



SmartPSS Plus











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
V1.0.6	<ul style="list-style-type: none"> 更新事件配置功能、事件中心、日志查询功能。 新增隐私协议。 	2021.06
V1.0.5	新增设备配置功能，事件中心。	2021.03
V1.0.4	新增选择应用场景。	2020.12
V1.0.3	新增方案，更新UI界面。	2020.11
V1.0.2	更新SmartPSS Plus智慧安防综合管理平台登录步骤、自动提取设备考勤数据和清除平台本地数据描述，新增问题反馈功能说明。	2020.09
V1.0.1	更新产品简介、查询日志描述。	2020.06

版本号	修订内容	发布日期
V1.0.0	首次发布。	2020.05

目 录

前言	I
第 1 章 简介	1
第 2 章 获取和登录	2
2.1 获取平台客户端	2
2.2 登录平台	2
2.3 重置密码	5
第 3 章 界面介绍	7
第 4 章 系统配置	9
4.1 基础设置	9
4.2 监控配置	10
4.3 事件	11
4.4 设置文件保存路径	12
4.5 数据管理	13
4.6 备份还原	14
4.7 软件授权	14
第 5 章 用户管理	15
5.1 添加角色	15
5.2 添加用户	16
第 6 章 设备管理	18
6.1 添加设备	18
6.1.1 通过搜索添加设备	18
6.1.2 手动添加设备	20
6.1.3 通过导入添加设备	21
6.2 配置设备	21
6.3 修改设备 IP 地址	25
6.4 初始化设备	26
第 7 章 配置设备事件	29
第 8 章 事件中心	33
8.1 配置预览视频	34
8.2 处理报警事件	35
8.2.1 操作步骤	35
8.2.2 特殊报警事件	37
8.2.2.1 触发报警	37
8.2.2.2 消除报警	37
第 9 章 日志查询	39
附录1 法律声明	40
附录2 网络安全建议	42

第 1 章 简介

SmartPSS Plus智慧安防综合管理平台（以下简称“平台”）与设备配套使用，旨在提供中小型场景下考勤、门禁控制、访客登记等业务的系统支持。

本文档主要介绍如何添加设备、修改设备IP地址、初始化设备等设备管理功能，以及如何查询系统和设备操作日志。关于方案对应的业务配置和业务使用，请参见各个方案的使用说明书。

第 2 章 获取和登录

2.1 获取平台客户端

设备上已预装平台客户端。若设备上未安装平台客户端，您可以联系技术支持人员获取安装包，根据提示安装平台客户端。您可以联系技术支持人员或通过大华工具管家获取平台客户端。在大华官网选择“服务支持 > 工具软件”可以下载到大华工具管家。大华官网

<https://www.dahuatech.com/>。

2.2 登录平台


步骤1 启动平台客户端。双击打开平台客户端。

- 如果已获取到平台客户端安装包，请双击安装包应用程序，然后根据提示安装并启动客户端。
- 如果通过大华工具管家获取平台客户端，请根据提示启动客户端。

步骤2 （可选）首次登录平台，需要选择对应的应用场景，单击“下一步”，平台会自动根据您的应用场景预勾选相应的方案，单击“确定”。您也可以选择“自定义场景”，单击下一步，选择实际使用中需要使用的方案，单击“确定”。



说明

如果首次使用平台时未选择需要的方案，但后续需要使用该方案，请在界面右上角选择“ > 切换方案”，选择需要使用的方案。


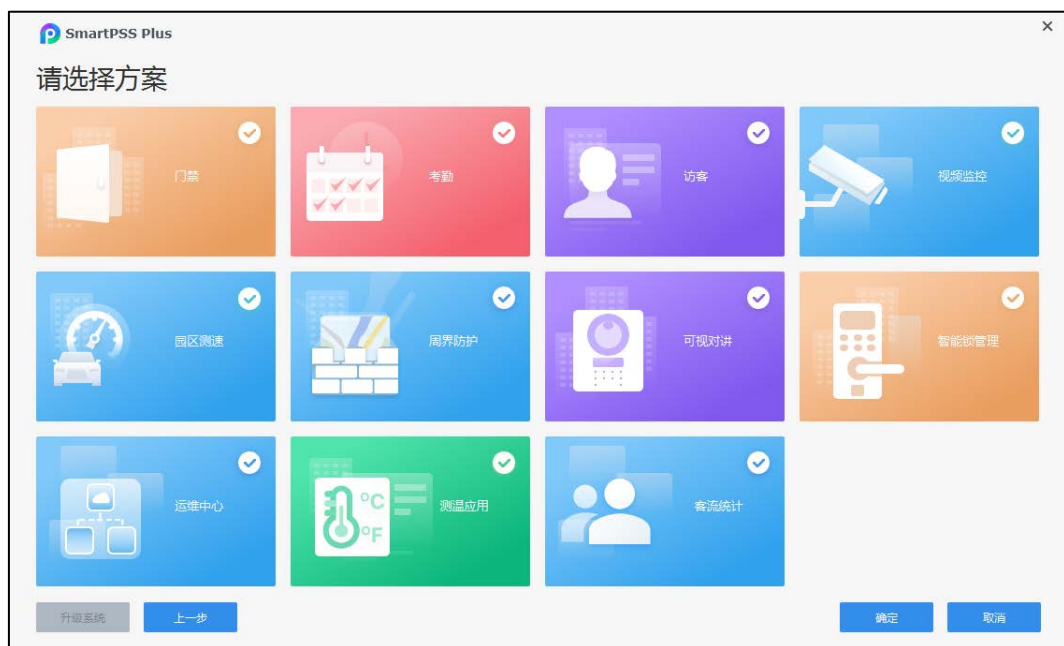
- 为下载最新的客户端安装包，请确保PC与外网互通。
- 如果首次使用平台时未选择需要的方案，但后续需要使用该方案，请在界面右上角选择“ > 切换方案”，选择需要使用的方案。

图2-1 选择应用场景



图2-2 加载方案



说明

单击“升级系统”可以将平台升级到最新版本。

- 步骤3 (可选) 首次登录平台，请阅读软件许可协议，单击“同意”。
- 步骤4 (可选) 首次登录平台，请阅读隐私协议，单击“同意”。
- 步骤5 (可选) 首次登录平台，请设置平台管理员admin的登录密码，单击“下一步”。

图2-3 设置admin的密码

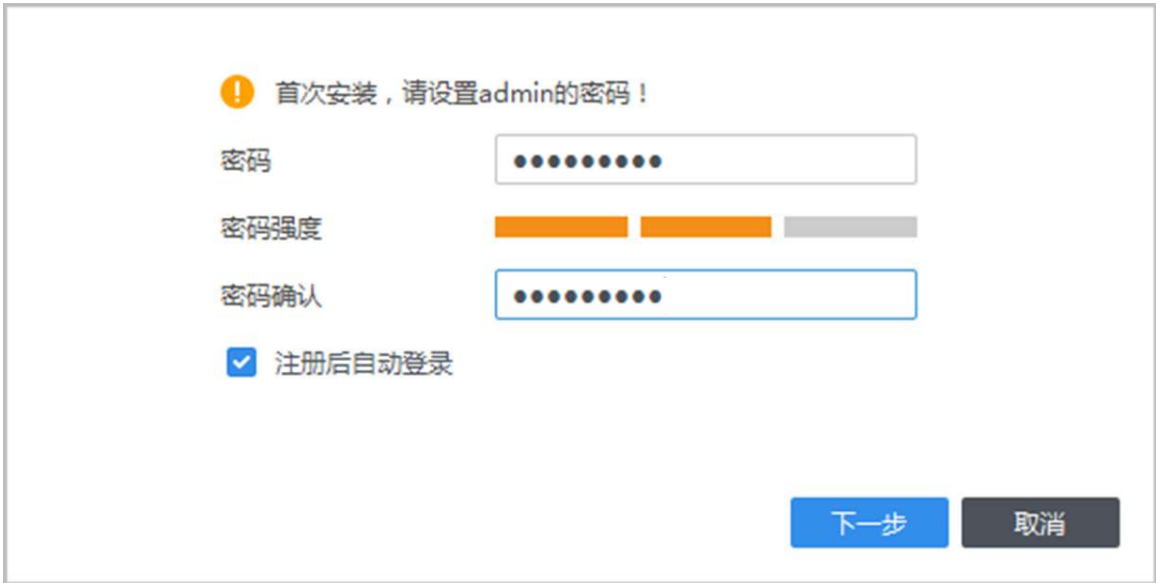


表2-1 初始化参数说明

参数	说明
密码	密码可设置为8位～32位字符，可以由大写字母、小写字母、数字、空格和特殊字符（除“!”、“@”、“;”、“:”、“&”外）组成，且至少包含2类字符。
密码强度	请根据密码强弱提示设置密码。
密码确认	再次输入密码。
注册后自动登录	选择后，注册完成后自动使用该账号登录平台；反之则显示登录界面。

