



SmartPSS Plus可视对讲方案











使用说明书



前言

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。
 防静电	表示静电敏感的设备。
 当心触电	表示高压危险。
 激光辐射	表示强激光辐射。
 风扇警告	表示危险运动部件，请远离运动风扇叶片。
 当心机械伤人	表示设备部件机械伤人。
 窍门	表示能帮助您解决某个问题或节省您的时间。
 说明	表示是正文的附加信息，是对正文的强调和补充。

修订记录




版本号	修订内容	发布日期
V2.0.0	<ul style="list-style-type: none"> 新增对讲配置章节。 更新对讲管理章节。 更新对讲记录章节。 	2021.08
V1.0.1	新增配置SIP服务器章节。	2021.02
V1.0.0	首次发布。	2020.12


目 录

前言.....	I
第 1 章 打开可视对讲方案.....	1
第 2 章 对讲配置	2
2.1 号码管理	2
2.2 呼叫分组	4
2.3 信息发布	6
第 3 章 对讲管理	9
第 4 章 对讲记录	14
4.1 对讲记录	14
4.2 门禁记录	15
4.3 报警记录	15
附录1 法律声明	17
附录2 网络安全声明和建议.....	19

第 1 章 打开可视对讲方案


不同场景打开可视对讲方案的操作方法不同。

- 如果是首次安装使用平台，在平台初始化过程中选择可视对讲方案。登录后，在主页的左侧导航栏单击  可视对讲，打开方案。
- 如果已初始化平台，但未选择可视对讲方案，在界面右上角选择“ > 切换方案”，选择可视对讲方案。登录后，在主页的左侧导航栏单击  可视对讲，打开方案。

关于加载方案的详细介绍请参见平台使用说明书。在界面右上角选择“ > 帮助手册”，获取平台使用说明书。

第 2 章 对讲配置

主要用于组织管理、呼叫号码管理等，同时可以进行呼叫配置、信息发布等。

选择“主页 > 设备管理”，添加可视对讲设备到系统，详细介绍请参见大华星睿_SmartPSS Plus 使用说明书。在界面右上角选择“ > 帮助手册”，获取大华星睿_SmartPSS Plus使用说明书。

2.1 号码管理

操作步骤


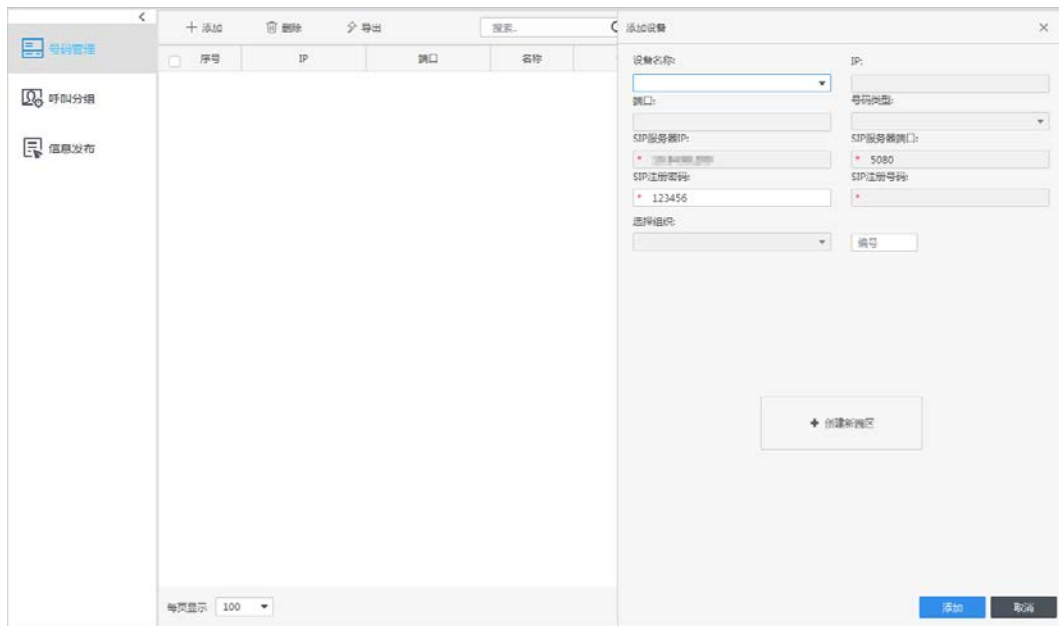
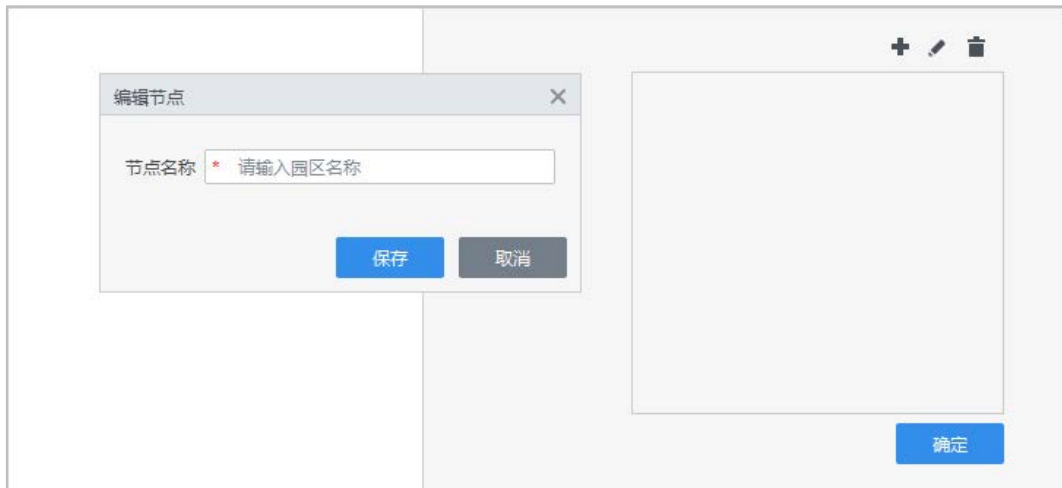
- 步骤1 打开“可视对讲”方案。
- 步骤2 在主页选择“对讲配置 > 号码管理”。
- 步骤3 单击  添加，然后在右侧界面中单击“创建新园区”。

