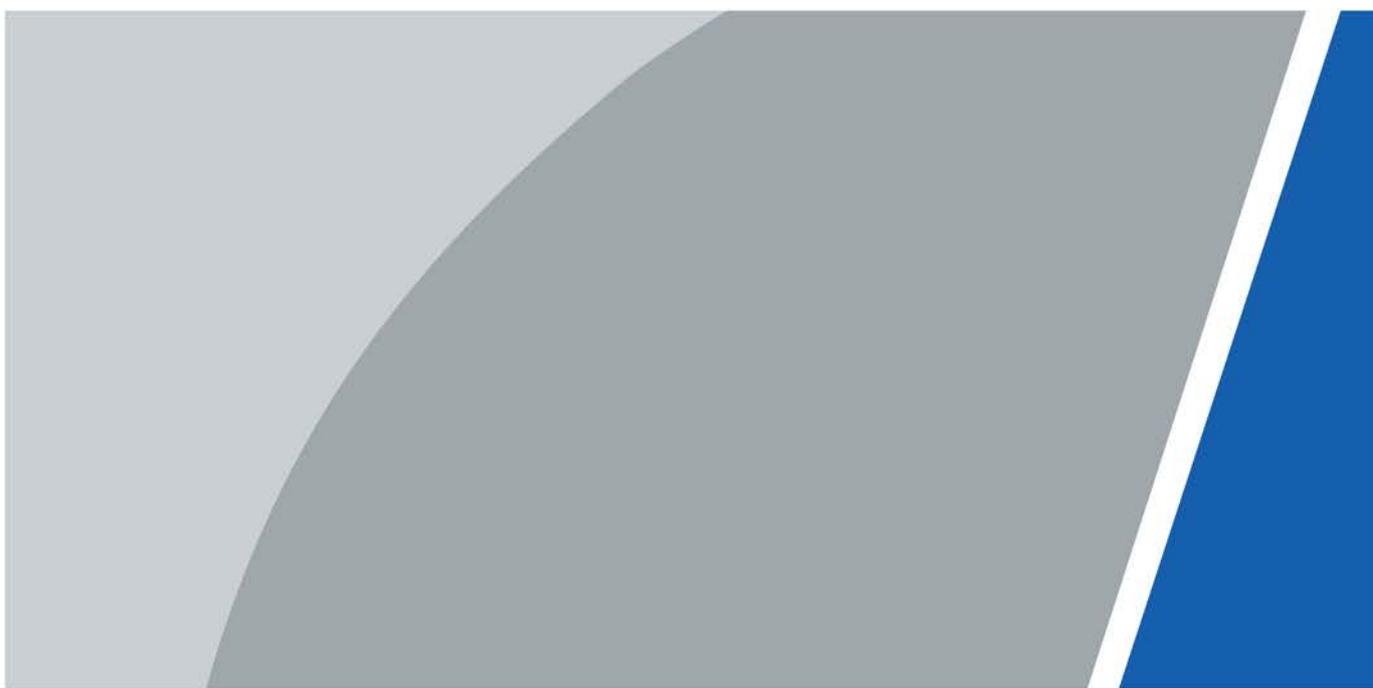


人脸门禁一体主机 使用说明书



前言

本档详细产品的功能及其操作等内容，使用前请仔细阅读，阅读后请妥善保存文档以便日后查阅。

符号约定

在本档中可能出现下列标识，代表的含义如下。

标识	说明
 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。
 说明	表示是正文的附加信息，是对正文的强调和补充。

通用按键

表1 按键说明

按键	说明
	确认键
	将列表翻至第一页
	将列表翻至最后一页
	翻动列表至上一页
	翻动列表至下一页
	返回上一层菜单
	启用
	关闭
	返回待机界面
	搜索
	删除

修订记录

版本号	修订内容	发布日期
V1.0.0	首次发布。	2023.03

使用安全须知

以下是关于产品正确使用的要求，为预防危险、防止财产受到损失，使用产品前请仔细阅读并在使用时严格遵守。

运输要求



请在允许的湿度和温度范围内运输产品。

贮存要求



请在允许的湿度和温度范围内存储产品。

安装要求



- 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



- 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

前言	I
使用安全须知	II
第 1 章 产品概述	1
第 2 章 本地操作	2
2.1 基本配置流程	2
2.2 设备初始化	2
2.3 待机界面	3
2.4 登录主菜单	5
2.5 开门方式	5
2.5.1 卡开门	5
2.5.2 指纹开门	5
2.5.3 用户密码开门	6
2.5.4 管理者密码开门	6
2.5.5 人脸开门	6
2.5.6 二维码开门	6
2.5.7 人证对比开门	6
2.6 人员管理	7
2.6.1 新建用户	7
2.6.2 查看用户和管理员	9
2.6.3 配置管理者密码	10
2.7 门禁管理	11
2.7.1 时间段管理	11
2.7.1.1 配置时段	12
2.7.1.2 配置假日组	13
2.7.1.3 配置假日计划	15
2.7.1.4 配置常开时间段	16
2.7.1.5 配置常闭时间段	16
2.7.1.6 配置远程验证时间段	16
2.7.2 开门模式管理	17
2.7.2.1 任意组合开门	17
2.7.2.2 分时段开门	18
2.7.2.3 多人组合开门	19
2.7.2.4 仅测温模式开门	20
2.7.2.5 人证模式	20
2.7.3 配置报警	21
2.7.4 配置门状态	22
2.7.5 配置门锁保持时间	22
2.8 通讯设置	23
2.8.1 配置网络	23
2.8.1.1 配置IP	23
2.8.1.2 配置主动注册	25
2.8.1.3 配置Wi-Fi	26
2.8.2 配置串口	26
2.8.3 配置韦根	27
2.9 系统设置	28
2.9.1 配置时间	28
2.9.2 配置人脸参数	29

2.9.3	配置图像模式	31
2.9.4	配置补光灯模式	32
2.9.5	配置补光灯亮度	32
2.9.6	配置音量	32
2.9.7	配置指纹参数	33
2.9.8	配置红外亮度	34
2.9.9	恢复出厂设置	34
2.9.10	重启设备	35
2.10	U盘管理	35
2.10.1	导出数据	35
2.10.2	导入数据	36
2.10.3	升级设备	37
2.11	功能设置	37
2.12	查看开门记录	39
2.13	自动测试	40
2.14	系统信息	42
2.14.1	查看数据容量	42
2.14.2	查看设备版本	42
第 3 章	WEB操作	43
3.1	设备初始化	43
3.2	登录	43
3.3	重置密码	44
3.4	报警联动	45
3.4.1	配置报警功能	45
3.4.2	查看报警记录	47
3.5	对讲设置	47
3.5.1	本门口机作为SIP服务器	47
3.5.1.1	配置SIP服务器	47
3.5.1.2	配置本机参数	48
3.5.1.3	添加门口机	49
3.5.1.4	室内机管理	51
3.5.1.4.1	单个添加室内机	51
3.5.1.4.2	批量添加室内机	52
3.5.1.5	添加管理机	53
3.5.1.6	查看在线状态	54
3.5.2	其他门口机作为SIP服务器	55
3.5.2.1	配置SIP服务器	55
3.5.2.2	配置本机参数	56
3.5.3	平台作为SIP服务器	56
3.5.3.1	配置SIP服务器	56
3.5.3.2	配置本机参数	57
3.5.3.3	注册管理	58
3.5.4	查看通话记录	59
3.6	查看数据容量	59
3.7	视频设置	60
3.7.1	配置视频参数	60
3.7.1.1	配置通道1视频参数	60
3.7.1.2	配置通道2视频参数	63
3.7.2	配置动态检测	66
3.7.3	配置图像模式	66
3.7.4	配置局部编码	67

3.8	配置人脸检测.....	68
3.9	网络设置.....	72
3.9.1	配置TCP/IP.....	72
3.9.2	配置端口.....	73
3.9.3	配置主动注册.....	74
3.9.4	配置P2P.....	74
3.9.5	配置4G.....	75
3.10	安全管理.....	77
3.10.1	IP权限.....	77
3.10.1.1	配置网络访问.....	77
3.10.1.2	配置禁止PING.....	78
3.10.1.3	配置防半连接.....	79
3.10.2	配置系统服务.....	79
3.10.2.1	创建服务器证书.....	80
3.10.2.2	下载与安装根证书.....	81
3.11	语音管理.....	82
3.12	用户管理.....	82
3.12.1	添加用户.....	83
3.12.2	添加ONVIF用户.....	83
3.13	自动维护.....	84
3.14	配置管理.....	85
3.14.1	配置文件导入.....	85
3.14.2	配置文件导出.....	85
3.15	系统升级.....	85
3.15.1	文件升级.....	86
3.15.2	在线升级.....	86
3.16	查看版本信息.....	87
3.17	查看在线用户.....	87
3.18	系统日志.....	87
3.18.1	查看系统日志.....	87
3.18.2	查看管理员记录.....	88
3.18.3	查看开门记录.....	88
3.19	查看实时测温数据.....	89
3.20	退出.....	89
第 4 章	SmartPSS Plus.....	90
4.1	登录客户端.....	90
4.2	初始化设备.....	90
4.3	添加设备.....	91
4.3.1	搜索添加.....	92
4.3.2	手动添加.....	93
4.4	添加人员.....	94
4.4.1	设置发卡类型.....	94
4.4.2	单个添加.....	94
4.4.3	批量添加.....	96
附录1	人脸录入/比对说明.....	98
附录2	指纹录入说明.....	101
附录3	对讲功能操作说明.....	102
附录4	扫描二维码说明.....	103
附录5	法律声明.....	104
附录6	网络安全建议.....	105

第 1 章 产品概述

本系列产品是一款新型门禁设备，支持刷卡、人脸、密码、二维码及其组合识别方式。内部集成高性能处理器，身份识别迅速、精准且可离线使用。外观大气时尚，配合管理平台，可实现多种功能，满足使用者多样化的使用需求。

本产品适用于园区、普通写字楼、学校、工厂、普通住宅区等场所。通过识别人脸来核对身份，实现无感化通行。

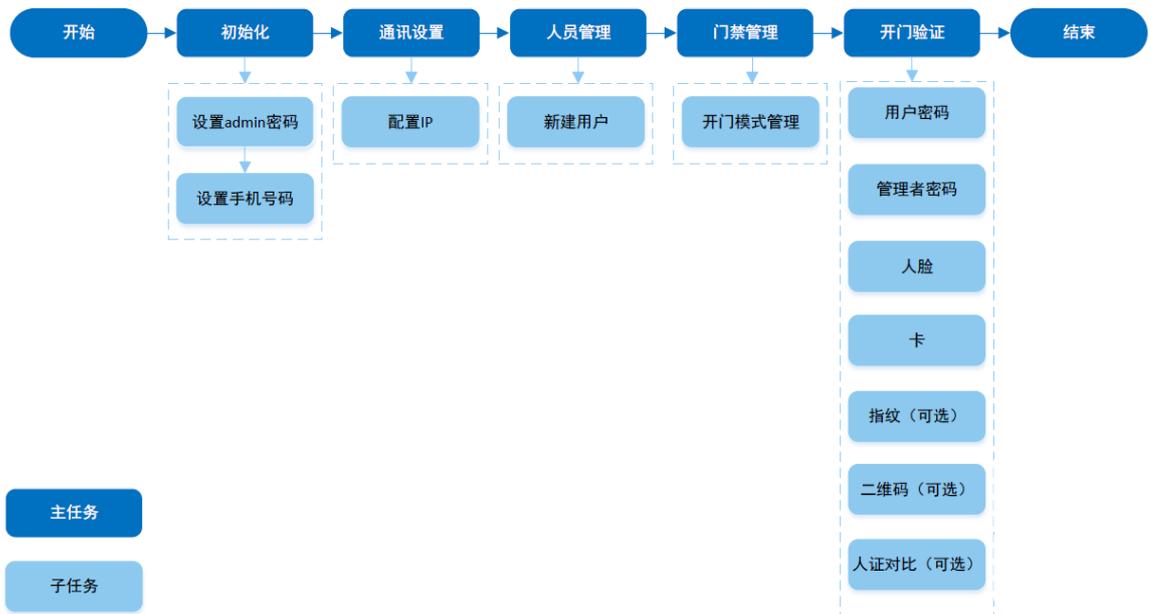
第 2 章 本地操作

- 不同设备本地配置界面不同，具体以实际为准。
- 此处以触摸款为例介绍。

2.1 基本配置流程

根据以下流程完成基本配置。

图2-1 基本配置流程



2.2 设备初始化

设备初次上电启动时，需要设置admin用户密码和手机号。该用户名和密码用于操作设备菜单，或登录配套的WEB端和软件平台。

图2-2 设备初始化



设备初始化

管理员 admin

密码输入

密码确认

手机

确定 清除

说明

- 手机即手机号码，若忘记设备管理员密码，可通过该手机号重置密码。重置密码详细操作请参见“3.3 重置密码”。
- 密码可设置为8位~32位非空字符，可以由大写字母、小写字母、数字和特殊字符（除“'”、“”、”、“;”、“:”、“&”、“空格”、“非打印字符”外）组成，且至少包含2类字符。新密码和确认密码需保持一致。请根据密码强弱提示设置高安全性密码。

2.3 待机界面

在待机界面通过识别人脸、输入密码和扫描二维码开门，并实现可视对讲拨号功能。

说明

待机界面仅供参考，以实际设备显示为准。

图2-3 待机界面



表2-1 待机界面说明

编号	名称	说明
1	开门方式指示	显示当前设备支持的开门方式，最多展示3种。
2	识别区	人脸进入识别区域，识别人脸信息。
3	设备主菜单	进入系统主菜单。仅admin用户和权限类型为管理员的用户可以进入主菜单，进入时需验证信息。 <ul style="list-style-type: none"> ● 管理员用户，验证管理员用户信息。 ● admin用户，输入admin用户密码。
4	密码开门	<ul style="list-style-type: none"> ● 使用管理者密码开门。 ● 使用用户密码开门。

编号	名称	说明
5	二维码开门	按此按钮，将二维码置于屏幕显示扫描框中，实现二维码开门。
6	可视对讲功能	<ul style="list-style-type: none"> ● 本设备作为服务器时，可呼叫室内机和管理机。 ● 平台做服务器时，可呼叫室内机、管理机和平台。 ● 配套云睿社区平台时，只呼叫手机App。
7	温度显示	显示检测的体温。
8	状态显示栏	显示Wi-Fi（如果有）、网络、U盘等状态。
9	显示日期时间	显示当前日期和时间。

2.4 登录主菜单

背景信息

仅admin用户和管理员用户可以进入主菜单，进入时需验证信息。设备首次使用时，需使用admin用户登录主菜单，创建管理员用户。

- admin用户：登录设备本地菜单和WEB界面，无门禁权限。
- 管理员用户：登录设备本地菜单并且有门禁权限。

操作步骤

步骤1 在待机界面，按.

步骤2 选择验证方式。



说明

不同设备验证方式不同，请以实际为准。

- 人脸，选择后管理员用户识别人脸成功后进入主菜单。
- 指纹，选择后管理员用户识别指纹成功后进入主菜单。
- 刷卡，选择后管理员用户识别卡片成功后进入主菜单。
- 密码，选择后输入管理员用户ID和管理员密码，进入主菜单。
- admin，选择后直接输入admin的密码进入主菜单。

2.5 开门方式

2.5.1 卡开门

将已下发的门禁卡放入刷卡区域，即可开门。

2.5.2 指纹开门

将已录入指纹的手指按在指纹区域，即可开门。

2.5.3 用户密码开门

背景信息

使用设置的用户密码开门。

操作步骤

- 步骤1 在待机界面，按.
- 步骤2 按“密码开门”。
- 步骤3 输入“用户ID”和“用户密码”，按“确定”。
验证成功，即可开门。

2.5.4 管理者密码开门

背景信息

通过管理者密码开门。使用管理者密码时，不需要输入用户ID，不受用户限制，不受开门模式、时间段、假日时间、反潜权限限制，只受常闭的门状态限制。



- 使用管理者密码开门时，请确认设备已设置并启用管理者密码，具体请参见“2.6.3 配置管理者密码”。
- 一台设备仅支持设置一个管理者密码。

操作步骤

- 步骤1 在待机界面，按.
- 步骤2 按“管理者密码开门”。
- 步骤3 输入管理者密码，按。
验证成功即可开门。

2.5.5 人脸开门

将已录入的人脸对准设备摄像头采集区域，人脸验证通过即可开门。

2.5.6 二维码开门

设备支持通过两种操作实现二维码开门。

- 按后将二维码置于摄像头前，验证通过后即可开门。
若处于黑暗环境下，在扫描界面按补光灯按钮，手动开启补光灯。
- 直接将二维码置于摄像头前，验证通过后即可开门。

2.5.7 人证对比开门

将开门模式设置为“人证模式”后，采集到的人脸和身份证照片对比成功后开门。

说明

仅具有人证功能的设备支持。

2.6 人员管理

添加用户和查看用户列表。

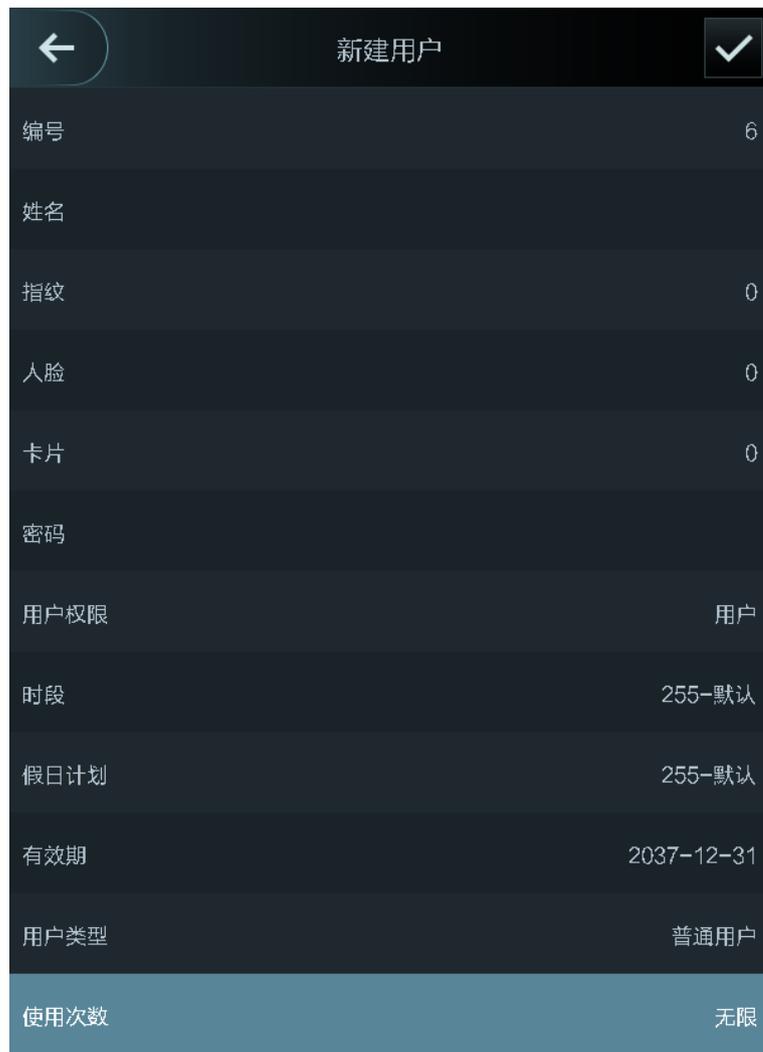
2.6.1 新建用户

通过录入编号、姓名、指纹、人脸等信息添加新用户，并为用户设置权限、有效期等信息。

操作步骤

- 步骤1 登录设备主菜单。
- 步骤2 选择“人员管理 > 新建用户”。
- 步骤3 设置参数项。

图2-4 新建用户



新建用户

编号	6
姓名	
指纹	0
人脸	0
卡片	0
密码	
用户权限	用户
时段	255-默认
假日计划	255-默认
有效期	2037-12-31
用户类型	普通用户
使用次数	无限