步骤6 （可选）首次登录平台，请设置密保问题，单击“完成”。



注意

请牢记密保问题答案。重置密码时如果忘记密保问题答案，需要重新安装平台客户端。

图2-4 设置密码保护问题



- 步骤7 输入账号和密码，单击“登录”。
- 进入平台主界面。

图2-5 登录平台



表2-2 登录界面参数说明

参数	说明
记住密码	下次登录时无需再次输入用户名和密码。
自动登录	再次打开客户端时直接以此次的用户账号登录平台。
忘记密码	忘记密码时，单击“忘记密码？”进入重置密码界面。

- 步骤8 （可选）首次登录平台，根据提示选择是否加入用户体验计划。



说明

- 单击“查看隐私政策”，了解平台的隐私保护详情。
- 加入用户体验计划后，支持随时退出用户体验计划。在界面右上角选择“⚙️ > 系统配置 > 基础设置”，在“用户体验计划”栏取消选择“加入”，退出用户体验计划。

2.3 重置密码

忘记密码时，可以通过回答密保问题重新设置密码。

- 步骤1 打开平台客户端。
- 步骤2 单击“忘记密码?”。

图2-6 忘记密码





步骤3 回答密保问题，并根据界面提示重置密码。

第 3 章 界面介绍

图3-1 界面组成



表3-1 界面组成说明

编号	名称	说明
1	功能页签	默认显示“主页”页签。 打开某个功能后，此处会添加该功能页签。
2	报警图标	<ul style="list-style-type: none"> 单击  或 ，关闭或打开报警声音。 数字表示上报且当前未处理的报警事件数量。单击数字，打开事件中心查看报警事件详情。事件中心详细介绍请参见“第 8 章 事件中心”。
3	用户	<ul style="list-style-type: none"> 用户管理：添加普通用户，同时为admin和普通用户配置权限，详细介绍请参见“第 4 章 系统配置”。 锁屏：锁定平台界面。输入正确的登录密码即可解锁。 切换用户：返回登录界面，用其他账号重新登录系统。 帮助手册：获取帮助文档。 问题反馈：反馈使用平台过程中发现的问题或建议。 关于：查看平台版本和日期。

编号	名称	说明
4	系统配置	<ul style="list-style-type: none"> 切换方案：返回场景选择界面，选择其他方案。 系统配置：详细介绍请参见“第 4 章 系统配置”。
5	系统状态	查看平台系统占用的CPU和内存情况。如果CPU占用率过高该图标变为红色。
6	最小化按钮	最小化界面。
7	最大化按钮	最大化界面。
8	关闭按钮	退出平台。
9	方案中主要业务模块	进入业务模块配置和处理业务。
10	设备管理	用于添加设备到平台，以及远程配置设备、修改设备IP地址、初始化设备等。
	日志查询	用于查询和导出系统、设备的相关日志信息。
	事件配置	配置设备事件联动报警。
11	方案导航栏	显示所有已加载的方案。
12	展开导航栏图标	展开或收缩导航栏。

第 4 章 系统配置

用于设备校时、日志保存时间、报表日期和时间的显示格式等。

4.1 基础设置

为设备校时、设置日志保存时间、加入用户体验计划等。

步骤1 在界面右上角选择“ > 系统配置 > 基础设置”。

步骤2 配置系统参数。

图4-1 配置系统参数



基础设置

☒ 自动校时 每天 8:00 或 [立刻校时](#)

☒ 开机自动启动

语言 中文

日志保存时间 30 天 重启后生效

日期格式 yyyy/MM/dd

时间格式 24小时制

网络性能 高

皮肤 灰白 重启后生效

用户体验计划 ☒ 加入 ? 重启后生效




软件最小化时 ☐ 显示事件悬浮窗

软件启动时打开 主页

关闭提示 最小化到系统托盘区 ☐ 不再提醒

表4-1 配置系统参数说明

参数	说明
校时	<ul style="list-style-type: none"> 选择“自动校时”并设置时间，设备将在该时间点自动校时。 单击“立刻校时”，立即将所管理设备的时间设置为当前PC的时间。
开启自动启动	PC开机后，自动启动平台客户端。
语言	切换平台语言。重启平台客户端后生效。该功能为预留功能，暂不支持。
日志保存时间	保存最近时间内的日志。例如设置为30天，则保存最近30天的日志。
日期格式	设置报表日期的显示格式。

参数	说明
时间格式	设置报表时间的显示格式。
网络性能	默认为高，使用默认设置无需修改。
皮肤	设置界面背景颜色，默认为灰白色。
用户体验计划	选择“加入”，加入用户体验计划，否则退出用户体验计划。  说明 单击“加入”右侧的  ，查看隐私政策。
软件最小化时	选择“显示事件悬浮窗”，软件最小化后，显示  ，提示触发的报警事件数量。
软件启动时打开	设置软件启动时默认打开的功能页签。
关闭提示	关闭软件时，自动弹出提示弹窗；若不需要，选择“不再提醒”。

步骤3 单击“应用”。

4.2 监控配置

配置预览默认码流、即时回放录像时间、默认设备树等。

步骤1 在界面右上角选择“ > 系统配置 > 监控设置”。

步骤2 配置监控参数。

图4-2 监控配置

监控配置

默认预览码流

自适应码流

即时回放时间

5分钟

本地录像时间

30

分钟

默认设备树

组织树 (按设备)

重启后生效

解码类型

软解码

窗口上墙模式

☒ 覆盖

☐ 轮巡

☐ 默认主码流上墙

☐ 恢复上次预览视图

☒ 显示智能规则

☐ 保存设备树勾选状态

表4-2 监控配置参数说明


参数	说明
默认预览码流	配置实时预览默认码流。
即时回放时间	设置即时回放时长。例如设置30s，则回放前面30s的视频录像。

参数	说明
本地录像时间	设置录像时间。例如设置为30分钟，则系统录像30分钟，然后自动将录像保存到PC本地默认路径，默认路径为平台客户端安装路径的“\Data\User\Record”。
默认设备树	设置设备树默认类型。 <ul style="list-style-type: none"> ● 组织树（按设备）：以设备作为节点展示。 ● 区域树（按通道）：以通道作为节点展示。
解码类型	<ul style="list-style-type: none"> ● 软解码：通过CPU完成视频解码。 ● 硬解码：通过显卡完成视频解码。
窗口上墙模式	视频监控方案中，窗口画面对应的通道上墙方式有以下两种。 <ul style="list-style-type: none"> ● 覆盖：窗口仅能绑定一个通道或设备，重新绑定通道或设备将覆盖之前的画面。 ● 轮巡：窗口支持添加多个通道或设备，添加的通道依次排列在当前通道之后，通过设置通道画面停留时间及顺序配置窗口轮巡。
默认主码流上墙	视频监控方案中，通道画面上墙时，默认主码流视频上墙。
恢复上次预览视图	重新启动平台客户端，自动打开本次预览的实时视频。
显示智能规则	选择后，在监控画面显示智能规则信息。
保存设备树勾选状态	预留，暂不支持。

步骤3 单击“应用”。

4.3 事件

配置触发事件后联动报警的报警声音、联动发送邮件相关的发件人和收件人等。

步骤1 在界面右上角选择“ > 系统配置 > 事件”。



步骤2 配置事件。

图4-3 配置事件

☒ 循环播放

☐ 全局声音

 外部报警 ▼

 音频文件路径  

☒ SMTP (邮件)

 SMTP服务器

 端口

 用户名

 密码

 发件人

 收件人 +

 加密方式 ▼

 发送间隔时间 (s)

