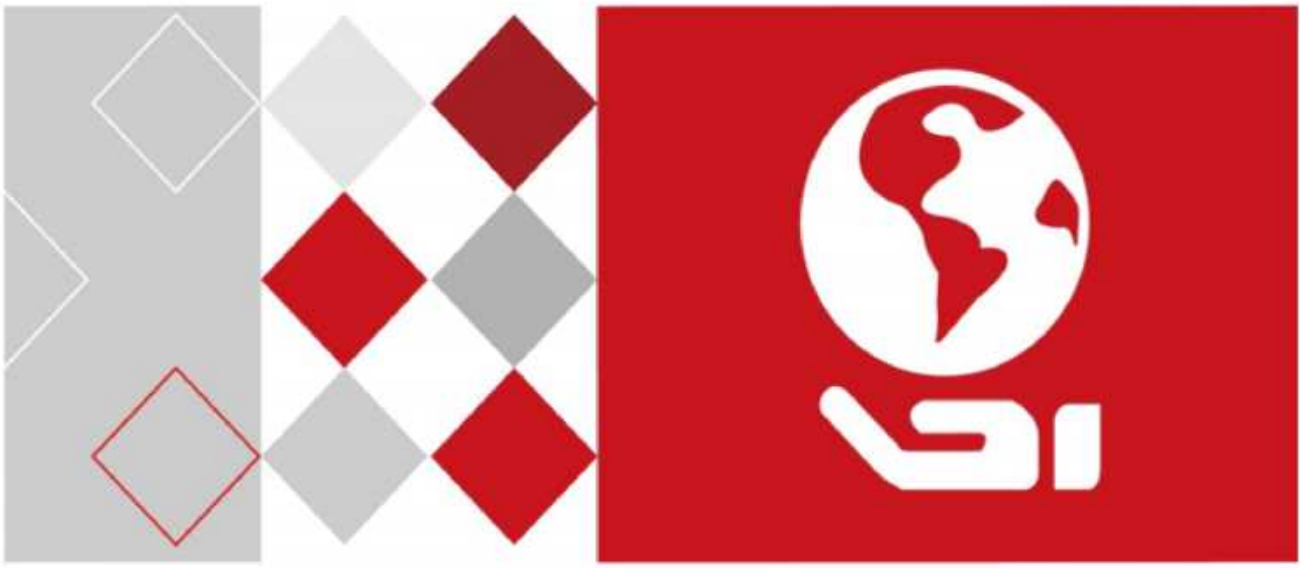


DS-K2800 系列门禁控制主机
用户手册

UD05670B

关于本手册

本手册描述的产品仅供中国大陆地区销售和使用。

本手册适用于门禁控制主机，包括以下名称。

产品系列	产品型号	产品名称
DS-K2800 门禁控制主机	DS-K2801	单门禁控制主机
	DS-K2802	双门禁控制主机
	DS-K2804	四门禁控制主机

本手册作为指导使用。手册中所提供照片、图形、图表和插图等，仅用于解释和说明目的，与具体产品可能存在差异，请以实物为准。因产品版本升级或其他需要，本公司可能对本手册进行更新，如您需要最新版手册，请您登录公司官网查阅（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

海康威视 HIKVISION 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，本手册所描述的产品（含其硬件、软件、固件等）均“按照现状”提供，可能存在瑕疵、错误或故障，本公司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、不侵犯第三方权利等保证；亦不对使用本手册或使用本公司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、数据或文档丢失产生的损失。

若您将产品接入互联网需自担风险，包括但不限于产品可能遭受网络攻击、黑客攻击、病毒感染等，本公司不对因此造成的产品工作异常、信息泄露等问题承担责任，但本公司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。若本产品被用于侵犯第三方权利或其他不当用途，本公司概不承担任何责任。

如本手册内容与适用的法律相冲突，则以法律规定为准。

前言

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
	表示有中度或低度潜在危险，如果不能避免，可能导致人员轻微或中等伤害。
	表示有潜在风险，如果忽视这些文本，可能导致设备损坏、数据丢失、设备性能降低或不可预知的结果。
	表示是正文的附加信息，是对正文的强调和补充。
	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。

目录

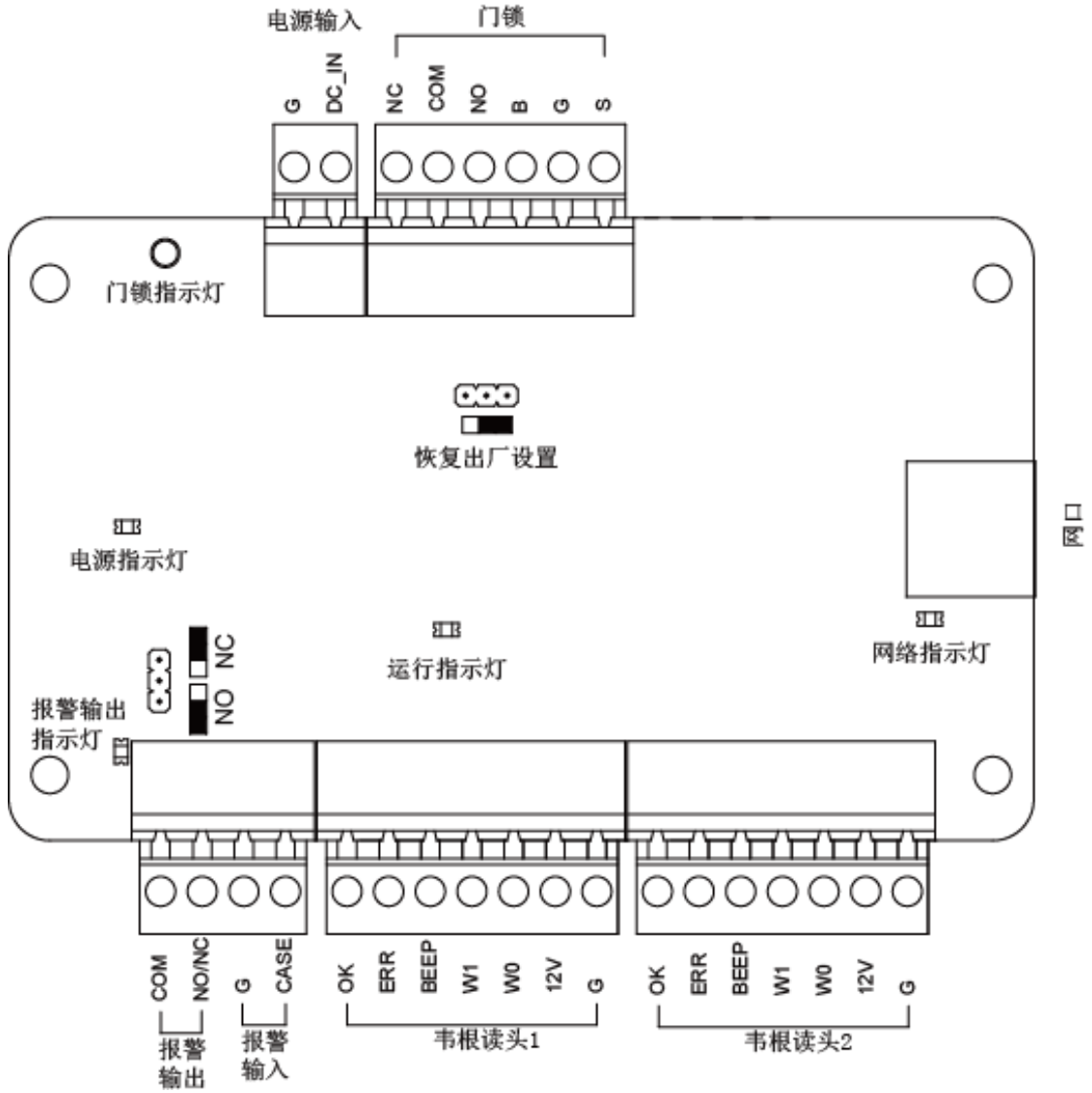
第1章 产品主要功能

- 32 位高速处理器，性能强劲、速度快。
- 支持 TCP/IP 网络通信，网速自适应，通讯数据采用特殊加密处理，更安全，无泄密之忧。
- 主机可支持长度为 20 位的卡号识别和存储。
- 主机可存储 1 万笔合法卡，5 万笔刷卡记录。
- 系统支持 RTC 时钟、手动校时、自动校时、远程、NTP 校时功能。
- 主机支持首卡开门及首卡授权功能，超级卡、超级密码开门、中心远程开门功能，在线升级功能。
- 主机具门未关妥报警功能、门被外力开启报警功能、开门等待超时报警功能、胁迫卡和胁迫码报警功能、黑名单报警、非法卡超次刷卡报警功能。
- 主机韦根格式支持标准韦根协议及 HIK 私有韦根协议。
- 主机支持普通卡/残疾人卡/黑名单/巡更卡/来宾卡/胁迫卡/超级卡等多种卡片类型。
- 支持通过网络方式升级设备程序及设备固件备份功能。
- 清晰完善的事件记录和上传;显示功能，便于用户快速定位事件信息。
- 灵活的计划模板配置，同时支持周计划和假日计划。
- 脱机记录保持功能、支持纪录储存空间不足警告功能。
- 主机断电后数据可以永久保存。
- 无缝兼容第三方韦根接口读卡器。
- 支持 30 条事件及卡号联动。
- 多种事件上传方式：通道上传、中心组上传、监听上传。
- 支持 500 组认证码。
- 支持设备内反潜回功能。

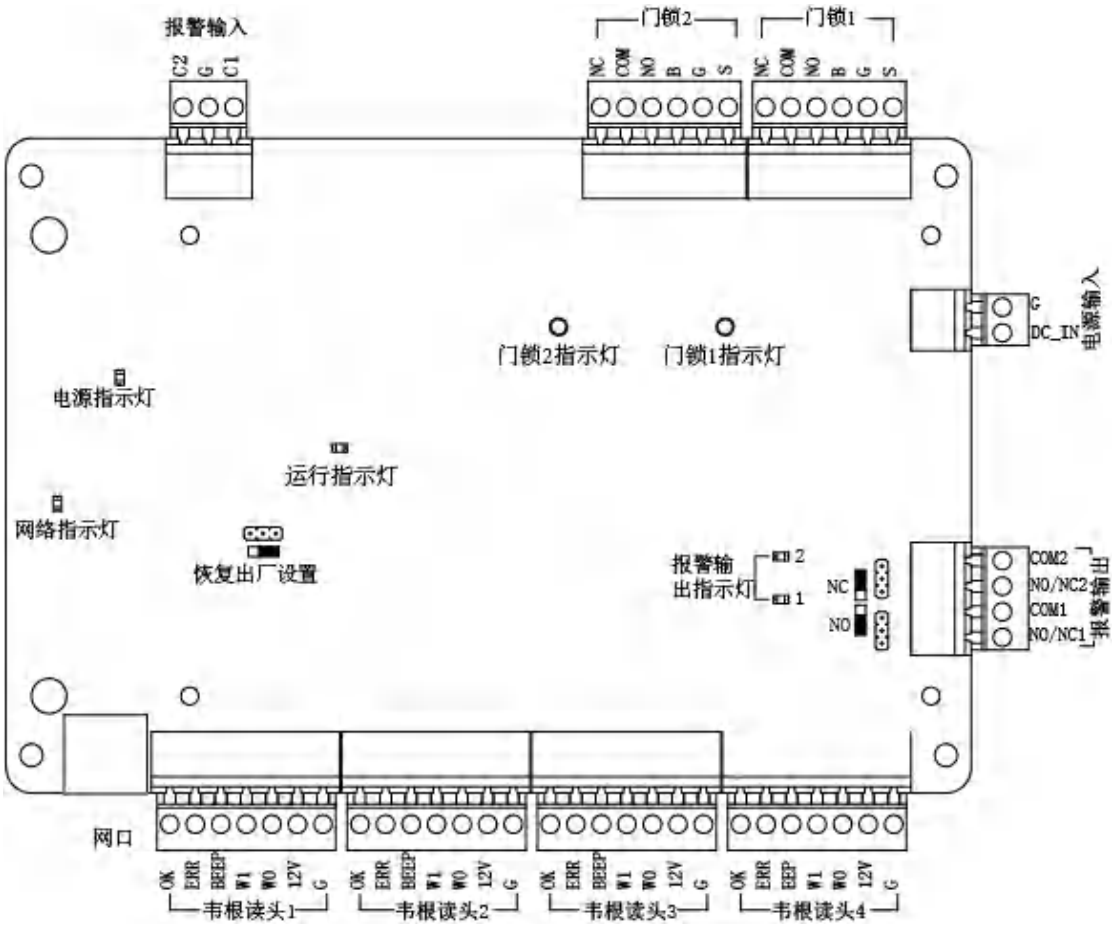
第2章 主板外观

2.1 正面外观说明

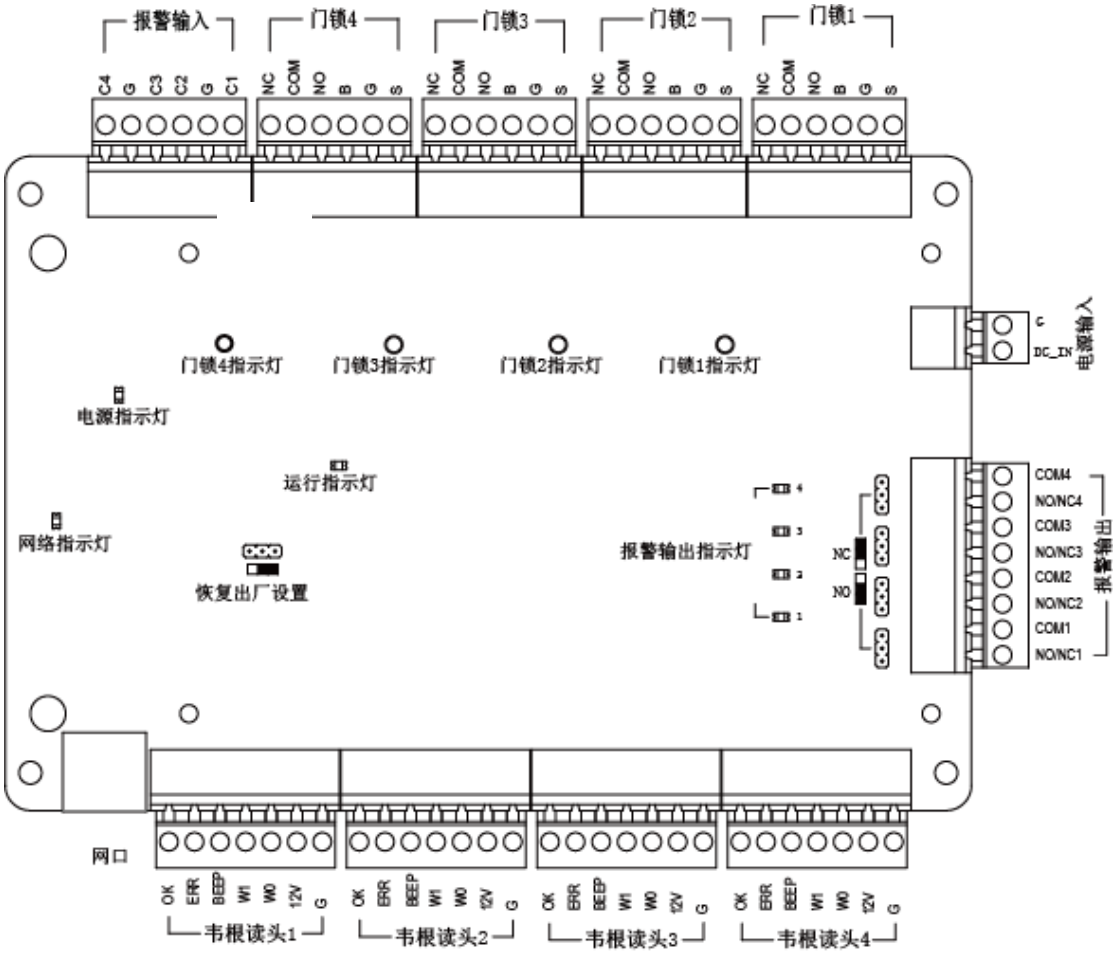
2.1.1 单门禁控制主机 正面外观



2.1.2 双门禁控制主机 正面外观



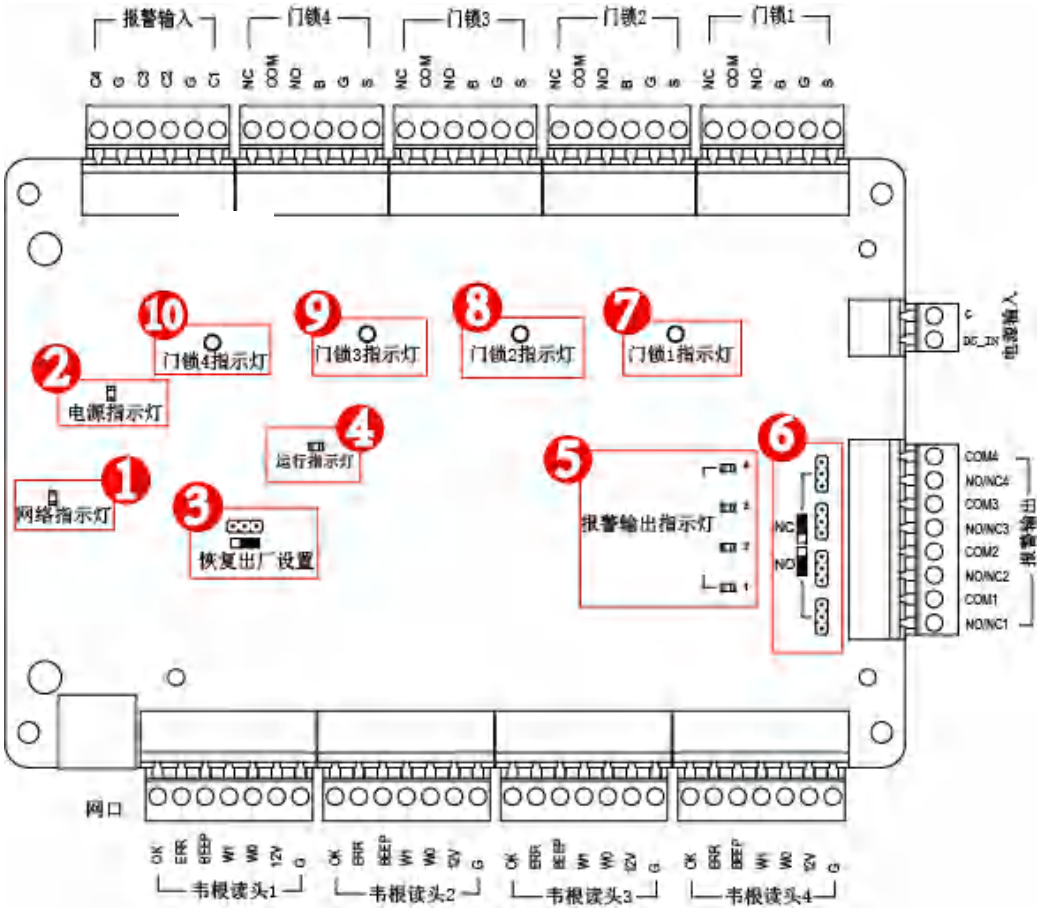
2.1.3 四门禁控制主机 正面外观



2.2 灯号及开关示意图及说明

2.2.1 门禁控制主机灯号及开关示意图

门禁控制主机灯号以及开关示意以四门禁控制主机为例。



2.2.2 门禁控制主机组件说明

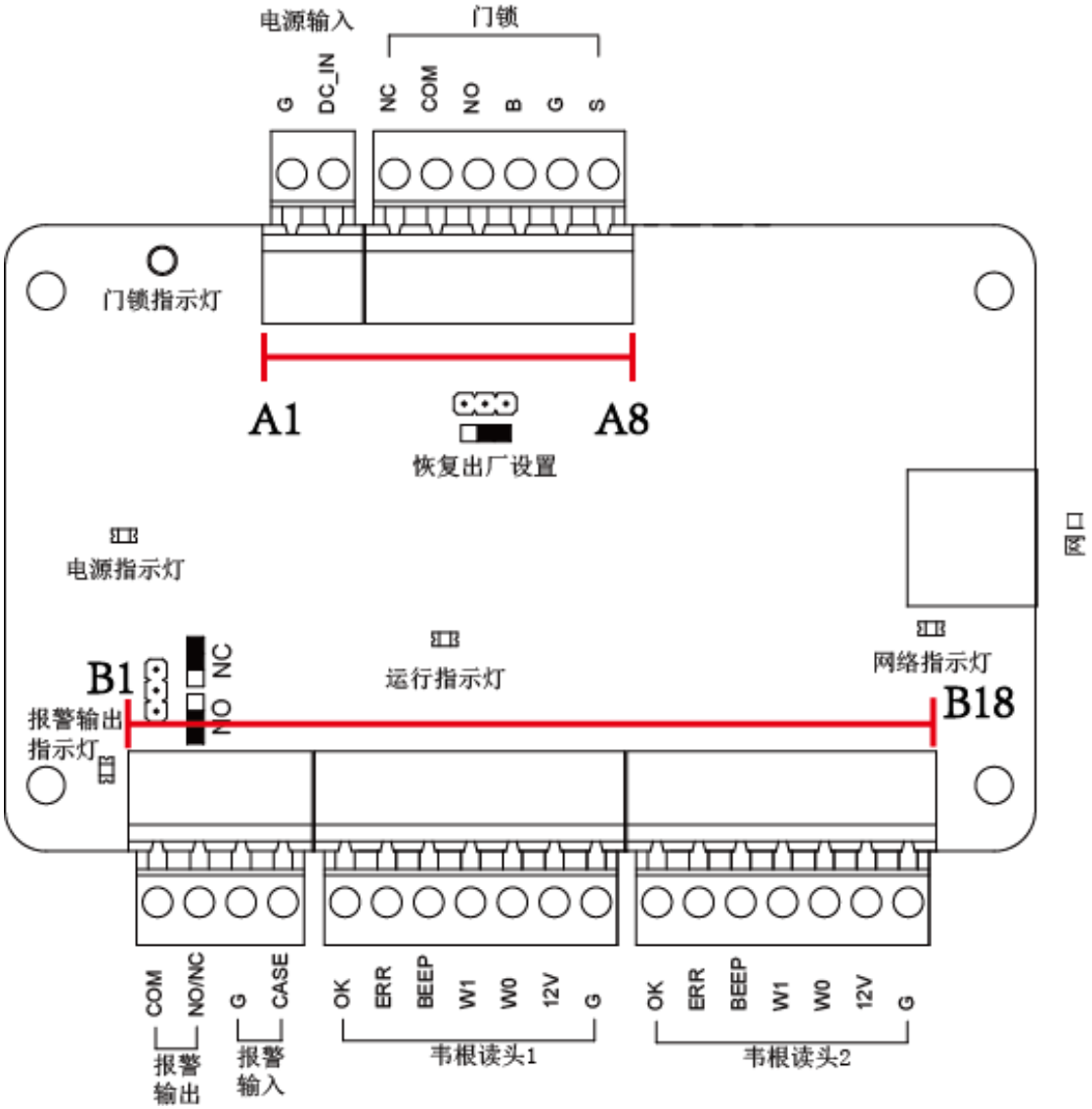
灯号及开关描述

组件序号	组件说明		
	单门禁控制主机	双门禁控制主机	四门禁控制主机
1	网络指示灯	网络指示灯	网络指示灯
2	电源指示灯	电源指示灯	电源指示灯
3	恢复出厂值设置选择	恢复出厂值设置选择	恢复出厂值设置选择
4	运行指示灯	运行指示灯	运行指示灯
5	报警输出指示灯	报警输出指示灯	报警输出指示灯
6	报警输出（NO/NC）选择	报警输出（NO/NC）选择	报警输出（NO/NC）选择
7	门锁指示灯	门锁 1 指示灯	门锁 1 指示灯
8		门锁 2 指示灯	门锁 2 指示灯
9			门锁 3 指示灯
10			门锁 4 指示灯

第3章 连接端子说明

3.1 连接端子及端子说明

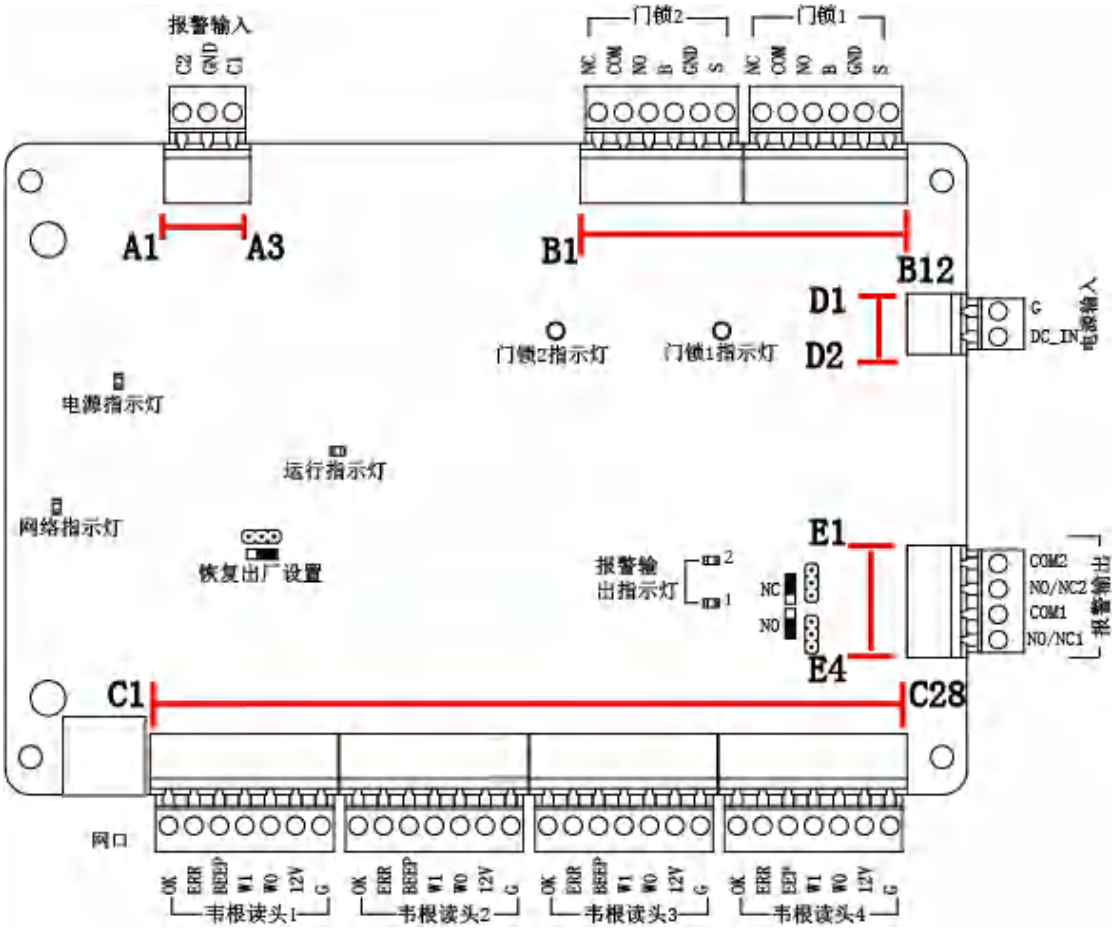
3.1.1 单门禁控制主机连接端子及端子说明



单门禁控制主机连接端子描述

端子序号	单门禁控制主机		
A1	电源	GND	DC12V 接地输入
A2		+12V	DC12V 正极输入
A3	门锁	NC	门锁继电器输出干接点
A4		COM	
A5		NO	
A6	开门按钮	BUTTON	开门按钮输入
A7		GND	开门按钮和门磁侦测公用接地信号
A8	门磁侦测	SENSOR	门磁侦测
B1	报警输出	COM	报警继电器输出(干接点)
B2		NO/NC	
B3	报警输入	GND	信号接地
B4		IN	事件输入
B5	韦根读头 1	OK	读卡器灯号控制输出(有效卡输出)
B6		ERR	读卡器灯号控制输出(无效卡输出)
B7		BZ	读卡器蜂鸣器控制输出
B8		W1	韦根读头数据输入 Data1
B9		W0	韦根读头数据输入 Data0
B10		PWR	读卡机电源输出
B11		GND	
B12	韦根读头 2	OK	读卡器灯号控制输出(有效卡输出)
B13		ERR	读卡器灯号控制输出(无效卡输出)
B14		BZ	读卡器蜂鸣器控制输出
B15		W1	韦根读头数据输入 Data1
B16		W0	韦根读头数据输入 Data0
B17		PWR	读卡机电源输出
B18		GND	

