智能身份核验终端

快速操作手册

V1.0.1

前言

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。

修订记录

版本号	修订内容	发布日期
V1.0.1	修改表 2-1 设备接线中第二排颜色顺序	2020.08
V1.0.0	首次发布。	2020.01

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，并确保设备上未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

第 1 章 结构外观

图1-1 单屏外观尺寸（单位：mm）

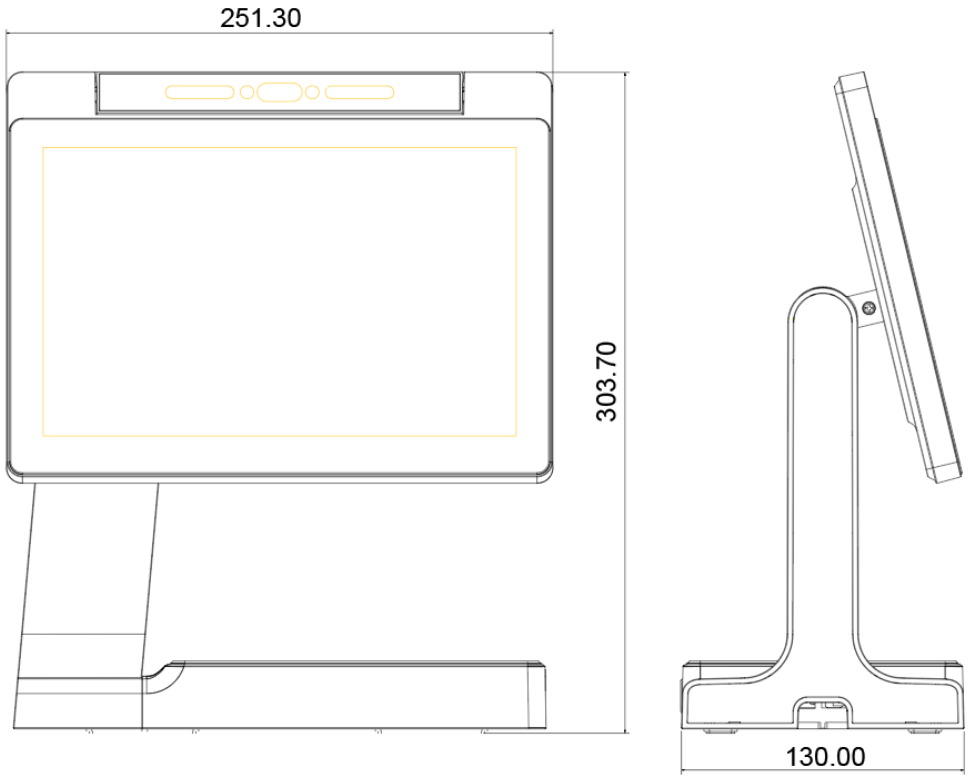
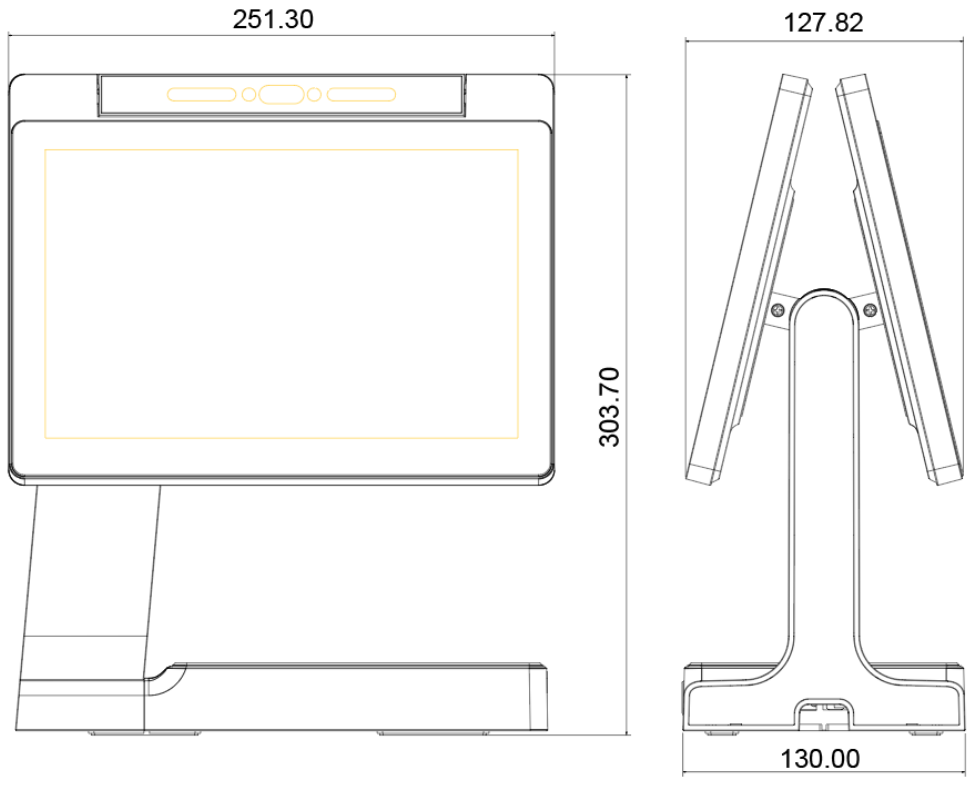


