

# 人脸门禁一体主机 使用说明书






# 前言

本文档详细介绍产品本地操作、WEB 操作和软件操作等内容，使用产品前请仔细阅读，阅读后请妥善保存文档以便日后查阅。

## 符号约定

在本文档中可能出现下列标识，代表的含义如下。

标识	说明
 <b>警告</b>	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。
 <b>注意</b>	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。
 <b>说明</b>	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	说明书优化。	2022.01
V1.0.2	<ul style="list-style-type: none"><li>更新错误。</li><li>更新使用安全须知。</li></ul>	2021.07
V1.0.1	更新“10 寸设备”章节，增加一个 10 寸设备。	2020.12
V1.0.0	首次发布。	2020.09

# 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



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！



- 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
<b>第 1 章 产品概述 .....</b>	<b>1</b>
1.1 产品简介 .....	1
1.2 功能特点 .....	1
1.3 应用场景 .....	1
<b>第 2 章 本地操作 .....</b>	<b>3</b>
2.1 基本配置流程 .....	3
2.2 常用按键 .....	3
2.3 设备初始化 .....	4
2.4 待机界面 .....	4
2.5 登录主菜单 .....	5
2.6 开门方式 .....	7
2.6.1 卡开门 .....	7
2.6.2 指纹开门 .....	7
2.6.3 用户密码开门 .....	7
2.6.4 管理者密码开门 .....	7
2.6.5 人脸开门 .....	7
2.6.6 二维码开门 .....	8
2.6.7 人证比对开门 .....	8
2.7 人员管理 .....	8
2.7.1 新建用户 .....	8
2.7.2 用户列表和管理员列表 .....	9
2.7.3 管理者密码 .....	11
2.8 门禁管理 .....	11
2.8.1 时间段管理 .....	12
2.8.2 开门模式管理 .....	18
2.8.3 配置报警 .....	22
2.8.4 配置门状态 .....	23
2.8.5 配置门锁保持时间 .....	23
2.9 通讯设置 .....	23
2.9.1 配置网络 .....	23
2.9.2 配置串口 .....	26
2.9.3 配置韦根 .....	26
2.10 系统设置 .....	27
2.10.1 设置时间 .....	27
2.10.2 设置人脸参数 .....	28
2.10.3 设置图像模式 .....	29
2.10.4 设置补光灯模式 .....	30
2.10.5 设置补光灯亮度 .....	30
2.10.6 设置音量 .....	31
2.10.7 设置指纹参数 .....	32

2.10.8 设置红外亮度 .....	33
2.10.9 恢复出厂设置 .....	34
2.10.10 重启设备 .....	35
2.11 U 盘管理 .....	35
2.11.1 U 盘导出 .....	35
2.11.2 U 盘导入 .....	36
2.11.3 U 盘升级 .....	36
2.12 功能设置 .....	36
2.12.1 功能设置 .....	36
2.12.2 隐私设置 .....	37
2.12.3 提示功能 .....	38
2.13 记录管理 .....	41
2.14 自动测试 .....	42
2.15 系统信息 .....	43
2.15.1 数据容量 .....	43
2.15.2 设备版本 .....	43
<b>第 3 章 WEB 操作 .....</b>	<b>44</b>
3.1 设备初始化 .....	44
3.2 登录 .....	46
3.3 重置密码 .....	46
3.4 报警联动 .....	48
3.4.1 报警联动 .....	48
3.4.2 报警记录 .....	49
3.5 对讲设置 .....	50
3.5.1 本机设置 .....	50
3.5.2 SIP 服务器 .....	52
3.5.3 门口机管理 .....	55
3.5.4 室内机管理 .....	56
3.5.5 管理机设置 .....	58
3.5.6 在线状态 .....	59
3.5.7 通话记录 .....	60
3.6 数据容量 .....	60
3.7 视频设置 .....	60
3.7.1 视频设置 .....	60
3.7.2 动检设置 .....	66
3.7.3 图像模式 .....	67
3.7.4 局部编码 .....	68
3.8 人脸检测 .....	68
3.9 网络设置 .....	70
3.9.1 TCP/IP .....	70
3.9.2 端口 .....	71
3.9.3 主动注册 .....	72
3.9.4 P2P .....	72
3.9.5 (可选) 4G .....	73
3.10 安全管理 .....	75
3.10.1 IP 权限 .....	75

3.10.2 系统服务.....	77
3.11 语音管理.....	81
3.12 用户管理.....	82
3.12.1 用户管理.....	82
3.12.2 ONVIF 用户.....	83
3.13 自动维护.....	85
3.14 配置管理.....	86
3.14.1 配置导出.....	86
3.14.2 配置导入.....	86
3.15 系统升级.....	86
3.15.1 文件升级.....	87
3.15.2 在线升级.....	87
3.16 版本信息.....	87
3.17 在线用户.....	88
3.18 系统日志.....	88
3.18.1 查询日志.....	88
3.18.2 备份日志.....	88
3.18.3 管理员记录.....	89
3.19 退出.....	89
<b>第 4 章 SmartPSS Plus 配置.....</b>	<b>90</b>
4.1 登录客户端.....	90
4.2 添加设备.....	90
4.2.1 搜索添加.....	90
4.2.2 手动添加.....	91
4.3 添加人员.....	92
4.3.1 设置发卡类型.....	92
4.3.2 单个添加.....	93
4.3.3 批量添加.....	94
4.4 添加门禁权限组.....	95
4.5 分配门禁权限.....	96
4.6 门禁管理.....	97
4.6.1 远程开关门.....	97
4.6.2 设置门常开或常关.....	98
4.6.3 查看门禁详情.....	99
4.6.4 重启门禁.....	99
<b>第 5 章 FAQ.....</b>	<b>101</b>
<b>附录 1 人脸录入/比对说明.....</b>	<b>102</b>
<b>附录 2 指纹录入说明.....</b>	<b>105</b>
<b>附录 3 对讲功能操作说明.....</b>	<b>107</b>
<b>附录 4 扫描二维码说明.....</b>	<b>108</b>
<b>附录 5 法律声明.....</b>	<b>109</b>
<b>附录 6 网络安全建议.....</b>	<b>110</b>

# 第 1 章 产品概述

## 1.1 产品简介

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。

## 1.2 功能特点

- 采用 LED 液晶显示屏，7 寸设备分辨率为 1024×600，10 寸设备分辨率为 1280×800。
- 支持刷卡、指纹、人脸、密码、二维码及其组合识别方式等多种识别认证方式，支持分时段开门。
- 支持显示人脸框，并实时检测最大人脸，支持识别区域及人脸目标大小设置。
- 采用 200 万广角宽动态双目摄像头，支持自动开启补光灯以及手动调节补光灯亮度。
- 支持面部识别距离 0.3 m~2.0 m，适应 0.9 m~2.4 m 身高范围。
- 基于深度人脸识别算法，精准定位目标人脸 360 个以上关键点位置。
- 人脸验证准确率高达 99.5%，识别速度快，准确率高。
- 适应侧脸，支持人脸识别的角度为 0°~90°。
- 支持活体检测。
- 支持胁迫报警、防拆报警、闯入报警、门超时报警、非法卡超次报警。
- 支持来宾用户下发、巡逻用户下发、黑名单用户下发、VIP 用户下发、普通用户下发、特殊用户下发。
- 支持 4 种识别提示模式及多种语音提示信息，方便用户选择。

## 1.3 应用场景

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。通过一体主机识别人脸来核对身份，实现无感化通行。



图1-1 7寸B设备组网

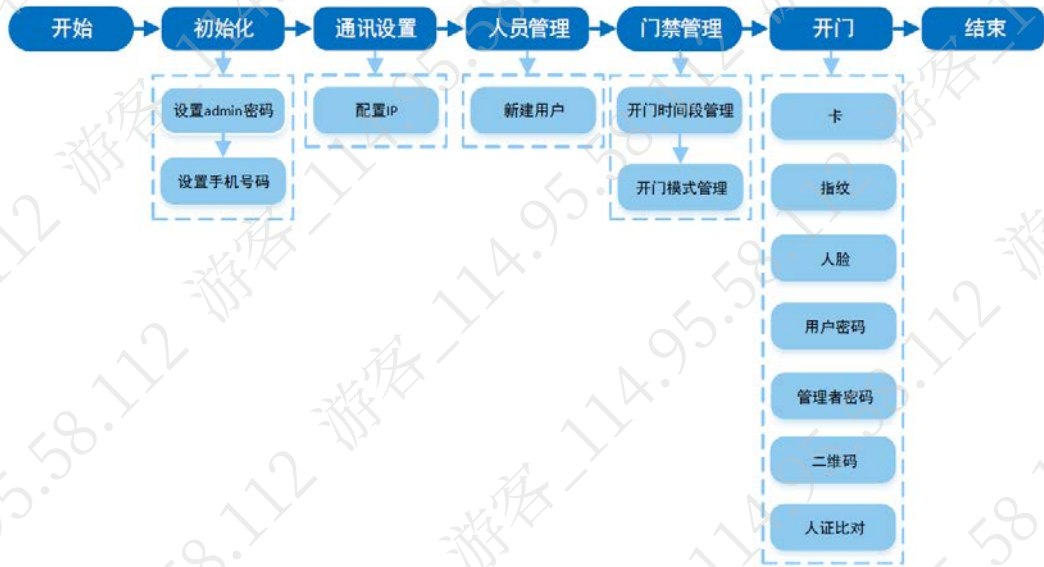


## 第 2 章 本地操作

### 2.1 基本配置流程

根据以下流程完成基本配置，即可使用人脸门禁一体主机。

图2-1 基本配置流程



### 2.2 常用按键

在配置和使用的过程中，将用到以下功能按键。

表2-1 按键说明

按键	说明
	主菜单键。
	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。

## 2.3 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，或通过 WEB 和平台登录设备。

图2-2 设备初始化

The screenshot shows a dark-themed interface for device initialization. The title '设备初始化' is at the top. Below it are four input fields: '管理员' (Administrator) with 'admin' entered, '密码输入' (Password Input), '密码确认' (Password Confirmation), and '手机' (Mobile Phone). At the bottom, there are two buttons: '确定' (Confirm) and '清除' (Clear).

### 说明

- 手机即手机号码，若忘记设备管理员用户密码，可通过该手机号重置密码。
- 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。

## 2.4 待机界面

在待机界面识别人脸、输入密码和扫描二维码开门。

### 说明

- 若您在一个界面无操作超过 30 秒，系统将返回到待机界面。
- 待机界面显示，以实际设备显示为主。


图2-3 待机界面



表2-2 待机界面说明

名称	说明
状态显示栏	显示 Wi-Fi (如果有)、网络和 U 盘等状态。
开门方式指示	显示当前设备支持的开门方式。
人脸识别区	人脸进入识别区域，识别人脸信息。
二维码开门	按该按钮，将二维码置于屏幕显示扫描框中，实现二维码开门。
对讲功能	按该按钮，进入对讲功能页面。详细介绍请参见“附录 3 对讲功能操作说明”。
密码开门	使用用户密码开门方式开门。 使用管理者密码开门方式开门。
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"> <li>• 管理员用户，验证管理员用户信息。</li> <li>• admin 用户，输入 admin 用户密码。</li> </ul>
显示日期时间	显示当前日期和时间。

## 2.5 登录主菜单


在待机界面，按 ，系统进入主菜单验证界面。

## 说明

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。

- 管理员用户，验证管理员用户信息。
- admin 用户，输入 admin 用户密码。

进入主菜单后，在设备主菜单中为设备设置相应的参数，操作步骤如下。

步骤1 在待机界面，按 。

## 说明

设备不同支持的开门方式不同，请以实际界面为准。

步骤2 选择登录方式。

- 人脸，选择后直接刷管理员人脸进入主菜单。
- 刷卡，选择后直接刷管理员卡进入主菜单。
- 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。

图2-4 主菜单





## 2.6 开门方式

### 2.6.1 卡开门


将已下发的门禁卡放入刷卡区域，即可开门。

### 2.6.2 指纹开门

将已录入的指纹对应的手指按在指纹区域，即可开门。

### 2.6.3 用户密码开门

使用设置的用户密码开门。



- 步骤1 在待机界面，按 。  
屏幕显示密码类型选择界面。
- 步骤2 按“密码开门”。
- 步骤3 输入用户 ID 和密码，按“确定”。  
设备提示开门成功。

### 2.6.4 管理者密码开门

使用管理者密码开门。管理者密码比用户密码权限更高。使用管理者密码时，不受用户、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。一台设备仅支持设置一个管理者密码。

#### 说明

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，详细介绍请参见“2.7.3 管理者密码”。


- 步骤1 在主界面，按 。  
屏幕显示密码类型选择界面。
- 步骤2 按“管理者密码开门”。
- 步骤3 输入管理者密码，按  保存。  
设备提示开门成功。

### 2.6.5 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。

## 2.6.6 二维码开门

通过扫描访客机生成的打印纸条二维码，使用二维码开门。

- 步骤1 在主界面按。  
主界面显示二维码扫描框。
- 步骤2 纸条对准摄像头，确保二维码完整显示在屏幕框中。
- 步骤3 设备识别二维码，验证通过即可开门。

## 2.6.7 人证比对开门

支持人证的设备可以在设备刷卡区刷身份证开门，开门模式设置参见“2.8.2.4 人证模式”。

## 2.7 人员管理

通过人员管理功能，您可以添加用户并设置用户类型、用户权限等。

### 2.7.1 新建用户

通过录入编号、姓名、人脸等信息添加新用户，并为用户设置权限、有效期等信息。


- 步骤1 在待机界面中，按。
- 步骤2 使用管理员权限登录系统，选择“人员管理 > 新建用户”。
- 步骤3 设置参数项。


图2-5 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2-3 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。详细介绍请参见“2.8.3 配置报警”。</p> <p> <b>说明</b></p> <ul style="list-style-type: none"> <li>● 不建议将第一枚指纹设置为胁迫指纹。</li> <li>● 仅带有指纹功能的设备支持指纹开门功能。</li> </ul>
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。详细介绍请参见“附录 1 人脸录入/比对说明”。
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。详细介绍请参见“2.8.3 配置报警”。</p>
密码	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。
用户权限	<p>设置用户权限。</p> <ul style="list-style-type: none"> <li>● 用户，仅有门禁权限。</li> <li>● 管理员，可登录系统，配置设备相关参数。</li> </ul>
时段	为用户添加门禁时段序号，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	为用户配置假日时段序号，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。
用户类型	<p>用户类型可设置为以下类型：</p> <ul style="list-style-type: none"> <li>● 普通用户，该类型用户可以正常使用门禁权限。</li> <li>● 黑名单用户，该类型用户进入时，后台会对服务人员进行提醒。</li> <li>● 来宾用户，该类型用户有门禁使用次数/时间的限制，超过使用次数/时间后，门禁权限失效。</li> <li>● 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。</li> <li>● VIP 用户，当该类型用户进入时后台对服务人员进行提醒。</li> <li>● 特殊用户，当该类型用户进入时，开门持续时间增加 5 s。</li> </ul>
使用次数	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 参数配置完成后，按  保存。

