手机客户端

快速操作手册

V1.0.1

法律声明

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。

网络安全建议

保障设备基本网络安全的必须措施：

1.修改出厂默认密码并使用强密码

没有更改出厂默认密码或使用弱密码的设备是最容易被“黑”的。建议用户必须修改默认密码，并尽可能使用强密码（最少有 8 个字符，包括大写、小写、数字和符号）。

2.更新固件

按科技行业的标准作业规范，NVR、DVR 和 IP 摄像机的固件应该要更新到最新版本，以保证设备享有最新的功能和安全性。

以下建议可以增强设备的网络安全程度：

1.定期修改密码

定期修改登录凭证可以确保获得授权的用户才能登录设备。

2.更改默认 HTTP 和 TCP 端口

- 更改设备的默认 HTTP 和 TCP 端口这两个端口是用来进行远程通讯和视频浏览的。
- 这两个端口可以设置成 1025～65535 间的任意数字。更改默认端口后，减小了被入侵者猜到你使用哪些端口的风险。

3.使能 HTTPS/SSL 加密

设置一个 SSL 证书来使能 HTTPS 加密传输。使前端设备与录像设备间的信息传输被全部加密。

4.使能 IP 过滤

使能 IP 过滤后，只有指定 IP 地址的设备才能访问系统。

5.更改 ONVIF 密码

部分老版本的 IP 摄像机固件，系统的主密码更改后，ONVIF 密码不会自动跟着更改。你需要更新摄像机的固件或者手动更新 ONVIF 密码。

6.只转发必须使用的端口

- 只转发必须使用的网络端口。避免转发一段很长的端口区。不要把设备的 IP 地址设置成 DMZ。
- 如果摄像机是连接到本地的 NVR，你不需要为每一台摄像机转发端口，只有 NVR 的端口需要被转发。

7.关闭 SmartPSS 的自动登录功能

如果你使用 SmartPSS 来监控你的系统而你的电脑是有多个用户，请必须把自动登录功能关闭。增加一道防线来防止未经授权的人访问系统。

8.在 SmartPSS 上使用不同于其他设备的用户名和密码

万一你的社交媒体账户，银行，电邮等账户信息被泄漏，获得这些账户信息的人也无法入侵你的视频监控系统。

9.限制普通帐户的权限

如果你的系统是为多个用户服务的，请确保每一个用户只获得它的作业中必须的权限。

10. UPnP

- 启用 UPnP 协议以后，路由器将会自动将内网端口进行映射。从功能上来说，这是方便用户使用，但是却会导致系统自动的转发相应端口的数据，从而导致本应该受限的数据被他人窃取。

- 如果已在路由器上手工打开了 HTTP 和 TCP 端口映射，我们强烈建议您关闭此功能。在实际的使用场景中，我们强烈建议您不开启此功能。

11. SNMP

如果您不使用 SNMP 功能，我们强烈建议您关闭此功能。SNMP 功能限于以测试为目的的临时使用。

12. 组播

组播技术适用于将视频数据在多个视频存储设备中进行传递的技术手段。当前为止尚未发现有过任何涉及组播技术的已知漏洞，但是如果您没有使用这个特性，我们建议您将网络中的组播功能关闭。

13. 检查日志

如果您想知道您的设备是否安全，可以通过检查日志来发现一些异常的访问操作。设备日志将会告知您哪个 IP 地址曾经尝试过登录或者用户做过何种操作。

14. 对您的设备进行物理保护

为了您的设备安全，我们强烈建议您对设备进行物理保护，防止未经授权的物理操作。我们建议您将设备放在有锁的房间内，并且放在有锁的机柜，配合有锁的盒子。

15. 强烈建议您使用 PoE 的方式连接 IP 摄像机和 NVR

使用 PoE 方式连接到 NVR 的 IP 摄像机，将会与其它网络隔离，使其不能被直接访问到。

16. 对 NVR 和 IP 摄像机进行网络隔离

我们建议将您的 NVR 和 IP 摄像机与您的电脑网络进行隔离。这将会保护您的电脑网络中的未经授权的用户没有机会访问到这些设备。

概述

本文档描述了手机客户端的主要功能、安装及操作说明。

符号约定

在本文中可能出现下列标志，代表的含义如下：

符号	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
 电击防护	表示高压危险
 激光辐射	表示强激光辐射
	表示能帮助您解决某个问题或节省您的时间
	表示是正文的附加信息，是对正文的强调和补充

修订记录

编号	版本号	修订内容	发布日期
1	V1.0.1	1、 增加 GDPR 隐私提醒和更新文本档内容； 2、 增加法律声明和网络安全须知； 3、 更新前言中的符号约定。	2018.6.8

使用安全须知

下面是关于产品的正确使用方法以及预防危险、防止财产受到损失等内容，使用时请务必遵守。在使用此产品前，请认真阅读此手册并妥善保存以备日后参考。

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。
- 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。
- 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。

