

2020

D.one[®] DW-68 系列一卡通门禁系统用户手册

日期：2021-01

由于产品不断更新，本公司不承诺实际产品与该数据一致，同时也不承担由于实际技术参数与本数据不符而导致的任何争议，任何改动恕不提前通知。



目 录

第 1 章 系统简介	2
1.1 系统功能简介	2
1.2 系统流程介绍	2
第 2 章 客户端的安装	4
2.1 客户端的安装	4
2.2 数据库创建	5
2.3 设备数据服务系统	5
第 3 章 系统管理	7
3.1 登录系统	7
3.2 退出系统	7
3.3 修改密码	7
3.4 部门添加	7
3.5 角色管理	7
3.5.1 角色添加	7
3.5.2 角色的编辑、删除	8
3.5.3 角色权限分配	8
3.5.4 角色授权	8
3.6 操作员添加	8
3.7 数据字典	9
3.7.1 卡片类型	9
第 4 章 平台管理	10
4.1 部门管理	10
4.1.1 新增部门	10
4.1.2 部门编辑	11
4.2 人员管理	11
4.2.1 新增人员	11
4.2.2 人员批量添加	12
4.2.3 人员信息维护	12
4.2.4 添加人员指纹信息	13
4.3 卡片增加	14
4.3.1 卡片的操作	14
4.3.2 发卡器批量添加卡片	14
4.3.3 读头加卡	14
4.3.4 指纹仪管理	15
4.3.5 CPU 卡管理	18
4.3.6 人脸识别管理	19
第 5 章 设备管理	20
5.1 设备区域设置	20
5.2 设备管理	20
5.2.1 设备网络参数设置	20
5.2.2 设备添加	21
5.2.3 设备编辑、删除及导出	23
5.2.4 复制设备参数	23
5.3 设备端口管理	23
5.4 人脸管理	24
5.4.1 设备扫描添加	24
5.4.2 手动添加设备	24
5.4.3 人脸阈值设置	26
5.4.4 屏幕显示设置	26
5.4.5 获取设备状态	27
5.4.6 远程升级	27
5.4.6 设备操作	27

5.4.7 添加黑名单功能	28
5.5 人脸控制一体机管理	28
5.5.1 添加设备	28
5.5.2 设备管理设置	29
5.5.3 门管理设置	30
5.5.3 人脸下发	30
第6章 门禁管理	31
6.1 门禁时间	31
6.1.1 周编程	31
6.1.2 假日编程	32
6.2 门开闭时段管理	32
6.3 门设置	33
6.3.1 单个修改门参数操作步骤	33
6.3.2 批量修改门参数	35
6.3.3 非远程确认开门段	35
6.3.4 启用开放管制时间段	35
6.3.5 查询	35
6.4 门禁权限的设置	35
6.4.1 设备权限组管理	35
6.4.2 人员权限管理	37
6.5 互锁设置	38
6.6 联动设置	38
6.7 反潜回配置	39
6.8 门禁黑名单	40
6.9 设备任务管理	40
6.10 设备的初始化与恢复出厂设置	41
6.11 实时监控	42
6.11.1 打开的监控界	42
6.11.2 设置界面	43
6.11.3 动态码功能	46
6.11.4 开关服务功能	46
6.11.5 报警处理	47
6.11.6 电子地图	47
6.12 点名功能	48
第7章 报表	50
7.1 门禁报表	50
7.1.1 记录报表	50
7.1.2 历史记录报表	51
7.1.3 入库超时报警表	51
7.1.4 访客报表	51
7.1.5 综合报表	51
7.1.6 停车场报表	51
7.1.7 门禁报表 683	51
第8章 数据库管理	52
第9章 用户使用 FAQ	53



名词解释

超级用户：即拥有系统全部操作权限的用户，可以在系统中分配新用户（如公司管理人员、登记员、门禁管理员等）并配置相应用户的角色。

角色：在日常使用过程中，超级用户需要分配一些具有不同权限级别的新用户，为避免对每个用户一一进行设置，可以在角色管理中设置一类具有一定权限的角色，在新增用户时直接将合适的角色分配给用户。

门禁时间段：用于门的时间设置，可以设置读头仅在指定门的有效时间段可用，其他时间段不可用，也可以用于设置门的常开时间段；时间段可以用于设置门禁权限，指定用户只能在指定时间段访问指定门（含门禁权限组和首卡常开设置）

门磁延时：门被打开后，延迟检查门磁的时间。如果门在非“常开”时段处于开状态，则开始计时，当达到门磁延时设置的时间，则发生报警，如果将门关闭，则报警停止。门磁延时需大于锁驱动时长。

首卡开门：每天，当有首卡常开权限的人员第一次刷卡后，门将开启并且其它受首卡限制权限的人员才可以刷卡开门，过零点后重新支行逻辑

受首卡限制：与首卡开门权限配合使用，该权限的人要在具有首卡权限的人第一次刷卡后才可以刷卡开门

多卡开门：某些特定门禁场合需要启用该功能：要求同一个开门的组合中指定人数同时到场，并依次刷卡才能验证通过，通过验证前，不能插入其他卡（即使是该门其他组合的有效卡），否则要等待10秒后重新验证。

互锁：可设置一个控制器的两扇（或多扇）门之间的互锁管制，当要开启一扇门时，其他对应的门必须都是关闭的，否则无法开门。

反潜：特殊场合对安全性要求高，要求出入一一对应。例如，1-2门反潜：如果人员从1门入，必须从2门出；如果人员从2门入，必须从1门出。

联动设置：在门禁系统中的某个输入点触发某个特定事件后，会在指定的输出点产生一个联动动作，用来控制系统中的验证、开门、报警、异常等事件，并在监控事件列表中显示。

权限服务控制：设备启用权限服务控制后，需要具有开启权限服务权限的人员刷卡请求开启或关闭服务，并由中心确认开启或关闭服务。开启服务后其他具有开门权限的人员才可以正常验证开门，反之则无法开门。

断网特殊开门：在断网时间段内开门方式做特殊处理，用户自定义组合方式

注意：使用断网特殊时段开门方式要求如下，后续不再赘述

1. 必须建立3个权限组（主卡、副卡1、副卡2），3个权限组配置需一致且以主卡配置为准
2. 启用远程确认开门方式才可使用断网特殊开门方式；
3. 启用断网特殊时段开门方式时，副卡2只有在断网的情况下有效，有网情况下副卡2无效。

下班时段组合验证：启用下班时段组合验证，则上/下班时段使用不同的验证开门方式，用户自定义组合方式

第 1 章 系统简介

1.1 系统功能简介

安全管理在近些年的现代企业管理中越来越受到管理者的关注。本系统实现门禁系统管理统一化、流程化，并帮助客户实现运营安全。

◆ 系统特点

1. 强大的数据处理能力，能管理100000 个人的门禁数据。
2. 形象而合理的操作流程融合了多年的门禁经验。
3. 自动化的用户名单管理，使得管理更科学、高效。
4. 建立在多级管理角色上的权限管理，能保证用户数据的保密性。

◆ 客户端硬件配置：

CPU: 主频4.0G 以上。

内存: 2G 及以上，推荐4G。

硬盘: 可用空间50G 及以上，推荐使用NTFS 的硬盘分区作为系统安装目录

◆ 系统运行环境

操作系统: WinServer2008R2/Windows7旗舰版/ Windows8/Windows10

数据库: MSSQL Server2008以上，10G以上数据库不建议使用免费版的SQL（express版本）

屏幕: 建议19寸及以上

◆ 系统功能模块介绍 本系统主要分为四大功能模块：

人事: 主要包括两部分，一是部门管理设置，即设置公司的主要架构；二是人员管理设置，为系统录入人员，分配部门，然后进行人员维护管理。

设备: 设置连接设备的通信参数,通信参数正确才能够与设备正常通信,包括系统中的设置和设备中的设置。通信成功后就能查看到已连接设备的信息并能对设备进行远程监控、上传、下载等操作。

门禁: 基于C/S架构的管理系统，能够实现普通门禁功能，通过计算机对网络门禁控制器进行管理，实现对人员进出的统一管理。门禁系统是对已经登记用户的开门时间及权限进行设置；即在某个时间段内，在某些门上，允许某些用户可以验证开锁。

系统: 主要是分配系统用户并配置相应用户的角色；管理数据库，如备份、初始化、还原等；设置系统参数，管理系统操作日志等。

1.2 系统流程介绍

下面介绍系统的整个流程。

第一步：系统运行环境的搭建

1. 数据库（MSSQL）软件的安装。
2. 客户端的安装，详细操作请参阅[2.1 客户端的安装](#)。
3. 创建系统使用的数据库，详细操作请参阅[2.2 数据库创建](#)。

第二步：系统快速操作流程

1. 部门的添加

点击【门禁】→【部门管理】→【添加】，在弹出的窗口中填写相关信息即可，详细操作请参阅[4.1 部门管理](#)。

2. 人员的添加并绑定卡片

点击【人事】→【人员管理】→【添加】，在弹出的窗口中填写完人员信息后，再点【卡片】绑定卡片后保存即可，详细操作请参阅[4.2 人员管理](#)。

3. 添加设备

1) 用工具修改设备的网络参数

打开操作系统【开始】→【门禁管理系统】→【设备网络工具】，在弹出的窗口点【扫描设备】，在扫描出来的设备中，选择相应的设备点【设置IP地址】，设置网络参数即可，详细操作请参阅[5.2.1 设备网络参数设置](#)。

2) 开启监控服务，设备连接上服务，详细操作请参阅[2.3 设备数据服务系统](#)

3) 添加设备服务器区域

点击【设备区域管理】→【添加】，在弹出的窗口填写完区域信息即可，详细操作请参阅[5.1 设备区域设置](#)。

4) 客户端添加设备

点击【门禁】→【设备管理】→【添加】，在弹出的窗口中通过【选择设备】添加网络中在线的设备，然后【确定】即可，详细操作请参阅[5.2.2 设备添加](#)。

4. 对设备进行门参数的设置

【门禁】→【门管理】选择需要修改的门，点【编辑】在弹出的窗口修改相应的参数即可，详细操作请参阅[6.3 门设置](#)。

5. 设备绑定权限组

点击【门禁】→【设备权限管理】，在弹出的窗口中选择“设备权限组”，然后选择相应开门“验证方式”，再选择“绑定的设备”即可，详细操作请参阅[6.4.1 设备权限组管理](#)。

6. 添加人员权限

点击【门禁】→【人员权限管理】→【添加】，进入人员权限的设置窗口，分配人员的权限即可，详细操作请参阅[6.4.2 人员权限管理](#)。

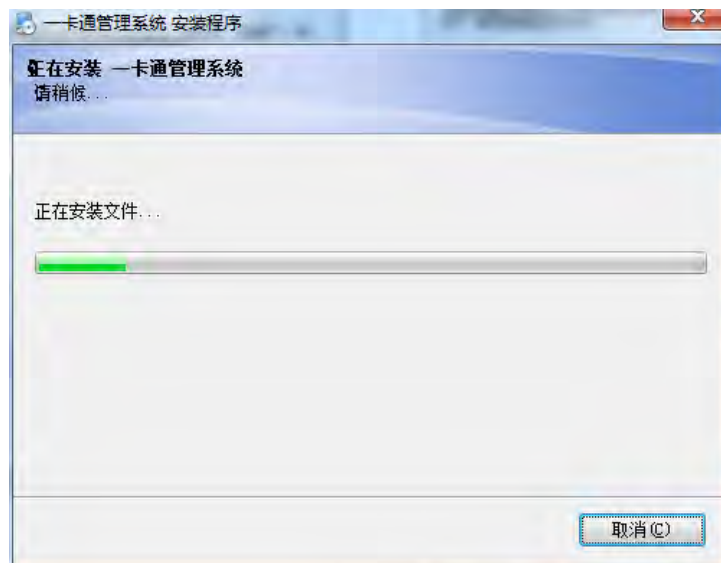
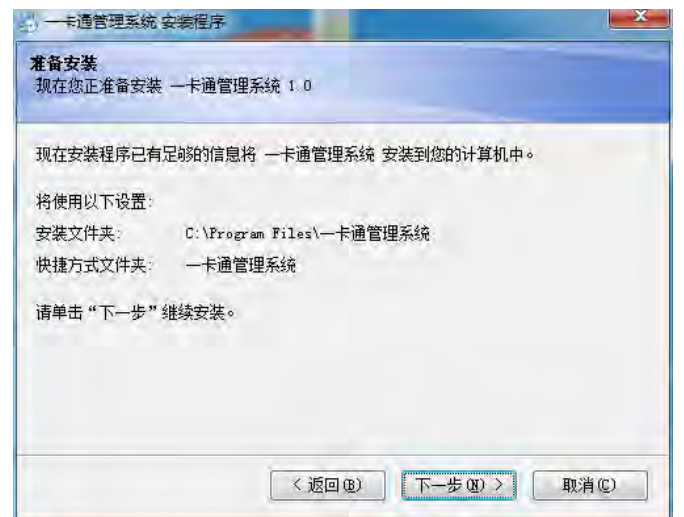
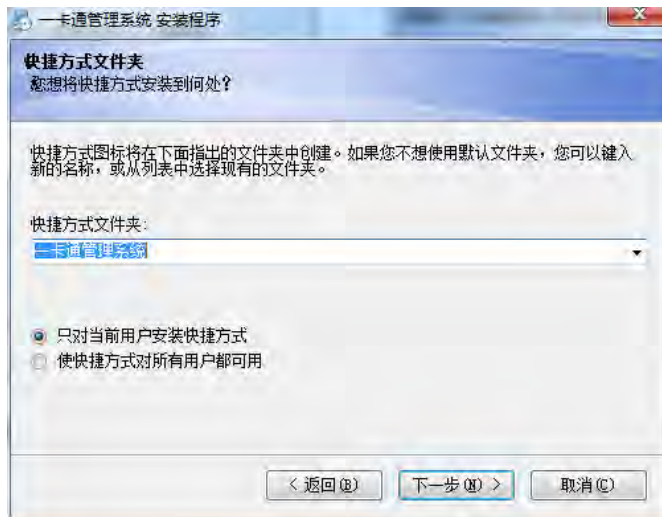
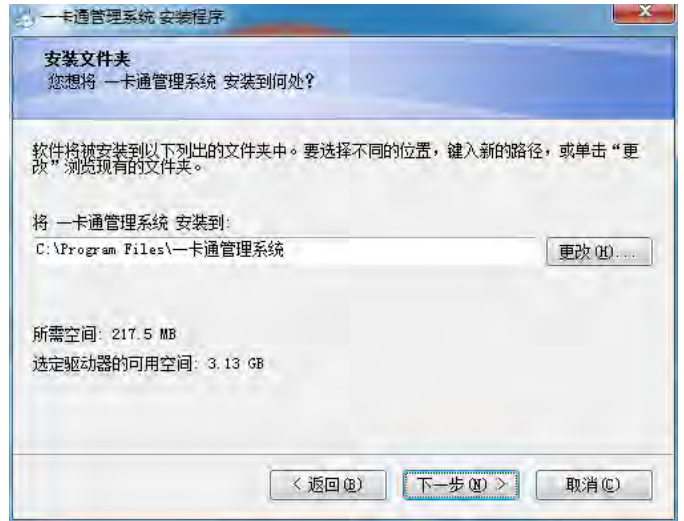
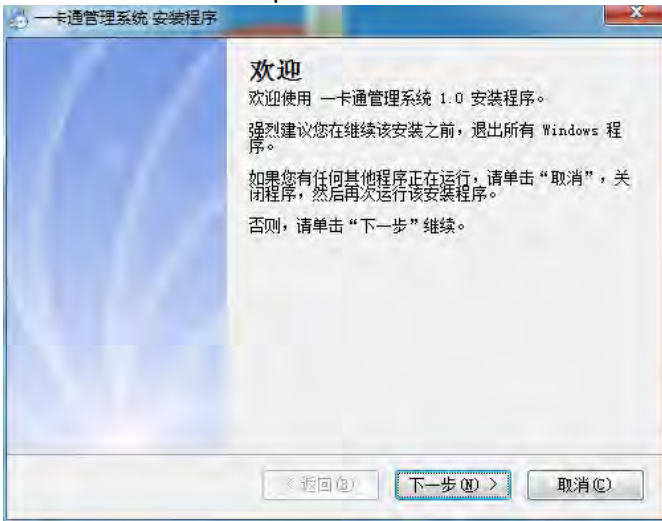
7. 下载参数到设备中

点【门禁】→【设备任务管理】→选择设备，右键在弹出的窗口中点“设置全部参数”、“设置全部人员权限”（可只选部分人员下载，人员数量少的可点全部下载），详细操作请参阅[6.7 设备任务管理](#)。

第 2 章客户端的安装

2.1 客户端的安装

打开安装文件“setup.exe”弹出界面，按照下图的指示安装即可



在安装之前安装程序会自动检测是否安装了 .NET Framework，若没有安装会弹出提示，点击确定提取 .NET Framework 的安装包，弹出 .NET Framework 的安装界面后按照提示安装即可。

2.2 数据库创建

打开数据库创建工具“CreateDB.exe”（在开始菜单中或监控客户端安装目录下），按要求填相应的信息
服务器：SQL：本地的可用点表示，局域网的可用IP来表示，建议服务器名称用IP方式

SQLEXPRESS（免费版）：.\sqlexpress来表示，此版本数据库有些没网络共享功能，只能单机使用

登录名：数据库SQL的登录名，默认sa

密码：数据库的密码

数据库名称：要创建的数据库的名称

数据库文件保存路径：可选择数据库要保存的路径，建议英文路径

测试：填写完前面的信息后，用来测试数据库的连接是否成功。

创建：填写完信息后点创建，待左下角出现“数据库创建完成”，关闭即可



2.3 设备数据服务系统


打开操作系统【开始】→【一卡通管理系统】→【监控服务】（或者桌面直接双击），弹出的窗口，点【服务设置】；输入设备服务IP（服务器电脑的IP），输入数据库的信息，具体请参阅[2.2 数据库建立](#)。

