HIKVISION

测温人脸识别终端

用户手册

法律声明

版权所有©杭州海康威视数字技术股份有限公司 2020。保留一切权利。

本手册的任何部分，包括文字、图片、图形等均归属于杭州海康威视数字技术股份有限公司或其关联公司（以下简称“海康威视”）。未经书面许可，任何单位或个人不得以任何方式摘录、复制、翻译、修改本手册的全部或部分。除非另有约定，海康威视不对本手册提供任何明示或默示的声明或保证。

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

- 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。
- 请不要将多个设备连接至同一电源适配器。
- 在接线、拆装等操作时请一定要将电源断开，切勿带电操作。
- 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。
- 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。
- 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）。

⚠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。
- 用错误型号的电池更换会有爆炸危险，务必按照说明处置用完的电池。
- 请使用符合 LPS 标准的适配器。

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
测温人脸识别终端	DS-K1T6Q-F70-3XF/TB

目 录

第 1 章 产品概述 1
1.1 产品简介 1
1.2 产品功能 1
第 2 章 外观介绍 2
第 3 章 安装说明 4
3.1 安装环境 4
3.2 嵌入式安装 4
3.3 明装 6
第 4 章 接线说明 9
4.1 接线端子说明 9
4.2 外接普通设备说明 11
4.3 外接门控安全模块说明 12
4.4 外接消防模块说明 13
4.4.1 断电开锁型接线说明 13
4.4.2 断电上锁型接线说明 15
第 5 章 激活 17
5.1 通过 SADP 软件激活设备 17
5.2 通过客户端软件激活设备 18
第 6 章 海康云眸操作 20
6.1 网页端管理 20
6.1.1 人员管理 20
6.1.2 卡片管理 22
6.1.3 门禁管理 23
6.1.4 查看设备信息 24
6.2 云眸社区客户端操作（物业） 24
6.2.1 用户管理 24

6.2.2 设备管理 26
6.2.3 住户审核 27
6.2.4 一键开门 28
6.2.5 预览 28
6.2.6 消息查看 29
6.3 云眸社区客户端操作（业主） 30
6.3.1 用户管理 31
6.3.2 房屋管理 33
6.3.3 住户审核 33
6.3.4 一键开门 34
6.3.5 消息查看 34
第 7 章 客户端软件配置 36
7.1 设备管理 36
7.1.1 添加设备 36
7.1.2 重置/恢复密码 41
7.1.3 分组管理 41
7.2 人员管理 43
7.2.1 添加组织 43
7.2.2 添加单个人员 44
7.2.3 批量导入/导出人员 53
7.2.4 从设备获取人员信息 55
7.2.5 更换人员所在组织 55
7.2.6 批量发卡 55
7.2.7 卡片挂失 56
7.3 门禁配置 57
7.3.1 计划模板 57
7.3.2 分配门禁权限 59
7.3.3 高级配置 60

7.3.4 配置更多参数 70
7.3.5 门禁事件配置 75
7.3.6 状态监控 78
7.4 事件中心 80
7.4.1 设备布撤防控制 80
7.4.2 查看实时事件 81
7.4.3 搜索历史事件 82
7.5 考勤管理 83
7.5.1 考勤参数设置 83
7.5.2 添加常规时间段 90
7.5.3 添加班次 92
7.5.4 排班管理 94
7.5.5 考勤处理 97
7.5.6 计算考勤数据 99
7.5.7 考勤统计 100
7.6 远程配置（网页端） 103
7.6.1 查看设备信息 103
7.6.2 修改设备密码 103
7.6.3 时间管理 104
7.6.4 系统维护 105
7.6.5 配置 RS-485 参数 105
7.6.6 安全模式选择 106
7.6.7 配置网络参数 106
7.6.8 上报策略配置 108
7.6.9 网络中心参数配置 108
7.6.10 配置 Wi-Fi 108
7.6.11 配置继电器参数 109
7.6.12 配置门禁参数 109

7.6.13 配置人证设备参数 110
7.6.14 配置人脸参数 111
7.6.15 配置补光灯参数 112
7.6.16 配置设备编号 112
7.6.17 配置视音频参数 113
7.6.18 继电器操作 113
7.6.19 查看状态 113
附录 A. 人脸识别注意事项 114
附录 B. 安装环境注意事项 116
附录 C. 尺寸图 118
附录 D. 技术参数 119
附录 E. 通信矩阵和设备命令 121

第 1 章 产品概述

1.1 产品简介

测温人脸识别终端是一款人脸识别类门禁考勤一体化产品。集成人员身份验证及体温检测模块，采用非接触式测温实现体温快速检测，人员身份信息与体温数据关联汇聚中心有效保障防控安全，可广泛应用于企业、车站、园区、场馆、工厂等场景，实现人员权限管理及体温监控，满足保障防疫防控要求。

1.2 产品功能

- 支持测温模式和快速测温模式（人脸检测+测温）。
- 支持配置身份验证+测温的验证方式：支持刷卡+测温、人脸识别+测温、刷卡+人脸+测温等多种验证方式。
- 支持配置快速测温模式（人脸检测+测温），即支持检测到人脸（不做身份验证）就做体温检测。
- 可配置提醒戴口罩、强制戴口罩。
- 支持配置体温检测报警阈值以及异常体温是否控制开门放行。
- 支持设备唤醒功能，当有人员靠近时，设备自动唤醒。

第 2 章 外观介绍

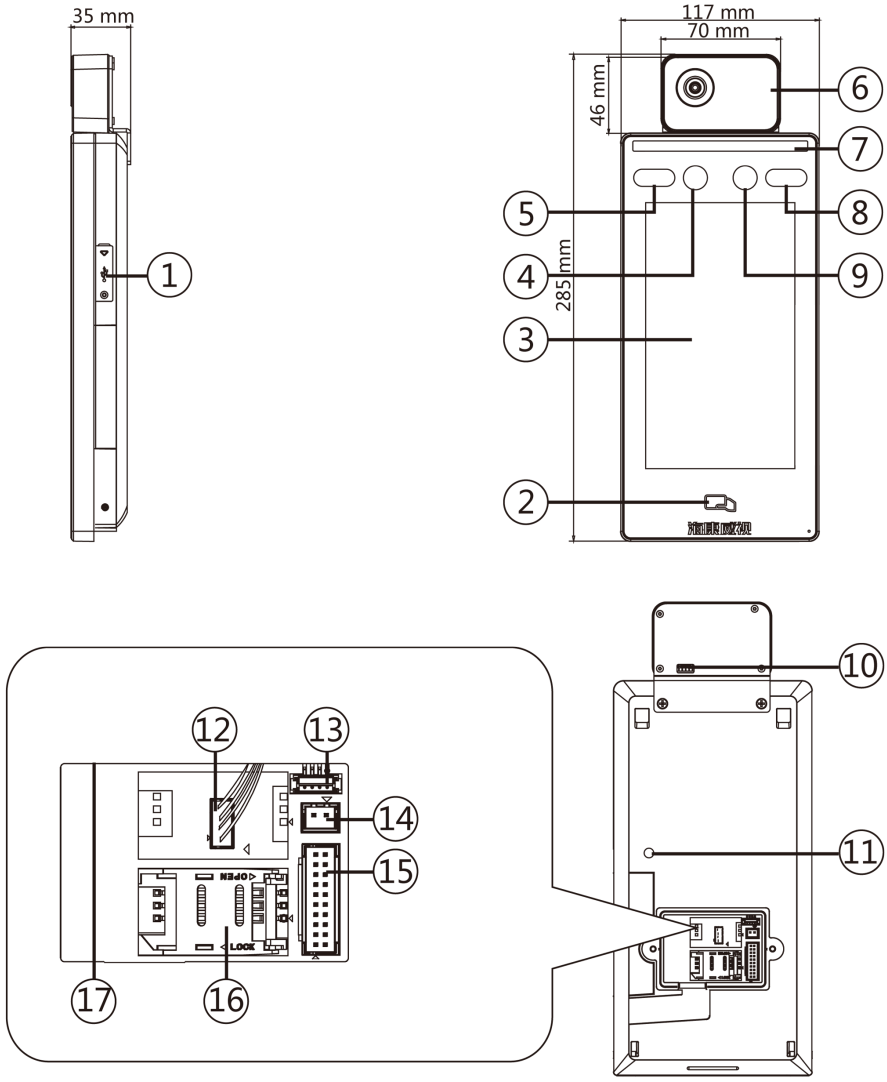


图 2-1 外观说明图

表 2-1 外观说明表

部件序号	名称	说明
1	USB 接口	连接 U 盘。
2	刷卡区域	在此处刷卡。
3	显示屏	7 寸显示屏。

部件序号	名称	说明
4	摄像头	拍摄图像或录像。
5	红外补光灯	为摄像头补红外光。
6	测温模块	测量被测目标温度。
7	白光补光灯	为可见光摄像头补光。
8	红外补光灯	为摄像头补红外光。
9	摄像头	拍摄图像或录像。
10	测温模块接口	（已连接）连接测温模块和设备主体。
11	防拆	防拆按钮。设备被暴力拆卸时，设备报警。
12	测温模块接口	（已连接）连接测温模块和设备主体。
13	调试串口	仅供调试时使用。
14	电源接口	通过此接口与电源连接。
15	外接排线	通过排线连接 RS-485 读卡器、韦根读卡器、门锁、报警输入、报警输出等外接设备。
16	PSAM 卡卡槽	预留
17	网口	通过此网口连接以太网。

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。
- 请知悉，阳光、风、空调冷暖风等易对人体体表温度和设备工作状态造成影响的外界因素可能导致测温偏差。为保证测温精度，请在室内无风环境使用（与外界相对隔离的区域），环境温度保持在 10° C ~35 ° C 之间。若无合适的室内环境（如正对室内并与室外连通区域、室外门口区域等），可在此区域搭建临时测温通道，为测温提供一个相对稳定的环境。
- 测温的影响因素：
  - 风：风可以带走人体体表热量，影响测温。
  - 汗：流汗是人体机制为保持体温而产生的一种降温方式，测温目标若有流汗，可能影响测温结果。
  - 冷空调：若室内温度较低，体表温度随之降低，可能影响测温结果。
  - 暖空调或暖气：若室内温度较高，体表温度随之升高，可能影响测温结果。
- 为确保测温模块工作正常，设备上电开机后需要预热 90 分钟以上。
- 具体安装注意事项请参见附录 *安装环境注意事项* 。

3.2 嵌入式安装

操作步骤

1. 在墙上开孔，并安装 86 盒。

说明

本产品出货不带 86 盒。

2. 将测温模块连接线绕过安装挂板后，将泡棉贴在安装挂板上，确保连接线夹在泡棉中心缝隙中。
3. 再用 4 枚配件包中的螺丝将安装挂板固定在 86 盒上。
4. 将外接设备线缆与排线线缆连接，整理线缆，确定出线方式。
5. 将设备自上而下扣挂在安装挂板上，并确保挂板下方突起部分插入设备背部凹槽处。

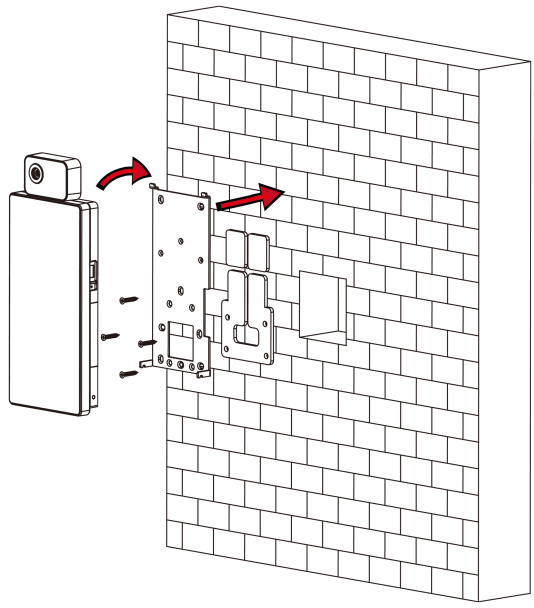


图 3-1 安装设备

6. 使用两枚紧固螺丝（SC-M4X14.5TP10-SUS）起入设备左右两侧的孔位，固定设备与安装挂板。

说明

螺丝旋入至头部与设备表面齐平即可将挂板固定。

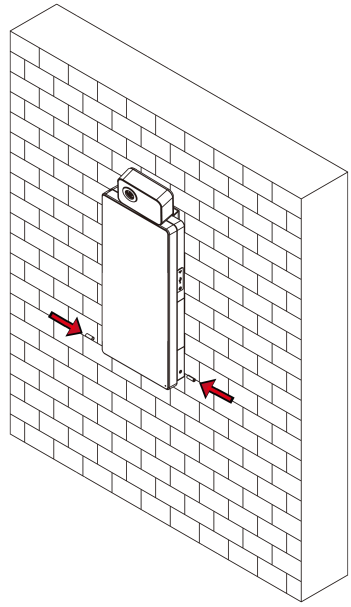


图 3-2 固定设备

3.3 明装

操作步骤

1. 根据安装贴纸上的基准线将安装贴纸贴在距离地面基准线 1.4 米处。

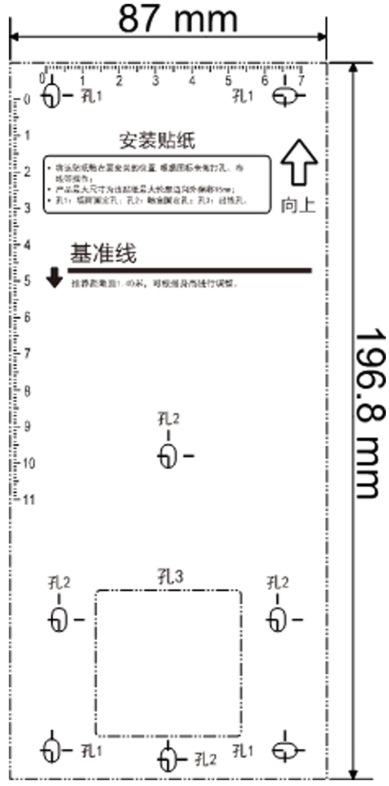


图 3-3 安装贴纸示意图

2. 根据安装贴纸上的打孔位置在墙上打 6 个孔。
3. 将提供的膨胀螺丝的塑料套筒插入打好的孔中。

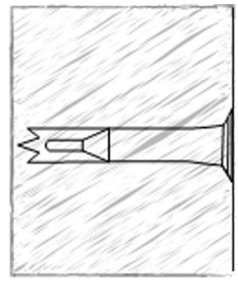


图 3-4 膨胀螺丝

4. 将挂板上的 6 个预留孔对准打好的孔，并起入螺丝固定挂板。
5. 将外接设备线缆与排线线缆连接，整理线缆，确定出线方式。
6. 将设备自上而下扣挂在安装挂板上，并确保挂板下方突起部分插入设备背部凹槽处。

