



网络硬盘录像机

FAQ










前言

本文档主要针对实际使用环境中遇到的常见设备故障、参数设置疑问、使用误区等问题提供解决思路及操作指导。

本文档中的描述内容需要结合实际现场设备具体分析，并不作为唯一的处理方式，如有疑问请联系相关技术支持代表。

符号约定

在本文档中可能出现下列标识，代表的含义如下。

标识	说明
 危险	表示有高度潜在危险，如果不能避免，会导致人员伤亡或严重伤害。
 警告	表示有中度或低度潜在危险，如果不能避免，可能导致人员轻微或中等伤害。
 注意	表示有潜在风险，如果忽视这些文本，可能导致设备损坏、数据丢失、设备性能降低或不可预知的结果。
 防静电	表示静电敏感的设备。
 当心触电	表示高压危险。
 激光辐射	表示强激光辐射。
 风扇警告	表示危险运动部件，请远离运动风扇叶片。
 当心机械伤人	表示设备部件机械伤人。
 窍门	表示能帮助您解决某个问题或节省您的时间。
 说明	表示是正文的附加信息，是对正文的强调和补充。

写作约定

- 本文档中的界面截图仅供参考，不同设备的界面不一致，请以实际为准。
- 如无特殊说明，本文档中出现的“设备”、“NVR”等均指“网络硬盘录像机”。
- 为保障个人隐私安全，本文档中出现的人脸、车牌等个人信息均已做过处理。
- 为保证设备安全，本文档中出现的 IP 地址、MAC 地址、序列号等信息均已做过处理。

修订记录

版本号	修订内容	发布日期
V1.0.0	首次发布。	2020.11

使用安全须知

下面是关于产品的正确使用方法、为预防危险、防止财产受到损失等内容，使用设备前请仔细阅读本说明书并在使用时严格遵守，阅读后请妥善保存说明书。

使用要求

- 请勿将设备放置和安装在阳光直射的地方或发热设备附近。
- 请勿将设备安装在潮湿、有灰尘或煤烟的场所。
- 请保持设备的水平安装，或将设备安装在稳定场所，注意防止本产品坠落。
- 请勿将液体滴到或溅到设备上，并确保设备上没有放置装满液体的物品，防止液体流入设备。
- 请将设备安装在通风良好的场所，切勿堵塞设备的通风口。
- 仅可在额定输入输出范围内使用设备。
- 请勿随意拆卸设备。
- 请在允许的湿度和温度范围内运输、使用和存储设备。

电源要求

- 请务必按照要求使用电池，否则可能导致电池起火、爆炸或燃烧的危险！
- 更换电池时只能使用同样类型的电池！
- 产品必须使用本地区推荐使用的电线组件（电源线），并在其额定规格内使用！
- 请务必使用设备标配的电源适配器，否则引起的人员伤害或设备损害由使用方自己承担。
- 请使用满足 SELV（安全超低电压）要求的电源，并按照 IEC60950-1 符合 Limited Power Source（受限制电源）的额定电压供电，具体供电要求以设备标签为准。
- 请将 I 类结构的产品连接到带保护接地连接的电网电源输出插座上。
- 器具耦合器为断开装置，正常使用时请保持方便操作的角度。

目录

前言	I
使用安全须知	II
第 1 章 录像类问题	1
1.1 本地回放录像时出现花屏	1
1.2 无法播放下载的录像文件	2
1.3 第三方平台查询录像失败	2
1.4 查询录像断断续续	3
1.5 本地回放无法查询到录像	3
1.6 预览画面及回放录像时出现马赛克	6
第 2 章 音频对讲类	8
2.1 设备连接音频拾音器时，没有声音	8
2.2 拾音器有很大的噪声或音质较差	9
2.3 如何选择拾音器安装位置	9
2.4 连接拾音器的注意事项	9
2.5 拾音器产生发闷、裂化声音	10
第 3 章 对接类问题	11
3.1 设备无法添加网络摄像机	11
3.2 设备数字通道无法连接 IPC，或者连接后总掉线	13
3.3 单画面显示正常，多分割无画面	15
3.4 多画面显示正常，单分割无画面	16
3.5 如何通过设备修改 IPC 的 IP 地址	18
3.6 通过 ONVIF 协议或私有协议接入第三方 IPC 问题	19
第 4 章 智能类问题	20
4.1 智能检测功能如何初始化检测的基准画面	20
4.2 人脸检测没有报警	20
4.3 徘徊检测容易产生误报	21
4.4 通用行为分析功能没有报警	23
4.5 区域入侵中的区域内检测和徘徊检测的区别	23
4.6 智能重建背景的目的是什么	23
第 5 章 网络类问题	24
5.1 WEB 无法访问设备，系统提示登录失败	24
5.2 国标 28181 协议接入第三方平台后，预览、回放卡顿	26
5.3 修改密码时发生密码锁定	28
5.4 如何重置设备登录密码	28
第 6 章 外接设备类	31
6.1 如何接入报警设备	31
6.2 设备外接报警感应器，重启感应器时会触发本地报警	31
6.3 本地界面操作，鼠标移动缓慢	32
6.4 VGA 和 HDMI 简介	33
6.5 显示器或显示异常黑屏	33
第 7 章 其他类问题	34

7.1 HDMI/VGA 异源输出简介	34
7.2 如果通过 U 盘手动升级.....	34
7.3 如何使用 ConfigTool 工具升级.....	35
附录 1 法律声明.....	36
附录 2 网络安全声明和建议.....	38

第 1 章 录像类问题

1.1 本地回放录像时出现花屏

现象描述

登录设备的本地界面，回放录像时出现花屏。

可能原因

- 画质设置太低。
- 硬盘数据线和硬盘跳线错误。
- 硬盘故障。

解决方法

步骤1 降低画质的值。

1. 使用鼠标、键盘、显示器直连设备，开启设备。
2. 登录设备的本地界面，在预览界面右键选择“主菜单”。
3. 在主菜单界面，选择“相机设置 > 编码设置 > 抓图设置”。
4. 修改“图片质量”，单击“应用”。

图1-1 图片码流



5. 检查问题是否已经解决。
如果已解决，则完成问题处理，否则请继续执行以下步骤。

步骤2 检查硬盘的数据线和电源线跳线连接。

如果连接错误，请重新连接，否则请继续执行以下步骤。

步骤3 检查硬盘是否故障。

1. 使用鼠标、键盘、显示器直连设备，开启设备。
2. 登录设备的本地界面，在预览界面右键选择“主菜单”。
3. 在主菜单界面，选择“存储管理 > 硬盘管理”。
4. 检查硬盘状态是否正常。

如果硬盘异常，请修复硬盘或更换硬盘，否则请联系相关技术支持。

图1-2 硬盘管理



1.2 无法播放下载的录像文件

下载 DAV 格式录像文件时，需要使用大华播放器。

1.3 第三方平台查询录像失败

现象描述

在第三方平台添加设备后，查询设备的录像失败。

可能原因

平台查询方式或查询时间错误。

解决方法

- 步骤1 修改平台的录像查询方式（例如文件查询，按时间查询）、录像查询时间（例如查询 1 小时、1 天等）。
- 步骤2 检查问题是否已经解决。
如果已解决，则完成问题处理，否则请联系相关技术支持。

1.4 查询录像断断续续

根据录像的断续时间，确认录像断续原因。

- 如果录像断续 1 分钟~2 分钟，可能是设备正常重启导致(包括设备自动维护、人为重启等)。
- 如果录像断续几秒到几分钟，可能是校时问题，设备是否开启 NTP、平台校时等。
- 如果录像断续 4 分钟左右，可能是设备异常重启导致设备出现异常，检查设备程序。
- 如果录像断续 10 分钟、1 小时、几天等录像，可能是设备处于断电状态，或者硬盘出现错误、坏道情况。