【日志管理】：是设备数据服务系统的操作日志、设备与设备服务系统连接情况的日志、下发的任务日志等



上图设备服务系统说明：

1. 左边的为设备列表框，显示设备的基本信息（Mac、IP、名称等）及设备最近一次在线及离线的时间，可以通过查询寻找设备
2. 双击单台设备时，可以单独显示此台设备的服务信息。
3. 列表下面有设备数量的统计及在线设备数量的统计，以及数据服务系统的运行时间。
4. 删除、删除所有是用来删除单台及全部不在线的设备。

 备注：此【设备数据服务系统】要一直开启，否则客户端无法进行操作。

第3章 系统管理

3.1 登录系统

(1) 打开系统，进入软件登录界面。



(2) 点击登录界面右上角倒三角按钮选择数据库设置，输入正确的数据库信息，点击确定即可连接数据库。测试按钮可以测试是否成功连接数据库。若还没有创建数据库，也可在此界面点击创建数据库按钮创建数据库，创建步骤参阅[2.2 数据库创建](#)。



(3) 进入系统时，需要进行身份验证，以保证系统安全。我们会为初次使用本系统的用户提供一个超级用户（拥有全部操作权限）。输入用户名和密码，单击【确定】。

 备注：超级用户的用户名为“admin”，密码：“SZ1z2020”用户首次登录系统后，为保证系统使用安全，

请在设置界面使用“修改密码”功能修改密码；

3.2 退出系统

直接单击右上角关闭按钮完全退出系统。

3.3 修改密码

超级用户和超级用户创建的新用户，可以使用“密码修改”功能修改登录密码，以保证系统的安全运行。在设置菜单界面单击【修改密码】弹出编辑界面，输入原密码、新密码、确定密码，单击【确定】完成修改

3.4 部门添加

操作方法见下文 [4.1 部门（区域）管理（下文以部门来统称）](#) 详细操作。

3.5 角色管理

3.5.1 角色添加

点【设置】→【角色管理】→【添加】，在弹出的界面上输入角色的名称，以及角色用来排序的序号及备注，这两项可填可不填。



3.5.2 角色的编辑、删除

选中需要操作的角色，可以进行角色的编辑或者删除。

3.5.3 角色权限分配

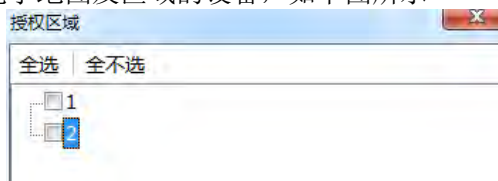
点【设置】→【权限设置】选中需要操作的角色，勾选需要分配的权限，为该角色分配软件的操作权限如下图所示：



在勾选权限的界面位置右键可全选所有权限。设置完权限之后点击【保存】即可完成各角色分配权限。

3.5.4 角色授权

选中需要操作的角色，点击【授权区域】、【授权地图】、【授权部门】，在弹出来的界面上，为该角色分配可查看的部门人员、电子地图及区域的设备，如下图所示



备注：部门、区域勾选了下级部门、区域了，该部门、区域的上级必须勾选；上图所示所有部门或区域都不勾选的话默认是具有所有的部门区域访问权限。

3.6 操作员添加

1) 在【设置】→【操作员管理】可以添加、编辑、删除操作员；添加时，在弹出的新建账号窗口填入相关的信息，部门、角色等。

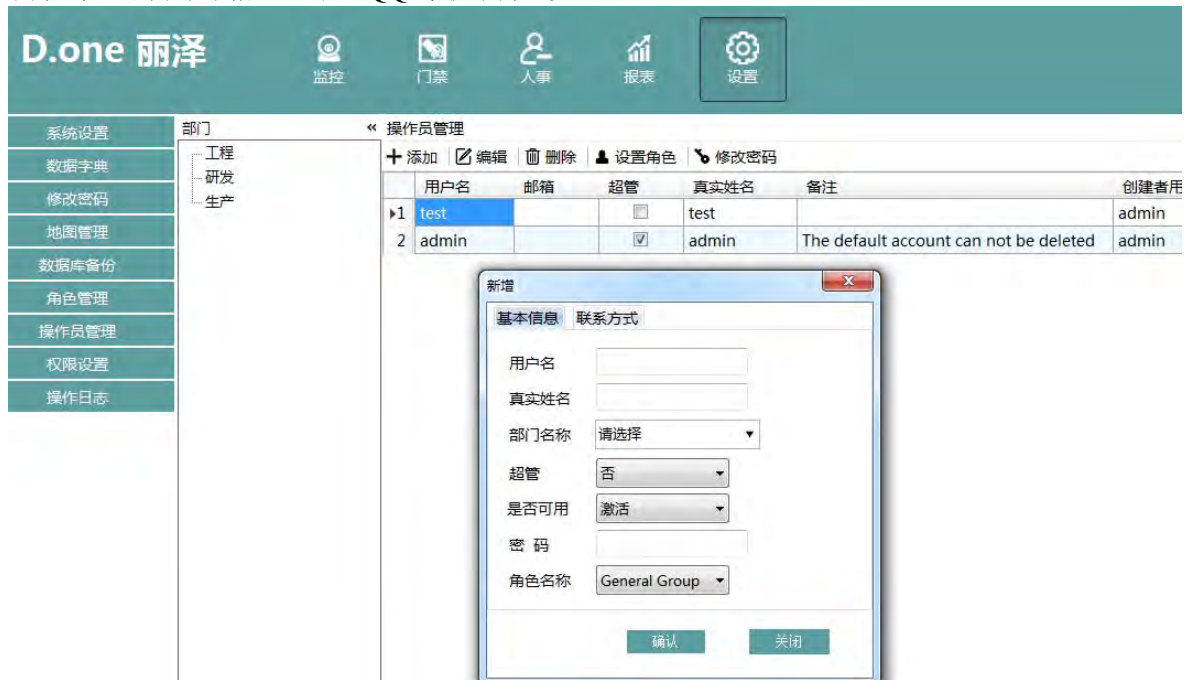
角色：为账号操作员选择角色，每个角色有不同的操作权限和部门权限。

是否超管：此操作员是否超级管理员

是否可用：可以禁用操作员，禁用后操作员无法登录，激活后才可登录

密码：新增操作员时密码可以任意设置，但修改密码必须由 6 位以上的数字或字母组成。

联系方式：可填写邮箱、电话、QQ 等联系方式。



备注：同一角色的操作员无法相互查看彼此账号；权限低的账户无法查看或修改权限高的账户

2) 操作角色分配：

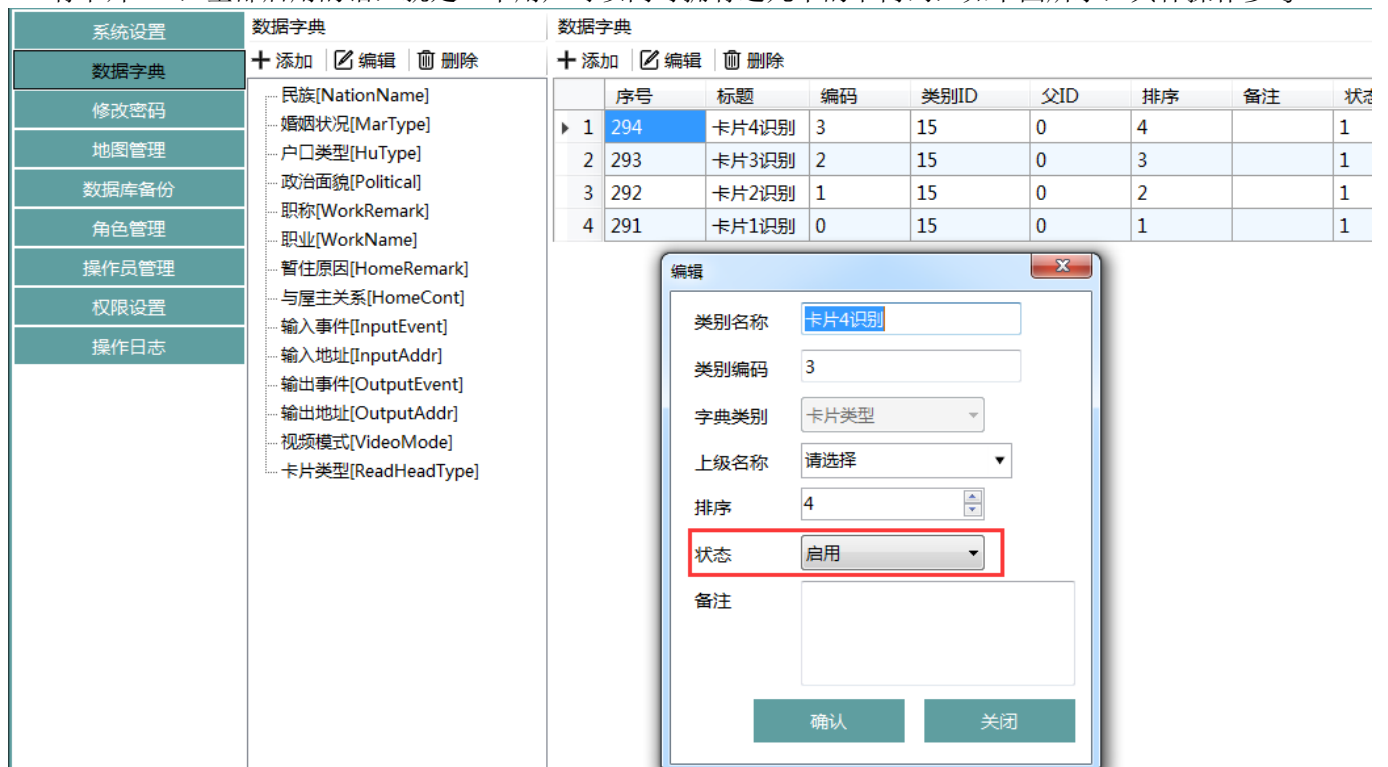
点【设置角色】—选择给操作员分配的角色（只能选 1 个）；上级角色创建的角色权限小于等于上级角色的权限。

3.7 数据字典

数据字典：就是软件上所有数据的一些字段信息如：民族、婚姻状态、户口类型等，这些大部分使用默认即可，不建议修改，除了“输入事件”里的自定义的事件名称可修改，其它信息及其它事件名称不能修改，“卡片类型”里是否启用不同类型的卡片可根据实际需要修改。

3.7.1 卡片类型

有卡片 1-4，全部启用的话，就是一个用户可以同时拥有这几个的卡内码，如下图所示，具体操作参考



第 4 章 平台管理

在使用系统的门禁功能之前，首先要进入平台管理进行设置：一是部门管理设置，即设置公司的主要架构；二是人员管理设置，为系统录入人员，分配部门，然后进行人员维护管理；三是卡片管理设置，为系统添加卡片

4.1 部门管理

对公司人员进行管理前，需要对公司的部门组织架构进行管理。

部门管理主要功能包括新增部门和部门维护。

部门编码	部门名称	上级部门编码	上级部门名称	部门负责人	联系电话
1	工程				
2	研发				
3	生产				

各字段说明如下：

部门名称：任意字符，名称不能重复。

部门编码：任意字符，编码不能重复。

上级部门：新增时，可以在下拉菜单中选择上级部门，选中后点击新增界面出下拉界面的任意其他位置即可确定。可不选。

部门负责人：任意字符，可不填。

联系电话：只能为数字，可不填。

权限组名称：可选择部门默认的权限组，往该部门添加新人员且同时发卡时会自动添加人员权限。


最大人数：设置该部门可容纳的最大人数，达到最大人数后不可再往该部门添加人员。

(2) 信息编辑完成后，点击【确定】完成新增，或点击【关闭】取消操作。新增部门还可以通过【导入】方式，将部门信息导入到本系统；也可以将系统的部门通过【导出】方式方便查看。其中【上级部门】项目是确定公司组织架构的重要参数。在界面左侧会以部门树的形式显示公司的组织结构图。

方法二：

(1) 点击【人事】，在人事界面的部门栏右键添加、编辑、删除部门。【导入数据】可以选择部门或者人员。操作方法与在部门管理类似。



 备注：部门信息导出时在部门信息表格处右键选择导出，导出的格式可为Excel和csv两种。本系统除监控菜单界面的监控记录外所有的表格都可以通过此种方式导出。

4.1.2 部门编辑

公司有部门变动或组织结构发生变化，用户可使用【编辑】功能进行修改，如部门的名称、编号或上级部门。直接点击部门名称或点击【编辑】，进入编辑页面进行修改。

对于需要删除的部门，选中该部门，点击【删除】。

 备注：部门有子部门，或者有人员时，不允许删除部门。删除部门可能会造成一些历史资料无法进行查询

4.2 人员管理

使用管理系统前，需要在系统中登记人员，或者通过导入的方式，将人员信息导入到本系统。



4.2.1 新增人员

1. 点击【人事】→【添加】，显示新增人员基础资料编辑界面。

注：用户编号、人员编号、人员姓名、所属部门为必填；用户编号、人员编号不能重复；身份证号码：18位的身份证号码；部门：点击下拉框后会弹出部门选择窗口，选中相应的部门即可。身份验证码需在系统设置中勾选后才会显示。

个人照片：两张相片（格式png、jpeg、jpg），图片不能大于0.5M，宽度为240-1018像素，高度为320-1920像素。

卡片：添加人员的时候可以直接绑定卡号。

指纹：添加人员的时候可以直接绑定指纹信息。

密码：密码为使用“卡+密码”的验证方式时用于验证开门的个人密码。

胁迫密码：遭受胁迫，且验证方式为“卡+密码”时，使用胁迫密码开门会产生报警事件到中心。

2. 人员信息编辑结束后，点击【确定】保存并退出，在人员列表会显示新增人员。
3. 人员信息有变化，用户可使用【编辑】功能进行修改。直接点击【编辑】，进入编辑页面进行修改。

备注：在编辑界面修改已发卡的卡号会提示是否退掉原来的卡，一旦确定，无论是否保存修改后的卡号，原来的卡都已经被退卡，请谨慎操作。

4. 可根据人员的姓名、卡号进行模糊查询

5. 对于需要删除的人员，选中该人员（可多选），点击【删除】。已发卡的人员无法删除。

4.2.2 人员批量添加

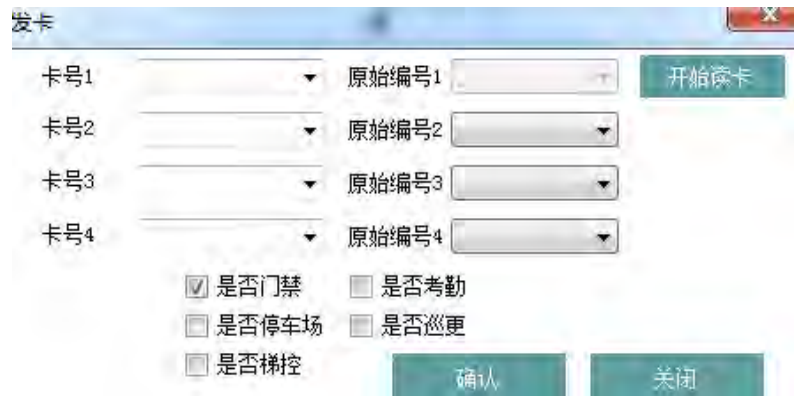
点击获取模板，按照样本的格式，输入需要导入的人员信息，再点【导入】选择导入的Excel文件即可，也可以通过【导出】选择需要的人员的信息，导出Excel文件。**Excel文件的后缀为：.xls。**

4.2.3 人员信息维护

人员信息维护包括人员发卡、退卡、挂失、解挂等操作。对于以上功能，均可直接点击人员列表下的人员，点击界面上的【发卡】、【退卡】、【挂卡】、【解挂】进行操作。

1. 人员发卡为人员分配卡号

选中需要发卡的人员，点发卡，经弹出的窗口点一下“开始读卡”，再在发卡器上刷一下卡片（，然后勾选此卡应用的范围（门禁、考勤、巡更等）；也可以在卡号上手动输入或下拉选择卡号（下拉选择前提是已添加有卡片，具体请参阅[4.3 卡片增加](#)）。每个人最多可以有四个卡号，需在数字字典启用，所有卡号可以发到任一卡类型（卡号1-4）。



2. 人员退卡

选中需要退卡的人员，点退卡即可，退卡的卡片不具有权限。

3. 人员卡片挂失

选中需要挂失卡片的人员，点挂失，此卡片就不能使用，直至解挂。

4. 人员卡片解挂

选中已挂失卡片的人员，点解挂，此卡片就可以重新使用。

4.2.4 添加人员指纹信息

此功能是方便在中心添加/编辑人员时，可以同时录入该人员指纹信息，无需再到前端指纹仪出录指纹。录入指纹信息之后，可通过指纹管理工具把指纹信息下载到指纹仪中。此功能需配套指纹采集仪使用。



用户类型：即指纹仪中的用户类型。分为普通用户，普通管理员，超级管理员，默认普通用户。

操作步骤：

步骤 1：把 USB 指纹采集仪连接电脑

步骤 2：添加人员并录入指纹信息。

选择【人事界面】，点击【添加】，在人员编辑界面输入人员信息，点击双手图中的指尖，左下角提示“请把手指平放在传感器上”时，把手指放在指纹录入仪的传感器上连续录入两次，手指无需离开传感器，指尖变成绿点即表示录入成功。点击保存后，自动给该人员发指纹仪卡号中选择的卡号。



步骤3: 使用指纹管理工具把人员指纹导入到指纹仪, 具体使用方法请参照 [4.3.4 指纹仪管理](#)。

4.3 卡片增加

4.3.1 卡片的操作

点击【门禁】→【卡片管理】→【添加】，手动输入11位数字的卡号（不足11位会在前面补0）；对于在[3.7.1 卡片类型](#)里添加了多个类型的，卡类型可不选择，发卡时不区分卡类型。

删除：选中需要删除的卡号（可多选），点删除即可，已发卡的卡号无法删除。



卡片管理界面

4.3.2 发卡器批量添加卡片

(1) 发卡器使用说明

发卡器通过USB 接口与PC 相连。

(2) 批量发卡操作步骤 点击【平台管理】→【卡片管理】→【批量添加】，显示批量发卡编辑界面，点【开始读卡】，刷卡片就可以依次的添加卡片，添加完成后点【停止读卡】，然后确认即可，如下图所示

