



SmartPSS Plus周界防护方案











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
V1.0.2	<ul style="list-style-type: none"> 更新周界防护章节。 新增入侵防护章节。 更新报警记录章节。 新增操作记录章节。 	2021.06
V1.0.1	新增报警录像功能。	2020.12
V1.0.0	首次发布	2020.11

目 录




前言	I
第 1 章 简介	1
第 2 章 打开周界防护方案	2
第 3 章 周界防护	3
第 4 章 入侵防护	10
第 5 章 周界记录	16
5.1 报警日志	16
5.2 操作日志	17
附录1 法律声明	18
附录2 网络安全建议	20


第 1 章 简介

SmartPSS Plus周界防护方案配套声光相机和报警主机，在导入的地图图片上部署设备，实时查看设备的在线、报警情况，单点、全局一键布撤防，通过查看报警抓图及录像处理报警事件，同时快速的查询和导出报警记录。

第 2 章 打开周界防护方案


不同场景打开周界防护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周界防护方案。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，但未选择周界防护方案，在界面右上角选择“ > 切换方案”，选择周界防护方案。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 周界防护

将添加的设备拖拽至导入的电子地图上部署，查看设备显示情况，支持将设备设置为布撤防、临时旁路、永久旁路等操作，同时处理发生的报警事件。

选择“主页 > 设备管理”，添加报警主机通道和声光相机到系统，详细介绍请参见SmartPSS Plus_使用说明书。在界面右上角选择“ > 帮助手册”，获取SmartPSS Plus使用说明书。

步骤1 打开周界防护方案。

步骤2 在主页单击“周界防护”页签。

步骤3 单击“添加地图”，填写地图名，单击，选择地图图片，图片大小不能超过10M。
页面展示地图区域。

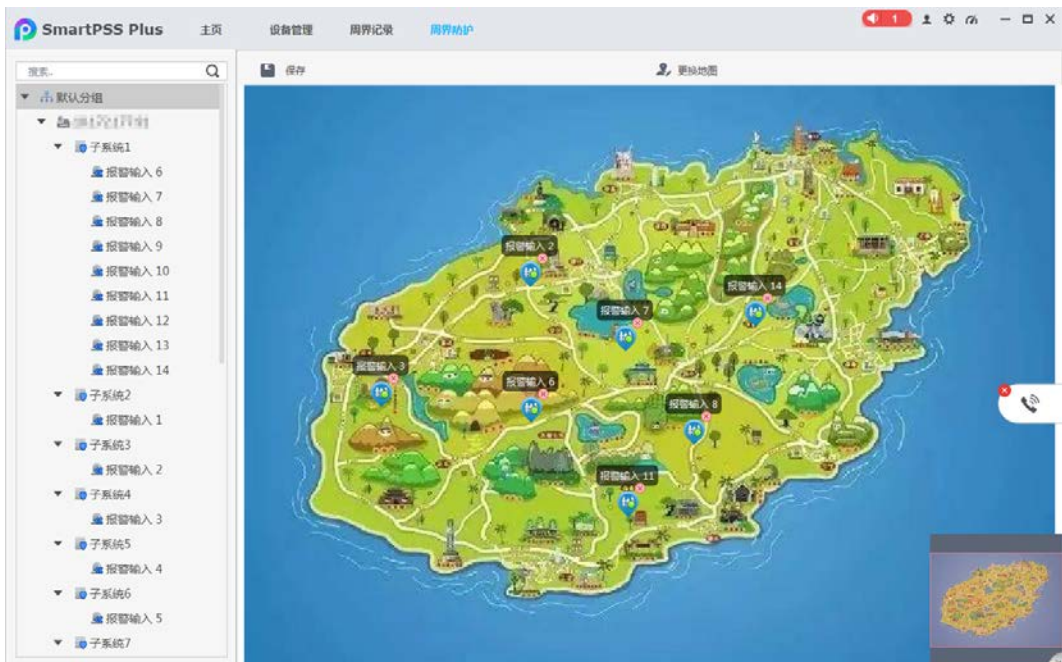
- 单击“保存”，保存配置。
- 单击“更换地图”，修改导入的地图名或导入新的地图。
- 单击“编辑”，返回部署设备界面。



说明

界面右下角红色区域显示地图图片放大/缩小后的局部图，滚动鼠标滚轮可放大/缩小地图图片。

图3-1 导入地图



步骤4 单击，展开设备列表。



说明

设备列表支持显示设备、子系统、虚拟子系统（有不属于任何子系统的防区时才存在）及子系统所属防区。

- 右键单击IP设备，可对设备层级设置布防、撤防、警号开关及报警输出开关，同时也可以查看设备状态。

图3-2 设置设备层级



表3-1 设置设备层级参数

参数	描述
布防	布防整个报警主机及内部防区（虚拟子系统除外）。
撤防	撤防整个报警主机及内部防区（虚拟子系统除外）。
警号开关	获取警号状态，控制警号开关。
报警输出控制	获取报警输出状态，控制报警输出开关。
查询报警主机状态	点击查看报警主机状态。