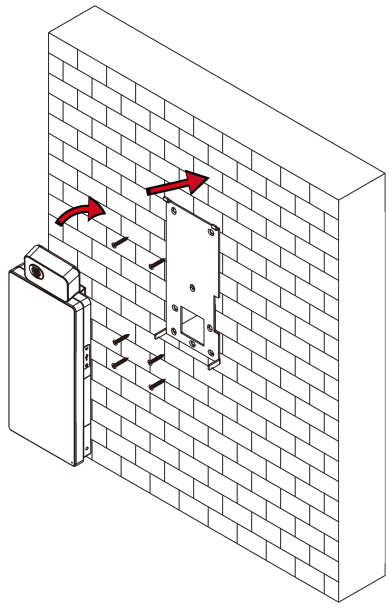


图 3-5 安装设备

7. 使用 2 枚螺丝（SC-M4X14.5TP10-SUS）起入设备左右两侧的孔位，固定设备与安装挂板。

说明

螺丝旋入至头部与设备表面齐平即可将挂板固定。

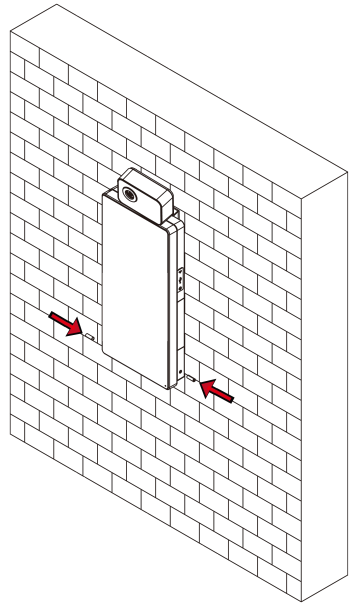


图 3-6 固定设备

说明

- 此处的安装高度 1.4 米为推荐安装高度，可根据身高情况自行调整。
- 为了更好的使用人脸识别终端设备，我们建议您使用产品自带的安装贴纸在墙上开孔，并安装设备。

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、报警设备等。

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 ALARM OUT 和 ALARM IN 端子连接报警输出设备和报警输入设备；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。

4.1 接线端子说明

设备的接线端子包括电源输入、报警输入、报警输出、RS-485、韦根输出和门锁。

线缆示意图如下所示：

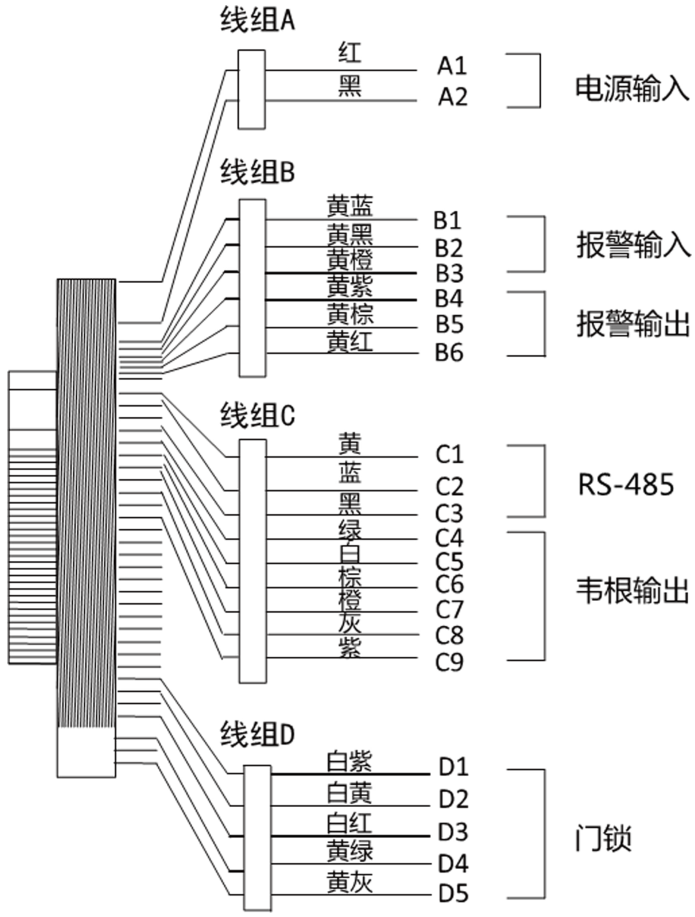


图 4-1 接线端子示意图

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	报警输入	黄蓝	IN1	报警输入 1
	B2		黄黑	GND	接地
	B3		黄橙	IN2	报警输入 2
	B4	报警输出	黄紫	NC	报警输出接线
	B5		黄棕	COM	

线组	序号	功能组	颜色	名称	端子说明
	B6		黄红	NO	
线组 C	C1	RS-485	黄	485+	RS-485 接线
	C2		蓝	485-	
	C3		黑	GND	接地
	C4	韦根输出	绿	W0	韦根数据线 0
	C5		白	W1	韦根数据线 1
	C6		棕	WG_OK	读卡器灯号控制输出（有效卡输出）
	C7		橙	WG_ERR	读卡器灯号控制输出（无效卡输出）
	C8		灰	TAMPER	读卡器防拆接线
	C9		紫	BUZZER	蜂鸣器控制线
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	SENSOR	门磁信号输入
	D5		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：

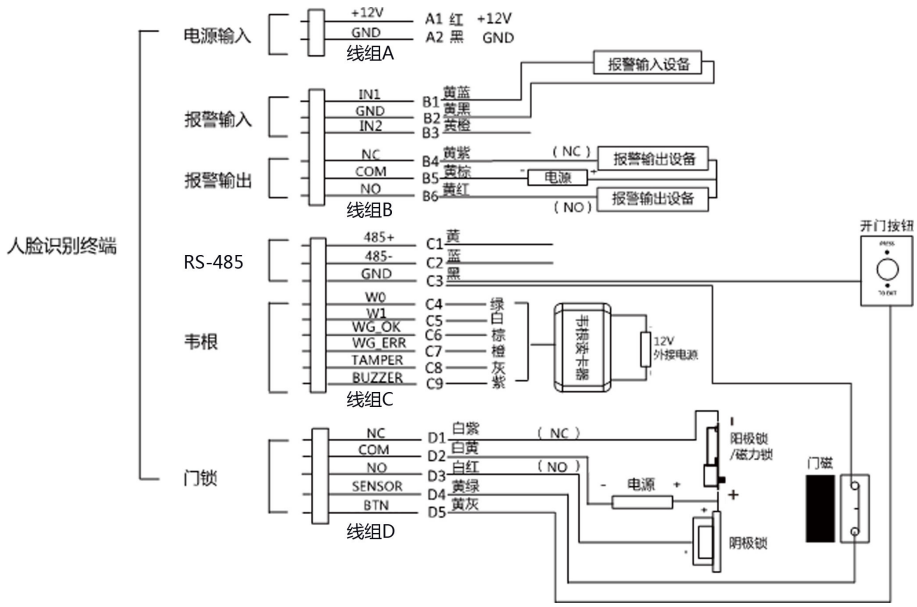


图 4-2 外接设备示意图

说明

- 外接门磁和开门按钮时，需要与 RS-485 或者电源共地。
- 图中所示的韦根接口为韦根输入接口，可连接韦根读卡器，此时需将韦根传输方向配置为“输入”。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。