表2-2 新建用户参数说明

参数	说明
编号	输入用户编号，用于识别不同的用户，每个编号都是唯一的，最多支持32个字符（包括数字、字母或者数字和字母的组合）。例如：工号。
姓名	输入用户姓名，最多支持10个汉字或者32个字符（包括数字、符号和英文）。
指纹	<p>采集用户指纹，一个用户最多可采集3枚指纹，每枚指纹需要验证3次，请根据语音提示进行操作，完成后提示“登记成功”。</p> <p>选择对应指纹下面的单选框，可将对应指纹设置为胁迫指纹。设备开启胁迫报警后，使用该指纹开门时，将触发胁迫报警。</p> <p> 说明</p> <ul style="list-style-type: none"> • 不建议将第一枚指纹设置为胁迫指纹。 • 仅具有指纹功能的设备支持指纹开门功能。 • 一个用户仅支持设置一枚胁迫指纹。
人脸	注册时请将人脸放置于采集框中心区域，自动完成抓拍，如对抓拍到的图片不满意，则选择重新录入。
卡片	<p>卡片信息，每个用户可以登记5张卡片。在卡片登记界面，输入卡号或在刷卡区刷卡，系统将自动识别该卡卡号。</p> <p>可将卡片设置为胁迫卡片。设备开启胁迫报警后，使用该卡片开门时，将触发胁迫报警。</p> <p> 说明</p> <p>一个用户仅支持设置一张胁迫卡片。</p>
身份证号录入	<p>刷身份证采集身份证号码。</p> <p> 说明</p> <p>仅具有人证功能的设备支持。</p>
密码	<p>开门密码，用户开门时所需输入的密码，密码支持1位~8位数字。</p> <p>开门密码最后一位数字+1即为胁迫密码。设备开启胁迫报警后，使用该胁迫密码开门时，将触发胁迫报警。</p> <p> 说明</p> <p>如设备无触摸功能，需要外接读卡器支持。</p>
用户权限	<p>设置用户权限。</p> <ul style="list-style-type: none"> • 用户，仅有门禁权限。 • 管理员，可登录系统，配置设备相关参数，同时具有门禁权限。
时段	为用户添加门禁时段，在该时段内，用户门禁权限有效。默认值为255，即不为该用户配置任何时段。
假日计划	为用户添加假日时段，在该时段内，用户门禁权限有效。默认值为255，即不为该用户配置任何假日计划。
有效期	设置该人员门禁有效时间。

参数	说明
用户类型	可设置以下类型： <ul style="list-style-type: none"> 普通用户，该类型用户可以正常使用门禁权限。 黑名单用户，该类型用户进入时有黑名单报警。 来宾用户，该类型用户有门禁使用次数的限制，超过使用次数后，门禁权限失效，选择来宾用户后会有来宾卡使用次数设置项显示。 巡逻用户，该类型用户可在任何时间巡逻打卡，但没有门禁权限。 VIP用户，当该类型用户进入时后台对服务人员提醒。 特殊用户，当该类型用户进入时，开门后延迟5 s关门。
使用次数	当用户类型为来宾用户时，可设置该用户门禁权限的使用次数。

步骤4 按  保存。

2.6.2 查看用户和管理员

查询系统内的用户或管理员，并对用户信息或管理员信息修改和删除。

- 用户列表用于显示当前设备中所有的用户信息。
- 管理员列表用于显示当前设备中所有的管理员信息。

登录设备主菜单，选择“人员管理 > 用户列表”或“人员管理 > 管理员列表”，屏幕显示所有用户或管理员信息。

图2-5 用户列表



图2-6 管理员列表



表2-3 用户列表和管理员列表参数说明

参数	说明
识别方式	<ul style="list-style-type: none"> • : 表示人脸方式。 • : 表示指纹方式 • : 表示刷卡方式。 • : 表示密码方式。
用户类型	对应显示该用户的类型。

- 修改用户信息，选择需要修改的用户或管理员，选择对应的参数修改。
- 查询用户，按 ，输入用户编号。
- 删除用户
 - ◇ 选择用户，按 ，删除选择用户。
 - ◇ 在用户列表界面，按 ，删除所有用户（包括管理员用户）。
 - ◇ 在管理员列表界面，按 ，删除所有管理员用户。

2.6.3 配置管理者密码

使用管理者密码时，不用输入用户ID，不受用户类型限制，一台设备仅支持设置一个管理者密码。

操作步骤

- 步骤1 登录设备主菜单。
- 步骤2 选择“人员管理 > 管理者密码”。
- 步骤3 按“管理者密码”，输入密码，按 保存。

图2-7 管理者密码



步骤4 按  开启。

2.7 门禁管理

设置开门模式、报警、门状态和门锁保持时间等。

按“门禁管理”进入门禁管理界面。

图2-8 门禁管理



2.7.1 时间段管理

设置门禁的时间段，包括假日时段、常开时间段和常闭时间段等。

说明

若配置的各时间段时间有重叠，权限优先级为：常开时间段>常闭时间段>其他时间段权限。

图2-9 时间段管理



2.7.1.1 配置时段

用户开门权限在设置的时间段内有效，其他时间开门无效。系统支持0~127，共128个时段配置。在每个时段中，可根据需要设置一周中的时段，每天支持4个时段。

操作步骤

- 步骤1 登录设备主菜单。
- 步骤2 选择“门禁管理 > 时间段管理 > 时段配置”。
- 步骤3 按界面右上角。
新建时段。

图2-10 新建时段



- 步骤4 按对应的参数设置。

图2-11 配置时段参数



表2-4 时段参数说明

参数	说明
编号	输入时段编号，范围为0~127，按 <input checked="" type="checkbox"/> 保存。
时段名称	输入时段名称，最多支持10个汉字或者32个字符（包括数字、符号和英文），按 <input checked="" type="checkbox"/> 保存。
时段配置	配置每日时段。 1. 选择对应星期，按对应时段，输入对应的起始和结束时间。 2. 依次配置其他星期时段，按 <input checked="" type="checkbox"/> 保存。

步骤5 按。

2.7.1.2 配置假日组

将假日分组，为假日组设置不同的假日计划。支持根据需要设置假日组的起止时间段，用户在该时段内，有门禁权限。系统支持0~127，共128个假日组配置，每个假日组支持16个假日。

操作步骤

- 步骤1 登录设备主菜单。
- 步骤2 选择“门禁管理 > 时间段管理 > 假日组配置”。
- 步骤3 按界面右上角。

图2-12 新建假日组



步骤4 按对应的参数设置。

图2-13 配置假日组参数



- 编号：输入假日组编号，范围为0~127，按 保存。
- 假日组名称：输入假日组名称，最多支持10个汉字或者32个字符（包括数字、符号和英文），按 保存。
- 假日组配置
 1. 按“假日组配置”。
 2. 按 ，新建假日。
 3. 设置“序号”、“假日名称”、“开始时间”和“结束时间”，按 保存。

图2-14 添加假日

序号	1
假日名称	
开始时间	2019-09-05
结束时间	2019-09-05

步骤5 按。

2.7.1.3 配置假日计划

将设置好的假日组添加到假日计划中。对所有假日进行统一管理，所有假日期间可按照假日时间段配置关联的时段开启门禁，其余时间则开门无效。

操作步骤

步骤1 登录设备主菜单。

步骤2 选择“门禁管理 > 时间段管理 > 假日计划配置”。

步骤3 按界面右上角。

图2-15 新建假日计划

编号	假日计划名称	假日组编号	操作
----	--------	-------	----

步骤4 按对应参数配置。

图2-16 配置假日计划参数

表2-5 假日计划参数说明

参数	说明
编号	输入假日计划编号，范围为0~127，按保存。
假日计划名称	输入假日计划名称，最多支持10个汉字或者32个字符（包括数字、符号和英文），按 <input checked="" type="checkbox"/> 保存。
假日组编号	输入已经设置的假日组编号，详细介绍请参见“2.7.1.2 配置假日组”。
假日时间段配置	假期期间，在该时段内，用户有门禁权限。支持4个时段，设置完成后，按 <input checked="" type="checkbox"/> 保存。

步骤5 按。

2.7.1.4 配置常开时间段

设置常开时段后，门禁在该时段内一直处于打开状态。

操作步骤

- 步骤1 登录设备主菜单。
- 步骤2 选择“门禁管理 > 时间段管理 > 常开时间段配置”。
- 步骤3 输入预先在“时段配置”中配置好的时段编号，按保存。

2.7.1.5 配置常闭时间段

操作步骤

- 步骤1 登录设备主菜单。
- 步骤2 选择“门禁管理 > 时间段管理 > 常闭时间段配置”。
- 步骤3 输入预先在“时段配置”中配置好的时段编号，按保存。

2.7.1.6 配置远程验证时间段

在该时间段中开门，需要设备端和平台端同时验证成功，才能开门。设备端验证成功后需上报平台，平台确认后下发远程开门指令，完成开门。

操作步骤

- 步骤1 登录设备主菜单。
- 步骤2 选择“门禁管理 > 时间段管理 > 远程验证时间段配置”。
- 步骤3 输入预先在“时段配置”中配置好的时段编号，按保存。
- 步骤4 按启用远程验证时间段。

2.7.2 开门模式管理

根据实际需求设置任意组合开门模式、分时段开门、多人组合开门、仅测温模式或人证模式。所选购的设备型号不同，开门方式会有差异，具体请以实际设备为准。

2.7.2.1 任意组合开门

使用刷卡、指纹、人脸和密码任何一种或者多种组合的方式开门。

操作步骤

- 步骤1 登录设备主菜单。
- 步骤2 选择“门禁管理 > 开门模式管理 > 任意组合开门”。
- 步骤3 选择组合元素。
再次按已选元素，从组合中删去该元素。



说明

组合元素请以实际设备为准。

- 步骤4 选择组合方式。
 - +与，表示和，例如：人脸+密码，表示先人脸，再密码才可以开门。
 - /或，表示或，例如：人脸/密码，表示使用人脸或者密码都可以开门。

图2-17 任意组合开门



步骤5 按保存。

2.7.2.2 分时段开门

不同时段分别设置不同的开门方式。例如：时段一选择人脸开门，时段二选择密码开门。

操作步骤

- 步骤1 登录设备主菜单。
- 步骤2 选择“门禁管理 > 开门模式管理 > 分时段开门”。
- 步骤3 按对应时段，设置时间，在下拉列表框中选择开门方式。
最多支持设置4个时间段，时间段设置不允许跨天，例：22:30~08:00。

图2-18 分时段开门

分时段开门配置

星期日 星期一 星期二 星期三 星期四 星期五 星期六

时段一 卡/指/脸/密

00 : 00 - 23 : 59

时段二 卡/指/脸/密

00 : 00 - 00 : 00

时段三 卡/指/脸/密

00 : 00 - 00 : 00

时段四 卡/指/脸/密

00 : 00 - 00 : 00

步骤4 按 保存。

2.7.2.3 多人组合开门

设置多个用户或者多个用户组授权后才能开门。

操作步骤

步骤1 登录设备主菜单。

步骤2 选择“门禁管理 > 开门模式管理 > 多人组合开门”。

图2-19 多人组合开门

多人组合开门配置

组号	用户列表	开门方式	有效人数(人)

步骤3 按。

图2-20 新建组



表2-6 新建组参数说明

参数	说明
用户列表	在新建组中添加开门授权人员。 1. 按“用户列表”。 2. 按  , 输入已有用户的用户ID。 3. 按  保存。
开门方式	选择开门方式, 包括卡、指纹、人脸和密码。
有效人数	有效人数即授权人数。 <ul style="list-style-type: none">● 若设置了一个组, 则该组内达到有效人数验证成功后即可开门。● 若设置了多个组, 则每个组均需达到有效人数验证成功后方可开门。  说明 有效人数不能大于人员总数。

步骤4 按后按保存。

步骤5 按启用。

2.7.2.4 仅测温模式开门

登录设备主菜单, 选择“门禁管理 > 开门模式管理 > 仅测温模式”。开启后, 无需验证用户权限, 测量人体的温度在正常范围内即可开门。

说明

仅具有测温功能的设备支持。

2.7.2.5 人证模式

说明

仅具有人证功能的设备支持。

登录设备主菜单, 选择“门禁管理 > 开门模式管理 > 人证模式”。

- “/”：表示其中一种方式验证通过即可开门成功。

- “+”：表示需要组合开门，即两种方式都验证通过才能开门成功。
- “人证”：将采集到的人脸与身份证中照片比对。
- “身份证”：采集的身份证号码与系统中的身份证号码比对。

图2-21 人证模式



2.7.3 配置报警

设置门禁异常报警，触发报警后及时通知管理员。

操作步骤

- 步骤1 登录设备主菜单。
- 步骤2 选择“门禁管理 > 报警设置”。
- 步骤3 设置报警参数。

图2-22 报警设置



表2-7 报警设置参数说明

参数	说明
反潜	<p>开启反潜功能后，人员需要先验证进门，再验证出门，否则触发报警。</p> <ul style="list-style-type: none"> ● 若人员已验证进门，但出门时未验证，则再次验证进门时无法开门，且触发报警。 ● 若人员进门时未验证身份，则无法出门并同时触发报警。 <p> 说明</p> <p>单门门禁设备默认本设备验证为进门，外接读卡器为出门，支持通过平台修改配置。</p>
胁迫	使用胁迫卡、胁迫密码、胁迫指纹进入，会产生胁迫报警。
非法卡超次	当同一张未授权卡50 s内连续刷卡5次，第5次刷卡将引发报警。
闯入	门磁打开的情况下，异常开门，会产生闯入报警。
门超时	<p>当门禁开门时间大于“门超时时间”时，会产生超时报警。</p> <p>门超时时间可设置范围为：1 s~9999 s。</p>
门磁启动	开启门磁，仅当门磁开启后，闯入和门超时报警生效。

2.7.4 配置门状态

操作步骤

- 步骤1 登录设备主菜单。
- 步骤2 选择“门禁管理 > 门状态设置”。
- 步骤3 选择门状态，对应状态后面显示表示启用。
- 常开，表示门禁状态为常开，任何情况下不会关闭。
 - 常闭，表示门禁状态为常关，任何情况下不会开启。
 - 正常，表示门禁会按照设置正常开启或关闭。

图2-23 门状态设置



2.7.5 配置门锁保持时间

门锁保持打开状态的时间，超过该时间门锁自动关闭。

操作步骤

- 步骤1 登录设备主菜单。
- 步骤2 选择“门禁管理 > 门锁保持时间”。
- 步骤3 输入门锁保持时间，按  保存。

2.8 通讯设置

配置网络、串口等参数，确保设备能够正常接入网络，串口和韦根通讯正常。



说明

串口和韦根接口会有不同，请以实际设备为准。

2.8.1 配置网络

配置网络，使设备能够正常接入网络，用于WEB访问、与平台对接管理设备。

2.8.1.1 配置IP

配置设备IP地址，使设备接入网络。

操作步骤

- 步骤1 登录设备主菜单。
- 步骤2 选择“通讯设置 > 网络设置 > IP设置”。
- 步骤3 按对应参数进入设置。

图2-24 IP设置



表2-8 IP设置参数说明

参数	说明
IP地址、子网掩码、网关地址	<p>设置设备IP地址、掩码和网关，IP地址和网关必须在同一网段，按保存。</p> <p> 说明</p> <p>仅部分型号支持双网卡。</p>
启/禁用DHCP	<p>DHCP（Dynamic Host Configuration Protocol动态主机配置协议）。</p> <p>启用DHCP功能，当网络中有DHCP服务器时，可自动获取IP地址，此时“IP地址”、“子网掩码”和“网关地址”不可设。</p>
云睿使能	<p>开启后接入云睿平台，支持通过远程连接门禁设备。默认开启。</p> <p>启用云睿使能，P2P一直开启；禁用云睿使能，支持手动开启或者关闭P2P使能。</p> <p>门禁设备正常接入外网后，手机安装配套App，扫描二维码添加设备。</p>

参数	说明
P2P	启用P2P功能，使用时无需申请动态域名、端口映射或部署中转服务器，即可管理设备。  说明 开启P2P后显示二维码。

步骤4 按。

2.8.1.2 配置主动注册

背景信息

通过主动注册功能，设备可以对接管理平台，通过管理平台管理设备。



注意

由于管理平台可清空人员配置并将设备初始化，请注意维护管理平台相关权限，以免操作不当，导致数据丢失。

操作步骤

- 步骤1 登录设备主菜单。
- 步骤2 选择“通讯设置 > 网络设置 > 主动注册”。
- 步骤3 按对应参数进入设置，按保存。

图2-25 主动注册



表2-9 主动注册参数说明

名称	参数
服务器IP地址	管理平台的IP地址。
端口	管理平台的端口号。
子设备ID	自定义，与服务器端的注册ID保持一致。

步骤4 按启用。

2.8.1.3 配置Wi-Fi

背景信息

通过无线网络将设备接入到网络。



仅具有Wi-Fi模块的设备支持此功能。

操作步骤

- 步骤1 登录设备主菜单。
- 步骤2 选择“通讯设置 > 网络设置 > Wi-Fi”。

图2-26 Wi-Fi



- 步骤3 按 ，开启Wi-Fi功能。
- 步骤4 按 ，搜索Wi-Fi。
- 步骤5 选择Wi-Fi，输入密码，按 保存。
- 步骤6 若没有搜索到Wi-Fi，按“SSID”，手动输入Wi-Fi名称。

2.8.2 配置串口

操作步骤

- 步骤1 登录设备主菜单。
- 步骤2 选择“通讯设置 > 串口设置”。
- 步骤3 根据连接设备的用途，选择RS-485接口类型。

图2-27 串口设置



- 串口输入：本机外接读卡器设备，识读卡片信息。
- 串口输出：本机作为识读设备，将门禁控制信息输出给门禁控制器，控制开门或关门。
 - ◇ 编号，若选择编号，则按照用户的编号，输出对应数据。
 - ◇ 卡号，若选择卡号，使用刷卡方式验证时，输出对应的刷卡数据；使用其他方式验证时，按照用户第一张卡卡号，输出对应数据。
- OSDP输入：本机外接OSDP协议读卡器设备，识读卡片信息。

