






可视报警终端

使用说明书

V1.0.2

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。
 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。

修订记录

版本号	修订内容	发布日期
V1.0.2	增加法律声明和网络安全须知	2018.12

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

- 请在设备布控后及时修改用户的默认密码，以免被人盗用。
- 请不要将设备放置和安装在阳光直射的地方或发热设备附近。
- 请不要将设备安装在潮湿、有灰尘或煤烟的场所。
- 请保持设备的水平安装，或安装在稳定的场所，注意防止本产品坠落。
- 请勿将液体滴到或溅到设备上，并确保设备上不能放置装满液体的物品，防止液体流入设备。
- 请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。
- 请不要随意拆卸设备。

电源要求

- 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。
- 如果使用电源插头或器具耦合器等作为断开装置，请保持断开装置可以方便的操作。

前言.....	I
使用安全须知.....	II
1 产品介绍.....	1
1.1 产品概述.....	1
1.2 产品特性.....	1
1.3 设备结构.....	1
1.4 典型组网.....	4
2 安装.....	5
2.1 螺钉规格.....	5
2.2 安装步骤.....	5
3 调测可视报警终端.....	8
3.1 设置本机信息.....	8
3.1.1 设置 IP 地址.....	8
3.1.2 设置系统时间.....	9
3.2 设置 FTP 信息.....	9
3.3 功能调测.....	10
3.3.1 呼叫功能.....	10
3.3.2 监视功能.....	10
3.3.3 刷卡巡更功能.....	10
3.3.4 广告投放.....	10
3.3.5 语音广播.....	10
3.3.6 防拆功能.....	10
3.3.7 环境光补偿功能.....	10
4 WEB 配置.....	11
4.1 登录 WEB 系统.....	11
4.2 系统设置.....	11
4.2.1 本机设置.....	11
4.2.2 网络设置.....	12
4.2.3 视频设置.....	13
4.3 退出 WEB 系统.....	14
附录 1 技术规格.....	16
附录 2 装箱清单.....	17
附录 3 法律声明.....	18
附录 4 网络安全建议.....	19

1.1 产品概述

可视报警终端支持与安保综合管理平台、数字管理机对接，实现一键报警、语音广播、视频监控、刷卡巡更、广告投放等功能。同时，可视报警终端支持 WEB 配置。

主要应用于银行或者农村信用社网点的可视化联网报警改造，也可以应用于城市化安保、监狱、能源等行业。

1.2 产品特性

- 130 万高清摄像头，720P 视频输出。
- 10 寸大屏显示，视频播放。
- 高清语音，数字降噪和回声抑制。
- IK09 防暴性能，全金属机身，铝面板 6mm 厚，针孔摄像头。
- IP55 防水防尘性能。
- 支持一键报警。
- 支持防拆报警，2 路报警输入和 2 路报警输出。
- 支持外接有源音箱。
- 支持标准 POE 供电。

