现的符号，说明如下所示。

符号	说明
说明	说明类文字，表示对正文的补充和解释。
注意	注意类文字，表示提醒用户一些重要的操作或者防范潜在的伤害和财产损失危险。如果不加避免，有可能造成伤害事故、设备损坏或业务中断。
危险	危险类文字，表示有高度潜在风险，如果不加避免，有可能造成人员伤亡的重大危险。

安全使用注意事项

电气安全

11. 设备安装使用过程中，必须严格遵守国家和使用地区的各项电气安全规定。

12. 根据国家相关标准，对弱电设备供电时，要求供电电流不超过 8 A 并且功率不超过 100 W，
防止发生安全事故。

13. 更换保险丝时，请使用正确的型号，否则有电击或着火危险。

14. 请使用正规厂家提供的电源适配器，电源适配器具体要求请参见产品参数表。

15. 请不要将多个设备连接至同一电源适配器（超过适配器负载量，可能会产生过多热量或导致火灾）。

16. 在强雷暴地区或高感应电压地带（如高压变电站等），必须采取额外加装大功率防雷设备以及安装避雷 等措施。

17. 在接线、拆装等操作时，请断开设备电源，切勿带电操作。

电池安全

18. 本设备不适合在儿童可能会出现的场所使用。
19. 警告：如果使用错误型号的电池可能导致爆炸危险。
20. 使用错误型号的电池更换（例如某些类型的锂电池）可能导致安全防护失效。
21. 请勿将电池投入火中或加热炉中，不要挤压、折弯或切割电池，可能会造成爆炸。
22. 请勿将电池放置在极高温度环境中，可能导致电池爆炸或泄漏可燃液体或气体。
23. 请勿将电池放置在极低气压环境中，可能导致电池爆炸或泄漏可燃液体或气体。
24. 废弃电池对环境会造成污染，请按照说明处置使用完的电池。

防火

设备上不要放置裸露的火焰源，如点燃的蜡烛。

防烫

25. 为了避免热量积蓄，请保持设备周边通风流畅。
26. 请勿直接触碰设备散热部件，以免烫伤。

机械安全

27. 请严格参照本指导书中的安装方法进行设备安装。
28. 为防止伤害，必须将设备牢固地固定于墙壁或天花板上。

补光灯安全

29. 部分产品补光灯可能有视网膜蓝光危害，补光灯工作时不得注视，可能伤害眼睛。
30. 在补光灯正常工作时，请勿近距离注视光源。
31. 在没有适当保护的前提下，安装或进行设备维护时，需处在安全距离范围外或者光源不能直接照射的区域，方可点亮光源。

设备保养与维护

32. 设备的串口仅用于调试，禁止用户使用。
33. 若设备带有透明罩，请勿直接触摸透明罩，避免酸性汗迹可能会腐蚀透明罩的表面镀层，影响图像质量。
34. 清洁透明罩时，请使用足够柔软的干布擦拭内外表面，避免硬物刮伤透明罩；切勿使用碱性清洁剂洗涤。
35. 清洁镜头时，请使用干燥的软棉布或镜头擦拭纸擦拭表面，避免硬物刮伤镜头。
36. 如果设备出现冒烟、异味或杂音等现象，请立即断开设备电源，及时与经销商或服务中心联系。

37. 如果设备工作不正常，请联系购买设备的商店或最近的服务中心，不要以任何方式拆卸或修改设备。（对未经认可的修改或维修导致的问题，本公司不承担任何责任）。

38. 请妥善保存设备的全部原包装材料，以便出现问题时，使用包装材料将设备包装好，寄到代理商或返回厂家处理。非原包装材料导致的运输途中的意外损坏，本公司不承担任何责任。

使用环境

39. 请避免物体摔落到设备上或大力振动设备，使设备远离存在磁场干扰的地点。避免将设备安装到表面振动或容易受到冲击的地方（忽视此项可能会损坏设备）。

40. 请勿在极热、极冷、多尘、有腐蚀性、高盐碱或者高湿度的环境下使用产品，具体温、湿度要求参见产品的参数表。

41. 请勿将镜头对准强光源，如太阳、白炽灯等，否则会造成镜头的损坏。

42. 请勿将室内使用的设备暴露在可能被雨淋到或潮湿的地方。

43. 设备需存放于干燥无腐蚀性气体的环境，避免将设备存放在阳光直射、通风不良或热源附近（如加热器、暖气）等地点，忽视此项可能会导致火灾危险。

系统安全

44. 设备接入互联网可能面临网络安全问题，请您加强个人信息及数据安全的保护。当您发现设备可能存在网络安全隐患时，请及时与我们联系。

45. 请您理解，您有责任合理配置所有的密码及其他相关产品安全设置，并妥善保管好您的用户名和密码。

安装须知

46. 对安装和维修人员的素质要求 具有从事视频监控系统安装、维修的资格证书或经历，并有从事相关工作（如高空作业等）的资格，此外还必须具有如下的知识和操作技能。

- 具有视频监控系统及组成部分的基础知识和安装技能。
- 具有低压布线和低压电子线路接线的基础知识和操作技能。
- 具备基本网络安全知识及技能，并能够读懂本手册内容。

47. 对升降设备的要求。

- 使用适合安装地点和设备安装方式的安全升降设备。
- 升降设备具有达到安装位置的足够的举升高度。
- 升降设备具有良好的安全性能。

目 录

第 1 章 产品简介 1

1) 产品介绍 1

2) 特色功能 1

第 2 章 激活设备 2

- 通过 SADP 软件激活 2
- 通过浏览器激活 3
- 登录 4
  - 浏览器登录 4
  - 插件安装说明 4
  - 重置密码 5

第 3 章 预览 6

- 预览参数 6
  - 开启及关闭预览 6
  - 画面分割 6
  - 调整预览画面比例 6
  - 选择预览码流 7
  - 选择播放插件 7
  - 像素计算器 7
  - 电子放大 8
  - 快速配置 8
  - PTZ 控制 8
  - 辅助聚焦 9
  - 镜头初始化 10
- 设置传输参数 10

第 4 章 PTZ 12

- PTZ 控制 12
  - 启用比例变倍 13
- 配置预置点 13
- 设置巡航扫描 13
  - 配置一键巡航 14
- 设置隐私遮蔽 15
- 设置定时任务 15
- 设置守望 16
  - 设置一键守望 16
- 设置掉电记忆 16

第 5 章 录像和抓图 18

- 存储路径 18
  - 设置存储卡 18
  - 配置 FTP 20
  - 配置网络硬盘 21
  - 配置云存储 22
- 录像配置 22
  - 自动录像 23
  - 手动录像 24
  - 回放与下载录像 24
- 抓图配置 25
  - 自动抓图 25
  - 手动抓图 26
  - 查看与下载图片 26

第 6 章 VOCs 气体检测 27

第 7 章 事件和报警 31

- 普通事件 31
  - 配置移动侦测 31
  - 配置遮挡报警 34
  - 配置报警输入 35
  - 配置异常报警 36
- Smart 事件配置 36
  - 配置音频异常侦测 36

第 8 章 视音频及图像参数 38

- 设置视频参数 38
  - 码流类型 38
  - 视频类型 38
  - 分辨率 39
  - 码率类型和码率上限 39
  - 图像质量 39
  - 视频帧率 39
  - 视频编码 39
  - 码流平滑 41
- 设置音频参数 41
  - 音频编码 41
  - 音频输入 41
  - 环境噪声过滤 42
- 开启语音对讲 42
- ROI 42
  - 配置固定区域 ROI 43
- 配置区域裁剪 43
- 设置视频遮盖 44
- 叠加码流信息 44

- 设置图像显示参数 45
  - 场景模式 45
  - 图像调节 45

8.8.3 曝光 45

8.8.4 聚焦 46

- 日夜转换 47
- 补光灯参数 48
- 背光补偿 48
- 宽动态 49
- 强光抑制 49
- 白平衡 50
- 数字降噪 50

8.8.12 透雾 51

8.8.13 电子防抖 52

8.8.14 镜像 52

- 镜头畸变矫正 52
- 视频制式 52
- 本地输出 52
- 配置图像参数切换 53

- OSD 参数 53
- 配置图片叠加 54

第 9 章 网络配置 55

- TCP/IP 参数 55
  - 多播设置 56
- 网络服务 56
- 端口参数 57

- 设置端口映射 58
  - 设置自动端口映射 58
  - 设置手动端口映射 59
  - 设置路由器端口映射 59
- 设置 SNMP 参数 59
- 设置 DDNS 域名访问 60
- 设置 PPPoE 61

9.8 设置 28181 61

- 设置 ISUP 62
- 配置开放型网络视频接口 62
- 设置视图库 63
- 配置报警服务器 63
- TCP 加速 63
- 流量整形 64
- SRTP 64

第 10 章 计划和联动配置 65

- 布防时间配置 65
- 联动配置 65
  - 联动录像 66
  - 联动上传中心 66
  - 联动 FTP/NAS/SD 卡 66
  - 联动 Email 66
  - 联动报警输出 67
  - 配置闪光报警灯输出 69
  - 配置声音报警输出 69

第 11 章 系统和安全参数 70

- 查看设备信息 70

- 重启设备 70
- 恢复设备参数 70
- 导入/导出配置参数 70
- 导出诊断信息 71
- 升级设备 71
- 查询和导出日志 71
- 查看开源码授权信息 72
- 设置时间 72
  - 设置 NTP 校时 72
  - 手动校时 72
  - 设置夏令时 73

11.10 设置 RS-485 参数 73

11.11 设置 RS-232 参数 73

- 功耗模式切换 74
- 安全配置 74
  - 安全使用建议 75
  - 设置认证方式 75
  - 设置 IP 地址过滤 76
  - 设置 MAC 地址过滤 76
  - SSH 77
  - 开启账户锁定 77
  - 控件超时配置 77
  - 证书管理 77
  - 设置 HTTPS 80
  - 设置 QoS 80

11.13.11 设置 IEEE 802.1X 81

- SRTP 81

- 安全审计日志.....81
- 管理设备用户.....83
- 设置用户账户和权限.....83
- 密码强度提示.....84
- 查看在线用户.....84
- 设置 Web 同时登录数.....84

第 1 章 产品简介

- 产品介绍

网络摄像机是集成了视音频采集、智能编码压缩及网络传输等多种功能的数字监控产品。采用嵌入式操作系统和高性能硬件处理平台，具有较高稳定性和可靠性，可满足多样化行业需求。

- 特色功能

从产品特色功能介绍网络摄像机，您可更快地了解及熟悉网络摄像机。

系统功能

48. 支持预览界面快速配置图像和音视频等参数。
49. 可通过系统管理员（admin），管理多个不同的用户，并对每个用户配置不同的权限。
50. 支持预览时的即时抓图及录像，也可安装存储卡或者配置网络存储盘后，配置录像及抓图的计划，实现计划录像及抓图。

VOCs 气体检测功能

通过预置点实现多场景 VOCs 气体检测。可定位泄漏源，实时显示泄漏气体轨迹，通过智能报警功能实现对危化品生产与存储区域 7 × 24 h 智能巡检，并可在预览画面中对气体区域叠加伪彩。

事件侦测功能

支持移动侦测、遮挡报警、异常报警、闪光报警灯和声音报警输出等普通事件。

第 2 章 激活设备

网络访问中，为了保护个人账户安全和隐私，提高监控的安全性，首次登录时，需设置 admin 用户密码激活设备。

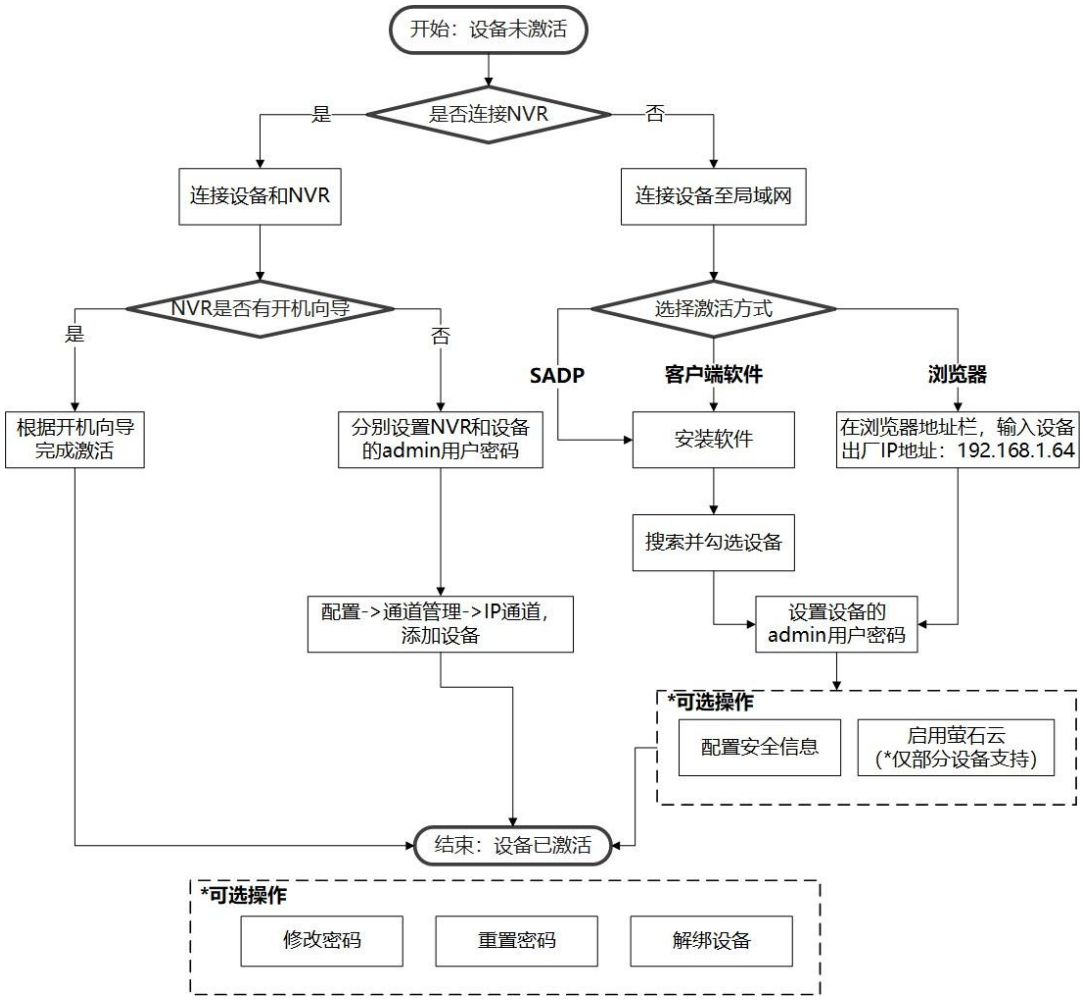


图 2-1 激活设备流程图

• 通过 SADP 软件激活

通过计算机上的 SADP 软件，搜索并激活与计算机处于同一局域网的设备。

前提条件

可通过如网站获取 SADP 软件，完成安装。

操作步骤

1. 将设备连接网络，确保设备与计算机处于同一局域网。

2. 运行 SADP 软件，搜索局域网内的在线设备。

3. 选择列表中需要激活，且**激活状态**为**未激活**的设备。

4. 在**激活设备**处设置设备激活密码。

注意

- 为保护您的个人隐私和企业数据，避免设备产品的网络安全问题，建议您设置符合安全规范的高强度密码。
- 为了提高产品网络使用的安全性，设置的密码长度需达到 8~16 位，至少由数字、小写字母、大写字母和特殊字符中的 2 种或 2 种以上类型组合而成，且密码中不能包含用户名。

5. 单击*确定*。

设备**激活状态**更新为**已激活**。

6. **可选操作**: 选择已激活的设备，在**修改网络参数**处设置设备的 IP 地址、子网掩码、网关等信息，输入激活密码，单击*修改*保存参数。

• 通过浏览器激活

通过浏览器访问设备，激活设备。

操作步骤

1. 将设备连接网络，确保设备与计算机处于同一局域网。

2. 修改计算机 IP 地址和设备 IP 地址在同一网段。

说明

设备出厂 IP 地址：192.168.1.64，计算机 IP 地址可以设置为 192.168.1.2~192.168.1.253 之间的任意一个 IP 地址（除 192.168.1.64 之外），例如：将计算机 IP 地址设置为 192.168.1.100。

