DS-K3B501SC 系列摆闸

用户手册

法律声明

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，海康威视可能对本手册进行更新，如您需要最新版手册，请您登录海康威视官网查阅（***http://www.hikvision.com***）。
海康威视建议您在专业人员的指导下使用本手册。

商标声明

- HIKVISION 海康威视 为海康威视的注册商标。
- 本手册涉及的其他商标由其所有人各自拥有。

责任声明

- 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。海康威视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康威视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。
- 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，海康威视不对因此造成的产品工作异常、信息泄露等问题承担责任，但海康威视将及时为您提供产品相关技术支持。
- 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。
- 如本手册内容与适用的法律相冲突，则以法律规定为准。

数据安全声明

- 您在使用产品的过程中，将收集、存储与使用个人数据。海康威视在产品开发过程中，贯彻个人数据保护原则。例如，若您使用具备人脸识别功能的设备，生物识别数据将经加密

处理，存储于您的设备；若您使用指纹设备，您的设备仅存储指纹模板，而非指纹图像，指纹模板无法被还原至指纹图像。

- 作为数据控制者，您在收集、存储与使用个人数据时，须遵循所适用的个人数据保护相关的法律法规，包括但不限于，对个人数据采取保护措施，例如，对设备进行合理的权限管理、加强设备应用场景的物理安全、定期进行安全评估等。

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。

安全注意事项

警告

- 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。
- 本产品必须可靠接地。
- 本产品不需要更换电源，如有特殊情况，请使用正规厂家提供的电源模块。
- 在接线、拆装等操作时请一定要将电源断开，切勿带电操作。
- 如果维修时必须打开盖子或门，且同时需要上电，请注意：
  1. 维修时务必断开风扇的电源，以免维修人员无意间接触造成机械伤害。
  2. 维修人员请勿接触裸露的高压带电部件。
  3. 维修后务必保证空开接线顺序是正确的。
- 每月进行一次漏电保护检查：将空开上的橙色按钮按下，空开会跳至断电状态，再将空开上电即可。
- 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）。
- 控制器重启时，请退出通道。

注意

- 人行通道产品的主要成分之一是不锈钢，不锈钢具有良好的不锈性（抵抗大气氧化的能力）和耐蚀性（在含酸、碱、盐的介质中耐腐蚀的能力），但其抗腐蚀能力会随其自身化学成分、使用环境等因素而改变。为了保持不锈钢的美观，延长使用寿命，需要对其定期进行保养维护。维护注意事项如下：
  1. 不同使用环境下需要选用不同规格的不锈钢，一般环境下可以选用 304 不锈钢，海边、化工厂等环境下建议选用 316 不锈钢。
  2. 保持产品表面清洁和干燥。
  3. 当产品表面出现污物时，可以用无纺布和酒精进行清洁。
  4. 当产品表面出现锈斑时，可以使用百洁布（切记不可用钢丝清洁球）在锈斑处顺着纹路来回擦拭直至清除，然后用无纺布和不锈钢保养剂整体擦拭一遍。
  5. 需要定期用无纺布和不锈钢保养剂对闸机整体擦拭进行保养维护。一般情况下建议一个月一次；若环境比较恶劣（如海边、化工厂等）建议一周一次。
- 请不要使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）。
- 请不要在高温、低温或者高湿度的环境下使用设备，具体温、湿度要求参考设备的参数表。
- 请勿在潮湿环境下操作。
- 请勿在易爆环境中操作。
- 避免接触裸露电路。产品加电时，请勿接触裸露的接点和部件。
- 设备仅适合安装在混凝土或不易燃的表面。

适用型号

产品名称	型号	说明
翼闸	DS-K3B501SC-L	左边道
	DS-K3B501SC-M	中间道
	DS-K3B501SC-R	右边道

目 录

第 1 章 产品简介

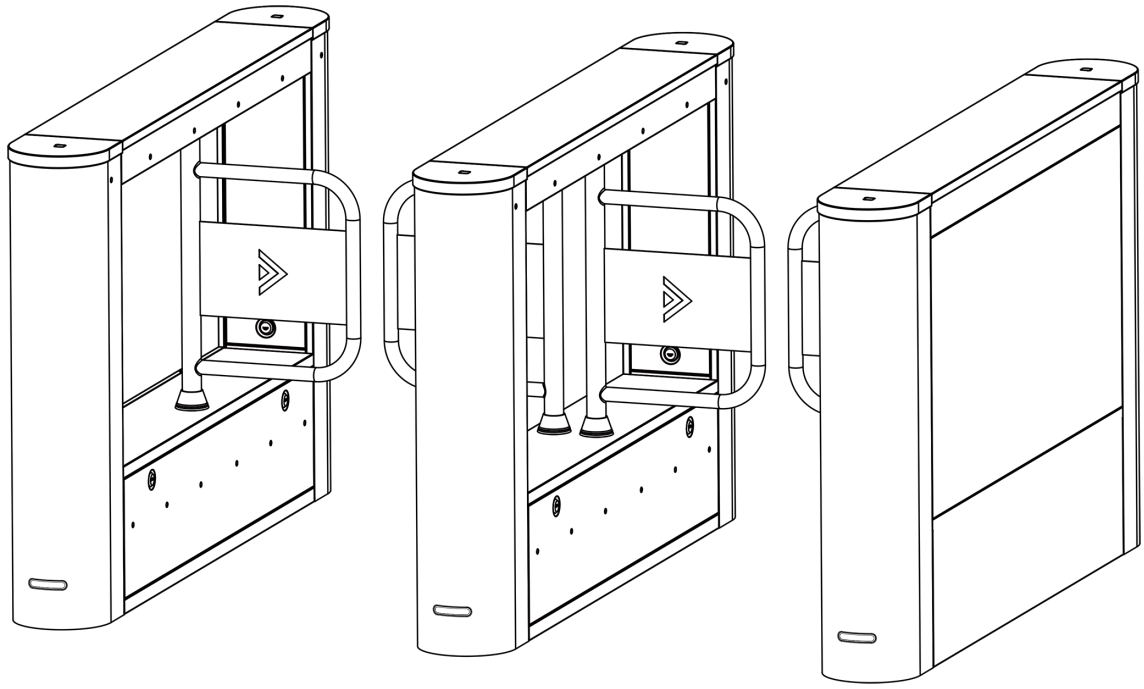


图 1-1 外观

- 32 位高速处理器，性能强劲、速度快
- 支持 TCP/IP 网络通信，网速自适应。通讯数据采用特殊加密处理，更安全
- 支持身份验证，经授权人员才可通过
- 可选择常开、常闭模式，支持双向通行，可根据人流量情况设定门翼开关速度
- 支持防尾随跟踪控制功能，防止非授权人员通行
- 支持防夹功能
  在门翼转动过程中遇阻时，在规定的时间内电机停止工作。
- 支持防冲功能，在未收到开门信号时，门翼会自动锁死。
- 支持自检测、自诊断、自动报警功能
- 支持声、光报警功能：当有误闯、尾随通行、翻越、反向闯入事件发生时，权限控制器蜂鸣器开始鸣叫
- 支持 IP 冲突检测
- 支持远程控制管理功能
- 支持可联网或脱机运行
- 支持 LED 通行方向指示，显示通行状态
- 支持断电通行，断电时闸门自动开启，人员可自由通行
- 支持消防报警后通行，消防信号触发后，闸门将自动开启，供人员紧急疏散

- 支持自动复位功能，可设定人员通行时间。开门后，在规定的时间内未通行时，系统将自动取消用户的本次通行的权限
- 支持按计划模板开关闸门
- 最多支持添加来宾卡 3000 张，非来宾卡 60000 张
- 最多可记录刷卡记录 180000 条
- 支持自定义语音播报内容

第 2 章 布线说明

安装和接线的前期准备工作。

操作步骤

1. 以最靠边的通道中心为基准，划两条平行线，其间距 L+200 mm (L 为通道宽度)。

2. 确定各机箱的安装孔位和出线孔并进行开槽和挖孔。

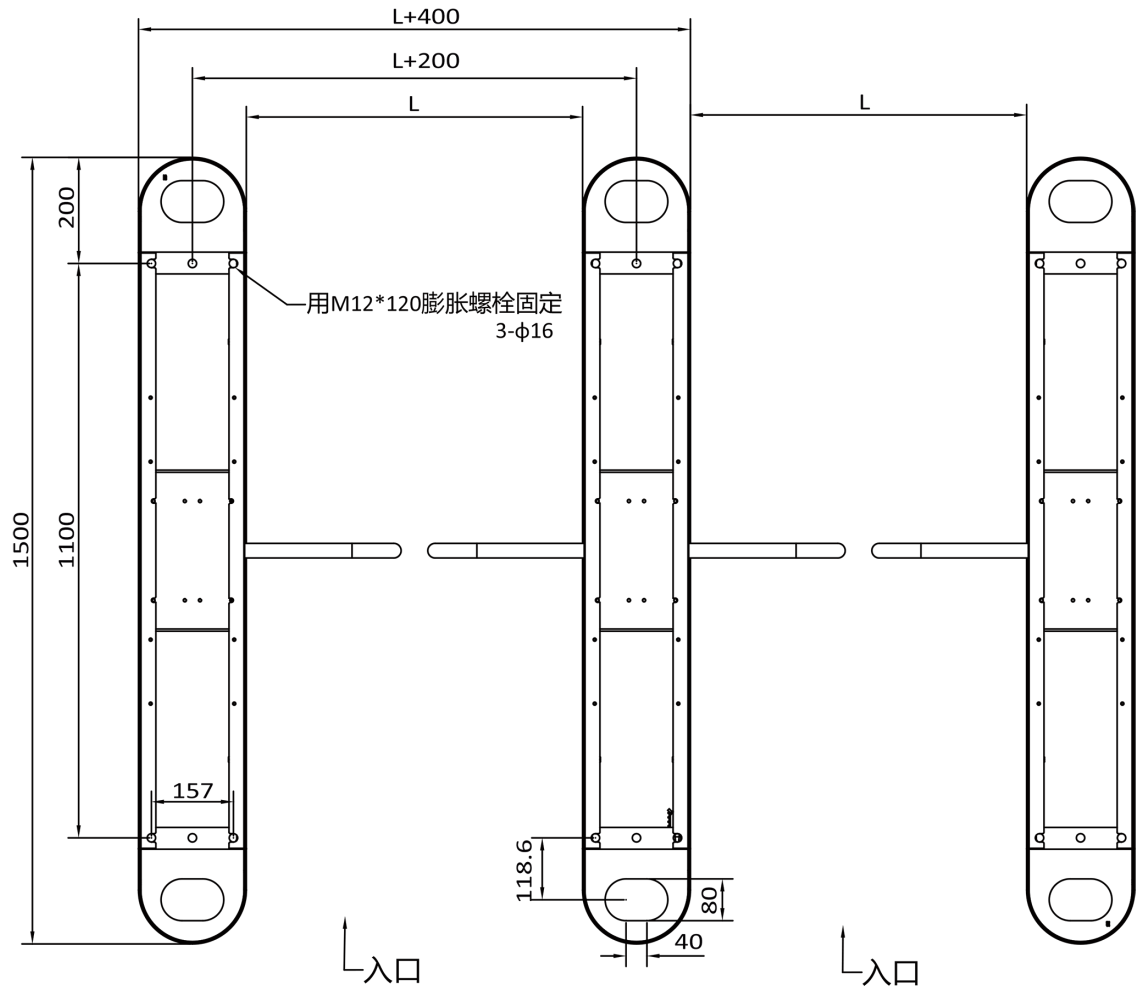


图 2-1 开孔图

3. 预埋线。

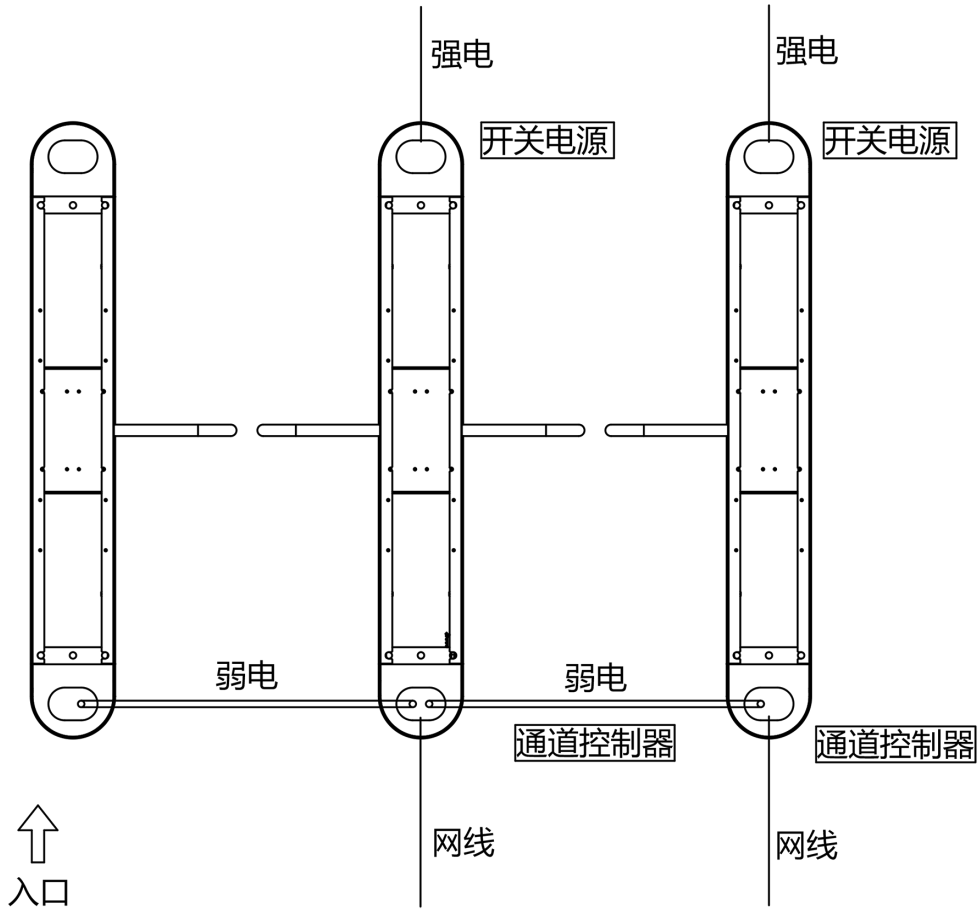


图 2-2 布线图（无人脸识别模块）

说明

- 同步线长 5.5 米。
- 走同步线的线管内径建议大于 30mm。
- 若需要在同一方向同时走强电线和同步线，需要强电线（交流电线）与同步线分管，保证互不干扰。
- 若需要额外连接外接设备时，视实际情况增加同步线管径或另挖一个线槽。
- 设备外接强电线缆需为加强（双重）绝缘线。
- 连接网络时建议使用超五类或性能更好的网线，线长建议不超过 100 m。

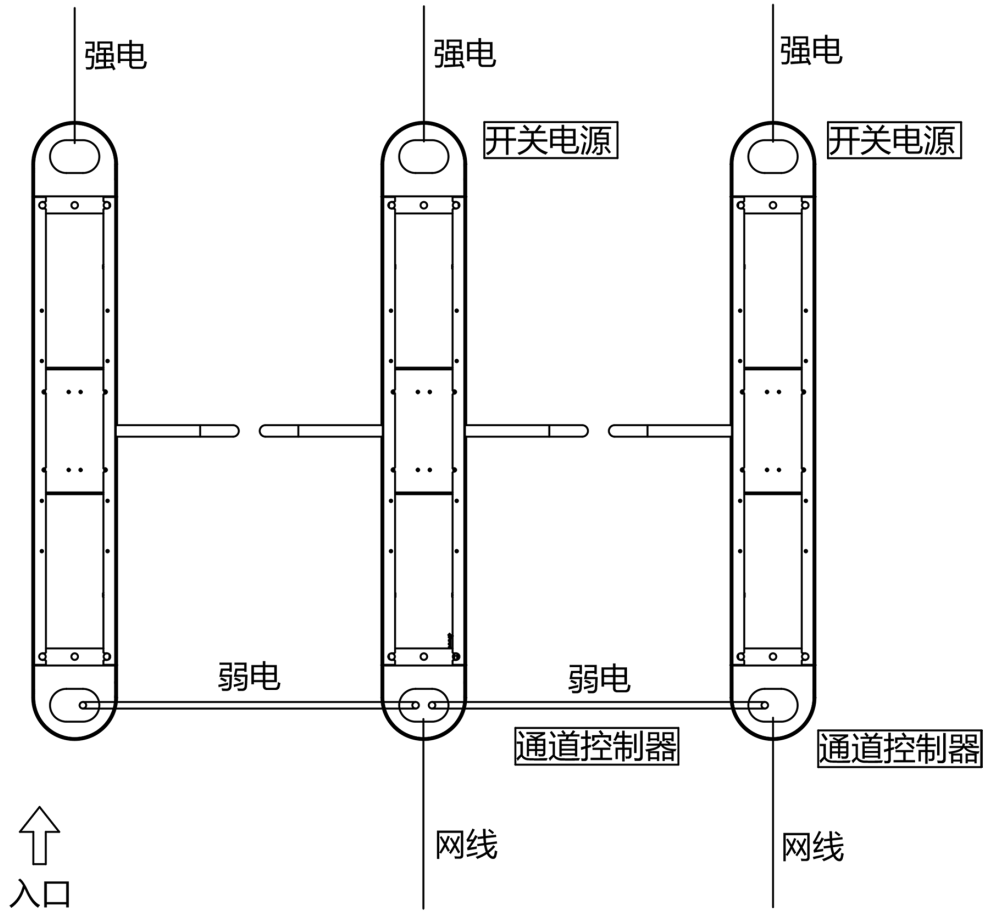


图 2-3 布线图（带人脸识别模块）

说明

- 左边道人脸识别模组从开关电源取电，开关电源从市电取电。
- 左边道及中间道需要预埋人脸开关量的同步线。
- 同步线长 5.5 米。
- 走同步线的线管内径建议大于 30mm。
- 若需要在同一方向同时走强电线和同步线，需要强电线（交流电线）与同步线分管，保证互不干扰。
- 若需要额外连接外接设备时，视实际情况增加同步线管径或另挖一个线槽。
- 设备外接强电线缆需为加强（双重）绝缘线。
- 连接网络时建议使用超五类或性能更好的网线，线长建议不超过 100 m。

第 3 章 安装

3.1 拆卸人行通道

在安装之前，您需要先使用钥匙打开整机机箱拆卸，具体门锁及孔位见下图所示说明。

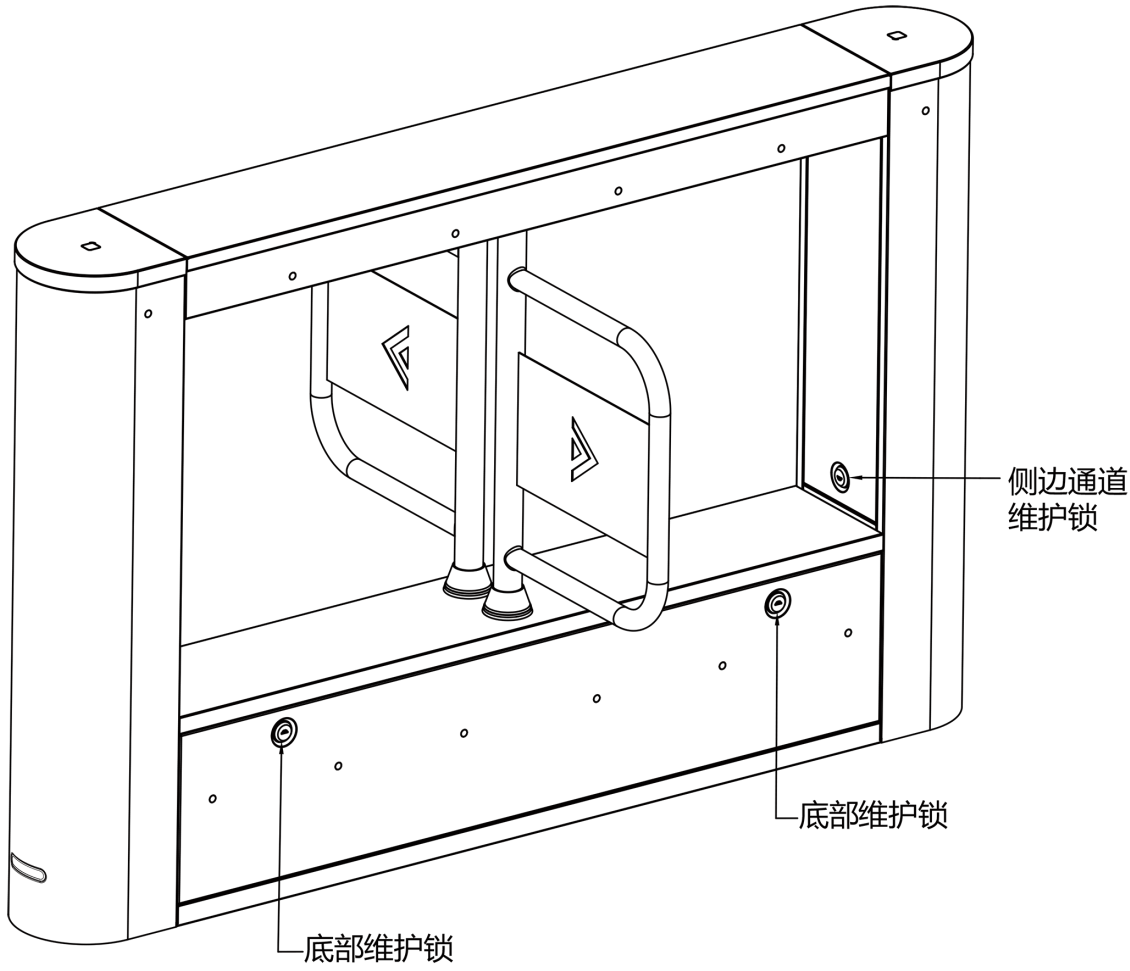


图 3-1 人行通道锁孔位置

说明

为避免短路，每次维护后请进行检查，防止螺钉及金属件掉落在强弱电模块中。

3.2 安装超级电容（选配）

超级电容可在断电状态下为主通道控制板和从通道控制板供电，实现设备在断电时自动开门，并处于开门状态。

操作步骤

说明

- 超级电容的位置如 *部件介绍* 中所示。
- 超级电容工作温度：-40 ℃ ~ 70 ℃
- 超级电容为选配配件。

1. 安装超级电容。
   1) 拧松超级电容结构件螺丝拆卸结构件。
   2) 放入超级电容后再重新安装结构件并拧紧螺丝固定在人行通道上。
2. 把超级电容插头插入通道控制板上的超级电容接入口中。