根据可能原因完成问题的排查，如果问题还未解决，请联系相关技术支持。

1.5 本地回放无法查询到录像

现象描述

登录设备的本地界面查询录像，无法查询到录像。

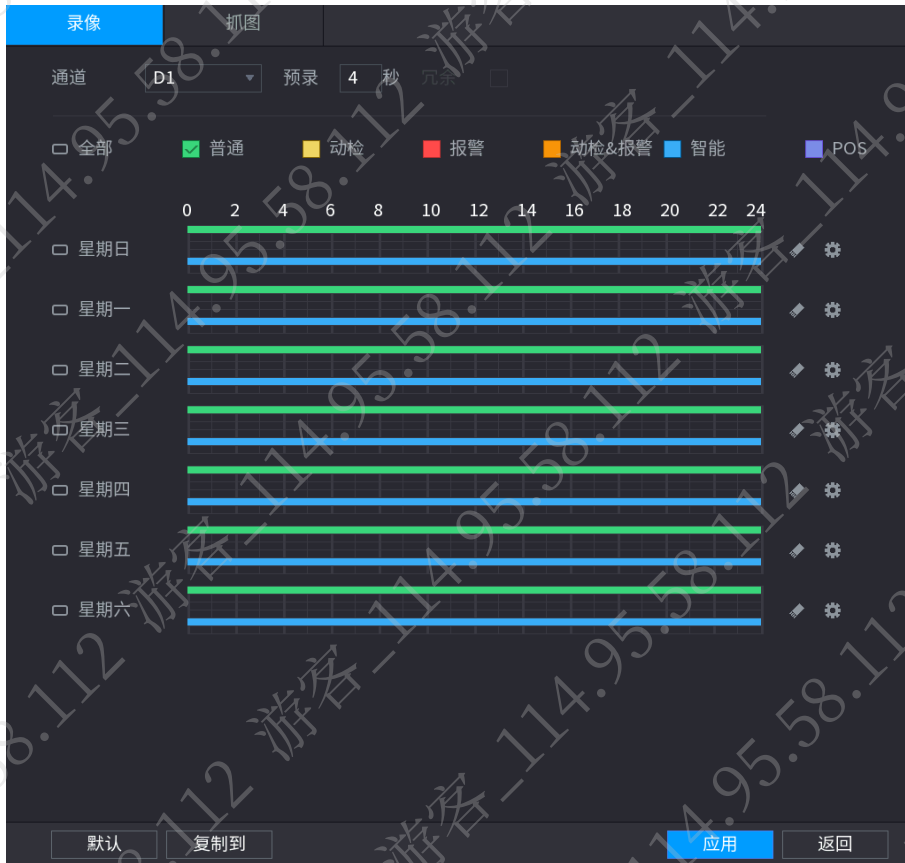
可能原因

- 未开启录像功能。
- 硬盘数据线或跳线错误。
- 硬盘故障。
- 系统版本错误。

解决方法

- 步骤1 检查是否已开启录像。
1. 使用鼠标、键盘、显示器直连设备，开启设备。
 2. 登录设备的本地界面，在预览界面右键选择“主菜单”。
 3. 在主菜单界面，选择“存储管理 > 录制计划 > 录像”。
 4. 检查是否已开启录像功能，以及录像时间段是否在设定的录像时间段内。
如果不是，请开启录像或修改录像时间，否则请继续执行以下步骤。

图1-3 录像



步骤2 检查硬盘的数据线和电源线跳线连接。

如果连接错误，请重新连接，否则请继续执行以下步骤。

步骤3 检查硬盘是否故障。

1. 使用鼠标、键盘、显示器直连设备，开启设备。
2. 登录设备的本地界面，在预览界面右键选择“主菜单”。
3. 在主菜单界面，选择“存储管理 > 硬盘管理”。
4. 检查硬盘状态是否正常。

如果硬盘异常，请修复硬盘或更换硬盘，否则请联系相关技术支持。

图1-4 硬盘管理



步骤4 升级系统版本。

1. 将升级文件放入 U 盘，将 U 盘插入设备的 USB 接口。
2. 使用鼠标、键盘、显示器直连设备，开启设备。
3. 登录设备的本地界面，在预览界面右键选择“主菜单”。
4. 在主菜单界面，选择“运维管理 > 维护管理 > 系统升级”。
5. 单击“系统升级”。

图1-5 系统升级



步骤5 检查问题是否已经解决。

如果已解决，则完成问题处理，否则请联系相关技术支持。

1.6 预览画面及回放录像时出现马赛克

现象描述

通过网络（如 WEB）预览视频画面及回放录像时，出现马赛克。

可能原因

- 网络连接异常。
- PC 资源限制。
- 设备采用组播模式。



说明

组播模式会有较多马赛克，不建议选择。

解决方法

步骤1 检查网络连接是否正常。

1. 使用鼠标、键盘、显示器直连设备，开启设备。
2. 登录设备的本地界面，在预览界面右键选择“主菜单”。
3. 在主菜单界面，选择“运维管理 > 网络信息 > 测试”。
4. 在“目标地址”输入框输入访问设备的 PC、平台等设备的 IP 地址，单击“测试”。
如果网络连接异常，请排查网络问题，否则请继续执行以下步骤。

图1-6 网络测试



步骤2 检查 PC 是否存在资源限制。

1. 在 PC 上，右键单击任务栏，选择“任务管理器”。
2. 选择“性能”页签，查看内存及 CPU 使用情况。

如果 PC 的资源受限，请关闭其他不需要使用的应用程序或更换登录的 PC，否则请继续执行以下步骤。

步骤3 检查设备是否采用组播模式登录。

如果是，请切换为其他登录模式，否则请联系相关技术支持。

第2章 音频对讲类

2.1 设备连接音频拾音器时，没有声音

现象描述

使用音频拾音器时，没有采集到声音。

可能原因

- 线缆连接错误或接触不良。
- 拾音器未连接电源。
- 拾音器的输入电压不是指定电压。

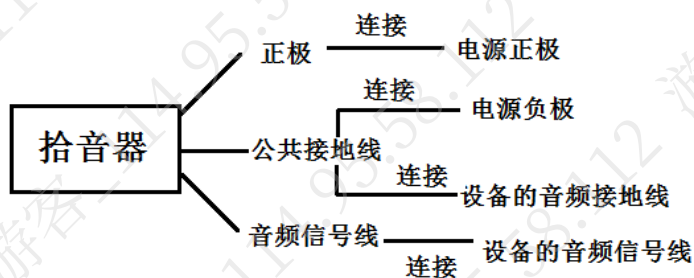
解决方法

步骤1 检查拾音器线缆。

1. 参考配套的使用说明书，检查设备的音频接口接线是否正确。

- ◇ 当拾音器只有三根接线时，三根线的定义分别为电源正极、公共接地和音频信号线。拾音器正极接电源正极。
- ◇ 公共接地线需要一分为二，一根接电源负极，另外一根公共接地线接设备的音频接地线或者莲花头外层。
- ◇ 拾音器音频信号线接设备的音频信号线或者莲花头中间。

图2-1 接线示意图



2. 检查拾音器线缆是否松动。

如果线缆连接错误或松动，请重新接线或更换线缆，否则请继续执行以下步骤。

步骤2 检查拾音器是否已接通电源。

如果没有，请接通拾音器电源，否则请继续执行以下步骤。

步骤3 检查拾音器的输入电压是否符合要求。

如果不符合，请调整输入电压，否则请联系相关技术支持。

2.2 拾音器有很大的噪声或音质较差

现象描述

使用拾音器时，拾音器中有很大的噪声或音质较差。

可能原因

- 拾音器供电异常。
- 拾音器与音箱位置太近。
- 拾音器布线不合理。
- 拾音器声音增益电位器或音量调节不合理。

解决方法

步骤1 检查拾音器的供电情况。

如果拾音器供电情况，建议使用拾音器专门的供电电源，否则请继续执行以下步骤。

步骤2 检查拾音器与音箱的位置。

如果拾音器与音箱位置太近，建议重新安装拾音器或音箱，否则请继续执行以下步骤。

步骤3 检查拾音器的布线情况。

如果拾音器布线不合理，请参考拾音器配套的资料重新布线，否则请继续执行以下步骤。

说明

- 建议拾音器单独布线，不要同交流电等强电使用同一缆槽，并且和强电保持至少50cm~80cm的距离。
- 如果拾音器无法避免与强电共用线槽，建议使用屏蔽线缆或者穿金属管，同时尽量远离变压器、灯具整流器等强电磁干扰设备。使用拾音器专门的供电电源。

步骤4 调整拾音器的增益电位器和音量。

步骤5 检查问题是否已经解决。

如果已解决，则完成问题处理，否则请联系相关技术支持。

2.3 如何选择拾音器安装位置

拾音器可以在天花板上吸顶安装和在墙面侧挂安装。安装位置尽量靠近主要的谈话区域。例如，审讯室内人拾音器安装在被审人附近；教室内的拾音器安装在讲台附近；小型会议室的拾音器安装在天花板中央等。