表4-3 配置事件说明

参数	说明
循环播放	选择“循环播放”后，一旦发生异常报警，将循环播放报警提示音。
全局声音	<ul style="list-style-type: none"> 选择“全局声音”，并在“音频文件路径”选择PC本地的声音，对应事件触发后，将播放该声音。 不选择“全局声音”，在下拉列表框选择声音或在“音频文件路径”选择PC本地的声音，对应事件触发后，将播放该声音。
SMTP（邮件）	<p>当需要联动发送邮件时，需要配置“SMTP（邮件）”。选择“SMTP（邮件）”，并配置SMTP参数，然后单击“邮件测试”，检查邮件配置是否成功。</p> <ul style="list-style-type: none"> SMTP服务器：填写SMTP服务器IP地址。 端口：填写SMTP服务器端口号。 用户名：填写SMTP服务器登录用户名。 密码：填写SMTP服务器登录密码。 发件人：填写发件人地址。 收件人：填写收件人地址 加密方式：选择SMTP服务器支持的加密方式。 发送间隔时间：设置后，平台将按照该时间间隔发送异常报警信息。

步骤3 单击“应用”。

4.4 设置文件保存路径

设置设备端采集到的事件图片、录像等数据的保存位置。

步骤1 在界面右上角选择“ > 系统配置 > 文件路径”。

步骤2 配置文件保存路径。

图4-4 文件路径配置

文件路径

事件图片路径

nal_IS_V1.001.0000000.1.R.200811/Data/User/Picture/Capture

录像路径

164-Internal_IS_V1.001.0000000.1.R.200811/Data/User/Record

步骤3 单击“应用”。

4.5 数据管理

设置定时提取设备的考勤数据，以及定时清除保存在PC本地的数据、图片和录像。

步骤1 在界面右上角选择“ > 系统配置 > 数据管理”。

步骤2 设置定时提取设备的考勤/门禁数据和定时清除平台的数据。

图4-5 数据管理

数据管理

☒ 定时提取考勤记录
 ☒ 定时提取门禁记录

☒ 图片

定时提取时间

每天

08:00

+

☒ 数据清理

数据库保存时间

3650

 天

图片录像保存时间

365

 天

人体测温计数 ☐ 清零 重启后生效

人体测温保存图片和视频模式

超温记录

 重启后生效

表4-4 数据管理

参数	说明
定时提取考勤/门禁记录	<p>按照设置时间自动提取设备的考勤/门禁记录及图片。</p> <p> 说明</p> <ul style="list-style-type: none"> 如需提取门禁设备中的考勤记录，需要先将其设置为考勤点。详细介绍请参见考勤方案的使用说明书。 当定时提取时间配置为“每天提取”时，每天最多配置5个时间点。
数据清理（除测温数据）	按照实际需求设置数据、图片和录像保存时间。平台在每天零点以及启动时自动清除超过保存时间的数据，实时清除超过保存时间的图片和录像。
测温数据清理	<ul style="list-style-type: none"> 按照实际需求选择清零测温计数，重启后生效。 设置测温记录图片和视频的保存模式，重启后生效。 <ul style="list-style-type: none"> 仅保存超温事件记录的图片和视频。 仅保存超温和无口罩事件记录图片和视频。 保存所有记录的图片和视频。

步骤3 单击“应用”。

4.6 备份还原

备份及还原平台配置。

步骤1 在界面右上角选择“ > 系统配置 > 备份还原”。

步骤2 备份配置到本地。支持如下任意一种备份方式。

- 手动备份。单击“手动备份”，在弹出的对话框选择保存路径并设置配置名称，单击“应用”。

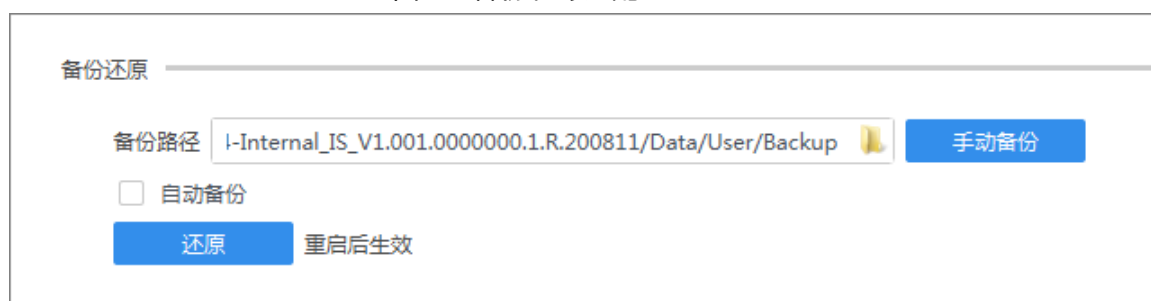
保存平台当前配置到本地。

- 自动备份。选择“自动备份”，并设置自动备份时间，单击“应用”。

在设置时间点自动保存平台当前配置到本地。

步骤3 导入配置到平台。单击“还原”，选择需要导入的配置文件，单击“应用”。

图4-6 备份和导入配置



4.7 软件授权

通过导入License文件更新平台软件授权信息。

前提条件

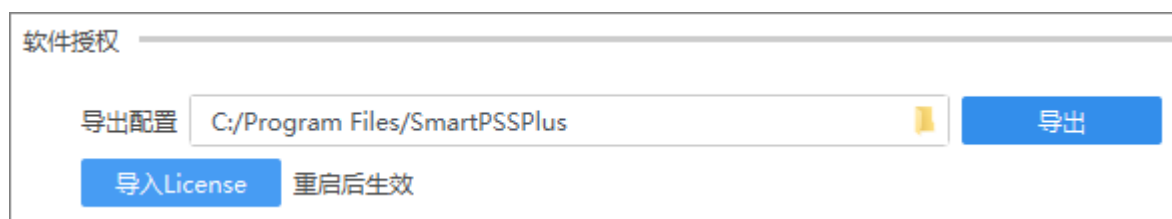
请提前联系技术支持人员，帮助获取License文件。

操作步骤

步骤1 在界面右上角选择“ > 系统配置 > 软件授权”。

步骤2 选择导出配置路径，单击“导出”将设备配置信息导出到本地。

图4-7 软件授权



步骤3 将配置文件提供给技术支持人员，获取对应的License文件。

步骤4 单击“导入License”，选择License文件，导入License信息到设备。

步骤5 单击“应用”。

第 5 章 用户管理


支持增加用户，同时支持给admin和普通用户配置菜单权限，完成配置并登录系统后，只能看到和使用具有权限的菜单。

角色是用户的集合，具有“用户管理”权限的用户均支持创建用户和角色。

5.1 添加角色

支持添加角色，并赋予角色菜单权限。

操作步骤

步骤1 在界面右上角选择“ > 用户管理”。


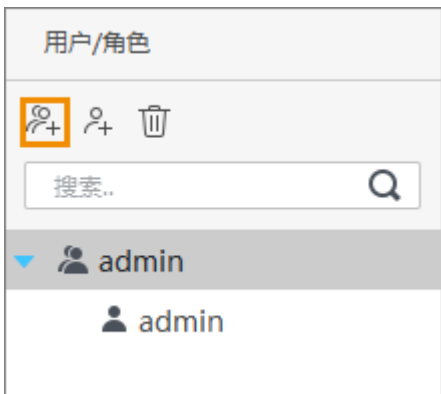
步骤2 在导航树单击。

图5-1 单击添加角色图标



步骤3 在界面右侧填写角色名称，并选择需要赋予该角色权限的业务，单击“保存”。

图5-2 设置角色权限

角色名称: 考勤

备注:

菜单权限:



☒ 全选

☐ 门禁管理
☒ 考勤管理
☒ 日志查询
☒ 设备管理
☒ 设备配置
☒ 人事管理
☒ 考勤监控
☒ 系统配置
☒ 考勤向导
☐ 门禁监控
☐ 门禁向导
☐ 事件配置

保存

取消

相关操作

- 修改角色：在导航树单击待修改角色右侧的。在右侧界面修改角色信息，单击“保存”。
- 删除角色：在导航树选择待删除角色，单击.

5.2 添加用户

支持添加用户，并赋予用户菜单权限。

操作步骤



- 步骤1 在界面右上角选择“ > 用户管理”。
- 步骤2 在界面左侧单击.

