门禁一体主机

使用说明书

V1.1.4

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
 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。
 注意	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。
 防静电	表示静电敏感的设备。
 电击防护	表示高压危险。
 激光辐射	表示强激光辐射。
 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
V1.1.4	• 删除前言中的概述。 • 在系统设置的日期设置增加时区设置的说明。	2019.12

重要安全须知

下面是关于产品的正确使用方法、为预防危险、防止财产受到损失等内容，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。

注意

- 请在设备布控后及时修改用户的默认密码，以免被人盗用。
- 请不要将设备放置和安装在阳光直射的地方或发热设备附近。
- 请不要将设备安装在潮湿、有灰尘或煤烟的场所。
- 请保持设备的水平安装，或安装在稳定的场所，注意防止本产品坠落。
- 请勿将液体滴到或溅到设备上，并确保设备上不能放置装满液体的物品，防止液体流入设备。
- 请安装在通风良好的场所，切勿堵塞设备的通风口。
- 仅可在额定输入输出范围内使用设备。
- 请不要随意拆卸设备。
- 请在允许的湿度和温度范围内运输、使用和存储设备。

警告

- 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！
- 更换电池时只能使用同样类型的电池！
- 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 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。
- 如果使用电源插头或器具耦合器等作为断开装置，请保持断开装置可以方便的操作。

特别声明

- 产品请以实物为准，说明书仅供参考。
- 说明书和程序将根据产品实时更新，如有升级不再另行通知。
- 如不按照说明书中的指导进行操作，因此造成的任何损失由使用方自己承担。
- 说明书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。

目录

1 概述

门禁一体主机是一款集读卡、配置和执行为一体的门禁设备，产品外观简洁时尚，适合中高端商业大厦、集团物业和智能社区。

该机具备丰富的功能：

- 触摸按键+液晶显示，TCP/IP 传输协议，支持 3 万张有效卡和 15 万条刷卡记录。
- 支持卡、密码、卡+密码、卡或密码和分时段 5 种开门模式。
- 支持门超时报警、闯入报警、胁迫报警和防拆报警。
- 支持添加来宾卡、胁迫卡、黑白名单和巡逻卡，并支持设定卡片使用有效期限或次数。
- 支持 128 组时间表、128 组时段表以及 128 组假日时段表。

