SIP 服务器

使用说明书

V1.0.1

符号约定

在本文档中可能出现下列标识，代表的含义如下。

标识	说明
 危险	表示有高度潜在危险，如果不能避免，会导致人员伤亡或严重伤害。
 警告	表示有中度或低度潜在危险，如果不能避免，可能导致人员轻微或中等伤害。
 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。
	表示能帮助您解决某个问题或节省您的时间。
	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
V1.0.1	增加法律声明和网络安全须知	2018.12

使用安全须知

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

使用要求

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

电源要求

- 产品必须使用本地区推荐使用的电线组件（电源线），并在其额定规格内使用。
- 请使用满足 SELV（安全超低电压）要求的电源，并按照 IEC60950-1 符合 Limited Power Source（受限制电源）的额定电压供电，具体供电要求以设备标签为准。
- 如果使用电源插头或器具耦合器等作为断开装置，请保持断开装置可以方便的操作。

目录

1 产品概述

SIP 系统包括：室内机、门口机、SIP 服务器、H700 平台和网络传输设备五部分，结构如图 1-1 所示，具体介绍请参见表 1-1。

图1-1 结构图

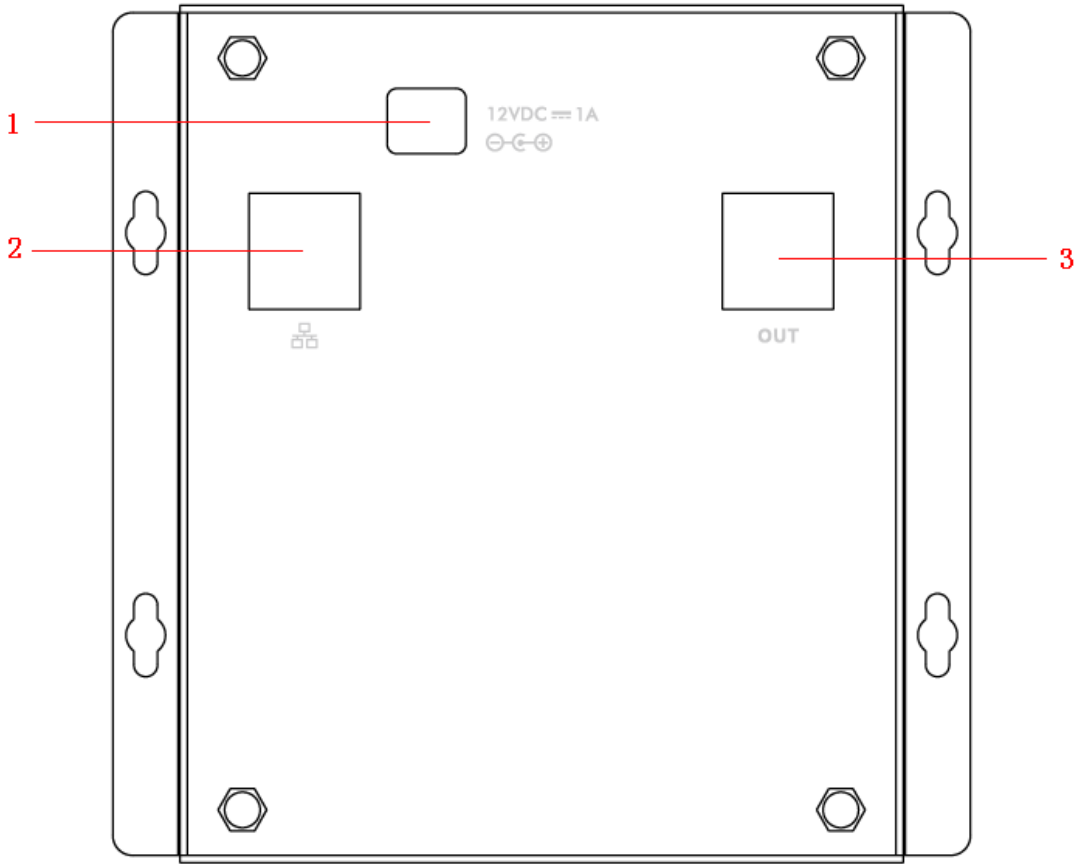


表1-1 部件介绍

编号	名称	描述
1	电源插座	12V DC 电源输入
2	网络口	连接网络
3	输出口	—

2 系统登录/退出

2.1 设备初始化

首次使用门口机时，需要初始化登录密码。

在登录 WEB 界面配置网络服务器前，请先配置 PC 机的 IP 地址，确保 PC 能正常访问门口机。