- 右键单击需要重命名的子系统，选择“修改子系统名称”，可对子系统重命名。

图3-3 修改子系统名称



说明

- ◇ 虚拟子系统不支持重命名。
- ◇ 子系统要处于撤防未报警的状态才能重命名。
- 右键单击需要重命名的防区，选择“修改通道名称”，可对防区重命名。

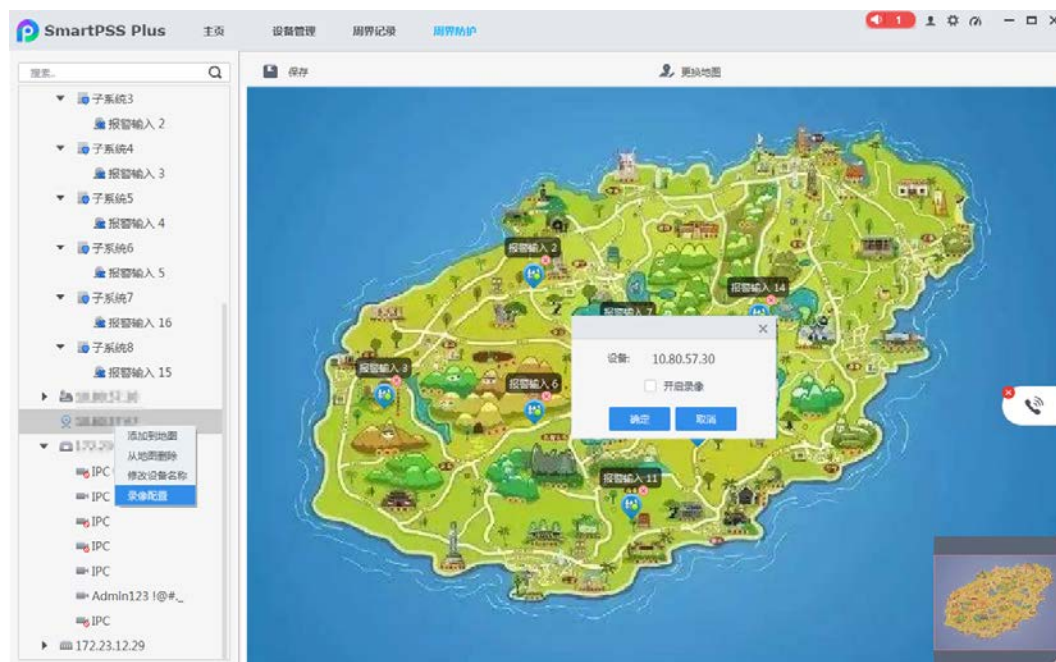
图3-4 修改防区名称



步骤5 根据施工现场安装点位将设备拖拽至电子地图相应位置。

- 开启声光相机的报警录像功能。
 1. 右键单击声光相机设备名称选择“录像配置”。
 2. 选择“开启录像”。
 3. 单击“确定”。

图3-5 声光相机的录像配置

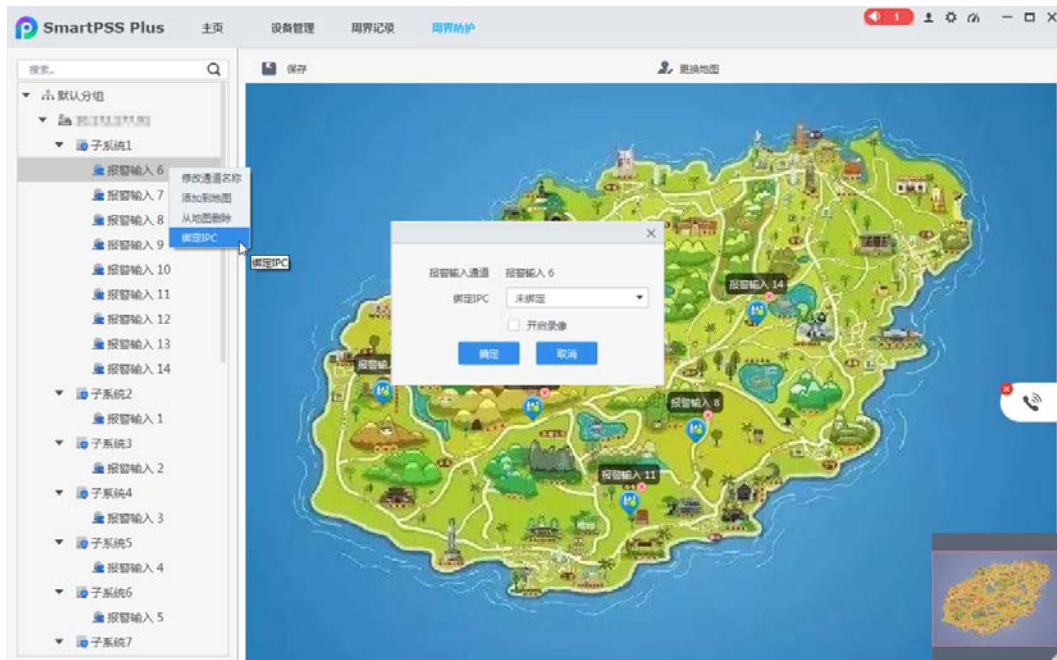


- 开启报警主机的报警录像功能。
 1. 右键单击已添加到地图的报警输入通道，选择“绑定IPC”。
 2. 选择需绑定IPC的设备名称或NVR的前端通道。
 3. 选择“开启录像”。
 4. 单击“确定”。