注意

主通道控制板和从通道控制板上均有超级电容接入接口，且主从通道板上均需要接入超级电容，否则断电自动开门功能会存在异常。

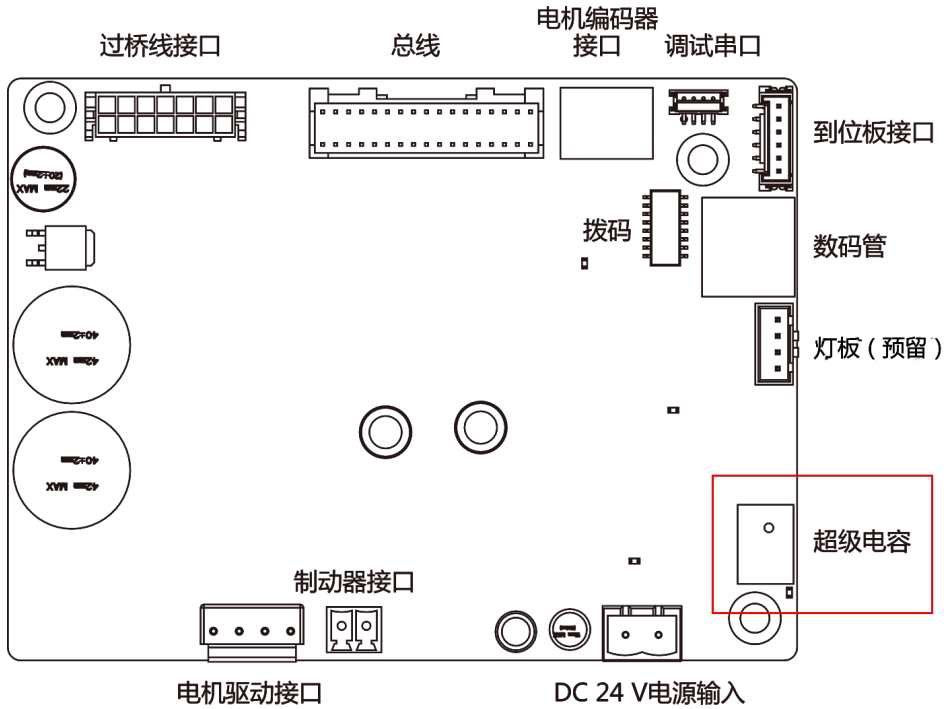


图 3-2 接入超级电容

3.3 安装人行通道

- 仅适宜安装在混凝土或不易燃的表面。
- 若安装位置靠墙，则墙面与闸机的直线距离至少为 10 mm，否则无法打开闸机。

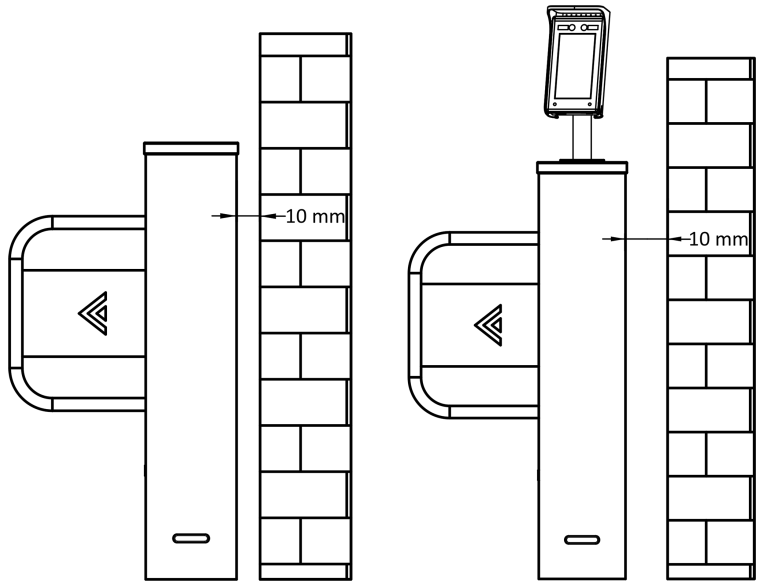


图 3-3 靠墙距离

- 双通道设备尺寸图如下所示。

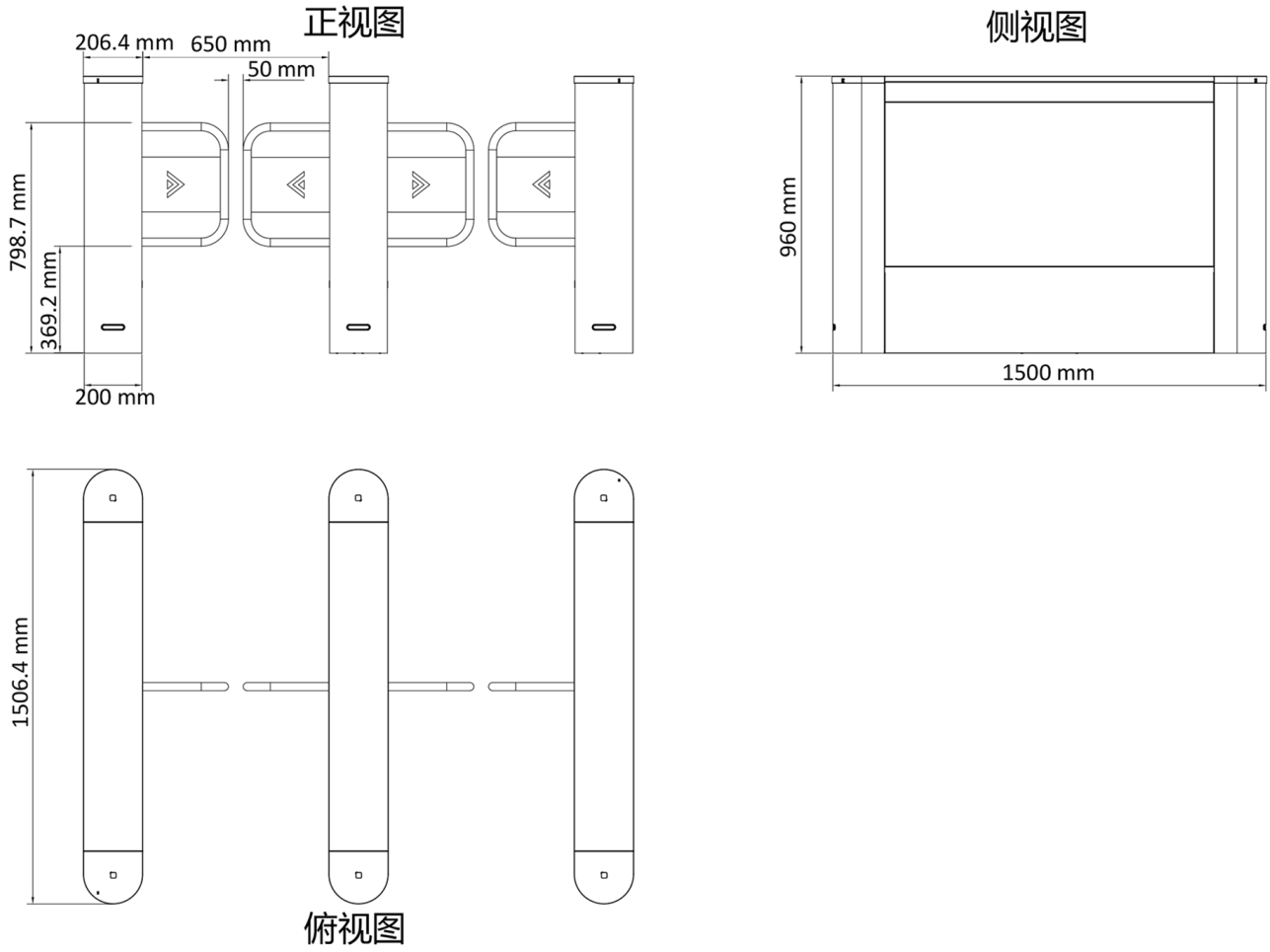


图 3-4 双通道设备尺寸图

操作步骤

1. 准备安装设备的工具，清点配件，整理安装设备的地基基面。

2. 确定安装孔位位置之后，钻孔，埋下膨胀螺丝。

3. 根据人行通道上的标签进出方向，将人行通道分别搬到相应的安装位，逐个对准地脚螺栓并拧紧螺母。

说明

避免人行通道腔体浸泡在水中，特殊情况下，浸泡高度不得超过 150 mm。

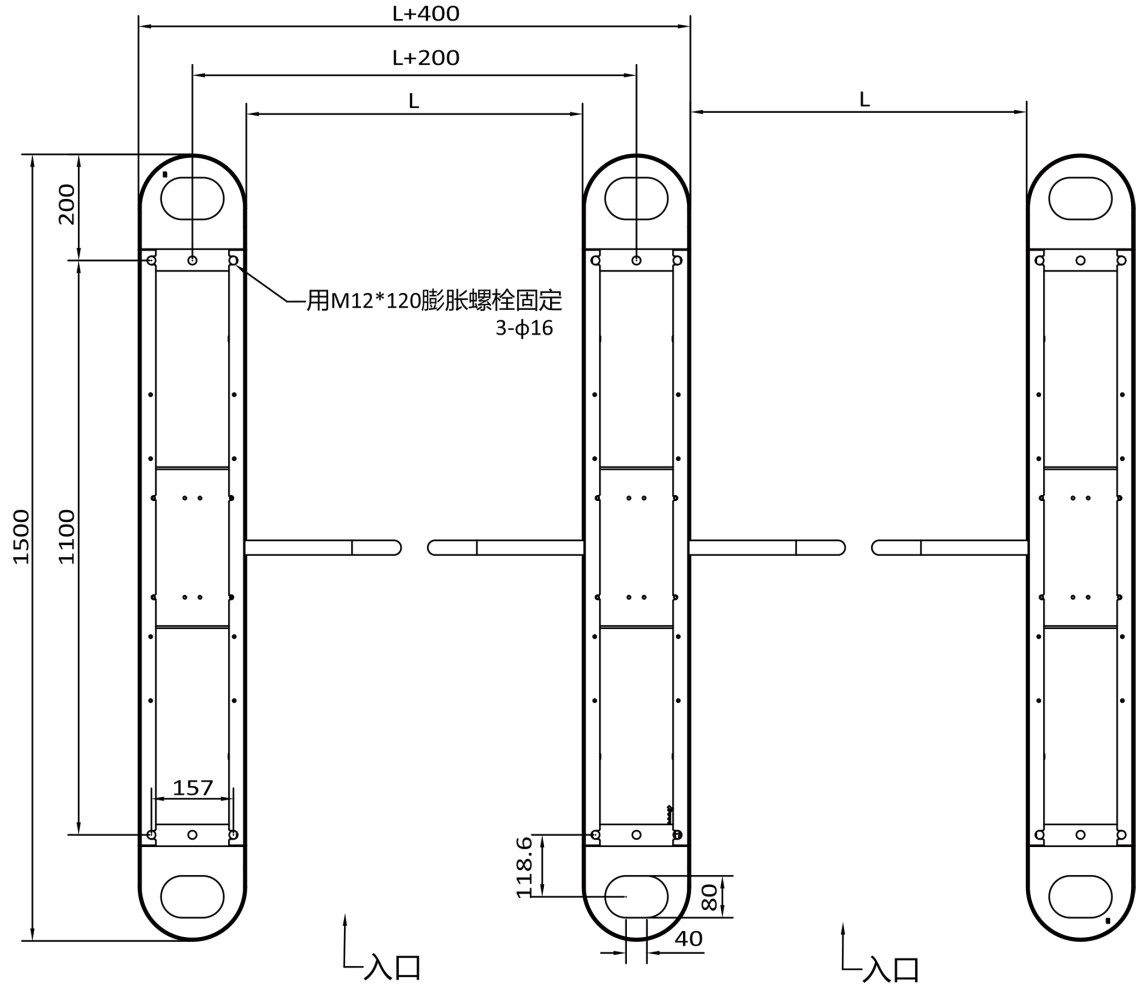


图 3-5 双通道安装仰视图

第 4 章 接线

4.1 部件介绍

设备出厂时，基本的电气连接线缆已经连接完毕，用户安装时只需要连接同步线，就可以实现通道之间的正常通讯、并接入市电为整个系统供电。市电输入范围为 AC 100 ~ 240 V，50 ~ 60Hz。

设备具体电器部件位置如下图所示。

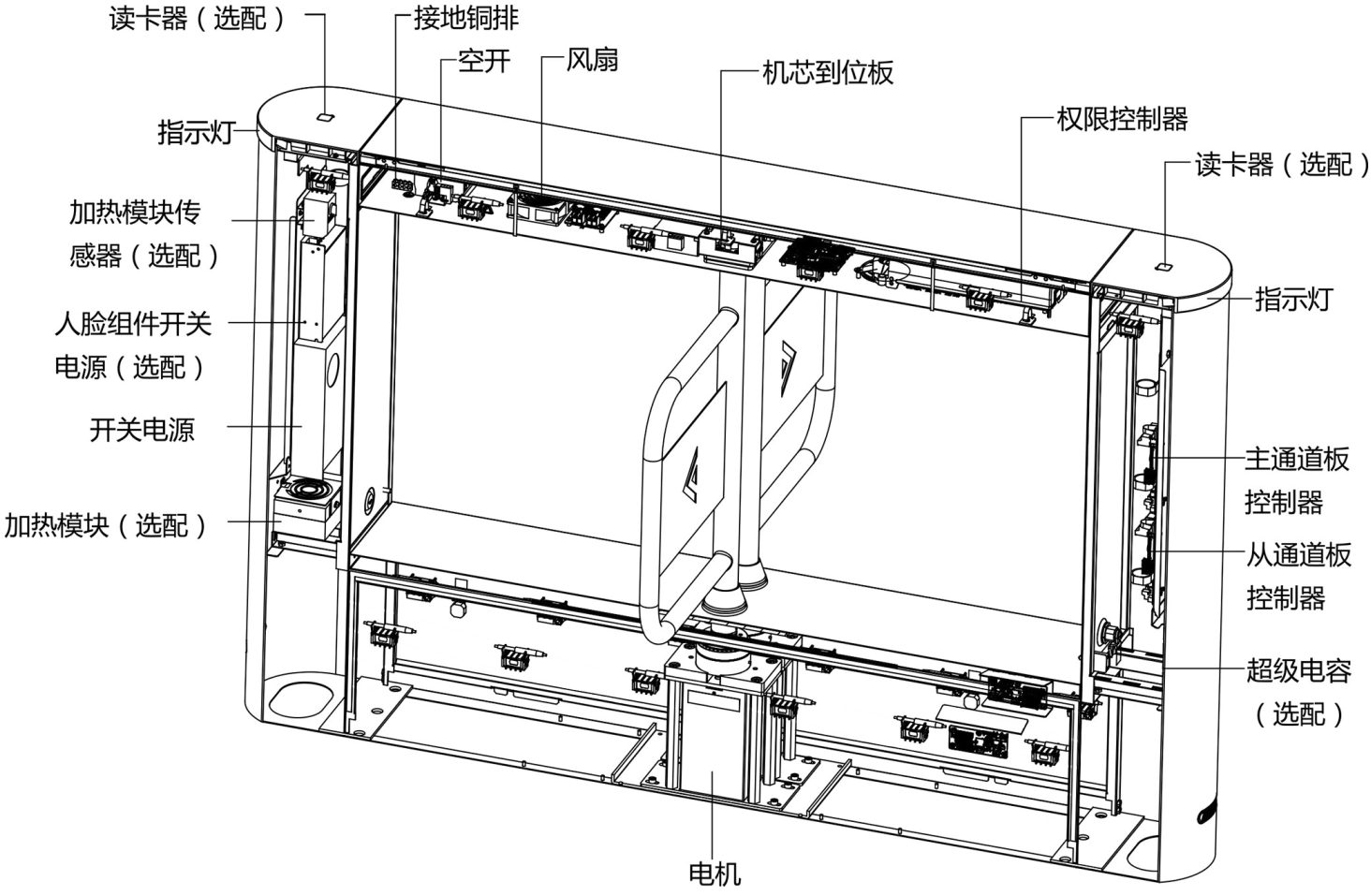


图 4-1 部件介绍

设备具体红外转接模块、红外发射/接收模块位置及对应编号如下图所示：

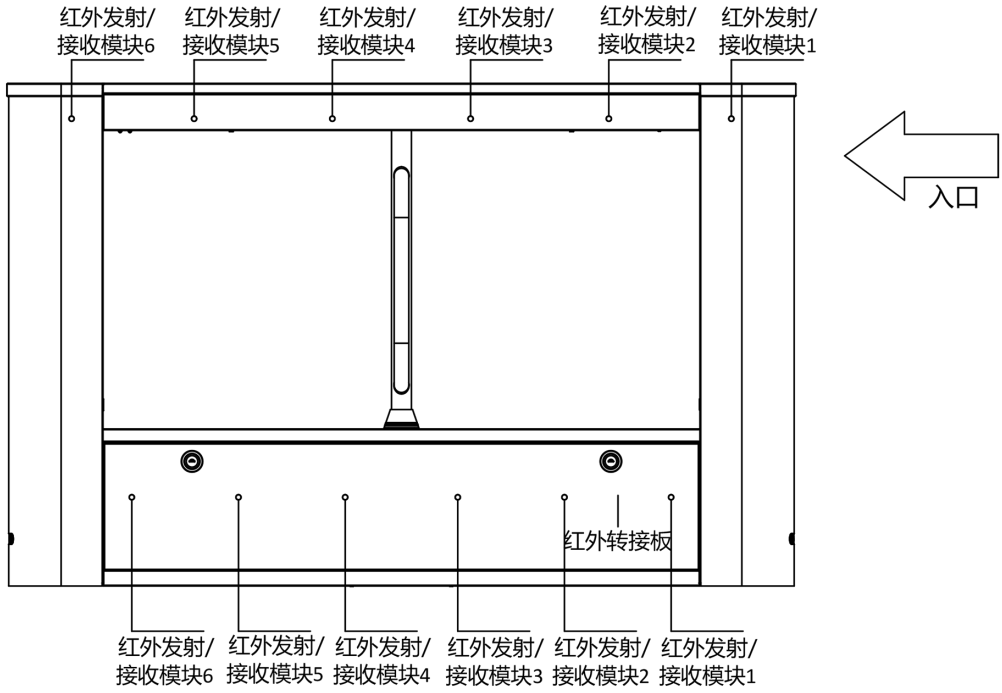


图 4-2 红外发射/接收模块及红外转接模块说明

说明

以入口方向为基准，若为双通道闸机，左边道上的为红外发射模块，右边道上的为红外接收模块，中间道的左侧为红外接收模块、右侧为红外发射模块。

4.2 系统进线

将市电接到电控柜里面的空气开关上，标识为 L、N、PE。空气开关上面为 L（火线）、N（零线），黄绿色的为 PE 端子，需要接地。

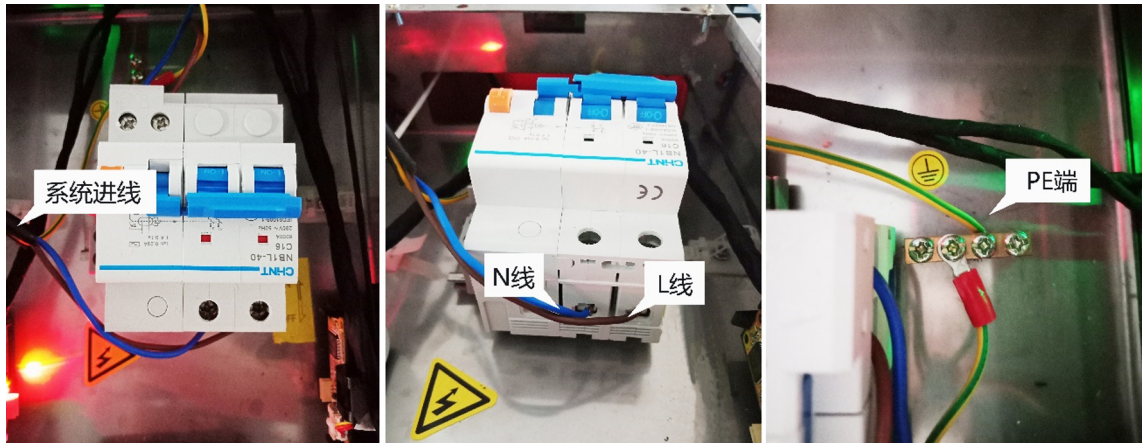


图 4-3 系统进线介绍

注意

PE 端必须接地，避免人员触碰设备时造成伤害。

说明

- 线缆（尤其是裸线线缆）剥开绝缘皮的长度不应超过 8mm，建议剥线后浸锡，如果有条件，浸锡后可以在绝缘前方加上绝缘帽，严禁接线后有裸露端子或者线丝露出。
- 接线时，请勿将 L 线和 N 线接反，并请勿将输入输出端接反。
- 为防止人员受伤或设备损坏，测试时，等电位端子间接地电阻不能大于 2Ω。
- 建议与 UPS 配合使用。