4.3.3 读头加卡

在读头加卡界面上，选择相应的设备和读头，启动读卡，然后在选择的读头上刷卡，每 6s 会上传刷过的卡片信息，然后点确定即可。



发卡器批量发卡界面



读头加卡界面

4.3.4 指纹仪管理

点【指纹仪管理】，显示指纹仪的管理界面，此管理工具只适用于本公司的FP1-S、FP1-SIC和FP3系列的指纹仪，其它的都不适用；【EP100】为EP100系列半导体指纹控制器专用的管理工具。

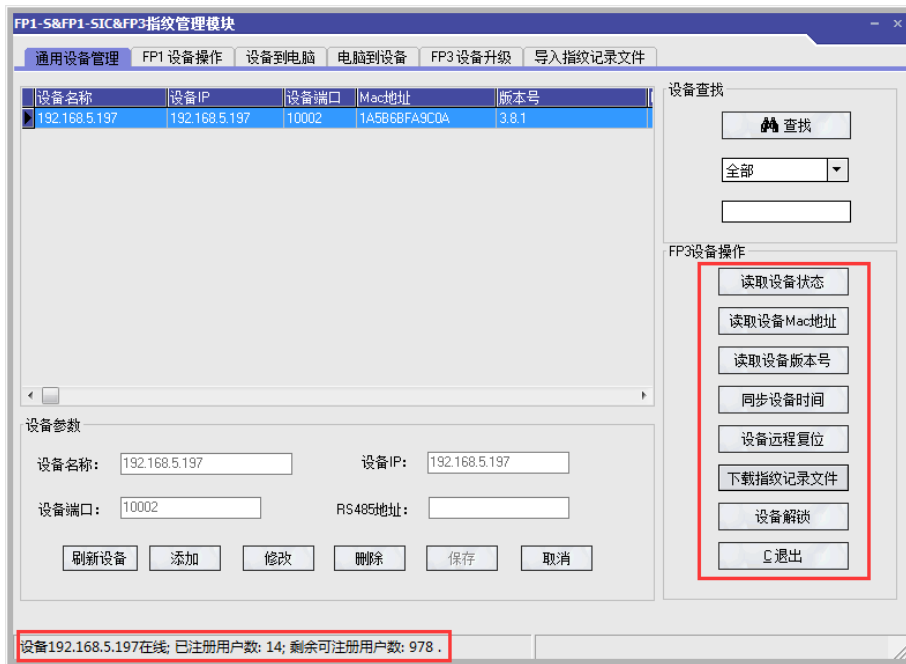
备注：两种管理工具的操作方法类似，下面以其中一种来展示，不再赘述。


操作步骤：

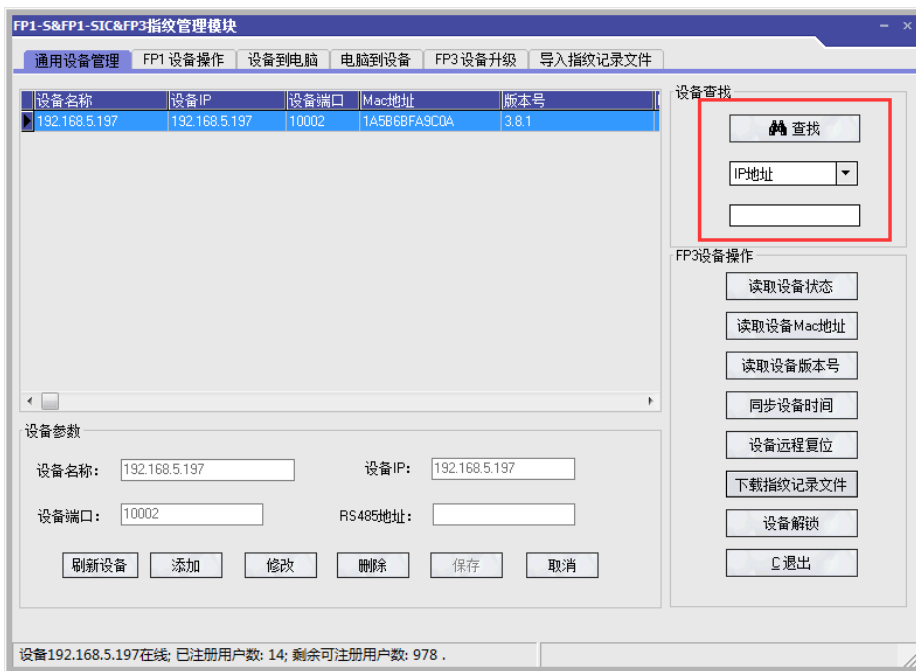
1) 添加设备，单击“添加”按钮，输入“设备名称、设备IP、设备端口”，最后保存，添加设备完毕，勾选上“上用户图片到指纹仪”，则在上传指纹数据的同时也上传对应人员照片。



2) 单击“读取设备状态”，指纹管理仪管理模块右下角会显示在线提示，如下图所示：表示门禁示控制器和指纹仪已连接成功。



3) 点击“读取 Mac 地址”将读取到设备的 Mac 地址；点击“同步时间”将设备时间与电脑时间同步；点击“设备远程复位”将远程重启设备；点击“读取版本号”将读取当前设备的版本；在上传/下载数据的过程中，指纹仪管理软件异常退出设备无法解锁时点击“解锁”按钮进行解锁；点击下拉框可以选择“设备名称、IP 地址”，在输入框中输入相应的内容点击“”即可查询，如下图：



4) 在“设备到电脑”界面可以将指纹仪中的指纹用户可以导入电脑中；在“电脑到设备”界面可以将电脑中保存的指纹仪用户可以导入到指纹仪中；同时也可以删除电脑或者指纹仪中的用户；在数据上传或者下载的过程中，可以停止数据的上传下载，由于显示/删除数据库中的用户速度较快，“停止”按钮不起作用。

由于上传用户到设备、下载用户到数据库、删除设备中用户的操作步骤基本相同，下面就以下载用户到数据库为例：（上传用户到设备就不再赘述）

- ① 在设备下拉框中选择相应的设备名称，点击“下载设备中的用户”，将所有数据下载到左边信息框（如下左图），也可以在编号框中输入单个编号，进行单个下载（如下右图），下载过程中可以按“停止”键停止下载。




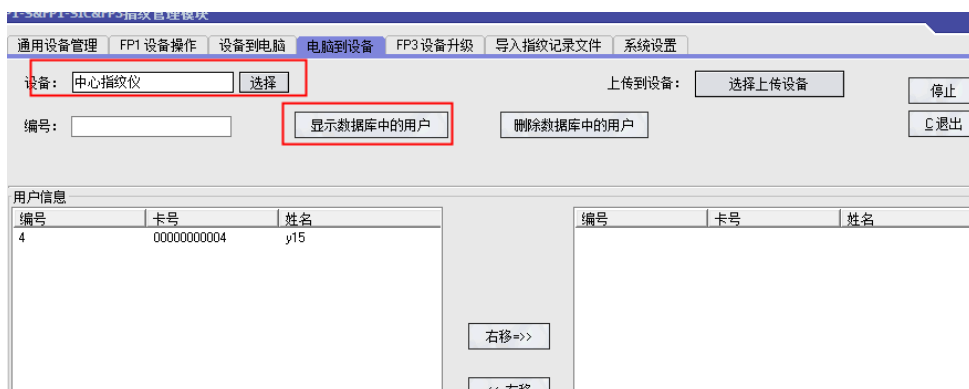
②下载结束后，可以选中单个/部分人员，点击“右移=>”移到右边用户信息框中，点击“删除设备中的用户”则可以删除右边信息框中的设备用户；点击“下载用户到数据库”则将右边信息框中的用户信息下载到数据库中。

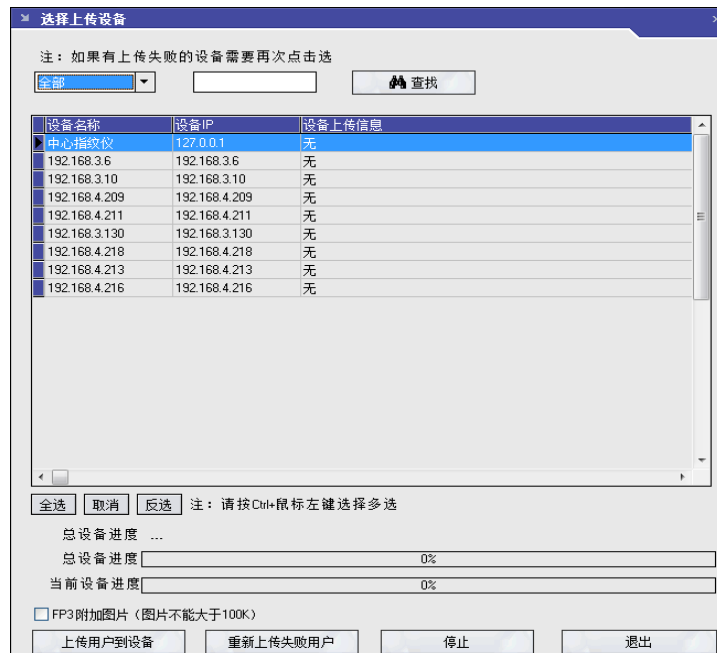


当有用户信息下载失败时，点击“重新下载失败用户”即可重新下载失败的用户；选中单个/部分用户信息，点击鼠标右键，可将所选的用户在信息框中删除，或者全部清空信息框中的用户信息。（此处的删除只是删除信息框中的用户，并非删除设备中的用户）

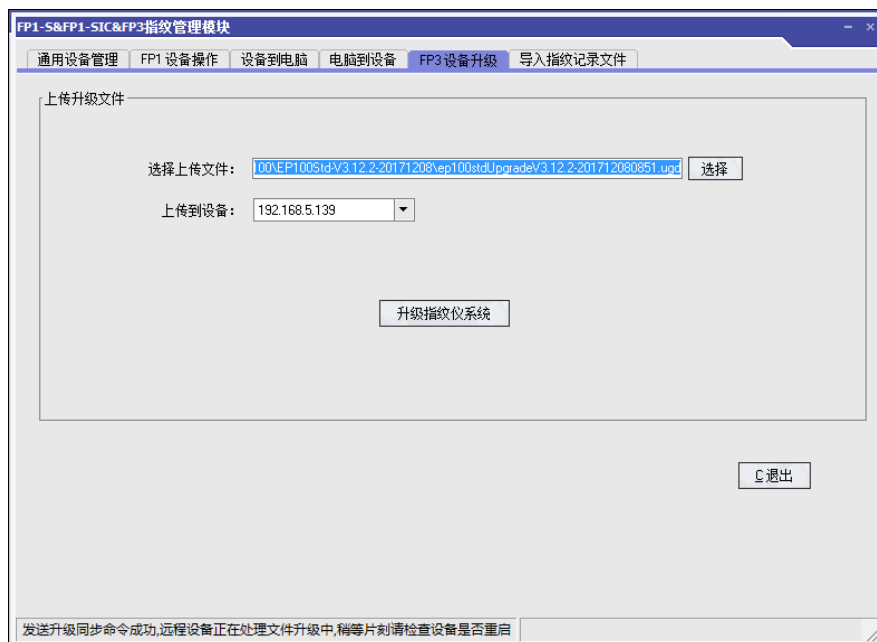
上传到设备时可以批量选择设备进行上传，选择需要上传的设备，然后等待上传完毕即可。上传失败的用户可以再次选择设备然后点击重新上传即可。

 备注：中心指纹仪为虚拟的指纹仪，使用指纹采集仪在中心录入指纹时，所有的指纹数据保存在该中心指纹仪中，用户只需把该中心指纹仪的数据传到需要上传的设备即可。





③进入“指纹仪系统升级”界面，点击“选择”按钮，选择对应的升级文件，单击“升级指纹仪系统”则可给相应的指纹仪进行系统升级，升级完成后指纹仪会重启，如下图所示：



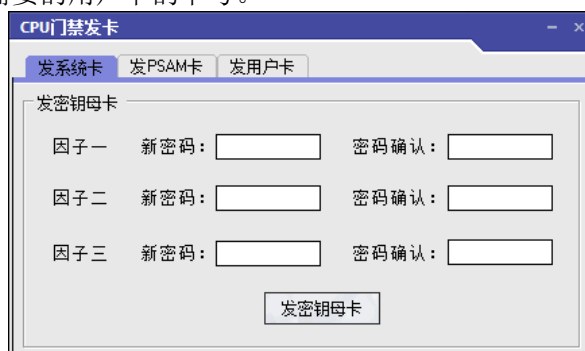
4.3.5 CPU 卡管理

点界面上的【CPU卡管理】，在弹出来的窗口中进行CPU卡片的操作。

发系统卡：即发母卡的操作，母卡设置3个密钥因子，密码为8位，点发密钥母卡即可。

发PSAM卡：直接点发PSAM卡即可，此卡放在CPU读卡器上配合使用。

发用户卡：根据需要发所需要的用户卡的卡号。

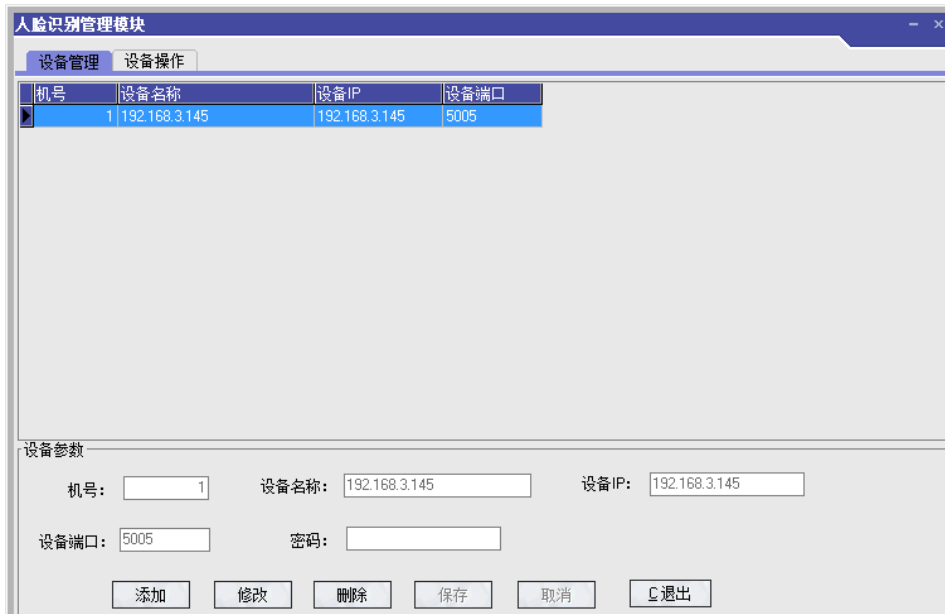


4.3.6 人脸识别管理

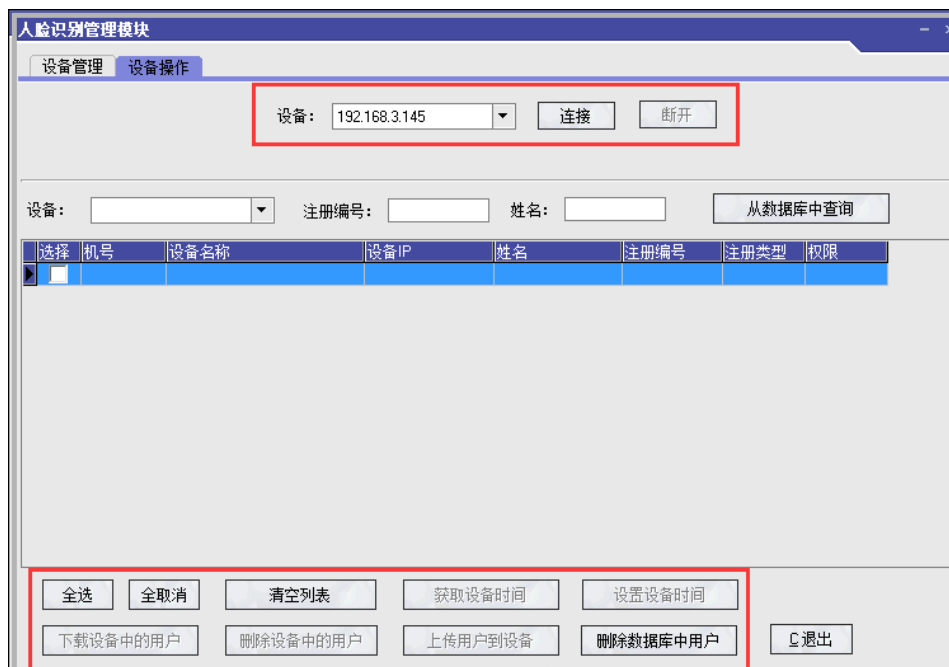
人脸识别工具可对人脸识别仪进行管理，对数据进行导入导出以及删除等操作。

操作步骤：

1) 添加设备，点击界面上的【人脸识别】，弹出人脸识别的管理工具，在设备管理页面点击【添加】，一般输入设备的机号、设备名称及设备 IP 即可，设备端口一般默认为 5005，密码默认为空。如改改了端口号或设置了密码，添加设备也需做相应的修改。



2) 管理设备，选择一台设备进行连接，连接成功之后，就可以对设备中的用户进行下载、删除等操作，也可以把下载到数据库的用户上传到另外一台设备。还可以对设备的时间进行同步。



第5章 设备管理

本系统需要连接门禁控制器,才能实现门禁系统功能。为实现通过系统管理设备,须先安装设备并将设备连至网络,其次设置系统参数。通过系统管理设备,输出各类报表,实现企业的数字化管理。


5.1 设备区域设置

区域是一个空间概念,方便用户对特定区域内的设备进行管理。设置区域后,实时监控时可以根据区域对设备(门)进行过滤。


区域设置操作包括新增区域、编辑区域、删除区域、导出区域操作。

1. 新增区域, 点击【门禁】→【设备区域管理】→【添加】, 显示新增区域设置编辑界面如下图所示:

主要字段说明如下: 区域名称: 任意字符, 要求不能重复; 上级区域: 决定设备区域架构; 服务器本地IP: 决定此区域绑定的设备对应的服务器; 其它字段信息可不填; 设置完成后, 点击【确定】完成新增。