说明

由于报警主机不带视频功能，如需保存报警抓图和录像，报警主机需和前端设备配套使用，将报警主机通道和IPC绑定。

图3-6 报警主机的录像配置



步骤6 所有相机点位在地图上部署完成后，单击“保存”。
已完成周界防护配置，开始进入运维视图。

图3-7 查看部署设备

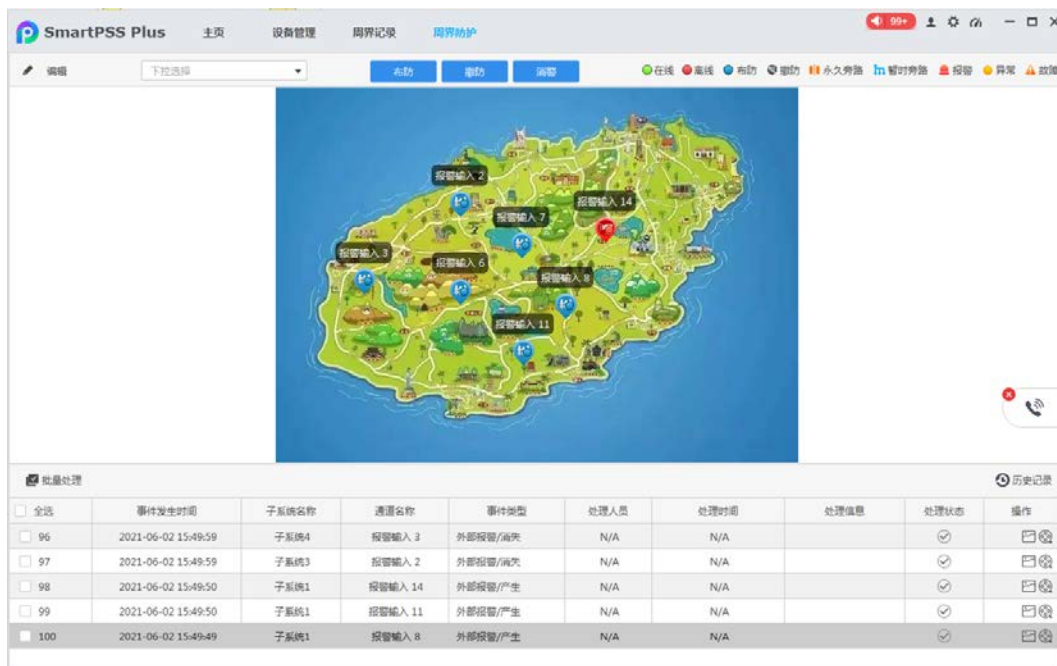



表3-2 状态显示

状态	说明
在线	设备正常使用。


状态	说明
离线	设备不在线。
布防	布防区域内的单台设备。
撤防	撤防区域内的单台设备。
永久旁路	该防区被停用，在设备撤防后再布防时，该永久旁路的防区仍为停用。
暂时旁路	该防区在此次布防时被屏蔽，当设备撤防时，防区将恢复为非旁路状态。
报警	防区发生报警事件，并伴随报警音。
异常	防区出现异常情况。  说明 报警主机通道在撤防下触发报警，也显示为异常。
故障	防区设备故障。