1.3 设备结构

前面板

图1-1 前面板示意图

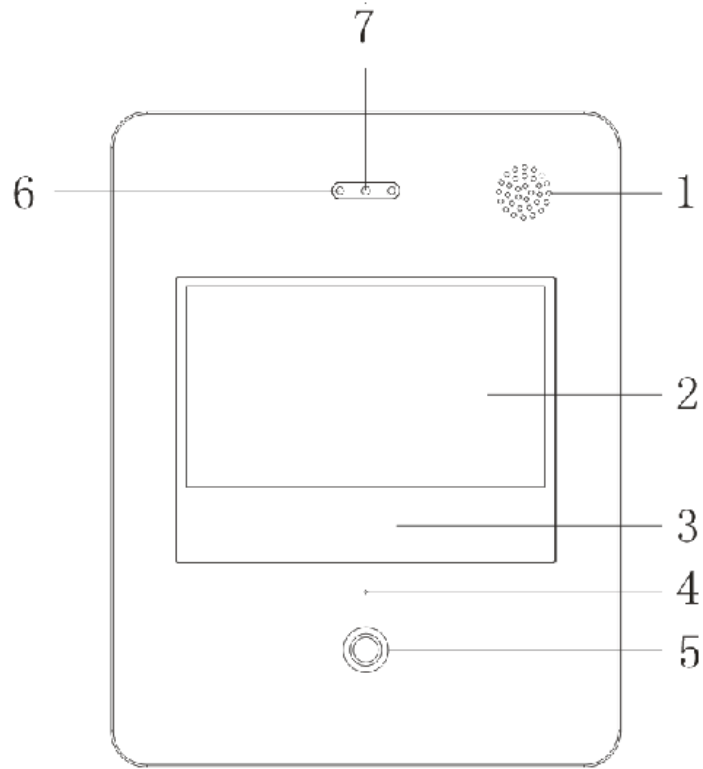


表1-1 前面板

序号	部件名称	部件说明
1	喇叭	声音输出。
2	显示屏	高清显示屏。
3	刷卡	刷卡区域。
4	麦克	声音输入。
5	报警按钮	报警至管理中心。
6	补光灯	在光线不足的环境下，如果可视报警终端处于被监视状态，或者呼叫状态、通话状态时，可视报警终端自动打开补光灯。
7	摄像头	监视区域图像。