系统提示“添加用户成功”。

## 2.7.2 用户列表和管理员列表

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。

在主菜单界面，选择“人员管理 > 用户列表”或者“人员管理 > 管理员列表”，屏幕显示所有用户或者管理员信息。





图2-6 用户列表







图2-7 管理员列表



表2-4 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"> <li>: 表示人脸方式。</li> <li>: 表示指纹方式。</li> <li>: 表示刷卡方式。</li> <li>: 表示密码方式。</li> </ul>
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，查询用户信息。
- 删除用户
  - ◇ 选择用户，在编辑用户界面，按 ，删除该用户。
  - ◇ 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。

### 2.7.3 管理者密码

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

步骤1 登录主菜单界面。

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。

步骤4 启用管理者密码。

图2-8 管理者密码



### 2.8 门禁管理

对门分时段管理、设置开门模式、报警、状态和门保持时间等。

按“门禁管理”进入门禁管理界面。

图2-9 门禁管理



## 2.8.1 时间段管理

通过该功能，您可以设置门禁的时间段，包括假日时段、常开时间段和常闭时间段等。

图2-10 时间段管理



### 2.8.1.1 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。

步骤1 登录主菜单界面。

步骤2 选择“门禁管理 > 时间段管理 > 时段配置”。

步骤3 在屏幕右上角按 ，新建时段。

图2-11 时段配置






步骤4 按对应参数进入设置。

图2-12 新建时段



表2-5 时段配置参数说明

参数	说明
编号	输入时段编号，范围为 0~127，按  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  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  保存。

步骤5 按  保存时段配置。

屏幕提示“保存成功”，显示时段配置列表。

### 说明

按 ，删除该时段配置。

### 2.8.1.2 配置假日组

将假日分组，为假日组设置不同的假日计划。可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。

步骤1 登录主菜单界面。

步骤2 选择“门禁管理 > 时间段管理 > 假日组配置”。

步骤3 按 ，新建假日组。

图2-13 假日组配置



步骤4 按对应参数进入设置。

图2-14 新建假日组

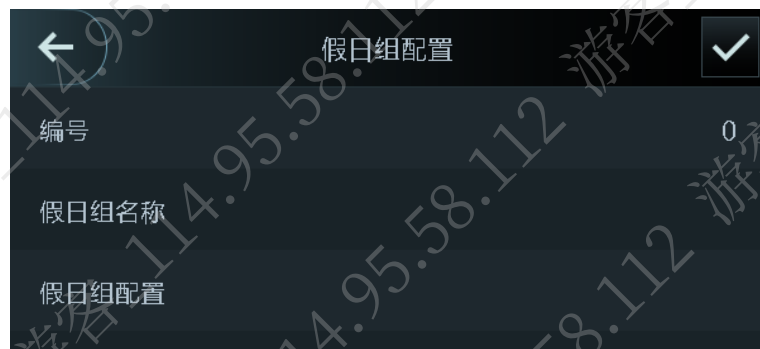




表2-6 时段配置参数说明

参数	说明
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。

步骤5 按“假日组配置”，在假日组中添加假日。

图2-15 添加假日



1. 按 , 新建假日。

图2-16 配置假日时段




2. 设置“序号”、“假日名称”、“开始时间”和“结束时间”，按  保存。

图2-17 假日列表



### 说明

按 , 删除对应假日。

3. 您可以按  继续添加假日，在列表界面按  保存。



返回到新建假日组界面。


步骤6 按  保存。

屏幕提示“保存成功”，显示假日组列表，显示所有假日组。

图2-18 假日组列表



### 说明

- 若需要在假日组内增加假日，在列表中选择对应的组，按“假日组配置”即可添加。
- 按 ，删除对应假日组。

## 2.8.1.3 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。

步骤1 登录主菜单界面。

步骤2 选择“门禁管理 > 时间段管理 > 假日计划配置”。

步骤3 按 ，添加假日计划。

图2-19 假日计划






步骤4 按对应参数进入设置。

图2-20 添加假日计划



表2-7 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  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“2.8.1.2 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  保存。

步骤5 按  保存假日计划。

图2-21 假日计划列表



### 说明

按 ，删除对应假日计划。




#### 2.8.1.4 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。

步骤1 登录主菜单界面。

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。



#### 说明

常开（常闭）时间段的权限高于其他时间段权限。


#### 2.8.1.5 配置常闭时间段

设置常闭时段后，门禁在该时段内一直处于关闭状态。

步骤1 登录主菜单界面。

步骤2 选择“门禁管理 > 时间段管理 > 常闭时间段配置”。

屏幕显示“常闭时间段配置”界面。

步骤3 输入预先在“时段配置”中配置好的时段编号，按保存。


#### 2.8.1.6 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。

步骤1 登录主菜单界面。

步骤2 选择“门禁管理 > 时间段管理 > 远程验证时间段配置”。

屏幕显示“远程验证时间段配置”界面。

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 启用远程验证时间段。

### 2.8.2 开门模式管理

开门模式包括任意组合开门、分时段开门和多人组合开门模式。所选购的设备型号不同，开门方式会有差异，具体请以设备实际显示为准。

#### 2.8.2.1 任意组合开门

使用刷卡、指纹、人脸和密码任意一种或者多种组合的方式开门。

步骤1 登录主菜单界面。

步骤2 选择“门禁管理 > 开门模式管理 > 任意组合开门”。



#### 说明

设备不同支持的开门方式不同，请以实际界面为准。

步骤3 选择门禁组合元素。

再次按已选元素，从组合中删去该元素。

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2-22 任意组合开门



步骤5 按  保存。

屏幕返回到“开门模式管理”界面。

步骤6 启用任意组合开门。

### 2.8.2.2 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。

步骤1 登录主菜单界面。

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。

图2-23 分时段开门配置



步骤4 按  保存。

屏幕返回到“开门模式管理”界面。

步骤5 启用分时段开门。

### 2.8.2.3 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。

步骤1 登录主菜单界面。

步骤2 选择“门禁管理 > 开门模式管理 > 多人组合开门”。

图2-24 多人组合开门






步骤3 按  新建组。

图2-25 新建组



表2-8 新建组参数说明

参数	说明
用户列表	<p>在新建组中添加开门授权人员。</p> <ol style="list-style-type: none"> <li>按“用户列表”。</li> <li>屏幕显示“用户列表”界面。</li> <li>按 , 输入已有用户的用户 ID。</li> <li>按  保存。</li> </ol>
开门方式	选择开门方式, 包括卡、指纹、人脸和密码。
有效人数	<p>有效人数即授权人数。达到有效人数后, 才可开门。</p> <ul style="list-style-type: none"> <li>有效人数不能大于人员总数。</li> <li>当有效人数等于人员数时, 需组内所有人员开门后, 开门成功。</li> <li>当有效人数小于人员数时, 组内任意人员达到有效人数即可, 均开门后, 开门成功。</li> </ul>

步骤4 按 .

返回上一层菜单。

步骤5 按  保存。

屏幕提示“设置成功”。

步骤6 启用多人组合开门。

## 2.8.2.4 人证模式

### 说明

仅支持人证的设备支持此功能。

您可以根据需要选择开门方式。

在主菜单界面, 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2-26 人证模式



## 2.8.3 配置报警


通过报警设置，管理员可对来访人员的门禁权限进行有效的控制。


- 步骤1 登录主菜单界面。
- 步骤2 选择“门禁管理 > 报警设置”。
- 步骤3 设置报警参数。

图2-27 报警设置



表2-9 报警设置参数说明

参数	说明
反潜	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。 <ul style="list-style-type: none"> <li>● 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。</li> <li>● 若人员进门时未验证身份，直接验证出门，会触发报警。</li> </ul>
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	当未授权卡 50 s 内连续刷卡超过 5 次后，再次刷卡将引发报警。
闯入	门磁未打开的情况下，异常开门，会产生闯入报警。  <b>说明</b> 仅当门磁启动开启后，闯入报警生效。

参数	说明
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。 门超时时间可设置范围为：1 s~9999 s。</p> <p> <b>说明</b></p> <p>仅当门磁启动开启后，门超时报警生效。</p>
门磁启动	开启门磁。

## 2.8.4 配置门状态

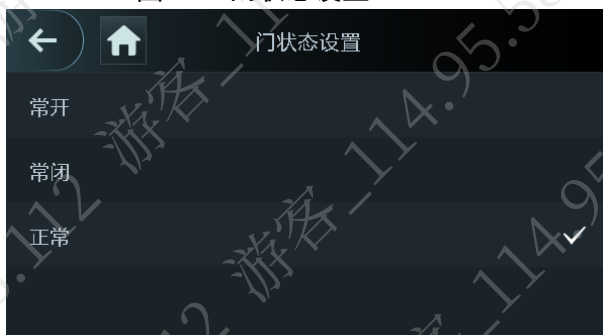
设置门禁的状态为正常、常开或常闭。

步骤1 登录主菜单界面。

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。

图2-28 门状态设置



- 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。

## 2.8.5 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。

步骤1 登录主菜单界面。

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。

## 2.9 通讯设置

配置网络、串口和韦根参数，确保设备能够正常接入网络，串口和韦根通讯正常。

### 2.9.1 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。



### 2.9.1.1 配置 IP

配置设备 IP 地址，使设备接入网络。

步骤1 登录主菜单界面。



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2-29 IP 设置



表2-10 IP 设置参数说明

参数	说明
IP 地址、子网掩码、网关地址	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。  <b>说明</b> 双网卡设备支持两个 IP 的设置。
启/禁用 DHCP	DHCP（Dynamic Host Configuration Protocol 动态主机配置协议）。 启用 DHCP 功能，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。

参数	说明
云睿使能	默认开启。启用云睿使能，P2P 一直开启；禁用云睿使能，可以手动开启或者关闭 P2P 使能。  <b>说明</b> P2P 开启时，支持使用手机扫描二维码将设备添加到相关平台和手机 App 上。

### 2.9.1.2 主动注册

主动注册功能可以使设备对接管理平台，通过管理平台管理设备。

步骤1 登录主菜单界面。

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界面，按  保存。

图2-30 主动注册



表2-11 主动注册参数说明

名称	参数
服务器 IP 地址	配置平台的 IP 地址。
端口	配置平台的端口号。
子设备 ID	配置平台子设备编号。

步骤4 启用主动注册。

### 2.9.1.3 Wi-Fi

通过无线网络将设备接入到网络。

#### 说明

具有 Wi-Fi 模块的设备具有此功能，具体以实物为主。

步骤1 登录主菜单界面。


步骤2 选择“通讯设置 > 网络设置 > WiFi”。



图2-31 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。

返回“WiFi”界面，显示所连接 Wi-Fi 的信息。

## 2.9.2 配置串口

根据连接设备的用途，选择输入输出方式。

登录主菜单界面，选择“通讯设置 > 串口设置”。

图2-32 串口设置



- 当外接其他识读设备时，选择“串口输入”，人脸门禁一体主机可通过外接读卡器设备，将门禁卡信息发送给主机或管理平台。
- 当设备本身作为识读设备时，选择“串口输出”，人脸门禁一体主机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，则按照用户第一张卡卡号，输出对应数据。
- 当外接 OSDP 协议的读卡器时，选择“OSDP 输入”，人脸门禁一体主机可通过外接读卡器设备，将门禁卡信息发送给主机或管理平台。

## 2.9.3 配置韦根

根据连接设备的用途，选择输入输出方式。

登录主菜单界面，选择“通讯设置 > 韦根设置”。

- 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。

图2-33 韦根设置



表2-12 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"> <li>• 韦根 26，识别 3 个字节，6 位。</li> <li>• 韦根 34，识别 4 个字节，8 位。</li> <li>• 韦根 66，识别 8 个字节，16 位。</li> </ul>
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"> <li>• 编号，若选择编号，则按照用户的编号，输出对应数据。</li> <li>• 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。</li> </ul>

## 2.10 系统设置

### 2.10.1 设置时间








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。

- 步骤1 登录主菜单界面。
- 步骤2 选择“系统设置 > 时间设置”。
- 步骤3 选择需要设置的参数。

图2-34 时间设置



表2-13 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"> <li>按“日期设置”。</li> <li>输入年月日。</li> <li>按  保存。</li> </ol>
时间设置	<ol style="list-style-type: none"> <li>按“时间设置”。</li> <li>输入时间。</li> <li>按  保存。</li> </ol>
日期格式	<ol style="list-style-type: none"> <li>按“日期格式”。</li> <li>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。</li> <li>按  保存。</li> </ol>
夏令时设置	<ol style="list-style-type: none"> <li>按“夏令时设置”。</li> <li>按启用后面的开关，显示  表示启用。</li> <li>按“夏令时类型”，选择按周或者按月。</li> <li>按“开始时间”和“结束时间”，设置时间。</li> </ol>
NTP 校时	<p>设置 NTP 校时功能。</p> <ol style="list-style-type: none"> <li>按“NTP 校时”。</li> <li>设置参数，按  保存。 <ul style="list-style-type: none"> <li>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。</li> <li>端口，填写校时服务器的端口号。</li> <li>间隔（min），设置校时的间隔时间。</li> </ul> </li> <li>按启用后面的开关，显示  表示启用。</li> <li>按  保存。</li> </ol>
时区	根据当地时区选择。

## 2.10.2 设置人脸参数

通过设置人脸参数可以改变设备人脸识别的精准度，提升门禁防护能力。

### 说明

该参数建议由专业人员调试使用，不建议随意调整。

步骤1 登录主菜单界面。

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2-35 人脸参数设置



表2-14 人脸参数说明

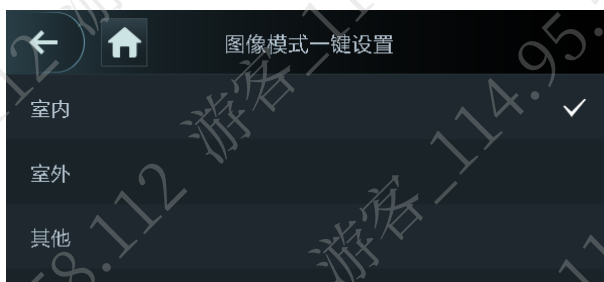
参数	说明
人脸识别阈值	设置设备识别人脸的精准度。数值越大，精准度越高。
人脸识别最大偏角	设置设备拍摄人侧脸的角度。数值越大，识别的侧脸范围越大。
眼间距	双眼之间的像素值，与人脸大小、人脸与镜头距离相关。 比如：一般成年人距离镜头 1.5 m 时，眼间距为 50 px~70 px。
有效人脸间隔时间	设置同一有权限人员在同一台设备上识别，重复提示识别成功的间隔时间。
无效人脸间隔时间	设置同一人员在同一台设备上识别，重复提示识别失败的间隔时间。
防假使能	防止使用有权限人员的照片、模型等冒用人脸信息情况的发生。 <ul style="list-style-type: none"> <li>● 关闭：关闭防假使能。</li> <li>● 普通、高：设置防假使能等级。</li> </ul>
人证阈值	将采集到的人脸与身份证中照片比对，阈值越大，人脸相似度越大，但是识别成功率越低。  <b>说明</b> 仅支持人证的设备有此参数。

### 2.10.3 设置图像模式

根据实际的使用环境，自行设置图像的模式。

登录主菜单界面，选择“系统设置 > 图像模式一键设置”。

图2-36 图像模式一键设置



- 室内，正常室内场景。
- 室外，正常室外场景。
- 其他，过道、半户外等逆光场景。

## 2.10.4 设置补光灯模式

根据实际的使用环境，自行设置补光灯的模式。

登录主菜单界面，选择“系统设置 > 补光灯模式设置”。

图2-37 补光灯模式设置



- 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。
- 常开，补光灯处于常亮状态。
- 常闭，不开启补光灯，补光灯常闭。

