D13 系列人脸识别终端

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

⚠危险

- 请不要将多个设备连接至同一电源适配器。
- 为了避免热量积蓄，请保持设备周边通风流畅。 如果设备出现冒烟现象，产生异味，或发出杂音，请立即关掉电源并且将电源线拔掉，及时与经销商或服务中心联系。
- 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。
- 设备的插头或插座是断开电源的装置，请勿遮挡，便于插拔。
- 1. 不要吞咽电池，化学灼伤危险！
  2. 本产品包含纽扣电池。如果吞食纽扣电池，在 2 个小时内就可能导致严重的内部灼伤并可能导致死亡。
  3. 让儿童远离新的和使用过的电池。
  4. 如果电池仓未安全闭合，停止使用该产品并使之远离儿童。
  5. 如果你认为电池可能被吞食或放置在身体的任何部位内，立即寻求医疗救助。
  6. 警告：如果使用错误型号的电池可能导致爆炸危险。
  7. 使用错误型号的电池更换（例如某些类型的锂电池）可能导致安全防护失效。
  8. 请勿将电池投入火中或加热炉中，不要挤压、折弯或切割电池，可能会造成爆炸。
  9. 请勿将电池放置在极高温度环境中，可能导致电池爆炸或泄漏可燃液体或气体。
  10. 请勿将电池放置在极低气压环境中，可能导致电池爆炸或泄漏可燃液体或气体。
  11. 废弃电池对环境会造成污染，请按照说明处置使用完的电池。

⚠注意

- 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。
- 请不要将设备的镜头瞄准强光物体，如太阳、白炽灯等，否则会造成镜头的损坏。
- 在室内使用的设备，不能暴露安装在可能淋到雨或非常潮湿的地方。
- 避免将设备放在阳光直射地点、通风不良的地点，或如加热器或暖气等热源附近（忽视此项可能会导致火灾危险）。
- 请使用足够柔软的干布或其它替代品擦拭表面，切勿使用碱性清洁剂洗涤，避免硬物刮伤设备。
- 设备接入互联网可能面临网络安全问题，请您加强个人信息及数据安全的保护。当您发现设备可能存在网络安全隐患时，请及时与我们联系。
- 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，并妥善保管好您的用户名和密码。

- 请妥善保存设备的全部原包装材料，以便出现问题时，使用包装材料将设备包装好，寄到代理商或返回厂家处理。非原包装材料导致的运输途中的意外损坏，本公司不承担任何责任。
- 生物识别产品无法 100%适用于任何防伪环境。高安全级别场所，请使用组合认证方式。
- 设备可以直接或需要时经修改能与 IT 配电系统连接。
- 设备上不要放置裸露的火焰源，如点燃的蜡烛。
- 设备的串口仅用于调试，禁止用户使用。
- 仅支持使用本手册中列出的厂家和型号的电源。
- 1、请严格参照本指导书中的安装方法进行设备安装。
  2、壁挂式安装：为防止伤害，必须将设备牢固地固定于墙壁或天花板上。
- 注意！本支架预定仅与特定型号设备一起配套使用，与其他设备一起使用可能会导致不稳定而产生伤害。
- 注意！本设备仅能与配套支架一起使用，与其他（如手推车、架子或搬运装置）一起使用可能会导致不稳定而产生伤害。
- 若用户更换适配器，可能引起安全风险。

说明

- 具有门禁系统及组成部分的基础知识和安装技能。
- 具有低压布线和低压电子线路接线的基础知识和操作技能。
- 具备基本网络安全知识及技能，并能够读懂本手册内容。

适用型号

产品名称	产品型号
人脸识别考勤机	D13
	D13 S
	D13 Pro
	D13 Plus

仅支持使用本手册中列出的厂家和型号的电源。

型号	生产商
TS-A012-120010C1	深圳创芯技术有限公司

目 录

第 1 章 概述

1.1 产品简介

人脸识别终端是一款人脸识别类门禁考勤一体化产品。根据不同型号支持人脸、指纹、刷卡、密码多种验证方式，支持人脸识别管控门禁电锁、办公人脸识别考勤，可用于楼宇、企业、写字楼、金融网点、重点区域防护等场所。

1.2 产品功能

- 采用 4.3 英寸触摸显示屏，显示软件界面及操作提示及人脸框，实时检测最大人脸（支持本地视频预览）。
- 采用 200 万广角双目摄像头。
- 支持照片视频防假功能。
- 面部识别距离 0.3 m ~ 2 m。
- 人脸比对时间 ＜ 0.2 s/人，人脸验证准确率 ≥ 99%。
- 采用深度学习算法，支持 500 人脸容量。识别速度快，准确率更高。
- 支持 1000 卡片、500 指纹（部分型号支持）和存储 10 万事件。
- 通过 USB 接口将本地注册人脸、事件记录从设备端导出。
- 本地登录后台管理、查询、设置设备参数。
- 支持通过手机网页端远程配置。
- 支持黑夜补光功能。设备交互界面在夜间自动调亮。

第 2 章 外观介绍

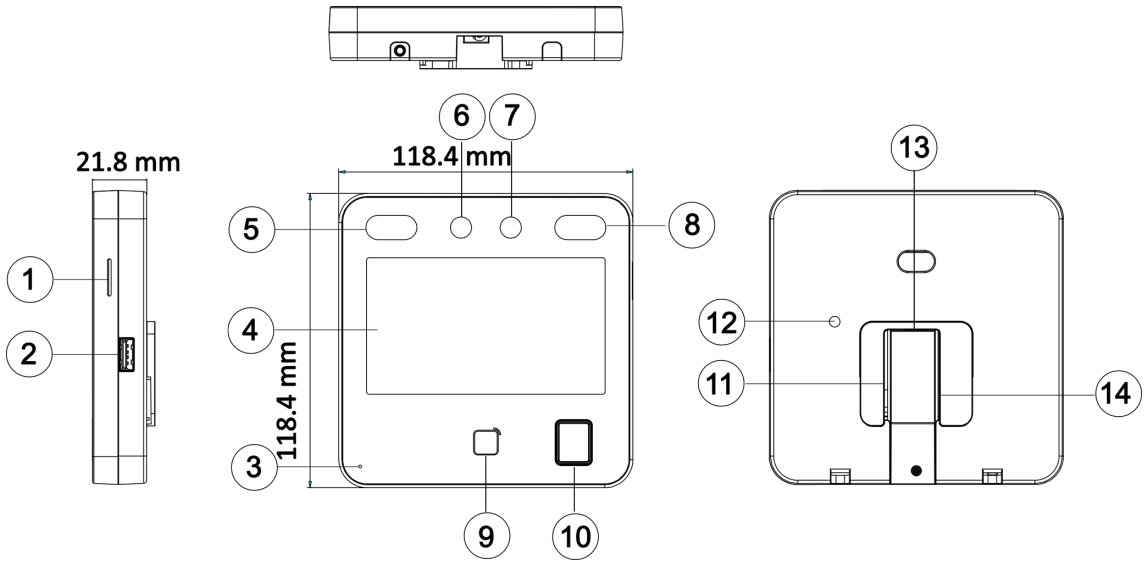


图 2-1 外观说明图（带指纹模组）

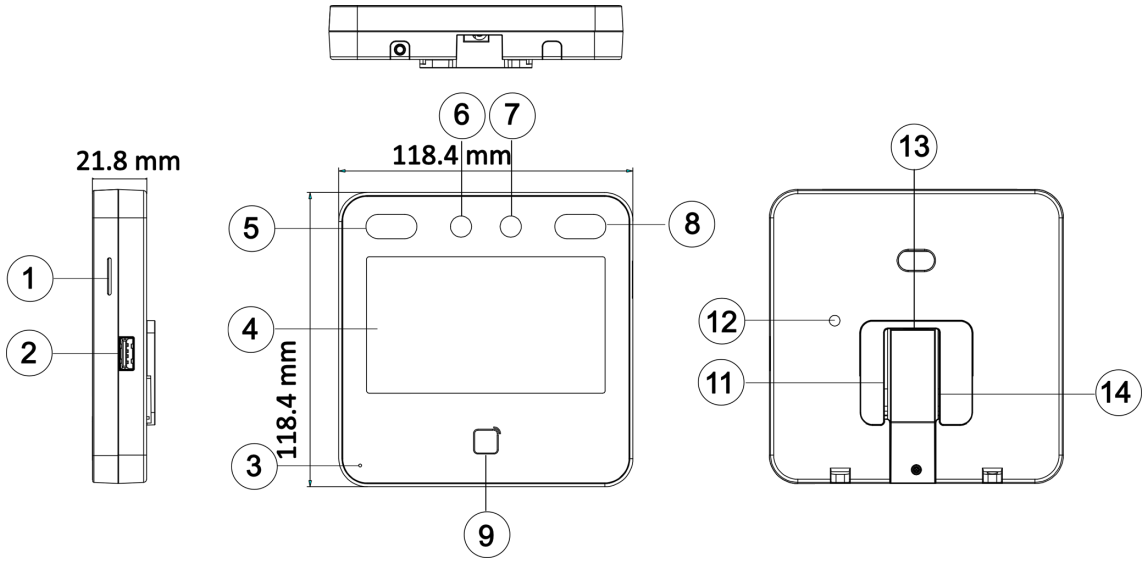


图 2-2 外观说明图（无指纹模组）

表 2-1 外观说明表

部件序号	名称
1	扬声器
2	USB 接口
3	MIC
4	触摸显示屏
5	红外补光灯
6	摄像头
7	摄像头
8	红外补光灯
9	刷卡区域
10	指纹识别区域 **说明** 仅支持指纹功能的设备含有指纹模组。
11	外接排线（含电源线）
12	防拆
13	网口
14	调试串口（仅供调试使用）

第 3 章 安装说明

3.1 安装环境

避免逆光、阳光直射、折射和反射。在有一定光源的环境下进行人脸识别，效果更佳。

说明

具体安装注意事项请参见附录 *安装环境注意事项* 。

3.2 桌面安装

操作步骤

1. 将线缆从过线孔穿出，并将桌面支架紧贴设备后壳。

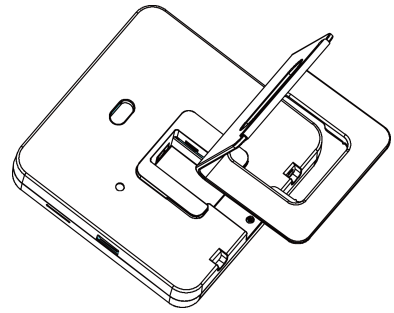


图 3-1 支架紧贴设备后壳

2. 双手按压支架，并确保设备后壳与支架扣合处贴合。沿箭头方向扣合。

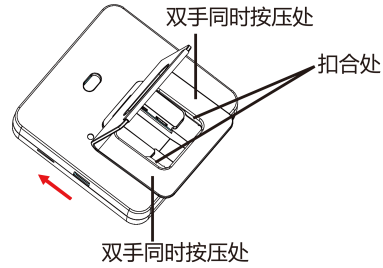


图 3-2 沿箭头方向扣合

3. 卡合到底，完成安装。

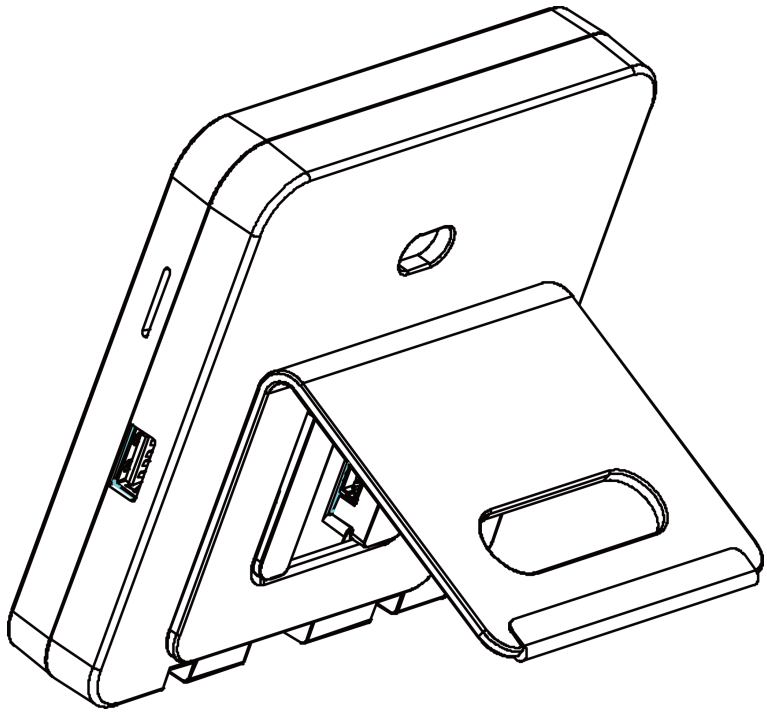


图 3-3 完成安装

3.3 墙面安装

操作步骤

1. 确保墙上已预埋 86 盒。

说明

需用户自备 86 盒。

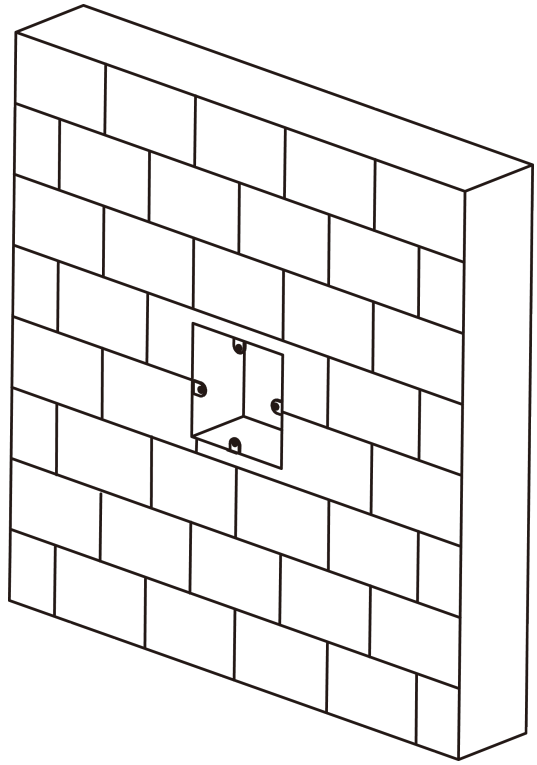


图 3-4 安装 86 盒

2. 用 4 枚螺丝（M4）将安装挂板固定在 86 盒上。

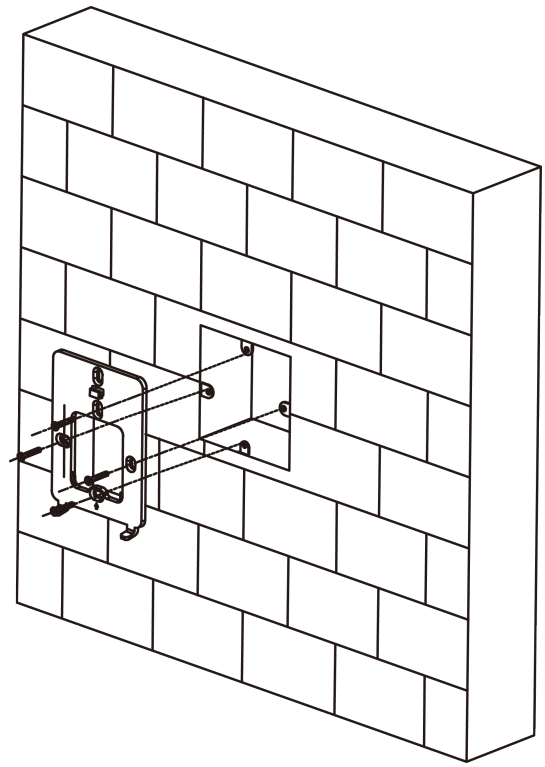


图 3-5 安装挂板

3. 整理线缆，确定出线方式。

4. 将设备与挂板对齐后扣入挂板，并在设备左下角用 1 枚螺丝（M3）固定设备与安装挂板。

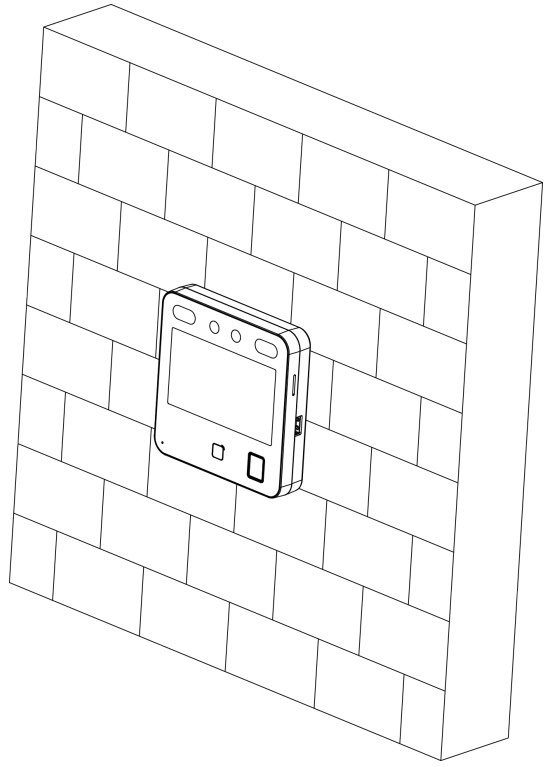


图 3-6 固定设备

第 4 章 接线说明

可通过接线端子连接 RS-485 读卡器、门锁、开门按钮、门磁等。

通过 RS-485 端子连接 RS-485 读卡器，通过 LOCK 端子连接门锁；通过 SEN、BTN、GND 端子连接开门按钮；通过韦根端子连接韦根读卡器和门禁主机。

通过韦根端子连接门禁主机时，人脸识别终端设备可输出认证信息到门禁主机中。

布线时需注意：

- 若使用 1.0 mm²国标线，则需采用 12 V 电源供电，现场施工布线距离（电源到设备的布线长度）不超过 20 m。
- 若使用 1.5 mm²国标线，则需采用 12 V 电源供电，现场施工布线距离（电源到设备的布线长度）不超过 30 m。
- 若使用 2.0 mm²及以上国标线，则需采用 12 V 电源供电，现场施工布线距离（电源到设备的布线长度）不超过 40 m。

说明

外接的读卡器、门锁、开门按钮、门磁等设备，需独立提供供电电源。

4.1 接线端子说明

设备的接线端子包括电源输入、RS-485、韦根输出和门锁。

接线端子具体说明如下表所示：

表 4-1 接线端子说明表

线组	序号	功能组	颜色	名称	端子说明
线组 A	A1	电源输入	红	+12 V	12 V 设备供电电源输入
	A2		黑	GND	接地
线组 B	B1	RS-485	黄	485+	RS-485 接线
	B2		蓝	485-	
	B3		黑	GND	接地
线组 C	C1	韦根输出	绿	W0	韦根数据线 0

线组	序号	功能组	颜色	名称	端子说明
	C2		白	W1	韦根数据线 1
	C3		黑	GND	接地
线组 D	D1	门锁	白紫	NC	电锁控制输出(常闭)
	D2		白黄	COM	公共端
	D3		白红	NO	电锁控制输出(常开)
	D4		黄绿	SEN	门磁信号输入
	D5		黑	GND	接地
	D6		黄灰	BTN	开门按钮接入

4.2 外接普通设备说明

接线说明图如下所示：

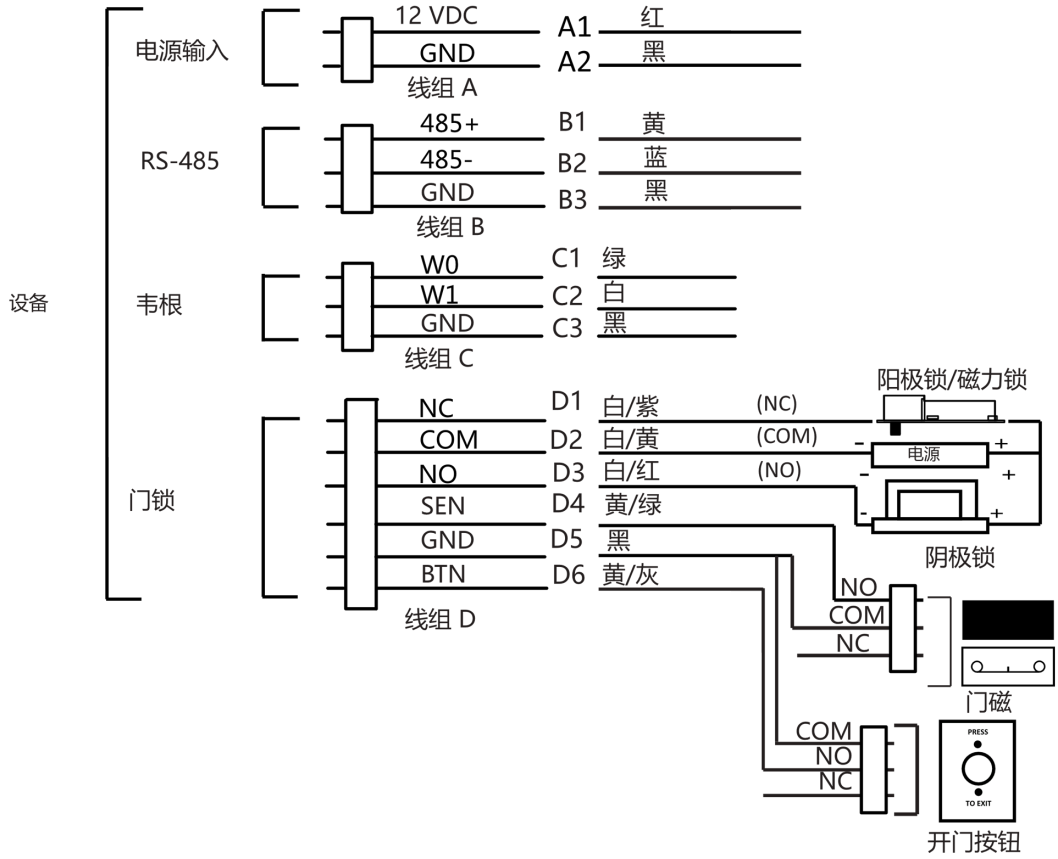


图 4-1 外接设备示意图

说明

- 外接门磁和开门按钮时，需要与 RS-485 或者电源共地。
- 若人脸识别终端外接门禁主机，则韦根接口为韦根输出接口，需将韦根传输方向配置为“输出”，此时可输出认证信息到门禁主机中。具体有关韦根传输方向的配置，请参见通讯设置章节下的设置韦根参数。
- 支持外接 12 V，1A 的门锁；韦根读卡器支持外接 12V，1A 的电源。
- 请勿直接将设备直接接入 220 V 市电。