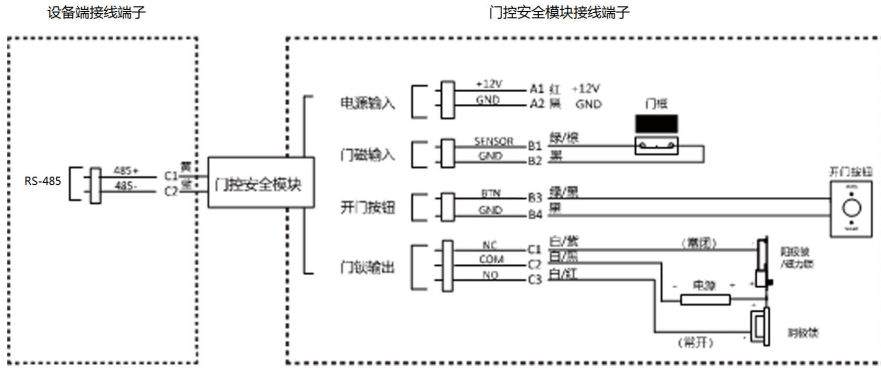


图 4-3 外接门控安全模块示意图

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：

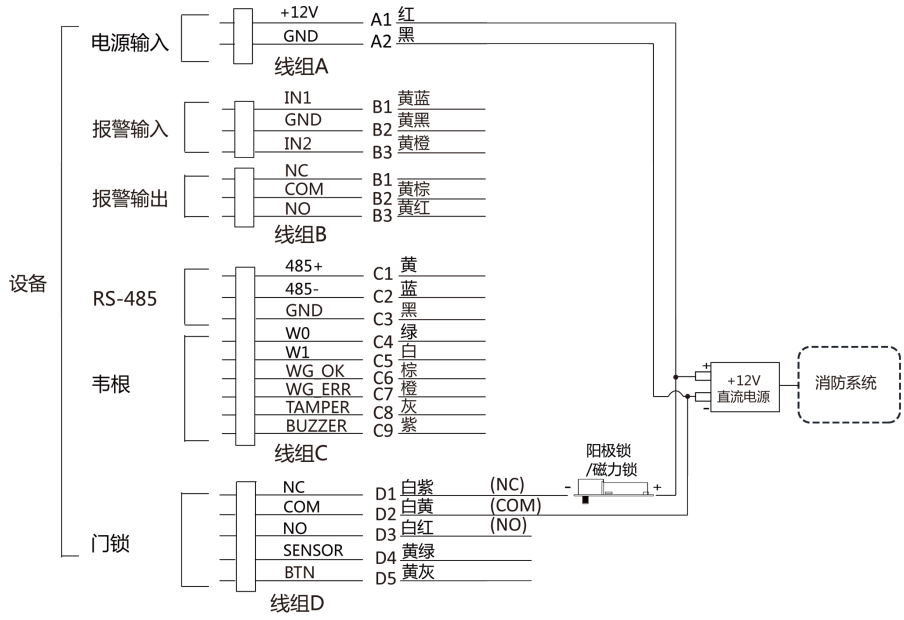


图 4-4 外接设备示意图

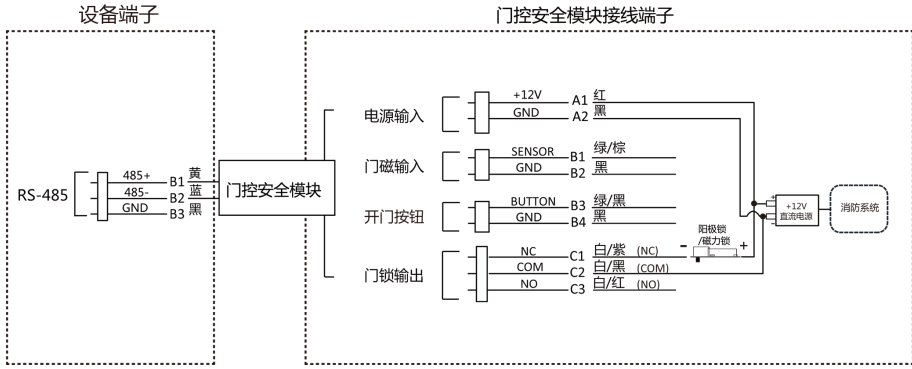


图 4-5 外接门控安全模块示意图

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：

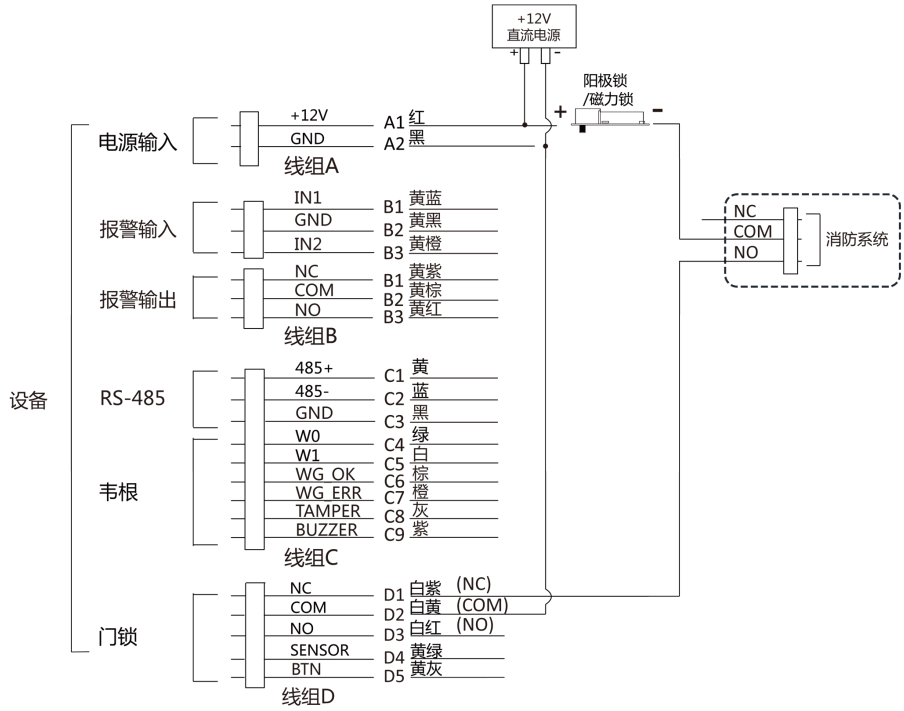


图 4-6 外接设备示意图

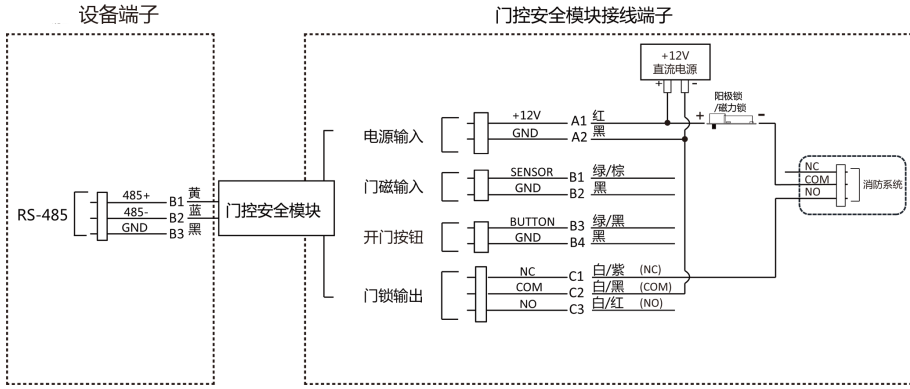


图 4-7 外接门控安全模块示意图

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：

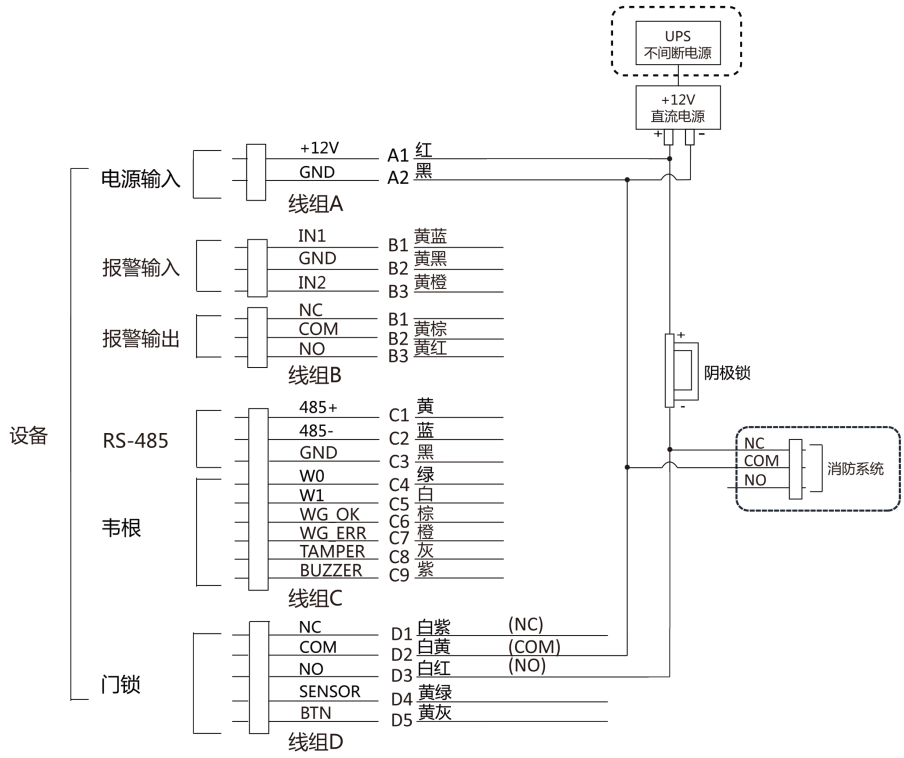


图 4-8 外接设备示意图

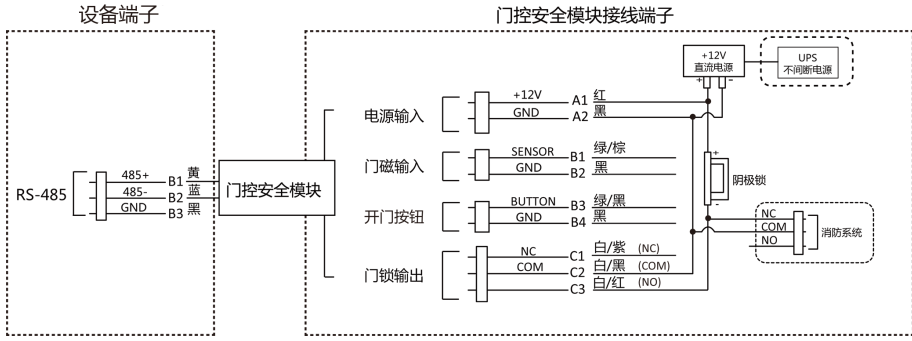


图 4-9 外接门控安全模块示意图

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：8000。
- 缺省用户名（管理员）：admin。

5.1 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 5-1 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。

5.2 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，单击 ***设备管理*** → ***设备*** → ***设备*** 进入设备界面。
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 6 章 海康云眸操作

海康云眸分为网页端和移动端。配合使用网页端和移动端，可有效管理社区、房屋、业主、家属和租户。

说明

仅部分设备支持云平台操作功能，请以具体型号为准。

6.1 网页端管理

物业公司通过网页端可管理下属的所有的小区、房屋、人员、权限和设备。还可发布信息，方便与业主沟通。

在管理人员、卡片、门禁设备、信息等操作前，需先注册并登录云眸网页端、添加社区和房屋。

在浏览器地址栏输入 *https://sq.hik-cloud.com/* 进入云眸网页端。

说明

- 在海康云眸中进行人员管理及权限下发配置后，请勿在客户端重复配置。
- 在海康云眸中进行人员管理及权限下发配置后，无法进行本地用户添加配置。

6.1.1 人员管理

操作步骤

1. 单击 *社区中心* → *人员管理* 并选择所在社区，进入人员管理界面。

图 6-1 人员管理界面

2. 单击*添加*，弹出添加人员界面。

图 6-2 添加人员

3. 配置人员基本信息及详细信息。
4. 单击*确定*完成添加。

编辑人员信息 单击 ，可修改人员信息。

人员开卡 单击 ，输入卡号，可为用户开卡。

删除人员 单击 ，根据提示单击*确定*可删除该人员。

5. **可选操作**：单击人员姓名，右侧弹框显示人员信息，可对该人员的卡片进行挂失、退卡和换卡操作。

6.1.2 卡片管理

操作步骤

1. 单击 *社区中心* → *卡片管理* ，进入卡片管理界面。

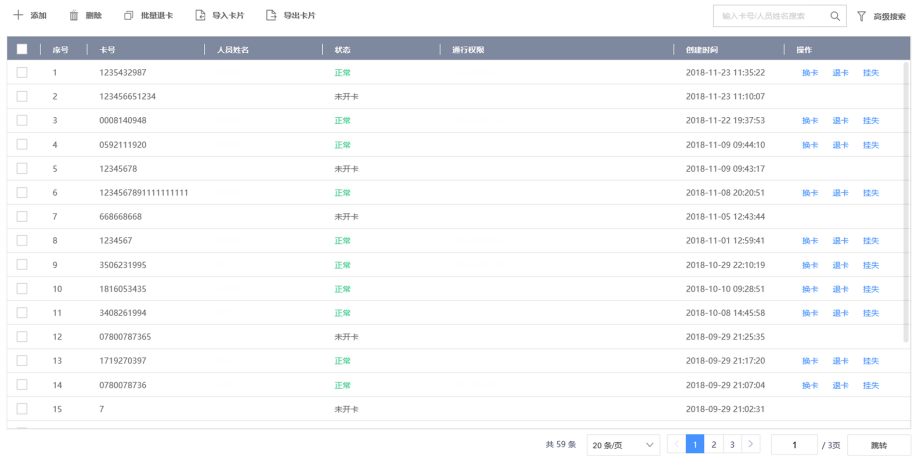


图 6-3 卡片管理界面

2. 单击*添加*并输入卡号，可添加空白卡片。

说明

刚添加的卡片状态为**未开卡**，当卡片状态为**正常**时，才可进行换卡、退卡、挂失操作。

3. 单击*导入卡片*，单击*浏览*，选择文件后，单击*确定*可将文件中的卡片数据导入到系统中。

说明

单击*下载模板*，可获取卡片数据模板。

4. 单击*导出卡片*，选择指定路径，可将系统中的卡片数据导出到指定路径。

换卡 选择卡片，单击*换卡*，并输入新卡卡号，可更换卡片。

退卡
- 选择卡片，单击*退卡*可对人员进行退卡。
- 勾选多个卡片，单击*批量退卡*，可对多个人员进行批量退卡。

挂失 选择卡片，单击*挂失*，可对卡片进行挂失。

6.1.3 门禁管理

操作步骤

1. 单击 *云门禁* → *门禁管理* 并选择区域。
2. 单击*门禁分组*，进入分组配置界面。

图 6-4 门禁管理

3. 单击*添加*，配置分组参数。
   1) 输入门禁分组名称。
   2) 单击*添加*，勾选门禁点，单击*确定*。

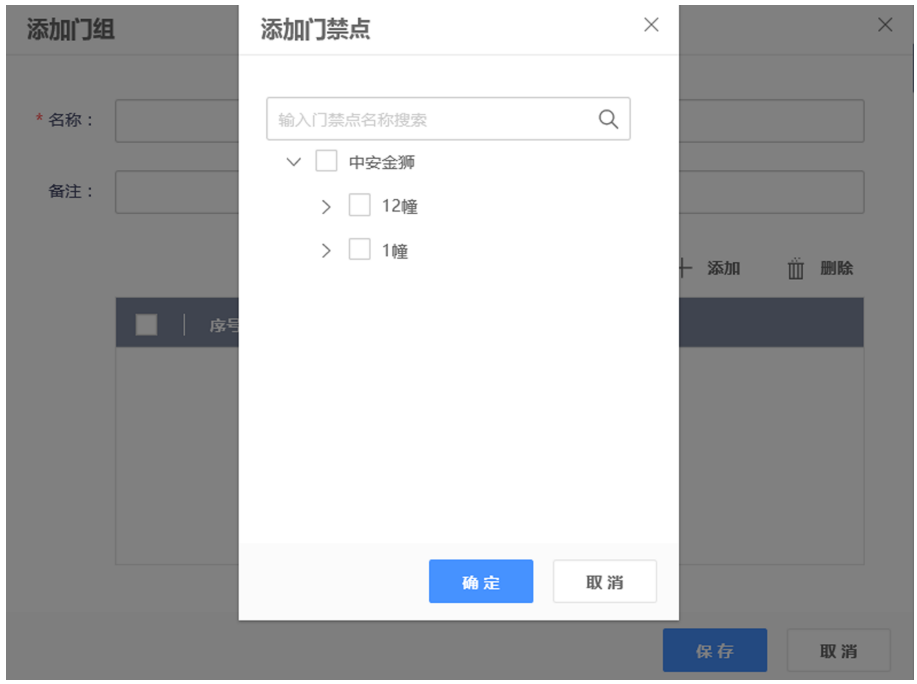


图 6-5 添加门组

4. **可选操作**：单击*编辑*，可修改分组参数。
5. 单击*门禁配置*，可配置设备/人员权限。
   1) 单击*添加权限*，选择授权方式，单击 *下一步*。
   2) 根据界面提示选择人员和门禁设备，并设置**权限有效期**，单击*完成*。

   删除权限　勾选需要删除的列表项，单击*删除权限*可批量删除。

   修改权限　选择需要修改的项，单击*编辑*，可对权限参数进行修改。
6. **可选操作**：在门禁配置界面中，单击门禁点，可查看卡片、人脸等信息下发状态。

6.1.4 查看设备信息

操作步骤

1. 单击 *系统管理* → *设备管理* ，并选择相应区域，进入设备信息查看界面。
2. 在此界面可查看区域中所有设备的**序列号**、**状态**、**名称**、**型号**、**设备类型**和**设备地址**。

6.2 云眸社区客户端操作（物业）

请先下载并安装“云眸·社区”物业版移动客户端。

登录云眸网页端，并单击 下载 APP 进行安装。

6.2.1 用户管理

可对人脸及密码等用户信息进行录入及修改。

人脸录入

前提条件

请先添加设备到客户端，并使用客户端下发权限到设备。

操作步骤

1. 点击 我的 → *我的人脸* ，进入人脸录入界面。

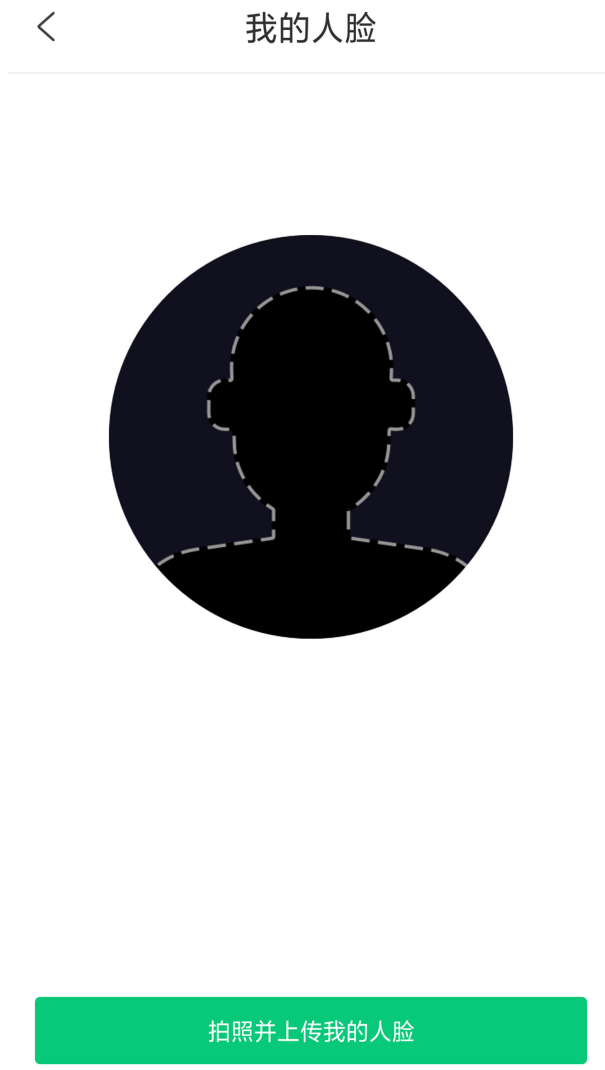


图 6-6 人脸录入

2. 点击*拍照并上传我的人脸*。
3. 按照界面提示框摆好姿势，点击相机图标进行拍照。

说明

拍照时，请保证光线充足，正面睁眼拍照。

4. 若拍摄照片不满意，可点击*重新上传*进行重新拍照。
5. 点击 完成录入。

结果说明

人脸录入后，可进行人脸开门。

密码修改

修改业主账户的密码，为确保您的账户安全，请定时更换密码。

操作步骤

1. 在客户端主界面中，点击 我的 → *密码修改* 。
2. 输入**旧密码**。
3. 输入**新密码**及**确认密码**。

> **说明**
> 密码必须包含字母、数字、特殊字符，且长度大于等于 8 位。

4. 点击*完成*修改。

6.2.2 设备管理

可对门禁设备和视频设备进行添加及修改。

操作步骤

1. 在客户端主界面中，点击*设备管理*。
2. 选择**门禁设备**。

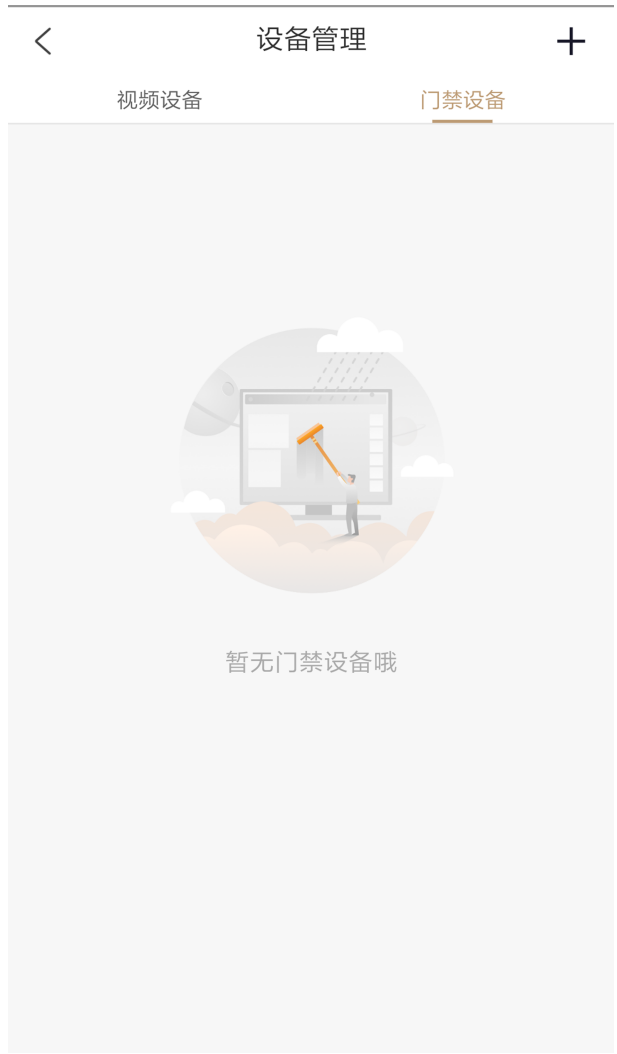


图 6-7 设备管理

3. 点击屏幕右上角+，添加设备。
   - 扫描设备二维码添加设备：扫描设备后背面板的二维码获取设备信息选择设备所属楼栋及单元，点击*确认提交*。
   - 手动添加设备：点击*手动输入*，输入设备名称、设备序列号、设备验证码，选择设备所属楼栋和单元，点击*确认提交*。
4. **可选操作**：点击设备右方...，可编辑或删除该设备。
5. **可选操作**：完成设备添加后，在主界面点击*社区视频*，可对设备进行预览。