步骤1　接通门口机电源，上电启动。

步骤2　在 PC 的浏览器地址栏中输入门口机的默认 IP 地址。

系统显示“密码设置”界面，如图 2-1 所示。

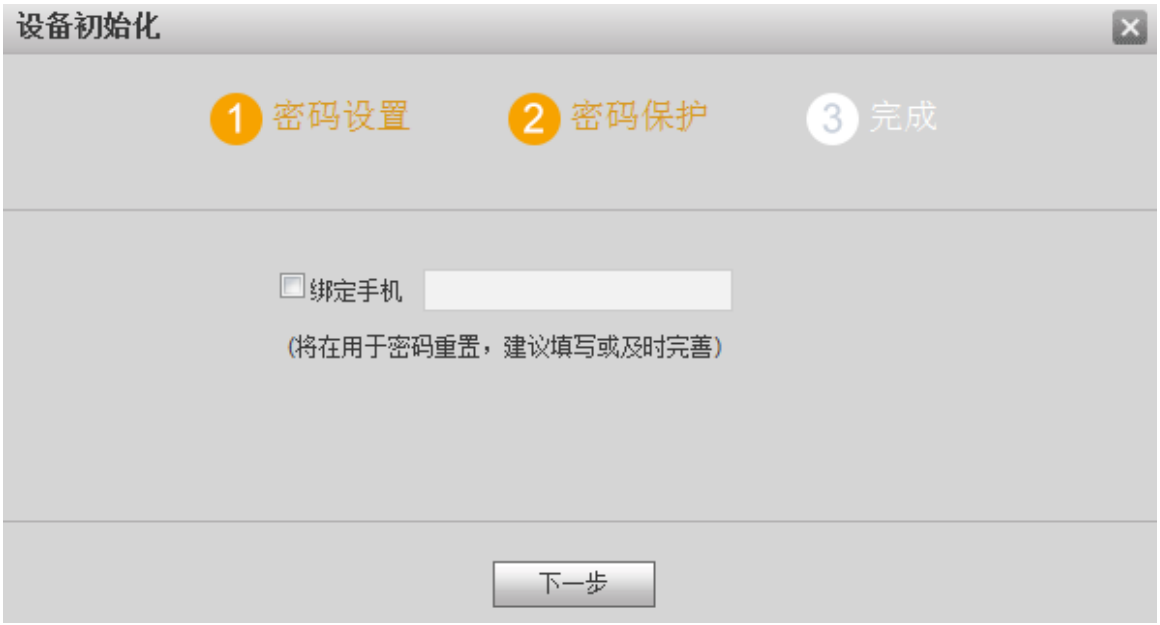
图2-1 密码设置界面

步骤3　输入“新密码”和“新密码确认”，单击“下一步”。

系统显示“密码保护”界面，如图 2-2 所示。

该密码用于登录 WEB 界面，要求密码设置为不少于 8 位，且至少包含数字、密码和常用字符中的两种。

图2-2 密码保护界面



步骤4　选择“绑定手机”，并输入手机号码。

该手机号码用于密码重置，建议设置。

步骤5　单击“下一步”。

系统显示“完成”界面，如图 2-3 所示，提示“设备初始化完成!”

图2-3 完成初始化界面

步骤6　单击“确定”。

系统显示 WEB 登录界面，如图 2-4 所示

图2-4 WEB 登录界面

步骤7　输入用户名和密码，单击“登录”。

2.2 密码重置

当您遗忘 admin 用户的登录密码，可以通过扫描二维码重置登录密码。

步骤1　通过浏览器登录设备的 WEB 界面。

系统显示登录界面，如图 2-5 所示。

图2-5 登录界面

步骤2　单击“忘记密码”。

系统显示“重置密码”对话框，如图 2-6 所示。

图2-6 重置密码（1）

步骤3　根据界面提示扫描二维码，并获取安全码。

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，该帐号将被锁定 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”。

系统显示设置新密码界面，如图 2-7 所示。

图2-7 重置密码（2）

步骤6　重新设置“新密码”和“确认密码”。

密码可设置为 8 位～32 位非空字符，可以由字母、数字和特殊字符（除“'”、“"”、“;”、“:”、“&”外）组成。密码必须由其中的 2 种或 2 种以上字符组成，请根据密码强弱提示设置高安全性密码。