4.3 外接门控安全模块说明

通过 RS-485 端子可外接门控安全模块。

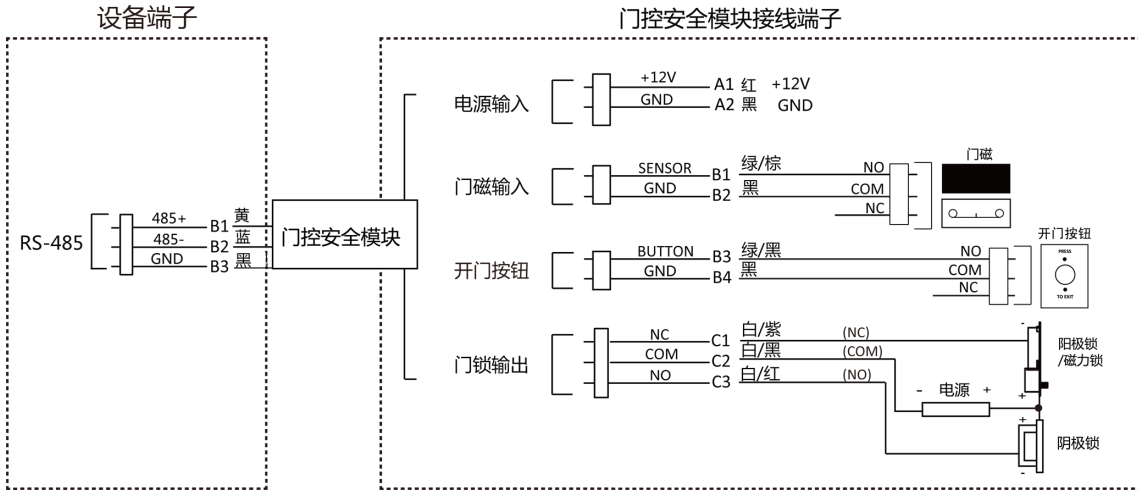


图 4-2 外接门控安全模块示意图

说明

门控安全模块需单独外接电源。支持外接 12 V，0.5 A 的电源。

4.4 外接消防模块说明

4.4.1 断电开锁型接线说明

锁类型：阳极锁、磁力锁、常开型电插锁

安全类型：断电开锁型

用途：主要用于消防通道

方案一

说明

消防系统控制门禁系统电源。

接线说明图如下所示：

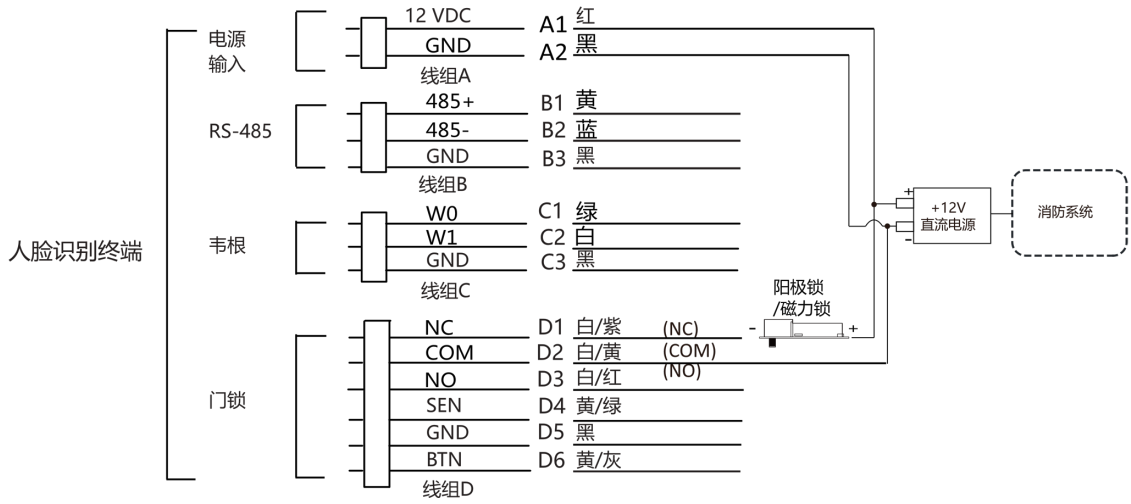


图 4-3 外接设备示意图

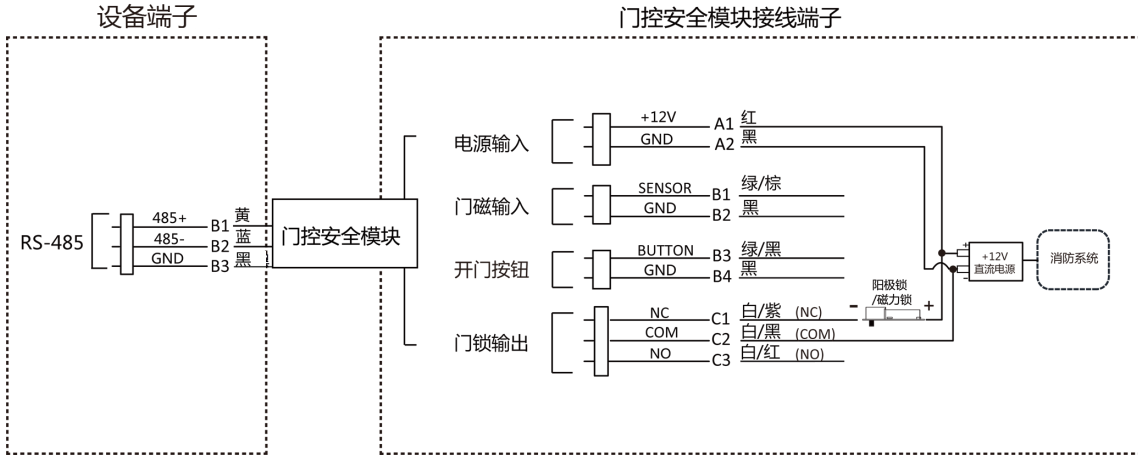


图 4-4 外接门控安全模块示意图

方案二

说明

消防系统串联在门锁与电源回路中，接入消防系统的断电常开端口（NO、COM）。消防事件触发时为默认开门状态，非触发时 NO、COM 为闭合状态。

接线说明如下图所示：

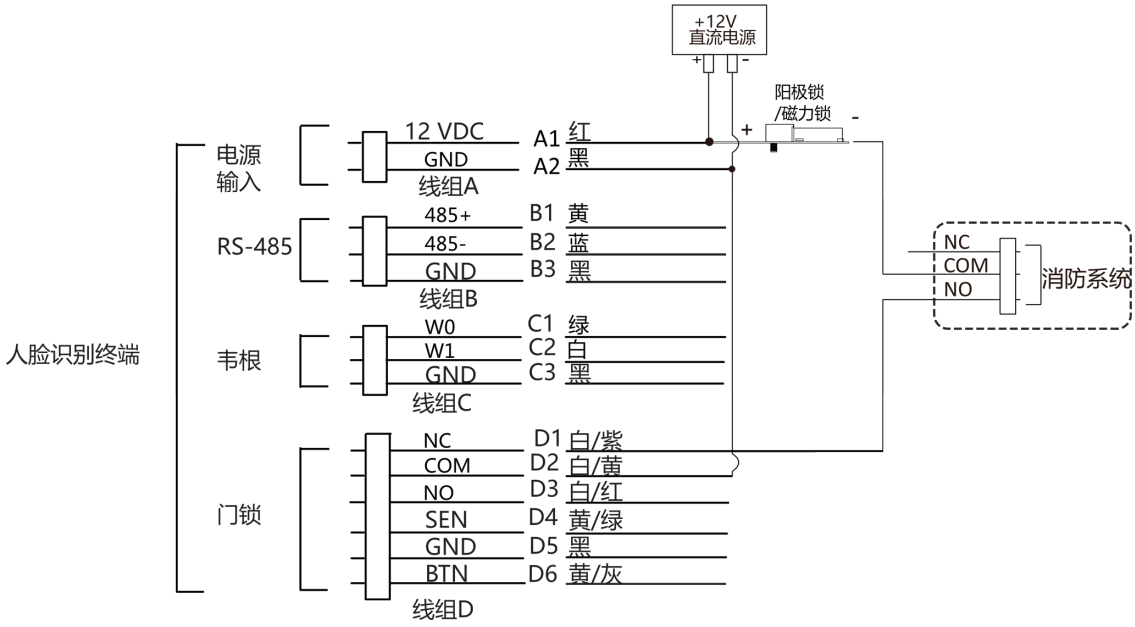


图 4-5 外接设备示意图

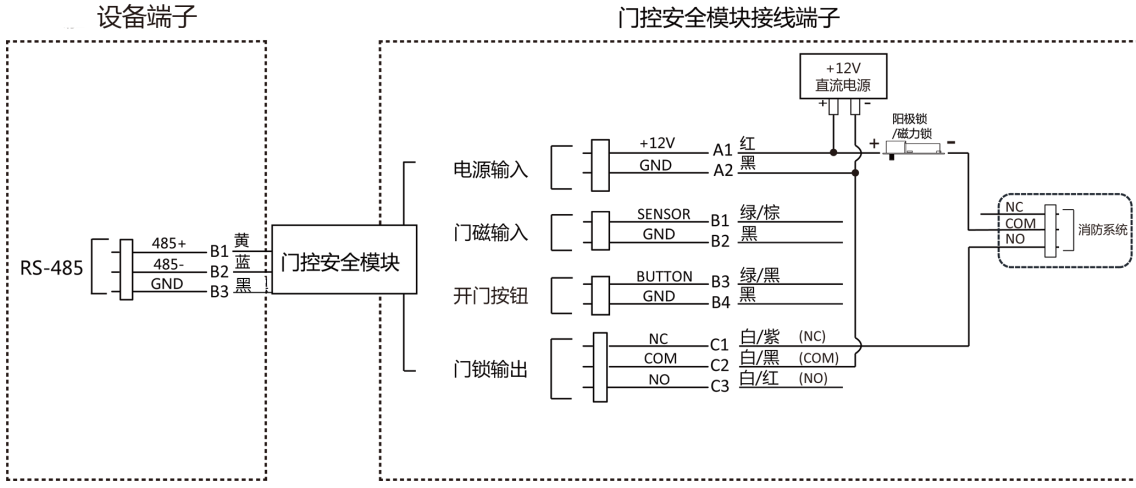


图 4-6 外接门控安全模块示意图

4.4.2 断电上锁型接线说明

锁类型：阴极锁、电锁口、常闭型电插锁

安全类型：断电上锁型

用途：非消防通道但有消防联动需求的出入口

说明

- 此接线方式需要配置 UPS 不间断电源。
- 消防系统串联在门锁和电源回路中，接入消防系统的断电常闭端口（NC、COM）。消防事件触发时为默认开门状态，非触发时 NC、COM 为断开状态。

接线说明如下图所示：

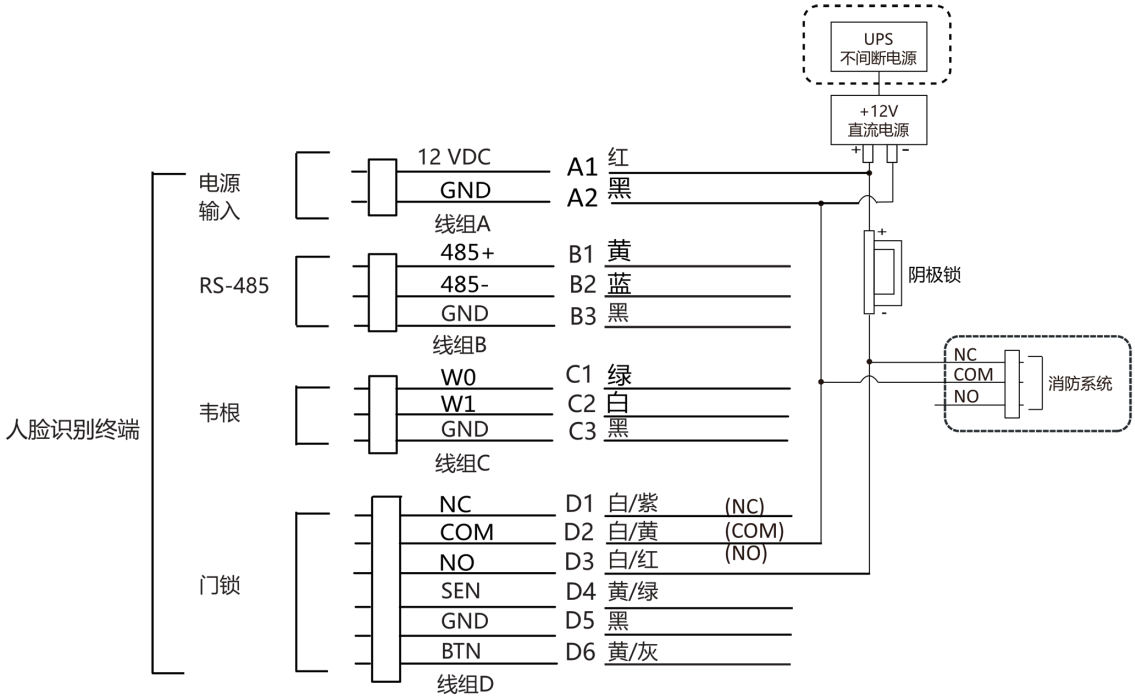


图 4-7 外接设备示意图

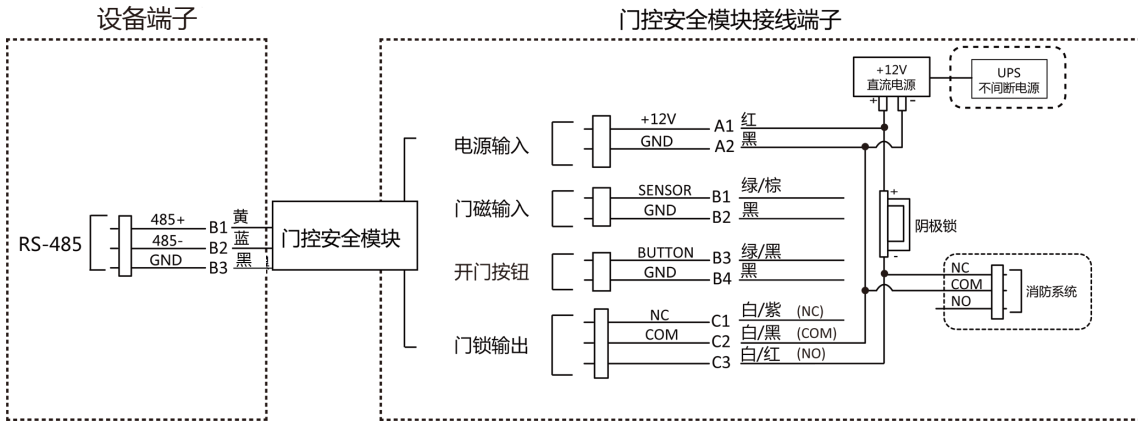


图 4-8 外接门控安全模块示意图

第 5 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：80、443。
- 缺省用户名（管理员）：admin。

5.1 通过设备本地激活

若设备在使用前未经过激活，则上电后会自动转入激活界面。

操作步骤

1. 点击输入密码编辑框，在界面软键盘上创建一个密码。
2. 点击确认密码编辑框，重复刚才输入的密码。
3. 点击 *下一步*进行激活。

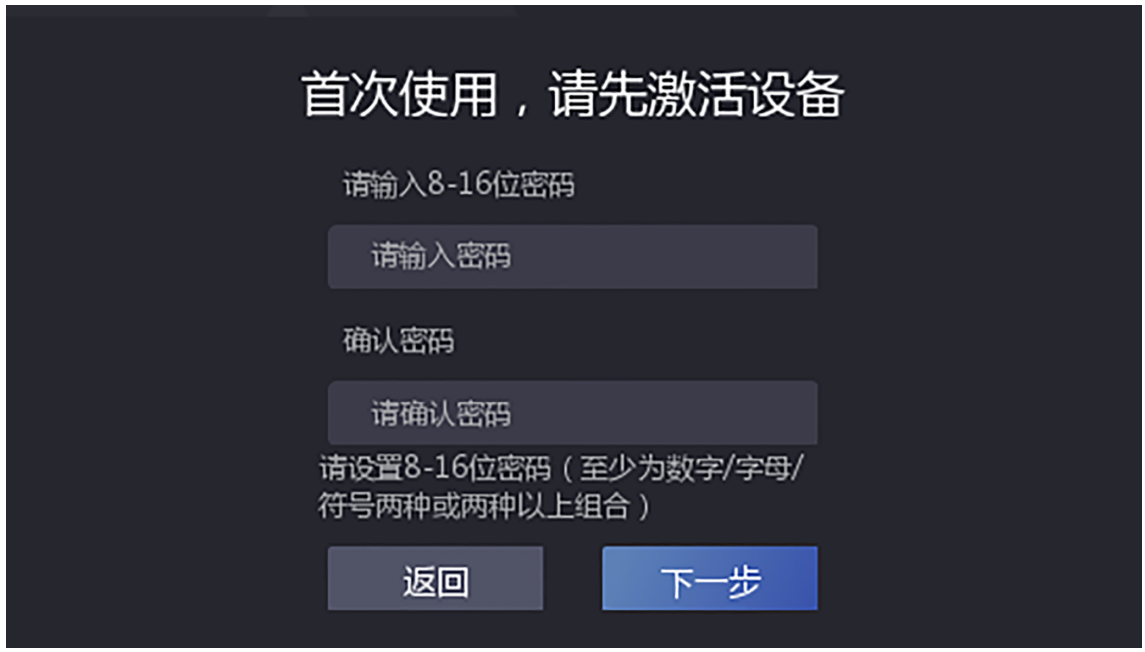


图 5-1 本地激活界面

说明

激活密码不支持包含 admin 和 nimda 字符。

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。

5.2 通过网页端激活设备

可通过设备网页端对未激活设备进行激活操作。

在网页端输入设备初始 IP 地址（192.0.0.64），并在弹出的窗口创建密码。确认密码后，可激活设备。

说明

- 请确保设备 IP 与电脑 IP 处于同一网段中。
- 激活密码不支持包含 admin 和 nimda 字符。

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。

图 5-2 激活页面

可通过 SADP 工具、设备本地、客户端软件修改设备 IP 地址、网关等信息。

5.3 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。
- 激活密码不支持包含 admin 和 nimda 字符。

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 5-3 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。

5.4 通过 iVMS-4200 客户端软件激活设备

通过 iVMS-4200 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。
- 激活密码不支持包含 admin 和 nimda 字符。

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 6 章 快速设置

6.1 选择使用环境

激活设备后，需要选择使用环境，方可正常使用设备。

图 6-1 选择使用环境

在下拉框中选择使用环境，并点击 *下一步*。

说明

- 在室内靠窗的场景、或使用体验不好的情况下，可选择*其他*。
- 若不配置此项，直接点击 *下一步*，设备默认使用**室内**作为环境模式。
- 若设备通过其他工具远程激活，系统将选择默认值（室内）作为使用环境，无需手动配置。

6.2 配置网络

激活设备后并选择使用环境后，需要配置网络，方可正常使用设备。

图 6-2 配置网络

说明

请确保设备已连接有线网络。

若开启 *DHCP*，系统自动分配 IP 地址等网络参数。

若不开启，需手动配置 IP 地址、子网掩码和网关。

点击 *下一步*。

或点击*上一步*返回使用环境选择页面。

6.3 启用云服务

可将设备接入云服务，通过移动客户端对设备进行操作。可根据需要进行选择。

操作步骤

1. 滑动启用 *云服务*，配置服务器地址，并输入操作码。

图 6-3 启用云服务

2. 点击 *下一步*完成配置。

说明

点击*上一步*可返回 Wi-Fi 配置界面，点击已连接的 Wi-Fi 或连接其它 Wi-Fi 后，可再次进入云服务配置界面。

6.4 隐私配置

激活设备后并选择使用环境、配置网络后，需配置隐私参数，包括图片上传及存储等相关信息。

根据需要进行选择。

图 6-4 隐私

上传识别抓拍图片

认证时抓拍的图片将上传到平台。

保存识别抓拍图片

认证时抓拍的图片将保存到设备。

保存注册图片

人员添加时的注册图片将保存到设备。

上传联动抓拍图片

联动抓拍到的图片将上传到平台。

保存联动抓拍图片

联动抓拍到的图片将保存到设备。

点击 *下一步*完成配置。

6.5 配置管理员

激活设备后，可以添加管理员，用来管理设备后台参数。

前提条件

激活设备、选择使用环境、选择网络并绑定 APP。

操作步骤

1. 在添加管理员页面输入管理员姓名，并点击 *下一步*。

图 6-5 添加管理员

2. 选择需要添加的凭证。

- ：将脸对准设备摄像头，确保人脸在设备界面的人脸标识内，并进行人脸识别。点击 进行录入。录入成功后，点击 确认录入。
- ：根据界面提示在设备端指纹采集区域按压指纹，点击 完成录入。
- ：在输入框内输入卡号，或在设备刷卡区域刷卡获取卡号。点击*完成*。