图1-2 双屏外观尺寸（单位：mm）



第 2 章 设备接线

设备底座如图 2-1 所示，设备的接线说明请参见表 2-1。

图2-1 设备底座

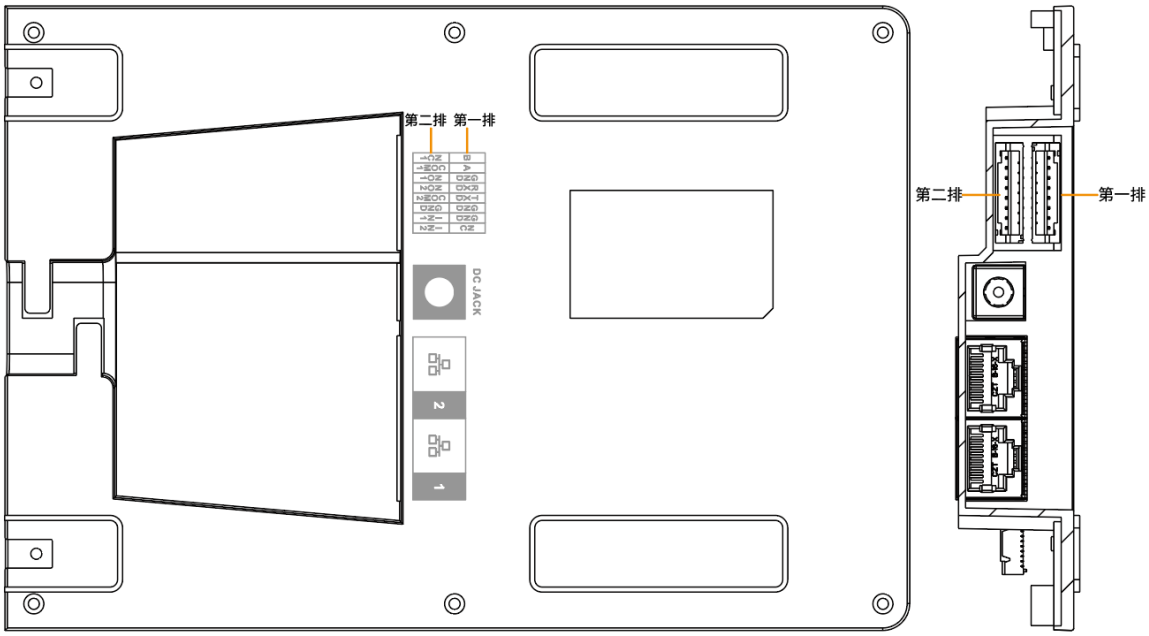


表2-1 设备接线

端口	线缆颜色	线缆名称	说明
第一排	紫色	B	RS-485 负输入
	黄色	A	RS-485 正输入
	棕色	GND	参考地
	绿色	RXD	RS-232 接收
	白色	TXD	RS-232 发送
	蓝色	GND	参考地
	黑色	GND	参考地
	红色	NC	悬空
第二排	红色	NC1	继电器 1 输出常闭端口
	黑色	COM1	继电器 1 输出公共端口
	蓝色	NO1	继电器 1 输出常开端口
	白色	NO2	继电器 2 输出常开端口
	绿色	COM2	继电器 2 输出公共端口
	棕色	GND	参考地
	黄色	IN1	报警 1 输入端口
	紫色	IN2	报警 2 输入端口