 备注: 服务器本地IP要和数据服务系统的设备及设备的服务IP对应。

2. 删除区域: 选中区域(可多选), 单击【删除】, 点击【确定】完成操作。


 备注: 已绑定设备的区域无法删除。

5.2 设备管理

正确设置系统和设备的通讯参数,可实现系统和设备的通讯,在系统中查看已连接设备的信息并对设备进行远程监控、上传、下载等操作。

5.2.1 设备网络参数设置

在安装有监控客户端的电脑, 打开操作系统【开始】→【一卡通管理系统】→【设备扫描】; 选中扫描上来的设备点击修改, 在设置界面修改设备的网络参数后点击设置即可。

 备注: 此工具只能是在局域网内使用, 设置网络参数后设备会重启, 使设置生效。



扫描设备：可以将在线的设备扫描上来，如上图



设备 IP 地址：填入控制器的 IP 地址

IP 获取方式：静态就是手动分配的 IP，动态就是自动分配 IP（需要有 DHCP 服务器才行）。

服务器 IP 地址：填入服务器电脑的 IP 地址，设备对应的服务器 IP 地址，最多可设两个，需设备支持。

服务器端口：数据服务系统的通讯的端口

服务器域名地址：填入服务器的域名地址

默认网关：填入与设备 IP 相应的网关。

DNS 开关：打开 DNS 开关

DNS 地址：输入 DNS 的地址

备注：服务器以 IP 的方式的话，DNS 的开关必须关闭，否则设备无法扫描，还会不断重启

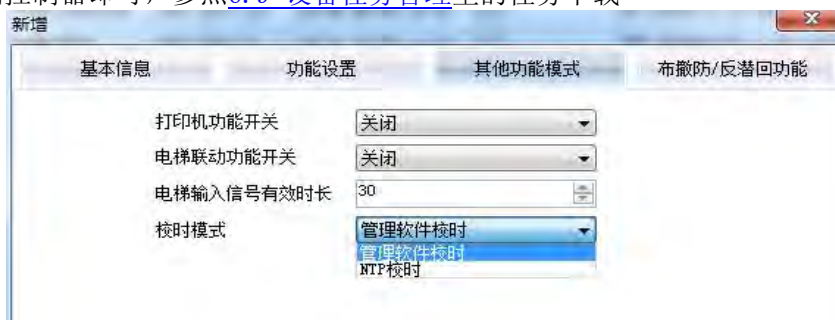
5.2.2 设备添加

新增设备可以通过点击【门禁】→【设备管理】→【添加】，在弹出的窗口中通过【选择设备】添加网络中在线的设备，然后【确定】，基本信息界面会显示设备的信息，下拉选择设备【所属部门】。

备注：基本信息只允许修改【设备名称】、选择【所属部门】及【设备描述】；**部门所属的服务器IP地址与设备的服务器IP地址要对应。**



【校时模式】：可直接选管理软件校时，也可选NTP校时并输入相关信息即可。软件校时手动与电脑软件校时，NTP校时输入网络上的服务器IP或者域名，校时间隔，确认控制器的网络能连通互联网，再下载到控制器即可，参照[6.9 设备任务管理](#)里的任务下载



【3G/4G功能】：3G/4G功能的启用与禁止，默认禁止；

【权限服务控制功能】、**【全局服务功能】**：权限服务控制功能的关闭和开启，默认关闭。开启之后，设备需要拥有权限服务控制的人员来打开或关闭服务。只开启权限服务控制功能，权限服务控制针对读头，若同时也开启全局服务功能，该功能就针对整个设备。设置拥有权限服务控制的权限组请参照[6.4.1 设备权限组管理](#)。

【RS485端口参数功能】：根据设备配置485端口，可选择FP1-S、485读卡器、二维码读卡器、透传二维码读卡器、语音模块，成功下载参数到设备后需重启设备。默认关闭。

【禁用所有按钮输入】：禁用所有开门按钮，默认否。

【禁用所有读头输入】：禁用所有读头输入，默认否。

【禁用门磁信号输入】：禁用所有门磁信号输入，默认否。

【禁用所有自定义输入】：禁用所有自定义输入，默认否。

【反潜回功能】、**【反潜回方式】**：反潜回功能开/关和反潜回方式：按单用户匹配、按多用户匹配，全局反潜回。默认关闭。具体功能使用请参照[6.7 反潜回配置](#)。

【非法卡最大次数】、**【非法卡间隔时间】**：这两个设置是配合使用，即在非法卡间隔时间内刷非法卡达到非法卡最大次数时产生非法卡超次报警。设0时为关闭。

【韦根式动态码】：针对动态码版本FP3指纹仪配合68系列门禁控制器使用时需要开启此功能。默认关闭。

【上报自定义输出端口状态】：开关自定义输出时是否在实时监控产生事件。默认关闭，暂不可用。

【短信控制开门】、**【短信有效时间】**：开启控制器的短信控制开门功能，该功能适用于在非法时段时需要开门的情况，可通过短信发送需要开门的门点到上位机，相应的门点即可在短信有效时间内可以开门。

【控制器防拆报警】：启用或禁用控制器的防拆开关。

【防拆蜂鸣功能】：触发控制器防拆时，蜂鸣器是否响。

【语音模式】：选择控制器语音输出的方式，可选择语音关闭，自带语音模块、485语音模块。选择语音关闭，控制器不会播报语音；选择自带语音模块，控制器自带语音模块播报语音；选择485语音模块，外接485语音模块播报语音。选择485语音模块需在485端口参数选择语音模块并在门参数中设置485语音模块地址。

【仅密码开门】：设置能否使用密码直接开门，设置为不允许，则直接输入开门密码不能开门。



5.2.3 设备编辑、删除及导出

选中设备点【编辑】，就可对设备进行编辑，只能编辑【设备名称】、选择【所属部门】及【设备描述】。选中设备，可直接通过左边的【部门】树或者【查询】快速查找相应设备，点击【删除】。

备注：删除设备后，对设备相关的数据都会删除。

5.2.4 复制设备参数

用来复制系统原有设备的设备参数如：门参数、开闭时间段、设备权限组、人员权限、事件联动等。如下图所示

【源设备】：选择被复制的设备

【目标设备】：需要复制参数的设备。

备注：需设备类型相匹配才可复制参数。

5.3 设备端口管理

每个设备都具有16个自定义的端口，自定义的端口可以设置端口是什么状态有效：闭合、开放。

操作步骤如下：

【门禁管理】→【设备端口管理】，选中需要修改的自定义端口，在弹出的界面中【输入端口有效状态】选择闭合有效、开放有效。闭合有效就是默认端口是闭合的；开放有效就是默认端口是断开的。

设备名称	端口编号	输入端口开关	输入端口类型	输出端口开关	输出端口类
1 设备684-1U2D192	1	打开	自定义	打开	自定义
2 设备684-1U2D192	2	打开	紧急全开	打开	自定义
3 设备684-1U2D192	3	打开	紧急全闭	打开	自定义
4 设备684-1U2D192	4	关闭	自定义	打开	自定义
5 设备684-1U2D192	5	关闭	自定义	打开	自定义
6 设备684-1U2D192	6	关闭	自定义	关闭	自定义
7 设备684-1U2D192	7	关闭	自定义	关闭	自定义
8 设备684-1U2D192	8	关闭	自定义	关闭	自定义
9 设备684-1U2D192	9	关闭	自定义	关闭	自定义
10 设备684-1U2D192	10	关闭	自定义	关闭	自定义
11 设备684-1U2D192	11	关闭	自定义	关闭	自定义
12 设备684-1U2D192	12	关闭	自定义	关闭	自定义
13 设备684-1U2D192	13	关闭	自定义	关闭	自定义
14 设备684-1U2D192	14	关闭	自定义	关闭	自定义
15 设备684-1U2D192	15	关闭	自定义	关闭	自定义

5.4 人脸管理

5.4.1 设备扫描添加

linux门禁一体机默认IP均为192.168.1.15，将电脑和门禁用网线直连，网线一头接电脑网口，一头接门禁网口；

设置同网络IP之后，电脑和门禁均配置掩码为255.255.255.0，网关192.168.1.1；

进入上位机-人脸管理-人脸管理-区域列表-扫描同网段设备IP（直连基本上只出现一个192.168.1.15的门禁设备）

当前选择的区域: 测试区

设备名称	IP地址	设备端口	读卡板版本	子网掩码	网关	应用版本	设备类型
1 3.231	192.168.3.231	80	v2.0	255.255.248.0	192.168.5.1	[FC2-D18]V6.2.11 B:202101191751	FaceL
2 3.253	192.168.3.253	80	v2.0	255.255.248.0	192.168.5.1	[FC2-D18]V6.2.11 B:202101191751	FaceL

设备名称	人脸设备IP	设备类型	添加状态	子网掩码	网关	应用版本	读卡板版本
	192.168.7.101	FaceL	未添加	255.255.248.0	192.168.5.1	[FC2-D18]V1.1.13...	v2.0
	192.168.3.247	FaceL	未添加	255.255.248.0	192.168.5.1	[FC2-D18]V6.2.3...	v2.0
	192.168.7.112	FaceL	未添加	255.255.248.0	192.168.5.1	[FC2-D18]V6.1.1...	v2.0
	192.168.5.128	AD	未添加	255.255.255.0	192.168.5.1	lize 20200725 V1.39	25
	192.168.1.128	AD	未添加	255.255.248.0	192.168.5.1	lize 20200725 VF...	25
	192.168.3.58	AD	未添加	255.255.248.0	192.168.5.1	lize 20200725 V1.33	25
	192.168.2.194	AD	未添加	255.255.248.0	192.168.5.1	lize 20200725 VF...	25
3.231	192.168.3.231	FaceL	已添加	255.255.248.0	192.168.5.1	[FC2-D18]V6.2.11...	v2.0
	192.168.3.249	FaceL	未添加	255.255.248.0	192.168.5.1	[FC2-D18]V6.2.1...	v2.0

扫描出同网段门禁设备后，添加目标设备

5.4.2 手动添加设备

输入ip以及名称，通信密码默认为12345678，设备类型选择FaceL，选择区域后保存。

打开编辑按钮，对目标主机进行编辑，修改IP以及网关，掩码，修改完成后保存。

当前选择的区域: 测试区

查询 | +扫描 | +手动添加 | +批量添加 | 编辑 | 参数设置 | 设备操作 | 删除
已注册人员 | 黑名单 | 事件记录 | 报警记录 | 操作记录

设备名称	IP地址	设备端口	读卡板版本	子网掩码	网关	应用版本	设备类型
1 3.231	192.168.3.231	80	v2.0	255.255.248.0	192.168.5.1	[FC2-D18]V6.2.12 B:202101272056	FaceL
2 3.223	192.168.3.223	80	v2.0	255.255.248.0	192.168.5.1	[FC2-D18]V6.2.1 B:202012241425	FaceL
3 3.253	192.168.3.253	80	v2.0	255.255.248.0	192.168.5.1	[FC2-D18]V6.2.11 B:202101191751	FaceL
4 3.246	192.168.3.246	80	v2.0	255.255.248.0	192.168.5.1	[FC2-D18]V6.2.7 B:202101051140	FaceL
5 3.247	192.168.3.247	80		255.255.248.0	192.168.5.1		FaceL

手动添加

名称: 1.1 IP: 192.168.1.1 一体机

端口: 80 通信密码: *****

网关: 子网掩码:

设备类型: FaceL

当前选择的区域: 测试区

区域列表: ...测试区

添加成功后，编辑门禁地址配置，配置成实际所在局域网同网段地址，网关和掩码，设备类型选择“FaceL”，选中区域列表中的区域后点击确定保存。

当前选择的区域: 测试区

查询 | +扫描 | +手动添加 | +批量添加 | 编辑 | 参数设置 | 设备操作 | 删除
已注册人员 | 黑名单 | 事件记录 | 报警记录 | 操作记录

设备名称	IP地址	设备端口	读卡板版本	子网掩码	网关	应用版本
1 3.231	192.168.3.231	80	v2.0	255.255.248.0	192.168.5.1	[FC2-D18]
2 3.253	192.168.3.253	80	v2.0	255.255.248.0	192.168.5.1	[FC2-D18]

编辑

名称: 3.231 IP: 192.168.3.231

端口: 80 通信密码: *****

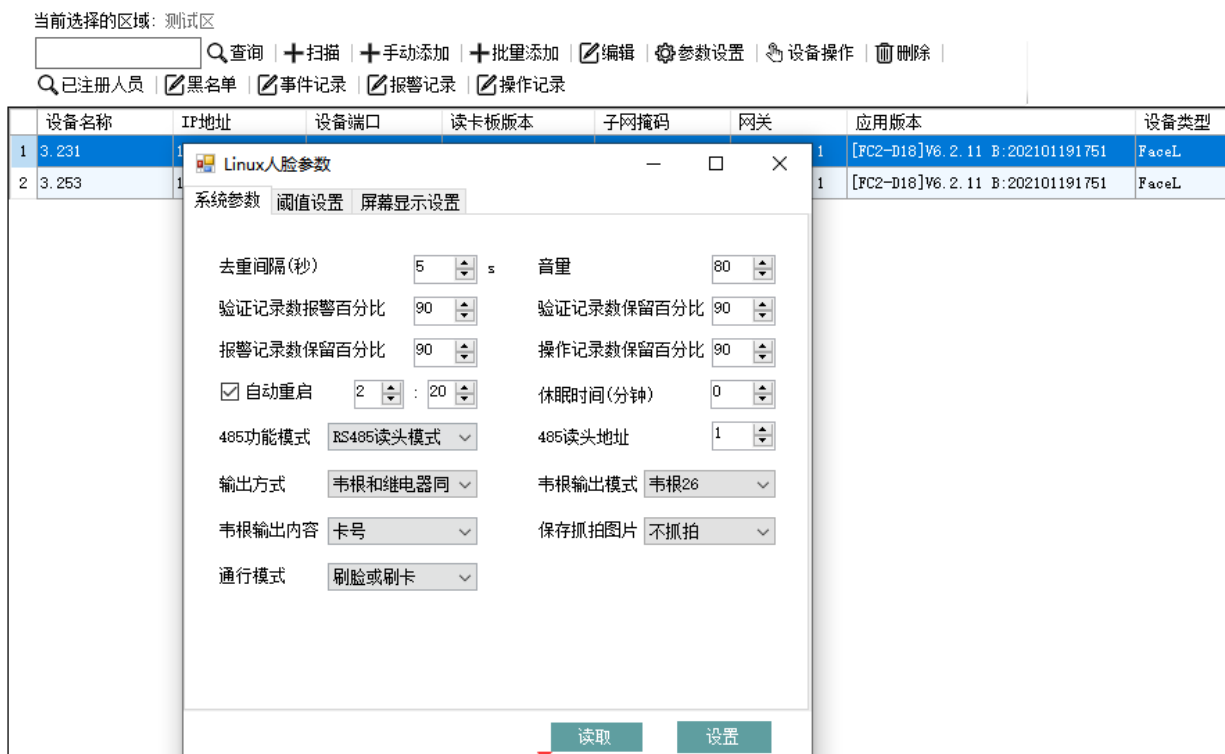
网关: 192.168.5.1 子网掩码: 255.255.248.0

设备类型: FaceL

当前选择的区域: 测试区

区域列表: ...测试区

读取门禁参数，成功读取后表示连接成功。读取成功后，方可进行参数修改，修改参数后点击设置按钮保存。



5.4.3 人脸阈值设置

当前Linux人脸机用的是阅面人脸算法, 参数设置包括距离/活体开启/阈值配置, 识别距离是人脸和门禁之间的可识别距离;活体开启设置参数为1, 则为开启状态。设置为0, 则为关闭状态; 阈值相似匹配默认为40, 提高识别精度就设置大于40的数值, 减少识别精度则设置低于40的数字。