2.8.3 配置韦根

背景信息

根据连接设备的用途，选择韦根输入输出方式。

- 当外接其他识读设备时，选择“韦根输入设置”。
- 当设备本身作为识读设备时，选择“韦根输出设置”，可接入控制器或一体机设备。

操作步骤

步骤1 登录设备主菜单。

步骤2 选择“通讯设置 > 韦根设置”。

步骤3 选择韦根类型。

- 韦根输入设置：外接其他识读设备。
- 韦根输出设置：设备本身作为识读设备，外接控制器或其他一体机设备。

图2-28 韦根输出设置



表2-10 韦根输出设置参数说明

参数	说明
韦根输出类型	<p>即设备能够识别的输出卡号或者编号的位数。</p> <ul style="list-style-type: none"> • 韦根26，识别3个字节，6位。 • 韦根34，识别4个字节，8位。 • 韦根66，识别8个字节，16位。
脉冲宽度	设置韦根输出的脉冲宽度和间隔。
脉冲间隔	
输出数据类型	<p>获取数据的类型。</p> <ul style="list-style-type: none"> • 编号，若选择编号，则按照用户的编号，输出对应数据。 • 卡号，若选择卡号，则按照用户第一张卡的卡号，输出对应数据。

2.9 系统设置

2.9.1 配置时间

通过时间设置功能，根据使用习惯设置系统日期、时间显示格式，夏令时和NTP校时等。

操作步骤

- 步骤1 登录设备主菜单。
- 步骤2 选择“系统设置 > 时间设置”。
- 步骤3 设置参数。

图2-29 时间设置



表2-11 时间设置参数说明

参数	说明
24小时制	开启后，时间按照24小时制显示，否则按照12小时制显示。
日期设置	<ol style="list-style-type: none"> 1. 按“日期设置”。 2. 输入年月日。 3. 按 <input checked="" type="checkbox"/> 保存。
时间设置	<ol style="list-style-type: none"> 1. 按“时间设置”。 2. 输入时间。 3. 按 <input checked="" type="checkbox"/> 保存。
日期格式	<ol style="list-style-type: none"> 1. 按“日期格式”。 2. 在弹出的界面中按文本框，选择日期格式，包括日-月-年、年-月-日、月-日-年可选。 3. 按 <input checked="" type="checkbox"/> 保存。
夏令时设置	<p>当设备所在地实行夏令时时，需要启用夏令时。开启夏令时后，时间在标准时间上加一。例：标准时间为10:00，开启夏令时后，时间变为11:00。</p> <ol style="list-style-type: none"> 1. 按“夏令时设置”。 2. 按 <input checked="" type="checkbox"/> 启用。 3. 按“夏令时类型”，选择按周或者按日期。 4. 按“开始时间”和“结束时间”，设置时间。
NTP校时	<p>设置NTP校时功能。</p> <ol style="list-style-type: none"> 1. 按“NTP校时”。 2. 设置参数，按 <input checked="" type="checkbox"/> 保存。 <ul style="list-style-type: none"> ● 服务器IP地址，填写校时服务器的IP地址，设备将按照该服务器校时。 ● 端口，填写校时服务器的端口号。 ● 间隔（min），设置校时的间隔时间。 3. 按 <input checked="" type="checkbox"/> 启用。
时区	根据当地时区选择。

2.9.2 配置人脸参数

背景信息

通过设置人脸参数可以改变设备识别人脸的精准度，提升门禁防护能力。



注意

该参数建议由专业人员调试使用。

操作步骤

- 步骤1 登录设备主菜单。
- 步骤2 选择“系统设置 > 人脸参数设置”。
- 步骤3 按对应参数进入设置，按 保存。

图2-30 人脸参数设置



表2-12 人脸参数说明

参数	说明
人脸识别阈值	设置人脸比对时的阈值。阈值越大，识别人脸时误识率越低，同时识别成功率越低。
人脸识别最大偏角	设置设备拍摄人侧脸的角度。数值越大，识别的侧脸范围越大。
眼间距	双眼之间的像素值，与人脸大小、人脸与镜头距离相关。比如：一般成年人距离镜头1.5 m时，眼间距为50像素~70像素。
有效人脸间隔时间	设置同一有权限人员在同一台设备上识别，重复提示识别成功的间隔时间。
无效人脸间隔时间	设置同一无权限人员在同一台设备上识别，重复提示识别失败的间隔时间。
防假使能	开启后，防止使用有权限人员的照片、模型等冒用人脸信息情况的发生。默认为“普通”。
人证阈值	<p>将采集到的人脸与身份证中照片比对，阈值越大，要求人脸相似度越大，识别成功率越低。</p> <p> 说明</p> <p>仅具有人证功能的设备支持。</p>
安全帽检测使能	<p>开启后可检测人员是否佩戴安全帽。</p> <p> 说明</p> <ul style="list-style-type: none"> 仅部分非测温设备支持此功能。 与口罩检测使能互斥。

参数	说明
测温参数	<ul style="list-style-type: none"> ● 体温测量：启用后，可检测体温温度。 ● 测温区域框：启用后，显示人脸测温区域框。 ● 测温距离（厘米）：默认设置为150 cm，如果设置为其他值时，则支持定点测温，距离以设置值为主，如果定点测温，建议设置80 cm。 ● 测温矫正时长（毫秒）：设置时间值，检测时间超过这个时间阈值，本次测温结束。显示屏将提示：未获取温度，请靠近测温。 ● 高温阈值：设置温度值，大于等于这个温度判断为高温。 ● 温度最大值：设置测量的最高体温值。默认为45 °C。 ● 温度最小值：设置测量的最低体温值。默认为35 °C。 ● 温度矫正值：调试参数。由于测温环境差异，被测者温度可能会产生误差。调试时可选择多个被测样本站在测温距离，根据测量值和实际值比较，通过此参数修正。例如测量温度比实际值低0.5 °C，此处矫正值设置为0.5 °C；如果测量温度比实际值高0.5 °C，此处矫正值设置为-0.5 °C。 ● 温度单位：分为°C（摄氏温度）和°F（华氏温度）。 <p> 说明</p> <p>仅具有测温功能的设备支持。</p>
口罩参数	<ul style="list-style-type: none"> ● 口罩模式 <ul style="list-style-type: none"> ◇ 不检测：检测人脸时不检测是否戴口罩。 ◇ 口罩提醒：识别人脸时，当检测到人员未戴口罩，界面及语音提示“请戴口罩”，允许通行。 ◇ 口罩拦截：识别人脸时，当检测到人员未戴口罩，界面及语音提示“请戴口罩”，且禁止通行。 ● 口罩识别阈值：设置识别口罩功能的强度值。默认为75。 <p> 说明</p> <p>与安全帽检测使能互斥。</p>

2.9.3 配置图像模式

操作步骤

步骤1 登录设备主菜单。

步骤2 选择“系统设置 > 图像模式一键设置”。

步骤3 根据实际安装环境，选择图像模式。

- 室内：设备位于室内环境且图像中不含室外环境或室外环境占比较小的场景，此类场景无日光照明，光源多为人造光源且空间亮度较均匀。
- 室外：光源为日光，亮度较高且亮度较均匀。
- 其他，过道、半户外等逆光场景。

图2-31 图像模式一键设置



2.9.4 配置补光灯模式

操作步骤

- 步骤1 登录设备主菜单。
- 步骤2 选择“系统设置 > 补光灯模式设置”。
- 步骤3 根据实际使用环境，选择补光灯模式。

图2-32 补光灯模式



2.9.5 配置补光灯亮度

操作步骤

- 步骤1 登录设备主菜单。
- 步骤2 选择“系统设置 > 补光灯亮度设置”。
- 步骤3 按 **+** 或 **-** 调节亮度。

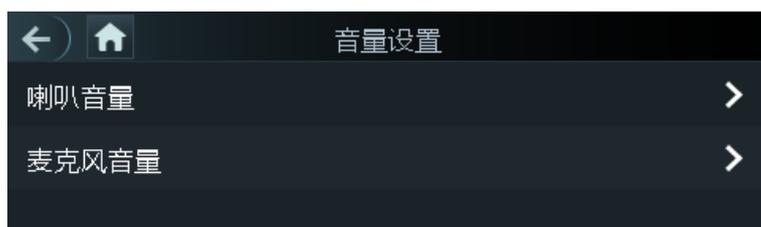
2.9.6 配置音量

根据实际的使用需求，调节设备语音播报的音量大小。

操作步骤

- 步骤1 登录设备主菜单。
- 步骤2 选择“系统设置 > 音量设置”。
- 步骤3 按“喇叭音量”或“麦克风音量”。

图2-33 音量设置



步骤4 按 **+** 或 **-** 调节音量。

2.9.7 配置指纹参数

背景信息

请根据实际情况设置指纹识别精度，数值越大指纹比对精度越高，误识率越低，同时通过率也降低。

说明

仅指纹款设备显示此设置。

操作步骤

- 步骤1 登录设备主菜单。
- 步骤2 选择“系统设置 > 指纹参数设置”。
- 步骤3 按 **+** 或 **-** 调节阈值等级。

图2-34 指纹参数设置



2.9.8 配置红外亮度

根据实际画面设置红外摄像头的亮度，红外摄像头主要用于实现活体检测。

操作步骤

- 步骤1 登录设备主菜单。
- 步骤2 选择“系统设置 > 红外亮度设置”。
- 步骤3 按**+**或**-**调节亮度。

2.9.9 恢复出厂设置



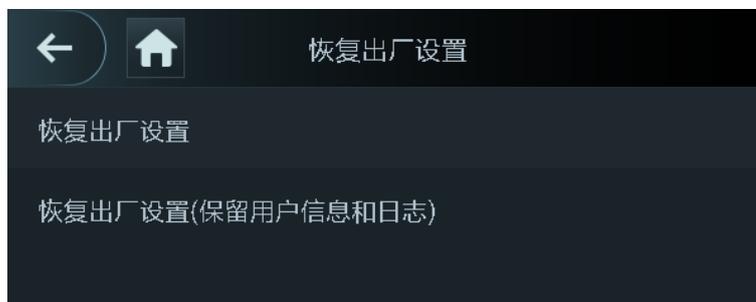
注意

执行恢复出厂设置，会导致数据丢失，请谨慎操作。

对设备恢复出厂默认设置并根据需要选择是否保留用户信息和日志。

- 恢复出厂设置：恢复人员在内的所有设置，设备信息、人员信息等将被清空。
 - 恢复出厂设置（保留用户信息和日志）：除用户信息和日志，其他配置均恢复到出厂设置。
- 登录设备主菜单，选择“系统设置 > 恢复出厂设置”。选择恢复出厂设置的方式并按“确认”。

图2-35 恢复出厂设置



2.9.10 重启设备

登录设备主菜单，选择“系统设置 > 重启设备”，按“确定”确认重启，对设备执行重启操作。

2.10 U盘管理

将用户信息导出/导入至U盘中，也可以通过U盘对系统执行升级操作。

说明

- 导入/导出用户信息和升级前请确认已插入U盘，导入/导出或者升级过程中请勿拔出U盘或者执行其他操作，否则将导致导入/导出信息或者升级失败。
- U盘的导入，需先从其他设备中导出数据，再将该数据导入设备，不支持直接通过USB导入人脸照片。

2.10.1 导出数据

插入U盘后，将设备中的数据导出到U盘中，导出的数据受加密保护，不可编辑。

操作步骤

- 步骤1 登录设备主菜单。
- 步骤2 选择“U盘管理 > U盘导出”。
- 步骤3 选择需要导出的信息。

图2-36 U盘导出



步骤4 按“确定”，确认导出信息。
导出的信息将保存到U盘中。

2.10.2 导入数据

仅支持从一个设备中导出的数据，导入到另一台设备中。

操作步骤

- 步骤1 登录设备主菜单。
- 步骤2 选择“U盘管理 > U盘导入”。
- 步骤3 选择需要导入的信息。

图2-37 U盘导入



- 步骤4 按“确定”，确认导入信息。
将U盘中的信息导入到设备中。

2.10.3 升级设备

通过U盘对系统执行升级操作。

操作步骤

- 步骤1 将升级文件重命名为“update.bin”，存放在U盘根目录下，将U盘插入设备。
- 步骤2 登录设备主菜单。
- 步骤3 选择“U盘管理 > U盘升级”。
- 屏幕显示“确认升级”。
- 步骤4 按“确定”。
- 系统开始升级，升级完成后自动重启设备。

2.11 功能设置

登录主菜单界面，按“功能设置”。

说明

不同设备界面显示不同，具体以实际为准。

图2-38 功能设置



表2-13 功能设置

参数	说明
隐私设置	<ul style="list-style-type: none"> ● 密码重置：开启密码重置功能，用户可重置密码。默认开启。 ● HTTPS使能：HTTPS协议用于为HTTP数据传输建立安全的信息传输通道。HTTPS开启后，使用HTTPS协议访问CGI命令，否则将使用HTTP访问。 <p> 说明</p> <p>当开启HTTPS使能后，设备将会重启。</p> <ul style="list-style-type: none"> ● CGI使能：CGI是公共网关接口，用于外部应用程序与WEB服务器间的数据通信。CGI开启后，可正常使用对应CGI命令。默认开启。 ● SSH使能：SSH协议是用于远程登录会话和网络服务提供安全保障的协议。SSH开启后，为数据传输提供加密服务。 ● 指纹图像：开启指纹图像，指纹开门时显示指纹。 <p> 说明</p> <p>仅指纹款设备支持。</p> <ul style="list-style-type: none"> ● 抓拍功能：开启抓图功能，开门时设备自动抓拍图片；本功能默认开启。 ● 删除所有抓拍照片：删除开门时设备自动抓拍到的所有图片。
卡号反转	用韦根输入对接第三方设备时，获取的卡号顺序与实际卡号顺序不一致时，可开启该功能。

参数	说明
门控安全模块	门控安全模块启用时，本设备的开门按钮、锁控制和消防联动开门均无效。
外接读卡器测温	启用后，使用外接读卡器开门时会进行测温。  说明 仅具有测温功能的设备支持。
门磁类型	设置门磁状态。 <ul style="list-style-type: none"> ● 常开：门磁信号线断开表示门开。 ● 常闭：门磁信号线短路表示门开。
提示功能	根据需求设置验证开门时待机界面显示模式。默认为极速模式。 <ul style="list-style-type: none"> ● 极速模式：待机界面仅显示“验证成功”或“未授权”。 ● 简易模式： <ul style="list-style-type: none"> ◇ 验证成功时，待机界面显示人员编号、姓名和验证时间。 ◇ 验证失败时，待机界面显示“未授权”和验证时间。 ● 标准模式： <ul style="list-style-type: none"> ◇ 验证成功时，待机界面显示底库照片、人员编号、姓名和开门时间。 ◇ 验证失败时，待机界面显示“未授权”和验证时间。 ● 对比模式： <ul style="list-style-type: none"> ◇ 验证成功时，待机界面左侧显示现场抓拍照片，右侧显示底库照片，并在下方显示人员编号、姓名和验证时间。 ◇ 验证失败时，待机界面显示“未授权”和验证时间。
语音管理	选择验证成功的语音提示。

2.12 查看开门记录

通过记录管理功能，查询所有用户的开门记录。

操作步骤

- 步骤1 登录设备主菜单。
- 步骤2 选择“记录管理 > 开门记录查询”。

图2-39 开门记录

编号	姓名	时间	结果	识别方式
1	admin1	09-07 10:35	成功	卡
1	admin1	09-07 09:26	成功	人脸
1	admin1	09-07 09:26	成功	人脸
1	admin1	09-07 09:26	成功	人脸
2	test1	09-07 09:26	成功	人脸
1	admin1	09-07 09:26	成功	人脸
1	admin1	09-07 09:25	成功	人脸
2	test1	09-07 09:25	成功	人脸
3	test2	09-07 09:25	成功	人脸
		09-06 17:25	失败	人脸
		09-06 17:10	失败	人脸
		09-06 16:52	失败	人脸

2.13 自动测试

用户初次购买设备或当设备遇到故障时，通过自动测试，检查设备基础功能是否正常。请按屏幕提示进行测试操作。

图2-40 自动测试



表2-14 自动测试

测试项	说明
屏幕测试	用于测试设备屏幕显示是否正常。
语音测试	用于测试设备语音是否正常。
按键测试	用于测试设备屏幕触摸是否正常。
指纹测试	用于测试设备指纹功能是否正常。  说明 仅指纹款支持。
图像测试	用于测试设备录入图像功能是否正常。
时钟测试	用于测试设备钟点计时功能是否正常。
自动测试	选择自动测试时，设备顺序自动执行上述所有测试项目。
设备自检	设备自动完成RTC时钟、网卡、指纹芯片和摄像头的检测，并显示检测结果是否正常。

2.14 系统信息

查询设备存储的数据信息和设备版本。

2.14.1 查看数据容量

登录设备主菜单，选择“系统信息 > 数据容量”，可查看设备存储的用户、卡片、指纹、人脸等数据情况。

2.14.2 查看设备版本

登录设备主菜单，选择“系统信息 > 设备版本”，查看设备序列号、MAC地址、软件版本等信息。

第 3 章 WEB操作

本设备支持在WEB端配置和操作，通过WEB可以配置设备的网络参数、视频参数、门禁参数等，轻松实现对设备的维护和升级。

不同设备WEB界面略有不同，请以实际设备为准。

3.1 设备初始化

设备首次使用或恢复出厂后登录WEB界面，需要初始化设备。

前提条件

PC与设备在同一局域网内。

操作步骤

步骤1 打开浏览器，在地址栏里输入设备的IP地址（默认地址为192.168.1.108），按【Enter】键。



说明

推荐使用最新版谷歌或火狐浏览器。

步骤2 按照提示完成初始化设置，设置密码和手机号码。



说明

- 为确保设备安全，设备初始化后请妥善保存admin的登录密码，并定期修改。
- 手机号码用于重置密码时接收安全码。

3.2 登录

操作步骤

步骤1 打开浏览器，在地址栏里输入设备的IP地址，按【Enter】键。

步骤2 输入“用户名”和“密码”。

图3-1 登录



说明

- 设备默认管理员用户名为admin，密码为设备初始化时设置的登录密码。为确保安全，建议您定时更改管理员密码，并妥善保存。
- 如果您遗忘admin的登录密码，可单击“忘记密码？”重置，详细介绍请参见“3.3 重置密码”。

步骤3 单击“登录”。

3.3 重置密码

若忘记admin用户的登录密码时，可以通过预留手机重置密码。

操作步骤

- 步骤1 在登录界面，单击“忘记密码”。
- 步骤2 在弹出的提示窗口，单击“确定”。
- 步骤3 根据界面提示扫描二维码，并获取安全码。

图3-2 重置密码



注意

- 扫描同一个二维码最多可获取两次安全码，如需再次获取安全码，请刷新二维码扫描界面。
- 预留手机接收到安全码后，请在24小时内使用安全码重置密码，否则安全码将失效。
- 安全码连续输错5次后，该账号将被锁定5分钟。