后面板

图1-2 后面板示意图

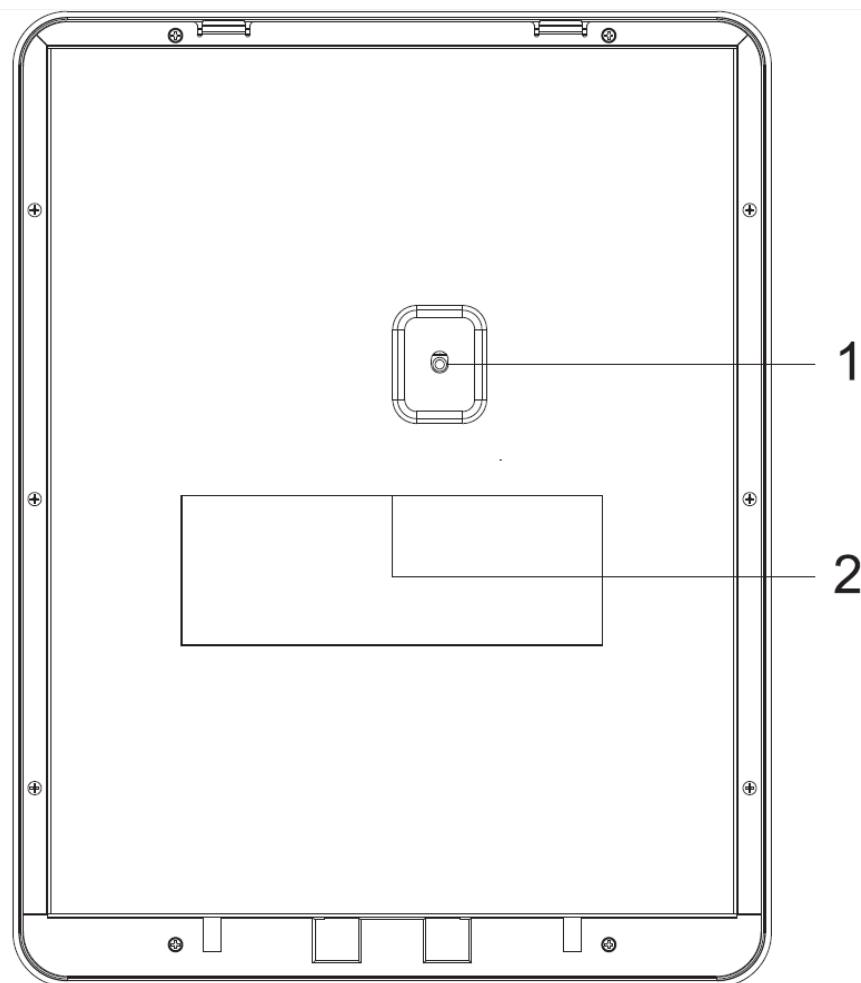


表1-2 后面板

序号	部件名称	部件说明
1	防拆按钮	防拆按钮。
2	设备接口	用于接入音箱、喇叭、报警输入输出、电源、和 RS485 等。

设备接口说明

图1-3 设备接口图

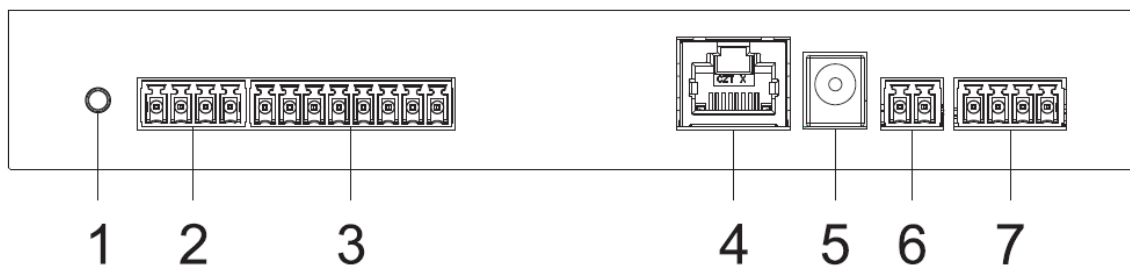


表1-3 设备接口

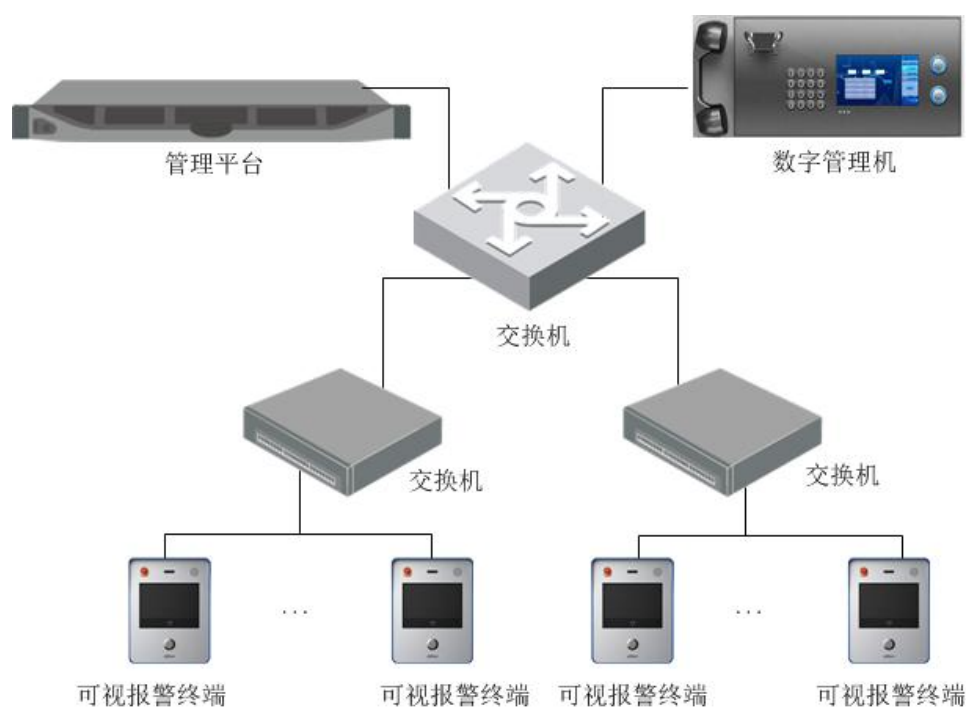
序号	部件名称	部件说明
1	复位按键	功能复位。
2	音频接口	外接音频。

序号	部件名称	部件说明
3	报警接口	外接报警。
4	网络接口	外接网线。
5	电源 A	连接 12V 直流电源。
6	电源 B	连接 12V 直流电源。
7	485 接口	外接 485。

1.4 典型组网

可视报警终端与数字管理机或智能楼宇综合管理平台对接，实现可视对讲、视频监控等功能，如图 1-4 所示。

图1-4 组网图






说明

组网中可以不出现数字管理机。

本节主要介绍可视报警终端安装方法。

2.1 螺钉规格

表2-1 螺钉规格

部件名称	示意图	数量
膨胀管 $\Phi 6 \times 30\text{mm}$		6 个
ST4.2×25 十字槽盘头尖尾螺钉		6 个
M5×20 十字槽沉头平尾机牙螺钉		2 个