图2-1 号码管理页面



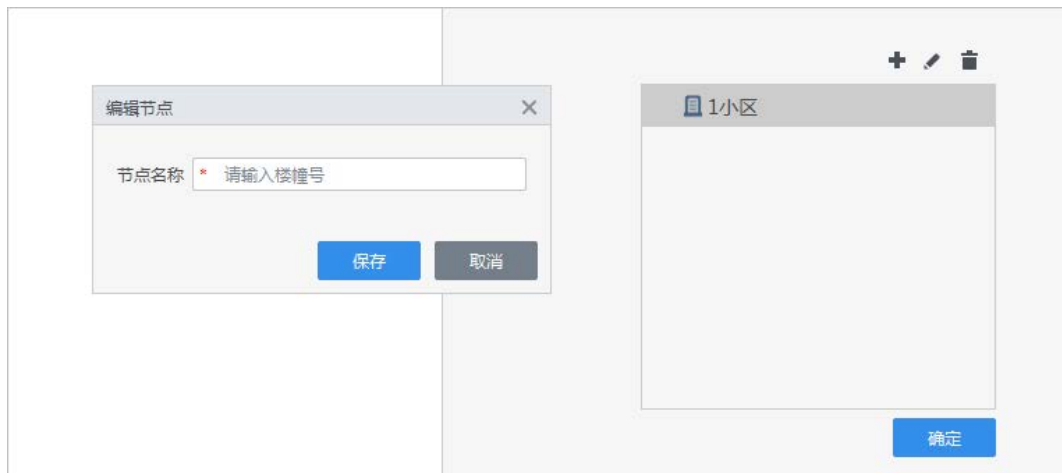
1. 单击 ，在弹窗界面中输入园区名称，单击“保存”。

图2-2 新增园区名称



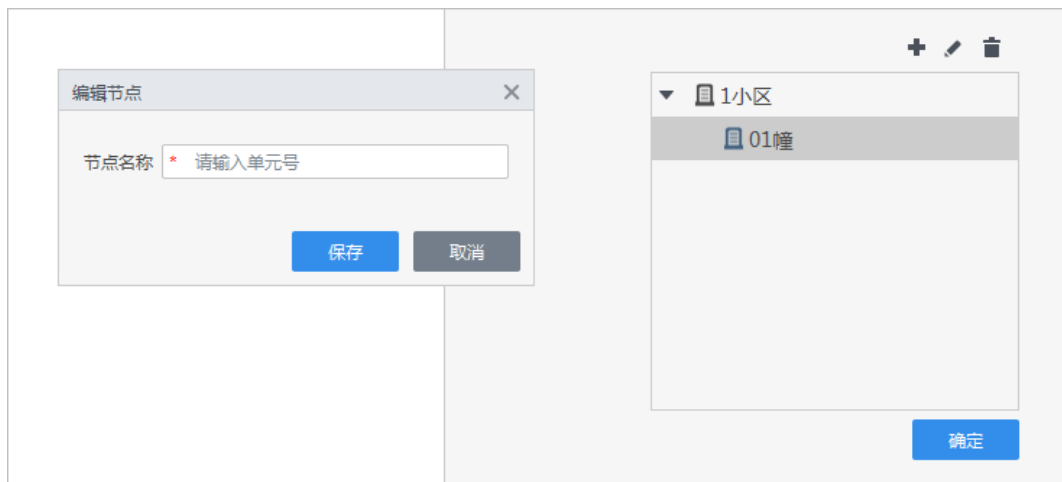
- 选中需要增加楼幢的园区名称，单击 $+$ ，在弹窗界面中输入楼幢号，单击“保存”。

图2-3 新增楼幢号



- 选中需要增加单元的园区名称，单击 $+$ ，在弹窗界面中输入单元名称，单击“保存”。

图2-4 新增单元号



说明

- 选中需要编辑的园区组织，单击 ✎ ，编辑该园区组织名称；选中需要删除的园区组织，单击 ✖ ，删除该园区组织。

- 组织下无设备时支持删除组织。

4. 单击“确定”。

步骤4 在下拉列表中选择需要添加的设备名称，选择号码类型及组织。单击“添加”。



图2-5 添加设备







说明

- 门口机、围墙机和管理机需要输入编号（不超过2位）；室内机需要输入编号（不超过5位）和分机号（不超过2位）。
- 门口机和室内机只能添加到单元层级；围墙机和管理机默认添加到园区层级。
- 单击“修改组织”可再次编辑园区组织树。

步骤5 查看设备状态。

- 选择需要导出的设备，单击“导出”，导出选择的设备信息到本地。
- 选择需要删除的设备，单击“删除”或单击设备对应的，删除设备信息。
- 单击，弹出“添加设备”界面，编辑设备信息。
- 在搜索栏中输入需要搜索的设备别名或IP搜索设备。

相关操作

- 单击 每页显示 ，选择每页显示信息条数。
- 单击，查看前一页/后一页。
- 单击，查看首页/尾页。
- 在 跳到  页，输入页数，单击“转到”，转至相应页数。