4.3 连接同步线

通过同步线连接不同边道的主通道控制器和从通道控制器。

您需要使用同步线将主通道板与从通道板进行连接，使设备正常使用。

同步线孔位如下图所示：

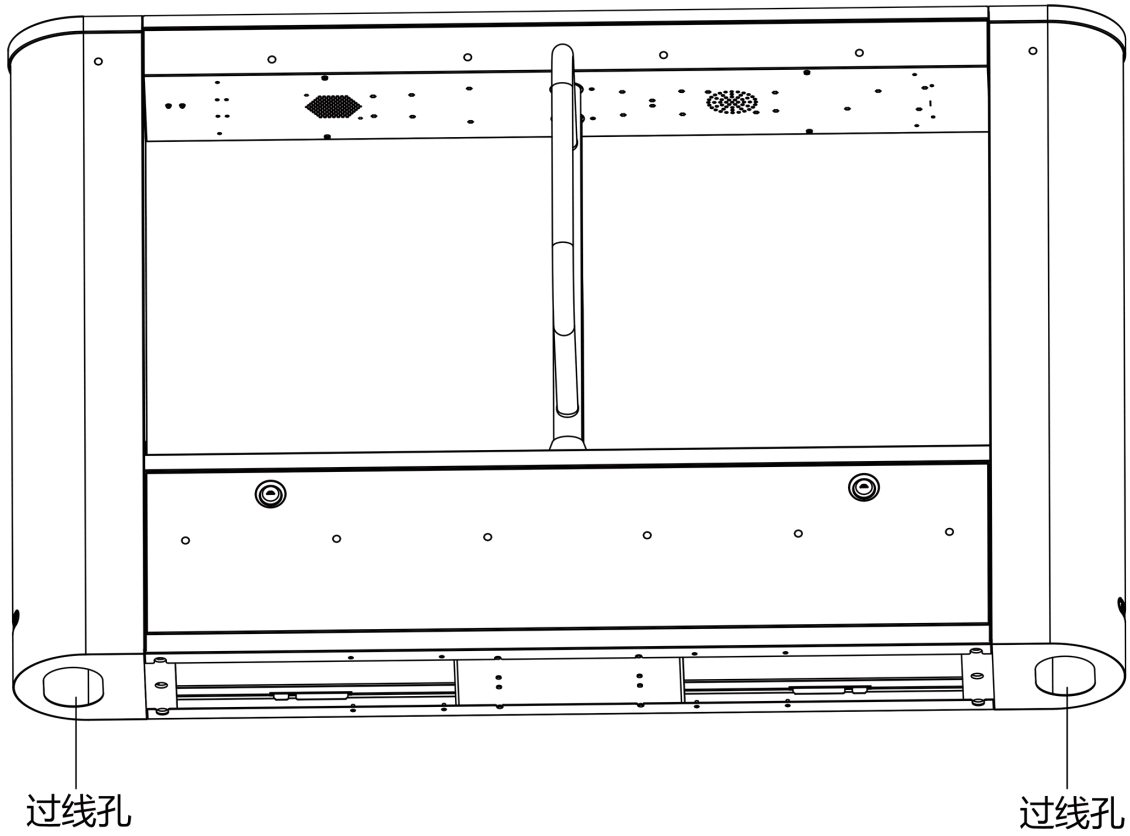


图 4-4 同步线孔位示意图

根据下图所示连接同步线，不同控制板上的接口详见 *端子介绍* 。

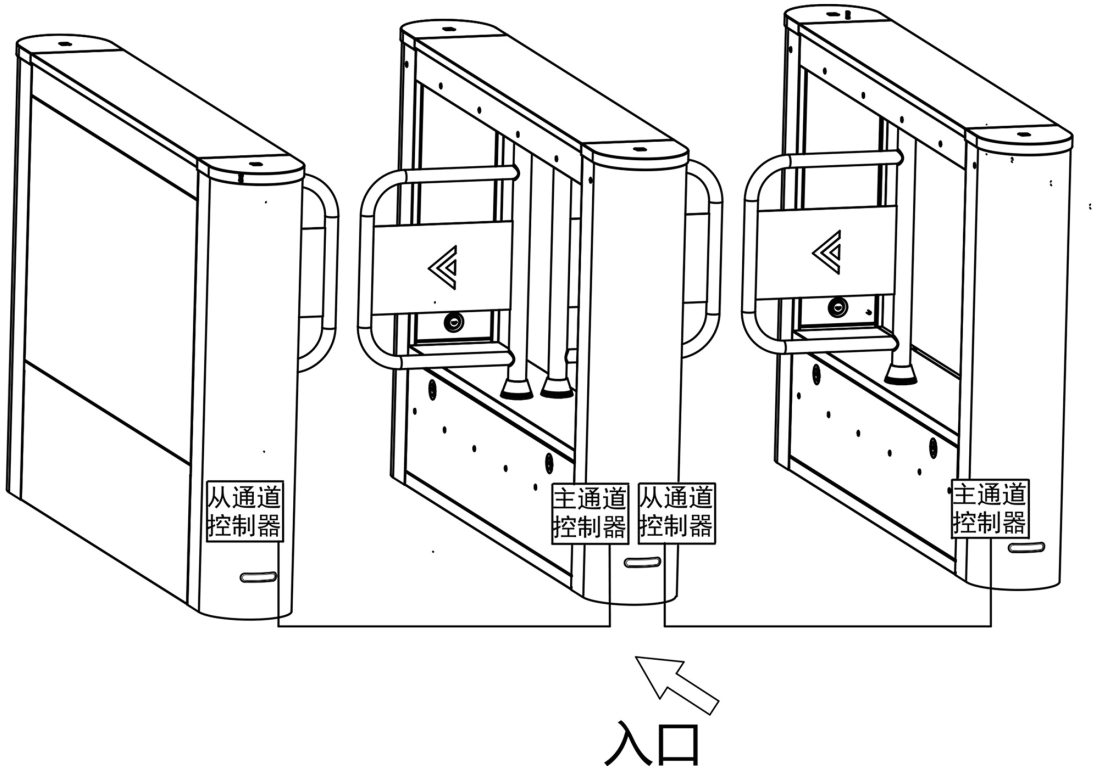


图 4-5 连接同步线

4.4 连接交换机

连接网线。

操作步骤

1. 使用 L 型 M4 内六角扳手拧松顶部螺丝，打开人行通道顶盖。

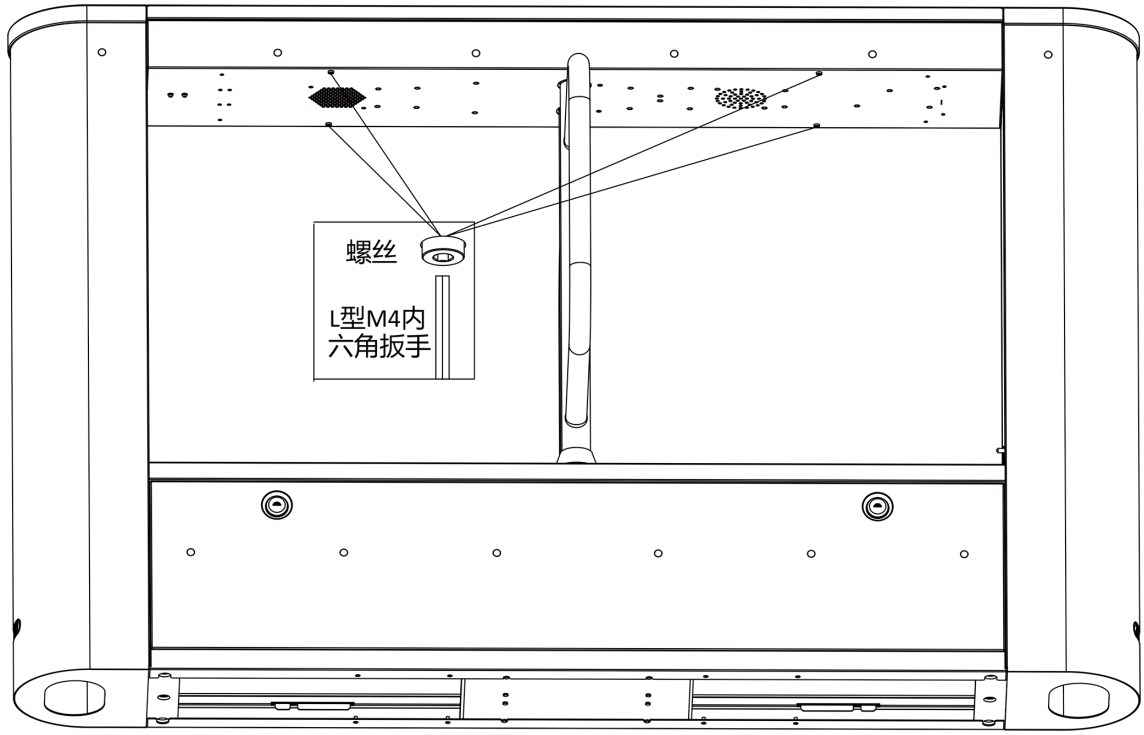


图 4-6 拧松顶部螺丝

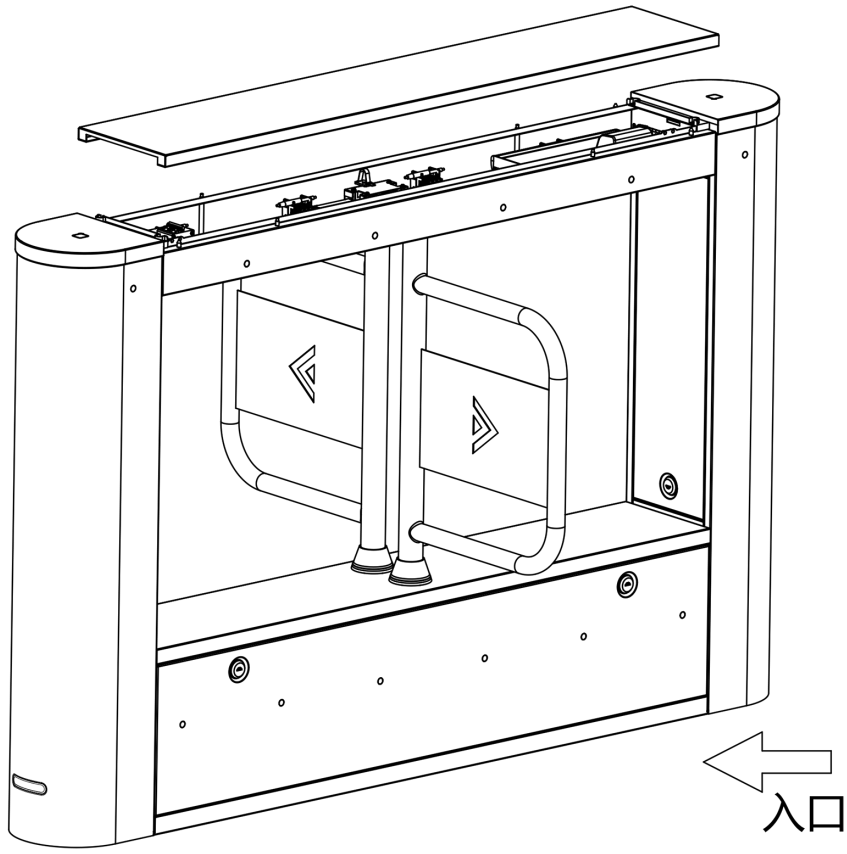


图 4-7 打开顶盖

交换机在图示位置。

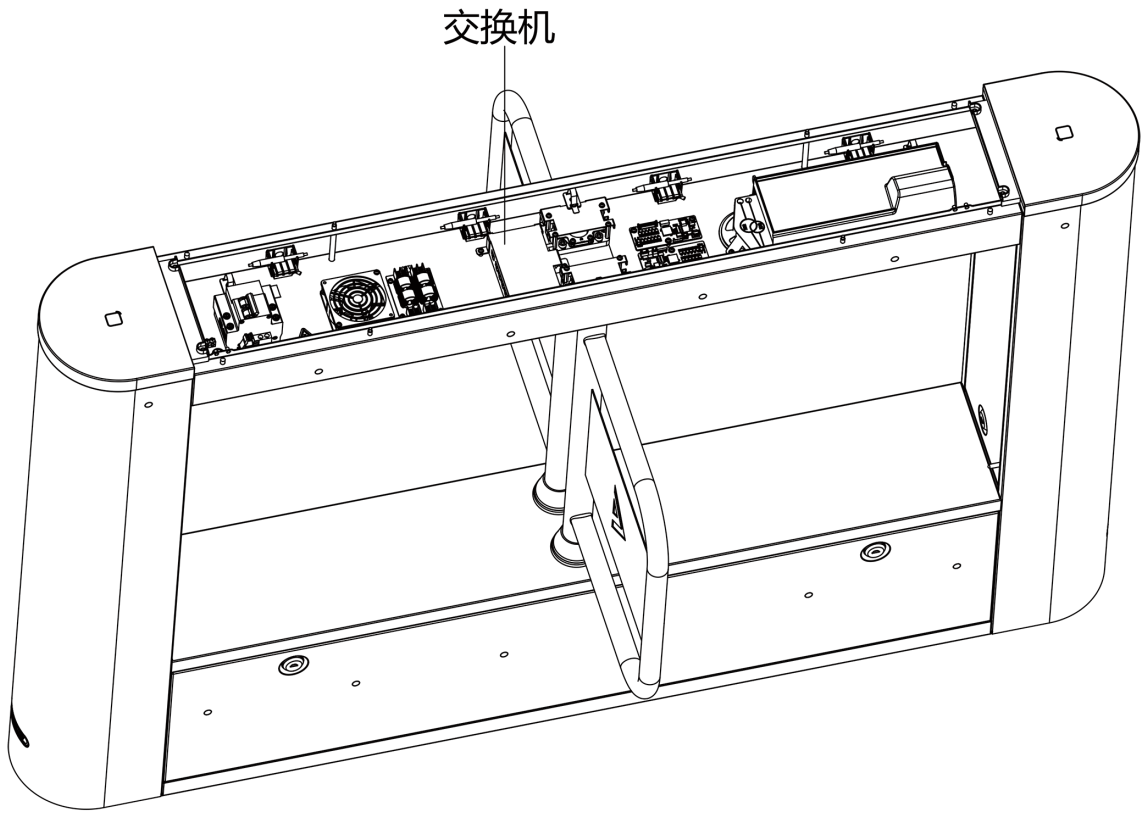


图 4-8 交换机位置

2. 从开关电源处引出 12V 电源，接入交换机电源接口。
3. 根据需要连接网线。

4.5 端子介绍

通道控制器分为主通道控制器和从通道控制器，主要用来控制红外、电机等部件的工作。

4.5.1 主通道控制器端子介绍

主通道控制板上包括过桥线接口、总线接口、电机编码器接口、调试串口、到位板接口、数码管、灯板接口（预留）、超级电容接口、电源输入接口、制动器接口、电机驱动接口和拨码接口。

主通道控制板如下图所示：

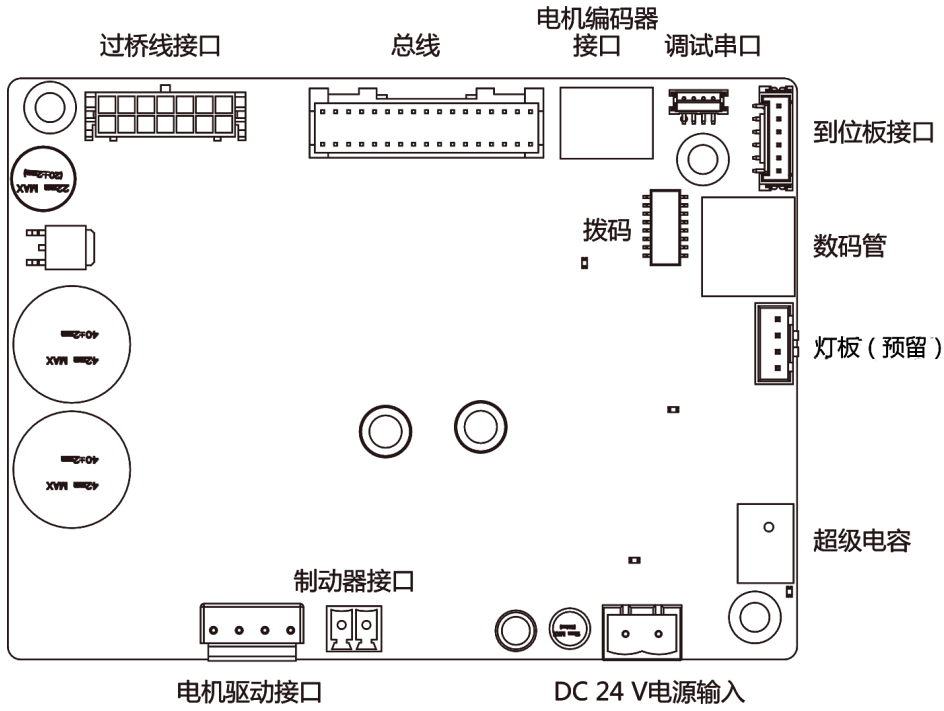


图 4-9 主通道控制板

4.5.2 从通道控制器端子介绍

从通道控制板上包括过桥线接口、总线接口、电机编码器接口、调试串口、到位板接口、数码管、灯板接口（预留）、超级电容接口、电源输入接口、制动器接口和电机驱动接口。

从通道控制板如下图所示：

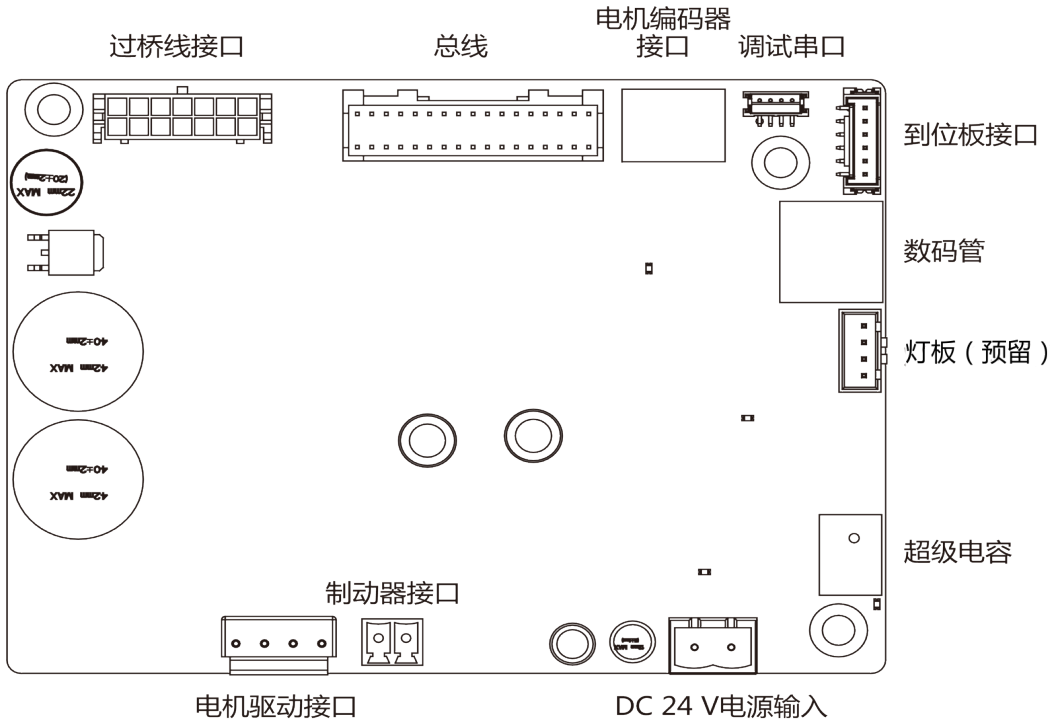


图 4-10 从通道控制板

4.5.3 权限控制器端子介绍

权限控制器主要用来权限认证，外接设备，并跟上层平台、通道控制器通讯。

权限控制板如下图所示：

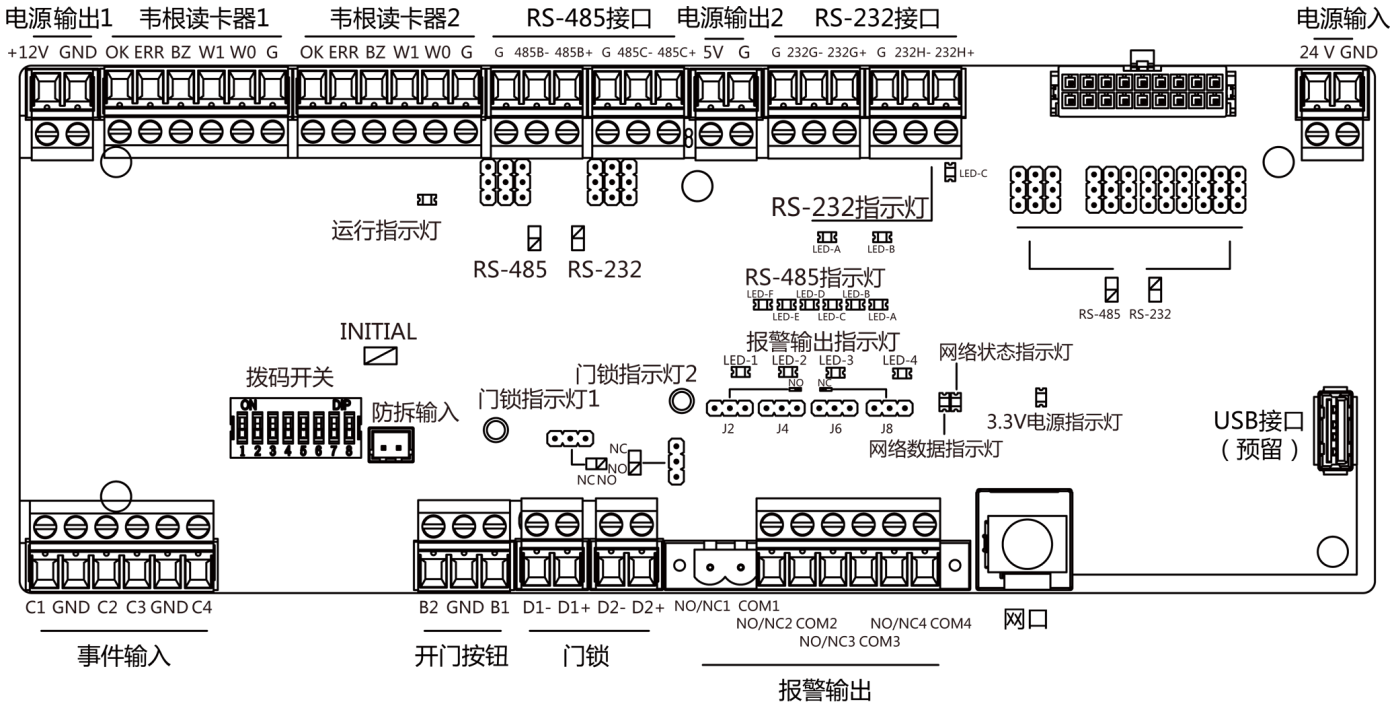


图 4-11 权限控制器端子介绍

权限控制器端子介绍		
电源输出 1	+12V	电源输出
	GND	接地端
韦根读卡器 1	OK	读卡器灯号控制输出(有效卡输出)
	ERR	读卡器灯号控制输出(无效卡输出)
	BZ	读卡器蜂鸣器控制输出
	W1	韦根读卡器数据输入 Data1
	W0	韦根读卡器数据输入 Data0
	GND	接地端
韦根读卡器 2	OK	读卡器灯号控制输出(有效卡输出)

权限控制器端子介绍		
	ERR	读卡器灯号控制输出(无效卡输出)
	BZ	读卡器蜂鸣器控制输出
	W1	韦根读卡器数据输入 Data1
	W0	韦根读卡器数据输入 Data0
	GND	接地端
RS-485 接口	GND	接地端
	RS-485 B-	读卡器 RS-485-端接入
	RS-485 B+	读卡器 RS-485+端接入
	GND	接地端
	RS-485 C-	读卡器 RS-485-端接入
	RS-485 C+	读卡器 RS-485+端接入
电源输出 2	5V	5 VDC 电源输出
	GND	接地端
RS-232 接口	GND	接地端
	RS-232 G-	RS-232-端接入
	RS-232 G+	RS-232+端接入
	GND	接地端
	RS-232 H-	RS-232-端接入
	RS-232 H+	RS-232+端接入
电源输入	+24V	24 VDC 正极输入
	GND	接地端
事件输入	C1	事件报警输入 1

权限控制器端子介绍		
	GND	接地端
	C2	消防输入
	C3	事件报警输入 3
	GND	接地端
	C4	事件报警输入 4
开门按钮	B2	门 2 信号输入
	GND	接地端
	B1	门 1 信号输入
门锁 （开关量）	D1-	门 1 门锁继电器输出(干接点)
	D1+	
	D2-	门 2 门锁继电器输出(干接点)
	D2+	
报警输出	NO/NC1	报警继电器 1 输出(干接点)
	COM1	
	NO/NC2	报警继电器 2 输出(干接点)
	COM2	
	NO/NC3	报警继电器 3 输出(干接点)
	COM3	
	NO/NC4	报警继电器 4 输出(干接点)
	COM4	
网络接口	LAN	网络接入

- 事件报警输入硬件接口为常开型，仅只支持接入常开信号，可联动主机蜂鸣器输出、读卡器蜂鸣器输出、报警继电器输出、开门继电器输出等。
- RS-485 读卡器 ID 出厂拨码设定为 1 和 3，1 为通道进门， 4 为通道出门。若用户配置了来宾卡，需要将出门接入两个读卡器，一个拨码为 4，一个拨码为 3，3 号读卡器和收卡器配合使用，普通用户在 4 号读卡器上刷卡，来宾卡用户在 3 号读卡器上刷卡。
- 韦根读卡器 1、2 分别对应通道进门读卡器，及通道出门读卡器。
- 报警输出：支持开关量输出。
- 如有需要，门锁继电器可用于控制第三方闸门开关，D1 控制普通进门开门，D2 控制普通出门开门。详见 *通道门控信号接线* 。
- 事件输入端 C3 和 C4 输入可复用为人数统计端口，C3 对应进门统计，C4 对应出门统计，当这两个端口有脉冲信号输入权限控制器时，权限控制器会进行人数的叠加。具体统计方式以及查看人数信息，详见人行通道用户手册中的人数统计章节。
- 具体拨码对应值详见 *拨码* 。

4.5.4 权限控制器串口 ID 与功能介绍

可通过权限控制板上的跳帽切换权限控制板上对应端口的通信模式。可通过跳帽在 RS-485 通信和 RS-232 通讯之间切换。具体通过跳帽切换接口通讯模式的描述，请参见 *接口（RS-485/RS-232）转换* 。

权限控制板如下图所示：

说明

图片为示意图，请以实际设备外观为准。

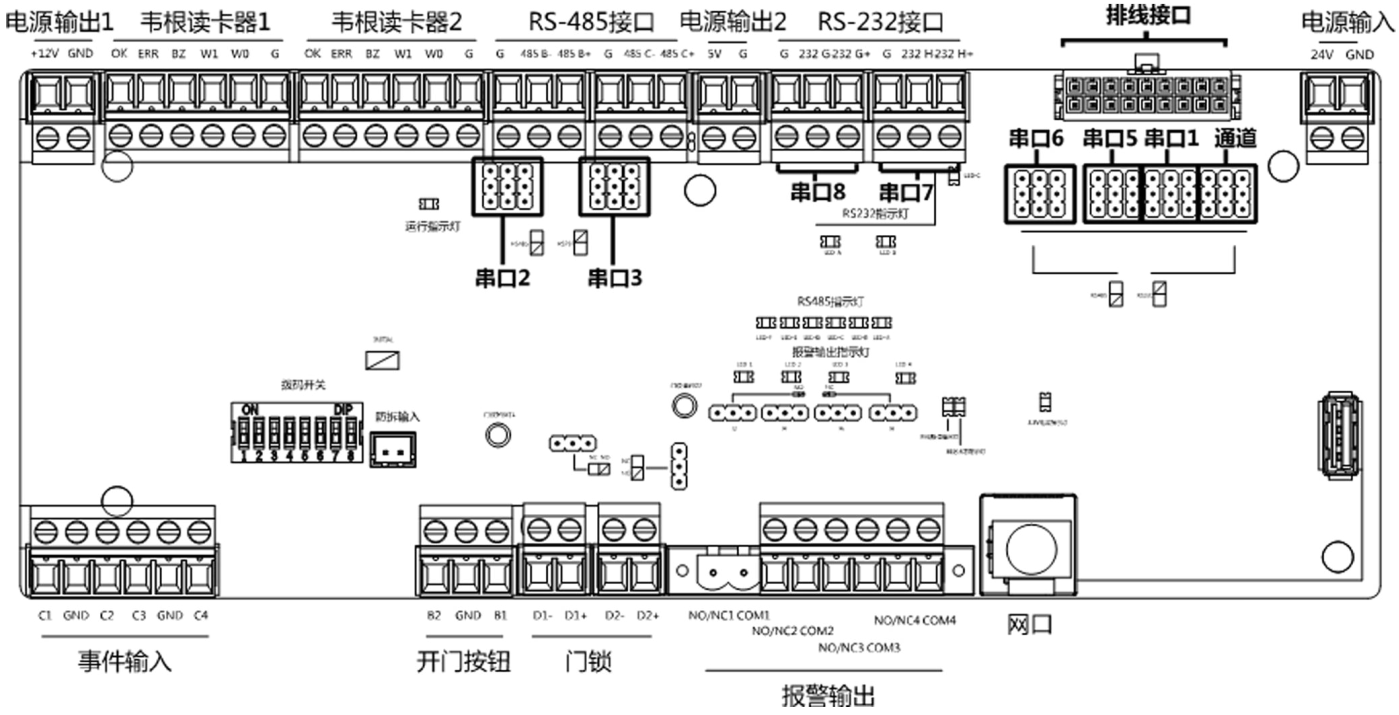


图 4-12 权限控制板

如图所示，RS-485 接口对应串口 2 和串口 3；RS-232 接口对应串口 7 和串口 8；排线接口中包括串口 1，串口 4，串口 5，串口 6，和通道串口。

描述如下：

串口 2/串口 3 跳帽	预留串口。通过跳帽可切换串口通讯模式。可在 RS-485 通信模式和 RS-232 通讯模式间切换。默认为 RS-485 通讯模式。
串口 6 跳帽	通过跳帽可切换与从通道控制器的串口通讯模式。可在 RS-232 通信模式和 RS-485 通讯模式间切换。默认为 RS-232 通信模式。
串口 5 跳帽	通过跳帽可切换与从通道控制器的串口通讯模式。可在 RS-485 通信模式和 RS-232 通讯模式间切换，默认为 RS-485 通信模式。

串口 1 跳帽	通过跳帽可切换与主通道控制器的串口通讯模式。可在 RS-485 通信模式和 RS-232 通讯模式间切换，默认为 RS-485 通信模式。
通道跳帽	可通过跳帽切换与通道控制器的通信模式切换，出厂时串口已连接，默认为 RS-485 通信模式。若需接入其他控制器(兼容海康通信协议)，则可通过跳帽切换串口模式。可在 RS-485 和 RS-232 通讯模式间切换。
串口 4	在图中表示的排线接口中, 外接主通道控制器固定的 RS-232 通讯模式，无跳帽，不能通过跳帽改变通讯模式。
串口 7/串口 8	预留串口。固定的 RS-232 接口，无跳帽，不能通过跳帽改变通讯模式。可接二维码扫描器、收卡器和字符屏。