2 设备结构和安装

设备外观、尺寸及安装方法如图 2-1、图 2-2、图 2-3 和图 2-4 所示，尺寸单位为 mm。

图2-1 设备结构 1

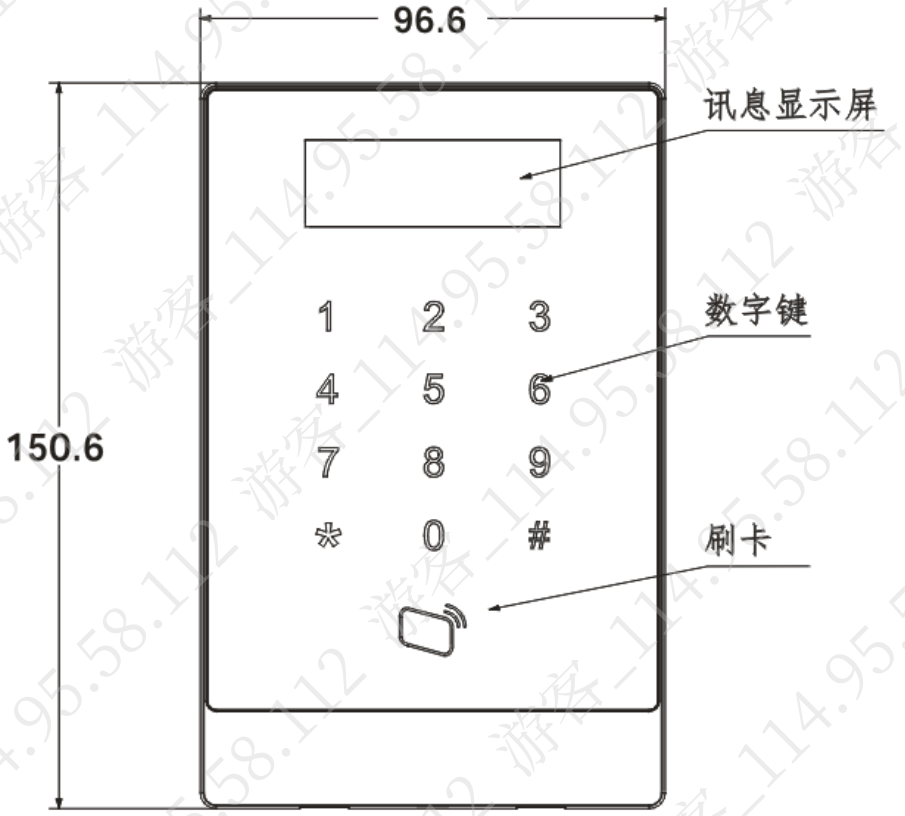


图2-2 设备结构 2

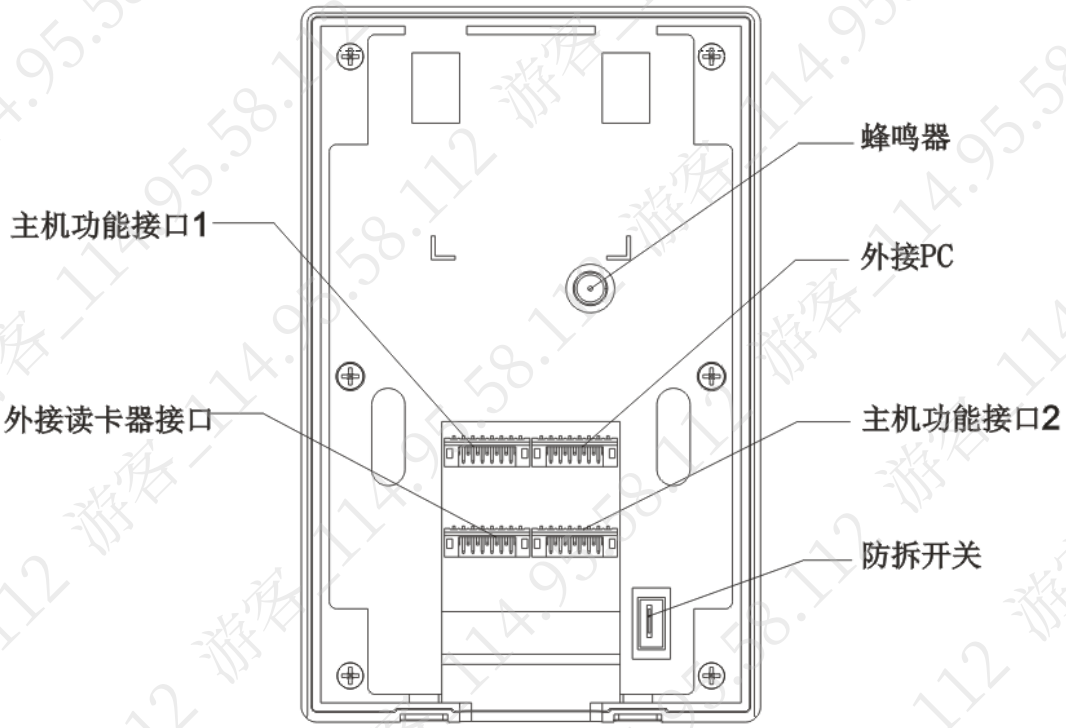


图2-3 设备安装 1

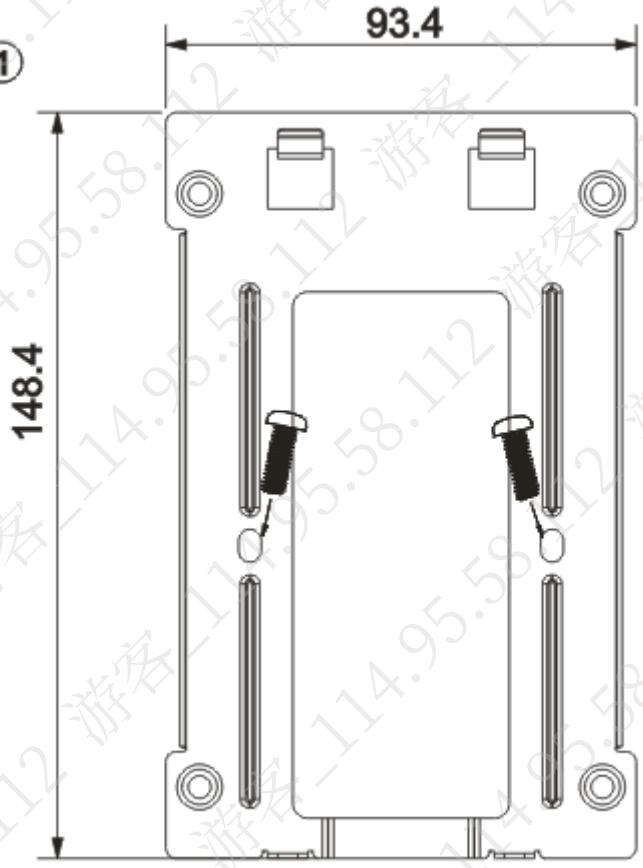
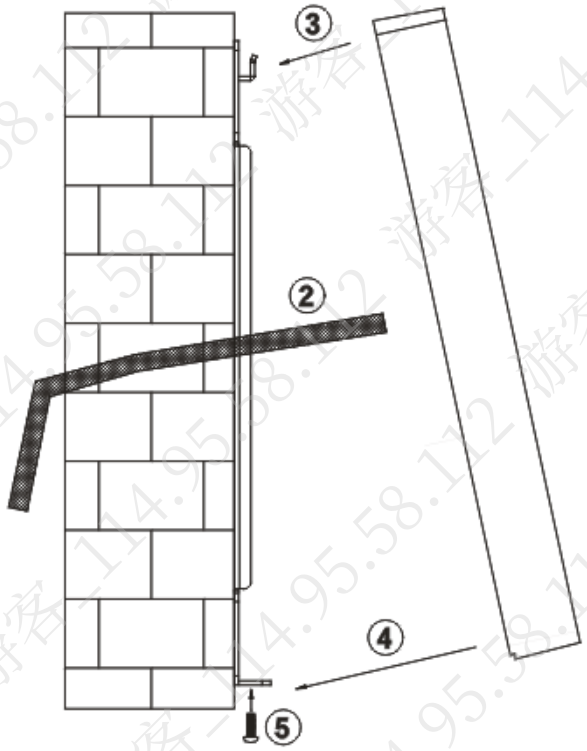