步骤7　单击“确定”，完成密码重置。

2.3 系统登录

您可以参照以下步骤登录 SIP 服务器。

步骤1　在 IE 地址栏中，输入 SIP 服务器的 IP 地址，并按【Enter】键。

系统显示如图 2-8 所示的登录界面。

图2-8 登录界面

步骤2　输入“用户名”和“密码”。

管理员默认的用户名为“admin”，默认密码为“admin”。

步骤3　单击“登录”。

登录后的首页，如图 2-9 所示。

图2-9 登录后的首页

2.4 系统退出/重启

单击“系统设置＞退出系统＞退出系统”，退出系统。

单击“系统设置＞退出系统＞重启设备”，重启设备。

3 配置系统参数

3.1 本机设置

本机设置：用户可以根据需求，更改重启日期；变更后系统将会在“星期二”自动重启。

系统时间：用户可以更改系统的时间，并与 PC 端同步；还可以对 NTP 服务进行设置。

配置设置：用户可以对配置进行导入和导出操作，或者恢复出厂设置。

如图 3-1 所示。

图3-1 本机设置

3.2 联网配置

您可以在联网配置开启支持幢、支持单元、支持群呼，如图 3-2 所示。

图3-2 联网配置

3.3 网络设置

3.3.1 网络设置

用户可以进行网络设置，设置 SIP 服务器的 IP 地址、子网掩码和默认网关；修改完 IP 地址后，设备将会重启。

如图 3-3 所示。

图3-3 网络设置

3.3.2 FTP 设置

用户可以进行 FTP 设置，设置 FTP 服务器的 IP 地址、端口，设置用户名和密码，如图 3-4 所示。

图3-4 FTP 设置

3.3.3 应用端口设置

用户可以进行应用端口设置，包括设置 WEB 端口、SIP 端口、RIP 端口和路由设置。

具体操作步骤如下：

步骤1　选择“系统设置 > 网络设置 > 应用端口设置”，如图 3-5 所示。

图3-5 应用端口设置

步骤2　单击“路由设置”。

系统显示如图 3-6 所示界面。

图3-6 路由表信息

步骤3　输入“平台 IP 地址”，端口为“5080”。

步骤4　单击“确定”。