2.2 安装步骤

步骤1 钻孔。

根据明装盒的螺钉孔位，在墙上钻 6 个孔。

步骤2 安装膨胀管。

将膨胀管固定到孔里。

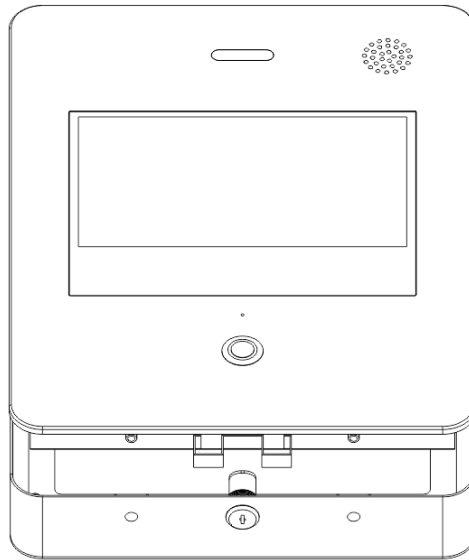
步骤3 固定明装盒。

通过螺钉（ST4.2×25 十字槽盘头尖尾螺钉），把明装盒固定到墙上。

步骤4 安装裸机。

1. 将明装盒底部的锁，处于打开位置（锁舌与明装盒垂直）。
2. 将裸机顶部以斜 45° 左右的角度，自下而上推送至明装盒顶部卡槽，使裸机顶部挂钩卡进卡槽，如图 2-1 所示。

图2-1 安装裸机顶部



3. 将裸机底部向明装盒推进，接触到锁舌时，边推送裸机边逆时针旋转钥匙，使裸机锁上明装盒。

步骤5 固定明装盒和裸机。

通过螺钉（M5×20 十字槽沉头平尾机牙螺钉），固定明装盒和裸机。

 说明

室内安装和室外安装采用的明装盒不同，详细区别如图 2-2 和图 2-3。

图2-2 室内安装图

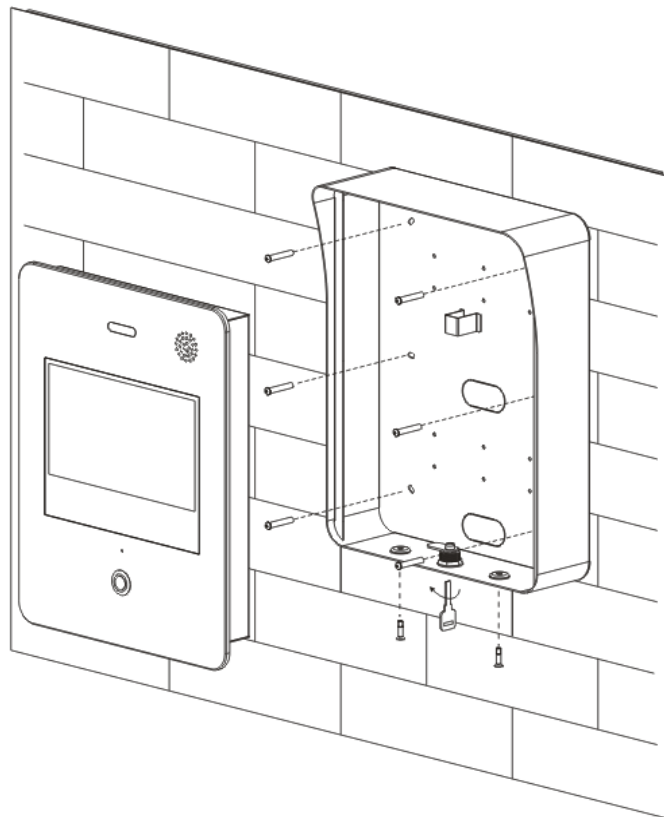
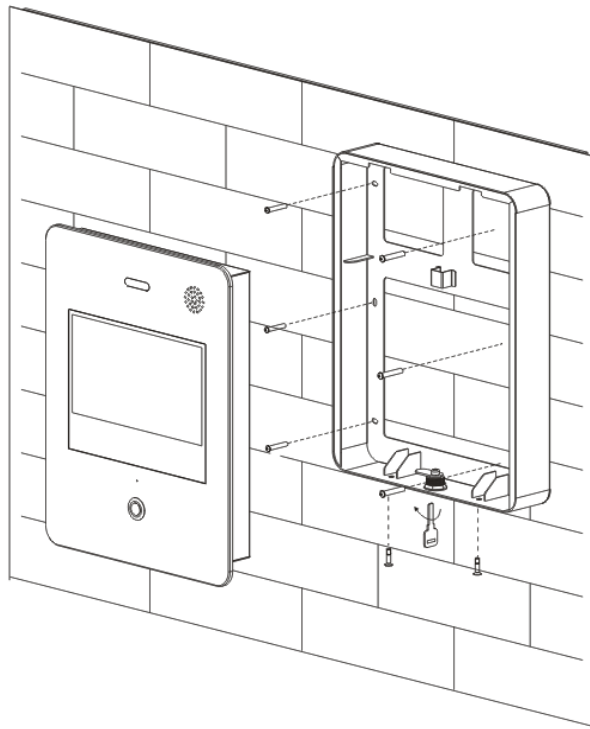