步骤4 在“请输入安全码”文本框中输入接收到的安全码。

步骤5 单击“下一步”。

步骤6 重新设置“新密码”和“确认密码”。

密码可设置为8位~32位可见字符，且至少包含数字、字母和常用字符中的两种（除“空格”、“!”、“”、“;”、“:”、“&”外）。

步骤7 单击“确定”，完成密码重置。

3.4 报警联动

设置报警输入、输出，查看报警记录。

3.4.1 配置报警功能

背景信息

设置报警输入、输出和门禁联动。

说明

若设备接入软件客户端，相关参数配置将同步客户端，客户端修改对应参数也与设备同步。

操作步骤

步骤1 登录设备WEB界面。

步骤2 选择“报警联动 > 报警联动”。

图3-3 报警联动

报警输入	名称	报警类型	报警输出通道	修改
1	防区1	常开	1	
2	防区2	常开	1	

步骤3 单击修改报警联动参数。

图3-4 修改报警联动参数

修改
✕

报警输入

名称

报警输入类型

消防联动启用

报警输出启用

持续时间(秒) (1~300)

报警输出通道 1 2

门禁联动启用

通道类型

表3-1 门禁参数设置说明

参数	说明
报警输入	报警输入编号。不支持修改。
名称	自定义。
报警输入类型	<ul style="list-style-type: none"> ● 请根据购买的报警设备设置报警输入类型。 ● 常开，常开是指设备保持开路状态，报警时线路闭合。 ● 常闭，常闭是指设备保持闭合状态，报警时线路开路。

参数	说明
消防联动启用	消防联动启用后，当产生消防报警，设备联动报警输出、联动门禁。  说明 若启用消防联动，设备默认启用报警输出和门禁联动常开。
报警输出启用	报警输出启用后，有报警输入触发时，联动继电器向外输出报警信息。设置报警持续时间，并根据报警设备实际连接的通道，选择报警输出通道。
持续时间（秒）	
报警输出通道	
门禁联动启用	启用后，有报警信号输入时，设备联动门常开或常闭。
通道类型	通道类型可选择常开或常闭。 <ul style="list-style-type: none"> 常开，当有报警信号输入时，门常开。 常闭，当有报警信号输入时，门常闭。

步骤4 单击“确认”，完成参数设置。

3.4.2 查看报警记录

查看报警记录，包含设备报警的类型和报警发生的时间。

操作步骤

步骤1 登录设备WEB界面。

步骤2 选择“报警联动 > 报警记录”。

步骤3 选择“时间范围”、“类型”，单击“查询”。

图3-5 报警记录



3.5 对讲设置

设置系统配套的SIP服务器信息，将门口机和室内机注册到SIP服务器上，通过SIP协议实现可视对讲。

支持本机作为SIP服务器、其他门口机作为SIP服务器或者平台作为SIP服务器。

3.5.1 本门口机作为SIP服务器

3.5.1.1 配置SIP服务器

说明

本设备作为SIP服务器时，最大系统容量为50台，即可接入的其他门禁设备和室内机等最大数量为

50台。

操作步骤

- 步骤1 登录设备WEB界面。
- 步骤2 选择“对讲设置 > SIP服务器”。
- 步骤3 选择“启用”，其他参数保持默认。

图3-6 本机作为SIP服务器

SIP 服务器

SIP 服务器 启用

服务器类型 VTO

IP地址

端口 5060

用户名 8001

密码

SIP注册域 VDP

SIP服务器用户名 admin

SIP服务器密码

警告:修改以上SIP服务器使能项会影响门口机和室内机连接,需要重启设备。

确认 刷新 恢复默认

- 步骤4 单击“确认”，保存设置。

3.5.1.2 配置本机参数

操作步骤

- 步骤1 登录设备WEB界面。
- 步骤2 选择“对讲设置 > 本机设置”。
- 步骤3 设置参数。

图3-7 本机设置-本机作为SIP服务器



表3-2 本机参数说明（1）

参数	说明
设备类型	选择单元机。
管理中心	设置门口机呼叫管理中心的号码，设置为888888+管理机编号。  说明 管理机编号请查看管理机本地界面“本机设置”的“编号”。
编号	不可设置。
群呼	开启群呼后，当本门口机呼叫某一主室内机时，会同时呼叫其分室内机。  说明 设置群呼功能后，门口机会自动重启后设置生效。
传输模式	默认选择“模式1”。 <ul style="list-style-type: none"> ● 模式1：通用对讲传输模式。 ● 模式2：用于特殊场景，群呼场景体验提升。

步骤4 单击“确定”。

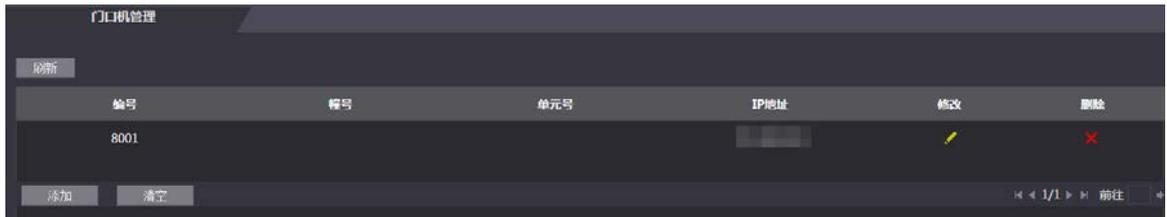
3.5.1.3 添加门口机

本门口机作为SIP服务器且有多个门口机存在时，需要添加其他门口机，使这些门口机注册到本SIP服务器上，实现可视对讲功能。

操作步骤

- 步骤1 登录设备WEB界面。
- 步骤2 选择“对讲设置 > 门口机管理”。
- 步骤3 单击“添加”。

图3-8 门口机管理界面



步骤4 设置门口机参数。

图3-9 门口机添加界面

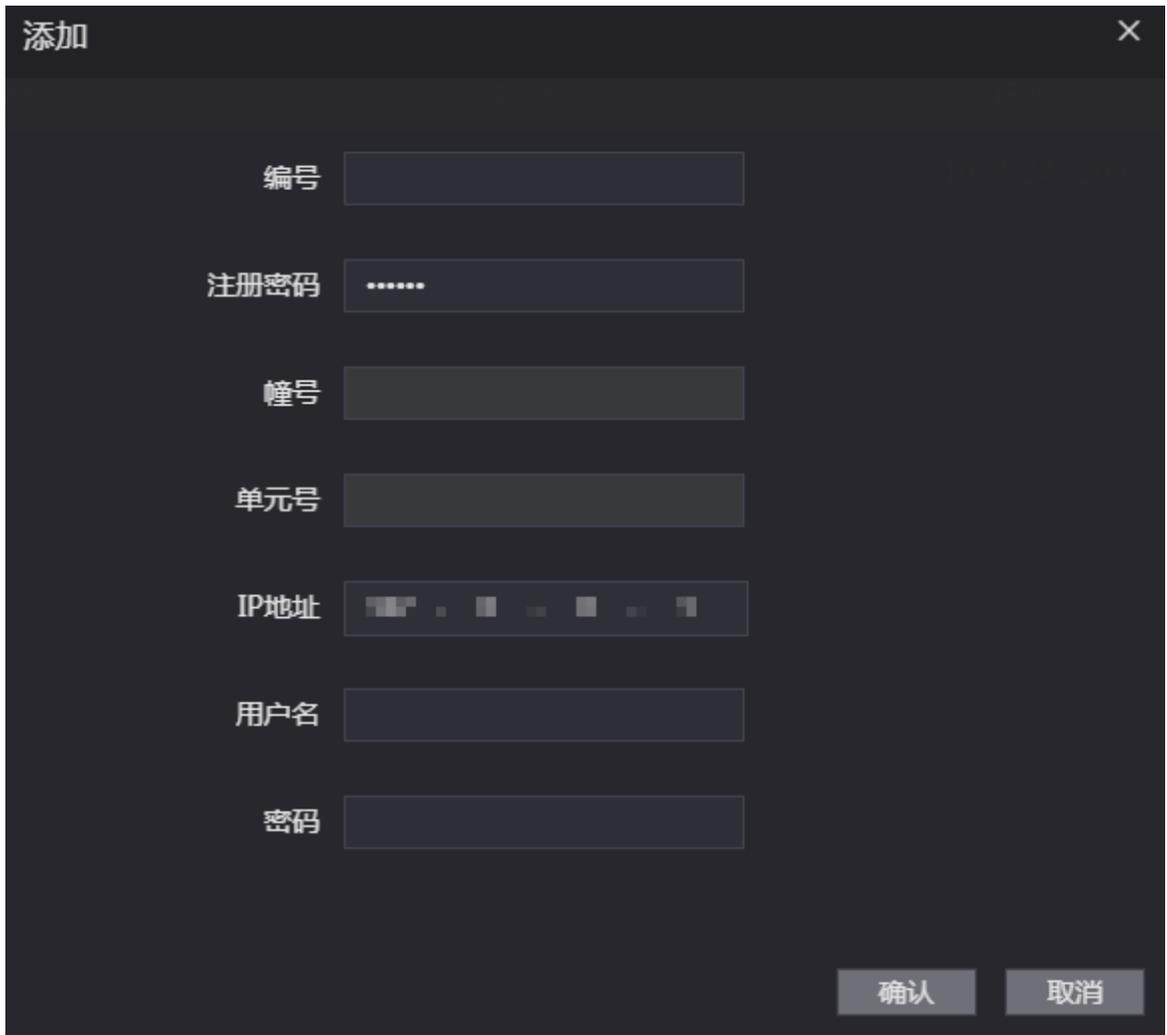


表3-3 门口机参数说明

参数	说明
编号	被添加门口机的编号。在门口机WEB界面的“本机信息”界面查看门口机编号。
注册密码	SIP系统中信令交互使用，使用默认值即可。
幢号	不可编辑。
单元号	
IP地址	被添加门口机的IP地址。
用户名	登录该门口机WEB界面的用户名和密码。
密码	

步骤5 单击“确认”，完成添加。

相关操作

- 单击“清空”，清空添加的所有门口机信息。
- 单击，编辑已添加的门口机信息。
- 单击，单个删除门口机。

3.5.1.4 室内机管理

当本门口机作为SIP服务器使用时，需要添加本单元内的所有室内机，使室内机注册到本SIP服务器上，实现可视对讲功能。

- 当有主室内机和分室内机时，需要先开启群呼功能后，再在此界面分别添加主室内机和分室内机。开启群呼功能操作请参见“3.5.1.2 配置本机参数”。
- 最多添加1024个室内机。

3.5.1.4.1 单个添加室内机

操作步骤

- 步骤1 登录设备WEB界面。
- 步骤2 选择“对讲设置 > 室内机管理”。
- 步骤3 单击“添加”。

图3-10 单个添加室内机



- 步骤4 填写用户信息。

图3-11 添加界面

表3-4 室内机信息参数

参数	说明
姓	设置室内机的用户名和昵称，用于识别室内机。
名	
昵称	
房间号	设置室内机房间号。 <ul style="list-style-type: none"> ● 房间号由1~5位数组成，必须与室内机设备上设置的房间号一致。 ● 当包含主室内机和分室内机时，主室内机的房间号以“-0”结尾，分室内机的房间号以-1、-2、-3结尾。例如主室内机为101-0，分室内机为101-1、101-2…。 ● 当无分室内机时，房间号无需以“-0”结尾，例如101、102…。
注册方式	SIP系统中信令交互使用，使用默认值即可。
注册密码	

步骤5 单击“保存”，完成添加。

3.5.1.4.2 批量添加室内机

操作步骤

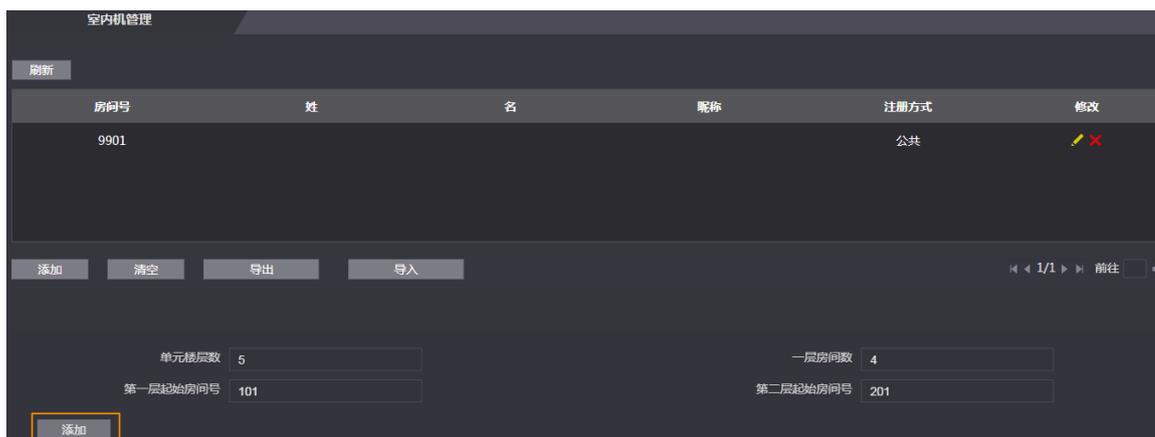
步骤1 登录设备WEB界面。

步骤2 选择“对讲设置 > 室内机管理”。

步骤3 在界面下方输入“单元楼层数”、“一层房间数”、“第一层起始房间号”、“第二层

起始房间号”。

图3-12 批量添加室内机



说明

- 楼层数范围为1~99，一层房间数范围为1~99，起始房间号范围为1~99999。
- 第二层起始房间号必须在第一层起始房间号基础上满足一层房间数。

步骤4 单击“添加”，完成添加。

相关操作

- 单击“导出”，将室内机信息导出到PC本地。
- 单击“导入”，将室内机信息导入其他设备，完成批量添加。
- 单击“清空”，清空添加的所有室内机信息。

3.5.1.5 添加管理机

本门口机作为SIP服务器时，需要添加各个管理机，使这些管理机注册到本SIP服务器上，实现可视对讲功能。

操作步骤

- 步骤1 登录设备WEB界面。
- 步骤2 选择“对讲设置 > 管理机设置”。
- 步骤3 单击“添加”。
- 步骤4 设置管理机的“VTS名称”、“注册密码”和“IP地址”。

图3-13 管理机添加

添加

VTS名称

注册密码

IP地址

确认 取消

- VTS名称为888888+管理机编号，最多支持9为数字。
管理机编号请查看管理机本地界面“本机设置”的“编号”。
- 注册密码保持默认值。
- IP地址为管理机IP。

步骤5 单击“确认”。

相关操作

- 修改管理机
当管理机的注册密码和IP地址变更时，需要同步更新，否则会出现注册失败的情况。
单击，输入新的“注册密码”或“IP地址”，单击“确认”。
- 删除管理机
单击，删除管理机。

3.5.1.6 查看在线状态

本门口机作为SIP服务器时，查看接入本SIP服务器且正常在线的设备信息。

操作步骤

- 步骤1 登录设备WEB界面。
- 步骤2 选择“对讲设置 > 在线状态”。

图3-14 在线状态

在线状态

刷新

序号	房间号	在线状态	IP:端口号	注册时间	断线时间
1	8001	在线	[redacted]	2021-09-13 19:46:59	0

1/1 前往

3.5.2 其他门口机作为SIP服务器

3.5.2.1 配置SIP服务器

操作步骤

- 步骤1 登录设备WEB界面。
- 步骤2 选择“对讲设置 > SIP服务器”。
- 步骤3 设置SIP服务器参数。
在启用参数关闭状态下，选择服务器类型为“VTO”。

图3-15 其他门口机作为服务器

SIP 服务器

SIP 服务器 启用

服务器类型 VTO

IP地址

端口 5060

用户名 8001

密码

SIP注册域 VDP

SIP服务器用户名 admin

SIP服务器密码

警告:修改以上SIP服务器使能项会影响门口机和室内机连接,需要重启设备。

确认 刷新 恢复默认

表3-5 SIP服务器参数说明（1）

参数	说明
IP地址	作为SIP服务器使用的门口机的IP地址。
端口	使用默认为5060。
用户名	使用默认值即可。
密码	
SIP注册域	SIP服务器的注册域必须为VDP。
SIP服务器用户名	登录SIP服务器的用户名和密码。
SIP服务器密码	

- 步骤4 单击“确认”，保存设置。

3.5.2.2 配置本机参数

操作步骤

- 步骤1 登录设备WEB界面。
- 步骤2 选择“对讲设置 > 本机设置”。
- 步骤3 设置参数。

图3-16 本机设置-其他门口机作为SIP服务器



表3-6 本机参数说明（2）

参数	说明
设备类型	选择单元机。
管理中心	门口机呼叫管理中心的号码，保持默认888888即可。
编号	设置本单元门口机的编号。  说明 <ul style="list-style-type: none">• 编号为4位，前两位固定80，后两位从01开始，如8001。• 如果一个单元内有多台门口机，编号不能重复。
传输模式	默认选择“模式1”。

步骤4 单击“确定”。

3.5.3 平台作为SIP服务器

3.5.3.1 配置SIP服务器

操作步骤

- 步骤1 登录设备WEB界面。
- 步骤2 选择“对讲设置 > SIP服务器”。
- 步骤3 设置SIP服务器参数。
在启用参数关闭状态下，选择服务器类型为“私有SIP服务器”。

图3-17 平台作为SIP服务器

表3-7 SIP服务器参数说明（2）

参数	说明
IP地址	平台的IP地址。
端口	使用默认为5080。
用户名	使用默认值即可。
密码	
SIP注册域	SIP服务器的注册域，可为空或保持默认值。
SIP服务器用户名	登录平台的用户名和密码。
SIP服务器密码	
备用IP地址	设置备用服务器后，当平台出现异常无法连接时，系统自动启用备用服务器，保证室内机与门口机之间的正常对讲。 <ul style="list-style-type: none"> “备用服务器”启用，则设置为本门机作为备用服务器。 “备用服务器”不启用，输入备用服务器IP、用户名和密码，则设置除本机外的其他门口机作为备用服务器。
备用服务器用户名	
备用服务器密码	
备用服务器	
备用管理机IP	输入组网内备用管理机IP，设置后，当平台出现异常无法连接时，系统自动启用备用管理机，保证管理机、本单元门口机和本单元内室内机的对讲功能正常使用。

步骤4 单击“确认”，保存设置。

3.5.3.2 配置本机参数

操作步骤

- 步骤1 登录设备WEB界面。
- 步骤2 选择“对讲设置 > 本机设置”。

步骤3 设置参数。

图3-18 本机设置-平台作为SIP服务器

表3-8 本机参数说明 (3)