目录

法律声明 ..... **I**
网络安全建议 ..... **II**
前言 ..... **IV**
使用安全须知 ..... **V**
1 产品概述 **1**
1.1 产品简介 1
1.2 产品功能 1
2 安装 **2**
3 客户端操作 **3**
3.1 使用前准备 3
3.2 主界面介绍 3
3.3 添加设备 4
3.4 布撤防 5
3.5 实时预览 6
3.6 录像回放 7
3.7 删除设备 9
3.8 修改设备信息 9
3.9 报警消息查看 10

1 产品概述

1.1 产品简介

本产品是专为安防领域设计的一款优秀的移动平台监控软件。该软件结合移动设备特点，在传统的监控软件的基础上增加了布撤防、报警推送、P2P 功能支持等特色操作，可在 3G 和 WIFI 网络环境下实现对通道视频的实时预览回放功能。

本产品支持 IOS 和 Android 平台。

1.2 产品功能

- 支持若干个设备管理。
- 支持布撤防。
- 支持通道视频实时预览和回放。
- 支持报警信息推送。
- 支持报警信息视频复核。

2 安装

- IOS 用户请在 APP Store 搜索下载 iAMS 应用程序并进行安装。
- Android 用户请在 Google Play 中搜索下载 gAMS 应用程序并进行安装。

3 客户端操作

3.1 使用前准备

1. 报警控制器已正常运行，且手机客户端与设备处于同一网段中。若不是，请进行网络设置。
2. 开启设备的 P2P 功能。在 Web 客户端界面中，选择“设置 > 网络 > P2P”，进入 P2P 设置界面，如图 3-1 所示。勾选“启用”，单击“保存”，保存配置。若连接成功，则状态显示“在线”；若未连线，则显示“离线”。

图3-1 P2P 设置

说明

使用手机客户端时，TCP/IP 配置中的首选 DNS 服务器和备用 DNS 服务器建议设置为 8.8.8.8。

3.2 主界面介绍

打开软件，系统显示主界面，如图 3-2 所示。点击某一设备上的∨，展开菜单列表，如图 3-3 所示。

图3-2 主界面

图3-3 显示菜单列表

3.3 添加设备

步骤1　在主界面中，点击，进入设备信息设置界面，如图 3-4 所示。

步骤2　点击每一行，设置相应的参数内容。

设置序列号时需要点击，进入二维码扫描界面，如图 3-5 所示，扫描 Web 客户端 P2P 设置界面中的二维码，读取序列号。

说明

也可以扫描设备上粘贴的产品序号二维码，进行识别。

步骤3　点击，进行保存。

图3-4 添加界面

图3-5 二维码扫描

3.4 布撤防

步骤1　点击 

，进入布撤防操作界面，如图 3-6 所示。支持整体布防、在家布防、外出布防和立即布防。

步骤2　点击布防按钮，系统进行布防，如图 3-7 所示，按钮切换为撤防状态。

步骤3　再点击该按钮，可撤销布防。

点击“ 

”，查看各个防区的状态， 
表示防区有报警； 
表示防区处于打开状态； 
表示防区正常。

点击 

，实现有声报警。

点击 

，实现无声报警。

图3-6 布撤防界面

图3-7 布防界面

3.5 实时预览

点击 

，进入通道视频实时预览界面，如图 3-8 所示。

双击某一通道可全屏预览，如图 3-9 所示，此时左右滑动屏幕，可切换通道。

图3-8 实时预览

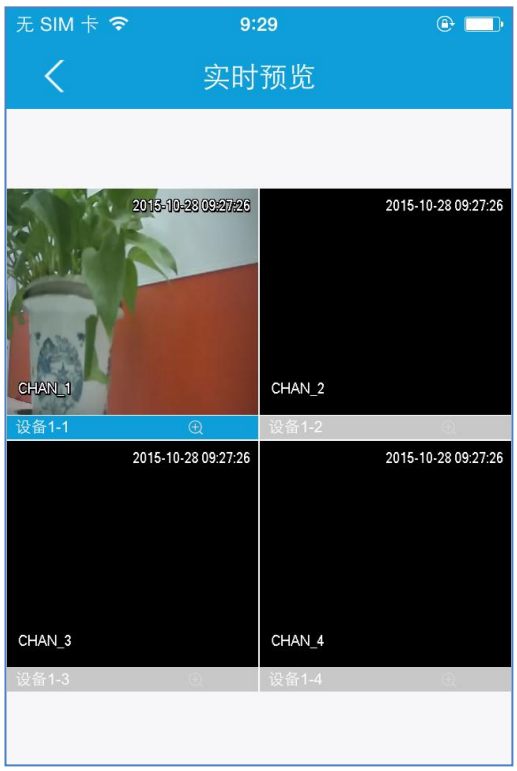
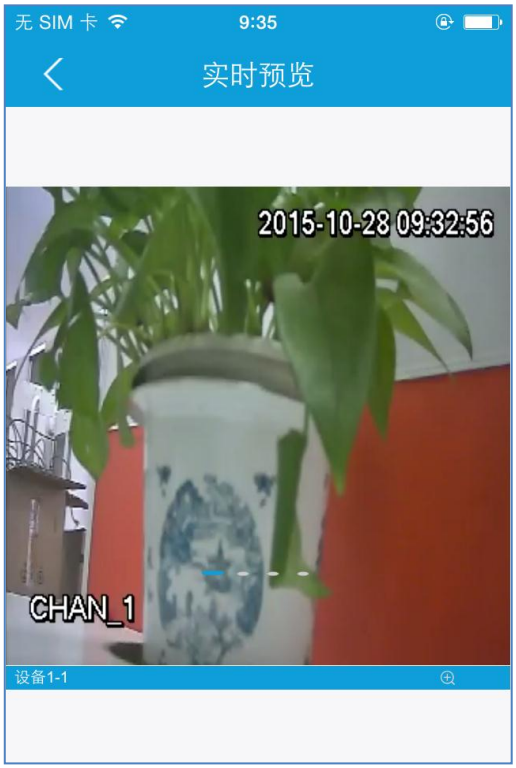