## 2.10.5 设置补光灯亮度

根据实际使用环境，设置补光灯的亮度。

步骤1 登录主菜单界面。

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。

图2-38 补光灯亮度设置



## 2.10.6 设置音量

根据实际的使用需求，调节设备语音播报或麦克风录音的音量。

步骤1 登录主菜单界面。

步骤2 选择“系统设置 > 音量设置”。

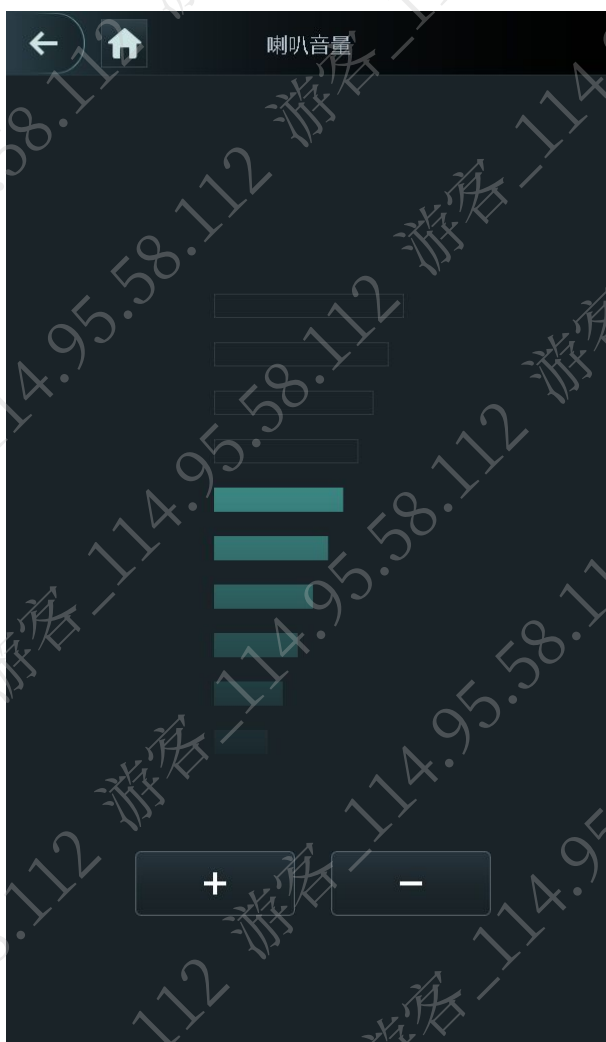
界面显示喇叭音量和麦克风音量。

步骤3 按“喇叭音量”或“麦克风音量”。

步骤4 按  或  调节音量。



图2-39 喇叭音量设置



### 2.10.7 设置指纹参数

#### 说明

仅支持指纹功能的设备由此参数。

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。

步骤1 登录主菜单界面。

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2-40 指纹参数设置



### 2.10.8 设置红外亮度

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。

步骤1 登录主菜单界面。

步骤2 选择“系统设置 > 红外亮度设置”。

步骤3 按  或  调节阈值等级。



图2-41 红外亮度设置



### 2.10.9 恢复出厂设置



#### 注意

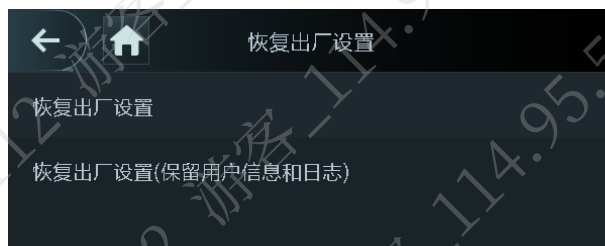
执行恢复出厂设置，会导致数据丢失，请谨慎操作。

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。

登录主菜单界面，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2-42 恢复出厂设置



## 2.10.10 重启设备

登录主菜单界面，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。

## 2.11 U 盘管理



### 注意

- 导出用户信息和升级前请确认已插入 U 盘，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。

将用户信息导出或导入至 U 盘中，也可以通过 U 盘对系统执行升级操作。

### 2.11.1 U 盘导出

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。

步骤1 登录主菜单界面。

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2-43 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。

## 2.11.2 U 盘导入

仅支持从一个设备中导出的数据，导入到另一台设备中。

- 步骤1 登录主菜单界面。
- 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2-44 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。

## 2.11.3 U 盘升级

通过 U 盘对系统执行升级操作。

- 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 登录主菜单界面。
- 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。

## 2.12 功能设置

### 2.12.1 功能设置

登录主菜单界面，按“功能设置”。

图2-45 功能设置



表2-15 功能设置

参数	说明
隐私设置	一些信息涉及隐私，通过该界面根据实际情况选择开启或者关闭。具体请参见“2.12.2 隐私设置”。
卡号反转	用韦根输出对接第三方设备时，获取的卡号顺序与实际卡号顺序不一致时，可开启该功能。
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。
门磁类型	设置门磁状态。 <ul style="list-style-type: none"> <li>● 常开：门磁信号线短路标示门开。</li> <li>● 常闭：门磁信号线断开标示门开。</li> </ul>
提示功能	设置“极速模式”、“简易模式”、“标准模式”或“对比模式”。具体请参见“2.12.3 提示功能”。
语音管理	根据实际需要选择不同的语音播报提示。

## 2.12.2 隐私设置

根据需求选择一些隐私信息功能是否开启。

步骤1 登录主菜单界面。

步骤2 按“功能设置”。

步骤3 在“功能设置”界面按“隐私设置”。

图2-46 隐私设置



表2-16 隐私设置参数说明

参数	说明
密码重置	开启密码重置功能，用户可重置密码。 本功能默认开启。
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。 <b>说明</b> 当开启 HTTPS 使能后，设备将会重启。
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；本功能默认开启。
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。
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。

### 2.12.3 提示功能

检测结果的提示功能，根据自己的需要设置显示模式，即“对比模式”、“标准模式”、“简易模式”、“极速模式”四种方式的对比分析。



图2-47 提示功能



### 说明

以上四种模式为四选一，不可多选。

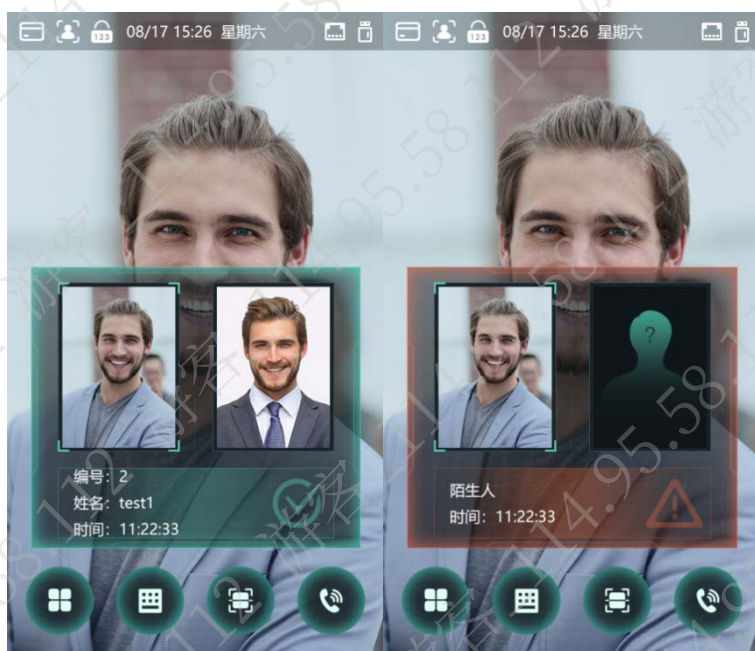
## 对比模式

将“提示功能”设置为“对比模式”，即左侧为现场抓拍的照片，右侧为底库照片，并在界面下方显示员工姓名、工号、开门时间等信息。

### 说明

左侧为识别成功显示界面，右侧为识别失败显示界面。

图2-48 对比模式





## 标准模式

将“提示功能”设置为“标准模式”，即显示底库照片主界面风格，并在界面下方显示员工姓名、工号、开门时间等信息。

### 说明

左侧为识别成功显示界面，右侧为识别失败显示界面。

图2-49 标准模式



## 简易模式

将“提示功能”设置为“简易模式”，即只显示人员信息主界面风格。

### 说明

左侧为识别成功显示界面，右侧为识别失败显示界面。

图2-50 简易模式



## 极速模式

将“提示功能”设置为“极速模式”，即只显示成功失败主界面风格。

### 说明

左侧为识别成功显示界面，右侧为识别失败显示界面。

图2-51 极速模式

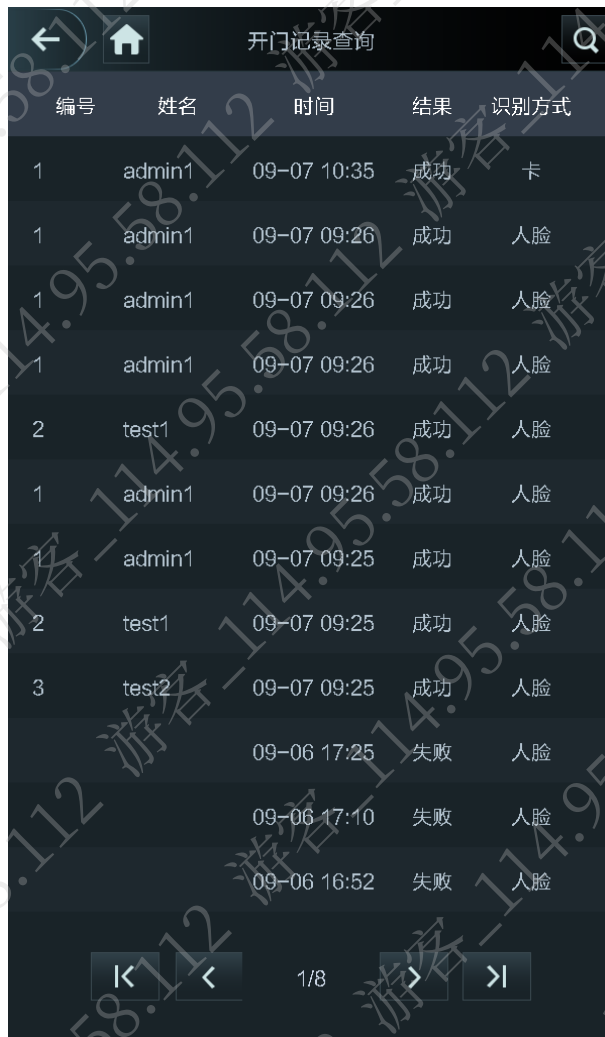


## 2.13 记录管理

通过记录管理功能，查询所有用户的开门记录。

登录主菜单界面，选择“记录管理 > 开门记录查询”，查询设备开门记录。

图2-52 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

## 2.14 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2-53 自动测试



表2-17 自动测试说明

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。
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。

## 2.15 系统信息

登录主菜单界面，在系统信息菜单中，管理员查询与该设备相关的系统信息。

### 2.15.1 数据容量

登录主菜单界面，选择“系统信息 > 数据容量”，可查看设备存储的数据情况。

### 2.15.2 设备版本

登录主菜单界面，选择“系统信息 > 设备版本”，可查看设备版本信息。



## 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。

### 3.1 设备初始化

首次登录设备 WEB 或设备恢复出厂设置后登录时，需要初始化设备。

#### 说明

请选择 IE8 以上版本的浏览器，否则将不能正常登录。

步骤1 打开 IE 浏览器，在地址栏里输入人脸一体机的 IP 地址（默认地址为 192.168.1.108），按【Enter】键。

#### 说明

- PC 与设备在同一局域网内。
- 7 寸 B 设备支持双网口，网口 1 的默认地址为 192.168.1.108，网口 2 的默认地址为 192.168.2.108。

步骤2 输入“新密码”、“确认密码”，选择“预留手机”，输入手机号码，单击“下一步”。

图3-1 设备初始化



开机向导

① 设备初始化 自动检测

用户名 admin

新密码

弱 中 强

确认密码

密码不少于8位，且至少包含数字、字母和常用字符中的两种

预留手机

(将用于密码重置,建议填写或及时完善)

下一步

## 说明

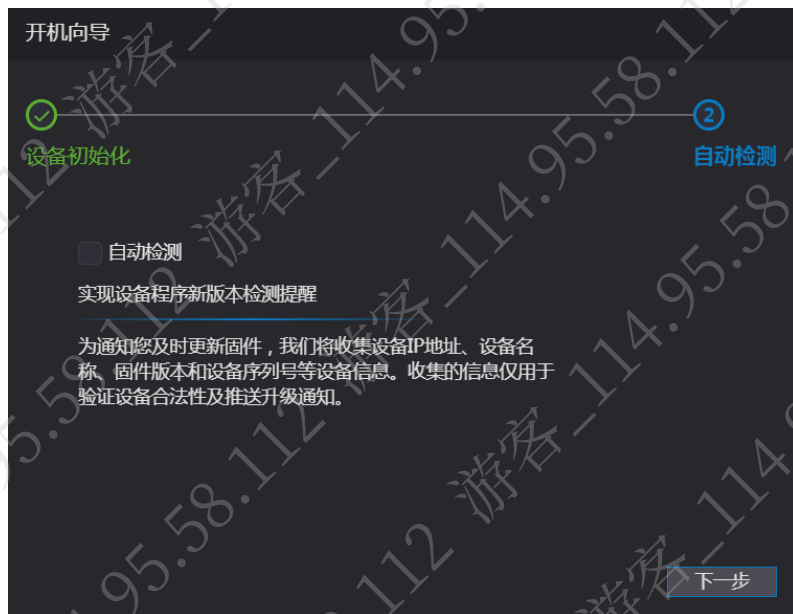
- 为确保设备安全，设备初始化后请妥善保存 admin 的登录密码，并定期修改。
- 该密码用于登录本地界面和 WEB 界面，密码可设置为 8 位~32 位非空字符，可以由大写字母、小写字母、数字和特殊字符（除“非打印字符”、“空格”、“'”、“””、“;”、“:”、“&”外）组成，且至少包含 2 类字符。新密码和确认密码需保持一致。请根据密码强弱提示设置高安全性密码。
- 扫描二维码重置密码时，需要使用预留手机接收安全码，通过安全码重置 admin 用户的密码。

步骤3 选择是否启用自动检测，单击“下一步”。

## 说明

选择复选框，表示启用。为了能够及时获取最新程序，建议您启用自动检测。

图3-2 自动检测



步骤4 单击“完成”，完成设备初始化。

图3-3 设置完成





## 3.2 登录

登录设备 WEB 系统，使用 WEB 系统中的各项功能。

步骤1 打开 IE 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3-4 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。
- 如果您遗忘了 `admin` 的登录密码，可单击“忘记密码?”重置，重置密码的详细介绍请参见“3.3 重置密码”。