图5-3 添加用户

用户名:

角色:

密码:

密码确认:

备注:

菜单权限:



☒ 全选

☒ 门禁管理
☒ 考勤管理
☒ 日志查询
☒ 设备管理
☒ 设备配置
☒ 人事管理
☒ 考勤监控
☒ 系统配置
☒ 考勤向导
☒ 门禁监控

保存

取消

相关操作

- 修改用户：在导航树单击待修改用户右侧的，在右侧界面修改用户信息，单击“保存”。
- 删除用户：在导航树选择待删除用户，单击。

第 6 章 设备管理

主要用于添加设备到系统，这是业务搭建的第一个环节。设备添加完成后，支持通过平台远程配置和操作已添加的设备。



说明

使用设备管理功能时，请务必关闭ConfigTool、SmartPSS、DSS系列软件，否则部分功能的使用会受到影响，例如通过搜索添加设备时，可能搜索不到全部设备。

6.1 添加设备

平台最多支持添加64台设备、64个门禁通道、64个或256个视频通道。



说明

SMB-H1上的平台最多添加256个视频通道；其他情况下的平台最多添加64个视频通道。

支持通过如下任意一种方式添加设备，请根据添加设备数量、网段等情况选择合适方式。

- 通过搜索
- 手动添加
- 通过导入

6.1.1 通过搜索添加设备

通过搜索特定网段内的所有IP来添加设备。

操作步骤

- 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。支持通过如下任意一种方式搜索设备。
 - 方式一：单击“自动搜索”，自动搜索与PC同一局域网的设备。
 - 方式二：填写设备网段范围，单击“搜索”，搜索网段范围内的所有设备。

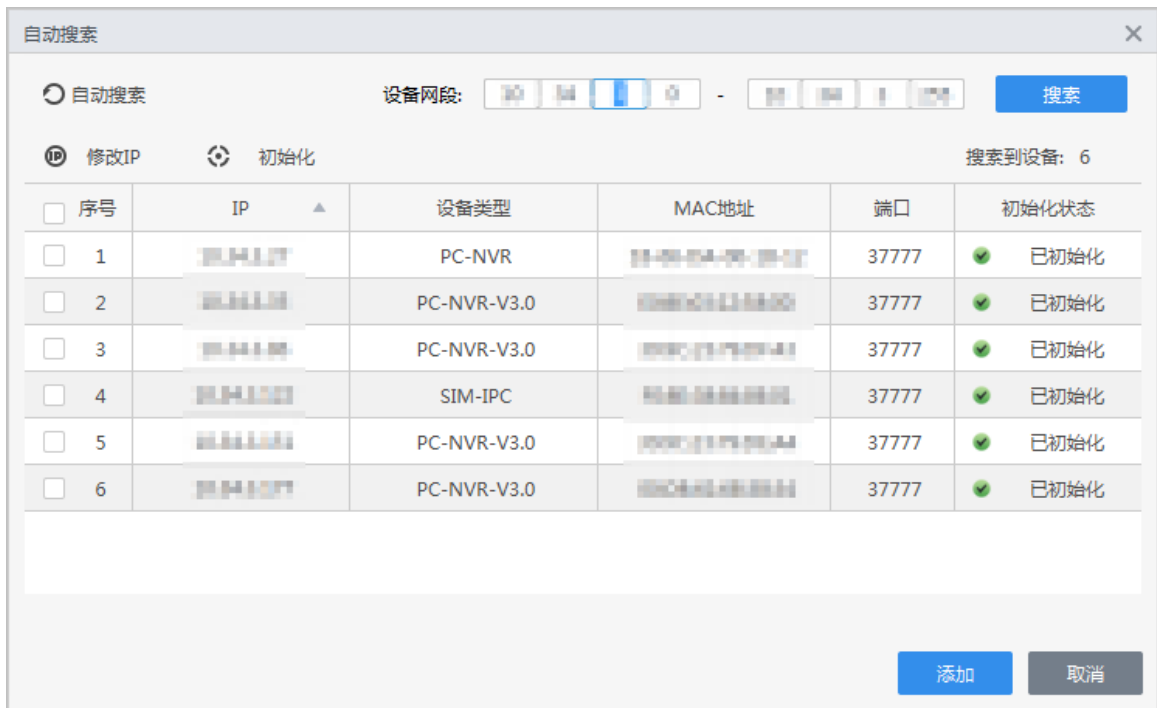


说明

使用该搜索方式需确保平台与设备网络互通。

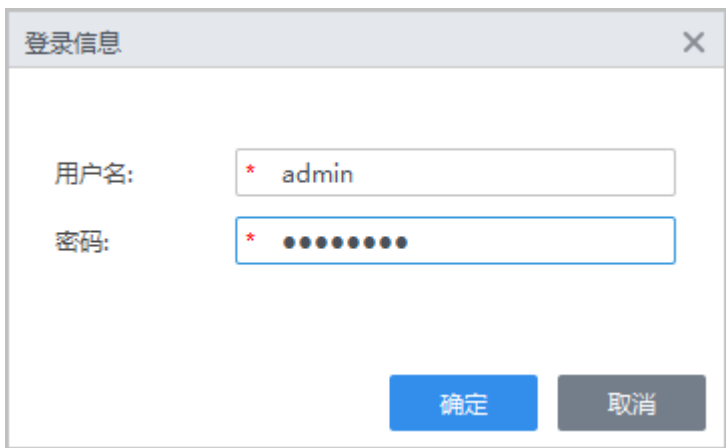
- 步骤3 选择需要添加的设备，单击“添加”。

图6-1 搜索结果



步骤4 输入登录设备的“用户名”和“密码”，单击“确定”。
成功添加设备，同时自动登录设备。如果登录成功，则在线状态显示为“在线”，否则为“离线”。

图6-2 登录设备



相关操作

- 导出设备信息。在设备列表，选择要导出信息的设备，单击“导出”，根据界面提示导出设备信息到本地。
- 修改设备登录信息。在设备列表，单击设备右侧的✎或双击设备，修改设备登录信息，例如设备IP地址、端口号、登录账号和密码。
- 删除设备。在设备列表，单击设备右侧的🗑，或选择需要删除的设备，单击“删除”，根据界面提示删除设备。