参数	说明	
设备类型	根据安装位置选择单元机或围墙机。	
管理中心	设置门口机呼叫管理中心的号码，保持默认888888即可。	
区号	平台开启期功能，并设置期编号，此处需要单击“区号”后的复选框，开启区号功能，设置区号为期编号。	区号、幢号、单元号、编号与平台添加本设备时保持一致。 <ul style="list-style-type: none"> ● 区号，为2位，如01，与平台的期编号保持一致。 ● 幢号，如果平台开启期功能，为3位，如001；如果没有开启，为2位，如01。 ● 单元号，为2位，如01。 ● 编号为4位，前两位固定80，后两位从01开始，如8001。
幢号	单击“幢号”后的复选框，开启幢功能，设置单元门口机所在的幢号。	
单元号	单击“单元号”后的复选框，开启单元功能，设置单元门口机所在的单元号。	
编号	设置本单元门口机的编号。  说明 如果一个单元内有多台门口机，编号不能重复。	

步骤4 单击“确定”。

3.5.3.3 注册管理

当平台作为SIP服务器，设备被配置为备用服务器时，平台断网之后，可管理查看其他设备。

图3-19 注册管理

序号	客户端IP	设备类型	模拟室内机起始号码	模拟室内机结束号码	设备长号	修改	删除
1	10.111.211.11	VTS			888888	✎	✖
2	10.111.211.11	VTH5900+52			01029901	✎	✖
3	10.111.211.11				01028006	✎	✖
4	10.111.211.11	VTH5296			01029901#2	✎	✖
5	10.111.211.11	VTH5010-52			01029902-6	✎	✖
6	10.111.211.11	VTH5016			01029902.2	✎	✖
7	10.111.211.11	A563110-MW			8001	✎	✖

3.5.4 查看通话记录

查看门口机的呼叫、通话等记录，最多可保存1024条记录。

操作步骤

- 步骤1 登录设备WEB界面。
- 步骤2 选择“对讲设置 > 通话记录”。
- 步骤3 (可选) 单击“导出数据”，导出门口机的通话记录。

图3-20 通话记录

序号	呼叫类型	房间号	开始时间	通话时长(分)	结束状态
1	呼出	9901	2020-05-09 14:56:02	00:00	未接
2	呼出	9901	2020-05-09 14:55:45	00:05	已接听
3	呼出	9901	2020-05-06 14:15:32	00:00	未接
4	呼入	9901	2020-05-06 14:15:16	00:09	已接听

3.6 查看数据容量

登录设备WEB界面，单击“数据容量”，查看设备中“用户”、“卡片”、“人脸”、“指纹”等数据的存储记录。

说明

不同设备显示的数据不同，请以实际为准。

3.7 视频设置

通过视频设置功能，在不同的通道下，用户可以设置视频的码流、图像的亮度等参数。还可根据需要设置设备视频动检范围。



说明

以下所涉及参数建议使用系统默认值。

3.7.1 配置视频参数

设置视频码流、图像、曝光等参数。

- 视频制式：选择P制。
 - ◇ P制：PAL制式，默认码流帧率是25帧/秒。
 - ◇ N制：NTSC制式，默认码流帧率是30帧/秒。
- 通道1：设置该通道可见光视频码流、图像、曝光等参数。
- 通道2：设置该通道红外光视频图像、曝光参数。
- 恢复默认：单击“恢复默认”，当前页参数恢复默认设置。
- 抓图：单击“抓图”，截取设备当前显示图像。

3.7.1.1 配置通道1视频参数

登录设备WEB界面，选择“视频设置 > 视频设置”，通道号选择“1”。

码流设置

图3-21 码流



表3-9 码流参数说明

参数		说明
主码流	视频格式	请根据实际需要选择视频分辨率。  说明 设备作为门口机使用接入室内机时，室内机拉流限制为720P。若分辨率切换为1080P，可能会影响对讲和预览功能。
	帧速	调节画面传输的速度。
	带宽	请根据实际设备接入的网络选择合适的速率。
辅码流	视频格式	本设备辅码格式支持D1、VGA、QVGA。
	帧速	调节画面传输的速度范围：1帧~25帧。
	带宽	请根据实际设备接入的网络选择合适的速率。

图像设置

图3-22 图像（1）



表3-10 图像参数说明

参数	说明
亮度	用于调节图像的整体亮度，数值越大图像越亮。
对比度	用于调节图像的对比度，数值越大图像明暗反差越大，反之越小。
色度	用于调节图像颜色深浅，数值越大，颜色越深，反之越浅。
饱和度	用于调节图像颜色鲜艳度。值越大图像色彩越鲜艳，反之越暗淡。  说明 该值不会影响图像的整体亮度。

参数	说明
情景模式	不同的情景模式会影响图像的整体色调。本机默认为“自动”模式。 <ul style="list-style-type: none"> ● 关闭：不设置任何模式。 ● 自动：根据镜头感光程度，自动调节情景模式，使图像颜色正常。 ● 晴天：设置为晴天模式时，图像色调将被降低。 ● 晚上：设置为晚上模式时，图像色调将被提高。
日/夜模式	日夜模式影响设备的补光状态。 <ul style="list-style-type: none"> ● 自动：根据镜头感光程度，自动调节模式，使图像颜色正常。 ● 彩色：图像色调显示为彩色。 ● 黑白：图像色调显示为黑白。
补偿模式	根据实际的使用场景，选择合适的补偿模式，使视频满足使用需求。  说明 人脸在逆光情况下，建议开启宽动态。 <ul style="list-style-type: none"> ● 关闭：不执行任何补偿。 ● 背光补偿：背光补偿能避免在逆光环境下拍摄主体较暗部分出现剪影的现象。 ● 宽动态：系统根据环境亮度，将高亮度区域亮度降低，低亮度区域亮度提高，使高亮度区域和低亮度区域景物都能清晰显示。 ● 强光抑制：系统会抑制图像高亮区域的亮度，减小光晕区域的大小，使整个图像亮度降低。
镜像	选择“启用”，将摄像机图像左右翻转。
翻转	选择“启用”，将摄像机图像上下翻转。

曝光设置

图3-23 曝光（1）



表3-11 曝光参数说明

参数	说明
防闪烁	<ul style="list-style-type: none"> ● 50 Hz: 在市电为50 Hz的情况下, 根据场景亮度, 自动调整曝光的同时, 确保图像不出现横条纹。 ● 60 Hz: 在市电为60 Hz的情况下, 根据场景亮度, 自动调整曝光的同时, 确保图像不出现横条纹。 ● 室外: 该模式下可切换曝光模式, 达到相应曝光模式下的效果。
曝光模式	<p>摄像机的曝光模式。</p> <ul style="list-style-type: none"> ● 自动: 根据环境自动调整图像显示的亮度。 ● 快门优先: 在正常曝光范围内根据不同场景亮度, 设备优先按照设置的快门范围自动调整。若图像亮度未达到效果且快门值已到上限或者下限, 设备会自动调节增益值, 使图像达到最佳亮度。 ● 手动: 手动设置增益值和快门值, 调节图像显示的亮度。 <p> 说明</p> <ul style="list-style-type: none"> ● 当“防闪烁”为“室外”时, “曝光模式”可以设置为“快门优先”模式。 ● 不同设备的曝光模式不同, 请以实际界面为准。
快门	<p>可以根据实际需要设置快门大小。 快门值越大, 曝光时间越小, 图像越暗。</p>
快门范围	当选择“用户定义区间”时, 可自定义快门范围。
增益范围	设置增益区间后, 设备可提升视频效果。
曝光补偿	设置曝光补偿后可提高视频亮度。
3D降噪	启用3D降噪后, 可减少视频噪点, 提高视频清晰度。
等级	<p>当“3D降噪”为“开启”时, 可以设置该参数。 数值越大, 视频越清晰。</p>

3.7.1.2 配置通道2视频参数

登录设备WEB界面, 选择“视频设置 > 视频设置”, 通道号选择“2”。

图像设置

图3-24 图像 (2)



表3-12 通道2图像参数说明

参数	说明
亮度	用于调节图像的整体亮度，数值越大图像越亮。
对比度	用于调节图像的对比度，数值越大图像明暗反差越大，反之越小。
补偿模式	<p>根据实际的使用场景，选择合适的补偿模式，使视频满足使用需求。</p> <p> 说明</p> <p>人脸在逆光情况下，建议开启宽动态。</p> <ul style="list-style-type: none"> ● 关闭：不执行任何补偿。 ● 背光补偿：背光补偿能避免在逆光环境下拍摄主体较暗部分出现剪影的现象。 ● 宽动态：系统根据环境亮度，将高亮度区域亮度降低，低亮度区域亮度提高，使高亮度区域和低亮度区域景物都能清晰显示。 ● 强光抑制：系统会抑制图像高亮区域的亮度，减小光晕区域的大小，使整个图像亮度降低。

曝光设置

图3-25 曝光 (2)



表3-13 通道2曝光参数说明

参数	说明
防闪烁	<ul style="list-style-type: none"> ● 50 Hz: 在市电为50 Hz的情况下, 根据场景亮度, 自动调整曝光的同时, 确保图像不出现横条纹。 ● 60 Hz: 在市电为60 Hz的情况下, 根据场景亮度, 自动调整曝光的同时, 确保图像不出现横条纹。 ● 室外: 该模式下可切换曝光模式, 达到相应曝光模式下的效果。
曝光模式	<p>摄像机的曝光模式。</p> <ul style="list-style-type: none"> ● 自动: 根据环境自动调整图像显示的亮度。 ● 快门优先: 在正常曝光范围内根据不同场景亮度, 设备优先按照设置的快门范围自动调整。若图像亮度未达到效果且快门值已到上限或者下限, 设备会自动调节增益值, 使图像达到最佳亮度。 ● 手动: 手动设置增益值和快门值, 调节图像显示的亮度。 <p> 说明</p> <ul style="list-style-type: none"> ● 当“防闪烁”设置为“室外”时, “曝光模式”可以设置为“快门优先”模式。 ● 不同设备的曝光模式不同, 具体请以实际界面为准。
曝光补偿	设置曝光补偿后可提高视频亮度。
3D降噪	启用3D降噪后, 可减少视频噪点, 提高视频清晰度。
等级	当“3D降噪”为“开启”时, 可以设置该参数。 数值越大, 视频越清晰。

3.7.2 配置动态检测

操作步骤

- 步骤1 登录设备WEB界面。
- 步骤2 选择“视频设置 > 动检设置”。
- 步骤3 设置参数。

图3-26 动检设置

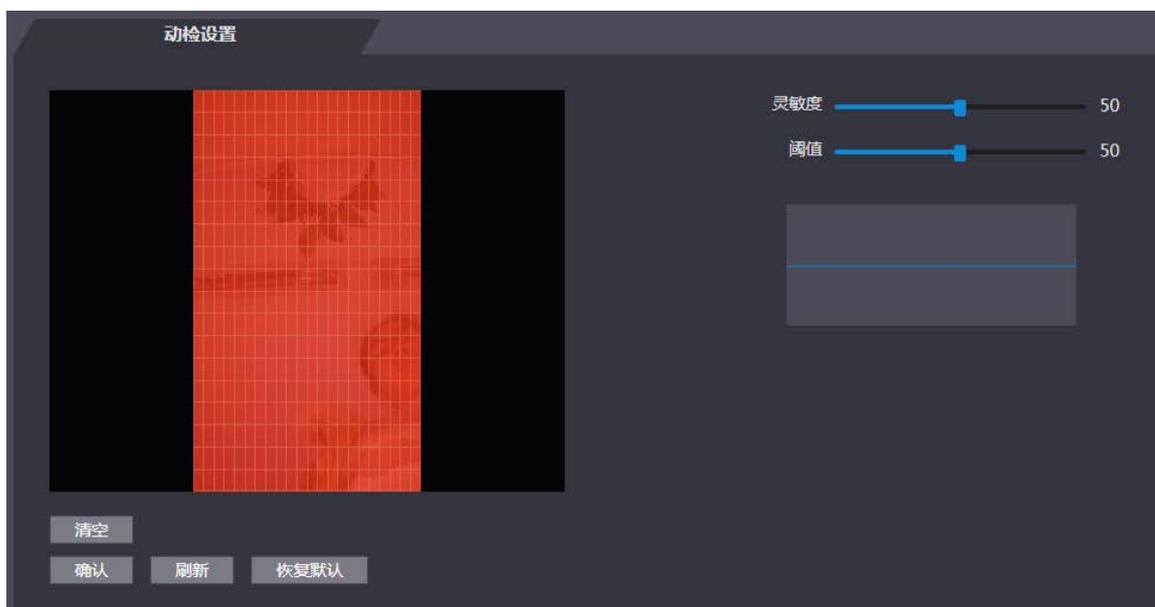


表3-14 动检设置参数说明

参数	说明
灵敏度	每个动检的格子的感知能力，数值越大越灵敏。
阈值	动检触发的条件，数值越小越容易触发。

- 步骤4 按住鼠标左键在视频画面上拖动，设置动检范围。



说明

- 红色格子表示为动检区域，默认为整个画面全部为动检区域。
- 若单独绘制，建议先单击“清空”，再绘制指定动检范围。
- 若在默认的情况下绘制，则绘制的区域为非动检区域。

- 步骤5 单击“确认”。

3.7.3 配置图像模式

根据实际的安装环境光照，选择合适的图像模式。

操作步骤

- 步骤1 登录设备WEB界面。
- 步骤2 选择“视频设置 > 图像模式”。
- 步骤3 单击, 打开下拉菜单选择图像模式类型。

图3-27 图像模式设置



- 室内：设备位于室内环境且图像中不含室外环境或室外环境占比较小的场景，此类场景无日光照明，光源多为人造光源且空间亮度较均匀。
- 室外：光源为日光，亮度较高且亮度较均匀。
- 其他，过道、半户外等逆光场景。

步骤4 单击“确认”，完成设置。

3.7.4 配置局部编码

设置可视对讲功能中对讲和预览的画面区域。



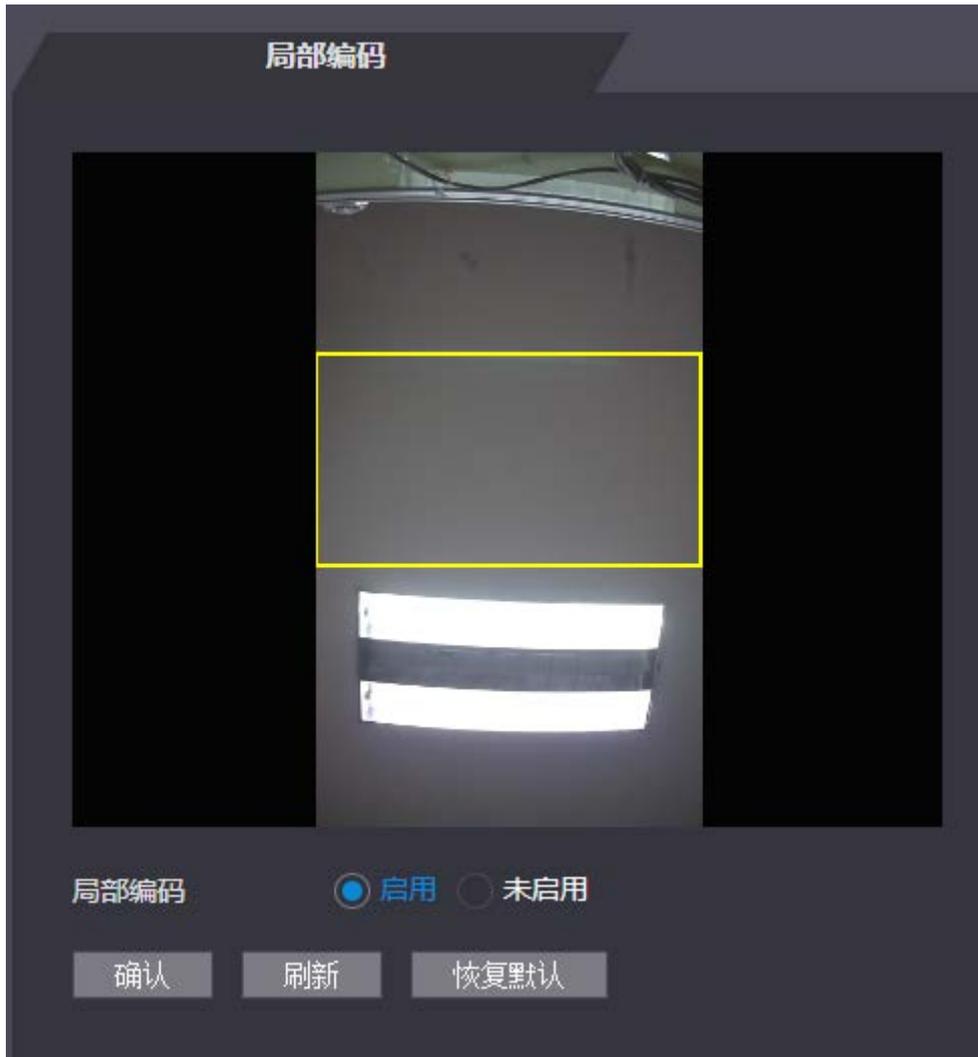
注意

搭配室内机使用时默认开启，关闭此功能可能会出现无法获取预览画面问题，

操作步骤

- 步骤1 登录设备WEB界面。
- 步骤2 选择“视频设置 > 局部编码”。
- 步骤3 选择“启用”，启用局部编码功能。
- 步骤4 拖动图中方框至任意位置。
在图框中显示对讲和预览的画面。