3. 点击*完成*，进入设备认证界面。

状态栏图标说明

/

设备已布防/未布防。

/

萤石云已开启/未开启。

/ /

Wi-Fi 已连接/未连接/IP 冲突。

/ /

网络已连接/未连接/连接错误。

认证界面图标说明

说明

可自定义控制是否显示认证界面按钮。详细配置方式, 请参见 ***基础设置*** 中的主界面快捷方式。

- 输入房间号并点击 *OK* 进行呼叫。
- 点击 呼叫管理中心。

说明

需将设备添加到管理中心后，方可进行呼叫。

可输入密码进行认证。

第 7 章 设备本地操作

7.1 登录

若需要配置后台参数，需先登录后台。根据实际情况选择登录方式：若未配置管理员，需输入设备激活密码登录；若设备已设置管理员，可通过管理员人脸或卡片认证登录后台。

7.1.1 激活密码登录

若需要配置后台参数，需先登录后台。若激活后未配置管理员，需输入激活密码登录。

操作步骤

1. 在认证界面，用手指长按主显示屏非按键区域 3 s，根据界面上方手势，向左或向右滑动进入后台管理窗口。
2. 输入密码。
   - 如果已添加管理员，单击 输入密码或根据当前认证方式进行人脸直接管理员认证。
   - 如未添加管理员，直接输入密码。
3. 点击*确定*进入后台主菜单界面。

图 7-1 主菜单页面

说明

- 若连续输入 5 次错误密码，设备将被锁定 30 分钟。
- 登录后台后，默认 1 分钟内未进行任何操作，设备自动退出后台，返回认证界面。菜单超时退出时间可配置。

7.1.2 管理员登录

若需要配置后台参数，需先登录后台。若设备设置了管理员，且管理员添加了人脸和卡片，可通过认证人脸或者刷卡登录后台。

前提条件

添加管理员，并为管理员添加人脸卡片。具体添加方式，请参见 *添加管理员用户* 。

操作步骤

1. 在认证界面，用手指长按主显示屏非按键区域 3 s，根据界面上方手势，向左或向右滑动进入管理员验证界面。

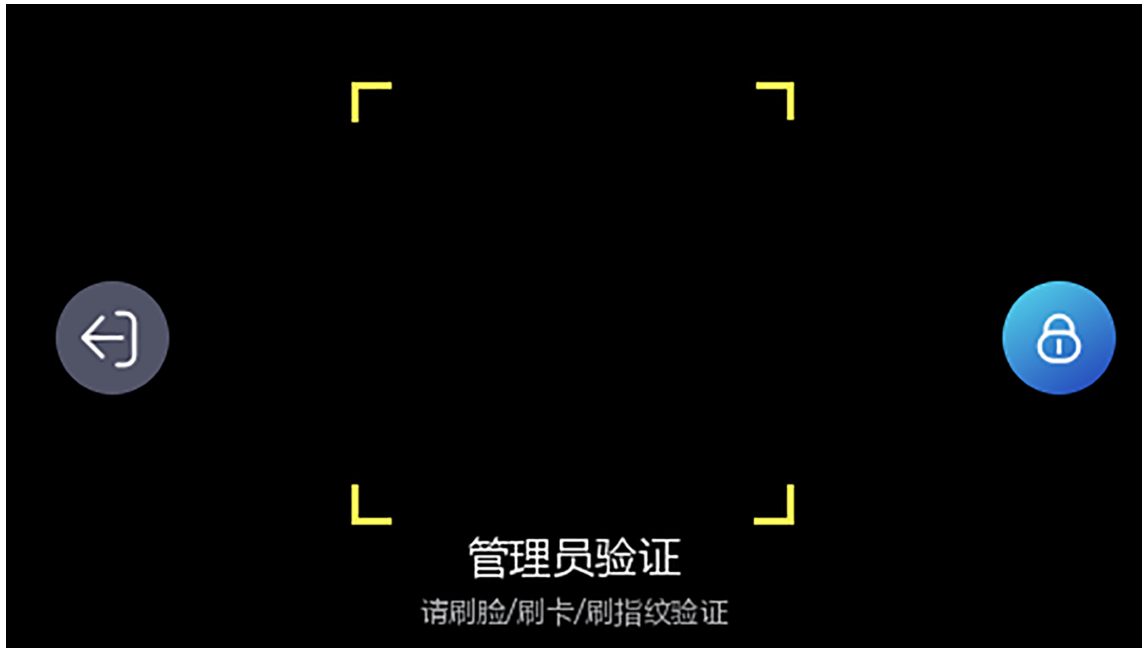


图 7-2 管理员验证界面

2. 验证管理员人脸、指纹或刷管理员卡片后，进入主菜单界面。

图 7-3 主菜单界面

说明

若连续验证 5 次错误，设备将被锁定 30 分钟。

3. **可选操作**: 点击 ，可输入设备激活密码进行登录。
4. **可选操作**: 点击 ，可退出管理员验证页面。

说明

登录后台后，大约若 1 分钟未进行任何操作，设备自动退出后台，返回认证界面。

7.2 通讯设置

配置设备网络参数、Wi-Fi 参数、RS-485 参数、韦根参数及 ISUP 参数。

7.2.1 网络设置

配置设备的网络参数，包括 IP 地址、子网掩码、网关地址和 DNS。配置完成后，设备可与客户端软件、平台等进行通讯。

操作步骤

1. 在主菜单界面中点击*通讯设置*进入通讯设置界面。
2. 点击*有线网络*进入网络设置界面。

图 7-4 有线网络设置页面

3. 配置**网络参数**，包括 DHCP、网口 IP 地址、网关地址、子网掩码、DNS。

说明

- 设备 IP 地址与电脑 IP 地址需处于同一网段中。
- 启用 *DHCP* 后，系统自动给设备分配 IP 地址、网关和子网掩码。
- 若不启用 *DNS 自动获取*功能，需配置首选 DNS 服务器和备用 DNS 服务器。若启用 *DNS 自动获取*，系统自动分配 DNS 服务器。

7.2.2 设置 Wi-Fi 参数

在 **Wi-Fi** 界面中选择是否开启 Wi-Fi，并配置相应的 Wi-Fi 参数。

操作步骤

说明

部分设备型号支持 Wi-Fi 功能。

1. 在菜单界面中点击 *通讯设置* → *Wi-Fi* 进入 Wi-Fi 配置界面。

图 7-5 Wi-Fi 配置

2. 点击滑块，开启 Wi-Fi。

3. 配置 Wi-Fi 参数。

- 选择列表中已有的 Wi-Fi，并输入 Wi-Fi 密码。点击***确定***进行连接。
- 若列表中无 Wi-Fi，可点击***添加 Wi-Fi***，并输入 Wi-Fi 名称和密码，点击***确定***进行连接。

说明

密码支持数字、大小写字母和符号。

4. **可选操作**: 点击已连接的 Wi-Fi，配置详细参数。

- 默认设备开启 *DHCP*，系统自动分配 IP 地址、子网掩码和网关地址。
- 若不启用 DHCP，则需设置 IP 地址、子网掩码和网关地址。

7.2.3 设置 RS-485 参数

人脸识别终端设备可通过 RS-485 接口外接门禁主机、门控安全模块、读卡器或梯控。在此处设置 RS-485 参数，以便连接外接设备。

操作步骤

1. 在**通讯设置**界面中点击 *RS-485* 进入 **RS-485** 界面。

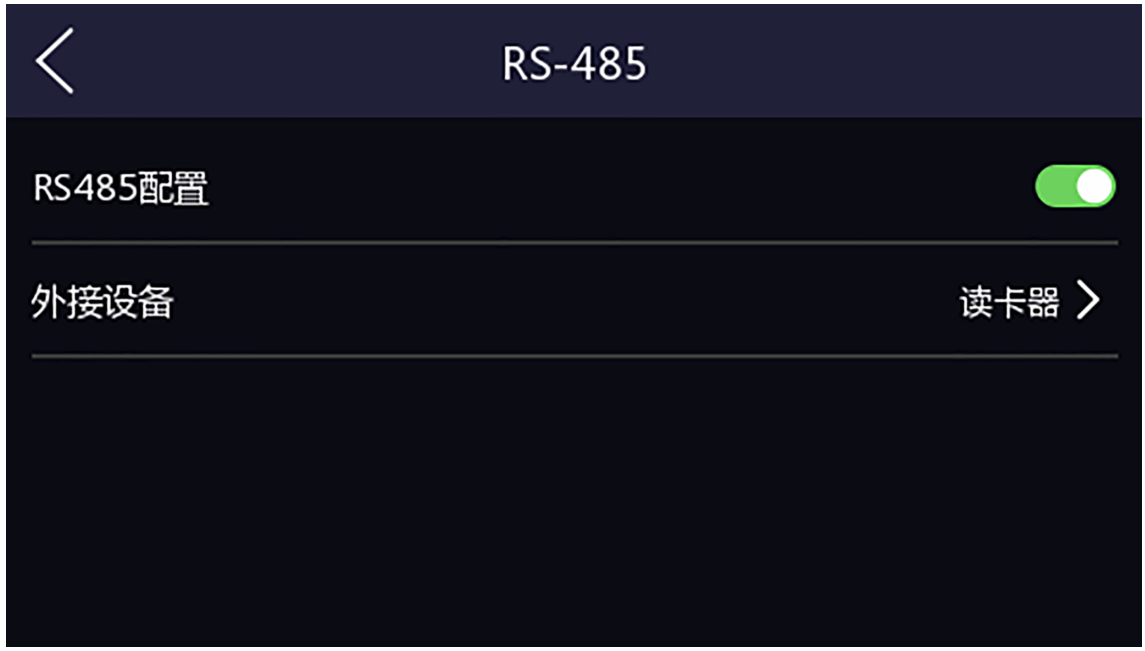


图 7-6 RS-485 设置界面

2. 根据实际外接设备连接情况选择一个外接设备。可选择*门禁主机*、*门控模块*、*读卡器*或者*梯控模块*。

说明

当外接设备选择*门禁主机*时，若外接设备为一体机，需设置外接设备对应的本机 RS-485 地址为 2；若外接设备为门禁主机，需要根据对应的门编号配置 RS-485 地址。

3. 点击左上角后退按钮，系统提示需重启后参数方可生效，点击*确认*，系统开始重启。

7.2.4 设置韦根参数

在此处可设置韦根参数。

操作步骤

1. 在**通讯设置**界面中点击*韦根*进入**韦根**界面。

图 7-7 韦根设置界面

2. 移动滑块选择是否开启韦根功能。

3. 选择韦根传输方向。

- 输出：人脸识别终端可外接门禁主机，通过 Wiegand 26、34、27 或 35 模式传输卡号。

7.2.5 设置 ISUP 参数

设置 ISUP 参数后，设备可通过 ISUP 协议上传数据到中心组。

前提条件

确保设备已连接网络。

操作步骤

1. 点击 ***通讯设置*** → ***ISUP***，进入 ISUP 界面。

图 7-8 ISUP 设置

2. 点击启用 ISUP 功能，并设置 ISUP 参数。

协议版本

根据实际 ISUP 协议选择协议类型。如果选择 ISUP5.0，您需要创建一个协议账户和密钥。如果选择其他版本，您只需要创建账户即可。

说明

- 请妥善保管 ISUP 账户和密钥。在设备通过 ISUP 协议与其他平台通信时，您需要输入账户名和密钥完成通信。
- 密钥范围：8~16 个字符。

中心组

启用中心组后，数据将通过 ISUP 协议上传至中心组。

主通道

支持配置主通道为 N1 或无。

说明

N1 代表有线网络通讯。

ISUP

启用后，设备将通过 ISUP 协议传输数据。

地址类型

启用 ISUP 后，根据实际情况选择一个地址类型。

说明

可选择 IP 地址或域名。

IP 地址/域名

设置 ISUP 服务器的 IP 地址或域名。

端口号

设置 ISUP 服务器的端口号。

说明

端口号范围：1~65535 内的数值。

设备 ID

设置设备的编号。

7.2.6 云服务配置

设备接入云服务平台，可通过移动客户端对设备进行操作。

操作步骤

1. 点击 *通讯设置 → 云服务* 。

图 7-9 云服务配置

2. 滑动启用*云服务*，配置服务器地址，并输入操作码。
3. 点击*保存*完成配置。

7.3 用户管理

在用户管理菜单中，您可以新增、编辑、删除、查找用户。

7.3.1 添加管理员用户

操作步骤
1. 在设备菜单界面点击 *用户管理* → + 进入添加用户界面。

图 7-10 添加用户界面

2. 点击*工号*，可编辑用户的工号。

说明

工号不能超过 32 个字符，可以为大小写字母和数字的组合，不能为 0。

3. 点击*姓名*，并输入新增的姓名。您可在弹出的软键盘上输入用户姓名。

说明

- 姓名支持数字、中文、大小写英文和字符。
- 输入的姓名建议在 32 个字符以内。

4. 根据需要配置管理员人脸、卡片或指纹。

说明

请根据 *添加用户人脸*、 *添加用户卡片*、 *添加用户指纹* 来添加人脸、卡片或指纹。

5. 配置管理员认证模式。请根据 *自定义权限认证方式* 进行配置。

6. 选择用户类型为 *管理员*。

7. 点击 保存设置。

7.3.2 添加用户人脸

操作步骤

说明

最多可添加 500 张人脸。

1. 在设备菜单界面点击 *用户管理* → + 进入添加用户界面。

图 7-11 添加用户界面

2. 点击*工号*，可编辑新增用户的工号。

说明

工号不能超过 32 个字符，可以为大小写字母和数字的组合。

3. 点击*姓名*，并输入新增的姓名。您可在弹出的软键盘上输入用户姓名。

说明

- 姓名支持数字、中文、大小写英文和字符。
- 输入的姓名建议在 32 个字符以内。

4. 点击*人脸*进入人脸录入界面。

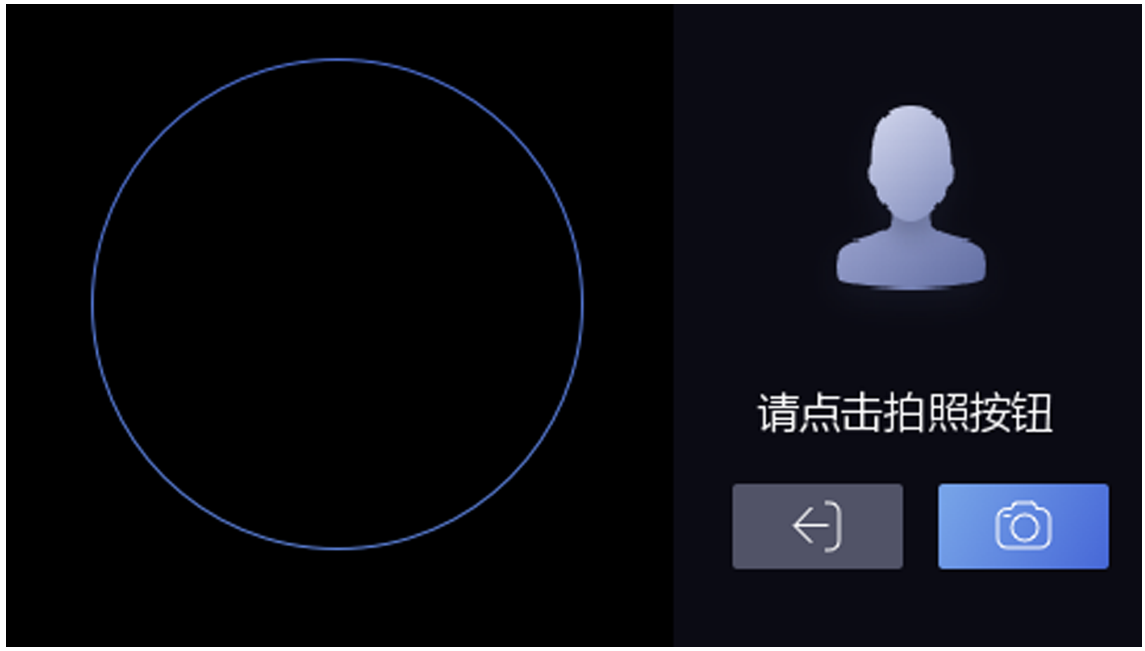


图 7-12 人脸录入界面

5. 将脸对准设备摄像头，确保人脸在界面的人脸标识内，点击 ，并点击 确认录入。

6. 点击 保存设置。

7.3.3 添加用户指纹

操作步骤

说明

- 最多可添加 500 枚指纹。
- 仅部分型号支持该功能。

1. 在设备菜单界面点击 *用户管理* → + 进入添加用户界面。

图 7-13 添加用户界面

2. 点击*工号*，可编辑新增用户的工号。

说明

工号不能超过 32 个字符，可以为大小写字母和数字的组合，不能为 0。

3. 点击*姓名*，并输入新增的姓名。您可在弹出的软键盘上输入用户姓名。

说明

- 姓名支持数字、中文、大小写英文和字符。
- 输入的姓名建议在 32 个字符以内。

4. 点击*指纹*，进入指纹录入界面。

5. 将需要录入指纹的手指放置在指纹扫描区域上。

6. 根据界面提示抬起并放置手指，至指纹录入完成。

说明

- 相同指纹不可重复录入。
- 一个工号最多可添加 10 个指纹。
- 指纹也可以用客户端或指纹录入仪采集，再下发到设备中。
- 关于录入指纹的具体注意事项，参考 *指纹识别注意事项* 。

7. 点击 保存设置。

7.3.4 添加用户卡片

操作步骤

说明

最多可添加 1000 张卡片。每人最多可添加 5 张卡片。

1. 在用户列表界面点击+按钮进入“添加用户”界面。

图 7-14 添加用户界面

2. 点击*工号*，可编辑新增用户的工号。

说明

工号不能超过 32 个字符，可以为大小写字母和数字的组合，不能为 0。

3. 点击*姓名*，并输入新增的姓名。您可在弹出的软键盘上输入用户姓名。

说明

- 姓名支持数字、中文、大小写英文和字符。
- 输入的姓名建议在 32 个字符以内。

4. 点击*卡号*并添加卡片信息。

1) 点击+并输入卡号或在设备的刷卡位置刷卡读取卡号。

说明

- 卡号不能为空。
- 卡号最长可输入 20 位。
- 卡号不能重复。

2) 根据实际需要选择卡片类型。

3) 点击 保存设置。

7.3.5 查看密码

操作步骤

1. 在设备菜单界面点击 *用户管理* → + 进入添加用户界面。

图 7-15 添加用户界面

2. 点击*工号*，可编辑新增用户的工号。

说明

工号不能超过 32 个字符，可以为大小写字母和数字的组合。

3. 点击*姓名*，并输入新增的姓名。您可在弹出的软键盘上输入用户姓名。

说明

- 姓名支持数字、中文、大小写英文和字符。
- 输入的姓名建议在 32 个字符以内。

4. 点击*密码*，进行查看。

说明

密码不可配置，仅支持通过平台下发。

5. 点击 保存设置。

7.3.6 自定义权限认证方式

操作步骤

1. 在设备菜单界面点击 *用户管理* → + 进入添加用户界面。

2. 单击*认证模式*。

3. 选择认证方式。

认证模式	说明
设备模式	需要在门禁设置模块中设置设备认证方式。详见 *门禁设置* 。该人员在验身份时，需使用配置的设备认证方式进行认证。此模式便于批量修改人员已认证方式。
自定义模式	自定义组合认证方式。该人员在设备端认证身份时，优先使用该自定义认证模式进行身份认证。此模式便于配置单个需要有特殊权限的人员。