6.1.2 手动添加设备

添加单个设备，且已获取设备的IP地址时，建议采用手动添加方式添加设备。

步骤1 在主页选择“设备管理”，单击“添加”。

步骤2 在“添加设备”界面，输入设备参数。

图6-3 手动添加设备

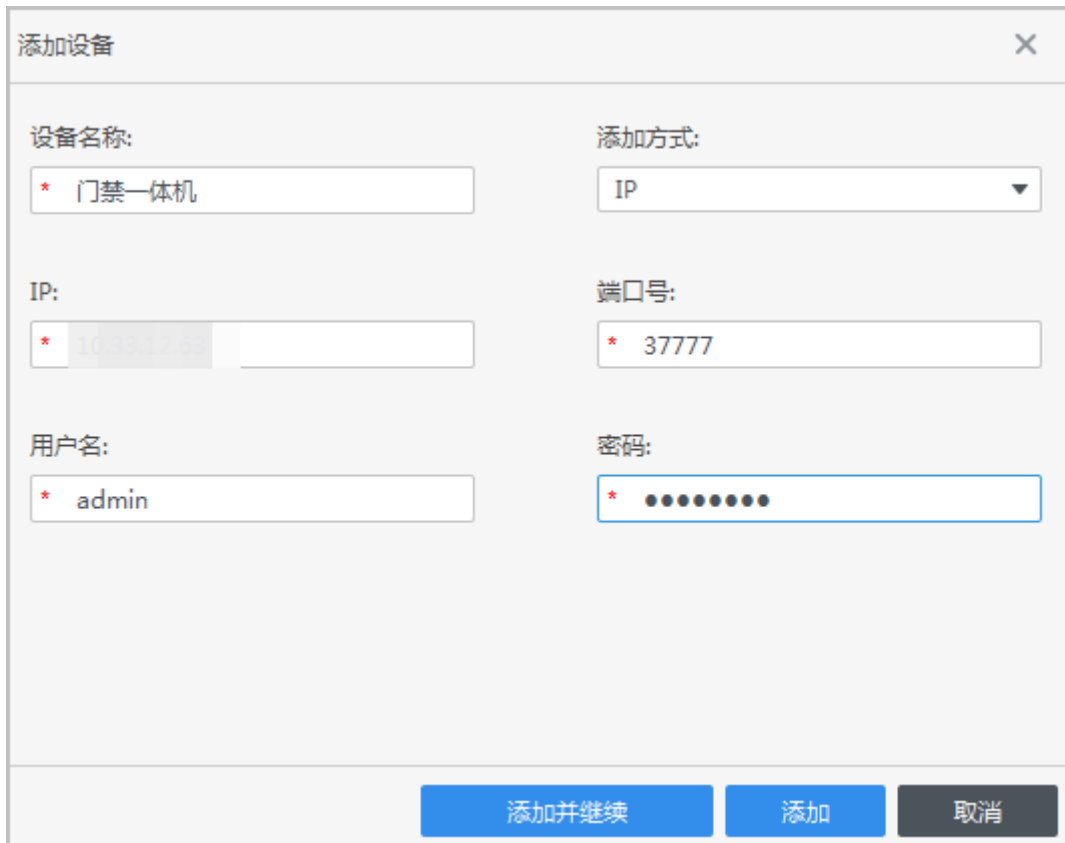



图6-3展示了“添加设备”的界面。该界面包含以下输入项：

- 设备名称:** 输入框，内容为“* 门禁一体机”。
- 添加方式:** 下拉菜单，选择“IP”。
- IP:** 输入框，内容为“* 10.33.12.52”。
- 端口号:** 输入框，内容为“* 37777”。
- 用户名:** 输入框，内容为“* admin”。
- 密码:** 密码输入框，显示为“* ”。

界面底部有三个按钮：“添加并继续”（蓝色）、“添加”（蓝色）和“取消”（灰色）。

表6-1 添加设备参数说明

参数	说明
设备名称	填写设备的名称。
添加方式	支持通过设备的IP地址和设备序列号添加设备。 <div>  说明 仅支持P2P功能的设备支持通过序列号添加。 </div>
IP/序列号	填写该设备IP地址/设备序列号。
端口号（可选）	当添加方式为“IP”时，填写设备的端口号，默认端口号为37777。
用户名	登录设备的用户名。
密码	登录设备的密码。

步骤3 单击“添加”，完成设备添加。

6.1.3 通过导入添加设备

支持通过导入xml格式的设备信息文件添加设备。

前提条件

已导出xml格式的设备信息文件。

操作步骤

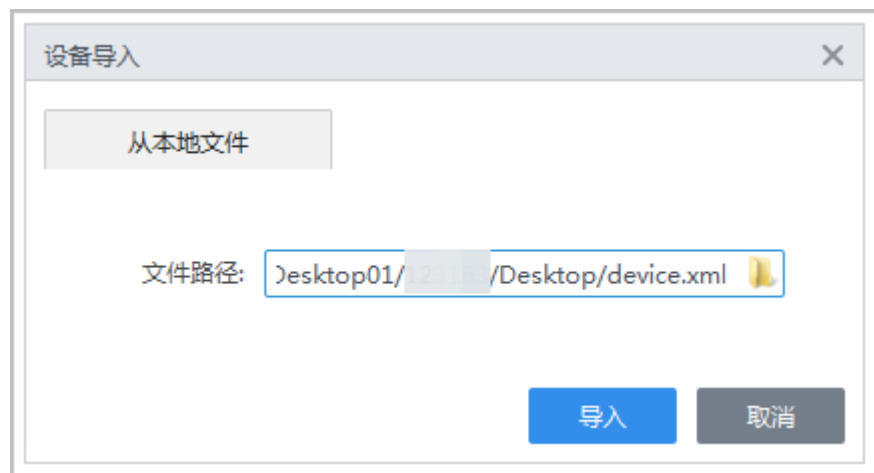
- 步骤1 在主页选择“设备管理”，单击“导入”。
- 步骤2 选择保存在本地的设备信息文件，单击“导入”。



说明

设备添加完成后，会自动登录设备。如果登录成功，则在线状态显示为“在线”，否则为“离线”。

图6-4 导入设备



6.2 配置设备

设备类型不同配置功能不同，本文以门禁设备为例介绍。对已管理的在线的门禁设备，支持查看设备信息、设置时间、重启，也支持提取该设备采集到的所有人员及其考勤数据等。

- 步骤1 在主页选择“设备管理”。
- 步骤2 在设备列表单击设备右侧的⚙️。

图6-5 配置和操作设备（1）

<input checked="" type="checkbox"/>	序号	名称	A	IP	设备类型	设备型号	端口	通道数	在线状态	序列号	操作
<input checked="" type="checkbox"/>	1				门禁一体机		37777	0/0/2/2	● 在线		

- 步骤3 在设备配置和操作界面，单击需要使用的功能模块，进行设备配置和操作。



说明

不同设备支持的配置不同，请以实际界面为准。

- 时间设置。设置设备的事件。
单击“时间设置”，在弹出的界面手动设置设备的时间。

图6-6 设置设备时间



表6-2 设置设备时间参数说明

参数	说明
日期格式	设置设备上的日期的显示格式。 <ul style="list-style-type: none"> • yyyy-MM-dd: 年-月-日 • MM-dd-yyyy: 月-日-年 • dd-MM-yyyy: 日-月-年
时间格式	设置设备上的时间格式。
时区	设置设备所在地的时区。
系统时间	设置设备当前的日期和时间，单击“同步PC”，则设置设备的时间和PC时间相同。
夏令时	根据实际情况决定是否设置夏令时，如果设备所在地存在夏令时，则设置夏令时，在“夏令时类型”栏选择设置方式，然后设置夏令时的开始和结束时间。
NTP设置	如果需要同步NTP服务器的时间给设备，选择“NTP设置”，并填写NTP服务器的IP地址、端口，在“更新周期”文档框输入同步NTP服务器的时间给设备的间隔时间。

- 升级。升级设备程序。
单击“升级”，根据提示选择设备最新程序安装包，单击“升级”，根据提示完成设备升级。
- 重启。重新启动设备。
单击“重启”，根据提示重启设备。
- 本地报警联动（可选）。
单击“本地报警联动”，在弹出的界面配置报警联动信息，单击“保存”。

图6-7 配置报警联动

外部报警

报警输入 1

报警输出 ☒ 1 2

输出延时 300 秒 (1-300)

复制当前配置到 无

表6-3 配置报警联动参数说明

参数	说明
报警输入	该设备发生报警后，会联动输出报警。
报警输出	选择外部报警发生后，联动的报警输出设备。例如报警输入选择1，报警输出选择2，则与门禁连接的报警输入1通道设备发生报警后，会联动与门禁连接的报警输出2通道设备输出报警。
输出延时	设置报警持续时间。
门联动	设置触发报警后门禁的工作状态。 <ul style="list-style-type: none"> 常开：门处于始终打开状态。 常闭：门处于始终关闭状态，将无法验证开门。
复制当前配置到	选择复制报警配置通道。

- 人员提取。提取设备上采集到的人员信息到平台。
单击“人员提取”，在人员列表选择要提取信息的人员，单击“提取”，根据提示提取人员信息。
- 考勤记录提取（仅部分设备支持）。提取设备的考勤记录到平台。
单击“考勤记录提取”，设置提取时间段，提取时间段内的考勤记录。



说明

对于门禁设备，需确保已设置为考勤点，才能提取该设备上的考勤记录。设置考勤点的详细介绍请参见考勤方案的使用说明书。

- 软复位/硬复位（仅部分设备支持）。
 - ◇ 软复位：恢复设备默认参数。
 - ◇ 硬复位：恢复设备出厂设置。
- 修改密码（仅部分设备支持）。
单击“修改密码”，输入旧密码和新密码，单击“保存”。
- 防火墙（仅部分设备支持）。
 1. 单击“防火墙”。
 2. 打开“启用”，根据实际需求选择模式。
 - ◇ 允许名单：只允许下表中的IP/MAC对应的源主机通过网络连接访问本设备对应端口号。
 - ◇ 禁用名单：禁止下表中的IP/MAC对应的源主机通过网络连接访问本设备的对

应端口号。

图6-8 防火墙



- 单击 $+$ ，添加IP地址及端口，单击“确定”。

图6-9 添加



- IP配置（仅部分设备支持）。配置DHCP及DNS服务器
 - 单击“IP配置”。
 - 根据实际需求启用或禁用配置。

表6-4 IP配置

参数	说明
DHCP使能	DHCP是一个局域网的网络协议，用于给内部网络或网络服务提供商自动分配IP地址，为管理计算机IP地址提供统一的管理手段。

参数	说明
动态获取DNS服务器	动态域名系统指将用户的动态IP地址映射到一个固定的域名解析服务上，用户每次连接网络时客户端会通过信息传递把该主机的动态地址传送给位于服务商主机上的服务器程序，服务器程序负责提供DNS服务并实现动态域名解析。即用户无需记录不断变更的IP地址，只需通过域名访问登录设备或地址。