步骤7 在下拉框中选择需要查询的设备。



说明

下拉框支持全部、虚拟子系统、子系统筛选。

步骤8 当发生报警事件时，界面弹出报警提示框。，显示报警个数，单击可查看报警事件详情，详细介绍请参见SmartPSS Plus_使用说明书。

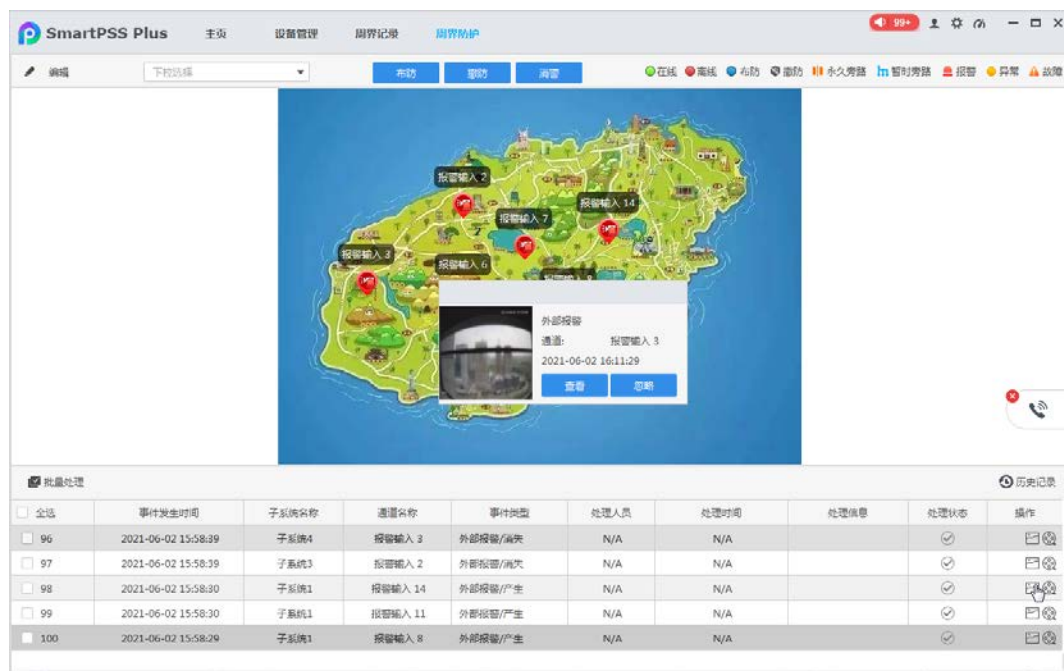
- 单击“查看”，处理报警事件。
- 单击“忽略”，忽略本次报警事件。



说明

绑定设备后，自动配置报警事件，报警音默认关闭，如需开启，请前往“事件配置”界面配置。

图3-8 发生报警事件





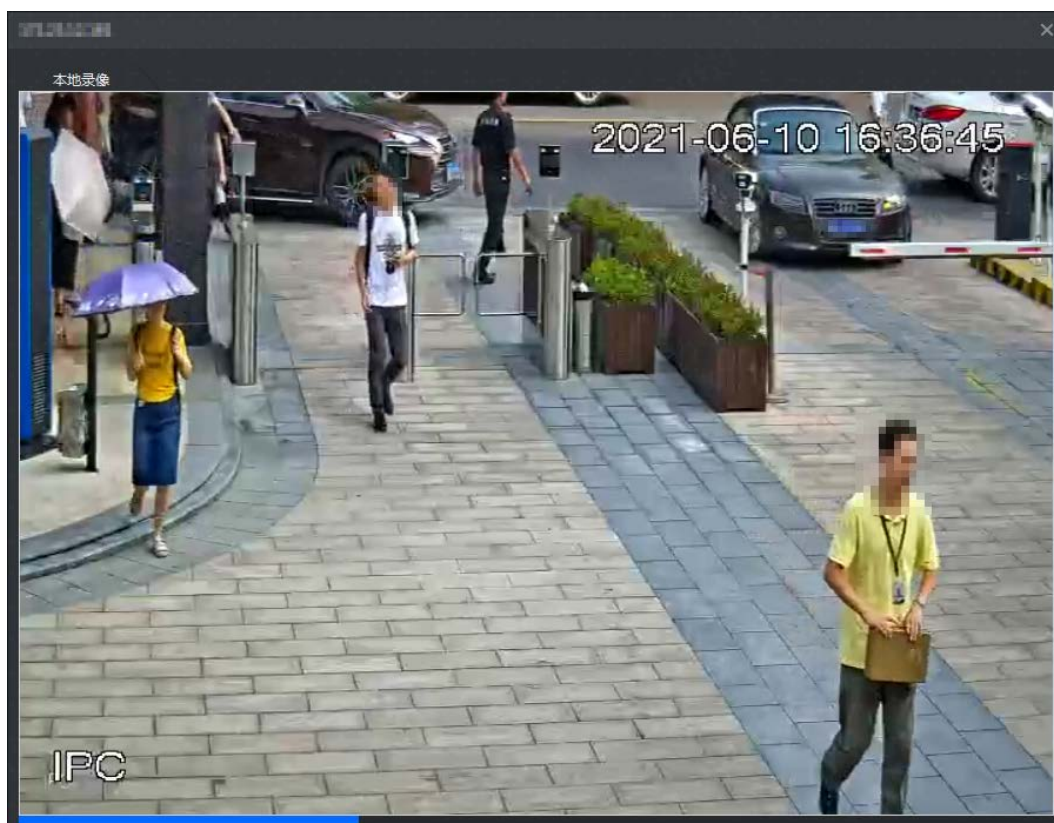

- 单击, 查看报警抓图。
- 单击, 查看报警录像, 填写备注信息, 单击“确定”。


图3-9 查看报警录像



说明

支持查看发生报警时的前5秒和后15秒的视频录像。

步骤9 单击报警事件处理状态的, 处理报警事件信息。

表示已处理。

步骤10 若配置单个子系统, 单击需要配置的子系统, 可对单个子系统进行“在家布防”、“外出布防”、“撤防”、“消警”操作; 若需要配置全部子系统, 单击“布防”、“撤防”或“消警”, 对一键对地图中所有防区和通道生效。