6.2.3 住户审核

审核业主提交的房屋申请。

操作步骤

1. 在客户端主界面中，点击*住户审核*。
2. 在审核列表中选择待审核的申请单可查看申请单信息。

图 6-8 申请审核

3. 查看申请单信息后，选择设置门禁卡**失效时间**，点击*同意*通过申请。

说明

- 门禁卡失效时间不能早于生效时间。
- 若审核不通过，可点击*拒绝*驳回申请单。

6.2.4 一键开门

远程通过移动客户端开门。

前提条件

- 在进行远程开门前，需将设备添加至系统，详见 *设备管理* 。
- 在进行远程开门前，需在网页端给人员配置权限，详见 *门禁管理* 下的门禁权限配置。

操作步骤

1. 在客户端主界面中，点击*一键开门*，进入一键开门设备列表。
2. 点击对应设备进行一键开门。

6.2.5 预览

操作步骤

1. 在客户端主界面单击*社区视频*，进入视频预览界面。

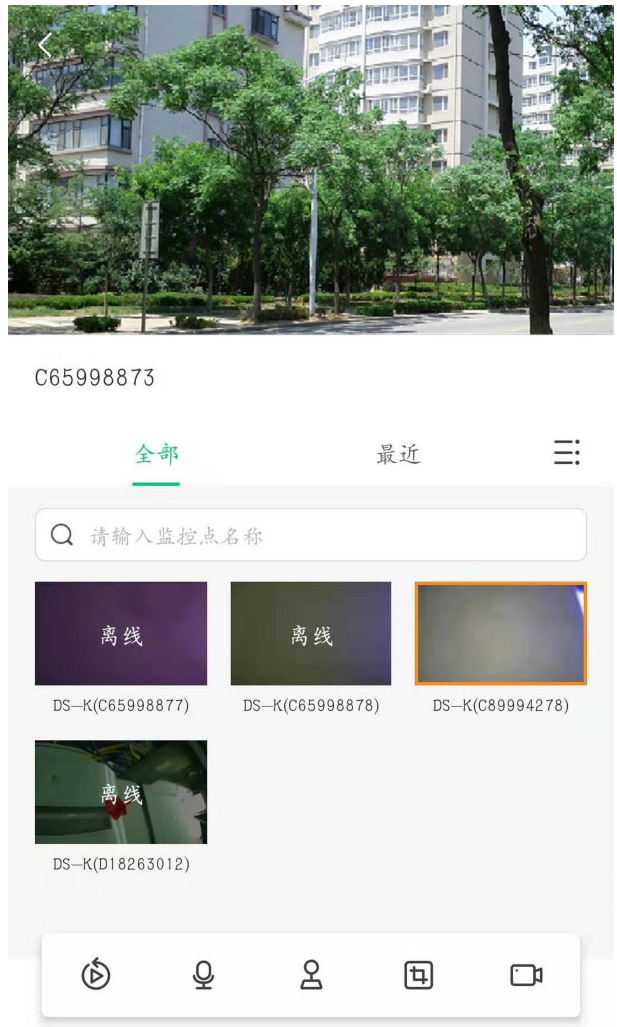


图 6-9 预览界面

2. 在此界面可预览设备。如设备支持，还可点击 进行抓图。

6.2.6 消息查看

操作步骤

1. 在客户端主界面中，点击右上角消息按钮，进入消息中心。

图 6-10 查看消息

2. 点击*系统消息*、*报警消息*或*社区公告*，可查看系统消息（房屋审核等）、设备报警消息及社区公告。

6.3 云眸社区客户端操作（业主）

请先下载并安装“云眸·社区”业主版移动客户端。

若手机系统为 iOS 系统，可从苹果商店搜索“云眸·社区”下载安装。

若手机系统为 Android 系统，可从应用商店中搜索“云眸·社区”下载安装。

6.3.1 用户管理

普通用户注册完成后，需进行实名认证，并可通过用户管理对人脸及密码等用户信息进行录入及修改。

实名认证

业主首次创建用户名密码，成功登录 App 后，需要对业主进行实名认证。

操作步骤

1. 在客户端主界面中，点击*实名认证*。
2. 点击界面上传位置补充信息。
   - 即时拍摄身份证正反面，并上传进行验证。
   - 从相册中获取并上传身份证正反面照片进行验证。
3. 设备将自动获取用户信息。
4. 点击*下一步*进行身份验证。

结果说明

实名验证通过后，客户端将显示**您已完成实名认证**。

人脸录入

前提条件

请先添加设备到客户端，并使用客户端下发权限到设备。

操作步骤

1. 点击 我的 → *我的人脸* ，进入人脸录入界面。

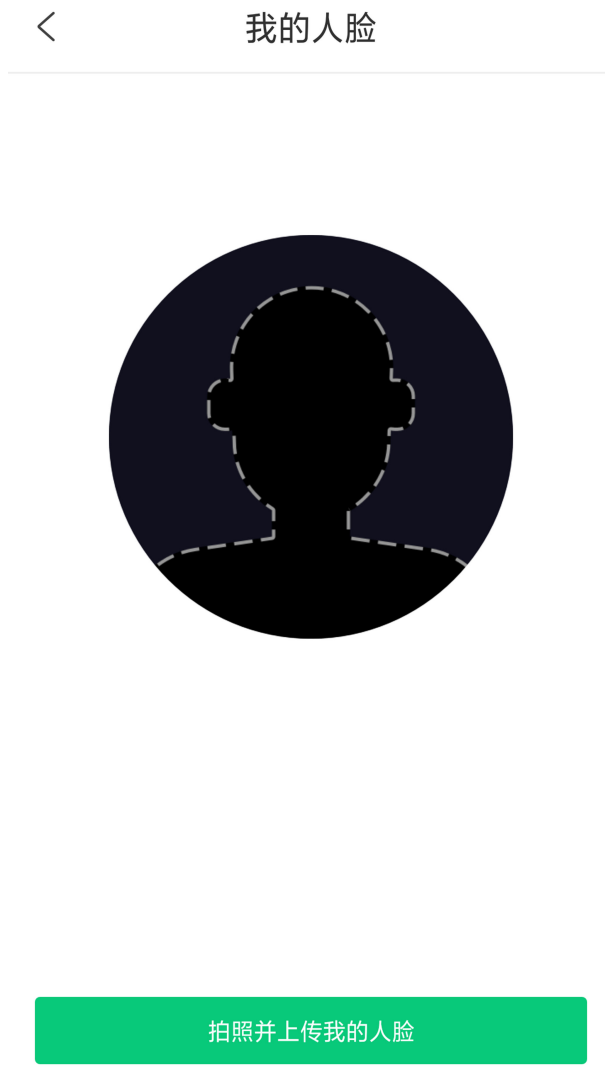


图 6-11 人脸录入

2. 点击*拍照并上传我的人脸*。
3. 按照界面提示框摆好姿势，点击相机图标进行拍照。

说明

拍照时，请保证光线充足，正面睁眼拍照。

4. 若拍摄照片不满意，可点击*重新上传*进行重新拍照。
5. 点击 完成录入。

结果说明

人脸录入后，可进行人脸开门。

密码修改

修改业主账户的密码，为确保您的账户安全，请定时更换密码。

操作步骤

1. 在客户端主界面中，点击 我的 → *密码修改* 。
2. 输入**旧密码**。
3. 输入**新密码**及**确认密码**。

> **说明**
> 密码必须包含字母、数字、特殊字符，且长度大于等于 8 位。

4. 点击*完成*修改。

6.3.2 房屋管理

前提条件

添加房屋前，请先完成业主实名认证。

操作步骤

1. 在客户端主界面中，点击*房屋管理*。
2. 点击*添加新房屋*。
3. 配置房屋所在**小区**及**楼栋房号**。
4. 设置身份为**业主**、**家属**或**租客**。
5. 选择**入住时间**。
6. 点击*确认提交*，等待审核通过后，房屋即添加成功。

> **说明**
> - 若身份为业主，等待物业审核通过后，房屋即可添加成功。
> - 若身份为家属或者租客，等待业主审核通过后，房屋即可添加成功。

7. **可选操作**：勾选需要删除的房屋，点击*删除房屋*，即可将其删除。

6.3.3 住户审核

审核家属或租户提交的房屋申请。

操作步骤

1. 在客户端主界面中，点击*住户审核*。
2. 在审核列表中，选择待审核的申请单。
3. 根据实际情况设置房屋入住时间、或租客租赁开始/结束时间，并点击*同意*或*拒绝*通过或驳回申请。

说明

门禁卡失效时间不能早于生效时间。

6.3.4 一键开门

远程通过移动客户端开门。

前提条件

- 在进行远程开门之前，需将设备添加至系统，详见 *设备管理* 。
- 在进行远程开门前，需在网页端给人员配置权限，详见 *门禁管理* 下的门禁权限配置。

操作步骤

1. 在客户端主界面中，点击*一键开门*，进入一键开门设备列表。
2. 点击对应设备进行一键开门。

6.3.5 消息查看

操作步骤

1. 在客户端主界面中，点击右上角消息按钮，进入消息中心。

图 6-12 查看消息

2. 点击*系统消息*、*报警消息*或*社区公告*，可查看系统消息（房屋审核等）、设备报警消息及社区公告。

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

客户端软件运行后，将设备添加到客户端，可以进行远程配置和管理。

说明

若需打开远程配置库，需要单击 ⚙ 。

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。

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。

通过 EHome 账号添加设备

支持通过 EHome 协议将设备添加到客户端上，无需固定 IP 地址。

操作步骤

1. 在维护与管理区域，单击 *设备管理* → *设备* 。
2. 单击*添加*。
3. 添加模式选择 EHome。
4. 设置参数。

   别名

   自定义设备名称。

   设备账号

   EHome 协议上注册的账户名称。

5. **可选操作**：勾选**同步设备时间**，保持设备时间与本地计算机时间一致。
6. **可选操作**：勾选**导入至分组**，可以通过设备别名创建一个组，并导入该设备的所有通道。
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设备。

说明

通过 EHome 方式添加到客户端的设备，不支持上传带有图片的事件至客户端，同时也不支持将人脸图片下发到设备。

8. **可选操作**：根据实际情况，可执行如下相关操作。

   查看设备状态 单击 ，可查看在线设备状态信息。

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。

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。

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。

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) 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

   • 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。

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、手机号码和该人员访问权限的有效期限等。

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。
3. 设置基本信息，包括人员姓名、性别、电子邮件、手机号码、有效期限、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。
4. 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。

添加普通卡

添加人员时，支持为人员添加普通卡。

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* → *卡片* 。

   说明

   - 若弹出添加智能卡窗口，请单击*发卡配置*，选择发卡类型为**普通卡**，保存并重新切换至添加普通卡窗口。
   - 一个人最多可添加 5 张卡，包括智能卡和普通卡。
4. 设置普通卡参数。
   1) 手动输入或通过单击*开始读取*自动获取卡号。
   2) 选择**卡类型**。

说明

不同设备支持的卡类型不同，请以实际界面可配置的参数为准。

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。

5. **可选操作**：单击*发卡配置*，配置相关参数。

模式

本地

连接发卡器，选择发卡器、卡号类型和扇区，卡片放在发卡器上，可获取卡号。

远程

在设备下拉列表选择一个门禁设备下的读卡器，可在读卡器上刷卡，使客户端获取卡号。

说明

客户端需对设备布防成功，否则无法采集到卡号。

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。

说明

建议加密第 13 扇区。

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。

添加的卡片将显示在卡片列表中。

7. **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

已连接身份证阅读器、指纹录入仪和读卡器。

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。

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。

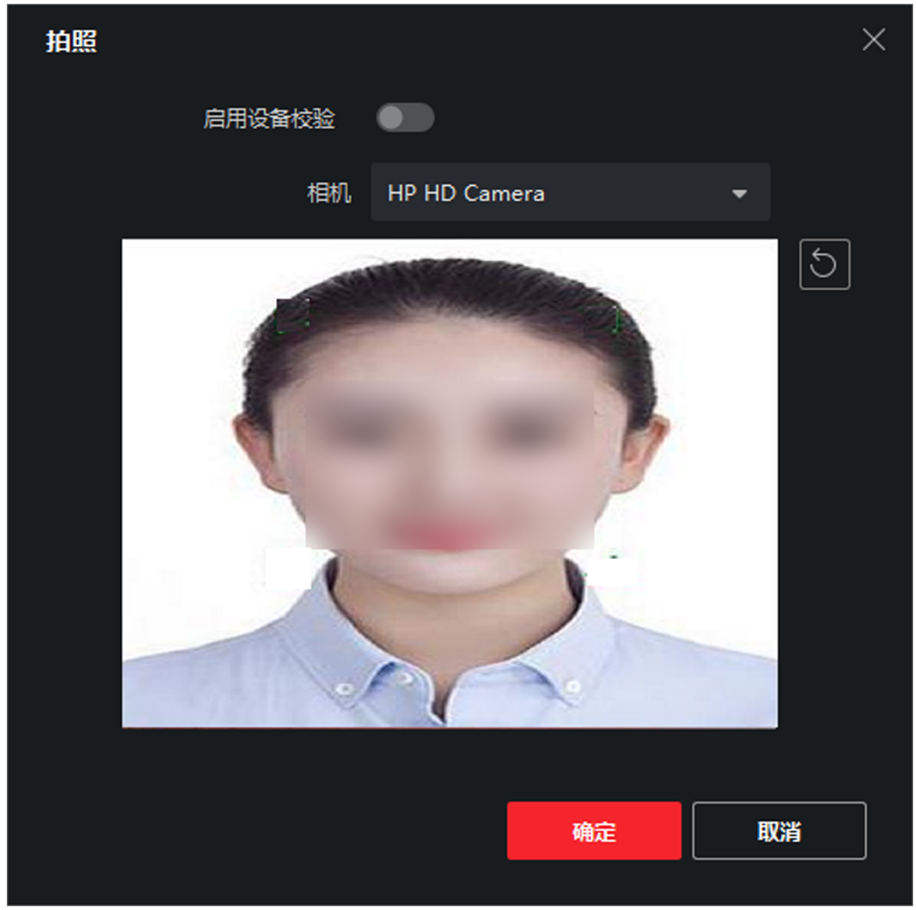


图 7-2 本地采集人脸

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*。

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。也可启用真人检测功能并配置真人检测安全等级。

真人检测

该功能开启后，则设备可判断所检测到的人脸是否为真实的人脸。若非真实人脸，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。可从低、中、高三个等级中选择。等级越高，误识率越低，拒认率越高。