4. 点击 保存设置。

7.3.7 编辑/查询用户

查询用户

在*用户列表*界面，点击搜索栏进入搜索页面，可通过工号、卡号或者姓名搜索列表中的用户。

编辑用户

在*用户列表*界面，点击需要编辑的用户，对已添加的用户信息做修改。

说明

工号不能编辑。

7.4 数据管理

在数据管理模块中导入数据、导出数据和删除数据。

7.4.1 删除数据

在*数据管理*模块中可删除用户数据。

在主菜单界面中点击*数据管理*，根据需求选择以下功能。

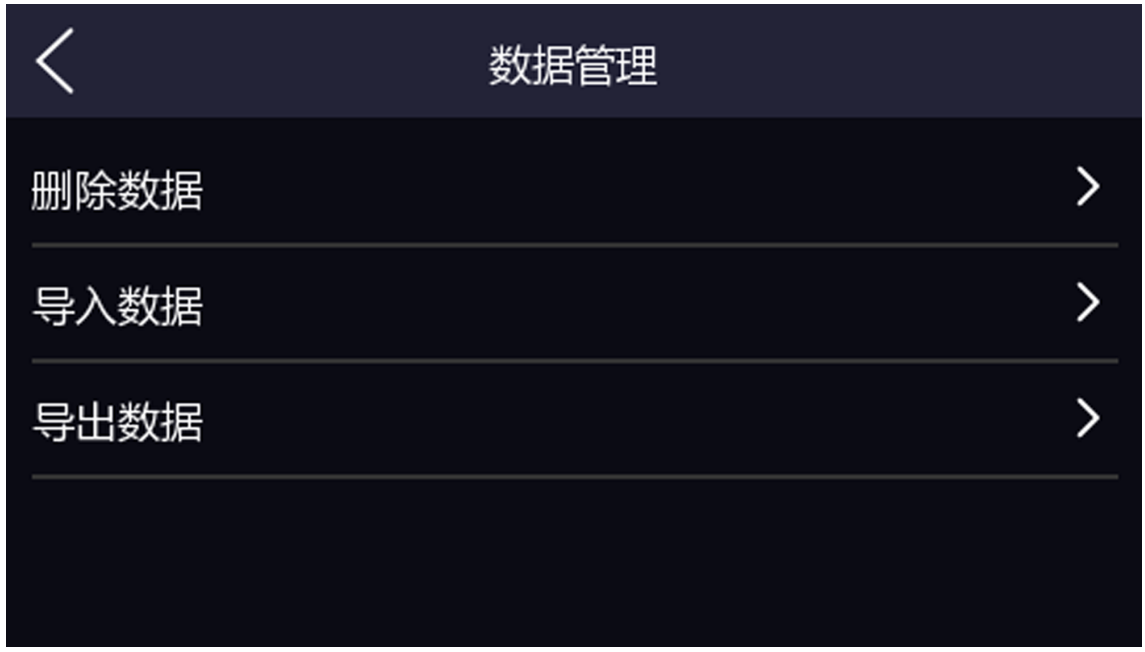


图 7-16 数据管理

用户数据

删除系统中所有的用户数据。

7.4.2 导入数据

操作步骤

1. 在设备的 USB 接口处插入 U 盘。

2. 在主菜单界面点击*数据管理*，进入数据管理页面。

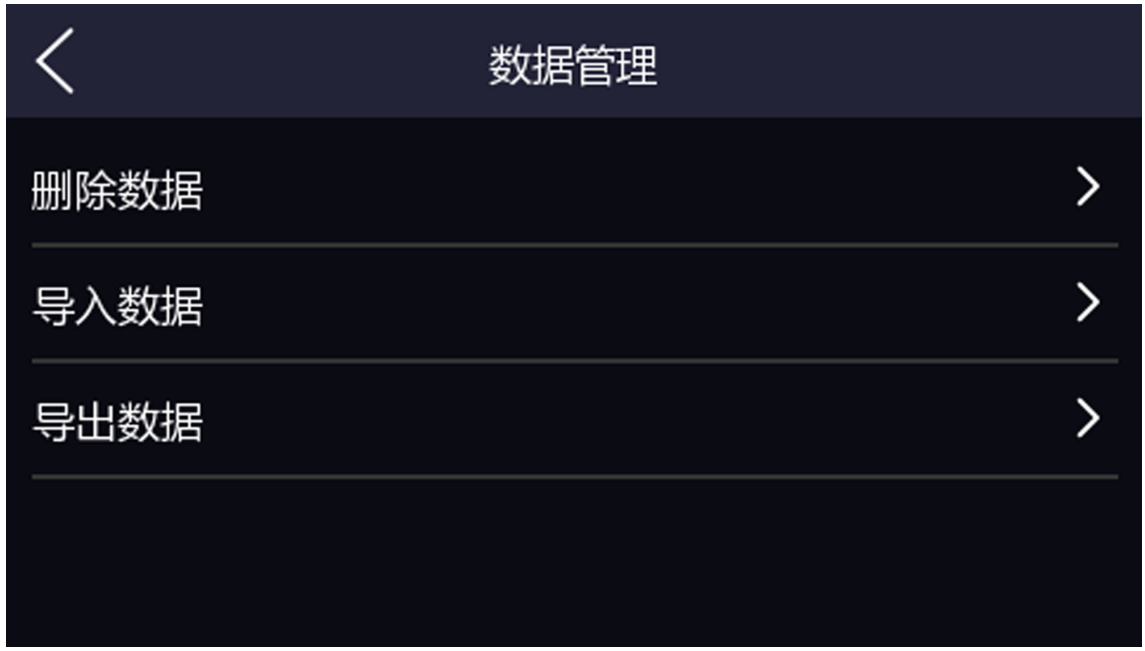


图 7-17 数据管理页面

3. 在数据管理页面点击*导入数据*。

4. 选择*用户数据*、*人脸数据*或*门禁参数*。

说明

导入的门禁参数为设备的配置文件。

5. 输入数据导出时创建的密码，若未配置密码，置空并点击*确认*。数据将从 U 盘中导入到设备中。

说明

- 若需要将设备 A 中所有的用户信息导入到设备 B 中，需先将设备 A 中的用户数据导入到 U 盘，再通过 U 盘将用户数据导入到设备 B 中。
- 支持的 U 盘格式为 FAT32 或 exFat。
- 若需手动导入图片，则图片需保存在 U 盘根目录 enroll_pic 中。图片名称须符合命名规则：卡号_姓名_部门_工号_性别.jpg。工号不能超过 32 个字符，可以为大小写字母和数字的组合，不能为 0。
- 若手动导入的图片较多，enroll_pic 无法存下所有图片时，可在根目录下另外创建 enroll_pic1、enroll_pic2、enroll_pic3、enroll_pic4 文件夹存储图片。图片名称需符合图片命名规则。
- 人脸照片要求：脸正面免冠照，jpeg 或 jpg 格式，图片像素需为 640 × 480 像素或以上，图片大小需为 60 KB ~ 200 KB。

7.4.3 导出数据

操作步骤

1. 在设备的 USB 接口处插入 U 盘。

2. 在主菜单界面点击*数据管理*，进入*数据管理*界面。

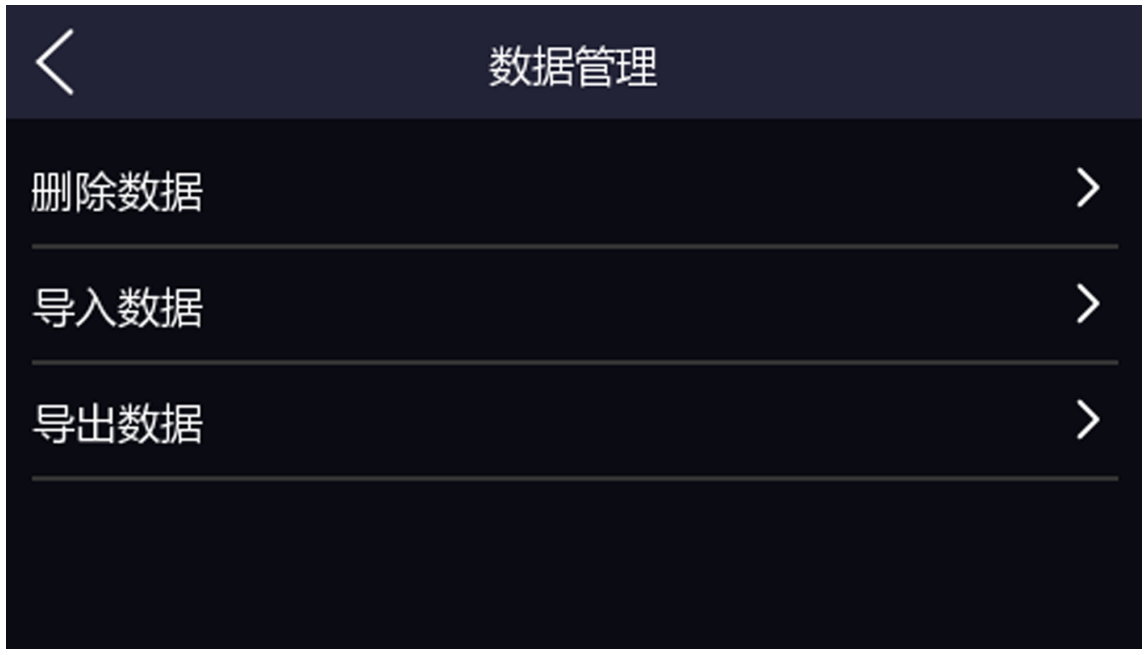


图 7-18 数据管理页面

3. 在数据管理页面点击*导出数据*。

4. 选择*事件数据*、*用户数据*、*人脸数据*或*门禁参数*。

说明

导出的门禁参数为设备的配置文件。

5. 创建导出数据时的密码，若将此数据导入到其他设备中，需输入相同的密码方可导出成功。

说明

- 创建的导出密码可为空。
- 支持的 U 盘格式为 FAT32 或 exFAT。
- USB 支持 1 G ~ 32 G 的 U 盘。请确保 U 盘剩余空间在 512 M 以上。
- 导出的数据为 DB 格式的加密文件，不可编辑。

身份验证

在后台配置完网络、系统参数以及人员后，可返回认证界面，进行人员身份验证的操作。

在认证之前，您需对设备认证方式进行配置，详见 *自定义权限认证方式* 。

根据系统设置中的配置的认证方式可进行比对验证。

注意

生物识别产品无法 100%适用于任何防伪环境。高安全级别场所，请使用组合认证方式。

单凭证认证

在进行认证之前，需配置用户的验证方式，具体配置方式，请参见 *自定义权限认证方式* 。

若配置的认证方式为人脸，将人脸对准摄像头，进行人脸认证。

若配置的认证方式为指纹，在指纹识别区域进行指纹认证。

若配置的认证方式为卡片，在刷卡区域刷卡，进行卡片认证。

若配置的认证方式为纯密码，可输入人员密码进行认证。

认证成功时，设备显示“认证成功”。人员可通过设备。

组合认证

若配置的认证方式为组合认证，可根据选择组合方式进行认证。

前提条件

在进行组合认证之前，需配置用户的验证方式，具体配置方式，请参见 *自定义权限认证方式* 。

操作步骤

1. 根据配置的组合方式对其中一种凭证进行认证。

   认证成功后，将看到“请继续认证”的提示。

2. 第一种凭证认证成功后，根据提示认证第二种凭证。

   认证成功后，将看到“请继续认证”的提示。

3. **可选操作**: 如配置了三种凭证的组合认证，根据提示认证第三种凭证。

说明

- 具体指纹识别注意事项，*参考指纹识别注意事项*。
- 人脸认证时，为确保设备正常识别人脸，认证人员的身高需在 140 ~ 190 cm 之内，且验证人员距离设备的距离需在 30 ~ 100 cm 之内。
- 具体人脸识别注意事项，*参考人脸识别注意事项*。

结果说明

认证成功后，设备显示屏上将显示“认证成功”。人员可通过设备。

7.5 基础设置

可配置设备认证界面快捷方式、主题、声音、时间、期号、楼号和单元号。

登录后台，点击 ***基础设置***，可配置相应参数。

图 7-19 基础设置页面

认证界面快捷方式

可配置显示在认证界面的快捷功能，包括呼叫功能和密码功能。

主题

可选择设备的默认主题或简洁主题。

可配置设备认证时的提示界面主题。可选择*默认主题*或*简洁主题*。若选择*简洁主题*，认证界面预览关闭，认证时不显示认证人员的姓名、工号、人脸图片等信息。

声音设置

可启用设备的语音提示，并设置语音音量。

语音提示

开启后，设备会进行语音提示。

语音音量

可调节语音音量。

说明

可配置的语音范围为 0~10。数字越大，音量越大，反之，音量越小。

时间设置

可配置设备所在时区，还可设置设备当前时间。

期号

设置设备所处的期号。

楼号

设置设备所处的楼层号。

单元号

设置设备所处的单元号。

7.6 生物识别参数设置

通过自定义配置设备生物识别时的参数，让设备识别人脸等生物信息时达到更好的效果。可配置的参数包括环境模式、真人检测安全等级、识别距离、连续识别间隔、人脸 1:N 比对阈值、人脸 1:1 比对阈值、环保设置和面部口罩检测设置。

长按待机界面 3 s，并根据手势提示向左或向右滑动，登录后台，在后台管理页面点击*生物识别*进入生物识别界面，并配置生物识别参数。

图 7-20 生物识别参数界面

各参数含义如下所示：

环境模式

根据实际情况选择室内或者其他。

真人检测安全等级

开启真人检测功能后的人脸匹配安全等级。可从普通、高、极高三个等级中选择。等级越高，误识率越低，拒认率越高。

识别距离

配置可有效识别人脸的人员与设备镜头的距离。

连续识别间隔

认证过程中，前后两次人脸识别的间隔时间。

说明

需填写 1~10 之间的数字。

人脸 1:N 比对阈值

人脸 1:N 匹配时的匹配阀值。阈值越大，识别人脸时误识率越低，拒认率越高。最大可填 100。

人脸 1:1 比对阈值

人脸 1:1 匹配时的匹配阀值。阈值越大，识别人脸时误识率越低，拒认率越高。最大可填 100。

环保设置

启用环保模式后，在弱光或无光环境下，设备启用红外摄像头进行人脸比对。可配置环保切换阈值、环保模式 1:N 阈值、环保模式 1:1 阈值、环保模式口罩人脸 1:1 阈值及环保模式口罩人脸 1:N 阈值。

环保切换阈值

启用环保模式后，需配置环保切换阈值，阈值越大，设备越容易进入环保模式；阈值越小，越不容易进入环保模式。阈值与光照强度有关。阈值范围为：0 ~ 7。

环保模式 1:N 阈值

通过红外摄像头进行人脸 1:N 匹配时的匹配阀值。阈值越大，识别人脸时误识率越低，拒认率越高。最大可填 100。

环保模式 1:1 阈值

通过红外摄像头进行人脸 1:1 匹配时的匹配阀值。阈值越大，识别人脸时误识率越低，拒认率越高。最大可填 100。

环保模式口罩人脸 1:1 阈值

进行环保模式下戴口罩人脸 1:1 匹配时的阈值。阈值越大，识别人脸时的误识率越低，拒认率越高。最大可填 100。

环保模式口罩人脸 1:N 阈值

进行环保模式下戴口罩人脸 1:N 匹配时的阈值。阈值越大，识别人脸时的误识率越低，拒认率越高。最大可填 100。

面部口罩检测设置

启用面部口罩检测功能后，可配置*未带口罩策略*、*口罩人脸 1:1 阈值*和*口罩人脸 1:N 阈值*。

未带口罩策略

可配置*无提示*、*提醒戴口罩*和*必须戴口罩*。

无提示

认证人员若未佩戴口罩，设备不提示口罩相关信息。

提醒戴口罩

认证人员若未佩戴口罩，设备提示戴口罩，且开门。

必须戴口罩

认证人员若未佩戴口罩，设备提示戴口罩，且不开门。

口罩人脸 1:1 阈值

戴口罩人脸 1:1 匹配时的匹配阀值。阈值越大，识别戴口罩人脸的误识率越低，拒认率越高。最大可填 100。

口罩人脸 1:N 阈值

戴口罩人脸 1:N 匹配时的匹配阀值。阈值越大，识别戴口罩人脸的误识率越低，拒认率越高。最大可填 100。

7.7 门禁设置

可设置门禁权限，包括主机认证设置、副读卡器认证设置、启用 NFC 卡、启用 M1 卡、直通模式、门磁状态、门锁动作时间和重复认证间隔。

在主菜单界面点击*门禁设置*进入“门禁设置”界面，修改门禁参数后，保存配置。

图 7-21 门禁参数设置

门禁参数项说明如下表所示：

主机认证方式

设置设备认证的认证类型和认证方式。您可选择不同的组合方式进行认证方式的选择。

说明

部分设备型号不支持指纹相关认证。

注意

生物识别产品无法 100%适用于任何防伪环境。高安全级别场所，请使用组合认证方式。

副读卡器认证方式

可配置副读卡器认证方式，认证类型同主机类型相同。

启用 NFC 卡

开启后，设备可识别 NFC 卡。

启用 M1 卡

开启后，设备可识别 M1 卡。

直通模式

开启后，对于持普通卡片用户，设备不验证计划模板，即可通过。对于持身份证用户，设备不判断身份证权限，仅判断认证 方式、身份证有效期，即可通过。

门磁状态

可选择门磁状态常开或者常闭。默认为常闭。

门锁动作时间

设置门开锁后的动作时间。若在设置时间内不开门，门将自动锁住。可设置范围 1~255 秒。

重复认证间隔

认证过程中，同一人员前后 2 次通过任意凭证识别的间隔时间。在配置的时间段内，同一个人员只能进行一次认证。可设置范围重复认证间隔 0~65535 秒。

7.8 系统维护

可查看设备系统信息和容量信息，还可升级、绑定 APP 账户、恢复出厂设置、恢复默认设置和重启设备。

在认证界面，用手指长按主显示屏非按键区域 3 s，根据界面上方手势，向左或向右滑动，通过管理员验证后，在后台管理页面点击*系统维护*。

图 7-22 系统维护

系统信息

可查看设备型号、序列号、固件版本、MCU 版本、MAC 地址、出厂信息、二维码信息和开源代码许可。

说明

不同型号的此界面可能会有差别，请以实际界面为准。

设备容量

可查看已录入用户数量、人脸数量、事件数量和指纹数量。

设备升级

U 盘插入 USB 接口，点击界面中的 ***设备升级 → 确认***，设备将会读取 U 盘中的 digicap.dav 的升级文件进行系统升级。

萤石解绑

若设备已绑定萤石云账户，如需解绑，可在此设置将设备从萤石云 APP 中解绑。

恢复出厂设置

进行恢复出厂设置操作后，设备将自动重启。

恢复默认设置

系统将保留通讯配置、远程管理用户配置，其他参数将恢复为默认参数。进行恢复默认设置操作后，设备将自动重启。

重启

重启设备。

长按右上角 ，输入管理员密码后可查看设备版本信息。

7.9 呼叫

将设备添加到客户端后，可通过客户端呼叫设备、可通过设备呼叫客户端、可通过设备呼叫管理机、也可通过设备呼叫室内机。

7.9.1 设备呼叫客户端

前提条件

安装从官网下载的客户端软件，并运行客户端软件。

操作步骤

1. 运行客户端后，在主界面单击 ***设备管理 → 设备 → 添加*** 。
2. 添加设备至客户端。具体添加方式请参见 ***添加设备*** 。
3. 在设备端的认证界面，点击  ，并在弹出的界面中点击  （管理中心）。
4. 在客户端界面弹出的来电窗口中点击***接听***，可与设备端进行语音通话。

说明

若设备被多个客户端添加，设备呼叫客户端时，仅首个添加设备的客户端会弹出来电窗口。

7.9.2 设备呼叫管理中心

前提条件

安装从官网下载的客户端软件，并运行客户端软件。

操作步骤

1. 运行客户端后，在主界面单击 *设备管理 → 设备 → 添加* 。
2. 添加设备至客户端。具体添加方式请参见 *添加设备* 。
3. 在*远程配置*界面配置管理机 IP 和 SIP 地址。

说明

有关如何配置管理机 IP 和 SIP 地址，请参见管理机用户手册。

4. 呼叫管理中心。
   - 若在 *基础设置* 中配置呼叫管理机，点击 可直接呼叫管理中心。
   - 若未在基础设置中配置呼叫管理中心或指定房间，在设备端的认证界面，点击 ，并在弹出的界面中点击 （管理中心）。
5. 管理中心接听后，即可进行语音通话。

说明

呼叫管理中心时，设备优先呼叫管理机。

7.9.3 客户端呼叫设备

前提条件

安装从官网下载的客户端软件，并运行客户端软件。

操作步骤

1. 运行客户端后，在主界面单击 *设备管理 → 设备 → 添加* 。
2. 添加设备至客户端。具体添加方式请参见 *添加设备* 。
3. 进入预览界面，并双击设备打开设备预览画面。具体设备预览功能。

说明

请确保门禁监控点已添加到分组。具体如何添加分组，详见 *分组管理* 。

4. 在预览画面右击鼠标打开右键菜单。
5. 选择*开始对讲*，即可开启客户端和设备的语音对讲功能。

7.9.4 设备呼叫室内机

通过本设备可呼叫房间内安装的室内机。

操作步骤

1. 在客户端中添加室内机和本设备，将用户与对应室内机进行绑定，并为室内机设置一个房间号。
2. 呼叫室内机。

- 若在 ***基础设置*** 中配置呼叫固定房间，点击 可直接呼叫固定房间。
- 在***设备认证***界面，点击 。在***拨号***界面输入房间号，并点击 开始呼叫对应房间的室内机。

3. 室内机确定通话后可设备进行通话。

7.9.5 设备呼叫海康云眸移动客户端

通过本设备可呼叫海康云眸移动客户端（业主）。

操作步骤

1. 在海康云眸移动客户端（物业）中添加本设备，并在海康云眸移动客户端（业主）中添加房屋信息。
2. 在***设备认证***界面，点击 。
3. 在***拨号***界面输入房间号，并点击 开始呼叫海康云眸移动客户端（业主）。
4. 在移动客户端弹出呼叫界面中点击***接听***即可与设备进行通话。

第 8 章 通过手机网页配置设备

8.1 登录

可通过手机登录 IP 进行远程配置。

说明

- 请确保设备已激活，具体激活配置，请参见 *通过设备本地激活* 。
- 开启设备 Wi-Fi，为设备配置一个 IP 地址，连接后需确保手机和设备在同一个 Wi-Fi 下，详见 *设置 Wi-Fi 参数* 。

在手机中

输入用户名和设备激活密码，点击*登录*。

8.2 事件查询

点击*事件查询*进入查询页面。

输入搜索条件，包括工号、姓名、卡号、搜索的开始时间和结束时间，并点击*查询*。

说明

支持搜索 32 位以内的姓名。

搜索结果将展示在列表中。

8.3 管理人员

在人员管理中，您可以添加、编辑、删除、查找人员。

操作步骤

1. 在主菜单中点击*人员管理*，进入配置界面。

2. 添加人员。

1) 点击右上角*+*。

图 8-1 添加人员

2) 输入**工号**、**姓名**、**层号**和**房间号**。

说明

- 工号不能超过 32 个字符，可以为大小写字母和数字的组合，不能为 0。
- 姓名支持数字、中文、大小写英文和字符，输入的姓名建议在 32 个字符以内。

3) 选择**性别**和**用户类型**。
4) 添加人脸。点击***导入***，选择所需上传方式上传人脸图片。
5) 添加指纹。点击指纹界面右上角+，在设备指纹录入区域录入指纹。
6) 设置该人员权限的**开始日期**和**结束日期**。
7) **可选操作**: 如需将该人员设置为设备管理员，可启用***设备管理员***。
8) 设置该人员的**认证类型**。

同设备

认证类型与设备配置的认证模式相同。该人员验证身份时，需使用设备验证方式进行验证。 添加人员时默认选择采用主机认证模式。此模式方便批量修改人员验证方式。

自定义

若该人员需要使用有别于设备验证模式的特殊验证方式，可选用自定义验证方式。该人员在设备端认证时优先使用该配置的验证方式进行身份证。此模式方便配置单个需要有特殊权限的人员。

9) 点击***保存***。

3. 可选操作: 编辑人员。可点击需要编辑的人员，对已添加的人员信息进行修改。
4. 可选操作: 删除人员。可点击需要删除的人员，点击右上角 删除人员。
5. 可选操作: 查询人员。在人员管理界面点击搜索栏进入搜索页面，可通过工号或姓名搜索列表中的人员。