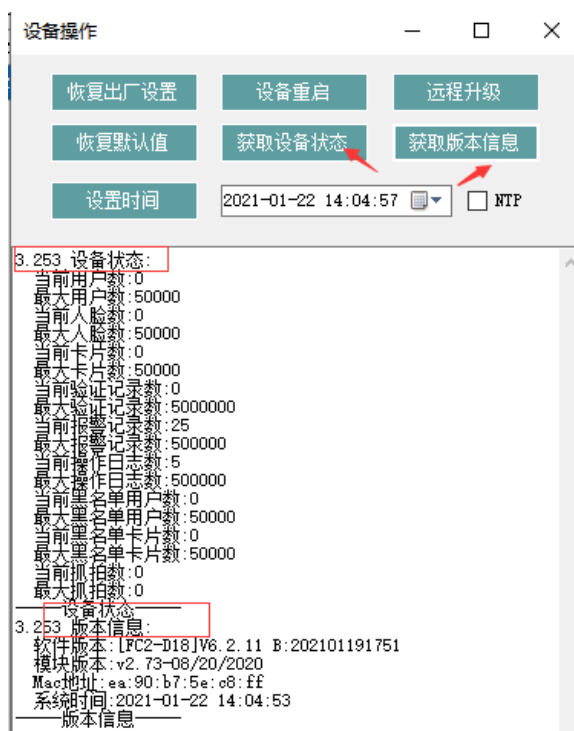
5.4.4 屏幕显示设置

设置屏幕显示信息, 包括自定义公司名称, 显示信息信息自定义, 根据需要勾选选项, 勾选后该功能开启。



5.4.5 获取设备状态

获取设备状态，包括人脸/验证记录/黑名单当前数量和总数量；版本信息查看则是显示该门禁软件信息版本号。



5.4.6 远程升级

远程升级版本，选中目标升级文件，提示升级成功后，查看版本是否升级成功。升级不会造成原配置丢失。



5.4.6 设备操作

设备重启-linix版本暂时不支持触屏和USB连线操作，只能远程控制网络重启

恢复出厂设置-删除一切配置，回到初始化状态

恢复默认配置-回到配置参数修改前状态

设置时间=获取服务器时间，和服务器时间保持同步



5.4.7 添加黑名单功能

卡片添加-输入卡号后添加添加，提示添加成功则黑名单生成，刷卡提示黑名单人员。

移除卡片黑名单-输入卡号后点击移除，提示成功则黑名单人员恢复正常

人员黑名单-选择部门，点击搜索按钮，在人员列表中选择一个人员，添加即可。人脸比对时出现黑名单提示。

同样支持直接输入人员姓名名称

人员黑名单移除-选择黑名单人员，点击移除人员黑名单，成功后再次人脸比对，黑名单提示消失

添加卡号和人员姓名任一种，都会自动生成黑名单，对刷卡和刷脸同时生效



5.5 人脸控制一体机管理

人脸控制一体机使用时，需要在设备管理处添加门禁；

5.5.1 添加设备

首先扫描出控制器IP和设备信息。



选中目标添加门禁，双击左键，进入配置页面，注意要修改服务器IP为实际的服务器IP地址，配置完成后点击配置按钮保存。

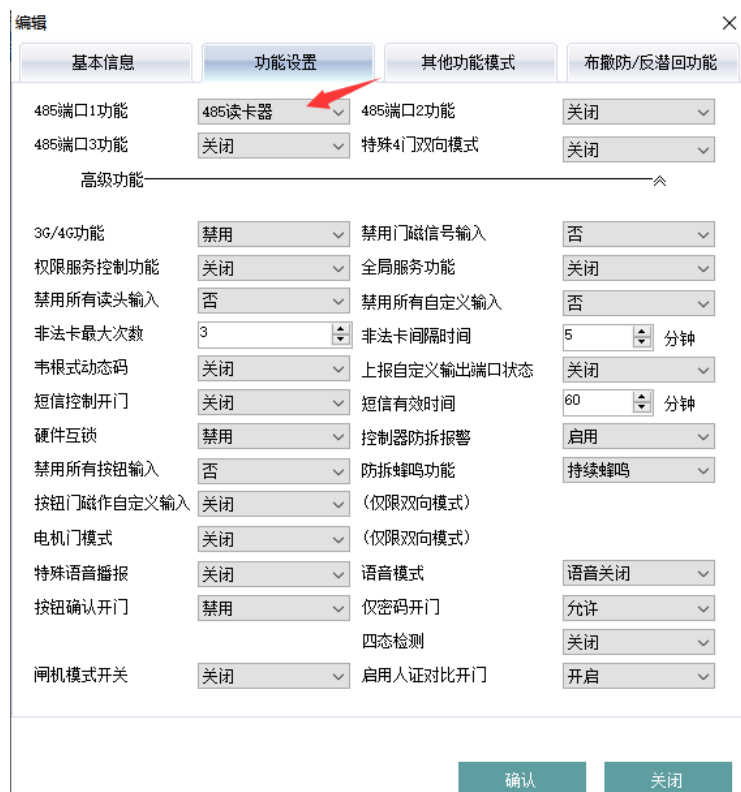


配置好开始添加设备，按照1, 2, 3步骤添加后点击确认



5.5.2 设备管理设置

在设备管理页面，点击编辑-功能设置，打开485通信端口，选择485读卡器



5.5.3 门管理设置

在门管理页面，点击编辑-门管理信息，添加门禁人脸信息和视频人脸信息，如下图



5.5.3 人脸下发

在主页面，点击人脸管理-任务管理，可进行人脸参数下发；

进入人脸管理-任务管理-选中设备列表，点击下载全部人脸，生成任务后右键查看任务详情



人脸开始下发到人脸机上，人脸机显示屏右下角count人脸数字开始增加。进行人脸和刷卡比对，能正常识别即下发人脸成功。

第 6 章 门禁管理


1. 系统工作原理

本门禁系统是基于C/S架构的管理系统，能够实现普通门禁功能，通过计算机对网络门禁控制器进行管理，实现对人员进出的统一管理。

门禁系统对已登记用户的开门权限进行设置，即在某个时间段内，在某些门上，允许某些人员可以验证开门。

2. 门禁系统操作功能介绍

门禁系统管理主要包括：门禁时间段、门禁节假日、门管理、门禁权限、实时监控等。

 备注：本章节各参数的定义可参考[名词解释](#)。

6.1 门禁时间

门禁时间包括：周编程、假日编程，用于门的时间设置，可以指定读头仅在指定门的有效时间段可用，其他时间段不可用；时间段可以用于设置门禁权限，具体请参阅[6.4.1 设备权限组管理](#)。

系统按照门禁时间的设置控制门禁。整个系统最多可以定义 255 个周编程。每个周编程可定义一周或一周内任意一天，时间区间也可以任意设置，只是同一天时间区间不能交叉，每个区间为每天 24 个小时内的有效时间段。时间段的每个时间区间格式：HH: MM~HH: MM，即按照 24 小时制精确到分钟。

系统初始默认生成一个名称为【24小时通行】的门禁时间段，可以被修改，不可被删除。用户可以新增门禁时间段，新增的门禁时间段可以被修改或删除。

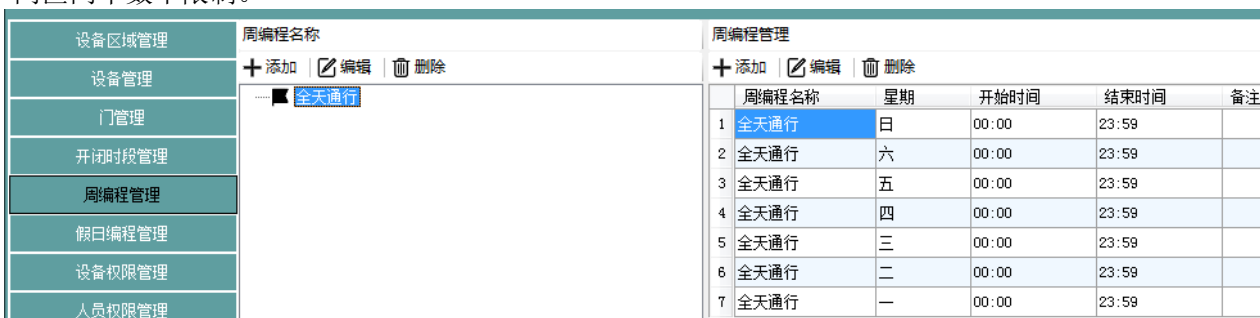
6.1.1 周编程

1. 新增周编程


点击【门禁管理】→【周编程管理】，进入周编程的设置界面。

在【周编程名称】栏里点【添加】，在弹出的窗口上输入周编程的名称即可，名称不能重复。

在【周编程管理】栏里点【添加】，在弹出的窗口，选择【周编程名称】、【星期】、相应的时间区间，时间区间个数不限制。



周编程名称	星期	开始时间	结束时间	备注
1 全天通行	日	00:00	23:59	
2 全天通行	六	00:00	23:59	
3 全天通行	五	00:00	23:59	
4 全天通行	四	00:00	23:59	
5 全天通行	三	00:00	23:59	
6 全天通行	二	00:00	23:59	
7 全天通行	一	00:00	23:59	

 备注：周编程的备注信息包含对当前时间段的解释以及主要应用场合，方便用户本人或者其他相同权限用户查看时间段信息。

2. 编辑周编程

周编程数据需要变化，用户可使用【编辑】功能进行修改，可以修改周编程的名称、周编程列表的时间区间信息。

3. 删除周编程

在【周编程】栏选中，点击【删除】，会把周编程及相关的的时间区间删除，如果只想删除时间区间的，在【周

编程管理】列表选中，点击删除。

 备注：删除使用的周编程会影响到权限组，具体请参阅[6.4.1 设备权限组管理](#)

6.1.2 假日编程

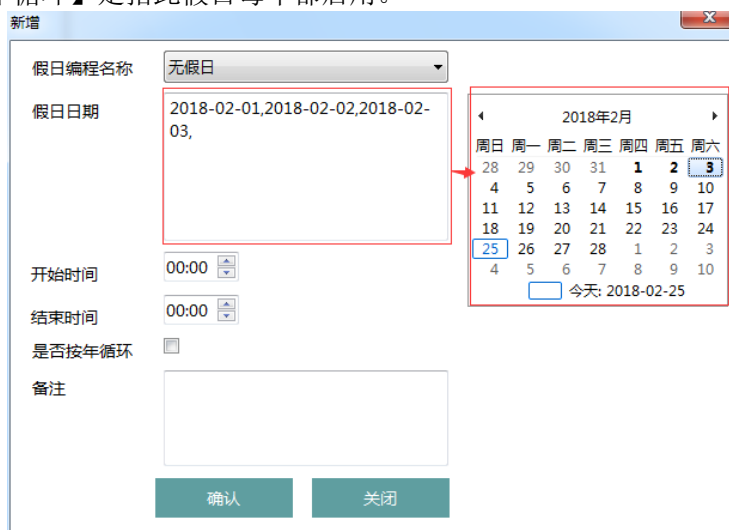
节假日的门禁时间可能与平时的门禁时间不同，为了简便操作，系统提供节假日设置，专门针对节假日设置门禁时间。


操作步骤如下：

在【假日编程名称】栏里点【添加】，在弹出的窗口上输入假日编程的名称即可，名称不能重复。

点击【门禁】→【假日编程管理】→【添加】，进入假日编程的设置界面。如下图，点击假日日期的文本框处会弹出右边的日历，在日历中选中假日日期会在文本框中，再点击相同日期会取消选中，其它操作与周编程类似。

假日编程里的【是否按年循环】是指此假日每年都启用。



 备注：在门禁系统中，节假日优先级比普通星期高。例如2015年的儿童节（6月1号）是星期四，新增节假日时，用户将国庆节设置为假日，则在2015年10月1日当天，设备按照已设定的假日时间表进行门禁时段的管理，而不是按照已设定的星期四的时段进行管理。

6.2 门开闭时段管理

门开闭时段是用来管理哪些门在指定的时间段里门常开或者常闭。

1. 新增门开闭时段

点击【门禁管理】→【门开闭时段管理】，进入周编程的设置界面。

在【开闭时段表】栏里点【添加】，在弹出的窗口，填入相关信息，【确定】即可

设备名称：选择相应的设备

门名称：选择设备相应的门

星期：1~7

开始时间、结束时间：时间部门

事件：是常开或者常闭

2. 编辑门开闭时段

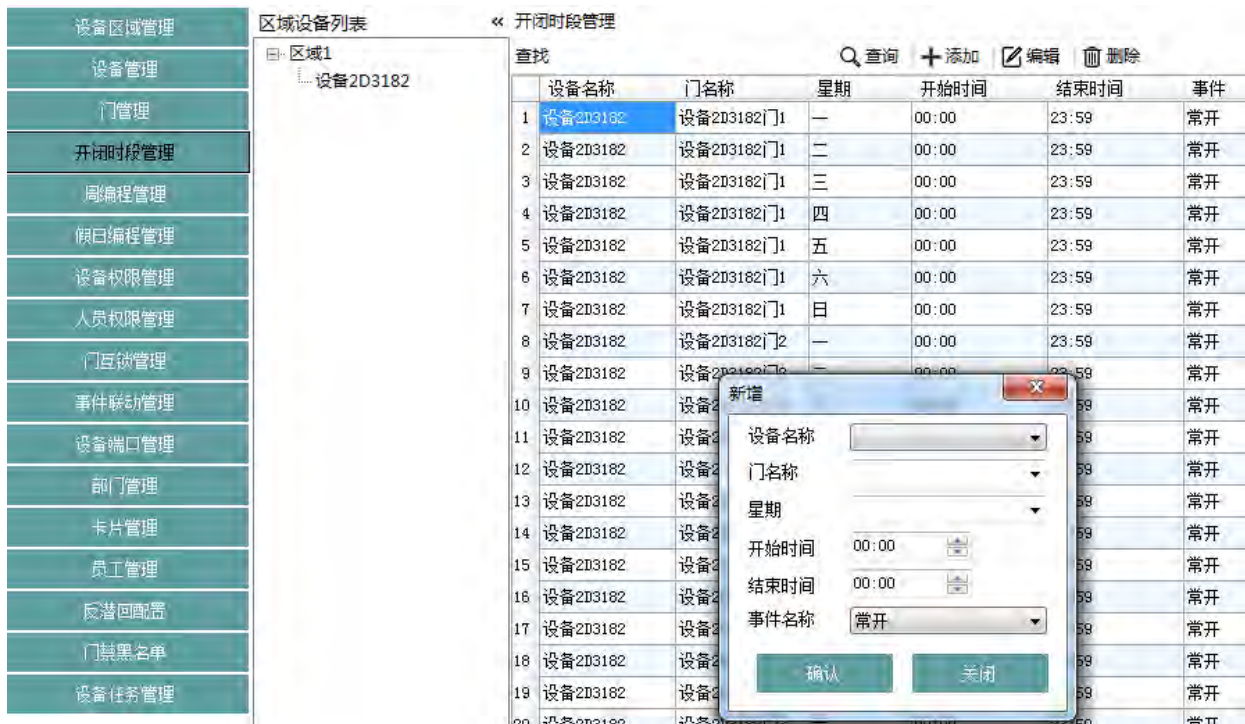
门开半数据需要变化，用户可使用【编辑】功能进行修改，可以修改【星期】、【开始时间】、【结束时间】、【事件】。

3. 删除门开闭时段

选中要删除的时段表，点击【删除】，再点击【确定】。

4. 查询周编程

可以方便快速根据【开闭时段表】的特殊字段信息找到相应的周编程。



备注：在门禁系统中，门开闭时段的优先级高于假日编程与周编程（门开闭时段>假日编程>周编程）。例如 2015 年的国庆节（10 月 1 号）是星期四，会先查找星期四当天是否有【开闭时段表】，有的话先按照【开闭时段表】执行，在【开闭时段表】时间之外的时间按【假日编程】的时段表执行，没有【假日编程】时段表的就按照【周编程】时段执行。

6.3 门设置

6.3.1 单个修改门参数操作步骤

【门禁管理】→【门管理】选择需要修改的门，单击【编辑】显示编辑界面。

备注：双向的设备门参数锁类型以奇数的设置为准，如门1，3，5，7。



1. 门名称

【门名称】默认值：“设备名称-门编号”，可任意修改。

2. 锁类型

电插锁：通电锁，断电开；磁力锁：通电锁，断电开；电控锁：通电开。

3. 开门密码与胁迫密码

每个门可以设置1~8位纯数字的开门密码和胁迫密码（4位以上的密码需要换输入密码时要按#号确认的读卡器），在读头上密码键盘输入相应的密码就可以开门，胁迫密码开门同时会有报警信息。

4. 是否考勤

选择这个设备的读头是否当做考勤的设备。

5. 锁驱动时长

控制开锁继电器的通断时间，0~65535s，默认为3s，如设置成“0”，表示关闭锁控功能。一般情况下，建议不要设置为“0”。开门之后超过此时间没有关门，则会开始报警，这段时间就是门磁延时。

☞备注：电控锁的开锁时间不受此影响

6. 485地址

设置每个读头上关联的485地址，配合485读卡器使用，关联的485读卡器就会操作相关联的门。

7. 视频模式

目前支持 onvif 协议的网络摄像机，然后在下面的【视频 IP】中输入摄像机的 IP，通道选 1 即可。视频模式选择暂不可用。若网络摄像机需要用户名和密码登录，可在【系统设置】->【视频监控设置】中填写相应的用户名和密码

☞备注：网络摄像机直接抓拍的通道只能选择1通道。

8. 开门指纹确认

此功能与系统设置的用户开门方式中验证控制器指纹的验证方式相关，具体参阅[6.11.2 设置界面](#)用户开门方式。一个门开启了这个功能后，对应的门的指纹仪将用作远程确认，不再用作开门。

9. 按钮远程请求确认

开启此功能后，相应的门使用开门按钮开门时需要中心远程确认才可以开门。如果设备为双向，设置以出的门为准。如双向有门1进、门1出，门1进关闭了此功能，而门1出开启了此功能，则门1使用开门按钮开门时需要中心远程确认。

10. 多卡刷卡间隔

可以设置多卡之间每张卡刷卡间隔的最长时间（默认60秒），超过这个时间就需重新刷卡。

11. 入库超时报警

开启此功能后，刷卡进门超过一定时间后没有刷卡出门即会产生超时报警，设备类型为双向才能正常使用该功能。如门1进设置入库超时报警为1分钟，门1出无需设置，则从门1进刷卡进门1分钟后（从门磁断开开始计时），监控会产生报警记录且弹窗，在弹窗中可选择已处理或者延时，报警期间从门1出刷卡出门或者选择已处理会立即停止报警，选择延时会暂停报警，在达到延时时间后如果还没有刷卡出门则又会产生延时报警并弹窗，同样可以选择已处理或者延时，以此类推。入库超时报警必须中心选择已处理或者刷卡出门才会停止报警。

12. 门磁闭合电平

可设置门磁闭合电平为高电平还是低电平。

13. 485语音模块地址

设置每个读头上关联的485地址，配合485语音模块使用，关联的485语音模块就会播报相关联的门语音。

14.人脸设备IP

设置每个读头上关联的人脸设备IP，配合人脸设备使用

6.3.2 批量修改门参数

在门管理列表序号处选中需要修改的门的参数，点击【批量修改】即可，修改信息与单个修改一致。

备注：批量修改时，不会显示原有的参数，因为批量修改的门参数有可能不一样。

6.3.3 非远程确认开门段

开启此功能后，需要中心远程确认的事件在此时间段无需中心确认。如勾选了通过 IP 网络远程确认权限的人员在此时段请求开门，则中心无需确认，就可以直接开门。最多可以设置四个时间段，每个时段的开始时间必须大于结束时间且不能交叉重复。

6.3.4 启用开放\管制时间段

在此界面勾选设置开放\管制时间段即可启用开放\管制时间段。此功能用于门开闭时段的启用或禁用。

6.3.5 查询

可以方便快捷根据门参数的特殊字段信息找到相应的门，快速查看、编辑门信息

6.4 门禁权限的设置

门禁权限设置包括两部分：设备权限组管理、人员权限管理。

【设备权限组管理】：是将设备与门的开门方式进行绑定，如设备1绑定了设备1门1开门方式的普通组等。

【人员权限管理】：就是将人员与设备【设备权限组管理】进行绑定，使人员具有操作哪个设备的权限。

6.4.1 设备权限组管理

1. 新增设备权限组

门名称	权限组名称	验证方式	门号	周编程名称
1 设备1U2D192门2出	单卡-设备1U2D192	普通组(不受首卡/双卡限制)	4	全天通行
2 设备1U2D192门2进	单卡-设备1U2D192	普通组(不受首卡/双卡限制)	3	全天通行
3 设备1U2D192门1出	单卡-设备1U2D192	普通组(不受首卡/双卡限制)	2	全天通行
4 设备1U2D192门1进	单卡-设备1U2D192	普通组(不受首卡/双卡限制)	1	全天通行

