门禁

FAQ

浙江大华技术股份有限公司

V1.0.3

前言

本文档主要针对实际使用环境中遇到的常见设备故障、参数设置疑问、使用误区等问题提供解决思路及操作指导。

本文档中的描述内容需要结合实际现场设备具体分析，并不作为唯一的处理方式，若有疑问请联系相关技术支持代表。

符号约定

在本文档中可能出现下列标识，代表的含义如下。

标识	说明
 危险	表示有高度潜在危险，如果不能避免，会导致人员伤亡或严重伤害。
 警告	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。
 窍门	表示能帮助您解决某个问题或节省您的时间。
 说明	表示是正文的附加信息，是对正文的强调和补充。

修订记录

版本号	修订内容	发布日期
V1.0.3	更新内容。	2022.12
V1.0.2	更新内容。	2022.04
V1.0.1	更新内容。	2021.09
V1.0.0	首次发布。	2020.12

使用安全须知

以下是关于产品的正确使用方法的要求，为预防危险、防止财产受到损失，使用设备前请仔细阅读本说明书并在使用时严格遵守，阅读后请妥善保存说明书。

运输要求

注意

请在允许的湿度和温度范围内运输产品。

贮存要求

注意

请在允许的湿度和温度范围内存储产品。

安装要求

警告

- 严禁将电源适配器上电后再连接设备，请在断电状态下连接电源适配器和设备。
- 请严格遵守当地各项电气安全标准，确保环境电压稳定并符合设备供电要求。
- 请勿同时对设备提供两种及以上供电方式，否则可能导致设备损坏或造成安全风险。
- 请务必按照要求使用电池，否则可能导致电池起火、爆炸或燃烧的危险！

注意

- 请勿将设备放置和安装在阳光直射的地方或发热设备附近。
- 请勿将设备安装在潮湿、有灰尘或煤烟的场所。
- 请保持设备的水平安装，或将设备安装在稳定场所，注意防止本产品坠落
- 请将设备安装在通风良好的场所，切勿堵塞设备的通风口。
- 请使用产品制造商提供的适配器或机箱电源。
- 产品必须使用本地区推荐使用的电线组件（电源线），并在其额定规格内使用！
- 请使用满足 SELV（安全超低电压）要求的电源，并按照 GB8898（IEC60065）或 GB4943.1（IEC60950-1 符合 Limited Power Source（受限制电源））的额定电压供电，具体供电要求以设备标签为准。
- 请将 I 类结构的产品连接到带保护接地连接的电网电源输出插座上。

操作要求

注意

- 请在设备运行前检查供电电源是否正确。
- 请勿在适配器上电时拔下设备侧电源线。
- 仅可在额定输入输出范围内使用设备。
- 请在允许的湿度和温度范围内使用产品。
- 请勿将液体滴到或溅到设备上，并确保设备上没有放置装满液体的物品，防止液体流入设备。
- 请勿拆卸设备。

目录

第 1 章 门禁控制器

1.1 一代门禁控制器默认 IP 地址/端口/账号/密码

- 出厂默认 IP 地址：192.168.0.2。
- 端口：37777
- 账号：admin
- 密码：123456

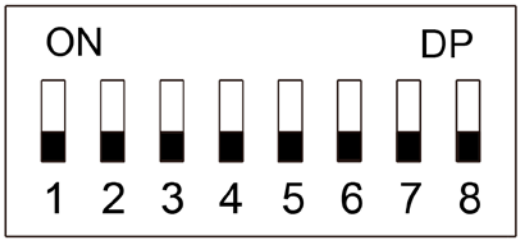
1.2 忘记修改后的门禁主机 IP

- 使用门禁配置工具 ACSConfig 自动搜索 IP。
  打开 ACSConfig 工具，单击“搜索”设置，设置设备的 IP 网段，单击“确定”。通过设备类型、型号、MAC 地址等信息找到设备。

图1-1 自动搜索

- 恢复出厂设置重新修改 IP。
  通过设备拨码开关恢复出厂设置后，重新设置设备的 IP 地址。

图1-2 拨码开关



开关在 ON 表示 1；开关在下表示 0。

◇ 1、3、5、7 为 1，其他为 0，设备重启后系统恢复出厂状态。

◇ 2、4、6、8 为 1，其他为 0，设备重启后系统恢复出厂状态，但保留用户信息。

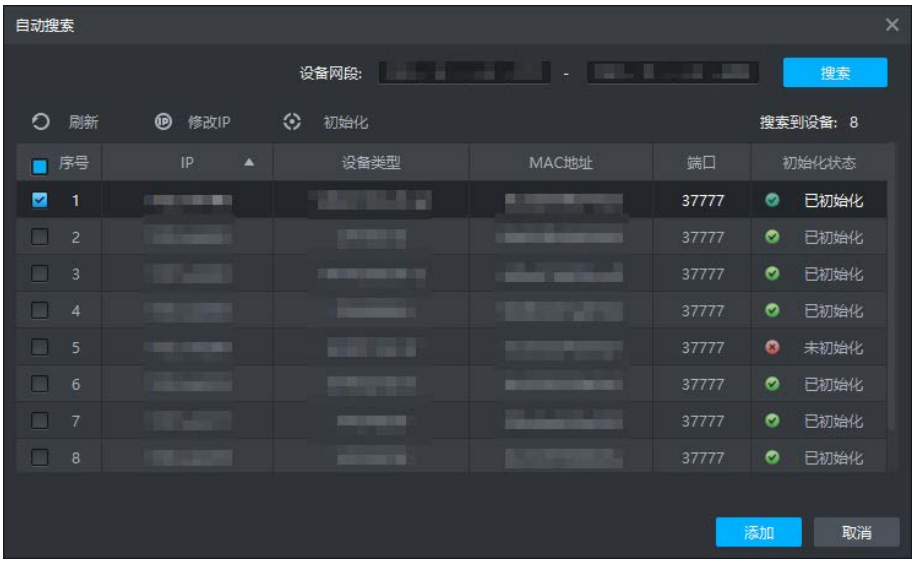
1.3 如何修改设备 IP

步骤1 登录 SmartPSS Plus 客户端。

步骤2 在“设备管理”界面，单击“自动搜索”。

步骤3 设置设备的 IP 网段，单击“修改 IP”。

图1-3 自动搜索



步骤4 设置设备的 IP 地址、子网掩码和网关 IP。

图1-4 修改设备 IP

步骤5 单击“确定”。

1.4 门禁控制器如何恢复出厂设置

- 单门控制器：拨码开关 1、3 拨到 ON，断电重启听到滴一声后再拨回来。
- 双门/四门控制器：1、3、5、7 拨到 ON，断电重启听到滴一声后再拨回来。
- 门禁一体机：进入管理员菜单，在“系统配置”界面进行恢复出厂设置操作。