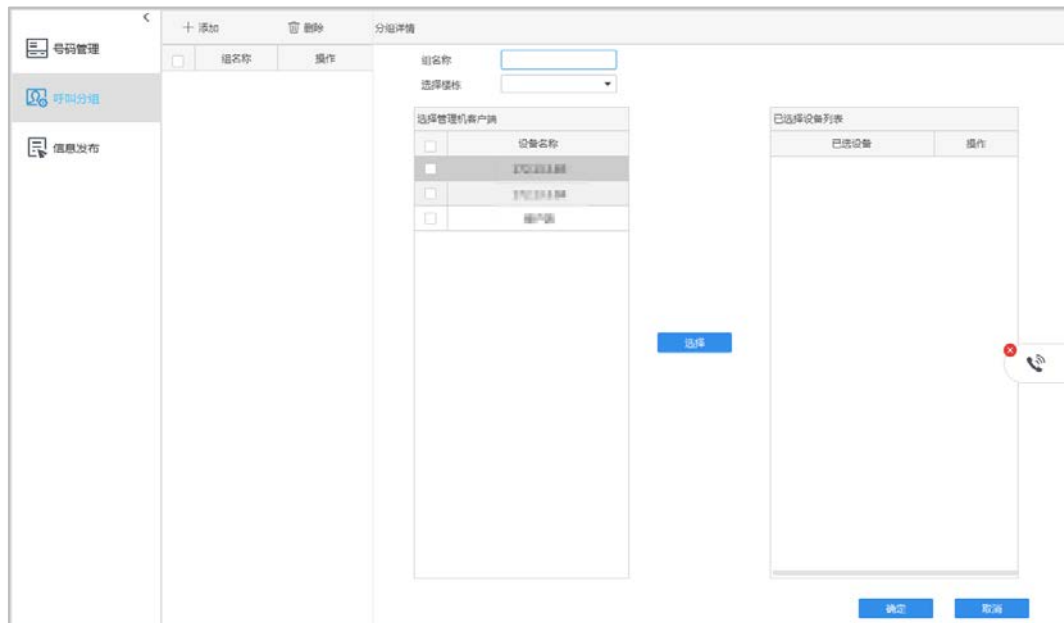
2.2 呼叫分组

呼叫分组将管理机与客户端进行分组并分配给相应楼栋，使楼栋能按顺序呼叫对应分组的管理机或客户端。

操作步骤

- 步骤1 打开“可视对讲”方案。
- 步骤2 在主页选择“对讲配置 > 呼叫分组”页签。

图2-6 呼叫分组页面



- 步骤3 编辑组名字，并在下拉列表中选择需要配置的楼栋。
- 步骤4 选择需要添加的管理机客户端，单击“选择”，设备出现在“已选择设备列表”中。

图2-7 已选设备列表



- 单击↑优先呼叫此设备。
- 单击↓降低此设备优先级。
- 单击🗑️删除此条设备信息。




说明

当楼幢未添加分组时，楼幢下设备呼叫物业会统一由平台接听；围墙机呼叫物业只能由平台接听；管理机无法呼叫物业。

步骤5 单击“确定”。

相关操作

- 单击页面右侧的“添加”可添加多条分组。
- 单击分组对应的，或选择需要删除的分组，单击“删除”，删除分组信息。

2.3 信息发布

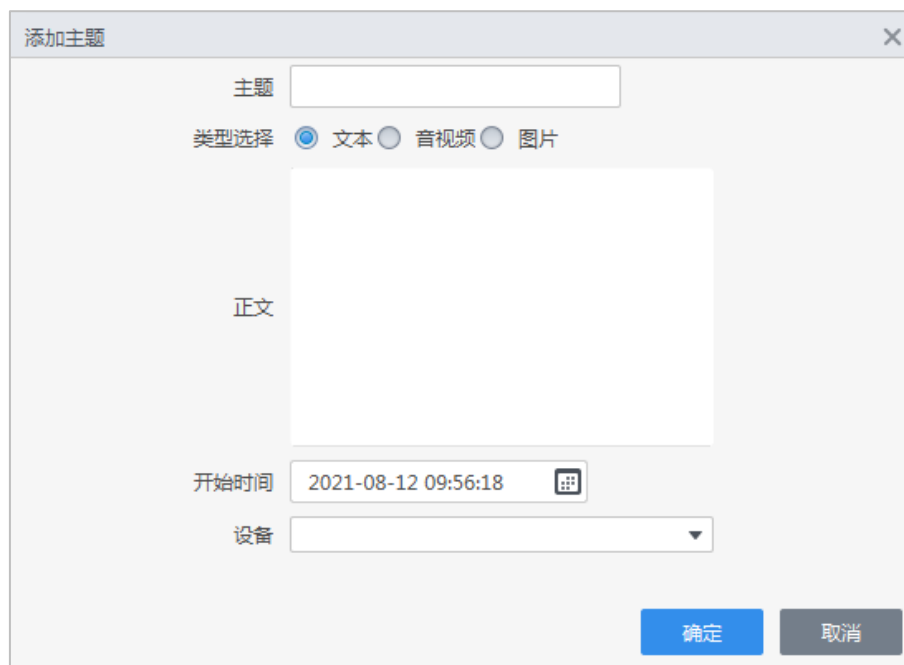
前提条件

只有设备管理中设备类型为VTO或VTH的设备，且在可视对讲解决方案中有绑定号码的设备才支持该功能。

操作步骤

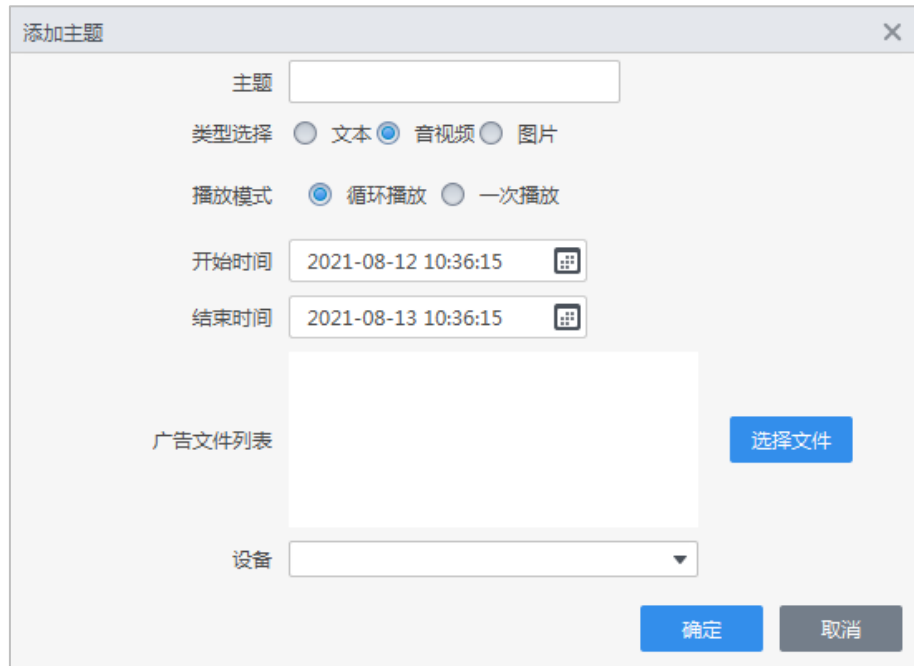
- 步骤1 打开“可视对讲”方案。
- 步骤2 在主页选择“对讲配置 > 信息发布”页签。
- 步骤3 单击“添加”，添加主题。
- 步骤4 编辑主题内容，选择需要添加的主题类型。
 - 若选择的主题类型为文本，编辑需要添加的文本，并设置开始时间。

图2-8 添加文本



- 若选择的主题类型为音视频，选择播放模式，并设置开始和结束时间。单击选择文件，从本地上传需要导入的广告文件。

图2-9 添加音视频



添加主题

主题

类型选择 ☐ 文本 ☒ 音视频 ☐ 图片