3. 在浏览器中输入 *192.168.1.64*，显示激活界面。

4. 在**激活设备**处设置设备激活密码。

注意

- 为保护您的个人隐私和企业数据，避免设备产品的网络安全问题，建议您设置符合安全规范的高强度密码。
- 为了提高设备网络使用的安全性，设置的密码长度需达到 8~16 位，至少由数字、小写字母、大写字母和特殊字符中的 2 种或 2 种以上类型组合而成，且密码中不能包含用户名和用户名的倒写。

5. 单击*确定*。

6. 输入激活密码，登录设备。

7. 可选操作: 进入 *配置* → *网络* → *基本配置* → *TCP/IP* ， 修改设备 IP 地址和当前网络处于同一网段。

• 登录

• 浏览器登录

通过浏览器登录设备，插件安装的方法。

操作步骤

1. 在浏览器中输入设备的 IP 地址，弹出登录画面。
2. 设备提示安装浏览器插件。根据界面提示，安装插件。
3. 再次打开浏览器，输入设备的 IP 地址。
4. 输入用户名和密码，单击*登录*。
5. 可选操作: 单击*注销*，安全退出登录。

• 插件安装说明

通过不同的操作系统、浏览器登录设备时，可能会有不同的功能显示，为了保证功能正常显示和使用时，请根据使用情况安装插件或设置参数，请以实际设备界面为准。

操作系统	浏览器版本	安装插件操作
Windows	11 IE 11 及以上版本 12 Google Chrome 56 及以下版本 13 Mozilla Firefox 51 及以下版本	请根据系统提示完成插件的安装。
	1. Google Chrome 57 及以上版本 **2.** Mozilla Firefox 52 及以上版本	单击预览页面，单击 插件下载 下载并安装插件，可以获得高质量的显示并完成设备功能操作。

操作系统	浏览器版本	安装插件操作
其它	IE 11 及以上版本	请根据系统提示完成插件的安装。
	1. Google Chrome 57 及以上版本 **2.** Mozilla Firefox 52 及以上版本 **3.** Mac Safari 12 及以上版本	为了正常预览，可进入 ***配置 → 网络 → 高级配置 → 网络服务***， 开启 WebSocket 或 WebSockets，开启后一些功能 的显示和操作会受到限制，例 如回放和图片不可用等，请以 实际设备界面为准。

- **重置密码**

通过配置账号安全信息，当 admin 用户忘记密码时，单击登录界面的忘记密码，可重置密码。

您可通过安全问题或安全邮箱，重置 admin 用户的密码。

说明

重置 admin 用户密码时，请确保设备和计算机的 IP 在同一局域网网段。

安全问题

在激活时进行账号安全设置，或通过 ***配置 → 系统 → 用户管理***，单击***账号安全设置***，选择安全问题，并填写问题的答案。

安全邮箱

在激活时进行账号安全设置，或通过 ***配置 → 系统 → 用户管理***，单击***账号安全设置***，选择安全邮箱，并填写安全邮箱信息。

第 3 章 预览

介绍设备预览时，预览参数、功能图标参数、传输参数等调节。

• 预览参数

介绍设备在预览图像时进行的一些参数调节。

说明

多通道设备请先选择通道后设置其预览参数。

• 开启及关闭预览

选择*预览*。单击 开启全部通道预览，单击 关闭全部通道预览。

• 画面分割

调节预览界面布局。

- 表示显示 1 × 1 的画面分割。
- 表示显示 2 × 2 的画面分割。
- 表示显示 1 × 2 的画面分割。
- 表示显示 2 × 1 的画面分割。

说明

画面分割仅多通道设备支持，请以实际设备为准。

• 调整预览画面比例

用于调整预览画面的显示比例。

操作步骤

1. 单击*预览*。

2. 单击 ，选择显示比例。

- 预览画面以 4 比 3 的比例显示图像。
- 预览画面以 16 比 9 的比例显示。
- 预览画面以原始尺寸显示。

- 预览画面自适应显示。
- 预览画面以原始比例显示。

• 选择预览码流

选择预览时实况画面的码流。

主码流

实况画面的分辨率、码率和图像质量较高，建议可在网络带宽充足时选择。

子码流

实况画面的分辨率、码率和图像质量较低，建议可在网络带宽不足时选择，保证实况画面的流畅性。

第三码流、第四码流、第五码流

请根据实际情况选择预览码流。

• 选择播放插件

当浏览器不能正常进行预览时，您可以根据浏览器选择不同的播放插件进行安装并预览。

操作步骤

1. 单击*预览*。

2. 单击 选择播放插件。

- 当您使用 IE 核心浏览器，可选择插件为 Webcomponents 和 QuickTime。
- 当您使用非 IE 核心浏览器，可选择插件为 Webcomponents。

• 像素计算器

用于快速测量绘制区域高度和宽度的像素值。

操作步骤

说明

像素计算器功能视型号而定，请以实际设备为准。

1. 单击 ，开启像素计器功能。

2. 在实况画面中绘制 1 个需要计算像素的区域框。

显示该区域框宽度和高度的像素值。

- **电子放大**

若需要查看画面某一区域的细节时，可使用电子放大功能。

操作步骤

说明

电子放大功能视型号而定，请以实际设备为准。

1. 单击 ，开启电子放大功能。
2. 在实况画面，左上向右下拖拽鼠标，框选需要放大的区域。
3. 单击实况画面中任一处，即可恢复到原始画面。

- **快速配置**

用于在预览时快速配置云台参数、通用参数和智能参数。

操作步骤

10单击 ，开启快速配置功能。

11设置云台参数、通用参数、和智能参数。其中通用参数包括显示设置、OSD 设置和视音频参数设置。

11.1 云台参数设置请参见 *PTZ 控制* 。

11.2 显示参数设置请参见 *设置图像显示参数* 。

11.3 OSD 参数设置请参见 *OSD 参数* 。

11.4 视音频参数设置请参见 *视音频及图像参数* 。

说明

快速配置功能视型号而定，请以实际设备界面为准。

- **PTZ 控制**

通过 PTZ 可以远程控制监控设备，实时调整监控画面图像。

云台控制方向

长按云台控制方向键可控制水平、垂直等方向转动。

调焦

51. 按住 ，镜头拉近，景物放大。

52. 按住 ，镜头拉远，景物变小。

聚焦

53. 按住 ，近处的物体变得清楚，远处的物体逐渐变得模糊。

54. 按住 ，远处的物体变得清晰，近处的物体逐渐变得模糊。

速度调节

-

滑动进度条，调节变倍、聚焦和光圈的速度。

光圈

55. 按住 ，可增大光圈。

56. 按住 ，可减小光圈。

- **辅助聚焦**

适用于配备电动镜头的设备，在设备聚焦不清楚的情况下使用辅助聚焦，可使设备呈现的图像变清楚。

对于支持 ABF 的设备可配合自动背焦调节来进行聚焦，调整好镜头视场，先进行粗聚焦，再按下设备背部 ABF 调节按钮，设备则可通过自动背焦调节聚集至最清晰位置。

单击 ，实现镜头自动完成聚焦。

说明

57. 若辅助聚焦出现难以聚焦清楚的情况，可参见 *镜头初始化* 设置后，再次使用辅助聚焦使图像变清楚。

58. 若辅助聚焦出现难以聚焦清楚的情况，可使用手动调焦和聚焦，使图像变清楚。

- **镜头初始化**

适用于配备电动镜头的设备，在设备变倍、聚焦时间过长导致图像不清楚的情况下，可使用镜头初始化，将镜头参数重置。

单击 ，实现设备镜头参数的 1 次重置。

• 设置传输参数

视频预览时，受网络环境的影响，可能出现设备预览画面不稳定。在不同的网络环境下，通过设置传输协议和播放参数，可缓解该问题。

操作步骤

1. 进入 *配置 → 本地*，选择播放参数。

2. 设置影响视频传输的参数。

传输协议

TCP

适用于比较稳定的网络环境，可以保证视频的完整性。

UDP

适用于对视频流畅性要求不高且自身网络环境不稳定的情况。

MULTICAST

适用于客户端较多且选择前需要配置组播地址。

说明

选择 MULTICAST 前，请参见 *TCP/IP 参数* 配置多播地址。

HTTP

适用于第三方客户端向设备取流的情况。

播放参数

最短延时

设备优先保证视频预览的实时性，但可能会影响视频的流畅性。

均衡

设备兼顾视频预览的实时性和流畅性。

流畅性好

设备优先保证视频预览的流畅性。如果网络环境差，设置为流畅性好也不能保证预览画面流畅。

自定义

网络状况不佳时，可降低缓存帧率，以提升视频流畅性。降低帧率可能导致规则信息丢失。

3. 单击*保存*。

第 4 章 PTZ

PTZ 是 Pan/Tilt/Zoom 的简写，通过 PTZ 可实现设备全方位（上、下、左、右）移动及镜头变倍、变焦等操作。

说明

PTZ 功能视型号而定，请以设备实际支持为准。

• PTZ 控制

通过 PTZ 可以远程控制监控设备，实时调整监控画面图像。

云台控制方向

长按云台控制方向键可控制水平、垂直等方向转动。

调焦

59. 按住 ，镜头拉近，景物放大。

60. 按住 ，镜头拉远，景物变小。

聚焦

61. 按住 ，近处的物体变得清楚，远处的物体逐渐变得模糊。

62. 按住 ，远处的物体变得清晰，近处的物体逐渐变得模糊。

速度调节

-

滑动进度条，调节变倍、聚焦和光圈的速度。

光圈

63. 按住 ，可增大光圈。

64. 按住 ，可减小光圈。

- **启用比例变倍**

勾选表示打开比例变倍功能。即在键控状态下设备自动随着变倍倍率的变化而变化。当变倍倍率增大时，设备移动速度自动变慢；当变倍倍率减少时，设备移动速度自动加快。

• 配置预置点

预置点可用于记录设备画面位置。通过预置点的配置和调用，可实现设备自动移动到所设置的位置。

操作步骤

1. 单击*预览*中的 ，单击 。

2. 控制云台方向键，将设备转到所需位置。

3. 选择一个待配置的预置点，单击 完成 1 个预置点的设置。

说明

特殊预置点不允许设置，只能调用。

4. 重复上述步骤，可设置多个预置点。

单击 调用预置点。

单击 清除预置点。

说明

如需删除所设置的所有预置点，可进入 *配置* → *PTZ* → *配置清除*，单击*清除所有预置点*，单击*保存*。

• 设置巡航扫描

巡航扫描可实现设备在多个预先设置的预置点间自动循环运动。

前提条件

请配置好 2 个或 2 个以上的预置点，预置点设置方法请参见 *配置预置点* 。

操作步骤

1. 单击*预览*的 。

2. 单击 。

3. 单击选择 1 条待配置的巡航路径。

4. 单击 。

5. 单击 ，根据需要，添加预置点。

预置点

选择已配置的预置点。

速度

设置预置点间的运动速度。

时间

设置需要在该预置点停留的时间。

单击 ×删除巡航路径中的预置点。

单击 ↓ ↑调节巡航路径中的预置点顺序。

说明

1 条巡航路径中至少需要添加 2 个预置点，最多允许添加 32 个预置点。

6. 单击*确定*，完成一条巡航路径的设置。
7. 重复上述步骤可设置多条巡航路径。
8. 单击 ▶，运行巡航扫描。

单击 ■停止巡航扫描。

单击 ×删除巡航扫描。

单击 ⚙重置巡航路径信息，操作方法与设置巡航路径一致。

说明

若需删除所设置的所有巡航路径，进入 *配置* → *PTZ* → *配置清除*，勾选**清除所有巡航路径**，单击*保存*。

• 配置一键巡航

用于将已设置好的几个预置点自动添加到一条巡航路径中，执行巡航操作。

操作步骤

1. 在 1~32 号预置点之间，提前设置 2 个或 2 个以上预置点，预置点设置方法请参见 *配置预置点*。

   设备自动将预置点添加到巡航路径 8 中。
2. 开启一键巡航。
   - 单击 。
   - 调用巡航路径 8。
   - 选择并调用 45 号预置点。

• 设置隐私遮蔽

用于遮盖用户不希望看到的场景，保护个人隐私。无论设备进行任何方式的移动及变化，遮盖场景始终不可见。

操作步骤

9 单击 *配置 → PTZ → 隐私遮蔽* 。

10勾选*启用隐私遮蔽*。

11单击*绘制区域*，在实况画面中，单击鼠标左键并拖动鼠标，绘制出 1 个封闭的区域后松开鼠标左键。

拖动区域框的锚点 调整区域框的大小。

单击*停止绘制* 停止绘制。

单击*清除全部* 清除画面中绘制的所有区域。

12单击*停止绘制*。

13单击*保存*。

• 设置定时任务

设置设备在某段时间内执行特定动作，若当前动作关联了智能类型，则设备在运行该动作的同时，执行对应的智能功能。

前提条件

设备已配置所选动作，且所选动作下已配置并开启了智能类型。例如：当动作选择巡航扫描，智能类型选择烟火检测时，需保证设备配置了巡航路径，且巡航路径下配置并开启了烟火检测，动作和智能功能才均可生效。

操作步骤

1. 进入 *配置 → PTZ* 选择*定时任务*。

2. 勾选 *启用定时任务* 。

3. 选择定时任务类型并设置定时任务的时间段。其中定时任务的时间段设置请参见 *布防时间配置* 。

4. 单击选中所需时间段，修改动作路径编号并新增**智能类型**。**智能类型**选择*无*时，不运行智 能功能。

5. 重复上述步骤，可设置多个不同定时任务。

6. 设置**任务恢复时间**。

任务恢复时间

设备的定时任务优先级低于手动操作任务，因此手动操作会打断正在进行中的定时任务。当手动操作结束后，设备经过设置的任务恢复时间，将继续执行打断前的定时任务。

7. 设置完毕后，单击*保存*。

说明

若需清除设置的所有定时任务，进入 *配置* → *PTZ* → *配置清除*，勾选**清除所有定时任务**，单击*保存*。

• 设置守望

用于设置在守望等待时间内没有收到控制信号时，设备需要执行的某项动作（如预置点、花样扫描等）或者回到某个位置。

前提条件

设置守望之前，需先设置好所需的守望模式，如守望巡航扫描，请先设置好巡航扫描，巡航的具体设置请参见 *设置巡航扫描*。

操作步骤

1. 单击 *配置* → *PTZ* → *守望*，勾选*开启守望*。
2. 设置守望等待时间，用于当设备没有接收到控制信号的情况下，需要等待的时间。
3. 根据实际需求，选择守望模式。
4. 单击*保存*。

• 设置一键守望

用于快速开启守望功能。

操作步骤

1. 参见 *设置守望* 设置守望功能。
2. 开启一键守望。
- 单击 。
- 调用 32 号预置点。

• 设置掉电记忆

设备重新上电后可恢复至断电前的最新记忆点位置。

操作步骤

1. 进入 *配置* → *PTZ* → *基本配置*。
2. 选择掉电记忆模式，即该位置成为记忆点需要停留的最短时间。

3. 单击*保存*。

第 5 章 录像和抓图

介绍自动或手动的方式进行视频录像或图片抓取，可实现录像或抓图文件的回放、下载等操作。

• 存储路径

介绍设备几种常用的存储路径的设置方法。

• 设置存储卡

存储到 MicroSD 卡时，需要先进行 MicroSD 卡的安装及格式化。当 MicroSD 卡状态正常后，可将录像或抓图文件存储到 MicroSD 卡上。

前提条件

设备插入 1 张未加密的 MicroSD 卡或全新的 MicroSD 卡。MicroSD 卡安装操作请参见设备的*快速入门指南*。

操作步骤

1. 进入 *配置* → *存储* → *存储管理* → *硬盘管理* 。

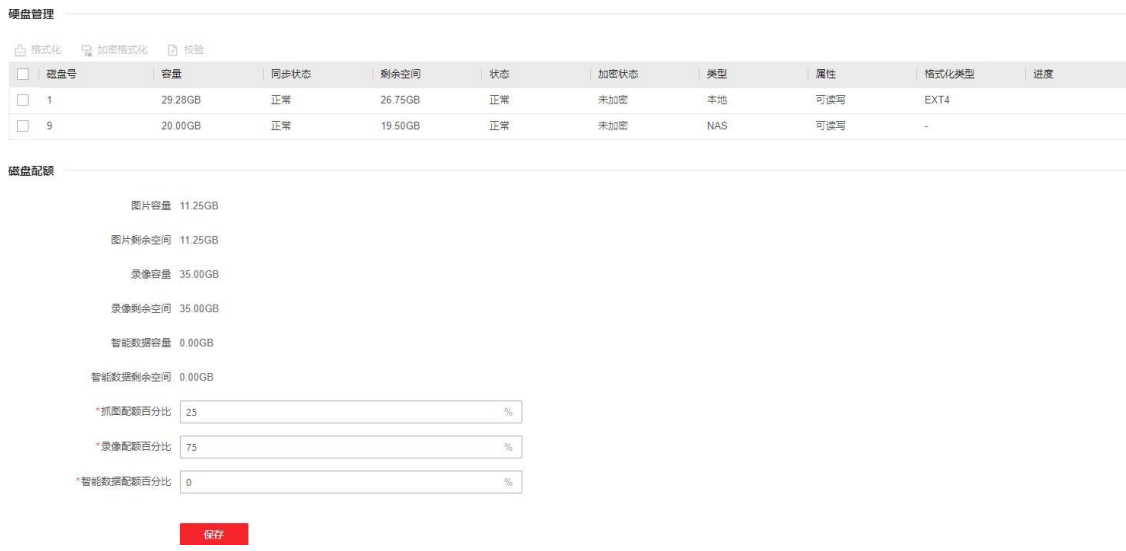


图 5-1 硬盘管理

2. 可选操作: 配置磁盘配额，请根据需求设置不同类型数据和文件的存储百分比。

3. 格式化 MicroSD 卡，并根据需求选择是否对卡进行加密。

格式化 勾选检测到的 MicroSD 卡，单击*格式化*。

格式化成功后，**状态**显示为*正常*。此时，MicroSD 卡可进行正常存储。

加密格式化 MicroSD 卡格式化后通过设置加密密码进行加密存储。支持对所有类型的 MicroSD 卡进行加密存储。

勾选检测到的 MicroSD 卡，单击*加密格式化*并设置**加密密码**。

加密格式化成功后，**状态**显示为*已加密*。此时，MicroSD 卡可进行加密存储。

说明

1. 加密密码不支持修改，只能重新加密格式化，建议妥善保管。
2. 已加密的 MicroSD 卡，单击*格式化*可切换为不加密状态。格式化操作会导致存储卡数据丢失，请先备份数据。