安装原则：尽量靠近主要的谈话区域，这样的拾音效果更佳。

2.4 连接拾音器的注意事项

- 确保拾音器与其它音频放大、音频扩音或录音设备各级之间的连接正确。如果连接错误，将

影响拾音效果，甚至损坏拾音器及其他器材。

- 在所有连接过程中或拨动开关时，将放大设备的音量调节到最小，避免瞬间的电冲击。

2.5 拾音器产生发闷、裂化声音

现象描述

使用拾音器时，拾音器产生发闷、裂化声音。

可能原因

- 拾音器安装位置不通风。
- 拾音器损坏。
- 拾音器的音频分配器较差。

解决方法

步骤1 检查拾音器的安装位置。

如果拾音器安装位置不符合要求，请选择合适的安装位置并重新安装拾音器，否则请继续执行以下步骤。



说明

拾音器工作时可能会发热，因此需要安装在通风干燥的地方，并且与其他设备距离 10cm 以上。

步骤2 检查拾音器是否损坏。

检查拾音器是否有电源线损坏、液体或其他物品进入拾音器内部、拾音器受雨淋或受潮等情况，如果有，请根据实际情况维修或更换拾音器，否则请继续执行以下步骤。

步骤3 为拾音器选用优质的拾音器音频适配器。

步骤4 检查问题是否已经解决。

如果已解决，则完成问题处理，否则请联系相关技术支持。

第 3 章 对接类问题

3.1 设备无法添加网络摄像机

现象描述

设备无法添加网络摄像机。

可能原因

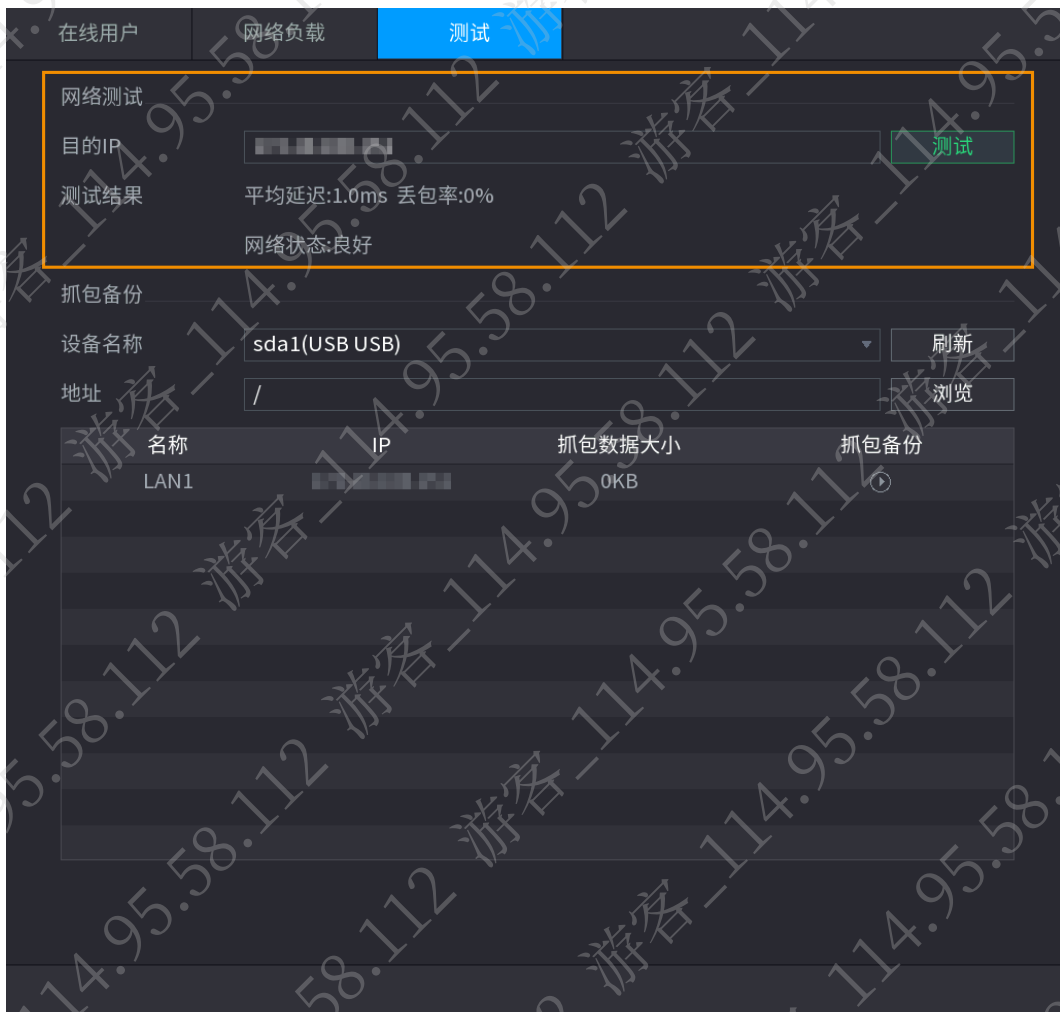
- 设备和网络摄像机的网络不通。
- 网络摄像机的参数填写错误。

解决方法

步骤1 检查网络摄像机与设备的网络连接是否正常。

1. 使用鼠标、键盘、显示器直连设备，开启设备。
2. 登录设备的本地界面，在预览界面右键选择“主菜单”。
3. 在主菜单界面，选择“运维管理 > 网络信息 > 测试”。
4. 在“目标地址”输入框输入访问设备的 PC、平台等设备的 IP 地址，单击“测试”。
如果网络连接异常，请排查网络问题，否则请继续执行以下步骤。

图3-1 网络测试



步骤2 检查添加网络摄像机的参数是否填写正确。


1. 使用鼠标、键盘、显示器直连设备，开启设备。
2. 登录设备的本地界面，在预览界面右键选择“主菜单”。
3. 在主菜单界面，选择“相机设置 > 远程设备 > 远程设备”。
4. 在“已添加设备”列表中，双击远程设备或者单击远程设备对应的 .
5. 检查网络摄像机的 IP 地址、厂商、端口、用户名、密码、远程通道号是否正确。如果错误，请根据实际情况修改，否则请联系相关技术支持。

图3-2 远程设备



3.2 设备数字通道无法连接 IPC，或者连接后总掉线

现象描述

设备数字通道无法连接 IPC，或者连接成功后 IPC 频繁掉线。

可能原因

- IPC 的 IP 地址冲突。
- IPC 的端口错误或冲突。
- IPC 的协议选择错误。
- IPC 密码错误，导致账号被锁定。
- IPC 开启黑白名单。

解决方法

步骤1 修改 IPC 的 IP 地址。


1. 使用鼠标、键盘、显示器直连设备，开启设备。
2. 登录设备的本地界面，在预览界面右键选择“主菜单”。
3. 在主菜单界面，选择“相机设置 > 远程设备 > 远程设备”。
4. 在“已添加设备”列表中，双击远程设备或者单击远程设备对应的 .
5. 修改 IPC 的 IP 地址，单击“确定”。

图3-3 远程设备



6. 检查问题是否已经解决。

如果已解决，则完成问题处理， 否则请继续执行以下步骤。

步骤2 参考步骤 1，修改 IPC 的端口号、协议和密码，检查问题是否已经解决。

如果已解决，则完成问题处理， 否则请继续执行以下步骤。

步骤3 关闭 IPC 的黑名单，或者将设备的 IP 地址加入 IPC 的白名单。

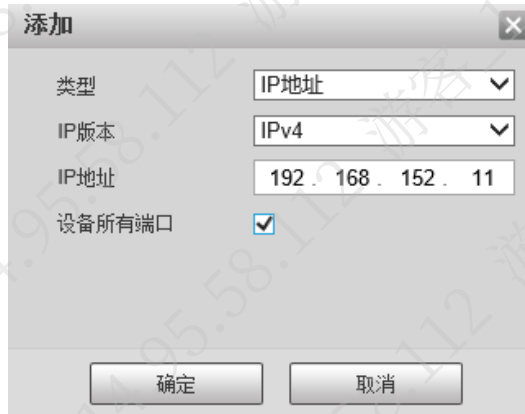
1. 登录 IPC 的 WEB 界面。
2. 选择“设置 > 系统管理 > 安全管理 > 防火墙”。
3. 选择类型为“网络访问”，选择“启用”。
4. 选择模式为“白名单”，单击“添加”。