图2-4 设备安装 2



安装步骤如下：

步骤1　将安装支架固定在墙上或 86 盒内。

步骤2　将设备线接上，并将各接线端子插上。

步骤3　设备上方对准安装支架定位卡槽。

步骤4　将设备往安装支架方向密合。

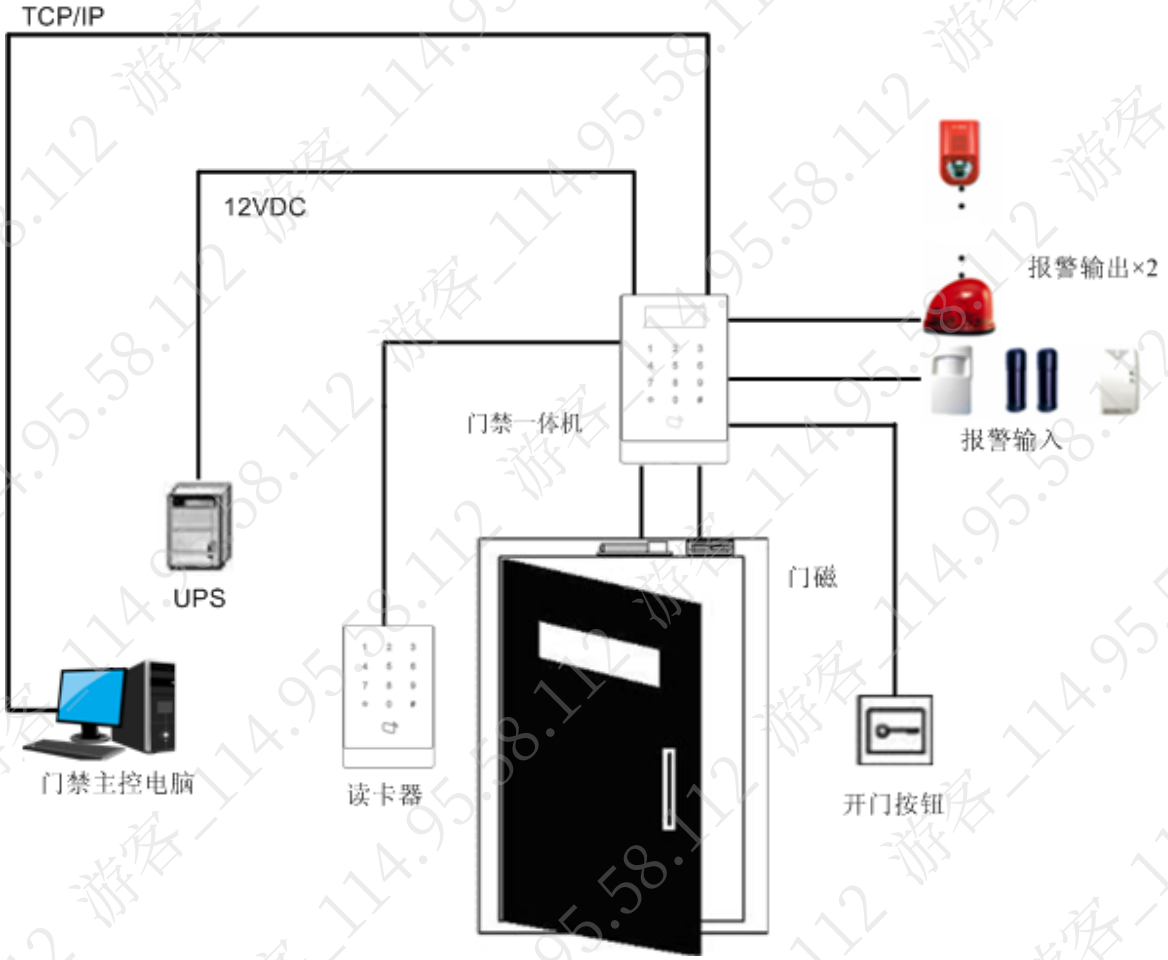
步骤5　将螺丝从下方由底部密合锁上。

3 系统架构

3.1 系统架构图

门禁一体主机与读卡器、报警设备、门禁主控电脑等之间的系统架构图如图 3-1 所示。

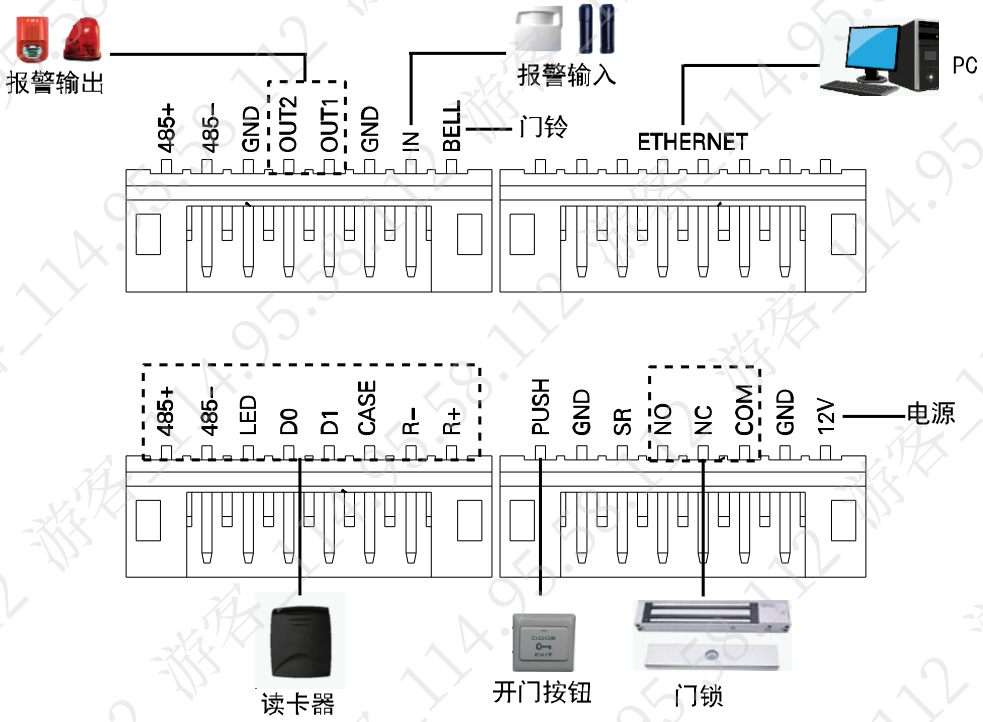
图3-1 系统架构图



3.2 接线示意