1.5 门禁控制器如何升级

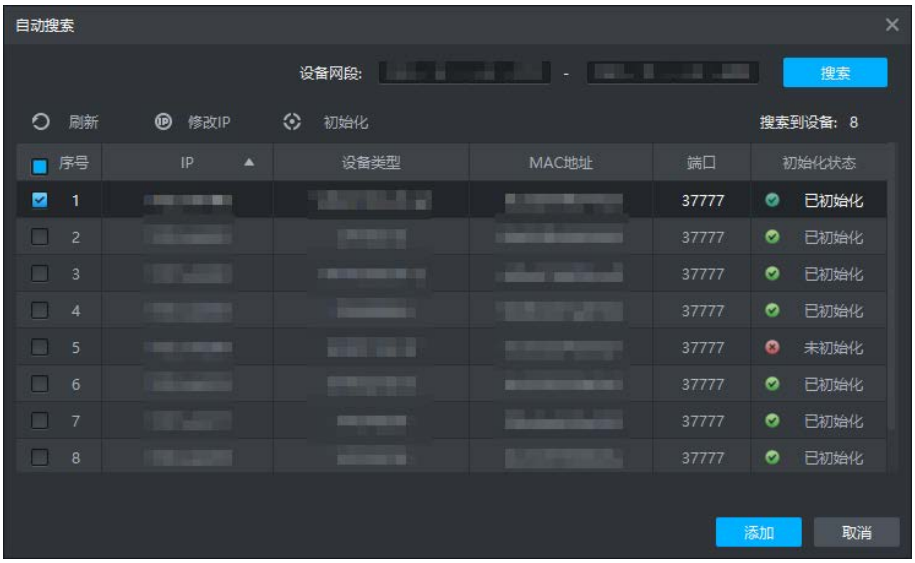
获取正确版本的升级文件后，通过 SmartPSS Plus 客户端。

步骤1　登录 SmartPSS Plus 客户端。

步骤2　选择“设备管理”，添加设备。

- 搜索添加
  1. 在“设备管理”界面，单击“自动搜索”。
  2. 设置设备的 IP 网段，单击“搜索”。
  3. 选择需要添加的设备，单击“添加”。

图1-5 自动搜索

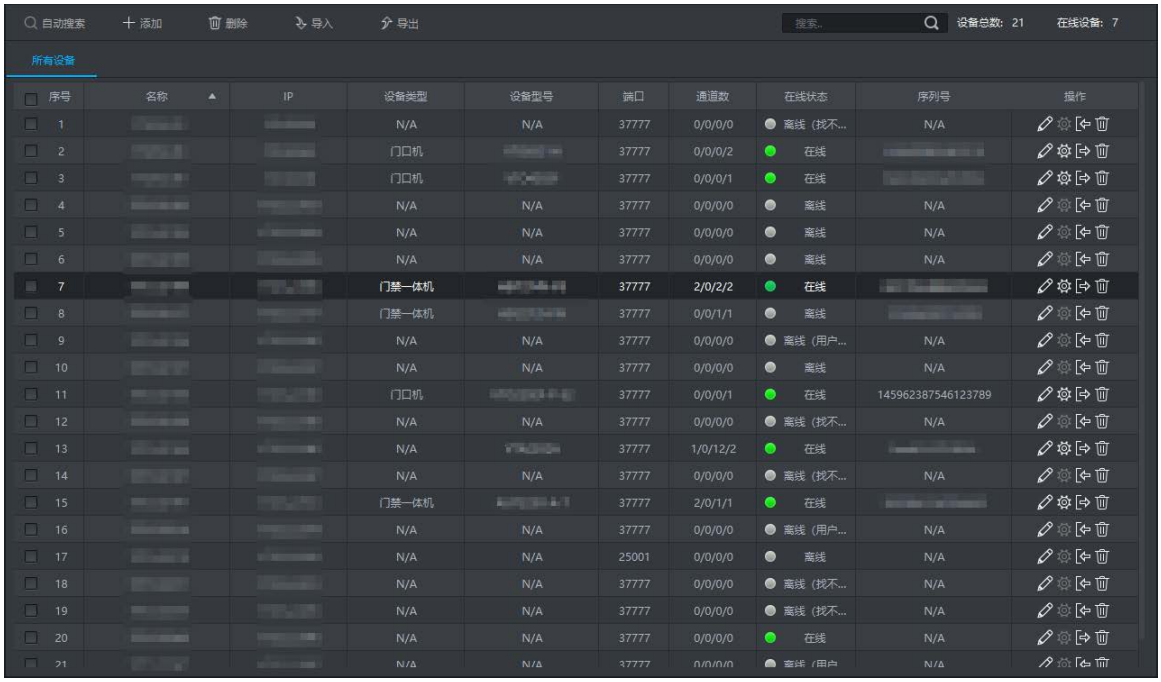


- 手动添加
  1. 在“设备管理”界面，单击“添加”。
  2. 输入设备信息后，单击“添加”。

图1-6 添加设备

步骤3　单击设备对应的  。

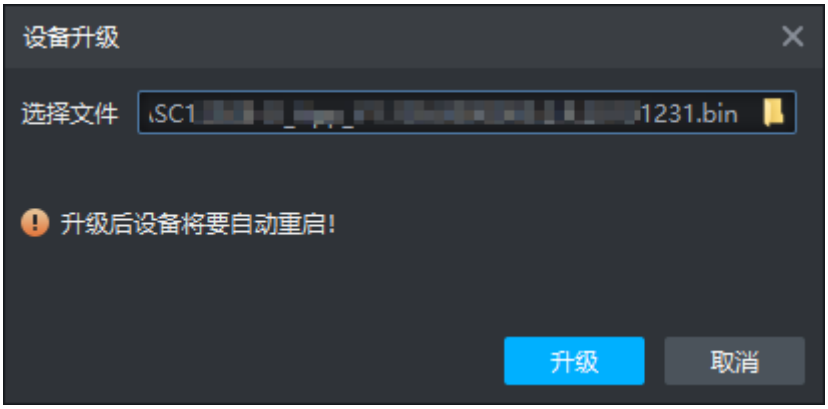
图1-7 设备管理



步骤4　单击“升级”。

步骤5　选择升级文件后，单击“升级”。

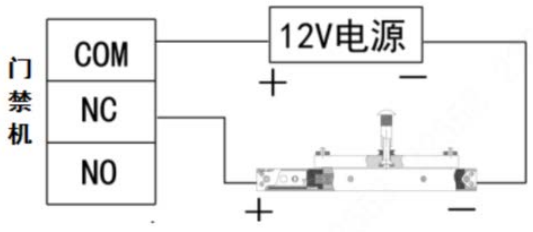
图1-8 设备升级



1.6 门禁控制器与磁力锁、电插锁如何接线

外接电源正极接门禁控制器 COM 口，门禁控制器 NC 口接锁的正极，锁的负极接外接 12 V 负极。

图1-9 接线示意图



1.7 门禁控制器与读卡器如何接线

1 个门禁控制器仅支持接入一种类型的读卡器，485 和韦根只能选择其一。

- 只接 485 信号线：红（12 V）、黑（GND）、黄（485-）、紫（485+）。
- 只接韦根信号线：红（12 V）、黑（GND）、绿（D0）、白（D1)。

图1-10 接线说明

接线颜色	接线端子	说明
红	12V 电源	读卡器电源
黑	GND	
蓝	CASE	韦根读卡器
白	D1	
绿	D0	
棕	LED	
黄	RS485-	RS485 读卡器
紫	RS485+	

说明

- 网线接口的读卡器线序白橙（485+），橙(485-)，白绿(LED)，蓝(D0)，白蓝(D1)，绿(CASE)，白棕(GND)，棕(12 V+)
- 从读卡器到控制器接线建议使用超 5 类以上网线，控制器到门锁建议使用 rvv4*1.0 的 4 芯纯铜线缆。读卡器距离较远的(超过 100 米)需要独立供电。

1.8 单元门口机联动门禁控制器开门，该如何接线

外接 12 V 电源正极接门禁控制器 COM 口，门禁控制器 NC 口接单元门口机 COM 口，单元门口机 NC 口接锁的正极，锁的负极接外接 12 V 电源的负极。