点击【门禁】→【设备权限管理】，进入设备权限组的设置界面。

在【权限组】栏里点【添加】，在弹出的窗口上输入设备权限组的名称即可，名称不能重复。

在【设备权限组管理】栏里点【添加】，在弹出的窗口，选择该权限能控制的门，再选择开门方式，【确定】即可。若该权限组控制的门开门方式不一样的话，先添加一种开门方式，然后再重新添加另一种。想要删除设备权限组里个别的门的控制，可以通过【查看设备验证组】里选中某个门，然后点【删除】即可。

门名称	权限组名称	验证方式	门号	周编程名称
1 设备FP3One130门1	单卡-设备FP3One130	普通组(不受首卡/双卡限制)	1	全天同行
2 设备684-1U2D192门2出	单卡-设备684-1U2D192	普通组(不受首卡/双卡限制)	4	全天同行
3 设备684-1U2D192门2进	单卡-设备684-1U2D192	普通组(不受首卡/双卡限制)	3	全天同行
4 设备684-1U2D192门1出	单卡-设备684-1U2D192	普通组(不受首卡/双卡限制)	2	全天同行
5 设备684-1U2D192门1进	单卡-设备684-1U2D192	普通组(不受首卡/双卡限制)	1	全天同行

设备较多时，可以通过上方的查询设备，查询条件为设备的名称可模糊查询。

开门方式说明如下：

【验证方式】：有普通卡（单卡）、双卡、首卡、受首卡限制、主卡、副1、副2。

【校验密码】：否的话，就是仅刷卡，是的话，就是卡加密码的方式

【门号】：选择对应的门号，如门1、门2、门3等

【周编程】、【假日编程】，选择对应周编程与假日编程

【是否通过IP网络远程确认】：不勾选的话，就是不需要中心远程确认；勾选的话就是需要中心远程确认。

此方式的话需要开实时监控

【是否开启服务控制】：勾选了此项的权限组人员具有开启服务控制的权限，仅限普通卡（单卡）勾选此功能才生效，其它验证方式勾选此项无效。

【组号】：可以为此权限组分配组号：无，1~15个；此功能只对双卡开放

【是否要求同组】：分配了组号，不勾选的话，就是需要不同组的卡片；勾选的话就是相同组号的卡片组合；这个只对同等级别的权限，如主副卡里彼此不关联

【主卡】：五星卡，组合方式的一种，选择组合的卡数量，最多支持6张，不可为0。

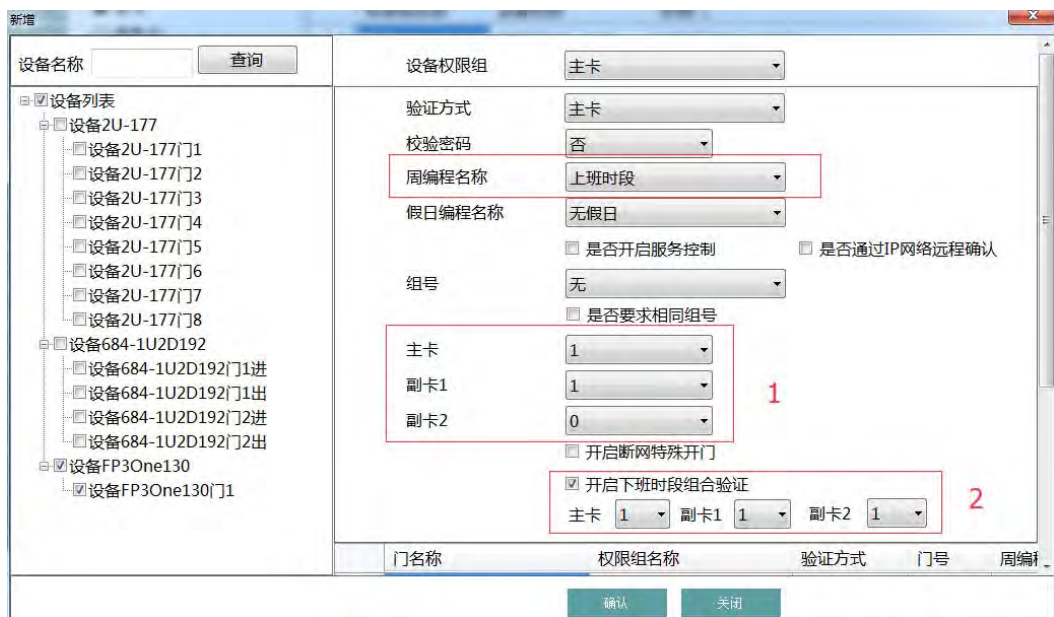
【副卡1】：四星卡，组合方式的一种，选择组合的卡数量，最多支持6张

【副卡2】：三星卡，组合方式的一种，选择组合的卡数量，最多支持6张

【开启断网特殊开门】：此功能针对断网后，勾选了IP网络远程确认功能，中心无法远程确认开门的情况，仅对主副卡开放。勾选了此功能后，副卡2仅作为具有断网特殊开门权限的卡，在网络正常的情况下此卡不启用。设备断网后才可用副卡2组合验证开门。如下图，勾选了IP网络远程确认及断网特殊开门功能的主副卡组合1-0-1，网络正常的情况下，只需刷主卡，中心收到请求远程确认开门后进行确认即可开门；在断网情况下，则无需中心确认，直接用主卡+副卡2即可开门。



【开启下班时段组合验证】：上、下班时段使用不同的组合方式进行验证才可开门，仅对主副卡开放。如下图，选择一个周编程，周编程时间范围之外都属于下班时段。勾选下班组合验证后可选择主副卡组合，如主副卡组合1-1-0，下班时段组合1-1-1，上班时段按下图方框1组合验证即可开门，若在下班时段，则需按方框2组合验证才可以开门。



备注：主卡、副卡1、副卡2一般是组合使用的，三种组合方式建议设置一样

2. 删除设备权限组

在【设备权限组】栏选中，点击【删除】，会把设备权限组列表内容删除及人员权限列表（具体请参阅 [6.4.2 人员权限管理](#)）。

6.4.2 人员权限管理

1. 新增设备权限组

点击【门禁】→【人员权限管理】→【组权限分配】，进入人员权限的设置界面。



在【待选择人员列表】中会列出所有未分配权限即未与设备权限组绑定的人员，在复选框中勾选需要分配的人员移到右边的待保存人员列表中，再选择需要绑定的【设备权限组】即可，如下图所示：

也可以通过上面的查询条件，选择满足条件的人员进行分配

【用户密码】：即卡加密码方式开门时，用户的密码（4位纯数字），不设置的话默认为1111。

【有效期】：是指此人员具有权限的时限，超过时限就无法操作。

【使用次数】：是指此人员卡片能刷卡开门的次数，超过次数就无法刷卡开门，最大100次。

【开门时长】：是个人的开门时间。

 备注：已分配过的无法再次分配

2. 编辑人员权限

人员权限数据需要变化，用户可使用【编辑】功能进行修改，可以修改【设备权限组】、【用户密码】、【有效期】、【使用次数】，只能单个编辑，保存编辑后会立即下载人员权限

3. 删除人员权限

任意的选中人员，会在人员权限前面的复选框勾选，然后点【删除】即可，也可以全选，在人员姓名前的复选框上勾选就全选，然后点【删除】即可，删除人员会自动下载人员权限


6.5 互锁设置

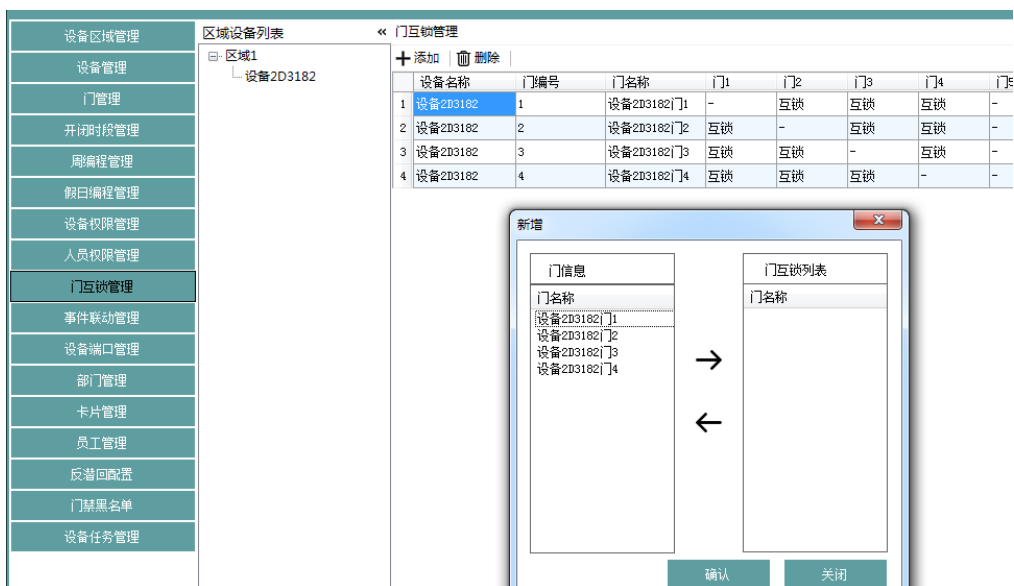
可设置一个控制器上的两扇（多扇）门之间的互锁管制，当其中一扇门开启时，其他对应的门都关闭，当要开启一扇门时，其他对应的门必须都是关闭的，否则无法开门。

设置互锁前，请确保门磁已经连接正确。

新增互锁设置操作步骤：

1. 点击【门禁管理】→【门互锁管理】，进入互锁设置编辑界面；
2. 选择设备，在【部门设备列表】中选择相应的设备，点【添加】，在弹出的窗口中选择相应的门号移到门共享器列表中，点【确定】。看互锁设置的事件以门编号来看，如图中，以门1那一列来看，门2, 3上有互锁，即门1, 2, 3三个门互锁，也可以以横排来看。

 备注：一个门不能在多个互锁事件中，如门1与门2互锁为一个事件，再想设置门1与门4互锁的事件是无法实现的；双向的设备两个读卡器控制一个门，设置时要把两个读头都添加，如：双门双向设备要设置门1, 2互锁，添加互锁条件时：门1、门2、门3、门4都添加进去。



删除互锁事件：

选中相应的设备，然后删除，会删除完此设备的互锁事件，然后再重新设置。

 备注：单门没有互锁，互锁只对两门及以上的才可；双向的程序里门名称对应的是读头。

6.6 联动设置

联动设置，指门禁系统中的某个输入点触发某条特定事件后，在指定的输出点产生一个联动动作，用以控制系统中的验证、开门、报警、异常等事件，并在在实时监控列表中显示。

新增联动设置：

1. 点击【门禁管理】→【事件联动设置】→【新增】，显示联动设置界面：



各字段说明如下：

触发条件：只要是实时监控有记录的都是触发条件。

设备名称：选择需要设置的设备。

门名称：选择需要设置的门。

输入事件：触发的事件条件。

输入点地址：任意的读头、自定义输入、门磁、按钮等（设备的具体输入点请参考设备参数）；选择【自定义输入】的话触发条件为短接相应的自定义输入端。

输出点地址：门锁1~8、自定义输出1~16。

输出事件：继电器关闭、打开，如果打开，则需要设置延时时间。 延时：范围：1s~65535s（此项在动作类型为打开时有效）。

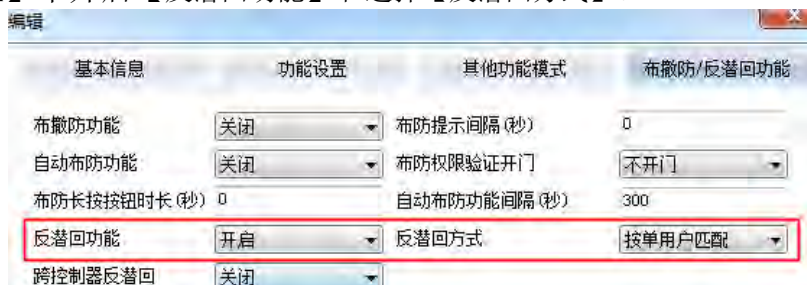
2. 编辑完成后，点击【确定】保存并退出，在联动设置列表显示新增联动设置。 例如：触发条件选择“正常刷卡开门”，输入点：门1，输出点：门锁1，动作类型：打开，延时范围：60s，那么在门1有人“正常刷卡开门”后，在门锁1，则联动产生“打开”的动作，门打开维持时间60s。

备注：1) 编辑时不可以修改设备，只可以修改联动设置名称和配置项，当删除某台设备时，同时删除设备中的联动设置记录。

2) 系统不允许某台设备在在特定触发条件下，存在相同的输入点和输出点。

6.7 反潜回配置

1、在【设备管理】中开启【反潜回功能】和选择【反潜回方式】。



2、在反潜回配置界面选择一台设备后点击新增就可以配置设备的各个门点作为反潜回进或反潜回出。当有人人员潜回时就会触发反潜回报警，产生相应的报警记录。



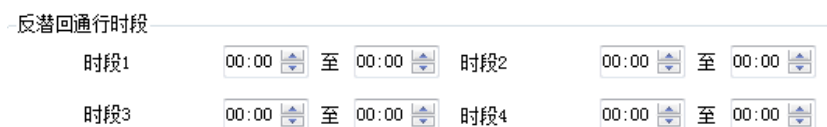
反潜回方式具体逻辑如下图所示：第 1 组反潜回门 1 为进、门 2 为出；第 2 组反潜回门 3 为进、门 4 为出。

(1) **单用户匹配**：考虑用户与反潜回组号，张三可在门 1、3 进，但是从门 1 进后需要从门 2 出才能重新在门 1 进，同理从门 3 进后需要从门 4 出才能重新在门 3 进。

(2) **多用户匹配**：只能在特定场合使用，标准版暂不用该功能。

(3) **全局反潜回**：只考虑用户，不考虑组号，张三只能从门 1 进或者门 3 进，只能从门 2 出或者门 4 出。

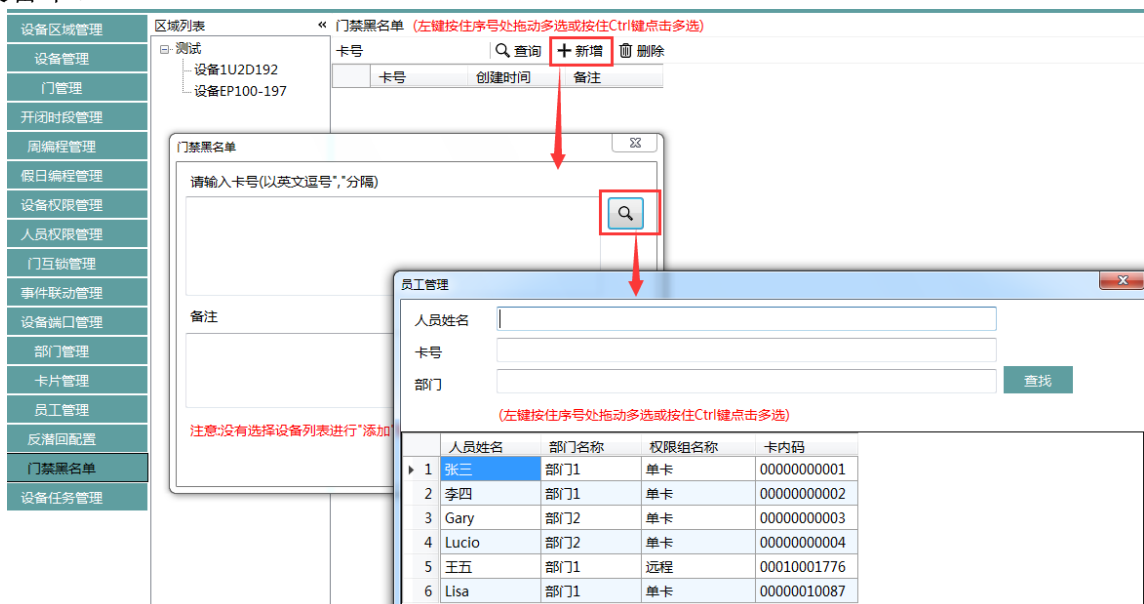
3、在【门管理】中还可以根据门点设置【反潜回处理措施】，默认禁止通行，可选择允许通行或者特定时段通行。特定时段通行需同样在门管理中设置【反潜回时段】，在该时段内允许通行。



6.8 门禁黑名单

门禁黑名单可以把卡号添加进黑名单，在黑名单中的卡号将失去所有权限，无法开门等，直至从黑名单中删除。黑名单中的卡号刷卡会产生黑名单报警上传到上位机。

点【门禁】→【门禁黑名单】，在黑名单界面的区域列表选择一个设备点击新增，可以在文本框内输入卡号，每输入一个卡号以英文逗号','结束。或者点击文本框旁的查询按钮直接查询卡号，选择卡号按确认添加到文本框中。卡号输入完毕后按确定即可把卡号加入黑名单。新增或删除黑名单会自动下载到设备中。