8.4 配置

8.4.1 查看设备基本信息

查看设备名称、设备编号、设备型号、序列号、版本号、设备容量等信息。

点击 ***配置 → 系统 → 系统设置 → 基本信息***，进入配置页面。

可查看设备名称、设备编号、设备型号、序列号、版本号、设备容量等信息。

8.4.2 配置设备时间

配置本机所使用的时区、校时方式以及显示的时间。

点击 ***配置 → 系统 → 系统设置 → 时间配置***，进入配置页面。

图 8-2 时间配置

配置参数后，点击*保存*可保存配置。

时区

从下拉框中选择设备所在的时区。

校时方式

手动校时

默认为手动校时，可手动配置设备时间。

NTP 校时

需配置 NTP 校时的服务器地址、端口和校时间隔。

8.4.3 查看开源声明

可查看设备开源信息声明。

点击 *配置 → 系统 → 系统设置 → 关于设备*，进入界面。

点击*查看*，可查看所有开源信息。

8.4.4 网络配置

可配置设备端口和 Wi-Fi 参数。

设置端口

端口配置参数包括 HTTP 端口、RTSP 端口、HTTPS 端口和服务端口。通过网络访问设备时可根据需要设置相应的端口。

点击 *配置 → 网络 → 基本配置 → 端口*，进入配置页面。

HTTP 端口

使用浏览器登录时需要在地址后面加上修改的端口号。如当 HTTP 端口号改为 81 时，当您使用浏览器登录时，需要输入 http://192.0.0.65:81。

RTSP 端口

实时传输协议端口，请确保您修改的端口可用即可。

HTTPS 端口

配置设备 HTTPS 端口，用于浏览器访问时，但需要证书验证。

服务端口

查看和修改设备的服务端口。

配置 Wi-Fi 参数

配置设备所连接的 Wi-Fi 参数。

操作步骤

说明

需设备支持方可配置 Wi-Fi 参数。

1. 点击 *配置 → 网络 → 基本配置 → Wi-Fi*，进入配置界面。
2. 勾选*启用 Wi-Fi*。

图 8-3 Wi-Fi 界面

3. 在 Wi-Fi 列表中选择所需连接的 Wi-Fi，输入密码进行连接。

4. **可选操作**: 添加 Wi-Fi。

1) 点击*+*。

2) 输入 **Wi-Fi 名称**，选择 Wi-Fi 的**工作模式**和**加密方式**。

3) 点击*保存*。

5. 输入 Wi-Fi 密码并点击*确定*。

6. 配置 WLAN 参数。

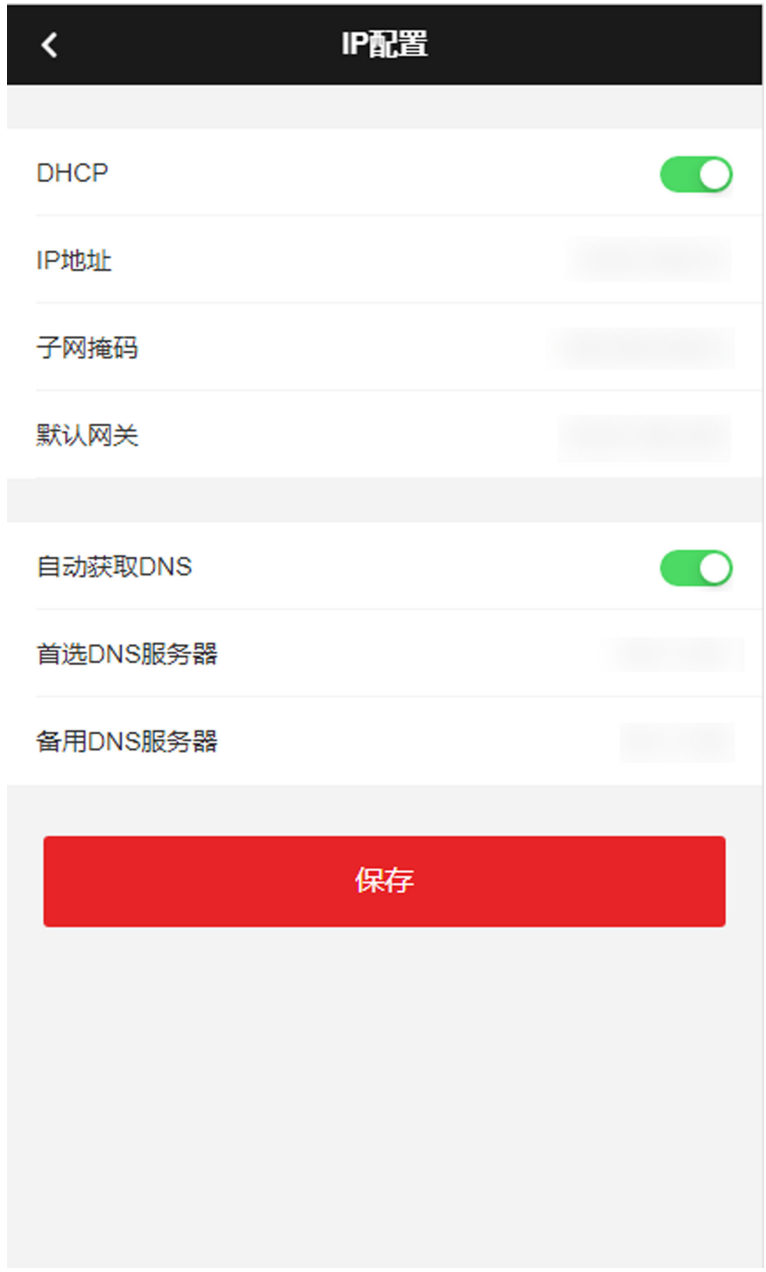


图 8-4 配置 WLAN 参数

1) 配置 IP 地址、子网掩码和默认网关。或勾选 *DHCP*，系统将自动分配 IP 地址、子网掩码、默认网关、首选 DNS 服务器地址和备用 DNS 服务器地址。
2) 点击 *保存*。

结果说明

Wi-Fi 配置完成后，可通过远程配置设备。

8.4.5 通用配置

认证参数配置

配置认证参数。

操作步骤

1. 点击 *配置 → 通用配置 → 认证配置*，进入配置页面。

2. 配置参数后，单击*保存*可保存配置。

设备类型

主读卡器

配置设备主读卡器参数。如果您选择主读卡器，需配置**读卡器种类**、**读卡器描述**、**启用读卡器**、**认证失败超次报警/失败超次报警次数**、**防拆检测使能**和**卡号翻转使能**等参数信息。

副读卡器

配置外接读卡器参数。如果您选择副读卡器，需配置**读卡器种类**、**读卡器描述**、**启用读卡器**、**认证失败超次报警/失败超次报警次数**、**防拆检测使能**、**读卡器掉线检测时间**和**密码输入超时时间**等参数信息。

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）

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。

认证失败超次报警/失败超次报警次数

启用**认证失败超次报警**后可配置失败超次报警次数，认证失败超过配置的次数后，设备自动生成报警事件并上报。

防拆检测使能

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

卡号翻转使能

启用该功能则读卡器读取卡号后将卡号顺序反转。

读卡器掉线检测时间

在设定的时间内读卡器若无法与主机联系上，则读卡器已掉线。

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。

配置隐私参数

可配置事件存储方式、图片上传和存储相关参数及图片清空相关参数。

点击 *配置 → 通用配置 → 隐私*，进入配置界面。

事件存储方式

可选择**定期删除旧事件**、**指定时间删除旧事件**、或**循环覆盖**。

定期删除旧事件

在输入框输入删除旧事件的周期。所有事件将根据设置的周期删除。

指定时间删除旧事件

配置时间，所有事件将在指定的时间删除。

循环覆盖

事件存储满 95%后，系统自动删除存储的最早的 5%的事件。

图片上传和存储配置

可配置图片上传和存储。

上传识别抓拍图片

认证时抓拍的图片将上传到平台。

保存识别抓拍图片

认证时抓拍的图片将保存到设备。

保存注册图片

人员添加时的注册图片将保存到设备。

上传联动抓拍图片

联动抓拍到的图片将上传到平台。

保存联动抓拍图片

联动抓拍到的图片将保存到设备。

清空设备图片

清空设备中存储的人脸或认证或抓拍图片。

清空人脸图片

选择**人脸图片**，点击*清空*，设备中所有注册的人脸图片将被清空。

清空认证或抓拍图片

选择**认证/抓拍图片**，点击*清空*，设备中所有的认证或抓拍图片将被清空。

配置卡片安全

配置设备适配的卡片。

点击 *配置 → 通用配置 → 卡片安全*，进入配置界面。

图 8-5 卡片安全配置

配置卡片相关参数。点击*保存*。

启用 NFC 卡

为防止手机获取门禁设备数据，出现非法通行情况。通过启用 NFC 功能，使门禁设备访问受保护。

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。

M1 卡加密校验

启用 M1 卡加密校验可以提升门禁卡安全性，使得门禁卡更不容易被拷贝。勾选后需配置扇区编号。

扇区

启用 M1 卡加密验证后，配置加密扇区编号。

说明

建议加密第 13 扇区。

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。

说明

若设备外接可读 EM 卡片的读卡器，启用此功能后，也可以在外接读卡器上刷 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。

CPU 卡读内容

启用 CPU 卡读内容后，设备可读取 CPU 卡内的内容。

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。

配置卡号认证参数

配置通过卡号认证时，设备读取的卡号内容。

点击 *配置 → 通用配置 → 卡号认证*。

选择卡号认证模式，并点击*保存*。

全卡号

全部卡号内容将被读取。

Wiegand26（3 字节）

卡号通过 Wiegand26 协议来读取（仅读 3 字节卡号）。

Wiegand34（4 字节）

卡号通过 Wiegand34 协议来读取（仅读 4 字节卡号）。

8.4.6 配置人脸参数

配置人脸相关参数。

人脸参数配置

点击 *配置 → 智能配置 → 智能参数*，进入配置页面。

图 8-6 配置人脸参数

说明

不同型号支持的参数项有所不同，请以实际界面为准。

配置人脸参数。

启用真人检测

选择是否开启检测真人人脸功能。开启此功能后，设备可判断是否为真实的人脸。若检测的人脸不是真实的人脸，则认证失败。

真人检测安全等级

开启真人检测功能后的人脸匹配安全等级。可从普通、高、极高三个等级中选择。等级越高，误识率越低，拒认率越高。

识别距离

选择实际环境下人脸识别的距离。

环境模式

根据实际情况选择**室内**或**其他**。在室外场景、室内靠窗的场景、或使用体验不好的情况下，可选择**其他**。

说明

若设备未通过其他工具激活，设备默认使用室内作为环境模式。

人脸识别模式

普通模式

设备通过摄像头进行人脸识别。

深度模式

适用于较为复杂的环境，识别的人群范围更广。

设备通过摄像头进行人脸识别。

连续识别间隔时间

认证过程中，前后 2 次人脸识别的间隔时间。

说明

需填写 1~10 之间的数字。

人脸 1:1 阈值

人脸 1:1 匹配时的匹配阀值。阈值越大，识别人脸时误识率越低，拒认率越高。最大可填 100。

人脸 1:N 阈值

人脸 1:N 匹配时的匹配阀值。阈值越大，识别人脸时误识率越低，拒认率越高。最大可填 100。

人脸识别超时时间

配置人脸识别时的超时时间。若人脸识别时长超过配置的值，设备提示人脸识别超时。

启用面部口罩检测

启用面部口罩检测功能后，可配置*未带口罩策略*、*口罩人脸 1:N 阈值*和*环保模式口罩人脸 1:N 阈值*。

未带口罩策略

可配置*无提示*、*提醒戴口罩*和*必须戴口罩*。

无提示

认证人员若未佩戴口罩，设备不提示口罩相关信息。

提醒戴口罩

认证人员若未佩戴口罩，设备提示戴口罩，且开门。

必须戴口罩

认证人员若未佩戴口罩，设备提示戴口罩，且不开门。

口罩人脸 1:1 阈值

戴口罩人脸 1:1 匹配时的匹配阀值。阈值越大，识别戴口罩人脸的误识率越低，拒认率越高。最大可填 100。

口罩人脸 1:N 阈值

戴口罩人脸 1:N 匹配时的匹配阀值。阈值越大，识别戴口罩人脸的误识率越低，拒认率越高。最大可填 100。

环保模式口罩人脸 1:1 阈值

进行环保模式下戴口罩人脸 1:1 匹配时的阈值。阈值越大，识别人脸时的误识率越低，拒认率越高。最大可填 100。

环保模式口罩人脸 1:N 阈值

进行环保模式下戴口罩人脸 1:N 匹配时的阈值。阈值越大，识别人脸时的误识率越低，拒认率越高。最大可填 100。

环保模式

启用环保模式后，在弱光或无光环境下，设备启用红外摄像头进行人脸比对。可配置环保模式（1:N）及环保模式（1:1）。

环保模式阈值

环保模式（1:N）及环保模式（1:1）匹配时的匹配阈值。

1:1 阈值

环境模式 1:1 匹配时的匹配阈值。

1:N 阈值

环境模式 1:N 匹配时的匹配阈值。

人脸识别区域配置

点击 *配置 → 智能配置 → 区域配置*，进入配置页面。

在预览画面中拖动蓝色框的边界，可调整左右上下人脸识别有效区域进行边界配置。
或在右侧拖动滑块或输入数值，配置人脸识别有效区域。
点击*保存*可保存配置。

8.4.7 对讲配置

设备编号配置

设备可作为门禁设备、门口机或围墙机来使用，可配置设备的可视对讲相关参数。

配置参数后，单击*保存*可保存配置。

若设备类型选择*门口机*或*门禁设备*，可配置设备所处期号、幢号（楼号）、编号、单元号、层号、和小区编号。

图 8-7 编号配置（门口机）

设备类型

设备可作为门口机使用，从下拉框中选择设备类型。

期号

设备所在的期号。

幢号

设备所在的幢号。

编号

自定义设备作为门禁设备或门口机的编号。

说明

- 若设备类型为**门口机**或**门禁设备**，编号可选择 0~99。
- 若修改设备类型或编号，需重启设备方可生效。

单元号

设备所在的单元号。

层号

设备所在的楼层。

小区编号

设备所在小区编号。

若设备类型选择*围墙机*，可配置设备所处期号、围墙机编号和小区编号。

设备类型

设备可作为围墙机使用，从下拉框中选择设备类型。

期号

设备所在的期号。

编号

自定义设备作为围墙机的编号。

说明

- 若设备类型为**围墙机**，编号可选择 1~99。
- 若修改设备类型或编号，需重启设备方可生效。

小区编号

设备所在小区编号。

说明

若修改设备类型或编号，需重启设备方可生效。

关联网络参数配置

可配置关联设备的 SIP 服务器 IP 地址和管理机 IP 地址。完成配置后，可实现门禁设备与可视对讲门口机、室内机、管理机、平台等间的通话。

点击 *配置 → 对讲配置 → 关联网络配置* 进入关联网络配置页面。

图 8-8 关联网络配置

可配置关联设备的 SIP 服务器 IP 地址和管理机 IP 地址。完成配置后，您可实现门禁设备与可视对讲门口机、室内机、管理机、平台等间的通话。

点击*保存*可保存配置。

配置呼叫类型

配置设备按键对应的呼叫目标。

操作步骤

1. 单击 *配置 → 对讲配置 → 按键配置*，进入配置界面。
2. 选择**呼叫类型**。可选择*呼叫房间号*、*呼叫管理中心*或*呼叫特定房间号*。

呼叫房间号

通过输入房间号，可呼叫某个房间。

呼叫管理中心

呼叫管理中心，管理中心接听后，即可进行通话。呼叫管理中心时，设备优先呼叫管理机。

呼叫特定房间号

呼叫指定的房间。

3. 点击*保存*配置生效。

说明

仅部分设备支持按键呼叫功能，请以实际设备配置界面为准。

结果说明

- 若**呼叫类型**设置为*呼叫房间号*，可在拨号界面输入房间号，并点击 可直接呼叫房间。
- 若**呼叫类型**设置为*呼叫管理中心*，可点击 可直接呼叫管理中心。
- 若**呼叫类型**设置为*呼叫特定房间号*，可点击 可直接呼叫特定房间。

8.4.8 门禁配置

门参数配置

设置门参数，包括门序号、名称、门锁动作时间、开门超时报警时间、门磁类型、出门按钮类型、门锁掉电状态、关门延迟时间、首人常开持续时间、胁迫码和超级密码等参数。

点击 *配置 → 门禁配置 → 门参数*，进入配置页面。

图 8-9 门禁参数配置

配置参数后，点击*保存*可保存配置。

门序号

选择设备所在门序号。

名称

为此门创建名称。

门锁动作时间

普通卡刷卡后，门锁开启时间。

开门超时报警时间

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。

门磁类型

可控制门磁常开或者常闭。正常情况下应处于常闭状态（特殊需求除外）。

出门按钮类型

正常情况下应处于常开状态（特殊需求除外）。

门锁掉电状态

配置门锁掉电后门的状态，默认为常闭。

关门延迟时间

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开启时间。

首人常开持续时间

配置首人常开的持续时间。配置首人常开模式的人员认证通过后，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认证即可通行，常应用于大批量人员通过的场景，如团体访客进入旅游景点。

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。

超级密码

指定人员输入超级密码即可开门。

说明

胁迫码和超级密码不能重复，一般为 4-8 位的数字。

配置 RS-485 参数

设备可通过 RS-485 接口外接门禁主机、扩展模块或读卡器模块。在此处设置 RS-485 参数，以便连接外接设备。

点击 *配置* → *门禁配置* → *RS-485 配置*，进入配置页面。

图 8-10 RS-485 配置

配置参数后，点击*保存*可保存配置。

外接设备类型

根据实际外接设备连接情况选择一个外接设备。可选择**读卡器模块**、**扩展模块**、或**门禁主机**。

说明

改变外接设备，并保存参数后，设备将自动重启。

RS-485 地址

根据实际情况配置 RS-485 地址。

说明

当外接设备选择**门禁主机**时，若外接设备为一体机，需设置外接设备对应的本机 RS-485 地址为 2；若外接设备为门禁主机，需要根据对应的门编号配置 RS-485 地址。

波特率

通过 RS-485 通讯时的波特率。

数据位

通过 RS-485 通讯时的数据位。

停止位

通过 RS-485 通讯时的停止位。

校验/流控/通讯模式

默认已选择。

配置韦根参数

设备可通过韦根接口外接设备。可在此处可设置韦根参数。

操作步骤

1. 点击 *配置* → *门禁配置* → *韦根配置*，进入配置页面。

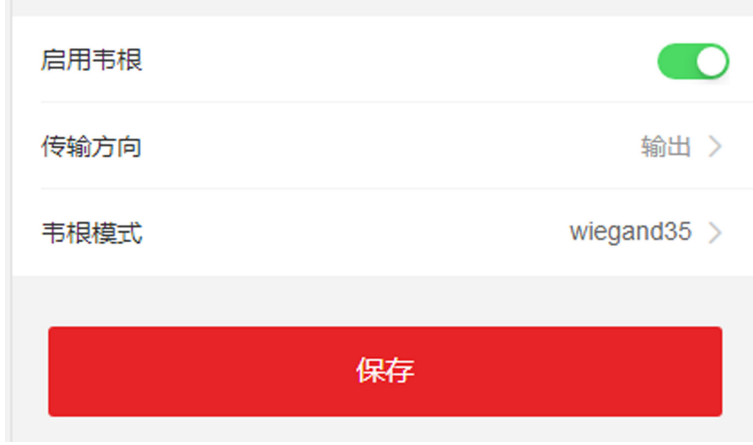


图 8-11 韦根参数配置

2. 启用 *Wiegand*，开启韦根通讯功能。

3. 选择韦根传输方向。

说明

- 开启韦根通讯功能后，传输方向默认为输出。
- 人脸识别终端可外接门禁主机，通过韦根 26、34、27 或 35 传输卡号。

4. 配置参数后，点击*保存*可保存配置。

第 9 章 网页端操作说明

9.1 登录

可通过网页端、客户端软件远程配置库入口登录。

说明

请确保设备已激活，具体激活配置，请参见 *激活* 。

通过网页端登录

在浏览器地址栏中输入 *https://设备 IP 地址*, 按键盘上的回车键进入登录界面。输入用户名和密码，单击*登录*。

通过客户端软件远程配置库入口登录

下载并安装客户端软件，添加设备后，单击 进入网页端配置界面。

9.2 预览

预览设备拍摄的画面，可进行抓拍、录像等操作。

登录后进入*预览*页面，可进行画面预览、抓拍、录像等操作。

图 9-1 预览

功能说明：

说明

不同设备支持的功能不同，请以实际界面为准。

选择预览时的画面大小。

设置预览时的音量大小。

说明

音量调节条仅用于调节预览伴音的音量，如果打开了语音对讲，再调节音量条，会导致听到重复的声音。

预览时抓拍照片。

放大预览画面。

与设备对讲。

开门按钮。

预览画面开启和关闭。

预览时录像功能开启和关闭。

预览时码流类型选择。可选择主码流或子码流。

选择预览时画面分割类型。可选择 1 画面、4 画面、9 画面或 16 画面。

全屏预览。

9.3 添加人员

添加人员基本信息

单击 *人员管理* → *添加* 进入添加人员页面。
创建人员工号、姓名、性别，选择用户类型，并输入人员层号和房间号。

设置人员权限时间

单击 *人员管理* → *添加* 进入添加人员页面。
输入人员权限的开始时间和结束时间。

设置访问控制

单击 *人员管理* → *添加* 进入添加人员页面。
在访问控制中勾选设备管理员后，添加的人员可通过人脸认证登录后台。
可在房间号中，单击*添加*输入访问控制的层号和房间号。

添加认证类型

单击 *人员管理* → *添加* 进入添加人员页面。
配置认证类型。

同设备

认证类型与设备配置的认证模式相同。该人员验证身份时，需使用设备验证方式进行验证。

添加人员时默认选择采用主机认证模式。此模式方便批量修改人员验证方式。

自定义

若该人员需要使用有别于设备验证模式的特殊验证方式，可选用自定义验证方式。该人员在设备端认证时优先使用该配置的验证方式进行身份验证。此模式方便配置单个需要有特殊权限的人员。