1.9 门磁反馈线如何连接门禁控制器

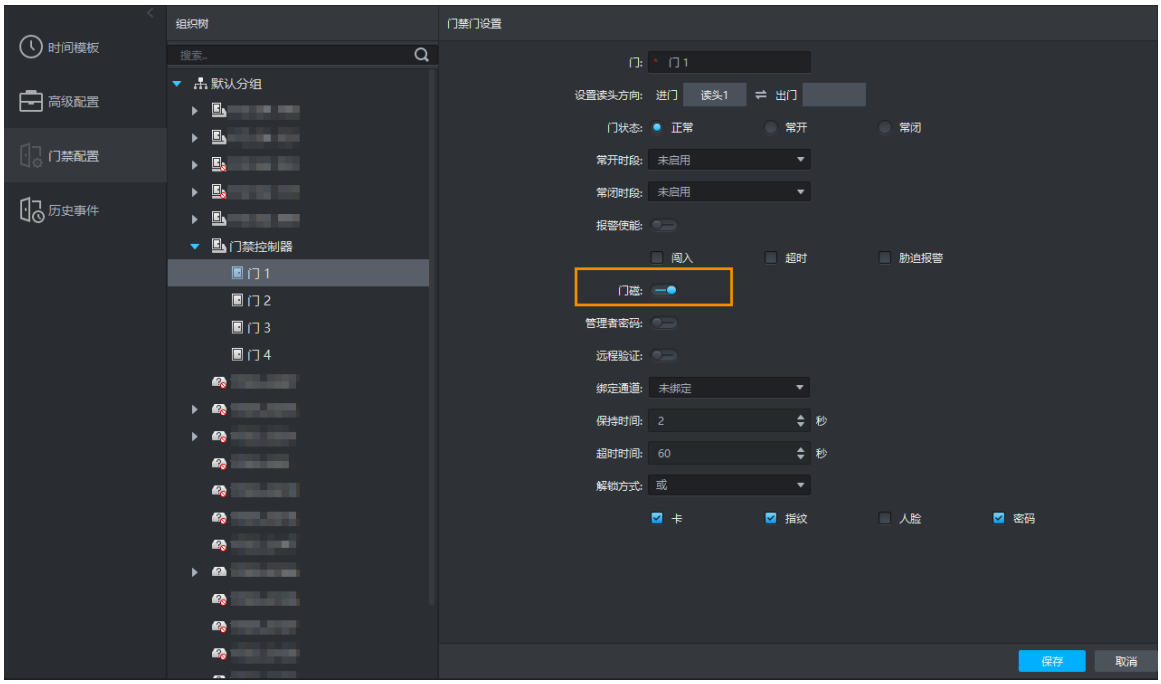
连接门禁控制器的 SR 和 GND 口。同时需要开启门磁使能。

步骤1　登录 SmartPSS Plus 客户端。

步骤2　选择“门禁配置 > 门禁配置”。

步骤3　选择门禁控制器，开启门磁使能。

图1-11 门禁配置



步骤4 单击“保存”。

1.10 消防联动如何连接门禁控制器

连接门禁控制器的 Alarm1 和 GND 口，当有信号输入时，所有门保持常开状态。

1.11 门禁读卡器如何判断是使用何种卡片的

通过门禁读卡器的型号命名判断，默认使用 IC 卡，-D 表示使用 ID 卡，-C 表示使用 CPU 卡。

以 ASR1100A 为例，ASR1100A 是使用 IC 卡的，ASR1100A-D 是使用 ID 卡的，ASR1100A-C 是使用 CPU 卡的。

1.12 如何设置胁迫卡、胁迫密码、胁迫指纹

在软件中添加人员的时候，将卡片类型选为胁迫卡，对应的指纹就是胁迫指纹，基线程序不支持胁迫密码。

1.13 门禁控制器胁迫卡为何不能开门

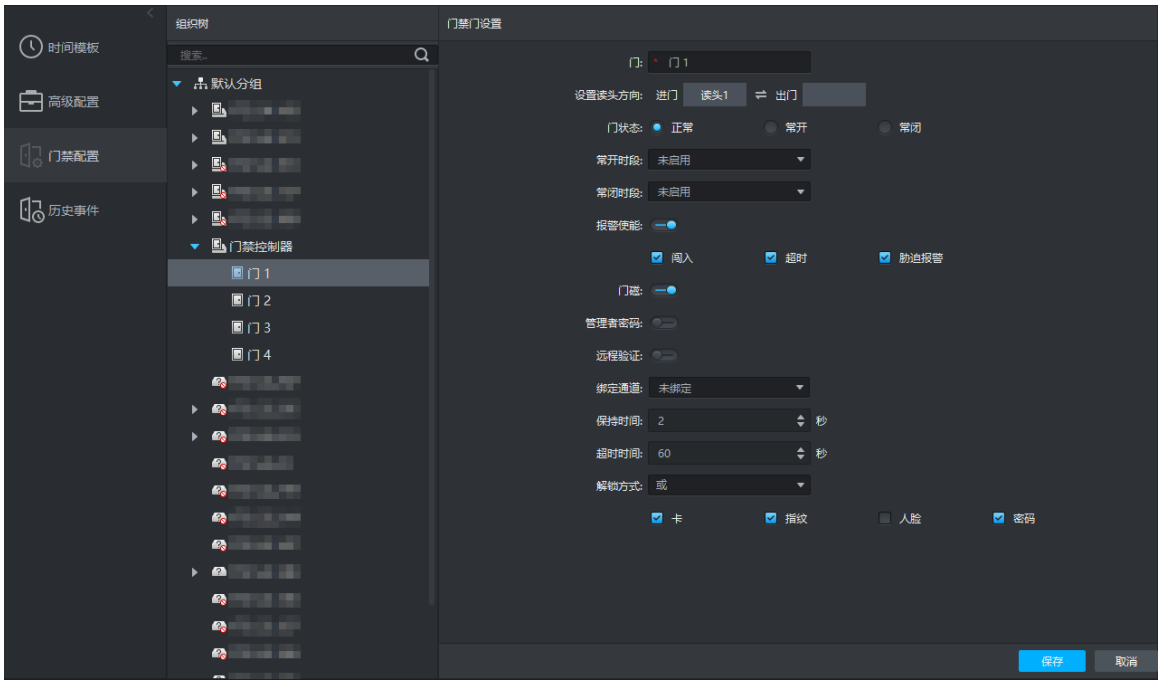
将卡片类型设置成胁迫卡，需要在门配置里开启报警使能，才可以实现胁迫卡开门并上传报警信息。