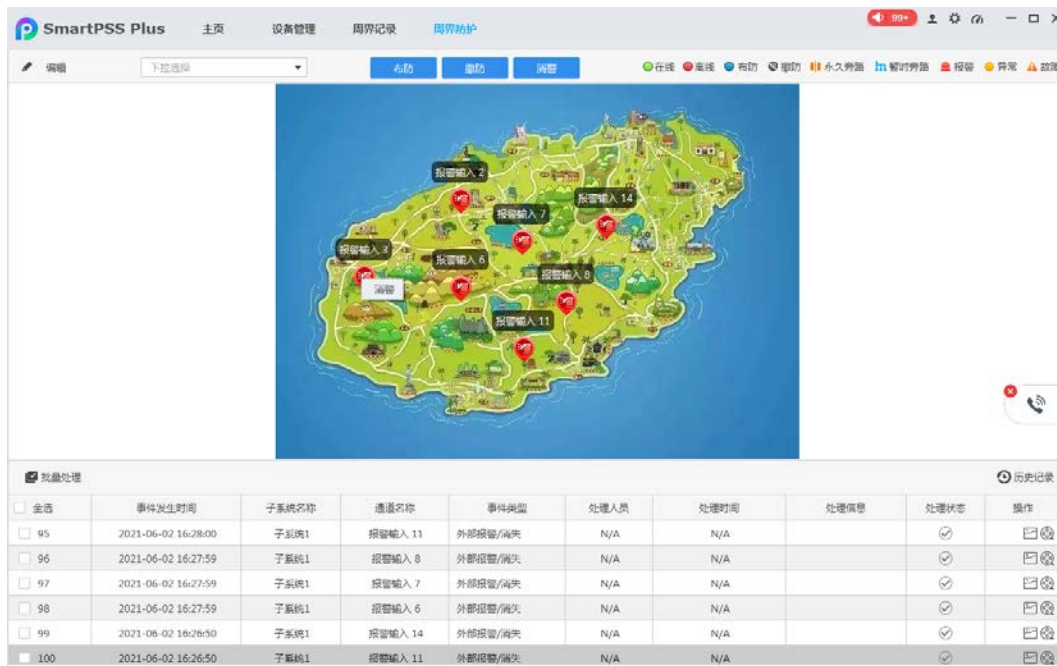


说明

虚拟子系统和二代报警主机子系统没有外出布防和在家布防功能。


步骤11 当发生报警事件时, 右键单击显示报警的设备的“消警”, 设备取消报警, 恢复正常布防状态。

图3-10 消警



第 4 章 入侵防护

用于列表展示子系统防区状态，进行布防撤防，处理报警等。

选择“主页 > 设备管理”，添加报警主机通道和声光相机到系统，详细介绍请参见SmartPSS Plus_使用说明书。在界面右上角选择“ > 帮助手册”，获取SmartPSS Plus使用说明书。

步骤1 打开周界防护方案。

步骤2 在主页单击“入侵防护”页签。

步骤3 在设备列表中选择需要查看的报警主机设备。



说明

设备列表支持显示设备、子系统、虚拟子系统（有不属于任何子系统的防区时才存在）及子系统所属防区。

- 右键单击设备，可对设备层级设置布防、撤防、警号开关及报警输出开关，同时也可查看设备状态。

图4-1 设置设备层级



表4-1 设备层级参数

参数	描述
布防	布防整个报警主机及内部防区（虚拟子系统除外）。
撤防	撤防整个报警主机及内部防区（虚拟子系统除外）。
警号开关	获取警号状态，控制警号开关。
报警输出控制	获取报警输出状态，控制报警输出开关。
查询报警主机状态	点击查看报警主机状态。

- 右键单击需要重命名的子系统，选择“修改子系统名称”，可对子系统重命名。

图4-2 修改子系统名称

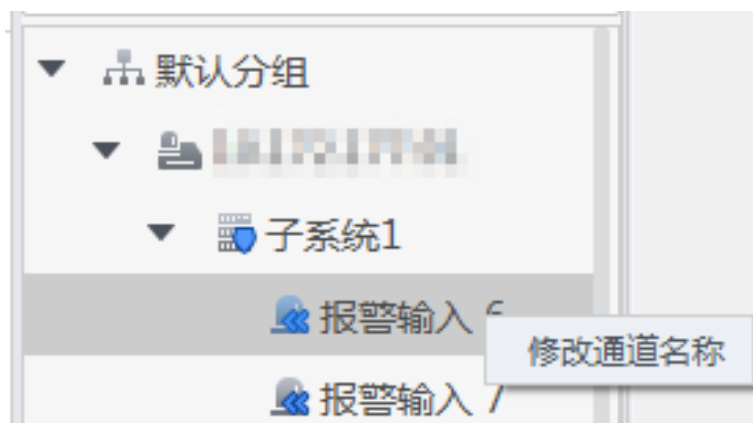


说明

虚拟子系统不支持重命名。

- 右键单击需要重命名的防区，选择“修改通道名称”，可对防区重命名。

图4-3 修改防区名称



- 在设备列表中，可查看子系统是否存在防区及防区状态。
 - ◇ 表示该子系统存在防区。
 - ◇ 表示该子系统不存在防区。

说明

子系统默认按照有防区-无防区排序显示。

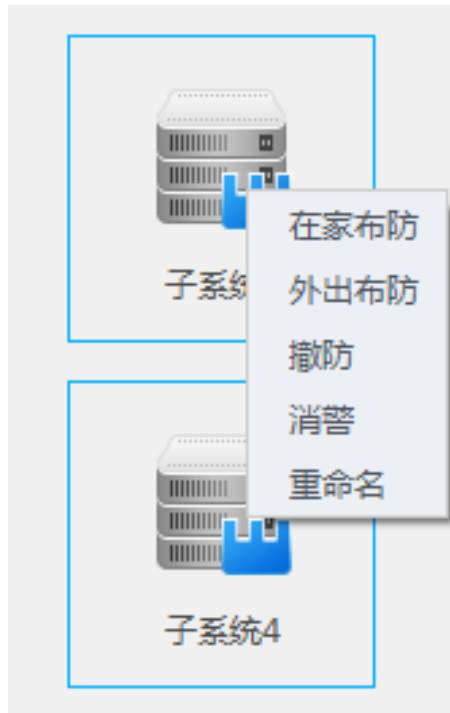
步骤4 配置子系统。

图4-4 子系统界面



- 若要配置单个子系统，单击需要配置的子系统，右键选择需要进行的操作。

图4-5 单个子系统配置





- 若要配置多个子系统，单击所有需要配置的子系统，或单击“全选”。
单击上方“外出布防”、“在家布防”、“撤防”或“消警”，一键操作所选择的子系统。

表4-2 配置参数

参数	说明
在家布防	将房屋周围的防区加入在家布防模式中，回家时，开启在家布防。
外出布防	将所有防区都加入外出布防模式中，外出时，开启外出布防。外出布防时有退出时间和进入延时。
撤防	撤出所有子系统和防区的防护。
消警	消除所有子系统及防区的警报。