图3-9 全屏预览



3.6 录像回放

说明

- 回放前请确认该设备信息中设置的回放码流类型，若与实际录像的码流类型不符，则无法回放。
- 该回放功能实现的是硬盘中存储的视频录像回放。

步骤1　点击录像回放，进入回放界面。

步骤2　点击某一通道，进入录像时间和通道设置，如图 3-10 所示。

点击开始时间和结束时间，设置时间，再点击通道号选择播放通道。

图3-10 录像选择

步骤3 点击，返回回放界面，浏览录像内容，如图 3-11 所示。

双击该通道可全屏回放，如图 3-12 所示。

点击和，可以调节回放速率，支持 3 种快放速率：×2、×4、×8，以及 3 种慢放速率：×1/2、×1/4、×1/8。

点击，暂停回放。

点击，结束回放。

图3-11 录像回放

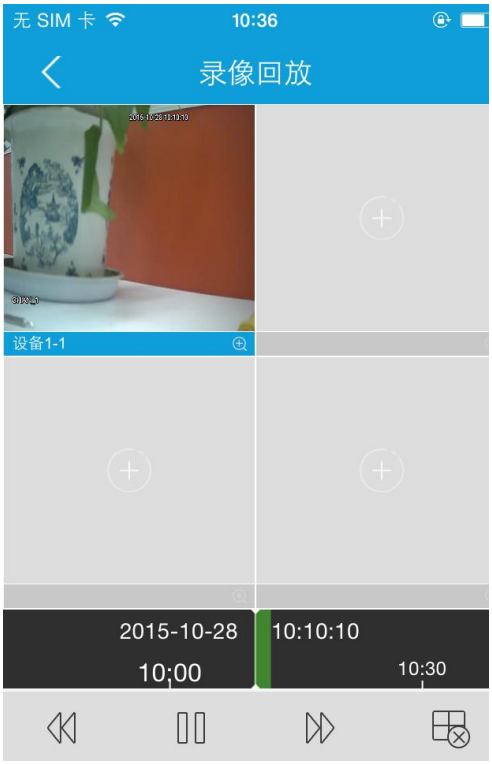
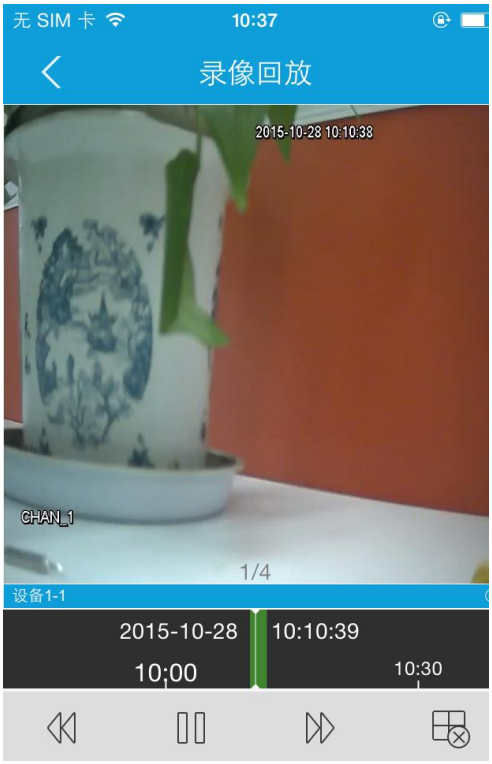


图3-12 全屏回放



3.7 删除设备

点击 

，弹出确认提示框，点击“确认”即可删除该设备。

3.8 修改设备信息

点击 

，下方弹出操作按钮，如图 3-13 所示。选择“编辑设备”，进入设备信息设置界面，具体修改操作请参见“3.3 添加设备”。

图3-13 修改设备信息

说明

Android 终端操作时，点击编辑，直接进入设备信息设置界面。

3.9 报警消息查看

点击，再点击，通过切换按钮，开启或关闭报警信息。开启订阅后，在界面中可以查看报警消息。