添加人员指纹

单击 *人员管理* → *添加* 进入添加人员页面。
单击*添加指纹*，将手指放入指纹识别区进行识别，添加后单击*完成*。

添加人员人脸照片

单击 *人员管理* → *添加* 进入添加人员页面。
单击+，并从本地选择照片上传。

说明

图片格式为 JPEG 或 PNG，且小于 200K。

9.4 事件查询

单击*事件查询*进入查询页面。

图 9-2 事件查询

输入搜索条件，包括工号、姓名、卡号、搜索的开始时间和结束时间，并单击*查询*。

说明

支持搜索 32 位以内的姓名。

搜索结果将展示在界面右侧。

9.5 配置

9.5.1 设置本地参数

配置播放时的码流类型、播放性能、自动开启预览功能、抓图文件格式，还可配置录像文件打包大小、录像文件和抓图文件的保存位置。

单击 *配置* → *本地*，进入页面。

播放参数

码流类型

您可根据实际情况设置码流类型。

播放性能

根据需求选择*最短延时*、*均衡*或*流畅性好*。

自动开启预览

若选择*是*，开启预览时，界面自动播放预览画面；若选择*否*，开启预览时，需手动单击播放按钮方可播放预览画面。

抓图文件格式

设置抓取的图片的保存格式。

录像文件

录像文件打包大小

可根据需求选择录像文件打包的大小。

录像文件保存路径

录像文件存放在本地的路径，可选择 更改路径，单击*打开*可打开存档路径下的文件夹。

抓图和剪辑

预览抓图保存路径

抓图文件在本地存放的路径，可选择 更改路径，单击*打开*可打开存档路径下的文件夹。

说明

仅 IE 浏览器支持保存路径的配置，其他浏览器默认为 C 盘下载路径，具体操作请以实际设备界面为准。

9.5.2 查看设备基本信息

查看设备名称、语言、型号、序列号、二维码、版本号、通道个数、报警输入个数、报警输出个数、电锁个数、本地 485 个数和设备容量等信息。

单击 *配置 → 系统 → 系统设置 → 基本信息*，进入页面。

可查看设备名称、语言、型号、序列号、二维码、版本号、通道个数、报警输入个数、报警输出个数、电锁个数、本地 485 个数和设备容量等信息。

9.5.3 配置设备时间

配置本机所使用的时区、校时方式以及显示的时间。

单击 *配置 → 系统 → 系统配置 → 时间配置*，进入配置页面。

图 9-3 时间配置

配置参数后，单击*保存*可保存配置。

时区

从下拉框中选择设备所在的时区。

校时方式

手动校时

默认为手动校时，可手动配置设备时间，或勾选*与计算机时间同步*，设备自动同步计算机时间。

NTP 校时

需配置 NTP 校时的服务器地址、端口和校时间隔。单击*测试*可测试与服务器的通信情况。

9.5.4 查看开源声明

可查看设备开源信息声明。

单击 *配置 → 系统 → 系统设置 → 关于设备*，进入界面。

单击*查看*，可查看所有开源信息。

9.5.5 系统升级和维护

重启设备、恢复设备参数、升级设备。

重启设备

单击 *配置 → 系统 → 系统维护 → 升级维护*，进入配置页面。

单击*重启*，设备开始重启。

恢复参数

单击 *配置 → 系统 → 系统维护 → 升级维护*，进入配置页面。

恢复默认值

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

设备恢复出厂设置，设备需要重新激活方可再次使用。

参数导入导出

单击 *配置 → 系统 → 系统维护 → 升级维护*，进入配置页面。

参数导出

单击*导出*可导出维护日志或设备参数。

说明

导出的设备参数可通过参数导入到另一个设备中。

参数导入

单击 从电脑本地选择需要导入的文件，单击*导入*可进行参数导入操作。

升级设备

单击 *配置 → 系统 → 系统维护 → 升级维护*，进入配置页面。
从下拉框中选择升级类型，单击 从本地选择升级文件，并单击*升级*，设备自动获取升级文件进行升级。

说明

升级过程需要大概 2 分钟，升级过程中请不要关闭电源，完成升级后设备将自动重启。

9.5.6 搜索和查看日志

可进行设备日志的搜索和查看。

单击 *配置 → 系统 → 系统维护 → 日志查询*，进入配置界面。

选择日志主类型和次类型，选择需要查询的开始时间和结束时间，单击*查询*，列表显示日志信息，包含序号、时间、主类型、次类型、通道号、本地/远程用户及远程主机地址。

9.5.7 安全管理

选择登录时的安全等级，还可使能 SSH 和 HTTP。

单击 *配置 → 系统 → 安全管理 → 安全服务*，进入配置界面。

安全模式

登录时用户信息校验安全级别高。

兼容模式

登录时兼容旧版客户端用户信息校验方式。

启用 SSH

SSH 一般用于远程调试，当无需使用该服务时，建议不启用 SSH，提高设备安全性。

启用 HTTP

网络访问中，要提高浏览器访问的安全性，可通过启用 HTTPS 协议构建安全、加密的网络传输，通过身份认证和加密通讯，保证传输数据的安全性。

单击*保存*可保存配置。

9.5.8 证书管理

用于创建、集中管理设备所有通信证书、CA 证书等。

创建证书请求和安装证书

用于导入由设备生成证书请求，并经受信任机构签名的证书。

前提条件

已创建自签名证书。

操作步骤

1. 进入 *配置 → 系统 → 安全管理 → 证书管理* 。
2. 在**证书请求文件**模块中选择证书类型。
3. 单击*创建*。
4. 设置证书请求信息。
5. 单击*确定*。

弹窗显示证书详情。上下滑动可查看全文。

6. 复制证书详情并将其存成本地的请求文件。
7. 将请求文件发送到证书认证机构进行签名。
8. 导入证书认证机构发送回的证书。
1) 在**秘钥导入**模块中选择证书类型，并从本地选择秘钥，单击*安装*。
2) 在**通信证书导入**（公钥导入）模块中选择证书类型，并从本地选择通信证书（公钥），单击*安装*。

安装第三方机构签名证书

用于导入由第三方机构进行认证的签名证书。

前提条件

已获取第三方机构签名证书。

操作步骤

1. 进入 *配置 → 系统 → 安全管理 → 证书管理* 。
2. 在**秘钥导入**模块和**通信证书导入**模块中选择证书类型，从本地上传已有第三方机构签名的证书，并单击*安装*。

安装 CA 证书

用于导入由权威证书签证机关(CA)颁发的证书（一般权威的 CA 组织需要收费），提高访问的安全等级。

前提条件

已获取 CA 证书。

操作步骤

1. 进入 *配置 → 系统 → 安全管理 → 证书管理* 。

2. 在**信任 CA 证书导入**模块中自定义证书 ID

3. 从本地上传 CA 证书，并单击*安装*。

9.5.9 修改管理员密码

修改管理员的登录密码。

操作步骤

1. 单击 *配置 → 系统 → 用户管理*，进入配置页面。

2. 单击 admin 用户操作列下的 。

3. 输入旧密码、创建新密码并确认密码。

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。
- 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。

4. 单击*确认*。

设备密码将被修改，需重新登录网页端。

9.5.10 查看布防

查看设备布防类型及布防 IP 地址。

单击 *配置 → 系统 → 用户管理 → 布防一览*，进入配置界面。

用户可查看设备的布防信息，主要包括序号、布防类型及 IP 地址，单击*刷新*可即时刷新当前布防信息。

9.5.11 网络配置

配置 TCP/IP、端口、Wi-Fi 参数和平台接入。

配置基本网络参数

配置设备 TCP/IP 信息。

单击 *配置* → *网络* → *基本配置* → *TCP/IP*，进入配置页面。

图 9-4 基本网络参数配置

配置参数后，单击*保存*可保存参数。

网卡类型

在下拉框中选择网卡类型，默认为自适应。

自动获取

若不勾选此项，需手动配置 IPv4 地址、IPv4 子网掩码、IPv4 默认网关、MTU 和设备端口。

若勾选此项，系统自动分配 IPv4 地址、IPv4 子网掩码、IPv4 默认网关和 MTU。

首选 DNS 服务器及备用 DNS 服务器

根据实际需求配置 DNS 服务器地址。

设置端口

端口配置参数包括 HTTP 端口、RTSP 端口、HTTPS 端口和服务端口。通过网络访问设备时刻根据需要设置相应的端口。

单击 *配置 → 网络 → 基本配置 → 端口*，进入配置页面。

HTTP 端口

使用浏览器登录时需要在地址后面加上修改的端口号。如当 HTTP 端口号改为 81 时，当您使用浏览器登录时，需要输入 http://192.0.0.65：81。

RTSP 端口

实时传输协议端口，请确保您修改的端口可用即可。

HTTPS 端口

配置设备 HTTPS 端口，用于浏览器访问时，但需要证书验证。

服务端口

查看和修改设备的服务端口。

配置 Wi-Fi 参数

配置设备所连接 Wi-Fi 参数。

操作步骤

说明

需设备支持方可配置 Wi-Fi 参数。

1. 单击 *配置 → 网络 → 基本配置 → Wi-Fi*，进入配置界面。

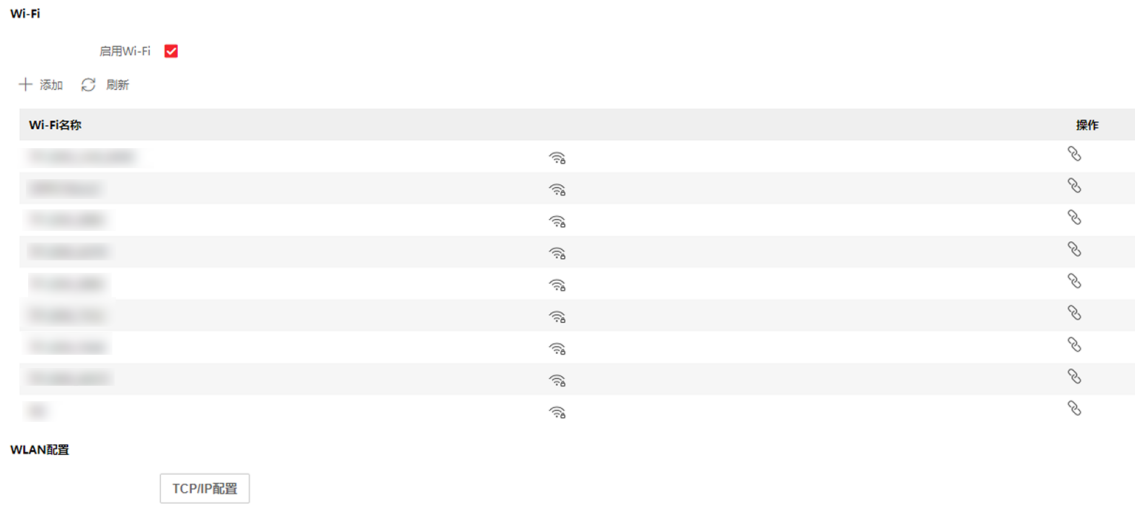


图 9-5 Wi-Fi 配置

2. 勾选*启用 Wi-Fi*。

3. 添加 Wi-Fi。

1) 单击*添加*。

2) 输入 Wi-Fi 的 SSID、工作模式和加密方式。

3) 单击*连接*。

4) 单击*确定*。

4. 选择一个 Wi-Fi，并单击操作列下的 。

5. 输入 Wi-Fi 密码并单击*确定*。

6. 配置 WLAN 参数。

1) 单击 *TCP/IP 配置*。

2) 配置 IP 地址、子网掩码和默认网关。或勾选*启用 DHCP*，系统自动分配 IP 地址、子网掩码和默认网关。

3) **可选操作**: 勾选*自动获取 DNS*，系统将自动分配 DNS 服务器地址。若不勾选，需手动填写首选 DNS 服务器地址和备用 DNS 服务器地址。

上报策略配置

通过配置中心组以及通道，您可通过 ISUP 协议传输日志。

单击 *配置 → 网络 → 基本配置 → 上报策略* 进入配置界面。配置数据上传的中心组，系统可通过 ISUP 协议传输日志。单击*保存*保存配置的参数。

中心组

选择合适的中心组。

主通道

勾选**启用**，配置通讯的主通道。设备将通过配置的主通道网络与平台进行通讯。

说明

N1 代表有线网络通讯。

平台接入设置

设备接入云平台，可通过移动客户端对设备进行操作。

操作步骤

1. 单击 *配置 → 网络 → 高级配置 → 平台接入*，进入配置界面。
2. 选择平台接入方式为*萤石云*。
3. 勾选**启用**，配置服务器地址，并输入验证码/加密密钥。
4. 单击*保存*完成配置。

配置 ISUP 参数

配置通过 ISUP 协议通讯的参数。

操作步骤

说明

需设备支持方可配置 ISUP 参数。

1. 单击 *配置 → 网络 → 高级配置 → 平台接入*，进入配置界面。
2. 平台接入方式选择 *ISUP*。
3. 勾选*启用*。
4. 配置 ISUP 协议版本、服务器地址类型、端口、设备 ID。

说明

若选择协议版本为 ISUP5.0，需配置 ISUP 密钥。

5. 单击*保存*。

设置 HTTP 监听

设备通过 HTTP 协议的方式发送报警信息给目的 IP 或域名，要求目的 IP 地址或域名支持 HTTP 或 HTTPS 协议传输。

操作步骤

1. 进入 *配置 → 网络 → 高级配置 → HTTP 监听* 。

2. 输入事件报警 IP 或域名、URL 地址和端口，选择协议类型。

3. 单击*测试*。

说明

单击*重置*，可重新设置目的 IP 地址或域名的信息。

4. 单击*保存*。

9.5.12 设置视频和音频参数

可配置设备摄像头的图像质量、分辨率等以及设备音量。

配置视频参数

单击 *配置 → 视音频 → 视频*，进入配置界面。

配置码流类型、视频类型、分辨率、码率类型、图像质量、视频帧率、码率上限、视频编码和 I 帧间隔。

配置参数后，单击*保存*可保存配置。

配置音频参数

单击 *配置 → 视音频 → 音频*，进入配置界面。

根据需要配置码流类型和音频编码。

移动滑块可配置输入和输出音量。

配置参数后，单击*保存*可保存配置。

9.5.13 设置自定义语音

自定义认证成功、认证失败时设备输出的语音。

操作步骤

1. 单击 *配置 → 视音频 → 提示音*，进入配置界面。

2. 勾选 *TTS*(Text to Speech)，设备将开启文本转化为语音功能。

3. 选择左侧需要设置的时间计划。

4. 启用自定义语音功能。

5. 选择播报称呼。

6. 配置认证成功时间段。

1) 单击*添加*

2) 配置时间段，在该时间段内，若认证成功，设备输出自定义的语音提示。

3) 配置语音输出语言。

4) 输入认证成功语音内容。

5) **可选操作**: 重复子步骤 1~4。
6) **可选操作**: 单击 可删除时间段。

7. 配置认证失败时间段。
1) 单击*添加*
2) 配置时间段，在该时间段内，若认证失败，设备输出自定义的语音提示。
3) 配置语音输出语言。
4) 输入认证失败语音内容。
5) **可选操作**: 重复子步骤 1~4。
6) **可选操作**: 单击 可删除时间段。

8. 可选操作: 单击左侧*添加假日计划*，重复步骤 3~6，可添加假日提示音配置。
9. 单击*保存*。

9.5.14 配置图像参数

配置设备预览页面的视频制式、宽动态、画面亮度、对比度、饱和度和锐度。

操作步骤

1. 单击 *配置* → *图像*，进入配置页面。
2. 配置参数。

视频制式

设置远程预览时，视频的帧率。修改制式后，需重启设备，方可生效。

PAL

每秒 25 帧画面，适用于中国大陆、中国香港、中东地区和欧洲等国家和地区。

NTSC

每秒 30 帧画面，适用于美国、加拿大、日本、中国台湾、韩国、菲律宾等国家和地区。

宽动态

开启或关闭宽动态功能。宽动态可以一种可以使场景中特别亮的部位和特别暗的部位同时都能看得特别清楚的技术。

亮度/对比度/饱和度/锐度

根据需求拖动滑块或输入数值配置亮度、对比度、饱和度和锐度。

单击*恢复默认值*可恢复默认参数。

开始/结束录像。

抓拍预览画面。

9.5.15 通用配置

认证参数配置

配置认证参数。

单击 *配置* → *门禁配置* → *认证配置*，进入配置页面。

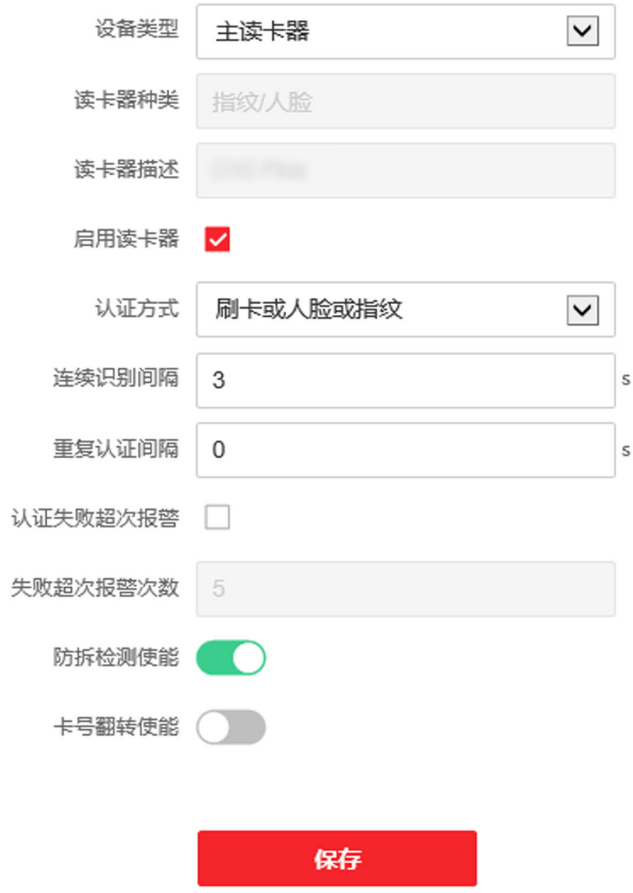


图 9-6 认证参数配置

配置参数后，单击*保存*可保存配置。

设备类型

主读卡器

配置设备主读卡器参数。

副读卡器

配置外接读卡器参数。

如果选择主读卡器：

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)

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。

认证方式

根据需求从下拉框中选择一个认证方式。

连续识别间隔

认证时，同一人员可重复认证的间隔时间。同一人员在配置的间隔时间内重复认证视为无效。

重复认证间隔

认证过程中，同一人员前后 2 次通过任意凭证识别的间隔时间。在配置的时间段内，同一个人员只能进行一次认证。若在配置的时间段内有其他人员进行认证,该人员可重新认证。

认证失败超次报警/失败超次报警次数

勾选**认证失败超次报警**后可配置失败超次报警次数，认证失败超过配置的次数后，设备自动生成报警事件并上报。

防拆检测使能

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

卡号反转使能

启用该功能则读卡器读取卡号后将卡号顺序反转。

如果选择副读卡器：

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)

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。

认证方式

根据需求从下拉框中选择一个认证方式。

连续识别间隔

认证过程中，前后两次人脸识别的间隔时间。

重复认证间隔

认证过程中，同一人员前后 2 次通过任意凭证识别的间隔时间。在配置的时间段内，同一个人员只能进行一次认证。

认证失败超次报警/失败超次报警次数

勾选**认证失败超次报警**后可配置失败超次报警次数，认证失败超过配置的次数后，设备自动生成报警事件并上报。

读卡器掉线检测时间

在设定的时间内读卡器若无法与主机联系上，则读卡器已掉线。

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。

OK LED 极性/Error LED 极性

可选择主板的阴极或者阳极。

防拆检测使能

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

配置隐私参数

可配置事件存储方式、认证结果显示、图片上传和存储相关参数及图片清空相关参数。

单击 *配置 → 通用 → 隐私* 。

事件存储方式

可选择**定期删除旧事件**、**按指定事件删除旧事件**、或**循环覆盖**。

定期删除旧事件

拖动滑块选择或直接在输入框输入删除旧事件的周期。所有事件将根据设置的周期删除。

按指定时间删除旧事件

配置时间，所有事件将在指定的时间删除。

循环覆盖

事件存储满 95%后，系统自动删除存储的最早的 5%的事件。

认证配置

认证结果显示

可勾选认证结果显示相关内容，如照片、姓名、工号等。还可以勾选姓名脱敏显示，勾选后，姓名会进行部分显示。

图片上传和存储配置

可配置图片上传和存储。

上传识别抓拍图片

认证时抓拍的图片将上传到平台。

保存识别抓拍图片

认证时抓拍的图片将保存到设备。

保存注册图片

人员添加时的注册图片将保存到设备。

上传联动抓拍图片

联动抓拍到的图片将上传到平台。

保存联动抓拍图片

联动抓拍到的图片将保存到设备。

清空设备图片

清空设备中存储的人脸或认证或抓拍图片。

清空人脸底图

设备中所有注册的人脸图片将被清空。

清空认证或抓拍图片

设备中所有的认证或抓拍图片将被清空。

配置终端参数

配置设备的终端参数。

单击 *配置 → 门禁配置 → 人证参数*，进入配置页面。

工作模式

配置设备的工作模式。

门禁模式

门禁模式为普通模式，需验证卡片或身份证权限访客通过。

身份证阅读器型号

选择外接身份证阅读器型号。

身份证核验中心

配置身份证验证方式。

黑名单核验

启用后，进行一次黑名单校验。

配置卡片安全

配置设备适配的卡片。

单击 *配置 → 门禁配置 → 卡片安全*，进入配置界面。

图 9-7 卡片安全配置

配置卡片相关参数。单击*保存*。

启用 NFC 卡

为防止手机获取门禁设备数据，出现非法通行情况。通过启用 NFC 功能，使门禁设备访问受保护。

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。

M1 卡加密校验

启用 M1 卡加密校验可以提升门禁卡安全性，使得门禁卡更不容易被拷贝。勾选后需配置扇区编号。

扇区

启用 M1 卡加密验证后，配置加密扇区编号。

说明

建议加密第 13 扇区。

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。

说明

若设备外接可读 EM 卡片的读卡器，启用此功能后，也可以在外接读卡器上刷 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。