闸机预留的串口接线端子位置对应的权限控制板上的串口号如下图所示：

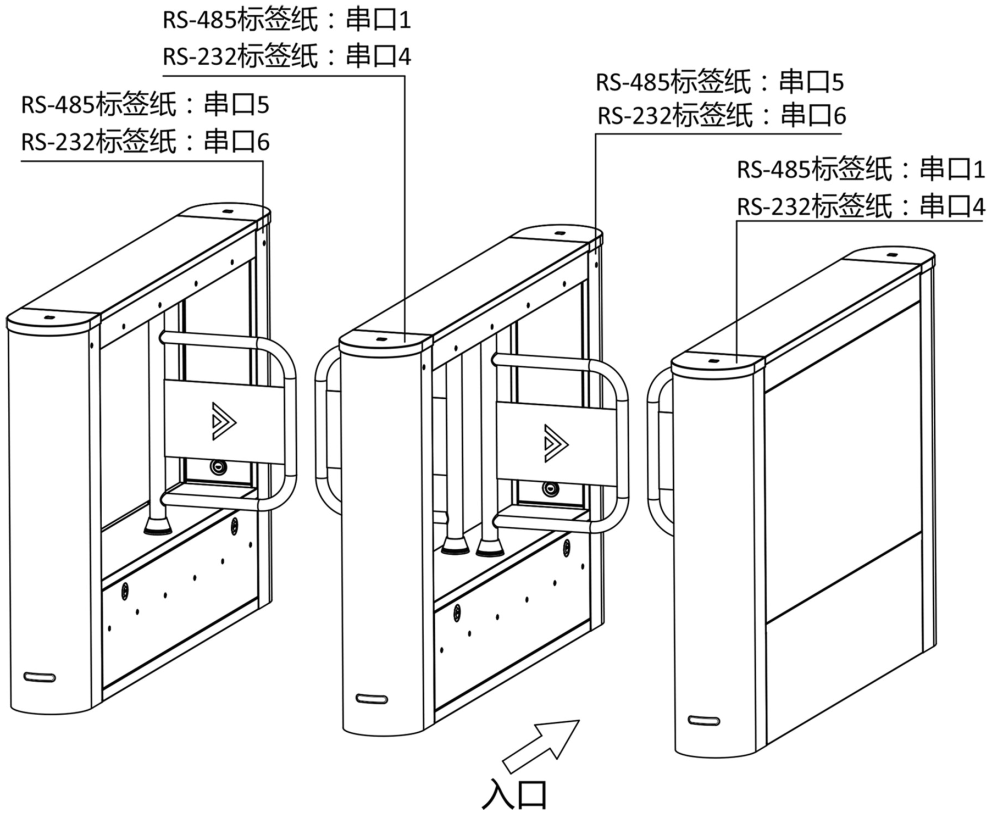


图 4-13 串口号对应图

4.5.5 RS-485 接线

人行通道权限控制器共配有 4 个 RS-485 接口，可以接身份证读卡器、IC 读卡器、二维码扫描器、指纹读卡器、收卡器、字符屏、指纹头和人证设备 8 种外接设备。此处以 RS-485 读卡器的接法为例。

说明

- 具体有关字符屏的配置，详见用户手册中的远程配置章节。
- RS-485 接读卡器时，拨码默认为进 1，出 4。
- 有其他 RS-485 设备接入时，RS-485 ID 不能冲突。

4 个 RS-485 接口均可转换成 RS-232 接口使用。

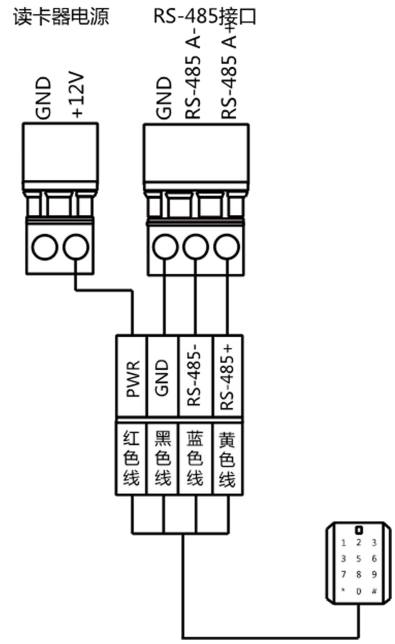


图 4-14 RS-485 读卡器连接

4.5.6 RS-232 接线

说明

- 人行通道权限控制器共配有 3 个 RS-232 接口（串口 4、串口 7 和串口 8），其中串口 7 和串口 8 可以接二维码扫描器、收卡器、和字符屏；串口 4 可以接二维码扫描器、收卡器、字符屏及人证设备。
- 具体有关字符屏的配置，详见用户手册中的远程配置章节。
- 此处以字符屏的接法为例。

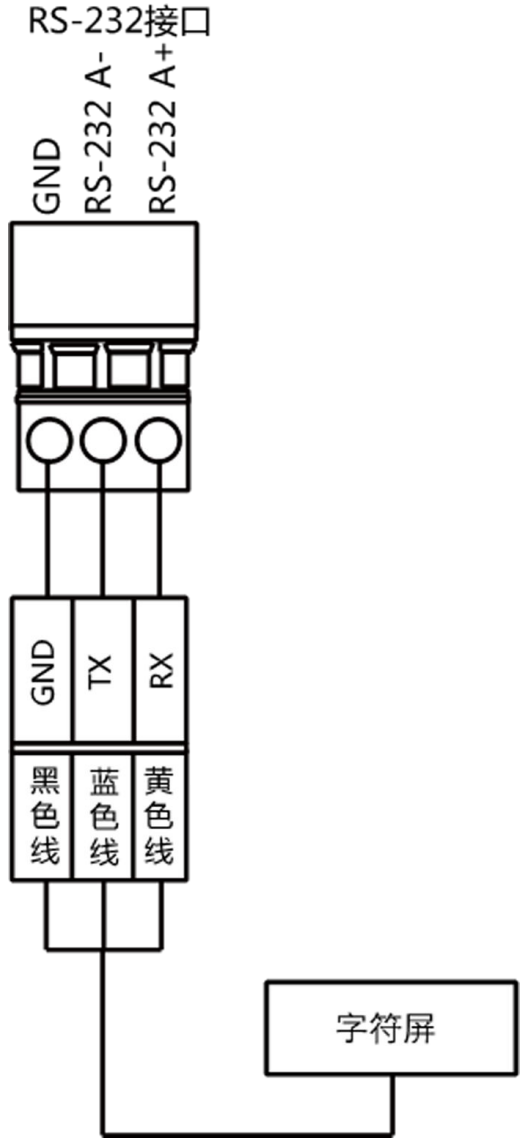


图 4-15 RS-232 字符屏连接

4.5.7 韦根接线

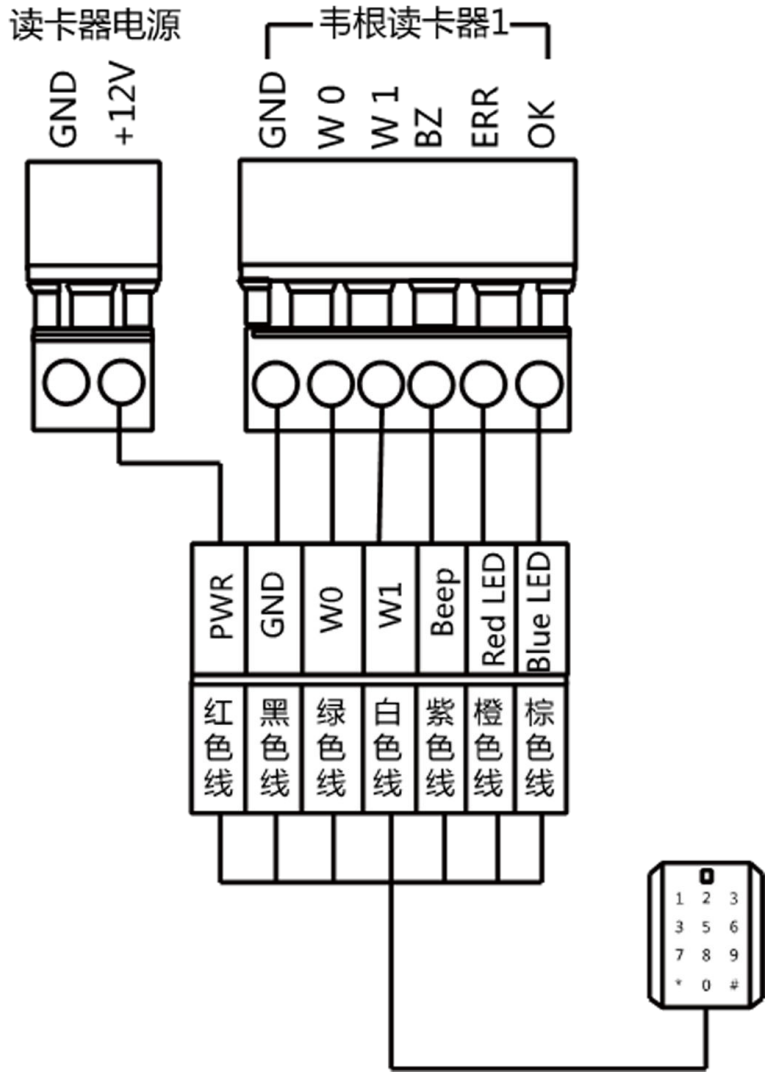


图 4-16 韦根读卡器连接

说明

主机如果要控制韦根读卡器的蜂鸣声和 LED，必须将 OK/ERR/BZ 端子接好。

4.5.8 通道门控信号接线

默认闸门已连接通道控制板，控制闸门开关。如有需要，可外接第三方通道主板，控制第三方闸门开关，D1 控制普通进门开门，D2 控制普通出门开门。

具体通过跳帽切换继电器输出状态的描述，请参见 *4.5.1 门控信号继电器输出状态示意图*。

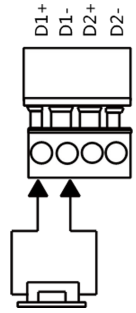


图 4-17 通道进门安装示意图

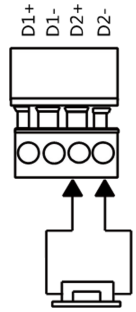


图 4-18 通道出门安装示意图

4.5.9 报警输出接线

具体通过跳帽切换继电器输出状态的描述，请参见 *4.5.2 报警继电器输出状态示意图*。

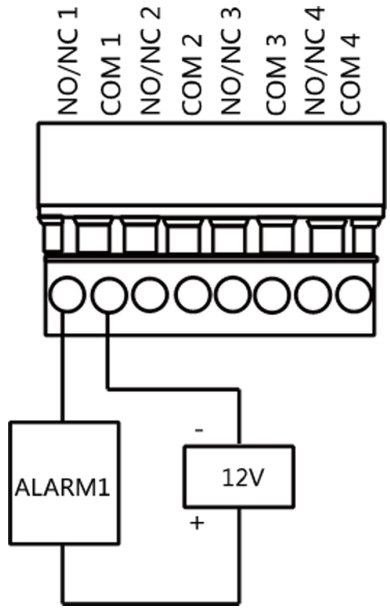


图 4-19 外接报警设备连接

4.5.10 消防联动接线

可通过控制器的接线端子连接消防开关。

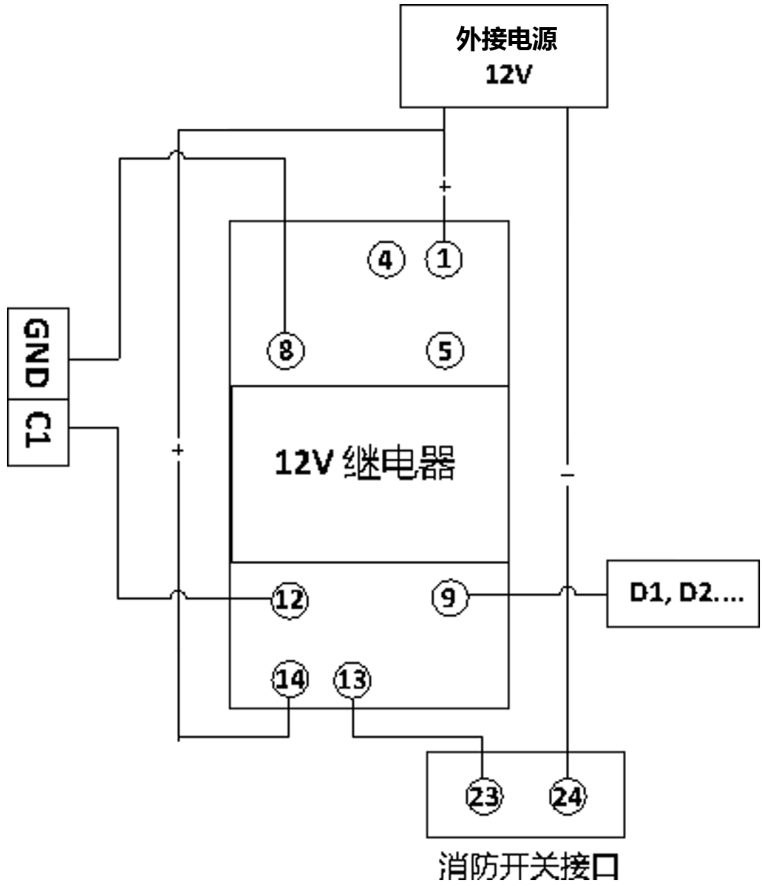


图 **4-20** 消防联动接线示意图

第 5 章 硬件测试

安装完毕并接线完成，需要设定摆闸关闭位置（学习模式）方可进入正常模式。此外还可以通过权限控制板上的拨码配置闸机测试模式、通行模式、记忆模式，配置闸机遥控器对码，初始化硬件、转换 RS-485 和 RS-232 接口状态和查看继电器输出 NO/NC 示意图。

学习模式

闸门自动学习闸机的关门位置。

正常模式

正常模式下，设备正常工作。学习模式时设定的关门位置即为正常工作模式下闸机关门时的位置。

测试模式

除无法上传报警、事件、或进出人数信息，其他同正常模式一致。

说明

测试时，需将人行通道盖板盖上，否则影响调试结果。

通行模式

共有 9 种通行模式，分别是双向受控、进受控出禁止、进受控出自由、进出自由、进自由出受控、进自由出禁止、进出禁止、进禁止出受控、进禁止出自由。

记忆模式

默认情况下，记忆模式开启。记忆模式下，允许多次刷卡时，多人通行。在通行人数到达刷卡次数后，或在上一个人通行后，开门时间内无人通行时，闸门自动关闭。

说明

除上述操作外，还可通过权限控制板上的拨码开关配置进出门控制方式、遥控器对码等操作。具体拨码对应值请参见 *拨码值对应表*。

5.1 遥控器配对（选配）

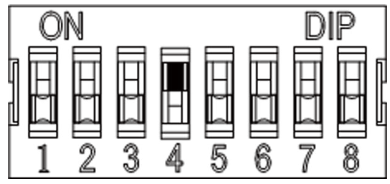
人行通道可选配开/关门遥控器，在使用遥控器前需要将遥控器与人行通道进行配对操作。具体操作内容请参见具体遥控器用户手册。

操作步骤

说明

最多支持添加 32 个遥控器。

1. 将闸机断电，并将权限控制板上的第 4 位拨码开关拨至 ON。



2. 将设备重新上电，人行通道处于遥控器对码模式中。

3. 按住遥控器*关门*按钮 10 秒以上。对码成功后，遥控器指示灯将闪烁两次。您也可以在客户端配对人行通道与遥控器，具体操作请详见 ***管理遥控器用户*** 。

4. 对码成功后，将拨码开关 4 拨回数字侧，并重启人行通道，完成遥控器对码。

说明

- 同一时间，只有一台闸机可以与遥控器进行配对，若有多台闸机都处于遥控器对码模式，遥控器会随机选择其中一台进行配对，配对成功后不再进行对码。
- 具体拨码对应值请参见 ***拨码值对应表*** 。

5. **可选操作**: 在客户端远程配置中进入 *系统 → 用户 → 遥控器用户*，删除不需要的遥控器。

5.2 硬件初始化

操作步骤

1. 将初始化排针上的跳帽（权限控制板上）从排针上拿开。

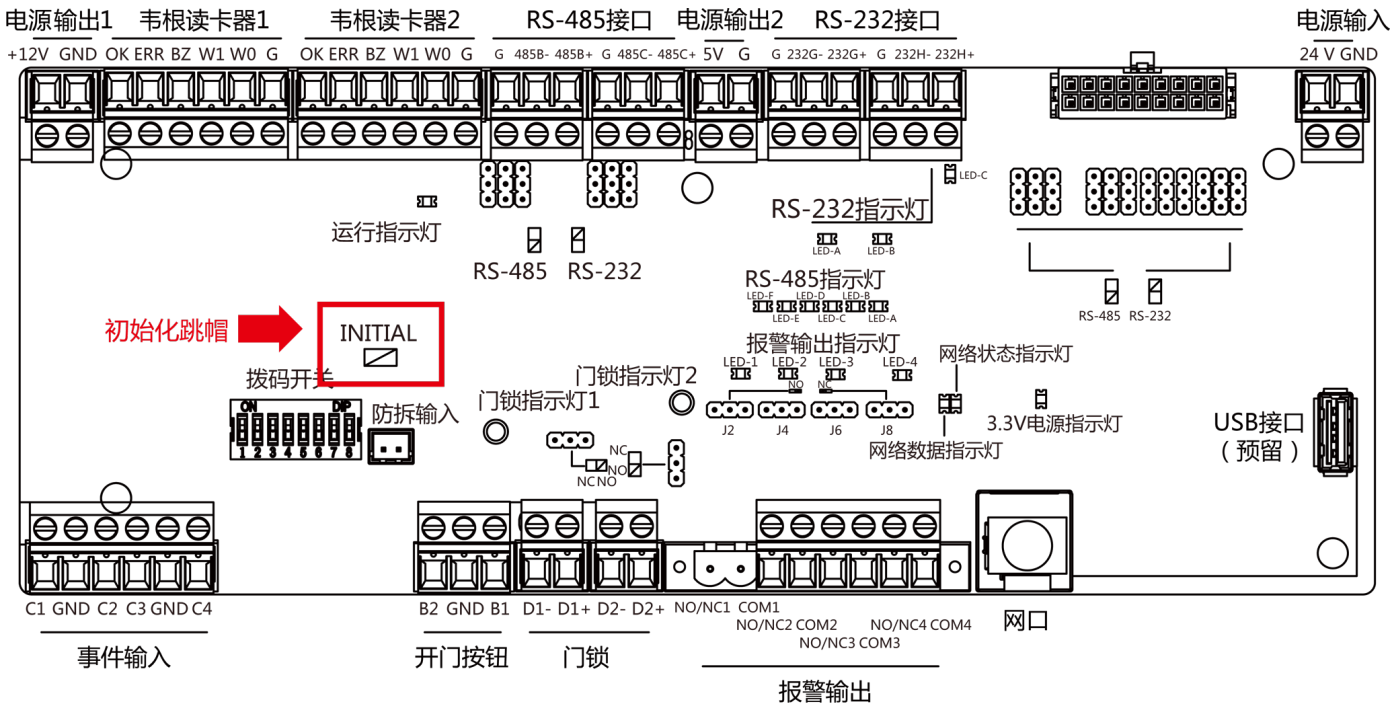


图 5-1 初始化跳帽位置

2. 断电重启，控制器上的蜂鸣器开始鸣叫，此时蜂鸣器是“滴”声长鸣。

3. 蜂鸣器停止鸣叫后，将跳帽跳回至排针上，再次断电重启即可。

注意

硬件初始化会将设备恢复出厂状态，需重新激活设备方可使用。

说明

设备上电或重启过程中需确保通道内无人员。

5.3 接口（RS-485/RS-232）转换

以权限控制板上串口 4 为例。若跳帽在下图所示位置（黑色部分为跳帽），则对应的接口为 RS-485 接口。

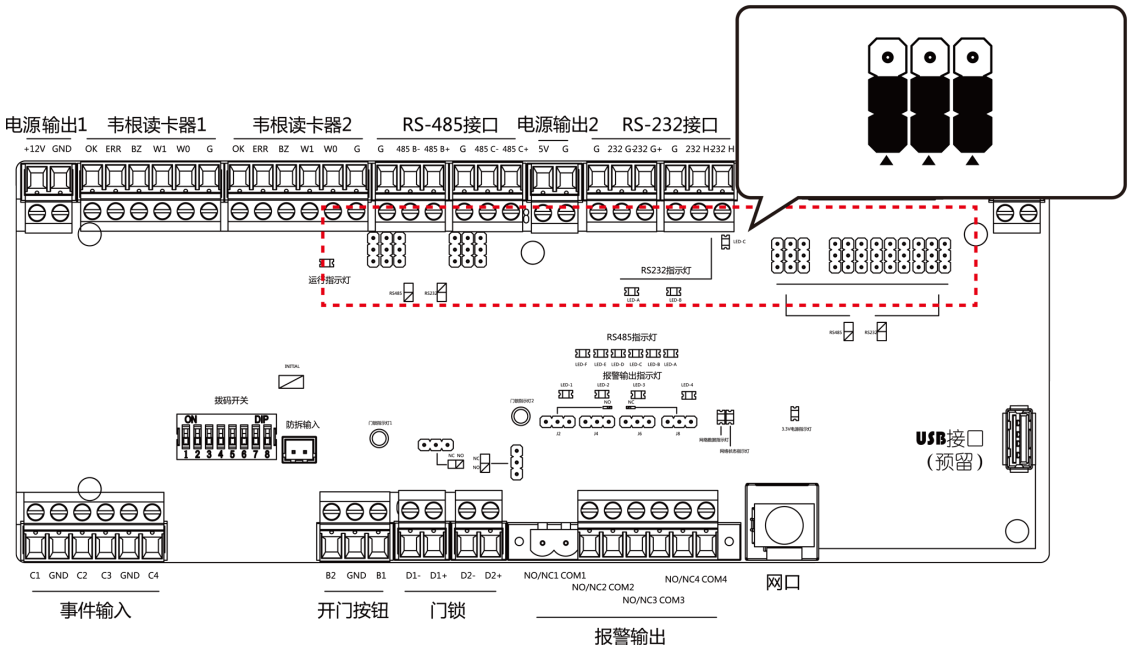


图 5-2 RS-485 接口跳帽状态

若跳帽在下图所示位置（黑色部分为跳帽位置），则对应的接口为 RS-232 接口。

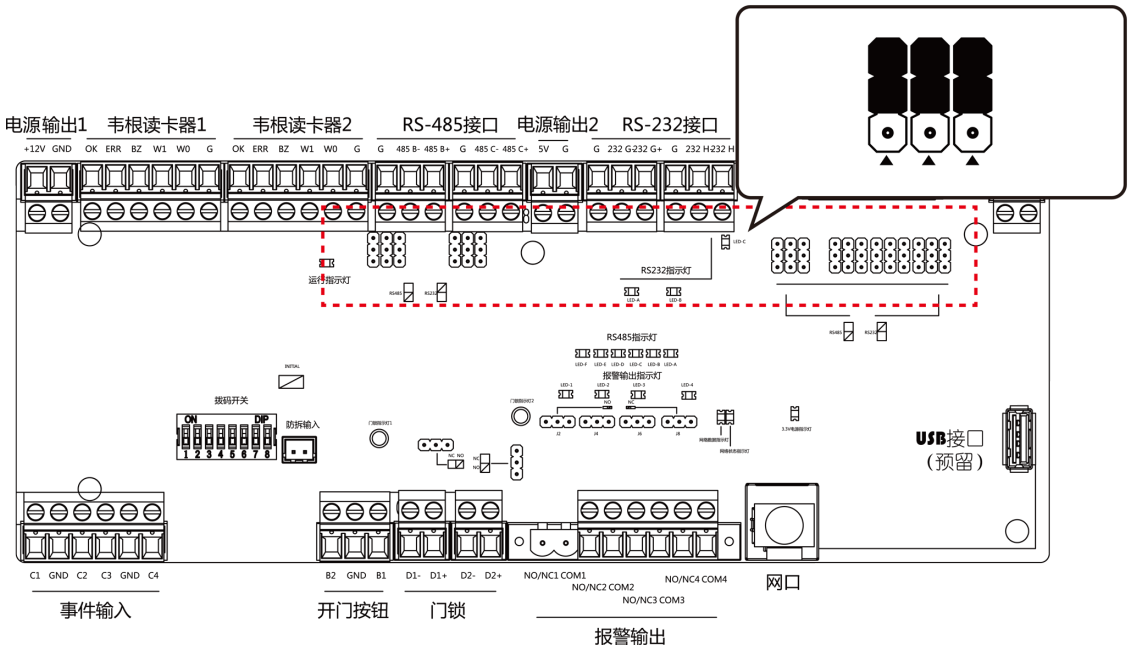


图 5-3 RS-232 接口跳帽状态

5.4 继电器输出 NO/NC 选择示意图

5.4.1 门控信号继电器输出状态说明

权限控制板上的门锁接口排针位置如下图所示：

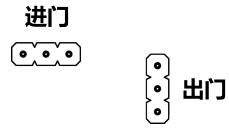


图 5-4 排针位置

门锁继电器进门常开（NO）跳帽位置如下图所示：

图 5-5 门锁继电器进门常开（NO）状态

门锁继电器出门常开（NO）跳帽位置如下图所示：

图 5-6 门锁继电器出门常开（NO）状态

门锁继电器进门常闭（NC）跳帽位置如下图所示：

图 5-7 门锁继电器进门常闭（NC）状态

门锁继电器出门常闭（NC）跳帽位置如下图所示:

图 5-8 门锁继电器出门常闭（NC）状态

5.4.2 报警继电器输出状态示意图

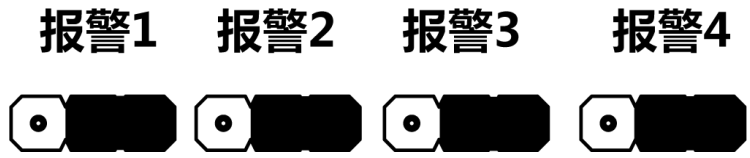


图 5-9 报警继电器输出常开（NO）状态

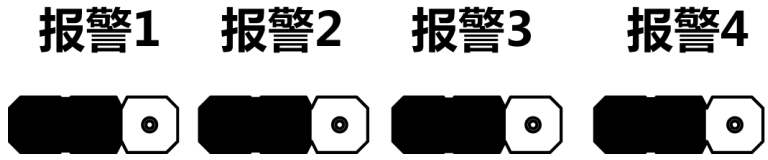


图 5-10 报警继电器输出常闭（NC）状态

第 6 章 激活

设备首次使用时需要进行激活并设置密码，才能正常登录和使用。

设备出厂缺省值如下所示：

- 缺省 IP 为：192.0.0.64。
- 缺省端口为：8000。
- 缺省用户名（管理员）：admin。

6.1 通过 SADP 软件激活设备

下载 SADP 软件并运行，SADP 软件会自动搜索局域网内的所有在线设备，列表中会显示设备类型、IP 地址、安全状态、设备序列号等信息。通过 SADP 软件可对未激活设备进行激活操作。

操作步骤

1. 从官网下载 SADP 软件并运行。

2. 选中需要激活的设备，列表右侧将显示设备的相关信息。

3. 在激活设备栏处设置设备密码，并单击***确定***完成激活。

注意

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，且至少由数字、小写字母、大写字母和特殊字符中的两种或两种以上类型组合而成。

成功激活设备后，列表中激活状态会更新为**已激活**。

4. 修改设备 IP 地址

1) 在设备列表中勾选中已激活的设备。

2) 在右侧的**修改网络参数**中输入 IP 地址、子网掩码、网关等信息。

说明

设置 IP 地址时，请保持设备 IP 地址与电脑 IP 地址处于同一网段内。

3) 修改完毕后输入激活设备时设置的密码，并单击*修改*。

图 6-1 修改设备 IP 地址

提示**修改参数成功**则表示 IP 等参数设置生效。

6.2 通过客户端软件激活设备

通过客户端的设备管理界面可搜索到局域网内的所有在线设备，并对未激活设备进行激活操作。

操作步骤

1. 从官网下载客户端软件，运行客户端软件后，在维护与管理区域，选择 ***设备管理 → 设备***。

2. 单击放大镜按钮，界面出现在线设备列表。

通过 SADP 协议搜索到的在线设备展示在列表中。

3. 选择某一设备，单击***激活***。

4. 输入密码并确认密码。

注意

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，且至少由数字、小写字母、大写字母和特殊字符中的两种或两种以上类型组合而成。

5. 单击***确定***。

成功激活设备后，列表中安全状态列会更新为**已激活**。

6. 修改设备网络信息

1) 在 SADP 搜索列表中单击已激活的在线设备，并单击 。

2) 在弹出的页面中修改设备的 IP 地址、网关等信息。

3) 输入激活设备时设置的密码，并单击***确定***。

说明

设置 IP 地址时，请保持设备 IP 地址与电脑 IP 地址处于同一网段内。

第 7 章 客户端软件配置

通过客户端软件配置设备参数、控制和操作设备。

安装随机光盘中或从官网下载客户端软件，运行客户端软件。

7.1 设备管理

客户端软件可以对不同类型的设备进行管理。客户端支持添加多种类型的设备，包括可视对讲、门禁设备、等等。例如：添加门禁设备后，可进行访问控制和考勤管理。

7.1.1 添加设备

用户可通过多种方式添加设备至客户端，包括 IP/域名模式、IP 段模式和 ISUP 模式。当待添加设备数量较多时，还可通过批量导入的方式一次添加多台设备至客户端。设备添加至客户端后，可对其进行远程配置和管理。

添加在线设备

客户端可自动检测与当前计算机处于同一网段的在线设备，并自动获取识别到的设备信息（如 IP 地址）。基于该功能，可快速将检测到的设备添加至客户端。支持一次添加多台设备。

说明

请确保要添加的设备与客户端所在的计算机处于同一网段。

添加单个在线设备

用户可在客户端搜索到的在线设备列表中，选择一台设备添加至客户端。

操作步骤

1. 选择 *设备管理 → 设备* 。
2. 单击*在线设备*。

   页面下方出现在线设备列表。

图 7-1 搜索在线设备

3. 在“在线设备”列表中勾选需要添加的设备，单击*添加*。

4. 在添加设备面板中设置相关参数。

名称

可根据设备型号或所在位置自定义。

IP 地址

设备 IP 地址，可自动获取。

端口

可自动从设备端获取端口号，也可手动修改。

用户名

输入登录设备的用户名。

密码

输入设备密码。

注意

- 为更好保护您的隐私并提升产品安全性，我们强烈建议您根据如下规则设置较为复杂的密码：密码长度必须在 8~16 位之间，由数字、大小写字母、特殊字符的两种及以上类型组合而成。
- 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。

5. 可选操作: 勾选**传输加密（TLS）**来启用传输加密功能，以加强数据安全。

说明

- 该功能需要设备支持。
- 若启用了验证证书，必须单击*打开证书目录*来打开安全证书默认目录，并将设备的安全证书复制至该默认目录下。在 TLS 加密的基础上，再通过验证设备安全证书来加强数据安全性。
- 可通过 Web 浏览器登录设备，获取设备的安全证书。

6. **可选操作**: 勾选**同步设备时间**，对设备进行一次校时且与本地计算机时间一致。

7. **可选操作**: 勾选**导入至分组**，可以以设备名称创建一个组，并将该设备的所有通道导入该组。

8. 单击*添加*。

批量添加在线设备

当客户端检测到的在线设备使用相同的用户名和密码时，选中多台设备，批量添加至客户端。

操作步骤

1. 选择 *设备管理* → *设备* 。

2. 单击*在线设备*。

页面下方出现在线设备列表。

3. 勾选需要添加的设备，单击*添加*打开添加设备面板。

4. 输入用户名和密码。

注意

- 为更好保护您的隐私并提升产品安全性，我们强烈建议您根据如下规则设置较为复杂的密码：密码长度必须在 8~16 位之间，由数字、大小写字母、特殊字符的两种及以上类型组合而成。
- 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。

5. **可选操作**: 勾选**同步设备时间**，对设备进行一次校时且与本地计算机时间一致。

6. **可选操作**: 勾选**导入至分组**，可以以设备名称创建一个组，并将该设备的所有通道导入该组。

7. 单击*添加*。

通过 IP/域名添加设备

如果已知待添加设备的 IP 地址或域名，则可以通过输入 IP 地址或域名等信息添加设备到客户端。

操作步骤

1. 选择 *设备管理* → *设备* 。

2. 单击*添加*打开添加设备面板。

3. **添加模式**选择 **IP/域名**。

4. 设置参数，包括名称、IP 地址/域名、端口、用户名和密码。

注意

- 为更好保护您的隐私并提升产品安全性，我们强烈建议您根据如下规则设置较为复杂的密码：密码长度必须在 8~16 位之间，由数字、大小写字母、特殊字符的两种及以上类型组合而成。
- 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。

5. **可选操作**: 若设备当前处于离线状态，可勾选**添加离线设备**，并输入设备的通道数和报警输入数。

添加成功后，设备的网络状态为**离线**；当设备在线时，网络状态将自动切换为**在线**。

6. **可选操作**: 勾选**传输加密（TLS）**来启用传输加密功能，以加强数据安全。

说明

- 该功能需要设备支持。
- 若启用了验证证书，必须单击*打开证书目录*来打开安全证书默认目录，并将设备的安全证书复制至该默认目录下。在 TLS 加密的基础上，再通过验证设备安全证书来加强数据安全性。
- 可通过 Web 浏览器登录设备，获取设备的安全证书。

7. **可选操作**: 勾选**同步设备时间**，对设备进行一次校时且与本地计算机时间一致。

8. **可选操作**: 勾选**导入至分组**，可以以设备名称创建一个组，并将该设备的所有通道导入该组。

9. 单击*添加*，关闭该界面；或单击*添加并继续*，在该界面继续添加其他设备。

通过 IP 段添加设备

若待添加的多台设备 IP 地址在一定范围内，且具有相同的端口号、用户名和密码，可选择 IP 段方式添加设备。指定设备的起始 IP 地址和结束 IP 地址，可以快速添加设备至客户端。

操作步骤

1. 选择 *设备管理 → 设备* 。

2. 单击*添加*打开添加设备面板。

3. **添加模式**选择 **IP 段**。

4. 在添加设备面板中设置参数，包括起始 IP 地址、结束 IP 地址、端口、用户名和密码。

注意

- 为更好保护您的隐私并提升产品安全性，我们强烈建议您根据如下规则设置较为复杂的密码：密码长度必须在 8~16 位之间，由数字、大小写字母、特殊字符的两种及以上类型组合而成。
- 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。

5. 可选操作: 若设备当前处于离线状态，可勾选**添加离线设备**，并输入设备的通道数和报警输入数。

添加成功后，设备的网络状态为**离线**；当设备在线时，网络状态将自动切换为**在线**。

6. 可选操作: 勾选**传输加密（TLS）**来启用传输加密功能，以加强数据安全。

说明

- 该功能需要设备支持。
- 若启用了验证证书，必须单击*打开证书目录*来打开安全证书默认目录，并将设备的安全证书复制至该默认目录下。在 TLS 加密的基础上，再通过验证设备安全证书来加强数据安全性。
- 可通过 Web 浏览器登录设备，获取设备的安全证书。

7. 可选操作: 勾选**同步设备时间**，对设备进行一次校时且与本地计算机时间一致。

8. 可选操作: 勾选**导入至分组**，可以通过设备名称创建一个分组，并导入该设备的所有通道。

9. 单击*添加*，关闭该界面；或单击*添加并继续*，在该界面继续添加其他设备。

批量导入设备

当待添加的设备数量较多时，可以在模板中输入设备信息，将编辑好的模板上传，实现批量添加设备。

操作步骤

1. 选择 *设备管理 → 设备* 。

2. 单击*添加*。

3. 添加模式选择**批量导入**。

4. 单击*导出模板*，保存 CSV 格式的模板文件到本地。

5. 打开模板，输入设备信息。

注意

- 为更好保护您的隐私并提升产品安全性，我们强烈建议您根据如下规则设置较为复杂的密码：密码长度必须在 8~16 位之间，由数字、大小写字母、特殊字符的两种及以上类型组合而成。
- 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。

6. 在添加设备界面，单击图标 ，选择本地已编辑好的模板。

7. 单击*添加*。

7.1.2 重置/恢复密码

客户端集成 SADP 工具软件功能，若忘记设备密码，即可通过客户端重置设备密码或恢复默认密码。

重置密码

若忘记搜索到的在线设备密码时，可以通过密钥认证方式，为设备设置新密码。根据实际情况，选择合适的密码重置方式。

操作步骤

说明

该功能需要设备支持，界面仅显示设备支持的重置方式。

1. 选择 ***设备管理 → 设备*** 。

2. 单击*在线设备*。

通过 SADP 协议搜索到的在线设备展示在列表中。

3. 在“在线设备”列表中勾选待重置密码的设备，单击 。

4. 根据设备所支持功能，选择重置密码方式。

- **密钥认证**

  通过将导出的 XML 密钥文件给相关技术人员，从而获取 **Encrypt.xml 文件**，并将该文件上传即可。

5. 输入新密码和确认密码。

注意

- 为更好保护您的隐私并提升产品安全性，我们强烈建议您根据如下规则设置较为复杂的密码：密码长度必须在 8-16 位之间，由数字、大小写字母、特殊字符的两种及以上类型组合而成，且密码中不能包含用户名。
- 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。

6. 单击*确定*。

恢复密码

对于比较老的固件版本的设备，由于未使用激活机制，可以通过提供设备的完整序列号和设备时间提供给技术支持人员，获取设备安全码后，将设备密码恢复至缺省密码 12345。

操作步骤

说明

该功能需要设备支持。

1. 选择 ***设备管理 → 设备 → 设备***，进入设备界面。

2. 单击*在线设备*。

通过 SADP 协议搜索到的在线设备展示在列表中。

3. 在“在线设备”列表中勾选待恢复密码的设备，单击 。

4. 输入获取的安全码。

说明

通过提供设备上标识的完整序列号和设备时间提供给技术支持人员，获取设备安全码。

5. 单击*确定*。

密码恢复至初始密码 12345。

注意

- 为更好保护您的隐私并提升产品安全性，我们强烈建议您根据如下规则设置较为复杂的密码：密码长度必须在 8-16 位之间，由数字、大小写字母、特殊字符的两种及以上类型组合而成，且密码中不能包含用户名。
- 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。

7.1.3 分组管理

为便于管理，可以将某个区域下不同类型的设备资源添加至一个分组。例如，把楼层 A 中所有的门禁点、雷达添加至同一个分组，将分组命名为“楼层 A”，可以快速查看该楼层下不同类型的资源信息，进行快捷管理。还可以以客户端上的某台设备的名称建立分组，该设备下的所有资源将同时导入至该分组。导入至分组后，可以查看门状态。

添加分组

软件提供自定义添加分组或者以设备名称生成分组，前者添加分组后，需要手动将资源通道导入到分组，选择后者时，设备包含的通道资源会自动导入到对应分组下，用户可根据实际需求选择分组建立方式。通过建立分组，方便用户进行设备管理。

操作步骤

1. 在维护与管理区域，选择 ***设备管理 → 分组*** 。

2. 添加分组。

- 在上方工具栏中，单击*添加分组*，并在“新建分组”输入分组名称。

- 在上方工具栏中，单击*以设备生成分组*，可将勾选的设备导入至分组中。

说明

- 最多允许添加 256 个分组。
- 按住 Shift 或 Ctrl 键的同时，单击可选择多个分组。

导入资源到分组

软件支持将相同或不同通道资源导入到一个分组中，可根据通道资源类型等建立分组，方便通道资源管理。

前提条件

已添加设备和分组。

操作步骤

说明

一个分组下不能重复添加同一个通道，但一个通道可以同时添加到不同的分组下。

1. 在维护与管理区域，单击 *设备管理 → 分组* 。
2. 选中分组下的通道类型。
3. 根据需要导入的通道类型，单击*导入*。
4. 勾选待导入的资源，单击*导入选择*，将所选择的资源导入到分组中。
5. 可选操作: 可根据实际情况，执行如下相关操作。

展开或收起可导入资源列表	单击箭头可以展开和收起分组资源列表。
搜索设备资源	输入关键字并单击 ，可根据条件搜索出待添加的通道资源。

修改资源信息

支持修改分组中的通道资源的相关信息等。

前提条件

已添加设备和分组。

操作步骤

1. 在维护与管理区域，单击 *设备管理 → 分组* 。
2. 在分组列表中，选择某一分组。

右侧区域显示该分组下的设备资源列表。

3. 选择通道资源，如门禁点、雷达，单击修改 图标。
4. 修改通道资源信息，名称等。
5. 单击*确定*。
6. 可选操作: 可根据实际情况，执行如下相关操作。

查看设备信息 单击 ，可查看该设备的基本信息。

删除 选择某分组，勾选该分组下的通道，单击*删除*，可删除该分组下的通道资源。

移除分组中的资源

选中分组中的资源，可将该资源从分组中移除。

前提条件
已添加设备和分组。

操作步骤
1. 在设备管理界面，选择*分组*页签。
2. 在左侧资源列表中，选择 1 个分组，则右侧区域显示该分组下的资源列表。
3. 选择一个资源，单击*删除*。

7.2 人员管理

支持添加人员，通过添加人员可设置人员的基本信息和访问权限，控制人员出入；也可以根据人员居住地址绑定室内机，进行可视对讲；支持将人员添加到指定组织，方便为人员进行批量配置考勤规则，统计考勤数据，通过组织方便人员管理。

7.2.1 添加组织

支持通过自定义组织名称的方式逐一添加组织，完成可以继续为该组织添加下级组织。

操作步骤
1. 进入人员管理界面。
2. 在左侧组织列表区域，选择 1 个上级组织。
3. 单击组织区域上方*添加*。
4. 输入组织名称。

新添加的组织作为所选组织的下级组织展示在列表中。

说明

最多支持添加 10 级组织。

5. 可选操作: 添加组织后，如有需要可执行以下操作。

修改组织 选择已添加的组织，单击 可以修改组织名称。

删除组织 选择已添加的组织，单击 可以删除该组织。

说明

- 删除时，请先确认该组织下没有人员，否则无法删除。
- 删除上级组织时，同时会删除其下级子组织。

显示子组织成员 勾选**显示子组织成员**单击某一组织，成员列表将显示该组织及其下级组织成员。

后续处理

添加组织后，需要把人员信息添加至对应组织中。参见 *配置人员基本信息* 和 *批量导入/导出人员* 。

7.2.2 添加单个人员

支持逐个添加人员到客户端并配置人员信息，包括基本信息、凭证（卡片、指纹）、访问控制、住户信息、扩展信息等。

自动读取人员身份信息

添加人员时，可以通过身份证阅读器读取人员相关信息，并自动填充到基本信息以及扩展信息项中，如扩展信息项中的证件类型，姓名，证件号码，生日。

前提条件

1. 请确保已为待添加人员建立对应组织。参见 *添加组织* 。
2. 请确保已将身份证阅读器正确连接至当前客户端运行的计算机。

操作步骤

1. 进入人员管理界面。

2. 在右侧区域上方，单击*添加*。

3. 设置身份证阅读器。

1) 单击*配置*。

2) 选择身份证阅读器型号。

说明

- 选择阅读器类型为 DS-K1F1001F 时，可设置是否启用校验指纹信息。
- 身份证阅读器为 USB 接入，客户端只需要选择型号即可。

3) **可选操作**: 勾选*校验指纹信息*。

指纹安全等级

输入指纹安全等级。可输入 1~5 的数值，数值越高，等级越高，指纹误识率越低，拒认率越高。

指纹识别超时时间

当读取身份证后，在所设置的时间内未识别到指纹，则会提示错误信息。

4) 单击*确定*。

4. 单击*读取证件信息*，根据提示刷证件，自动录入身份属性信息。

说明

- 若已开启指纹比对且卡内无指纹，将会提示是否录入身份证信息，单击确定录入身份证信息，否则当身份证内无指纹时，将采集失败。
- 身份证阅读器 DS-K1F1001F 除支持身份证外，还支持中国绿卡和港澳台居民居住证。

5. 完成人员添加。

- 单击*添加*，添加人员并关闭该窗口。
- 单击*添加并继续*，保存配置信息，同时在此窗口继续添加。

后续处理

为已添加人员发卡、采集生物特征（如人脸、指纹等）、配置其他信息。根据需要参见后续章节。

配置人员基本信息

添加人员时，需要配置人员基本信息，如姓名、性别、手机号码、该人员访问权限的有效期限等。

前提条件

请确保已为待添加人员建立对应组织。参见 *添加组织* 。

操作步骤

1. 进入人员管理界面。

2. 在右侧区域上方，单击*添加*。

右侧滑出添加人员窗口。

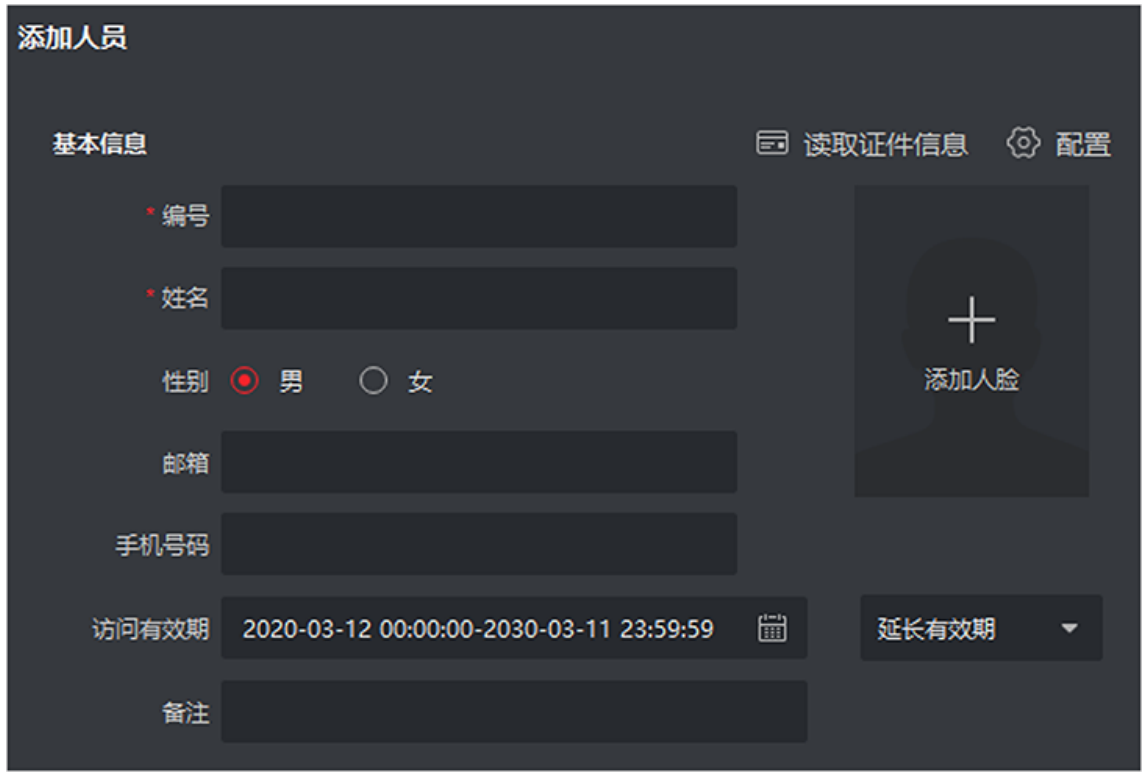


图 7-2 配置人员基本信息

3. 设置基本信息，包括人员姓名、性别、电子邮件、手机号码、访问有效期、备注等信息。

说明

当人员信息超出有效期限，则该人员凭证认证无效，包括指纹、刷卡、人脸识别等。可一键延长有效期，单击*延长有效期*，从下拉框选择延长人员访问有效期为 1 个月、3 个月、6 个月或 1 年。

4. 完成配置人员基本信息。

- 单击*添加*，关闭该界面。
- 单击*添加并继续*，在该界面继续添加其他人员。

后续处理

可根据需要为已添加人员发卡、采集生物特征（如人脸、指纹等）和配置其他人员信息。根据需要参见后续章节。

通过本地模式发普通卡

本地模式是指将发卡器连接至安装客户端的计算机上，通过刷卡后实时读取卡号，从而为人员分配普通卡的卡号。

前提条件

1. 请确保发卡器已正确连接至当前客户端运行的计算机上。
2. 请确保待发放卡片能够正常使用。

操作步骤

1. 进入人员管理界面。

2. 在右侧区域上方，单击*添加*。

说明

配置人员基本信息，具体操作请参考 *配置人员基本信息* 。

3. 单击 *凭证* → + 。

说明

一个人最多可添加 5 张卡，包括智能卡和普通卡。

4. 单击*发卡配置*，进入配置发卡界面。

1) 选择发卡类型为**普通卡**。

2) 选择模式为**本地**。

3) 设置普通卡相关参数。

发卡器

选择发卡器类型，当选择 DS-K1F100-M 时，需输入串口参数项。

蜂鸣

勾选启用蜂鸣，则刷卡成功后会发出嘀一声提示音，刷卡失败则会快速发出滴滴滴提示音。

M1 卡加密

启用 M1 卡加密可以提升门禁卡安全性，使得门禁卡更不容易被拷贝。

4) 单击*确定*。

5. 手动输入或通过单击*开始读取*，同时在发卡器上刷卡，成功后显示读取的卡号。

6. 选择**卡类型**。

正常卡

默认情况下卡片即为正常卡，不需特殊配置。

胁迫卡

胁迫卡刷卡后，除开门外，门禁系统还将上报胁迫事件。

巡更卡

用于根据巡查卡的刷卡时间查询巡查人员的值勤情况，可以根据需要为巡查人员设置门禁权限，或者仅有刷卡值勤功能但无开门权限。

解除卡

刷卡后可解除报警。

7. 单击*添加*。

添加的卡片将显示在卡片列表中。

8. 可选操作: 添加完成后，可根据实际需要执行以下操作。

挂失 选择丢失的卡片，单击 ，卡片置为挂失状态；挂失解挂后需要单击确定按钮后才会弹出同步通知，可选择是否立即下发；下发后，卡片权限从设备中删除。

解挂 选择一个已挂失的卡片，单击 ，可将其卡片取消挂失操作。弹出数据同步通知，可以选择是否立即下发；立即下发后，卡片权限下发到设备中。

为人员发智能卡

添加人员时，支持为人员添加智能卡，并在智能卡中录入指纹、身份证信息。在设备端刷智能卡时，设备将卡片中存储的指纹或身份证信息与认证时采集的指纹或身份证信息进行比对。