3.1.2 双门禁控制主机连接端子及端子说明

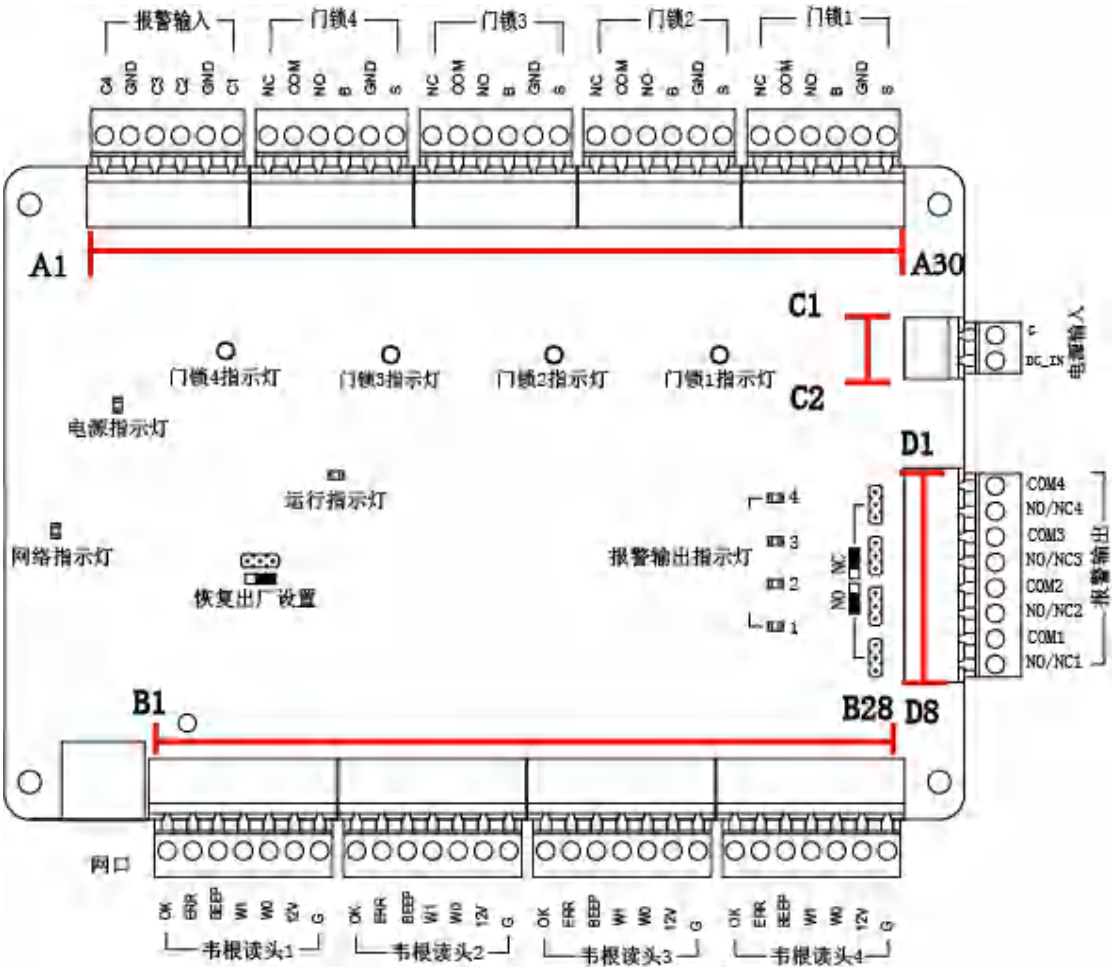


双门禁控制主机连接端子描述

端子序号	双门禁控制主机		
A1	报警输入	IN2	事件输入 2
A2		GND	信号接地
A3		IN1	事件输入 1
B1	门锁 2	NC	门锁继电器输出干接点
B2		COM	
B3		NO	
B4	开门按钮 2	BUTTON	开门按钮输入
B5		GND	开门按钮和门磁侦测公用接地信号
B6	门磁侦测 2	SENSOR	门磁侦测
B7	门锁 1	NC	门锁继电器输出干接点
B8		COM	
B9		NO	
B10	开门按钮 1	BUTTON	开门按钮输入
B11		GND	开门按钮和门磁侦测公用接地信号
B12	门磁侦测 1	SENSOR	门磁侦测

端子序号	双门禁控制主机		
D1	电源	GND	DC12V 接地输入
D2		+12V	DC12V 正极输入
E1	报警输出 2	COM2	报警继电器 2 输出(干接点)
E2		NO/NC2	
E3	报警输出 1	COM1	报警继电器 1 输出(干接点)
E4		NO/NC1	
C1	韦根读头 1	OK	读卡器灯号控制输出(有效卡输出)
C2		ERR	读卡器灯号控制输出(无效卡输出)
C3		BZ	读卡器蜂鸣器控制输出
C4		W1	韦根读头数据输入 Data1
C5		W0	韦根读头数据输入 Data0
C6		PWR	读卡机电源输出
C7		GND	
C8	韦根读头 2	OK	读卡器灯号控制输出(有效卡输出)
C9		ERR	读卡器灯号控制输出(无效卡输出)
C10		BZ	读卡器蜂鸣器控制输出
C11		W1	韦根读头数据输入 Data1
C12		W0	韦根读头数据输入 Data0
C13		PWR	读卡机电源输出
C14		GND	
C15	韦根读头 3	OK	读卡器灯号控制输出(有效卡输出)
C16		ERR	读卡器灯号控制输出(无效卡输出)
C17		BZ	读卡器蜂鸣器控制输出
C18		W1	韦根读头数据输入 Data1
C19		W0	韦根读头数据输入 Data0
C20		PWR	读卡机电源输出
C21		GND	
C22	韦根读头 4	OK	读卡器灯号控制输出(有效卡输出)
C23		ERR	读卡器灯号控制输出(无效卡输出)
C24		BZ	读卡器蜂鸣器控制输出
C25		W1	韦根读头数据输入 Data1
C26		W0	韦根读头数据输入 Data0
C27		PWR	读卡机电源输出
C28		GND	

3.1.3 四门禁控制主机连接端子及端子说明



四门禁控制主机连接端子描述

端子序号	双门禁控制主机		
A1	报警输入	IN4	事件输入 4
A2		GND	信号接地
A3		IN3	事件输入 3
A4		IN2	事件输入 2
A5		GND	信号接地
A6		IN1	事件输入 1
A7	门锁 4	NC	门锁继电器输出干接点
A8		COM	
A9		NO	
A10	开门按钮 4	BUTTON	开门按钮输入
A11		GND	开门按钮和门磁侦测公用接地信号
A12	门磁侦测 4	SENSOR	门磁侦测

端子序号	双门禁控制主机		
A13	门锁 3	NC	门锁继电器输出干接点
A14		COM	
A15		NO	
A16	开门按钮 3	BUTTON	开门按钮输入
A17		GND	开门按钮和门磁侦测公用接地信号
A18	门磁侦测 3	SENSOR	门磁侦测
A19	门锁 2	NC	门锁继电器输出干接点
A20		COM	
A21		NO	
A22	开门按钮 2	BUTTON	开门按钮输入
A23		GND	开门按钮和门磁侦测公用接地信号
A24	门磁侦测 2	SENSOR	门磁侦测
A25	门锁 1	NC	门锁继电器输出干接点
A26		COM	
A27		NO	
A28	开门按钮 1	BUTTON	开门按钮输入
A29		GND	开门按钮和门磁侦测公用接地信号
A30	门磁侦测 1	SENSOR	门磁侦测
B1	韦根读头 1	OK	读卡器灯号控制输出(有效卡输出)
B2		ERR	读卡器灯号控制输出(无效卡输出)
B3		BZ	读卡器蜂鸣器控制输出
B4		W1	韦根读头数据输入 Data1
B5		W0	韦根读头数据输入 Data0
B6		PWR	读卡机电源输出
B7		GND	
B8	韦根读头 2	OK	读卡器灯号控制输出(有效卡输出)
B9		ERR	读卡器灯号控制输出(无效卡输出)
B10		BZ	读卡器蜂鸣器控制输出
B11		W1	韦根读头数据输入 Data1
B12		W0	韦根读头数据输入 Data0
B13		PWR	读卡机电源输出
B14		GND	
B15	韦根读头 3	OK	读卡器灯号控制输出(有效卡输出)
B16		ERR	读卡器灯号控制输出(无效卡输出)
B17		BZ	读卡器蜂鸣器控制输出

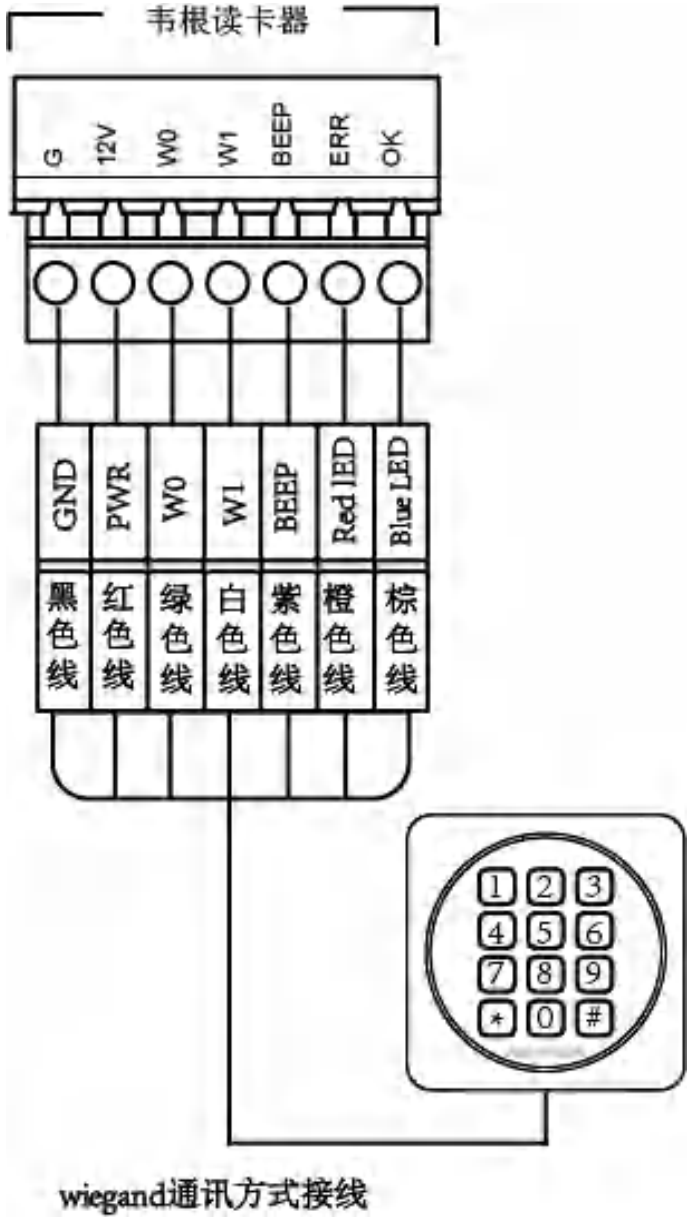
端子序号	双门禁控制主机		
B18		W1	韦根读头数据输入 Data1
B19		W0	韦根读头数据输入 Data0
B20		PWR	读卡机电源输出
B21		GND	
B22	韦根读头 4	OK	读卡器灯号控制输出(有效卡输出)
B23		ERR	读卡器灯号控制输出(无效卡输出)
B24		BZ	读卡器蜂鸣器控制输出
B25		W1	韦根读头数据输入 Data1
B26		W0	韦根读头数据输入 Data0
B27		PWR	读卡机电源输出
B28		GND	
C1	电源	GND	DC12V 接地输入
C2		+12V	DC12V 正极输入
D1	报警输出 4	COM4	报警继电器 1 输出(干接点)
D2		NO/NC4	
D3	报警输出 3	COM3	报警继电器 1 输出(干接点)
D4		NO/NC3	
D5	报警输出 2	COM2	报警继电器 1 输出(干接点)
D6		NO/NC2	
D7	报警输出 1	COM1	报警继电器 1 输出(干接点)
D8		NO/NC1	

说明

单门禁控制主机：韦根读卡器 1 对应门 1 的进门读卡器，韦根读卡器 2 对应门 1 的出门读卡器。**双门禁控制主机**：韦根读卡器 1、3 分别对应门 1、2 的进门读卡器，韦根读卡器 2、4 分别对应门 1、2 的出门读卡器。**四门禁控制主机**：韦根读卡器 1、2、3、4 分别对应门 1、2、3、4 的进门读卡器。

读卡器电源由主机电源输入端所供应，每一个读卡器的消耗电流约 150mA，安装时请视读卡器的数量与传输距离，适量增加主机电源输入电流的安培数或将读卡器的电源独立;读卡器电源独立供电时，务必将读卡器的 GND 与主机上读卡器电源供应端的 GND 端连接。

3.2 韦根读卡器接法



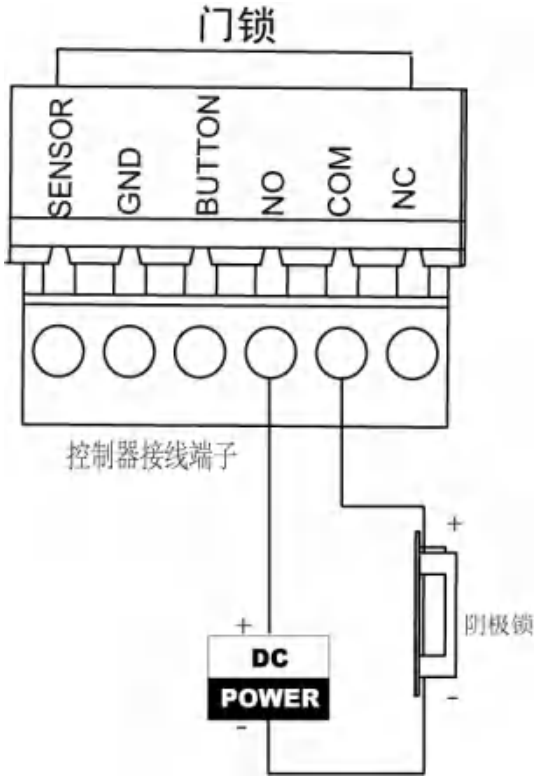
wiegand通讯方式接线

说明

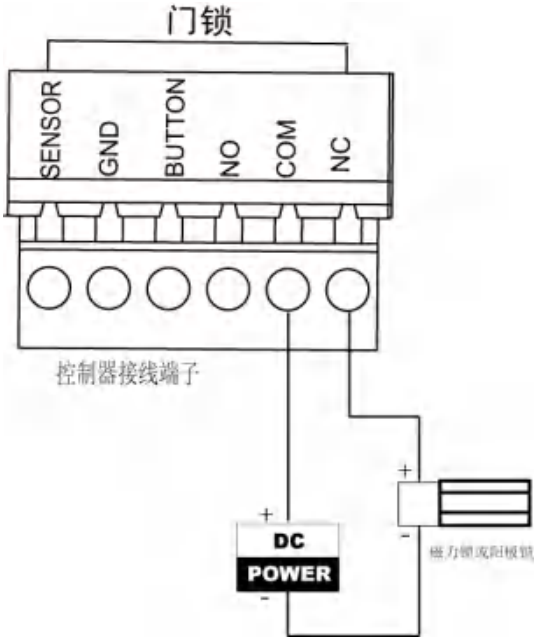
主机如果要控制韦根读卡器的蜂鸣声和LED，必须将OK/ERR/BZ端子接好。

3.3 电锁安装示意图

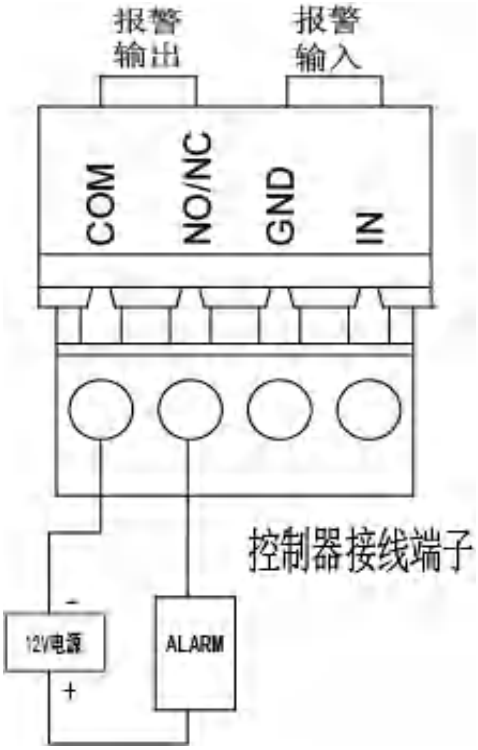
3.3.1 阴极锁安装示意图



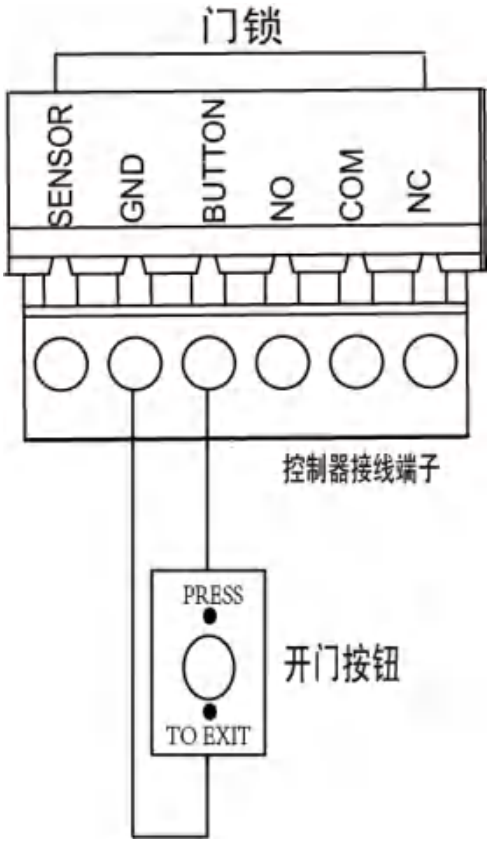
3.3.2 磁力锁/阳极锁安装示意图



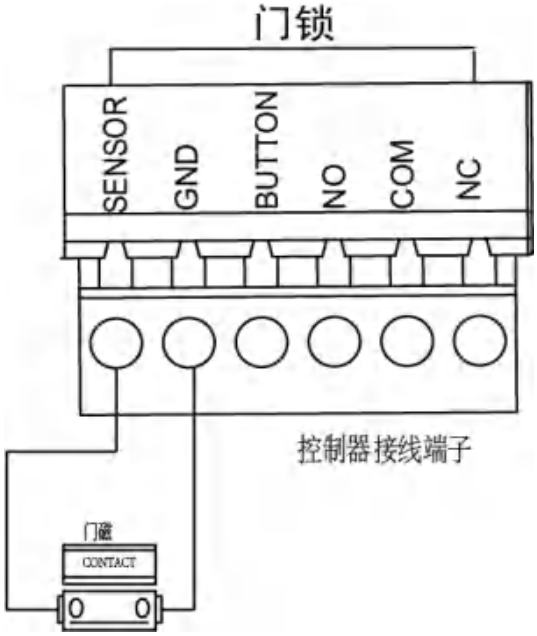
3.4 外接报警设备示意图



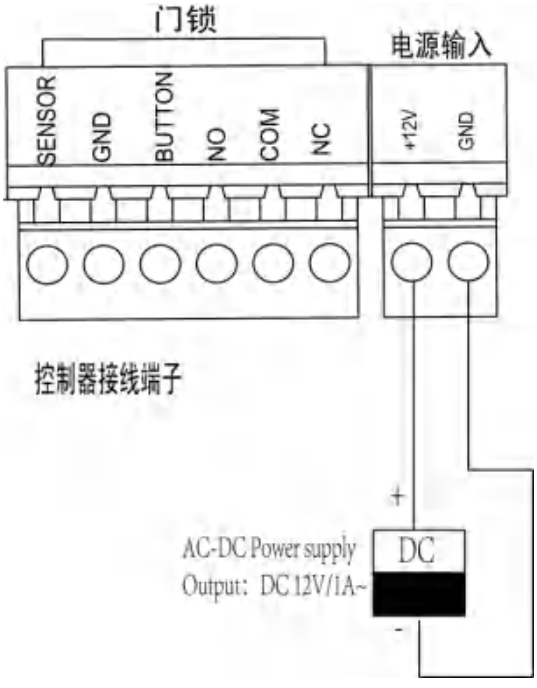
3.5 开门按钮接线图



3.6 门禁侦测连接示意图



3.7 电源供应器安装示意图



第4章

第4章 设定

4.1 硬件初始化设定

方案一:

从 Normal 端拔掉跳帽;

将设备断电重启，设备发出滴---的长鸣;

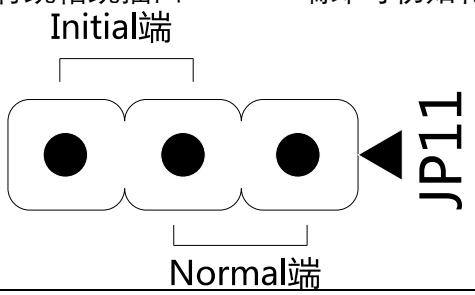
蜂鸣器停止鸣叫后，再将短路帽插回 Normal 端即可初始化硬件;

方案二:

将 JP40 的跳帽从 Normal 端跳到 (INITIAL)端;

将设备断电重启，此时设备发出滴---的长鸣。

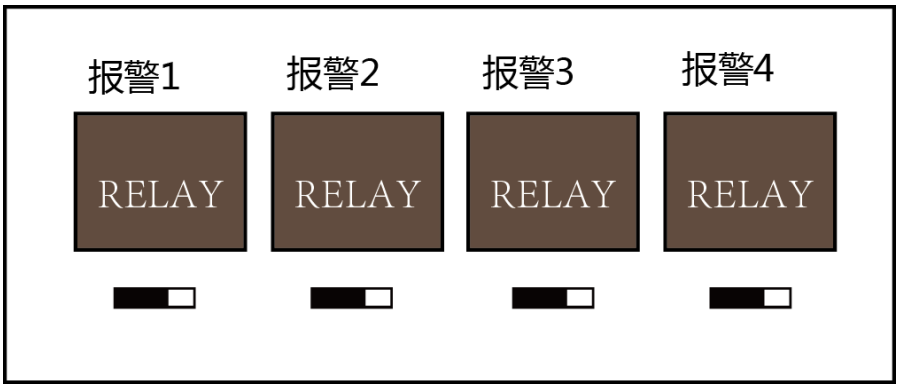
蜂鸣器停止鸣叫后，将跳帽跳插回 Normal 端即可初始化硬件。



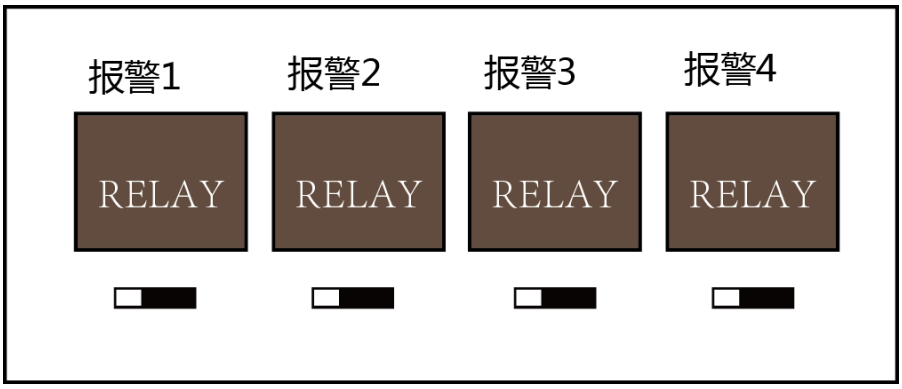
硬件初始化会将设备所有参数恢复默认，同时清除设备事件。

4.2 报警继电器输出 NO/NC 状态示意图

报警继电器输出常开（NO）状态



报警继电器输出常闭（NC）状态


报警1
报警2
报警3
报警4
RELAY
RELAY
RELAY
RELAY

第5章 激活及配置

控制主机首次使用时需要进行激活并设置登录密码，才能正常登录和使用。您可以通过两种方式激活控制主机，分别是通过 SADP 软件以及 iVMS-4200 客户端软件方式激活。