步骤5　完成应用端口配置。

3.3.4 DDNS 设置

用户可以通过在网络设置界面设置 DDNS，包括服务器的类型、名称、端口、域、用户名、密码和 DDNS 有效时间等参数信息。

如图 3-7 所示。

图3-7 DDNS 设置

3.4 IPC 信息

您可以在“系统设置＞IPC 信息”界面，查看所有 IPC 信息。

3.5 公告信息

您可以在“系统设置＞公告信息”界面，发布及查询公告信息。

发布信息的操作步骤如下：

步骤1　选择“系统设置＞公告信息”。

　　系统显示“发送公告”界面。

步骤2　选择有效期及发送人群，输入标题和内容。

　　如图 3-8 所示。

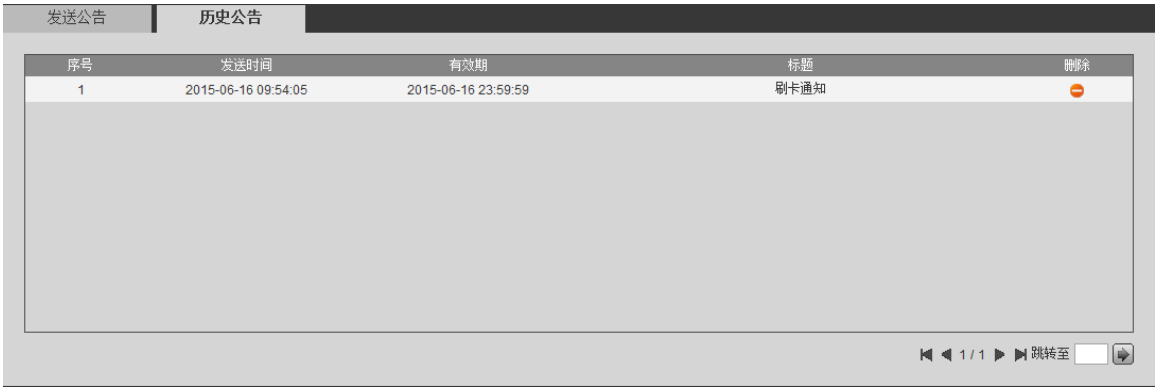
图3-8 发送公告

步骤3　单击“发送”，完成公告信息发布。

单击“历史公告”，用户可以查询所有历史发布的公告信息。

如图 3-9 所示。

图3-9 历史公告



4 用户管理

您可以根据需要添加、删除用户或者修改用户的密码。

4.1 添加用户

步骤1　选择“系统设置 > 用户管理 > 用户管理”。

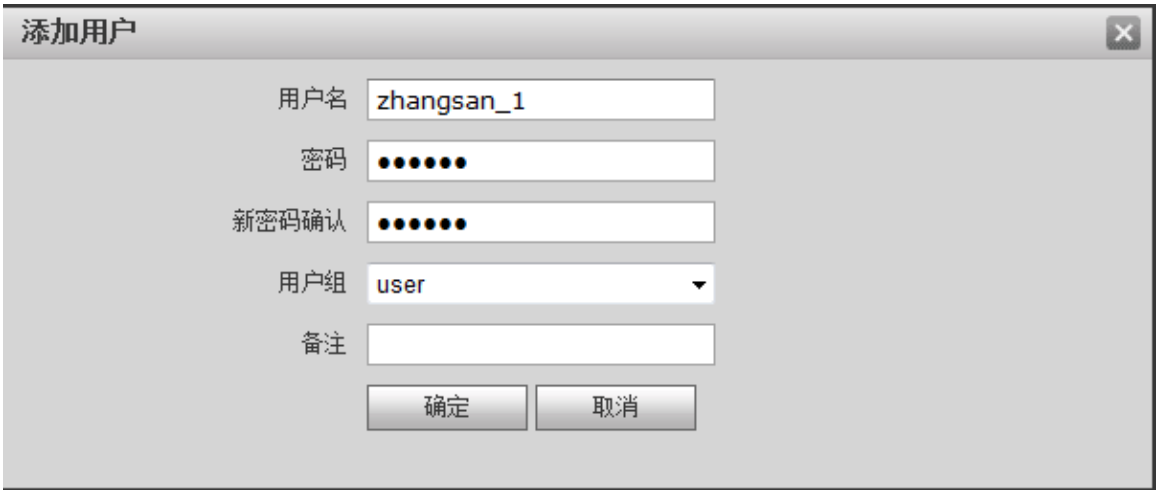
系统显示“用户管理”界面。

步骤2　单击“添加用户”。

系统显示“添加用户”界面。

步骤3　配置界面参数信息，如图 4-1 所示。

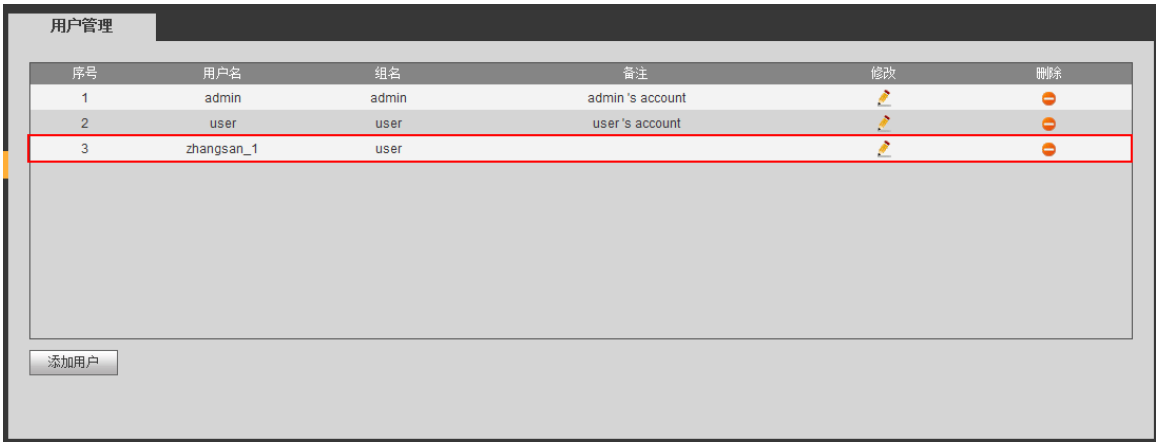
图4-1 添加用户



目前系统支持两种用户组类型的用户：admin 和 user。admin 具有较高权限，可以查看、编辑、删除系统配置的权限；user 仅拥有查看系统配置的权限。

步骤4　单击“确定”，完成用户添加，如图 4-2 所示。

图4-2 用户添加成功



4.2 删除用户

选择需要删除的用户，单击“”，删除对应用户。

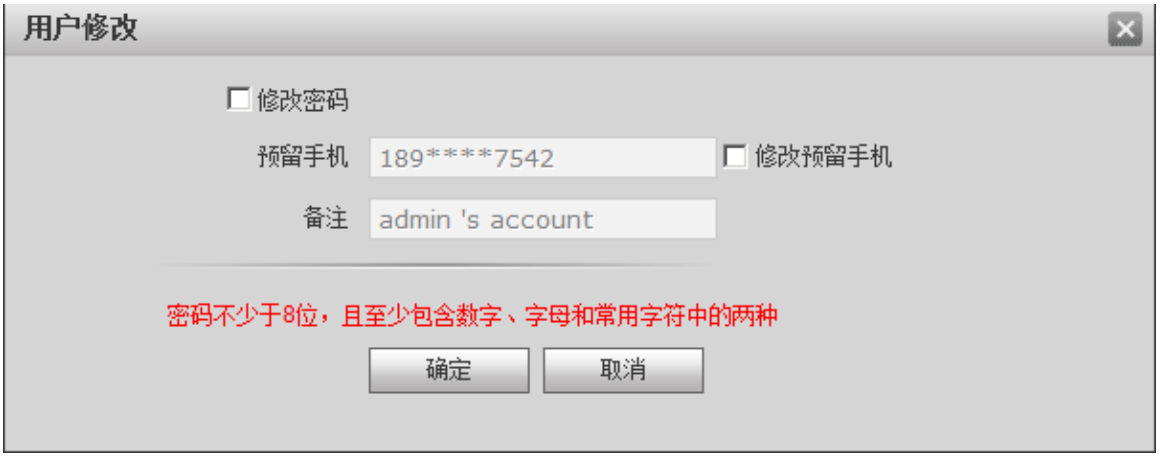
4.3 修改 admin 用户信息

admin 用户可以修改自己的用户密码和预留手机。预留手机号码用于密码重置，接收信息。