图2-3 室外安装图



- 调试前，调试人员应熟悉各种相关资料，了解设备的安装，连线和使用。
- 调试前，检测线路是否存在短路或开路情况。
- 检查线路一切正常后，再给设备上电。
- 调试结束后，清理现场（包括接头处理、设备固定等）。

3.1 设置本机信息

本机信息包括可视报警终端 IP 地址、系统时间等。

3.1.1 设置 IP 地址

可视报警终端出厂时默认 IP 地址为 192.168.1.110，使用可视报警终端前，需要修改 IP 地址为规划的 IP 地址。

步骤1 接通可视报警终端电源。

电源接通后，约 60s 后系统启动完毕进入工作状态。

步骤2 通过直连网线连接设备与 PC，设置 PC 的 IP 地址与可视报警终端 IP 地址在同一网段。

步骤3 在 PC 上使用 ping 可视报警终端 IP 命令检验网络。

如果网络互通，则继续执行步骤 4；如果网络不通，请检查线缆连接、IP 地址设置、设备正常上电等。

步骤4 登录可视报警终端 WEB 界面，修改 IP 地址。

1. 在浏览器地址栏中输入可视报警终端的默认 IP 地址，系统显示登录界面。
2. 输入用户名和密码，单击“登录”，如图 3-1 所示。

 说明

默认的用户名和密码是 admin 和 admin。首次登录成功后，请及时修改密码。

图3-1 登录界面



- 选择“系统设置 > 网络设置 > TCP/IP”，设置可视报警终端的 IP 地址、子网掩码和默认网关，单击“确定”，如图 3-2 所示。

修改完 IP 地址后，WEB 界面将会重启，直接跳转到新的 IP 地址界面。

图3-2 网络设置



表3-1 参数解释-网络设置

参数	说明
IP 地址	输入事先规划的 IP 地址，然后设置相应的 IP 地址的“子网掩码”和“默认网关”。
子网掩码	
默认网关	
MAC 地址	显示主机的 MAC 地址，不可更改
DNS 地址	DNS 服务器 IP 地址，建议保持默认值，如果组网中配置 DNS 服务器，则修改为组网中的 DNS 服务器 IP。