第 3 章 系统操作

3.1 设备初始化

设备初次上电启动时，需要设置 admin 用户密码和手机号，该用户名和密码用于登录设备。

图3-1 设备初始化

- 若忘记设备管理员密码，可通过手机号重置密码。
- 密码可设置为 8 位～32 位非空字符，可以由大写字母、小写字母、数字和特殊字符（除“'”、“"”、“;”、“:”、“&”外）组成 ，且至少包含 2 类字符。新密码和确认密码需保持一致。请根据密码强弱提示设置高安全性密码。

3.2 添加用户

通过录入编号、姓名、人脸等信息添加新用户。

步骤1 在主界面中，单击。

步骤2 使用管理员权限登录系统，选择“人员管理 > +新增”。

步骤3 设置参数，详细参数说明请参见表 3-1。

图3-2 新建用户

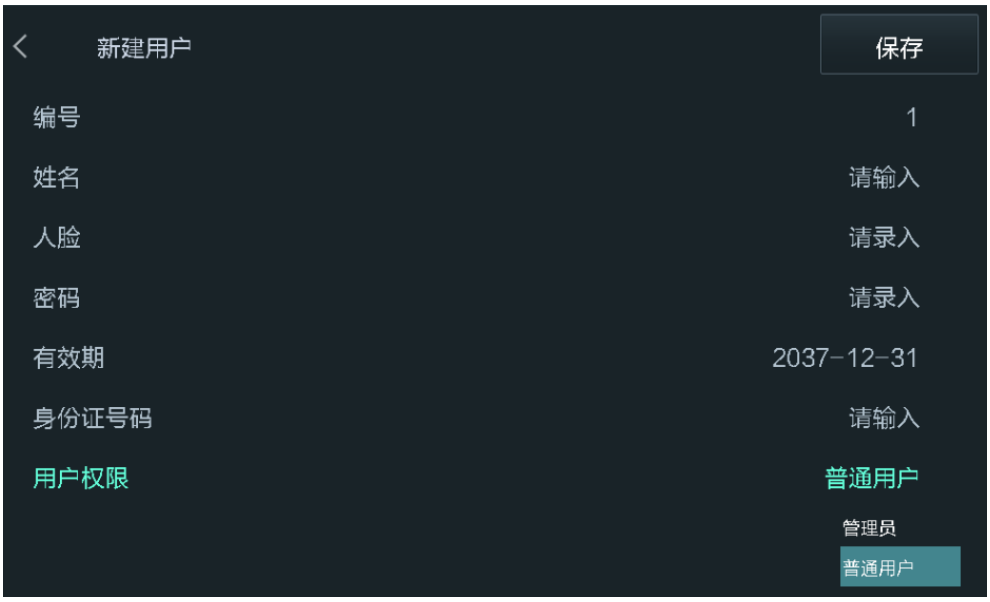


表3-1 新建用户参数说明

参数	说明
编号	输入用户编号，用于识别不同的用户，每个编号都是唯一的，最多支持 18 个字符（包括数字、字母或者数字和字母的组合）。例如：工号。
姓名	输入用户姓名，最多支持 10 个汉字或者 32 个字符（包括数字、符号和英文）。
人脸	注册时请将人脸放置于采集框中心区域，自动完成抓拍，如对抓拍到的图片不满意，则选择重新录入。
密码	管理员用户登录后台的密码，密码支持 1 位～8 位数字。
有效期	设置该用户身份核验有效时间。
身份证号码	输入用户的身份证号码。
用户权限	设置用户权限。 ● 普通用户，仅有身份核验权限。 ● 管理员，可登录设备后台，配置设备相关参数。