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*。

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 *配置个人认证方式* 。

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，比如民族、紧急联系人等。

操作步骤

1. 进入人员管理界面。
2. 在工具栏中选择**自定义属性**，从右侧滑出**自定义信息**窗口。
3. 单击*添加*。

   字段名称下方，自动添加一行待输入的自定义信息项。

4. 单击 ，输入待添加的属性名称，如邮箱地址。
5. 单击*确定*。

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

已添加可视对讲设备。

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

已添加了待导入人脸图片的人员信息。

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，包括身份信息等，方便管理组织人员信息。

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*，并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。
5. 单击*导出*。
6. 选择保存路径，单击*保存*。

   人员身份属性信息导出为 CSV 文件并保存在本地。

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。

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，详细操作请参见 *添加组织* 和 。

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。

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。

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 7-3 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。

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。

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。

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。

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。

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。

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。

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**。

  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。

  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。

- 胁迫码和超级密码不能重复，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。

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

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。

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）

5. 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。

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。

人脸信息

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。

人脸识别间隔

在此处可配置两次人脸识别的时间间隔。

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 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。

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。

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。

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。

6. 单击*确定*。
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

报警输出需设备支持。

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、人脸、人脸+刷卡等。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*。

配置个人认证方式

个人认证方式指以人为为中心进行认证，可通过人员的 ID 绑定相关该人员的指纹、人脸等认证信息，对一些需要更高或更低的权限认证，可选择个人认证方式，选取不同方式的组合认证。

前提条件

添加人员，并下发人员到设备。详细操作请参见 *人员管理* 和 *分配门禁权限* 。

操作步骤

1. 进入访问控制界面。
2. 在左侧功能区域，选择 *高级配置* → *认证方式* 。
3. 在控制器列表中，选择一个门禁设备，进入个人认证界面。

> **说明**
> 该功能需要添加了支持以人为中心的设备。

4. 单击*添加*。
5. 在弹出的窗口中勾选需要添加认证的人员，并在下拉框中选择认证方式。
6. 单击*确定*。

> **说明**
> 个人认证方式优先级高于其他认证方式。若配置了个人认证方式，人员在设备端认证时，需使用个人认证方式，方可通过认证。

7. **可选操作**：在个人认证方式界面，选择一个人员，并单击*认证方式*，可修改人员的认证方式。
8. **可选操作**：选择人员，单击*下发*将添加的个人认证方式进行下发。

配置首人开门

首人开门支持设置首人常开。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。

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。
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。

配置多网卡参数

配置设备网卡参数信息，解决设备 IP 与 PC 机不在同一局域网段内或者设备 IP 地址被占用等问题。

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*多网卡参数*。
5. 选择网络模式和需要配置参数的网卡。
6. 配置网卡类型、IPv4 地址、子网掩码、端口号等参数。
7. 单击*保存*。

配置网络参数

添加门禁设备后，可以配置网络参数，包括日志上传方式、网络中心。

说明

网络参数配置功能需要设备支持。

设置上传方式

设置上传中心组和通道后可以通过 ISUP 协议传输日志。

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*网络配置*。
5. 网络类型选择**上传方式配置**。
6. 选择**中心组**。

说明

不同型号的门禁设备中心组可能不同。

7. 打开**是否启用**滑块。
8. 在**主通道**和**备份通道**下拉列表中，选择上传方式。

说明

主通道和备份通道不能同时选择 N1 或 G1。

9. 单击*保存*。

设置网络中心

配置 ISUP 账号和参数后，可以在有线模式下，通过 ISUP 协议添加设备。

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*网络配置*。
5. 网络类型选择**网络中心配置**。
6. 选择**中心组**。
7. 地址类型选择 IP 或**域名**。
8. 根据选择的地址类型，输入 IP 地址或域名。
9. 输入协议端口号。

说明

端口号应与 ISUP 端口号保持一致。

10. 协议类型选择 ISUP 并输入 ISUP 账号。
11. 单击*保存*。

配置抓拍参数

抓拍参数可以配置联动抓拍和手动抓拍参数，当触发报警后，联动抓拍；也可以根据实际监控场景，进行手动抓拍。

说明

- 抓拍配置功能需设备支持。
- 配置抓拍参数前，需提前配置存储服务器用于图片存储，相关内容请参考客户管用户手册中的*配置图片存储*。

设置联动抓拍参数

通过客户端设置设备联动抓拍参数。设备已配置事件、客户端、工号或卡号联动抓图，当触发某个事件源，设备将按照已配置的抓拍次数、抓拍间隔进行抓拍，并根据已设置的图片大小和质量生成图片。

操作步骤

1. 进入**访问控制**界面。
2. 在左侧功能栏中，选择 *高级配置* → *更多参数* ，单击*抓拍设置*。
3. 选择抓拍类型为*联动抓拍*。
4. 设置图片尺寸和图片质量。
5. 设置联动抓拍次数。
6. 设置抓拍间隔。
7. 单击*保存*。

设置手动抓拍参数

通过客户端设置设备手动抓拍参数。根据监控场景需求，通过按键进行抓拍，并根据已设置的图片大小和质量生成图片。

操作步骤

1. 进入**访问控制**界面。
2. 在左侧功能栏中，选择 *高级配置* → *更多参数* ，单击*抓拍设置*。
3. 选择抓拍类型为*手动抓拍*。
4. 设置图片尺寸和图片质量。
5. 单击*保存*。

配置终端参数

支持通过客户端配置人证设备的终端参数。

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。

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。

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。

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。

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。

身份证阅读型号

选择外接身份证阅读器型号。

认证工作模式

配置设备的工作模式为门禁模式。

门禁模式下，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 *添加普通卡* 。

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、波特率、数据位、校验类型、通行模式等参数。

说明

当连接方式为*连接门禁主机*时，支持远程设备以*卡号*或*人员编号*的类型输出。

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*。

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、卡号和人员联动等。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、人员触发目标联动录像、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

可为门禁事件（如门状态开启、玻璃碎裂等）配置事件联动，实现门禁事件触发后联动监控点录像、蜂鸣器蜂鸣、门禁点开门或防区撤防等动作，从而及时提醒相关人员处理事件。

操作步骤

1. 进入**访问控制**模块。
2. 在左侧功能栏，选择*联动配置*。
3. 在设备列表中，选择一个设备。
4. 单击*添加*。
5. 事件源选择**事件联动**。
6. 选择事件类型。

说明

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。

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、防区、门禁点、语音播放。

蜂鸣

分为主机蜂鸣和读卡器蜂鸣。主机蜂鸣是指门禁主机上的蜂鸣器鸣响。读卡器蜂鸣是指某个读卡器上的蜂鸣器鸣响。

开门/关门

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”）。 对于某些事件，无法联动“开”、“常开”动作，配置时界面会有对应的提示。

说明

门事件源中选择的门与联动开/关门的门不能是同一个门。

说明

联动动作需设备支持才可配置。

8. 单击*保存*。

配置卡号联动

选择某一卡号，当读卡器识别到该卡号时，则联动目标发起蜂鸣、开门、撤防或语音通报等动作，从而实现对特定持卡人员的重点监控或对其免除监控如可为某办公场所的特定员工配置卡号联动（如工牌号），该员工刷卡即可联动对该办公场所进行撤防。

操作步骤

1. 进入**访问控制**模块。
2. 在左侧功能栏，选择*联动配置*。
3. 在设备列表中，选择一个设备。
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，设置读卡器识别到配置的卡号时的联动动作，包括主机蜂鸣、读卡器蜂鸣、监控点录像/抓拍、报警输出、防区布撤防、门禁点开门/关门、语音播放。

说明

联动动作需设备支持才可配置。

9. 单击*保存*。

配置人员联动

选择某一人员的人员编号，当识别到该编号时，则联动读卡器或主机蜂鸣、门禁点开门、防区撤防或语音通报等动作，从而实现对组织内特殊人员的重点监控和管理

前提条件

已添加人员。详情参见 *人员管理* 。

操作步骤

1. 进入**访问控制**模块。
2. 在左侧功能栏，选择*联动配置*。
3. 在设备列表中，选择一个设备。
4. 事件源选择*人员联动*
5. 在下拉框中选择一个人员。
6. 在联动目标区域框内，配置联动动作，包括主机蜂鸣、读卡器蜂鸣、监控点录像/抓拍、报警输出、防区布撤防、门禁点开/关门、语音播放。
7. 单击*保存*。

说明

联动动作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，包括未戴口罩、温度异常等，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。

当设备检测到温度异常时，客户端弹出弹框提示。

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撤防。布防后，客户端可以接收到设备的报警信息。

操作步骤

1. 单击 菜单图标，选择 *工具* → *设备布防控制* 。
2. 单击 ，使图标显示 ，表示执行撤防；再次单击图标，则执行布防。
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*，可对已添加的全部门禁设备执行布防操作。

全部撤防 单击*全部撤防*，可对已添加的全部门禁设备执行撤防操作。

执行布撤防命令后，需进入事件中心，选择左侧报警主机，右侧查看子系统布撤防状态，如布防失败，客户端仍持续尝试进行布防。

说明

一台门禁设备只能被一个客户端布防。

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、设备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. 进入事件中心界面。
2. 在左侧功能栏单击*事件查询*。
3. 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

门禁设备的事件时间指的是事件被触发的时间，非门禁设备的事件时间指的是客户端接收处理显示的时间。

设备类型

触发事件的设备类型。

分组

设备分组。

事件级别

事件紧急程度。“未归类”表示该事件类型未设置事件级别。

处理状态

可选择事件的处理状态。

4. 单击*搜索*。
   显示搜索到的报警事件。
5. 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。

6. **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	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，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*。
导出事件	单击*导出*，可将事件日志以 CSV 文件格式导出至 PC 本地。

7.5 考勤管理

通过考勤管理模块配置班次、部门排班、人员排班或者临时排班。另外，还可以统计考勤数据、处理签到、签退、请假等考勤情况。

说明
人员管理模块下添加的组织即为考勤管理中的部门。

7.5.1 考勤参数设置

可根据内部需求配置考勤的基本规则、考勤点、假日、请假类型和考勤报表的呈现内容；并支持接入第三方数据库同步原始考勤记录。

设置周末

周末设置即为设定除工作日外的休息日。因不同国家或地区的周末时间不同，不同行业的休息时间也不同，例如一些图书馆、游泳馆周一闭馆休息，即可设置周一为休息日，通过设置周末可灵活配置休息日。

操作步骤

1. 进入考勤管理界面。

2. 在左侧导航栏，选择 *考勤设置* → *基本规则* 。
3. 勾选周末时间，如星期六、星期日。
4. 单击*保存*。

设置加班参数

支持为不同的加班时长划分不同加班等级，每个加班等级对应不同的工时倍率，如加班 2 个小时，设置加班等级 1，工时倍率为 1；加班 4 个小时，前两个小时的工时倍率为 1，后两个小时加班等级为 2，工时倍率可设置为 2，意味着前两个小时按正常工时计算，后两个小时按工时的 2 倍计算。

操作步骤

1. 进入考勤管理界面。
2. 在左侧导航栏，选择 *考勤设置* → *加班设置* 。
3. 勾选加班等级，移动光标在显示不同颜色的时间条两侧，变为左右箭头时，可拖动箭头设置加班时长。
4. 设置工时倍率，即根据不同加班等级，计算工作时长。

说明

工时倍率是指对加班时长按不同倍率进行计算。超出正常工作的时间，可设置不同加班等级，加班等级 1、加班等级 2 和加班等级 3。可为三种加班等级设置不同的工时倍率。例如，加班工时按正常工时计算时，加班等级 1 对应的工时倍率框中选择 1；如果按 2 倍的工时计算，则选择 2，既实际工作 1 小时，计算考勤按工作 2 小时统计；以此类推。

5. **可选操作**：选择**周末加班规则设置**的计算方法，可快捷设置非工作日的工时倍率。
6. 单击*保存*。

图 7-4 设置加班参数

设置考勤点

设置读卡器作为考勤点，通过读卡器刷卡记录考勤签到或签退操作。

前提条件

已添加门禁设备。

已添加门禁设备的读卡器初始默认状态均为上下班考勤点，如需修改读卡器的考勤类型，可按以下步骤进行操作。

操作步骤

1. 进入考勤管理界面。
2. 在左侧功能栏，选择 *考勤设置* → *考勤点设置* 。
3. 单击禁用**设置所有为上下班考勤点**。
4. 在左侧设备资源列表中，勾选待设置考勤点的读卡器（单个或多个）。
5. 单击下拉按键，选择**考勤点类型**为上班考勤点、下班考勤点或上下班考勤点。

   上班考勤点

从设备端上传的考勤状态都将计算为签到。

下班考勤点

从设备端上传的考勤状态都将计算为签退。

上下班考勤

根据设备端的实际考勤状态，计算为签到或签退。

6. 单击*设置为考勤点*。

设置成功后，将提示操作成功信息，界面右侧区域显示已设为考勤点的设备信息列表。

7. **可选操作**：添加后，根据需要可执行以下操作。

修改考勤点 勾选待修改考勤信息的某个或多个设备，单击*修改*，右侧滑出修改窗口，显示可修改考勤点的信息。

取消考勤点 选择待移除考勤信息的设备，单击*移除*，则删除对应的考勤点。

设置假日

支持定期和不定期的假日设置，定期假日可以设置常规假日，以年为周期循环，例如新年、中秋等法定假日；不定期假日可根据实际情况，临时将某月的第几周的周六或周末，调整为工作日，所设置的假日可根据情况设置加班等级。