3.1.2 设置系统时间

登录 WEB 界面后，选择“系统设置 > 本机设置 > 系统时间”，设置系统日期、时间的显示格式，输入系统日期和时间，单击“确定”。

您也可以单击“同步 PC”，设置系统时间与本地 PC 的时间一致。

3.2 设置 FTP 信息

设置 FTP 之后，可以将数据信息存储在 FTP 服务器。

选择“系统设置 > 网络设置 > FTP 设置”，输入 FTP 服务器的 IP 地址、端口号、用户名和密码，单击“确定”。

3.3 功能调测

3.3.1 呼叫功能

如果已实现与管理平台或数字管理机对接，按可视报警终端上的“报警按钮”可以呼叫管理平台和数字管理机。

3.3.2 监视功能

管理中心可以对可视对讲终端发起监视监听，远程查看可视对讲终端的摄像头监视画面，同时可以获取语音。

3.3.3 刷卡巡更功能

刷卡巡更功能即巡逻人员可以在各个可视报警终端上刷卡，留下巡逻记录。巡逻人员到了巡逻点，将已发卡的卡贴到可视报警终端的刷卡区进行登记。

 说明

发卡在平台处实现。

3.3.4 广告投放

可以设置在不同时间段进行图片或者视频的投放，在显示屏处输出。

3.3.5 语音广播

接收管理中心发出的语音广播信息。

3.3.6 防拆功能

当可视报警终端被拆离墙面的时候，会发出报警声，同时向管理中心上报报警信息。

3.3.7 环境光补偿功能

可视报警终端在环境光线比较暗或夜里，采用摄像头自动感光技术，实现自动补光功能，以保证摄像画面更清晰。

本章介绍可视对讲终端 WEB 管理界面的各项参数配置。

4.1 登录 WEB 系统

步骤1 在浏览器地址栏中，输入可视对讲终端的默认 IP 地址。系统显示报警联网终端界面，如图 4-1 所示。

图4-1 本机设置



步骤2 输入用户名和密码。默认用户名和密码均为 admin。



说明

为保证系统的安全性，登录后，请及时修改设备的用户名和密码。

步骤3 单击“登录”，进入 WEB 界面。

4.2 系统设置

4.2.1 本机设置

本机设置

选择“系统设置 > 本机设置 > 本机设置”，进入“本机配置”界面。如图 4-2 所示。

图4-2 本机设置

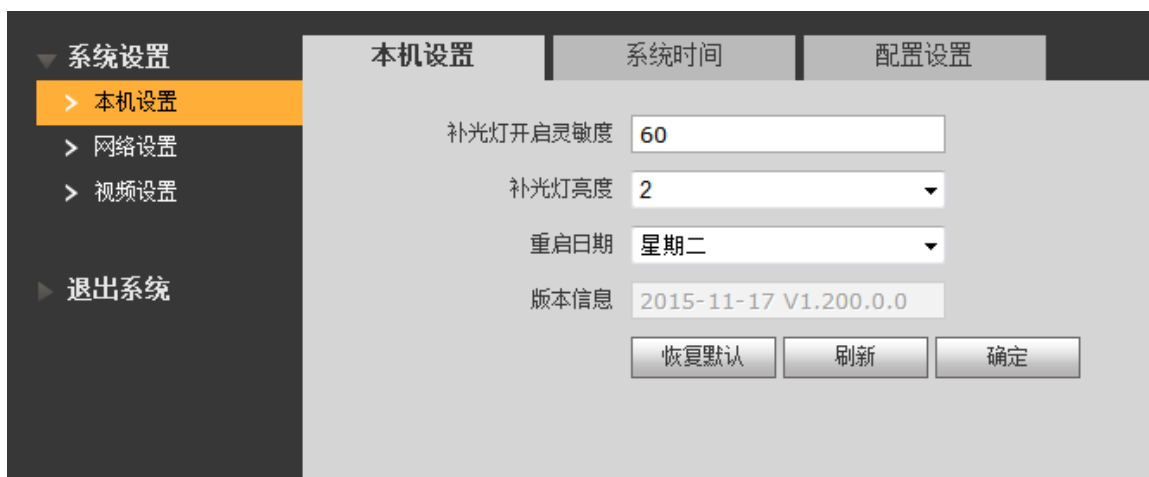


表4-1 本机设置

参数名	参数说明
补光灯开启灵敏度	0~255，默认设置为 60。外面光线较暗时，门口机呼叫平台，智能开启补光灯。
补光灯亮度	0~5， 值越高越亮，默认设置为 2。
重启日期	在设定日期的凌晨 2 点，自动重启可视报警终端。
版本信息	显示设备的软件版本号。
恢复默认	仅将当前“本机设置”页签的参数恢复到出厂状态。