图3-4 网络访问



5. 输入设备的 IP 地址，选择“设备所有端口”，单击“确定”。

图3-5 添加



步骤4 检查问题是否已经解决。

如果已解决，则完成问题处理，否则请联系相关技术支持。

3.3 单画面显示正常，多分割无画面

未开启 IPC 的辅码流。

步骤1 使用鼠标、键盘、显示器直连设备，开启设备。

步骤2 登录设备的本地界面，在预览界面右键选择“主菜单”。

步骤3 在主菜单界面，选择“相机设置 > 编码设置 > 音视频”。

步骤4 启用辅码流视频功能，并设置视频参数。

图3-6 音视频



步骤5 单击“应用”。

3.4 多画面显示正常，单分割无画面

现象描述

预览界面切换为多画面分割时，可以正常预览，切换为单画面分割时，预览窗口无画面。

可能原因

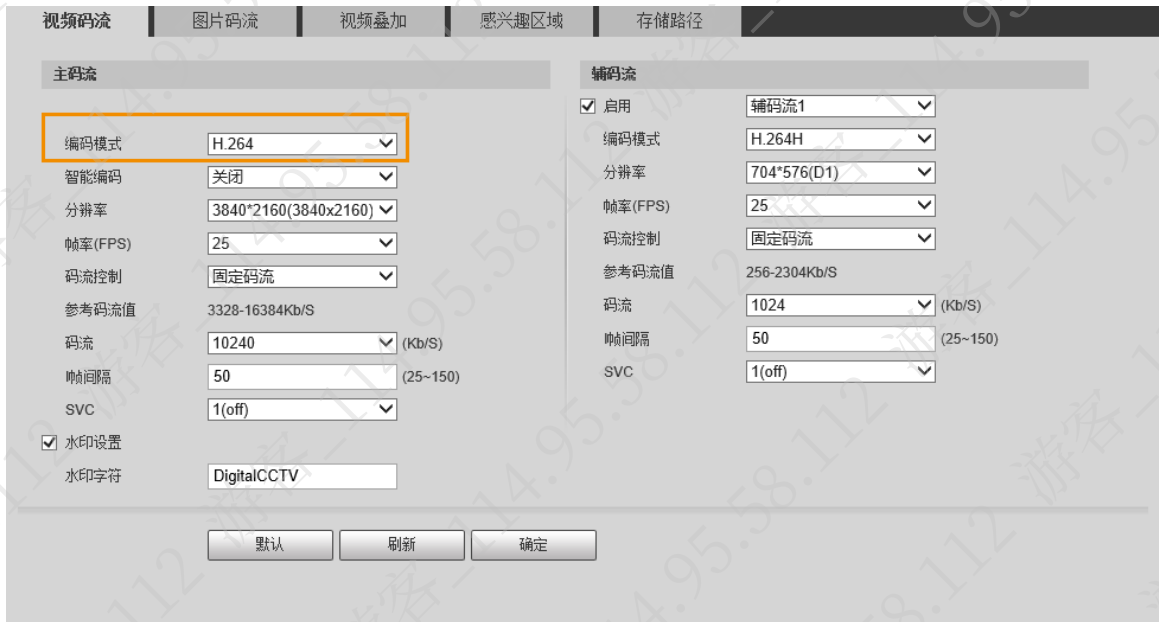
- IPC 主码流编码模式不是 H.264 格式。
- IPC 主码流编码分辨率与设备支持的分辨率不符。
- IPC 的网络传输能力达到上限。

解决方法

步骤1 设置 IPC 主码流的编码模式为 H.264。

1. 登录 IPC 的 WEB 界面。
2. 选择“设置 > 相机设置 > 视频> 视频码流”。
3. 设置主码流的“编码模式”为“H.264”，单击“确定”。

图3-7 视频码流



视频码流	图片码流	视频叠加	感兴趣区域	存储路径
主码流				
编码模式	H.264			
智能编码	关闭			
分辨率	3840*2160(3840x2160)			
帧率(FPS)	25			
码流控制	固定码流			
参考码流值	3328-16384Kb/S			
码流	10240 (Kb/S)			
帧间隔	50 (25-150)			
SVC	1(off)			
<input checked="" type="checkbox"/> 水印设置				
水印字符	DigitalCCTV			
<input type="button" value="默认"/> <input type="button" value="刷新"/> <input type="button" value="确定"/>				
辅码流				
<input checked="" type="checkbox"/> 启用	辅码流1			
编码模式	H.264H			
分辨率	704*576(D1)			
帧率(FPS)	25			
码流控制	固定码流			
参考码流值	256-2304Kb/S			
码流	1024 (Kb/S)			
帧间隔	50 (25-150)			
SVC	1(off)			

4. 检查问题是否已经解决。
如果已解决，则完成问题处理，否则请继续执行以下步骤。

步骤2 IPC 主码流编码分辨率。

1. 登录 IPC 的 WEB 界面。
2. 选择“设置 > 相机设置 > 视频> 视频码流”。
3. 设置主码流的“分辨率”，单击“确定”。
需要设置为设备支持的分辨率，包括 1080P、720P、960H、D1 等。

图3-8 视频码流

主码流		辅码流	
编码模式	H.264	<input checked="" type="checkbox"/> 启用	辅码流1
智能编码	关闭	编码模式	H.264H
分辨率	3840*2160(3840x2160)	分辨率	704*576(D1)
帧率(FPS)	25	帧率(FPS)	25
码流控制	固定码流	码流控制	固定码流
参考码流值	3328-16384Kb/S	参考码流值	256-2304Kb/S
码流	10240 (Kb/S)	码流	1024 (Kb/S)
帧间隔	50 (25~150)	帧间隔	50 (25~150)
SVC	1(off)	SVC	1(off)
<input checked="" type="checkbox"/> 水印设置			
水印字符	DigitalCCTV		

4. 检查问题是否已经解决。
如果已解决，则完成问题处理，否则请继续执行以下步骤。

步骤3 检查 IPC 的在线用户是否超过最大数。

1. 登录 IPC 的 WEB 界面。
2. 选择“设置 > 系统管理 > 在线用户”。
3. 检查 IPC 的在线用户是否超过最大连接数。
如果没有超过，请联系相关技术支持处理，否则请继续执行以下步骤。

图3-9 在线用户

序号	用户名	用户所在组	地址	用户登录时间
1	admin	admin	10.33.10.96	2020-10-31 15:11:15

刷新

4. 选择“设置 > 网络 > 端口”。
5. 修改“最大连接数”，单击“确定”。

图3-10 端口

端口名称	端口号	范围
最大连接数	10	(1-20)
TCP端口	37777	(1025-65534)
UDP端口	37778	(1025-65534)
HTTP端口	80	
RTSP端口	554	
RTMP端口	1935	(1025-65534)
HTTP端口	443	
AOL端口	8088	(1025-65534)
5000端口	<input type="radio"/> 启用 <input checked="" type="radio"/> 关闭	

- 步骤4 检查问题是否已经解决。
如果已解决，则完成问题处理，否则请联系相关技术支持。

3.5 如何通过设备修改 IPC 的 IP 地址


- 步骤1 使用鼠标、键盘、显示器直连设备，开启设备。
步骤2 在预览界面右键选择“主菜单”，在主菜单界面，选择“相机设置 > 远程设备”。
步骤3 单击“搜索设备”。
步骤4 在设备搜索列表中选择设备，单击.

图 6-142 修改 IP

修改IP

已选中设备数：1

DHCP 用户名 admin

静态 密码

IP地址 192 . 168 . 192 . 128 递增量 1

子网掩码 255 . 255 . 255 . 0

默认网关 192 . 168 . 192 . 1

序号	IP地址
1	192.168.192.128

确定 取消

- 步骤5 输入远程设备的用户名和密码，设置远程设备 IP 地址。

说明

同时修改多个远程设备时，请确保所有远程设备的用户名和密码一致。

- 当网络中存在 DHCP 服务器时，可选择“DHCP”，设备自动获取一个动态 IP 地址，无需手动设置 IP 地址等信息。
- 若选择“静态”，则需要输入“IP 地址”、“子网掩码”、“默认网关”以及“递增量”。系统将根据此 IP 地址的第四位递增，依次为远程设备分配 IP 地址。
- 仅当同时修改多个远程设备时需要设置“递增量”。系统将根据设置的递增量，在 IP 地址的第四位递增，依次为所选的远程设备分配 IP 地址。
- 修改静态 IP 时，若 IP 地址有冲突，则系统会提示用户 IP 冲突。若是批量修改 IP 地址，则系统会自动跳过冲突 IP，重新根据递增量进行分配。

步骤6 单击“确定”。

3.6 通过 ONVIF 协议或私有协议接入第三方 IPC 问题

目前，通过 ONVIF 协议接入的第三方 IPC，支持的功能包括但不限于如下功能：

- 修改通道名称。
- 设置动态检测录像报警。
- 修改 IPC 分辨率、码流值和帧率。
- 上下左右转动网络球机、设置预置点等。

使用过程中，如果功能存在异常，请联系相关技术支持。

第 4 章 智能类问题

4.1 智能检测功能如何初始化检测的基准画面

开机后，系统显示的第一个稳定画面，即为基准画面，后续的智能检测都是基于基准画面。对接平台，并且平台支持重建智能检测背景时，可以通过该功能初始化智能检测功能的基准画面，详细配置请参见平台配套的资料。