前提条件

请确保身份证阅读器、指纹录入仪和读卡器已正确连接至当前客户端运行的计算机。

操作步骤

1. 进入人员管理界面。

2. 在右侧区域上方，单击*添加*。

说明

配置人员基本信息，具体操作请参考 *配置人员基本信息* 。

3. 单击 *凭证* → 。

4. 配置发卡参数。

1) 单击*发卡配置*，发卡类型选择**智能卡**。

2) 选择**发卡模式**。

3) 选择**发卡器型号**或**指纹录入仪类型**。

4) 单击*确定*。

界面切换至添加智能卡窗口。

说明

根据所选择的发卡模式，例如获取指纹或证件信息。

5. 添加智能卡。以选择**指纹+身份证+卡**模式为例。

1) 单击*开始录入*，将手指放置指纹录入仪上。

界面提示指纹已录入。

2) 单击 *下一步*，进入刷身份证窗口，再单击*开始录入*，将证件放置读卡器上开始读取证件信息。
3) 单击 *下一步*，进入读取卡号窗口，再单击*开始录入*，将智能卡放置读卡机上读取信息。
4) 单击*完成*。

添加的卡片将显示在卡片列表中。

6. 可选操作: 添加完成后，可根据实际需要执行以下操作。

编辑 选择一个卡片，单击 ，可以修改卡片信息。

删除 选择一个卡片，单击 可以删除该卡片。

挂失 选择丢失的卡片，单击 ，卡片置为挂失状态；若卡片已配置过权限，则弹出数据同步通知，选择是否立即下发；下发后，卡片权限从设备中删除。

解挂 选择一个已挂失的卡片，单击 ，可将其卡片取消挂失操作。弹出数据同步通知，可以选择是否立即下发；立即下发后，卡片权限下发到设备中。

本地上传人脸

通过本地 PC 支持上传格式为 JPG 或 JPEG、单张或多张人脸图片打包压缩为 ZIP 格式进行上传，从而获取人脸信息。

前提条件

请确保已将符合格式要求的人脸图片保存至当前客户端运行的计算机本地。

操作步骤

1. 进入人员管理界面。
2. 在右侧区域上方，单击*添加*。

说明

配置人员基本信息，具体操作请参考 *配置人员基本信息* 。

3. 单击 *添加人脸 → 上传* 。
4. 弹出本地文件，选择人脸图片进行上传。
5. 可选操作: 启用设备校验。

说明

开启设备校验，可对上传的人脸图片检验是否符合识别要求。

6. 单击*添加*，关闭该界面；或单击*添加并继续*，在该界面继续添加其他人员。

本地采集人脸

添加人员时，可在客户端本地对人脸进行采集，将其作为该人员的图片。

前提条件

请确保客户端所在的 PC 自带摄像头，或已连接其他 USB 相机至 PC。

操作步骤

1. 进入人员管理界面。

2. 在左侧组织列表选择一个组织。

3. 在右侧区域上方，单击*添加*。

说明

配置人员基本信息，具体操作请参考 *配置人员基本信息* 。

4. 单击 *添加人脸* → *拍照*，进入拍照窗口。

5. **可选操作**: 启用设备校验，并选择支持人脸识别的设备。

说明

该功能开启后，可检验上传的人脸图片是否符合识别要求。

6. 单击 ，从下拉框中选择电脑自带摄像头或外接 USB 相机。

7. 单击 ，进行人脸采集。

说明

请面向摄像头，摆正头部，确保人脸正常录入。

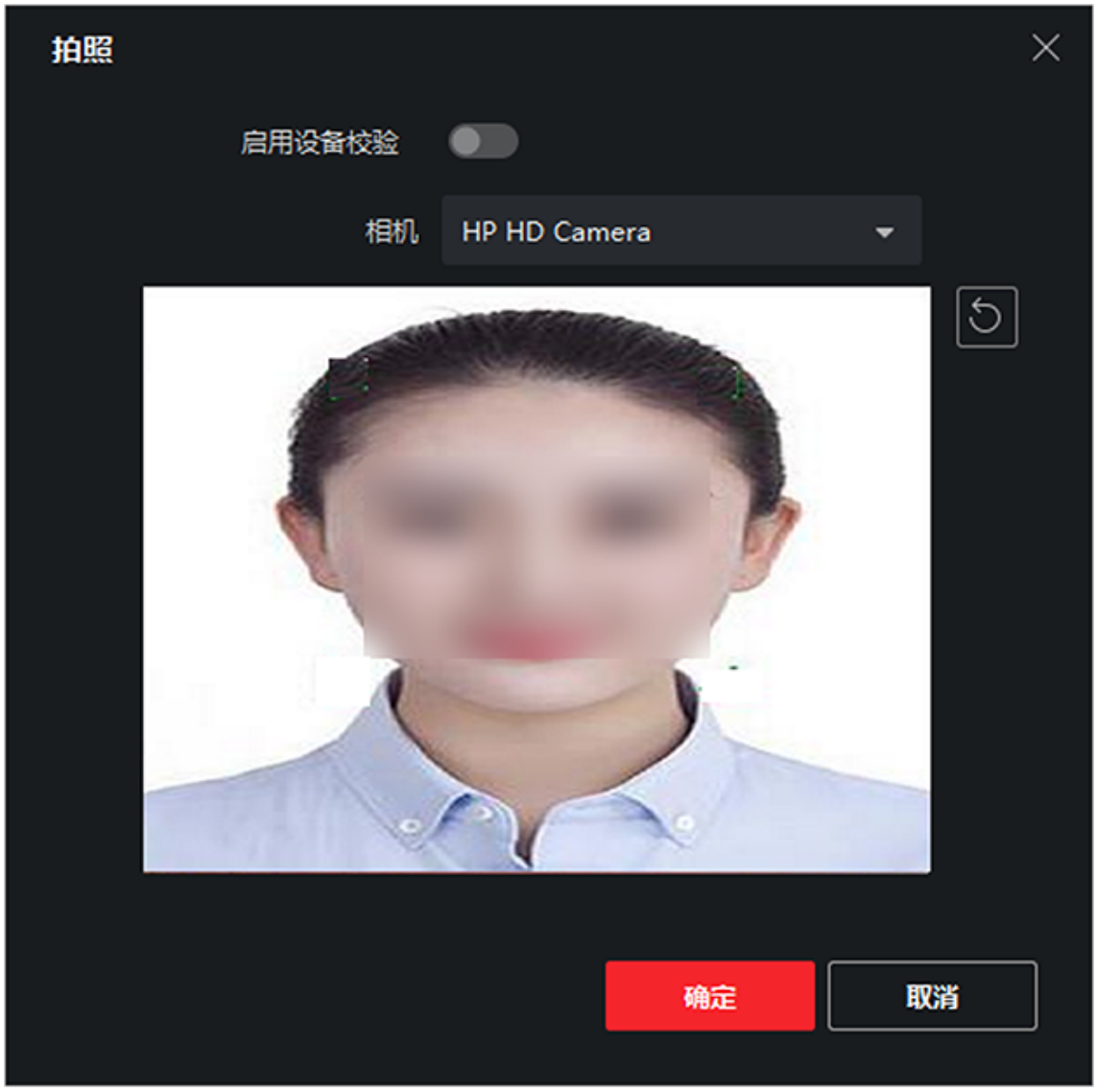


图 7-3 本地采集人脸

8. 单击*确定*，完成人脸图片采集。

9. 可选操作: 根据实际情况，可执行如下相关操作。

重新采集 单击 ，进行图片重新抓拍、上传。

删除 单击 ，将删除已采集的人脸图片。

远程采集人脸

添加人员时，支持人脸采集功能的终端远程采集人脸信息，请人员面向摄像头，摆正头部，确保人脸正常录入。

前提条件

已添加支持人脸采集的门禁设备到客户端。

操作步骤

1. 进入人员管理界面。

2. 在右侧区域上方，单击*添加*。

说明

配置人员基本信息，具体操作请参考 *配置人员基本信息* 。

---

3. 单击 *添加人脸* → *远程采集* 。

4. 单击*选择设备*，选择一台人脸识别一体机，单击*确定*。

5. 单击*开始采集*，采集人脸图片。

6. 可选操作: 根据实际情况，可执行如下相关操作。

重新采集 单击 ，进行再次抓图。

删除 单击 ，将删除已采集的抓拍图片。

7. 单击*确定*。

本地录入指纹

添加人员时，通过装有客户端的 PC 连接指纹录入仪采集人员的指纹信息，方便通过指纹即可识别人员。

前提条件

请确保已连接支持该功能的指纹录入仪，并正确设置参数。

操作步骤

1. 进入人员管理界面。

2. 在右侧区域上方，单击*添加*。

说明

配置人员基本信息，具体操作请参考 *配置人员基本信息* 。

---

3. 单击 *凭证* → *指纹* 。

4. 采集模式选择**本地**。

5. 选择设备类型。

说明

当选择设备类型为 DS_K1F800_F 时，需要设置串口号，否则设备连接失败。

6. **可选操作**: 单击*指纹录入仪设置*，设置串口等参数项，单击*确定*。

7. 将手指放置在指纹机正确位置上，单击*开始录入*，设备开始录入指纹。

指纹模板数据采集后，当相同指纹多次采集，将会提示指纹重复信息。

8. 单击*添加*。

说明

指纹添加完成后，指纹类型无法修改。

远程录入指纹

添加人员时，支持远程录入人员的指纹信息。

前提条件

已添加支持指纹的门禁设备到客户端。

操作步骤

1. 进入人员管理界面。

2. 在右侧区域上方，单击*添加*。

说明

配置人员基本信息，具体操作请参考 *配置人员基本信息* 。

3. 单击 *凭证 → 指纹* 。

4. 采集模式选择**远程**。

5. 单击设备类型对应的下拉按钮，在下拉列表中选择一个采集指纹的设备。

6. 单击*开始录入*，根据语音提示开始录入指纹。

录入完成后，开始录入按键变为重新录入。

7. 单击*添加*。

说明

指纹添加完成后，指纹类型无法修改。

配置访问控制信息

添加人员时，可为人员配置访问权限。通过绑定权限组，授予访问门禁点和访问时间的权限，并支持为该用户配置操作权限。通过配置人员的访问控制信息，便于灵活快捷配置用户访问权限和操作权限。

操作步骤

1. 进入人员管理界面。

2. 在右侧区域上方，单击*添加*。

3. 在**添加人员**窗口，单击*访问控制*选项卡，为该人员设置相关访问权限。

4. 单击 ，勾选已添加的权限组，添加权限组详细操作请参见 *分配门禁权限* 。

5. 设置**密码**，当刷卡、指纹或人脸后，输入人员密码才可开门通行，增加多重验证的安全性。

说明

设置的密码一般为 4-8 位数字，仅当读卡器或个人认证方式设置为需要人员密码时，该密码生效。读卡器认证方式配置详细内容请参见 *配置读卡器认证方式*，个人认证方式详细操作请参见 。

6. 根据实际情况，勾选该人员的操作权限。

超级用户

设备为超级用户，可不遵循常闭，反潜回，首卡授权等验证方式，均可有效通行。

延长关门时间

老人或儿童等行动不便，通过配置该参数后可适当延迟刷卡后门磁闭合时间。

标记为黑名单

设置该人员为黑名单后，该人员认证后通行，但会触发报警事件，提示黑名单事件信息。

标记为访客

可以设置刷卡次数。当刷卡次数超过设置值时，刷卡无效。

设备管理员

勾选此功能，则该人员认证凭证通过后，可进入设备后台进行配置，如可修改设备参数等信息。

说明

超级用户、延长开门时间、标记为黑名单和标记为访客，该四项参数功能互斥，无法同时设置，最多可设置其中一项。

7. 单击*添加*，关闭该界面；或单击*添加并继续*，在该界面继续添加其他人员。

自定义人员属性

添加人员时，可输入该人员的基本信息，居住地、出生日期、证件号等，除此之外，还可以根据需求自定义需要输入的属性名称，比如邮箱地址、紧急联系人等。

操作步骤

1. 进入人员管理界面。

2. 设置自定义信息。

1) 在工具栏中选择**自定义属性**。
2) 单击*添加*。
3) 单击 ，输入待添加的属性名称，如邮箱地址。
4) 单击*确定*。

3. 当添加人员时，设置自定义信息。
1) 在组织列表中选择一个组织，单击*添加*，添加人员到该组织中。

说明

输入人员基本信息，相关详细操作请参见 *配置人员基本信息* 。

2) 在自定义信息区域，输入添加人员的相关信息。
3) 单击*添加*，关闭该界面。单击*添加并继续*，在该界面继续添加其他人员。

配置住户信息

配置人员的详细居住信息，绑定室内机后，可在可视对讲界面点击该人员就可以呼叫该人员绑定的室内机进行通话。

前提条件

请确保已添加可视对讲设备至当前客户端。

操作步骤

1. 进入人员管理界面。
2. 在右侧区域上方，单击*添加*。
3. 在**添加人员**窗口，单击*住户信息*选项卡。
4. 单击绑定设备对应的下拉按钮，选择需要绑定的对讲设备、数字/半数字室内机。

说明

若需要使用可视对讲模块，需绑定可视对讲设备。如果需要绑定半数字室内机，则需要关联门口机，并输入房间号；如果需要绑定数字室内机，则可不用关联门口机也不用输入房间号。

5. 输入*房间号*。
6. 单击*添加*，关闭该界面；或单击*添加并继续*，在该界面继续添加其他人员。

配置人员扩展信息

添加人员时，支持根据实际情况配置人员的职务、入职日期或所住地址等扩展信息。

操作步骤

1. 进入人员管理界面。
2. 在左右侧区域上方，单击*添加*。

说明

配置人员基本信息，具体操作请参考 *配置人员基本信息* 。

3. 在**添加人员**窗口，单击*扩展信息*选项卡。

4. 设置扩展信息，包括出生日期、证件类型、证件号码、职务、入职日期、住址等信息。

5. 单击*添加*，关闭该界面；或单击*添加并继续*，在该界面继续添加其他人员。

7.2.3 批量导入/导出人员

通过导入模板文件可以将人员信息或人脸信息批量导入到客户端，也可以将客户端的人员信息和照片导出到本地 PC。

导入人员信息

通过人员导入模板可以批量导入人员身份属性信息到客户端，包括姓名、性别、出生日期、联系电话等等。

操作步骤

1. 进入人员管理界面。

2. 单击*导入*。

3. 选择导入*人员信息*。

4. 单击 *下载人员导入模板*，下载模板到本地。

5. 在下载的模板中，编辑需要导入的人员信息。

说明

- 导入的人员数目不能超过 5000 人。
- 若导入的人员编号在客户端数据库中已经存在，则无法再添加该人员到其他组织中，需删除已有人员信息。

6. 单击 ...，选择已编辑好的人员模版导入，单击*导入*。

导入人脸图片

添加人员后，可以将含多张人脸图片的 JPG 格式的文件一次导入到客户端。

前提条件

1. 请确保已添加对应的人员信息至当前客户端。
2. 确保待导入的人脸图片已保存至当前客户端运行的计算机本地。

操作步骤

1. 进入人员管理界面。

2. 选择一个已添加的组织，或单击左上方*添加*，新建一个组织。
3. 单击*导入*。
4. 单击 ...，选择导入的人脸图片文件。
5. **可选操作**: 启用设备校验，并选择支持人脸识别的设备。

说明

开启设备校验，可对上传的人脸图片检验是否符合识别要求。

6. 单击 ...，选择本地人脸图标上传。

说明

待导入的人脸文件格式需为 zip，图片以**工号_姓名**命名，单张图片需小于 200K。

7. 选择导入文件，单击*导入*。

导出人员信息

支持将已添加的人员信息导出到本地，包括人员编号、组织名称、人员名称等，方便管理组织人员信息。

前提条件

请确保已添加待导出的人员信息指当前客户端。

操作步骤

1. 进入人员管理界面。
2. 在左侧组织区域，选择一个组织。

说明

选中的组织中已添加成员。

3. 单击*导出*。
4. 选择导出*人员信息*。
5. 勾选需要导出的人员信息类别，如编号、组织、姓名、出生日期、联系电话、指纹等。
6. 单击*导出*。
7. 选择保存路径及导出文件的格式（CSV/Excel 文件）。
8. 单击*保存*。

人员信息文件将导出并保存在电脑本地。

导出人脸图片

支持将已添加的人员的人脸图片导出到本地 PC 存储查看。

操作步骤

1. 进入人员管理界面。

2. 在左侧组织区域，选择一个组织。

说明

选中的组织中已添加成员。

3. 单击*导出*。

4. 选择导出*人脸*。

5. 单击*导出*。

6. 选择保存路径，单击*保存*。

导出已添加人员的人脸照片，照片名称以**工号_姓名**命名，文件格式为 ZIP。

7.2.4 从设备获取人员信息

如果添加到客户端的门禁设备已配置过人员，可以获取设备端的人员信息到客户端。

操作步骤

1. 进入人员管理界面。

2. 选择一个已添加的组织，或单击左上方*添加*，新建一个组织。

3. 单击*获取人员*。

4. 选中已配置人员的设备，并将该设备的人员信息导入该组织中。

说明

- 从设备端获取的人员信息如果已经存在在客户端，则将不会替换客户端的用户信息。
- 客户端最大支持添加 5000 人或 50000 卡。若从设备获取到的人员或卡片超过上限，客户端将不再获取人员。

设备中的人员信息被导入到客户端，并显示在组织成员列表中。

7.2.5 更换人员所在组织

当某人员或某个组织调整变更到其他组织下，可通过更换组织功能实现。

前提条件

已添加组织和人员。

操作步骤

1. 进入人员管理界面。

2. 在左侧组织成员列表中，选中某一组织。

3. 勾选待更换组织的部分或全部人员。

4. 单击*更换组织*。
5. 选择更换到的新组织名称，也可通过搜索快速查询到组织。
6. 单击*确定*。

7.2.6 批量发卡

支持给某组织未发卡人员发卡，通过读卡器或者发卡器获取卡号后自动下发卡片，一人发一卡。

前提条件

请确保待发卡的组织中已添加人员信息。

操作步骤

1. 进入人员管理界面。
2. 选择一个已添加人员的组织。
3. 单击*批量发卡*，进入批量发卡窗口。

说明

若连接好的发卡器，已完成发卡配置，可跳过步骤 4。

4. **可选操作**: 单击*发卡配置*，并选择发卡模式。
- 选择发卡模式为**本地**：
  a. 选择已连接的发卡器。
  b. 选择发卡器类型和卡号类型。

  说明

  - 勾选蜂鸣，则刷卡成功后会发出嘀一声提示音，刷卡失败则会快速发出滴滴滴三声提示音。
  - 若卡类型选择 EM 卡，则包括 IC 和 ID 卡，默认读取 IC 卡；若卡号类型选择韦根 26，则卡号经过规则处理由 10 位数转换为 8 位数。
  - 启用 M1 卡加密，可勾选扇区；单击扇区下方*修改*，可设置扇区数量。 启用 M1 卡加密可以提升门禁卡安全性，使得门禁卡更不容易被拷贝。

  c. 单击*确定*。
- 选择发卡模式为**本地**，则在下拉列表选择一个门禁设备下的读卡器，单击*添加*。

5. 单击*初始化*，对读卡器/发卡器的配置参数设为默认值。

后续处理

回到添加卡片窗口，单击*开始读取*，同时在读卡器/发卡器上刷卡，成功后显示不同人员读取到的卡号。

7.2.7 卡片挂失

卡片遗失后，需及时对卡片进行挂失，禁用相关的门禁权限，防止被不法利用。

操作步骤

1. 进入人员管理界面。
2. 选择需要挂失卡片的人员，单击*修改*。
3. 单击 *凭证 → 卡片* 。
4. 选择丢失的卡片，单击 。

卡片置为挂失状态。

5. 可选操作: 若卡片已找到，选择卡片单击 ，可以取消卡片挂失操作。

卡片状态显示为正常状态。

6. 若卡片已配置过权限，会弹出数据同步通知，选择是否立即下发使卡片权限从设备中删除。

7.3 门禁配置

通过客户端可进行人员管理、卡片管理、门禁权限配置、状态监控、高级配置等相关功能和操作。

说明

只有具备门禁控制模块权限的用户才允许进入门禁控制界面对设备进行管理。门禁控制模块用户权限设置请参考*用户管理*。

7.3.1 计划模板

支持配置计划模板，包括周计划和假日计划。应用计划模板，可以使门禁设备权限在模板设置的有效时间内生效。

添加假日计划

可设置法定假日或指定日期为假日，所设置的有效时间的认证权限高于基本考勤规则的认证权限。当某人员或部门已设置了基本考勤规则，如周一到周五正常 9:00~17:00 上班，那么周一到周五的上班时间需执行考勤规则；若该人员或部门又设置了十一假日计划，该假日计划包括周一到周五，那么优先执行假日计划的有效时间段，未设置的时间段则按照基本规则的有效权限执行。

操作步骤

1. 进入访问控制界面。
2. 在左侧功能区域，选择 *计划模板 → 假日计划* 。

3. 单击*添加*。
4. 在左侧列表中，输入假日计划名称。
5. 在右侧区域，单击*添加*。

说明

最多可添加 64 个假日计划，一个假日最多可设置 8 个时段。

6. 设置假日开始日期和结束日期。
7. 在对应的时间条上单击并拖动，绘制有效刷卡时间段。
8. 可选操作: 执行以下操作，调整已绘制的时间段。
- 移动光标到有效时间条上，当光标显示为手掌图标，单击并拖动时间条到合适的时间段。
- 移动光标到有效时间条一端位置，当光标显示为双向箭头，单击并拖动箭头调整起止时间。
- 单击时间条，直接在输入框中编辑起止时间，完成后单击*确定*。

9. 单击*保存*。

添加计划模板

计划模版包括周计划和假日计划，支持设置周计划，通过计划模版，可为不同组织或人员设定门禁权限的时间点。

操作步骤

1. 进入访问控制界面。
2. 在左侧功能列表中，选择 *计划模板* → *计划模板* 。

说明

软件默认已添加两种计划模板，分别为全天有效和全天无效，默认计划模板不可编辑或删除。

全天有效

对应默认启用周计划且不关联假日计划，一周中的每一天刷卡有效。

全天无效

对应默认禁止周计划且不关联假日计划，一周中的每一天刷卡无效。

3. 单击*添加*。
4. 输入计划模板名称。
5. 设置周计划。
1) 在右侧区域，单击*周计划*选项卡。
2) 选择需要设置有效刷卡时间段的一天，在对应的时间条上单击并拖动，绘制有效刷卡时间段。

说明

- 一天最多支持绘制 8 个时间段。
- 可移动光标到有效时间条上，当光标显示为手掌图标时，可单击并拖动时间条到合适的时间段。
  移动光标到有效时间条一端位置，当光标显示为双向箭头，单击并拖动箭头调整起止时间。
  单击时间条，直接在输入框中编辑起止时间，完成后单击*确定*。