图 5-2 加密格式化

4. 单击*保存*。

检测 MicroSD 卡状态

对海是智能 MicroSD 卡状态进行检测。当 MicroSD 卡出现异常时，能够及时得到状态变化的反馈。

前提条件

请在设备中安装 MicroSD 卡。

操作步骤

1. *配置 → 存储 → 存储管理 → SD 卡状态检测* 。

2. 设置布防时间和联动方式，详细请参见 *布防时间配置* 和 *联动配置* 。

3. 单击*保存*。

单击*健康监测*，查看 MicroSD 卡预计剩余寿命和健康状态。

4. **可选操作**：单击*读写锁定*，可设置 MicroSD 卡的读写权限。

- 将锁定开关选择为**开启**。
- 设置锁定密码。
- 单击*保存*。

说明

1. 读写锁定仅限 admin 用户登录设置。

2. 锁定状态的 MicroSD 卡不可读写。

- **配置 FTP**

通过抓图或事件联动获取到图片，将图片上传到指定的 FTP 服务器上存储。

前提条件

请先获取 FTP 服务器地址。

操作步骤

- 单击 *配置 → 网络 → 高级配置 → FTP 设置* 。
- 设置 FTP 参数。

FTP 协议

可选择 FTP 和 SFTP。使用 SFTP 将通过加密的方式传输文件，相对更安全。

服务器地址和端口

表示 FTP 服务器地址和对应的端口。

用户名和密码

表示具备上传权限的用户名和密码。

如果匿名用户也具备上传权限，可勾选*匿名登录*，则设备通过匿名方式访问 FTP 服务器。

目录结构

表示文件在 FTP 服务器上的保存路径。

图片归档间隔

在 FTP 服务器上自动生成文件夹，将抓拍的图片以天为单位进行存档，方便后续检索。

如果图片归档间隔设置为 1 天，设备将以“年_月_日-年_月_日”为名称，每天生成 1 个文件夹。依此类推，如果图片归档间隔设置为 2 天，则设备每 2 天生成 1 个文件夹。

图片名

根据需求设置 FTP 抓图的图片名。选择默认时，抓拍的图片将以设备的 IP 地址为前缀。

说明

配置参数项视型号而定，请以实际设备为准。

- **可选操作**: 勾选*上传图片*，开启抓图上传 FTP 的功能。
- **可选操作**: 勾选*断网续传*。

断网续传

当设备的网络出现异常的时候，将数据自动缓存至设备 SD 卡，待网络恢复正常，设备将上传断网缓存的数据。

- **可选操作**: 单击*测试*，查看设置的 FTP 服务器是否可用。
- 单击*保存*。

• 配置网络硬盘

将网络中的服务器作为网络硬盘，存储录像或抓图文件。

前提条件

请先获取网络硬盘服务器地址。

操作步骤

9 进入 *配置* → *存储* → *存储管理* → *网络硬盘* 。

10 设置服务器地址和文件路径。**服务器地址**

网络硬盘的 IP 地址。

文件路径

网络硬盘内的文件保存路径。

11 设置挂载方式，可选 **NFS** 和 **SMB/CIFS**。当挂载方式选择为 **SMB/CIFS** 时，需设置认证的用户名和密码。

12 单击*测试*，查看设置的网络硬盘是否可用。

13 单击*保存*。

• 配置云存储

用于将抓拍到的图片和信息上传至云端，平台可直接向云端请求图片，可更快速的进行图片查看及分析，该功能请以实际设备为准。

操作步骤

注意

云存储开启时，图片优先存储在云存储服务器上。

1. *配置* → *存储* → *存储管理* → *云存储* 。

2. 勾选*启用云存储*。

3. 设置基本参数。

协议版本	云存储服务器的协议版本。
接入服务器 IP	云存储服务器的地址，支持 IPv4 地址。
接入服务器 Port	云存储服务器的端口，缺省为 6011，不建议修改。
用户名和密码	云存储服务器的用户名和密码。
密码确认	重复输入密码进行密码确认。
接入秘钥	登录云存储服务器的秘钥。
加密秘钥	对于存储到云存储服务器上的数据进行加密的秘钥。
图片池 ID	云存储服务器端存储设备上传图片的存储区域编号。需要确保图片池 ID 和云存储服务器的存储区域编号一致。

说明

用户名、**密码**、**密码确认**，**接入秘钥**和**加密秘钥**视云存储协议而定，请以实际的协议版本 为准。

4. 单击*测试*，测试所配置的云存储是否正确。

5. 单击*保存*。

• 录像配置

介绍通过自动或手动的方式配置录像，以及录像文件的回放和下载等操作。

• 自动录像

自动录像是指在设定的计划时间段内，自动执行录像任务。

前提条件

除定时录像类型外，其它的录像类型需在对应事件的联动方式中勾选联动录像，具体事件设置方法请参见 *事件和报警*。

操作步骤

1. 进入 *配置* → *存储* → *计划配置* → *录像计划* 。

2. 选择通道。

3. 勾选*启用*，开启录像计划。

4. 选择录像类型。

定时

表示根据计划录像配置的时间进行录像。

移动侦测

表示有物体移动时，可触发指定通道录像。

报警

表示报警输入产生报警时进行录像。

动测或报警

移动侦测或开关量报警任意一个发生时即可触发指定通道录像。

动测和报警

移动侦测和开关量报警同时发生时，才触发指定通道录像。

事件

有事件发生时，才触发指定通道录像。

说明

1. 移动侦测、动测或报警、动测和报警和事件录像都需要提前设置事件类型，具体请参见 *事件和报警* 。

2. 录像类型请以实际界面为准。

---

5. 单击*高级参数*，进行参数配置。

循环写入

若勾选*循环写入*，当存储空间满之后，将覆盖最早的录像文件；若不勾选，则存储空间 满后将停止录像。

预录时间

录像计划开始时间节点前的预先录像时间。

录像延时

录像计划结束时间节点后的延时录像时间。

码流类型

录像存储的码流类型。

说明

选择码流较高的码流时，预录时间或录像延时时间可能少于设定值 。

6. 录像计划时间配置请参见 *布防时间配置* 。
7. 单击*保存*。

• 手动录像

在实况画面中，手动控制按键实现录像。

操作步骤

1. **可选操作**：进入 *配置* → *本地* ，设置**录像文件打包大小**和**录像文件保存路径**，单击*保存*。
2. 在图像附近，录像操作如下。

单击 开启录像。

单击 停止录像。

• 回放与下载录像

用于查询、回放和下载已存储的录像。

操作步骤

1. 单击*回放*。
2. 选择通道号。
3. 设置搜索条件，单击*查找*。

符合条件的录像文件将显示在时间轴上。

4. 单击 ，开始回放录像文件。
   - 单击 ，开始对录像文件进行剪辑，再次单击该按钮，停止剪辑。
   - 单击 ，可以全屏回放录像文件，隐藏菜单信息，按 *ESC* 退出全屏。

说明

回放时剪辑的录像文件有默认保存路径，可进入 *配置* → *本地* ，选择**回放剪辑保存路径**，更改保存路径。

5. 单击 ，选择需要下载的文件，单击 *下载*。

说明

回放时下载的录像文件有默认保存路径，可进入 *配置* → *本地* ，选择**回放下载保存路径**，更改保存路径。

电子放大

若需要查看画面某一区域的细节时，可使用电子放大功能。

操作步骤

说明

电子放大功能视型号而定，请以实际设备为准。

1. 单击 ，开启电子放大功能。
2. 在实况画面，左上向右下拖拽鼠标，框选需要放大的区域。
3. 单击实况画面中任一处，即可恢复到原始画面。

• 抓图配置

介绍通过自动或手动的方式配置抓图，以及抓图文件的回放和下载等操作。

• 自动抓图

自动抓图是指在设定的计划时间段内，自动执行抓图任务。

操作步骤

1. 单击 *配置* → *存储* → *计划配置* → *抓图* → *抓图参数* 。
2. 选择通道号。
3. 设置*定时*抓图类型。
4. 设置抓图**图片格式、分辨率、图片质量、抓图时间间隔、抓图数量**。
5. 抓图计划时间请参见 *布防时间配置* 。
6. 单击*保存*。

• 手动抓图

手动控制按键实现抓图。

操作步骤

8 **可选操作**: 进入 *配置* → *本地* 。

9 设置**抓图文件格式**和抓图保存路径。

JPEG

压缩后的文件较小，便于网络传输。

BMP

压缩后的图像无失真，图质较好。

10单击*保存*。

11单击实况画面附近的 ，抓拍图片。

• 查看与下载图片

用于查询、回放和下载已存储的图片。

操作步骤

H 单击*图片*。

I 选择**通道号**。

J 设置搜索条件，单击*查找*。

符合条件的图片将显示在文件预览列表中。

K 单击 *下载*。

K.264 设置搜索条件。

K.265 选中需要查看的图片，单击 *下载*。

说明

可进入 *配置* → *本地* ，在**回放下载保存路径**中，单击*浏览*更改保存路径。

第 6 章 VOCs 气体检测

通过预置点实现多场景 VOCs 气体检测。可定位泄漏源，实时显示泄漏气体轨迹，通过智能报警功能实现对危化品生产与存储区域 7 × 24 h 智能巡检，并可在预览画面中对气体区域叠加伪彩。

VOCs 气体检测功能配置的整体流程如下图。

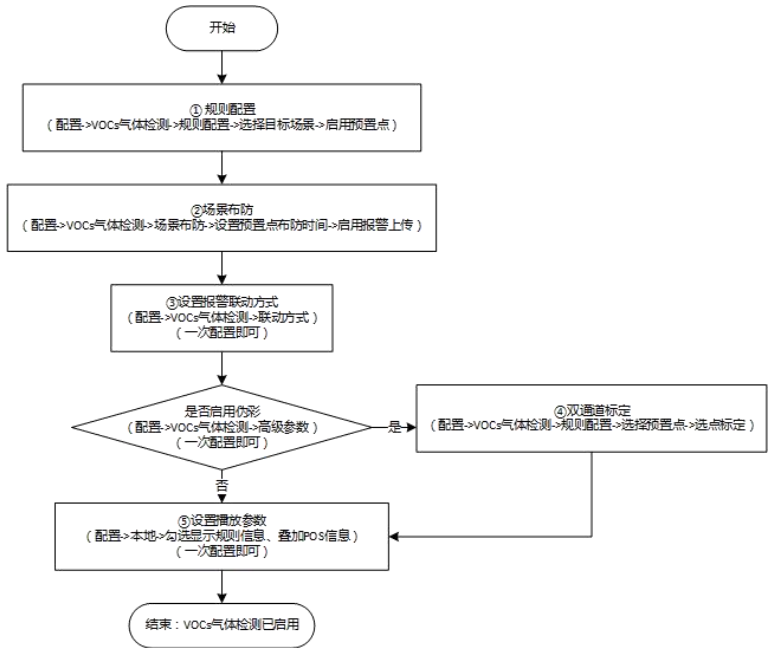


图 6-1 VOCs 气体检测配置流程

操作步骤

8 设置场景。

设置多个检测场景后，设备可在场景之间进行巡航检测，即场景布防。

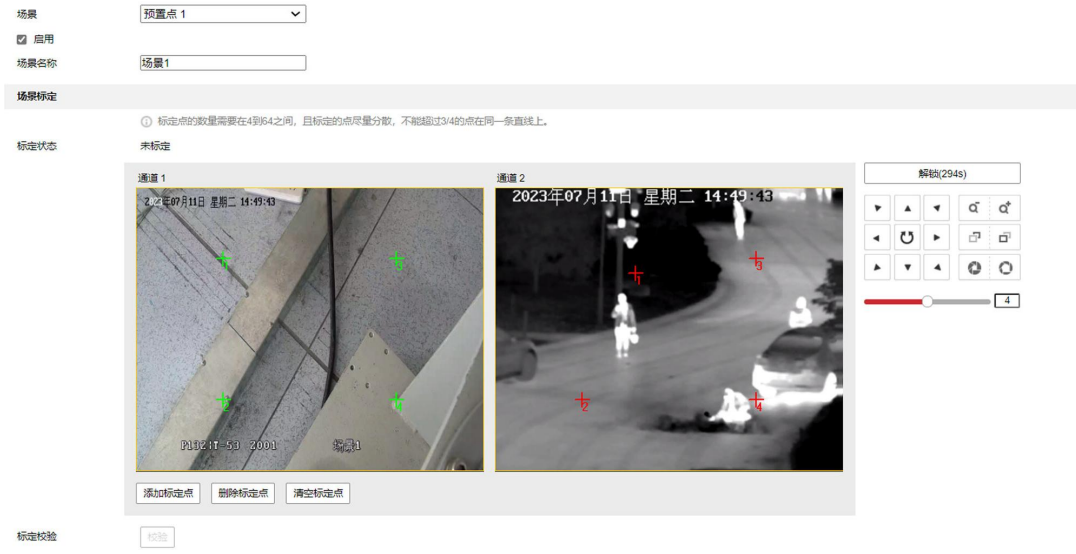


图 6-2 规则配置

8.1 进入 *配置* → *VOCs 气体检测* → *规则配置* 。

8.2 选择**场景**。

8.3 勾选*启用*。

8.4 设置**场景名称**。

8.5 通过云台控制键调整画面至目标场景。

8.6 单击*保存场景*。

8.7 重复以上步骤设置其它场景。

9 标定场景：设备首次安装完成后，需要进行场景标定。通过标定建立通道 1 和通道 2 坐标的对应关系，可将气体区域叠加至可见光通道显示。

9.1 单击***添加标定点***，移动通道 1 中的标定点（绿色十字）至画面中的某一参照点，将通道
2 相同编号的标定点（红色十字）移至画面对应的参照点上。

9.2 **可选操作**：单击***删除标定点***，可删除选中的标定点；单击***清空标定点***，可删除所有已添加的标定点。

9.3 重复以上步骤，将新添加的标定点移至画面中不同的参照物，建议添加 4~64 个标定点，
且标定的点尽量分散，不能超过 3/4 的点在同一条直线上。标定添加完成后，单击***保存场景***开始标定。

