



# SmartPSS Plus 商显控制方案











## 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
 <b>危险</b>	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。
 <b>警告</b>	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。
 <b>注意</b>	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。
 <b>防静电</b>	表示静电敏感的设备。
 <b>当心触电</b>	表示高压危险。
 <b>激光辐射</b>	表示强激光辐射。
 <b>风扇警告</b>	表示危险运动部件，请远离运动风扇叶片。
 <b>当心机械伤人</b>	表示设备部件机械伤人。
 <b>窍门</b>	表示能帮助您解决某个问题或节省您的时间。
 <b>说明</b>	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	<ul style="list-style-type: none"> <li>新增两个屏显示考勤展示内容、自动搜索大屏 IP，显示当前进出人员体温、在场人数及人员信息。</li> <li>更新 UI 界面。</li> </ul>	2020.11
V1.0.0	首次发布。	2020.09

# 目录


前言 .....	I
第 1 章 简介.....	1
第 2 章 打开商显控制方案 .....	2
第 3 章 方案操作 .....	3
3.1 首次操作 .....	3
3.2 日常操作 .....	6
3.2.1 创建节目 .....	6
3.2.2 切换商显控制器 .....	7
3.2.3 调节 LED 屏亮度.....	8
3.2.4 设置定时开屏或手动开屏 .....	9
附录 1 法律声明 .....	11
附录 2 网络安全声明和建议 .....	13


# 第 1 章 简介

SmartPSS Plus 商显控制方案是一套与门禁设备、LED 屏和 LED 屏控制器配合使用的用于 LED 屏的显示控制的方案。使用该方案，能设置 LED 屏上显示的项目名称、当前日期、倒计时和提示信息等，同时上传部门人员数量和门禁设备的验证通行数据到 LED 屏展示。

## 第 2 章 打开商显控制方案

不同场景打开商显控制方案的操作方法不同。

- 如果是首次使用 **SmartPSS Plus**，登录过程中加载商显控制方案。登录后，在主页的左侧导航栏单击 ，打开商显控制方案。

- 如果已打开 **SmartPSS Plus**，但未加载商显控制方案，在界面右上角选择“ > 切换方案”，

加载商显控制方案。登录后，在主页的左侧导航栏单击 ，打开商显控制方案。

关于加载方案的详细介绍请参见 **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。

## 第 3 章 方案操作

SmartPSS Plus 商显控制方案将一套 LED 屏信息定义为一个节目。用户创建节目后，SmartPSS Plus 将节目发布给 LED 屏。

### 3.1 首次操作

首次使用商显控制方案，需要完成一系列的基础配置后，才能创建节目并将节目发布到 LED 屏。

#### 前提条件

请确保商显控制器、门禁设备和 SmartPSS Plus 所在 PC 之间网络互通。

#### 操作步骤

- 步骤1 打开商显控制方案。
- 步骤2 选择“主页 > 人事管理”，添加所有人员到系统，并将人员划分到指定部门，然后赋予所有人员门禁设备的通行权限。详细介绍请参见 SmartPSS Plus 门禁方案\_使用说明书。配置后，人员可通过刷卡等验证进场和出场，SmartPSS Plus 显示人数总数量，并统计进场和出场人员总数量、场内各个部门人员数量，并通过节目发送到 LED 屏幕展示。
- 步骤3 添加门禁设备并设置进门和出门读头。  
商显控制器会获取和分析添加到系统的所有门禁设备进出门数据，并通过节目发送到 LED 屏展示。
1. 选择“主页 > 设备管理”，添加进出口所有门禁设备到系统。

#### 说明

初次使用设备时，建议手动同步 PC 时间，使设备和平台时间保持一致，以保证业务功能正常运行。关于添加设备到系统的操作方法，请参见 SmartPSS Plus 门禁方案\_使用说明书。