说明

基准画面一般需要保证图像中无人和异常物体出现。

4.2 人脸检测没有报警

现象描述

开启人脸检测功能后，经常出现检测到人脸但没有报警的情况。

可能原因

- 摄像机未拍摄到完整的脸。
- 人脸处于背光环境。
- 人脸大小不符合要求。

解决方法

步骤1 调节摄像机的安装角度。

1. 参考摄像机的安装指导手册，调整摄像机的安装位置、角度等。
2. 检查问题是否已经解决。

如果已解决，则完成问题处理，否则请继续执行以下步骤。

步骤2 调节摄像机的背光效果。

1. 登录摄像机的 WEB 界面。
2. 选择“设置 > 相机设置 > 摄像头属性 > 背光”。
3. 根据画面效果，设置背光模式和阈值。

图4-1 背光



步骤3 参考设备配套的资料，检查人脸大小是否符合要求。

如果人脸大小不符合，可适当调整摄像机的安装位置、角度等，否则请联系相关技术支持。

4.3 徘徊检测容易产生误报

徘徊检测的最短持续时间设置太小。

步骤1 使用鼠标、键盘、显示器直连设备，开启设备。

步骤2 登录设备的本地界面，在预览界面右键选择“主菜单”。

步骤3 在主菜单界面，选择“智能 > 参数设置 > 通用行为分析”。


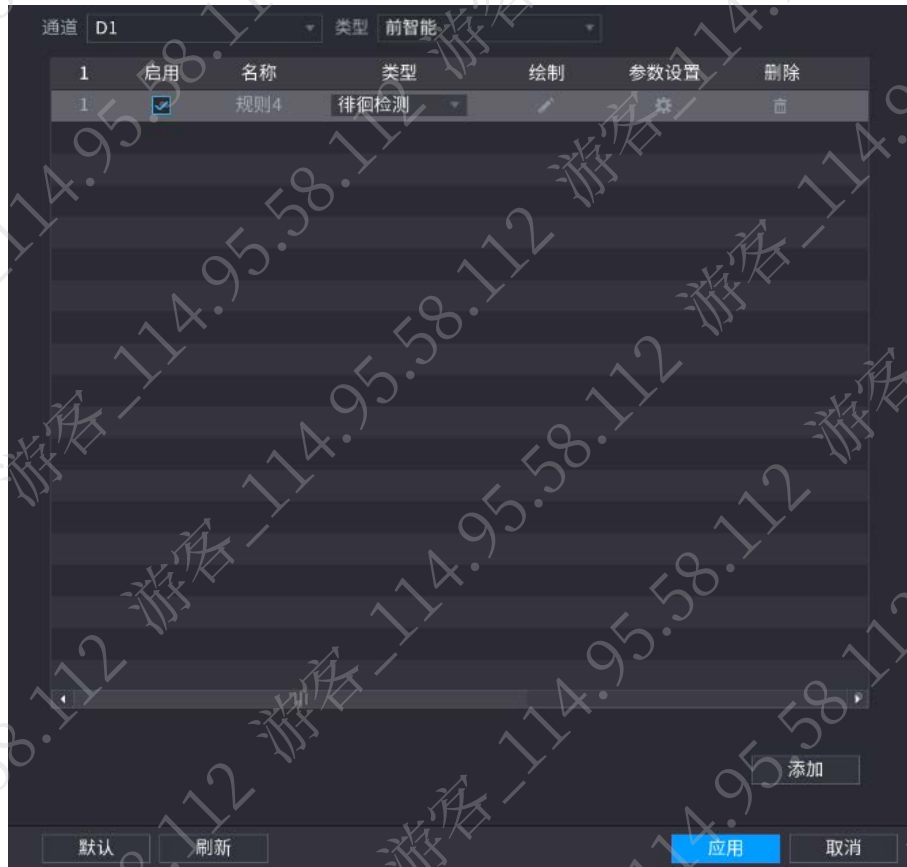
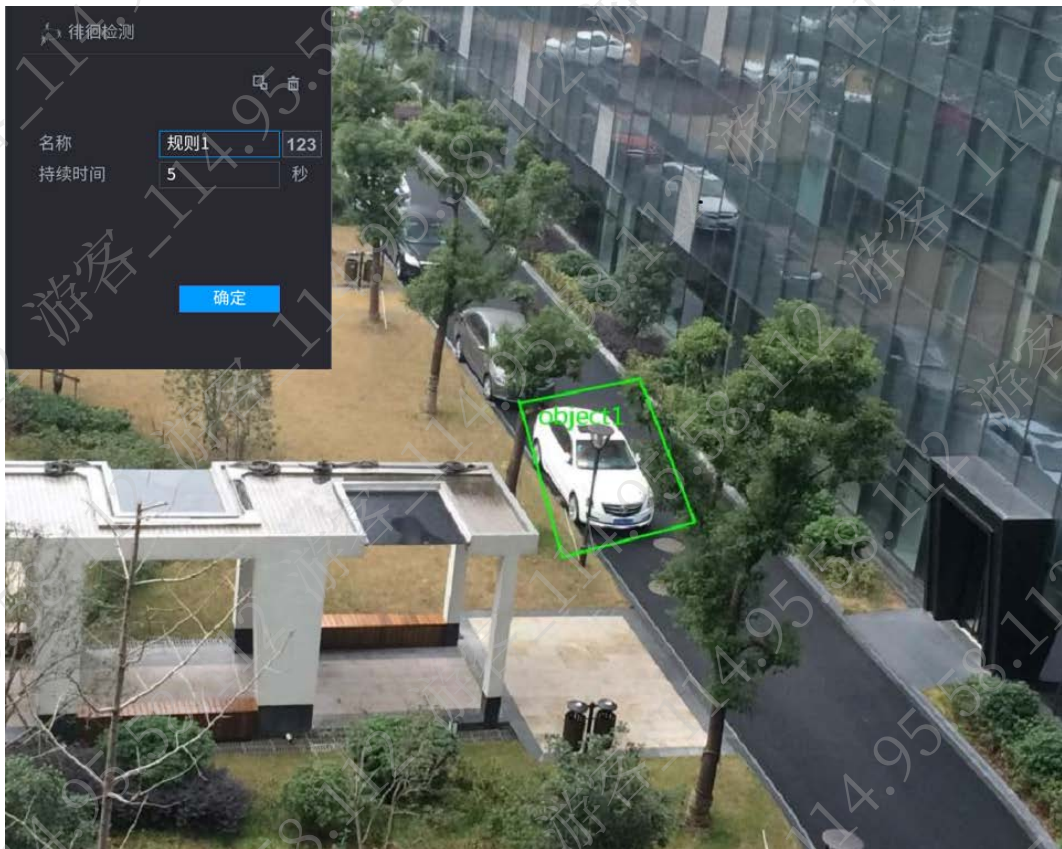
步骤4 单击徘徊检测对应的 。

图4-2 智能检测



步骤5 设置持续时间，单击“确定”。

图4-3 徘徊检测



4.4 通用行为分析功能没有报警

监控的视频图像效果差（例如图像噪点大、图像抖动、图像有强烈光线等），系统没有检测到报警目标。

根据实际情况排查图像异常问题，如果问题已解决，则完成问题处理，否则请联系相关技术支持。

4.5 区域入侵中的区域内检测和徘徊检测的区别

两者的主要区别是考察对象不一样。

- 区域内检测是将警戒区作为考察对象，当区域目标个数超过报警阈值一定时间，在考察时间段内可能有目标进出区域，但是区域内的目标个数始终满足报警条件，就会触发报警。
- 徘徊检测是将具体的运动目标作为考察对象，只要该目标在报警区域内停留时间超过设定时间机会触发报警。

4.6 智能重建背景的目的是什么

重建背景的目的是让系统建立参考背景，在后续的智能检测中，如果出现异于背景的目标，系统将以目标进行检测。

重建背景简化算法背景学习过程以及避免背景学习异常的情况，因此重建时应尽量以没有目标的画面作为背景。

第5章 网络类问题

5.1 WEB 无法访问设备，系统提示登录失败

现象描述

网络可以 ping 通，但无法通过 WEB 界面访问设备，系统提示登录失败。

可能原因

- 设备 IP、网关、子网掩码或端口号设置错误。
- 设备的在线用户超过最大连接数。
- 跨网段访问设备。

解决方法

步骤1 修改设备的 IP、网关、子网掩码或端口号。

1. 使用鼠标、键盘、显示器直连设备，开启设备。
2. 登录设备的本地界面，在预览界面右键选择“主菜单”。
3. 在主菜单界面，选择“网络设置 > TCP/IP”。
4. 根据网络规划，修改设备的 IP 地址、子网掩码、网关和端口号等。

