SmartPSS Plus测温应用方案

使用说明书

浙江大华技术股份有限公司

V1.0.0

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
V1.0.0	首次发布	2021.03

目 录

前言 I
第 1 章 简介 1
第 2 章 打开测温应用方案 2
第 3 章 主界面 3
第 4 章 预览界面操作 4
第 5 章 热成像设置 5
第 6 章 处理异常报警 8
第 7 章 查询测温记录 9
附录1 法律声明 10
附录2 网络安全建议 12

第 1 章 简介

测温应用方案集合热成像设备、门禁一体机设备和SmartPSS Plus（以下简称“平台”），热成像设备通过感知实时监控范围内的人体温度，通过IVSS设备实时监测画面中人员戴口罩信息，当出现体温超过设置的阈值或发现画面中人员不戴口罩时，将报警信息上传到平台，触发平台报警铃声，并实时提取当前视频。同时本方案支持查询报警信息（包含图片及录像等信息）。

第 2 章 打开测温应用方案

不同场景打开测温应用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测温应用方案。登录后，在主页的左侧导航栏单击 ，打开方案。
- 如果已初始化平台，但未选择测温应用方案，在界面右上角选择“ > 切换方案”，选择测温应用方案。登录后，在主页的左侧导航栏单击 ，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 3 章 主界面