步骤1 登录 SmartPSS Plus 客户端。

步骤2 选择“门禁配置 > 门禁配置”。

步骤3　选择门禁控制器，开启报警使能，并选择“胁迫报警”。

图1-12 门禁配置



步骤4　单击“保存”。

1.14 修改门禁控制器密码后，修改前的密码还能用

修改密码时，需要先删除旧密码后，再添加新密码。如果忘记旧密码，需要使用 JSON 工具删除卡片信息后，重新设置密码。

步骤1　联系相关技术支持获取 JSON 工具。

步骤2　双击.exe 文件，输入门禁控制器的 IP 地址、用户名和密码，单击“登录”。

图1-13 登录

步骤3　选择“卡片管理”页签，输入卡号后，单击“获取卡”。

图1-14 卡片管理

步骤4　单击“删除卡”。

1.15 下发权限后，无法刷卡开门

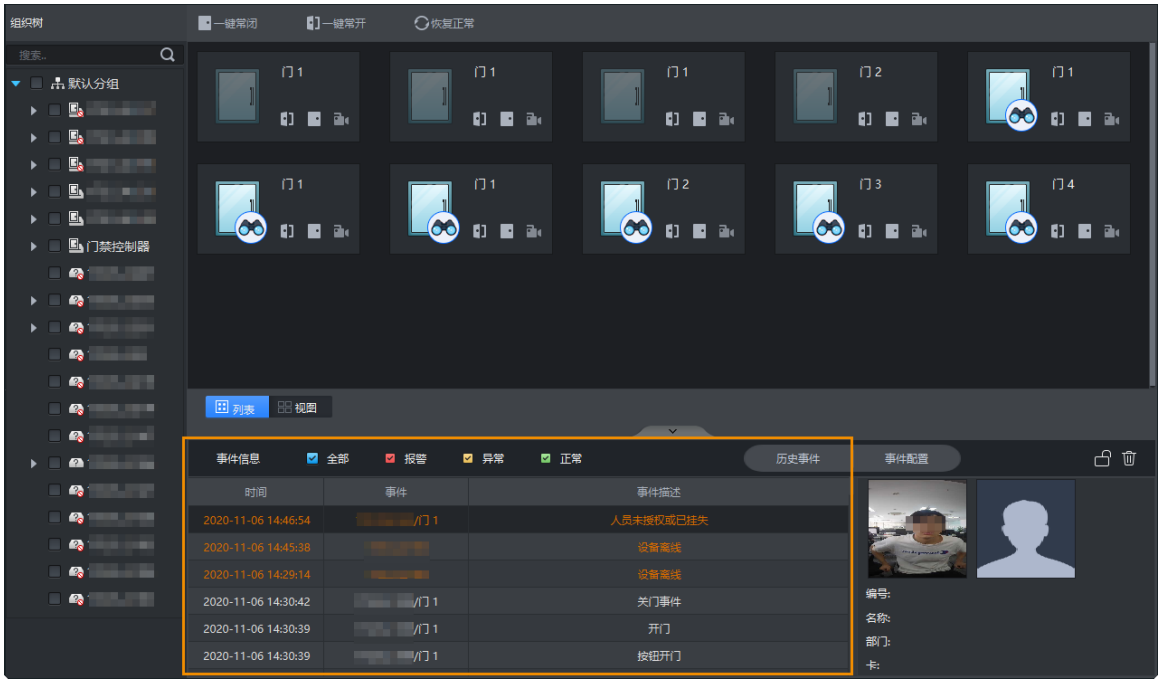
步骤1　登录 SmartPSS Plus 客户端。

步骤2　选择“门禁管理”。

步骤3　根据事件描述信息判断，并排查相关问题。

- 若无事件上报，说明读卡器线路异常，请重新接线或更换设备。
- 若上报正常开门，说明锁的接线异常，请重新接线或更换设备。
- 若上报其余事件，如卡片有效期错误、开门模式错误等，请根据对应的描述信息进行排查。

图1-15 门禁配置



1.16 门禁控制器命名后缀-D\-S 代表什么

-D 表示双向开门，-S 表示单向开门。

1.17 门禁设备如何作为考勤使用

登录 SmartPSS Plus 客户端，选择“门禁控制器 > 考勤管理”，设置考勤点、人员排班，时间段等，详细介绍请参见配套的资料。

说明

- 考勤点最多设置 10 个。
- 考勤原理是将每个人一天当中的第一条和最后一条刷卡记录作为考勤记录。

1.18 C 款门禁控制器主板一直蜂鸣

步骤1 拆除五根供电线中的红黑黄三根线，保留红黑两根线。

步骤2 检查问题是否已经解决。

如果已解决，则完成问题处理，否则请联系相关技术支持。

1.19 门禁控制器在平台时而在线时而离线

现象描述

在平台添加门禁控制器后，门禁控制器时而在线，时而离线。

可能原因

- IP 冲突。
- 交换机异常。
- 平台异常。

解决方法

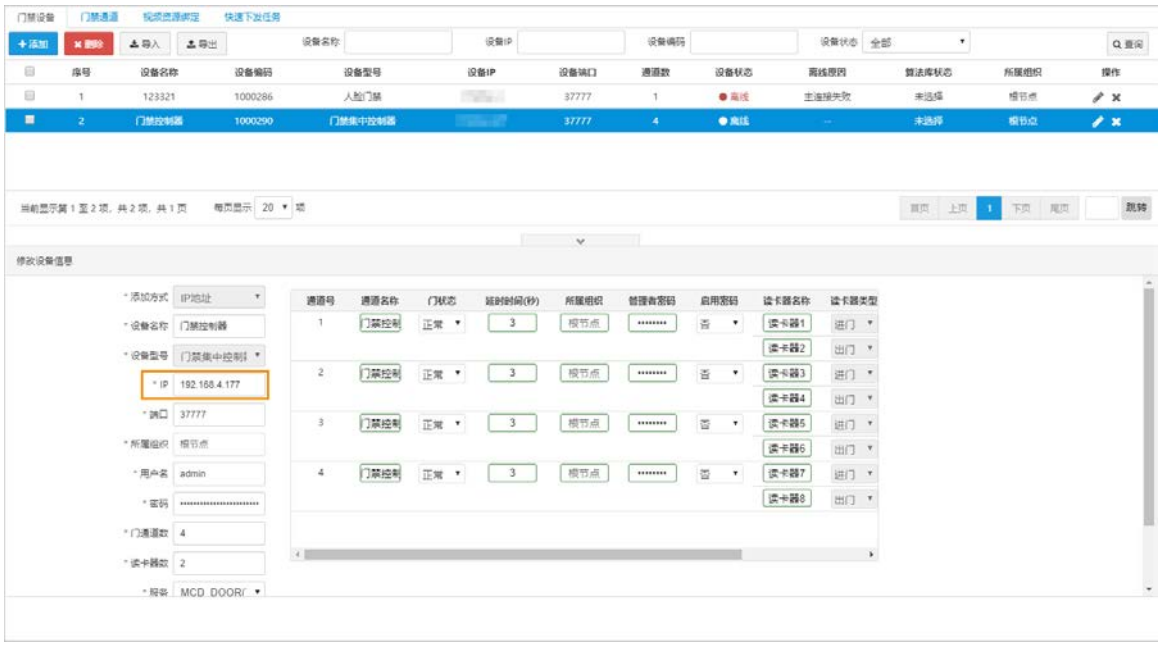
步骤1　修改设备的 IP 地址。

说明

以下操作以智慧园区综合管理平台为例。

1. 登录智慧园区综合管理平台。
2. 选择“业务导航 > 一卡通应用 > 门禁管理 > 设备管理”。
3. 单击设备对应的 。
4. 修改设备的 IP 地址，单击“确定”。
   确保修改后的 IP 不存在冲突。

图1-16



5. 检查问题是否已经解决。
   如果已解决，则完成问题处理，否则请继续执行以下步骤。

步骤2　检查离线期间，同一网段的其他设备是否离线。

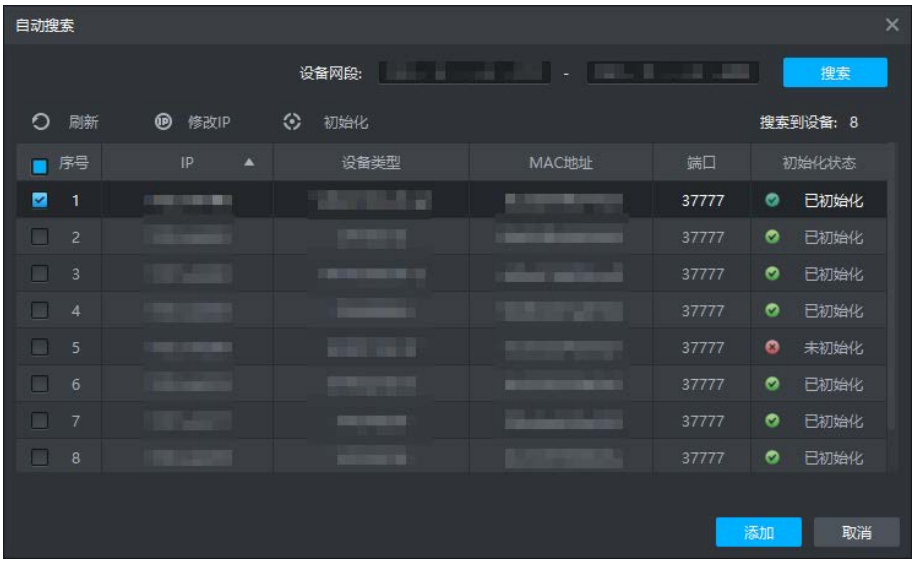
如果是，说明书交换机异常，请排查供电、网络等问题，否则请继续执行以下步骤。

步骤3　使用 SmartPSS Plus 添加设备。

1. 登录 SmartPSS Plus 客户端。
2. 选择“设备管理”，添加设备。
   - ◇ 搜索添加

     单击“自动搜索”，设置设备的 IP 网段，单击“搜索”，选择需要添加的设备，单击“添加”。

图1-17 自动搜索



   - ◇ 手动添加

     单击“添加”，输入设备信息后，单击“添加”。

图1-18 添加设备

步骤4　检查问题是否已经解决。

如果已解决，说明平台异常，请排查平台问题，否则请联系相关技术支持。

1.20 门禁控制器多门互锁功能如何实现

步骤1　确保电锁的门磁反馈信号线接入门禁控制器的 SR 和 GND 口。

步骤2　在 SmartPSS Plus 的门配置中开启门磁使能。

步骤3　在 SmartPSS Plus 的权限管理中，设置门与门的互锁关系。

1.21 门禁控制器人员权限丢失

判断设备程序版本是否为最新程序，如果不是先将程序升级至最新基线程序。通过 SmartPSS Plus 主控台里，右键单击门禁控制器，选择“提取卡信息”，查看门禁控制器内是否有该人员权限。