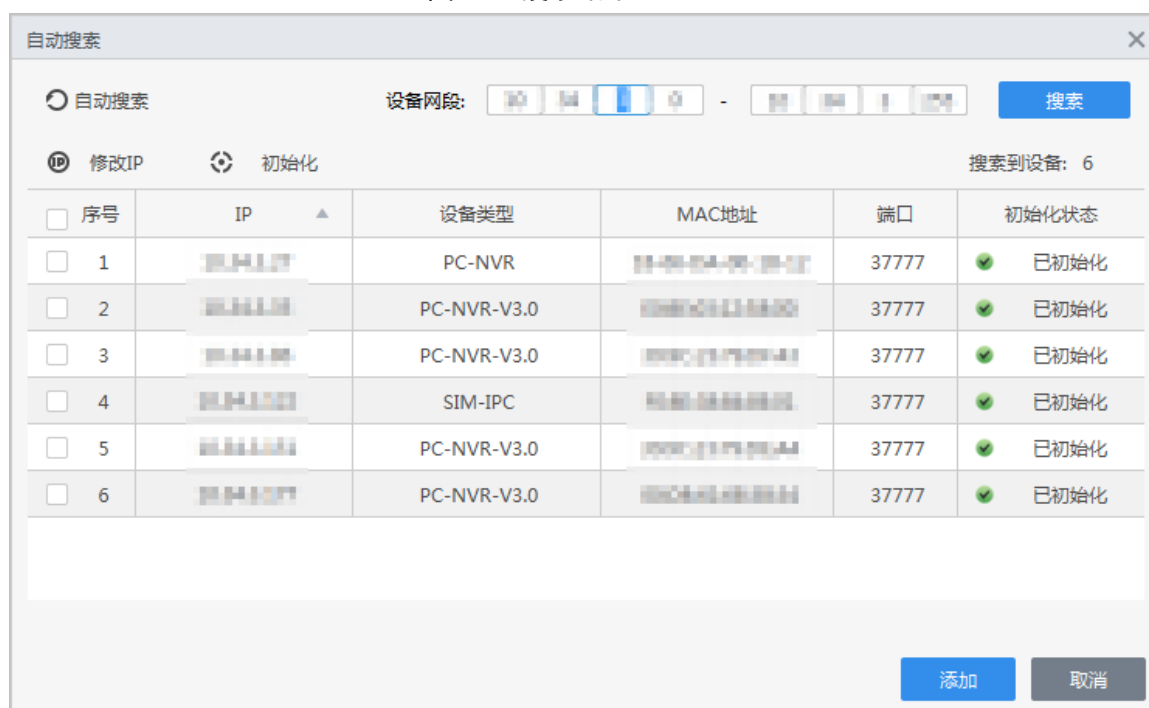
- 配置文件（仅部分设备支持）。导入配置文件配置设备或导出设备当前配置到本地。
 - ◇ 导入配置文件（需要重启软件还原配置）：选择“配置文件 > 导入配置文件”，选择配置文件，单击“确定”。
 - ◇ 导出配置文件：选择“配置文件 > 导出配置文件”，选择文件保存路径，单击“保存”。

6.3 修改设备IP地址

通过平台修改设备的IP地址。

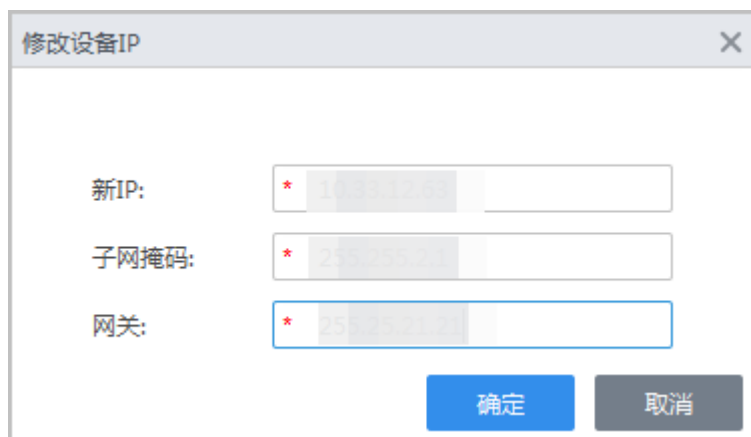
- 步骤1 在主页选择“设备管理”，单击“自动搜索”。
- 步骤2 在“自动搜索”界面，输入设备网段范围，单击“搜索”。
- 步骤3 在设备列表，选择需要修改IP地址的设备，单击“修改IP”。

图6-10 搜索结果



- 步骤4 设置设备的IP地址、子网掩码和网关，单击“确定”。如果是批量修改设备IP，请注意以下事项。
- 所有选中设备的用户名和密码必须相同。
 - 设置的IP地址将赋予设备列表中选择的最上面的设备，从上向下设备IP地址按1递增，例如您选择两台设备修改IP地址，当设置的IP地址为192.168.1.10，则设备列表中选择的最上面设备的IP地址为192.168.1.10，下一台设备的IP地址为192.168.1.11。
 - 设置的子网掩码和网关将同时赋予所有设备。

图6-11 修改单台设备IP



修改设备IP

新IP: * 193.12.63

子网掩码: * 255.255.255.0

网关: * 255.255.255.255

确定 取消

图6-12 批量修改设备IP



批量修改设备IP

2 台设备被选中！

起始IP: * 10.33.1.1

子网掩码: * 255.255.255.0

网关: * 255.255.255.255

确定 取消

步骤5 输入该设备的登录用户名和密码，单击“确定”。

6.4 初始化设备

仅支持对与PC处于同一网段的设备进行初始化，支持如下初始化操作。

- 设置设备admin用户的登录密码。
- 绑定电话号码。当忘记密码时，通过该电话号码可以重置密码。
- 修改设备的IP、子网掩码和网关。

步骤1 在主页选择“设备管理”，单击“自动搜索”。

步骤2 填写设备网段范围，单击“搜索”。

步骤3 在设备列表中选择需要初始化的设备，单击“初始化”。

步骤4 设置admin的登录密码，单击“密码安全”。

图6-13 设置admin用户的登录密码



用户名: admin

密码: *

密码确认: *

密码8~32位, 且至少包含数字、字母和常用字符中的两种。

密码安全 → 取消

步骤5 设置用于找回密码的电话号码, 单击“修改IP”。

图6-14 绑定邮箱



电话

绑定电话号码: *

上一步 修改IP → 取消

步骤6 设置新IP、子网掩码和网关, 单击“完成”。如果未设置新IP、子网掩码和网关, 则设备的IP、子网掩码和网关为出厂默认设置。

图6-15 设置IP等设备信息

1.设置密码

2.密码安全

3.修改IP

新IP:

10

88

12

8

✓

子网掩码:

*255

255

255

0

网关:

*10

88

12

6

上一步

完成

取消

第 7 章 配置设备事件

配置设备事件联动报警。报警类型包括发出报警声音、发送邮件提醒、地图闪烁、保存录像、详情弹窗、联动摄像机录像和联动报警设备输出报警。

说明

- 不同设备支持的联动事件类型不同，请以实际界面为准。
- 配置门禁防反潜功能时，通过“事件配置”配置防反潜模式后，还需要在门禁方案中配置进门和出门对应的读头、生效时间等。详细介绍请参见平台门禁方案使用说明书。

本章以配置视频遮挡报警联动为例。

步骤1 在主页选择“事件配置”。

步骤2 在导航树选择相应设备。

步骤3 选择“通道事件 > 视频遮挡”。

步骤4 单击“视频遮挡”右侧的 ，开启视频遮挡报警功能。

步骤5 按照实际需求配置视频遮挡报警联动。

- 开启报警通知。
 - ◇ 报警声音：一旦发生视频遮挡事件，平台会发出声音提醒。
 - ◇ 地图闪烁：一旦发生视频遮挡事件，发生该事件的地图将会以闪烁形式提醒发生了报警事件。
 - ◇ 发送邮件：启用“发送邮件”，跳转到系统配置界面，配置邮件相关信息。例如SMTP服务器地址、端口号、邮件收件人等。配置后，一旦发生视频遮挡事件，系统会自动发送视频遮挡报警信息邮件给指定收件人。
 - ◇ 详情弹窗：一旦发生视频遮挡事件，平台会弹出弹窗提醒发生报警事件。
 - ◇ 保存录像：一旦发生视频遮挡事件，平台会自动按照设定的时间保存报警事件录像。