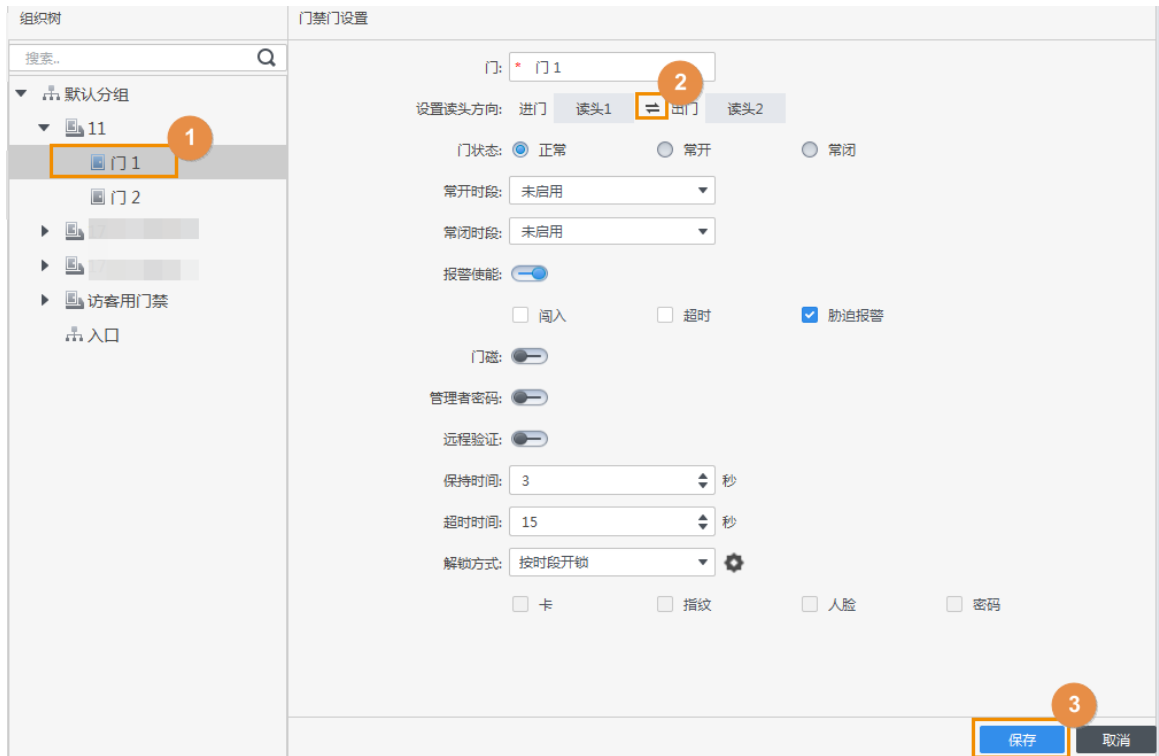
2. 设置进门和出门读头。  
选择“主页 > 门禁配置 > 门禁配置”，在组织树选择需要设置的门禁设备通道，在右侧界面按照实际情况通过单击 ，设置进门和出门读头。

图3-1 设置进出门读头



步骤4 添加商显控制器到系统。

1. 选择“主页 > 商显控制”。
2. 在商显控制器界面单击“添加设备”，在弹出的对话框填写商显控制器的 IP 地址，单击“确定”。

#### 说明

- 使用网线连接电脑和控制板卡，单击“直连搜索”，无需手动输入，直接获取 LED 屏的 IP 地址。
- 在添加设备界面，编辑设备 IP，端口号为默认不需修改，连接新设备，单击“确定”。
- 需要修改设备 IP 时，使用网线连接电脑和控制板卡。在对应的设备右侧，单击“修改 IP”，填写新 IP、子网掩码、网关，修改 IP 地址，单击“确定”。

图3-2 切换商显控制器（2）

编辑设备

设备一:

IP:

\*

直连搜索

修改IP

端口:

\*

名称

\*

test

设备二:

IP:

\*

直连搜索

修改IP

端口:

\*

名称:

\*

test2

确定

取消

步骤5 配置节目并发布到 LED 屏，详细介绍请参见“3.2.1 建”。

步骤6 配置 LED 屏上显示的时间，使时间与 PC 时间保持一致。


1. 在商显控制界面单击 .