1.22 门禁控制器能否清空卡片信息或开门密码而不改变 IP

步骤1　联系相关技术支持获取 JSON 工具。

步骤2　双击.exe 文件，输入门禁控制器的 IP 地址、用户名和密码，单击“登录”。

图1-19 登录

步骤3　选择“卡片管理”页签，输入卡号后，单击“删除卡”或“清空卡”。

图1-20 卡片管理

步骤4　单击“删除卡”。

1.23 门禁控制器升级后无法开门，系统提示门处于常闭状态

获取 JSON 工具，登录设备，进入“门参数设置”界面，获取信息后，将常闭时段由 0 改为 255。

步骤1　联系相关技术支持获取 JSON 工具。

步骤2　双击.exe 文件，输入门禁控制器的 IP 地址、用户名和密码，单击“登录”。

图1-21 登录

步骤3　选择“门参数”页签，单击“获取”。

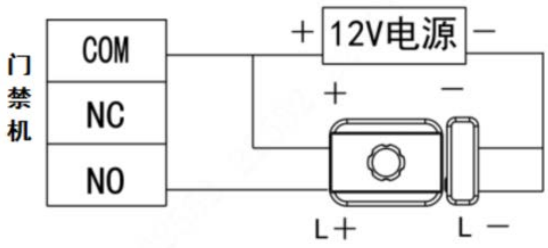
步骤4　设置“常闭时间段”为“255”，单击“设置”。

图1-22 门参数

1.24 门禁控制器与电机锁如何接线

外接电源正极接电机锁正极，外接电源负极接电机锁负极，外接电源正极接门禁控制器的 COM 口，门禁控制器的 NO 口接电机锁的 L+，L-接外接电源负极。

图1-23 接线示意图



1.25 门禁控制器端刷一次卡在平台上报两次事件

现象描述

门禁控制器端刷一次卡在平台上报两次事件。

可能原因

读卡器跟控制器端的连线异常，485 和韦根同时接入，刷卡验证时刷了一次上报了两次人员信息。

解决方法

拆除 485 或者韦根其中一个的接线。

1.26 二代控制器使用人员 ID 开门，输入一遍 ID+#，未输密码，就提示 ID 正确，密码错误

现象描述

二代控制器在使用人员 ID 开门时，输入一遍 ID+#，未输密码，就提示 ID 正确，密码错误。

可能原因

读卡器和二代控制器之间的接线错误，485 和韦根同时接入，导致传输两遍 ID+#，以至于报错。

解决方法

拆除 485 或者韦根其中一个的接线。

1.27 二代门禁控制器的默认 IP，端口，用户名，密码

- 默认 IP：192.168.1.108
- 端口：37777
- 用户名：admin
- 密码：admin123

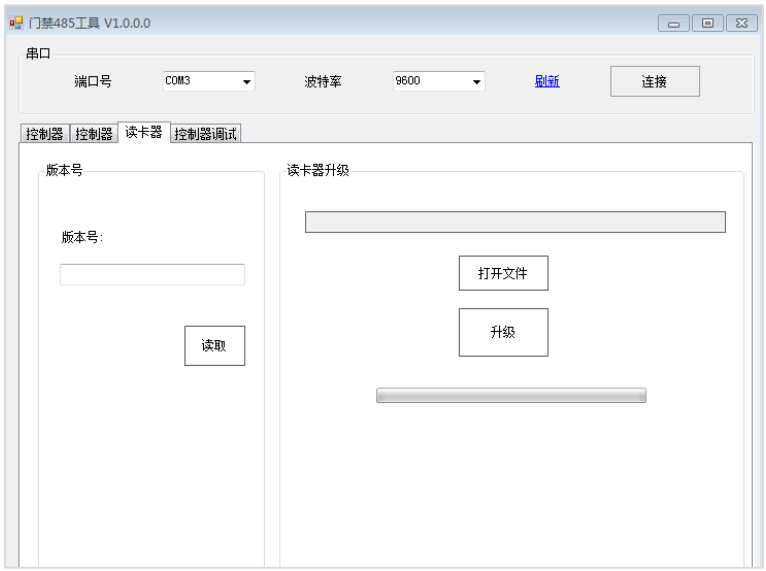
1.28 门禁控制器时间同步失败

没有定制功能的前提下，需要将门禁控制器版本升级至最新。

1.29 读卡器版本如何获取

- 通过 485 接入门禁控制器，且门禁控制器版本需升级至 210620 版本以上，通过 json 工具可查询读卡器版本。
- 通过 USB 转 485 工具，配合门禁 485 工具查看。

图1-24 门禁 485 工具



1.30 一代门禁控制器外接 4 个 ASI1212D，下发人员权限后，刷卡正常，但指纹只有读卡器 1 能用

若 ASI1212D 为 210802 版本，需将一代门禁控制器升级至最新基线版本。

1.31 二代控制器通过主动注册到三方平台，平台在下发人员时设备经常离线

平台在下发时，需要收到设备的回复后才能再次下发。

第 2 章 门禁一体主机

2.1 门禁一体主机 ASI1212A 能否作为读卡器使用

可以，使用 485 协议接入门禁读卡器位置，并将一体机的工作模式修改为读卡器模式。

说明

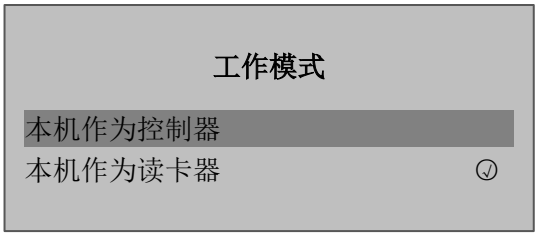
建议门禁一体机 ASI1212A 单独供电。

设置读卡器模式的操作步骤如下：

步骤1　使用 485 协议，将门禁一体机接入门禁控制器的读卡器位置。

步骤2　修改门禁一体机的工作模式为读卡器模式。

1. 登录主界面。
2. 在主界面，通过按【↑】键或【↓】键，选择“系统设置”，并按【√】键。
3. 通过按【↑】键或【↓】键，选择“模式设置”，并按【√】键。
4. 选择“工作模式”，并按【√】键。
5. 通过按【↑】键或【↓】键，选择工作模式，并按【√】键。
   选择成功后，工作模式后面会显示“✓”。