标定状态显示为**已标定**，表示标定完成。

9.4 标定完成后，单击***校验***，在通道 2 的画面上选择 1 个参照点，验证通道 1 画面上的点是否在同一参照点上。

当通道 2 与通道 1 在同一参照点时，表示标定成功，此时可以确认设备端已接收到相应的坐标关系；若标定点在实际场景不准确，气体叠加区域与实际泄漏点可能存在出入。

10设置场景布防。

图 6-3 场景布防

10.1 进入 *配置* → *VOCs 气体检测* → *场景布防* 。

10.2 勾选*启用*。

10.3 设置**检测停留时间**。**检测停留时间**

设备在当前预置点停留该设置的时间后，再巡航至下个预置点。

10.4 单击 ＋ ，选择**预置点名称**，完成多个场景添加。

10.5 对场景排序：按序号依次选择预置点名称或鼠标悬停在预置点列表行并单击 调整顺序。

10.6 设置布防时间，请参见 *布防时间配置* 。

10.7 单击*保存*。

11设置报警联动。

11.1 进入 *配置* → *VOCs 气体检测* → *联动方式* 。

11.2 设置联动方式，请参见 *联动配置* 。

11.3 单击*保存*。

12**可选操作**: 设置算法参数。

12.1 进入 *配置* → *VOCs 气体检测* → *高级参数* 。

12.2 勾选*启用伪彩叠加*。

启用伪彩叠加

启用后，可见光通道的预览画面可以看到实时的气团运动（气团位置）与浓度变化。设备可将气体浓度数据转换为不同颜色，叠加在可见光通道的预览画面内。气体浓度越高颜色越靠近红色，反之越靠近蓝色。

气云成像机芯波特率

根据实际情况，选择与气云成像机芯一致的波特率，确保设备与气云成像机芯能正常通信。

12.3 单击*保存*。

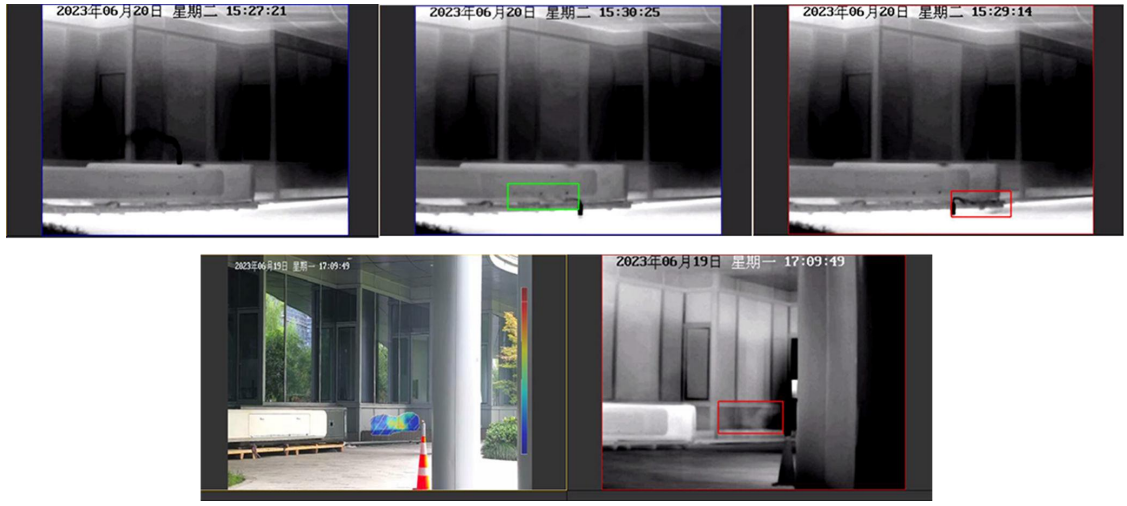


图 6-4 效果展示

12.3.1 预览画面最外侧边框为规则框。蓝色规则框表示 VOCs 气体检测功能已开启；红色规则框表示触发 VOCs 气体检测报警。

12.3.2 预览画面内部边框为目标框。绿色目标框表示检测出 VOCs 气体，疑似存在气体泄露；红色目标框表示触发 VOCs 气体检测，存在气体泄露。

第 7 章 事件和报警

介绍设备支持的各个事件的功能配置，根据需求配置相应的事件，触发设备执行联动动作。

• 普通事件

介绍设备基本的事件配置。

• 配置移动侦测

移动侦测是指在规格区域中，侦测是否有物体移动，并触发设备执行联动。

操作步骤

1. 进入 *配置 → 事件 → 普通事件 → 移动侦测* 。

2. 选择通道号。

3. 勾选*启用移动侦测*。

4. **可选操作**: 将画面中移动的物体设置成绿色高亮显示。

- 勾选*启用动态分析*，并保存。
- 进入 *配置 → 本地* 。
- 选择**规则信息**为*启用*，并保存。

5. 选择**配置模式**，设置规则区域和规则参数。

1. 普通模式设置请参见 *普通模式* 。

2. 专家模式设置请参见 *专家模式* 。

6. 设置布防时间请参见 *布防时间配置* ， 设置联动方式请参见 *联动配置* 。

7. 单击*保存*。

普通模式

根据设备默认参数设置移动侦测。

操作步骤

1. **配置模式**中选择*普通模式*。

2. 设置**灵敏度**。

灵敏度数值越高，移动侦测越灵敏；如果灵敏度设置为 *0*，移动侦测和动态分析将不起作用。

3. 单击*绘制区域*，在实况画面中按住鼠标左键并拖动鼠标，然后松开鼠标左键，完成 1 个区域的绘制。

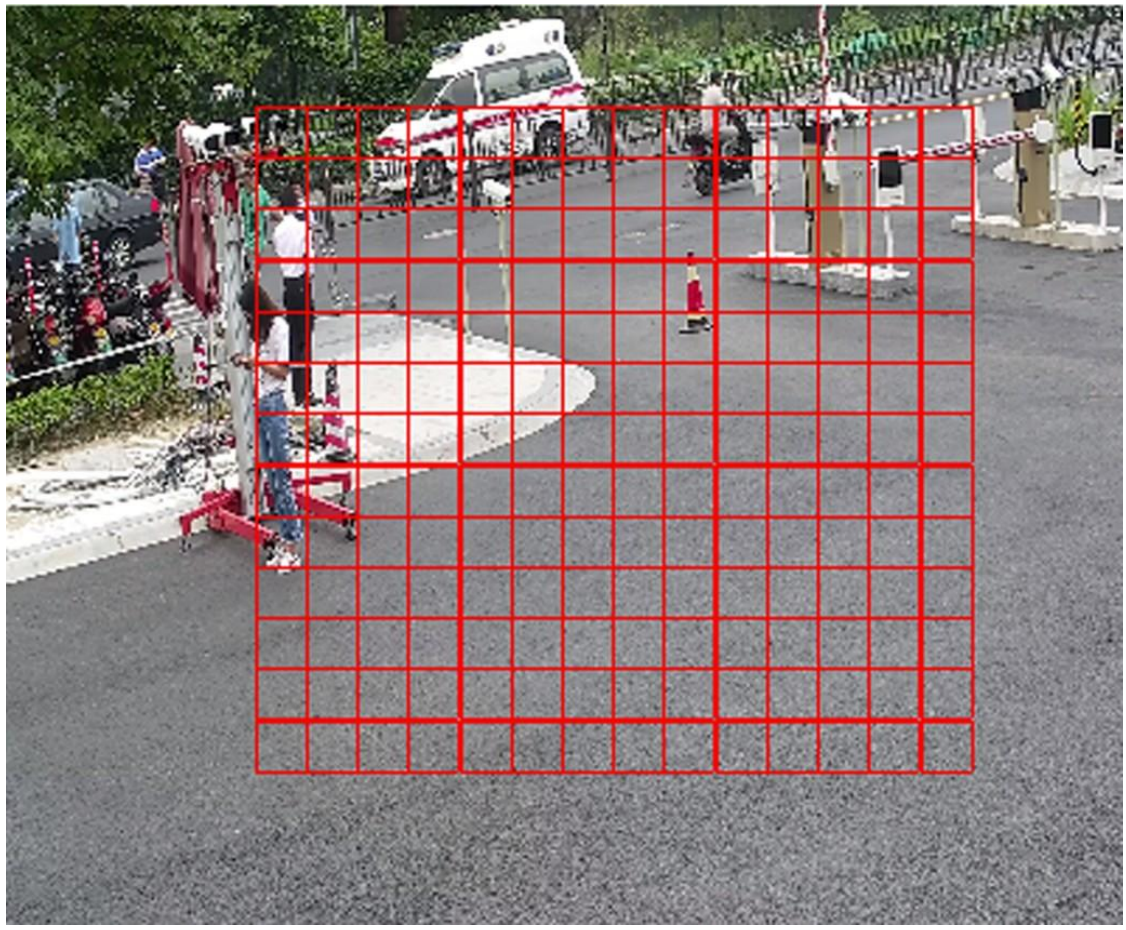


图 7-1 设置规则和参数

单击***停止绘制*** 结束区域绘制。

单击***清除全部*** 删除绘制的区域。

4. 可选操作: 重复上述步骤可以设置多个规则区域及规则参数。

专家模式

根据需求自定义设置白天、晚上的移动侦测参数。

操作步骤

1. 在**配置模式**中选择***专家模式***。

2. 设置专家模式参数。

日夜参数转换

关闭

表示不进行日夜切换。

自动切换

系统将根据环境的变化自动切换白天和夜晚模式，白天模式画面为彩色，夜晚模式画面为黑白。

定时切换

根据设置的时间进行切换，在设置的时间段内为白天模式，时间段外为夜晚模式。

灵敏度

灵敏度数值越高，移动侦测越灵敏。如果灵敏度设置为 *0*，移动侦测和动态分析将不起作用。

3. 选择 1 个**区域**，单击***绘制区域***，在实况画面中拖拽鼠标绘制区域。

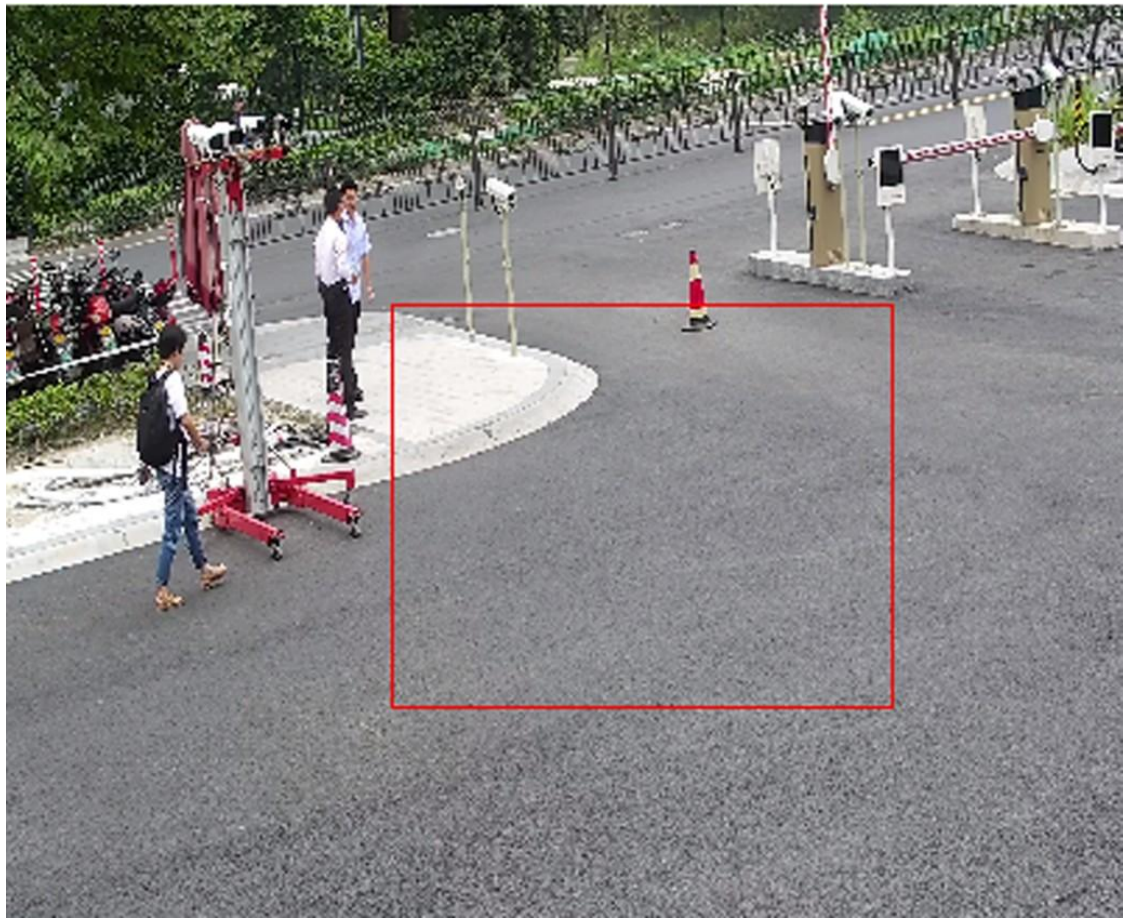


图 7-2 设置规则

单击***停止绘制*** 结束区域绘制。

单击***清除全部*** 删除已绘制的区域。

4. **可选操作**: 重复上述方法可以设置多个警戒区域规则参数。

5. 单击*保存*。

• 配置遮挡报警

当预先指定的遮挡区域被遮挡，无法对该区域进行正常监控，触发设备执行联动动作。

操作步骤

1. 进入 *配置* → *事件* → *普通事件* → *遮挡报警* 。

2. 选择通道。

3. 勾选*启用*。

4. 设置**灵敏度**，灵敏度数值越高，检测越灵敏。

5. 单击***绘制区域***，在实况画面中单击鼠标左键并拖动鼠标，然后松开鼠标左键，完成 1 个区域的绘制。

单击***停止绘制*** 结束区域绘制。

单击***清除全部*** 删除已绘制的区域。

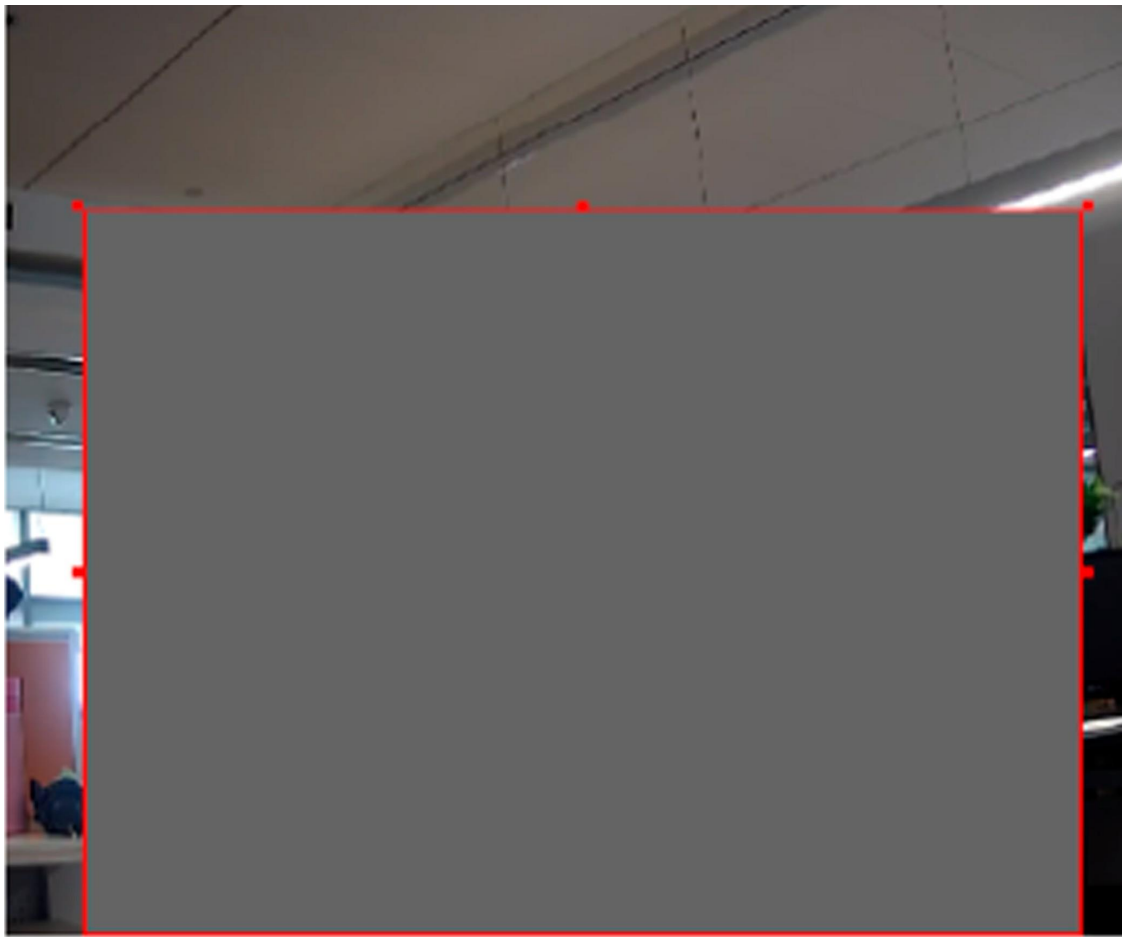


图 7-3 遮挡报警

6. 设置布防时间请参见 *布防时间配置* ，设置联动方式请参见 *联动配置* 。

7. 单击*保存*。

• 配置报警输入

设备的报警输入接口外接报警设备，当外接报警设备产生报警信号时，触发设备执行联动动作。

前提条件

设备的报警输入接口外接报警设备，接线方法请参见*快速入门指南*。

操作步骤

说明

报警输入功能视型号而定，请以实际设备为准。

- 进入 *配置 → 事件 → 普通事件 → 报警输入* 。
- 勾选*处理报警输入*。
- 选择**报警输入号**和**报警类型**，填写**报警名称**。

说明

根据连接的报警设备设置报警类型。

- 布防时间设置请参见 *布防时间配置* ，联动方式设置请参见 *联动配置* 。
- 单击*复制到*，复制该报警输入设置信息至其他的报警输入通道。
- 单击*保存*。