CPU 卡读内容

启用 CPU 卡读内容后，设备可读取 CPU 卡内的内容。

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。

配置卡号认证参数

配置通过卡号认证时，设备读取的卡号内容。

单击 *配置 → 门禁配置 → 卡号认证配置* 。

选择卡号认证模式，并单击*保存*。

全卡号

全部卡号内容将被读取。

Wiegand26（3 字节）

卡号通过 Wiegand26 协议来读取（仅读 3 字节卡号）。

Wiegand34（4 字节）

卡号通过 Wiegand34 协议来读取（仅读 4 字节卡号）。

9.5.16 对讲配置

设备编号配置

设备可作为门禁设备、门口机或围墙机来使用，可配置设备的可视对讲相关参数。

编号配置

单击 *配置 → 对讲配置 → 编号配置*，进入配置界面。
配置参数后，单击*保存*可保存配置。

若设备类型选择*门口机*或*门禁设备*，可配置设备所处期号、幢号（楼号）、单元号、层号、门口机编号（设备编号）和小区编号。

图 9-8 编号配置（门口机）

设备类型

设备可作为门口机使用，从下拉框中选择设备类型。

期号

设备所在的期号。

幢号

设备所在的幢号。

单元号

设备所在的单元号。

层号

设备所在的楼层。

门口机编号

自定义设备作为门口机的编号。

小区编号

设备所在小区编号。

若设备类型选择*围墙机*，可配置设备所处期号、围墙机编号和小区编号。

设备类型

设备可作为围墙机使用，从下拉框中选择设备类型。

期号

设备所在的期号。

围墙机编号

自定义设备作为围墙机的编号。编号可选择 1~99。

小区编号

设备所在小区编号。

说明

若修改设备类型或编号，需重启设备方可生效。

关联网络参数配置

可配置关联设备的 SIP 服务器 IP 地址及管理机 IP 地址。

单击 *配置 → 对讲配置 → 关联网络配置* 进入关联网络配置页面。

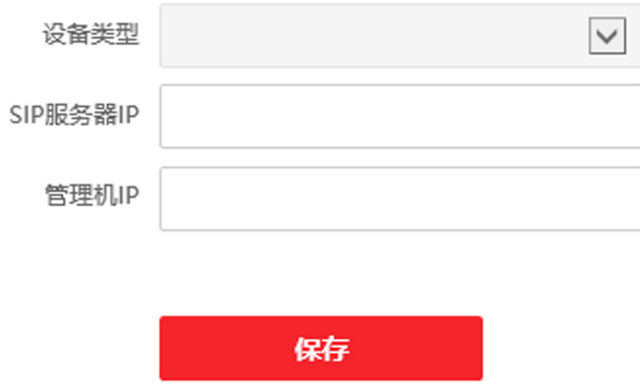


图 9-9 关联网络配置

完成配置后，您可实现门禁设备与可视对讲门口机、室内机、管理机、平台等间的通话。

单击*保存*可保存配置。

配置呼叫类型

配置设备按键对应的呼叫目标。

操作步骤

1. 单击 *配置 → 对讲配置 → 按键配置*，进入配置界面。
2. 选择**呼叫类型**。可选择*呼叫房间号*、*呼叫管理中心*或*呼叫特定房间号*。

   呼叫房间号

   通过输入房间号，可呼叫某个房间。

   呼叫管理中心

   呼叫管理中心，管理中心接听后，即可进行通话。呼叫管理中心时，设备优先呼叫管理机。

   呼叫特定房间号

   呼叫指定的房间。
3. 点击*保存*配置生效。

说明

仅部分设备支持按键呼叫功能，请以实际设备配置界面为准。

结果说明

- 若**呼叫类型**设置为*呼叫房间号*，可在拨号界面输入房间号，并点击 可直接呼叫房间。
- 若**呼叫类型**设置为*呼叫管理中心*，可点击 可直接呼叫管理中心。
- 若**呼叫类型**设置为*呼叫特定房间号*，可点击 可直接呼叫特定房间。

9.5.17 门禁配置

门参数配置

设置门参数，包括

单击 *配置 → 门禁配置 → 门参数*，进入配置页面。

图 9-10 门禁参数配置

配置参数后，单击*保存*可保存配置。

门序号

选择设备所在门序号。

名称

为此门创建名称。

门锁动作时间

普通卡刷卡后，门锁开启时间。

开门超时报警时间

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。

门磁类型

可控制门磁常开或者常闭。正常情况下应处于常闭状态（特殊需求除外）。

出门按钮类型

正常情况下应处于常开状态（特殊需求除外）。

门锁掉电状态

配置门锁掉电后门的状态，默认为常闭。

关门延迟时间

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开启时间。

首人常开持续时间

配置首人常开的持续时间。配置首人常开模式的人员认证通过后，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认证即可通行，常应用于大批量人员通过的场景，如团体访客进入旅游景点。

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。

超级密码

指定人员输入超级密码即可开门。

说明

胁迫码和超级密码不能重复，一般为 4-8 位的数字。

配置 RS-485 参数

设备可通过 RS-485 接口外接门禁主机、门控安全模块或读卡器。在此处设置 RS-485 参数，以便连接外接设备。

单击 *配置 → 门禁配置 → RS-485 配置*，进入配置页面。

图 9-11 RS-485 配置

配置参数后，单击*保存*可保存配置。

外接设备类型

根据实际外接设备连接情况选择一个外接设备。可选择**读卡器**、**扩展模块**、或**门禁主机**。

说明

改变外接设备，并保存参数后，设备将自动重启。

RS-485 地址

根据实际情况配置 RS-485 地址。

说明

当外接设备选择**门禁主机**时，若外接设备为一体机，需设置外接设备对应的本机 RS-485 地址为 2；若外接设备为门禁主机，需要根据对应的门编号配置 RS-485 地址。

波特率

通过 RS-485 通讯时的波特率。

数据位

通过 RS-485 通讯时的数据位。

停止位

通过 RS-485 通讯时的停止位。

校验/流控/通讯模式

默认已选择。

配置韦根参数

设备可通过韦根接口外接设备。可在此处可设置韦根参数。

操作步骤

1. 单击 *配置 → 系统 → 系统配置 → 韦根配置*，进入配置页面。

图 9-12 韦根参数配置

2. 勾选*启用韦根*，开启韦根通讯功能。

3. 选择韦根传输方向。

输出

人脸识别终端可外接门禁主机，通过韦根 26、34、27 或 35 传输卡号。

4. 配置参数后，单击*保存*可保存配置。

9.5.18 配置生物识别参数

配置生物识别相关参数。

生物识别参数配置

单击 *配置* → *智能配置* → *智能配置*，进入配置页面。

说明

不同型号支持的参数项有所不同，请以实际界面为准。

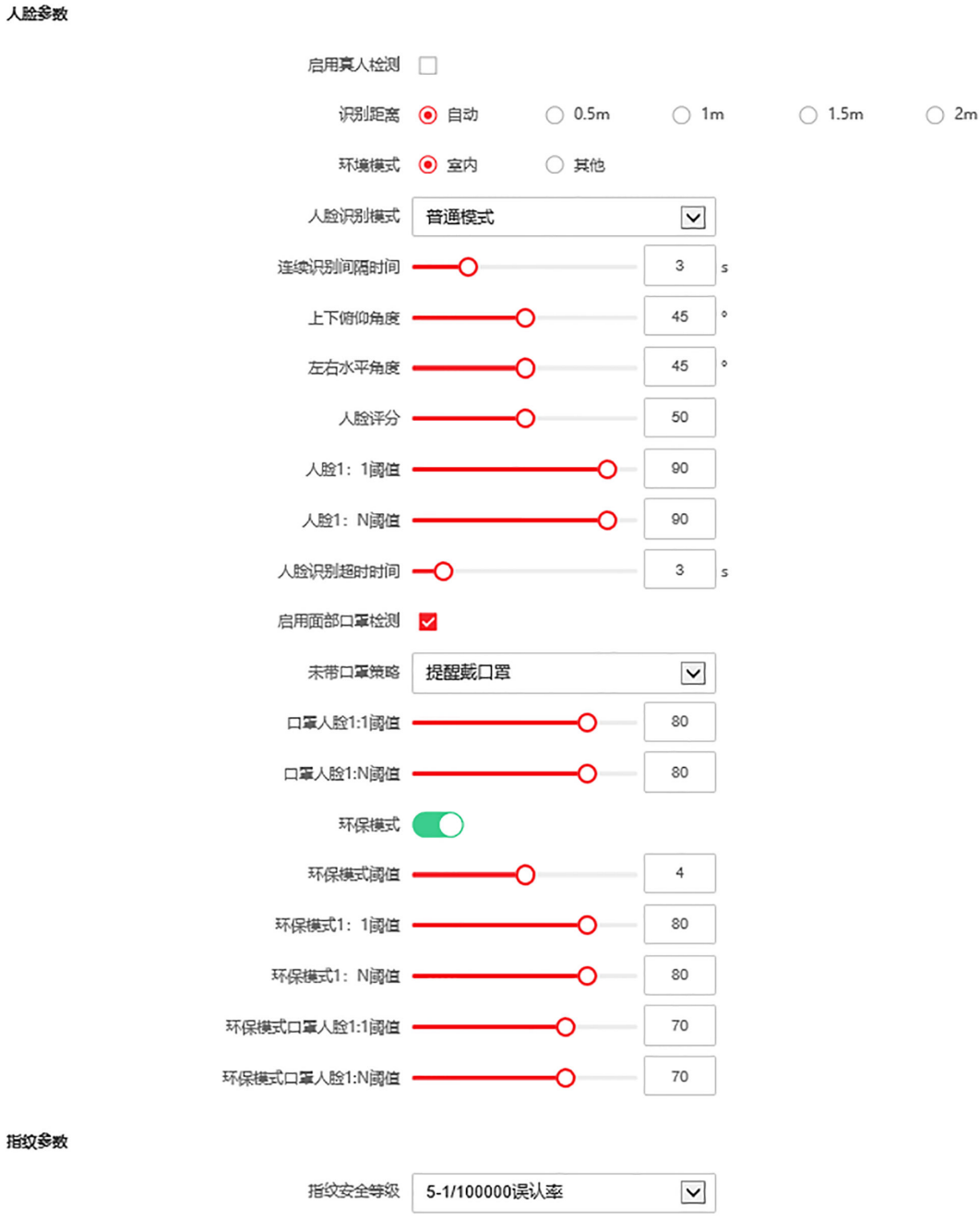


图 9-13 生物参数配置

配置人脸参数。

启用真人检测

选择是否开启检测真人人脸功能。开启此功能后，设备可判断是否为真实的人脸。若检测的人脸不是真实的人脸，则认证失败。

真人检测安全等级

开启真人检测功能后的人脸匹配安全等级。可从普通、高、极高三个等级中选择。等级越高，误识率越低，拒认率越高。

识别距离

选择实际环境下人脸识别的距离。

环境模式

根据实际情况选择**室内**或**其他**。在室外场景、室内靠窗的场景、或使用体验不好的情况下，可选择**其他**。

说明

若设备未通过其他工具激活，设备默认使用室内作为环境模式。

人脸识别模式

普通模式

设备通过摄像头进行人脸识别。

深度模式

适用于较为复杂的环境，识别的人群范围更广。

连续识别间隔时间

认证过程中，前后 2 次人脸识别的间隔时间。

说明

需填写 1~10 之间的数字。

上下俯仰角角度

人脸检测时，可抬头或者低头的最大角度。人脸比对或者录入时，抬头或者低头的角度需小于配置的值。

左右水平角度

人脸检测时，可向左或者向右转动的最大角度。人脸比对或者录入时，向左或者向右转动的角度需小于配置的值。

人脸评分

人脸质量评分（预留）。

人脸 1:1 阈值

人脸 1:1 匹配时的匹配阀值。阈值越大，识别人脸时误识率越低，拒认率越高。最大可填 100。

人脸 1:N 阈值

人脸 1:N 匹配时的匹配阀值。阈值越大，识别人脸时误识率越低，拒认率越高。最大可填 100。

人脸识别超时时间

配置人脸识别时的超时时间。若人脸识别时长超过配置的值，设备提示人脸识别超时。

启用面部口罩检测

启用面部口罩检测功能后，可配置*未带口罩策略*、*口罩人脸 1:N 阈值*和*环保模式口罩人脸 1:N 阈值*。

未带口罩策略

可配置*无提示*、*提醒戴口罩*和*必须戴口罩*。

无提示

认证人员若未佩戴口罩，设备不提示口罩相关信息。

提醒戴口罩

认证人员若未佩戴口罩，设备提示戴口罩，且开门。

必须戴口罩

认证人员若未佩戴口罩，设备提示戴口罩，且不开门。

口罩人脸 1:1 阈值

戴口罩人脸 1:1 匹配时的匹配阀值。阈值越大，识别戴口罩人脸的误识率越低，拒认率越高。最大可填 100。

口罩人脸 1:N 阈值

戴口罩人脸 1:N 匹配时的匹配阀值。阈值越大，识别戴口罩人脸的误识率越低，拒认率越高。最大可填 100。

环保模式口罩人脸 1:1 阈值

进行环保模式下戴口罩人脸 1:1 匹配时的阈值。阈值越大，识别人脸时的误识率越低，拒认率越高。最大可填 100。

环保模式口罩人脸 1:N 阈值

进行环保模式下戴口罩人脸 1:N 匹配时的阈值。阈值越大，识别人脸时的误识率越低，拒认率越高。最大可填 100。

环保模式

启用环保模式后，在弱光或无光环境下，设备启用红外摄像头进行人脸比对。可配置环保模式阈值、环保模式（1:N）及环保模式（1:1）。

指纹安全等级

可配置指纹安全等级。等级越高，误识率越低，拒认率越高。

人脸识别区域配置

单击 *配置 → 智能配置 → 区域配置*，进入配置页面。
在预览画面中拖动黄色框的边界，可调整左右上下人脸识别有效区域。
或在右侧拖动滑块或输入数值，配置人脸识别有效区域。
单击*保存*可保存配置。
单击预览画面中的 或 可录像或抓拍。

9.5.19 设置待机主题

配置设备待机时的主题。

操作步骤

1. 上传媒体库文件。
1) 单击 *配置 → 主题配置 → 媒体库*，进入配置页面。
2) 单击*添加*，从本地选择需要添加的文件。
3) 单击*上传*。
2. 单击 *配置 → 主题配置 → 主题配置*，进入配置页面。

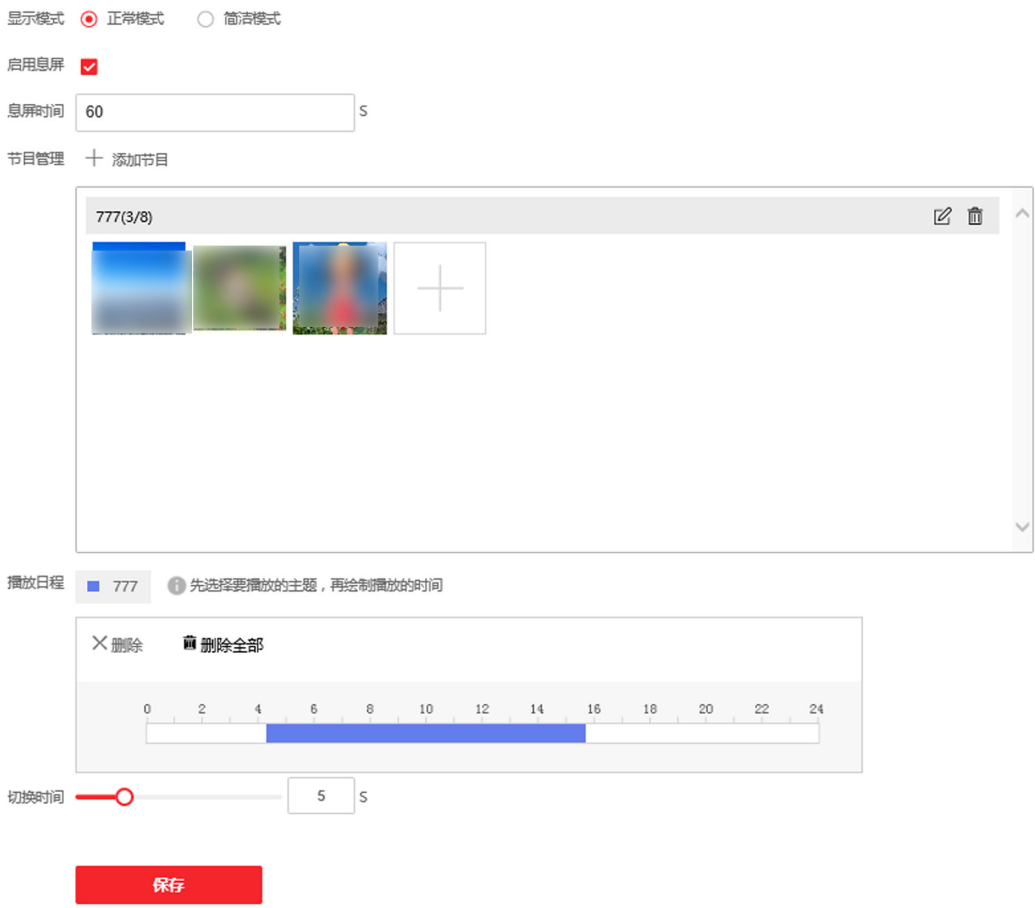


图 9-14 主题配置

3. 可配置设备认证时的**显示模式**。可选择*简洁模式*或*正常模式*。若选择*简洁模式*，认证界面预览关闭，认证时不显示认证人员的姓名、工号、人脸图片等信息。

4. 勾选*启用息屏*，并配置息屏时间，若设备在配置的时间内无操作，则开始播放待机图片。

5. 添加节目。

说明

目前仅支持添加一个节目。

6. 在素材管理模块中，单击+选择媒体库中上传的文件，并单击*确定*。

7. 单击素材管理模块右上角的 可创建或修改节目名称，节目名称将显示在播放日程中。

8. 配置播放日程。

1) 在播放日程模块中选择一个需要播放的主题。

2) 在时间轴中拖动时间条，配置图片播放的时间。

3) **可选操作**: 选中时间段，可编辑时间段开始和结束时间，单击*保存*或*删除*以保存或删除时间段。

4) **可选操作**: 选中时间段并单击*删除*可删除配置的时间段，或单击*删除全部*，将所有配置删除。

9. 拖动滑块或直接输入数值配置图片切换时间。

10. 单击*保存*。

第 10 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。

官网下载客户端软件，运行客户端软件。

10.1 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。

10.1.1 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 10-1 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。

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*。

10.1.2 查看设备状态

已添加成功的设备，通过客户端软件可以查看设备状态信息。

前提条件

已成功添加设备到客户端。

操作步骤

1. 在设备管理界面，选择*设备*页签。

2. 设备类型区域选择**海康设备**。

3. 在**管理的设备**列表中，选择设备，单击*设备状态*。

4. 打开**设备状态**窗口，查看设备状态信息。

说明

- 单击*刷新*可实时查看最新状态。
- 不支持断网录像的设备其断网录像值显示为“N/A”。
- 不同设备类型显示的状态信息不同，请以实际界面为准。例如：门禁设备可查看设备门状态、主机状态、读卡器状态、报警输入口状态、报警输出口状态、事件传感器状态、布防状态、闸机本地拨码信息、闸机总体状态、闸机红外对射状态以及闸机器件状态。

10.2 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。

10.2.1 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。

10.2.2 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。

10.3 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。

10.3.1 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 和 *批量导入/导出人员* 。

10.3.2 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（CSV/Excel 文件）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。

10.3.3 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。

前提条件

请确保待获取信息的门禁设备已添加至当前客户端，或确保带获取信息的多功能采集仪能够正常使用。

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. 选中一台已配置人员的门禁设备或多功能采集仪，将该设备的人员信息导入该组织中。

说明

- 若选择多功能采集仪，需点击*登录*，配置设备的 IP 地址、端口、用户名和密码。
- 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 16000 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。

10.3.4 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。

10.3.5 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。

10.4 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*。

10.4.1 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*。

10.4.2 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 10-2 查看下发状态

10.4.3 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、读卡器信息等。

配置门禁设备参数

配置门禁设备参数，启用门禁设备可选功能，如语音提示、图片上传等。

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. 在左侧功能区域，选择 *高级配置 → 设备参数* 。

3. 选择门禁设备，配置设备参数信息。

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。

是否允许按键输入卡号

支持手动输入门口卡号，识别后可开启门。

NFC 使能

为防止手机获取门禁设备数据，出现非法通行情况。通过启用 NFC 功能，使门禁设备访问受保护。

M1 卡使能

启用 M1 卡后，设备可识别 M1 卡，用户可在设备上刷 M1 卡。

EM 卡使能

启用 EM 卡后，设备可识别 EM 卡，用户可在设备上刷 EM 卡。

CPU 卡使能

启用 CPU 卡后，设备可识别 CPU 卡，用户可在设备上刷 CPU 卡。

ID 卡使能

启用 ID 卡后，设备可识别 ID 卡，用户可在设备上刷 ID 卡。

人脸识别模式

普通模式

设备通过摄像头进行人脸识别。

深度模式

适用于较为复杂的环境，识别的人群范围更广。

显示人脸检测图片

在认证时，设备界面上会显示检测到的人脸图片。

显示卡号

在认证时，设备界面上会显示认证的卡号。

显示用户信息

在认证时，设备界面上会显示正在认证的用户信息。

图片中叠加用户信息

用户信息将显示在抓拍到的图片中。

语音提示

设备的语音提示功能将被开启。

联动抓拍是否上传图片

联动抓拍到的图片将上传到客户端。

保存联动抓拍图片

联动抓拍到的图片将保存到设备。可在客户端的事件搜索中查看抓拍的图片。

是否启用 Wi-Fi 探针

设备的 Wi-Fi 探针功能将被开启，可获取一定范围内已开启 Wi-Fi 的设备信息。

3G4G 使能

设备的 3G/4G 网络功能将被开启。

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。

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。

门磁

可控制门磁常开或者常闭。正常情况下应处于常闭状态（特殊需求除外）。

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。

开门超时报警

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。

关门延迟时间

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开启时间。

是否启用闭门回锁

启用该功能，则开门后没有达到门锁动作时间，闭门之后门锁也会立即锁定。禁用则不会在闭门之后立即锁定。

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

门禁点报警时输入解除码即可解除报警。

说明

- 单击***更多配置***，可设置**关门延迟时间**、**是否启用闭门回锁**、**胁迫码**和**解除码**四项参数。
- 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。