2.2 门禁一体主机 ASI1201A 能否作为读卡器接入控制器

不能，目前门禁一体机 ASI1201A 不支持读卡器模式。

2.3 门禁一体主机升级失败，如何恢复

联系相关技术支持，获取正确的升级程序，再次升级。

2.4 指纹门禁一体主机 ASI1212D 如何通过 U 盘升级

步骤3　将升级文件重命名为“AutoUpDate.bin”，存放在 U 盘根目录，将 U 盘插入设备。

步骤4　在一体机主界面，选择“系统设置”，按【OK】键。

步骤5　选择“U 盘升级”，按【OK】键。

步骤6　通过按【↑】键或【↓】键，选择“是”，并按【OK】键。
系统开始升级，升级完成后自动重启设备。

2.5 测温一体主机对接 NVR，无法收到高温报警邮件

NVR 需要开启邮箱设置的报警使能。

步骤1　使用显示器、鼠标连接 NVR，开启 NVR。

步骤2　登录 NVR 的本地界面，在预览界面右键选择“主菜单”。

步骤3　在主菜单界面，选择“网络设置 > EMAIL”。

步骤4　启用邮箱报警功能，单击“应用”。

图2-1 Email 设置

2.6 A300 系列智能识别设备如何作为读卡器接入门禁控制器

步骤1　使用韦根协议，将智能门禁设备接入门禁控制器。

说明

智能门禁设备需要和门禁控制器共地。

步骤2　需要将智能门禁设备中的 10 进制人员工号转为 8 或 16 进制，作为卡号添加到门禁控制器，并下发权限。

2.7 ASI1212D 人员权限中的密码无法开门，开门模式设置的是密码

密码只能是公共密码开门，个人密码需要配合卡操作，开门方式为卡+密码。

2.8 ASI1201E 通过平台下发卡片失败

该款门禁一体机在平台上添加用户时 userid 不能超过 8 位，且首位不能为 0。

第 3 章 智能门禁一体机

3.1 ASI4214F/ASI6214F 一体机无法下发人脸

此型号设备为红外人脸设备，不可直接通过照片下发人脸。

步骤1 设备前端进行人脸录入。

步骤2 通过 SmartPSS 提取一台设备的红外特征值，然后下发给另一台设备。

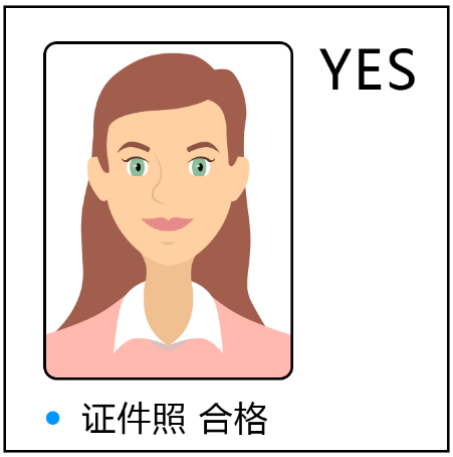
步骤3 使用 U 盘导出一台设备的数据，然后导入另一台设备。

3.2 人脸门禁设备照片无法下发

步骤1 检查一体机在平台上添加时选择的型号是否正确。

步骤2 照片选择 JPG 格式。

图3-1 照片示例



注意

有些照片后缀是 jpg，实际编码格式不是 jpg 格式，可尝试使用软件另存为 jpg，直接修改后缀是不可行的。照片要求小于 100KB 且清晰，人脸的图片占比小于 2/3。

3.3 人脸门禁设备无识别人脸功能

步骤1 尝试使用 web 端的恢复出厂设置，然后断电重启。

步骤2 打印日志分析是否人脸算法过期，若是联系研发同事进行 license 申请。

3.4 人脸门禁设备刷人脸无法开门

步骤1 检查人脸是否已经下发至设备。

步骤2 检查开门方式是否包含人脸开门，检查功能设置的人脸识别启动时段设置，人脸验证时是否在人脸识别启动时间段内。

步骤3　检查人脸底图是否模糊、与实际人脸相似度不高。
步骤4　尝试修改设备 web 端的识别阈值为 85。
步骤5　通过上报的平台的信息进行判断。
步骤6　使用万用表检测设备是否正常输出开关量信号。
步骤7　打印设备日志进行分析，并提供人脸底图以及识别时的视频流。

3.5 人脸门禁设备搭配门禁控制器使用，刷卡不开门

步骤1　进入设备端管理后台。
步骤2　在“通讯设置 > 串口设置 > 串口输出”，将一体机的串口输入改为串口输出模式。
步骤3　需下发人员权限给人脸一体机和门禁控制器。

3.6 人脸门禁设备识别太灵敏，很远就开始识别人脸

在设备的 WEB 端，人脸检测界面，调整瞳距以及、绘制目标检测区域等相关参数。

3.7 人脸门禁设备逆光严重怎么调整

登录设备的 WEB 端调整参数。

说明

老七寸、十寸 v1 一体机无第二路红外参数，只要设置第一路就可以。

室外阳光场景

- 人脸检测：人脸曝光开启，人脸曝光间隔检测时间 10 秒。
- 视频设置：
  - ◇ 第一路彩色：图像，宽动态等级 50。
  - ◇ 第二路红外：图像，宽动态等级 50；曝光，曝光补偿 50。

半室内强逆光场景：

- 人脸检测：人脸曝光开启，其他使用默认配置。
- 视频设置：
  - ◇ 第一路彩色：图像，宽动态等级 50；曝光，曝光补偿 70～80。
  - ◇ 第二路红外：图像，背光补偿；曝光，曝光补偿 65～75。

室内场景

- 人脸检测：使用默认配置。
- 视频设置：
  - ◇ 第一路彩色：使用默认配置。
  - ◇ 第二路红外：图像，宽动态等级 50；曝光，曝光补偿 50。

3.8 人脸门禁设备在室外设备屏幕内部产生雾气

此现象由温差过大造成，设备通电运行一段时间后会自动除雾，后续设备已完善优化此问题。

3.9 一体机插上 U 盘没有反应

首先确认 U 盘是否正常未损坏，其次建议使用 Fat32 格式的 U 盘。

3.10 忘记一体机的密码

说明

此密码泛指设备的 web 端登录密码或设备添加到平台的密码。

- 进入设备端后台，进行恢复出厂设置后，重新设置密码。
  - ◇ 例如：ASI1212D 一体机密码忘记，可输入管理员密码（默认 88888888）进入后台，恢复出厂设置后，重新设置密码。
  - ◇ 七寸或十寸人脸一体机密码忘记，管理员可通过输入管理员密码、刷卡、刷脸等进入设备端后台，出厂设置后，重新设置密码。
- 使用工具进行恢复出厂设置后，重新设置密码。

例如：ASI1212A 一体机密码忘记，可以使用 json 工具进行恢复出厂。

图3-2 ASI1212A

- 使用预留手机号找回密码。

例如：七寸或十寸人脸一体机密码忘记，在浏览器输入设备 IP，进入登录界面，用扫描二维码的方式通过预留的手机号重置密码。

- 联系相关技术人员解决。

3.11 CGI 命令

CGI 命令可以通过在浏览器上输入命令直接修改设备的参数（需要浏览器所在电脑与设备在同一网络下）。

- 功能：开启门禁设备 SSH 使能（true 为开启，false 为关闭）

CGI 命令：http://***设备 IP***/cgi-bin/configManager.cgi?action=setConfig&SSHD.Enable=**true**

- 功能：修改熄屏时间（30 代表 30 秒，十寸 V2 以及之前设备默认为 600 秒）

CGI 命令：http://设备 ip/cgi-bin/configManager.cgi?action=setConfig&GUISet[0].LCDCloseTime=**30**

- 功能：查询单个用户卡号等信息编号

CGI 命令：https://***设备 ip***/cgi-bin/recordFinder.cgi?action=find&name=AccessControlCard&condition.UserID=*用户编号*

- 功能：查询单用户是否有人脸照片

CGI 命令：http://***设备 ip***/cgi-bin/recordFinder.cgi?action=find&name=FaceEigenValue&condition.StrFilePath=/mnt/appdata/FaceImage/*用户编号*.jpg

注意

最前面的 IP 改为需要操作的设备 IP，最后的值输入需要修改或查询的值，输入命令后回车出现弹框，需要输入设备的用户名和密码。

3.12 一体机插上 U 盘没有反应

首先确认 U 盘是否正常未损坏，其次建议使用 Fat32 格式的 U 盘。

3.13 智能门禁设备在智能识别界面出现竖条纹闪动

可能原因

延长线缆质量较差导致阻抗加大，到设备的电压不足导致异常。

解决方法

现场若需改造电源，需测量末端电压是否为 12 V。

3.14 人脸门禁+控制器，人脸设备接韦根没有输出

可能原因

现场没有接 GND。

解决方法

韦跟接 4 根线，D0\D1\LED\CASE。

3.15 智能门禁识别人脸后将识别记录传给 IVSS 失败

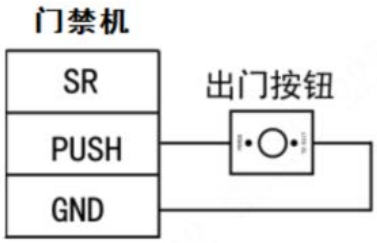
基线设备支持的是设备比对完上报给平台，上报的是 accesscontrol 事件，现场需要的是设备端抓拍到人脸就上报给平台，走的是 facedetection 事件，需要走定制支持。