控制主机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

从官网下载的 SADP 软件，运行软件后，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。

选中需要激活的控制主机，将在列表右侧显示控制主机的相关信息。

在“激活设备”栏处设置控制主机密码，并单击“确定”完成激活。

成功激活控制主机后，列表中“激活状态”会更新为“已激活”。

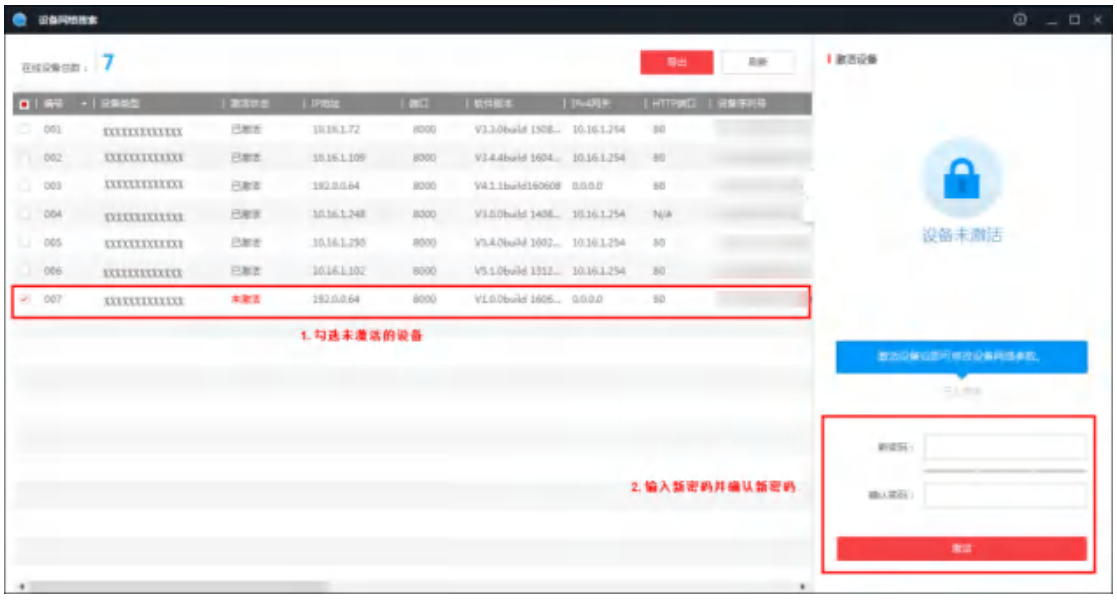


图5-1 激活设备

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。

修改设备 IP 地址。

在设备列表中勾选中已激活的设备。

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。

修改完毕后输入激活设备时设置的密码，并点击“修改”。提示“修改参数成功”则表示 IP 等参数设置生效。

说明

设置 IP 地址时，请保持控制主机 IP 地址与电脑 IP 地址处于同一网内。

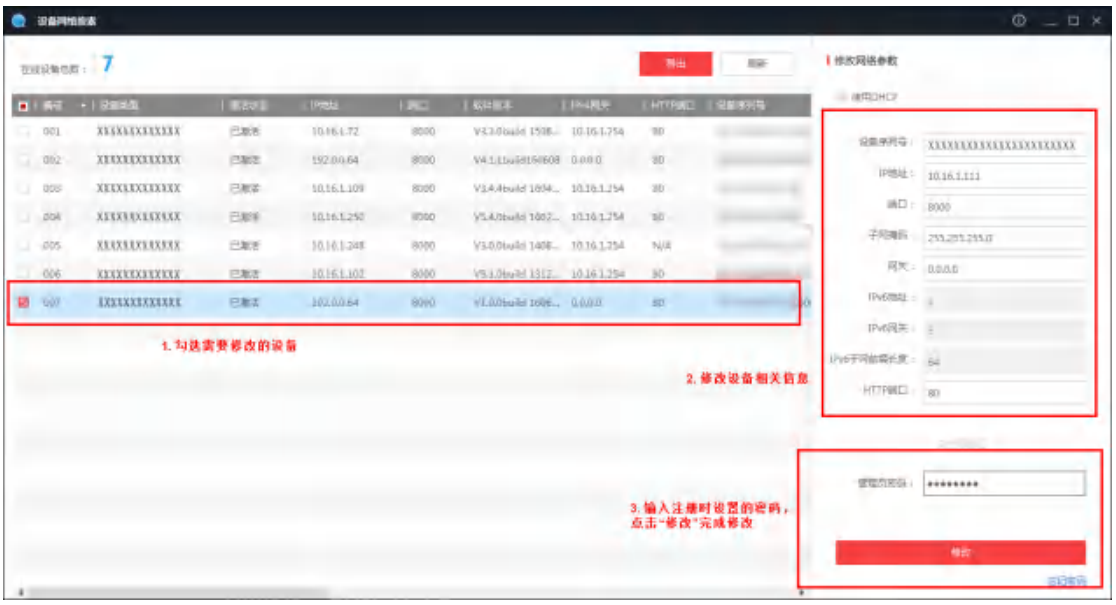


图5-2 修改控制主机信息

5.2 通过客户端软件激活

安装随机光盘或从官网下载的客户端软件，运行客户端软件后，点击控制面板下的“设备管理”进入设备管理界面。

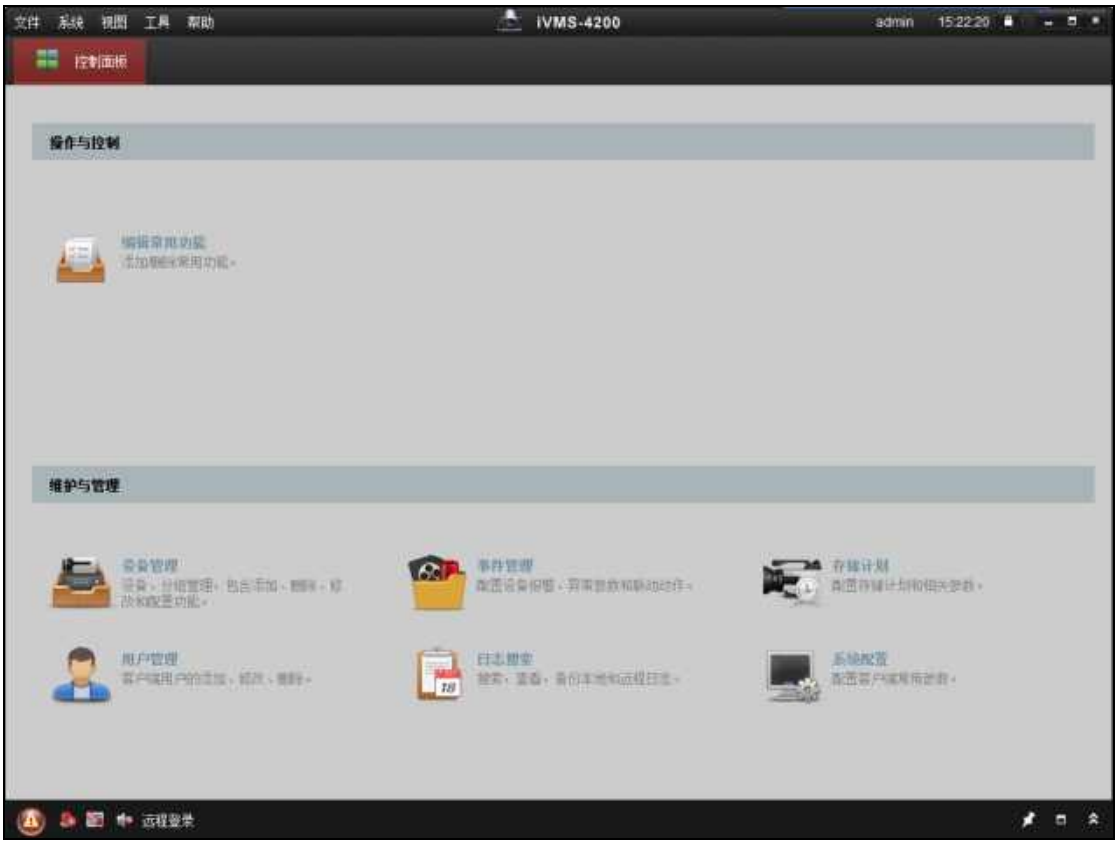


图5-3 设备管理

在弹出的“控制器管理”界面，可查看到“在线设备”列表。

图5-4 设备列表

选中需要激活的设备行，然后单击“激活”按钮。

在弹出的“激活”页面，输入“admin”用户的密码并单击“确定”。成功激活设备后，列表中“安全状态”会更新为“已激活”。

图5-5 激活控制主机

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。

修改设备网络信息。

勾选已激活的控制主机行，单击“修改网络信息”，在弹出的页面中修改控制主机的 IP 地址、网关等信息。修改完毕后输入激活设备时设置的密码，单击“确定”。

说明

设置 IP 地址时，请保持控制主机 IP 地址与电脑 IP 地址处于同一网内。

第6章 客户端操作

您可通过 iVMS-4200 客户端配置、操作门禁设备。本章节将介绍门禁相关的客户端功能及操作步骤，不包含全部客户端功能及操作步骤。有关全部客户端功能及操作，请参考 iVMS-4200 客户端用户手册。

6.1 功能模块

iVMS-4200 控制面板如下所示：

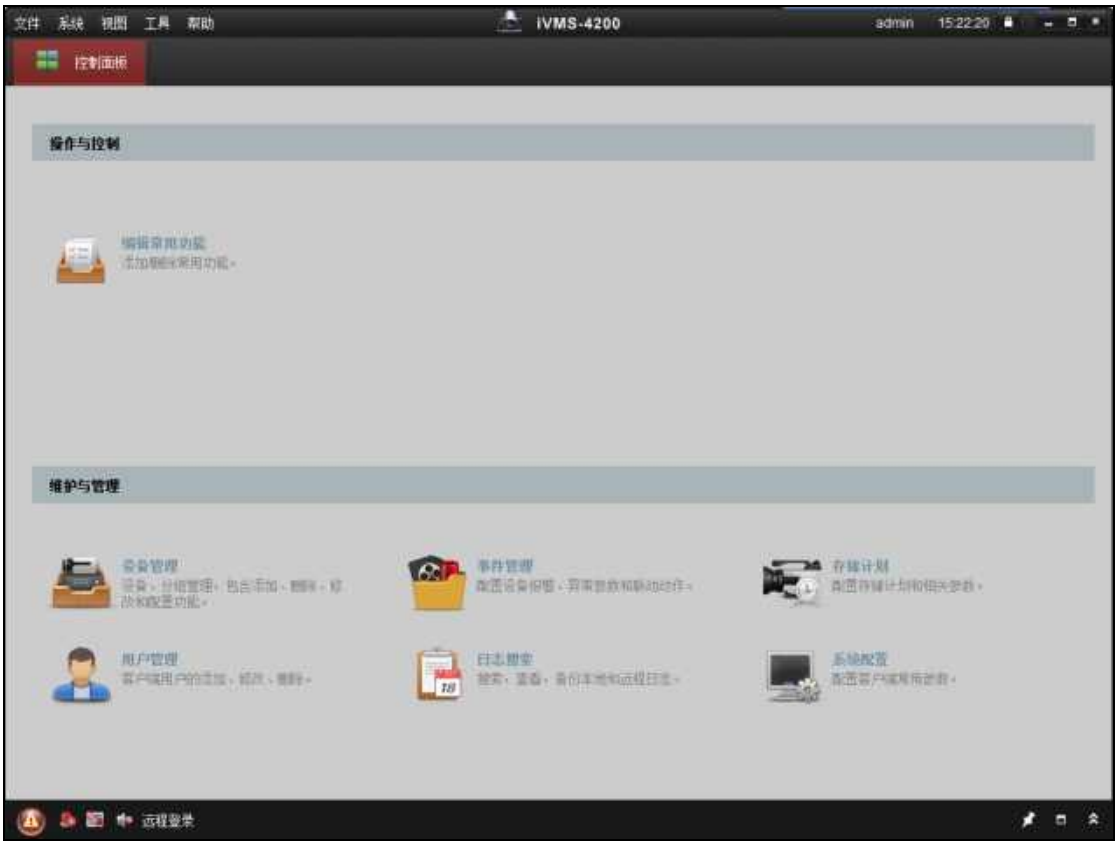


图6-1 控制面板

具体菜单内容如下表所示：

菜单说明表

文件	**打开抓图文件**	搜索并查看存储在本地的抓拍图片。
	打开视频文件	搜索并查看存储在本地的录像。
	打开日志文件	查看日志文件。
	退出	退出 iVMS-4200 客户端。
系统	**加锁**	锁住屏幕。锁住后点击屏幕任意处，并重新登录以解锁。
	切换用户	切换登录用户。
	导入客户端配置文件	从本地导入客户端配置文件。

	导出客户端配置文件	将客户端配置文件导出到本地。
	定时导出	可定时导出日志文件。
视图	**1024*768**	1024*768 像素窗口。
	1280*1024	1280*1024 像素窗口。
	1440*900	1440*900 像素窗口。
	1680*1050	1680*1050 像素窗口。
	最大化	将窗口最大化。
	控制面板	进入控制面板界面。
	主预览	打开主预览页面。
	远程回放	打开远程回放页面。
	门禁控制	打开门禁控制页面。
	状态监控	打开状态监控页面。
	考勤管理	打开考勤管理页面。
	报警主机	打开报警主机页面。
	实时处警	打开实时处警页面。
	电视墙	打开电视墙页面。
	电子地图	打开电子地图页面。
	辅屏预览	打开辅屏预览窗口。
工具	**设备管理**	打开设备管理页面。
	事件管理	打开事件管理页面。
	存储计划	打开存储计划页面。
	用户管理	打开用户管理页面
	日志搜索	打开日志搜索页面。
	系统配置	打开系统配置页面。
	广播	选择设备进行广播。
	设备布防控制	配置设备布防状态。
	报警输出控制	开启/关闭报警输出。
	批量控制雨刷	批量开启/关闭设备雨刷。
	批量校时	批量为设备校时。
	播放器	打开播放器播放录像文件。
	视频摘要回放	查看视频摘要录像。
	邮件队列	查看等待发送的邮件队列。
帮助	**打开视频向导**	打开客户端视频向导。
	打开电视墙向导	打开电视墙向导，可快速配置并使用电视墙模块。
	打开报警向导	打开报警向导，可快速配置并使用报警模块。
	打开门禁可视对讲向导	打开门禁和可视对讲向导,可快速配置和使用门禁及可视对讲模块。
	打开考勤向导	打开考勤向导，可快速配置和使用考勤模块。

	用户手册	查看用户手册。或按 F1 键查看。
	关于	查看客户端的基本信息。
	语言	查看客户端语言。

点击控制面板中的“编辑常用功能”按钮打开“编辑常用功能”窗口，可勾选需要添加的模块。

点击“确定”。选择的模块将在控制面板的“操作与控制”中显示。

图6-2 编辑常用功能窗口

功能模块详细信息如下所示：

	显示监控点的预览或回放画面，以及监控点的操作功能。
	搜索并回放监控点的远程录像文件，以及回放的相关操作功能。
	对门禁设备的人员、卡片以及事件的配置。也可管理可视对讲设备。
	监控门禁设备的门状态，查看报警以及刷卡记录。
	配置考勤规则以及统计和查看考勤结果。
	控制和监控报警主机的防区和子系统。
	实时处理报警主机 CID 报警，也可查看历史处警信息。

	显示报警事件列表。
	电视墙的配置以及操作功能。
	可添加、修改和删除地图。也可配置地图热点和热区。
	控制和监视报警主机的防区和子系统。
	设备以及分组管理，包括添加、删除、修改和配置设备。
	配置设备报警、异常参数和联动动作。
	配置存储计划和相关参数。
	客户端用户的添加、修改和删除。
	搜索、查看和备份本地以及远程日志。
	配置客户端常用参数。

6.2 用户登录

首次运行软件需要创建一个超级用户，用户名和密码自定义。

图6-3 注册超级用户

说明

- 用户名不能包含字符：\/:*?"<>|
- 密码长度必须为 8-16 位，由数字、小写字母、大写字母、特殊字符的两种及以上类型组合而成，密码不能与用户名相同或相反。

若软件已经注册了管理员账户，则启动软件后将显示用户登录对话窗口。

选择用户名，输入密码后点击“登录”进入软件运行界面，勾选“启用自动登录”，则下次启动软件以当前用户自动登录。

图6-4 登录界面

6.3 系统配置

步骤1. 在控制面板中选择  ，进入系统配置界面。

图6-5 门禁参数设置

步骤2. 点击“门禁”进入门禁配置页面。

步骤3. 可勾选“自动同步门禁事件”后，将设备漏传的门禁事件同步到客户端中。

勾选后可配置自动同步时间，客户端将在设置的时间自动从设备中同步漏传的门禁事件到客户端。

6.4 门禁管理

在控制版面点击 编辑常用功能按钮，勾选“门禁控制”，系统将自动将跟门禁控制模块相关的模块显示在控制面板中。

控制面板点击 门禁控制按钮进入门禁控制模块。

首次打开门禁控制模块，需要选择场景。可选择住宅模式和非住宅模式。点击“确定”完成选择。

若选择住宅模式，无法在添加人员时配置考勤规则。

图6-6 场景选择窗口

导航按钮如下所示：

	组织管理	管理组织、人员以及卡片
	计划模板	配置周计划、假日组和计划模板
	权限组	为人员和设备分配门禁权限
	高级配置	包括配置门禁参数、读卡器认证、多重认证、首卡开门、反潜回、多门互锁、手机白名单和认证码
	可视对讲	配置客户端和住户之间的可视对讲功能，搜索通话记录以及发布公告
	信息查询	搜索门禁历史事件、通话记录、开锁记录和公告信息
	设备管理	管理门禁和可视对讲设备

6.4.1 设备管理

在门禁控制模块点击界面左侧设备管理图标进入门禁控制下的设备管理界面。

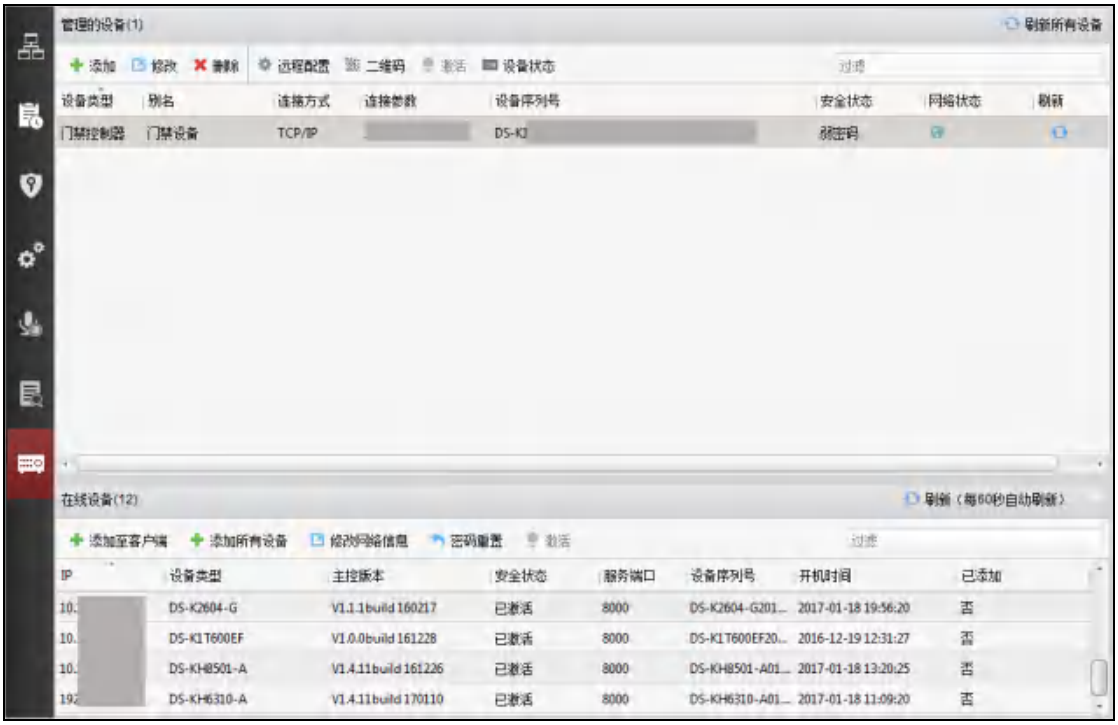


图6-7 设备管理界面

说明

添加完设备后，需要在“工具”-“布防配置”中查看设备布防状态。若设备未布防，您将无法从客户端接收设备上传的实时事件。具体如何布防/撤防设备，详见 6.9 布防控制。

设备添加

添加在线设备

步骤1. 在在线设备列表中选择一台设备并点击“添加至客户端”。

图6-8 添加单个在线设备

步骤2. 在弹出的添加设备对话框中，输入别名、用户名、密码。

步骤3. 点击“添加”即可完成局域网在线设备的添加。

或批量添加在线设备。

1） 在在线设备列表中，点击“添加所有设备”。

或按住 Ctrl 键选择在线并已激活设备的某几台设备，并点击“添加至客户端”。

2） 在弹出的添加设备对话框，输入用户名和密码。

3） 点击“添加”即可完成批量添加设备。

说明

默认勾选导入至分组，组名以设备别名命名，并导入该设备所有的编码通道和报警输入资源和门禁点。

批量添加设备要求设备用户名和密码一致，以设备 IP 自动生成分组。

通过IP/域名添加设备

步骤1. 在管理设备列表中点击“添加”。

步骤2. 在弹出的对话框中选择 IP/域名添加模式。

图6-9 添加设备对话框-IP/域名

步骤3. 输入别名、IP/域名地址、端口、用户名和密码。

步骤4. 点击“添加”完成设备的添加。

说明

默认勾选导入至分组，组名以设备别名命名，并导入该设备所有的编码通道和报警输入资源和门禁点。

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。

通过IP段添加设备

在管理设备列表栏中选择“添加”，

在弹出对话框中选择 IP 段添加模式。

图6-10 添加设备对话框-IP 段

输入别名、IP 地址、端口、用户名和密码。

点击“添加”完成设备的添加。

说明

默认勾选导入至分组，组名以设备别名命名，并导入该设备所有的编码通道和报警输入资源和门禁点。

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。

通过EHome账号添加设备

可通过EHome协议添加门禁设备。在添加设备前，需要在网络配置中心配置网络参数，详见6.4.1 设备管理下的网络配置章节。

在添加窗口中选择 EHome 添加模式。

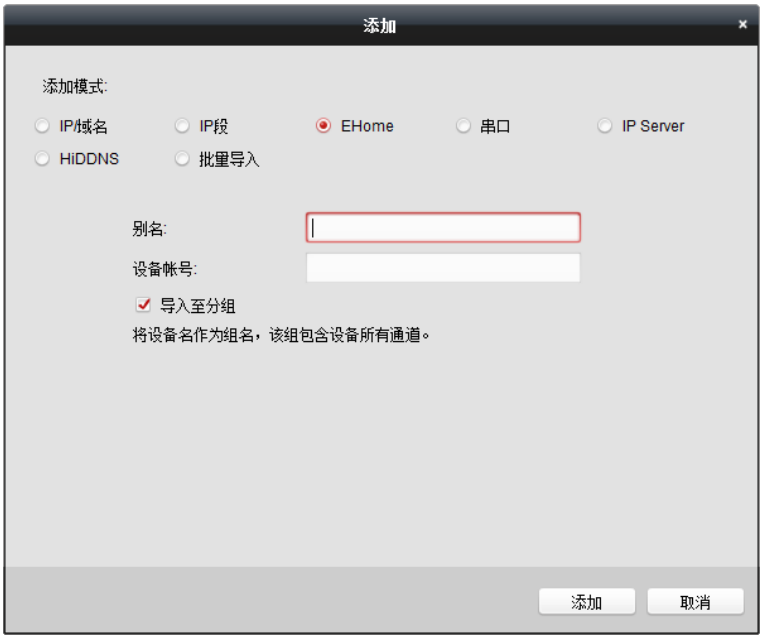


图6-11 添加设备对话框-EHome

输入 EHome 的别名和账号。

点击“添加”完成设备添加。其中账号为您在 EHome 协议上注册的账户名称。

说明

默认勾选导入至分组，组名以设备别名命名，并导入该设备所有的编码通道和报警输入资源和门禁点。

通过串口添加设备

可通过门禁设备的串口添加设备。

在添加窗口中选择串口添加模式。

图6-12 添加设备对话框-串口

配置别名、串口号、波特率和拨码。

点击“添加”完成设备添加。此处拨码为设备的拨码地址。

说明

默认勾选导入至分组，组名以设备别名命名，并导入该设备所有的编码通道和报警输入资源和门禁点。

通过IP Server添加设备

- 在添加窗口中选择 IP Server 添加模式。

图6-13 添加设备对话框-IP Server

- 配置别名、服务器地址、设备标识、用户名和密码。
- 点击“添加”完成设备添加。

此处服务器地址为 IP Server 的服务器地址；设备标识为远程设备名或设备序列号。

说明

默认勾选导入至分组，组名以设备别名命名，并导入该设备所有的编码通道和报警输入资源和门禁点。

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。

通过HiDDNS添加设备

步骤1. 在添加窗口中选择 HiDDNS 添加模式。

图6-14 添加设备对话框-HiDDNS

步骤2. 配置别名、服务器地址、设备域名、用户名和密码。

步骤3. 点击“添加”完成设备添加。

此处设备域名为域名解析服务器的地址，默认为 www.hiddns.com。

说明

默认勾选导入至分组，组名以设备别名命名，并导入该设备所有的编码通道和报警输入资源和门禁点。

- 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。

批量导入

通过导入 CSV 文件批量导入设备。可点击“导出模板”，将模板导出。

在添加窗口中选择批量导入添加模式，并点击 ... 选择需要导入的 CSV 文件。点击“添加”可批量添加设备。

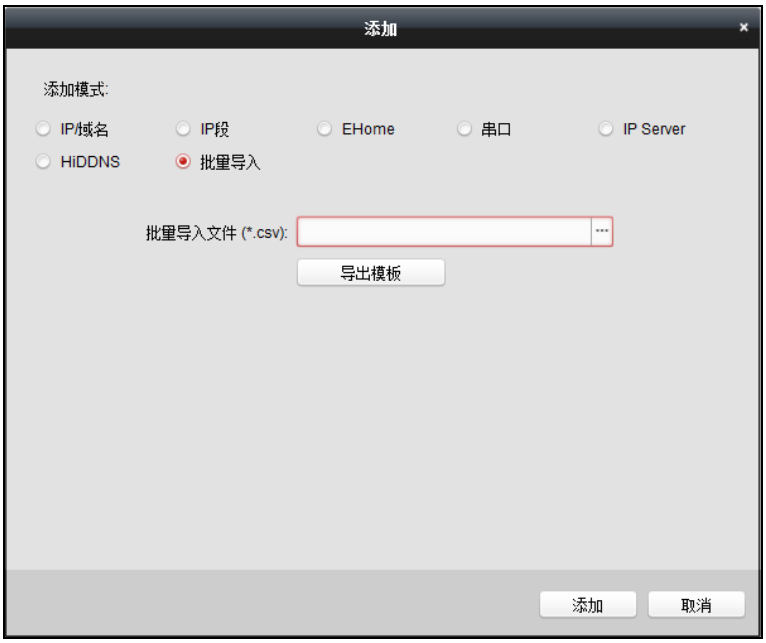


图6-15 添加设备对话框-批量导入

修改门禁设备

可修改门禁设备参数，包括设备基本信息、网络参数、抓拍参数、RS485参数、韦根参数以及M1卡加密参数。

修改基本信息

- 在设备管理界面选择一个门禁设备。
- 点击“修改”按钮，进入修改窗口。

图6-16 修改门禁设备窗口

- 可配置门禁设备的基本信息，包括设备添加模式、别名、地址、用户名和密码。

◆ 点击“修改”可保存参数。

网络配置

在修改界面，选择“网络配置”，可以网络配置，配置内容包括报告上传方式配置、网络中心配置和无线中心配置。

需设备支持才能使用此网络配置功能。

上传方式配置

通过配置上传中心组以及通道，您可上传通过 EHome 协议传输日志。

- 在管理的设备列表中，选择某一门禁设备，点击“修改”进入修改窗口。
- 点击“网络配置”，进入网络设置界面。
- 点击“上传方式配置”进入上传方式配置页面。

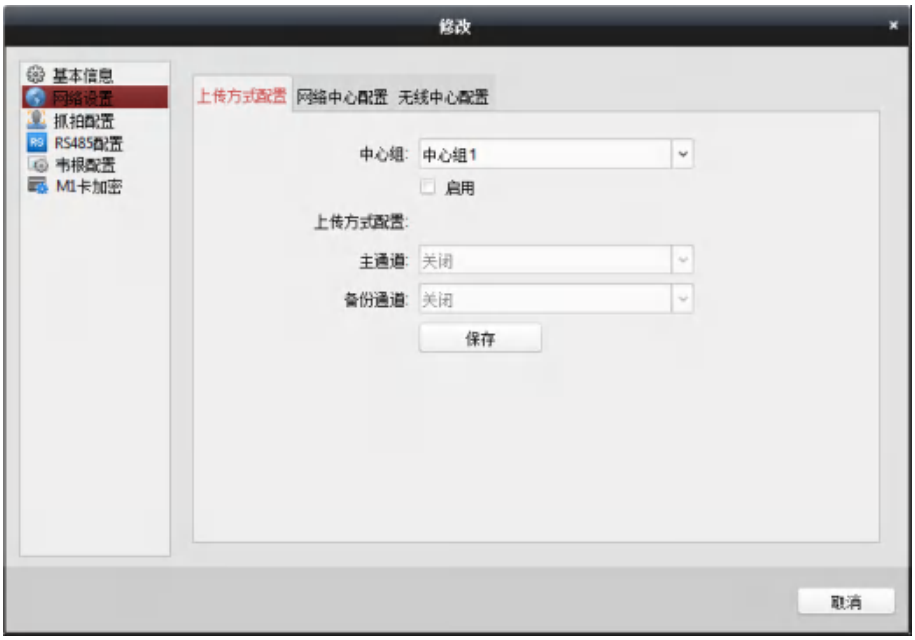


图6-17 上传方式配置

- 选择中心组。勾选“启用”，即启用已选择的中心组。
- 中心组开启后，可配置上传方式，包括主通道和备份通道。更多关于上传方式配置的参数内容，请参考下表。

上传方式配置信息表

内容	含义
中心组	在下拉菜单中选择需要上传的中心组。该型号的门禁指纹一体机有两个中心组可选。
主通道	在下拉菜单中选择“关”，“N1”和“G1”。
备份通道	在下拉菜单中可选择“关”，“N1”和“G1”。当主通道选择“关”时，备份通道默认“关”状态；当主通道选择 N1，备份通道只可选择 G1；当主通道选择 G1 时，备份通道只可选择 N1。