图7-1 配置视频遮挡报警提示



- 配置联动摄像机录像。
 1. 单击“联动视频”页签。







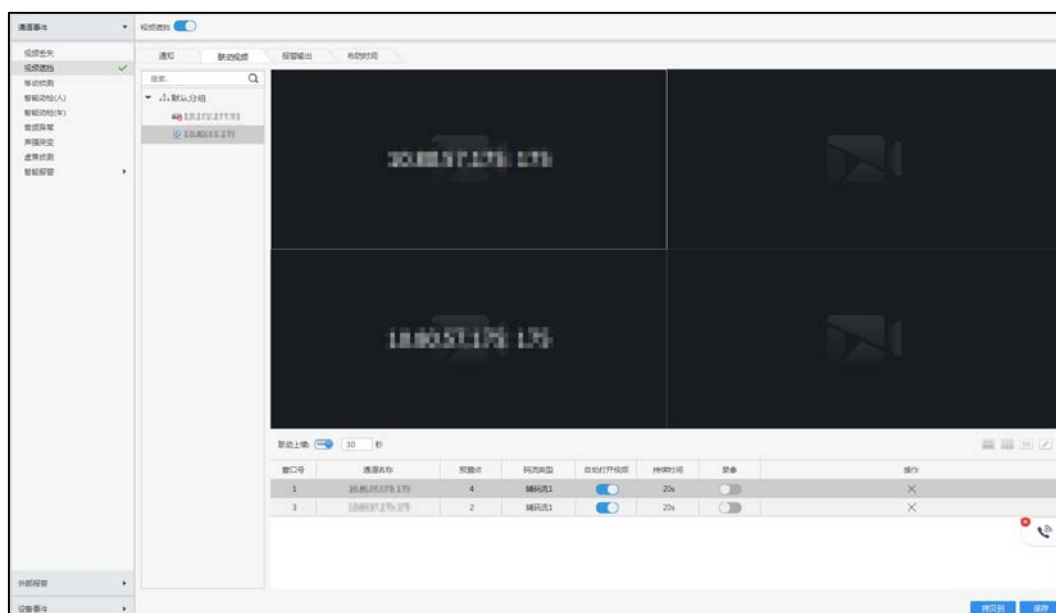
2. 在组织树中将需要联动的摄像机拖动到需要显示的视频窗口。
3. 开启“联动上墙”功能，设定上墙时间，可将发生报警事件的窗口自动联动到电视墙上。关于电视墙的相关操作和功能，详细介绍请参见SmartPSS Plus视频监控方案_使用说明书。在客户端主界面左边列表中选择“视频监控”，点击右下角“监控说明书”，获取相关说明书。
4. 选择    ，选择该视频窗口的分割形式。
5. 在下方列表配置摄像机参数。
 - ◇ 单击“预置点”列，选择联动时摄像机位置对应的预置点，触发报警时，自动转到该预置点所在位置。
 - ◇ 单击“码流类型”列，设置使用摄像机实时预览时使用的码流类型。
 - ◇ 选择是否启用“自动打开视频”，默认已启用。发生视频遮挡报警后，平台会自动打开摄像机的实时预览画面。
 - ◇ 单击“录像”列的 ，开启录像功能
 - ◇ 单击 ，删除已关联的IPC。

图7-2 配置联动视频




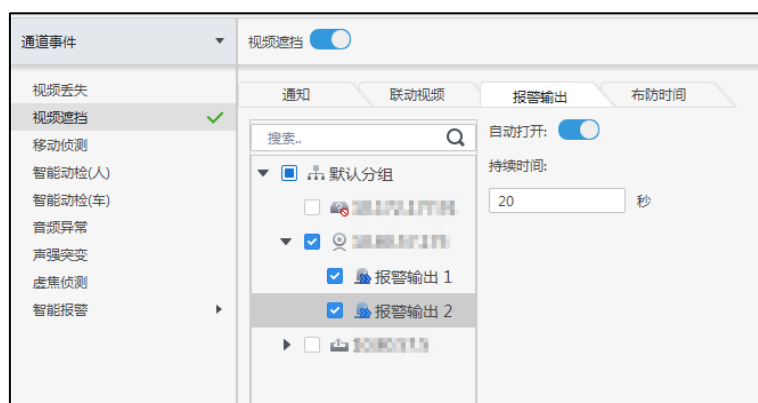
- 配置联动报警输出。
 1. 单击“报警输出”。
 2. 在导航树选择发生视频遮挡事件需要联动的设备，单击“自动打开”右侧的 ，开启联动报警输出功能。
 3. 设置联动报警持续时间。
发生视频遮挡事件后，联动设备会按照设置时间输出报警。

图7-3 配置视频遮挡联动报警

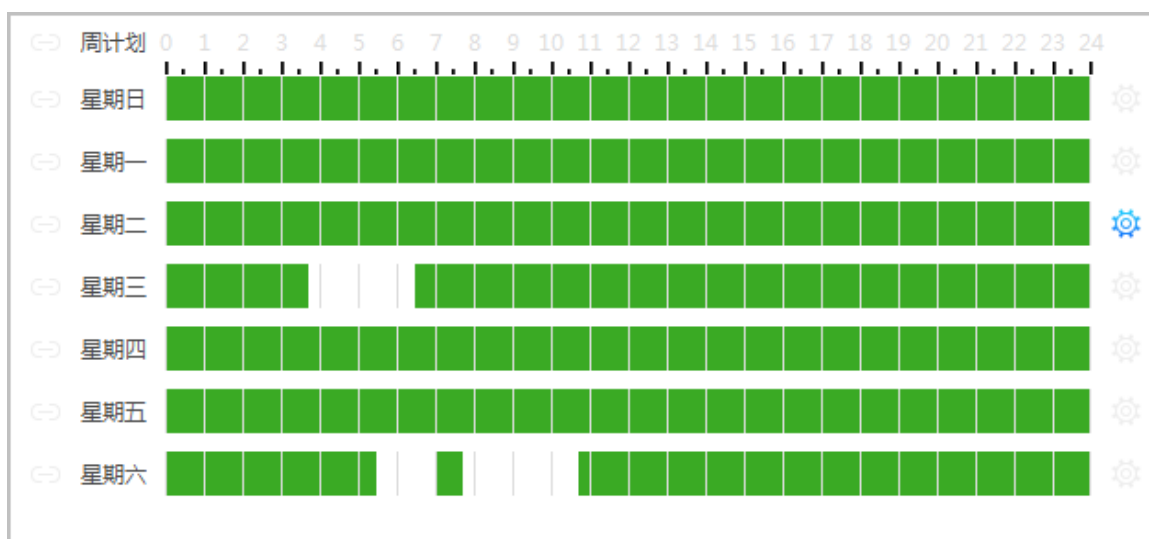


- 设置布防时间。

默认周一～周日全时段布防，如果需要修改布防时间，使用如下任意一种方式。

- ◇ 方式一：请将光标移动到绿色时间块，光标会变成橡皮擦，擦去不布防的绿色时间块。时间块显示灰色表示该时间段未布防。
- ◇ 方式二：单击任意一天时间块右侧的⚙️，设置布防时间。

图7-4 设置布防时间



- 步骤6 在界面右下角单击“拷贝到”，选择要使用该配置的其他设备，单击“确定”。该配置在这些设备上同样生效。

图7-5 选择要应用的设备



步骤7 在界面右下角单击“保存”，完成视频遮挡事件联动配置。

第 8 章 事件中心


查看实时报警事件信息，处理报警事件。单击界面右上角  99+ 内数字，进入事件中心。

图8-1 事件中心



表8-1 事件中心界面介绍

参数	说明
事件数据统计	<p>实时统计各类事件数量及处理率。</p> <ul style="list-style-type: none"> 事件总数/处理率：实时显示当前事件总数及处理率饼图。单击饼图，可查看未处理事件信息。根据实际情况选择处理事件。 各事件处理率：实时显示各类事件的今日处理数量/今日上报总数、处理率条形统计图。 七日事件趋势：显示今日之前七日（不包含今日）中，报警事件数量前五名的事件类型曲线图。将光标移动至图中，显示报警事件数量的具体数值。 单击>显示各类事件详细数据。单击事件饼图，可查看该类型事件中未处理事件信息。根据实际情况选择处理事件。
视频预览	预览已配置的通道视频画面。单击⏏收起预览画面。
实时事件	实时报警事件。根据报警类型及设备可筛选事件信息。