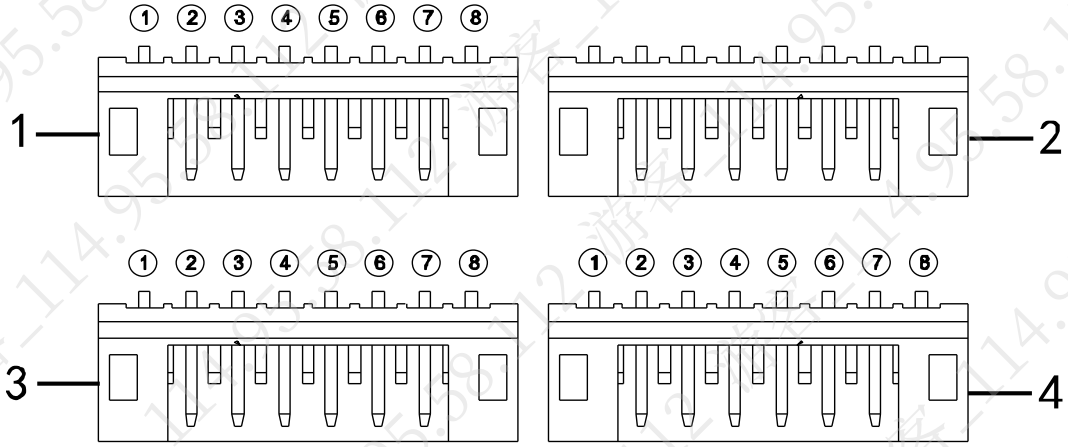
门禁一体主机的接线示意如图 3-2 所示。

图3-2 接线示意图



接线端口如图 3-3 所示。

图3-3 接线端口



序号	端口序号	端口说明
1	① 485+	RS-485+。
	② 485-	RS-485-。
	③GND	接 GND
	③ OUT2	报警输出 2（5V 电平开关量），外接电压不超过 12V。
	④ OUT1	报警输出 1（5V 电平开关量），外接电压不超过 12V。
	⑤ GND	接 GND。
	⑥ IN	报警输入。
	⑦ BELL	门铃控制。
2	—	TCP/IP，网络接口。