步骤3 单击“登录”。

## 3.3 重置密码

当您遗忘 `admin` 用户的登录密码时，可以通过预留手机重置密码。



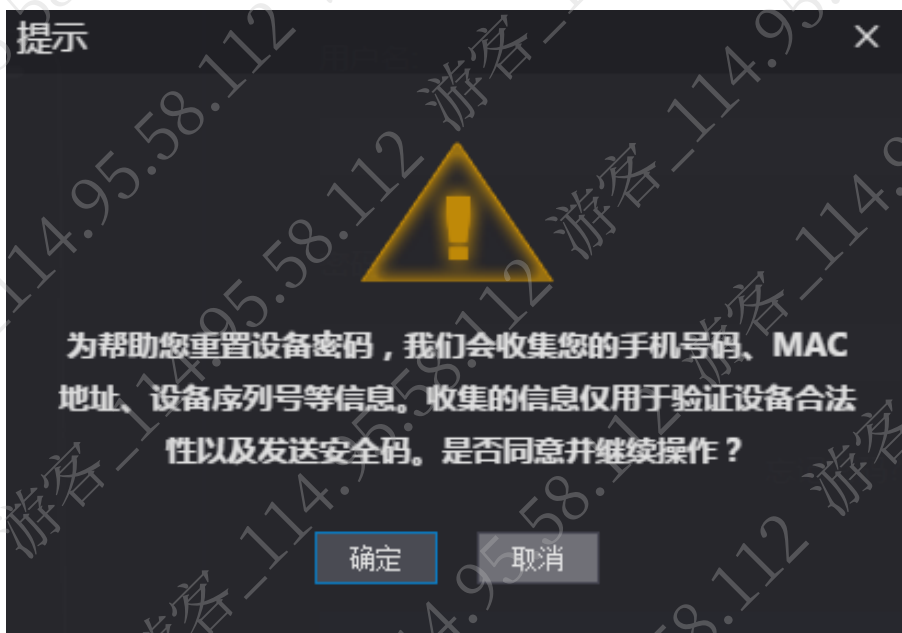
### 说明

重置密码需要在系统服务里启用“密码重置”。详细介绍请参见“3.10.2 系统服务”。

步骤1 在登录界面，单击“忘记密码”。

步骤2 在弹出的提示框中单击“确定”。

图3-5 提示



步骤3 根据界面提示扫描二维码，并获取安全码。

图3-6 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，单击“下一步”。

步骤5 重新设置“新密码”和“确认密码”。



### 说明

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6 单击“确定”，完成密码重置。

## 3.4 报警联动

设置报警输入类型，当产生报警时联动对应的报警输出和门禁状态。

### 3.4.1 报警联动

本设备支持接入报警输入设备，用户可根据需要修改报警配置的参数。

#### 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会同步到设备。

步骤1 登录设备 WEB 系统。

步骤2 选择“报警联动”。

图3-7 报警联动



报警联动

刷新

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3-8 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

确认 取消

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。
名称	自定义。
报警输入类型	<p>请根据购买的报警设备设置报警输入类型。</p> <ul style="list-style-type: none"> <li>常开，常开是指设备保持开路状态，报警时线路闭合。</li> <li>常闭，常闭是指设备保持闭合状态，报警时线路开路。</li> </ul>
消防联动启用	<p>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。</p> <p> <b>说明</b></p> <p>若启用消防联动，设备默认启用报警输出和门禁联动常开。</p>
报警输出启用	报警输出启用后，继电器可向外输出报警信息。
持续时间（秒）	报警持续时间，时间范围可设置为 1 s~300 s。
报警输出通道	人脸门禁一体主机有两路报警输出，请根据您的报警设备，选择报警输出通道。
门禁联动启用	启用后，当有报警信号输入时，设备联动门常开或常闭。通道类型可选择常开或常闭。
通道类型	<ul style="list-style-type: none"> <li>常开，当有报警信号输入时，门常开。</li> <li>常闭，当有报警信号输入时，门常闭。</li> </ul>

步骤4 单击“确认”，完成参数设置。

### 3.4.2 报警记录

通过查看报警记录，用户可以查看设备报警的类型和报警发生的时间。

步骤1 登录设备 WEB 系统。

步骤2 选择“报警联动 > 报警记录”。

图3-9 报警记录



步骤3 选择“时间范围”、“类型”，单击“查询”。

图3-10 查询结果



### 3.5 对讲设置

人脸门禁一体主机作为门口机或者围墙机使用时，可实现可视对讲功能。

#### 3.5.1 本机设置

设置设备类型和编号。

##### 3.5.1.1 本设备作为 SIP 服务器

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



图3-11 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	本设备只能作为单元门口机使用。
管理中心	设置门口机呼叫管理中心的号码，888888+3 位分机号。
编号	不可设置。



参数	说明
群呼	<p>单击 ，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。</p> <p> <b>说明</b></p> <p>设置群呼功能后，门口机会自动重启并使设置生效。</p>
传输模式	<ul style="list-style-type: none"> <li>● 模式 1：通用对讲传输模式。</li> <li>● 模式 2：用于特殊场景，群呼场景体验提升。</li> </ul>

步骤4 单击“确定”，保存设置。

### 3.5.1.2 其他设备作为 SIP 服务器

步骤1 登录设备 WEB 系统。

步骤2 选择“对讲设置 > 本机设置”。

步骤3 设置参数。

图3-12 本机设置界面-其他门口机作为 SIP 服务器

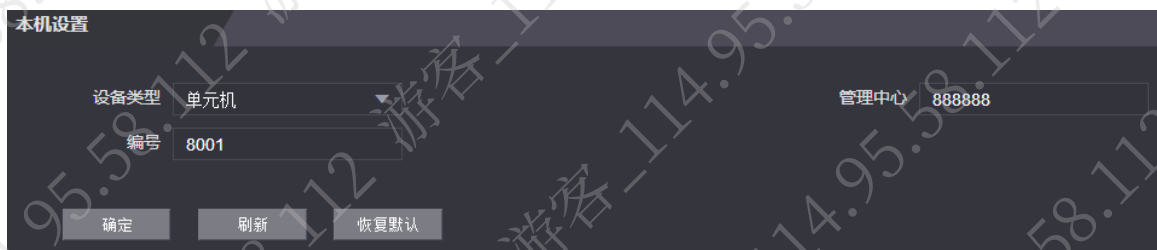



表3-3 本机参数说明 (2)

参数	说明
设备类型	本设备只能作为单元门口机使用。
管理中心	设置门口机呼叫管理中心的号码，888888+3 位分机号。
编号	<p>设置本单元门口机的编号。</p> <p> <b>说明</b></p> <ul style="list-style-type: none"> <li>● 编号为 4 位，前两位固定 80，后两位从 01 开始，如 8001。</li> <li>● 如果一个单元内有多台门口机，编号不能重复。</li> </ul>

### 3.5.1.3 平台作为 SIP 服务器

步骤1 登录设备 WEB 系统。

步骤2 选择“对讲设置 > 本机设置”。

步骤3 设置参数。



图3-13 本机设置界面-平台作为 SIP 服务器



表3-4 本机参数说明 (3)

参数	说明
设备类型	本设备可作为单元门口机和围墙机使用，根据安装位置选择。
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。
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	<p>设置本单元门口机的编号。</p> <p><b>说明</b></p> <p>如果一个单元内有多台门口机，编号不能重复。</p>
	<p><b>说明</b></p> <p>区号、幢号、单元号、编号与平台添加本设备时保持一致。</p> <ul style="list-style-type: none"> <li>区号和单元号范围是 1~99，幢号范围是 1~999。</li> <li>当设备类型为围墙机时，幢号有两种情况。                             <ul style="list-style-type: none"> <li>开启区号功能，为 999，不能修改。</li> <li>未开启区号功能，为 99，不能修改。</li> </ul> </li> <li>编号为 4 位，前两位固定 80，后两位从 01 开始，如 8001。</li> </ul>

### 3.5.2 SIP 服务器

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。

#### 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为 50 台。

#### 3.5.2.1 本设备作为 SIP 服务器

步骤1 登录设备 WEB 系统。

步骤2 选择“对讲设置 > SIP 服务器”。

步骤3 选择“启用”，图标切换为，其他参数保持默认。

图3-14 本机作为 SIP 服务器界面

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”，设备重启并开启 SIP 服务器功能。

### 3.5.2.2 其他设备作为 SIP 服务器

步骤1 登录设备 WEB 系统。

步骤2 选择“对讲设置 > SIP 服务器”。

步骤3 确认启用参数关闭状态下，选择服务器类型为“VTO”。

步骤4 设置参数。

图3-15 其他门口机作为服务器界面

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	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5 单击“确认”，保存设置。

### 3.5.2.3 平台作为 SIP 服务器

步骤1 登录设备 WEB 系统。

步骤2 选择“对讲设置 > SIP 服务器”。

步骤3 确认启用参数关闭状态下，选择服务器类型为“私有 SIP 服务器”。

步骤4 设置参数。

图3-16 平台作为 SIP 服务器界面

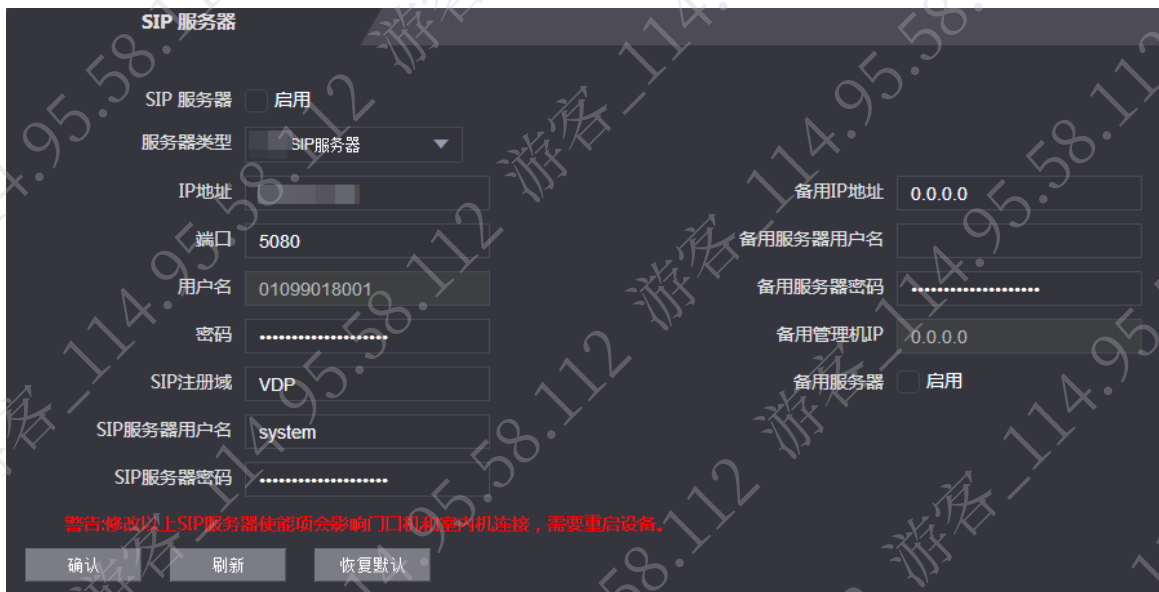



表3-6 SIP 服务器参数说明 (2)

参数	说明
IP 地址	平台的 IP 地址。
端口	默认为 5080。
用户名	输入用户名和密码，默认密码为 123456。
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	设备备用服务器后，当平台出现异常时，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。
备用服务器用户名	

参数	说明
备用服务器密码	<ul style="list-style-type: none"> <li>选择“备用服务器”，则启用本机作为备用服务器。</li> <li>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。</li> </ul>
备用服务器	
	 <b>说明</b> 建议主门口机启用“备用服务器”。
备用管理机 IP	设置备用管理机后，当平台出现异常时，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。

步骤5 单击“确认”，保存设置。

### 3.5.3 门口机管理

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。

步骤1 登录设备 WEB 系统。

步骤2 选择“对讲设置 > 门口机管理”。

步骤3 单击“添加”。

图3-17 门口机管理界面



步骤4 设置门口机参数。

图3-18 门口机添加界面

表3-7 门口机参数说明

参数	说明
编号	门口机的编号。
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	不可编辑。
IP 地址	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，默认密码为 123456。
密码	

步骤5 单击“确认”，完成添加。

### 3.5.4 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。

#### 说明

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。

#### 3.5.4.1 单个添加室内机

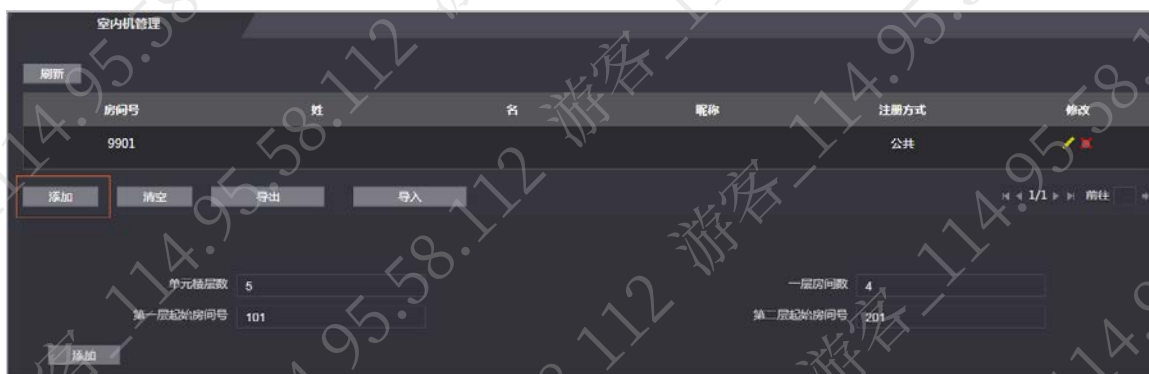
步骤1 登录设备 WEB 系统。

步骤2 选择“对讲设置 > 室内机管理”。

步骤3 单击“添加”。



图3-19 单个添加室内机




步骤4 填写用户信息。

图3-20 添加界面



表3-8 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。  <b>说明</b> <ul style="list-style-type: none"> <li>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。</li> <li>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……。</li> </ul>
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。

 **说明**

通过单击“导出”，将该设备房间号导出，保存导出的文件，然后单击“导入”，将导出的文件导入至其他设备，也可完成单个添加室内机。



### 3.5.4.2 批量添加室内机

最多添加 1024 个室内机。

步骤1 登录设备 WEB 系统。

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”。

#### 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。

图3-21 批量添加室内机



### 3.5.5 管理机设置

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 系统。

步骤2 选择“对讲设置 > 管理机设置”。

步骤3 单击“添加”。

图3-22 管理机添加界面



步骤4 设置管理机的“VTS 名称”、“注册密码”和“IP 地址”。

- VTS 名称支持 9 位数字，设置为管理机的编号。
- 注册密码为登录管理机的密码，建议使用默认值。


步骤5 单击“确认”。


图3-23 管理机添加完成界面



## 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。

## 3.5.6 在线状态

本门口机作为 SIP 服务器时，管理人员可查看接入本 SIP 服务器且正常在线的设备信息。

步骤1 登录设备 WEB 系统。

步骤2 选择“对讲设置 > 在线状态”。

图3-24 在线状态

序号	房间号	在线状态	IP:端口号	注册时间	断线时间
1	8001	离线	:5060	2020-05-11 08:38:04	2020-05-11 08:38:44
2	9901	在线	:5060	2020-05-12 19:47:00	2020-05-12 19:45:03

### 3.5.7 通话记录

用于查看门口机的呼叫、通话等记录，最多可保存 1024 条记录。

步骤1 登录设备 WEB 系统。

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3-25 通话记录界面

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	叮出	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 数据容量