图5-1 TCP/IP



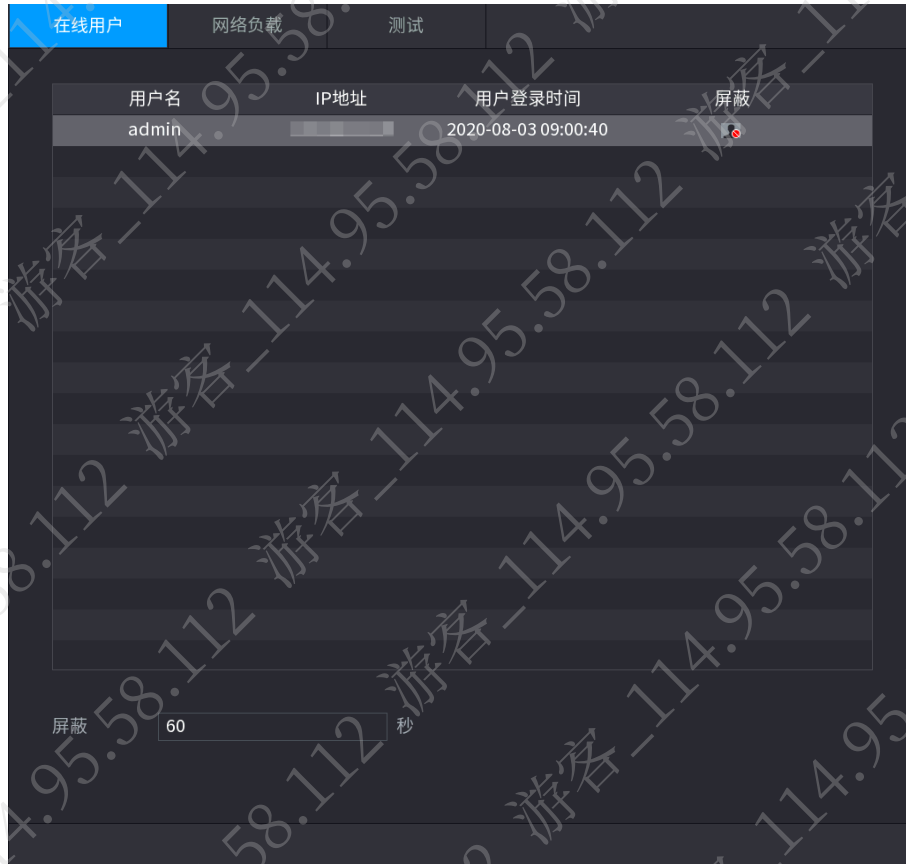
5. 检查问题是否已经解决。
如果已解决，则完成问题处理，否则请继续执行以下步骤。

步骤2 检查设备的在线用户是否超过最大连接数。

1. 使用鼠标、键盘、显示器直连设备，开启设备。

2. 登录设备的本地界面，在预览界面右键选择“主菜单”。
3. 在主菜单界面，选择“运维管理 > 网络信息 > 在线用户”。
4. 检查设备的在线用户是否超过最大连接数。
如果没有超过，请继续执行以下步骤，否则请继续执行步骤 3。

图5-2 在线用户



5. 在主菜单界面，选择“网络设置 > 端口”。
6. 修改“最大连接数”，单击“应用”。

图5-3 端口

最大连接数	128	(0 -128)
TCP端口	37777	(1025 - 65535)
UDP端口	37778	(1025 - 65535)
HTTP端口	80	(1 - 65535)
HTTPS端口	443	(1 - 65535)
RTSP端口	554	(1 - 65535)
NTP服务端	123	(1 - 65535)
POS端口	38800	(1025 - 65535)

应用 返回

步骤3 使用笔记本电脑直连登录。

1. 使用网线连接笔记本电脑和设备的网口。
2. 在笔记本电脑上通过 WEB 访问设备。

步骤4 检查问题是否已经解决。

如果已解决，则完成问题处理，否则请联系相关技术支持。

5.2 国标 28181 协议接入第三方平台后，预览、回放卡顿

现象描述

设备通过国标 28181 协议接入第三方平台后，实时预览和录像回放时卡顿。

可能原因

- 网络带宽不足。
- 设备码流和分辨率设置较高。

解决方法

步骤1 检查网络带宽情况。

1. 使用鼠标、键盘、显示器直连设备，开启设备。
2. 登录设备的本地界面，在预览界面右键选择“主菜单”。

3. 在主菜单界面，选择“运维管理 > 网络信息 > 测试”。
4. 在“目标地址”输入框输入第三方的 IP 地址，单击“测试”。
如果网络连接异常，请排查网络问题，否则请继续执行以下步骤。

图5-4 网络测试



步骤2 降低设备的码流和分辨率。

1. 使用鼠标、键盘、显示器直连设备，开启设备。
2. 登录设备的本地界面，在预览界面右键选择“主菜单”。
3. 在主菜单界面，选择“运维管理 > 网络信息 > 测试”。
4. 根据图像效果，适当降低分辨率和码流值，单击“应用”。

图5-5 音视频



- 步骤3 检查问题是否已经解决。
如果已解决，则完成问题处理，否则请联系相关技术支持。

5.3 修改密码时发生密码锁定

修改设备密码前，需要先在已添加该设备的平台上删除该设备；修改设备密码后，在平台端重新以新密码添加设备。否则，平台不断以旧密码访问该设备，当密码错误 5 次时将被锁定。

5.4 如何重置设备登录密码

当遗忘 admin 用户的登录密码时，可通过手机扫描二维码、密保问题验证和硬件复位的方式，重置登录密码。

- 开启密码重置功能时，可通过手机扫描二维码的方式重置密码。
- 关闭密码重置功能时，包括以下情况：
 - ◇ 已设置密保问题，可通过密保问题验证的方式重置密码。
 - ◇ 未设置密保问题，需要通过硬件复位功能的方式恢复出厂设置。



说明

- 仅部分设备支持硬件复位功能。
- 以下内容主要介绍手机重置密码。

步骤1 使用鼠标、键盘、显示器直连设备，开启设备。

步骤2 启用密码重置功能。

1. 登录本地界面，在预览界面右键选择“主菜单”。
2. 在主菜单界面，选择“用户管理 > 密码重置”。
3. 选择“启用”，设置预留手机号码和密保问题答案，单击“应用”。

说明

系统默认已启用重置密码功能。

图5-6 密码重置

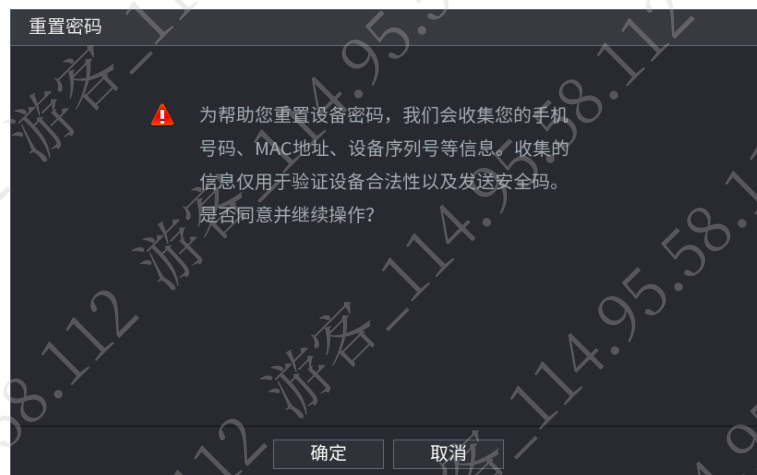
步骤3 重置密码。

1. 在本地预览界面，右键选择任意功能菜单。
2. 在“登录系统”界面，单击。

说明

设置手势密码后，系统默认显示手势密码登录界面，可单击“忘记手势”，进入密码输入登录界面。

3. 仔细阅读提示信息后，单击“确定”。

图5-7 重置密码 (1)


4. 根据界面提示扫描二维码并获取安全码，在“请输入安全码”文本框中输入预留手

机接收到的安全码，单击“下一步”。

图5-8 重置密码（2）



5. 界面提示，设置新密码和确认密码，单击“确定”。

图5-9 重置密码（4）



第 6 章 外接设备类

6.1 如何接入报警设备

设备可以提供的电量是 12V，如果报警设备的启动电压是 12V，可以接入 CTRL 12V 和接地供电；如果报警设备的启动电压大于 12V，报警设备需要使用单独电压供电。

- 报警设备使用单独电源时，接入 NO 和 C 报警输出接口即可。
- 报警输入类型不限，可以是常开型也可以是常闭型。
- 报警探测器的地端（GND）与 com 端并联（报警探测器应由外部电源供电）。
- 报警探测器的接地端与硬盘录像机接地端并接。
- 报警探测器的 NC 端接到设备报警输入端（ALARM）。
- 当用外部电源对报警设备供电时需与设备共地。