步骤1　单击 admin 用户信息行上的。

系统显示“用户修改”界面，如图 4-3 所示。

图4-3 修改密码界面（1）

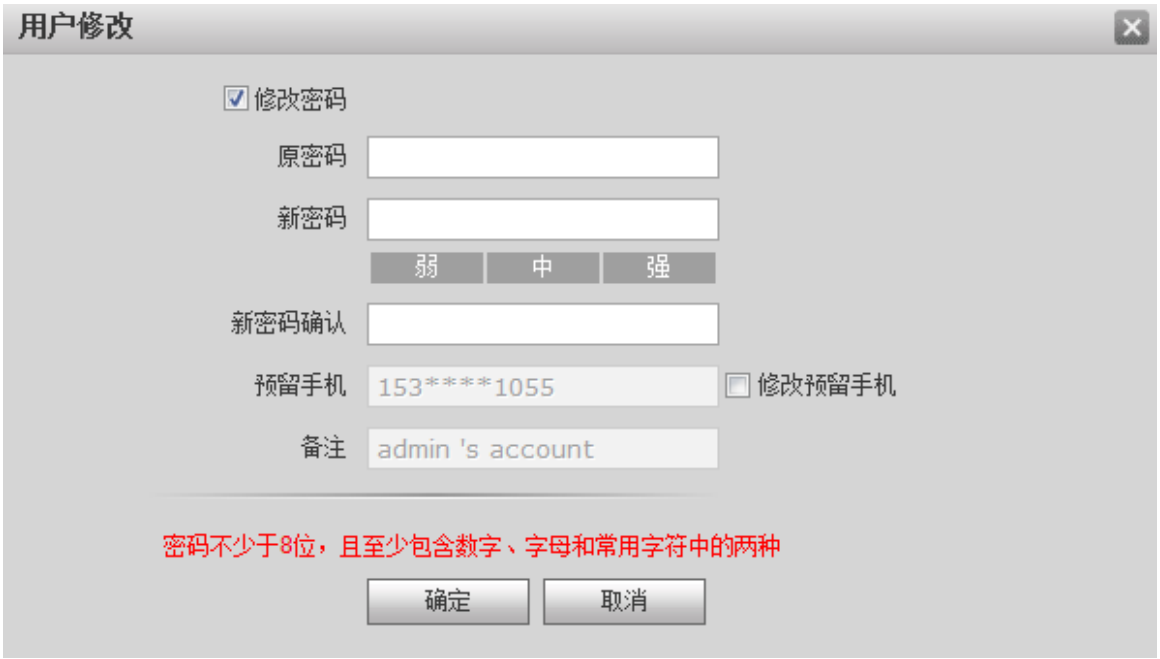


步骤2　修改用户信息。

1. 选择“修改密码”。

   系统显示密码修改界面，如图 4-4 所示。

图4-4 修改密码界面（2）



2. 输入“原密码”、“新密码”和“新密码确认”。
3. 选择“修改预留手机”，输入手机号码。

4. 单击“确定”。

4.4 修改普通用户信息

步骤1 选择需要修改的用户，单击 。

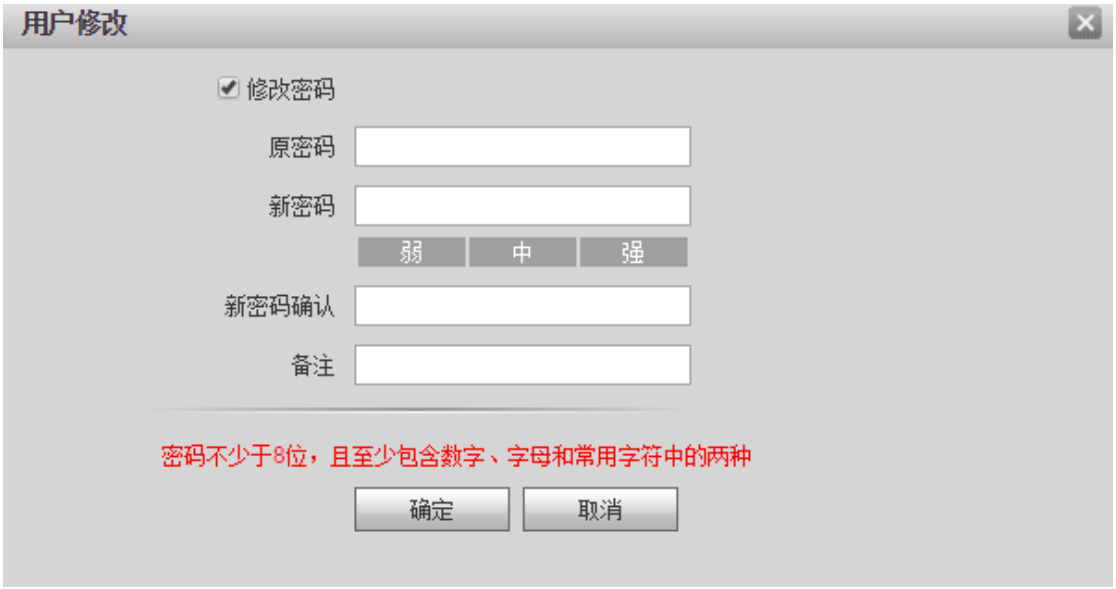
系统显示“修改用户”界面，如图 4-5 所示。

图4-5 修改用户

步骤2 选择“修改密码”复选框。

界面显示“原密码”、“新密码”和“新密码确认”，如图 5-30 所示。

图4-6 密码修改



步骤3 配置界面参数信息。

步骤4 单击“确定”，完成密码修改。

5 设备管理

您可以进行单独添加或者批量添加门口机和室内机，具体操作步骤如下：

5.1 批量添加门口机、室内机

以批量添加 5 幢 3 单元，20 层，每层 6 户为例。

步骤1　选择“系统设置＞联网配置＞小区配置”。

系统显示“小区配置”界面。

步骤2　配置参数信息。

如图 5-1 所示。

图5-1 小区配置

步骤3　单击“确定”，批量添加完成。

说明

一般情况下，1 个单元配备 1 个 SIP 服务器，1 个 SIP 服务器大约可以管理 250 台设备。

5.2 单独添加门口机、室内机设备

以添加“门口机”为例，操作步骤如下：

步骤1　选择“系统设置＞设备管理＞门口机管理”。

系统显示“门口机”界面。

步骤2　单击“添加”。

系统显示“添加”界面。

步骤3　填写 VTO 编号，格式为“800X”；填写栋号和楼内单元号。

如图 5-2 所示。

图5-2 添加

步骤4　单击“确定”，完成门口机的添加。

如图 5-3 所示。