序号	端口序号	端口说明
3	① 485+	RS-485+，485 读卡器。
	② 485-	RS-485-，485 读卡器。
	③ LED	LED_OUT，韦根读卡器。
	④ D0	D0，韦根读卡器。
	⑤ D1	D1，韦根读卡器。
	⑥ CASE	读卡器防剪断报警。
	⑦ R-	接 GND。
	⑧ R+	12V 读卡器电源。
4	① PUSH	接开门按钮。
	② GND	接 GND。
	③ SR	门磁检测。
	④ NO	门锁 NO 端。
	⑤ NC	门锁 NC 端。
	⑥ COM	门锁 COM 端。
	⑦ GND	接 GND。
	⑧ 12V	12V 电源输入。

4 功能设置

4.1 登录

登录主界面的步骤如下：

步骤1　插上电源，设备进入开机状态。

步骤2　按【#】键，屏幕显示“工程密码”。

步骤3　输入“工程密码”，并按【#】键，进入主界面。

出厂默认的工程密码为“88888888”。

您可以选择进入“用户管理”、“开门模式”、“时间段设置”、“系统设置”、“系统重启”和“本机信息”6 个一级子菜单进行查询和设置。

- 按【2】数字键，往上选择。
- 按【8】数字键，往下选择。
- 按【#】键，进入或确认。
- 按【*】键，返回或退出。

4.2 用户管理

您可以进行添加或删除卡、密码的操作。

卡类型包括普通卡、VIP 卡、来宾卡、巡逻卡、黑名单卡和胁迫卡。

对这几种卡的介绍如表 4-1 所示。

表4-1 卡类型说明

卡类型	说明
普通卡	普通用户卡。新增普通卡时，系统会提示是否设置卡绑定密码、时间段和有效期。
VIP 卡	VIP 用户卡，在持卡者进入时后台对服务人员提醒。 新增卡时，系统会提示是否设置卡绑定密码、时间段和有效期。
来宾卡	新增来宾卡时，还需要设置卡的使用次数，当超过使用次数后，此卡失效。
巡逻卡	巡逻卡只能在巡逻点进行刷卡记录，不能成功开门。新增卡时，系统会提示是否设置密码、时间段和有效期。
黑名单卡	黑名单卡，在持卡者进入时后台对服务人员提醒。 新增卡时，系统会提示是否设置密码、时间段和有效期。
胁迫卡	胁迫卡在设置胁迫报警后起效，可以正常打开门禁，但系统会产生报警信息上传至管理中心。

说明

所有这些卡刷卡都会上传管理中心，管理平台会根据卡的类型进行处理。

密码用户是通过输入设置的密码进出的用户。

说明

- 卡用户未设置密码，需要将“开门模式”设置为卡开门、卡或密码，才能正常进入。
- 卡用户设置了卡绑定密码，需要将“开门模式”设置为卡开门、卡+密码、卡或密码，才能正常进入。
- 设置了时间段的卡用户，只能在该时间段内，使用正确的开门模式，才能正常进入。
- 密码用户，需要将“开门模式”设置为卡或密码、密码开门，才能正常进入。