第 4 章 其他设备

4.1 开门按钮如何连接门禁控制器

连接门禁控制器的 PUSH 和 GND 口。

图4-1 连接示意



4.2 电动移门和控制器如何接线

电动移门使用 220 VDC 供电，将电动移门的开锁信号正负线串联在门禁控制器的 COM 口和 NO 口。

4.3 单通道双向的闸机如何连接门禁控制器

单通道双向的闸机要使用双门门禁控制器 ASC1202B，控制器的 NO1 接闸机左开，控制器的 NO2 接闸机右开，控制器的 COM1 和 COM2 接在闸机的公共端。读卡器接在 1 和 3 的位置上。

4.4 指纹读卡器在阳光照射下自动上报开门记录

光学指纹模块在阳光强照下会影响识别，请调整安装环境或者联系技术支持。

4.5 门禁考勤机是否可配套平台和软件使用

可以。

4.6 双向进出摆闸，在两边刷卡，摆闸摆动方向一致

门禁读卡器的接线位置错误。

遵循右手刷卡原则，两个读卡器应接在读卡器 1 和读卡器 3。

4.7 在 SmartPSS Plus 中下发门组权限时找不到已建好的人员

下发权限绑定的是卡号，需要填写卡号后，才能进行权限下发。

4.8 消费机添加到平台后离线

消费机的子网掩码只能设置成 255.255.255.0。其余掩码暂不支持，否则会出现频繁掉线丢包的情况。

4.9 在读卡器上刷卡没有反应，无事件上报

步骤1　参考配套的安装指导，重新连接读卡器。
步骤2　使用电压表检测读卡器两端电压，确保两端电压在 10 V 以上。
步骤3　检查问题是否已经解决。
　　如果已解决，则完成问题处理，否则请联系相关技术支持。

4.10 ASF809 电插锁正常接线后，加上磁片无法正常开门

ASF809 电插锁的接线与普通电插锁接线不同，需要开门信号通过 12 V 电源和门禁控制器的 COM、NO 口串联，因此，ASF809 电插锁是上电锁开，断电锁关。

4.11 磁力锁出现过吊装条脱落

- 调慢闭门器的关门速度，让门与锁接触时的速度减缓，若门与锁长期碰撞，会导致锁体螺丝松动。
- 把现有吊装条的安装位置后移。
  步骤1　固定吸板位置，关上门。
  步骤2　确定锁体与吸板安装的位置，做好标识。
  步骤3　后移吊装条的位置，避免吸板与锁体碰撞。

4.12 读卡器支持 ID、IC、CPU 卡依次型号是哪些

以设备命名进行区分，-D 代表是支持 ID 卡，-C 代表是支持 CPU 卡，不带后缀的代表为支持 IC 卡

- ID 卡(带-D 的)：ASR1102A-D、DH-ASR1102A-D、DHI-ASR1102A-D、ASR2102A-D。
- IC 卡（不带后缀的）：DH-ASR1102A、ASR1102A、DHI-ASR1102A、ASR2102A。
- CPU 卡（带-C 的）：DH-ASR1102A-C、ASR1102A-C、DHI-ASR1102A-C、ASR2102A-C。

4.13 IC 卡加密的规则，是否能 NFC 复制

目前 IC 卡出厂不加密，可通过手机 NFC 功能复制物理卡号。

若现场涉及到安全性，需要防复制。可以定制程序，升级发卡器和读卡器。

加密后，卡片扇区内容不能被复制。需要卡片扇区和读卡器扇区对应上，才能刷卡，即达到防复制的效果。

4.14 有效卡无法开门

- 检查管理员是否设置了常闭模式，或者处于常闭时间段内；
- 检查电控锁是否正常，检查电源或更换电控锁；
- 检查锁舌与锁扣是否发生机械卡死，修复机械故障或更换零件；
- 查看控制板指示灯，检查门禁控制器与模块之间通讯是否正常，排除通讯故障；
- 检查读卡器是否供电正常，更换供电电源线或单独供电；
- 检查读卡器功能是否正常，更换读卡器；
- 检查读卡器与门禁控制器之间通讯是否正常，更换通讯线；
- 检查是否设置了门禁配置，开启了时间模板高级配置（首卡开门、多人开门、反潜或多门互锁）；
- 检查操作人员是否对门禁系统进行了初始化或者通过其他命令取消门卡授权。

4.15 门禁通讯异常

- 检查串口是否设置错误（确认所使用的串口）；
- 检查门禁通讯线是否存在短路或者断路；
- 检查 RS-485 通讯端口是否损坏；
- 检查网线、水晶头是否完好，检测网线是否畅通，检查网络是否存在时延、抖动或者丢包。

4.16 读卡器无法读卡

- 检查门禁控制器设置，门禁设置是否生效。
- 检查 IC 卡在授权时已做读卡器有效时间段设置（可将 IC 卡权限恢复至默认全天）。
- 检查读卡器供电是否正常，线路是否有断点。
- 检查读卡器是否故障，更换读卡器。
- 检查门禁控制器是否工作正常，更换门禁控制器。

4.17 磁力锁吸合后，门锁震动，吸合不牢固

- 检查磁力锁安装是否牢固，紧固螺钉是否有松动。
- 检查磁力锁吸合面与铁板是否已经完全吸合且无夹杂异物。
- 检查电源适配器电压、电流是否满足要求。

4.18 ASM100-D 无法添加卡片到 DSS 平台

目前 DSS 基线版本不支持添加 ID 卡。

版本支持时，在人员添加界面上方，选择好对应的卡片类型再进行添加卡片的操作。

4.19 ASM202 在 DSS 平台无法添加指纹

现象描述

ASM202 接入到安装有 DSS 的 PC 端，提示驱动存在异常，且在指纹添加界面添加指纹时提示注册失败。

解决方法

在 PC 端安装一个邦融工具，在工具界面将指纹仪打开后即可正常使用。

工具请联系总部技术支持提供。

4.20 吸板放在锁体上，指示灯亮红灯

步骤1　检查吸板是否放在锁体黑色部位。

图4-2 锁体

步骤2　用万用表测亮 V+/V-的电压是否≥10 VDC。

步骤3　检查跳线帽是否正常插好。

步骤4　如以上都没有问题，更换新线路板再测试。

针对双门磁力锁，先把吸合之后显示绿灯的电源断掉，去测试另一边看看是否会变绿灯，如果变绿灯，说明是电压不足，如果还是红灯，说明是线路板出现问题，需要更换线路板。

4.21 磁力锁吸力不足

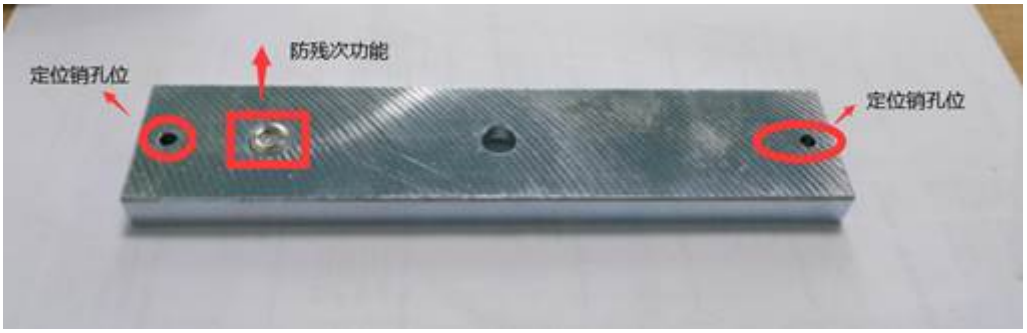
步骤1　检查吸板是否放好。

步骤2　用万用表测量电锁电源电压是否≥9 VDC。

步骤3　检查跳线帽是否正常插好或跳线帽是否有脱落。

步骤4　调整防残次，不要出来太多；吸板不能固定死，要使用定位销。

图4-3 吸板



步骤5　若以上都没有问题，更换新线路板再测试。

4.22 集中控制器上分控离线

- 分控是否是手拉手接，如果不是该种连接方式，需要改为手拉手连接
- 主控和分控的速率需要设置一致。
- 各个分控的编号不能冲突，编号通过拨码区分。
- 主控 WEB 上对分控进行校时。