图3-28 局部编码



步骤5 单击“确认”。

3.8 配置人脸检测

设置人脸检测的各项参数和检测区域，提高设备识别人脸的精准度。

操作步骤

- 步骤1 登录设备WEB界面。
- 步骤2 单击“人脸检测”，配置参数。

图3-29 人脸检测

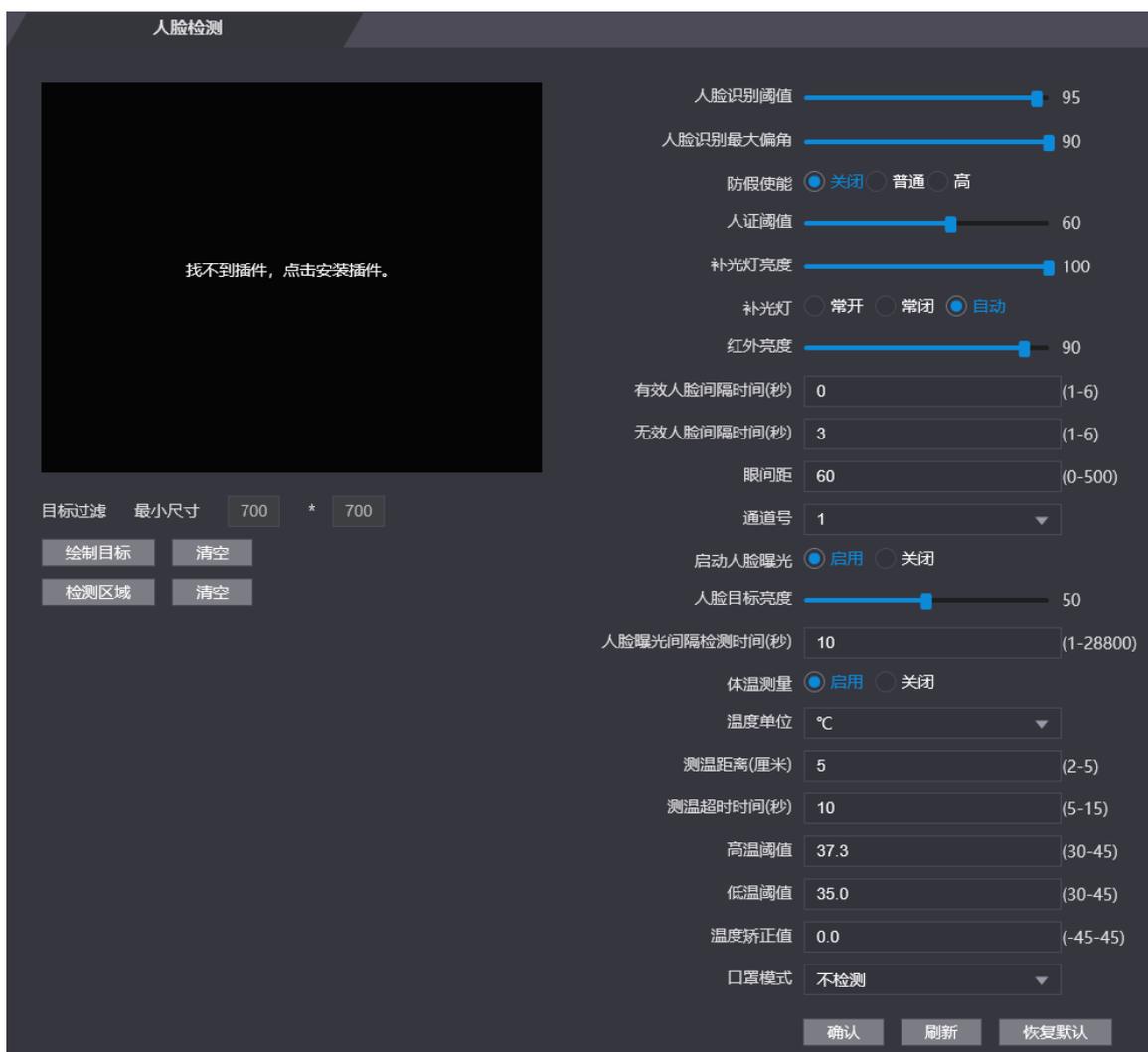


表3-15 人脸检测参数说明

参数	说明
人脸识别阈值	设置人脸比对时的阈值。阈值越大，识别人脸时误识率越低，同时识别成功率越低。
人脸识别最大偏角	偏角越大，可检测到人脸的范围也更大。
防假使能	开启后，可防止使用有权限人员的照片、视频等冒用人脸信息情况的发生。默认为“普通”。
人证阈值	<p>将采集到的人脸与身份证中照片比对，阈值越大，要求人脸相似度越大，识别成功率越低。</p> <p> 说明</p> <p>仅具有人证功能的设备支持。</p>
补光灯亮度	调整设备识别人脸时，白光补光灯的亮度。

参数	说明
补光灯	<p>设置设备识别人脸时白光补光的情况。</p> <ul style="list-style-type: none"> ● 常开：补光灯保持开启状态。 ● 常闭：补光灯保持关闭状态。 ● 自动：当周围光线充足的情况下（例如白天），补光灯关闭；当周围光线暗的情况下（例如夜晚），补光灯开启。
红外亮度	调整设备识别人脸时，红外补光灯的亮度。
有效人脸间隔时间	设置同一有权限人员在同一台设备上识别，重复提示识别成功的间隔时间。
无效人脸间隔时间	设置同一人员在同一台设备上识别，重复提示识别失败的间隔时间。
眼间距	<p>双眼之间的像素值，与人脸大小、人脸与镜头距离相关。</p> <p>比如：一般成年人距离镜头1.5 m时，眼间距为50像素~70像素。</p>
通道号	<ul style="list-style-type: none"> ● 1为白光视频。 ● 2为红外光视频。
启动人脸曝光	<p>室外环境下，启动后，仅对人脸部分曝光，更能清晰的识别人脸，提高识别率。</p> <ul style="list-style-type: none"> ● 人脸目标亮度：室外环境下，启动人脸曝光后，根据设定的人脸目标亮度，对人脸部分单独曝光，更能清晰的识别人脸，提高识别率。 ● 人脸曝光间隔检测时间：人脸曝光后，在间隔时间内再次检测人脸时，不会重新对人脸部分曝光，因为上一次的曝光还在持续中，直到超过间隔时间。
人脸目标亮度	
人脸曝光间隔检测时间	

参数	说明
体温测量	<p>启用后，可检测体温温度。</p> <p> 说明</p> <p>仅具有测温功能的设备支持。</p> <ul style="list-style-type: none"> ● 温度单位：分为℃（摄氏温度）和°F（华氏温度）。 ● 测温区域框：启用后，主界面显示可测温的识别区域。 ● 测温距离（厘米）：默认设置为150 cm，如果设置为其他值时，则支持定点测温，距离以设置值为主，如果定点测温，建议设置80 cm。 ● 测温矫正时长（毫秒）：设置时间值，检测时间超过这个时间阈值，本次测温结束。显示屏将提示：未获取温度，请靠近测温。 ● 高温阈值：设置温度值，大于等于这个温度判断为高温。 ● 温度最大值：设置测量的最高体温值。 ● 温度最小值：设置测量的最低体温值。 ● 温度矫正值：调试参数。由于测温环境差异，被测者温度可能会产生误差。调试时可选择多个被测样本站在测温距离，根据测量值和实际值比较，通过此参数修正。例如测量温度比实际值低0.5 ℃，此处矫正值设置为0.5 ℃；如果测量温度比实际值高0.5 ℃，此处矫正值设置为-0.5 ℃。
口罩模式	<ul style="list-style-type: none"> ● 不检测：检测人脸时不检测是否戴口罩。 ● 口罩提醒：识别人脸时，当检测到人员未戴口罩，界面及语音提示“请戴口罩”，允许通行。 ● 口罩拦截：识别人脸时，当检测到人员未戴口罩，界面及语音提示“请戴口罩”，且禁止通行。 <p> 说明</p> <p>与安全帽检测使能互斥。</p>
安全帽检测使能	<p>开启后可检测人员是否佩戴安全帽。</p> <p> 说明</p> <ul style="list-style-type: none"> ● 仅部分非测温设备支持此功能。 ● 与口罩检测使能互斥。

步骤3 单击“确认”，完成设置。

相关操作

- 绘制目标
 - ◇ 单击“绘制目标”，绘制最小识别框的大小。
 - ◇ 单击“清空”，清空绘制的识别框。
- 检测区域
 - ◇ 单击“检测区域”，调整识别区域，拖动四个顶点，可调整为多边形区域。
 - ◇ 单击“清空”，清空检测区域。

3.9 网络设置

对TCP/IP、端口、主动注册和P2P功能修改设置。

3.9.1 配置TCP/IP

将设备IP地址修改为规划IP地址，接入组网。

操作步骤

- 步骤1 登录设备WEB界面。
- 步骤2 选择“网络设置 > TCP/IP”。
- 步骤3 配置参数。

图3-30 TCP/IP配置

表3-16 TCP/IP参数说明

参数	说明
IP版本	只支持IPv4。
MAC地址	显示设备MAC地址。
模式	设置设备获取IP的模式。 <ul style="list-style-type: none">静态：手动设置IP地址、子网掩码、网关，单击“确认”后，WEB页面自动跳转到新设置IP地址的登录界面。DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）：当网络中存在DHCP服务器时，选择“DHCP”，设备自动获取动态IP地址，无需手动设置IP地址等信息。
IP地址	当“模式”选择“静态”时，需要根据网络规划，输入设备的IP地址、

参数	说明
子网掩码	子网掩码和默认网关。
默认网关	 说明 IP地址和默认网关必须在同一网段。
首选DNS服务器	DNS服务器IP地址。
备选DNS服务器	备用DNS服务器的IP地址。

步骤4 单击“确认”。

3.9.2 配置端口

设置通过客户端（包括WEB客户端、平台客户端、手机客户端等）同时访问本设备的最大连接数及各个端口号。

操作步骤

- 步骤1 登录设备WEB界面。
- 步骤2 选择“网络设置 > 端口”。
- 步骤3 配置该设备的各个端口值。



除“最大连接数”和“RTSP端口”以外，修改其他参数设置，需重启后生效。

图3-31 端口



端口配置界面显示以下参数：

参数	当前值	范围
最大连接数	10	(1~999)
TCP端口	37777	(1025~65535)
HTTP端口	80	(1~65535)
HTTPS端口	443	(1~65535)
RTSP端口	554	(1~65535)

底部按钮：确认、刷新、恢复默认

表3-17 端口参数说明

参数	说明
最大连接数	设备允许同时登录的客户端（如WEB客户端、平台客户端、手机客户端等）个数。  说明 平台客户端如SmartPSS Plus不占用个数。
TCP端口	TCP协议通讯提供服务的端口，可根据用户实际需要设置，默认为37777。
HTTP端口	HTTP通讯端口，可根据用户实际需要设置，默认为80，若设置为其他数值，使用浏览器登录时需要在地址后加上修改的端口号。

参数	说明
HTTPS端口	HTTPS通讯端口，可根据用户实际需要设置，默认为443。
RTSP端口	RTSP端口号，可根据用户实际需要设置，默认为554。

步骤4 单击“确认”，完成设置。

3.9.3 配置主动注册

主动注册指的是设备主动注册到服务器，向用户指定的服务器汇报当前设备网络所在位置，方便服务器客户端软件访问设备。

操作步骤

步骤1 登录设备WEB界面。

步骤2 选择“网络设置 > 主动注册”。

步骤3 选择“启用”，输入“主机IP”、“端口”和“子设备ID”。

图3-32 主动注册

表3-18 主动注册参数

参数	说明
主机IP	需要注册到的服务器IP地址或者服务器域名。
端口	服务器用于主动注册的端口号。
子设备ID	自定义，与服务器端的注册ID保持一致。

步骤4 单击“确认”，完成设置。

3.9.4 配置P2P

P2P是一种私网穿透技术。用户可下载手机应用并注册账号，通过扫描二维码远程管理多个设备。使用时无需申请动态域名、进行端口映射或部署中转服务器，轻松便捷。

前提条件

设备需接入外网。

操作步骤

步骤1 登录设备WEB界面。

步骤2 选择“网络设置 > P2P”。

步骤3 选择“启用”。

图3-33 P2P界面



步骤4 单击“确认”，完成设置。

3.9.5 配置4G



说明

仅4G款支持。

操作步骤

- 步骤1 登录设备WEB界面。
- 步骤2 选择“网络设置 > 4G”。
- 步骤3 选择“启用”，开启4G通讯功能。
- 步骤4 设置参数。

图3-34 4G

表3-19 4G参数

参数	说明
无线模式	选择4G通讯制式，默认为Auto。
APN	设备访问网络时的接入点名称，根据使用的SIM卡自动识别。 <ul style="list-style-type: none"> ● CTNET：中国电信2G&3G。 ● CTLTE：中国电信4G。 ● CMNET：中国移动。 ● UNINET：中国联通。 ● 3GNET：中国联通，同UNINET。
鉴权模式	选择鉴权模式。系统会根据SIM卡自动识别鉴权模式。 <ul style="list-style-type: none"> ● No：不需要鉴权。 ● PAP：PAP鉴权。 ● CHAP：CHAP鉴权。
拨号号码	输入SIM卡号码。系统会根据SIM卡自动识别号码。 <ul style="list-style-type: none"> ● *99#：电信号码。 ● *98*1#：移动号码。 ● *99#：联通号码。

参数	说明
用户名	<ul style="list-style-type: none"> ● 移动联通SIM卡默认为空。 ● 电信SIM卡使用默认用户名密码。 <ul style="list-style-type: none"> ◇ 用户名: ctnet@mycdma.cn。 ◇ 密码: vnet.mobi。
密码	
IP地址	显示设备的4G通讯IP地址。默认分配，不可修改。
信号强度	显示设备的4G通讯信号。

步骤5 单击“确认”。

3.10 安全管理

3.10.1 IP权限

通过设置网络访问、禁止PING、防半连接加强设备的网络和数据的安全性，保证网络入口、出口安全。

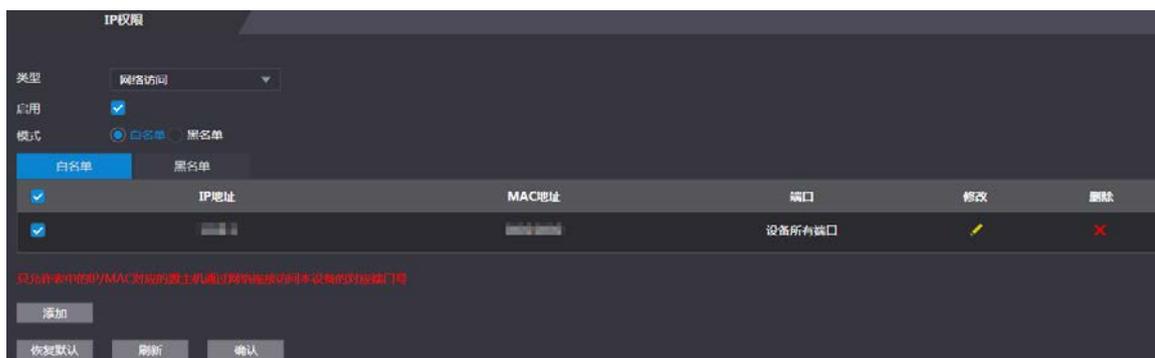
3.10.1.1 配置网络访问

通过设置黑白名单，限制用户的访问权限。

操作步骤

- 步骤1 登录设备WEB界面。
- 步骤2 选择“安全管理 > IP权限”。
- 步骤3 类型选择“网络访问”。
- 步骤4 选择“启用”。
- 步骤5 添加白名单或黑名单。

图3-35 网络访问



1. 选择“模式”为“白名单”/“黑名单”或单击“白名单”/“黑名单”页签。
2. 单击“添加”。
3. 配置添加信息。

图3-36 添加

 **说明**

单击，打开下拉菜单选择，可添加网段。

表3-20 IP地址参数说明

参数	说明
类型	选择要加入黑名单或白名单的地址类型，IP地址、IP网段、MAC地址和所有IP。  说明 若类型选择为“MAC地址”，则只需输入“MAC地址”，即可设置。
IP版本	默认IPV4地址。
IPV4地址	输入要加入黑名单或白名单的IPV4地址。
设备所有端口	选择后该设置适用于所有端口；取消选择，需设置“设备起始服务端口”、“设备结束服务端口”，则此设置适用于在该范围内的端口。

4. 单击“保存”。

步骤6 单击“确认”，保存设置。

相关操作

- 单击，修改白名单或黑名单参数。
- 单击，删除黑白名单。

3.10.1.2 配置禁止PING

启用禁止PING功能，设备不回复PING请求。

操作步骤

- 步骤1 登录设备WEB界面。
- 步骤2 选择“安全管理 > IP权限”。
- 步骤3 类型选择“禁止PING”。
- 步骤4 选择“启用”。

图3-37 选择禁止PING启用界面



- 步骤5 单击“确认”，保存设置。

3.10.1.3 配置防半连接

启用防半连接功能，在半连接攻击下，设备可以正常提供服务。

操作步骤

- 步骤1 登录设备WEB界面。
- 步骤2 选择“安全管理 > IP权限”。
- 步骤3 类型选择“防半连接”。
- 步骤4 选择“启用”。

图3-38 选择防半连接启用界面



- 步骤5 单击“确认”，保存设置。

3.10.2 配置系统服务

操作步骤

- 步骤1 登录设备WEB界面。
- 步骤2 选择“安全管理 > 系统服务”。
- 步骤3 根据实际使用情况设置。

图3-39 系统服务



表3-21 系统服务参数

参数	说明
SSH使能	选择后，开启远程登录会话。
密码重置	选择后，开启密码重置功能，当密码忘记后可以重新修改密码。
CGI使能	选择后，支持CGI协议。
ONVIF使能	选择后，开启ONVIF接口协议。
HTTPS使能	选择后，开启HTTPS协议认证。
认证模式	<p>设置认证模式，支持安全模式和兼容模式。推荐选择“安全模式”。</p> <ul style="list-style-type: none"> ● 安全模式：不支持通过Digest、DES和明文的认证方式访问设备，提高设备使用的安全性。 ● 兼容模式：支持通过Digest、DES和明文的认证方式访问设备，安全性降低，不推荐使用。
创建服务器证书	用户可安装手动创建的服务器证书，详细介绍请参见“3.10.2.1 创建服务器证书”。
下载根证书	用户可下载并安装根证书，详细介绍请参见“3.10.2.2 下载与安装根证书”。

步骤4 单击“确认”。

3.10.2.1 创建服务器证书

背景信息

在HTTPS设置界面，用户可安装手动创建的服务器证书，使PC能够通过HTTPS正常登录，保证通信数据的安全性，以可靠稳定的技术手段为用户信息及设备安全提供保障。

说明

- 首次使用HTTPS或者更换设备的IP地址后，需要创建服务器证书和安装根证书。
- 创建服务器证书和安装根证书后，如果更换登录WEB的PC，需要在新的PC上重新下载并安装根证书或者将下载后的根证书拷贝至新的PC上安装。

操作步骤

- 步骤1 单击“创建服务器证书”。
- 步骤2 填写对应信息，填写完毕后单击“确认”。
创建成功后系统提示“创建成功”，设备将重新启动。

图3-40 创建服务器证书



3.10.2.2 下载与安装根证书

操作步骤

- 步骤1 单击“下载根证书”。
弹出“文件保存”对话框，选择所需保存的路径保存证书。
- 步骤2 双击下载的证书文件，单击“打开”。
- 步骤3 单击“安装证书”。
- 步骤4 单击“下一步”。
- 步骤5 选择“将所有的证书放入下列存储”，单击“浏览”，选择位置为“受信任的根证书颁发机构 > 本地计算机”，单击“下一步”。