• 配置异常报警

当设备出现网络断开等异常情况时，触发设备执行联动动作。

操作步骤

1. 进入 *配置 → 事件 → 普通事件 → 异常* 。

2. 根据需求，选择**异常类型**。

硬盘满 表示设备中的安装的存储录满时将触发联动动作。

硬盘错误 表示设备中安装的存储设备状态出现错误时触发联动动作。

网线断开 表示设备没有连接网线或网线脱落时触发联动动作。

IP 地址冲突 表示设备 IP 地址与网络中的其它设备 IP 地址相同时触发联动动作。

非法访问 表示设备输入错误的用户名或密码时触发联动动作。

3. 联动方式设置请参见 *联动配置* 。

4. 单击*保存*。

• Smart 事件配置

针对特定场景选择并配置 Smart 事件。当有目标触发规则，设备将执行联动动作。

• 配置音频异常侦测

音频异常侦测用于侦测当设备和拾音器的连接断开时，产生声音异常，触发设备执行联动动作。

操作步骤

7 选择 *配置 → 事件 → Smart 事件 → 音频异常侦测* 。

8 选择通道号。

9 选择 1 项或多项音频异常侦测。

音频输入异常

勾选表示当设备音频输入发生异常时自动生成报警信息。

声强陡升

勾选后，设置**灵敏度**或**声音强度阈值**，调整进度条或设置参数值，根据结果判断报警和联动。

说明

9.1 灵敏度数值越小，则输入声音强度变化超过持续环境音量更多才能被判断为音频异常，用户需要根据实际环境测试调节。

9.2 声音强度阈值过滤环境噪音，如果环境噪音越大，则该值需要设置的越高，用户需要根据实际环境测试调节。

声强陡降

勾选后，设置**灵敏度**，调整进度条或设置参数值，根据结果判断报警和联动。

10布防时间设置请参见 *布防时间配置* ，联动方式请参见 *联动配置* 。

11单击*保存*。

说明

音频异常侦测视型号而定，请以实际设备为准。

第 8 章 视音频及图像参数

介绍设备的视频、音频及图像的参数及参数设置，具体参数请以实际设备为准。

1) 设置视频参数

用于设置设备码流类型、编码协议和分辨率等视频参数。

通过 *配置* → *视音频* → *视频*，设置视频参数。

说明

多通道设备请先选择通道后设置其预览参数。

- **码流类型**

根据使用需求选择码流类型。

主码流

码流大，清晰度高，占用带宽大，适用于本地存储。

子码流

实图像较流畅，占用带宽小，适用于低带宽网络传输或标清存储。

第三码流、第四码流、第五码流

请根据使用需求选择对应码流并设置参数。

说明

第三码流、第四码流、第五码流视型号而定，请以实际设备为准。

- **视频类型**

选择视频中包含的流类型。

视频流

仅包含视频流。

复合流

包含视频流和音频流。

说明

复合流视型号而定，请以实际设备为准。

- **分辨率**

根据实际对视频清晰度的要求来选择，分辨率越高，对网络的带宽要求越高。

- **码率类型和码率上限**

定码率

表示码率维持在平均码率进行传输，压缩速度快，但可能会造成视频马赛克现象。

变码率

表示在不超出**码率上限**的基础上自行调整码率，压缩速度相对较慢，但能够保证复杂场景时的画面清晰度。

- **图像质量**

当码率类型为变码率时可设置图像质量，根据实际需求对图像清晰度进行选择。图像质量越高，对网络的带宽要求越高。

- **视频帧率**

表示视频每秒的帧数。视频帧率越高，画面越流畅逼真。但需要的带宽越和存储空间越大，请根据实际带宽情况设置。

- **视频编码**

介绍设备支持的视频编码技术。

说明

视频编码参数项视型号而定，请以实际设备为准。

H.264

1) 是一种高性能的视频编解码技术，压缩比高，且处理灵活，超低码率，节省网络传输带宽和存储空间。

Smart264

Smart264 是一种编码方式，可进一步提高压缩性能，减少存储空间。视频编码 H.264 时才支持 Smart264 功能。

开启 Smart264 功能后，**I 帧间隔**将不可设置。

说明

开启 Smart264 后，会显示**平均码率**，系统根据码率上限自动给出平均码率的推荐值。在复杂监控场景下，默认平均码率图像质量欠佳时，可手动设置，提高平均码率参数值，参数值上限应小于码率上限。

H.265

2) 是一种高性能的视频编解码技术，压缩比高，且处理灵活，超低码率。压缩性能相比当前 H.264 提升了一倍，更一步节约带宽和存储空间。

Smart265

Smart265 是一种编码方式，可进一步提高压缩性能，减少存储空间。视频编码 H.265 时才支持 Smart265 功能。

开启 Smart265 功能后，**I 帧间隔**将不可设置。

说明

开启 Smart265 后，会显示**平均码率**，系统根据码率上限自动给出平均码率的推荐值。在复杂监控场景下，默认平均码率图像质量欠佳时，可手动设置，提高平均码率参数值，参数值上限应小于码率上限。

MJPEG

MJPEG 是一种的视频编解码技术，压缩图像质量较好，在画面变动情况下无马赛克。

编码复杂度

表示相同码率下编码复杂度越高，图像质量越高，但对网络带宽的要求也越高。

I 帧间隔

表示前后两个关键帧之间的帧数。

I 帧间隔越大，码流越小，但图像质量相对较差；反之则码流越大，图像质量越好。

SVC

SVC 是一种可扩展视频编码技术，可用于带宽不足时的编码存储。此功能需要配合后端存储设备实现。

• 码流平滑

码流平滑是通过调整 I 帧大小，使图像平滑，可用于缓解由于 I 帧过大带来的网络冲击。

拖动进度条或输入码流平滑值，数值越高则平滑度越好，但图像将相对不清晰，反之则图像平滑度差，图像相对清晰。

• 设置音频参数

用于设置设备音频编码、环境燥声过滤等音频参数。

通过 *配置* → *音视频* → *音频*，设置音频参数。

请根据需求选择通道号。

说明

音频参数视型号而定，请以实际设备为准。

• 音频编码

请根据使用需求选择音频编码类型。

• 音频输入

设置设备音频输入参数。

说明

65. 请根据使用需求连接好音频输入设备。

66. 音频输入项视型号而定，请以实际界面为准。

连接 LineIn 设备	选择**音频输入**为 *LineIn*。表示设备连接自身音频输出功率比较大的设备（如 MP3、合成器和有源拾音器等），以免出现没有声音或声音太小的情况。
连接 MicIn 设备	选择**音频输入**为 *MicIn*。表示设备连接自身音频输出功率比较小的设备（如麦克风和其他无源音频输入设备等），以免出现音频信号失真的情况。

输入音量

音频输入源的增益控制数值，请根据实际需求调节。

- **环境噪声过滤**

当监控环境中声音较为嘈杂，开启此功能，可减少音频中的噪声。

• 开启语音对讲

用于实现监控中心与监控画面内的目标进行语音对讲。

前提条件

67. 请确保连接设备的拾音器、麦克风或扬声器能够正常使用，请参见产品参数表连接有源或无源的音频输入、输出设备。

68. 如果设备已内置麦克风和喇叭，可直接开启语音对讲功能。

操作步骤

说明

语音对讲功能视型号而定，请以实际设备为准。

1. 单击*预览*。

2. 单击 ，开启对讲。

3. 单击 选择 ，调节滑动条，可以调节音量大小。

4. 单击 ，停止对讲。

• ROI

ROI 即感兴趣区域，选定图像中的某一个区域作为重点关注区域，提升该区域的图像质量，在预览或录像时选定区域内的图像比其它区域的图像更清晰。

• 配置固定区域 ROI

ROI 为感兴趣区域编码，开启 ROI 功能后，设备会提升选定区域的图像编码质量，降低所选区域外的编码质量，在图像预览或录像时选定区域内的图像更清晰。

前提条件

视频编码设置为 *H.264* 或 *H.265* 时支持 ROI 功能，请检查视频编码类型。

操作步骤

1. 选择 *配置* → *视音频* → *ROI* 。

2. 勾选*启用*。

3. 选择通道号。

4. 选择**码流类型**。

5. 选择**固定区域** 的**区域编号**。

6. 绘制感兴趣区域。

- 单击*绘制区域*。
- 使用鼠标在实况画面上框选固定区域。
- 单击*停止绘制*。

说明

选择要调整的固定区域 ，鼠标拖动可以调整固定区域的位置。

7. 设置固定区域的**区域名称**和**提升等级**。

8. 单击*保存*。

说明

提升等级设置越高，检测区域图像越清晰。

9. **可选操作**: 如果需要绘制多个区域，请选择其它区域编号，重复以上步骤设置。

• 配置区域裁剪

为了减少网络传输带宽和存储空间，可以监控区域进行局部裁剪，对重要区域的图像进行传输和存储。

操作步骤

1. 进入 *配置* → *视音频* → *区域裁剪* 。

2. 勾选*启用区域裁剪*，将**码流类型**选择为**第三码流**。

说明

开启区域裁剪后，三码流分辨率将不支持配置。

3. 选择**裁剪分辨率**，根据需求选择一种适合的分辨率。

在视频图像中心显示红色的矩形框。

4. 使用鼠标拖动红色矩形框至关注区域。

5. 单击*保存*完成配置。

说明

- 区域裁剪视型号而定，请以实际设备为准。
- 区域裁剪与部分功能互斥，启用后相关功能将失效，请以实际设备为准。

• 设置视频遮盖

监控图像时，如果需要屏蔽设备的某个区域画面，可以设置视频遮盖，遮盖该区域的画面显示，达到保护隐私的作用。

操作步骤

1. 进入 *配置* → *图像* → *视频遮盖* 。

2. 选择通道号。

3. 勾选*启用视频遮盖*。

4. 单击*绘制区域*，拖动鼠标框选需要遮盖的区域。

拖动区域框的端点 调整区域框的大小。

拖动区域框 移动区域框的位置。

单击*清除绘制* 清除画面中绘制的所有区域。

5. 单击*添加*，添加 1 个遮盖区域，并设置区域的参数。

隐私块标题

可自定义隐私区域名称。

类型

可选择黑色、马赛克。

6. 单击*保存*。

结果说明

在实况画面上将根据类型遮盖对应的区域。

• 叠加码流信息

用于配合存储产品或客户端软件，回放时实现二次检索。

操作步骤

- 进入 *配置* → *视音频* → *码流信息叠加* 。

- 勾选*启用支持智能后检索*，实现智能回放的二次检索。
- 单击*保存*。

说明

功能视型号而定，请以实际界面为准。

• 设置图像显示参数

用于调节实况画面图像质量的参数。

选择 *配置* → *图像* → *显示设置* 。

选择通道号。

单击*恢复默认值*，则将显示参数将恢复到初始状态。

• 场景模式

请根据设备的实际安装环境和使用条件选择合适的场景。

• 图像调节

通过调整**图像亮度**、**饱和度**、**对比度**和**锐度**，使图像呈现最佳显示效果。

气云成像机芯长期工作需要进行图像校正，防止温度变化较大、长时间运行等导致图像出现噪点、亮度异常等情况。

背景校正

需人员提前将均温物体遮挡镜头，再单击*校正*进行图像校正。

手动校正

通过气云成像机芯控制镜头前的光圈实现镜头遮挡。单击*校正*可手动进行图像校正。

• 曝光

曝光由光圈、快门、感光度的组合来控制。可通过设置曝光参数调节图像效果。

自动

自动模式下，可根据实际场景调节其**光圈**和**快门**的限制值，**光圈**、**快门**、**增益**自动调节。

光圈优先

光圈优先模式下，可根据实际场景调节**光圈**值，**快门**和**增益**自动调节。

快门优先

快门优先模式下，可根据实际场景调节**快门**值，**光圈**和**增益**自动调节。

手动

手动模式下，**光圈**、**快门**、**增益**需要通过手动设置。

最大/最小光圈限制

限制光圈范围，通过范围锁定可以适用更多场景，如果侧重近景监控目标，可以将光圈调大；如果侧重远景监控，可以适当调小光圈。

最大/最小快门限制

限制快门范围，通过范围限定可以适用更多场景，快门速度越快，曝光度越低，图片越暗；快门速度越慢，曝光度越高，图片越亮。

增益

调节视频信号的放大程度，增益越大，图像噪点越明显。

增益限制

可拖动进度条或者设置增益限制值。

低照度电子快门

开启和关闭低照度快门，可设置电子快门级别，当慢快门数值越高，表示快门越慢，当处于低照度环境时可看清监控画面。

- **聚焦**

聚焦是指设备采取某种方式获得清晰的焦点位置来校准焦距的过程，是保证所记录的影像取得清晰效果的关键步骤。

聚焦模式

请根据不同场景拍摄需求选择聚焦模式。

自动

表示设备根据监控场景变化自动聚焦。

说明

当聚焦模式设置为*自动*出现聚焦不清时，请减少场景内的灯光，同时避开闪烁的灯光。 也可通过适当放大倍率减少图像内的灯光。

半自动

表示设备在镜头变倍后聚焦 1 次。聚焦清晰后，即使场景变化也不再聚焦。

手动

表示设备需在实况画面的云台控制处，手动调节聚焦使图像清晰。

说明

69. 聚焦模式项视型号而定，请以实际设备为准。

70. 选择自动或半自动模式时，支持聚焦**灵敏度**设置。

• 日夜转换

根据设备的补光情况设置日夜转换模式，以获取高质量的图像。

白天

白天模式时，图像为彩色。

夜晚

夜晚模式时，图像为黑白。

自动

自动模式时，设备根据外界环境亮度自动切换白天模式和夜晚模式。

定时

定时模式时，需要设置白天的开始时间和结束时间，在时间段内，设备将自动使用白天模式，其余时间，设备将自动使用夜晚模式。

报警输入触发

报警输入触发模式时，**触发状态**可选择白天和夜晚。如果触发状态为夜晚，无报警输入触发时，设备保持白天模式；当报警输入触发，设备切换到夜晚模式。

说明

日夜转换项视型号而定，请以实际设备为准。

灵敏度

夜晚模式到白天模式转换阈值。灵敏度越高，越容易切换到白天模式，越难切换到夜晚模式；灵敏度越低，越容易切换到夜晚模式，越难切换到白天模式。

过滤时间

当环境照度满足转换要求且保持的时间超过设定的阈值时间后才会进行日夜的切换。

- **补光灯参数**

设置补光灯的参数，该参数请以实际设备为准。

防补光过曝

采用智能图像处理技术，防止因设备开启补光导致中心区域过曝。当补光灯关闭时，该功能无效。

补光模式

当设备支持补光时，可选择补光模式。

红外模式

设备将启用红外补光灯进行补光。

白光模式

设备将启用白光补光灯进行补光。

混合补光

设备将启用白光和红外补光灯进行补光。

关闭

关闭补光灯。

说明

补光模式视型号而定，请以实际设备为准。

亮度调节模式

自动

补光灯的亮度由设备根据环境自行控制。

手动

补光灯的亮度可通过拖拽进度条或设置数值进行调节。

- **背光补偿**

用于有效补偿设备在逆光环境下拍摄时画面主体黑暗的缺陷。用户可根据实际场景，选择需要补偿的区域。

- **宽动态**

宽动态适用于监控光线强度差异较大的监控环境。当在强光源（日光、灯具或反光等）照射下的高亮度区域与阴影、逆光等相对亮度较低的区域在监控画面中同时存在时，可以开启宽动态功能并调整等级来看清监控画面。