播放模式 ☒ 循环播放 ☐ 一次播放

开始时间 2021-08-12 10:36:15

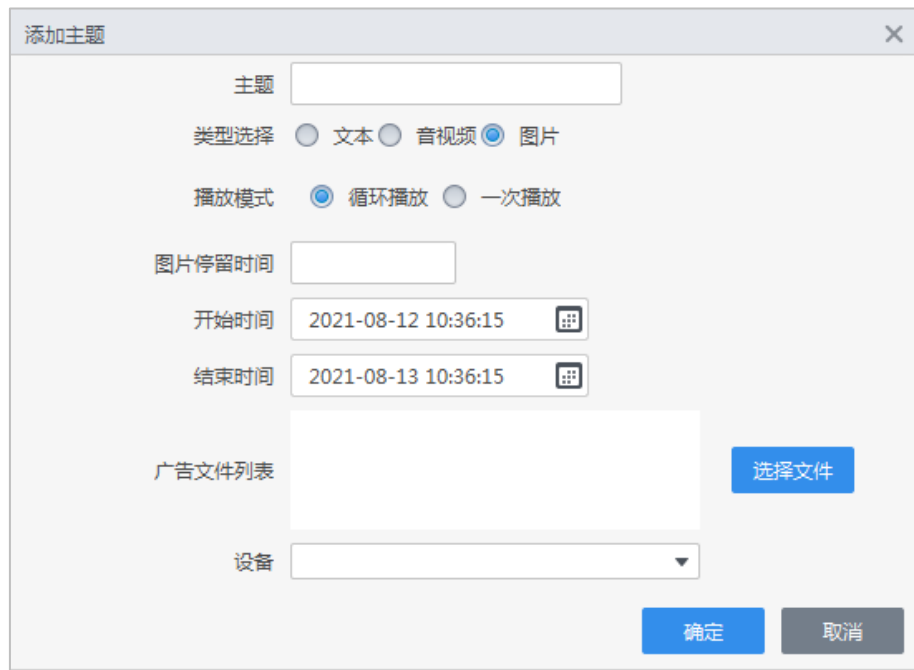
结束时间 2021-08-13 10:36:15

广告文件列表

设备

- 若选择的主题类型为图片，选择播放模式，并设置图片停留时间及开始和结束时间。单击选择文件，从本地上传需要导入的广告文件。

图2-10 添加图片



添加主题

主题

类型选择 ☐ 文本 ☐ 音视频 ☒ 图片

播放模式 ☒ 循环播放 ☐ 一次播放

图片停留时间

开始时间 2021-08-12 10:36:15

结束时间 2021-08-13 10:36:15

广告文件列表

设备

步骤5 从下拉列表中选择需要添加到的设备，单击“确定”。

步骤6 查看添加的主题信息。

图2-11 查看主题信息

号码管理

呼叫分组





信息发布

+ 添加

删除

发送

<input type="checkbox"/>	主题	设备	信息	状态	操作
<input type="checkbox"/>	1	<div></div>	文字播放	<div></div>	已发布
<input checked="" type="checkbox"/>	2	<div></div>	图片播放	<div></div>	已发布
<input type="checkbox"/>	3	<div></div>	文字播放	<div></div>	未发布
<input type="checkbox"/>	4	<div></div>	图片播放	<div></div>	未发布

- 单击主题对应的编辑添加的主题信息。
- 单击主题对应的, 或选择需要删除的主题, 单击“删除”, 删除主题信息。
- 单击主题对应的, 或选择需要发布的主题, 单击“发送”, 发布信息到设备端。发布成功则“状态”显示“已发布”。
- 单击查看主题详细信息。