4.2.2 新增用户

4.2.2.1 新增单张卡

以新增普通卡为例，新增单张卡的步骤如下：

步骤1 在主界面，通过按【2】键或【8】键，往上或往下选择“用户管理”，并按【#】键。

步骤2 按【2】键或【8】键，往上或往下选择“添加用户”，并按【#】键。

步骤3 按【2】键或【8】键，往上或往下选择“添加卡”，并按【#】键。

步骤4 按【2】键或【8】键，往上或往下选择“单张卡”，并按【#】键。

步骤5 按【2】键或【8】键，往上或往下选择“普通卡”，并按【#】键。

步骤6 使用按键输入卡号或将已开通的卡放在刷卡处进行扫描。

讯息显示屏上会显示新增的卡号。

步骤7 按【#】键。

系统提示“绑定密码？”。

步骤8 根据实际情况选择是或否。

如果选择是，则需要输入密码。

密码位数为 6 位。

如果选择否，系统直接提示“设置时间段？”。

步骤9 按【#】键，设置时间段，再按【#】键。

时间段与“时间段设置”中的“刷卡时间段”一致，具体请参见“4.4.1 刷卡时间段”。

设置完成后，系统提示“设置有效期？”。

步骤10 按【#】键，设置有效期，再按【#】键。

设置完成后，系统提示“是否保存？”。

步骤11 按【#】键，保存设置。

4.2.2.2 新增连续卡

以新增普通卡为例，新增连续卡的步骤如下：

步骤1 在“添加卡”界面，按【2】键或【8】键，往上或往下选择“连续卡”，并按【#】键。

步骤2 按【2】键或【8】键，往上或往下选择“普通卡”，并按【#】键。

步骤3 输入卡数量，并按【#】键。

步骤4 输入首卡的号码或将已开通的首卡放在刷卡处进行扫描，并按【#】键。

系统提示“绑定密码？”。

接下来的步骤，可参见“4.2.2.1 新增单张卡”的“步骤 8～步骤 11”。

4.2.2.3 新增密码用户

新增密码用户的步骤如下：

步骤1 在“添加用户”界面，通过按【2】键或【8】键，往上或往下选择“添加密码”，并按【#】键。

系统显示“序号”和“密码”。

步骤2 输入密码，并按【#】键。

密码必须为 6 位数。

系统提示“是否保存？”。

步骤3 按【#】键，保存设置。

4.2.3 删除用户

4.2.3.1 删除卡用户

您可以删除单张卡、连续卡和所有的卡用户。

删除单张卡的步骤如下：

步骤1 在“用户管理”界面，通过按【2】键或【8】键，往上或往下选择“删除用户”，并按【#】键。

步骤2 按【2】键或【8】键，往上或往下选择“删除卡”，并按【#】键。

步骤3 按【2】键或【8】键，往上或往下选择“单张卡”，并按【#】键。

步骤4 输入要删除的卡号或将要删除的卡放在刷卡处进行扫描，并按【#】键。

系统提示“是否删除？”。

步骤5 按【#】键，删除单张卡。

删除连续卡的步骤如下：

步骤1 在“删除卡”界面上，往上或往下选择“连续卡”，并按【#】键。

步骤2 输入要删除的卡的数量，并按【#】键。

步骤3 输入首卡的卡号或将首卡放在刷卡处进行扫描，并按【#】键。

系统提示“是否删除？”。

步骤4 按【#】键，确认删除。

系统显示删除成功和失败的数量。

删除所有卡的步骤如下：

步骤1 在“删除卡”界面上，往上或往下选择“所有卡”，并按【#】键。

系统提示“是否删除？”。

步骤2 按【#】键，确认删除。

系统提示“删除成功!”。

4.2.3.2 删除密码用户

您可以删除单个密码用户或删除所有的密码用户。

删除单个密码用户的步骤如下：

步骤1 在“删除用户”界面，通过按【2】键或【8】键，往上或往下选择“删除密码”，并按【#】键。

步骤2 按【2】键或【8】键，往上或往下选择“单个密码”，并按【#】键。

步骤3 输入需要删除的密码用户的序号，并按【#】键。

系统提示“是否删除？”。

步骤4 按【#】键，确认删除。

删除所有密码用户的步骤如下：

步骤1 在“删除密码”界面，通过按【2】键或【8】键，往上或往下选择“所有密码”，并按【#】键。

系统提示“是否删除？”。

步骤2　按【#】键，确认删除。

4.3 开门模式

开门模式包括卡开门、密码开门、卡+密码、卡或密码和分时段。

设置步骤如下：

步骤1　在主界面，通过按【2】键或【8】键，往上或往下选择“开门模式”，并按【#】键。
进入开门模式的设置界面。

步骤2　通过按【2】键或【8】键，选择需要设置的开门模式，并【#】键。
选择成功后，开门模式后面会显示“√”。

4.4 时间段设置

您可以设置开门的时间段，包括刷卡时间段、假期时间段和模式时间段。

4.4.1 刷卡时间段

刷卡时间段可设置为 0～127，共 128 个时间段。在每个时间段中，又需要设置周一至周日每天的时间表。当新增卡时，设置了刷卡时间段值，则用户在刷卡开门时，门禁会判断当前时间是否处在时间段设置的值内。

例如设置时间段 1，且时间段 1 中的周一至周日的设置如表 4-2 所示。

表4-2 时间段规划

星期	时间段
周一	0800-2200（有效时间：08:00 到 22:00）。
周二	0800-2200（有效时间：08:00 到 22:00）。
周三	0800-2200（有效时间：08:00 到 22:00）。
周四	0800-2200（有效时间：08:00 到 22:00）。
周五	0800-2200（有效时间：08:00 到 22:00）。
周六	0800-2200（有效时间：08:00 到 22:00）。
周日	0800-2200（有效时间：08:00 到 22:00）。