图5-3 门口机添加成功

单击，修改门口机参数信息。

单击，删除添加的门口机。

说明

添加“室内机”时，添加的“VTH 短号”即室内机的房间号。

6 信息查询

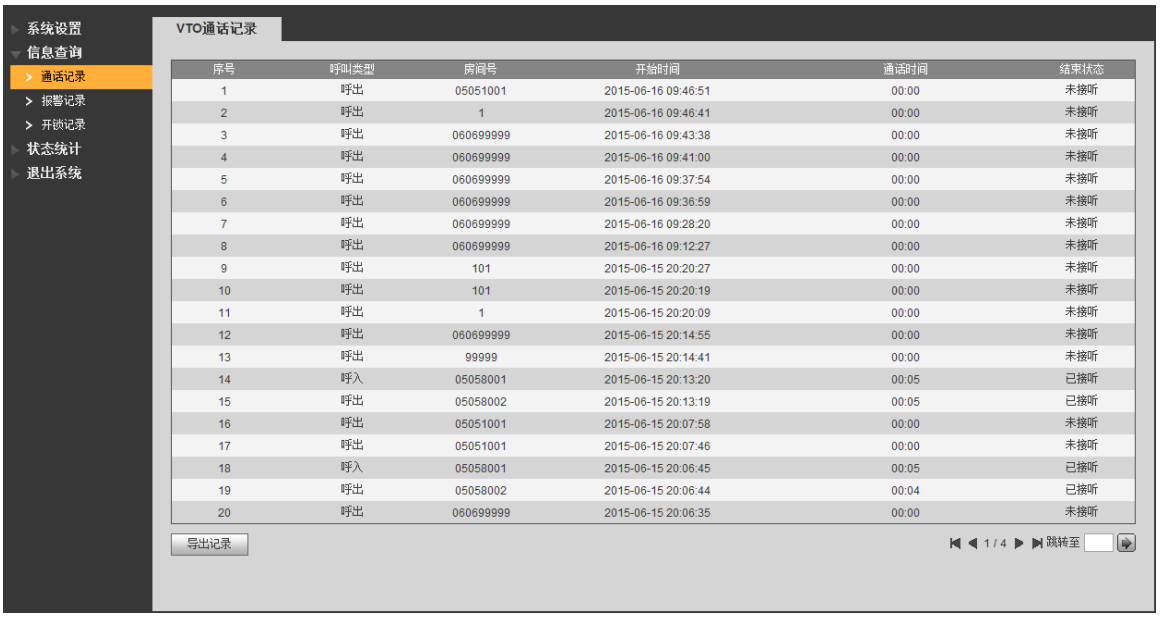
用户可以在信息查询界面查询所有的 VTO 通话记录、报警记录和门口机开锁记录。

6.1 通话记录

用户可以在“信息查询＞通话记录”界面，查询所有 VTO 通话记录。

如图 6-1 所示。

图6-1 通话记录



单击“导出记录”，可以导出所有通话记录信息。

6.2 报警记录

用户可以在“信息查询＞报警记录”界面，查询所有报警记录。

如图 6-2 所示。

图6-2 报警记录

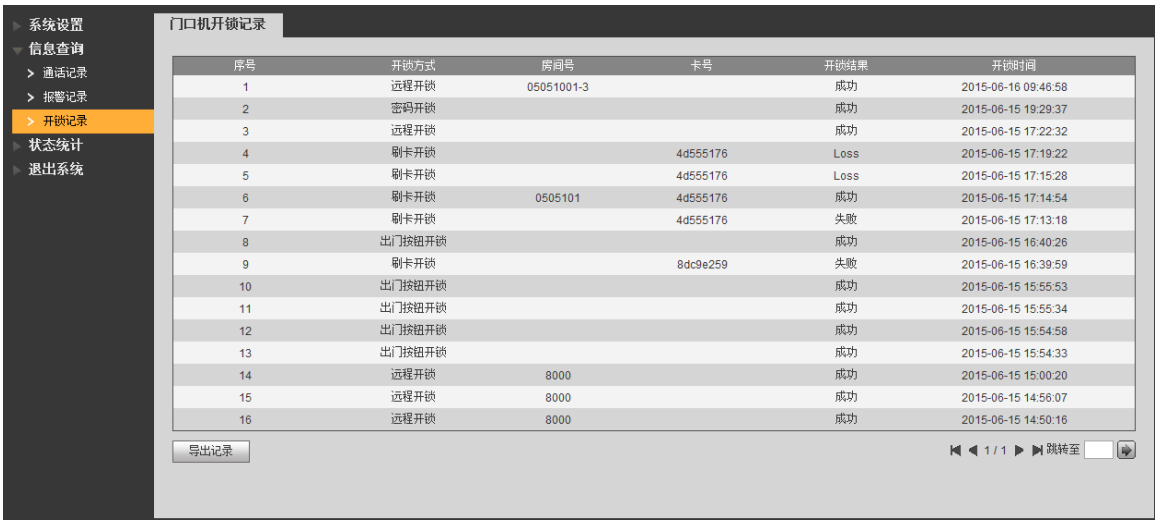
单击“导出记录”，可以导出所有报警记录信息。

6.3 开锁记录

用户可以在“信息查询＞开锁记录”界面，查询所有开锁记录。

如图 6-3 所示。

图6-3 开锁记录



单击“导出记录”，可以导出所有开锁记录信息。

附录1 技术规格

型号	VTNS2000B-S
操作系统	嵌入式 LINUX 操作系统
电源	DC 12V
网络	TCP/IP 10M/100Mbps
功耗	待机功耗≤1W； 最大功耗≤7W
工作温度	-10℃～+55℃
工作湿度	10~95%RH
尺寸	130mm×130mm×31mm
重量	0.7 Kg

装 箱 清 单

所列内容为本包装箱内应包括的设备和资料，请在开箱时认真检查，并妥善保管。

部件名称	数量	备注
☐ 主机	一台	
☐ 产品说明书	一本	
☐ 电源适配器	一个	
☐ 安装螺钉	一包	

附录3 法律声明

商标声明

- VGA 是 IBM 公司的商标。
- Windows 标识和 Windows 是微软公司的商标或注册商标。
- 在本文档中可能提及的其他商标或公司的名称，由其各自所有者拥有。

责任声明

- 在适用法律允许的范围内，在任何情况下，本公司都不对因本文档中相关内容及描述的产品而产生任何特殊的、附随的、间接的、继发性的损害进行赔偿，也不对任何利润、数据、商誉、文档丢失或预期节约的损失进行赔偿。