图3-3 配置 LED 屏上显示的当前时间（1）

SmartPSS Plus

主页

商显控制

大屏1 已连接

IP:

大屏2 已连接

IP:

入场人数: 3

XXXXXXXXXX项目

2020年11月04日 星期三 13:29:57 倒计时: 180

某某班组:200 某某班组:100 总人数:999

某某班组:200 某某班组:100 进场数:100

某某班组:200 某某班组:100 出场数:10

某某班组:200 某某班组:100

人员:某某某 某某班组 出门 10:05:28

进入工地注意安全, 自觉佩戴安全帽

☒ 倒计时
 ☒ 体温
 ☒ 安全帽

预览 保存 发布

XXXXXXXXXX项目

2020年11月04日 星期三 13:29:57

隐患显于明火

防患胜于救灾

责任重于泰山

XXXXXXXXXX项目

2020年11月04日 星期三 13:31:58

隐患显于明火

防患胜于救灾

责任重于泰山

XXXXXXXXXX项目

2020年11月04日 星期三 13:33:59

隐患显于明火

防患胜于救灾

责任重于泰山

XXXXXXXXXX项目

2020年11月04日 星期三 13:35:00

隐患显于明火

防患胜于救灾

责任重于泰山

5

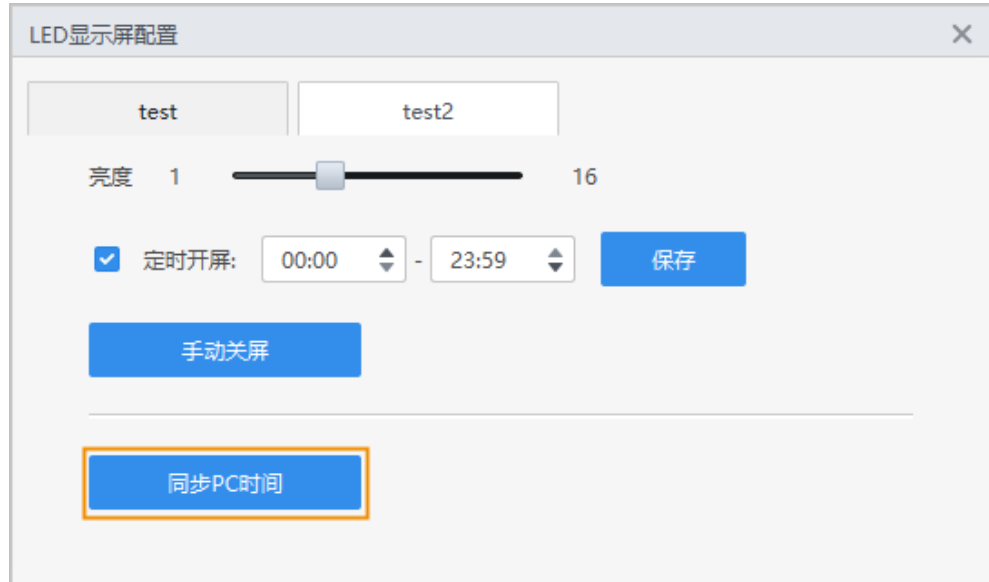


2. 在弹出的对话框单击“同步 PC 时间”。  
LED 屏上显示的当前时间切换为 PC 时间。

#### 说明

支持切换 LED 屏，配置不同 LED 屏的当前时间。

图3-4 配置 LED 屏的当前时间（2）



## 3.2 日常操作

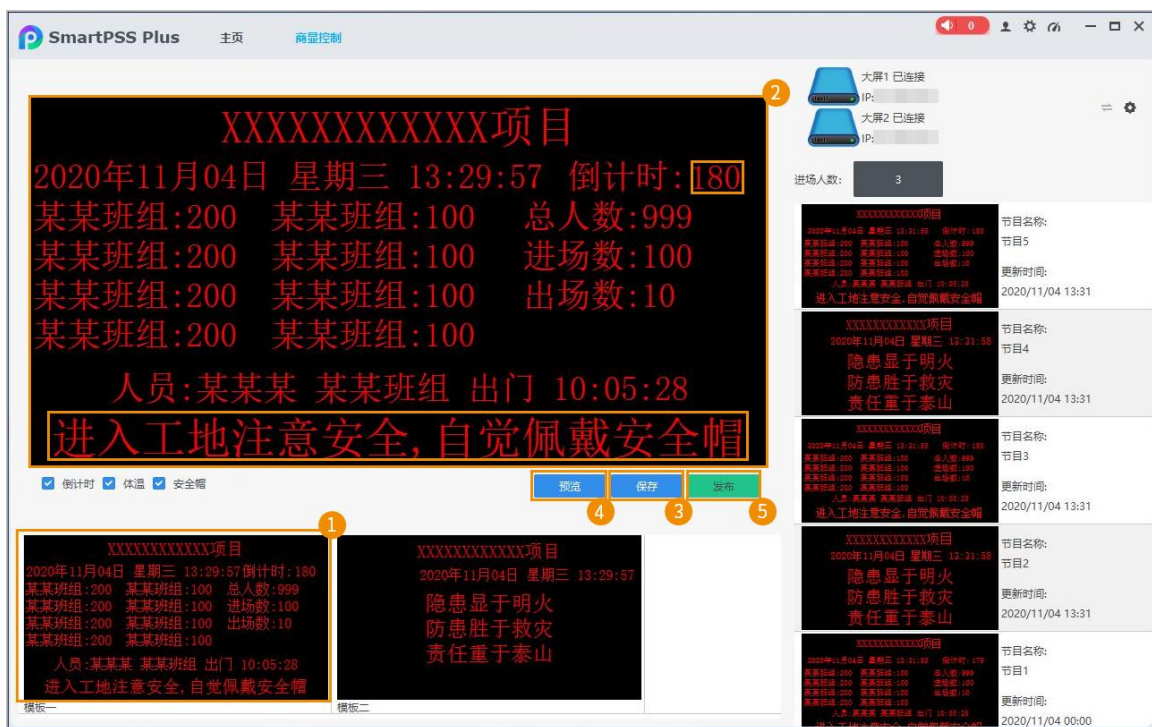