图3-41 证书存储



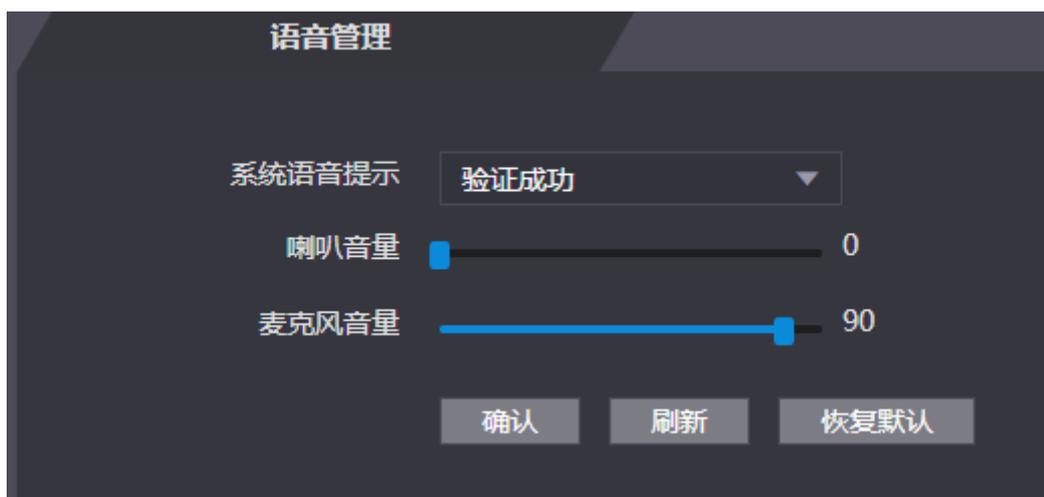
- 步骤6 单击“完成”。
- 弹出“导入成功”对话框，即证书安装导入完成。

3.11 语音管理

操作步骤

- 步骤1 登录设备WEB界面。
- 步骤2 选择“语音管理”。
- 步骤3 选择验证成功后的提示音。

图3-42 语音管理



- 步骤4 拖动进度条调节语音播报音量大小。
- 步骤5 单击“确认”，完成设置。

3.12 用户管理

根据设备使用协议的不同，分别在“用户管理”、“ONVIF用户”页签中实现添加用户，修改用

户信息等功能。

3.12.1 添加用户

系统默认用户为admin，支持增加新用户，此用户仅用于登录设备WEB界面。

操作步骤

- 步骤1 登录设备WEB界面。
- 步骤2 选择“用户管理 > 用户管理”。
- 步骤3 单击“添加”。

图3-43 用户管理



- 步骤4 输入“用户名”、“密码”、“确认密码”和“备注”。

图3-44 添加用户



- 步骤5 单击“确认”，完成添加。

3.12.2 添加ONVIF用户

ONVIF用户只用于ONVIF协议，开门前，需要验证ONVIF用户信息。

操作步骤

- 步骤1 登录设备WEB界面。
- 步骤2 选择“用户管理 > ONVIF用户”。
- 步骤3 单击“添加”。

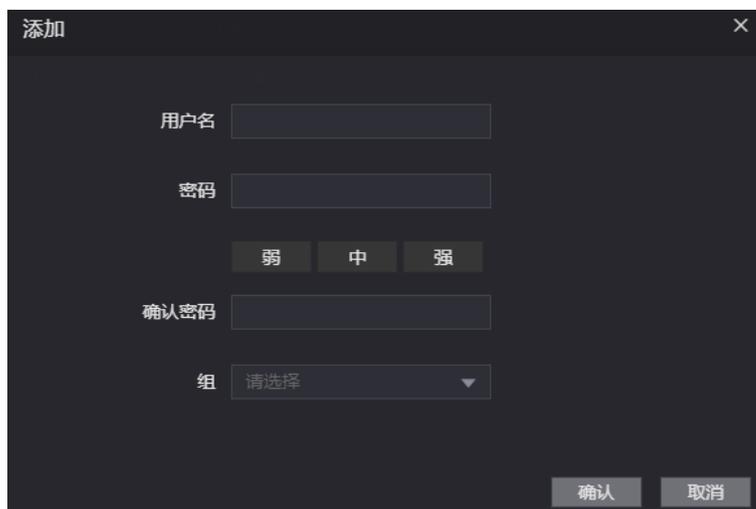
图3-45 ONVIF用户



序号	用户名	组	修改	删除
1	admin	admin		

步骤4 输入“用户名”、“密码”、“确认密码”。

图3-46 添加ONVIF用户



步骤5 选择“组”。

步骤6 单击“确认”，完成添加。

3.13 自动维护

当设备运行时间较长时，设置在空闲的时间内，设备自动重启，以提高设备运行速度。

操作步骤

步骤1 登录设备WEB界面。

步骤2 单击“自动维护”，选择“自动重启系统”的时间。

图3-47 自动维护



说明

系统默认“自动重启系统”时间为每星期二02:00。

步骤3 单击“确认”，完成自动维护设置。



说明

单击“重启设备”，设备执行重启。

3.14 配置管理

导入或者导出系统配置文件，当多台设备需要进行相同的参数配置时，可使用配置备份文件。

3.14.1 配置文件导入

操作步骤

- 步骤1 登录设备WEB界面。
- 步骤2 单击“配置管理”。
- 步骤3 单击“浏览”，选择需要导入的配置文件。
- 步骤4 单击“配置导入”，完成备份数据的系统配置导入。



说明

只有型号相同的设备才可以成功导入配置文件。

3.14.2 配置文件导出

操作步骤

- 步骤1 登录设备WEB界面。
- 步骤2 单击“配置管理”。
- 步骤3 单击“配置导出”，选择路径，单击“保存”。
保存WEB端的所有配置文件。



说明

配置导出不会导出IP。

3.15 系统升级



注意

- 升级过程中，请勿断电、断网、重启或者关闭设备。
- 请选择正确的升级文件，升级错误的程序可能会导致设备无法正常使用。

登录设备WEB界面，选择“系统升级”，系统显示“系统升级”界面。

图3-48 系统升级



3.15.1 文件升级

背景信息

对系统执行升级操作，升级文件为*.bin类型文件。

操作步骤

- 步骤1 登录设备WEB界面。
- 步骤2 单击“系统升级”。
- 步骤3 在“文件升级”区域，单击“浏览”，选择升级文件。
- 步骤4 单击“升级”，开始升级。
完成升级后，设备自动重启。

3.15.2 在线升级

背景信息

通过与云端交互，检测最新版本，实现在线升级。

操作步骤

- 步骤1 登录设备WEB界面。
- 步骤2 单击“系统升级”。
- 步骤3 在“在线升级”区域，选择检测方式。

- 选择“自动检测”，单击“确认”，开启自动检测，设备会定时跟云端交互，检测是否有新版本。如有新版本，则WEB界面右上方会提示“发现新版本”，在“系统升级”页签显示可更新文件。
- 单击“手动检测”，可实时查看本设备在云端的最新版。

步骤4 若有新版本，单击“马上升级”，开始升级。
完成升级后，设备自动重启。

3.16 查看版本信息

登录设备WEB界面，单击“版本信息”，查看设备“MAC地址”、“序列号”、“法律信息”等信息。

3.17 查看在线用户

登录设备WEB界面，选择“在线用户”，显示当前登录WEB用户的信息，包括“用户名”、“IP地址”和“用户登录时间”。

图3-49 在线用户

序号	用户名	IP地址	用户登录时间
1	admin	192.168.1.101	2021-09-14 13:39:10

3.18 系统日志

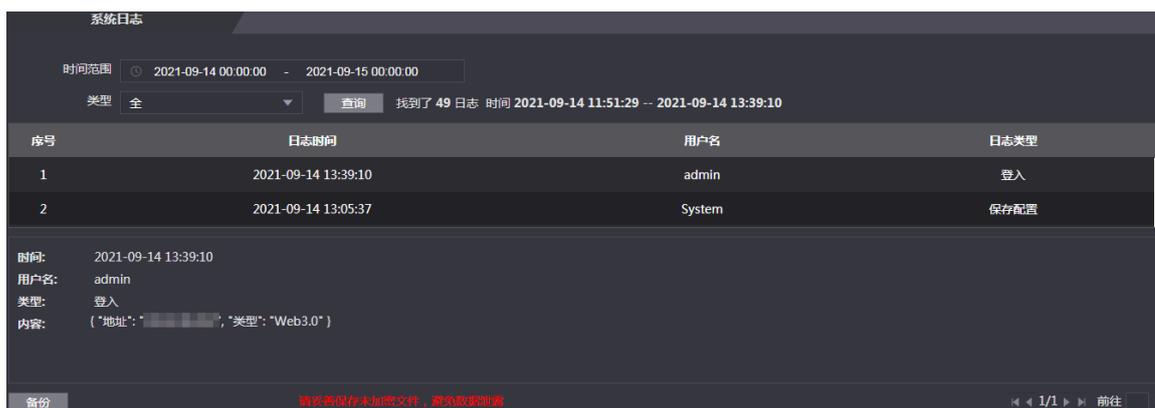
3.18.1 查看系统日志

为了维护方便，可以查看和备份系统日志。

操作步骤

- 步骤1 登录设备WEB界面。
- 步骤2 选择“系统日志 > 系统日志”。
- 步骤3 选择“开始时间”、“结束时间”和“类型”，单击“查询”。

图3-50 系统日志



相关操作

单击“备份”，将日志信息下载到PC端。

3.18.2 查看管理员记录

操作步骤

- 步骤1 登录设备WEB界面。
- 步骤2 选择“系统日志 > 管理员记录”。
- 步骤3 输入管理员ID编号，单击“查询”。
admin用户ID为0。

图3-51 管理员记录



3.18.3 查看开门记录

操作步骤

- 步骤1 登录设备WEB界面。
- 步骤2 选择“系统日志 > 开门记录查询”。
- 步骤3 选择“时间范围”和“类型”，单击“查询”。

图3-52 开门记录



相关操作

- 单击，预览相应记录下采集的人脸图片。
- 单击，下载相应记录下采集的人脸图片。
- 单击“导出数据”，将开门记录（不包含人脸图片）下载到PC上。

3.19 查看实时测温数据

登录设备WEB界面，选择“高级设置”，查看“测温距离”、“环境温度”、“体内温度”和“体表温度”。



- 需刷新页面后查看下一组实时数据。
- 仅测温功能设备支持。

3.20 退出

单击，确认后，退出设备WEB界面。



将鼠标悬停在上，可显示当前用户的信息。

第 4 章 SmartPSS Plus

4.1 登录客户端

安装配套的Smart PSS客户端，双击运行。根据界面提示完成初始化配置，登录客户端。

4.2 初始化设备

背景信息

仅支持对与PC处于同一网段的设备进行初始化，支持如下初始化操作。

- 设置设备admin用户的登录密码。
- 绑定电话号码。当忘记密码时，通过该电话号码可以重置密码。
- 修改设备的IP、子网掩码和网关。

操作步骤

- 步骤1 在主页选择“设备管理”，单击“自动搜索”。
- 步骤2 填写设备网段范围，单击“搜索”。
- 步骤3 在设备列表中选择需要初始化的设备，单击“初始化”。
- 步骤4 设置admin的登录密码，单击“密码安全”。

图4-1 设置admin用户的登录密码



1. 设置密码 2. 密码安全 3. 修改IP

用户名: admin

密码: * ●●●●●●●●

密码确认: * ●●●●●●●●

密码8~32位，且至少包含数字、字母和常用字符中的两种。

密码安全 → 取消

- 步骤5 设置用于找回密码的电话号码，单击“修改IP”。

图4-2 绑定邮箱

步骤6 设置新IP、子网掩码和网关，单击“完成”。如果未设置新IP、子网掩码和网关，则设备的IP、子网掩码和网关为出厂默认设置。

图4-3 设置IP等设备信息

4.3 添加设备

在Smart PSS Plus中添加设备，支持搜索添加和手动添加两种方式。

4.3.1 搜索添加

背景信息

要求待添加的设备处于同一网段。

操作步骤

- 步骤1 在主页选择“设备管理”，单击“自动搜索”。
- 步骤2 搜索设备。
 - 单击“自动搜索”，搜索局域网内设备。
 - 设置“设备网段”，单击“搜索”，搜索对应网段内设备。

图4-4 搜索设备

<input type="checkbox"/>	序号	IP	设备类型	MAC地址	端口	初始化状态
<input type="checkbox"/>	1		PC-NVR		37777	✔ 已初始化
<input type="checkbox"/>	2		DSS V8		443	✔ 已初始化



说明

选择设备，单击“修改IP”，修改设备的IP地址，请参见配套的SmartPSS Plus客户端说明书。

- 步骤3 选择需要添加的设备，单击“添加”。
- 步骤4 输入登录设备的“用户名”和“密码”，单击“确定”。

图4-5 登录信息

用户名: *

密码: *

确定 取消



说明

- 设备添加完成后，系统继续停留在“自动搜索”界面，您可以继续添加设备或者单

击“取消”退出“自动搜索”界面。

- 设备添加完成后，SmartPSS Plus自动登录设备，登录成功，则在线状态显示为“在线”，否则为“离线”。

图4-6 设备列表

序号	名称	IP	设备类型	设备型号	端口	通道数	在线状态	序号号	操作
1	4.3寸		门禁一体机		37777	0/0/1/0	● 在线		✎ ⏻ ↺

表4-1 操作说明

图标	说明
	单击该图标，进入“修改设备”界面，支持修改设备信息，包括设备名称、IP/域名、端口、用户名和密码。或双击设备，进入“修改设备”界面。
	单击该图标，进入“设备配置”界面，可升级、网络设置、普通设置和用户管理。
	<ul style="list-style-type: none"> 设备处于登录状态，图标显示为，单击图标，退出设备登录，同时图标变为。 设备处于离线状态，图标显示为，单击图标，登录设备登录（要求设备信息正确），同时图标变为。
	单击该图标，删除设备。

4.3.2 手动添加

背景信息

添加设备时需要预知设备的IP地址或域名。

操作步骤

- 步骤1 在主页选择“设备管理”，单击“添加”。
- 步骤2 输入设备参数。

图4-7 手动添加

表4-2 添加参数说明

参数	说明
设备名称	自定义设备名称，建议以设备安装区域命名。

参数	说明
添加方式	选择“IP”。通过设备的IP地址添加设备。
IP	设备的IP地址。
端口号	设备的端口号，默认端口号为37777，请根据情况填写。
用户名/密码	被添加设备的用户名和密码。

步骤3 单击“添加”。

若需继续添加，单击“添加并继续”。重复上述步骤。

4.4 添加人员

支持录入人员信息、给人员发卡、赋予人员权限。

4.4.1 设置发卡类型

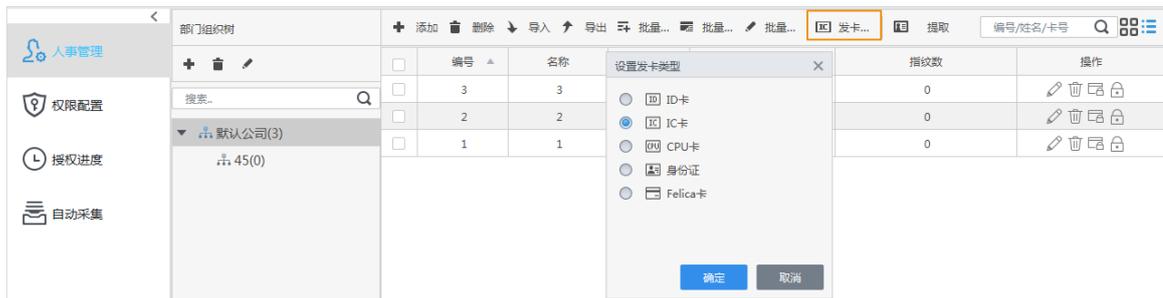


注意

发卡类型必须与发卡器保持一致，否则无法读取卡号。

在主页选择，单击“发卡类型”，设置使用的卡片类型。

图4-8 设置发卡类型



4.4.2 单个添加

操作步骤

步骤1 在主页选择。

步骤2 单击“添加”。

步骤3 输入人员基本信息。

1. 单击“基本信息”页签。
2. 输入人员信息并上传照片，单击“保存”。

图4-9 添加人员基本信息

编号:	* 123		
名称:	* [blurred]		
部门:	默认公司		
人员类型:	普通用户		
有效时间:	2021/8/23 0:00:00		3653 天
	2031/8/23 23:59:59		
使用次数:	无限		
^			
详细信息			
性别:	<input checked="" type="radio"/> 男 <input type="radio"/> 女	证件类型: 身份证	
民族:	汉族	证件号: [blurred]	
籍贯:	浙江温州	单位: HGST	
出生年月:	1984/3/15	岗位: 软件工程师	
婚姻状况:	未婚	技术等级: [empty]	
学历:	本科	入职时间: 2021/8/22 11:21:07	
联系电话:	[blurred]	离职时间: 2031/8/23 11:21:07	
电子邮件:	[empty]	通信地址: [empty]	
管理员:	<input checked="" type="checkbox"/>		
备注:	[empty text area]		

步骤4 设置人员认证信息。

1. 单击“认证”页签。
2. 设置人员开门密码。在“密码”区域，单击“添加”，在弹出的对话框设置开门密码。
3. 添加人员卡号。在“卡”区域单击“添加”，输入人员卡号，或者在“卡”区域单击右侧的，在弹出的对话框中选择读卡设备，单击“添加”通过读卡设备读取卡号。