人体测温模块用于实时查看监控画面、异常报警信息（高温和未戴口罩）、温度信息等。

选择“人体测温”进入人体测温界面。

图3-1 人体测温

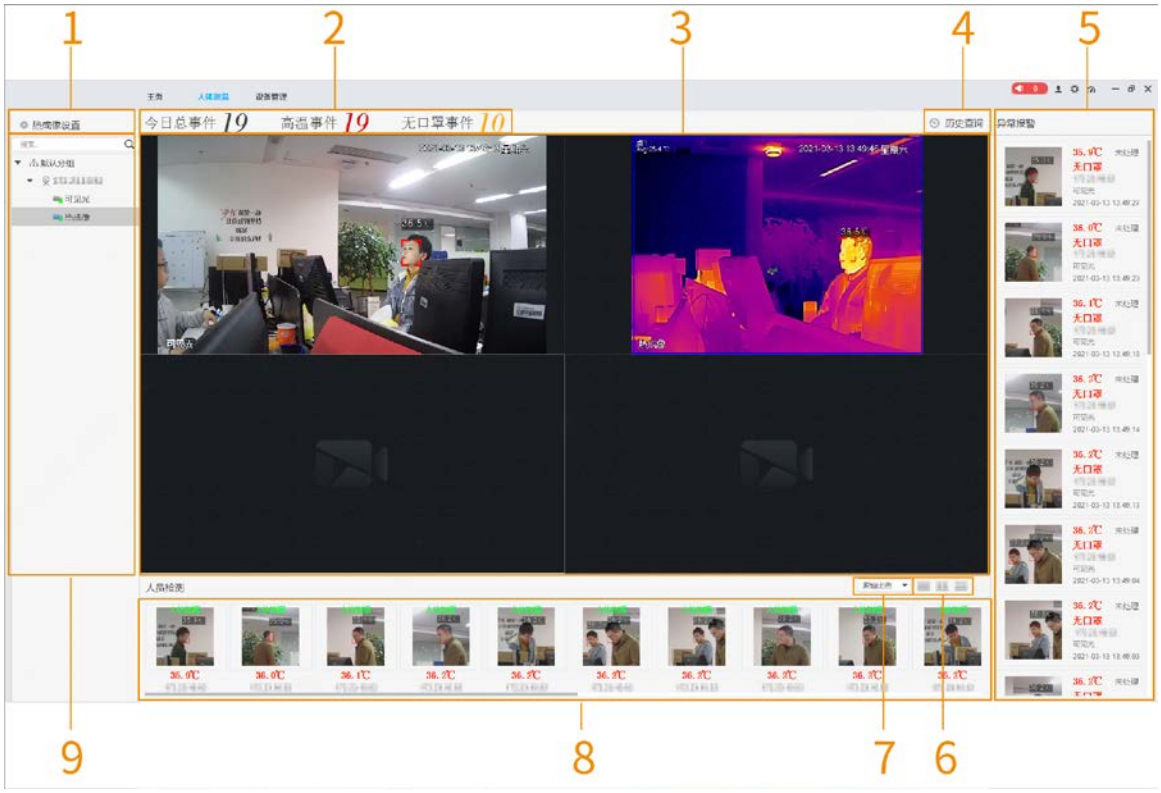


表3-1 界面参数

序号	参数	说明
1	热成像设置	配置热成像通道。详细介绍请参见“第 5 章 热成像设置”。
2	事件数	显示今日触发事件总数及高温、无口罩事件数量。
3	预览画面	双击设备树中的设备，或拖动设备至预览窗口，打开对应通道的预览画面。
4	历史记录	单击“历史记录”可跳转至测温记录界面。
5	异常报警	显示实时异常报警记录及处理情况。双击图片可查看详细信息或处理异常。
6	调整通道数	调整预览画面的通道数量。
7	画面比例	调整预览画面的比例。
8	人员检测情况	显示实时检测到的人体体温信息。
9	设备树	显示已添加设备的组织树信息。

第 4 章 预览界面操作

预览界面操作。

表4-1 预览操作

图标	图标含义	说明
	本地录像	单击该图标，系统开始录制当前视频窗口中的音视频；再次单击该图标，停止录像，存储到PC本地。默认保存在平台客户端安装路径“…/Data/User/Record”下。如需修改保存路径，在界面右上角选择“ > 系统配置 > 文件路径 > 录像路径”，设置修改后的保存路径。
	抓图	将当前视频窗口中的图像以图片形式保存在PC本地（一次保存一张），默认保存在平台安装路径“…/Data/User/Picture/Capture”下。如需修改保存路径，在界面右上角选择“ > 系统配置 > 文件路径 > 事件图片路径”，设置修改后的保存路径。
	音频	打开或关闭摄像机的音频。
	对讲	打开或关闭相应摄像机的对讲功能。
	框选放大	框选局部放大，放大后支持滚动鼠标滚轮缩放。
	关闭	单击该图标，关闭该视频。