- 点击“保存”保存参数。

网络中心配置

需在此先配置 EHome 账号及其参数，方可在添加设备处添加 EHome 协议下的设备。

步骤1. 在修改窗口，点击“网络配置”，进入网络设置界面。

步骤2. 点击“网络中心配置”进入网络中心配置页面。

图6-18 网络中心配置

步骤3. 选择一个网络中心组，配置地址类型、配置 IP 地址/域名、输入端口号、为该网络中心选择一个协议类型，并输入设备账号名。

说明

协议类型只支持 EHome 协议。设备账号为 1-32 位字母、数字的组合。

EHome 端口号需设置为 1~65535。

门禁 EHome 端口号需配置为 7660。

可在远程配置中的 NTP 配置服务器地址中配置域名。详见远程配置章节中的修改时间。

步骤4. 点击“保存”保存参数。

无线中心配置

在修改窗口，点击“网络配置”，进入网络设置界面。

点击“无线中心配置”进入无线中心配置页面。

图6-19 无线中心配置

在下拉菜单中选择 APN 名称。可选择 CMNET 或 UNINET。并输入 SIM 卡号码。

选择网络中心组，输入 IP 地址和端口号并为该网络中心选择协议类型并设备账号。

说明

协议类型只支持 EHome 协议。

点击“保存”保存参数。

抓拍设置

需设备支持才能使用此功能。

在管理的设备列表中，选择某一设备，点击“修改”进入修改窗口。

点击“抓拍配置”可在弹出的配置框中设置联动抓拍和手动抓拍。

联动抓拍：

点击“联动抓拍”，配置抓拍次数和抓拍间隔。

可选择的抓拍次数有 1、2、3、4、5。

抓拍时间间隔为 100ms~1000ms。

点击“保存”即可保存参数。

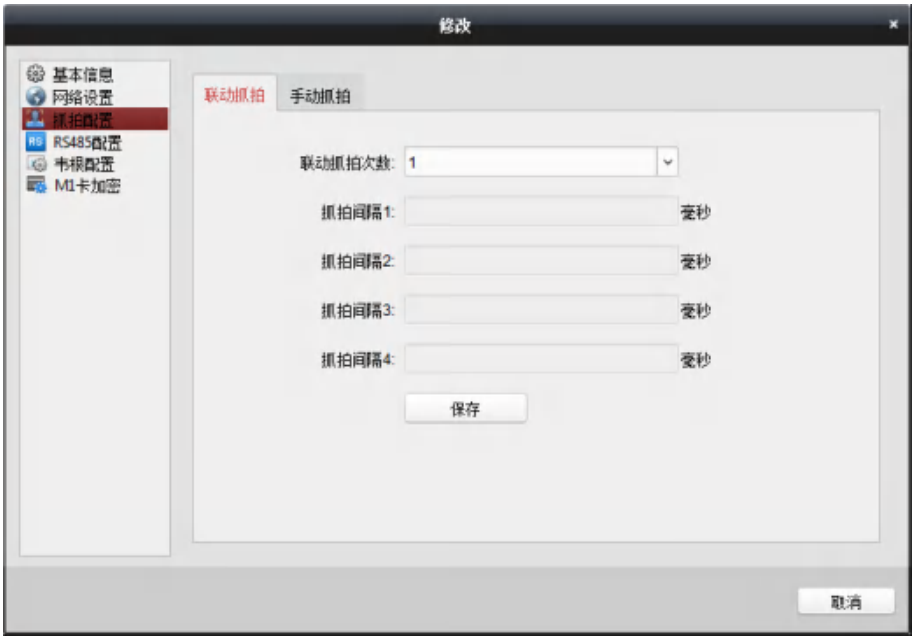


图6-20 联动抓图配置框

手动抓拍：

1） 点击“手动抓拍”，可配置抓拍图片的尺寸和图片质量。

图6-21 手动抓拍配置框

2） 点击“保存”保存参数。

可点击“恢复默认”恢复手动抓拍默认参数。

RS485配置

需设备支持才能使用此功能。

可设置设备的 RS485 参数，包括串口号、波特率、数据位、停止位、校验类型、通讯模式、和工作模式。根据设备功能才能显示相应的参数。

在管理的设备列表中，选择某一门禁设备，点击“修改”进入修改窗口。

点击“RS485 配置”可设置设备 RS485 参数，包括串口号、波特率、数据位、停止位、校验类型、通讯模式、和工作模式。

图6-22 RS485 配置框

点击“保存”完成配置，保存的配置将下发到设备。

说明

修改 RS485 工作模式后，需重启设备，配置才能生效。

韦根配置

需设备支持才能使用此功能。可配置设备的韦根参数，包括韦根编号和通信方向。

在管理的设备列表中，选择某一门禁设备，点击“修改”进入修改窗口。

点击“韦根配置”可设置设备韦根参数。

韦根编号：设置设备的韦根编号。

通信方向：可选择接收或者发送。

图6-23 韦根配置框

说明

若通信方向选择“发送”，则可配置韦根模式。可配置韦根 26 或韦根 34。

图6-24 韦根配置框 2

点击“保存”完成配置，保存的配置将下发到设备。

说明

修改韦根通讯方向后，需重启设备，配置才能生效。

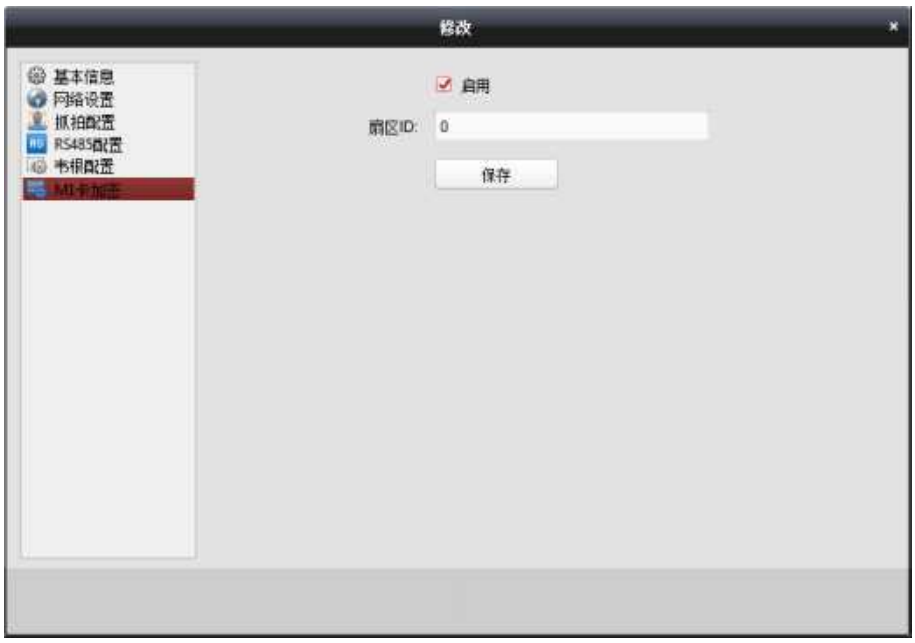
M1卡加密

M1 卡加密功能进一步提高了门禁权限认证安全级别。该功能启用前须使用本公司指定的发卡器配合客户端软件或者平台软件进行发卡。完成发卡动作后，即可在客户端上配置门禁控制器启用 M1 卡加密功能，配合使用该功能。

说明

- 门禁控制器及读卡器需支持该功能。
- 具体发卡操作详见 6.4.2 人员配置中的添加人员（管理卡片）章节。

- 在管理的设备列表中，选择某一门禁设备，点击“修改”进入修改窗口。
- 点击“M1 卡加密”进入 M1 卡加密页面。



- 在 M1 卡加密页面中勾选“启用”，以启用 M1 卡加密功能。
- 配置扇区 ID。
- 点击“保存”完成配置。保存的配置将下发到设备中。

说明

扇区 ID 范围为 1~100。

远程配置

点击“远程配置”，进入“远程配置”界面。在该界面可以远程远重启设备、恢复设备参数、远程配置报警触发器参数等。

设备信息

在远程配置界面，点击“系统”–“设备信息”进入现实设备基本信息界面。在此界面可查看设备基本信息和版本信息。

图6-25 远程配置设备信息界面

修改设备名称

在远程配置界面，点击“系统”–“常用”，可在此界面配置设备名称以及是否录像覆盖。点击“保存”将修改的参数保存。

图6-26 远程配置常用界面

修改时间

步骤1. 在远程配置界面，点击“系统”–“时间”。

步骤2. 在此界面可配置时区。

步骤3. （可选）勾选“启用 NTP”并配置 NTP 服务器地址、NTP 端口以及校时间隔。

步骤4. （可选）勾选“启用 DST”并配置夏令时开始时间、结束时间和偏移时间。

步骤5. 点击“保存”将配置的参数保存。

图6-27 远程配置时间界面

系统维护

在远程配置界面，点击“系统”–“系统维护”。

点击“重启”，此设备将重新启动。

或点击“恢复默认参数”，此设备的参数将恢复为默认参数，但不恢复设备 IP 地址信息。

或点击“完全恢复默认参数”，此设备的所有参数将被恢复成默认参数，再次使用此设备需要重新激活。

（可选）在远程升级部分，可在下拉框中选择升级文件类型，点击 ... 并选择升级文件。

说明

若选择读卡器升级文件类型，则需配置设备号后再选择升级文件。

仅使用 RS-485 接线的读卡器支持读卡器升级功能。

点击“升级”开始升级设备。

图6-28 远程配置系统维护界面

管理用户

在远程配置界面，点击“系统”-“用户”。

图6-29 远程配置用户界面

点击添加可以添加用户。（梯控设备不支持此功能。）

或选择一个用户，点击编辑可编辑该用户密码、IP 地址、物理地址以及用户权限。点击确定保存配置。

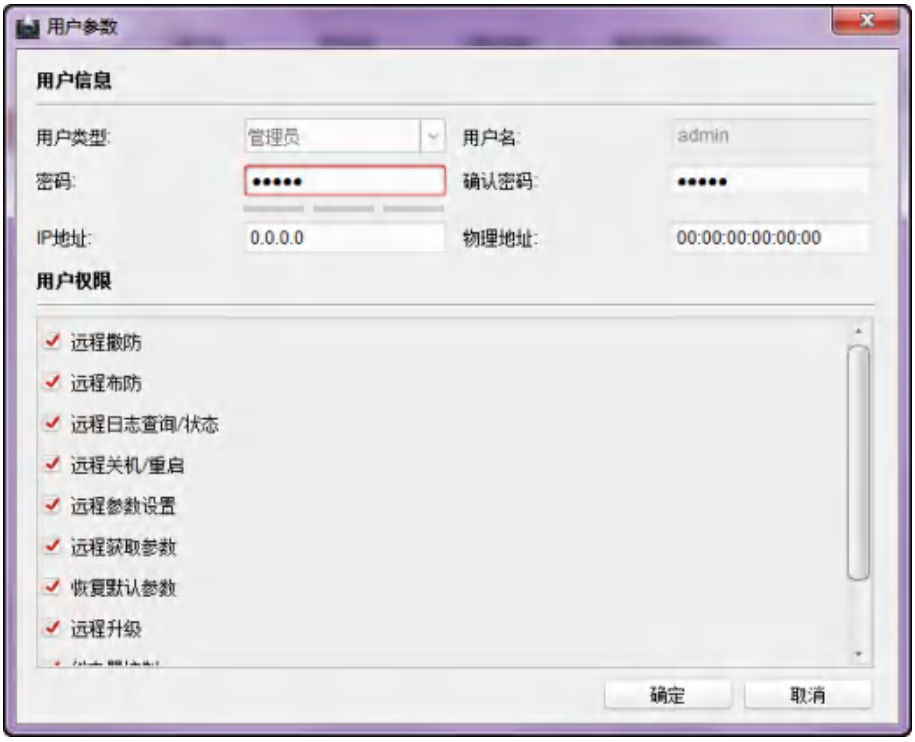


图6-30 用户参数修改窗口

配置安全参数

在远程配置界面，点击“系统”-“安全配置”。

选择安全模式等级。可选择兼容模式或者安全模式。

点击“保存”将配置保存。

图6-31 远程配置安全参数界面

配置设备网络参数

点击“网络”–“常用”可配置网络参数，包括网卡类型、IPv4 地址、掩码地址、网关地址、MTU、物理地址、MTU 和设备端口号。点击“保存”将配置保存。

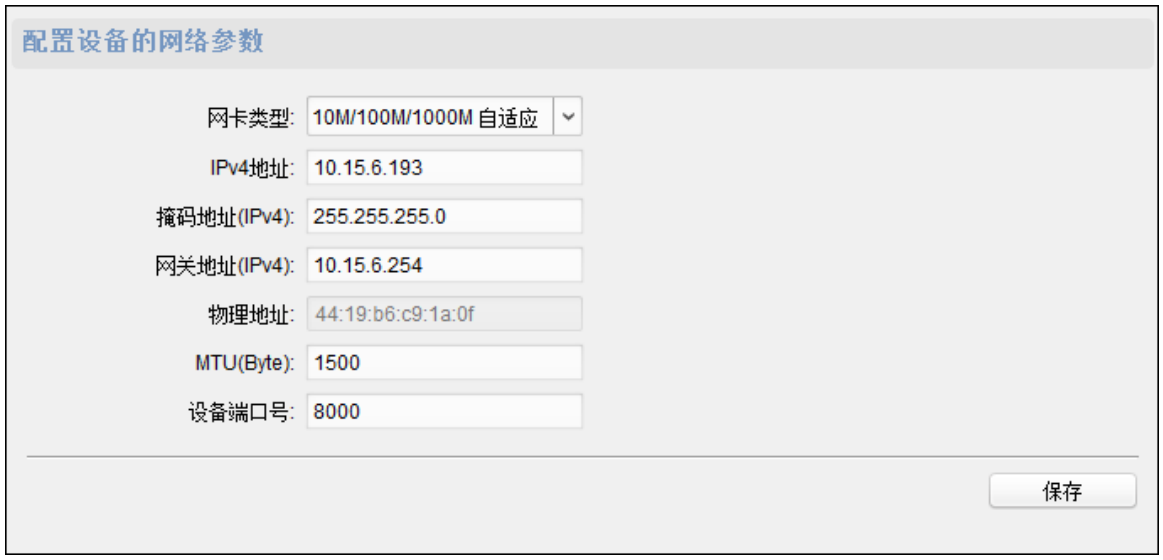


图6-32 远程配置设备网络参数界面

配置上传方式

通过配置上传中心组以及通道，您可上传通过 EHome 协议传输日志。

在远程配置界面，点击“网络”–“上报策略”。

选择需要配置的中心组。

勾选“启用”后，可配置上传方式。

配置上传的主通道和备份通道。根据选择的通道点击右侧“设置”设置网络配置中心或无线配置中心。

点击“保存”保存配置的参数。

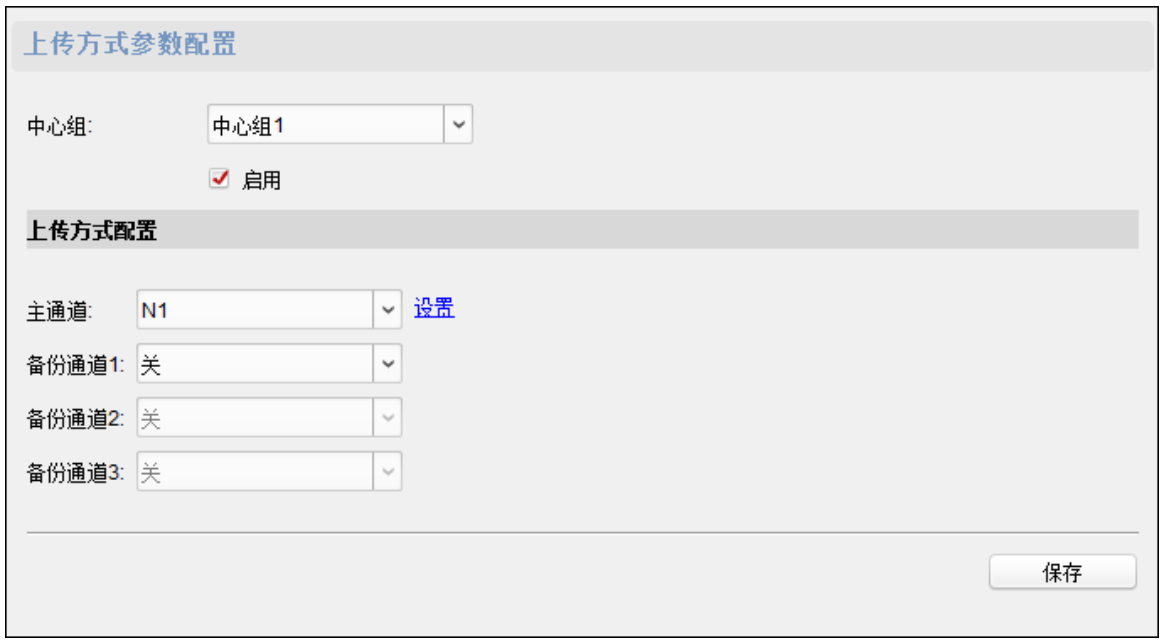


图6-33 上传方式配置

配置高级网络参数

点击“网络”–“高级配置”可配置 DNS 服务器地址、报警管理主机地址和报警管理主机端口号。点击“保存”可保存配置。

图6-34 远程配置高级网络参数界面

配置防区参数

在远程配置界面点击“报警”–“防区”可查看防区参数。

图6-35 配置防区参数界面

点击 进入防区参数设置窗口，可配置防区名称、探测器类型、防区类型和灵敏度。

点击“保存”可保存配置的参数。

或点击“复制到...”将参数复制到其他防区。

图6-36 防区参数设置窗口

配置继电器参数

在远程配置界面点击“报警”–“继电器”可查看继电器参数。

图6-37 配置继电器参数界面

点击 进入防区参数设置窗口。可配置继电器名称和输出延时时间。

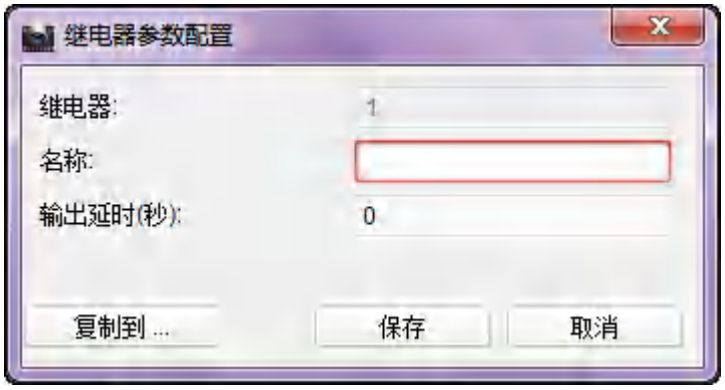


图6-38 继电器参数配置窗口

点击“保存”保存配置的参数。

或点击“复制到...”将参数复制到其他防区。

配置门禁参数

在远程配置界面点击“其他”–“门禁参数”，可勾选“下行 RS-485 通信备份”和“是否允许按键输入卡号”。点击“保存”可保存配置。

图6-39 远程配置门禁参数界面

底图上传（需设备支持）

在远程配置界面点击“其他”–“图片上传”。点击 从本地选择图片。点击“预览”可预览图片。点击“图片上传”开始上传该图片至设备。

或点击“删除图片”将图片删除。

图6-40 远程配置底图界面

人脸检测

在远程配置界面点击“其他”-“人脸检测”，在配置人脸检测参数界面勾选“启用”并点击“保存”即可启用设备的人脸检测功能。

仅带有摄像功能的设备才可使用此功能。

图6-41 人脸检测配置窗口

防区操作

◆ 在远程配置界面点击“操作”-“防区”，可查看防区信息。

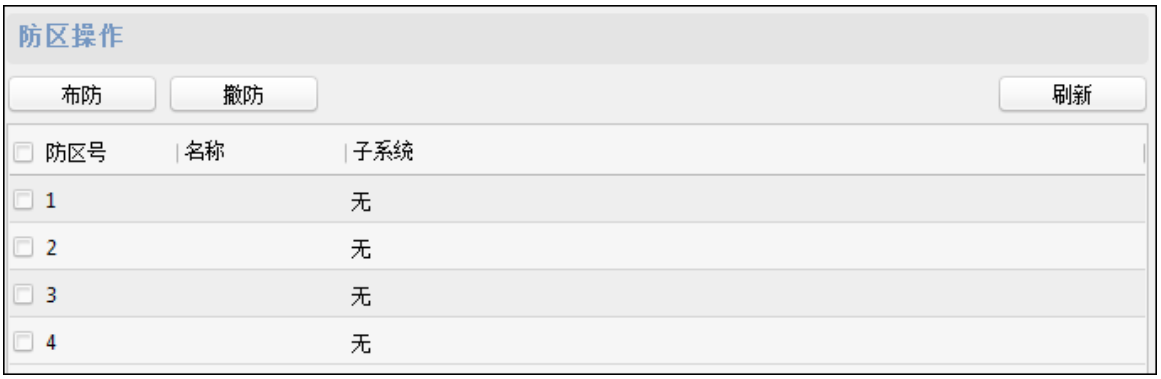


图6-42 防区操作界面

◆ 勾选防区，并点击“布防”或者“撤防”可对防区进行布撤防控制。

或点击“刷新”刷新防区状态。

继电器操作

在远程配置界面点击“操作”-“继电器操作”，可查看继电器状态。

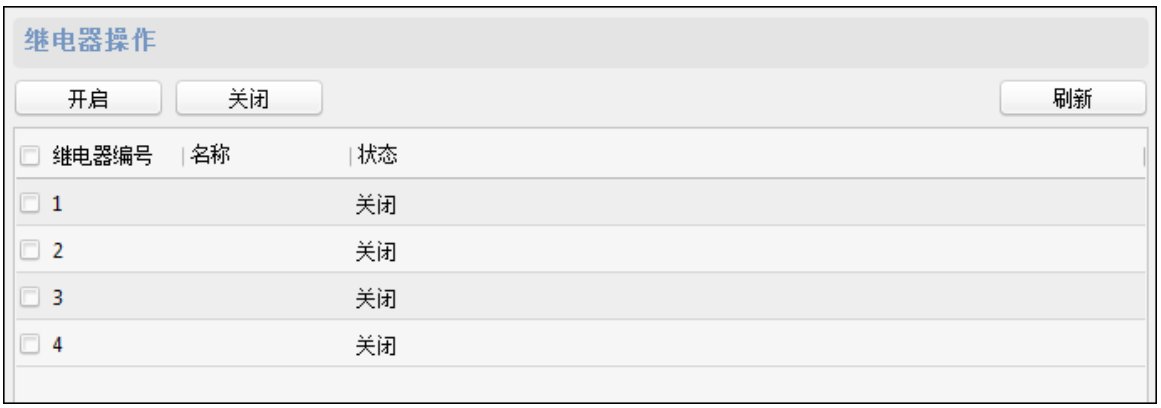


图6-43 继电器操作界面

勾选需要配置的继电器，点击“开启”或者“关闭”对继电器进行操作。

或点击“刷新”刷新继电器状态。

查看状态

点击“状态”–“继电器”可查看继电器的状态。点击界面右下角“刷新”按钮，可刷新继电器状态。

图6-44 继电器状态界面

查看设备状态

可查看设备的设备下的门、主机、读卡器、报警输入口、报警输出口、事件传感器、门控安全模块以及布防的状态。

图6-45 设备状态窗口

请以实际使用的客户端界面为准。

点击“刷新”可显示实时状态。

具体可查看的信息如下表所示：

设备状态信息表

门状态	门序号
	门锁状态
	门状态
	门磁状态
主机状态	蓄电池电压值
	蓄电池是否处于低压状态
	设备供电状态
	多门互锁状态
	反潜回状态
	主机防拆状态
	已添加卡片数量
读卡器状态	读卡器序号
	读卡器在线状态
	读卡器防拆状态
	读卡器当前验证状态
报警输入口状态	报警输入口序号
	状态（有、无输入）
报警输出口状态	报警输出口状态
	状态（有、无输出）
事件报警输入口状态	事件报警输入口序号
	状态（有、无输入）