说明

- 在子系统界面中，可查看子系统是否存在防区及防区状态。
 - ◇  表示该子系统存在防区。
 - ◇  表示该子系统不存在防区。
- 子系统默认按照有防区-无防区排序显示。

步骤5 配置防区。

图4-6 防区界面

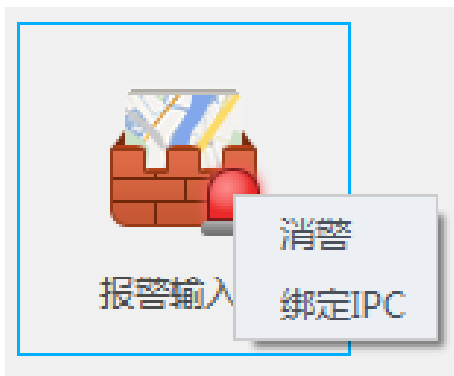


- 若要配置单个防区，单击需要配置的防区，右键选择需要进行的操作。

图4-7 撤防状态防区配置



图4-8 报警状态防区配置




- 若要配置多个防区，单击所有需要配置的防区，或单击“全选”。
单击上方“布防”、“撤防”或“消警”，一键操作所选择的防区。

表4-3 配置参数

参数	说明
布防	布防整个防区的防护。
撤防	撤出所有防区的防护。
消警	消除所有防区的警报。
永久旁路	该防区被停用，在设备撤防后再布防时，该永久旁路的防区仍为停用。
暂时旁路	该防区在此次布防时被屏蔽，当设备撤防时，防区将恢复为非旁路状态。
绑定IPC	详情请参见“第 3 章 周界防护”
视频预览	预览当前绑定的前端画面。

- 在防区界面中，可查看防区状态。

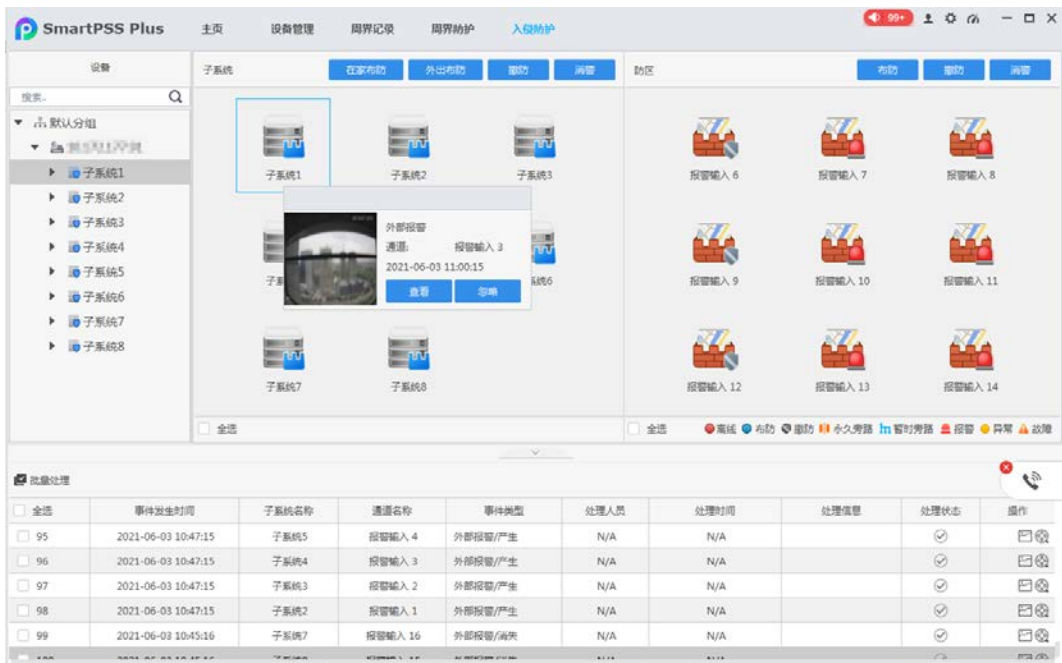
表4-4 状态显示

状态	说明
离线	设备不在线。
布防	防区为已布防状态。
撤防	防区为已撤防状态。
永久旁路	该防区被停用，在设备撤防后再布防时，该永久旁路的防区仍为停用。
暂时旁路	该防区在此次布防时被屏蔽，当设备撤防时，防区将恢复为非旁路状态。
报警	防区发生报警事件，并伴随报警音。
异常	防区出现异常情况。  说明 报警主机通道在撤防下触发报警，也显示为异常。
故障	防区设备故障。