第 5 章 热成像设置

配置测温报警、热成像设备、智能检测通道等。

前提条件

已添加设备到平台。详细介绍请参见平台配套的使用说明书。

操作步骤

步骤1　选择“人体测温”进入人体测温界面。

步骤2　选择需要设置的设备，单击“热成像设置”。

步骤3　单击“人体测温”，配置人体测温参数。

图5-1 人体测温

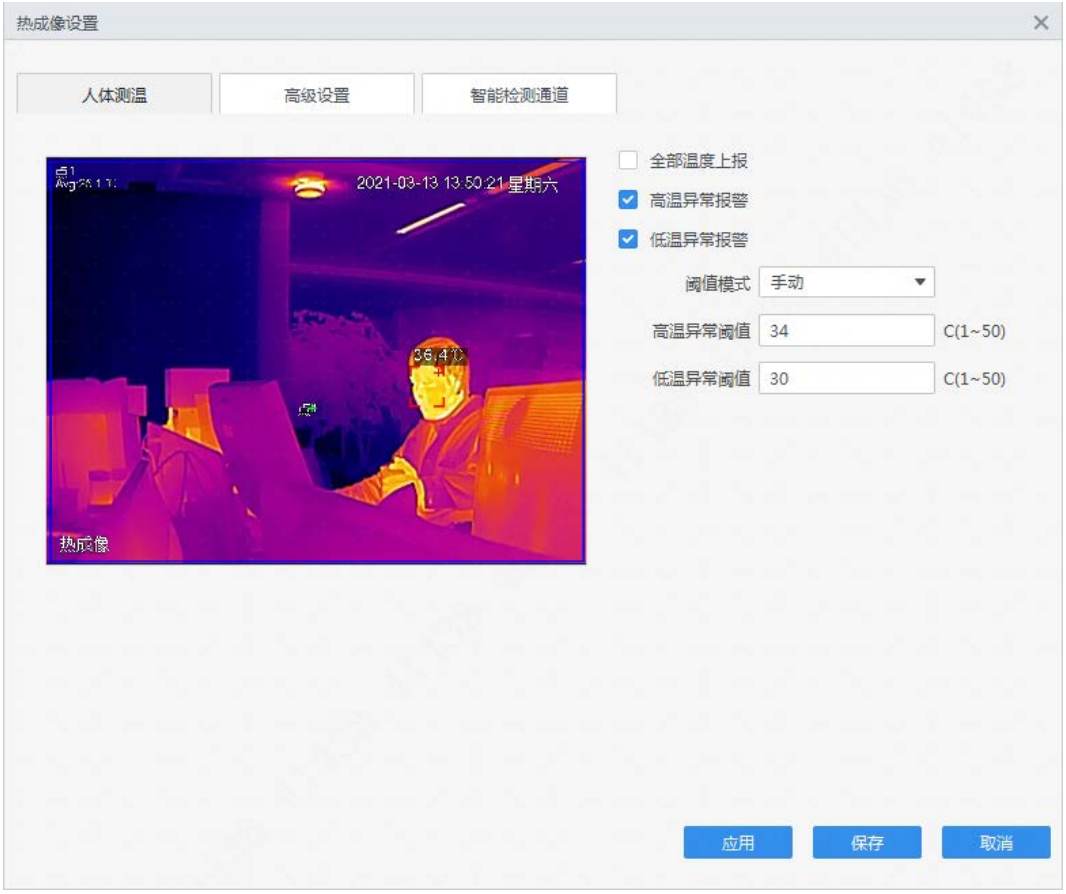


表5-1 人体测温参数

参数	说明
全部温度上报	当检测到人体温度时立即上报到平台。
高温异常上报	当检测到高温异常时上报事件到平台，并作为异常报警事件。
低温异常上报	当检测到低温异常时上报事件到平台。
阈值模式	● 手动：手动输入高温或低温异常阈值。 ● 自动：以人体标准温度判断是否高温。