8.1 配置预览视频

配置预览视频通道，支持抓取通道图片、录像、语音对讲等功能。

操作步骤

步骤1 进入事件中心界面，在 中选择屏幕数量。



说明

仅支持1、4、9分屏。

步骤2 单击一块屏幕，在弹出的设备树中选择需要绑定的设备。

步骤3 右键单击屏幕，单击“码流类型”，选择需要预览的视频码流通道。

步骤4 单击“设置”，根据实际需求设置信息。

图8-2 设置

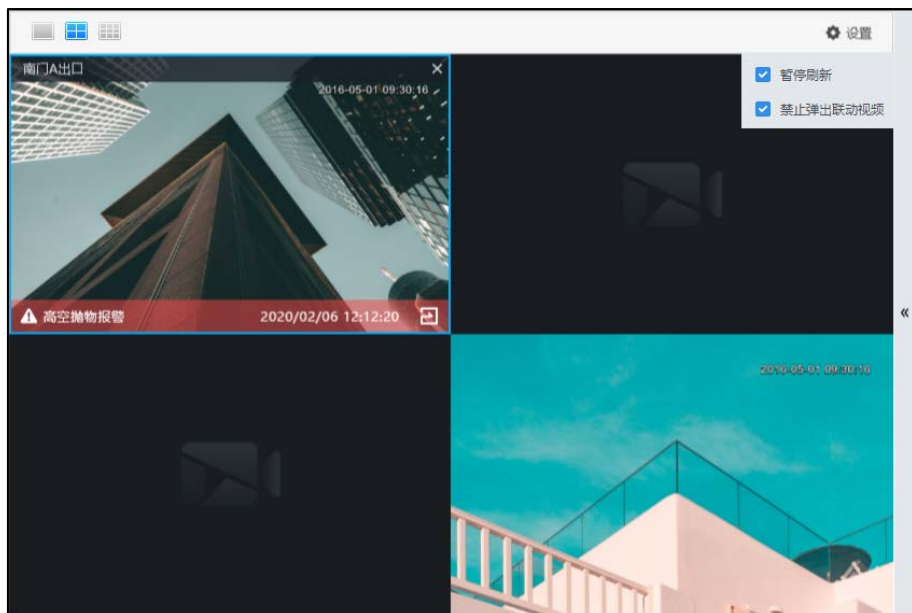


表8-2 设置









参数	说明
暂停刷新	暂时停止刷新实时报警事件。
禁止弹出联动视频	禁止弹出事件联动视频。

相关操作

预览视频操作。将鼠标移至视频窗口，窗口右上角显示快捷操作。

表8-3 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。

图标	图标含义	说明
	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。
	即时回放	开启或关闭即时回放，回放时间通过界面右上角“  > 系统配置 > 基础设置 > 即时回放时间”设置。即时回放的前提是设备端有录像。
	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。

8.2 处理报警事件

8.2.1 操作步骤


步骤1 单击事件统计区域的饼图打开未处理事件列表，或在实时报警事件列表中，单击。

图8-3 未处理事件



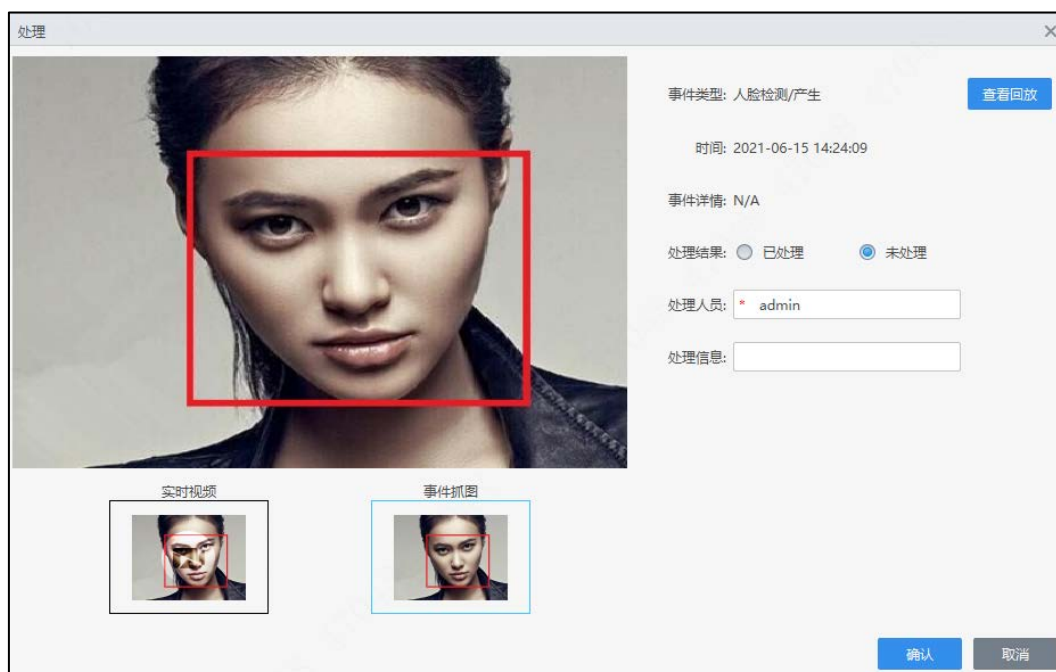
步骤2 在处理界面，查看事件类型、事件详情、事件回放、处理结果等。

图8-4 处理界面



步骤3 处理界面默认展示“实时视频”。单击“事件抓图”查看抓图；单击“查看回放”查看报警录像。

图8-5 查看事件抓图



步骤4 确认后，选择“已处理”，输入处理人员名称，单击“确认”。

批量处理。

1. 单击事件统计区域的饼图打开未处理事件列表，或在实时报警事件列表中单击“批量处理”。
2. 选择多条事件，单击“处理”。
3. 选择“已处理”，单击“确认”。

8.2.2 特殊报警事件

“非机动车入梯”、“非机动车入户”、“非机动车违停”及“视频遮挡”属于特殊报警事件，设有消警功能；其他报警事件暂时不支持消警功能。

本章以非机动车入梯报警事件为例。

8.2.2.1 触发报警

当非机动车进入电梯区域线内，摄像机监测到非机动车后会闪烁灯光并发出预设的提示音。若客户在“事件配置”事件配置中开启了“详情弹窗”使能，则会弹出弹窗并展示实时预览画面。

图8-6 非机动车入梯报警弹窗



8.2.2.2 消除报警

当发生报警且报警上报到平台时，可在客户端上消除警报，共有两种处理方式：

1. 手动消警。

- 若提前在“事件配置”中开启“详情弹窗”，可在客户端详情弹窗中消除报警信息。
当报警事件发生时，平台会展示报警信息的弹窗，在详情弹窗中点击“消除报警”，前端IPC立即停止声光报警，若是“非机动车入梯”事件会同时关闭所有报警输出通道，客户端事件更新已处理状态。
- 在“事件中心”的“实时事件”列表中，单击 打开客户端详情弹窗，重复上述操作。

2. 自动消警：若提前在“事件配置”中开启“详情弹窗”，当报警事件发生时，平台会展示报警信息的弹窗，若非机动车移出电梯，解除报警，平台报警弹窗消失，此时客户端事件状态为未处理状态。



说明

- 同个设备上报相同事件，只显示一个弹窗。

- 页面最多显示十条报警信息的弹窗。

第 9 章 日志查询

支持查询系统和关联设备的相关日志。

步骤1 选择在界面右上角选择“主页 > 日志查询”。

步骤2 选择日志类型，设置查询时间段，单击“搜索”。

图9-1 日志查询



序号	时间	用户	事件类型	设备	设备名称	备注
1	2020-04-29 08:44:46	admin	登录			

步骤3 单击“导出”，将日志导出到本地。

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