系统时间

选择“系统设置 > 本机设置 > 系统时间”，进入“系统时间”界面。

您可以设置系统日期、时间的显示格式，输入系统日期和时间，单击“确定”。

您也可以单击“同步 PC”，设置系统时间与本地 PC 的时间一致。

配置设置

选择“系统设置 > 本机设置 > 配置设置”，进入“配置设置”界面。

配置设置实现恢复出厂设置、导出配置和导入配置。

4.2.2 网络设置

网络设置

设置可视报警终端的 IP 地址、子网掩码和默认网关。修改完 IP 地址后，WEB 界面将会重启，直接跳转到新的 IP 地址界面。

详细情况请参见“3.1.1 设置 IP 地址”。

FTP

设置 FTP 之后，可以将数据信息存储在 FTP 服务器。

选择“系统设置 > 网络设置 > FTP 设置”，输入 FTP 服务器的 IP 地址、端口号、用户名和密码，

单击“确定”。

主动注册配置

主动注册，当设备连接外网时，会主动向用户指定的服务器汇报当前所在位置，方便客户端软件通过服务器来访问设备，进行预览和监视。

前提条件

- 设备支持自动注册的功能。
- 有一台服务器，用于主动注册。

操作步骤

步骤1 选择“系统设置 > 网络设置 > 主动注册配置”，界面显示主动注册配置界面。

步骤2 勾选“主动注册”，输入服务器地址、端口号，如图 4-3 所示。

图4-3 自动注册



表4-2 主动注册

参数	说明
IP 地址	需要注册到的服务器 IP 地址。
端口	服务器用于主动注册的端口号。

步骤3 单击“确定”。

4.2.3 视频设置

视频设置

选择“系统设置 > 视频设置 > 视频设置”，进入“视频设置”界面。

您可以在“视频设置”界面设置视频效果，如图 4-4 所示。

图4-4 视频设置



表4-3 视频设置

参数名	参数说明
视频格式	设置摄像头采集视频的格式，包括：WVGA、D1。 WVGA 分辨率为 800×480；D1 分辨率为 704×576。
帧速	设置 N 制请选择 30 帧，P 制请选择 25 帧。
亮度	该阈值主要是通过线性的调节方式调节图像的整体亮度。值越大图像越亮，反之相反。
对比度	该阈值主要是调节图像的对比度。值越大图像明亮反差越大，反之越小。值设的过大时，图像暗的地方太暗，亮的地方容易过曝。
色度	该阈值主要调整色彩的纯度和饱和程度。
饱和度	该阈值主要调整颜色深浅。值越大彩色将更浓，反之相反。
增益调节	视频基本参数的增益上限。
情景模式	选择使用情况，自动、晴天、夜晚等情景。
日/夜模式	彩色处理的模式。
补偿模式	特殊环境下补偿。
镜像	使图像镜像显示。
翻转	使图像翻转显示。
时间显示	使时间显示在预览画面上。
恢复默认	视频效果和音量效果恢复为出厂设置。

音频设置

选择“系统设置 > 视频设置 > 音频设置”，进入“音频设置”界面。

您可以在“音频设置”界面设置麦克风和喇叭音量。

4.3 退出 WEB 系统

在“退出系统”界面，您可以执行“重启设备”或者“退出系统”操作。

单击“退出系统”后，系统返回登录界面。

附录1 技术规格

型号		DH-VTT2610C-C
系统	操作系统	嵌入式 LINUX 操作系统
	扩展卡	标配，但支持最大 32GB
视频	摄像头	130 万 CMOS 高清摄像头
	镜头	针孔，防暴
	视频宽动态	软件支持
	字符叠加	支持通道名称或者网点名称叠加在视频上
音频	输入	全指向麦克风
	输出	内置优质喇叭、支持外接有源音箱、喇叭
	音效增强	回声抑制和数字降噪
操作模式	按键	1 个机械按键
	刷卡	支持
报警	防拆报警	支持
	报警输入	2 路，可实现报警联动。
	报警输出	2 路，可实现报警联动。
结构&安装	材质	铝合金
	安装	支持明装
防护性能	防暴	IK09
	防水防尘	IP55
常规参数	电源	DC 12V~24V，或标准 POE 供电
	功耗	≤10W
	工作温度	- 30℃~+60℃
	相对湿度	10%~95%RH

装 箱 清 单

所列内容为本包装箱内应包括的设备和资料，请在开箱时认真检查，并妥善保管。

部件名称	数量	备注
<input type="checkbox"/> 主机	一台	
<input type="checkbox"/> 附件	一份	
<input type="checkbox"/> 产品说明书	一本	

商标声明

- 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。

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。

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。
- 不包含帐户名称或帐户名称的倒序。
- 不要使用连续字符，如 123、abc 等。
- 不要使用重叠字符，如 111、aaa 等。

2. 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. 开启帐户锁定

出厂默认开启帐户锁定功能，建议您保持开启状态，以保护帐户安全。在攻击者多次密码尝试失败后，其对应帐户及源 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. 启用白名单

建议您开启白名单功能，开启后仅允许白名单列表中的 IP 访问设备。因此，请务必将您的电脑 IP 地址，以及配套的设备 IP 地址加入白名单列表中。

8. MAC 地址绑定

请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。

9. 合理分配帐户及权限

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。

10. 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。

11. 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。

12. 使用 PoE 方式连接设备

如果设备支持 PoE 功能, 建议采用 PoE 方式连接设备, 使摄像机与其他网络隔离。

13. 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。

14. 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。

15. 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。