3) **可选操作**: 完成后，根据实际需要，可以执行以下操作。

复制到本周 选择一个有效时间段，单击*复制到本周*，可以将所选择的计划复制到本周每一天。

删除时段 选择一个有效时间段，单击*删除*，可以将所选择的时间段删除。

清空 单击*清空*可以清空周计划中所有有效时间段。

6. 选择假日计划。

1) 单击*添加*，详细操作可参考 *添加假日计划* 。
2) 在右侧区域，单击*假日计划*选项卡。
3) 在待选择假日计划列表中勾选一个或多个假日计划。

说明

- 添加假日计划更多操作可以参考 *添加假日计划* 。
- 计划模板最多可添加 255 个，每个计划模板最多可添加 4 个假日计划。

7. 单击*保存*。

7.3.2 分配门禁权限

支持分配门禁权限到指定人员，使其获取通行指定门的权限。

前提条件

- 添加人员到客户端。
- 添加门禁设备并为门禁点分组。
- 添加计划模板。

操作步骤

1. 进入访问控制界面。
2. 在左侧功能区域，选择 *权限管理 → 权限组* 。
3. 单击*添加*。
4. 输入权限组名称。
5. 选择一个计划模板。

说明

添加权限组前，若不使用默认计划模版，可预先配置模板，更多相关操作请参考 ***添加计划模板***。

6. 在人员列表中，勾选需要分配权限的组织人员。

7. 在门禁设备列表中，选择门禁点。

说明

- 同一人同一门禁点最多只能添加到 4 个不同的权限组中。
- 最多支持添加 128 组权限组。

8. 单击 ***保存***。

完成后，已选择的人员将会具有所选门禁点设备的权限，通过关联的卡片、指纹、人脸认证识别后开门通行。

9. 添加权限组后，需要下发给对应设备生效。

说明

当修改权限组中的人员信息或其他信息后，界面右上方将出现***权限待下发***提示信息。

1) 勾选一个或多个权限组。

2) 根据需要，单击***全部下发***或***异动下发***。

全部下发

清空现有门禁设备上所有的权限，再将当前配置的门禁权限全部下发到设备中。门禁权限主要包括人员的基本信息、凭证信息、访问权限、住户信息、扩展信息等。

异动下发

只将修改过的门禁权限下发到设备中。

弹出当前权限下发进度窗口。

10. 可选操作: 可根据实际情况，执行如下相关操作。

搜索	在下发状态窗口的搜索框中输入人员，单击 ，可以查看该人员的凭证类型、关联门和权限下发状态。
查看下发状态	单击 ***下发状态***，可查看最近一次权限下发状态的详情，包括下发状态、凭证编号。

图 7-4 查看下发状态

7.3.3 高级配置

通过高级配置，可根据场景设置某些特殊需求，比如设备参数等。

注意

需要设备支持才可以配置高级功能中的功能。

配置门禁参数

添加门禁设备后，可以配置门禁参数，如设备参数、门信息、读卡器信息、通道控制器信息、报警输出参数。

配置门禁设备参数

配置门禁设备参数。

操作步骤

1. 进入访问控制界面。
2. 在左侧功能区域，选择 *高级配置* → *设备参数* 。
3. 选择某一门禁设备，配置参数信息。

说明

不同型号设备所需配置参数信息不同，请以实际界面为准。

下行 RS-485 通信备份

RS-485 读卡器通过冗余方式连接到门禁设备。

启用 NFC 卡

启用 NFC 卡后，设备可识别 NFC 卡，用户可在设备上刷 NFC 卡。

启用 M1 卡

启用 M1 卡后，设备可识别 M1 卡，用户可在设备上刷 M1 卡。

启用 EM 卡

启用 EM 卡后，设备可识别 EM 卡，用户可在设备上刷 EM 卡。

启用 CPU 卡

启用 CPU 卡后，设备可识别 CPU 卡，用户可在设备上刷 CPU 卡。

启用 ID 卡

启用 ID 卡后，设备可识别 ID 卡，用户可在设备上刷 ID 卡。

4. **可选操作**: 单击*复制到*可以将此处配置的门禁设备参数应用到其他门禁设备上。

5. 单击*确定*。

配置门信息

支持设置门磁状态、出门按钮类型、正常情况下门锁动作时间等信息。

操作步骤

1. 进入访问控制界面。

2. 在左侧功能区域，选择 *高级配置 → 设备参数* 。

3. 在控制器列表中，选择门禁设备下的门。

4. 设置相关参数。

别名

可以修改门的名称，并将修改后的名称同步到该门所关联的门禁设备上。

出门按钮类型

正常情况下应处于常开状态（特殊需求除外）。

门锁动作时间

普通卡刷卡后，门锁开启时间。

门开超时报警

若门在达到门锁动作时间后还未关闭，门禁点将发出报警。设置为 0 时，表示不启用报警。

超级密码

指定人员输入超级密码即可开门。

说明

- 单击*高级*，可设置**关门延迟时间**和**胁迫码**。

  胁迫码

  遇到胁迫时，输入胁迫码即可开门。同时，门禁系统将上报胁迫事件。

  解除码

  输入解除码可解除设备报警状态。
- 胁迫码、超级密码和解除码三者密码不能重复，一般为 4~8 位的数字。

---

5. 单击*确定*。

6. **可选操作**: 单击*复制到*，选择 1 个或多个需要复制到的门禁点，单击*确定*，可将当前配置的门参数连同状态时段下发到已选择的目标门禁点。

配置读卡器信息

支持配置读卡器基本参数信息，包括重复刷卡的最小时间间隔、读卡失败报警、人脸和指纹等基本信息。

操作步骤

1. 进入访问控制界面。

2. 在左侧功能区域，选择 *高级配置* → *设备参数* 。

3. 在控制器列表中，选择门禁设备下的读卡器。

4. 设置相关参数。以外接指纹读卡器为例，可配置参数项如下所示：

别名

配置读卡器名称，方便用户识别。

重复刷卡最小间隔时间

同张卡在规定间隔时间内重复刷卡无效。可设的间隔时间区间为 0~255 秒（设为 0 时，表示“重复刷卡间隔时间”未生效，同张卡可以无限次重复刷卡）。

是否启用读卡失败超次报警

若选“是”，表示当错误操作达到读卡器预设错误操作上限时，主机会自动生成报警事件。若选“否”，则不会生成报警事件。

最大读卡失败次数

表示读卡器允许读卡错误操作的上限次数。

读卡器种类

显示当前读卡器的种类。

读卡器描述

读卡器在线时，显示读卡器型号；不在线时，则提示不在线信息。(只读)

5. 单击*确定*。

6. 可选操作: 单击*高级*可配置更多参数。

基本信息

是否启用读卡器

启用该功能则该读卡器可以正常刷卡使用；禁用该功能则进门读卡器不可以正常刷卡使用。

OK LED 极性

可选择主板的阴极或者阳极。

Error LED 极性

可选择主板的阴极或者阳极。

蜂鸣器极性

可选择蜂鸣器主板的阴极或者阳极。

蜂鸣时间

触发报警后，持续蜂鸣报警的时间长度。

密码输入超时时间

输入密码的相邻两字符可停顿的最长间隔时间。即输完一个字符后，若在设定时间内未输入下一字符，则之前所输字符将自动清空。

是否使能防拆检测

启用该功能则读卡器被拆走或拿走时，主机会自动产生防拆报警事件。禁用该功能则不产生报警事件。

读卡器掉线时间检测

在设定的时间内读卡器若无法与主机联系上，则读卡器进入掉线模式。

指纹信息

指纹识别等级

可选择指纹识别等级，误认率越低，识别等级越高。默认为自适应安全等级-普通。

7. 可选操作: 单击*复制到*，选择 1 个或多个需要复制到的读卡器，单击*确定*，可将当前配置的读卡器参数下发到已选择的目标读卡器。

配置通道控制器信息

支持设置闸机通行模式、自由通行认证、开关门速度等参数。

操作步骤

1. 进入访问控制界面。

2. 在左侧功能区域，选择 *高级配置 → 设备参数* 。

3. 在控制器列表中，选择通道控制器。

4. 设置相关参数。

闸机通行模式

可选择控制闸机闸门状态的控制器。

以设备本地拨码为准

若选择此项，则以设备端拨码的模式为准。此时若通过软件改变通行模式，视为无效。

以门计划模板配置为准

若选择此项，则以与权限控制器通讯的软件所配置的计划为准。此时若通过设备端拨码改变通行模式，视为无效。

开关门速度

用以配置闸门的开门和关门速度。可选择 1~10 之间的数值，数字越大，开门/关门速度越快。

报警提示音时间

可配置报警提示音的持续时间。0 表示报警提示音持续到警情结束。

温度显示单位

可选择显示在设备状态中的温度单位。

灯板亮度

可调节设备灯板亮度。

门翼材质

选择门翼的材质。根据实际设备，从下拉框中可选择对应闸机的门翼材质。

说明

此处门翼材质的选择影响设备的运行。请选择正确的门翼材质，否则门翼可能无法开启。

通道长度

根据实际通道宽度配置。若与实际通道宽度不符，可能影响设备正常运行。

说明

此处通道长度的参数影响设备的运行。请设置正确的通道长度, 否则门翼可能无法开启。

通道内认证禁止开门

若勾选此项，用户若在通道内进行认证，认证成功后，闸门不会开启。

说明

此功能可避免同一用户认证后，多人通过人行通道。

5. 单击*确定*。

配置报警输出

支持从设备获取报警输出参数，并对其进行开启或关闭操作。

前提条件

已添加门禁设备，并确保设备支持报警输出。

操作步骤

1. 进入访问控制界面。

2. 在左侧功能区域，选择 *高级配置 → 设备参数* 。

3. 在左侧列表中，选中 1 个报警输出。

4. 设置报警输出参数。

别名

设置报警输出名称。

报警持续时间

报警信号产生后延后触发报警输出的时间。

5. 单击*确定*。

6. 可选操作: 配置完成后，单击右上角开关，可以开启或关闭该报警输出。

配置常开或常闭

门禁点可按照设置的常开/常关的时间计划，在对应的时间段内切换至常开或常闭状态。在常开时间段内，门禁点将处于未上锁的状态，所有人员无需凭证即可通过该门禁点；在常闭时间段内，门禁点将保持上锁状态，除超级用户外的其他人员（即使拥有通行权限）均不允许通过该门禁点。比如，在博物馆的开放时段内，可设置其大门为常开，游客无需凭证即可进入馆内；在闭馆时段内，可设置大门为常闭，任何人员（除了拥有超级用户权限的管理员）都不允许进入馆内。

前提条件

已添加门禁设备。

操作步骤

1. 进入访问控制界面。

2. 在左侧功能列表中，选择 *高级配置 → 常开常闭设置* 。

3. 在设备列表中，选择某一门禁设备所关联的门。

4. 若制定工作期间的门状态，可设置周计划的门状态。

1) 单击*常开*或*常闭*。

2) 根据实际情况，在周计划时间轴上，拖动鼠标，选择对应常开或常闭的时间段。

说明

当鼠标停留在时间条上，会显示样式为手的图标，单击左键，可设置具体时间点。

3) 单击*保存*。

5. 可选操作: 可根据实际情况，执行如下操作。

复制到本周 选中某一门状态的时间段，单击*复制到本周*，可将该时间段设置复制到周计划的其他时间上。

删除 选中某一门状态的时间段，单击*删除*，则删除该时间段。

清空 单击*清空*，则可将周计划设置的时间段全文删除。

6. 若制定法定假日的门状态，可选择假日计划。

1) 单击*常开*或*常闭*。

2) 设置假日开始和结束时间。

3) 根据实际情况，在假日计划时间轴上，拖动鼠标，选择对应常开或常闭的时间段。

说明

当鼠标停留在时间条上，会显示样式为手的图标，单击左键，可设置具体时间点。

4) 单击*保存*。

配置多重认证

多重认证是一种需要多名人员同时在场并全部认证成功后，才能通行的门禁认证机制。该机制常用于对安保要求较高的重要场所，如银行金库。可通过在场人员的互相监督，保证场所内资金、贵重物品、重要资料等的安全。

前提条件

已添加权限组，并将人员权限下发至待配置多重认证的门禁设备，详细操作请参见 *分配门禁权限* 。

操作步骤

1. 进入访问控制界面。

2. 在左侧功能列表中，选择 *高级配置 → 多重认证*。

3. 在控制器列表中，选择 1 台设备。

4. 添加群组。

1) 单击*添加*。

2) 输入群组名称。

3) 设置有效期。

说明

超过有效期后，该认证组认证成功后仍无法通行。

4) 勾选待添加至认证组的成员。

5) 单击*保存*。

5. 在设备下拉列表中，选择需要进行多重认证才可通行的门禁点。

6. 设置权限组成员之间的认证时间间隔。

7. 添加认证组。

1) 单击*添加*。

2) 在**计划模板**下拉列表中，选择 1 个已配置的计划模板。

3) 选择认证类型。

本地认证

指人员认证通过后即可通行，最多可添加 8 个认证组。

本地认证+远程开门

人员认证成功后，客户端出现信息弹框，告知管理员远程开门，最多可添加 7 个认证组。

本地认证+超级密码

人员认证成功后，并需要输入超级密码才可开门通行，最多可添加 7 个认证组。

4) **可选操作**: 根据实际需要，当选择**本地认证+远程开门**后，可启用离线认证。启用后，设备本地认证如已通过，但设备离线客户端无法执行远程开门时，可通过输入超级密码替代远程开门。

5) 在左侧窗口勾选组群。

6) 单击右侧窗口中需要配置组群成员数量。

说明

成员数量需大于 0 且小于认证组最多成员数，配置的认证组才有效。

7) 单击*保存*。

8. 在多重认证界面，单击*保存*。

9. 可选操作: 在群组列表上方，单击 *下发*，可以将客户端多重认证设置的权限下发给设备。

配置读卡器认证方式

配置门禁设备下读卡器的认证方式，包括刷卡、指纹或人脸等，并可根据周计划设置不同时间段的认证通行方式。

前提条件

已添加门禁一体机或添加已连接读卡器的门禁设备。

操作步骤

1. 进入访问控制界面。

2. 在左侧功能区域，选择 *高级配置 → 认证方式* 。

3. 在控制器列表中，选择门禁设备下的读卡器。

4. 单击*配置*，勾选读卡器认证方式，并单击*确定*。

说明

读卡器认证方式根据设备能力，可支持多种，如刷卡、刷卡+密码、指纹、刷卡+指纹、人脸、人脸+刷卡、人脸+刷卡+指纹等。界面仅显示设备支持的认证方式。

5. 选中认证方式，在对应时间条上单击并拖动绘制生效时间段。

6. 重复以上步骤，绘制其他认证模式下的生效时间段。

7. 可选操作: 选择绘制完成的时间段，单击*复制到本周*则本周每天都有相同的设置。

8. 可选操作: 单击*复制到*可以将此处配置的读卡器验证周计划应用到其他读卡器。

9. 单击*保存*。

配置首人开门

首人开门支持设置首人常开和首人授权模式，如团体访客。首人常开常应用于大批量人员通过的地点或场景。拥有首人常开权限的人员刷卡开门后，开门状态会持续一段时间，其他人员在此时间段内不用再进行权限认证即可通过。首人授权应用于安全要求比较高的场所，只有拥有首人授权权限的人员刷凭证后，其他人员才能够正常进行权限验证。

操作步骤

1. 进入访问控制界面。

2. 在左侧功能项中，单击 *高级配置 → 首人开门* 。

3. 在控制器列表中，选择一个门禁设备。

4. 单击*当前模式*列，选择授权模式。

启用首人常开

选择首人常开模式，需要设置常开持续时间，默认为 10 分钟。

禁用首人常开

禁用首人常开功能。

首人授权

选择首人授权模式后，除超级卡、超级密码、超级指纹、胁迫卡、胁迫密码、胁迫指纹外的其他认证凭证，都需要在首人认证后，再分别通过认证后，才可通行。

5. 添加人员。

1) 单击*添加*。

2) 选择需要添加的人员。

3) 单击*确定*。

6. 单击*保存*。

配置反潜回

反潜回功能是指用户必须按照设定的路线依次认证，否则下一通道认证无效，以防止代认证、尾随等异常出入事件。例如，某些研究机构规定参观人员必须从 A 门进，B 门出，如果参观人员未在 A 门认证进入，则无法在 B 门通过认证；同时，若无 B 门认证记录，则无法再次在 A 门进行认证。

前提条件

需要设备支持并开启反潜回功能。

操作步骤

1. 进入访问控制界面。

2. 在左侧功能列表中，选择 *高级配置* → *反潜回* 。

3. 在控制器列表中，选择一台设备。

4. 选择反潜回的首个读卡器。

5. 在已选择的首个读卡器对应的**配置后续读卡器**输入框中单击 。

6. 在打开的窗口中，勾选后续出门认证的读卡器，单击*确定*。

说明

最多可选择 4 个读卡器为后续读卡器。

7. 单击*保存*。

结果说明

当设备开启反潜回时，如非超级权限用户正在认证的读卡器使能反潜回功能，则设备对用户进行反潜回认证且认证时遵循以下规则：

- 未设置首个读卡器

- 若设备记录的用户上一次通过的读卡器未开启反潜回或该用户是新用户，则反潜回认证通过。
- 若设备记录的用户上一次通过的读卡器已开启反潜回，则需判断当前读卡器是否在上一次通过的读卡器的反潜回后续读卡器内，若是，则反潜回通过认证；若否，则反潜回认证失败。

- 已设置首个读卡器
  - 用户在任何情况下刷首个读卡器都反潜回认证通过。
  - 若设备记录的用户上一次通过的读卡器启用反潜回，则需判断当前读卡器是否在上一次通过的读卡器的反潜回后续读卡器内，若是则反潜回认证通过，否则反潜回认证失败；其他情况，用户反潜回认证都失败。

7.3.4 配置更多参数

添加门禁设备后，可以为其配置相关参数。

开启 M1 卡扇区加密验证

启用 M1 卡加密可以提升门禁卡安全性，使得门禁卡更不容易被拷贝。

操作步骤

说明

该功能需设备支持。

1. 进入访问控制界面。

2. 单击 *高级配置 → 更多参数* 。

3. 选择需要配置参数的设备，单击 *M1 卡扇区加密验证*

4. 启用该功能，并输入扇形编号。

说明

建议加密第 13 扇区。

5. 单击*保存*。

后续处理

启用 M1 卡加密功能后，需在配置卡片时配置卡片加密参数。具体配置方式，请参见 *通过本地模式发普通卡* 。

配置 RS-485 参数

当门禁设备通过 RS-485 接口外接设备（如读卡器）或作为外接读卡器连接主机时，需要配置 RS-485 参数，如串口号、波特率、数据位、停止位、校验类型等。

操作步骤

说明

该功能需设备支持，根据设备功能显示相应的参数。

1. 进入访问控制界面。
2. 选择 *高级配置 → 更多参数* 。
3. 选择需要配置参数的设备。
4. 单击 *RS-485 参数*。
5. 根据实际需求设置 RS-485 串口号、外接设备、认证中心、波特率、数据位、校验类型、通行模式等参数。
6. 单击 *保存*。

说明

配置 RS-485 参数后，重启设备以生效。

7.3.5 门禁事件配置

支持为门禁事件配置联动，包括客户端联动、事件联动和卡号。支持客户端直接发起报警声音和邮件，也根据设备功能支持配置不同报警事件、卡号触发目标联动录像、蜂鸣。

配置客户端联动

门禁事件可联动客户端，客户端接收报警事件，联动报警声音和发送邮件，并通过客户端发出报警信息。

操作步骤

1. 在维护与管理区域，单击 *事件管理 → 门禁事件* 。
2. 在中间区域展开门禁设备列表，选择 1 个门禁设备、报警输入、门禁点（门）或读卡器。
3. 勾选需要设置联动的事件类型。
4. 单击 *修改联动*。
5. 勾选**联动客户端动作**。

声音报警

触发客户端音频报警，勾选后，可单击下拉按钮选择不同类型的声音报警。

说明

可根据需求添加自定义的声音报警, 详细操作请参见客户端用户手册中*配置报警提示音*。

发送邮件

报警联动发送邮件给指定的邮箱。

6. 可选操作: 单击*修改优先级*，设置报警事件级别。

7. 单击*确认*。

8. 可选操作: 可根据实际情况，执行如下相关操作。

复制到 可以复制已配置的联动方式到其他门禁设备、报警输入、门禁点（门）或读卡器。

全部启用 可自动启用所有客户端联动事件。

全部禁用 可自动禁用所有客户端联动事件。

配置事件联动

配置某一报警事件（如门状态开启）触发后，联动目标录像、发起蜂鸣、开门、撤防或语音通报等动作。

操作步骤

1. 进入访问控制界面。

2. 在左侧功能栏，选择*联动配置*。

3. 在设备列表中，选择 1 个设备。

4. 单击*添加*。

5. 事件源选择**事件联动**。

6. 选择事件类型。

7. 在联动目标区域框，设置是否开启联动目标，包括主机蜂鸣、读卡器蜂鸣、录像、抓拍、报警输出、门禁点、语音播放。

8. 单击*保存*。

说明

- 同一扇门只能关联一个门动作（门关联动作只能是“开”、“关”、“常开”，或者“常关”）。 对于某些报警事件，无法联动“开”、“常开”动作，配置时界面会有对应的提示。
- 联动目标需设备支持才可配置。
- 门事件源中选择的门与联动目标的门不可是同一个门。
- 对于非设备事件，即报警输入事件、门事件和读卡器事件需要设置相应门禁设备的 ID。例如，报警输入事件的通道 ID、门事件的门禁点 ID、读卡器事件的读卡机 ID。

配置卡号联动

选择某一卡号，当识别到该卡号时，则联动目标录像、发起蜂鸣、开门、撤防或语音通报等动作。

操作步骤

1. 进入访问控制界面。
2. 在左侧功能栏，选择*联动配置*。
3. 在设备列表中，选择 1 个设备。
4. 单击*添加*。
5. 事件源选择**卡号联动**。
6. 在卡号联动其后的方框中输入卡号或在下拉列表选择卡号。
7. 选择读卡器作为卡号联动的对象。
8. 在联动目标区域框，设置是否联动目标，包括主机蜂鸣、读卡器蜂鸣、录像、抓拍、报警输出、门禁点、语音播放。
9. 单击*保存*。

说明

联动目标需设备支持才可配置。

7.3.6 状态监控

可在此模块中控制门状态、查看实时访问记录。

在进行相关配置前，请先添加门禁设备，并在“分组管理”中配置门组。具体请参考 *分组管理*。

控制门状态

支持通过客户端控制门禁设备某一门禁点的状态，包括开门、关门、常开、常闭、抓图。

前提条件

操作用户拥有对门的控制权限。权限配置可参见 *分配门禁权限* 。

操作步骤

1. 进入状态监控界面。
2. 在右侧“门禁分组”单击下拉框选择一个分组。
3. 选择要反控的门禁点，按住 Ctrl 键可多选。
4. 单击功能按钮实现相关操作。

开门

只能在指定时间内打开门。

关门

若门是打开状态，单击*关门*将门关闭。具有访问权限的人员可以使用凭据（门禁卡、人脸、指纹等）打开门。

常开

门一直呈打开状态。所有人员无需使用凭据即可进入门。

常闭

门呈关闭并锁住状态。任何人（超级用户除外）都无法开门。

抓图

手动抓拍图片。

说明

- 该功能需要设备支持。
- 同时只能对一个设备进行抓图。抓图文件保存运行客户端的 PC 机上。保存路径设置可参见客户端用户手册中*配置文件保存路径*。

门禁反控操作后，门的最新状态将会显示实时事件列表中，门的图标状态也会发生对应改变。

说明

- 请确认门接上了门磁设备，否则门状态将不会在操作日志中显示。
- 门状态发生变化前提是该门禁点不能被其他客户端布防。只允许一个客户端对门禁点进行布防。对该门禁点配置了布防的客户端可以收到门禁点的报警信息，并可以看到门禁点的更新状态，而其他客户端则不能收到报警信息且门禁点的状态不会更新。

查看实时访问记录

通过状态监控界面可查看在门禁设备上的实时访问记录，包括实时刷卡记录、人脸识别记录、指纹比对记录等。在人员访问时，可查看该人员信息和抓拍图片。

操作步骤

1. 进入状态监控界面。

在列表栏可查看实时访问记录。若门禁设备支持联动抓拍或人证对比，则认证事件信息可显示抓拍图片与持卡人信息（登记照片）或人脸抓拍图片与身份证信息。

说明

在事件类型列表上，右键单击表头，可以选择显示不同列表项。

2. 可选操作: 选择**事件类型**或**事件状态**，筛选认证事件或其他门禁事件。
3. 可选操作: 勾选*自动切换至最新记录*，自动显示当前最新上传的事件，列表默认按时间倒序排序。
4. 可选操作: 单击列表右侧对应的按钮，执行相关操作。
- 单击*人员*查看持卡人照片、编号、姓名、所属组织等信息。
- 单击*联动抓拍图片*查看认证时（如刷卡、人脸识别等）抓拍到的图片（需设备支持），双击图片可查看图片大图。

5. 可选操作: 单击 查看监控详情（包括持卡人详细信息、联动抓拍图片），单击 可全屏查看监控详情。

说明

当移动光标到事件列表与人员模块中间时，光标变为双向箭头，此时向左或向右移动，可调整事件列表与人员模块之间的宽度。

7.4 事件中心

通过客户端可为设备（如编码设备、门禁设备、可视对讲）配置事件联动，当设备某一事件发生并将事件上传至客户端时，可联动客户端报警。支持在客户端上查询、处理实时事件和历史事件，实现事件的监测和管理，保证有序、安全的监控环境。