门控安全模块状态	门编号
	在线状态
	防拆状态
布防状态	IP
	布防类型

6.4.2 人员配置

在门禁控制模块，点击组织管理图标进入组织管理界面。

管理组织

在组织管理界面左侧组织列表中，点击“+添加”。

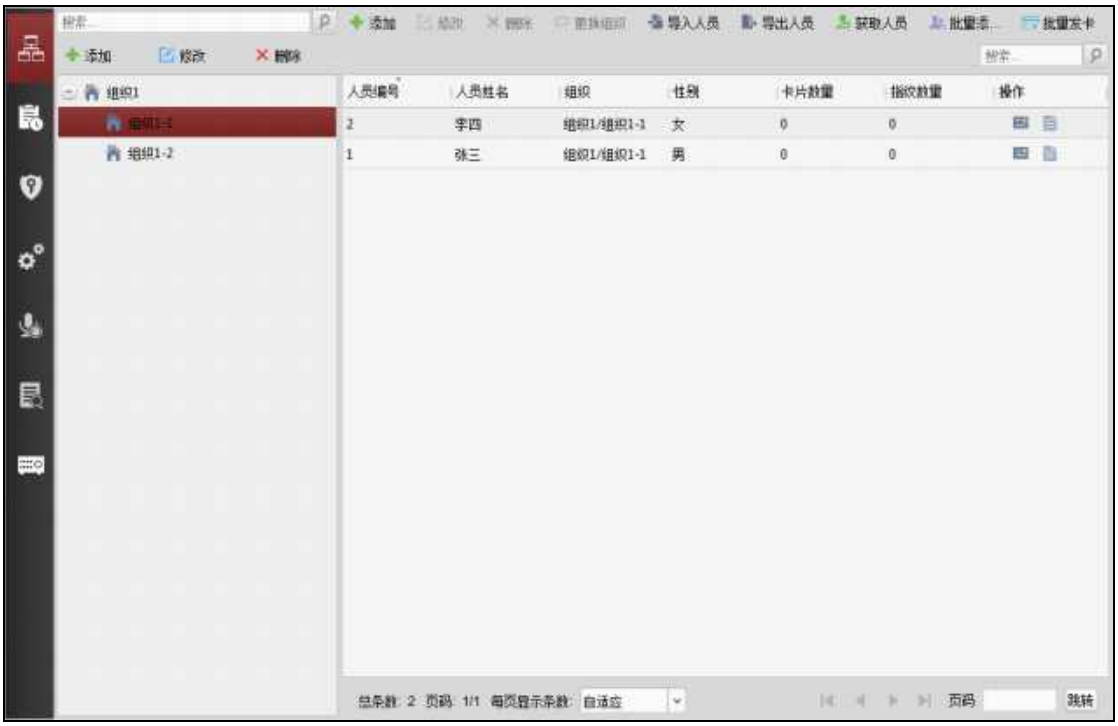


图6-46 组织管理界面

在弹出的窗口中输入组织名称。

图6-47 添加组织

点击“确定”，完成组织添加。

或在组织列表中选择一个组织并点击“修改”可修改组织信息。

或选择一个组织后，点击“删除”删除组织。

说明

最大支持 10 级组织的添加。

组织名称最多可输入 32 个字符，包括字母、数字、下划线和删除线。

组织数量无限制，仅限制添加人员总数：最多可添加 10000 人。

删除部门时，请先确认部门下没有人员，否则删除失败。

删除上级部门时，会同时删除下级子部门。

管理人员

- 添加人员（信息）

在组织管理界面左侧列表中选择一个需要添加人员的组织。

在界面右侧人员列表中点击“+添加”按钮。

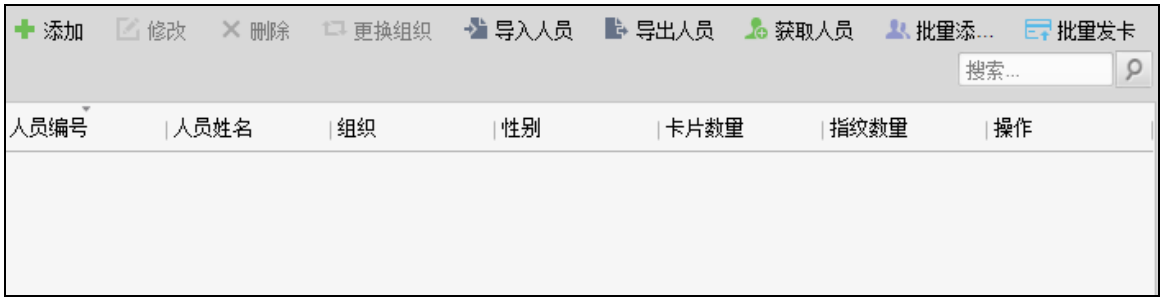


图6-48 添加人员按钮

在弹出的添加人员窗口中配置人员基本信息，包括人员编号、人员姓名、性别等。手机号码、出生日期、籍贯和电子邮件为选填项。

若有需要，您还可以在窗口下方“扩展信息”中可配置人员证件类型、证件号码、职务、国家、城市、学历、雇佣日期、雇佣年限、绑定设备、房间号、住址以及备注。

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。

图6-49 添加人员基本信息配置框

若有需要，点击窗口右侧“上传照片”按钮，可从本地上传人员照片信息。

还可点击“拍照”按钮，通过本地拍摄人员照片。（本地电脑需配有摄像头）

点击“确定”，完成人员添加。添加的人员将在组织管理界面的人员列表中显示。

如有需要，可点击人员按钮，查看该人员刷卡信息。

- 添加人员（权限层级）

可配置人员权限。

在添加人员窗口中配置人员基本信息。

点击“权限层级”可配置人员的权限层级。

图6-50 添加人员权限层级窗口

在下拉框中选择该人员的操作权限。

您可选择普通用户或管理员。

在可选权限组列表中勾选该人员的权限。

点击>按钮可将勾选的权限添加到已选权限组列表中，表示该人员有选中的权限。

或点击>>按钮，将可选权限组中所有权限添加到已选权限组中。

或在已选权限组列表中选择不需要添加的权限，并点击<按钮，可将已选权限组从列表中删除。（可多选）。

或点击<<按钮，将所有已选权限组从列表中删除。

点击“确认”按钮，完成人员添加。添加的人员将在组织管理界面的人员列表中显示。

如有需要，可点击人员按钮，查看该人员刷卡信息。

- **添加人员（管理卡片）**

可在添加人员时添加人员对应的卡片。

在添加人员窗口中配置人员基本信息。

点击“卡片”可为该人员添加卡片。

图6-51 添加人员卡片窗口

点击“添加”按钮进入添加卡片窗口。

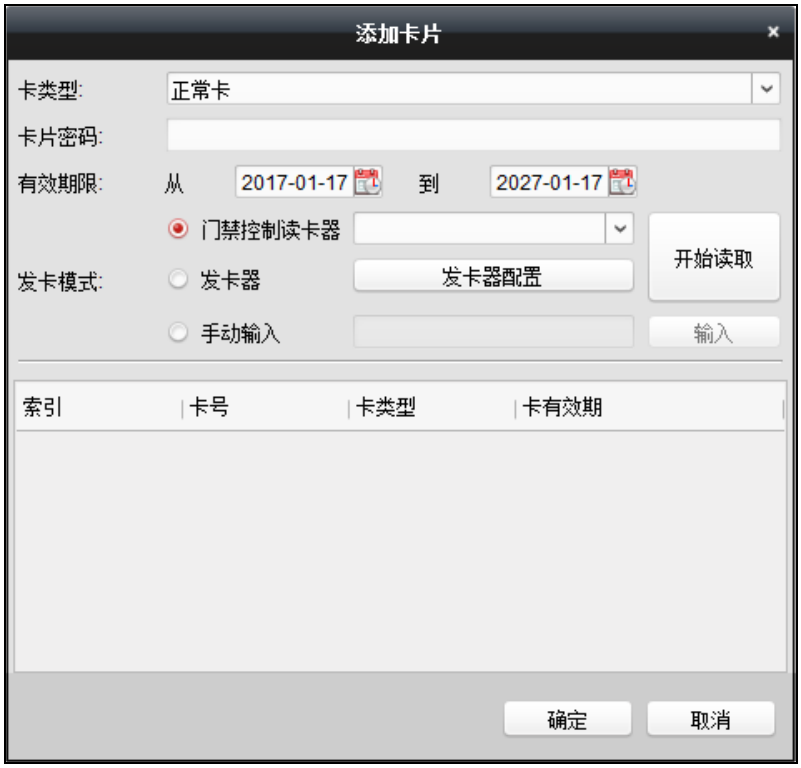


图6-52 添加卡片窗口

配置卡类型、卡片密码、卡片数量、卡片有效期限和发卡模式。

若发卡模式为门禁控制读卡器，则

在下拉框中选择一个门禁设备下的读卡器，点击“开始读取”。

可在读卡器上刷卡，让设备发卡。

说明

在发卡前，需在客户端对该设备进行布防，详见 6.9 布防控制。

卡片密码为 4-8 位数字。

当设置卡类型为访客卡时，需设置最大刷卡次数。最大刷卡次数范围为 0-225。当刷卡次数超过设置的值时，刷卡无效。若设置最大刷卡次数为 0 时，表示刷卡次数无限制。

若发卡模式为发卡器，则

点击“发卡器配置”按钮，进入发卡器配置窗口。

图6-53 发卡器配置窗口

配置发卡器类型、超时时间、是否蜂鸣、卡号类型。

若卡片为 M1 卡，如需启用 M1 卡加密功能，请进行如下操作:

勾选“启用”开启 M1 卡加密，配置扇区。点击“修改”配置扇区数量，并在扇区列表中勾选需要加密的扇区。

点击“保存”保存配置。

或点击“恢复默认”恢复默认参数。

返回批量发卡界面后，点击“开始读取”。

说明

在选择此发卡模式前，需连接对应的发卡器。

若发卡模式为手动输入，则

手动输入卡号。

点击“输入”。

点击“确定”完成卡片添加。

添加的卡片将在添加人员窗口下方的卡片列表中显示。

如有需要，选择一个卡片，点击“编辑”可编辑该卡片。

如有需要，选择一个卡片，点击“删除”可删除该卡片。

如有需要，选择一个卡片，点击“绑定指纹”可绑定已录入的指纹。

说明

在绑定指纹前，您需要录入指纹。详见添加人员（指纹录入）章节。

在添加人员窗口中点击“确定”按钮，完成人员添加。添加的人员将在组织管理界面的人员列表中显示。

如有需要，可点击人员按钮，查看该人员刷卡信息。

- **添加人员（指纹录入）**

可录入人员对应的指纹信息。

在添加人员窗口中配置人员基本信息。

点击“指纹录入”可为该人员录入指纹信息。

图6-54 添加人员指纹窗口

点击“指纹机设置”按钮进入指纹机配置窗口。

配置指纹机参数。

图6-55 指纹机配置窗口

点击“保存”可保存配置的参数。

或点击“恢复默认”恢复默认参数。

说明

步骤. 在配置指纹机参数前，需连接一台指纹机。

步骤. 此串口号需要与电脑中的串口号相同。您可以前往电脑中的设备管理器中查看指纹机的串口号。

在添加人员窗口下方的图片中选择需要录入指纹的手指。

将对应的手指放置在指纹机上，点击“开始注册”按钮，设备开始注册指纹。

点击“停止注册”可停止注册指纹。

也可以点击“设备采集”，选择设备后，在设备端进行指纹采集。（此功能需设备支持）

指纹注册完成之后，在添加人员界面点击“卡片”进入卡片添加界面。

点击“绑定指纹”将录入的指纹与卡片绑定。

若有需要，选择已录入的指纹，点击“删除”按钮可删除指纹。

若有需要，点击“清空”可清空所有已录入的指纹。

在添加人员窗口中点击“确定”按钮，完成人员添加。添加的人员将在组织管理界面的人员列表中显示。

如有需要，可点击人员按钮，查看该人员刷卡信息。

- 删除人员

步骤1. 人员管理列表中选择需要删除的人员。（可多选）

步骤2. 点击“删除”按钮。

步骤3. 在弹出的提示框中点击“确定”即可完成删除。

- 更换组织

可更换人员的组织。

在组织管理界面中，选择组织内的人员。

点击“更换组织”按钮，打开更换组织窗口。

图6-56 更换组织窗口

在弹出的配置窗口中选择需要移动到的组织。

图6-57 组织列表

点击“确认”按钮完成组织更换。

- 导入人员

在组织管理界面中的右侧人员列表中点击“导入人员”按钮。

在弹出的对话框中点击…，并选择需要导入的 CSV 文件。

图6-58 导入人员窗口

点击“确定”。系统将显示导入结果。

图6-59 导入结果窗口

点击“关闭”完成人员导入。

说明

点击“下载人员导入模板”可获取人员信息模板。

导入模板中包含以下内容：人员名称、性别、部门编码、证件类型、证件号码、联系电话以及联系地址。

若导入的人员编号在客户端数据库中已经存在，系统将自动替换原有人员信息。

最多可导入 10000 人，每人 5 张卡片。

- 导出人员

在组织管理界面中点击“导出人员”，打开导出人员配置框。

图6-60 导出人员配置框

在弹出的导出人员配置框中点击...并选择导出路径。

勾选需要导出的人员信息。

点击“确定”完成导出。客户端将导出所有人员信息。

- 获取人员

可从设备端获取人员信息。

步骤1. 在组织管理界面中点击“获取人员”，进入选择设备窗口。

图6-61 选择设备窗口

步骤2. 在弹出的获取人员配置框中点击选择一台设备。

步骤3. 双击选中的设备，或点击“确定”。设备中的人员信息将导入到本客户端中。

说明

使用连接方式为 COM 或者 EHome 方式添加的设备不支持人员获取功能。

- 批量添加人员
  - 在人员管理列表中选择一名用户用于复制其配置信息。
  - 点击“批量添加人员”按钮，进入批量添加人员配置框。

图6-62 批量添加人员配置框

- 点击 或 配置人员编号。
- 勾选需要复制的项。
- 点击“确定”完成配置。

说明

若导入的人员编号在客户端数据库中已经存在，系统将自动替换原有人员信息。

6.4.3 计划模板

配置周计划

- 添加/删除周计划

  在门禁控制模块，选择图标，进入计划模板界面。

  点击“周计划”，进入周计划页面。

图6-63 周计划页面

点击“添加周计划”按钮。

在弹出的配置框中输入周计划名称。

点击“确定”完成添加。

图6-64 添加周计划配置框

如有需要，选择需要删除的周计划，点击“删除周计划”即可删除选中的周计划。

客户端自带“默认启用周计划”和“默认禁用周计划”，且这两项不可修改和删除。

- 管理周计划

▪在界面左侧周计划列表中选择需要管理的周计划，在界面右侧将会显示该周计划的属性信息。

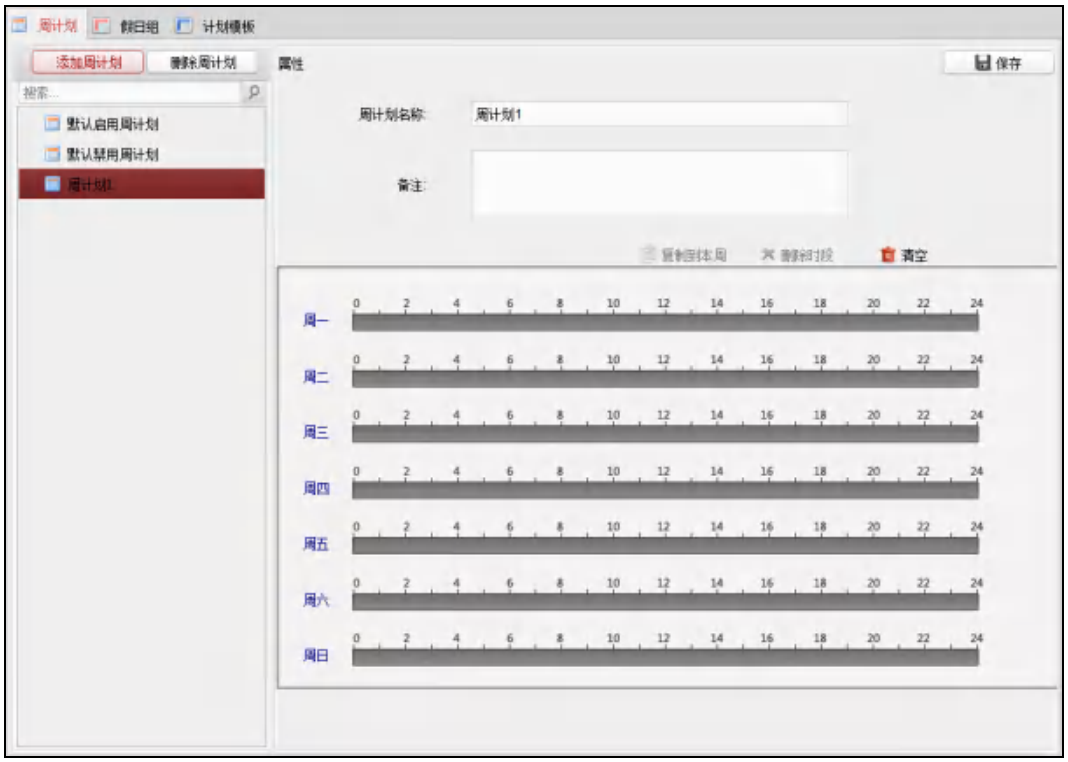


图6-65 周计划列表

- 在右侧属性界面中修改周计划名称。

如有需要，也可在右侧属性界面中添加备注。

- 在属性界面下方的计划表中点击并拖动鼠标，以设置每天的时间计划。划定的时间段将显示为蓝色。

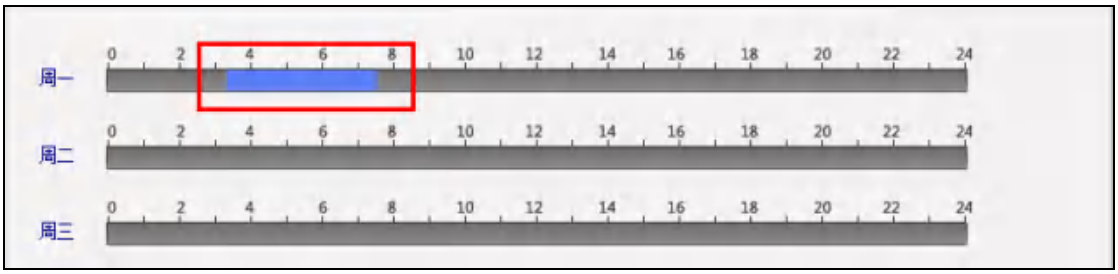


图6-66 设置时间计划

点击已划定时间计划，点击 可设置精确时间。点击“确定”保存设定。

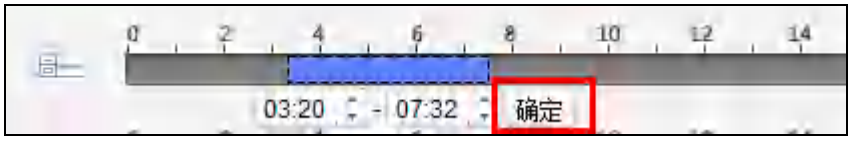


图6-67 设置精确时间计划

▪若一周内每日的计划相同，则选中需要的时间计划，点击“复制到本周”即可将选中的时间计划复制到整周。

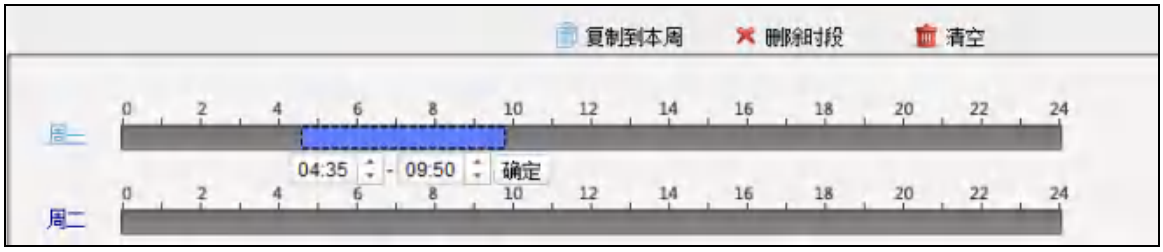


图6-68 复制到本周

或点击“删除时段”即可删除该段计划。

或点击“清空”，可将所有计划全部清空。

▪点击界面右上角“保存”保存配置的周计划。

配置假日组

- 添加/删除假日组

在计划模板界面，点击“假日组”，进入假日组页面。

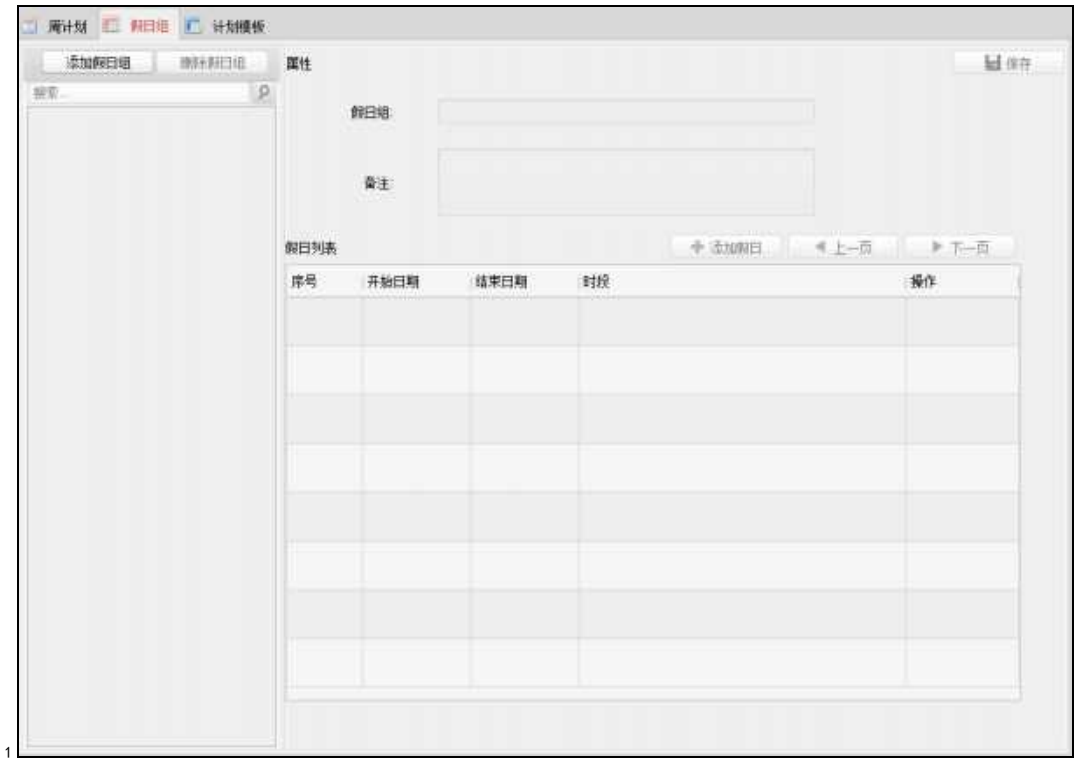


图6-69 假日组

点击“添加假日组”。

在弹出的配置框中输入需要添加的假日组名称。

点击“确定”完成添加。

图6-70 添加假日组配置框

如有需要，选择需要删除的假日组，点击“删除假日组”即可删除选中的假日组。

- 管理假日组

  ◆ 在界面左侧假日组列表中选择需要配置的假日组。

图6-71 假日组列表

◆ 在右侧属性界面中修改假日组名称。

或在右侧属性界面中添加备注。

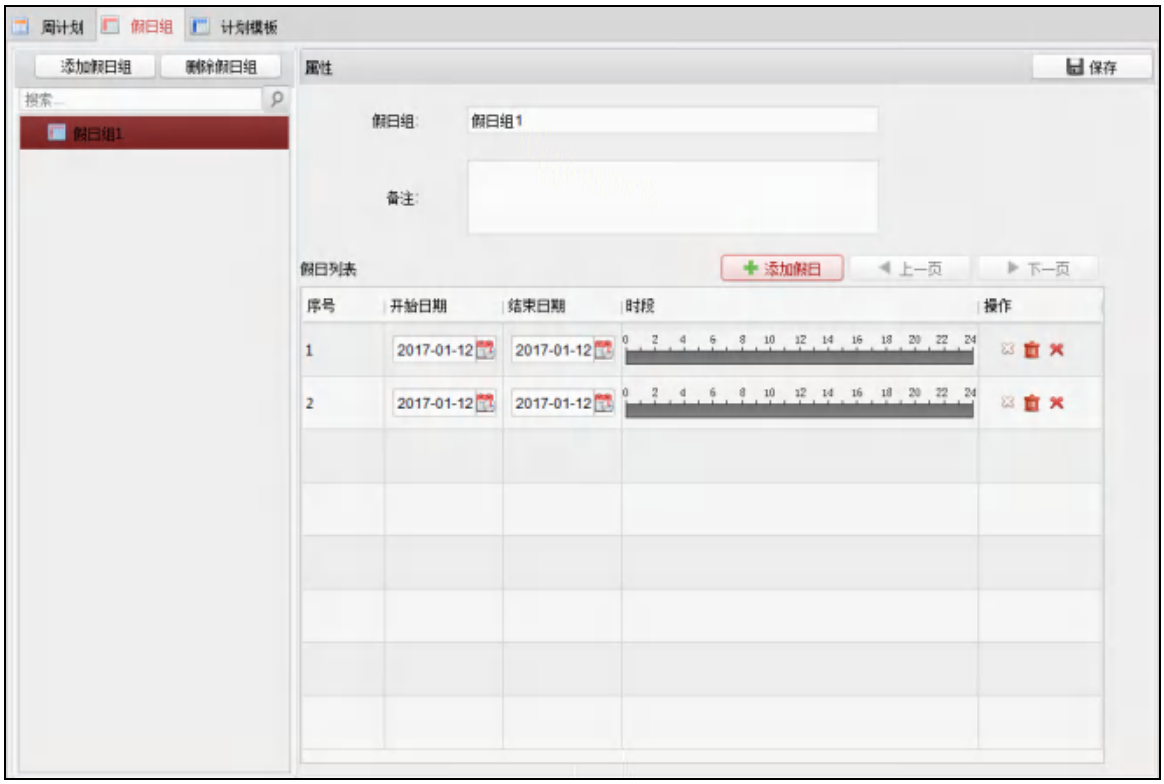


图6-72 假日组备注

- 在右侧属性界面中点击“添加假日”。属性界面下方的假日列表中将出现可以配置的假日条目。
- 点击设置开始日期和结束日期。
- 点击并拖动鼠标划定计划时间段。

图6-73 置假日时间

或者点击划定的时间段，可设置精确时间。点击“确定”保存设定。

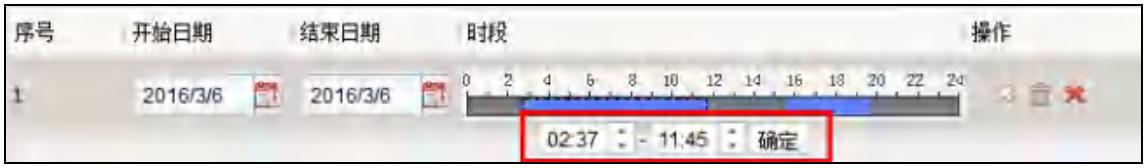


图6-74 设置精确时间

若有需要，选择不需要的时间段，点击按钮即可删除该时间段。

若有需要，点击删除所有划出的时间段。

若有需要，点击删除整个假日。

- 点击“保存”保存设置。

每个假日组最多可添加 16 个假日。

配置计划模板

计划模板是周计划和假日组的集合。

- 添加/删除计划模板

在计划模板界面中点击“计划模板”，进入计划模板页面。

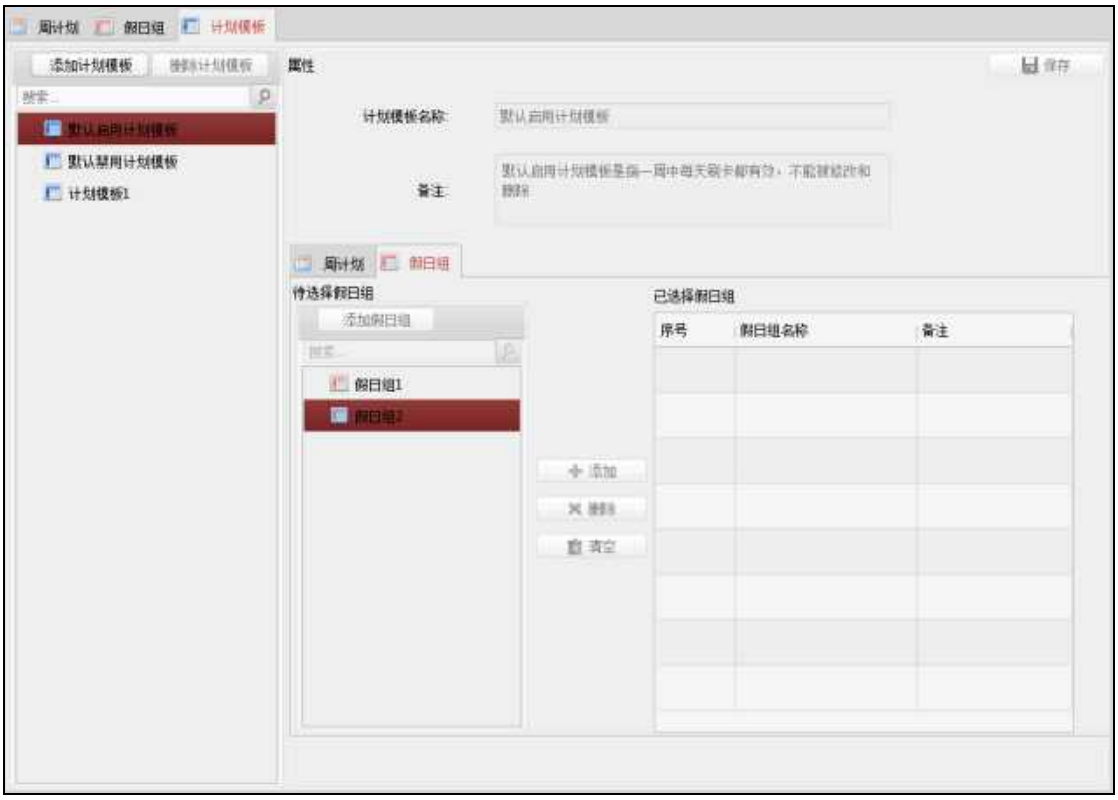


图6-75 计划模板

在弹出的对话框中输入需要添加的计划模板的名称。

点击“确定”完成添加。

图6-76 计划模板配置框

如有需要，选择需要删除的计划模板，点击“删除计划模板”即可删除。

- 管理计划模板

在界面左侧计划模板列表中选择需要配置的计划模板。

图6-77 计划模板列表

在右侧属性界面中修改计划模板名称。

也可在右侧属性界面中添加备注。

在属性界面下方点击“周计划”，进入计划模板的周计划页面，并在周计划下拉框中选择需要的周计划。

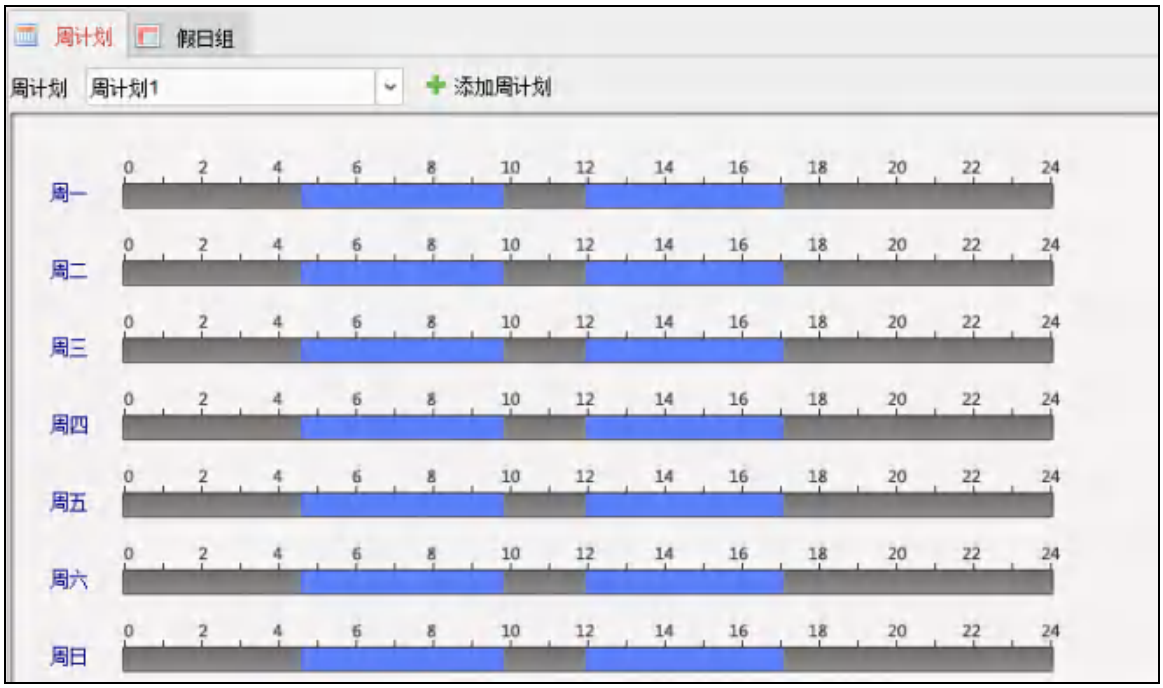


图6-78 选择周计划

如有需要，可点击“添加周计划”，

在弹出的窗口中配置新的周计划。

点击“确定”完成添加。

更多关于添加与配置周计划的内容，详见本章节中的添加/删除周计划。

在属性界面下方点击“假日组”，进入计划模板的假日组页面。

在待选择假日组列表中选择需要的假日组，并点击“+添加”按钮，添加的假日组将显示在右侧的已选择假日组列表中。

如有需要，可点击“添加假日组”按钮。

在弹出的窗口中配置假日组。

点击“确定”完成添加。

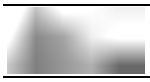
更多关于添加与配置假日组的内容，请查看本章节中的配置假日组。

如有需要，点击右侧不需要的假日组并点击“删除”，即可删除该假日组。

如有需要，点击“清空”即可清空已选择假日组列表中所有假日组。

图6-79 计划模板假日组页面

点击界面右上角“保存”按钮保存配置。



默认启用计划模板、默认禁止计划模板分别对应默认启用周计划和默认禁止周计划，且不关联假日组。

自定义计划模板可以对应默认启用周计划和默认禁止周计划，并且可以关联假日组。

每个计划模板最多可添加 4 个假日组。

6.4.4 门禁权限

可在此界面中添加、删除、下发门禁权限。

添加门禁权限

在门禁控制模块，点击权限组图标，进入权限组管理界面。

图6-80 权限组界面

点击“添加”按钮，打开添加权限组窗口。

图6-81 添加权限组窗口

配置权限组参数。

- 输入权限组名称。

- 在下拉框中选择计划模板。

或点击“添加计划模板”添加计划模板。详见 6.4.3 计划模板。

- 在窗口左侧可选人员列表中勾选人员。
- 点击>按钮将选择的人员添加到“已选人员”列表中。

或选择已选人员列表中的人员并点击<按钮删除已选人员。（可多选）

- 在可选门禁点/设备列表中勾选门禁点或设备。
- 点击>按钮将选择的门禁点或设备添加到“已选门禁点/设备”列表中。

或选择已选门禁点/设备列表中的门禁点/设备，并点击<按钮删除。（可多选）

点击“确定”完成权限组添加。

修改权限组

步骤1. 在权限组列表中选择一个权限组。

步骤2. 点击“修改”按钮，或点击“详细信息”，打开修改权限组配置窗口。

图6-82 修改权限组窗口

步骤3. 修改权限组参数。详见本章节中的添加门禁权限。

步骤4. 点击“确定”完成修改。

或在权限组列表中选择权限组并点击“删除”可删除权限组。

下发门禁权限

在权限组列表中选择权限组。（可多选）

点击“下发到设备”，系统将配置的权限组权限下发到对应的设备。

在弹出的下发结果窗口中显示下发结果。

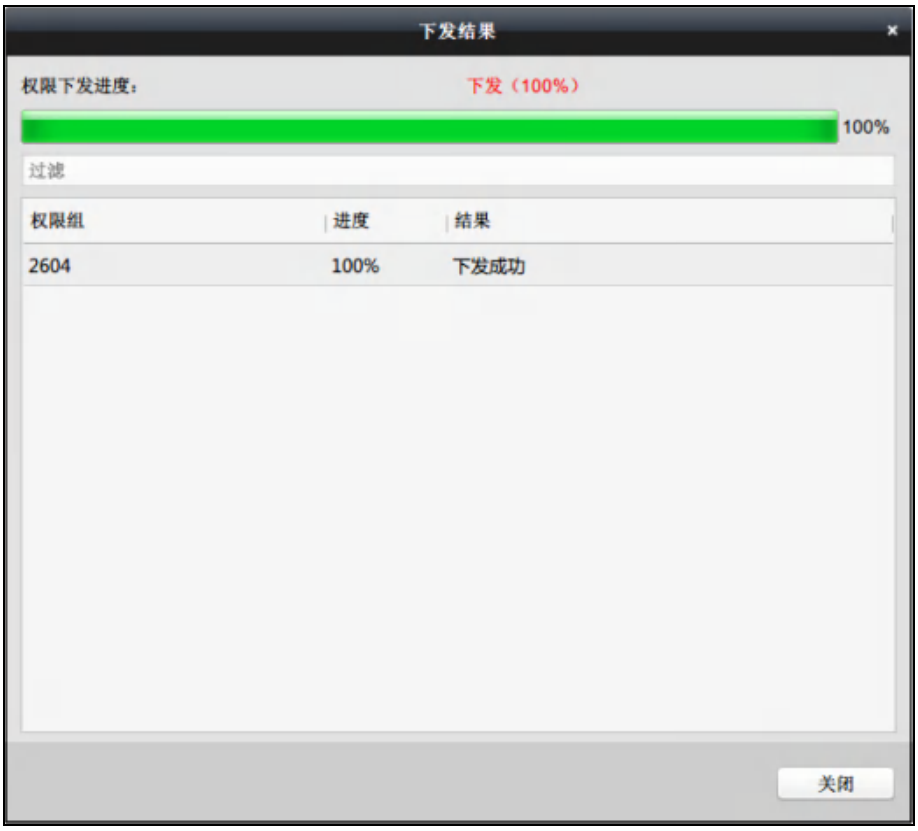


图6-83 下发结果窗口

6.4.5 高级配置

可以配置门禁参数、读卡器认证、多重认证、首卡开门、反潜回、多门互锁、手机白名单和认证码。

点击高级配置按钮进入高级配置界面。

与卡片相关的功能(门禁卡类型/首卡开门/多重认证/认证码)在添加卡片时只会列出已经下发过门禁权限的卡片。

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

可修改门禁设备的门信息和读卡器信息。

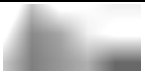
- 配置门信息

此界面可以设置门磁状态、出门按钮类型，正常情况下门锁动作时间等信息。

步骤1. 在高级配置界面点击“门禁参数”进入门禁参数页面。

步骤2. 在界面左侧设备列表中选择门禁设备下的门，并在页面右侧配置该门的参数。

图6-84 配置门参数

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。
残疾人卡开门时间:	因残疾人行动不便，配置该参数后可适当延迟刷卡后门磁开启时间。
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。  开门超时报警值设为 0 时，表示不启用报警。
是否启用闭门回锁:	选择“是”，即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。选择“否”，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。
超级密码:	指定人员输入超级密码便可开门。
解除码:	门禁点报警时输入解除码即可解除报警。

步骤3. 点击右上角“保存”按钮保存设置。

- 胁迫码、超级密码和解除码三者不能重复。
- 认证码只能为 4-8 位的数字。
- 胁迫码、超级密码和解除码分别不能与认证码重复。

- 配置读卡器信息

在门禁参数页面左侧选中设备下的读卡器，并在页面右侧配置该读卡器的信息。

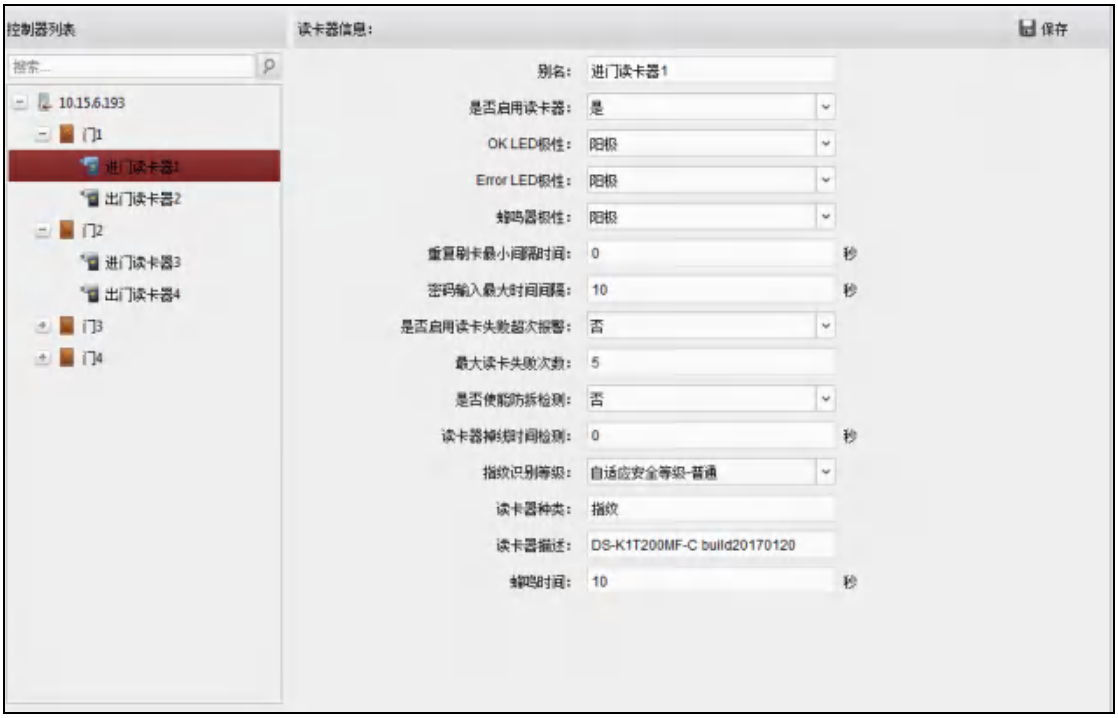


图6-85 配置门读卡器参数

别名:	可配置读卡器名称。
是否启用读卡器:	若选“是”，表示该读卡器可以正常刷卡使用；若选“否”，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。
重复刷卡间隔时间（秒）:	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）。
密码输入最大时间间隔（秒）:	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:	若选“是”，表示当错误操作达到读卡器预设错误操作上限时，主机会自动生成报警事件。若选“否”，则不会生成报警事件。
最大读卡失败次数:	表示读卡器允许读卡错误操作的上限次数。
是否使能防拆检测:	若选“是”，表示读卡器被拆走或拿走时，主机会自动产生防拆报警事件。若选“否”，则不产生报警事件。
读卡器掉线时间检测:	在设定的时间内读卡器若无法与主机联系上，则读卡器进入掉线模式。
指纹识别等级:	可选择指纹识别等级。默认为自适应安全等级-普通。
读卡器种类:	可查看读卡器种类，不可修改。
读卡器描述:	可查看读卡器描述，不可修改。
蜂鸣时间:	配置读卡器蜂鸣时间。可配置的范围是 0 到 5999 秒。其中 0 表示持续蜂鸣。

点击右上角“保存”保存设置。

配置读卡器认证

可在此模块下配置读卡器认证模式以及读卡器验证计划。可选择的读卡器认证模式有刷卡加密码，刷卡或认证码，指纹，卡片，刷卡或指纹，密码加指纹，刷卡加指纹，刷卡加密码加指纹。

在高级配置界面中点击“读卡器认证”，进入读卡器认证页面。

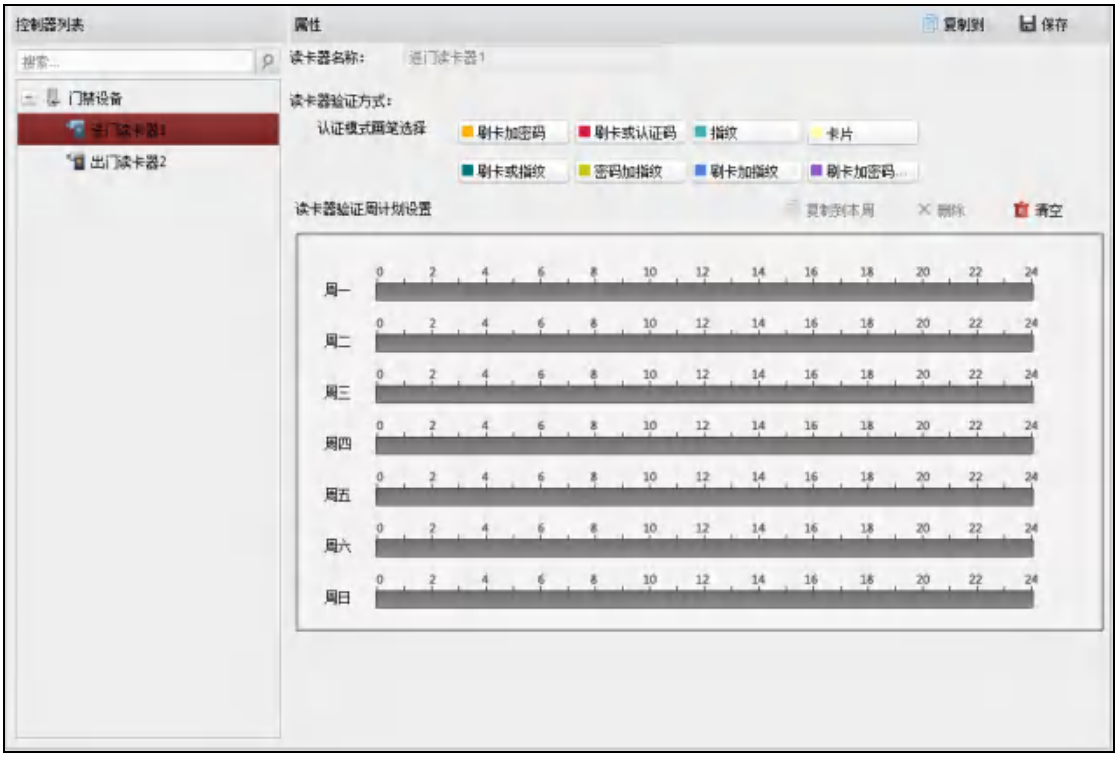


图6-86 读卡器认证

在界面左侧读卡器列表中选择设备下的读卡器。

在右侧属性界面中选择一个认证模式画笔。

可选择读卡认证模式：刷卡加密码，刷卡或认证码，指纹，卡片，刷卡或指纹，密码加指纹，刷卡加指纹，刷卡加密码加指纹。详细说明见图 308--16777216 读卡认证模式信息表。

读卡认证模式信息表

认证模式	含义
刷卡加密码	需同时刷卡并输入卡片密码才可开门。
刷卡或认证码	刷卡或者输入认证码便可开门。（关于认证码认证，请参考本章节中的配置认证码。）
指纹	只需输入指纹便可开门。
刷卡	只需刷卡就可开门。
刷卡或指纹	输入指纹或刷卡便可开门。
密码加指纹	需同时输入卡片密码并输入指纹才可开门。
刷卡加指纹	需同时刷卡并输入指纹才可开门。
刷卡加密码加指纹	需同时刷卡，输入指纹，并输入卡片密码才可开门。

需要有设备支持的认证模式，认证模式画笔按钮才能使用。

图6-87 读卡器认证方式

在读卡器验证周计划设置中点击并拖动鼠标划定生效时间段。

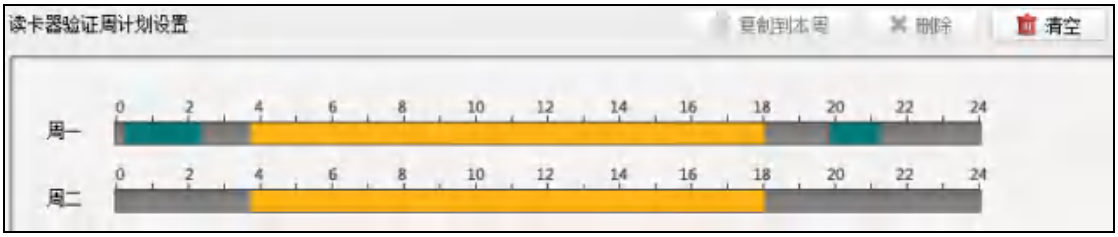


图6-88 设置读卡器验证计划

或者点击划定的时间段，可设置精确时间。点击“确定”保存设定。

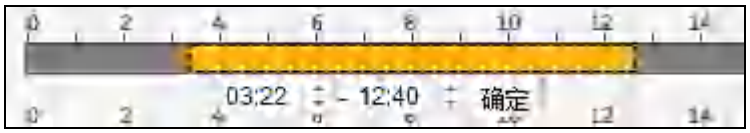


图6-89 设置读卡器验证精确计划

若一周内每日计划相同，则选中需要的时间计划，点击“复制到本周”即可将选中的时间计划复制到整周。

若有需要，选中某段时间计划，点击“删除”即可删除该段计划。

若有需要，点击“清空”，可将所有计划全部清空。

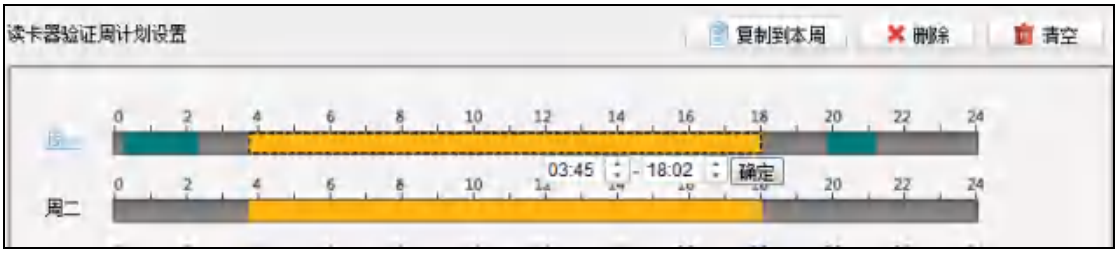


图6-90 读卡器验证周计划设置

点击“保存”保存设置。

若有需要，点击“复制到”，在弹出的配置框中勾选需要的被复制到的读卡器，可将此处配置的读卡器验证周计划复制到被勾选的读卡器中。

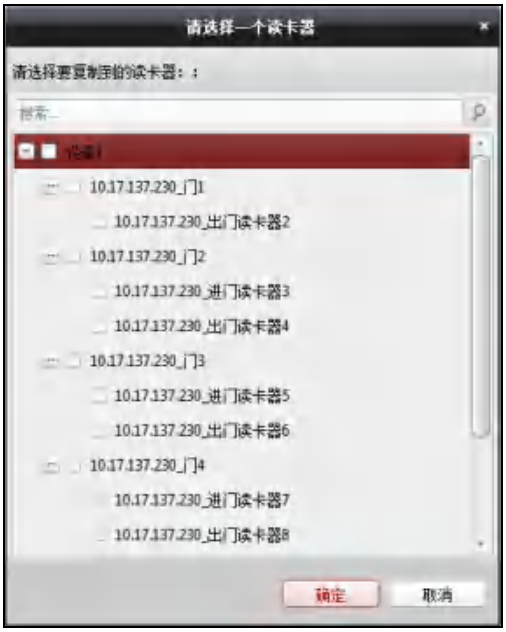


图6-91 选择读卡器

如果一张普通卡没有设置认证，那么这张卡在卡+认证码时间段内刷卡无法开门。

配置多重认证

配置为多重认证的门需要卡组内的成员按照配置的刷卡数量刷卡认证，门才能开启。

步骤1. 在高级配置界面，点击“多重认证”，进入多重认证页面。

图6-92 多重认证

步骤2. 在控制器列表中选择一个设备。

步骤3. 添加卡组。

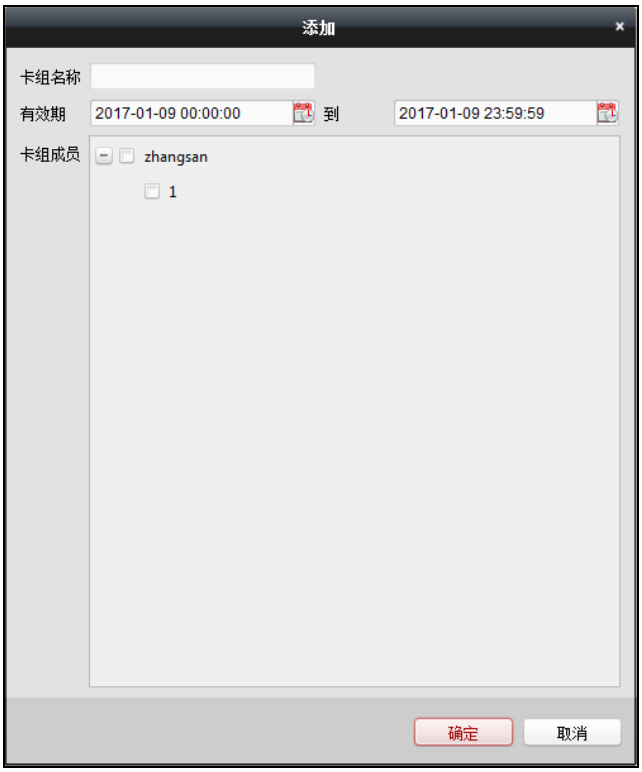


图6-93 添加卡组窗口

在设置卡组中点击“+添加”按钮。

在弹出的配置框中配置卡组名称、有效期，并勾选卡组成员。

点击“确定”完成卡组添加。

选择某一卡组并点击“编辑”按钮或者“详情”，可进入修改界面修改卡组。

或点击“删除”按钮删除卡组。

步骤4. 添加认证组。

图6-94 添加认证组窗口

在设置认证组中点击“+添加”按钮。

在弹出的配置框中配置参数：

门： 可在下拉框中选择要配置的门。

时间间隔： 配置相邻两张卡最大的刷卡时间间隔。

计划模板： 可在下拉框中选择配置过的计划模板。详见 6.4.3 计划模板。

认证类型： 本地认证（最多可添加 8 组卡组）；

本地认证+远程开门（最多可添加 7 组卡组）；

本地认证+超级密码（最多可添加 7 组卡组）

离线认证：勾选后离线默认启用超级密码认证。

在窗口下方左侧列表中选择一个卡组。

点击✚按钮添加到右侧列表中。

点击右侧列表中需要配置刷卡数量的卡组的“刷卡数量”，并在配置框内配置刷卡数量。

或在右侧列表中选择一个卡组，点击✕按钮删除。

或点击↑或者↓按钮改变卡组顺序。

刷卡数量需大于 0，配置的卡组才有效。

刷卡数量最多为 16。

刷卡数量不能超过卡片数量。

步骤5. 点击“确定”完成添加。并返回多重认证界面。

步骤6. 点击“保存”保存设置。

配置首卡开门

可对某一门禁点设置若干张首卡。首卡刷卡后可允许大批量人员通过或进行其他卡认证操作。首卡模式包括禁用首卡常开、首卡常开和首卡授权。

首卡常开指的是在首卡开门后允许大批量人员在设置的时间内不刷卡批量通过。首卡授权指的是所有卡和密码认证都需要在首卡刷卡授权后才可以进行，超级卡、胁迫卡、胁迫密码除外。