第 3 章 对讲管理

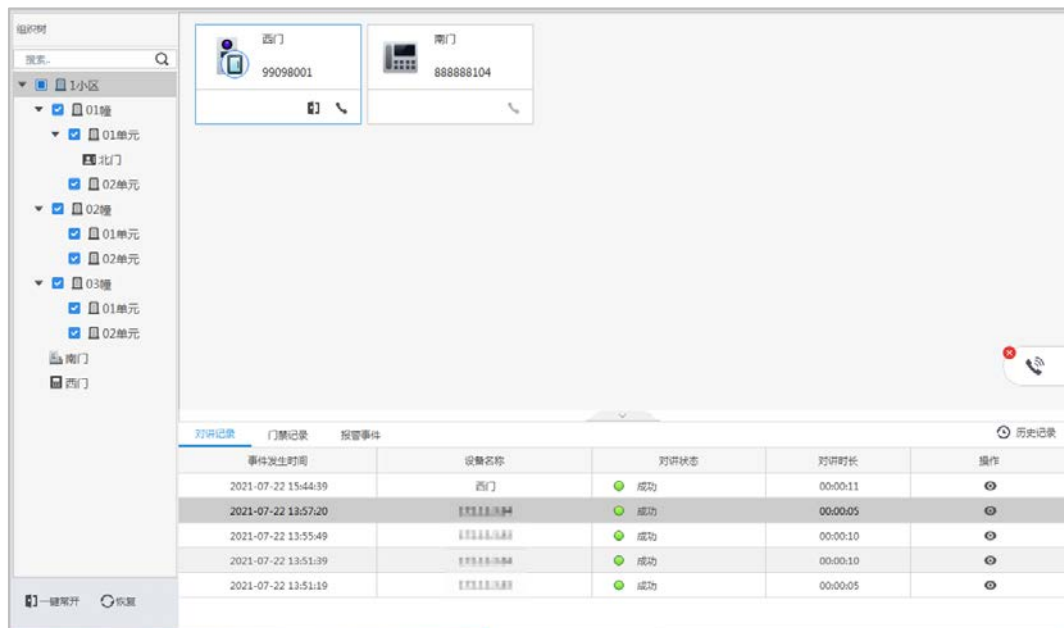
主要用于平台、管理机、门口机和室内机之间的可视对讲，同时可以远程开门、快捷呼叫、近期记录展示等。

操作步骤

步骤1 打开“可视对讲”方案。

步骤2 在主页单击“可视对讲管理”页签，然后在设备列表中选择需要查看的对讲设备。

图3-1 可视对讲管理

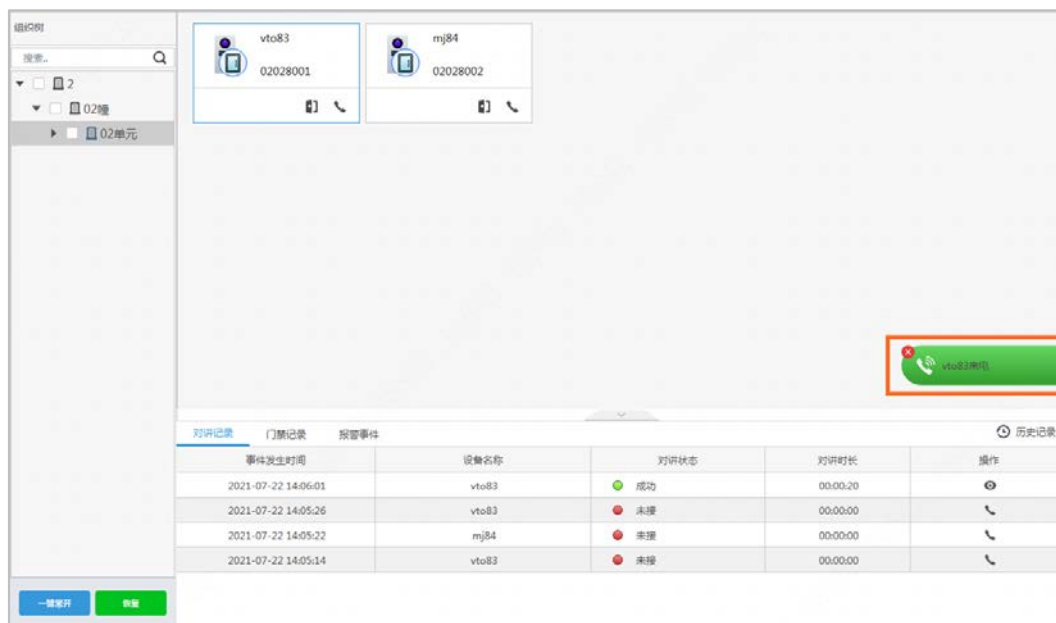


说明

设备列表组织树默认展示到单元级别。

- 发起通话。
当您需要与设备端可视通话时，单击设备下方的📞，弹出可视对讲通话界面。
- 设备端请求通话。
当设备端点击物业或者管理中心呼叫平台时，您可以按照实际需求进行操作。
 1. 单击悬浮窗接受通话，进入可视对讲界面。
 2. 单击❌，拒绝接听此次来电。