参数	说明
高温异常阈值	将高于该温度值的人体测温判定为高温异常。
低温异常阈值	将低于该温度值的人体测温判定为低温异常。

步骤4　配置高级设置。

为了使检测到的人体体温更加精准，需要根据实际情况调整黑体设备参数及相机参数。

1. 单击“高级设置”，输入密码检验，单击“确定”。

说明

具体密码请联系客服或售后获取。

2. 选择启用，配置黑体设备及相机参数。

图5-2 高级设置

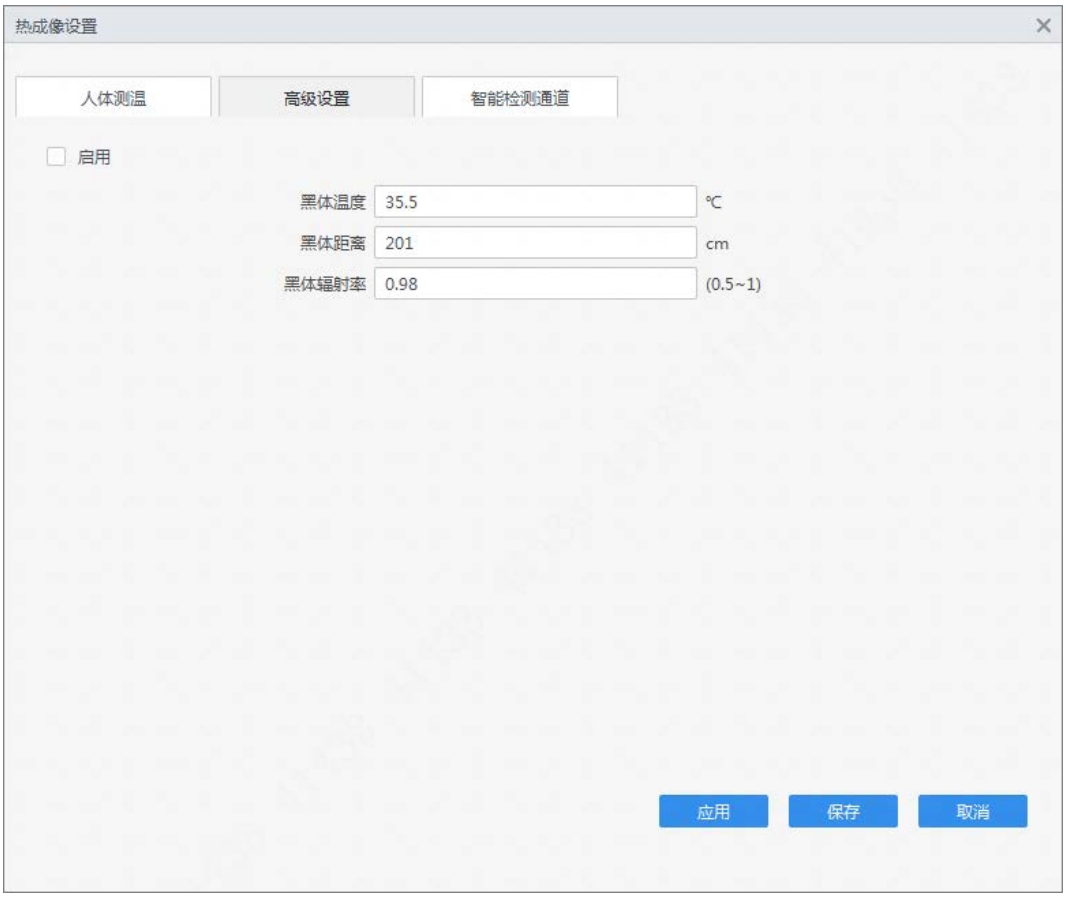


表5-2 高级设置参数

参数	说明
黑体温度	黑体设备的温度。
黑体距离	黑体设备中心点与热相机镜头中心点距离。
修正温度	需要修正的普遍性存在温差的温度。
黑体高度	黑体设备中心点距离地面高度。
黑体辐射率	默认为0.97。
相机高度	热成像相机镜头中心点距离地面高度。

参数	说明
相机俯视角	热成像相机与水平面的夹角。

步骤5　单击“智能检测通道”，配置智能检测通道。

- 可见光：将可见光通道设置为智能检测通道，并设置抓拍角度过滤值。
- 热成像：将热成像通道设置为智能检测通道。
- 按时间切换：按设置时间切换可见光通道或热成像通道。

图5-3 智能检测通道

步骤6　单击“应用”，立刻将配置应用到该设备。

步骤7　单击“保存”。

第 6 章 处理异常报警

平台检测到人体体温异常时产生异常报警，用户根据实际情况处理异常报警列表中的测温报警。

前提条件

已设置相应的人体测温图片和视频保存模式。在“⚙ > 系统配置 > 数据管理”设置“人体测温保存图片和视频模式”。

操作步骤

步骤1 选择“人体测温”进入人体测温预览界面。

步骤2 双击选择未处理的异常报警，单击可见光图片、热成像图片或视频查看异常报警详情。

说明

查看视频时，单击⬇，下载报警录像到本地。

图6-1 异常报警详情

步骤3 根据实际情况填写报警信息，单击“确定”。

说明

通过人证设备刷人员身份证可直接导入体温异常报警信息。

第 7 章 查询测温记录

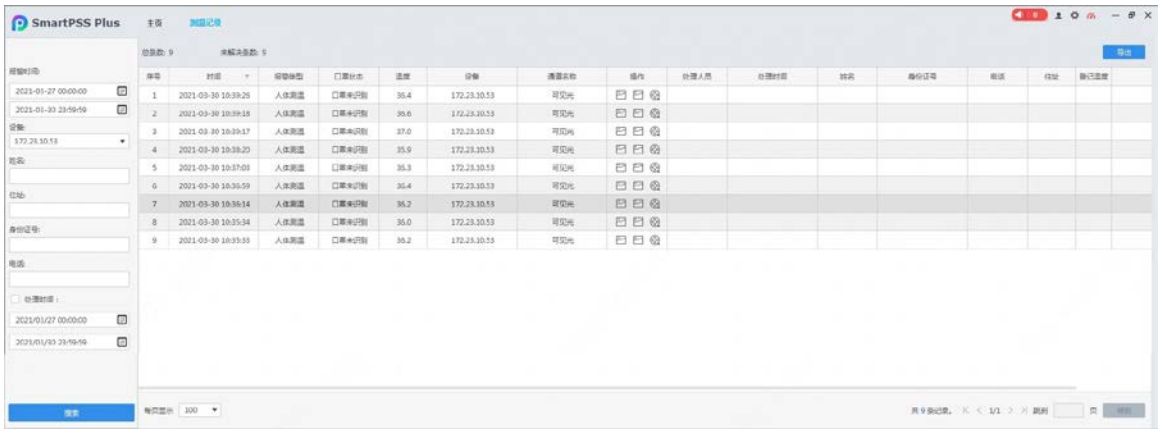
操作步骤

步骤1　选择“测温记录”。

步骤2　输入查询参数，单击“搜索”。

在右侧列表中可查看测温记录的详细信息。

图7-1 测温记录



相关操作

- 导出日志：单击“导出”，将当前列表保存至本地。
- 修改异常报警信息：双击记录，修改异常报警信息（可通过人证设备刷卡直接导入信息），单击“确定”。
- 查看抓图：单击操作列中的，查看该记录对应抓图。
- 查看视频：单击操作列中的，查看该记录对应录像回放。

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

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

关于本文档

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

附录2 网络安全建议

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，包括但不限于修改出厂默认密码并使用强密码、定期修改密码、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。

「 让社会更安全 让生活更智能 」

ENABLING A SAFER SOCIETY AND SMARTER LIVING