步骤6 当发生报警事件时，界面弹出报警提示框。

- 单击“查看”，处理报警事件。
- 单击“忽略”，忽略本次报警事件。

图4-9 发生报警事件





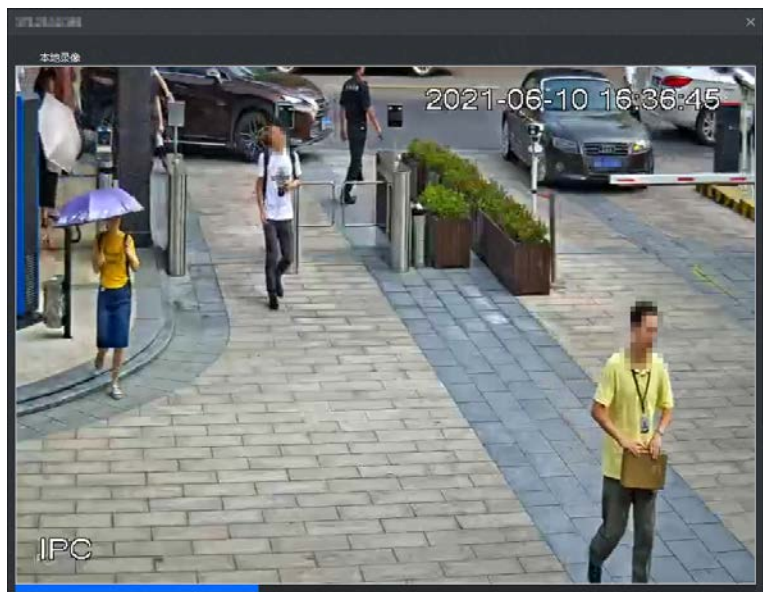

- 单击, 查看报警抓图。
- 单击, 查看报警录像。


图4-10 查看报警录像



说明

支持查看发生报警时的前5秒和后15秒的视频录像。

步骤7 单击报警事件处理状态的, 处理报警事件信息。

表示已处理。

第 5 章 周界记录

用于查看周界报警及操作记录，显示报警详情、操作详情、处理信息、导出报表等。

5.1 报警日志

查看发生报警事件时的记录，支持导出报警事件记录。

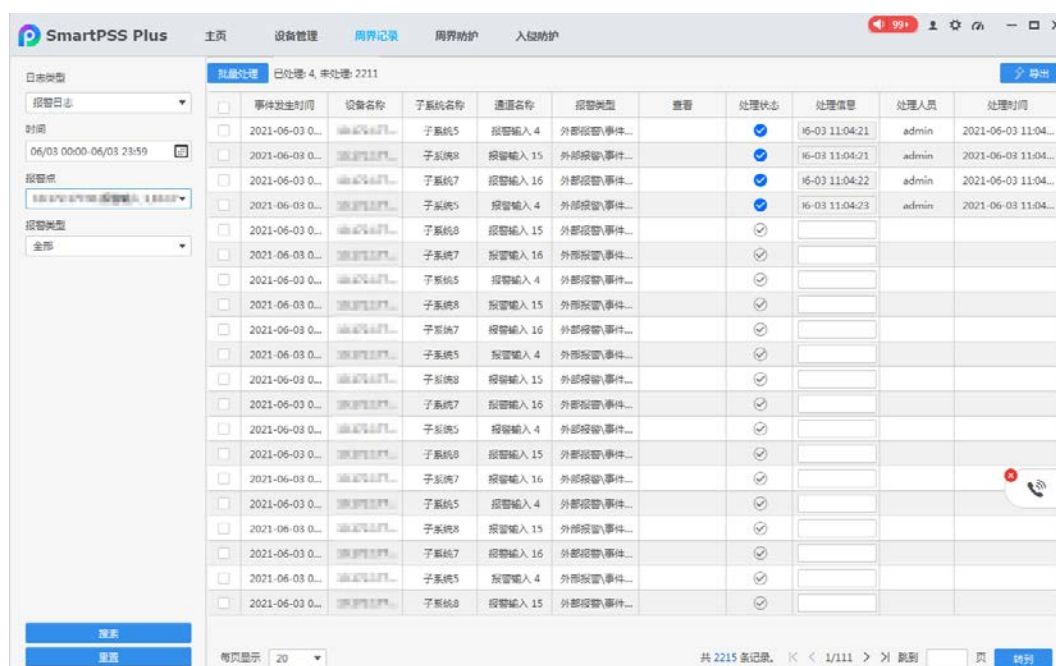
前提条件

确保系统内添加的报警主机和声光相机发生过报警事件。

操作步骤

- 步骤1 打开周界防护方案。
- 步骤2 单击“周界记录”，在“日志类型”中选择“报警日志”。
- 步骤3 在界面左侧选择“报警点”、“报警类型”，设置报警时间段。
- 步骤4 单击“搜索”。
- 单击“重置”，重置筛选条件。