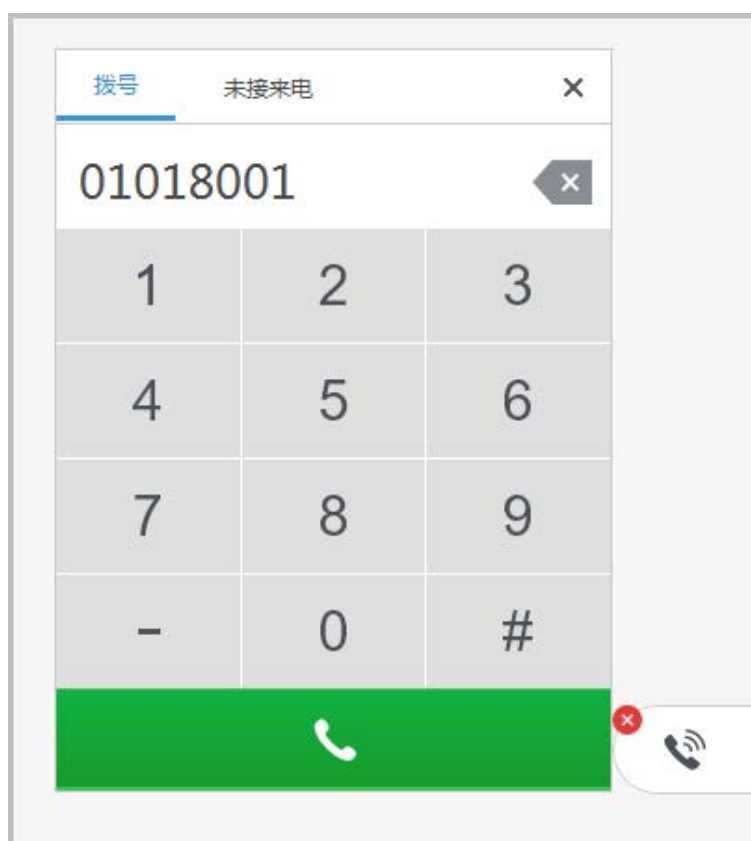
图3-2 设备端来电



- 呼叫对讲设备。

单击 ，弹出拨号界面，输入号码后可呼叫对应对讲设备。

图3-3 呼叫页面

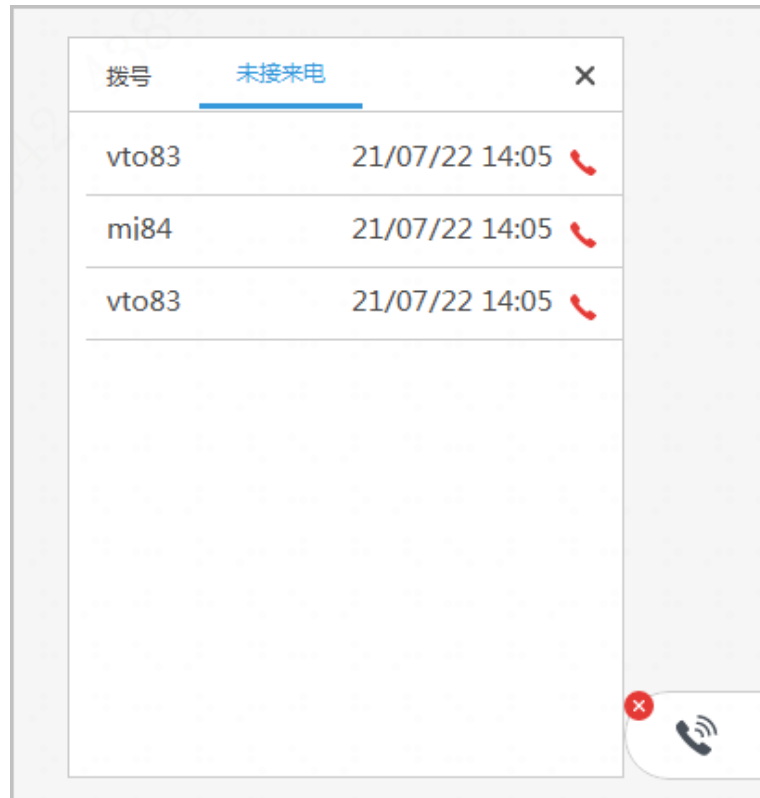


说明

呼叫界面只支持全号呼叫，不支持输房间号呼叫；如果要呼叫室内机，要输入编号和分机号。

单击“未接来电”，可查看未接的号码。

图3-4 未接号码



- 回拨未接来电。



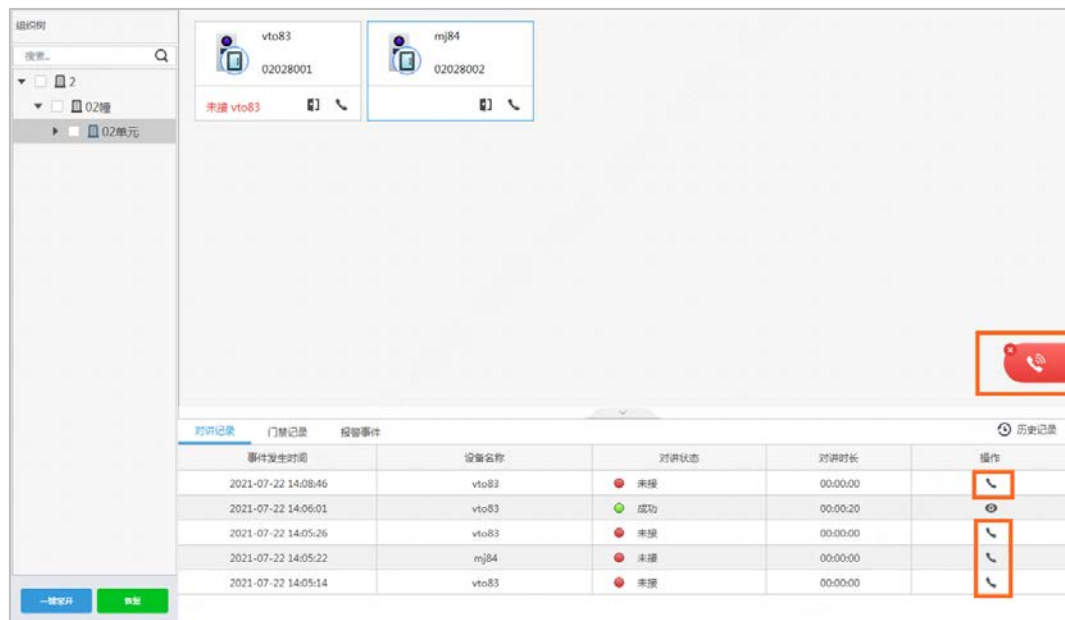
当有未接或拒接的来电记录时，您可以单击记录后面的进行回拨，或者单击悬浮窗，单击对应来电后面的进行回拨。