备注：不选择任何设备则默认所有设备，即该卡号会被添加进所有设备的黑名单。

6.9 设备任务管理

系统可以设置各种任务，然后下发到设备中，是与设备进行数据传输的方式。

点【门禁】→【设备任务管理】在弹出的设置页面：

设备名称	任务名称	设置时间	任务状态	执行时间	
设备2D3182	设置门参数.非远程确认开门。	2018-08-21 16:23:25	执行成功	2018-08-21 16:23:49	
设备2D3182	设置门互锁	2018-08-21 16:23:25	执行成功	2018-08-21 16:23:49	
设备2D3182	设置事件联动	2018-08-21 16:23:25	执行成功	2018-08-21 16:23:49	
设备2D3182	设置假日编程	2018-08-21 16:23:25	执行成功	2018-08-21 16:23:49	
设备2D3182	设置周编程	2018-08-21 16:23:25	执行成功	2018-08-21 16:23:49	
设备2D3182	设置权限组-权限组子表1-个人	2018-08-21 16:23:25	执行成功	2018-08-21 16:23:49	
设备2D3182	设置权限组-权限组子表1	2018-08-21 16:23:25	执行成功	2018-08-21 16:23:49	
设备2D3182	设置权限组-权限组子表1	2018-08-21 16:23:25	执行成功	2018-08-21 16:23:49	
设备2D3182	设置权限组	2018-08-21 16:23:25	执行成功	2018-08-21 16:23:49	
设备2D3182	设置权限组	2018-08-21 16:23:24	执行成功	2018-08-21 16:23:49	
设备2D3182	设置门开闭时段	2018-08-21 16:23:24	执行成功	2018-08-21 16:23:49	
设备2D3182	设置自定义输入有效状态	2018-08-21 16:23:24	执行成功	2018-08-21 16:23:49	
设备2D3182	设置门参数	2018-08-21 16:23:24	执行成功	2018-08-21 16:23:49	
设备2D3182	设置校时模式&&3G功能开关	2018-08-21 16:23:24	执行成功	2018-08-21 16:23:49	
设备2D3182	设置人员权限	2018-08-15 14:29:51	执行成功	2018-08-15 14:29:53	
设备2D3182	设置人员权限	2018-08-15 14:29:51	执行成功	2018-08-15 14:29:53	
17 区域1	设备2D3182	设置门参数.非远程确认开门。	2018-08-15 14:29:38	执行成功	2018-08-15 14:29:41
18 区域1	设备2D3182	设置门互锁	2018-08-15 14:29:38	执行成功	2018-08-15 14:29:41
19 区域1	设备2D3182	设置事件联动	2018-08-15 14:29:38	执行成功	2018-08-15 14:29:41

在【部门设备列表】勾选需要设置的设备，然后点鼠标右键已勾选的设备

读取时间：读取设备的时间

设置时间：同步设备与电脑的时间

读取设备端口状态：读取按钮、门磁、自定义端口的状态。

读取用户权限内容：读取用户的所有权限内容，包括用户的基本信息、所在权限组、以及权限组的详细权限等。

设备重启：远程让设备重启。

复位外围电源：将端口的电源全部切断

设备初始化：将设备的数据全部清空（设备参数、人员权限、记录），请慎重操作。

远程开/关门：选择相应的门，远程控制其开、关。

强制常开/闭门：选择相应的门，远程控制其常开、常闭。

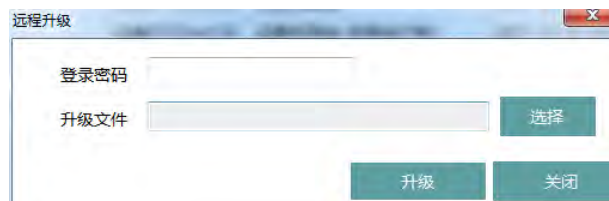
设置全部参数：将设置的门参数、权限组、假日编程、周编程、开闭时段、设置校时模式&&3G 功能开关、时间联动、门互锁、自定义输入有效状态等下发到设备中。

设置部分人员权限：将部分人员的人员权限参数下发到设备中，在窗口中，待下载人员列表会默认是显示所有的未下发过的人员，也可通过【查询】查找人员的（可选未下发过或者已下发过的）。

设置全部人员权限：将全部的人员权限列表的人员权限参数下发到设备中。

采集脱机记录：将设备脱机状态下产生的记录采集上来，此操作要设备联网在线的情况下。

远程升级：可以给设备进行程序的升级，步骤：打开远程升级窗口，然后输入操作员的登录密码，再选择升级文件的路径，点升级，等升级完成设备重启后即可。



6.10 设备的初始化与恢复出厂设置

设备初始化是在客户端上【设备任务管理】里，初始化是会把设备的所有数据（设备参数、人员权限、记录）全部清除。

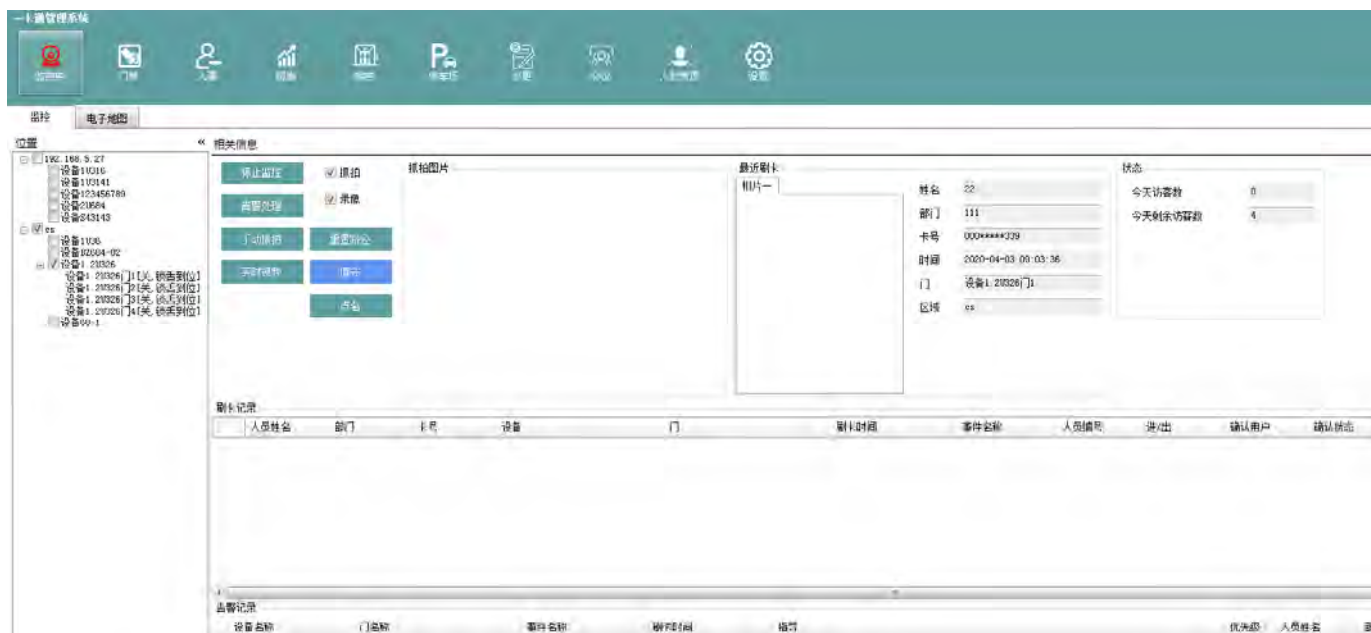
设备的恢复出厂设置要通过把拨码开关（靠近 TF 卡槽）全部拨到上面，然后再按住显示面板上的按钮 5s 以上，松手待设备重启后即可，恢复出厂后会把所有的数据恢复到出厂时的状态，包括网络参数、所有的数据等。

6.11 实时监控

实时监控系统内所有门的状态和实时事件，包括正常事件和异常事件（含报警事件）等。

6.11.1 打开的监控界

在【设备列表】中勾选需要监控的设备，可右键全选，再点【实时监控】即可，可以在监控设备列表看到设备门的状态。在【系统设置】中勾选【监舍锁舌状态】后可以监视到锁舌状态。



【人员照片显示】：如果实时监控时接收到人员验证的事件，并且人员设置了照片，则显示人员的照片。

【事件监控】：系统自动获取监控到的设备事件记录，包括正常事件和报警事件，报警事件显示红色。

最近的监控事件显示在最前面。

【告警处理】：点击告警处理可以对报警记录进行处理，一些设置了报警声音的事件需要处理后才能关闭声音。可选中一条点击处理进行单条处理，也可以全部一起处理。



【抓拍、录像】：如果连接了摄像机且勾选了抓拍和录像，任意事件上传到监控都会进行抓拍和录像，抓拍和录像的文件会保存在自动创建的 X_Capture 和 X_Video（X 为文件夹所在的盘名称，如在 C 盘创建的文件名称即为 C_Capture）共享文件夹，Capture 和 Video 文件夹优先创建在用户在【文件保存设置】里勾选的最后一个盘的根目录，一个盘满之后才会更换到另一个盘，如勾选了 C、D、E、F 盘，此时文件夹会优先创建在 F 盘，F 盘满后再到 E 盘，以此类推。

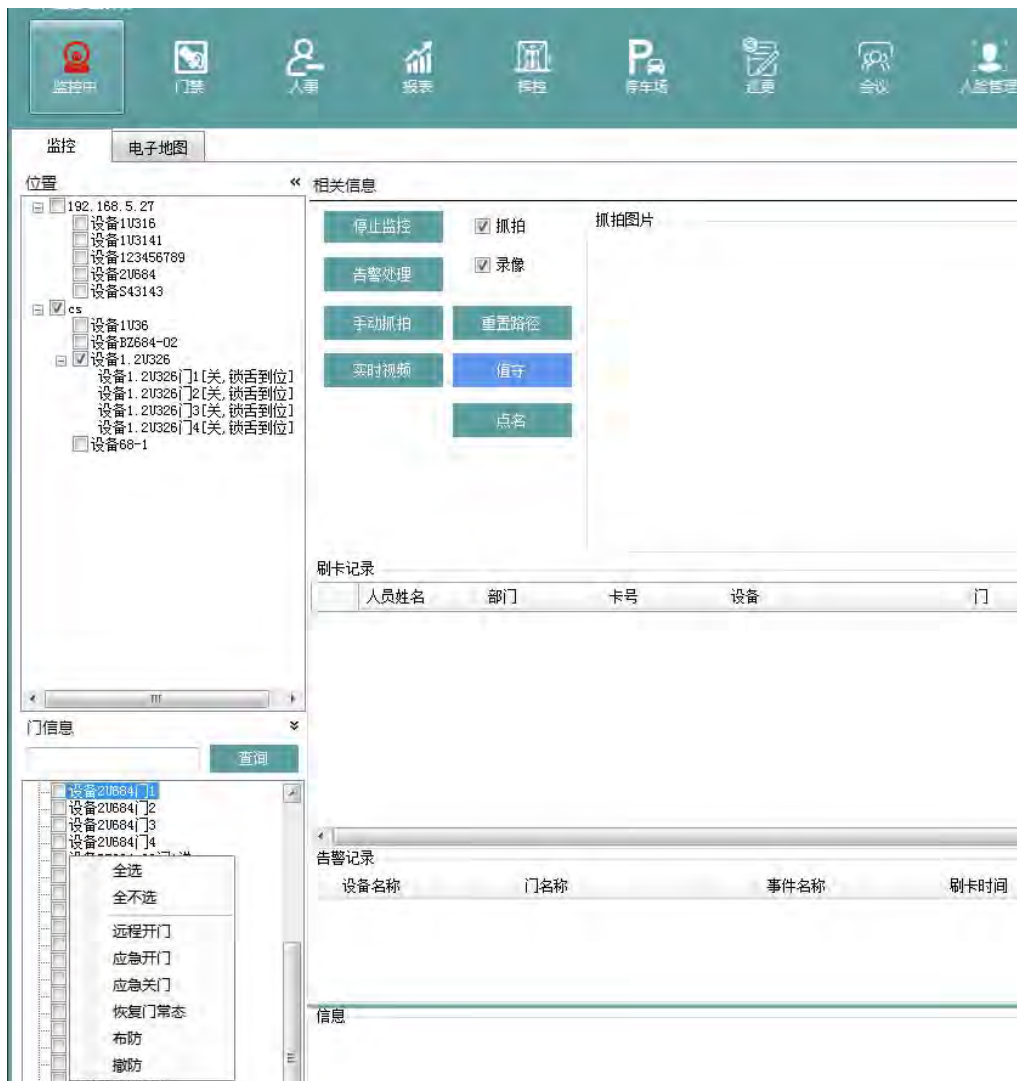
【实时视频】在【门信息】勾选一个门，然后点击【实时视频】就会弹出一个播放实时视频的窗口，仅支持


勾选一个门，不能多选。使用前确保该门连接有摄像机，即在【门管理】处对应的门设置了视频 IP。

【远程开门】：打开【监控】界面，点击门信息的展开按钮，在【门信息】里勾选需要远程开门的门，然后右键点【远程开门】就行，也在点【全选】按钮选择全部的门。

【应急开门】：打开【监控】界面，点击门信息的展开按钮，在【门信息】里勾选需要应急开门的门，然后右键点【应急开门】就行，也在点【全选】按钮选择全部的门。

【恢复状态】：打开【监控】界面，点击门信息的展开按钮，在【门信息】里勾选需要恢复门状态的门，然后右键点【恢复门状态】就行，也在点【全选】按钮选择全部的门。



 备注：如果远程开门一直失败，请检查设备列表是否有太多当前不在线的设备，如果是，请检查网络，否则操作失败。

6.11.2 设置界面

1. 【设置】→【系统设置】→【基本设置】：可以设置监控界面要显示的界面及功能，如下图所示：



初始预设抓图：勾选就是默认会抓拍。

初始预设录像：勾选就是默认会录像。

退出系统：勾选了就是退出监控边客户端时要验证操作员的密码

本机IP：针对电脑有多个网卡的，要输入对应的IP。

动态码功能：启用动态码功能，设置短信参数，使监控可以发送短信验证码。

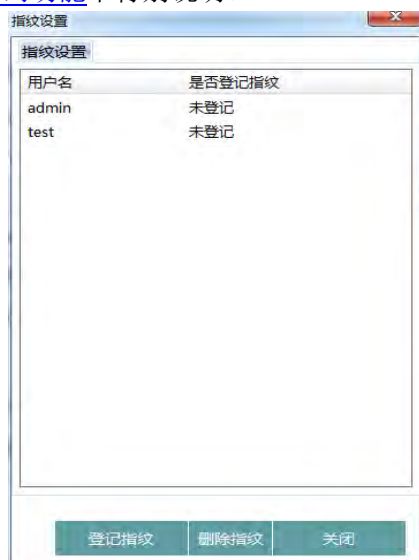
请求开门声音、按钮请求声音：设置远程请求开门或开门按钮远程请求开门时中心播放声音。

报警声音颜色：设置产生报警时报警的声音以及报警记录的颜色。

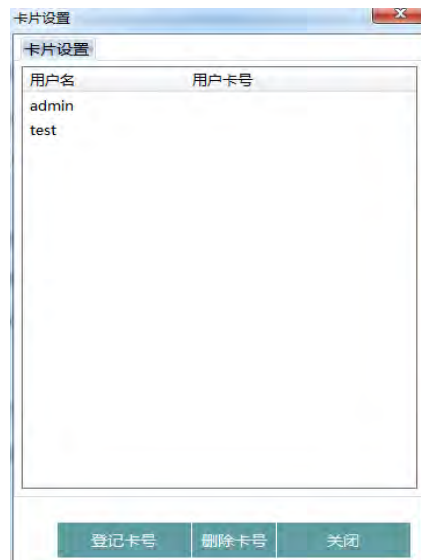
指纹设置：管理员通过USB指纹仪可登记指纹，用于远程确认开门。

卡片设置：管理员通过发卡器可登记卡号，用于远程确认开门。

启用身份验证码：启用后可在添加、编辑人员处显示身份验证码的输入框，具体使用方法参阅[6.11.3 动态码功能](#)中特别说明。



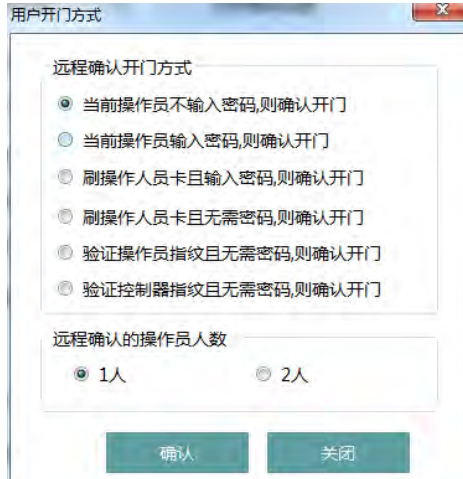
指纹设置



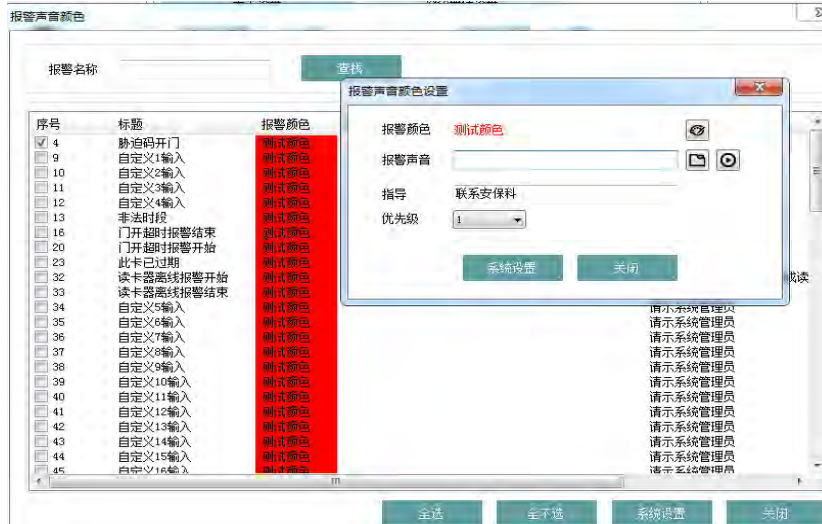
卡片设置

用户开门方式：管理员收到远程确认开门的请求时可用不同的验证方式来确认开门，请求开关服务和开门按钮远程请求开门也同样适用这种验证方式。验证方式如下图所示，刷操作员卡和验证操作员指纹需要电脑连接USB指纹仪和发卡器，验证控制器指纹需要在控制器连接指纹