操作步骤

1. 进入考勤管理界面。
2. 在左侧功能栏，选择 *考勤设置* → *假日设置* 。
3. 单击*添加*，右侧区域滑出添加假日页签。
4. **可选操作**：选择添加假日类型为**定期假日**。
   1) 输入假日名称。
   2) 设置假日开始的第一天。
   3) 设置假日天数。
   4) 设置该假日员工的工作状态，为正常工作或是不同加班等级。
   5) 根据实际情况，可勾选*按年循环*。
5. **可选操作**：选择添加假日类型为**不定期假日**。
   1) 输入假日名称。
   2) 设置假日开始的第一天。
   3) 设置假日天数。
   4) 设置该假日员工的工作状态，为正常工作或是不同加班等级。
   5) 根据实际情况，可勾选*按年循环*。

说明

- 若勾选按年循环，则设置的假日排班周期单位为年。
- 当添加的多个假日在某天有重合时，则以先添加假日优先执行生效，且日历上只显示最先添加的假日，涉及到考勤统计也会按先添加的假日来计算。

6. 单击*确定*。
   假日设置完成后，右侧的日历将会显示当月的假日信息。

设置请假类型

支持添加请假类型，每个主请假类型中又可添加多个子请假类型，如添加主请假类型为请假，请假中又可以添加事假、病假等多个子类型；添加的所有请假类型将会在考勤处理中显示，为工作人员请假提供分类选项。

操作步骤

1. 进入考勤管理界面。
2. 在左侧功能栏，选择 *考勤设置* → *请假类型设置* 。
3. 添加请假主类型。
   1) 在中间主请假类型列表区域，*添加*。
   2) 输入名称。
4. 添加请假子类型。
   1) 选择 1 个请假主类型，单击子类型区域上方的*添加*按键。
   2) 输入名称。

   已添加的请假主类型及其对应的子类型展示到列表中。

启用第三方数据库同步

客户端软件的考勤数据（认证记录）可以用于其他系统进行考勤计算等操作。支持客户端上考勤数据自动同步到第三方数据库中，便于数据查询或管理。

操作步骤

1. 进入考勤管理界面。
2. 在左侧功能栏，选择 *考勤设置* → *三方数据库导出* 。
3. 单击*启用数据库同步*，将客户端考勤数据同步至第三方数据库中。
4. 配置数据库参数，将客户端与数据库进行关联。

   数据库类型

   数据库类型支持 MySql 和 SQL Server。

说明

- 当选择数据库类型为 MySql 时，需要配置 MySql 库文件，需手动导入 32 位 libmysql.dll 文件。
- 当服务端安装在 C 盘时，导入 libmysql.dll 文件至 C:\Program Files (x86)\iVMS-4200 AC\iVMS-4200 AC Client\Server

服务器 IP

第三方数据库的 IP 地址。

数据库名称

对连接的第三方数据库名称。

用户名

数据库的账号名称。

密码

登录数据库的账号密码。

5. 对照客户端表字段，填写所连接数据库的配置信息，包括设备名称、设备序列号、人员名称和卡号等信息。可将考勤数据保存至指定数据中。
6. 单击*保存*。

说明

当同步的过程中，与三方服务器断链了，会每隔 30 分钟重连一次，重连成功后，会把这个时间段内没有同步到数据库的考勤数据同步过去。

设置报表显示参数

支持对生成报表的表头、日期格式和考勤状态符号及字体进行设置，方便查看报表数据。

操作步骤

1. 进入考勤管理界面。
2. 在左侧功能栏，选择 *考勤统计* → *报表显示* 。
3. 输入公司名称。
4. 设置报表显示的日期格式。
5. 设置考勤状态符号、周末符号及字体的颜色。

说明

报表中的符号均支持手动输入设置。

6. 单击*保存*。

设置休息时段考勤规则

可对正常工作日中的休息时段进行管理，如设置午休的开始和结束时间。

操作步骤

1. 进入考勤管理界面。
2. 在左侧导航栏，选择 *时间段* → *休息时间* 。
3. 单击*添加*。
4. 设置休息时间段名称和时长。
5. 设置休息时段的计算方式。

   自动扣除

   不记录该时段内的考勤数据，工作时长将自动扣除休息时段。

   实际打卡

   根据实际打卡记录计算休息时间是否超出休息时段，并根据实际休息时长，设置考勤计算规则。如休息早回即未超出休息时段，是算作加班工时或者正常工时；休息晚回即超出休息时段，可记为缺勤、早退等考勤类型。
6. 单击*保存*。

   在休息时间区域，显示所添加的休息时段信息。

说明

若设置的休息时段已被使用，则无法删除。

图 7-5 设置休息时段考勤规则

7.5.2 添加常规时间段

通过设置考勤规则，如上下班时间、有效签到/签退时间和迟到、早退允许时间，根据制定的考勤规则来监管员工考勤。主要应用于固定上、下班时间的普通早晚考勤场景。

操作步骤

1. 进入考勤管理界面。
2. 在左侧功能栏，选择*时间段*。

3. 单击*添加*。
4. 输入新建的时间段名称。

说明

在时间段名称右侧单击颜色框，可自定义该有效时间段的代表色。

5. 选择时间段类型**常规**。

说明

常规即是需要遵守已设置的考勤时间，在有效打卡时间内执行打卡才有效，严格遵守上下班时间。

6. 选择统计方式。

统计第一条和最后一条记录

记录第一次和最后一次有效打卡记录，计算出每天工作时长。

多次进出

当需要去除员工外出时长，可选择多次进出统计方式，记录每次进入和外出办公区域的打卡时间。

7. **可选操作**：启用设备考勤状态，将按照设备上传的实际考勤状态来统计计算。

说明

设备考勤状态启用需要设备支持该功能。 若设备不支持该功能，但通过设置上、下班考勤点，设备仍会根据考勤规则进行计算。

8. 设置考勤时间相关参数。

上班时间/下班时间

设置上下班考勤时间，并根据设置的时间点，自动计算出勤时长。

签到/签退有效时间

设置某时间段内签到或者签退才有效，其他时间范围外签到或者签退均无效。

允许迟到

签到时间超过上班时间点的 XX 分钟以上，记为迟到。例如，上班时间 9:00，签到有效时间 8:30~9:30，允许迟到 10 分钟，那么 9:10~9:30 之间签到均记为迟到。

允许早退

签退时间早于下班时间点的 XX 分钟以上，记为早退。例如，下班时间 18:00，签退有效时间 17:30~18:30，允许迟到 10 分钟，那么 17:30~17:50 之间签到均记为早退。

9. 设置缺勤参数。

已签到，迟到超过 XX 分钟，记为缺勤

签到时间超过上班时间点的 XX 分钟以上，记为缺勤。例如，上班时间 9:00，迟到超过 60 分钟，记为缺勤，那么 10:00 以后签到均记为缺勤。

已签到，早退超过 XX 分钟，记为缺勤

签退时间早于下班时间的 XX 分钟以上，记为缺勤。例如，下班时间 18:00，早退超过 60 分钟，记为缺勤，那么 17:00 之前签退均记为缺勤。

未签到/签退，记为 XX

在上班时间段内，没有签到/签退，记为缺勤或迟到/早退 XX 分钟。例如，在该上班期间内，未签到或签退，将记为缺勤。

10. 设置休息时间，更多详细操作，请参见 *设置休息时段考勤规则* 。
11. 单击*保存*。

图 7-6 添加时间段

7.5.3 添加班次

添加班次可为不同部门或人员设置排班周期（如每天、每周、每月）和考勤时段。并支持绘制多个时间段，例如，工厂员工每天 8:30~12:00 为上午班，13:30~18:00 为下午班，上午和下午考勤时间段都需要参与考勤，不允许迟到或早退。

操作步骤

1. 进入考勤管理界面。
2. 在左侧功能栏，选择*班次设置*。
3. 添加班次。

1) 单击*添加*。
2) 输入班次名称。
3) 选择班次周期。
4) 选择已添加的时间段，在对应的时间条上，单击并应用该时间段，时间条上呈现该时间段所设置的颜色。

说明

支持添加多个时间段，但若多个时间段（包括签到/签退有效时间）存在交集，则最后选择的时间段将替换掉之前所设置的时间段。例如，时间段 A：上班时间 9:00~12:00，签到有效时间 8:30~9:30，签退有效时间 11:30~12:30；时间段 B：上班时间 5:00~8:30，签到有效时间 4:30~5:30，签退有效时间 8:00~9:00；虽然上班时间没有交集，但签到和签退有效时间范围存在交集，当同时选择时间段 A 和时间段 B，时间段 B 也将替换时间段 A。

5) 单击*保存*。

保存班次设置后，取消按键将自动变为**分配**按键。

4. 分配班次至组织或人员。
1) 单击*分配*，进入分配班次界面。
2) 勾选部门或人员。
3) 设置该部门或人员班次执行的有效时间。
4) **可选操作**: 勾选免签到、免签退、假日排班和加班有效。
5) 单击*保存*。

图 7-7 班次设置示例图

7.5.4 排班管理

排班管理以部门或人员为单位，根据已设置的考勤规则进行管理，并可以通过列表或日历的形式呈现部门或人员的排班计划。

部门排班

以部门为单位进行排班，该部门的人员将按照部门的排班规则进行考勤，可一次性设置部门人员的班次和规则，方便人员考勤管理。

前提条件

在人员管理模块，已添加组织和人员。

操作步骤

说明

人员排班优先级高于部门排班。

1. 进入考勤管理界面。
2. 在左侧功能栏，选择*排班管理*。

3. 在左侧部门资源列表中，选择 1 个或多个组织。
4. 单击*部门排班*。
5. 选择**班次**。

说明

若所选班次添加了多个时间段，则不支持智能排班。

6. **可选操作**：开启**智能排班**。

说明

智能排班指在添加完可能用到的时间段后，考勤人员可在添加的任意一个时间段考勤，均为有效考勤。 例如考勤人员在 00:00~07:00，08:00~15:00 和 16:00~23:00 三段时间考勤均有效，则该考勤人员在 7:00 签到，系统自动将其签到时间归入 08:00~15:00 这个时间段内。

7. 设置部门排班的有效日期。
8. **可选操作**：勾选免签到、免签退、假日排班、加班有效。

说明

若勾选免签到、免签退，则该部门人员可无需认证打卡。

9. 单击*确定*。

人员排班

支持为一个或多个人员进行排班，所配置的人员将按照排班计划进行考勤。

前提条件

在人员管理模块，已添加组织和人员。

操作步骤

1. 进入考勤管理界面。
2. 在左侧功能栏，选择*排班管理*。
3. 单击*人员排班*
4. 在组织列表中，勾选多个组织和人员。
5. 选择**班次**。

说明

若所选班次添加了多个时间段，则不支持智能排班。

6. **可选操作**：开启**智能排班**。

说明

智能排班指在添加完可能用到的时间段后，考勤人员可再添加的任意一个时间段考勤，均为有效考勤。例如考勤人员在 00:00~07:00,08:00~15:00 和 16:00~23:00 三段时间考勤均有效，则该考勤人员在 7:00 签到，系统自动将其签到时间归入 00:00~07:00 这个时间段内。

7. 设置人员排班的有效日期。
8. **可选操作**：设置是否免签到、免签退、假日排班或加班有效。

说明

若勾选免签到、免签退，则人员可无需认证打卡。

9. 单击*保存*。

完成人员排班设置后，可通过部门考勤统计表查看人员排班。

临时排班

当遇到特殊情况，如假日需要临时加班，或员工临时调休时，可临时修改排班计划，临时排班优先级高于人员排班和部门排班。

前提条件

在人员管理模块，已添加组织和人员。

操作步骤

1. 进入考勤管理界面。
2. 在左侧功能栏，选择*排班管理*。
3. 单击*临时排班*。
4. 在左侧部门资源列表中，勾选多个组织或人员。
5. 在临时排班月历中，单击选中或拖动鼠标选择连续日期。
6. 设置临时排班类型，工作日或休息日。
   - 设置休息日，则选人员可不进行上班工作。
   - 设置工作日，则需设置如下参数项。

     计算为

     将该工作日设置为正常工作或是不同等级的加班。

     时间段

     为该工作日选择某时间段内的有效考勤规则。

     智能排班

     智能排班指在添加完可能用到的时间段后，考勤人员可在添加的任意一个时间段考勤，均为有效考勤。 例如考勤人员在 00:00~07:00，08:00~15:00 和 16:00~23:00

三段时间考勤均有效，则该考勤人员在 7:00 签到，系统自动将其签到时间归入 08:00~15:00 这个时间段内。

规则

若勾选免签到、免签退，可不用进行有效打卡记录考勤。

7. 单击*保存*。

查看排班信息

可查看人员的排班信息，对排班信息进行修改和查看。

前提条件

已完成部门或人员排班。

操作步骤

1. 进入考勤管理界面。
2. 在左侧功能栏，选择*排班管理*。
3. 在左侧部门资源列表中，选择某个部门或人员。

说明

勾选**包含子部门**，将显示该部门下的全部子部门，默认全部勾选，可根据需求取消勾选的子部门。

4. 以日历形式查看排班。

   右侧自动显示该部门或人员的排班计划，时间默认跳转至计划开始时间。

5. 单击右上角 ▦ 或 ☰ ，分别以日历和列表的形式查看排班计划。

说明

按日历形式查看排班计划，可直观获取上班和休息日期，临时排班也会记录，单击*临时排班*，可修改和删除临时排班。详细内容请参见 *临时排班* 。

7.5.5 考勤处理

由于某些原因，如忘签到、忘签退、出差、请假等，导致考勤状态异常时，可以通过提交补签单或者请假出差申请，修正考勤记录。

添加补签单

当人员考勤状态异常时（比如忘记打卡、未带工牌等），支持手动更正签到或签退记录。

操作步骤

1. 进入考勤管理界面。

2. 在左侧功能栏，选择*考勤处理*。
3. 单击*补签*。
4. 在左侧部门资源列表中，选择 1 个部门或选择该部门下的人员（可多选）。
5. 选择考勤异常的**补签日期**。
6. 根据实际情况选择**补签到**或**补签退**，并选中签到/签退时间点。