设置刷卡时间段的步骤如下：

步骤1　在主界面，按【2】键或【8】键，往上或往下选择“时间段设置”，并按【#】键。
进入时间段设置界面。

步骤2　按【2】键或【8】键，选择“刷卡时间段”，并按【#】键。
显示时间段设置界面。

步骤3　输入时间段，并按【#】键。
输入 0～127 之间的任意数字。例如输入 1。
屏幕显示配置周一的时间段。

步骤4　按照“表 4-2 时间段规划”中的规划，修改时间段为 0800-2200，并按【#】键。

步骤5　依次配置周二至周日的时间段。
系统提示“是否保存？”。

步骤6　按【#】键，保存设置。

当新增卡设置了时间段 1，该用户刷卡开门时，根据设置的时间段判断是否开门。只有在规划的时间段内，门禁开门。其他时间开门无效。

说明

默认时间段为全时段有效。

4.4.2 假期时间段

假期时间段可设置为 0～127，共 128 个时间段。当时间进入到 0～127 个假期时间段中的任意一个时间，所有的卡或密码均无法开门。

设置假期时间段的步骤如下：

步骤1　在时间段设置界面，通过按【2】键或【8】键，选择“假期时间段”，并按【#】键。

步骤2　输入时间段，并按【#】键。

输入 0～127 之间的任意数字。例如输入 1。

步骤3　修改起始时间，并按【#】键。

步骤4　修改结束时间，并按【#】键。

系统提示“是否保存？”。

步骤5　按【#】键，保存设置。

4.4.3 模式时间段

模式时间段为门禁在不同时间动态的分配开门模式提供了方法。

模式时间段设置为周一至周日 7 天，每天 4 个时间段。

说明

您需要将“开门模式”配置为分时段模式，此时模式时间段配置的时间才生效。开门模式的配置方法请参见“4.3 开门模式”。

模式时间段设置的步骤如下：

步骤1　在时间段设置界面，通过按【2】键或【8】键，选择“模式时间段”，并按【#】键。

系统显示配置周一至周日的时间段。

步骤2　例如选择“周一”，并按【#】键。

系统显示时间段 1 的界面。

步骤3　配置时间段 1 的时间，按【#】键。

系统显示配置模式界面。

步骤4　按【2】键或【8】键，配置模式 1，按【#】键。

步骤5　依次配置时间段 2、时间段 3 和时间段 4 的时间和模式。

系统提示“是否保存？”。

步骤6　按【#】键，保存设置。

步骤7　依次配置周二至周日的时间段和模式。

例如当前时间是周一时，门禁的开门方式就会根据 4 个时间段进行动态的管理。

4.5 系统设置

您可以在系统设置中进行 IP 设置、通讯设置、日期设置、开锁时间、报警设置、密码修改、母卡

管理和恢复默认。

4.5.1 IP 设置

设置当前门禁设备的 IP 地址、子网掩码和网关。

设置步骤如下：

步骤1　在主界面，通过按【2】键或【8】键，往上或往下选择“系统设置”，并按【#】键。
进入系统设置界面。

步骤2　通过按【2】键或【8】键，选择“IP 设置”，并按【#】键。

步骤3　修改 IP 地址、子网掩码和网关，并按【#】键。
系统提示“是否保存？”。

步骤4　按【#】键，保存设置。

4.5.2 通讯设置

设置当前门禁设备的通讯方式，通讯方式包括 RS485 和 TCP/IP。

设置步骤如下：

步骤1　在“系统设置”界面，通过按【2】键或【8】键，选择“通讯设置”，并按【#】键。

步骤2　通过按【2】键或【8】键，选择通讯方式，并按【#】键。
选择成功后，选项后面会显示“√”。

4.5.3 日期设置

设置当前设备的系统显示日期和时间。

说明

本产品时区配置，请通过配套的软件进行设置。

步骤1　在“系统设置”界面，通过按【2】键或【8】键，选择“日期设置”，并按【#】键。

步骤2　依次设置年、月、日、时、分和秒，并按【#】键。
系统提示“是否保存？”。

步骤3　按【#】键，保存设置。

4.5.4 开锁时间

设置当前设备的开锁时间。

步骤1　在“系统设置”界面，通过按【2】键或【8】键，选择“开锁时间”，并按【#】键。

步骤2　根据取值范围，设置开锁时间，并按【#】键。
系统提示“是否保存？”。

步骤3　按【#】键，保存设置。

4.5.5 报警设置

您可以在“报警设置”中开启或关闭报警，并设置门超时时间。系统报警包括门超时报警、闯入报警、胁迫报警和防拆报警。详细介绍如表 4-3 所示。

表4-3 报警介绍

报警类型	说明
门超时报警	当门禁开门时间大于“门超时时间”时，会产生超时报警。 门超时报警需要设置“门超时时间”，详细信息请参见“4.5.5.2 设置门超时时间”。
闯入报警	未经过刷卡或密码等方式闯入门禁时，会产生闯入报警。
胁迫报警	使用胁迫卡进入，会产生胁迫报警。 新增胁迫卡的方法请参见“4.2.2.1 新增单张卡”。
防拆报警	当门禁设备被拆除，则会触发防拆报警按钮，产生防拆报警。