 **说明**

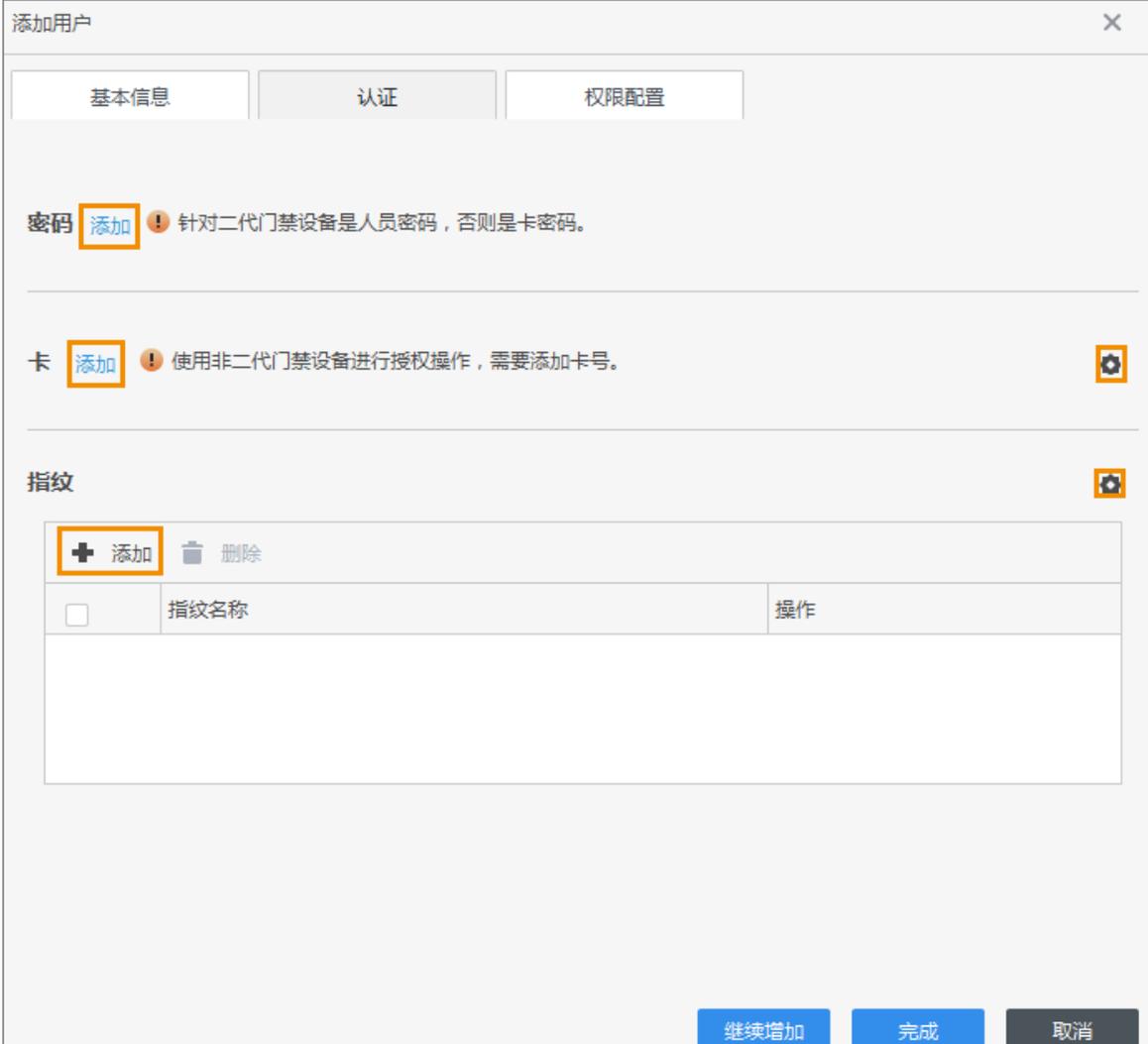
最多支持添加5张卡，支持设置1张主卡。

4. 上传人员指纹。在“指纹”区域单击右侧的，在弹出的对话框中选择指纹采集设备，然后在“指纹”区域单击“添加”，根据提示在设备上录入指纹。

说明

最多支持上传3个人的指纹，支持设置1个胁迫指纹。

图4-10 采集人员指纹信息



添加用户

基本信息 认证 权限配置

密码 **添加** ! 针对二代门禁设备是人员密码，否则是卡密码。

卡 **添加** ! 使用非二代门禁设备进行授权操作，需要添加卡号。

指纹

+ 添加  删除

<input type="checkbox"/>	指纹名称	操作
--------------------------	------	----

继续增加 完成 取消

步骤5 单击“权限配置”页签，在列表中选择支持该人员使用的设备对应的权限组。如果列表中无需要的权限组，请通过“添加组”将需要的权限组添加到列表。

步骤6 单击“完成”。

4.4.3 批量添加

操作步骤

步骤1 在主页选择。

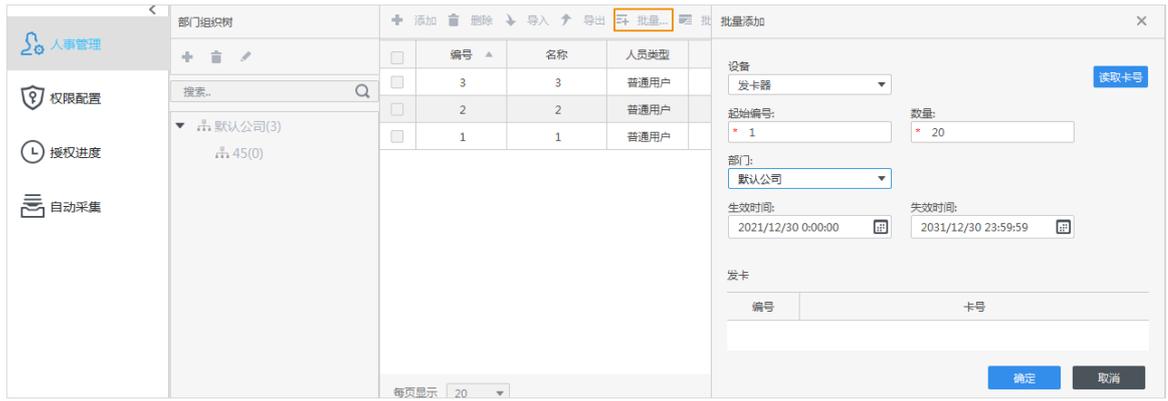
步骤2 在右侧单击“批量添加”。

步骤3 设置人员起始编号和人员数量，选择人员所属部门，设置卡片生效和失效时间。

步骤4 发卡。在“设备”下拉列表框选择读卡设备，单击“读取卡号”。在读卡设备上刷卡后，软件会自动读取人员卡号到列表。

步骤5 单击“确定”。

图4-11 批量添加人员



步骤6 在人员列表单击 ，完善人员信息。

附录1 人脸录入/比对说明

注意事项

- 登记时戴眼镜、戴帽子和胡须都可能影响登记效果。
- 戴帽子请勿遮住眉毛。
- 胡须过长或者面积过大会影响登记效果，建议登记和使用中胡须变化不要太大，否则会影响识别。
- 登记和验证时，请保持脸部清洁。
- 设备距离灯源至少2 m，距离窗口及门口至少3 m；避免逆光、阳光直射、斜射或灯光近距离照射。

注册说明

附录图1-1 人脸注册-设备端



说明

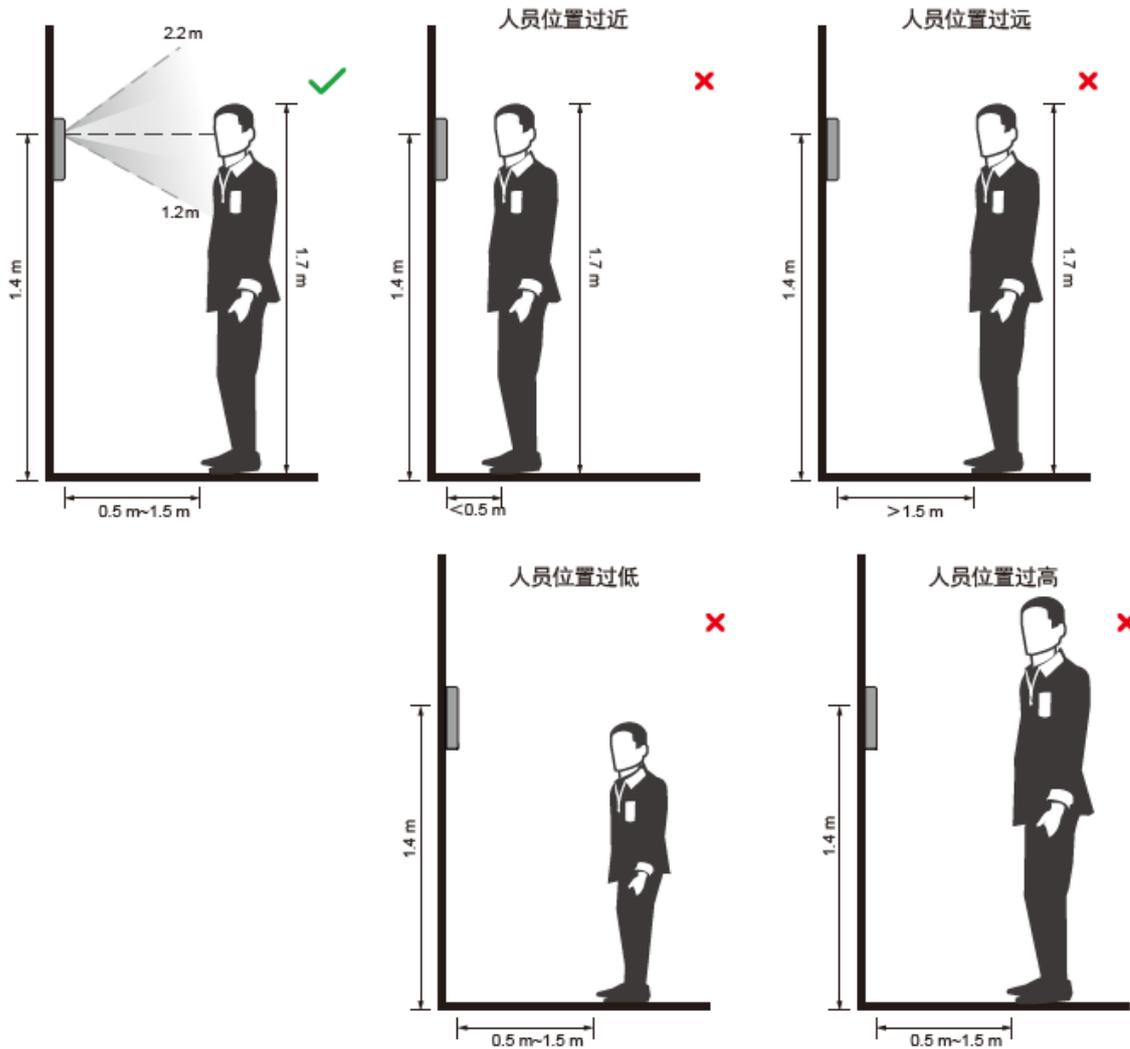
- 注册过程中请勿晃动，以免注册失败。
- 录入时请避免2张人脸同时出现在框内。

将人脸放置于采集框中心区域，设备自动抓拍，完成人脸采集。

人脸位置

人脸距离设备过高、过低、过近或者过远，均会影响录入和比对的效果，请参照正确示例录入和比对。

附录图1-2 人脸位置示意



人脸要求

为了保证人脸录入和比对的精确度，请注意以下事项。

- 请保持脸部清洁，建议露额，头发不要遮挡。
- 请勿戴眼镜、戴帽子、胡须过长或者面积过大，以及佩戴影响人脸特征采集的饰品。
- 请双眼睁开、表情自然，请勿偏头、侧面、仰头和低头。
- 录入和比对时，请将人脸尽量位于窗口中心位置，请勿过近或者过远。

附录图1-3 头部示意



附录图1-4 人脸位于窗口示意



录入说明

- 使用设备录入人脸时，录入过程中请勿晃动，以免录入失败。
- 通过软件平台导入图片时，请参考导入模板；图片像素范围处于 $150 \times 300 \leq \text{分辨率} \leq 600 \times 1200$ 之间，建议图片像素在500×500像素以上，小于100 KB，图片名称与人员编号一致。
- 人脸在图片中的占比要求大于整张图片的1/3，小于整张图片的2/3，整张图片的宽：高之比不超过1：2。

附录2 指纹录入说明

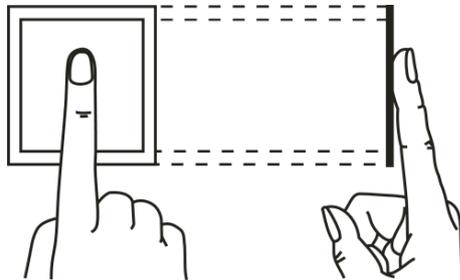
注意事项

- 指纹录入前手指及指纹采集面板应保持清洁，不沾油污、不沾水。
- 录入指纹时，手指平压于指纹采集窗口上，指纹纹心尽量对正窗口中心。
- 请勿将指纹采集面板置于阳光强光直射、温度过高、湿度过高环境。
- 指纹磨平或指纹较浅，请选择其他认证方式。

按压方法

- 正确方法

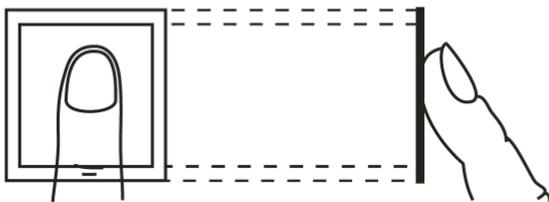
附录图2-1 正确按压示意



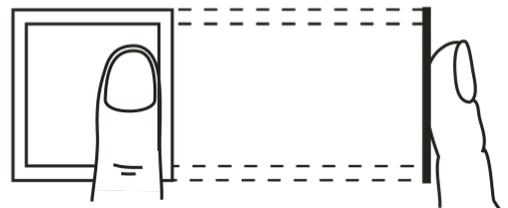
- 错误方法

附录图2-2 错误方法

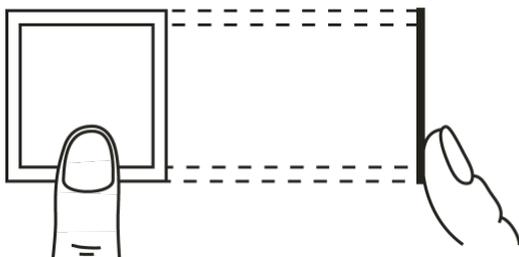
垂直



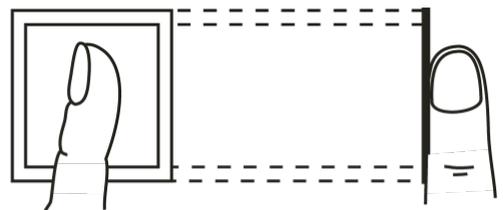
太偏



太靠下



倾斜



附录3 对讲功能操作说明

设备可作门口机使用，实现可视对讲功能。

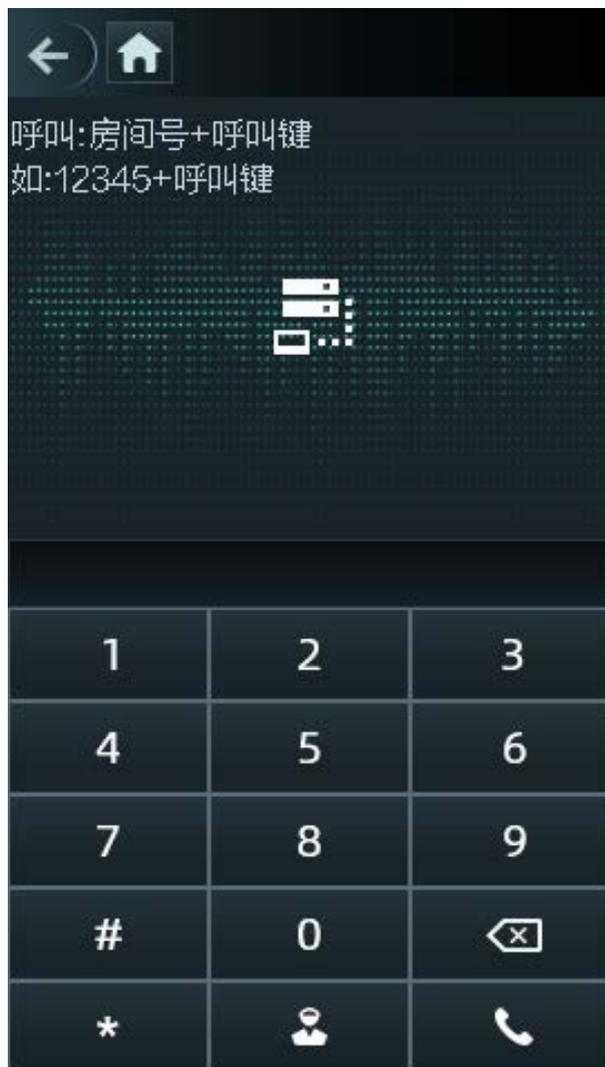
前提条件

已在门禁一体机和室内机上做好配置，实现和室内机的SIP协议互通，详细介绍请参见“3.5 对讲设置”。

操作步骤

- 步骤1 在待机界面，按。
- 步骤2 输入室内机房间号，按。

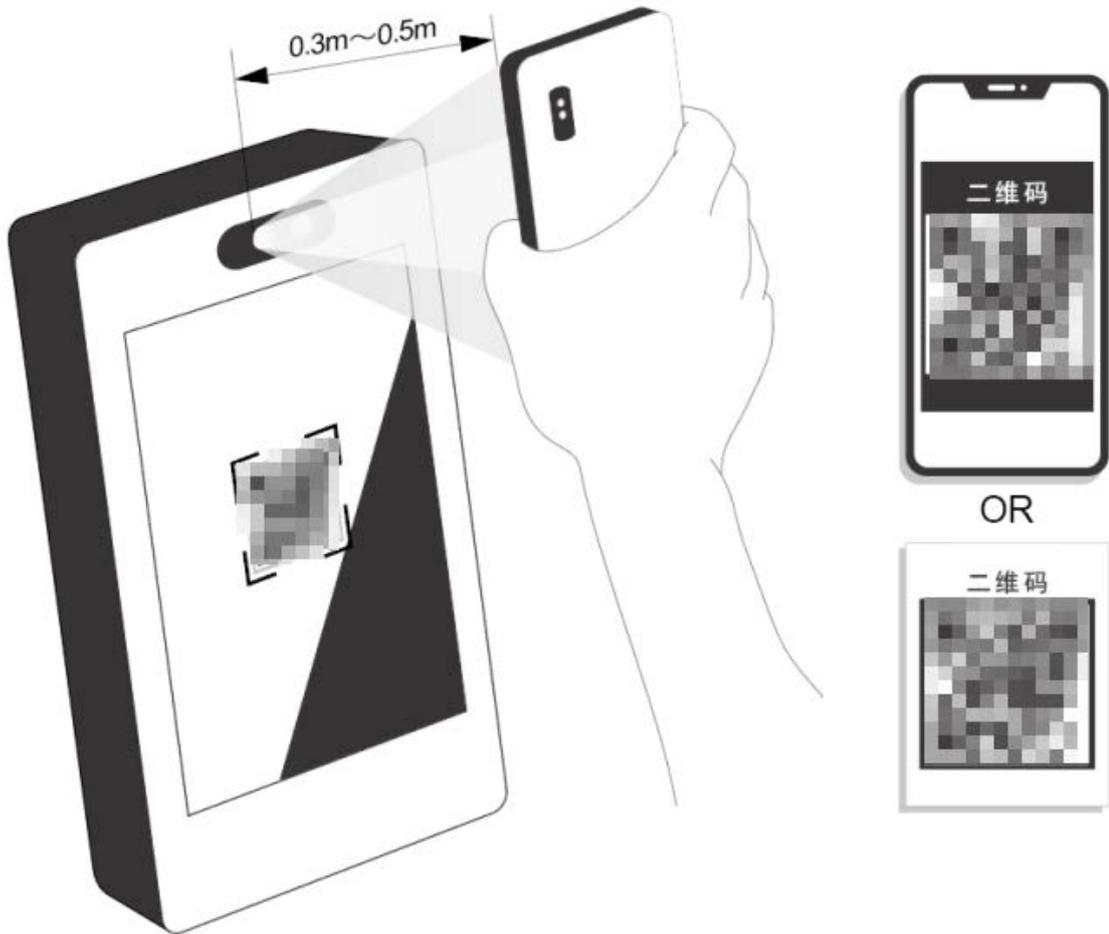
附录图3-1 呼叫室内机



附录4 扫描二维码说明

为了保证二维码扫描效果，请将二维码距离设备的摄像头或自带的二维码模块0.3 m~0.5 m，二维码大小应不小于30 mm×30 mm，二维码字节容量应小于100字节，并且需要保证二维码纸张平整。

附录图4-1 二维码与摄像头距离



附录5 法律声明

商标声明

- **HDMI™**：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。

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预览区域的存在，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6 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：

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。

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. 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。

8. 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。

9. 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。

10. 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。

11. 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。

12. 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。

13. 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。