图3-5 未接来电





步骤3 根据实际需求在可视对讲通话过程中操作。

图3-6 可视对讲界面



表3-1 可视对讲界面参数说明

参数	说明
	打开该设备对应的门。
自动抓图	启用后，每当该设备接通可视对讲后，系统将截取一张通话时画面保存至可视对讲记录。
自动录像	启用后，每当该设备接通可视对讲后，系统将截取通话录像保存至可视对讲记录。  说明 单次通话仅可保留一段录像。
话筒静音	启用后，您的话筒将静音。
静音	启用后，设备端话筒将静音。



说明

系统自动记录开关状态，下次对讲时同样生效。

步骤4 单击右上角  关闭界面，终止通话。


步骤5 单击设备下方的 ，打开设备门禁。



图3-7 打开门禁设备



说明

- 打开门禁后，设备图标由  变为 。
- 单击“组织树”下方的“一键常开”和“恢复”，可对设备进行一键开门操作。

相关操作

- 单击通话记录后面的 ，查看可视对讲通话时保存的图片及录像。
- 对讲事件、门禁事件和报警事件将实时记录在实时记录列表中。此列表仅显示最新的100条对讲记录、门禁记录和报警记录。单击  历史记录，进入可视对讲记录界面查看所有记录。

第 4 章 对讲记录

主要用于通话记录、门禁记录、报警记录的筛选、查询、导出等。

4.1 对讲记录

查看发生对讲事件时的记录，支持导出对讲事件记录。

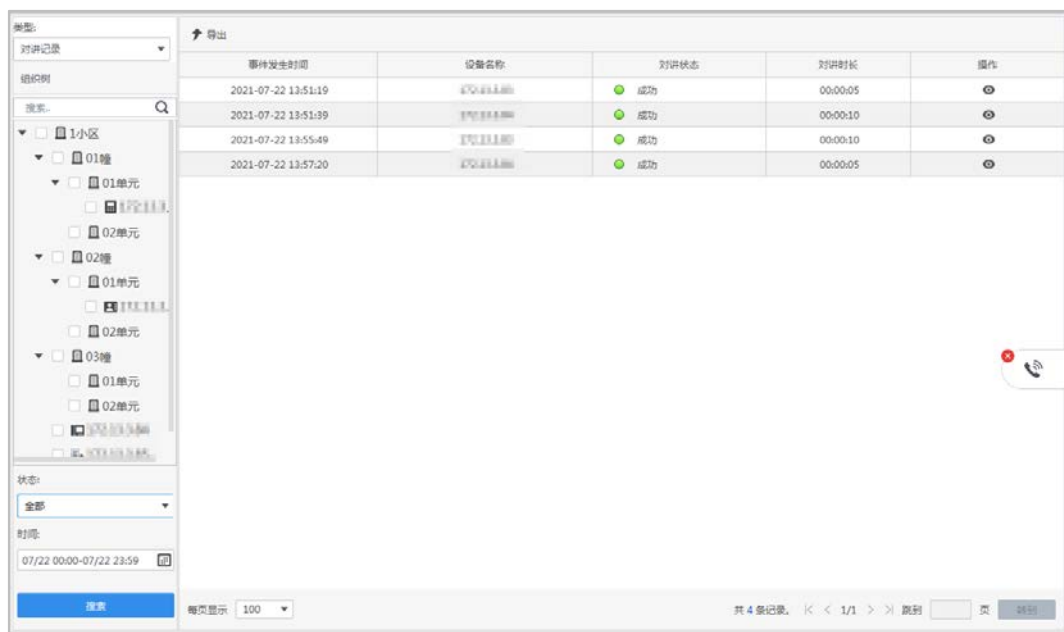
前提条件

确保系统内添加的可视对讲设备发生过对讲事件。

操作步骤

- 步骤1 打开“可视对讲”方案。
- 步骤2 在“类型”中选择“对讲记录”。
- 步骤3 在界面左侧组织树中选择需要查询的设备，选择“状态”类型，设置对讲时间段。
- 步骤4 单击“搜索”。

图4-1 查看对讲记录



说明

单击 查看可视对讲通话时保存的图片及录像。

- 步骤5 单击“导出”，导出所有对讲记录到本地。

相关操作

- 单击 每页显示 ，选择每页显示信息条数。
- 单击 ，查看前一页/后一页。
- 单击 ，查看首页/尾页。
- 在 跳到 页，输入页数，单击“转到”，转至相应页数。

4.2 门禁记录

查看发生开关门事件时的记录，支持导出门禁事件记录。

前提条件

确保系统内添加的可视对讲设备发生过门禁事件。

操作步骤

- 步骤1 打开“可视对讲”方案。
- 步骤2 在“类型”中选择“门禁记录”。
- 步骤3 在界面左侧组织树中选择需要查询的设备，设置记录时间段。
- 步骤4 单击“搜索”。

图4-2 查看门禁记录



- 步骤5 单击“导出”，导出所有门禁记录到本地。

相关操作

- 单击 每页显示 20，选择每页显示信息条数。
- 单击 </>，查看前一页/后一页。
- 单击 </>，查看首页/尾页。
- 在 跳到 页，输入页数，单击“转到”，转至相应页数。