- **设置首卡开门时间**
  - 点击“首卡开门”进入首卡开门界面。

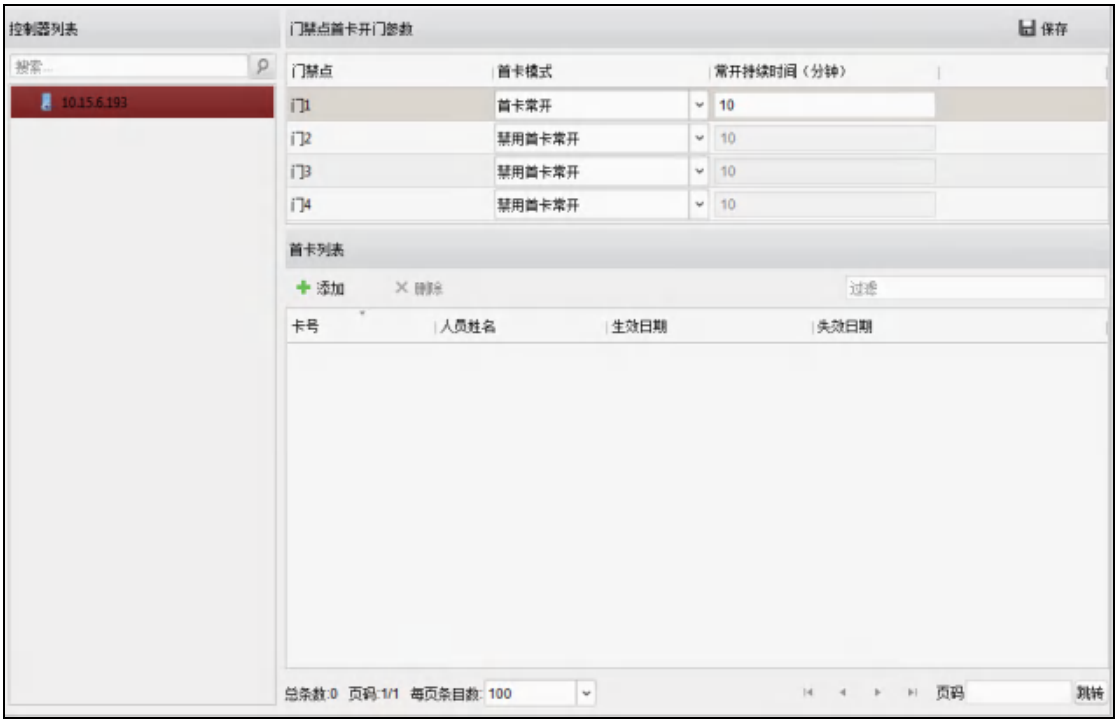


图6-95 首卡开门界面

- 在界面左侧控制器列表中选择需要配置的设备。
- 在界面右侧门禁点首卡开门参数中为需要设置的门选择首卡模式，并设置常开持续时间。

首卡模式包括禁用首卡常开、首卡常开和首卡授权。

说明

- 首卡授权模式下，可通过超级卡、胁迫卡或胁迫密码直接认证，不受首卡授权模式的限制。
- 首卡开门后，可再次刷此张首卡关闭首卡开门功能。
- 有效首卡授权时间为当天，当天 24 点后，授权失效。

- 点击“保存”保存配置。

可设置的常开持续时间为 0~1440 分钟。默认持续时间为 10 分钟。

- 添加首卡

在首卡开门界面左侧的控制器列表中选择需要配置的设备。

在右侧首卡列表中点击“添加”。

图6-96 添加首卡

在弹出的对话框中选择需要添加的卡片。（可多选）。

点击“确定”。

图6-97 添加首卡配置框

- 添加卡片时只会列出已经下发过门禁权限的卡片。
- 每个设备最多支持添加 10 万张首卡。

点击“保存”完成添加。

若有需要，选择不需要的首卡，点击“删除”即可删除该首卡（可多选）。

配置反潜回

可对单个门禁设备下的读卡器进行反潜回配置。反潜回功能是指在客户端中设置好刷卡开门路径，如果不按此路径刷卡，门将无法打开。可根据所需设置反潜回路径。某个用户如果刷卡后不进门，再次刷卡时门将无法打开，出门亦然。

- 设置读卡器顺序

  - 点击“反潜回”进入反潜回界面。

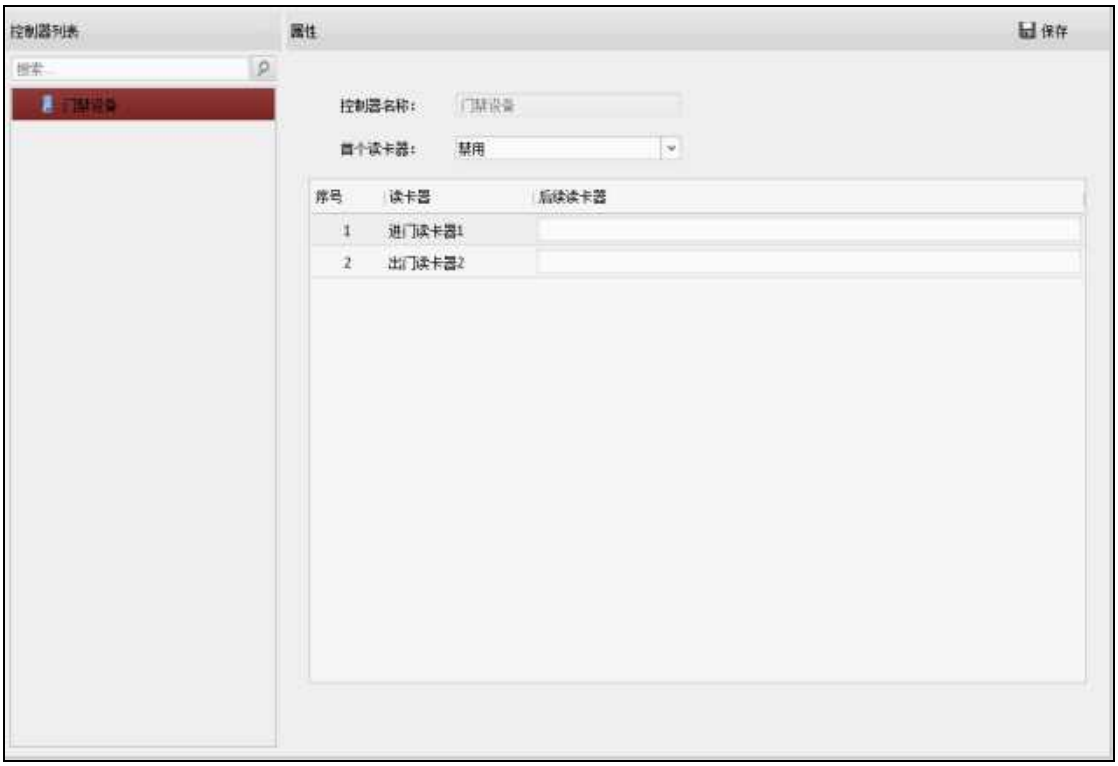


图6-98 反潜回界面

  - 在反潜回界面左侧控制器列表中选择一个设备。
  - 在界面右侧属性界面中配置反潜回的首个读卡器。
  - 点击“后续读卡器”下的输入框。

图6-99 后续读卡器列表

  - 在弹出的“选择读卡器”对话框中选择后续读卡器。并点击“确定”。

每个读卡器最多支持 4 个后续读卡器。

  - 勾选“启用反潜回”启用配置。

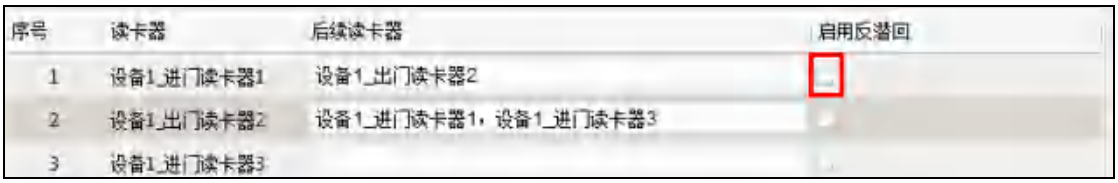


图6-100 启用反潜回

◆ 点击“保存”保存配置。

- 点击“下发配置”使配置在设备中生效。
- 设置反潜回时，需设备启用反潜回功能后，读卡器的反潜回设置才有效。
- 若设备已开启反潜回功能，且当前读卡器也已启用反潜回，则当用户刷卡认证通过时，设备会更新记录最新通过读卡器的卡 ID。
- 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：

  未设置首个读卡器时：

  第 条 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。

  第 条 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。

  设置了首个读卡器时：

  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。

- 删除后续读卡器

  在反潜回界面中点击“后续读卡器”下的输入框。

图6-101 后续读卡器列表

在弹出的选择读卡器对话框中取消勾选的读卡器。

点击“确定”完成操作。

配置跨主机反潜回

对多个门禁设备下的读卡器进行反潜回配置。反潜回功能是指在客户端中设置好刷卡开

门路径，如果不按此路径刷卡，门将无法打开。可根据所需设置反潜回路径。某个用户如果刷卡后不进门，再次刷卡时门将无法打开，出门亦然。

- 线路反潜回

需配置起始读卡器和后续读卡器。

点击“跨主机反潜回”进入跨主机反潜回界面。

勾选“启用跨主机反潜回”。

配置反潜回参数。

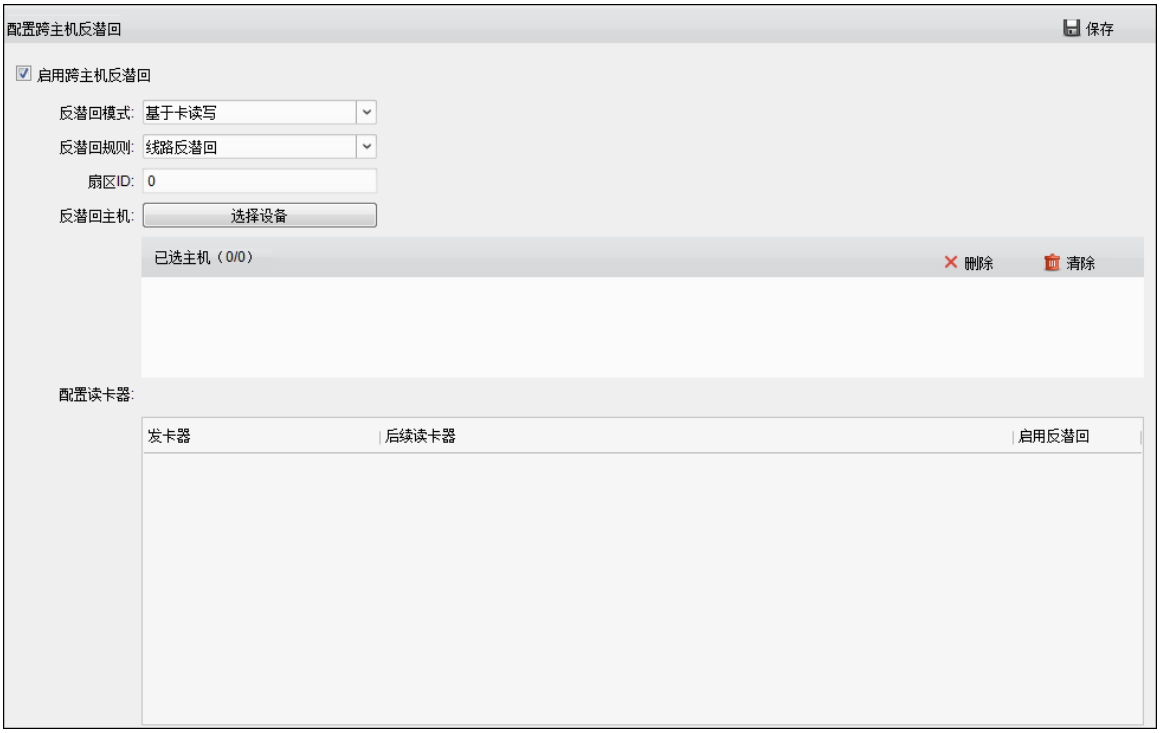


图6-102 线路反潜回界面

基于卡读写

说明

通过存于卡片上的进出门信息判断是否反潜回认证成功。

- 在反潜回模式中选择“基于卡读写”。
- 配置反潜回规则，选择“线路反潜回”。
- 配置扇区 ID。
- 点击反潜回主机配置项中的“选择主机”，并在弹出的配置框中选择需要反潜回认证的主机。

  可选择已选主机列表中的主机，并点击“删除”删除该主机。
- 在配置读卡器项中点击读卡器名称左侧的图标来选择首个读卡器。图标变为。
- 点击后续读卡器输入框，并在弹出选择读卡器窗口中按反潜回顺序勾选后续读卡器。

- 在“启用反潜回”项勾选对应反潜回的勾选框以启用反潜回。

- 显示在界面上的后续读卡器顺序为需要反潜回认证顺序。
- 最多可添加 64 台反潜回主机。
- 每个读卡器最多可添加 16 个后续读卡器。
- 目前支持 M1 卡的卡读写；且对应扇区不能加密。关于配置扇区加密的内容，详见 6.4.1 设备管理中的 M1 卡加密章节。

基于网络通信

说明

通过存于读卡器上的进出门信息判断是否反潜回认证成功。

1） 在反潜回模式中选择“基于网络通信”。

2） 配置反潜回规则，选择“线路反潜回”。

3） 在服务器下拉列表中选择一个服务器用于反潜回判断。

可点击“删除记录”，在弹出框中选择卡号，点击“确定”可删除所有设备中包含所选卡片的进出门信息。

4） 点击反潜回主机配置项中的“选择主机”，并在弹出的配置框中选择需要反潜回认证的主机。

可选择已选主机列表中的主机，并点击“删除”删除该主机。

5） 在配置读卡器项中点击读卡器名称左侧的图标来选择首个读卡器。图标变为 。

6） 点击后续读卡器输入框，并在弹出选择读卡器窗口中按反潜回顺序勾选后续读卡器。

7） 在“启用反潜回”项勾选对应反潜回的勾选框以启用反潜回。

- 显示在界面上的后续读卡器顺序为需要反潜回认证顺序。
- 最多可添加 64 台反潜回主机。
- 每个读卡器最多可添加 16 个后续读卡器。
- 服务器最多可以存 5000 张卡的刷卡记录。

- 进出反潜回

用户需从配置的任一进门读卡器刷卡进入，并从配置的任一出门读卡器刷卡出门。无需配置起始读卡器和后续读卡器。

在跨主机反潜回界面，勾选“启用跨主机反潜回”。

在反潜回模式中选择“基于卡读写”或者“基于网络通信”。

基于卡读写：通过存于卡片上的进出门信息判断是否反潜回认证成功。

基于网络通信：通过存于读卡器上的进出门信息判断是否反潜回认证成功。

配置反潜回规则，选择“进出反潜回”。

图6-103 进出反潜回界面

若选择的反潜回模式为“基于卡读写”，则需配置扇区 ID。

若选择的反潜回模式为“基于网络通信”，则需在服务器下拉列表中选择一个服务器用于反潜回判断。

点击反潜回主机配置项中的“选择追加”，并在弹出的配置框中选择需要反潜回认证的主机。

可选择已选设备列表中的主机，并点击“删除”删除该主机。

或点击“清空”清空所有列表中的主机。

勾选读卡器配置项中的需要启用反潜回的进门读卡器和出门读卡器。

点击“保存”保存配置的参数。

- 至少勾选一个进门读卡器和一个出门读卡器。
- 最多可添加 64 台反潜回设备。
- 选择“基于卡读写”时，目前支持 M1 卡的卡读写；且对应扇区不能加密。关于配置扇区加密的内容，详见 6.4.1 设备管理中的 M1 卡加密章节。
- 选择“基于网络通信”时，服务器最多可以存 5000 张卡的刷卡记录。

配置多门互锁

配置多门互锁后，在配置为多门互锁的门中，最多只能开启一扇门。且其他门必须处于

关闭状态时才能开启这扇门。

点击“多门互锁”进入多门互锁界面。

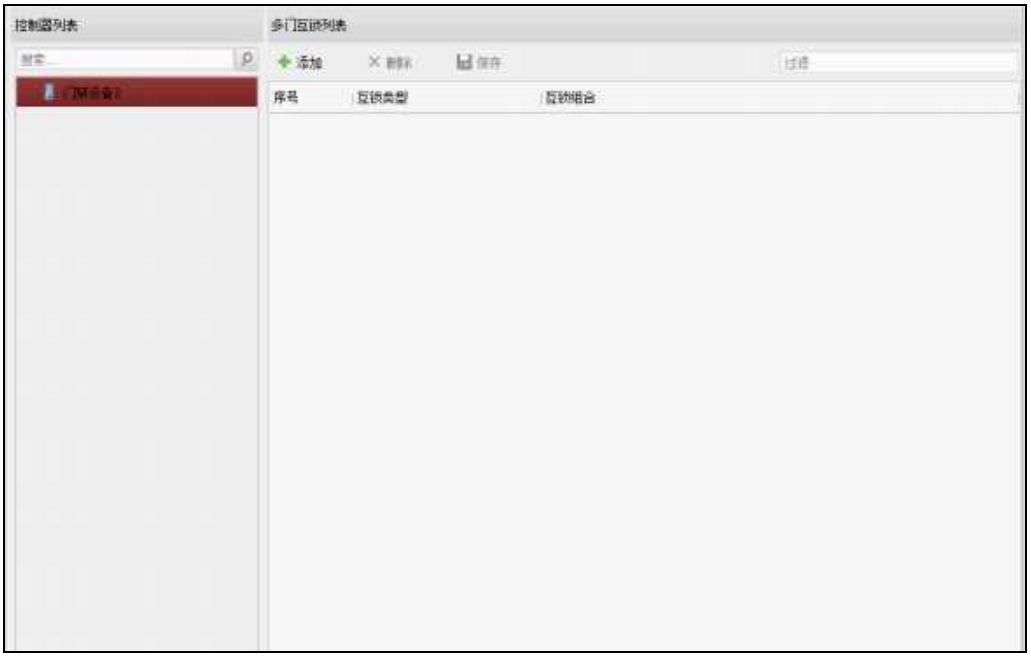


图6-104 多门互锁界面

在多门互锁界面左边控制器列表中选择一个设备。

点击右侧界面“添加”。

在弹出的配置框中勾选该设备下需要互锁的门（至少勾选两个门），并点击“确定”完成添加。

点击“保存”将配置的参数保存。

如有可能，选择需要删除的多门互锁，点击“删除”。在弹出的提示框中点击“确定”即可删除该多门互锁。（可多选）

每个设备最多可添加 4 个互锁组合。

配置手机白名单

在白名单中的手机可通过发送 SMS 控制指令对门禁主机进行远程控制。

点击“手机白名单”进入手机白名单界面。

图6-105 手机白名单界面

在手机白名单界面左侧的控制器列表中选择需要添加白名单的设备。

在右侧手机白名单配置界面中点击“添加”。

输入手机号码。

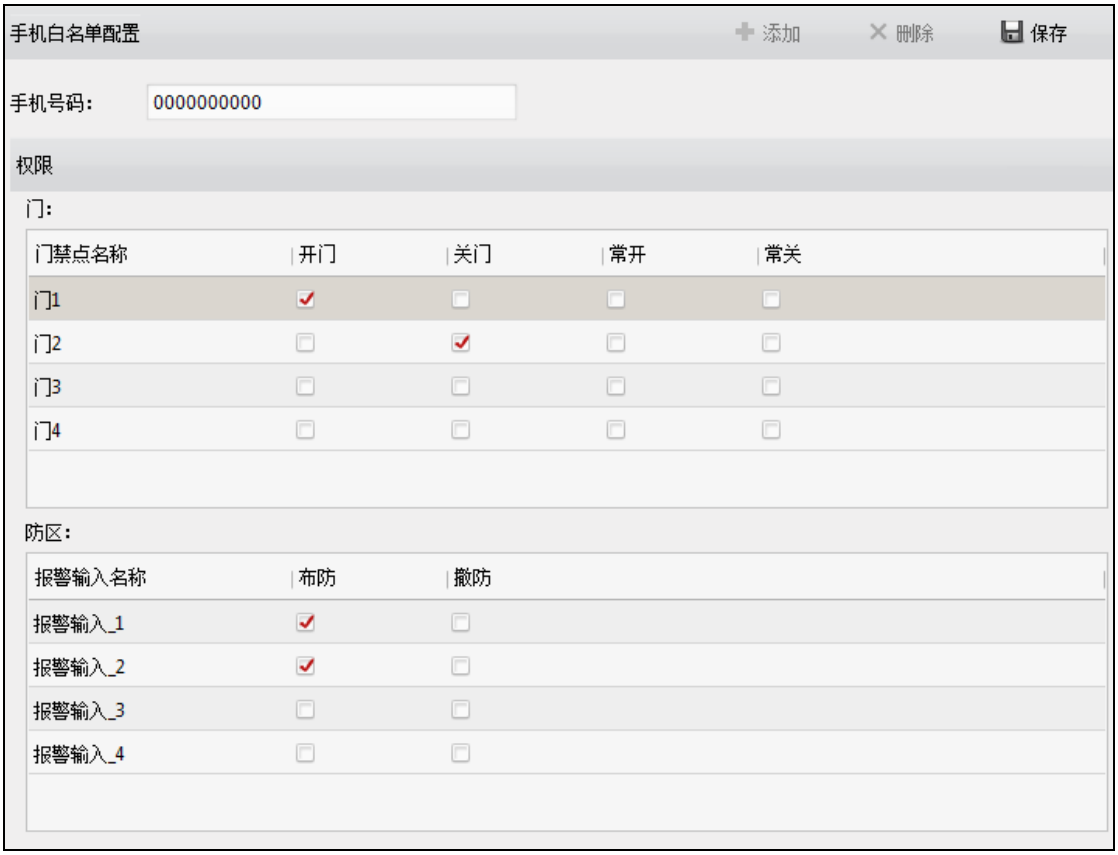


图6-106 手机白名单配置

勾选“门”和“防区”的权限。

门：选择是否允许该手机用户控制门的开/关/常开/常关。

防区：选择是否允许该手机用户进行防区报警输入的布撤防控制。

点击“保存”保存设置。列入白名单的手机将显示在左侧的设备下。

说明

可通过手机白名单中的手机所发送的 SMS 控制指令控制门和防区。

指令由“命令+操作范围+操作对象”组成，具体如下表所示：

控制指令

指令成分	位数	具体分类	格式
命令	3 位数	010-开门，011-关门，020-常开，021-常闭，120-撤防，121-布防	
操作范围	1 位数	1-所有有权限对象，2-单个操作	命令#1#
操作对象	3 位数	从 001 开始，根据命令对应门或防区	命令#2#操作对象#

举例：

如对门 1 进行开门操作，发送：010#2#001#；

如对本号码所有有权限的门进行常开操作，发送：020#1#。

- 点击“下发配置”使配置在设备中生效。
- 每个设备最多可添加 8 个手机。

配置认证码

对卡片设置认证码后，可通过输入认证码直接开门（不需刷卡）。

点击“认证码”进入密码认证页面。

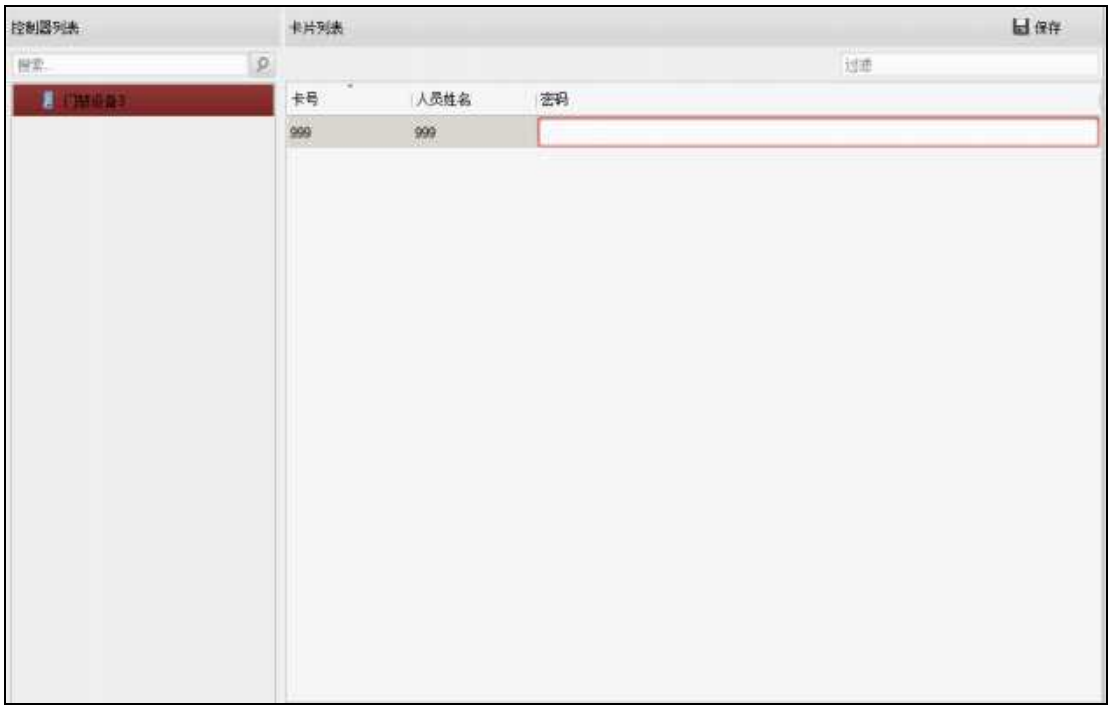


图6-107 认证码界面

在界面左侧控制器列表中选择需要配置认证码开门的设备。

在卡片列表界面中选择需要配置的人员，并点击密码栏。

在显示的输入框中输入认证码，并点击界面其他任何地方，认证码将设置成功。

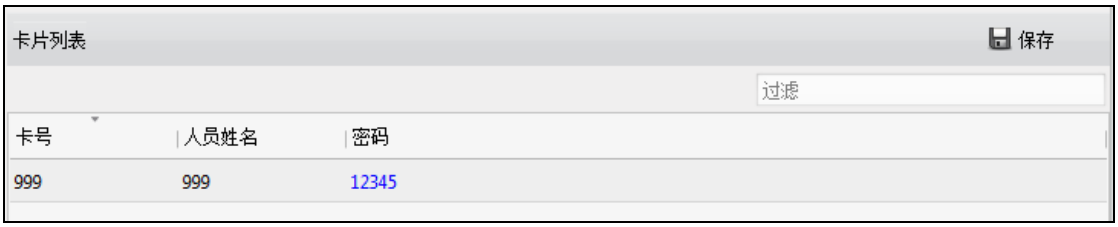


图6-108 添加卡片配置框

点击右上角“保存”按钮，将参数保存。

认证码应由 4-8 位数字组成。

认证码不可重复，并不可与读卡器参数中的超级密码、胁迫码、解除码重复。

一个设备最多可对 500 张卡片添加认证码。

只有当读卡器验证方式为“刷卡或认证码”验证时，认证才有效。更多关于读卡器认证的内容，请参考本章节中的配置读卡器认证。

6.5 门禁事件配置

6.5.1 门禁事件

可在此小节为门禁事件配置门禁联动。

说明

此处配置的联动为联动客户端自身的动作。

在事件管理界面选择“门禁事件”进入门禁事件页面。

门禁设备列表将显示在页面左侧列表中。

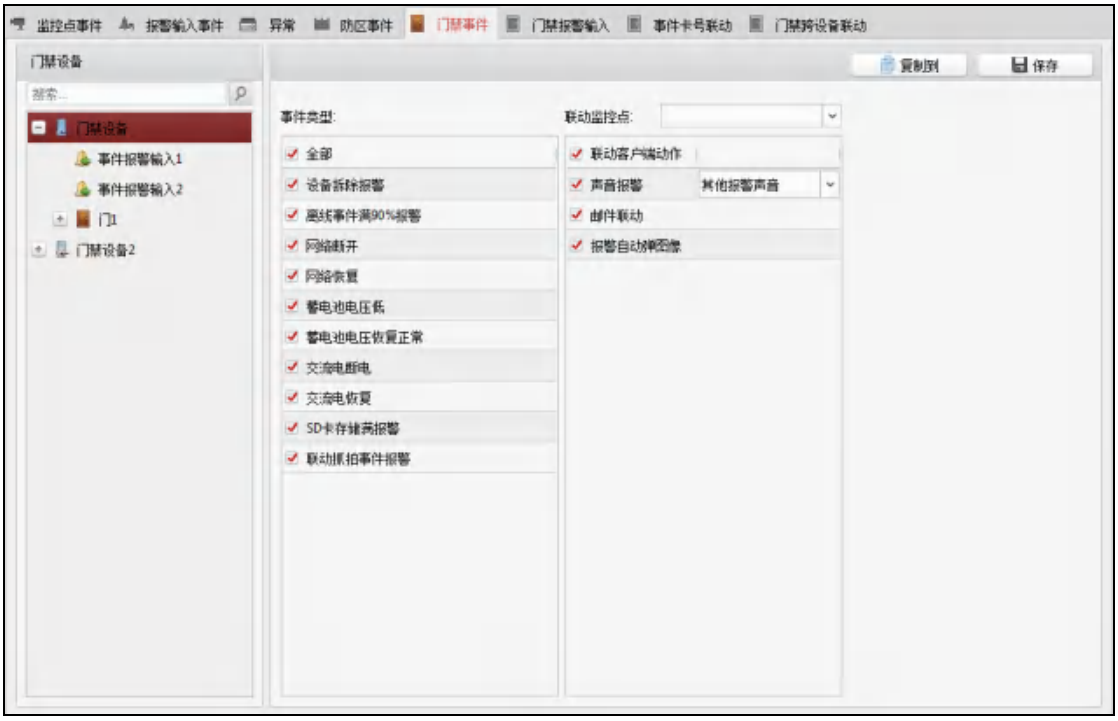


图6-109 门禁事件页面

选择一个门禁设备、报警输入、门禁点（门）或读卡器。

勾选事件类型。

在下拉框中选择联动监控点。

说明

如果触发报警，界面弹出联动的监控点画面。

若被关联的监控点设置存储录像到存储服务器中，且该存储服务器配置了图片存储空间，那么联动时，客户端会触发该监控点抓图，并保存到存储服务器中。

勾选联动动作。

声音报警：触发客户端音频报警。

邮件联动：报警联动发送 Email 给指定的邮箱。

报警自动弹图像：将报警图像单窗口显示，需要联动监控点。

电子地图报警：联动电子地图上报警。

6.5.2 门禁报警输入

在该界面可进行门禁设备的事件报警输入联动配置。需要门禁设备支持才可配置该界面。

说明

此处配置的联动为联动客户端自身的动作。

在事件管理界面选择“门禁报警输入”进入门禁报禁输入页面。

图6-110 事件报警输入联动界面

在界面左侧选择事件报警输入联动列表中的某个设备的事件报警输入。

在属性界面选择是否关联主机蜂鸣、读卡器蜂鸣、报警输出、门禁点。

点击右上角“保存”按钮保存配置的参数。

6.5.3 事件卡号联动

在该界面中可进行事件联动报警动作以及卡号联动报警动作的配置。

说明

此处配置的联动为联动客户端自身的动作。

事件联动

配置报警事件触发后联动本机报警动作。报警事件可分为设备事件，报警输入事件，门

事件，和读卡器事件。

在事件管理界面点击“事件卡号联动”，进入事件卡号联动页面。

图6-111 事件卡号联动界面

在界面左侧事件卡号联动列表中选择一个设备。

在界面右侧事件卡号联动详细信息界面中点击“添加”。

在事件源板块中选择“事件联动”。可选择设备事件、报警输入事件、门事件、或读卡器事件作为事件大类，在第二个拉菜单中选择相应的事件小类。

图6-112 事件联动

配置“联动目标”。可配置是否关联主机蜂鸣/停止蜂鸣、是否联动抓拍功能、是否关联读卡器蜂鸣/停止蜂鸣，是否关联报警输出/停止输出，是否关联防区布防/撤防以及是否关联开门/关门/常开/常关。