图6-1 报警接口

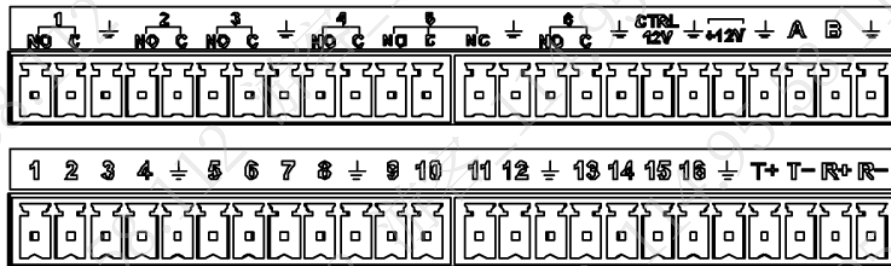
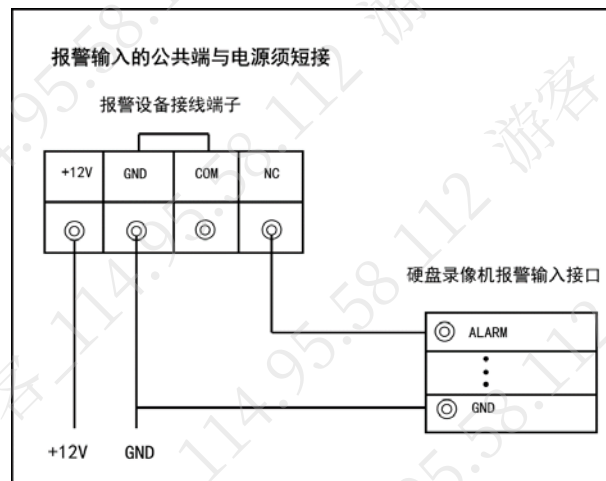


图6-2 常闭报警输入



6.2 设备外接报警感应器，重启感应器时会触发本地报警

现象描述

设备外接报警感应器，重启报警感应器时，触发本地报警。

可能原因

- 报警感应器异常。
- 报警设备类型设置错误。

解决方法

步骤1 检查报警感应器是否正常。

如果报警感应器故障或异常，请维修或更换报警感应器，否则请继续执行以下步骤。

步骤2 修改报警设备类型。

1. 使用鼠标、键盘、显示器直连设备，开启设备。
2. 登录设备的本地界面，在预览界面右键选择“报警设置 > 报警输入 > 本地”。
3. 选择报警输入通道，修改“设备类型”。

图6-3 报警输入



步骤3 检查问题是否已经解决。

如果已解决，则完成问题处理，否则请联系相关技术支持。

6.3 本地界面操作，鼠标移动缓慢

鼠标接口接触不良，请更换鼠标，如果问题还未解决，请联系相关技术支持。

6.4 VGA 和 HDMI 简介

- VGA（Video Graphics Array，视频图形阵列）是使用模拟信号的一种视频传输标准，具有分辨率高，显示速率快，颜色丰富等优点。VGA 数据线一般不超过 15 米，因为信号传输距离超过 15 米时，VGA 信号质量会严重下降。VGA 是模拟信号输出，信号会重新转换，所有信号均可以转成适合当前显示器的格式，例如 1080p@60Hz。
- HDMI（High Definition Multimedia Interface，高清晰度多媒体接口）是一种数字化视频/音频接口技术，无需在信号传送前进行 D/A 或者 A/D 转换，可同时传送无压缩的音频和视频信号。HDMI 是数字信号输出不经过转换，例如，如果原始信号是 1080p@25Hz，而当前显示器不支持这个格式，将会出现黑边或者图像溢出的情况。

6.5 显示器或显示异常黑屏

部分显示器不支持设备默认的分辨率 1280x1024，需要根据实际情况，修改设备的分辨率。

- 步骤1 使用鼠标、键盘、显示器直连设备，开启设备。
- 步骤2 登录设备的本地界面，在预览界面右键选择“主菜单”。
- 步骤3 在主菜单界面，选择“显示输出 > 显示输出”。
- 步骤4 修改显示器的分辨率。

图6-4 显示输出



- 步骤5 单击“应用”

第 7 章 其他类问题

7.1 HDMI/VGA 异源输出简介

HDMI/VGA 异源输出是指同时接入两个显示器，通过配置视频矩阵或动态检测关联视频矩阵，实现两个显示器输出不同的画面。

用作异源输出的接口类似于传统 DVR 的 spot 口，仅作模拟通道预览、不支持鼠标操作。将正在操作的显示器（VGA/HDMI）配置成视频矩阵输出口时，鼠标将无法操作，如果需要操作，可以将另一接口（HDMI/VGA）连接显示器，或者登录设备的 WEB 界面，选择“设置 > 系统 > 显示输出”，修改视频矩阵输出口。

7.2 如果通过 U 盘手动升级

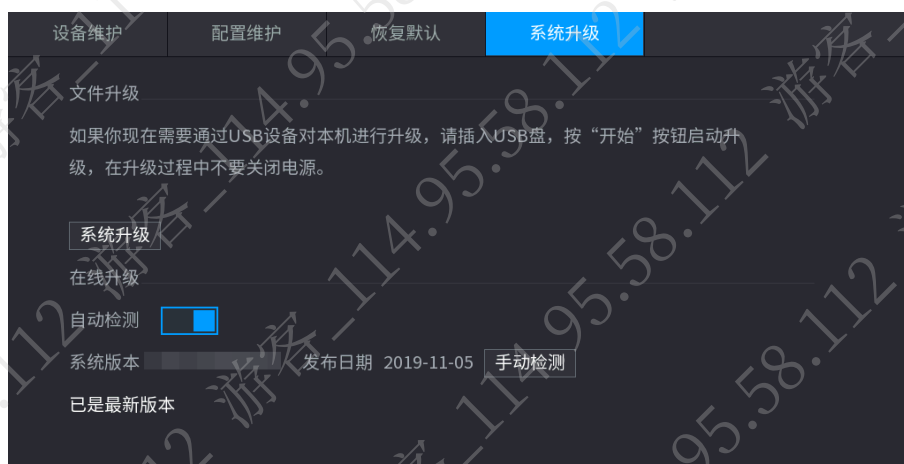


注意

- U 盘手动升级需要保证设备能够正常运行。
- U 盘如有重要资料请先做好备份，以免数据丢失。

- 步骤1 需将 U 盘格式化为 FAT32 格式，依次将升级固件和主程序拷贝到 U 盘。
- 步骤2 将 U 盘插入设备的 USB 接口。
- 步骤3 使用鼠标、键盘、显示器直连设备，开启设备。
- 步骤4 登录设备的本地界面，在预览界面右键选择“主菜单”。
- 步骤5 在主菜单界面，选择“设置 > 系统 > 系统升级”。
- 步骤6 单击“系统升级”。

图7-1 系统升级



7.3 如何使用 ConfigTool 工具升级



注意

ConfigTool 工具升级需要保证设备能够正常运行。

步骤1 在 PC 端打开 ConfigTool 工具，选择“设备升级”页签。

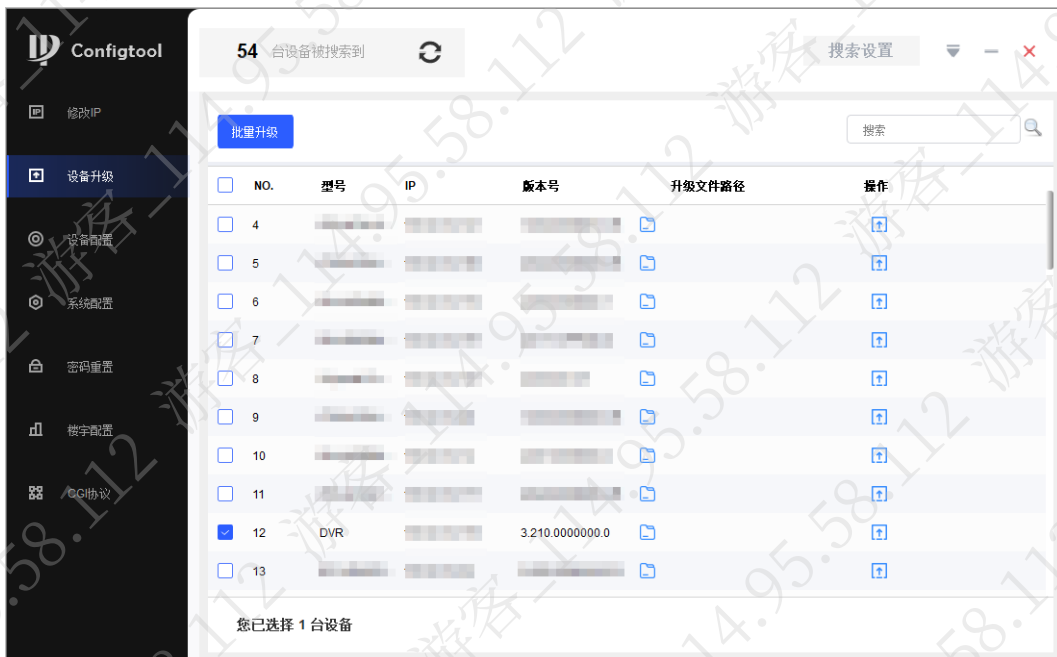
步骤2 单击“搜索设置”，输入设备的 IP、用户名和密码，单击“确定”。

图7-2 设置

步骤3 升级设备。

- 单个升级：单击设备对应的 ，选择升级文件后，单击 。
- 批量升级：选择设备，单击“批量升级”，在“批量升级”界面，选择升级文件。

图7-3 批量升级



附录1 法律声明

版权声明

© 2020 浙江大华技术股份有限公司。版权所有。

在未经浙江大华技术股份有限公司（下称“大华”）事先书面许可的情况下，任何人不能以任何形式复制、传递、分发或存储本文档中的任何内容。

本文档描述的产品中，可能包含大华及可能存在的第三人享有版权的软件。除非获得相关权利人的许可，否则，任何人不能以任何形式对前述软件进行复制、分发、修改、摘录、反编译、反汇编、解密、反向工程、出租、转让、分许可等侵犯软件版权的行为。