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。

基本信息

别名

配置读卡器名称，方便用户识别。

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。

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）。

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。

是否启用读卡失败超次报警

启用该功能则表示重复刷卡失败次数超过限定值时，主机会自动生成报警事件。禁用该功能后，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。

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。

蜂鸣时间

触发报警后，持续蜂鸣报警的时间长度。

读卡器种类

查看读卡器类型。（只读）

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）

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。

指纹容量

允许录入的指纹数量。

已存在指纹容量

已经录入的指纹数量。

人脸信息

人脸识别超时时间

配置人脸识别超时时间。若识别时间超出配置的时间时，设备会有识别超时提示。

人脸识别间隔

在此处可配置两次人脸识别的时间间隔。

人脸 1:1 匹配阈值

人脸 1:1 比对时的匹配阈值。阈值越大，识别人脸时误识率越低，拒认率越高。范围 0~100。默认 60。

人脸 1:N 匹配阈值

人脸 1:N 匹配时的匹配阀值。阈值越大，识别人脸时误识率越低，拒认率越高。范围：0~100。默认 60。

真人检测

选择是否开启检测真人人脸功能。开启此功能后，设备可判断是否为真实的人脸。若检测的人脸不是真实的人脸，则认证失败。

人脸 1:1 识别安全等级

脸 1:1 匹配时，可从普通、高、极高三个等级中选择安全等级。等级越高，误识率越低，拒认率越高。

人脸 1:N 识别安全等级

人脸 1:N 匹配时，可从普通、高、极高三个等级中选择安全等级。等级越高，误识率越低，拒认率越高。

最大人脸认证失败次数

反复认证人脸超过所设次数，则认证图像会被锁定 5 分钟。主要用于判断是否为真人，避免图片重复认证。

锁定认证失败的人脸

启用后，人脸认证失败，认证图像会被锁定。

人脸识别环境模式

根据实际情况可选择人脸识别时的环境，可选择室内或者其他证件。

说明

部分参数可通过*更多参数*进行设置。

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。

配置报警输入

支持从设备获取报警输入，配置报警输入参数，并为其进行布撤防操作并下发。

前提条件

已添加门禁设备，并确保设备支持报警输入。

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 个报警输入。
4. 设置报警输入参数，包括名称、探测器类型、防区类型、灵敏度和联动报警输出。
5. 单击*确定*。

说明

布防状态下无法保存修改后的参数，请先将其设置为撤防状态。

6. 可选操作: 配置完成后，单击布防或撤防开关，可以为该报警输入进行布防或撤防操作。

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。

10.4.4 配置更多参数

添加门禁设备后，可以为其配置相关参数。

配置终端参数

支持通过客户端配置设备的终端参数。

操作步骤

说明

- 该功能需设备支持。
- 部分参数项需设备支持，请以实际界面显示的参数项为准。

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。

4. 单击*终端参数*并配置相关参数。

人脸算法库

目前仅支持深度学习算法库。

保存认证图片

启用后，认证时的图片信息将存储到设备中。

环保模式

启用环保模式后，在弱光或无光环境下，可进行人脸比对。可配置环保切换阈值、环保模式（1:N）及环保模式（1:1）。

说明

仅普通模式下支持环保模式。

环保模式人脸比对阈值 1:1

进行人脸 1:1 匹配时的匹配阀值。阈值越大，识别人脸时误识率越低，拒认率越高。最大可填 100。

说明

仅普通模式下支持环保模式。

环境模式人脸比对阈值 1:N

进行人脸 1:N 匹配时的匹配阀值。阈值越大，识别人脸时误识率越低，拒认率越高。最大可填 100。

说明

仅普通模式下支持环保模式。

环保模式切换阈值

启用环保模式后，需配置环保切换阈值，阈值越大，设备越容易进入环保模式；阈值越小，越不容易进入环保模式。阈值与光照强度有关。阈值范围为：0 ~ 8。

说明

仅普通模式下支持环保模式。

认证工作模式

配置设备的工作模式为门禁模式。

门禁模式为普通模式，需验证卡片或身份证权限访客通过。

5. 单击*保存*。

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 。

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）时，需要配置 RS-485 参数。

操作步骤

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. 根据实际需求选择串口号和 RS-485 连接模式。

6. 单击*保存*。

说明

配置 RS-485 参数后，重启设备以生效。

配置韦根参数

支持通过客户端配置设备的韦根参数，用以设备通过韦根通讯外接读卡器。

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。
4. 单击*韦根配置*。
5. 设置韦根编号。
6. 选择**通信方向**为**接收**或**发送**。

说明

若**通信方向**选择**发送**，需要设置**韦根模式**为**韦根 26** 或**韦根 34**。

7. 勾选自用韦根，设备启用配置的韦根参数。
8. 单击*保存*。

10.4.5 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

通过客户端可以远程控制门禁设备的门状态，包括开门、关门、常开、常闭、一键常开、一键常闭等。

前提条件

- 确保已分配门禁权限到人员，使其获取通行门禁点的权限。详情请参见 *分配门禁权限* 。
- 确保操作用户拥有对门禁点的控制权限。权限配置可参见客户端用户手册中的*添加用户*。

操作步骤

1. 进入*状态监控*界面。
2. 在**门禁分组**下拉列表中，选择门所在的分组。
3. 选择一个或多个门（按住 Ctrl 键可多选）。
4. 执行以下操作。

开门	若门是关门状态，单击*开门*将门打开。一段时间后，门会自动关闭。
关门	若门是开门状态，单击*关门*将门关闭。具有访问权限的人员可以使用凭证（如刷卡、人脸、指纹等）通过。
常开	单击*常开*，则门一直呈开门状态，所有人员无需使用凭证即可通过。
常闭	单击*常闭*，则门一直呈关闭状态，任何人（超级用户除外）都无法开门。
一键常开	单击*一键常开*，同时将分组下的所有门设置为常开状态。
一键常关	单击*一键常关*，同时将分组下的所有门设置为常闭状态。
抓图	单击*抓图*，触发该设备的监控点抓拍图片。

说明

该功能需要设备支持，且同时只能对一个设备进行抓图。

操作成功后，门的图标状态会发生对应改变。

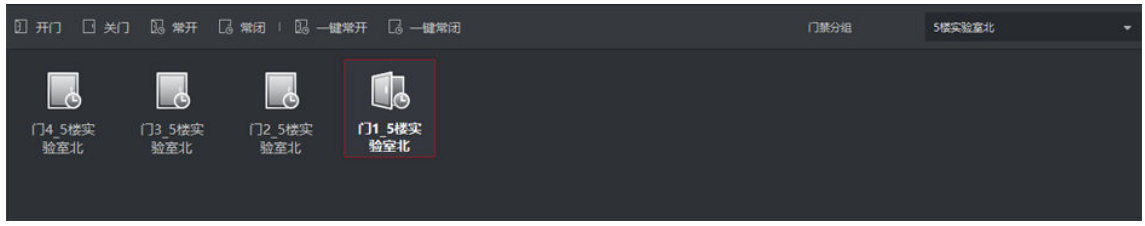


图 10-3 控制门状态

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

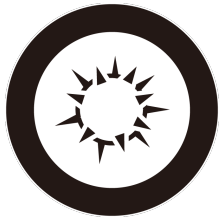
当移动光标到事件列表与人员模块中间时，光标变为双向箭头，此时向左或向右移动，可调整事件列表与人员模块之间的宽度。

附录 A. 安装环境注意事项

1. 安装环境光源参考值：

蜡烛：10 Lux

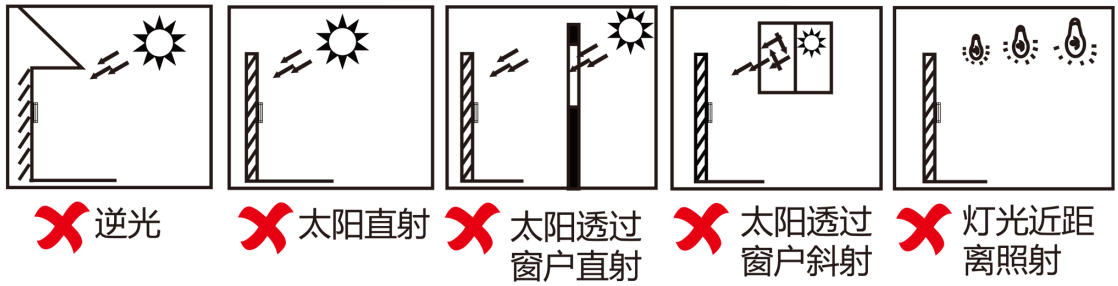
灯泡：100 ~ 850 Lux



日光：大于 1200Lux

2. 请将设备安装在室内。

3. 避免逆光、阳光直射、阳光透过窗户直射、阳光透过窗户斜射、灯光近距离照射。



附录 B. 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。

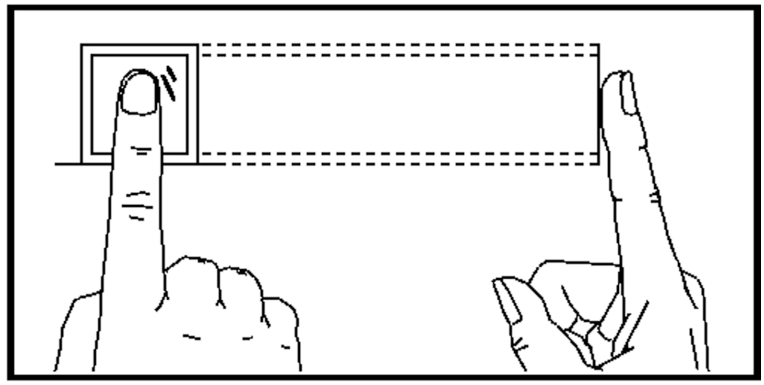


图 B-1 手指按压示意图

- 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。

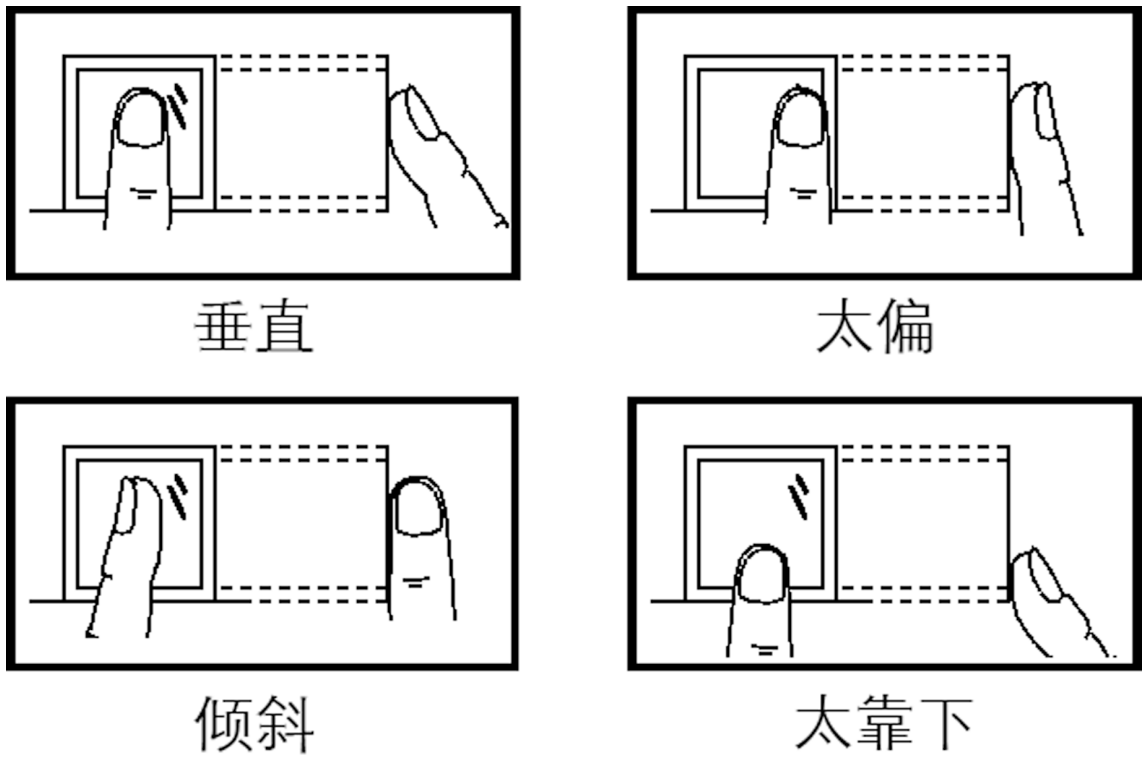


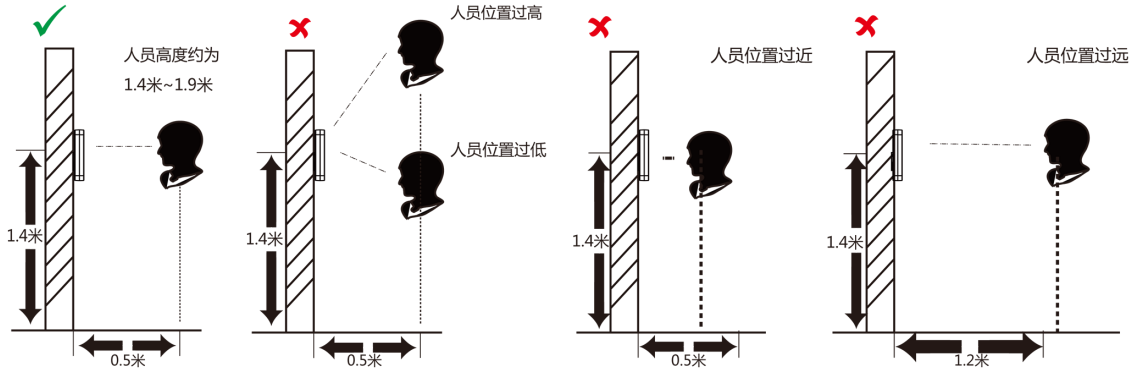
图 B-2 错误的按压方式

- 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。
- 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 C. 人脸识别注意事项

人脸录入/比对位置

人脸录入/比对位置如下图所示（以站距 0.5 m 为例）：



人脸录入/比对姿势

人脸表情

为保证人脸参数录入质量以及比对精确度，请务必在录入/比对过程中，保持自然的表情（如下图所示）。

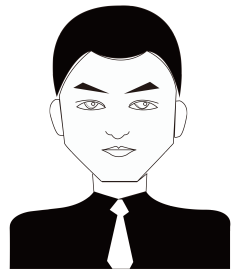


图 C-1 人脸自然表情

人脸姿势

为保证人脸参数录入质量以及比对精确度，请务必在录入/比对过程中，保证人脸正对录入窗口。

人脸录入/比对姿势说明图如下所示：

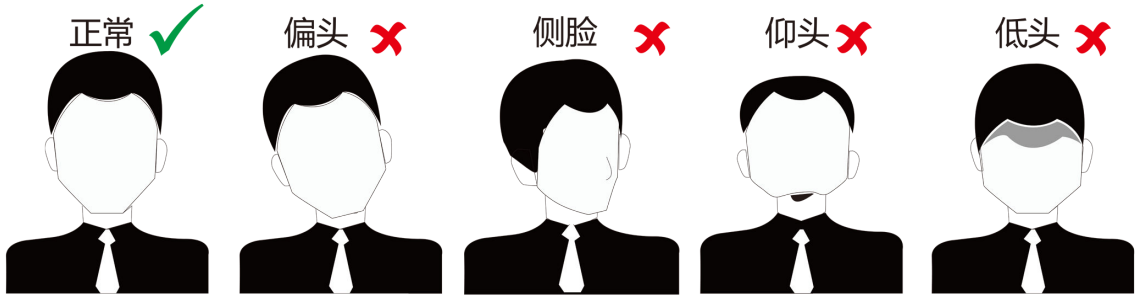


图 C-2 人脸录入/比对姿势示意图

人脸大小调整

在登记过程中，请您尽量使人脸位于窗口中心位置。

人脸大小调整示意图如下所示：

图 C-3 人脸大小调整示意图

附录 D. 尺寸图

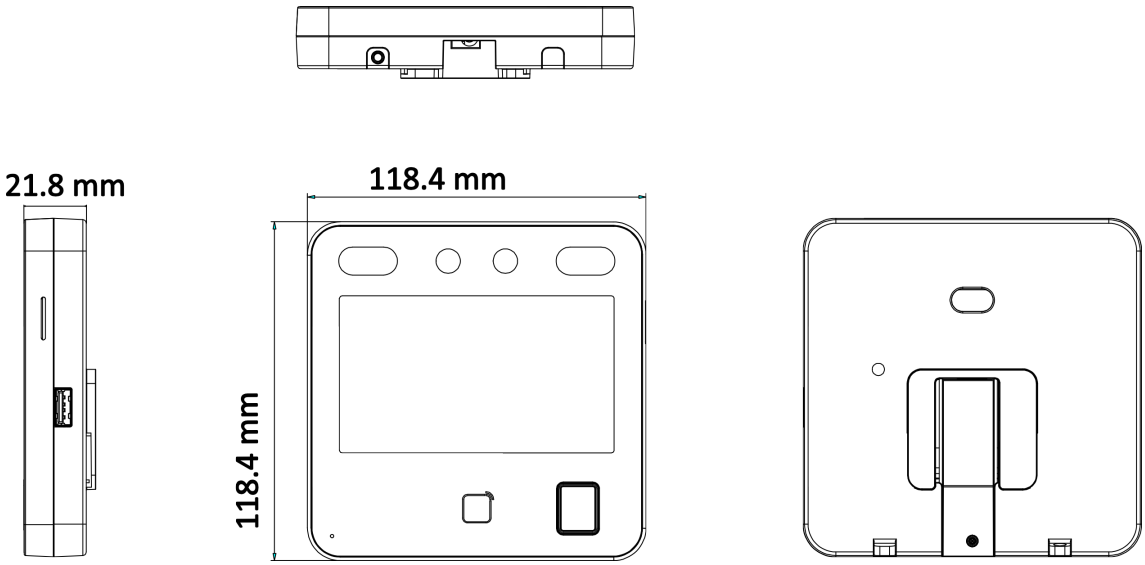


图 D-1 尺寸图（带指纹）

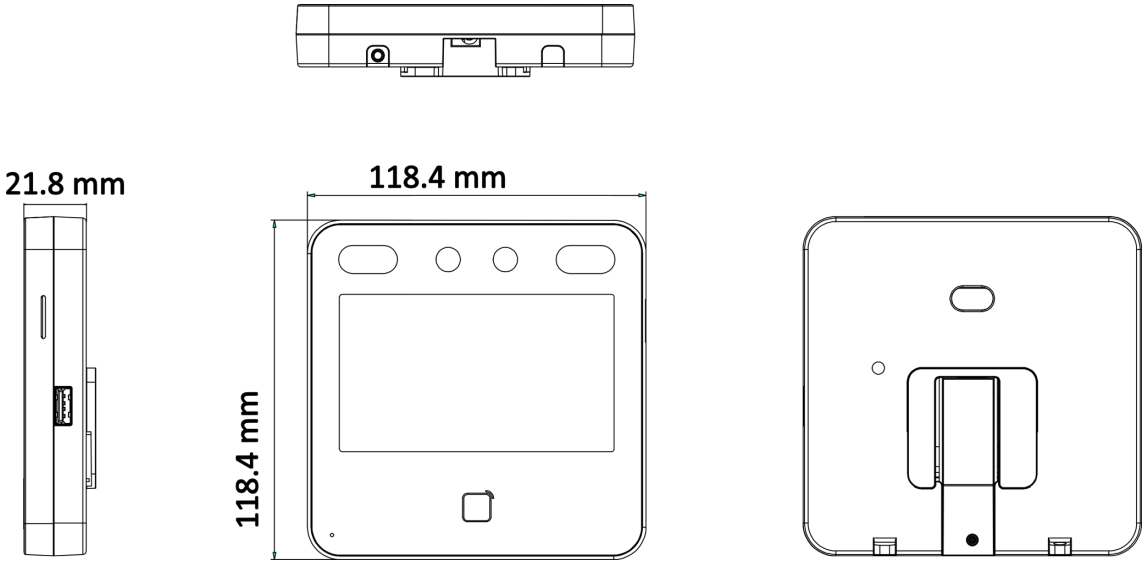


图 D-2 尺寸图（无指纹）

附录 E. 参数信息

型号	D13 Plus	D13 Pro	D13 S	D13
操作系统	Linux			
显示屏	4.3 英寸			
存储容量	4 GB			
指纹容量	500	500	/	/
人脸容量	500 张人脸			
事件容量	100，000			
抓拍图片容量	20，000 张			
人脸比对时间	1:N 比对时间＜ 0.2 s/人			
人脸识别距离	0.3 m ~ 2 m			
Wi-Fi	支持	/	支持	/
物理接口	USB2.0 × 1，网口×1，RS-485 × 1，韦根×1，门磁输入×1，门锁输出×1，开门按钮×1，防拆×1，外接排线接口×1（包含电源接口）			
摄像头	200 万像素双目摄像头			
设备电源	DC 12 V, 1 A			
相对湿度	0%至 90%（在不凝结水滴状态下）			
工作温度	-10 °C ~ 40 °C			
使用环境	室内			
尺寸 （宽 × 高 × 深）	118 mm × 118 mm × 20 mm			

附录 F. 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 F-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 F-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

UD27262B