### 3.2.1 建节目

如果当前节目无法满足需求，可创建新的节目，将新节目发布到 LED 屏。



#### 操作步骤

- 步骤1 打开商显控制方案。
  - 步骤2 选择“主页 > 商显控制”。
  - 步骤3 创建节目并发布到 LED 屏。
    1. 在界面下方选择模板。
    2. 在上方按照实际情况设置标题、工期倒计时和提示信息。
    3. 单击“保存”，在界面右侧生成节目。
    4. 单击“预览”，预览显示到 LED 屏后的效果。
    5. 确认信息没有问题后，单击“发布”。
- 创建的节目信息显示到 LED 屏。

图3-5 创建节目并发布到 LED 屏



## 相关操作

- 修改节目名称：在“商显控制”界面将光标移动到需要修改名称的节目的右侧，单击出现的 ，在弹出的对话框设置节目名称，单击“确定”。
- 修改节目信息：在“商显控制”界面单击需要修改的节目，左侧节目编辑区修改节目信息，单击“保存”；然后单击“预览”，预览显示到 LED 屏后的效果；最后单击“发布”，LED 屏上显示修改后的节目信息。
- 删除节目：在“商显控制”界面将光标移动到需要删除的节目的右侧，单击出现的 ，根据提示完成删除操作。

### 3.2.2 切换商显控制器

SmartPSS Plus 支持将数据最多投放到两个 LED 屏。如果需要将信息投放到其他 LED 屏，请在 SmartPSS Plus 切换商显控制器为需要连接的 LED 屏对应的商显控制器。切换后，SmartPSS Plus 和原商显控制器将断开连接，原商显控制器对应的 LED 屏数据会保留，但不会实时更新，发布节目至切换后的商显控制器对应的 LED 屏，才会刷新实时数据。