登录设备 WEB 系统，选择“数据容量 > 数据容量”，可查看设备存储的数据情况。

## 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 视频设置

在视频设置菜单中设置视频码流、图像、曝光等参数。

- 视频制式：选择 P 制。

### 说明

- P 制：PAL 制式，默认码流是 25 帧/秒。

- **N制**：NTSC制式，默认码流是30帧/秒。
- 通道1：可设置该通道可见光视频码流、图像、曝光等参数。
- 通道2：可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 通道1视频参数设置

#### 3.7.1.1.1 码流设置

- 步骤1 登录设备WEB系统。
- 步骤2 选择“视频设置 > 视频设置”。
- 步骤3 选择通道号“1”，单击“码流”页签。
- 步骤4 设置码流参数。

图3-26 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。 本设备的视频格式支持 D1、VGA、720P、1080P。
	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。



#### 3.7.1.1.2 图像设置

- 步骤1 登录设备WEB系统。
- 步骤2 选择“视频设置 > 视频设置”。
- 步骤3 选择通道号“1”，单击“图像”页签。
- 步骤4 设置图像参数。

图3-27 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。  <b>说明</b> 该值不会影响图像的整体亮度。
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"> <li>● 关闭：不设置任何模式。</li> <li>● 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。</li> <li>● 晴天：设置为晴天模式时，图像色调将被降低。</li> <li>● 晚上：设置为晚上模式时，图像色调将被提高。</li> </ul>
日/夜模式	日夜模式影响设备的补光状态。 <ul style="list-style-type: none"> <li>● 自动：根据镜头感光程度，自动调节模式，使图像颜色正常。</li> <li>● 彩色：图像色调显示为彩色。</li> <li>● 黑白：图像色调显示为黑白。</li> </ul>
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。  <b>说明</b> 人脸在逆光情况下，建议开启宽动态。 <ul style="list-style-type: none"> <li>● 关闭：不执行任何补偿。</li> <li>● 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。</li> <li>● 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。</li> <li>● 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。</li> </ul>
镜像	选择“启用”，将摄像机图像左右翻转。



参数	说明
翻转	选择“启用”，将摄像机图像上下翻转。

### 3.7.1.1.3 曝光设置

- 步骤1 登录设备 WEB 系统。  
 步骤2 选择“视频设置 > 视频设置”。  
 步骤3 选择通道号“1”，单击“曝光”页签。

图3-28 曝光 (1)



- 步骤4 设置曝光参数。

表3-11 曝光参数说明

参数	说明
防闪烁	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>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。</li> </ul>
曝光模式	<p>摄像机的曝光模式。</p> <p> <b>说明</b></p> <ul style="list-style-type: none"> <li>当“防闪烁”为“室外”时，“曝光模式”可以设置为“快门优先”模式。</li> <li>不同设备的曝光模式不同，具体请以实际界面为准。</li> </ul> <p>包括如下选项：</p> <ul style="list-style-type: none"> <li>自动，根据环境自动调整图像显示的亮度。</li> <li>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。</li> <li>手动，手动设置增益值和快门值，调节图像显示的亮度。</li> </ul>
快门	<p>可以根据实际需要设置快门大小。</p> <p>快门值越大，曝光时间越小，图像越暗。</p>



参数	说明
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	当“3D 降噪”为“开启”时，可以设置该参数。 数值越大，视频越清晰。

### 3.7.1.2 通道 2 视频参数设置

#### 3.7.1.2.1 图像设置

步骤1 登录设备 WEB 系统。

步骤2 选择“视频设置 > 视频设置”。

步骤3 选择通道号“2”，单击“图像”页签。


图3-29 图像（2）



步骤4 设置图像参数。

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。

参数	说明
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> <b>说明</b></p> <p>人脸在逆光情况下，建议开启宽动态。</p> <ul style="list-style-type: none"> <li>● 关闭：不执行任何补偿。</li> <li>● 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。</li> <li>● 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。</li> <li>● 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。</li> </ul>

### 3.7.1.2.2 曝光设置

步骤1 登录设备 WEB 系统。

步骤2 选择“视频设置 > 视频设置”。

步骤3 选择通道号“2”，单击“曝光”页签。


图3-30 曝光（2）



步骤4 设置曝光参数。

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"> <li>● 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。</li> <li>● 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。</li> <li>● 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。</li> </ul>

参数	说明
曝光模式	<p>摄像机的曝光模式。</p> <p> <b>说明</b></p> <ul style="list-style-type: none"> <li>当“防闪烁”为“室外”时，“曝光模式”可以设置为“快门优先”模式。</li> <li>不同设备的曝光模式不同，具体请以实际界面为准。</li> </ul> <p>包括如下选项：</p> <ul style="list-style-type: none"> <li>自动，根据环境自动调整图像显示的亮度。</li> <li>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。</li> <li>手动，手动设置增益值和快门值，调节图像显示的亮度。</li> </ul>
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。

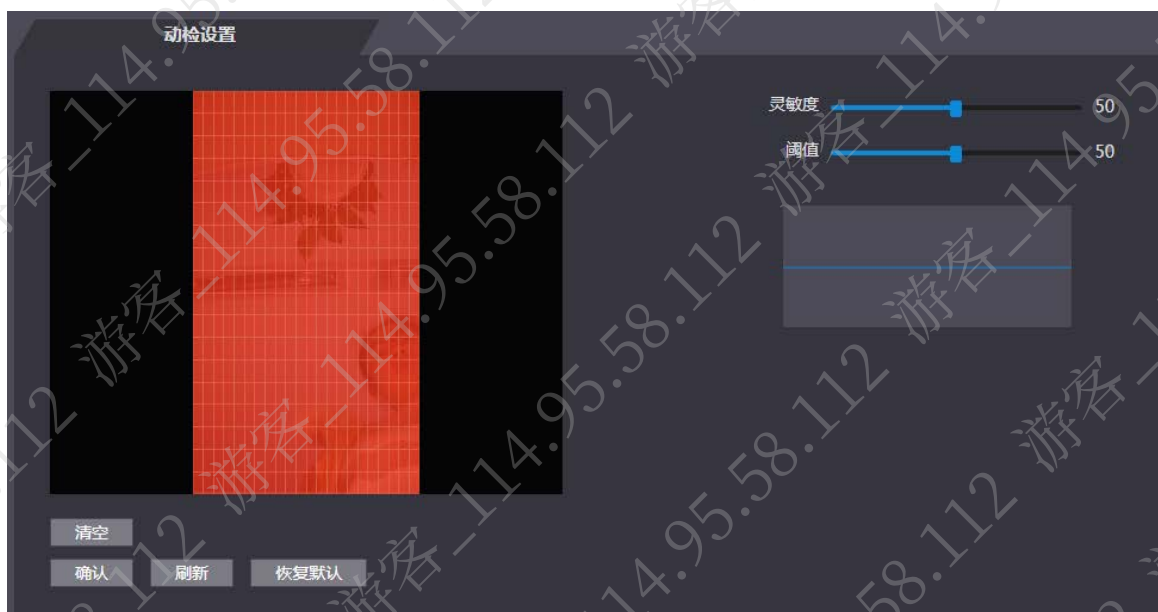
### 3.7.2 动检设置

设置设备上的动态检测范围。

步骤1 登录设备 WEB 系统。

步骤2 选择“视频设置 > 动检设置”。

图3-31 动检设置



步骤3 设置参数。

表3-14 动检设置参数说明

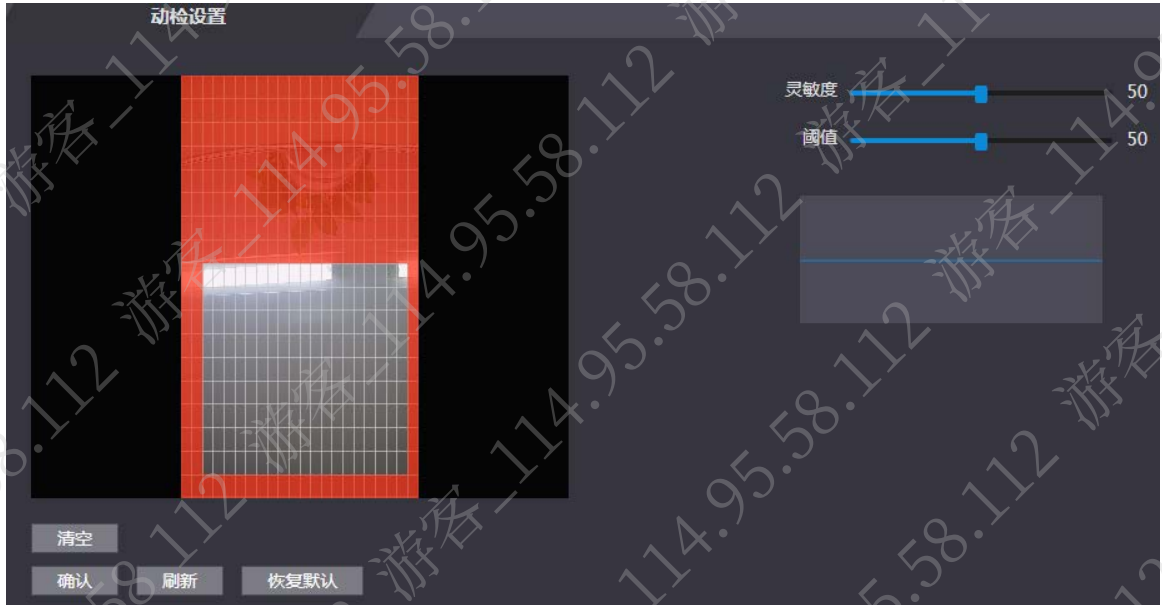
参数	说明
灵敏度	每个动检的格子的感知能力，数值越大越灵敏。
阈值	动检触发的条件，数值越小越容易触发。

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。

图3-32 动检范围



步骤5 单击“确认”，完成设置。

### 3.7.3 图像模式

设置设备的图像模式。

步骤1 登录设备 WEB 系统。

步骤2 选择“视频设置 > 图像模式 > 图像模式”。

图3-33 图像模式设置



步骤3 单击▾，在“图像模式一键设置”下拉框中选择图像模式类型。

- 室内，正常室内场景。
- 室外，正常室外场景。
- 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 局部编码

设置可视对讲功能中对讲和监视的画面区域。

步骤1 登录设备 WEB 系统。

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监视的画面。

图3-34 局部编码



步骤5 单击“确认”。

### 3.8 人脸检测

在该菜单下，设置人脸检测的各项参数，设置检测区域、提高设备人脸识别的精准度。

#### 操作步骤

步骤1 登录设备 WEB 系统。

步骤2 选择“人脸检测”。

步骤3 配置参数。



图3-35 人脸检测

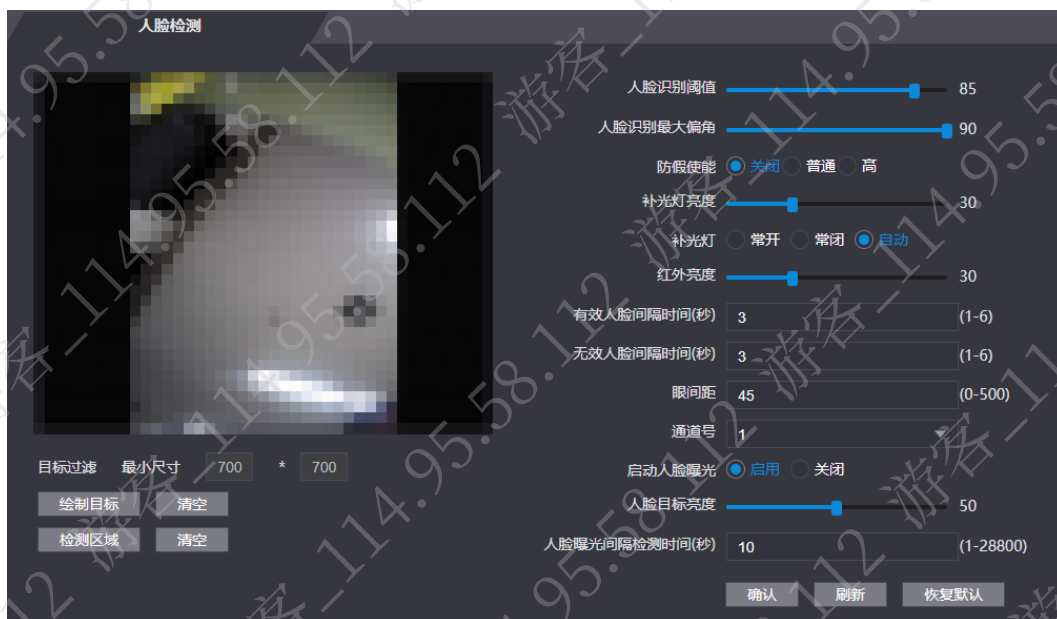


表3-15 人脸检测参数说明

参数	说明
人脸识别阈值	阈值越大，要求识别成功的相似度越大，但是识别成功率越低。
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	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。 <ul style="list-style-type: none"> <li>● 关闭：关闭防假使能。</li> <li>● 普通、高：设置防假使能等级。</li> </ul>
补光灯亮度	调整设备识别人脸时，白光补光灯的亮度。
补光灯	设置设备识别人脸时白光补光的情况。 <ul style="list-style-type: none"> <li>● 常开：补光灯保持开启状态。</li> <li>● 常闭：补光灯保持关闭状态。</li> <li>● 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。</li> </ul>
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(秒)	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(秒)	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	双眼之间的像素值，由人脸大小、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 px~70 px。
通道号	<ul style="list-style-type: none"> <li>● 1 为白光视频。</li> <li>● 2 为红外光视频。</li> </ul>
启动人脸曝光	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。 <ul style="list-style-type: none"> <li>● 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。</li> <li>● 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。</li> </ul>

步骤4 单击“确认”，完成设置。



## 相关操作

- 绘制目标
  - ◇ 单击“绘制目标”，绘制最小人脸识别框的大小。
  - ◇ 单击“清空”，清空绘制的人脸识别框。
- 检测区域
  - ◇ 单击“检测区域”，调整人脸识别区域，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 TCP/IP

需要配置 IP 地址和 DNS 服务器，保证与组网中的其他设备能够互通。

步骤1 登录设备 WEB 系统。


步骤2 选择“网络设置 > TCP/IP”。


图3-36 TCP/IP 配置



步骤3 配置 TCP/IP 参数。

表3-16 TCP/IP 参数说明

参数	说明
IP 版本	只支持 IPv4。  <b>说明</b> 双网卡设备支持两个 IP 的设置。
MAC 地址	显示设备 MAC 地址。

参数	说明
模式	设置设备获取 IP 的模式。 <ul style="list-style-type: none"> <li>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。</li> <li>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。</li> </ul>
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、子网掩码和默认网关。
子网掩码	
默认网关	 <b>说明</b> 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”，完成设置。

### 3.9.2 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。

步骤1 登录设备 WEB 系统。

步骤2 选择“网络设置 > 端口”。

图3-37 端口




步骤3 配置该设备的各个端口值。

#### 说明

除“最大连接数”以外，修改其他参数设置，需重启后生效。

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。  <b>说明</b> 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。
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 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。