门禁事件配置可参见*门禁事件配置*。

7.4.1 设备布撤防控制

可在此对设备进行布防和撤防。布防后，客户端可以接收到设备的报警信息。如果需要在客户端即时接收并查看事件信息，需确保设备已布防。

操作步骤

1. 单击 → *工具* → *设备布防控制*。
2. 在操作栏中，单击开关按钮执行布防和撤防控制。

图 7-5 设备布防控制

3. 可根据实际情况，执行如下相关操作。

全部布防 单击*全部布防*，可对已添加的全部设备执行布防操作。

全部撤防 单击*全部撤防*，可对已添加的全部设备执行撤防操作。

7.4.2 查看实时事件

查看实时报警事件详情（包括事件类型、名称、时间、级别、细节、处理记录等），并支持处理事件。

前提条件

设备已开启布防。具体操作可参见 *设备布撤防控制*。

操作步骤

1. 进入事件中心界面。

2. 在左侧功能栏选择*实时事件*。

在实时事件列表显示实时事件详细信息。

说明

右键点击表头，可以选择性展示/隐藏的表头项。

事件源

触发事件的设备、通道等。

事件时间

指事件被触发的时间。

事件级别

事件紧急程度，可根据事件级别搜索并处理事件。

说明

“未归类”表示该事件类型未设置事件级别。事件级别可在 *维护与管理 → 事件管理* 中配置。

状态

事件处理记录。支持批量处理或在事件详情区域逐个添加处理意见。

3. 可选操作: 选择**设备类型**和**事件级别**或在过滤框输入事件关键字筛选事件。

4. 在事件列表选中 1 个需要查看的事件，查看该事件详情。

说明

事件详情包括事件发生时设备抓拍的图片和其他事件细节。

5. 可选操作: 如有需要可执行以下操作。

处理单个事件	在事件详情区域单击*处理*添加处理意见，支持追加处理意见。
批量处理事件	勾选需要处理的事件，单击*批量处理*，提交处理意见。
邮件通知	**说明** 请先确认已配置邮箱，邮箱配置可参见*配置邮件参数*。 选中事件, 在事件详情区域单击*发送邮件*将事件信息通过邮件发送给指定邮箱。
下载事件图片	将光标移动到图片右上角，出现下载按钮，单击 *下载*。

自动选中最新报警	勾选**自动选中最新报警**将自动选中最新一条报警事件，显示报警详情。
清空	单击*清空*，清空事件列表。
打开/关闭报警声音	单击*打开声音/关闭声音*，即可打开/关闭报警声音。

7.4.3 搜索历史事件

支持按时间、设备类型、事件类型等搜索历史事件，并对事件进行处理或导出。

操作步骤

1. 选择 *事件中心 → 事件查询*。

2. 设置搜索条件。

说明

不同设备类型支持检索条件可能略有差异，请以实际界面为准。

时间

设备检测到事件发生时的时间。

搜索方式

按设备表示资源列表以设备为维度进行分类，根节点为设备，子节点为该设备下的所有资源通道；**按分组**表示资源列表以生成的分组为维度进行分类，根节点为分组名称，子节点为该分组下的所有资源通道，相同设备的不同通道可能属于不同的分组。

说明

按设备搜索时，可以选择是否同时搜索子节点事件。

设备类型

选择后仅搜索该设备类型的事件。

事件级别

配置事件时，按照紧急程度可以配置优先级，分为普通、重要和紧急。可根据事件级别筛选事件进行处理。

状态

选择后仅搜索已处理、未处理或全部的事件。

展示更多

若选择门禁设备，单击*展示更多*，可以设置事件类型、读卡器型号、姓名、卡号、组织进行搜索。

3. 单击*搜索*。

搜索到的历史事件显示在右侧区域。

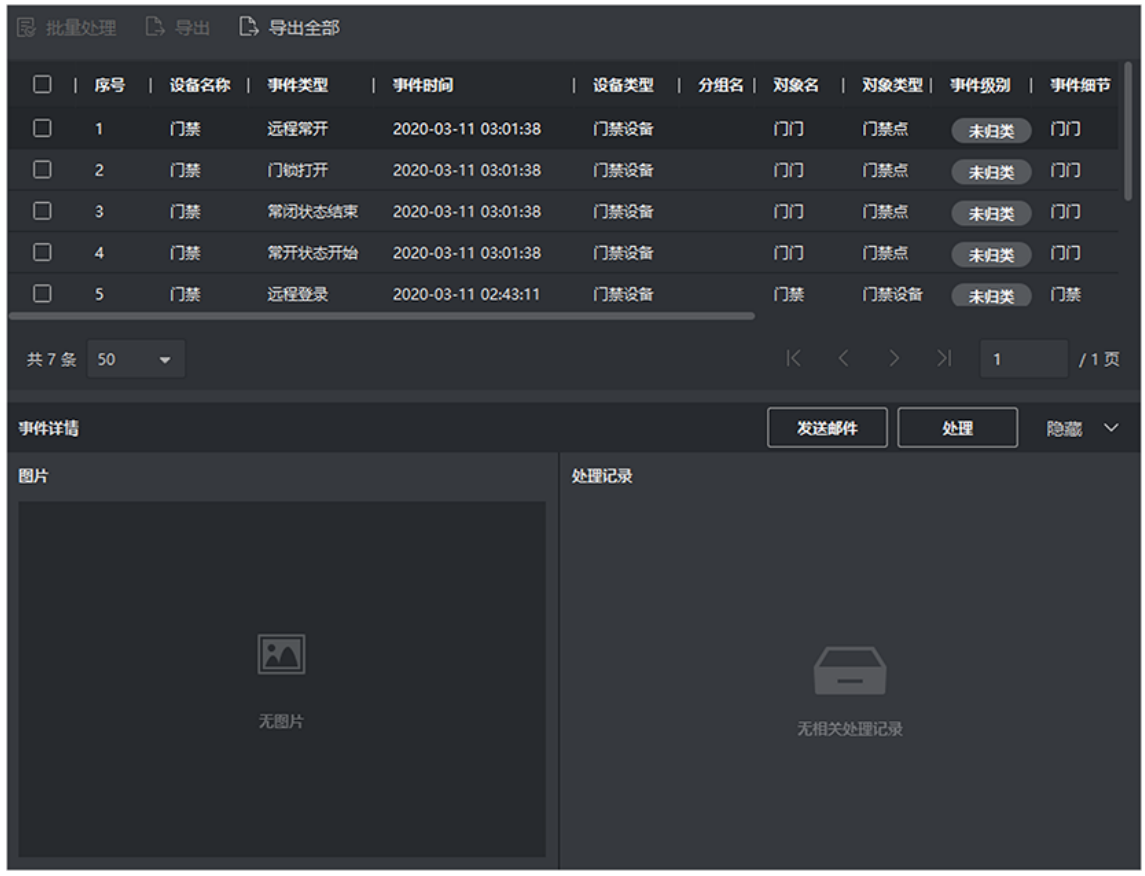


图 7-6 搜索历史事件

4. 在事件列表选中需要查看的事件，查看该事件详情。

说明

事件详情包括事件发生时设备抓拍的图片和其他细节信息。

5. 可选操作: 如有需要可执行以下操作。

处理单个事件	单击*处理*添加处理意见。支持追加处理意见。
批量处理事件	勾选需要处理的事件，单击*批量处理*，提交处理意见。
邮件通知	选中事件，单击*发送邮件*，将事件信息通过邮件发送给指定邮箱地址。

说明

请先确认已配置邮箱，邮箱配置可参见 。

下载事件图片 将光标移动到图片右上角，出现下载按钮，单击 *下载*。

导出 单击 *导出*或 *导出全部*，可将所选择的事件或搜索到的全部事件导出到本地，支持导出内容为全部、按日志和按图片。

第 8 章 远程配置（客户端本地）

8.1 查看设备信息

查看设备基本信息和版本信息。

在维护与管理页面，单击 *设备管理 → 设备* 。

单击 进入远程配置页面。

在远程配置界面，单击 *系统 → 设备信息* 进入设备基本信息界面。在此界面可查看设备基本信息和版本信息。

8.2 修改设备名称

在维护与管理页面，单击 *设备管理 → 设备* 。

单击 进入远程配置页面。

在远程配置界面，单击 *系统 → 常用*，可在此界面配置设备名称。单击*保存*将修改的参数保存。

8.3 修改时间

修改设备显示时间。

在维护与管理页面，单击 *设备管理 → 设备* 。

单击 进入远程配置页面。

在远程配置界面，单击 *系统 → 时间*，并设置时区。

勾选*启用 NTP* 或*启用 DST*，并配置相关参数。单击*保存*将配置的参数保存。

启用 NTP

配置 NTP 服务器地址、NTP 端口及校时间隔。

说明

此处服务器地址即可作为配置网络中心参数的 IP 地址或域名。

启用 DST

可配置夏令时开始时间、结束时间和偏移时间。

8.4 系统维护

重启、恢复设备默认参数、远程升级设备。

在维护与管理页面，单击 ***设备管理 → 设备*** 。

按住 CTRL 并单击 进入远程配置页面。

在远程配置界面，单击 ***系统 → 系统维护*** 。

重启

单击后设备将重新启动。

恢复默认参数

设备的参数将恢复为默认参数，但不恢复设备 IP 地址信息。

完全恢复默认参数

所有参数将被恢复成默认参数，再次使用此设备需要重新激活。

恢复部分默认参数

除通讯配置、远程管理用户配置外，其他参数将恢复为默认参数。

远程升级

在远程升级部分，在下拉框中选择升级文件类型，并选择升级文件，单击***升级***开始升级设备。

主机升级文件

选择设备升级包文件并升级设备。

读卡器升级文件

根据设备配置的设备号选择对应需要升级的读卡器，并选择读卡器升级包文件进行升级。

通道升级文件

需要选择主通道控制器或者从通道控制器，并对主通道控制器和从通道控制器进行升级。

说明

- 升级过程中，请勿将设备断电。
- 仅使用 RS-485 接线的读卡器支持读卡器升级功能。

8.5 管理网络用户

修改 admin 用户信息。

在维护与管理页面，单击 *设备管理 → 设备* 。

单击 进入远程配置页面。

在远程配置界面，单击 *系统 → 用户 → 网络用户* 。选择一个用户，单击*编辑*即可在弹出的对话框中编辑该用户密码、IP 地址以及用户权限。

单击*确定*保存配置。

8.6 管理遥控器用户

可在此页面进行遥控器对码，完成后可通过遥控器控制设备

操作步骤

1. 在维护与管理页面，单击 *设备管理 → 设备* 。
2. 单击 进入远程配置页面。
3. 在远程配置界面，单击 *系统 → 用户 → 遥控器用户* 。
4. 单击添加可以添加遥控器用户。
5. 勾选*启用*并输入遥控器的序列号。
6. 可选操作: 开启闸门的常开状态，对码成功后，遥控器可控制闸门常开。
7. 设置遥控器的开门方向。
8. 单击*确定*。

说明

最多可添加 32 个遥控器用户。

8.7 配置安全参数

配置登录设备端的安全参数，保障设备安全。

在维护与管理页面，单击 *设备管理 → 设备* 。

单击 进入远程配置页面。

在远程配置界面，单击 *系统 → 安全配置* ，并选择安全模式等级。

单击*保存*将配置保存。

兼容模式

登录时兼容旧版客户端用户信息校验方式。

安全模式

登录时用户信息校验安全级别高。

8.8 配置通道参数

可配置人行通道参数。

在维护与管理页面，单击 ***设备管理 → 设备*** 。

单击 进入远程配置页面。

在远程配置界面，单击 ***系统 → 通道参数配置*** 。

完成参数配置后，单击***保存***。

门推迟关闭时间

设置闸门关闭延迟的时间，人员认证通过闸门后，闸门将在设置的时间段后关闭。

最大误闯时间

若有人员误闯通道超过配置的时间，或者人员通过闸机时间超过配置的时间，设备开始误闯报警。0 表示不启用该功能。

说明

建议的最短检测时间为 2s。

滞留超时时间

若探测到通道内有人或物滞留超过设置的时间段，设备开始报警。

最长红外被阻挡时间

可设定最大红外被阻断的时间。若红外对射被阻挡超过设定的时间，设备开始报警。0 表示不启用该功能。

8.9 配置字符屏（显示屏）参数

设备可外接字符屏（显示屏）。可在此界面配置字符屏的显示参数。包括屏幕位置、屏幕型号、屏幕中字体大小、字体显示方向、行间距、列间距以及初始位置。

在维护与管理页面，单击 ***设备管理 → 设备*** 。

单击 进入远程配置页面。

在远程配置界面，单击 ***系统 → 显示屏配置*** 。

完成参数配置后，单击*保存*。

屏幕位置

可从下拉框中选择屏幕所在的在设备端的位置。 如选择*出口*，则屏幕在人员需要出门认证的位置。

屏幕型号

可在下拉框中选择屏幕的型号。

字体大小

可选择屏幕中显示的字体大小。

显示方向

可选择屏幕上显示的文字方向。

行间距

可设置两行字之间的间距。

列间距

可设置同行中两个字之间的间距。

初始位置

可配置在屏幕中开始显示文字的位置。

8.10 人数统计

可配置设备人数统计功能的参数。

在维护与管理页面，单击 *设备管理 → 设备* 。

单击 进入远程配置页面。

在远程配置界面，单击 *系统 → 人数统计* 。

完成参数配置后，单击*保存*。

设备人数清零

单击*清零*，可将设备上记录的人员统计数量清零。

设备人数统计

可选择开启或者关闭设备端人数统计功能。

客户端离线人数统计

可选择开启或者关闭客户端离线人数统计功能。 当开启客户端离线人员统计功能时，设备掉线期间的人员统计数量会自动存储在设备本地，待设备重新上线后，客户端可以自动读取设备离线期间的人员统计数量。

人数统计方式

无

不统计人数。此时若设备人数统计为*开启*状态，人数统计功能仍然不启用。

通行检测

通过设备端人员通过的数量来检测。

认证数量

通过在设备端认证的人员数量来统计人数。若认证失败，依然计算到人数中。

8.11 配置设备高级网络

配置 DNS 服务器地址、报警主机地址、报警管理主机地址及端口。

在维护与管理页面，单击 *设备管理 → 设备 →* 进入远程配置页面。

单击 *网络 → 高级配置* 可配置 DNS1 服务器地址和 DNS2 服务器地址。单击*保存*保存配置。

8.12 配置音频文件

可配置语音内容对应的播放场景，并将此对应的内容导出。还可以本地导入需要播放的音频文件。

操作步骤

1. 在维护与管理页面，单击 *设备管理 → 设备* 。

2. 单击 进入远程配置页面。

3. 单击 *其他 → 音频文件* 进入配置音频文件界面。

说明

系统默认有语音播放内容。具体索引对应的语音播放内容，请参见附录 *语音播放内容对应表* 。

4. 在播放场景中选择索引号（即语音播放内容）所对应的播放场景。

5. 可选操作: 添加播放场景备注。

6. 单击*保存参数*可将播放场景与索引号对应的语音播放内容相关联。

7. 可选操作: 单击导出，可将默认的音频文件导出到本地。

8. 单击...按钮从本地选择需要导入音频文件，并单击*导入*将本地音频文件导入到设备中。

说明

- 导入的音频文件需为 mem 格式。
- 有关如何将音频文件转换成 mem 格式，请参见具体音频格式转换手册。

8.13 查看状态

查看继电器状态。

在维护与管理页面，单击 ***设备管理*** → ***设备*** → 进入远程配置页面。

单击 ***状态*** → ***继电器*** 可查看继电器的状态。

附录 A. 指纹识别注意事项

查看在设备上采集指纹、验证指纹的注意事项。

推荐手指：食指、中指或无名指；避免使用大拇指或小拇指。

- 正确的手指按压方式：手指平压于指纹采集窗上，指纹纹心尽量正对指纹采集窗中心位置。

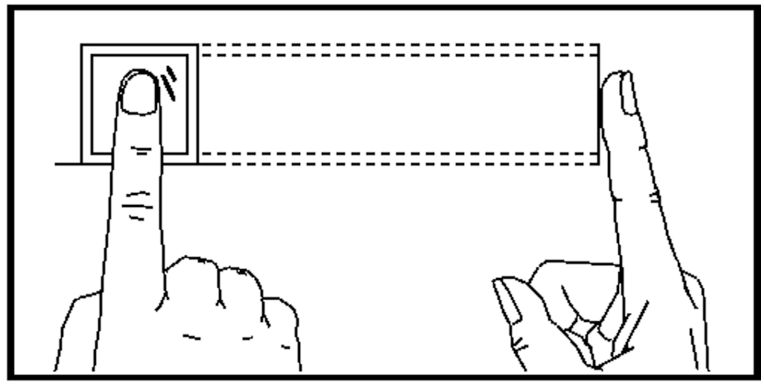


图 A-1 手指按压示意图

- 几种错误的按压方式：垂直指纹采集窗、偏离指纹采集窗中心、手指倾斜、手指太靠下。

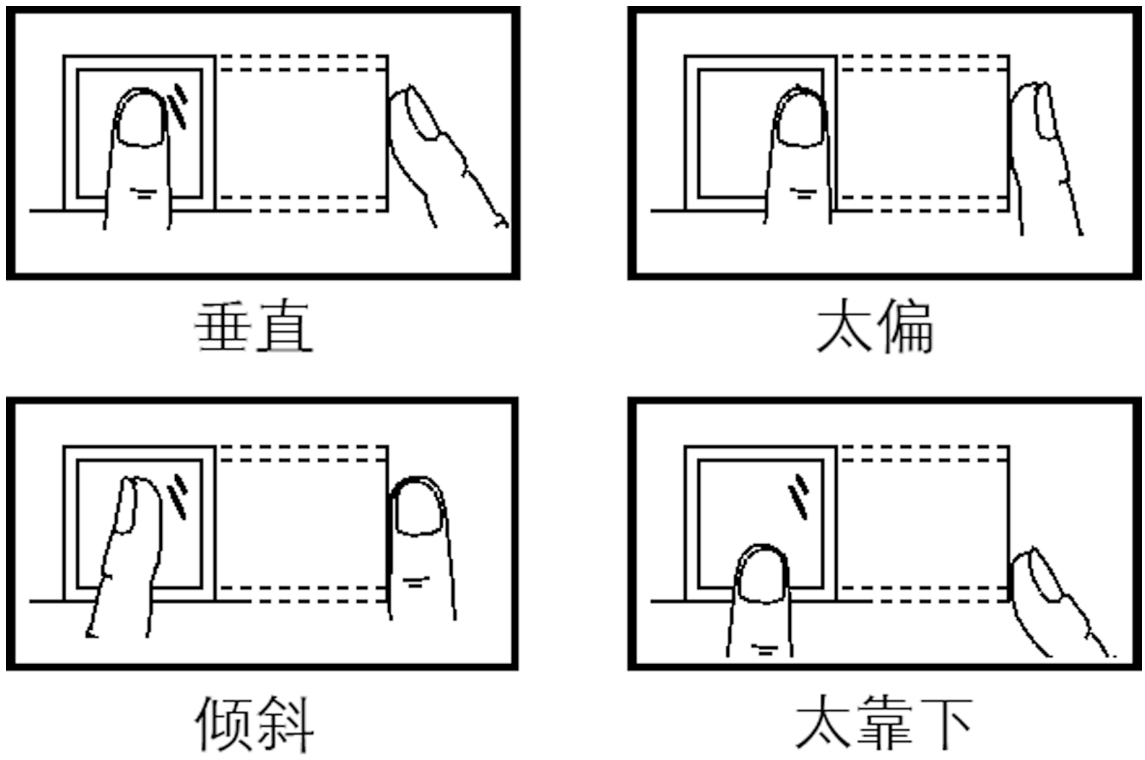


图 A-2 错误的按压方式

- 环境因素：阳光强光直射、温度过高、潮湿、雨水直淋都会对指纹设备产生影响。安装时要注意防水、防潮。如果安装在室外，还需要安装遮阳防水罩。
- 指纹识别小秘诀：冬天比较干燥时，会影响指纹识别的效果。此时在手指上哈一口气，再进行指纹识别，成功率会提高。

附录 B. 拨码

B.1 拨码说明

控制板上有一组 8 位拨码开关。从左到右为最低位到最高位，从左到右号码为 1~8。

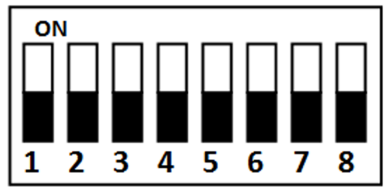


图 B-1 拨码开关示意图

说明

- ：开关在 ON 处表示开关开启（ON）。
- ：开关在 ON 的另一端表示开关关闭（OFF）。

示例

若您需要设置的拨码地址为 12（十进制），则对应的二进制地址为：0000 1100。拨码方式如图所示。

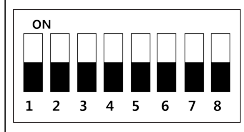
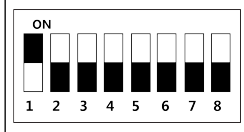
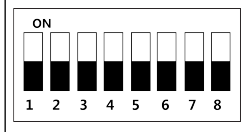
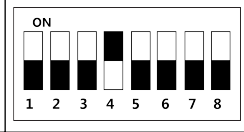
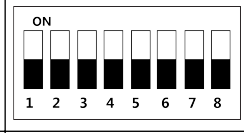
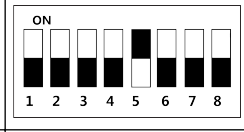
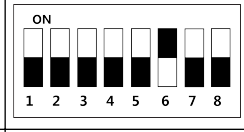
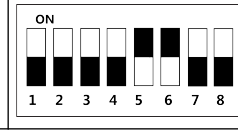
图 B-2 拨码地址举例

B.2 拨码值对应表

权限控制板上的 8 位拨码开关对应值介绍如下表所示。

说明

拨码后需重启设备方可生效。

序号	设备模式	功能	十进制值	拨码示意
1~2	工作模式	正常模式	0	
		学习模式	1	
		测试模式	2	
3	记忆模式	开启记忆模式	0	
		关闭记忆模式	1	
4	遥控器对码模式	开启遥控器本地对码	1	
		关闭遥控器本地对码	0	
5~8	通行模式	双向受控	0	
		进受控，出禁止	1	
		进受控，出自由	2	
		进出自由	3	

序号	设备模式	功能	十进制值	拨码示意
		进自由，出受控	4	
		进自由，出禁止	5	
		进出禁止	6	
		进禁止，出受控	7	
		进禁止，出自由	8	

附录 C. 事件及报警类型

事件	报警类型
尾随	指示灯+主板蜂鸣
反向闯入	指示灯+主板蜂鸣
外力冲撞	无
翻越	指示灯+主板蜂鸣
滞留	指示灯+主板蜂鸣
通行超时	无
误闯	指示灯+主板蜂鸣
自由通行时未认证通过	指示灯
摆臂被阻挡	无

附录 D. 语音播放内容对应表

索引	内容
1	认证通过
2	卡号不存在
3	卡号指纹不匹配
4	人员翻越报警
5	人员反向闯入
6	人员通行超时
7	人员误闯报警
8	外力强行冲撞闸门
9	尾随通行报警
10	无权限进出
11	认证超时
12	认证失败
13	证件过期
14	人员滞留报警

附录 E. 人行通道运行错误码提示说明

人行通道设备将在通道控制板上的数码管上显示错误码提示信息。不同数字代表不同错误原因。详见下表。

错误原因	数码管提示	错误原因	数码管提示
正常运行	00	下部第五颗红外被触发	17
上部第一颗红外被触发	01	下部第六颗红外被触发	18
上部第二颗红外被触发	02	下部第七颗红外被触发	19
上部第三颗红外被触发	03	下部第八颗红外被触发	20
上部第四颗红外被触发	04	下部第九颗红外被触发	21
上部第五颗红外被触发	05	下部第十颗红外被触发	22
上部第六颗红外被触发	06	下部第十一颗红外被触发	23
上部第七颗红外被触发	07	下部第十二颗红外被触发	24
上部第八颗红外被触发	08	进向灯板掉线	49
上部第九颗红外被触发	09	出向灯板掉线	50
上部第十颗红外被触发	10	上部红外转接板掉线	51
上部第十一颗红外被触发	11	下部红外转接板掉线	52
上部第十二颗红外被触发	12	CAN 总线异常	53
下部第一颗红外被触发	13	未学习	54
下部第二颗红外被触发	14	阻挡	55
下部第三颗红外被触发	15	学习超范围	56
下部第四颗红外被触发	16	电机异常	57

附录 F. 技术参数

型号	DS-K3B501SC
通讯方式	TCP/IP、I/O、RS-232、RS-485
红外检测对数	12 对
通行频率	20 ~ 60 人/分钟, 实际通行频率受人员通行速度和人行通道模式影响
电源	100 ~ 240 VAC， 50 ~ 60 Hz
工作温度	-25 ℃ ~ 70 ℃
工作湿度	10% ~95%（在不凝结水滴状态下）
通道宽度	550 mm ~ 1100 mm
门翼材质	不锈钢圆管/有机玻璃（可选）
通道箱体	AISI304 不锈钢 壁厚：1.2 mm
尺寸	1500 mm × 200 mm × 960 mm

附录 G. 通信矩阵和设备命令

通信矩阵

扫描下方二维码可获取设备通信矩阵。通信矩阵视产品型号而定，请以实际设备为准。

图 G-1 通信矩阵二维码

设备命令

扫描下方二维码可获取设备常用接口命令。常用接口命令视产品型号而定，请以实际设备为准。

图 G-2 设备命令二维码

杭州海康威视数字技术股份有限公司
HANGZHOU HIKVISION DIGITAL TECHNOLOGY CO., LTD.

www.hikvision.com
服务热线：400-800-5998

UD23779B-A