步骤1 打开商显控制方案。

步骤2 选择“主页 > 商显控制”。


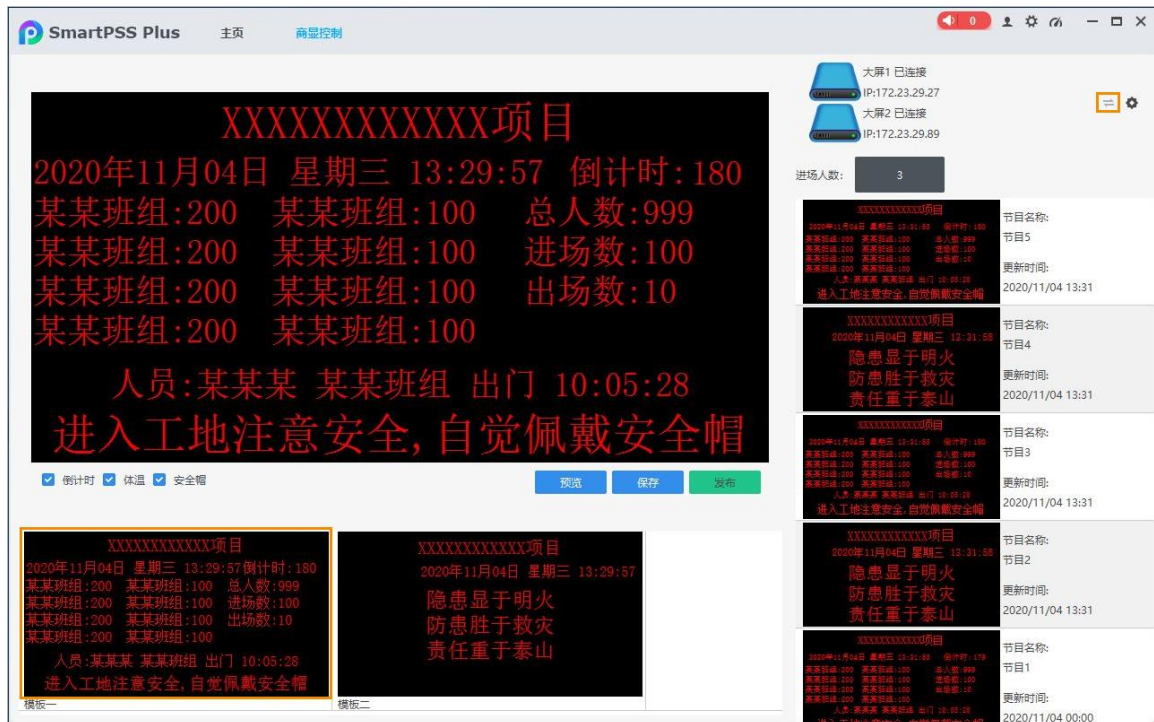
步骤3 在“商显控制”界面单击 ，在弹出的对话框填写需要切换的 LED 屏对应的商显控制器的 IP 地址和端口，单击“确定”，详细操作请参见 3.1 首次操作。