商标声明

- 、、、、**HDCVI** 是浙江大华技术股份有限公司的商标或注册商标。
- HDMI 标识、HDMI 和 High-Definition Multimedia Interface 是 HDMI Licensing LLC 的商标或注册商标。本产品已经获得 HDMI Licensing LLC 授权使用 HDMI 技术。
- VGA 是 IBM 公司的商标。
- Windows 标识和 Windows 是微软公司的商标或注册商标。
- 在本文档中可能提及的其他商标或公司的名称，由其各自所有者拥有。

责任声明

- 在适用法律允许的范围内，在任何情况下，本公司都不对因本文档中相关内容及描述的产品而产生任何特殊的、附随的、间接的、继发性的损害进行赔偿，也不对任何利润、数据、商誉、文档丢失或预期节约的损失进行赔偿。
- 本文档中描述的产品均“按照现状”提供，除非适用法律要求，本公司对文档中的所有内容不提供任何明示或暗示的保证，包括但不限于适销性、质量满意度、适合特定目的、不侵犯第三方权利等保证。

出口管制合规声明

大华遵守适用的出口管制法律法规，并且贯彻执行与硬件、软件、技术的出口、再出口及转让相关的要求。就本手册所描述的产品，请您全面理解并严格遵守国内外适用的出口管制法律法规。

隐私保护提醒

您安装了我们的产品，您可能会采集人脸、指纹、车牌、邮箱、电话、GPS 等个人信息。在使用产品过程中，您需要遵守所在地区或国家的隐私保护法律法规要求，保障他人的合法权益。如，提供清晰、可见的标牌，告知相关权利人视频监控区域的存在，并提供相应的联系方式。

关于本文档

- 本文档供多个型号产品使用，产品外观和功能请以实物为准。
- 如果不按照本文档中的指导进行操作而造成的任何损失由使用方自己承担。
- 本文档会实时根据相关地区的法律法规更新内容，具体请参见产品的纸质、电子光盘、二维码或官网，如果纸质与电子档内容不一致，请以电子档为准。
- 本公司保留随时修改本文档中任何信息的权利，修改的内容将会在本文档的新版本中加入，恕不另行通知。
- 本文档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，以公司最终解释为准。

- 如果获取到的 PDF 文档无法打开，请使用最新版本或最主流的阅读工具。

附录2 网络安全声明和建议

安全声明

- 若您将产品接入互联网需自担风险，包括但不限于可能遭受网络攻击、黑客攻击、病毒感染等，请您加强网络、设备数据和个人信息等的保护，采取保障设备网络安全的必要措施，包括但不限于使用复杂密码、定期修改密码、及时将固件更新至最新版本等。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任何责任，但本公司会提供产品相关安全维护。
- 在适用法律未明令禁止的程度下，对于因使用或无法使用本产品或服务而引起的任何利润、收入、销售损失、数据丢失或采购替代商品或服务的成本、财产损失、人身伤害、业务中断、商业信息损失，或者任何特殊的、直接的、间接的、附带的、经济性、覆盖性、惩罚性、特殊或从属损害，无论是基于何种责任理论（合同、侵权、过失或其他），本公司及其员工、许可方或附属公司都不承担赔偿责任，即使其已被告知存在此种损害的可能性也是如此。某些司法管辖区不允许对人身伤害、附带或从属损害等进行责任限制，则此限制可能不适用于您。
- 本公司对您的所有损害承担的总责任限额（除了因本公司过失导致人身伤亡的情况，需遵循适用法律规定）不超过您购买本公司产品所支付的价款。

安全建议

保障设备基本网络安全的必须措施：

1. 使用复杂密码

请参考如下建议进行密码设置：

- 长度不小于 8 个字符。
- 至少包含两种字符类型，字符类型包括大小写字母、数字和符号。
- 不包含账户名称或账户名称的倒序。
- 不要使用连续字符，如 123、abc 等。
- 不要使用重叠字符，如 111、aaa 等。

1. 及时更新固件和客户端软件

- 按科技行业的标准作业规范，设备的固件需要及时更新至最新版本，以保证设备具有最新的功能和安全性。设备接入公网情况下，建议开启在线升级自动检测功能，便于及时获知厂商发布的固件更新信息。
- 建议您下载和使用最新版本客户端软件。

增强设备网络安全的建议措施：

1. 物理防护

建议您对设备（尤其是存储类设备）进行物理防护，比如将设备放置在专用机房、机柜，并做好门禁权限和钥匙管理，防止未经授权的人员进行破坏硬件、外接设备（例如 U 盘、串口）等物理接触行为。

2. 定期修改密码

建议您定期修改密码，以降低被猜测或破解的风险。

3. 及时设置、更新密码重置信息

设备支持密码重置功能，为了降低该功能被攻击者利用的风险，请您及时设置密码重置相关

信息，包含预留手机号/邮箱、密保问题，如有信息变更，请及时修改。设置密保问题时，建议不要使用容易猜测的答案。

4. 开启账户锁定

出厂默认开启账户锁定功能，建议您保持开启状态，以保护账户安全。在攻击者多次密码尝试失败后，其对应账户及源 IP 将会被锁定。

5. 更改 HTTP 及其他服务默认端口

建议您将 HTTP 及其他服务默认端口更改为 1024~65535 间的任意端口，以减小被攻击者猜测服务端口的风险。

6. 使能 HTTPS

建议您开启 HTTPS，通过安全的通道访问 Web 服务。

7. MAC 地址绑定

建议您在设备端将其网关设备的 IP 与 MAC 地址进行绑定，以降低 ARP 欺骗风险。

8. 合理分配账户及权限

根据业务和管理需要，合理新增用户，并合理为其分配最小权限集合。

9. 关闭非必需服务，使用安全的模式

如果没有需要，建议您关闭 SNMP、SMTP、UPnP 等功能，以降低设备面临的风险。

如果有需要，强烈建议您使用安全的模式，包括但不限于：

- SNMP：选择 SNMP v3，并设置复杂的加密密码和鉴权密码。
- SMTP：选择 TLS 方式接入邮箱服务器。
- FTP：选择 SFTP，并设置复杂密码。
- AP 热点：选择 WPA2-PSK 加密模式，并设置复杂密码。

10. 音视频加密传输

如果您的音视频数据包含重要或敏感内容，建议启用加密传输功能，以降低音视频数据传输过程中被窃取的风险。

11. 安全审计

- 查看在线用户：建议您不定期查看在线用户，识别是否有非法用户登录。
- 查看设备日志：通过查看日志，可以获知尝试登录设备的 IP 信息，以及已登录用户的关键操作信息。

12. 网络日志

由于设备存储容量限制，日志存储能力有限，如果您需要长期保存日志，建议您启用网络日志功能，确保关键日志同步至网络日志服务器，便于问题回溯。

13. 安全网络环境的搭建

为了更好地保障设备的安全性，降低网络安全风险，建议您：

- 关闭路由器端口映射功能，避免外部网络直接访问路由器内网设备的服务。
- 根据实际网络需要，对网络进行划区隔离：若两个子网间没有通信需求，建议使用 VLAN、网闸等方式对其进行网络分割，达到网络隔离效果。
- 建立 802.1x 接入认证体系，以降低非法终端接入专网的风险。
- 开启设备 IP/MAC 地址过滤功能，限制允许访问设备的主机范围。

更多内容

请访问大华官网安全应急响应中心，获取安全公告和最新的安全建议。

「让社会更安全 让生活更智能」

ENABLING A SAFER SOCIETY AND SMARTER LIVING