说明

若员工的考勤统计方式为**多次进出**，则可添加多个补签时间。

7. **可选操作**：输入备注信息，一般为考勤异常原因。
8. 单击*确定*。
9. **可选操作**：可根据实际情况，执行如下相关操作。

删除 勾选 1 个或多个补签单，单击*删除*可以删除选中的补签单。

导出 勾选 1 个或多个补签单，单击*导出*可以将补签单导出到本地。

完成添加后，列表详情区域展示已添加的补签单。

添加请假/出差单

当人员请假或出差时，可以提交请假单或出差单。

操作步骤

1. 进入考勤管理界面。
2. 在左侧功能栏，选择**考勤处理**。
3. 单击*请假/出差*。
4. 在左侧部门资源列表中，选择 1 个部门或选择该部门下的人员（可多选）。
5. 选择待请假/出差的日期。
6. 选择请假类型，如请假或出差。
7. 选择假日子类型，可选择使用年休假、病假或出差。
8. 设置**请假时间**。
9. **可选操作**：输入备注信息，可填写请假事由或出差公办。
10. 单击*确定*。

完成添加后，列表详情区域展示已添加的请请假单或出差单。

11. **可选操作**：可根据实际情况，执行如下相关操作。

搜索 设置搜索条件，单击*搜索*可以过滤符合条件的结果。

生成报表 单击*生成报表*可以生成请假单/出差单报表。

导出 单击*导出*可以将请假单/出差单导出到本地。

7.5.6 计算考勤数据

查看考勤统计前必须先计算考勤数据。支持手动（让系统计算某一时间段的考勤数据）和自动（每天在预设时间点自动计算考勤数据）两种方式计算考勤数据。

自动计算考勤数据

设置自动计算考勤时间，系统每天在预设时间点，自动计算前一天的考勤数据。

操作步骤

1. 进入考勤管理界面。
2. 在左侧功能栏，选择 *考勤设置* → *基本规则* 。
3. 在界面下方，设置*自动计算考勤时间*。
4. 单击*保存*。

   设置成功后，系统在每天设置的时间点，自动计算前一天的考勤数据（不计算当天数据）。默认自动计算时间为凌晨 1 点。

手动计算考勤数据

通过手动设置待查看人员或部门的考勤信息，包括考勤时间，考勤状态（如缺勤、请假）等，即可获取该人员或部门的考勤数据详情。并支持将考勤数据生成报表导出，也可对缺勤状态进行补签，方便快捷修正考勤数据。当考勤处理、权限组或排班调整后，都可通过手动计算，获取最新的考勤数据。

操作步骤

1. 进入考勤管理界面。
2. 在左侧导航栏，选择 *考勤统计* → *考勤计算* 。
3. 输入待统计考勤数据的开始和结束日期。
4. 选择待统计考勤的部门。
5. **可选操作**：输入员工**姓名**或**编号**。
6. 勾选待统计的**考勤状态**，可多选。
7. 单击*计算*。

   界面下方将显示考勤数据列表。

8. **可选操作**：可根据实际需求，执行如下相关操作。

补签	选择某一考勤异常项，单击*补签*，既可自动处理该员工的补签时间点，并记录到考勤处理中。
自定义列表项	单击列表右上方 ⚙ ，或者右键表头，在弹框中勾选需要显示的列表项。

说明

- 默认展示的列表项包括编号、姓名、组织、日期、时间段和上/下班状态。
- 仅显示列表项对应的考勤数据。

生成报表 单击*生成报表*，可查看考勤统计结果。

导出 单击*导出*，考勤统计数据将以.csv 格式导出。

7.5.7 考勤统计

用户可以通过客户端考勤管理功能，制定考勤规则、班次、排班计划等，将部门中的人员在考勤点的签到、签退记录进行汇总和统计，同时结合补签、请假、出差等考勤处理，计算出人员的考勤数据，并生成报表，同时也可以根据实际情况，自定义报表的呈现形式。

说明

客户端将在次日凌晨 1 点自动计算前一天的考勤数据。请确保在次日凌晨 1 点，客户端处于运行状态。若客户端未在凌晨 1 点运行，则需手动计算考勤数据，具体请参考 *自动计算考勤数据* 。

查看考勤记录

通过设置待查看考勤信息的过滤条件，可搜索查看某部门或人员的考勤信息记录，包括考勤编号、姓名、部门、日期、考勤状态和考勤点等。

操作步骤

1. 进入考勤管理界面。
2. 在左侧功能栏，选择 *考勤统计* → *考勤记录* 。
3. **可选操作**：单击*获取设备事件*，选择设备，从而获取该设备的考勤数据。
4. 设置考勤开始和结束时间。
5. 选择部门或输入职员姓名。
6. 选择**数据来源**，可选择数据来源手动考勤处理、原始记录或全部。
7. 单击*搜索*。

   说明

   若正在自动计算考勤数据时，则无法搜索到考勤记录。

8. **可选操作**：单击*重置*，将清空已设置的过滤条件。
9. **可选操作**：可根据实际需要，执行如下相关操作。

   生成报表 单击*生成报表*将生成已设置条件的原始记录报表。

   导出 单击*导出*，将以.cvs 格式导出考勤数据信息。

自定义导出 可对某部门或人员的指定的考勤数据进行导出，更多详细操作，请参见 。

生成统计报表

支持按部门、单个或多个人员生成不同类型的统计报表，统计报表类型包括正常统计、异常统计和加班统计，可满足不同统计类型需求。

前提条件

已添加部门和人员，并设置好考勤规则，具体步骤请参见 *设置周末* 。

操作步骤

1. 进入考勤管理界面。
2. 在左侧功能栏，选择 *考勤统计* → *统计报表* 。
3. 选择待生成的报表类型。

> **说明**
> 鼠标悬浮处将显示报表类型说明。

4. 选择部门下的全部或部分人员。
5. 设置统计考勤记录时间。
6. 单击右侧*生成报表*。

定时发送报表

可根据实际情况定义报表内容，如报表统计人员、部门、报表类型等，包括生成指定人员或部门的月考勤、周考勤、加班等不同考勤报表，并可将生成的报表通过邮件定时发送给相关人员进行查看。

操作步骤

1. 进入考勤管理界面。
2. 在左侧导航栏，选择 *考勤统计* → *定时发送报表* 。
3. 单击*添加*，进入添加定时发送报表界面。
4. 输入报表名称。
5. 选择报表类型和报表时间。
6. 勾选待生成报表的统计人员。
7. 设置自动发送邮件。
   1) 设置自动发送邮件的有效期限。
   2) 勾选每周的发送日期。
   3) 设置发送当天的具体时间点。
   4) 输入收件人的邮箱地址。

说明

输入邮箱地址前，请先完成邮箱参数配置，详细操作请参见 。

5) **可选操作**：单击*预览*，可提示邮箱是否配置成功，并可预览发送邮件内容。

8. 单击*确定*。
9. 可根据实际情况，执行如下相关操作。

编辑自定义报表 选择已添加的某个自定义报表，单击*编辑*，可修改相关参数项。

生成报表 选择已添加的某个自定义报表，单击*生成报表*，可查看生成的报表。

删除自定义报表 选择已添加的某个或多个自定义报表，单击*删除*，可删除已选中的自定义报表。

图 7-8 定时发送报表

7.6 远程配置（网页端）

7.6.1 查看设备信息

查看配置设备名称，查看设备类型、序列号、版本、继电器个数和电锁个数。

在设备管理页面，选择一个设备并单击 ⚙ → *系统* → *设备信息* 进入设备信息页面。

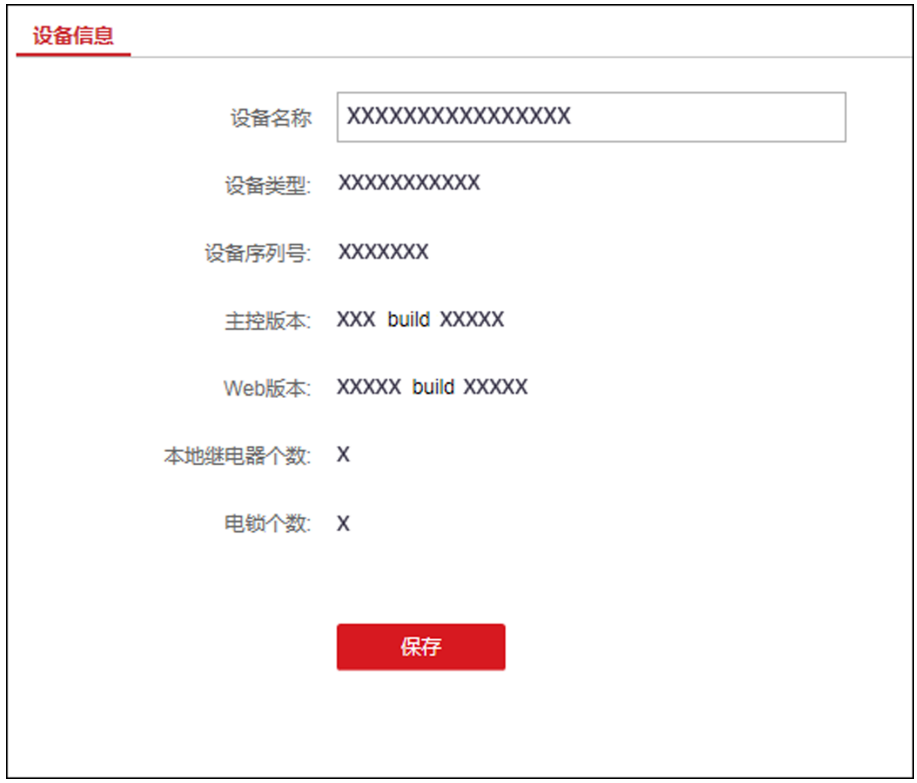


图 7-9 查看设备信息

可配置设备名称，查看设备类型、序列号、版本、继电器个数和电锁个数。单击*保存*。

7.6.2 修改设备密码

修改设备密码。

前提条件

激活设备。详见*激活*。

操作步骤

1. 在设备管理页面，选择一个设备并单击 ⚙ → *系统* → *用户管理* 进入用户管理页面。

图 7-10 用户管理页面

2. 选择用户，并单击*修改*进入修改窗口。
3. 输入旧密码、创建新密码并确认新密码。

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，在客户端设备管理页面需重新配置设备新密码方可重新连接设备。

7.6.3 时间管理

管理设备时区、设备校时方式和夏令时。

设备时区与校时

在设备管理页面，选择一个设备并单击 ⚙ → *系统* → *时间管理* 进入时间管理页面。
选择时区、NTP 校时或手动校时。

NTP 校时

设备自动与 NTP 校时，需配置 NTP 服务器地址、端口及校时间隔。

手动校时

需手动设置设备时间。

勾选*与计算机时间同步*，设置时间中显示此时客户端安装的电脑的本地时间。此时取消勾选*与计算机时间同步*，并单击 可手动设置时间。

夏令时

在设备管理页面，选择一个设备并单击 *远程配置* → *系统* → *时间管理* → *夏令时管理* 进入夏令时管理页面。
根据需要开启夏令时，并编辑夏令时偏移时间、开始时间和结束时间。单击*保存*。

7.6.4 系统维护

重启设备、恢复设备默认参数、升级设备。

重启设备

在设备管理页面，选择一个设备并单击 ⚙ → *系统* → *系统维护* 进入系统维护页面。
单击*重启*，设备开始重启。

恢复默认参数

在设备管理页面，选择一个设备并单击 *远程配置* → *系统* → *系统维护* 进入系统维护页面。

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。

恢复部分默认参数

部分设备参数将恢复默认。

完全恢复默认参数

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

在设备管理页面，选择一个设备并单击 *远程配置* → *系统* → *系统维护* 进入系统维护页面。
在参数导入中单击*浏览*可从电脑本地选择需要导入的文件，单击*导入*可进行参数导入设备。
在参数导出中单击*导出配置文件*，可将设备端的参数导出到电脑本地。

升级设备

在设备管理页面，选择一个设备并单击 *远程配置* → *系统* → *系统维护* 进入系统维护页面。
在**升级**部分从下拉框中选择升级类型，单击*浏览*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。

7.6.5 配置 RS-485 参数

选择需要配置的串口，并配置对应的 RS-485 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* → *RS-485* ，根据需要可配置 RS-485 参数。可配置 RS-485 地址、外接设备、认证中心、码率、数据位、停止位、校验类型、通讯模式和工作模式。

7.6.6 安全模式选择

选择登录时的安全等级及启用 SSH。

在设备管理页面，选择一个设备并单击 ⚙ → *系统* → *安全管理* 进入安全模式页面。

在下拉框中选择**安全模式**或**兼容模式**，并根据需要选择是否启用 SSH，并单击*保存*。

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

启用 SSH，使数据传输更安全。

7.6.7 配置网络参数

配置设备网络参数，包括网卡类型、DHCP 信息和 HTTP 信息。

在设备管理页面，选择一个设备并单击 ⚙ → *网络* → *网络参数* 进入网络参数配置页面并进行网络参数配置，单击*保存*保存配置的参数。

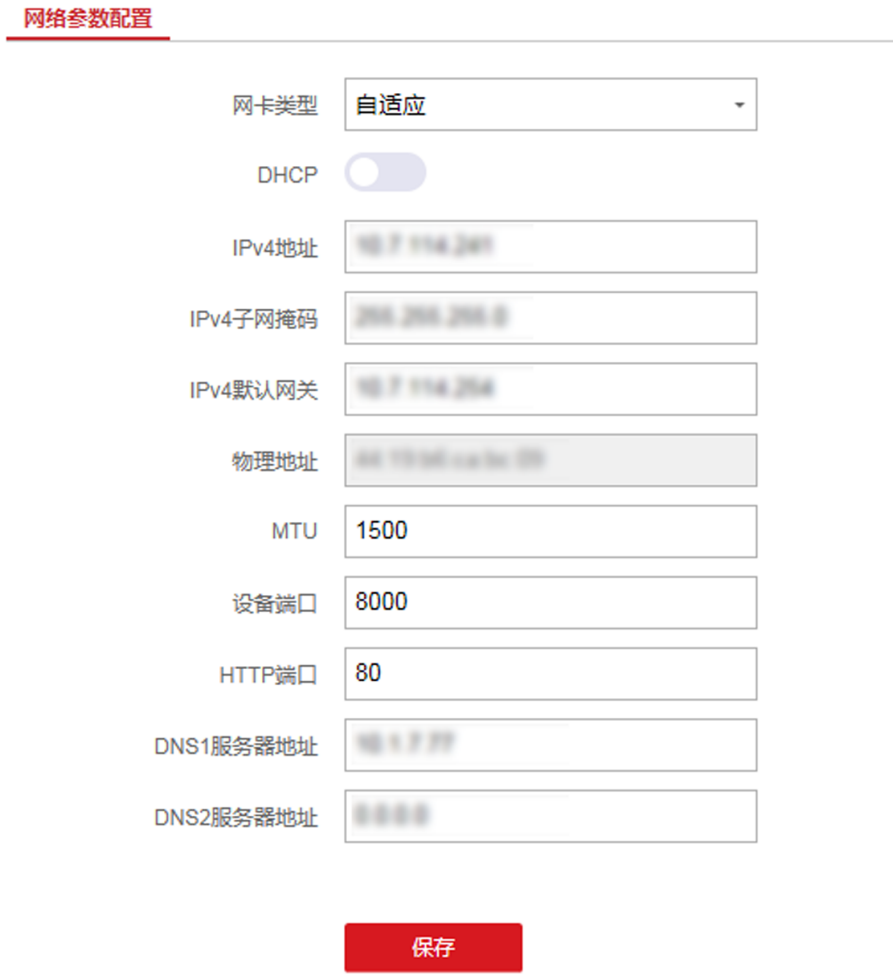


图 7-11 网络参数配置页面

网卡类型

根据实际情况配置网卡为自适应、10M 或 100M。

DHCP

若关闭此项，需手动配置 IPv4 地址、IPv4 子网掩码、IPv4 默认网关、MTU 和设备端口。

若开启此项，系统自动分配 IPv4 地址、IPv4 子网掩码和 IPv4 默认网关。

HTTP

可配置 HTTP 端口。

DNS1 服务器地址及 DNS2 服务器地址

根据实际需求配置 DNS 服务器地址。

7.6.8 上报策略配置

通过配置中心组以及通道，您可通过 EHome 协议传输日志。

在设备管理页面，选择一个设备并单击 ⚙ → *网络* → *上报策略* 配置数据上传的中心组，系统可通过 EHome 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/备份通道