图3-6 切换商显控制器（1）



### 3.2.3 调节 LED 屏亮度


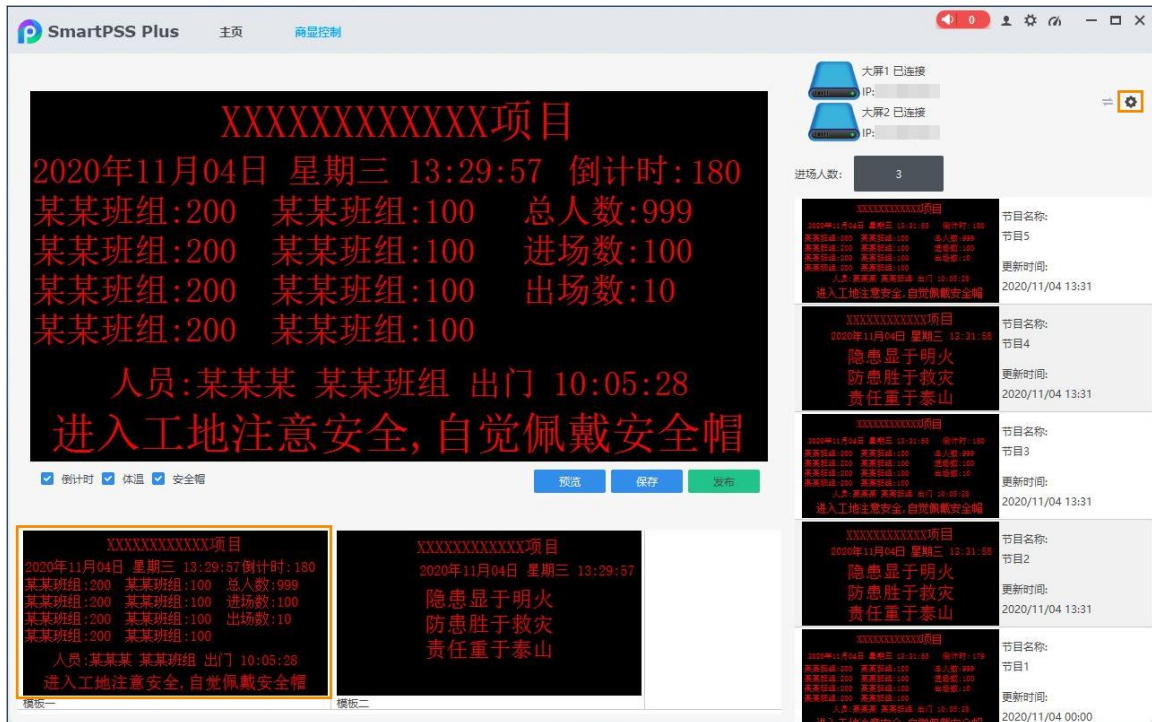
- 步骤1 打开商显控制方案。
  - 步骤2 选择“主页 > 商显控制”。
  - 步骤3 在“商显控制”界面单击 ，在弹出的对话框设置合适的亮度。
- 亮度调节在 LED 屏实时生效。

图3-7 设置 LED 屏亮度 (1)



步骤4 单击“保存”，配置生效。

图3-8 设置 LED 屏亮度 (2)



步骤5 单击 , 退出设置界面。

### 3.2.4 设置定时开屏或手动开屏

设置 LED 屏的打开时间，LED 屏只在设置的时间段内打开。同时也支持手动立即开屏。

步骤1 打开商显控制方案。

步骤2 选择“主页 > 商显控制”。


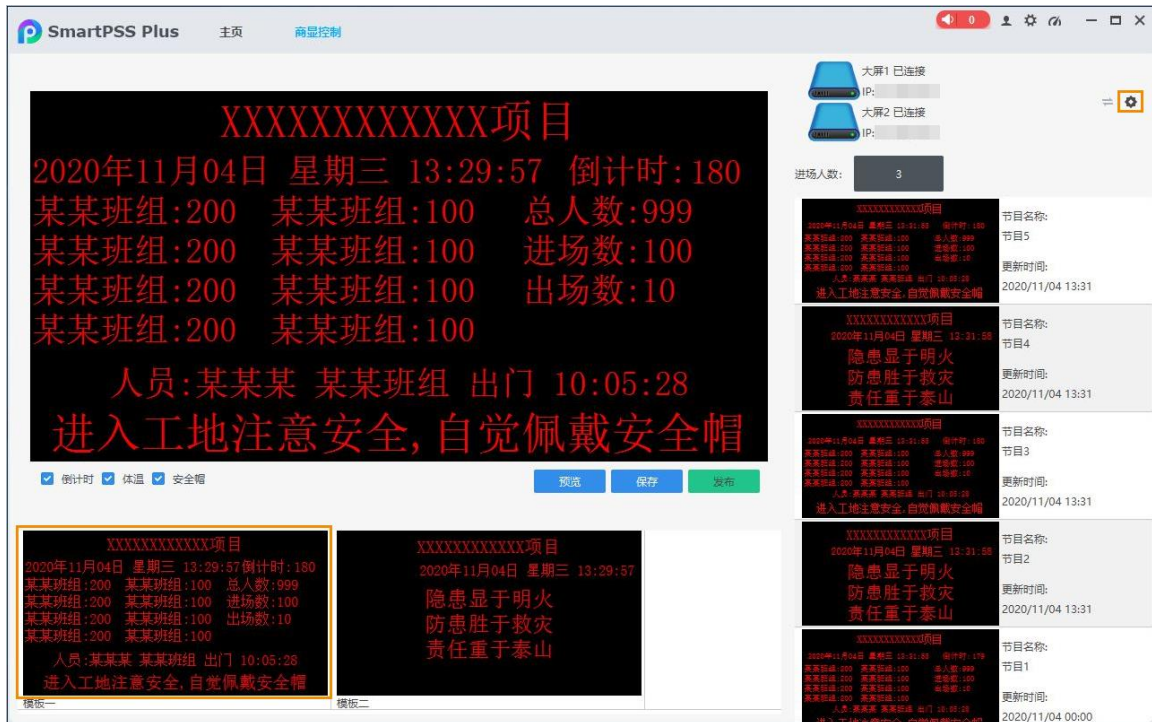
步骤3 在“商显控制”界面单击 .