4.5.5.1 开启报警

以开启闯入报警为例，设置报警的步骤如下：

步骤1　在“系统设置”界面，通过按【2】键或【8】键，选择“报警设置”，并按【#】键。

步骤2　通过按【2】键或【8】键，选择“闯入报警”，并按【#】键。

步骤3　通过按【2】键或【8】键，选择“开启”或“关闭”。

选择成功后，选项后面会显示“√”。

4.5.5.2 设置门超时时间

门超时报警需要设置“门超时时间”，设置步骤如下：

步骤1　在“报警设置”界面，通过按【2】键或【8】键，选择“门超时时间”，并按【#】键。

步骤2　配置时间，并按【#】键。

系统提示“是否保存？”。

步骤3　按【#】键，保存设置。

4.5.6 密码修改

您可以修改系统的工程密码，工程密码的位数为 8 位。

步骤1　在“系统设置”界面，通过按【2】键或【8】键，选择“密码修改”，并按【#】键。

步骤2　输入旧密码，按【#】键。

步骤3　输入新密码，并按【#】键。

步骤4　再次输入新密码，并按【#】键。

系统提示“是否保存？”。

步骤5　按【#】键，保存设置。

4.5.7 母卡管理

您可以使用母卡模式来新增卡用户。

4.5.7.1 母卡修改

母卡修改的步骤如下：

步骤1　在“系统设置”界面，通过按【2】键或【8】键，选择“母卡管理”，并按【#】键。

步骤2　按【2】键或【8】键，选择“母卡修改”，并按【#】键。

步骤3　输入修改的卡号或将卡放在刷卡处进行扫描，并按【#】键。
系统提示“是否保存？”。
步骤4　按【#】键。
系统提示“设置成功!”。

4.5.7.2 母卡增卡

母卡增卡即使用母卡来增加卡用户的方式。使用母卡增加的卡用户与“用户管理”中的相同。
以增加普通卡为例，增卡的步骤如下：
步骤1　在“母卡管理”界面，通过按【2】键或【8】键，选择“母卡增卡”，并按【#】键。
步骤2　通过按【2】键或【8】键，选择“普通卡”，并按【#】键。
系统提示“绑定密码？”。
步骤3　根据实际情况选择是或否。
- 如果选择是，则需要输入密码。
- 如果选择否，系统直接提示“设置时间段？”。

步骤4　按【#】键，设置时间段，再按【#】键。
时间段与“时间段设置”中的“刷卡时间段”一致，具体请参见“4.4.1 刷卡时间段”。
设置完成后，系统提示“设置有效期？”。
步骤5　按【#】键，设置有效期，再按【#】键。
设置完成后，系统提示“请刷母卡”。
步骤6　将母卡在刷卡处进行扫描。
系统提示“母卡模式”。
步骤7　将需要新增的卡放在刷卡处进行扫描。
系统显示“新增成功!”。

4.5.8 恢复默认

您可以将刷卡时间段、假日时间段、模式时间段恢复默认，也可以将所有信息恢复默认。
以恢复刷卡时间段为例，恢复默认的步骤如下：
步骤1　在“系统设置”界面，通过按【2】键或【8】键，选择“恢复默认”，并按【#】键。
步骤2　按【2】键或【8】键，选择“刷卡时间段”，并按【#】键。
系统提示“是否恢复？”。
步骤3　按【#】键，恢复默认。

4.6 系统重启

您可以在“系统重启”下对当前门禁一体主机进行系统重启。
步骤1　在主界面，通过按【2】键或【8】键，选择“系统重启”，并按【#】键。
系统提示“是否重启？”。
步骤2　按【#】键进行重启。按【*】键取消操作。

4.7 本机信息

您可以在“本机信息”下查看当前设备的卡数量、刷卡记录、密码数量、报警记录、通讯方式、IP 地址、MAC 地址和版本信息。

步骤1　在主界面，通过按【2】键或【8】键，选择“本机信息”，并按【#】键。

步骤2　查看卡数量、刷卡记录、密码数量、报警记录、通讯方式、IP 地址、MAC 地址和版本信息。

附录1 法律声明

商标声明

- 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。

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、邮箱、电话、GPS 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。
   - 不包含帐户名称或帐户名称的倒序。
   - 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：

1. **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。

2. **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。

3. **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。

4. **开启帐户锁定**

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

5. **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。

6. **使能 HTTPS**

   建议您开启 HTTPS，通过安全的通道访问 Web 服务。

7. **启用白名单**

   建议您开启白名单功能，开启后仅允许白名单列表中的 IP 访问设备。因此，请务必将您的电脑 IP 地址，以及配套的设备 IP 地址加入白名单列表中。

8. **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。

9. **合理分配帐户及权限**

   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。

10. **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。

11. 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。

12. 使用 PoE 方式连接设备

如果设备支持 PoE 功能，建议采用 PoE 方式连接设备，使摄像机与其他网络隔离。

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。