步骤4　参数配置完成后，按保存。

3.3 系统模式

系统模式有三种，分别为人证核验系统、访客系统、自助采集系统。

人证核验系统

支持人证模式和人脸模式核验身份。

步骤1　在主界面中，单击  。

步骤2　使用管理员权限登录系统，选择“系统模式 > 人证核验系统”。

步骤3　选择“模式设置 > 人证模式或人脸模式”。

访客系统和自助采集系统

只支持人证模式，采集身份信息上报给平台。

步骤1　在主界面中，单击  。

步骤2　使用管理员权限登录系统，选择“系统模式 > 访客系统或自助采集系统”。

3.4 模式设置

3.4.1 人证模式

人证核验系统下的人证模式

在主界面上将身份证放入身份证刷卡区，人脸对准人脸识别区即可。

图3-3 人证模式

访客系统和自助采集系统

以自助采集系统为例，在主界面上将身份证放入身份证刷卡区，人脸对准人脸识别区，自动完成抓拍，如对抓拍到的图片不满意，则选择重新采集。

3.4.2 人脸模式

说明

已在“设备管理-人员管理”新增用户并录入人脸，且模式设置为“人证核验模式-人脸模式”。在主界面直接用人脸对准人脸识别区即可。

图3-4 人脸模式

第 4 章 WEB 操作

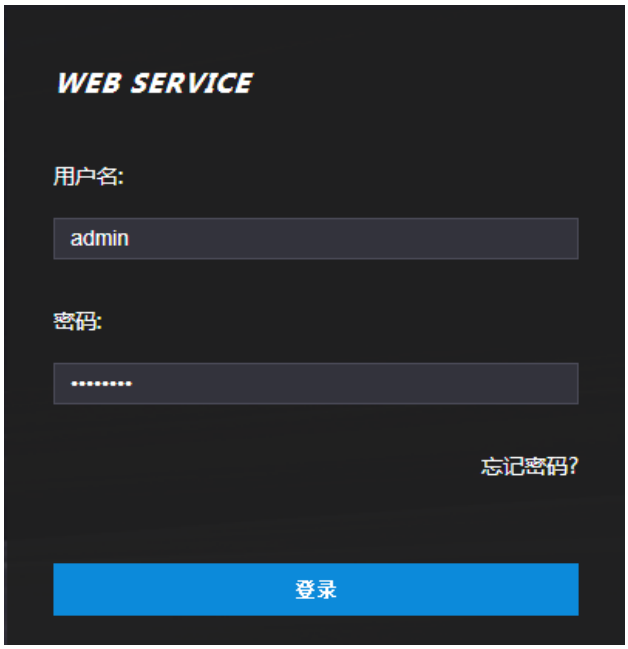
在 WEB 界面配置设备的网络参数、视频参数等，具体请参见配套使用说明书，本文只介绍 WEB 登录。

PC 与设备在同一局域网内。

步骤1　打开 IE 浏览器，在地址栏里输入设备的 IP 地址（默认地址为 192.168.1.108），按【Enter】键。

步骤2　输入“用户名”和“密码”。

图4-1 web 登录



- 设备默认管理员用户名为 admin，密码为设备初始化时设置的登录密码。为确保安全，建议定时更改管理员密码，并妥善保存。
- 如果遗忘了 admin 的登录密码，可单击“忘记密码”进行重置，重置密码的详细操作请参见配套使用说明书。

步骤3　单击“登录”。

第 5 章 常见问题

1. **身份证模块无法正常识别**
   请确认身份证是否是二代身份证或者是否放在正确的刷卡区域。
2. **忘记管理员密码导致无法执行相关设置**
   本地添加的管理员忘记管理员密码无法进入后台请使用工具恢复出厂设置，若管理员数量未满，请使用配套的平台添加一个管理员，或者联系技术支持人员。
3. **自己的身份证总是核验失败**
   请确认在人证核验时，周围是否有其他人脸出现。

附录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。

附录2 网络安全建议

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

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。

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. 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。

11. 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。