附录1 法律声明

版权声明

商标声明

- 、、、、HDCVI是浙江大华技术股份有限公司的商标或注册商标。
- ：本声明适用所有产品。如本产品使用 HDMI 技术，词语 HDMI、HDMI High-Definition Multimedia Interface（高清晰度多媒体接口）、HDMI 商业外观和 HDMI 徽标均为 HDMI Licensing Administrator, Inc.的商标或注册商标。本产品已经获得 HDMI Licensing Administrator, Inc.授权使用 HDMI 技术。
- VGA 是 IBM 公司的商标。
- Windows 标识和 Windows 是微软公司的商标或注册商标。
- 在本文档中可能提及的其他商标或公司的名称，由其各自所有者拥有。

责任声明

- 在适用法律允许的范围内，在任何情况下，本公司都不对因本文档中相关内容及描述的产品而产生任何特殊的、附随的、间接的、继发性的损害进行赔偿，也不对任何利润、数据、商誉、文档丢失或预期节约的损失进行赔偿。
- 本文档中描述的产品均“按照现状”提供，除非适用法律要求，本公司对文档中的所有内容不提供任何明示或暗示的保证，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。

出口管制合规声明

大华遵守适用的出口管制法律法规，并且贯彻执行与硬件、软件、技术的出口、再出口及转让相关的要求。就本手册所描述的产品，请您全面理解并严格遵守国内外适用的出口管制法律法规。

隐私保护提醒

您安装了我们的产品，您可能会采集人脸、指纹、车牌等个人信息。在使用产品过程中，您需要遵守所在地区或国家的隐私保护法律法规要求，保障他人的合法权益。如，提供清晰、可见的标牌，告知相关权利人视频监控区域的存在，并提供相应的联系方式。

关于本文档

- 本文档供多个型号产品使用，产品外观和功能请以实物为准。
- 如果不按照本文档中的指导进行操作而造成的任何损失由使用方自己承担。
- 本文档会实时根据相关地区的法律法规更新内容，具体请参见产品的纸质、电子光盘、二维码或官网，如果纸质与电子档内容不一致，请以电子档为准。
- 本公司保留随时修改本文档中任何信息的权利，修改的内容将会在本文档的新版本中加入，

恕不另行通知。

- 本文档可能包含技术上不准确的地方、或与产品功能及操作不相符的地方、或印刷错误，以公司最终解释为准。
- 如果获取到的 PDF 文档无法打开，请使用最新版本或最主流的阅读工具

附录2 网络安全声明和建议

安全声明

- 若您将产品接入互联网需自担风险，包括但不限于可能遭受网络攻击、黑客攻击、病毒感染等，请您加强网络、产品数据和个人信息等的保护，采取保障产品网络安全的必要措施，包括但不限于使用复杂密码、定期修改密码、及时将产品更新至最新版本等。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任何责任，但本公司会提供产品相关安全维护。
- 除非适用法律另有规定，否则因使用或无法使用本产品或服务而引起的任何利润、收入、销售损失、数据丢失或采购替代商品或服务的成本、财产损害、人身伤害、业务中断、商业信息损失，或者任何特殊的、直接的、间接的、附带的、经济性、覆盖性、惩罚性、特殊或从属损害不承担赔偿责任，无论是基于何种责任理论（合同、侵权、过失或其他），本公司及其员工、许可方或附属公司都不承担赔偿责任，即使其已被告知存在此种损害的可能性也是如此。
- 本公司对您的所有损害承担的总责任限额（除了因本公司过失导致人身伤亡的情况，需遵循适用法律规定）不超过您购买本公司产品所支付的价款。

安全建议

保障设备基本网络安全的必须措施：

1. **使用复杂密码**

   请参考如下建议进行密码设置：

   - 长度不小于 8 个字符。
   - 至少包含两种字符类型，字符类型包括大小写字母、数字和符号。
   - 不包含账户名称或账户名称的倒序。
   - 不要使用连续字符，如 123、abc 等。
   - 不要使用重叠字符，如 111、aaa 等。

2. **及时更新固件和客户端软件**

   - 按科技行业的标准作业规范，设备（如 NVR、DVR 和 IP 摄像机等）的固件需要及时更新至最新版本，以保证设备具有最新的功能和安全性。设备接入公网情况下，建议开启在线升级自动检测功能，便于及时获知厂商发布的固件更新信息。
   - 建议您下载和使用最新版本客户端软件。

增强设备网络安全的建议措施：

3. **物理防护**

   建议您对设备（尤其是存储类设备）进行物理防护，比如将设备放置在专用机房、机柜，并做好门禁权限和钥匙管理，防止未经授权的人员进行破坏硬件、外接设备（例如 U 盘、串口）等物理接触行为。

4. **定期修改密码**

   建议您定期修改密码，以降低被猜测或破解的风险。

5. **及时设置、更新密码重置信息**

   设备支持密码重置功能，为了降低该功能被攻击者利用的风险，请您及时设置密码重置相关信息，包含预留手机号/邮箱、密保问题，如有信息变更，请及时修改。设置密保问题时，建

议不要使用容易猜测的答案。

6. **开启账户锁定**

   出厂默认开启账户锁定功能，建议您保持开启状态，以保护账户安全。在攻击者多次密码尝试失败后，其对应账户及源 IP 将会被锁定。

7. **更改 HTTP 及其他服务默认端口**

   建议您将 HTTP 及其他服务默认端口更改为 1024～65535 间的任意端口，以减小被攻击者猜测服务端口的风险。

8. **使能 HTTPS**

   建议您开启 HTTPS，通过安全的通道访问 Web 服务。

9. **MAC 地址绑定**

   建议您在设备端将其网关设备的 IP 与 MAC 地址进行绑定，以降低 ARP 欺骗风险。

10. **合理分配账户及权限**

    根据业务和管理需要，合理新增用户，并合理为其分配最小权限集合。

11. **关闭非必需服务，使用安全的模式**

    如果没有需要，建议您关闭 SNMP、SMTP、UPnP 等功能，以降低设备面临的风险。

    如果有需要，强烈建议您使用安全的模式，包括但不限于：

    - SNMP：选择 SNMP v3，并设置复杂的加密密码和鉴权密码。
    - SMTP：选择 TLS 方式接入邮箱服务器。
    - FTP：选择 SFTP，并设置复杂密码。
    - AP 热点：选择 WPA2-PSK 加密模式，并设置复杂密码。

12. **音视频加密传输**

    如果您的音视频数据包含重要或敏感内容，建议启用加密传输功能，以降低音视频数据传输过程中被窃取的风险。

13. **安全审计**

    - 查看在线用户：建议您不定期查看在线用户，识别是否有非法用户登录。
    - 查看设备日志：通过查看日志，可以获知尝试登录设备的 IP 信息，以及已登录用户的关键操作信息。

14. **网络日志**

    由于设备存储容量限制，日志存储能力有限，如果您需要长期保存日志，建议您启用网络日志功能，确保关键日志同步至网络日志服务器，便于问题回溯。

15. **安全网络环境的搭建**

    为了更好地保障设备的安全性，降低网络安全风险，建议您：

    - 关闭路由器端口映射功能，避免外部网络直接访问路由器内网设备的服务。
    - 根据实际网络需要，对网络进行划区隔离：若两个子网间没有通信需求，建议使用 VLAN、网闸等方式对其进行网络分割，达到网络隔离效果。
    - 建立 802.1x 接入认证体系，以降低非法终端接入专网的风险。
    - 开启设备 IP/MAC 地址过滤功能，限制允许访问设备的主机范围。

更多内容

请访问大华官网安全应急响应中心，获取安全公告和最新的安全建议。

「让社会更安全 让生活更智能」

ENABLING A SAFER SOCIETY AND SMARTER LIVING

浙江大华技术股份有限公司 | 地址：杭州市滨江区滨安路1187号 | 网址：www.dahuatech.com | 服务热线：400-672-8166