步骤1 登录设备 WEB 系统。

步骤2 选择“网络设置 > 主动注册”。

图3-38 主动注册



步骤3 选择“启用”，输入“IP 主机”、“端口”和“子设备 ID”。

表3-18 主动注册

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	服务器端分配的，用于该设备的 ID，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 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。



### 注意

使用该功能，必须将设备接入外网，否则将无法正常使用。

- 步骤1 登录设备 WEB 系统。
- 步骤2 选择“网络设置 > P2P”。
- 步骤3 选择“启用”，开启 P2P 功能。

图3-39 P2P 界面



- 步骤4 单击“确认”，完成设置。

### 3.9.5 （可选）4G

开启设备 4G 无线通讯功能。



### 说明

仅 7 寸 B 款部分设备支持，默认不开启。如需使用，请先登录 WEB 并启用 4G 功能。

- 步骤1 登录设备 WEB 系统。
- 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，单击“确认”保存更改。

图3-40 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"> <li>• CTNET：中国电信 2G&amp;3G。</li> <li>• CTLTE：中国电信 4G。</li> <li>• CMNET：中国移动。</li> <li>• UNINET：中国联通。</li> <li>• 3GNET：中国联通，同 UNINET。</li> </ul>
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"> <li>• No：不需要鉴权。</li> <li>• PAP：PAP 鉴权。</li> <li>• CHAP：CHAP 鉴权。</li> </ul>
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"> <li>• *99#：电信号码。</li> <li>• *98*1#：移动号码。</li> <li>• *99#：联通号码。</li> </ul>
用户名	<ul style="list-style-type: none"> <li>• 移动联通 SIM 卡默认为空。</li> </ul>
密码	<ul style="list-style-type: none"> <li>• 电信 SIM 卡使用默认用户名密码： <ul style="list-style-type: none"> <li>◇ 用户名：ctnet@mycdma.cn。</li> <li>◇ 密码：vnet.mobi。</li> </ul> </li> </ul>
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。



## 3.10 安全管理

### 3.10.1 IP 权限

IP 权限设置有三种类型：网络访问、禁止 PING、防半连接。

- 网络访问：通过设置黑白名单，限制用户的访问权限。
  - ◇ 白名单：只有用户的 IP/MAC 在白名单列表中，才能访问设备，否则无法访问设备。如果同时设置了端口，用户只能访问已设置的端口。
  - ◇ 黑名单：用户的 IP/MAC 在黑名单列表中，无法访问设备。如果同时设置了端口，则用户无法访问设备的指定端口，但可以访问设备。
- 禁止 PING：启用禁止 PING 功能，设备不回复 ping 请求。
- 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。

#### 3.10.1.1 网络访问

步骤1 登录设备 WEB 系统。

步骤2 选择“安全管理 > IP 权限”。

步骤3 在“类型”下拉列表框中选择“网络访问”。

图3-41 选择网络访问启用界面



步骤4 选择“白名单”或“黑名单”，添加白名单或黑名单。

1. 单击“白名单”或“黑名单”页签。
2. 单击“添加”。


图3-42 添加





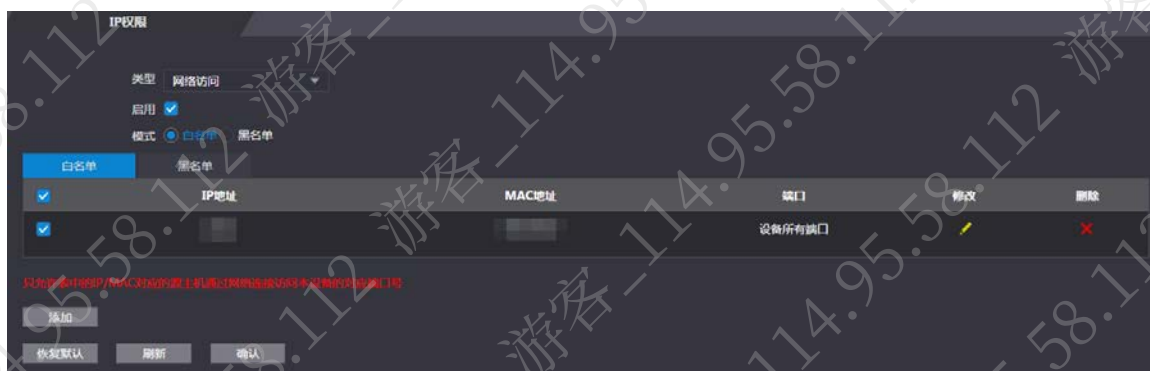
3. 配置添加信息。

表3-20 IP 地址参数说明

参数	说明
类型	在“类型”下拉列表框中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。  <b>说明</b> 若类型选择为“MAC 地址”，则只需输入“MAC 地址”，即可设置。
IP 版本	在“IP 版本”下拉列表框中选择“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”。

图3-43 IP 权限



步骤5 在白名单或黑名单的列表中，单击，修改黑白名单；单击，删除黑白名单。

步骤6 选择“启用”，开启网络访问模式。

步骤7 单击“确认”，保存设置。

### 3.10.1.2 禁止 PING

步骤1 登录设备 WEB 系统。

步骤2 选择“安全管理 > IP 权限”。

步骤3 在“类型”下拉列表框中选择“禁止 PING”。

图3-44 选择禁止 PING 启用界面



步骤4 选择“启用”，开启禁止 PING 模式。

步骤5 单击“确认”，保存设置。

### 3.10.1.3 防半连接

- 步骤1 登录设备 WEB 系统。
- 步骤2 选择“安全管理 > IP 权限”。
- 步骤3 在“类型”下拉列表框中选择“防半连接”。

图3-45 选择防半连接启用界面



- 步骤4 选择“启用”，开启防半连接模式。
- 步骤5 单击“确认”，保存设置。

### 3.10.2 系统服务

- 步骤1 登录设备 WEB 系统。
- 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3-46 系统服务

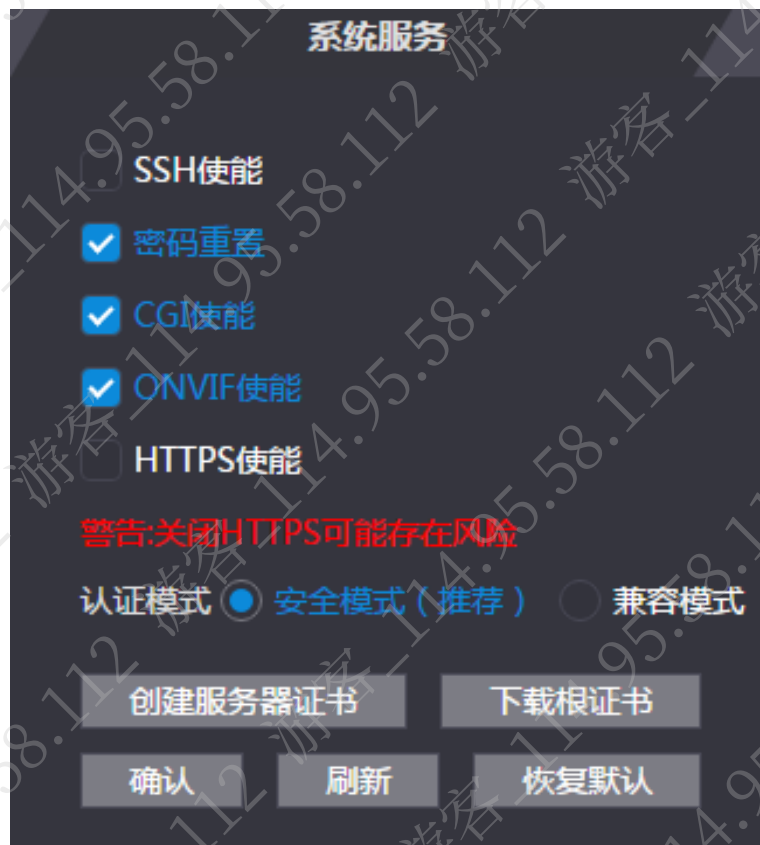


表3-21 系统服务参数说明

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。重置密码详细介绍参见“3.3 重置密码”章节。
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	推荐选择“安全模式”。
创建服务器证书	用户可安装手动创建的服务器证书，具体请参见“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，具体请参见“3.10.2.2 下载与安装根证书”。

### 3.10.2.1 创建服务器证书

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。

步骤1 单击“创建服务器证书”。

步骤2 填写对应的“地区”、“省份”等信息，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。

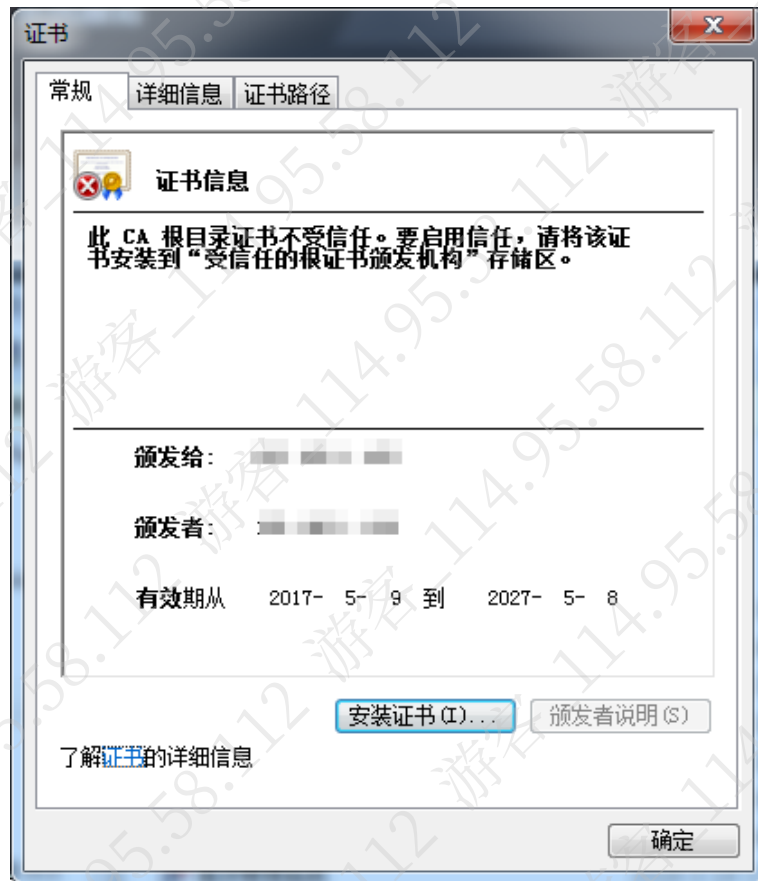
图3-47 创建服务器证书



### 3.10.2.2 下载与安装根证书

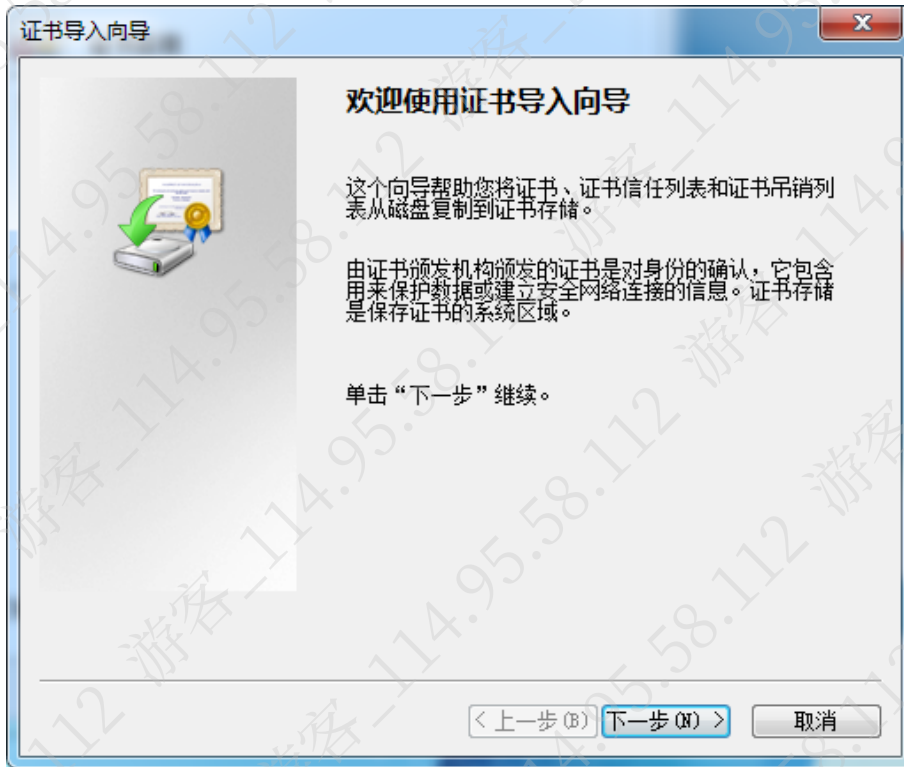
- 步骤1 单击“下载根证书”。
- 弹出“文件保存”对话框，选择所需保存的路径保存证书。
- 步骤2 双击下载的证书文件。
- 步骤3 单击“安装证书”。