宽动态自动平衡监控画面中最亮和最暗部分的画面，以便看到更多监控画面细节。

说明

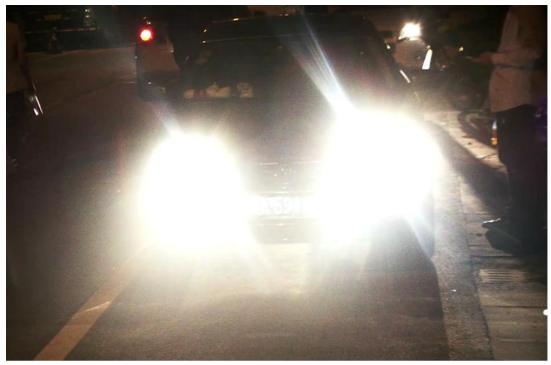
开启宽动态会与一些功能互斥，请以实际设备界面为准。

宽动态关闭　　宽动态开启

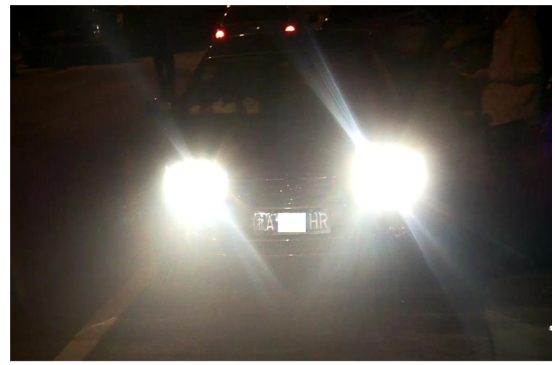
图 8-1 宽动态

- **强光抑制**

当监控画面出现明亮区域过度曝光、暗区欠曝光的时候，开启强光抑制，可弱化明亮区，亮化暗区，达到整体画面的光线平衡。



强光抑制关闭



强光抑制开启

图 8-2 强光抑制

- **白平衡**

在不同的光照环境中，物体颜色会因投射光线颜色而产生变化，根据使用环境选择合适的白平衡模式，可修正颜色误差。

冷色

暖色

自动白平衡

图 8-3 白平衡

- **数字降噪**

采用图像降噪技术，有效降低图像噪点，使图像更加柔和细腻。

普通降噪模式

通过设置降噪等级来控制降噪程度。

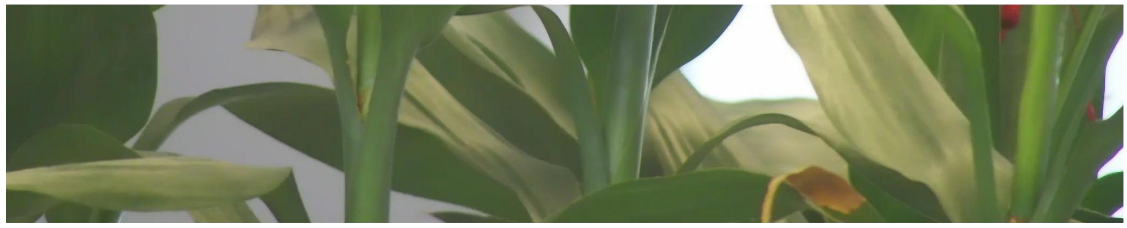
专家降噪模式

可通过空域降噪级别和时域降噪级别两个维度进行调节。

关闭

关闭数字降噪。

降噪关闭



降噪开启

图 8-4 数字降噪

- **透雾**

用于设备在有雾的环境下使用时，提高物体的可辨识程度，使画面清晰。

设置透雾模式。

开启

设置**透雾等级**，当等级参数设置到 *80* 以上时，将自动开启光学透雾，增强透雾能力。

自动

设备根据场景自动调节透雾参数。

关闭

关闭透雾功能。

透雾关闭

透雾开启

图 8-5 透雾

- **电子防抖**

通过抖动补偿技术用于提升视频画面的稳定性。

说明

电子防抖功能视型号而定，请以实际设备为准。

- **镜像**

当设备的预览界面与实际拍摄区域存在视角翻转时，可通过镜像调整画面至正常视角。

根据实际情况选择镜像类型。

说明

开启镜像模式后，平台录像将会出现短暂中断。

- **镜头畸变矫正**

对于电动镜头的设备，因镜头镜片弧度太大可能导致图像发生弯曲。开启镜头畸变矫正，可使图像显示平整。

说明

71. 该功能仅针对自带电动镜头的设备，请以实际设备为准。

72. 开启后图像将会有所损失。

- **视频制式**

表示视频信号制式，当选择 PAL（50 Hz）时，最高帧率为 25 fps 或者 50 fps，当选择 NTSC（60 Hz）时，最高帧率为 30 fps 或者 60 fps。

- **本地输出**

设备具有 BNC、CVBS 等接口，并支持输出相应的视频信号，连接相应的显示器可输出实况画面。

选择*开启*时，带有 BNC、CVBS 等接口的机型可输出实况画面；选择*关闭*时，则关闭输出视频信号。

说明

本地输出功能视型号而定，请以实际设备为准。

- **配置图像参数切换**

用于设置多个时间段对应不同场景。

前提条件

进入 *配置* → *图像* → *显示设置*，配置各场景对应的图像参数。

操作步骤

1. 进入 *配置* → *图像* → *图像参数切换* 。
2. 勾选*启用*。
3. 选择需要设置的场景，并绘制切换计划。

   说明

   单击 ，删除全部计划。

   单击 ，删除选中的计划。
4. 单击*保存*。

   说明

   参数切换时间段视型号而定，请以实际设备为准。

   设备将在时间段内，执行场景对应的图像参数。

- **OSD 参数**

介绍预览图像上的显示信息，并对显示信息进行调整。包括设置名称、日期等 OSD 信息和设置 OSD 的颜色、字体等属性，以及在图像上叠加字符信息。

选择 *配置* → *图像* → *OSD 设置*，可设置对应参数，保存后生效。

通道显示信息

设置实况画面上名称、日期、星期及显示格式的显示参数。

OSD 属性

设置**字体**、**颜色**、**对齐方式**等 OSD 参数。

字符叠加

在实况画面上，根据需求自定义叠加的字符信息。

• 配置图片叠加

叠加自定义图片到视频中。

前提条件

准备叠加在视频上的图片，要求为不大于 128 × 128 像素的 24 位 BMP 位图图片。

操作步骤

1. 进入 *配置* → *图像* → *图片叠加* 。

2. 选择通道号。

3. 单击*浏览*，选择需要叠加的图片，并单击*上传*。

提示图片上传成功，且视频画面内可以看到红色方框。

4. 勾选*启用图片叠加*。

5. 拖动红色方框调整图片显示的位置。

6. 单击*保存*。

说明

图片叠加功能视型号而定，请以实际设备为准。

第 9 章 网络配置

介绍网络参数的配置方法。

• TCP/IP 参数

配置设备的 TCP/IP 参数，使设备能在网络中正常使用。

选择 *配置* → *网络* → *基本配置* → *TCP/IP*，设置设备的基本网络参数，并单击*保存*。

网卡类型

根据网络环境选择。

IPv4 地址

勾选*自动获取*，设备将根据网络环境自动获取网络参数。

注意

当设备网络支持 DHCP（Dynamic Host Configuration Protocol）服务器，且设备为自动获取 IP 地址方式时，设备 IP 地址会被修改。可通过 SADP 工具来获取设备的 IP 地址。

不勾选*自动获取*，需手动填写**设备 IPv4 地址**、**IPv4 子网掩码**和 **IPv4 默认网关**等局域网参数信息。

说明

手动填写 IPv4 网络参数时，单击*测试*可确认该 IP 地址是否可用。

IPv6 地址

请根据需求填写 IPv6 网络参数，如不明确请咨询网络管理人员。

1. 路由公告模式使用公告的 IP 前缀加设备自身的物理地址生成 IPv6 地址。

2. 自动获取模式由相应的服务器、路由或网关下发 IPv6 地址。

3. 手动模式根据实际网络需要配置，如不明确请咨询网络管理人员。

MTU

表示最大传输单元，是指 TCP/UDP 协议网络传输中所通过的最大数据包的大小。

DNS

当设备设置了正确可用的 DNS 服务器地址后，可通过域名对设备进行访问。

动态域名

勾选*启用动态域名*并配置注册域名后，局域网中可以通过该注册域名搜索并访问设备。

说明

请先通过 *配置 → 网络 → 基本配置 → TCP/IP* 勾选*自动获取*。动态域名在开启自动获取(DHCP)后生效。

- **多播设置**

多播搜索

勾选*启用多播搜索*，设备将通过私有协议，将特定信息发送给多播组内的客户端或设备。

说明

当因多播风暴引起设备无法正常使用时，您可尝试关闭多播搜索缓解问题。

多播参数

选择 *配置 → 网络 → 基本配置 → 多播配置* ，填写相关参数后，可实现多个设备或地址，通过 RTSP 协议或 SRTP 协议对设备进行取流。

- **网络服务**

请根据需求开启和关闭各类网络服务协议，该功能请以实际设备为准。

操作步骤

- 进入 *配置 → 网络 → 高级配置 → 网络服务* 。
- 设置网络服务参数。

启用 WebSocket

勾选表示使用 HTTP 协议访问设备。

启用 WebSockets

勾选表示使用 HTTPS 协议访问设备。此时，请选择**服务端证书**，以保证数据传输的安全性。

说明

通过 *配置 → 系统 → 安全管理 → 证书管理* 可查看设备各类证书。

启用 SDK 服务

勾选表示通过 SDK 协议将设备添加到客户端软件。

启用增强型 SDK 服务

勾选表示通过 SDK over TLS 协议将设备添加到客户端软件。此时，请选择**服务端证书**，以保证数据传输的安全性。

说明

通过 *配置 → 系统 → 安全管理 → 证书管理* 可查看设备各类证书。

启用 TLS1.1 版本或启用 TLS1.2 版本

勾选表示设备支持 TLS1.1 协议或 TLS1.2 协议访问设备。

Bonjour

勾选表示允许设备在局域网内自动传播自己的服务信息并发现其他设备的服务信息。

- 单击*保存*。

• 端口参数

当设备因端口冲突导致无法进行网络访问时，可修改设备端口。

注意

请不要随意修改缺省端口参数，否则会导致设备无法访问。

选择 *配置 → 网络 → 基本配置 → 端口*，设置端口参数，保存后生效。

HTTP 端口

表示浏览器访问设备的端口。如当 **HTTP 端口**修改为 81 时，使用浏览器登录时，需要在浏览器输入 *http://192.168.1.64:81* 进行访问。

HTTPS 端口

表示浏览器证书访问的端口，当浏览器访问设备时，需要通过证书验证才能访问，安全级别高。

RTSP 端口

表示设备实时传输协议的端口。

SRTP 端口

表示设备安全实时传输协议的端口。

服务端口

表示客户端添加设备的端口。

服务增强型端口

表示客户端添加设备的端口，需要通过证书验证才能访问，安全级别高。

WebSocket 端口

基于 TCP 的全双工通信协议端口，用于无插件预览。

WebSockets 端口

基于 TCP 的全双工通信协议端口，用于无插件预览，需要通过证书验证才能访问，安全级别高。

说明

73. 服务增强型端口、WebSocket 端口和 WebSockets 端口视型号而定，具体请以实际设备界面为准。

74. 根据使用需求，进入 *配置 → 网络 → 高级配置 → 网络服务* 开启对应的端口。

• 设置端口映射

通过设置端口映射，可以访问指定端口的设备。

前提条件

当前设备中的端口与网络中的其它设备端口相同时，请参见 *端口参数* 修改设备端口。

操作步骤

1. 进入 *配置 → 网络 → 基本配置 → 端口映射* 。

2. 选择端口映射方式，设置设备端口映射。

自动映射 设置方法请参见 *设置自动端口映射* 。

手动映射 设置方法请参见 *设置手动端口映射* 。

3. 单击*保存*。

• 设置自动端口映射

自动分配设备和路由器上的端口映射，实现设备端口开放。

操作步骤

- 勾选*启用 UPnP™*，可根据需求设置一个别名。
- 端口映射方式选择**自动**。
- 单击*保存*。

说明

路由器上同时开启 UPnP™功能。

• 设置手动端口映射

手动设置设备和路由器上的端口映射，实现设备端口开放。

操作步骤

1. 勾选*启用 UPnP™*，可根据需求设置一个别名。
2. 端口映射方式选择手动，设置外部端口与内部端口相同。
3. 单击*保存*。

后续处理

进入路由器端口映射界面，将端口号和 IP 地址设置成与设备中的一致。

• 设置路由器端口映射

以某一款路由器的配置界面为例，介绍通过路由器进行端口映射。

操作步骤

5 根据网络环境，选择上网方式。
6 设置路由器的 **IP 地址**、**子网掩码**等网络参数。
7 在路由器 *转发规则* → *虚拟服务器*，填写设备的**端口号**和 **IP 地址**。
8 单击*保存*。

示例

图 9-1 路由器端口映射

上图所示设备端口号为 80、8000、554，设备 IP 地址为：192.168.1.5，表示将路由器的 80、8000、554 端口映射给设备 192.168.1.5，这样访问路由器的 80、8000、554 端口就是访问 192.168.1.5。

• 设置 SNMP 参数

通过配置 SNMP 网络管理协议可以获取和接收设备在网络传输中的异常和报警信息。

前提条件

需要有 SNMP 服务器，且保证 SNMP 服务端配置了相关参数及能够正常工作。

操作步骤

1. 进入 *配置 → 网络 → 高级配置 → SNMP* 。
2. 根据 SNMP 服务器端协议版本，勾选开启对应的 SNMP。

说明

SNMP v1.0 版本安全级别比较低，建议使用其它安全级别较高的版本。

3. 根据需求设置 SNMP 参数。
4. 单击*保存*。

• 设置 DDNS 域名访问

采用 DDNS（动态域名解析）访问设备，可将设备的动态 IP 地址映射到一个固定的域名解析服务器上，从而有效解决网络设备互联网访问问题。

前提条件

请先申请 DynDNS 或 NO-IP 服务器的域名。

操作步骤

1. 参见 *TCP/IP 参数*，设置 DNS 参数。
2. 进入 *配置 → 网络 → 基本配置 → DDNS* 。
3. 勾选*启用 DDNS*，选择 DDNS 类型。

DynDNS

采用 DynDNS 服务器进行域名解析。

NO-IP

采用 NO-IP 服务器进行域名解析。

4. 填写域名信息，单击*保存*。
5. 查看设备端口并完成端口映射。查看设备端口请参见 *端口参数* ，端口映射方法请参见 *设置端口映射*。
6. 访问设备。