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。

7.6.9 网络中心参数配置

通过配置网络中心、中心 IP 地址、端口号、EHome 用户名等，您可通过 EHome 协议传输数据。

在设备管理页面，选择一个设备并单击 ⚙ → *网络* → *网络中心参数* 配置上传中心信息。

启用后，可配置客户端所在的 IP 地址或域名、端口号，并创建 EHome 账户等。

单击*保存*保存配置的参数。

配置完成后，通过客户端通过 EHome 重新添加设备，客户端可通过 EHome 协议访问设备。

7.6.10 配置 Wi-Fi

配置设备所连接 Wi-Fi 参数。

操作步骤

1. 在设备管理页面，选择一个设备并单击 ⚙ → *网络* → *Wi-Fi* 进入配置 Wi-Fi 参数页面。
2. 启用 Wi-Fi。
3. 配置 Wi-Fi 的 SSID 名称与密码。或从 Wi-Fi 列表中选择一个 Wi-Fi，并单击*连接*。配置 Wi-Fi 的密码。
4. 从**安全模式**下拉框中选择一个接入 Wi-Fi 安全模式。
5. **可选操作**：单击*刷新*可刷新 Wi-Fi 连接状态。
6. 单击*保存*。
7. **可选操作**：配置 WLAN 参数。
   1) 在*配置 Wi-Fi 参数*页面单击 *WLAN 配置*。
   2) 关闭 *DHCP* 功能，并配置 IP 地址、网关地址、DNS1 服务器地址和 DNS2 服务器地址。

8. 单击*保存*。

7.6.11 配置继电器参数

查看和配置设备外接的继电器参数。

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 *报警* → *继电器* ，即可查看继电器参数。

此时选中一个继电器，并单击设置按钮进入继电器参数配置窗口，可配置继电器名称和输出延时时间。

7.6.12 配置门禁参数

操作步骤

1. 在设备管理页面，选择一个设备并单击 ⚙ → *其他* → *门禁参数* 进入配置门禁参数页面。
2. 勾选相关门禁参数以启用。

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。

仅测温模式

开启后，不进行人员权限认证，仅测温。关闭后，进行人员权限认证和测温。默认关闭。

抓拍白光图片

开启后，设备将抓拍白光图片，并上传至平台。如关闭此功能，设备仅将热成像镜头抓拍的照片上传至平台。

高温报警开门

开启后，检测到温度高于配置的阈值时，门不开启。默认开启。

强制佩戴口罩

启用该项后，认证人员必须佩戴口罩，否则认证失败。

未佩戴口罩提醒

启用该项后，认证人员若未佩戴口罩，设备提示戴口罩。

高温报警阈值设置

可配置检测的最高阈值，若被测目标温度高于配置的温度，设备提示异常。可设置的区间为 33 ° C ~ 44.9 ° C。

3. 单击*保存*。

7.6.13 配置人证设备参数

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。

单击 ***其他*** → ***人证设备参数*** 。可配置人证算法库、保存认证图片、设备环保模式，以及配置工作模式。单击*保存*可保存配置，并下发到设备。

人证算法库

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。

CPU 卡读取内容

配置读取 CPU 卡片的内容为序列号或文件。

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。

直通模式不验证卡或身份证权限，只判断卡或身份证有效期。

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 1:1

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。

说明

仅普通模式下支持环保模式。

环境模式 1:N

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。

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。

还可在修改设备参数功能中配置认证设备参数，详见修改门禁设备下的 *配置终端参数* 。

7.6.14 配置人脸参数

可配置设备比对或检测人脸时的参数，包括上下俯仰角度、左右水平角度、人脸检测左边界、人脸检测右边界、人脸检测上边界、人脸检测下边界、眼间距及人脸评分。

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。

上下俯仰角度

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。参考值：30 度。

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。参考值：45 度。

人脸检测左边界

人脸左侧至画面左侧的距离百分比。人脸比对时，检测到的距离百分比需大于配置的值，且设备其他边界及角度的值超过配置的值，方可进行人脸比对。

人脸检测右边界

人脸右侧至画面右侧的距离百分比。人脸比对时，检测到的距离百分比需大于配置的值，且设备其他边界及角度的值超过配置的值，方可进行人脸比对。

人脸检测上边界

人脸顶部至画面顶部的距离百分比。人脸比对时，检测到的距离百分比需大于配置的值，且设备其他边界及角度的值超过配置的值，方可进行人脸比对。

人脸检测下边界

人脸底部至画面底部的距离百分比。人脸比对时，检测到的距离百分比需大于配置的值，且设备其他边界及角度的值超过配置的值，方可进行人脸比对。

眼间距

人脸比对或者录入时瞳孔间的最小像素值。检测到的像素值需大于配置的值，方可进行人脸比对或者录入。参考值：40 像素。

人脸评分

配置人脸评分阈值。设备根据配置的上下俯仰角度、左右水平角度和眼间距对检测到人脸进行评分。若评分大于配置的值，人脸比对或者录入失败。

7.6.15 配置补光灯参数

可开启、关闭补光灯，还可调节补光灯亮度。

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 *其他* → *配置补光灯参数* 进入配置补光灯参数页面。在下拉框中配置补光灯编号和补光灯模式，若选择模式为*开启模式*，可调节补光灯亮度。

7.6.16 配置设备编号

配置设备的期号、幢号和单元号。

配置完成后，管理机可通过配置的编号呼叫该门禁设备。

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。

单击 *其他* → *配置设备编号* 并配置设备的期号、幢号和单元号，并单击*保存*。

7.6.17 配置视音频参数

可配置设备端摄像机的图像质量、分辨率及其他参数。

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 *图像* → *视音频* 。

说明

配置监控点的视音频参数，包括码流类型、码率类型、图像质量、视频帧率、音频编码类型、视频类型、码率、分辨率和 I 帧间隔。

4. 单击*保存*可保存配置，配置将被下发到设备中。

7.6.18 继电器操作

开启或关闭继电器。

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。

在远程配置界面点击 *操作* → *继电器* 。

勾选需要操作的继电器，点击*开启*或者*关闭*对继电器进行操作。

7.6.19 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* 。

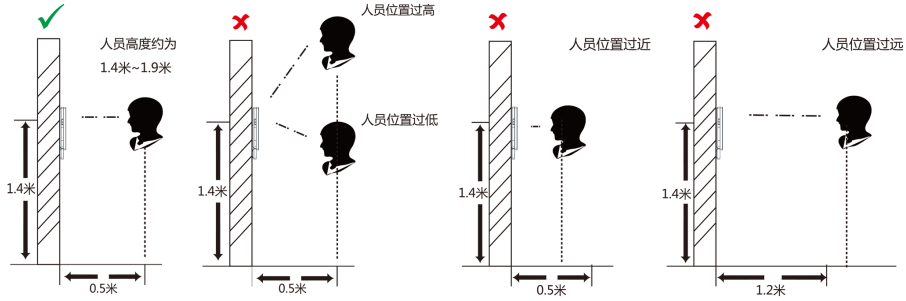
单击 ⚙ 进入远程配置页面。

单击 *状态* → *继电器* 可查看继电器的状态。

附录 A. 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）。

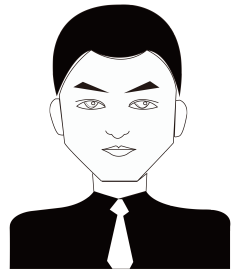


图 A-1 人脸自然表情

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：

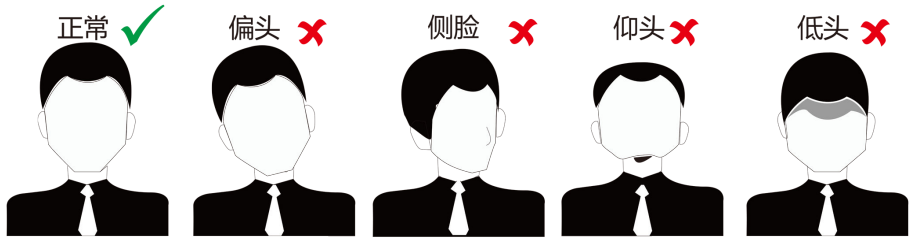


图 A-2 人脸录入/比对姿势示意图

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：

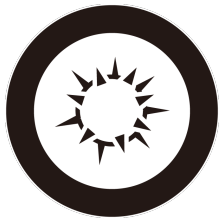
图 A-3 人脸大小调整示意图

附录 B. 安装环境注意事项

1. 安装环境光源参考值：

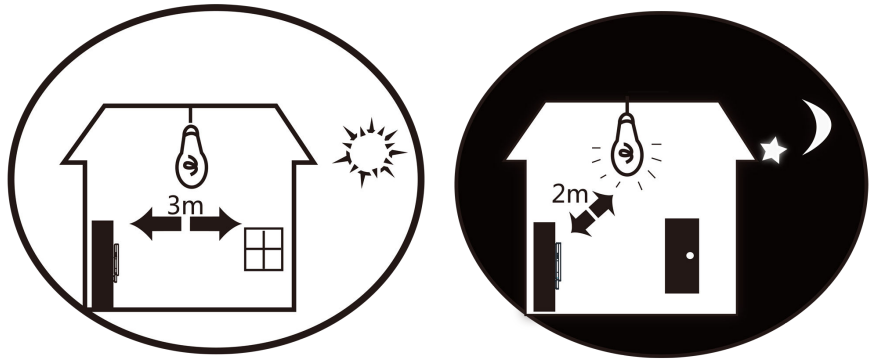
蜡烛：10 Lux

灯泡：100 ~ 850 Lux

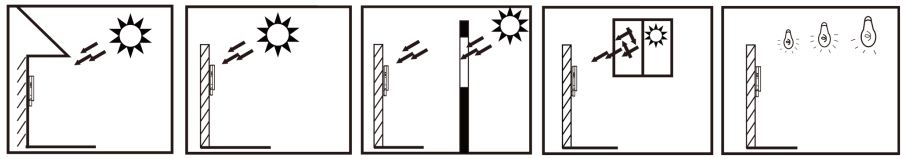


日光：大于 1200Lux

2. 请将设备安装在室内，距离灯源至少 2 米。距离窗口及门口至少 3 米。



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。



逆光　太阳直射　太阳透过窗户直射　太阳透过窗户斜射　灯光近距离照射

附录 C. 尺寸图

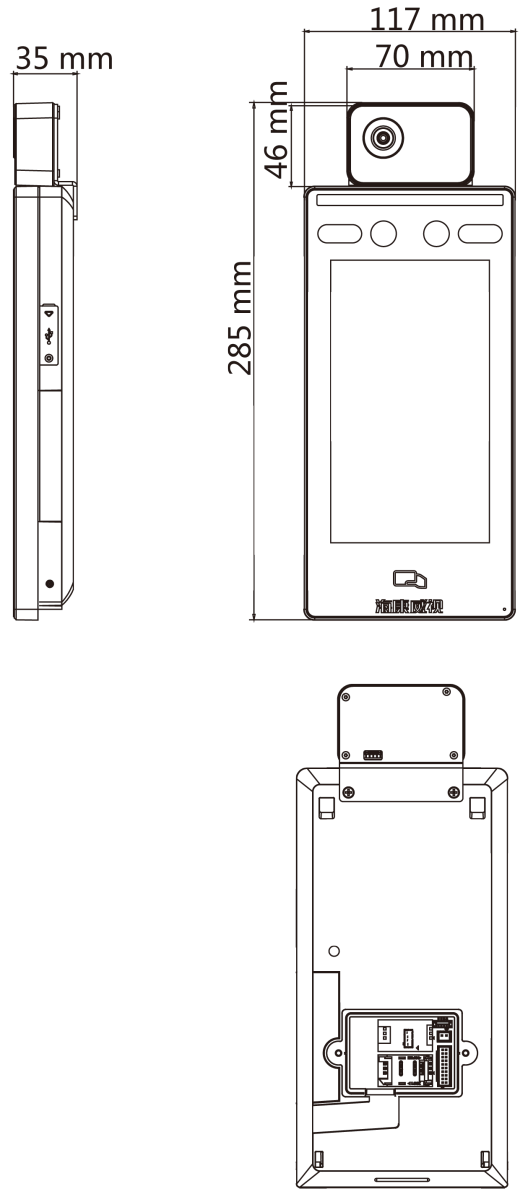


图 C-1 尺寸图

附录 D. 技术参数

型号	DS-K1T6Q-F70M-3XF/TB
操作系统	Linux
测温模块探测器类型	氧化钒(VOx)微测辐射热计
测温模块分辨率	160 × 120
测温模块帧率	25 fps
测温模块视场角	50° × 37.2°
测温范围	30 ° C ~ 45 ° C
测温精度	± 0.5 ° C
测温距离	0.3 m ~ 2 m
显示屏	7 英寸
存储容量	4 GB
事件容量	10 万条事件
人脸容量	5000 张人脸
人脸比对时间	＜ 0.2 s/人
人脸识别距离	0.3 m ~ 2 m
网口	10/100/1000Mbps 自适应网口
物理接口	韦根 × 1、USB × 2、电锁 × 1、门磁 × 1、IO 输出 × 1、IO 输入 × 2、防拆 × 1、开门按钮 × 1
摄像头	200 万像素双目摄像头，宽动态，支持室外逆光环境
设备电源	DC 12 V/2 A
相对湿度	10%至 90%（在不凝结水滴状态下）
工作温度	0 ° C ~ 50 ° C

型号	DS-K1T6Q-F70M-3XF/TB
使用环境	室内
尺寸 （宽 × 高 × 深）	117 mm × 285 mm × 35 mm

附录 E. 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 E-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 E-2 设备命令二维码

见远 行更远

See Far, Go Further

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

UD19349B-A