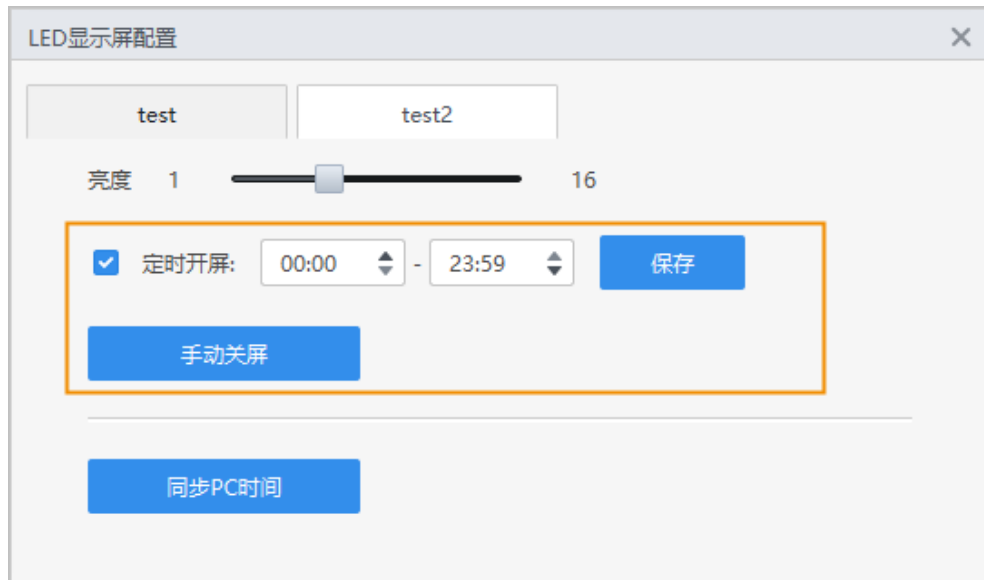
图3-9 设置定时开屏或手动立即开屏



步骤4 在弹出的对话框设置定时开屏或手动开屏。

- 设置 24 小时开屏：不选择“定时开屏”，单击“保存”。
- 设置定时开屏：选择“定时开屏”，设置开屏时间段，单击“保存”。
- 单击“手动开屏”，立即打开 LED 屏。

图3-10 设置开屏时间/手动开屏



步骤5 单击 ，退出设置界面。



## 附录1 法律声明

### 版权声明

© 2020 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

- 、、、、 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

- 产品请以实物为准，本文档仅供参考。
- 本公司保留随时维护本文档中任何信息的权利，维护的内容将会在本文档的新版本中加入，恕不另行通知。
- 本文档如有不准确或不详尽的地方，或印刷错误，请以公司最终解释为准。
- 本文档供多个型号产品做参考，每个产品的具体操作不逐一例举，请用户根据实际产品自行对照操作。
- 如不按照本文档中的指导进行操作，因此而造成的任何损失由使用方自行承担。

- 如获取到的 PDF 文档无法打开，请将阅读工具升级到最新版本或使用其他主流阅读工具。

## 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、财产损失、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. 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。

### 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。

- 启用设备的防火墙或者黑白名单功能，降低设备可能遭受攻击的风险。

## 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