4.3 报警记录

查看发生报警事件时的记录，支持导出报警事件记录。

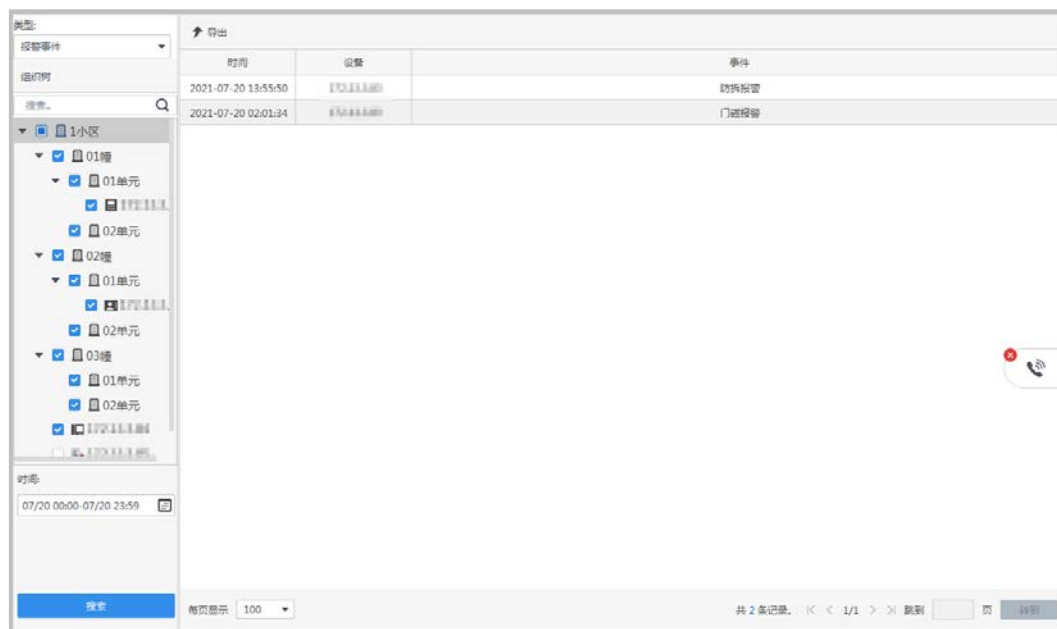
前提条件

确保系统内添加的可视对讲设备发生过报警事件。

操作步骤

- 步骤1 打开“可视对讲”方案。
- 步骤2 在“类型”中选择“报警记录”。
- 步骤3 在界面左侧组织树中选择需要查询的设备，设置报警时间段。
- 步骤4 单击“搜索”。

图4-3 查看报警记录



- 步骤5 单击“导出”，导出所有报警记录到本地。

相关操作

- 单击“每页显示 20”，选择每页显示信息条数。
- 单击“</>”，查看前一页/后一页。
- 单击“</>”，查看首页/尾页。
- 在“跳到”页，输入页数，单击“转到”，转至相应页数。

附录1 法律声明

版权声明

© 2021 浙江大华技术股份有限公司。版权所有。

在未经浙江大华技术股份有限公司（下称“大华”）事先书面许可的情况下，任何人不能以任何形式复制、传递、分发或存储本文档中的任何内容。

本文档描述的产品中，可能包含大华及可能存在的第三人享有版权的软件。除非获得相关权利人的许可，否则，任何人不能以任何形式对前述软件进行复制、分发、修改、摘录、反编译、反汇编、解密、反向工程、出租、转让、分许可等侵犯软件版权的行为。

商标声明

- 、、、、**HDCVI**是浙江大华技术股份有限公司的商标或注册商标。
- HDMI标识、HDMI和High-Definition Multimedia Interface是HDMI Licensing LLC的商标或注册商标。本产品已经获得HDMI Licensing LLC授权使用HDMI技术。
- VGA是IBM公司的商标。
- Windows标识和Windows是微软公司的商标或注册商标。
- 在本文档中可能提及的其他商标或公司的名称，由其各自所有者拥有。

责任声明

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

出口管制合规声明

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

隐私保护提醒

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

关于本文档

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

附录2 网络安全声明和建议

安全声明

- 若您将产品接入互联网需自担风险，包括但不限于可能遭受网络攻击、黑客攻击、病毒感染等，请您加强网络、设备数据和个人信息等的保护，采取保障设备网络安全的必要措施，包括但不限于使用复杂密码、定期修改密码、及时将固件更新至最新版本等。本公司不对因此造成的产品工作异常、信息泄露等问题承担任何责任，但本公司会提供产品相关安全维护。
- 在适用法律未明令禁止的程度下，对于因使用或无法使用本产品或服务而引起的任何利润、收入、销售损失、数据丢失或采购替代商品或服务的成本、财产损害、人身伤害、业务中断、商业信息损失，或者任何特殊的、直接的、间接的、附带的、经济性、覆盖性、惩罚性、特殊或从属损害，无论是基于何种责任理论（合同、侵权、过失或其他），本公司及其员工、许可方或附属公司都不承担赔偿责任，即使其已被告知存在此种损害的可能性也是如此。某些司法管辖区不允许对人身伤害、附带或从属损害等进行责任限制，则此限制可能不适用于您。
- 本公司对您的所有损害承担的总责任限额（除了因本公司过失导致人身伤亡的情况，需遵循适用法律规定）不超过您购买本公司产品所支付的价款。

安全建议

保障设备基本网络安全的必须措施：

1. 使用复杂密码

请参考如下建议进行密码设置：

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

2. 及时更新固件和客户端软件

- 按科技行业的标准作业规范，设备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。

更多内容

请访问大华官网安全应急响应中心，获取安全公告和最新的安全建议。