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”）。

联动目标需设备支持才可配置。

门事件源中选择的门与联动目标的门不可是同一个门。

卡号联动

配置卡号联动的本机报警动作。

在事件卡号联动界面左侧事件卡号联动列表中选择一个设备。

在右侧事件卡号联动详细信息界面中点击“添加”。

在事件源板块中选择“卡号联动”。并在卡号联动右侧文本框中输入卡号。

或点击卡号联动右侧按钮，并在下拉框中选择中卡号。

图6-113 卡号联动

选择读卡器作为卡号联动的对象。

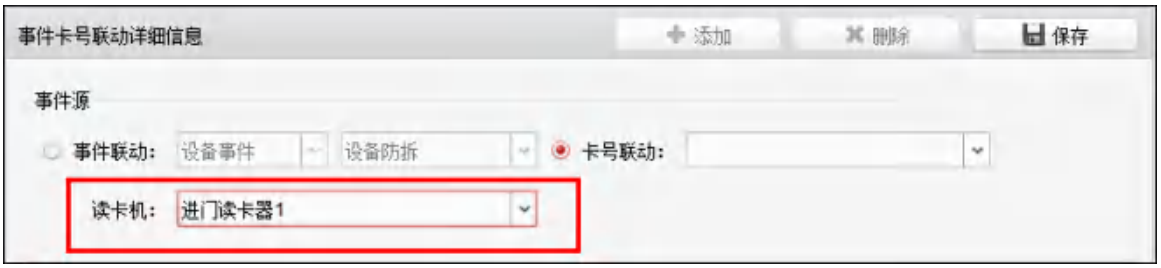


图6-114 选择读卡器

配置“联动目标”。可配置是否关联主机蜂鸣/停止蜂鸣、是否联动抓拍功能、是否关联读卡器蜂鸣/停止蜂鸣，是否关联报警输出/停止输出，是否关联防区布防/撤防以及是否关联开门/关门/常开/常关。

点击“保存”保存配置。

联动目标需设备支持才可配置。

修改/删除事件卡号联动

点击界面左侧在门禁设备下的时间卡号联动，即可修改联动目标。点击“保存”完成修改。

或点击右上角“X 删除”按钮，可删除该联动。

6.6 门禁跨设备联动

可配置联动触发其他设备的门禁点或报警输出。

6.6.1 添加门禁跨设备联动

点击“门禁跨设备联动”，进入门禁跨设备联动页面。

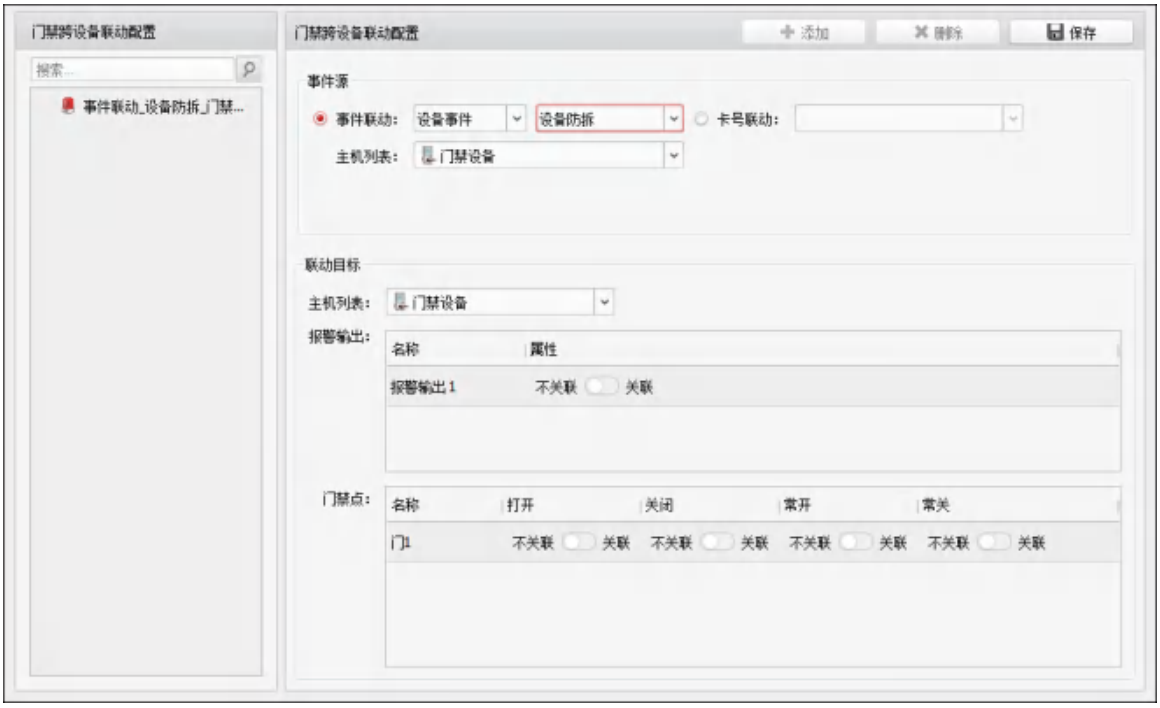


图6-115 跨设备联动界面

点击右侧客户端联动配置界面中的 “添加”。

在事件源“主机列表”下拉框中选择一个设备。

选择事件联动类型。可选择的事件联动类型有设备事件、报警输入事件、门事件和读卡器事件。根据所选的时间联动类型大类可选择事件小类。

图6-116 事件联动

若选择的是非设备事件，则需要选择相应内容。

图6-117 选择防区报警输入

如有需要，可勾选“卡号联动”，并输入卡号，进行卡号联动配置。

图6-118 卡号联动

选择需要配置设备和读卡器。

图6-119 勾选设备读卡器

配置目标设备的联动信息。

图6-120 配置目标设备的联动信息

点击“保存”保存配置。保存的客户端联动配置将显示在客户端联动配置列表中。

图6-121 门禁跨设备联动配置列表

事件联动类型下拉框中只显示设备支持的类型。

只有设备事件和报警输入事件可以联动门动作，且同一个门只能关联一种动作。

联动目标需设备支持才可配置。

6.6.2 修改/删除门禁跨设备联动

在门禁跨设备联动界面左侧配置列表中选择需要修改的联动事件。可修改右侧客户端联动配置界面联动目标模块下的报警输出属性和门状态。点击“保存”完成修改。

或点击“X 删除”按钮，可删除该联动。

6.7 门禁事件查询

可搜索并查看门禁历史事件。搜索方式分为从客户端本地搜索和从设备端搜索，并能够根据查询条件筛选出相应的事件信息，还可导出这些信息。

在门禁控制模块点击信息查询按钮，进入信息查询界面。

点击“门禁事件查询”进入门禁事件查询页面。

选择搜索来源。

若选择“客户端”，配置其他搜索条件，点击“查询”开始搜索。

可配置的项包括：

事件类型：包括设备事件、报警输入事件、门事件和读卡器事件。

持卡人姓名：可输入持卡人姓名搜索指定人员发生的事件。

卡号：可根据输入的卡号搜索事件。

开始时间和结束时间：可在时间段内搜索门禁事件。

读卡器类型：可根据读卡器类型搜索门禁事件。

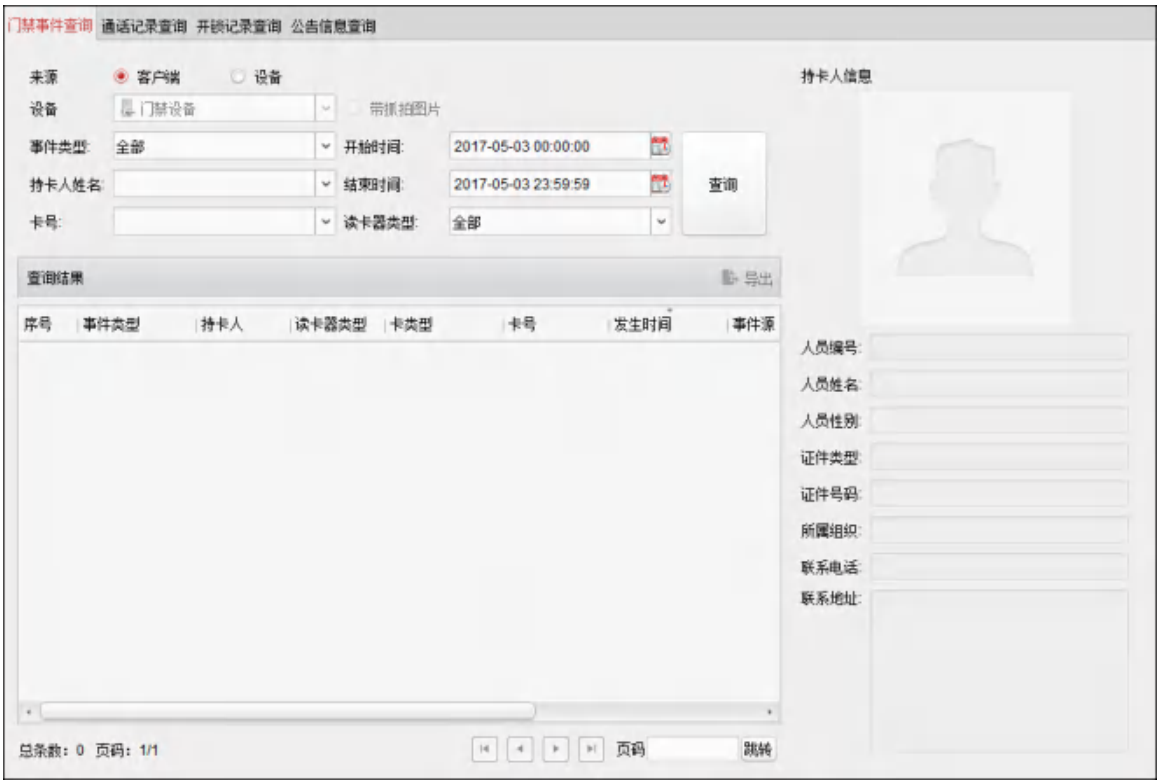


图6-122 搜索事件

若选择“设备”，配置其他搜索条件，点击“查询”开始搜索。

可配置的项包括：

设备：可在下拉框中选择需要搜索的设备。

带抓拍图片：若勾选，则搜索出来的的事件信息包含触发抓拍的事件。

事件类型：包括设备事件、报警输入事件、门事件和读卡器事件。

持卡人姓名：可输入持卡人姓名搜索指定人员发生的事件。

卡号：可根据输入的卡号搜索事件。

开始时间和结束时间：可在时间段内搜索门禁事件。

点击查询结果中的某条事件，根据事件类型及卡类型可在界面右侧查看触发此事件的持卡人信息。

如该人员在身份证读卡器上刷身份证，则设备上报身份证刷卡事件，在此处则可查看身份证正反面信息。

图6-123 持卡人信息

如该人员有登记身份证信息，则可查看身份证正反面信息。可点击查看身份证正反面信息。

如有需要，可导出所需查询结果。点击查询结果中的事件，点击“导出”按钮可将此信息导出到本地。

6.8 状态监控

可在此模块中控制门状态、查看刷卡记录并查看门禁设备的报警信息。

在进行以下配置前，请先添加门禁设备，并在“门组管理”中配置门组。

6.8.1 门状态

控制门状态

在客户端控制面板，点击 按钮，进入状态监控界面。

或点击“视图”-“状态监控”进入状态监控管理界面。

图6-124 门状态界面

在左侧门禁分组中选择一个分组。

在右侧“状态信息”中选择要反控的门禁点（按住 Ctrl 键可多选）。

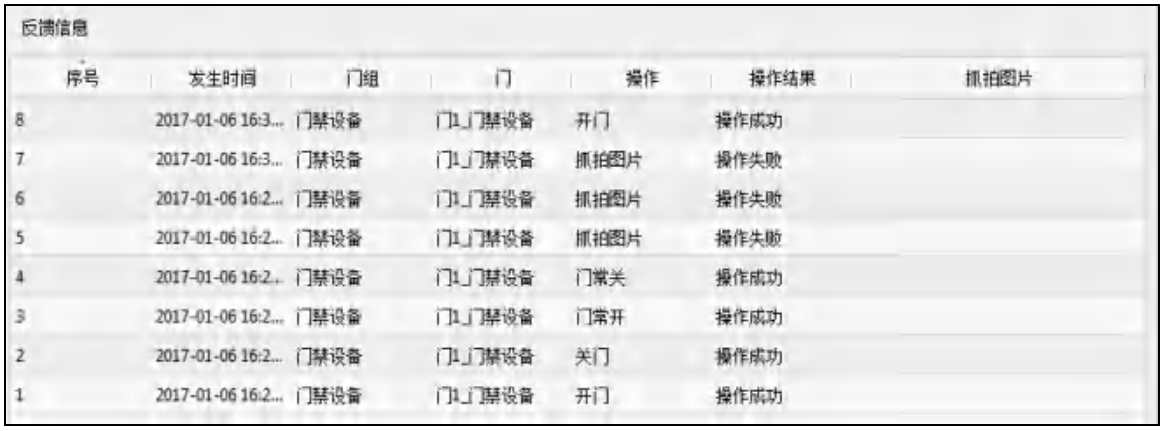
点击右上角控制按钮，可选择开门、关门、常开、常关或者抓拍图片（需设备支持才可选择）。抓拍图片后，点击图片可进行预览。

需配置存储服务器后方可进行抓拍。详见 iVMS-4200 客户端用户手册。

图6-125 状态信息栏

门禁反控操作后，门的最新状态将会在操作日志栏里。

操作日志中显示的信息主要包括：序号、发生时间、门组、门、操作、操作结果和抓拍图片。


反馈信息

序号	发生时间	门组	门	操作	操作结果	抓拍图片
8	2017-01-06 16:3...	门禁设备	门1_门禁设备	开门	操作成功	
7	2017-01-06 16:3...	门禁设备	门1_门禁设备	抓拍图片	操作失败	
6	2017-01-06 16:2...	门禁设备	门1_门禁设备	抓拍图片	操作失败	
5	2017-01-06 16:2...	门禁设备	门1_门禁设备	抓拍图片	操作失败	
4	2017-01-06 16:2...	门禁设备	门1_门禁设备	门常关	操作成功	
3	2017-01-06 16:2...	门禁设备	门1_门禁设备	门常开	操作成功	
2	2017-01-06 16:2...	门禁设备	门1_门禁设备	关门	操作成功	
1	2017-01-06 16:2...	门禁设备	门1_门禁设备	开门	操作成功	

图6-126 操作日志

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。只能有一个客户端可以对门禁点进行布防。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。布防设备可详见 iVMS-4200 客户端用户手册。

在门常关的状态下，仅超级卡或远程控制方可开门。

配置状态时段

步骤1. 点击左侧状态信息中的“状态时段”按钮。

步骤2. 在弹出的状态时段配置框的门禁点列表中选择某个设备的某个门禁点。

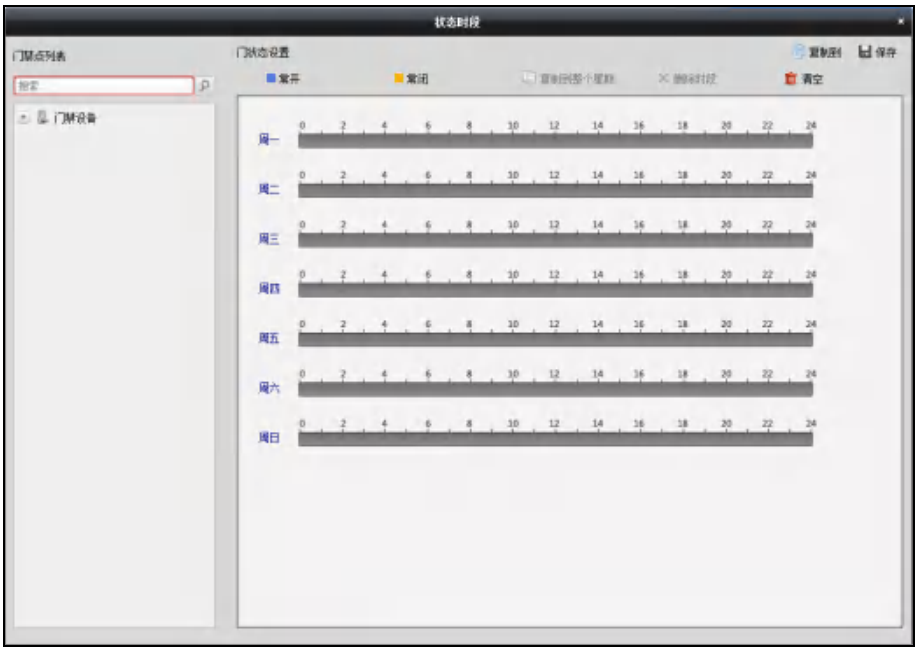


图6-127 状态时段配置框

步骤3. 选择“常开”或“常关”按钮。在界面下方的计划表中点击并拖动鼠标，以设置每天的门常开或常关计划。

说明

一天最多可添加 8 个时段。

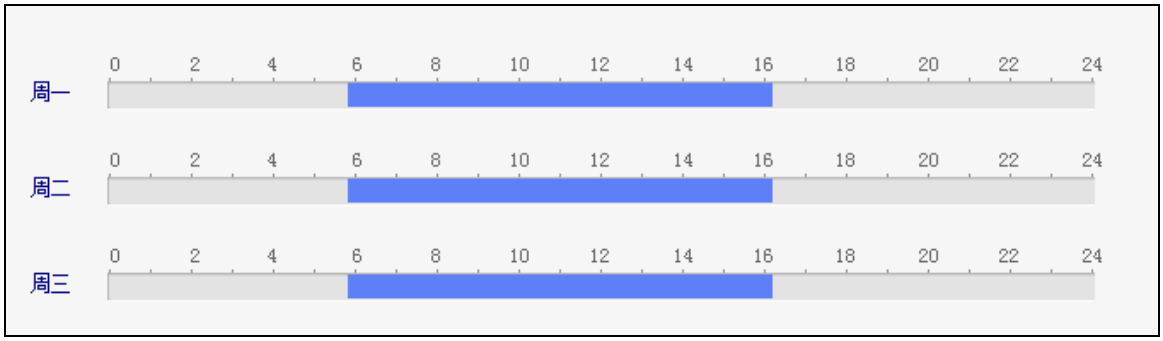


图6-128 配置常开常关时间计划

或者点击已划定时间计划，点击可设置精确时间。点击“确定”保存设定。

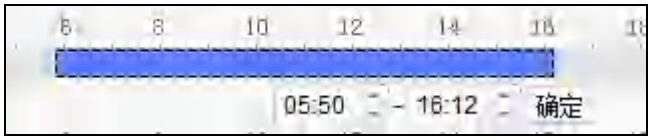


图6-129 配置常开常关精确时间计划

若一周内每日的计划相同，则选中需要复制的时间计划，点击“复制到整个星期”即可将选中的时间计划复制到整周。

若有需要，选中某段时间计划，点击“删除时段”即可删除该段计划。

若有需要，点击“清空”，可将所有计划全部清空。

步骤4. 点击右上角“保存”按钮保存设置的门常开、常关计划。

若有需要，点击“复制到”，在弹出的配置框中勾选需要的被复制到的门禁点，可将此处配置的门状态时段周计划复制到被勾选的门禁点中。

6.8.2 查看刷卡记录

点击“刷卡记录”进入刷卡记录界面，可查看在门禁设备上的刷卡记录。可查看卡号、人员姓名、部门、刷卡发生时间、门位置、方向。

点击操作栏下的可查看电子地图中的刷卡点（需要在电子地图中添加刷卡点）。

点击按钮可查看刷卡时的视频（需设备支持，并在门禁事件中联动监控点）。

点击按钮可查看刷卡时抓拍到的图片（需设备支持，并在门禁事件中联动监控点）。

图6-130 刷卡记录界面

6.8.3 查看报警信息

可在此查看订阅后的实时门禁报警信息。

在状态监控模块，点击“门禁报警”进入门禁报警界面。

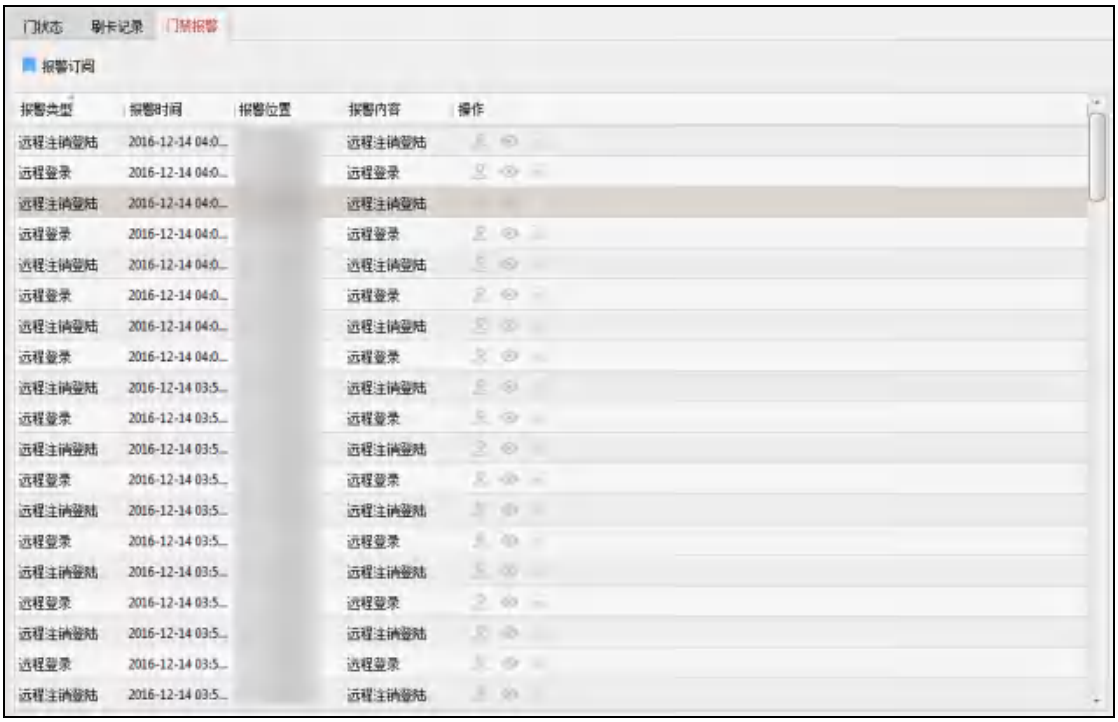


图6-131 门禁报警界面

点击“报警订阅”按钮，进入报警订阅窗口。

图6-132 报警订阅窗口

勾选需要订阅的报警信息。可订阅设备事件、门事件、读卡器事件和报警输入事件。

点击“确定”完成订阅。

可在门禁报警界面中查看发生的报警事件。

点击操作栏下的可查看电子地图中的刷卡点（需要在电子地图中添加刷卡点）。

点击按钮可查看刷卡时的视频（需设备支持，并在门禁事件中联动监控点）。

点击按钮可查看刷卡时抓拍到的图片（需设备支持，并在门禁事件中联动监控点）。

6.9 布防控制

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。

在菜单栏中点击“工具”-“设备布防控制”进入设备布防控制窗口。

图6-133 设备布防控制窗口

勾选需要布防的设备，布防状态将变为，或取消勾选需要撤防的设备，布防状态将变为。

科技呵护未来

First Choice for Security Professionals

海康威视客户服务

海康威视官方网站

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：400-700-5998