通过浏览器	在浏览器地址栏中输入域名和端口号访问设备。
通过客户端软件	在客户端软件中添加域名，访问设备，具体添加方法请参见客户端手册。

- **设置 PPPoE**

当采用 PPPoE 拨号方式连接网络时，拨号后会自动获取一个互联网的动态 IP 地址，实现互联网访问。

操作步骤

1. 进入 *配置 → 网络 → 基本配置 → PPPoE* 。

2. 勾选**启用 PPPoE**。

3. 设置 PPPoE 参数。

设备动态 IP

拨号成功后，显示的广域网的动态 IP 地址。

用户名

拨号上网的用户名。

密码

拨号上网的密码。

密码确认

再次输入拨号上网的密码。

4. 单击*保存*。

5. 访问设备。

通过浏览器 在浏览器地址栏中输入广域网动态 IP 地址访问设备。

通过客户端软件 在客户端软件中添加广域网动态 IP 地址，访问设备，具体添加方法请参见客户端手册。

说明

广域网动态 IP 地址经常变动，可参见 *设置 DDNS 域名访问* ，设置一个域名，通过域名进行访问。

9.8 设置 28181

遵循 GB/T28181 的要求，将设备注册到公安网平台，实现远程实时监控、管理设备等功能。

操作步骤

1. 进入 *配置 → 网络 → 高级配置 → 平台接入* 。

2. **平台接入方式**选择为 28181。

3. 勾选*启用*。

4. **可选操作**：勾选*启用国密模式*，设备注册到 28181 平台时，将需要通过证书进行双向认证。

启用证书交换

启用证书交换后，可通过国密模式接入支持 GB35114-2017 协议且支持证书交换的 SIP 服务器。

说明

国密模式是否支持以实际设备为准。

5. 根据 28181 协议，设置 28181 相关参数，可通过查找该协议的相关资料并进行配置。

6. 单击*保存*。

• 设置 ISUP

遵循 ISUP（原 Ehome）平台的要求，将设备注册 ISUP 平台，实现远程实时监控、管理设备等功能。

操作步骤

1. 进入 *配置 → 网络 → 高级配置 → 平台接入* 。

2. **平台接入方式**选择为 ISUP。

3. 勾选*启用*。

4. 根据 ISUP 协议，设置 ISUP 参数。

5. 单击*保存*。

刷新网页或者重启设备查看注册状态。

• 配置开放型网络视频接口

当需要通过开放型网络视频接口协议连接设备时，可根据需要配置对应的用户，从而加强设备的网络安全性。

操作步骤

1. 进入 *配置 → 网络 → 高级配置 → 集成协议* 。

2. 勾选*启用开放型网络视频接口*。

3. 单击*添加*，根据协议自定义开放型网络视频接口用户。

单击*删除* 删除该用户。

单击*修改* 修改用户信息。

4. 单击*保存*。

5. **可选操作**: 重复上述步骤，可根据实际需要添加多个用户。

• 设置视图库

设备通过公安视频图像信息数据库协议（简称视图库协议），发送设备报警信息至视图库平台。

操作步骤

说明

视图库功能视型号而定，请以实际设备为准。

1. 进入 *配置* → *网络* → *高级配置* → *视图库* 。
2. 设置平台接入参数。
3. 单击*保存*。

• 配置报警服务器

设备通过 HTTP、HTTPS 或 ISUP 协议的方式发送报警信息给目的 IP 或域名。

操作步骤

说明

报警服务器配置视型号而定，请以实际设备为准。

4 进入 *配置* → *网络* → *高级配置* → *报警主机配置* 。
5 输入**目的 IP** 或**域名**、**URL 地址**和**端口**。

说明

目的 IP 地址或域名需支持 HTTP、HTTPS 或 ISUP 协议传输。

6 单击*测试*。

说明

单击***重置***，可重新设置目的 IP 地址或域名的信息。

7 单击*保存*。

• TCP 加速

启用 TCP 加速，可解决在网络不稳定或网络带宽不佳的环境下产生丢包、延时等网络延迟和网络阻塞问题，保证图像预览时的流畅性。

• 流量整形

启用流量整形，可使传输码流趋于平滑，视频数据以相对均匀的速率传输，以解决瞬时带宽过大导致网络拥塞造成的数据丢失和延迟等问题，保证图像预览时的流畅性。

整形系数可选择**高**、**中**、**低**三个等级，建议您根据实际网络情况选择。

说明

75. 流量整形功能仅在协议类型为 **TCP** 或 **UDP** 时生效。前往 *配置 → 本地 → 播放参数* 可设置协议类型。

76. 该功能请以实际设备为准。

• SRTP

SRTP 为安全实时传输协议，通过选择服务端证书和加密算法可有效防止远程管理过程中的信息泄露问题。

操作步骤

1. 进入 *配置 → 网络 → 高级配置 → SRTP* 。

2. 选择**服务端证书**。

说明

通过 *配置 → 系统 → 安全管理 → 证书管理* 可安装和查看设备各类证书。

3. 选择**加密算法**。

4. 单击*保存*。

第 10 章 计划和联动配置

设备在设置的时间段内执行对应的操作，如：录像、抓图和布防。通过联动使设备执行相应的动作。

- 布防时间配置

设置任务执行的开始时间和结束时间。

操作步骤

1. 选中时间轴上的某点为起始点，按住鼠标左键在时间轴上拖动，拖动到结束点时松开鼠标，完成布防时间设置。

说明

一条时间轴上支持设置 8 个时间段。

2. 调整布防时间。

- 单击布防时间段，可手动输入开始时间和结束时间调整布防时间，单击*保存*。
- 单击布防时间段，时间段两端会显示两个圆圈，鼠标移动到时间段的两端，会显示左右方向的调节箭头，移动调节箭头可调整时间段。
- 鼠标拖动布防时间段到时间轴上的任一位置，可以重设时间段。

单击时间段的*删除* 删除当前时间段。

单击*删除* 删除选中的时间段。

单击*删除全部* 删除设置的所有时间段。

3. 可选操作: 单击时间轴右侧出现的 ，复制相同的布防时间到其它时间。

4. 单击*保存*。

- 联动配置

当有事件或报警发生时可开启报警联动。

说明

设备支持的联动方式视型号而定，请以实际设备为准。

- **联动录像**

勾选并配置好对应通道的录像，当触发报警时，可联动通道进行录像。配置方法请参见 *录像和抓图*。

- **联动上传中心**

勾选*上传中心*，当发生报警时，可将报警信息、图片等信息上传到远程的监控中心。

- **联动 FTP/NAS/SD 卡**

若勾选并配置好 FTP/NAS/SD 卡，当触发报警时，可将报警信息发送到 FTP 服务器、网络硬盘或 SD 卡中进行保存。

配置 FTP 服务器存储，请参见 *配置 FTP* 。

配置 NAS 存储，请参见 *配置网络硬盘* 。

配置 SD 卡存储，请参见 *设置存储卡* 。

- **联动 Email**

勾选并配置好邮件联动，当触发报警时，设备将报警信息发送至配置好的邮箱中。邮件配置请参见 *配置 Email* 。

配置 Email

若设置了 Email 参数，当有报警发生时，设备会将设备通道名称、事件类型、事件日期时间、设备类型、设备序列号等详细信息发送到指定的邮箱。

操作步骤

1. 进入 *配置 → 网络 → 高级配置 → Email 参数* 。

2. 设置 Email 参数。

- 填写发件人的邮箱信息，包括发件人邮箱对应的 **SMTP 服务器**和 **SMTP 端口**。
- 设置邮件加密。
  - 当邮件加密选择 SSL 或 TLS，不勾选*启用 STARTTLS* 时，邮件发送将经过 SSL 或 TLS 加密后发送，此时 SMTP 端口号需更改为 *465*。
  - 当邮件加密选择 SSL 或 TLS，勾选*启用 STARTTLS* 时，表示邮件通过 STARTTLS 加密发送，此时 SMTP 端口号需更改为 *25*。

- **可选操作:** 勾选*图片附件*，邮件中将附带即时抓图三张，根据实际需求设置抓图时间间隔。
- 勾选*服务器认证*，填写发件人邮箱对应的**用户名**和**密码**。
- 填写收件人邮箱信息，包括收件人名称及邮箱地址。

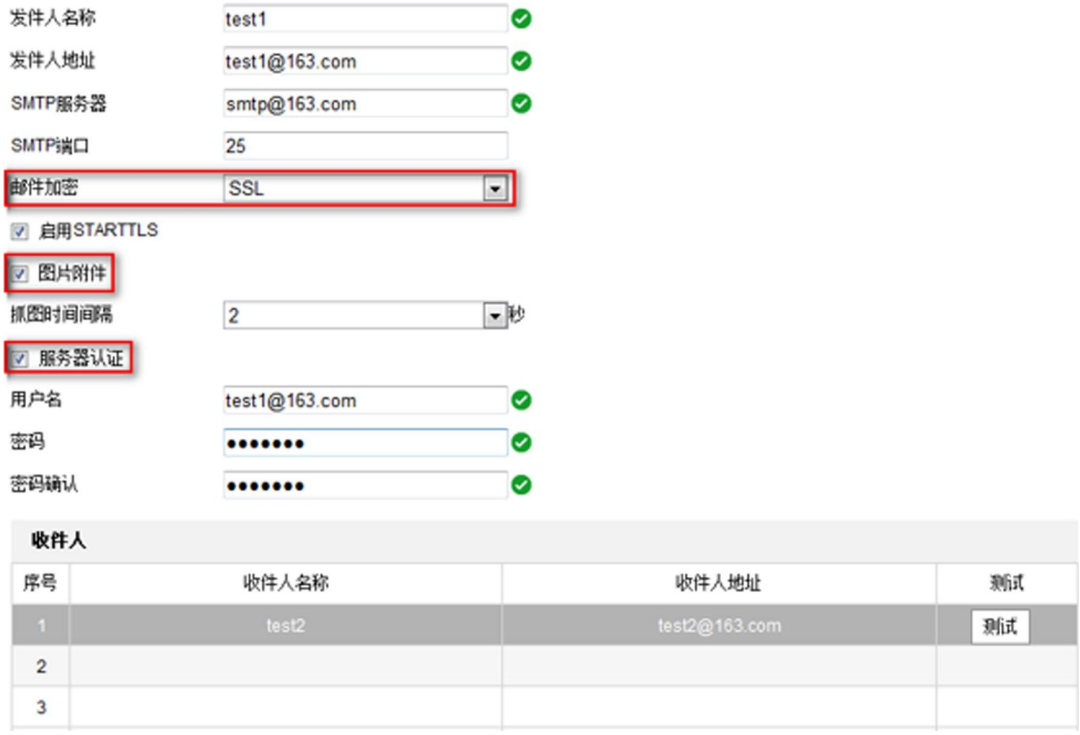


图 10-1 配置邮件

3. 单击*测试*，确认所输入的收件人地址是否正确。

4. 单击*保存*。

• 联动报警输出

设备的报警输出接口中连接了报警输出设备，勾选且配置好对应的报警输出通道，当触发报警时，报警信息将从连接的报警输出设备中输出。

操作步骤

说明

报警输出视型号而定，请以实际设备为准。

1. 进入 *配置 → 事件 → 普通事件 → 报警输出* 。

2. 设置报警参数。

自动报警输出　设置方法请参见 *自动报警* 。

手动报警输出　设置方法请参见 *手动报警* 。

3. 单击*保存*。

自动报警

若需在设置的布防时间内触发报警输出，请配置自动报警。

操作步骤

1. 设置自动报警参数。

报警输出号

根据外接报警设备连接的报警接口选择报警输出号。

延时

表示产生报警后，延长多长时间关闭报警，请根据实际需求进行选择。

说明

当选择为*手动*，当产生报警后，请单击*手动报警*和*清除报警*，关闭报警。

报警名称

自定义报警名称。

2. 设置布防时间，具体设置请参考 *布防时间配置* 。

3. 单击时间轴右侧出现的，设置其他报警输出通道的报警参数一致。

4. 单击*确定*。

手动报警

通过手动触发报警输出。

操作步骤

3 设置手动报警参数。

报警输出号

根据外接报警设备连接的报警接口选择报警输出号。

报警名称

自定义报警名称。

4 单击*手动报警*，开启手动触发报警输出。

说明

单击*清除报警*，关闭手动报警的报警输出。

- **配置闪光报警灯输出**

配置设备闪光报警灯的参数，在事件触发时，可联动设备上的闪光灯进行警示，该功能请以实际设备为准。

操作步骤

- 进入 *配置 → 事件 → 普通事件 → 闪光报警灯输出* 。
- 根据使用需求，设置闪光灯的**闪烁时间**，**闪烁频率**和**亮度**。
- 设置布防时间请参见 *布防时间配置* 。
- 单击*保存*。

后续处理

进入事件（部分类型）**联动方式**界面，勾选*闪光报警*。

- **配置声音报警输出**

当设备检测到警戒区域出现目标时，可通过设置警戒声音进行提醒，该功能请以实际设备为准。

操作步骤

- 进入 *配置 → 事件 → 普通事件 → 声音报警输出* 。
- 选择**音频类型**，并设置其参数。
  - 选择为提示音，按实际需求设置**外放音量**和**报警次数**。
  - 选择为警戒音，按实际需求选择**警戒音类型**并设置**外放音量**和**报警次数**。
  - 选择为自定义语音，支持添加、下载符合要求的自定义音频文件，并可设置**外放音量**和**报警次数**。

说明

设备音频类型视型号而定，请以实际设备为准。

- **可选操作**: 单击*测试*，设备播放选择的音频。
- 布防时间设置请参见 *布防时间配置* 。
- 单击*保存*。

后续处理

进入事件（部分类型）**联动方式**界面，勾选*声音联动*。

第 11 章 系统和安全参数

介绍设备的系统维护、系统配置及安全管理等参数及相关参数设置。

• 查看设备信息

用于查看设备编号、设备型号、序列号和版本等设备信息。

通过 *配置 → 系统 → 系统设置 → 基本信息*，查看设备信息。

说明

设备名称和编号可根据需求自定义。

• 重启设备

介绍设备重启的操作。

通过 *配置 → 系统 → 系统维护 → 升级维护*，单击*重启*。

• 恢复设备参数

介绍设备执行恢复默认参数的操作。

操作步骤

1. 进入 *配置 → 系统 → 系统维护 → 升级维护* 。

2. 根据实际需求单击*简单恢复*或*完全恢复*。

简单恢复 除用户信息、网络参数和视频制式等外，其他参数恢复至出厂状态，请谨慎使用。

完全恢复 恢复设备的所有全部参数至出厂状态，请谨慎使用。

• 导入/导出配置参数

通过导入/导出设备的配置文件，获取设备的配置参数，方便用户对其它设备进行相同参数的配置。

导入配置参数

通过 *配置 → 系统 → 系统维护 → 升级维护*，选择参数导入中的设备参数，根据界面提示操作完成导入设备的配置参数。

导出配置参数

通过 *配置 → 系统 → 系统维护 → 升级维护*，选择信息导出中的设备参数，根据界面提示操作完成导出设备的配置参数。

• 导出诊断信息

介绍导出设备运行状态的诊断信息。诊断信息包括 3 个模块，分别为软件状态信息、硬件运行信息和启动日志信息。

通过 *配置 → 系统 → 系统维护 → 升级维护*，根据实际情况勾选诊断信息模块并单击*导出诊断信息*，导出设备诊断信息。

• 升级设备

介绍设备执行升级的操作。

前提条件

获取正确的升级包，并存放在计算机中。

注意

设备升级过程中请勿关闭电源，升级完成后设备会自动重启。

操作步骤

1. 进入 *配置 → 系统 → 系统维护 → 升级维护*。

2. 选择升级方法。

- 当明确知道升级文件存放的路径时，选择升级文件，单击*浏览*选择升级文件。
- 当文件夹中包含多种升级包时，选择升级目录，单击*浏览*选择升级文件存放的目录，设 备将自动分辨目录下正确的升级文件。

3. 单击*升级*。

• 查询和导出日志

当系统发生未知故障时，可通过参考日志及时定位和排查问题。

操作步骤

1. 进入 *配置 → 系统 → 系统维护 → 日志*。

2. 选择**日志类型**、**开始时间**和**结束时间**。
3. 单击*查找*。
日志列表中显示符合查询条件的所有日志信息。
4. 单击*导出*，可将日志保存到计算机上。

• 查看开源码授权信息

用于查看设备开源码授权信息。

进入 *配置* → *系统* → *系统设置* → *关于设备*，单击*查看*。

• 设置时间

通过设置时区、校时和夏令时的方式设置设备时间。

• 设置 NTP 校时

若需要使用准确且可靠的时间源进行校时，可使用 NTP 校时。

前提条件

请先搭建或获取 NTP 服务器信息。

操作步骤

2 进入 *配置* → *系统* → *系统设置* → *时间配置* 。
3 选择**时区**。
4 单击 *NTP 校时*。
5 填写**服务器地址**、**NTP 端口**和**校时时间间隔**。

说明

服务器地址为 NTP 服务器的 IP 地址或域名。

6 单击*测试*，判断设备与 NTP 服务器之间正常连接。
7 单击*保存*。

• 手动校时

用于手动设置设备时间。

操作步骤

1 进入 *配置* → *系统* → *系统设置* → *时间配置*
2 选择**时区**。

3 单击*手动校时*。
4 选择校时方式。

4.1 选择**设置时间**，手动输入或选择日历设置设备时间。

4.2 勾选*与计算机时间同步*，保持设备与本地计算机的时间一致。

5 单击*保存*。

• 设置夏令时

若设备所处地区实行夏令时制，可通过配置夏令时，将设备与当地时间保持同步。该功能请以实际设备为准。

操作步骤

11进入 *配置 → 系统 → 系统设置 → 夏令时* 。
12勾选*启用夏令时*。
13根据设备所处地区夏令时制选择**开始时间**、**结束时间**和**偏移时间**。
14单击*保存*。

说明

夏令时功能视型号而定，请以实际设备为准。

• 设置 RS-485 参数

RS-485 可用于接入控制信号。

前提条件

使用 RS-485 线缆，连接设备和计算机或终端。

操作步骤

11进入 *配置 → 系统 → 系统设置 → RS-485* 。
12根据使用需求设置 RS-485 参数，请保持设备和计算机或终端的参数一致。
13单击*保存*。