- 本文档中描述的产品均“按照现状”提供，除非适用法律要求，本公司对文档中的所有内容不提供任何明示或暗示的保证，包括但不限于适销性、质量满意度、适合特定目的、不侵犯第三方权利等保证。

隐私保护提醒

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

关于本文档

- 本文档供多个型号产品使用，产品外观和功能请以实物为准。
- 如果不按照本文档中的指导进行操作而造成的任何损失由使用方自己承担。
- 本文档会实时根据相关地区的法律法规更新内容，具体请参见产品的纸质、电子光盘、二维码或官网，如果纸质与电子档内容不一致，请以电子档为准。
- 本公司保留随时修改本文档中任何信息的权利，修改的内容将会在本文档的新版本中加入，恕不另行通知。
- 本文档可能包含技术上不准确的地方、或与产品功能及操作不相符的地方、或印刷错误，以公司最终解释为准。
- 如果获取到的 PDF 文档无法打开，请使用最新版本或最主流的阅读工具。

附录4 网络安全建议

保障设备基本网络安全的必须措施：

1. **使用复杂密码**

   请参考如下建议进行密码设置：

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

2. **及时更新固件和客户端软件**

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

增强设备网络安全的建议措施：

1. **物理防护**

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

2. **定期修改密码**

   建议您定期修改密码，以降低被猜测或破解的风险。

3. **及时设置、更新密码重置信息**

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

4. **开启帐户锁定**

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

5. **更改 HTTP 及其他服务默认端口**

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

6. **使能 HTTPS**

   建议您开启 HTTPS，通过安全的通道访问 Web 服务。

7. **启用白名单**

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

8. **MAC 地址绑定**

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

9. **合理分配帐户及权限**

   根据业务和管理需要，合理新增用户，并合理为其分配最小权限集合。

10. **关闭非必需服务，使用安全的模式**

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

    如果有需要，强烈建议您使用安全的模式，包括但不限于：

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

11. 音视频加密传输

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

12. 使用 PoE 方式连接设备

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

13. 安全审计

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

14. 网络日志

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

15. 安全网络环境的搭建

为了更好地保障设备的安全性，降低网络安全风险，建议您：

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