仪，后三种方式才可设置2个操作员。（验证控制器指纹方式不适用于请求开关服务）



报警声音颜色： 点击‘设置’按钮，可自定义报警的颜色、声音、指导、优先级。



开门理由必填： 勾选后远程确认开门是操作员必须填写开门理由才能远程开门。

密码连续错误次数限制： 设置输入密码错误次数，如连续输入错误密码超过设定的数，则锁定登录界面。

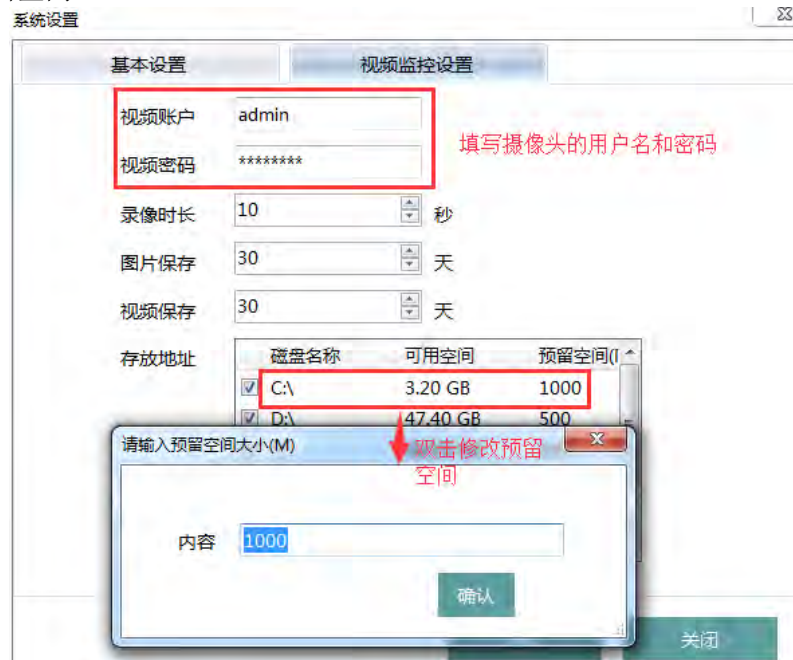
登录方式： 可选择密码、指纹、指纹+密码的登录方式。

监视锁舌状态： 勾选后可在监控界面查看锁舌状态，点击设置配置每个门对应的输入端口号。



2. 视频监控设置

若网络摄像头需要用户名、密码才能连接，可在此填写。可以设置录像、抓拍文件的保存位置以及保存的天数，还可以设置录像的时长。设置好后点击确定即可保存设置。双击每个盘所在的列可弹出设置每个盘的预留空间。




6.11.3 动态码功能

启用动态码功能，验证开门需要验证收到的短信验证码。操作步骤如下：

- 1、在【系统设置】中勾选使用动态码功能会显示【短信参数】的按钮，在【短信参数】设置连接短信猫。在电脑【设备管理】中【端口】查看短信猫所连接的端口，在【短信参数】串口处选择相应端口，然后【打开串口】，提示打开端口成功且显示短信中心号码即说明连接短信猫成功，点击【保存】即可。在下次打开系统无需重新设置，系统会自动打开串口。
- 2、在门管理中设置需要开启动态码功能的门，把动态码改为开启状态，然后在【设备任务管理】中下载参数到设备即可。



特别说明：旧版动态码功能还需启用身份验证码，在【系统设置】中勾选启用身份验证码，在人员管理添加、编辑人员的界面会显示身份验证码的输入框，输入1-4位的身份验证码（身份验证码需与在指纹仪中注册用户时的编号保持一致），确定保存后身份验证码会转化为11位的卡号显示在卡号1的位置。

 备注：如果卡号1原来已经有卡号，身份验证码转换的卡号会替换卡号1的卡号；身份验证码输入框为空时则不影响原来的卡号1。

6.11.4 开关服务功能

操作步骤：

1. 在【设备管理】中启用设备的权限服务控制功能，操作详情请参阅[5.2.2 设备添加](#)。
2. 设置具有开启服务的权限组，操作详情请参阅[6.4.1 设备权限组管理](#)，并给权限组分配人员，此权限组的人员即具有开关服务的权限。
3. 在【设置】→【系统设置】中设置开关服务卡数以及是否开服务同时开门。开关服务卡数可设置1-3张，设置1张卡时，刷具有权限服控制的卡可以直接请求开关服务，开关服务都需中心确认；设置2-3张卡时，仅可以刷1张具有一张具有权限服务控制的卡，再加1-2张具有其他任意开门权限的卡，不能同时使用两张以上具有权限服务控制的卡进行刷卡请求开关服务。

6.11.5 报警处理

点【报警处理】，在弹出的界面，会默认显示未处理的报警信息，可选中单条记录点【处理】，再选择处理的结果即可。也可以全部处理，点【处理所有】然后选择处理的结果即可，点【关闭】退出。



6.11.6 电子地图

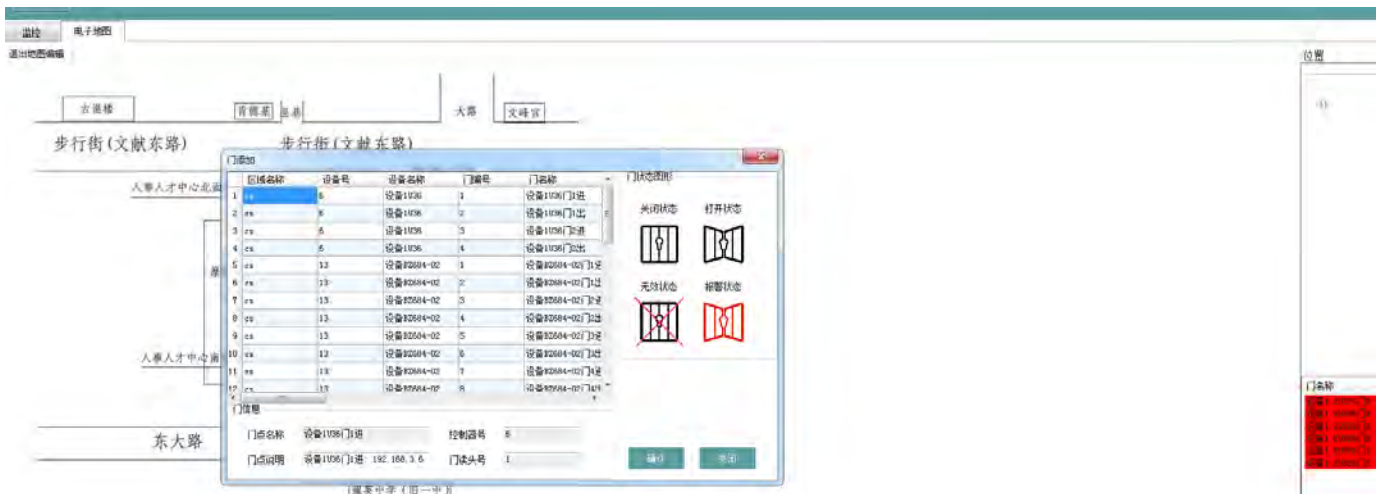
添加地图：操作员可以在位置栏右键添加地图，然后输入地图名称，选择地图背景即可（目前只支持图片），选择上级区域可以添加子地图

删除地图：选中要删除的地图，右键删除即可。

编辑地图：选中要编辑的地图，右键可以修改地图的图片，及名称。

添加地图后，用户可以在地图上进行添加门等操作，点击进入地图编辑。用户可以移动门、图标的位置以及改变地图或者门图标的位置，退出地图编辑保存当前的设置。

添加、删除门：用户可以在地图上添加门，可以移除已存在的门（选中门，点击界面上方“删除门”），以及调整门图标的位置（拖曳门图标）。



报警处理：电子地图右下角也会显示报警事件，鼠标悬浮在报警事件的门名称上会显示对应的处

置指导。双击事件也可以对报警事件进行处理, 如下图。

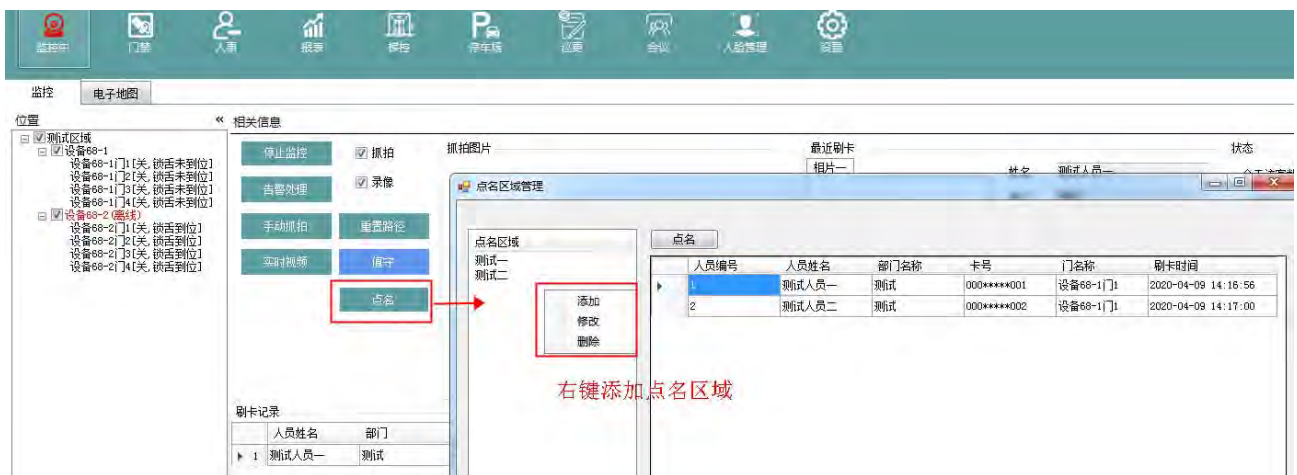


6.12 点名功能

点名功能可以统计一个受控区内的停留人数, 同时可设定最少停留数, 一旦少于设定的人数, 监控中心会产生报警。该功能必须联机使用, 控制器脱机无法使用该功能。

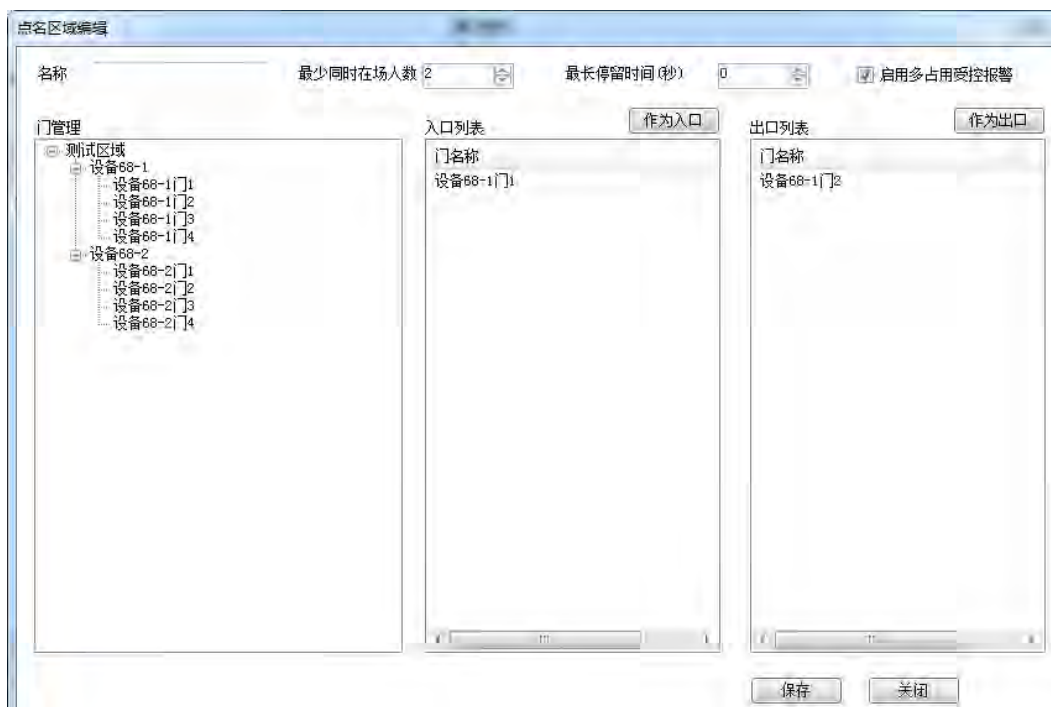
设置步骤如下:

(1) 点击【实时监控】的【点名】按钮, 弹出点名区域管理界面, 如下图。在“点名区域”一栏可以右键添加点名区域。选择“点名区域”, 然后点击右边的“点名”则会在右侧区域显示选中区域里停留的人数。



(2) 添加点名区域的界面如下图, 输入点名区域名称, 在设备门点列表中选择门点, 然后点击“作为入口”或“作为出口”, 然后点击“保存”即可。

(3) 设置了“最少同时在场人数”并勾选“启用多占用受控报警”, 当人数少于设定人数就会产生多占用受控报警。“最少停留时间”则为少于设定人数后多久之后报警, 设为“0”则马上报警。



第7章 报表

包括【门禁报表】、【访客报表】、【综合报表】、【停车场报表】4个报表，这几个子系统都使用同一个数据库。

包括【记录报表】、【历史记录报表】、可以选择全部导出或查询后导出。用户可以根据报表统计相关设备数据，包括卡验证信息、门操作信息、正常刷卡信息等。

7.1 门禁报表

7.1.1 记录报表

1、打开客户端，点击【报表】→【记录报表】，可以查询3个月以内的记录，界面如下图所示：

记录状态	人员姓名	部门名称	卡号	设备名称	门名称	刷卡时间	记录类型	事件名称	处理人	处理时间	进出类型
1 实时				设备2D3182		2018-08-22 16:04:18	报警	控制器防拆报警			
2 实时				设备2D3182	设备2D3182门4	2018-08-22 16:04:14	报警	门撬开报警开始			
3 实时				设备2D3182	设备2D3182门2	2018-08-22 16:04:11	报警	门撬开报警开始			
4 实时	张三	工程	00019645234	设备2D3182	设备2D3182门3	2018-08-22 14:40:13	开门	正常刷卡开门			
5 实时	张三	工程	00019645234	设备2D3182	设备2D3182门3	2018-08-22 14:39:47	开门	正常刷卡开门			
6 实时				设备2D3182	设备2D3182门3	2018-08-21 17:57:10	报警	门撬开报警结束			
7 实时				设备2D3182	设备2D3182门3	2018-08-21 17:57:08	报警	门撬开报警开始			
8 实时				设备2D3182	设备2D3182门3	2018-08-21 16:25:24	报警	胁迫码开门			
9 实时				设备2D3182	设备2D3182门3	2018-08-21 16:25:21	开门	密码无效			
10 实时				设备2D3182	设备2D3182门3	2018-08-21 16:25:05	报警	胁迫码开门			
11 实时				设备2D3182	设备2D3182门3	2018-08-21 16:25:02	开门	密码无效			
12 实时				设备2D3182	设备2D3182门3	2018-08-21 16:24:47	报警	胁迫码开门			
13 实时				设备2D3182	设备2D3182门3	2018-08-21 16:24:32	报警	胁迫码开门			
14 实时				设备2D3182	设备2D3182门3	2018-08-21 16:24:04	报警	胁迫码开门			
15 实时				设备2D3182		2018-08-17 18:19:38	报警	控制器防拆报警			
16 实时				设备2D3182	设备2D3182门4	2018-08-17 18:19:34	报警	门撬开报警开始			
17 实时				设备2D3182	设备2D3182门3	2018-08-17 18:19:33	报警	门撬开报警开始			
18 脱机				设备2D3182		2018-08-15 11:33:03	报警	控制器防拆报警			
19 脱机				设备2D3182	设备2D3182门4	2018-08-15 11:32:58	报警	门撬开报警开始			
20 脱机				设备2D3182	设备2D3182门3	2018-08-15 11:32:57	报警	门撬开报警开始			

可以根据日期段来查询记录，；可以选择查询记录的条件：记录状态、记录类型、部门、卡号、设备、门、事件名称、进出类型等；记录可以以Excel或CSV的格式导出。

2、记录报表可以双击一条记录弹出详细的记录信息窗口如下图：记录的基本信息，人员的相片，抓拍的图片以及录像。录像的播放局域网内可以直接播放（确认可以访问录像文件所在电脑）。

部门名称	人员姓名
身份证号码	
卡号	
设备名称	设备6D174
记录时间	2017-06-22 11:21:34
事件名称	控制器防拆报警
操作人	admin

记录状态	记录类型
实时	开门
进出类型	
操作时间	2017/10/27 14:26:54

7.1.2 历史记录报表

打开客户端，点击【门禁】→【历史记录报表】，可以查询3个月之前的记录，其余操作与记录报表操作一样。

7.1.3 入库超时报警表

查询入库超时报警的记录

7.1.4 访客报表

查询访客系统的报表数据，访客系统与门禁系统使用同一个数据库

7.1.5 综合报表

查询系统中人员在整个一卡通系统某段时间内的通行报表

7.1.6 停车场报表

包含【进出记录报表】、【收费记录报表】

7.1.7 门禁报表 683

包含【刷卡记录表】、【报警记录表】

第 8 章 数据库管理

打开【设置】→【数据库备份】菜单，点击数据库备份按钮即可备份数据库，数据库备份会在下方列表显示，可在列表选中其中一个数据库备份删除，下载会打开数据库备份文件所在的保存路径，可把需要还原的数据库拷贝出来还原。



第 9 章 用户使用 FAQ

1. 扫描不到设备？
设备没有联网、网络不通、跨网段。
2. 扫描工具可以扫到设备，但数据服务系统无法连上设备。
设备服务器本地 IP 是否正确（对应服务器的 IP 地址）
3. 系统到了登录界面，但无法登录进去？
检查所连接的数据库填写是否正确，免费版（EXPRESS 版本）的数据库的填写方式是否正确（不支持网络连接），免费版的需要加 `sqlexpress` 后缀，有些不支持 IP 方式，需要以点（`.\sqlexpress`）的方式。
4. 数据库测试连接成功，账号密码输入正确，依然无法登陆系统？
回到数据库设置，查看数据库相关参数是否被记住，，如果没有记住，请使用管理员权限重新打开系统设置数据库，此情况在 WIN10 系统容易出现。
5. 下载了任务，但执行不成功
网络是否连通，设备区域】服务器 IP 地址是否正确
6. 系统安装时提示需要权限
选中安装程序右键选择以管理员身份运行。
7. 打开数据服务系统，只出现连接数据库成功，没有启动设备服务成功的提示。
是数据服务系统软件没有管理员的权限运行，启用管理员权限即可，此情况在 WIN10 系统容易出现。
8. 勾选设备点击实时监控提示未找到文件保存位置，请到“设置”→“系统设置”中设置。
到“设置”→“系统设置”→“文件保存设置”中勾选相应的盘，然后确定即可，如已勾选就直接确定即可。
此时开启监控不再弹出提示。