图5-1 查询报警日志



事件发生时间	设备名称	子系统名称	通道名称	报警类型	查看	处理状态	处理信息	处理人员	处理时间
2021-06-03 0...	...	子系统5	报警输入 4	外部报警事件...		✓	16-03 11:04:21	admin	2021-06-03 11:04...
2021-06-03 0...	...	子系统8	报警输入 15	外部报警事件...		✓	16-03 11:04:21	admin	2021-06-03 11:04...
2021-06-03 0...	...	子系统7	报警输入 16	外部报警事件...		✓	16-03 11:04:22	admin	2021-06-03 11:04...
2021-06-03 0...	...	子系统5	报警输入 4	外部报警事件...		✓	16-03 11:04:23	admin	2021-06-03 11:04...
2021-06-03 0...	...	子系统8	报警输入 15	外部报警事件...		✓			
2021-06-03 0...	...	子系统7	报警输入 16	外部报警事件...		✓			
2021-06-03 0...	...	子系统5	报警输入 4	外部报警事件...		✓			
2021-06-03 0...	...	子系统8	报警输入 15	外部报警事件...		✓			
2021-06-03 0...	...	子系统7	报警输入 16	外部报警事件...		✓			
2021-06-03 0...	...	子系统5	报警输入 4	外部报警事件...		✓			
2021-06-03 0...	...	子系统8	报警输入 15	外部报警事件...		✓			
2021-06-03 0...	...	子系统7	报警输入 16	外部报警事件...		✓			
2021-06-03 0...	...	子系统5	报警输入 4	外部报警事件...		✓			
2021-06-03 0...	...	子系统8	报警输入 15	外部报警事件...		✓			
2021-06-03 0...	...	子系统7	报警输入 16	外部报警事件...		✓			
2021-06-03 0...	...	子系统5	报警输入 4	外部报警事件...		✓			
2021-06-03 0...	...	子系统8	报警输入 15	外部报警事件...		✓			
2021-06-03 0...	...	子系统7	报警输入 16	外部报警事件...		✓			
2021-06-03 0...	...	子系统5	报警输入 4	外部报警事件...		✓			
2021-06-03 0...	...	子系统8	报警输入 15	外部报警事件...		✓			
2021-06-03 0...	...	子系统7	报警输入 16	外部报警事件...		✓			
2021-06-03 0...	...	子系统5	报警输入 4	外部报警事件...		✓			
2021-06-03 0...	...	子系统8	报警输入 15	外部报警事件...		✓			

相关操作

- 导出报警记录。
 1. 导出指定报警记录：在报警记录界面选择需要导出的记录，单击“导出”，导出选择的报警记录到本地。
 2. 导出全部报警记录：不选择任何一条数据的情况下，直接单击“导出”，导出所有的报警记录到本地。
- 单击“批量处理”，批量处理报警事件信息。

- 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。
- ，查看首页/尾页。
- 在 跳到 页，输入页数，单击“跳到”，跳至相应页数。

5.2 操作日志

查看发生事件时的操作记录，支持导出操作日志记录。

操作步骤



- 步骤1 打开周界防护方案。
 - 步骤2 单击“周界记录”，在“日志类型”中选择“操作日志”。
 - 步骤3 在界面左侧设置时间段。
 - 步骤4 单击“搜索”。
- 单击“重置”，重置筛选条件。

图5-2 查询操作日志



<input type="checkbox"/>	时间	操作类型	设备名称	子系统名称	通信名称	操作人
<input type="checkbox"/>	2021-06-03 10:06:44	防区消警	防区117.11	子系统1	报警输入 9	admin
<input type="checkbox"/>	2021-06-03 10:06:44	防区消警	防区117.11	子系统1	报警输入 10	admin
<input type="checkbox"/>	2021-06-03 10:06:44	防区消警	防区117.11	子系统1	报警输入 11	admin
<input type="checkbox"/>	2021-06-03 10:06:44	防区消警	防区117.11	子系统1	报警输入 12	admin
<input type="checkbox"/>	2021-06-03 10:06:44	防区消警	防区117.11	子系统1	报警输入 13	admin
<input type="checkbox"/>	2021-06-03 10:06:44	防区消警	防区117.11	子系统1	报警输入 14	admin
<input type="checkbox"/>	2021-06-03 10:06:56	在家布防	防区117.11	子系统1		admin
<input type="checkbox"/>	2021-06-03 10:06:56	在家布防	防区117.11	子系统2		admin
<input type="checkbox"/>	2021-06-03 10:06:56	在家布防	防区117.11	子系统3		admin
<input type="checkbox"/>	2021-06-03 10:06:56	在家布防	防区117.11	子系统4		admin
<input type="checkbox"/>	2021-06-03 10:06:56	在家布防	防区117.11	子系统5		admin
<input type="checkbox"/>	2021-06-03 10:06:56	在家布防	防区117.11	子系统6		admin
<input type="checkbox"/>	2021-06-03 10:06:56	在家布防	防区117.11	子系统7		admin
<input type="checkbox"/>	2021-06-03 10:06:56	在家布防	防区117.11	子系统8		admin
<input type="checkbox"/>	2021-06-03 10:26:34	子系统消防	防区117.11	子系统1		admin
<input type="checkbox"/>	2021-06-03 10:26:43	防区消警	防区117.11	子系统1	报警输入 12	admin
<input type="checkbox"/>	2021-06-03 10:26:45	防区消警	防区117.11	子系统1	报警输入 9	admin
<input type="checkbox"/>	2021-06-03 10:26:46	防区消警	防区117.11	子系统1	报警输入 6	admin
<input type="checkbox"/>	2021-06-03 10:46:25	暂时旁路	防区117.11	子系统1	报警输入 6	admin
<input type="checkbox"/>	2021-06-03 10:46:28	暂时旁路	防区117.11	子系统1	报警输入 6	admin

相关操作

- 导出操作记录。
 1. 导出指定操作记录：在操作记录界面选择需要导出的记录，单击“导出”，导出选择的操作记录到本地。
 2. 导出全部操作记录：不选择任何一条数据的情况下，直接单击“导出”，导出所有的操作记录到本地。
- 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。
- ，查看首页/尾页。
- 在 跳到 页，输入页数，单击“跳到”，跳至相应页数。

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、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