说明

RS-485 功能视型号而定，请以实际设备为准。

• 设置 RS-232 参数

RS-232 可用于调试设备。

前提条件

使用 RS-232 线缆连接设备和计算机或终端。

操作步骤

说明

该功能请以实际设备为准。

11进入 *配置 → 系统 → 系统设置 → RS-232* 。
12设置 RS-232 参数，保持设备和计算机或终端的匹配。
13单击*保存*。

• 功耗模式切换

用于切换设备使用时的功耗。

说明

功耗模式视型号而定，请以实际设备为准。

通过 *配置 → 系统 → 系统设置 → 功耗模式* ，选择所需的功耗模式。

气云成像工作时间统计

用于显示气云成像机芯持续累计的工作时间。

定时休眠

可根据需求设置休眠时间，气云成像机芯将在设置的时间开启休眠状态。休眠时，设备不再进行 VOCs 气体检测任务。

说明

10定时休眠时间配置请参见 *布防时间配置* 。
11 当气云成像机芯处于休眠状态时，预览界面单击 可以手动唤醒设备。若设备休眠时间段内被手动唤醒，不执行 VOCs 气体检测任务。

• 安全配置

介绍设备安全相关的参数设置，可以提高系统的安全性。

• 安全使用建议

目前，接入网络的系统面临日趋严重的网络安全威胁，出现问题后，将可能造成业务中断，甚至造成设备或者系统崩溃。安全威胁日益严重且多样化，完全依赖技术很难保证系统的整体安全，因此除了设备本身需要具备的安全防御体系外，建议您根据安全使用建议和日常发现的问题，建立网络安全管理的制度，来保证系统安全、正常的运行。

77. 安全审计日志将会记录安全操作相关的日志。通过查询和分析设备内置存储中的安全日志，可排查非法入侵和安全事件引起的故障。由于存储空间有限，建议您设置日志服务器，将安全日志上传至日志服务器存储。

78. 网络访问中，HTTPS 协议通过身份认证和加密通讯，可建立安全、加密的数据传输，提高网络访问和数据传输的安全性。建议您设置 HTTPS，并使用 HTTPS 方式访问设备。

说明

启用 HTTPS 后，设备性能可能会降低 20%~40%左右。

79. SDK 监听目前不支持加密，布防方式支持加密，这个如果使用 SDK 协议来传输报警信息，建议您启用增强型 SDK 服务，通过 SDK over TLS 协议接入设备，并使用布防方式接收报警信息。

• 设置认证方式

设置 RTSP 认证和 WEB 认证，可提高网络访问的安全性。

通过 *配置 → 系统 → 安全管理 → 认证方式*，选择所需认证协议和认证方式。

RTSP 认证

支持 digest 和 digest/basic 认证方式，表示向设备发送 RTSP 请求时需要携带认证信息，如果选择 *digest/basic* 认证方式，表示支持 digest 或 basic 认证，选择 *digest* 认证方式时，表示只支持 digest 认证。

RTSP 摘要算法

进行 RTSP 认证时，支持 MD5、SHA256 和 MD5/SHA256 加密算法。启用 MD5 之外的摘要算法后，第三方平台由于兼容性问题可能无法登录设备或预览。请考虑实际场景选择算法类型，建议优先采用高强度的加密算法。

WEB 认证

支持 digest 和 digest/basic 认证方式，表示向设备发送 WEB 请求时需要携带认证信息，如果选择 *digest/basic* 认证方式，表示支持 digest 或 basic 认证，选择 *digest* 认证方式时，表示只支持 digest 认证。

WEB 摘要算法

进行 WEB 认证时，支持 MD5、SHA256 和 MD5/SHA256 加密算法。启用 MD5 之外的摘要算法后，第三方平台由于兼容性问题可能无法登录设备或预览。请考虑实际场景选择算法类型，建议优先采用高强度的加密算法。

说明

协议要求携带的认证信息请参看具体协议内容。

• 设置 IP 地址过滤

用于设置计算机或终端访问设备的权限。

IP 地址均指 IPv4 地址。

操作步骤

9 单击 *配置 → 系统 → 安全管理 → IP 地址过滤* 。

10勾选**启用 IP 地址过滤**。

11设置 IP 地址过滤方式。

禁止 除列表中的 IP 地址或 IP 段外，其它 IP 地址或 IP 段允许访问设备。

允许 只允许在列表中的 IP 地址或 IP 段访问设备。

12单击*添加*，输入 IP 地址或 IP 段。

单击*修改* 修改列表中所选的 IP 地址或 IP 段。

单击*删除* 删除列表中所选的 IP 地址或 IP 段。

13单击*保存*。

• 设置 MAC 地址过滤

通过 MAC 地址设置计算机或终端访问设备的权限。

操作步骤

9 单击 *配置 → 系统 → 安全管理 → MAC 地址过滤* 。

10勾选**启用 MAC 地址过滤**。

11设置 MAC 地址过滤方式。

禁止 除列表中的 MAC 地址外，其它 MAC 地址允许访问设备。

允许 只允许在列表中的 MAC 地址访问设备。

12单击*添加*，输入 MAC 地址。

单击*修改* 修改列表中所选的 MAC 地址。

单击*删除* 删除列表中所选的 MAC 地址。

13单击*保存*。

- **SSH**

建立在应用层基础上的安全协议，启用后可有效防止远程管理过程中的信息泄露问题。

单击 *配置 → 系统 → 安全管理 → 安全服务* 可控制*启用 SSH*。

- **开启账户锁定**

用于提升设备网络访问的安全性。

admin 用户可以设置密码错误尝试次数和锁定时间。当密码输入错误达到限定的次数，设备将自动锁定。达到设置的锁定时间后，设备自动解锁。

通过 *配置 → 系统 → 安全管理 → 安全服务*，勾选*开启非法登录锁定*，设置**错误尝试次数**和**锁定时间**。

- **控件超时配置**

通过浏览器操作设备时，在设定的时间范围内，如果没有对设备进行任何操作（不包括查看实时图像），设备将自动注销，需重新登录。

通过 *配置 → 系统 → 安全管理 → 高级安全*，勾选*启用控件超时*，设置**超时时间**，单击*保存*。

- **证书管理**

用于创建、集中管理设备所有证书。

服务器/客户端证书

说明

设备含默认安装的自签名证书，证书 ID 为 *default*。

创建自签名证书

操作步骤

8 进入 *配置* → *系统* → *安全管理* → *证书管理* 。

9 单击*创建自签名证书*。

10设置证书信息。

说明

证书 ID 须唯一不可重复。

11单击*确定*。

服务器端/客户端证书列表显示当前创建的自签名证书。

使用功能列可查看所有通过当前证书进行身份校验的协议类型。

12**可选操作**: 单击*证书属性*，查看证书更多属性，如证书颁发机构等。

创建证书请求和安装证书

介绍如果对网络访问安全要求高，通过 HTTPS 协议创建并安装带认证的证书，可以保证传输数据的安全性。

操作步骤

8 勾选*先创建证书请求，再继续安装*。

9 单击*创建*。

10根据界面提示，填写**国家**、**域名/IP**、**有效期**等申请参数。

11单击*确定*。

12导入证书。

12.8 当收到签署的有效证书后，选择*证书请求下载*，在**安装生成的证书**中安装下载来的安全 证书。

12.9 如果有已签名证书，勾选*已有已签名证书，直接安装*，在**安装生成的证书**中安装已签名

证书。

13单击*保存*。

安装第三方机构签名证书

用于导入由第三方机构进行认证的签名证书。

前提条件

已获取第三方机构签名证书。

操作步骤

8 进入 *配置 → 系统 → 安全管理 → 证书管理* 。

9 单击*导入*。

10设置证书 ID。

说明

证书 ID 须唯一不可重复。

11单击*浏览*，根据本地路径选择待导入的证书。

12选择*证书和密钥*导入方式。

独立私钥 适用于证书密钥存储在独立私钥文件的情况。

单击*浏览*，根据本地路径选择待导入的证书文件和私钥文件并输入**私钥密码**。

PKCS#12 适用于证书密钥和证书为同一个文件的情况 。此时输入**密码**即可。

13单击*确定*。

服务器端/客户端证书列表显示当前导入的证书。

使用功能列可查看所有通过当前证书进行身份校验的协议类型。

安装 CA 证书

用于导入由权威证书签证机关（CA）颁发的证书（一般权威的 CA 组织需要收费），提高访问的安全等级。

前提条件

已获取 CA 证书。

操作步骤

7 进入 *配置 → 系统 → 安全管理 → 证书管理* 。

8 单击*导入*，根据本地路径选择待导入的 CA 证书。

9 单击*确定*。

CA 证书列表显示当前导入的证书。

使用功能列可查看所有通过当前证书进行身份校验的协议类型。

证书过期报警

用于管理和监测设备证书的有效期，当发现证书有效期异常将进行联动报警。

通过 *配置 → 系统 → 安全管理 → 证书管理* ，设置相关参数。

启用证书报警

表示开启设备对证书有效期的管理和监测。

过期前提醒

设置证书过期前几天进行报警提醒。例如：证书过期前提醒日期设置为 2 天，则设备将按照证书有效截止时间前 2 天开始提醒。

报警频率

设置证书有效期异常后，触发报警的频率。

报警检测时间

设置设备每日对证书有效期的检测时间，当检测到证书有效期异常将立即进行联动报警。

• 设置 HTTPS

网络访问中，要提高浏览器访问的安全性，可通过 HTTPS 协议构建安全、加密的网络传输，通过身份认证和加密通讯，保证传输数据的安全性。

操作步骤

5 进入 *配置 → 网络 → 高级配置 → HTTPS* 。

6 勾选*启用*，通过 HTTPS 协议访问设备。

7 **可选操作**: 勾选*自动跳转 HTTPS*，可将输入的 IP 地址自动转换成 HTTPS 地址，提升网络安全性。

8 选择**服务端证书**。

说明

通过 *配置 → 系统 → 安全管理 → 证书管理* 可查看设备各类证书。

9 单击*保存*。

• 设置 QoS

通过配置 QoS 参数，可有效解决网络延迟和网络阻塞问题。

说明

QoS 功能需要传输路径上的网络设备（如路由器、交换机等）支持。

操作步骤

4 进入 *配置 → 网络 → 高级配置 → QoS* 。

5 根据 QoS 分类标准，设置**视/音频 DSCP**、**报警 DSCP** 和**管理 DSCP** 参数。

说明

网络可根据 DSCP 权值来判断数据传输的优先级。DSCP 值越大，优先级越高，配置时需要在路由器端设置相同的值。

6 单击*保存*。

• 设置 IEEE 802.1X

通过配置 802.1X 协议可实现对连接设备的用户权限认证。进

入 *配置 → 网络 → 高级配置 → 802.1x* ，启用 IEEE 802.1X。根

据路由器信息选择认证协议和版本。

80. 选择 EAP-MD5 或 EAP-LEAP 协议时，选择 EAPOL 版本，填写用户名、密码和密码确认，用

户名和密码即连接设备的用户名和密码。

81. 选择 EAP-TLS 协议时，设置身份，选择 EAPOL 版本、客户端证书和 CA 证书。

• SRTP

SRTP 为安全实时传输协议，通过选择服务端证书和加密算法可有效防止远程管理过程中的信息泄露问题。

操作步骤

3 进入 *配置 → 网络 → 高级配置 → SRTP* 。

4 选择**服务端证书**。

说明

通过 *配置 → 系统 → 安全管理 → 证书管理* 可安装和查看设备各类证书。

5 选择**加密算法**。

6 单击*保存*。

• 安全审计日志

安全审计日志是指安全操作相关的日志。通过查询和分析设备内置存储中的安全日志，可排查非法入侵和安全事件引起的故障。由于存储空间有限，建议您设置日志服务器，将安全日志上传至日志服务器存储。

说明

安全审计日志功能视型号而定，请以实际设备为准。

查询安全审计日志

用于查询和管理设备的安全日志。

操作步骤

2 进入 *配置 → 系统 → 系统维护 → 安全审计日志* 。

3 设置日志类型、**开始时间**和**结束时间**。

4 单击*查找*。

日志列表中显示符合查询条件的所有日志信息。

5 **可选操作**: 单击*导出*，可将日志保存到计算机上。

配置安全审计日志服务器

用于将安全日志上传并存储至日志服务器。

前提条件

82. 已获取到日志服务器的 IP 地址和端口。

83. 设备已安装客户端证书或 CA 证书。通过 *配置 → 系统 → 安全管理 → 证书管理* 可查看设备各类证书。

84. 若日志服务器端配置为双向认证，设备需同时选择客户端证书和 CA 证书；若日志服务器端配置为单向认证，则设备需只需选择 CA 证书。

操作步骤

1 进入 *配置 → 系统 → 系统维护 → 安全审计日志* 。

2 设置日志上传服务器。

2.1 勾选*启用日志上传服务器*。

2.2 勾选*启用传输加密*，设备发往服务器的日志将会进行加密传输。

说明

设备未选择客户端证书和 CA 证书时，加密传输不生效。

2.3 设置日志服务器参数

。**日志服务器地址**

需要存储日志的服务器地址，如 IP 地址。

日志服务器端口

日志服务器的数据端口。

2.4 **可选操作**: 选择**客户端证书**。

2.5 选择 **CA 证书**。

2.6 单击*测试*，测试设备和服务器连接状态。

测试成功表示设备能够正常连接到日志服务器。

3 单击*保存*。

结果说明

设备将定时上传安全审计日志到日志服务器。

说明

功能视型号而定，请以实际界面为准。

• 管理设备用户

• 设置用户账户和权限

介绍设备用户添加、修改、删除和用户权限分配。

注意

为了提高产品网络使用的安全性，请您定期更改用户名的密码，建议每 3 个月进行 1 次更新维护。如果设备在较高安全风险的环境中使用，建议每月或每周进行 1 次更新。

操作步骤

- 进入 *配置 → 系统 → 用户管理 → 用户管理* 。
- 单击*添加*，设置**用户名**，**用户类型**和**密码**，根据使用需求分配用户远程权限。 **管理员**

  管理员拥有一切操作权限，可以添加普通用户和操作员，并对添加的用户分配权限。

  普通用户

  只能查看实况、配置云台参数和修改自己的密码，无其他操作权限。

  操作员

  拥有除对管理员的操作权限，无创建用户的权限。

  选择用户，单击*修改* 修改所选用户的密码、权限等信息。

  选择用户，单击*删除* 删除所选用户。

说明

- 管理员最多可创建 31 个用户。
- 密码长度小于 8 位、密码只包含一类字符，密码与用户名相同，密码是用户名的倒转输入，密码包含用户名，密码包含倒转输入的用户名，以上几类密码属于风险密码，为更好保护您的隐私并提升产品安全性，建议您将风险密码更改为高强度密码。
- 密码强度规则如下：

- 强密码：包含三种或三种以上类型（如数字、小写字母、大写字母、特殊字符）组合的密码。
- 中密码：由数字和特殊字符、小写字母和特殊字符、大写字母和特殊字符、小写字母和大写字母组合的密码。
- 弱密码：由数字和小写字母组合、数字和大写字母组合的密码。

- 单击*确定*。

• 密码强度提示

为了提高产品网络使用的安全性，设置网络摄像机密码时，密码长度需达到 8-16 位，且至少由数字、小写字母、大写字母和特殊字符中的 2 种或 2 种以上类型组合而成。

⚠注意

为更好保护您的隐私并提升产品安全性，建议您使用高强度密码。

高强度密码

密码包含数字、小写字母、大写字母、特殊字符类型中的 3 种或 3 种以上。

中强度密码

密码为数字和特殊字符组合，小写字母和特殊字符组合，大写字母和特殊字符组合，小写字母和大写字母组合。

弱密码

密码为数字和小写字母组合，数字和大写字母组合。

风险密码

密码长度小于 8 位，密码只包含数字、小写字母、大写字母、特殊字符中的 1 类，密码与用户名一样或密码为用户名的倒写。

• 查看在线用户

用于显示网络中登录到设备上的用户列表。

通过 *配置 → 系统 → 用户管理 → 在线用户*，查看访问过设备的用户列表。

• 设置 Web 同时登录数

通过浏览器同时登录设备的数量，管理员（admin）用户支持功能设置。

通过 *配置 → 系统 → 用户管理*，单击*通用参数*，设置 **Web 同时登录数**，单击*保存*。

公司地址： 浙江省湖州市高新区欣安路199号49幢
公司电话： 4008-180-2180
公司网址：WWW.HIOTSE.COM