图3-48 证书



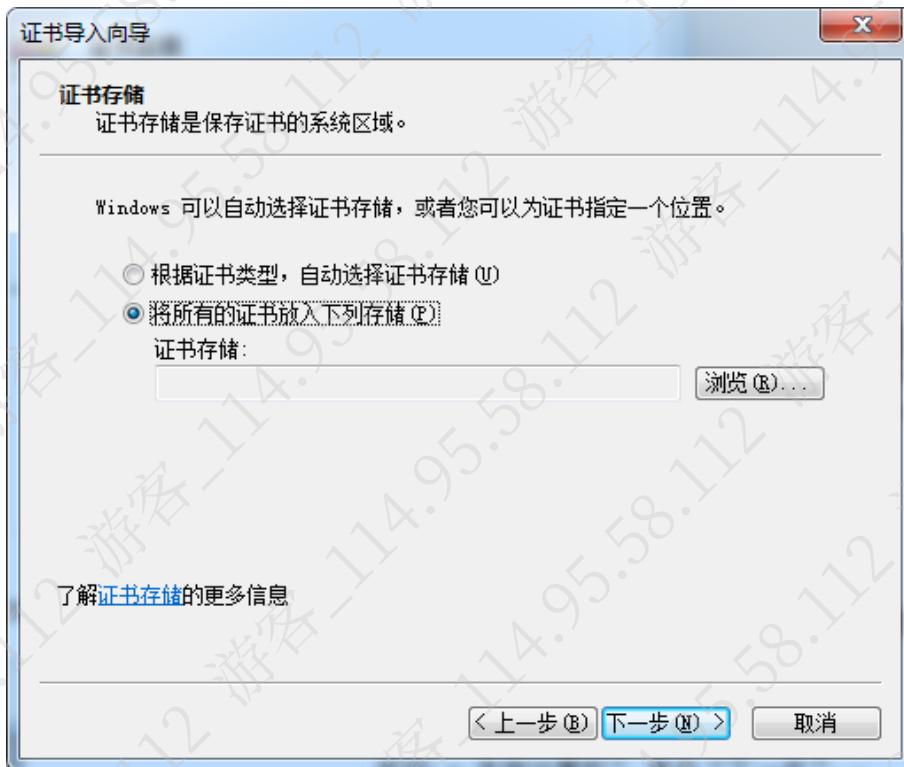
- 步骤4 单击“下一步”。

图3-49 证书导入向导



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”。

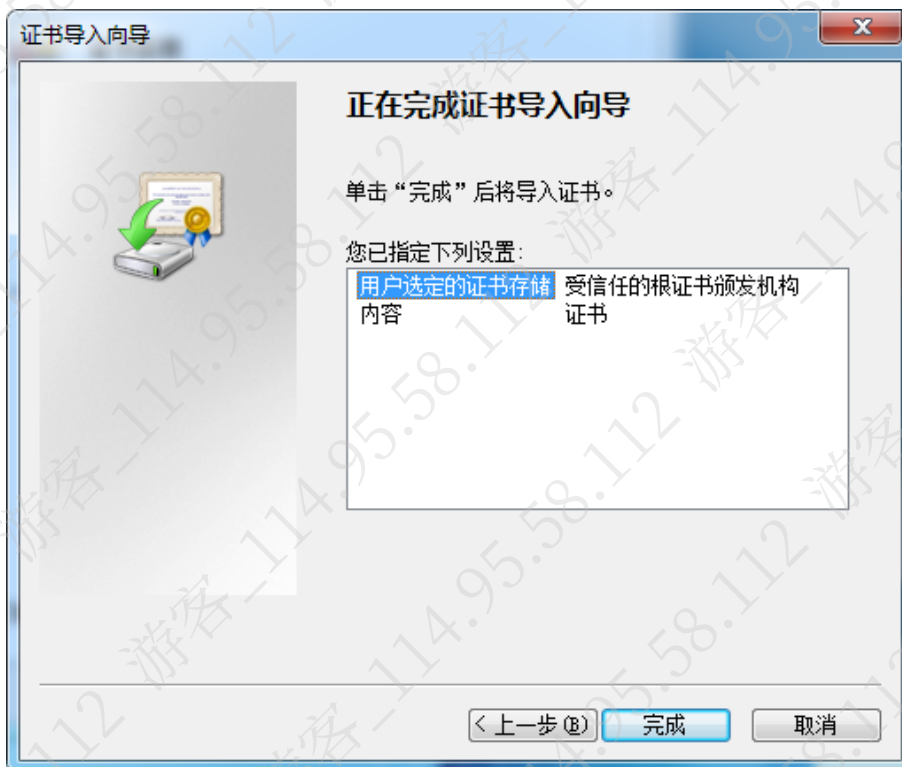
图3-50 证书存储



步骤6 单击“完成”。

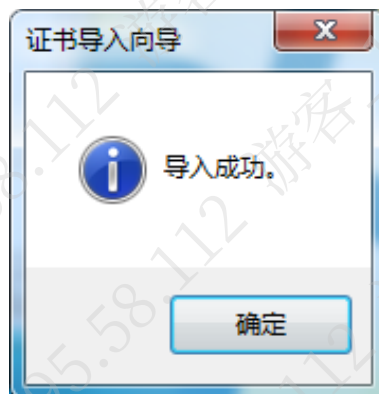


图3-51 正在完成证书导入向导



步骤7 弹出“导入成功”对话框，单击“确定”。

图3-52 导入成功



### 3.11 语音管理

根据实际需要选择不同的语音播报提示。

步骤1 登录设备 WEB 系统。

步骤2 选择“语音管理”。

步骤3 在下拉列表中选择“系统语音提示”类型。如“验证成功”、“开门成功”、“开锁成功”、“打卡成功”、“欢迎光临”、“欢迎再次光临”、“谢谢”或“无”。



图3-53 语音管理



步骤4 拖动进度条调节语音播报音量大小或麦克风输入音量大小。

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 用户管理



“用户管理”中用户指的是设备本地用户和登录设备 WEB 的用户。

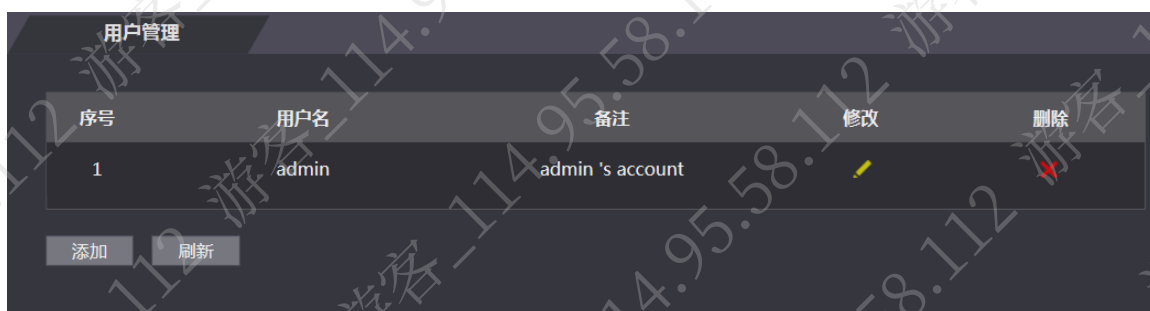
#### 3.12.1.1 添加用户

步骤1 登录设备 WEB 系统。

步骤2 选择“用户管理”。

步骤3 单击“添加”。

图3-54 用户管理



步骤4 输入“用户名”、“密码”、“确认密码”和“备注”。

图3-55 添加用户



步骤5 单击“确认”，完成添加。

### 3.12.1.2 修改用户信息

步骤1 在“用户管理”界面，单击.

步骤2 根据需要修改“备注”、“预留手机”、“密码”。

图3-56 修改用户



#### 说明

仅 admin 用户有预留手机。

步骤3 单击“确认”，完成修改。

## 3.12.2 ONVIF 用户

ONVIF 用户只用于 ONVIF 协议，开门前，需要验证 ONVIF 用户信息。

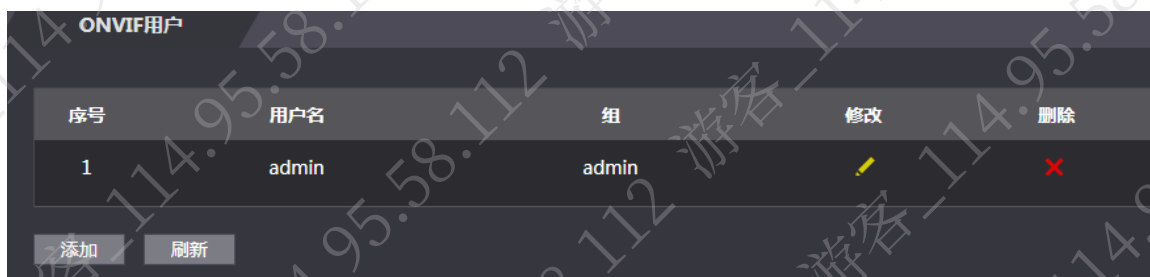
### 3.12.2.1 添加用户

步骤1 登录设备 WEB 系统。

步骤2 选择“用户管理 > ONVIF 用户”。

步骤3 单击“添加”。

图3-57 ONVIF 用户



步骤4 输入“用户名”、“密码”、“确认密码”。

图3-58 添加 ONVIF 用户

添加

用户名

密码

弱  中  强

确认密码

组

确认 取消

步骤5 选择“组”。

步骤6 单击“确认”，完成添加。

### 3.12.2.2 修改用户信息

修改对应用户名、组及密码。

步骤1 在“ONVIF 用户”界面，单击

步骤2 根据需要修改“用户名”、“组”。

图3-59 修改 ONVIF 用户

修改

用户名

组

修改密码

确认 取消

步骤3 选择“修改密码”。

步骤4 输入“旧密码”、“密码”和“确认密码”。

图3-60 修改 ONVIF 用户密码

修改

用户名 admin

组 admin

修改密码

旧密码

密码

弱 中 强

确认密码

确认 取消

步骤5 单击“确认”，完成修改。

### 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。

步骤1 登录设备 WEB 系统。

步骤2 选择“自动维护”。

步骤3 选择“自动重启系统”的时间。

图3-61 自动维护

自动维护

自动重启系统 星期二 02:00

重启设备

确认 刷新

#### 说明

系统默认“自动重启系统”时间为每星期二 02:00。

步骤4 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。

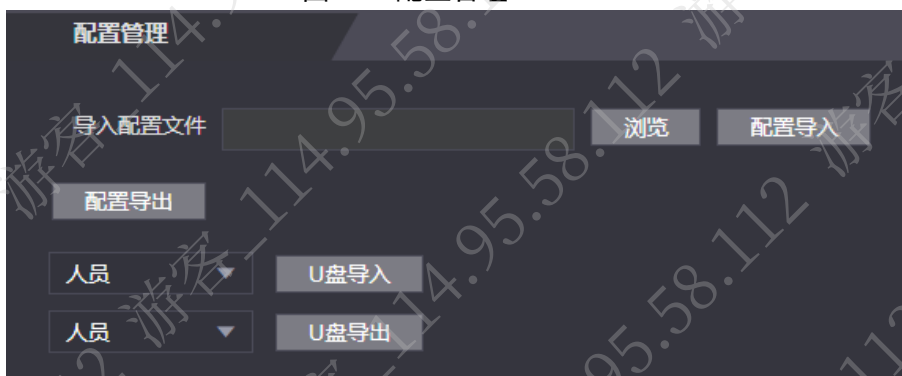
## 3.14 配置管理

### 说明

除配置导入和导出功能之外，其他功能仅部分型号支持。

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。登录设备 WEB 系统，选择“配置管理”。

图3-62 配置管理



### 3.14.1 配置导出

步骤1 在“配置管理”界面，单击“配置导出”。

步骤2 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。

### 3.14.2 配置导入

步骤1 在“配置管理”界面，单击“浏览”，选择需要导入的配置文件。

步骤2 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。

## 3.15 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 系统，选择“系统升级”，系统显示“系统升级”界面。



图3-63 系统升级



### 3.15.1 文件升级

对系统执行升级操作，升级文件为\*.bin 类型文件。

步骤1 单击“浏览”，选择升级文件。

步骤2 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

通过与云端交互，检测最新版本，实现在线升级。

步骤1 检测版本。

- 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。
  - ◇ 如果已经最新版本，则界面下方提示“已是最新版”。
  - ◇ 如果检测到有版本更新，系统将提示发现新版本的相关信息、发布日期，以及新版本的相关修改内容。

步骤2 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 版本信息

登录设备 WEB 系统，选择“版本信息”，系统显示“MAC 地址”、“序列号”、“WEB 版本号”等信息

息。

### 3.17 在线用户

登录设备 WEB 系统，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3-64 在线用户



序号	用户名	IP地址	用户登录时间
1	admin	192.168.1.108	2018-10-29 09:07:47

刷新

### 3.18 系统日志

为了维护方便，可以查看和备份系统日志。

选择“系统日志”，系统显示“系统日志”界面。

图3-65 系统日志



系统日志

时间范围: 2018-09-02 00:00:00 - 2018-09-03 00:00:00

类型: 全

查询

序号	日志时间	用户名	日志类型
暂无数据...			

时间:  
用户名:  
类型:  
内容:

备份

1/1 前往

#### 3.18.1 查询日志

选择“开始时间”、“结束时间”和“类型”，单击“查询”，系统显示查询结果。

#### 3.18.2 备份日志

单击“备份”，对查询结果进行备份。

### 3.18.3 管理员记录


选择“系统日志 > 管理员记录”，系统显示“管理员记录”界面。

输入管理员 ID 编号，单击“查询”，系统显示管理员的操作记录。

图3-66 管理员记录



### 3.19 退出

单击 ，确认后，退出设备 WEB 系统。

#### 说明

将鼠标悬停在  上，可显示当前用户的信息。

## 第 4 章 SmartPSS Plus 配置

### 4.1 登录客户端

安装配套的 SmartPSS Plus 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 添加设备

在 Smart PSS Plus 中添加设备，可选择搜索添加和手动添加两种方式。

#### 4.2.1 搜索添加

要求待添加的设备处于同一网段。

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。

图4-1 自动搜索



#### 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 (可选) 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4-2 登录信息



**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4-3 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	序列号	操作
1	4.3寸智能人脸识别终端		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。
和	<ul style="list-style-type: none"> <li>• 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 。</li> <li>• 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 。</li> </ul>
	单击该图标，删除设备。

## 4.2.2 手动添加

添加设备时需要预知设备的 IP 地址或域名。

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4-4 手动添加

表4-2 添加参数说明

参数	说明
设备名称	设备的名称，建议以设备所监视区域命名，便于维护。
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。

## 4.3 添加人员

支持录入人员信息、给人员发卡、赋予人员门禁通行权限。

### 4.3.1 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“门禁管理 > 人事管理”，单击“发卡类型”，设置使用的卡片类型。

图4-5 设置发卡类型

## 4.3.2 单个添加


- 步骤1 在主页选择“门禁 > 人事管理”。
- 步骤2 在左侧导航栏单击, 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. 输入人员并上传照片，单击“保存”。

图4-6 添加人员基本信息



编号: \* 123

名称: \*

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

使用次数: 无限

身份证读取  
摄像抓图  
上传图片

图片大小: 建议小于100KB

详细信息

性别:  男  女

证件类型: 身份证

民族: 汉族

证件号:

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:

学历: 本科

入职时间: 2021/8/22 11:21:07

联系电话:


离职时间: 2031/8/23 11:21:07

电子邮件:

通信地址:


管理员:

备注:

- 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 张胁迫卡、设置 1 张主卡。

- 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4-7 采集人员指纹信息



指纹名称	操作
------	----

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，详细介绍请参见“4.4 添加门禁权限组”和“4.5 分配门禁权限”。

步骤6 单击“完成”。

### 4.3.3 批量添加

步骤1 在主页选择“门禁 > 人事管理”。

步骤2 在左侧导航栏单击，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4-8 批量添加人员

编号	卡号
20	
21	

步骤6 在人员列表单击 ，完善人员信息。

## 4.4 添加门禁权限组

### 操作步骤

- 步骤1 在主页选择“门禁 > 人事管理”。
- 步骤2 在左侧导航栏单击“权限配置”，单击“添加”。
- 步骤3 填写权限组名称，选择时间模板，在设备导航树中选择设备，单击“确定”。

图4-9 添加权限组

增加权限组

基本信息

组名: 权限组1 备注:

权限组类型: 门禁权限组 时间模板: 全时间时间模板

认证方式:  卡  指纹  密码  人脸

所有设备 已选择 (0)

搜索..



默认分组

1

门 1

确定 取消

## 相关操作

- 修改权限组：在权限组列表单击权限组右侧的 ，修改权限组信息。
- 删除权限组：在权限组列表单击权限组右侧的 ，根据提示删除权限组。

## 4.5 分配门禁权限


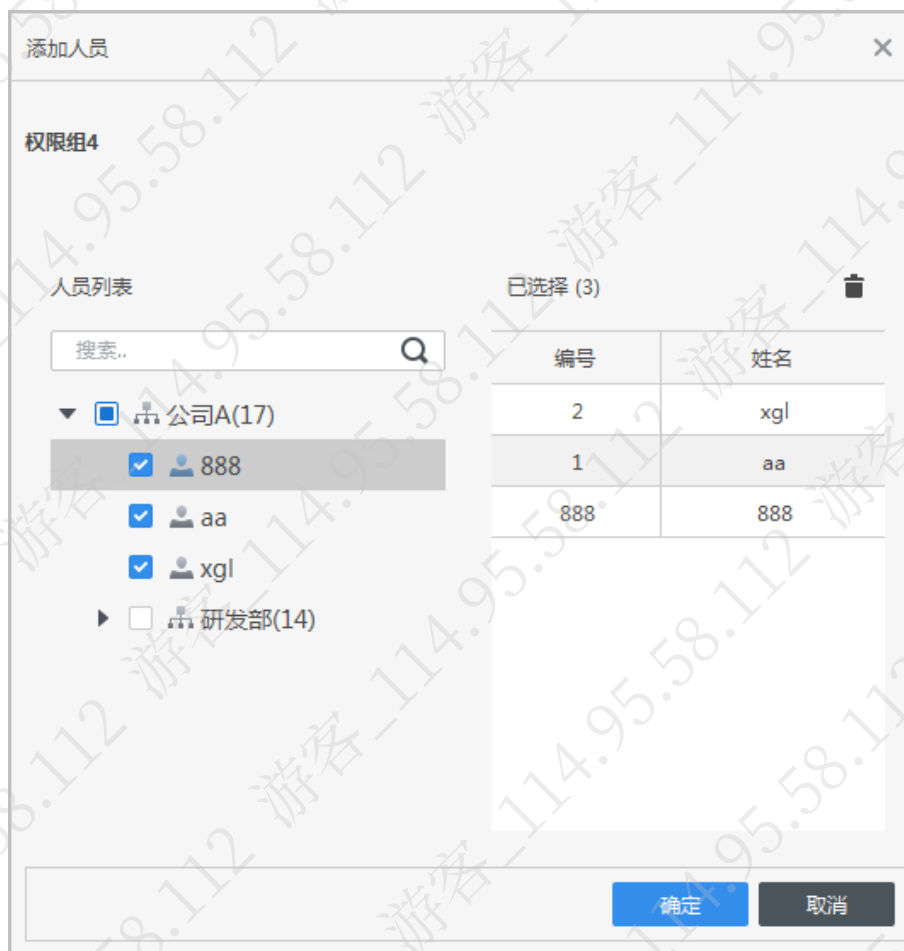
- 步骤1 在主页选择“门禁 > 人事管理”。
- 步骤2 在左侧导航栏单击“权限配置”，在权限组列表单击权限组右侧的 。
- 步骤3 在弹出的界面选择人员，单击“确定”。

图4-10 赋予人员门禁通行权限



## 4.6 门禁管理

完成门禁业务配置后，即可通过软件远程监控门禁状态和操作门禁，例如开关门。

### 4.6.1 远程开关门

#### 操作步骤

- 步骤1 在主页选择“门禁 > 门禁管理”。
- 步骤2 在门禁管理界面远程开关门。  
支持通过如下任意一种方式远程开关门。
  - 方式一：在组织树选择要远程控制的门禁，右键选择“开门”或“关门”。

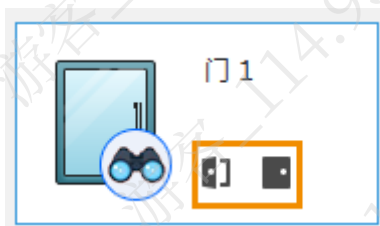


图4-11 远程开关门（方式一）





- 方式二：单击指定门右下角的和，远程控制该门的开和关。

图4-12 远程开关门（方式二）



## 相关操作

- 查看门禁信息。在“事件信息”列表，可以查看门禁的实时操作信息。重启软件后门禁信息会被清空。
- 筛选事件：在“事件信息”栏，选择需要查看的事件类型，事件列表显示该类型的事件，例如仅选择“报警”，则事件列表仅显示报警事件。
- 锁定事件刷新。在“事件信息”右侧单击，锁定事件列表，将无法查看到门禁的实时操作信息
- 删除所有事件。在“事件信息”右侧单击，清空事件列表的所有事件。

## 4.6.2 设置门常开或常关

设置门常开或门常关后，门将一直打开或一直关闭，此时无法手动开门或关门，需通过“恢复正常”将门恢复正常后，才能手动开门或关门。

步骤1 在主页选择“门禁 > 门禁管理”。

步骤2 在门禁管理界面组织树选择要设置为常开或常关的门，单击“一键常闭”或“一键常开”。

图4-13 设置门常开或常关



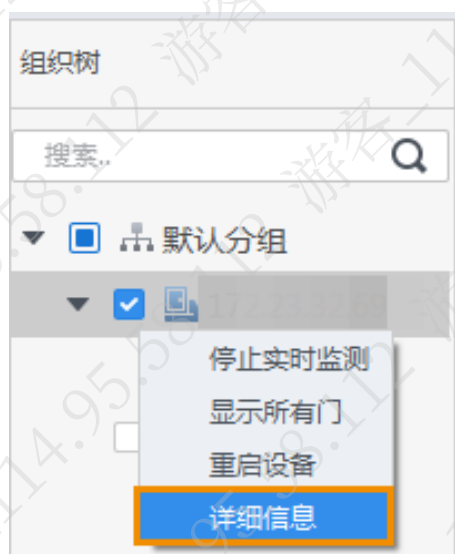
### 4.6.3 查看门禁详情

查看门禁设备 IP 地址、型号、状态、序列号和软件版本号等。

步骤1 在主页选择“门禁 > 门禁管理”。

步骤2 在门禁管理界面组织树单击要查看详细信息的门禁，在右键菜单栏选择“详细信息”，查看该门禁详情。

图4-14 查看门禁详细信息



### 4.6.4 重启门禁

支持通过软件远程重启门禁。

步骤1 在主页选择“门禁 > 门禁管理”。

步骤2 在门禁管理界面组织树单击要查看详细信息的门禁，在右键菜单栏选择“重启门禁”，根据提示重启门禁。

图4-15 查看门禁详细信息



## 第 5 章 FAQ

### 1. 设备上电后无法启动

请确认 12V 电源是否连接正确，是否按下左侧的开关按钮。

### 2. 开机后人脸无法识别

- 请确认“门禁管理 > 开门模式管理”中，开门方式是否选择了人脸方式，具体请参见“2.8.2 开门模式管理”。
- 请查看“门禁管理 > 开门模式管理 > 任意组合开门”中是否配置人脸模式，具体请参见“2.8.2.1 任意组合开门”。

### 3. 设备和第三方控制器对接韦根接口无信号输出

请确认设备 GND 线和第三方控制器 GND 线是否连接。

### 4. 忘记管理员导致无法执行相关设置

请使用配套提供的平台软件对管理人员进行删除，或者联系技术支持人员，使用专业软件工具进行远程解锁。

### 5. 人员信息、人脸导入出错

请确认是否改动 XML 文件的名称和表内的头名称，系统会根据名称进行自动判断文件。

### 6. 人脸出现自己人脸识别成其他人员

请确认自己在人脸录入的时候周边无其他人脸出现，如果出现此类问题请删除原有人脸后再重新录入。

# 附录1 人脸录入/比对说明

## 注意事项

- 登记时戴眼镜、戴帽子和胡子都可能影响登记效果。
- 戴帽子请勿遮住眉毛。
- 胡子过长或者面积过大会影响登记效果，建议登记和使用中胡子变化不要太大，否则会影响识别。
- 登记和验证时，请保持脸部清洁。
- 设备距离光源至少 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

在设备端和平台端注册人脸信息，平台端注册请参见配套的平台使用说明书。

附图图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。

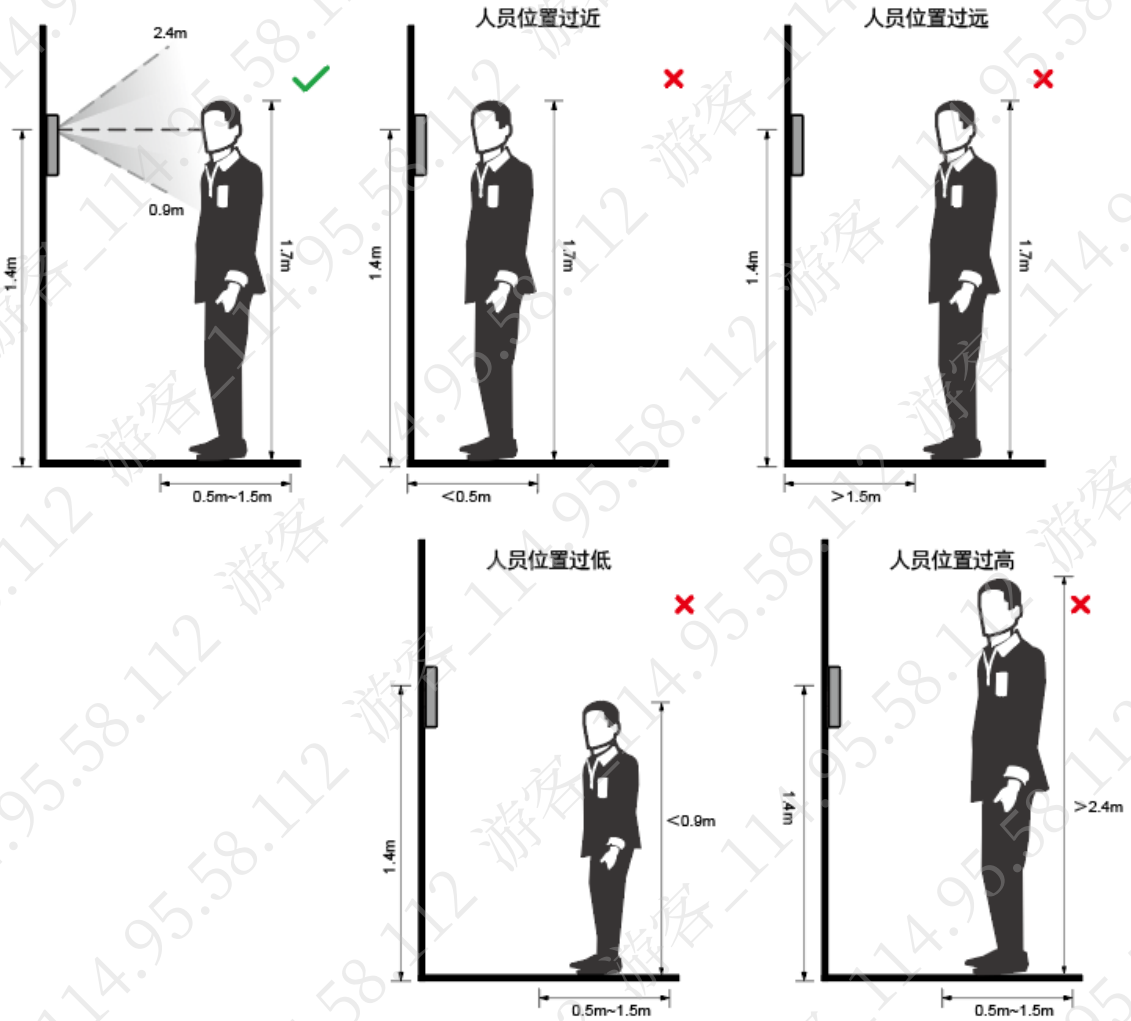
将人脸放置于采集框中心区域，设备自动完成抓拍，结束后完成人脸采集。

## 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、胡子过长或者面积过大，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 人脸位于窗口位置示意



## 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  $500 \times 500$  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

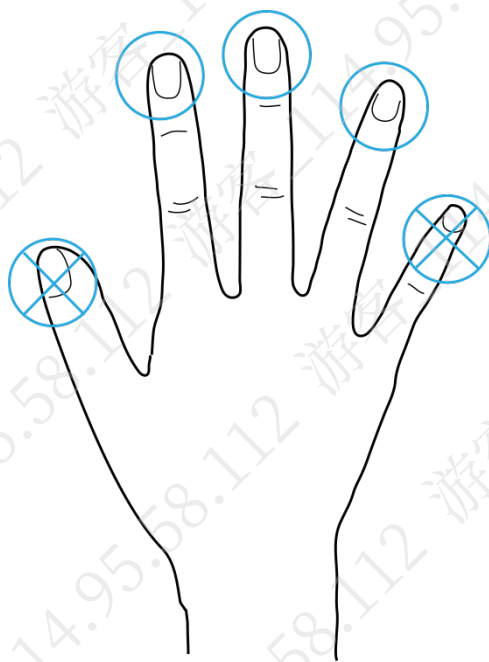
### 注意事项

- 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。

### 推荐手指

推荐使用食指、中指和无名指。大拇指和小拇指不容易放到采集窗口上。

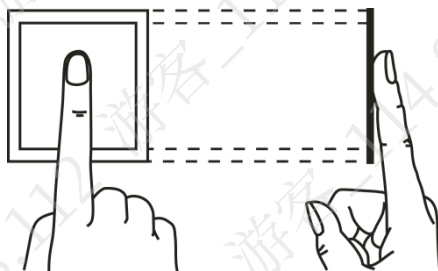
附录图2-1 推荐手指



### 按压方法

- 正确方法

附录图2-2 正确按压示意



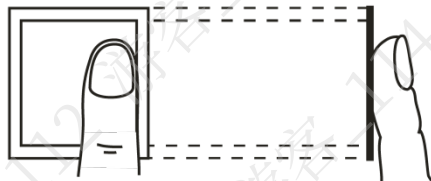
- 错误方法

附录图2-3 错误方法

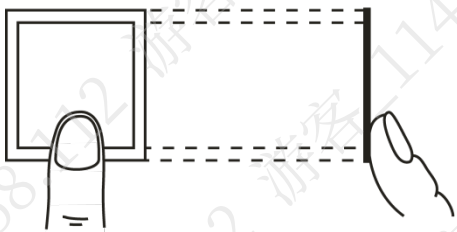
垂直



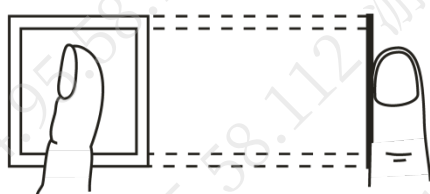
太偏



太靠下



倾斜




## 附录3 对讲功能操作说明


人脸门禁一体主机作门口机或围墙机使用，可实现可视对讲功能。

### 前提条件

已在人脸门禁一体主机和对讲系统中做好配置，实现人脸门禁一体主机和室内机、管理机、平台客户端、手机 App 的协议互通。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 输入呼叫的号码，按 。

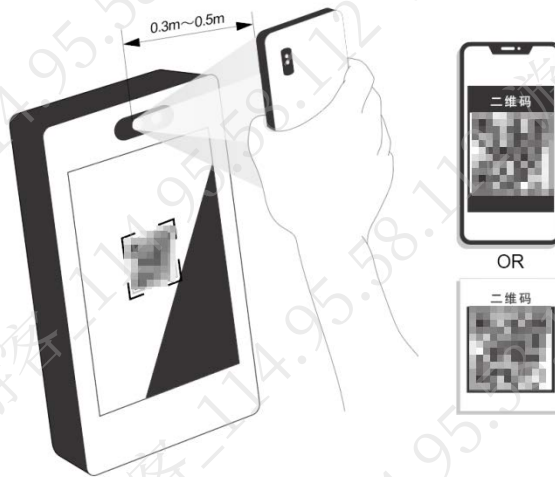
附录图3-1 拨号界面



## 附录4 扫描二维码说明

为了保证二维码扫描效果，请将二维码置于距离设备上的摄像头 0.3 m~0.5 m 处，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



### 说明

当开启测温功能，使用二维码扫描时，请不要遮挡脸部。

# 附录5 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。