SmartPSS Lite

User's Manual

V1.0.3

Foreword

General

This manual introduces the functions and operations of the SmartPSS Lite (hereinafter referred to as "the Platform"). Read carefully before using the platform, and keep the manual safe for future reference.

Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results.
TIPS	Provides methods to help you solve a problem or save time.
NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.3	• Updated the system settings function.	April 2023
V1.0.2	• Updated basic setting function. • Updated adding device function. • Updated device configuration function.	December 2022
V1.0.1	• Updated home page. • Updated data management function. • Updated backup and restore function.	August 2022
V1.0.0	First release.	April 2022

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by

implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Contents

Foreword I

1 Overview 1

2 Installation and Login 2

2.1 Installation 2

2.2 Initialization 2

2.3 Login 5

2.4 Password Reset 6

2.5 Feedback 6

3 Home Page 8

4 System Configurations 10

4.1 Basic Setting 10

4.2 Monitor Setting 11

4.3 Device Setting 12

4.4 Event Setting 12

4.5 Local Path 14

4.6 Data Management 14

4.7 Attendance Setting 15

4.8 Video Intercom Settings 16

4.9 Backing up and Restoring 17

5 Device Management 19

5.1 Adding Devices 19

5.1.1 Adding Device by Auto Search 19

5.1.2 Adding Device One by One 20

5.1.3 Importing Device in Batches 22

5.2 Deleting Devices 23

5.3 Exporting Devices 23

5.4 Editing Devices 23

5.4.1 Editing Devices 23

5.4.2 Initializing Devices 24

5.4.3 Changing IP Addresses 26

5.4.4 Configuring Devices 27

5.4.5 Alarm Configuration 31

6 Log Query 32

7 Event Configuration 33

8 Event Center 36

8.1 Overview.....36
8.2 Configuring Live View Video.....37
Appendix 1 Cybersecurity Recommendations.....39

1 Overview

SmartPSS Lite is a client software developed for small and medium-sized solutions. You can download various solutions as needed. This manual introduces the general functions and operations.

2 Installation and Login

2.1 Installation

Contact technical support or download ToolBox to get the SmartPSS Lite.

- If you get the software package of the SmartPSS Lite, install and run the software according to page instructions.
- If you get the software by the ToolBox, run the SmartPSS Lite according to page instructions.

2.2 Initialization

Initialize SmartPSS Lite when you log in for the first time, including setting a password for login and security questions for resetting password.

Procedure

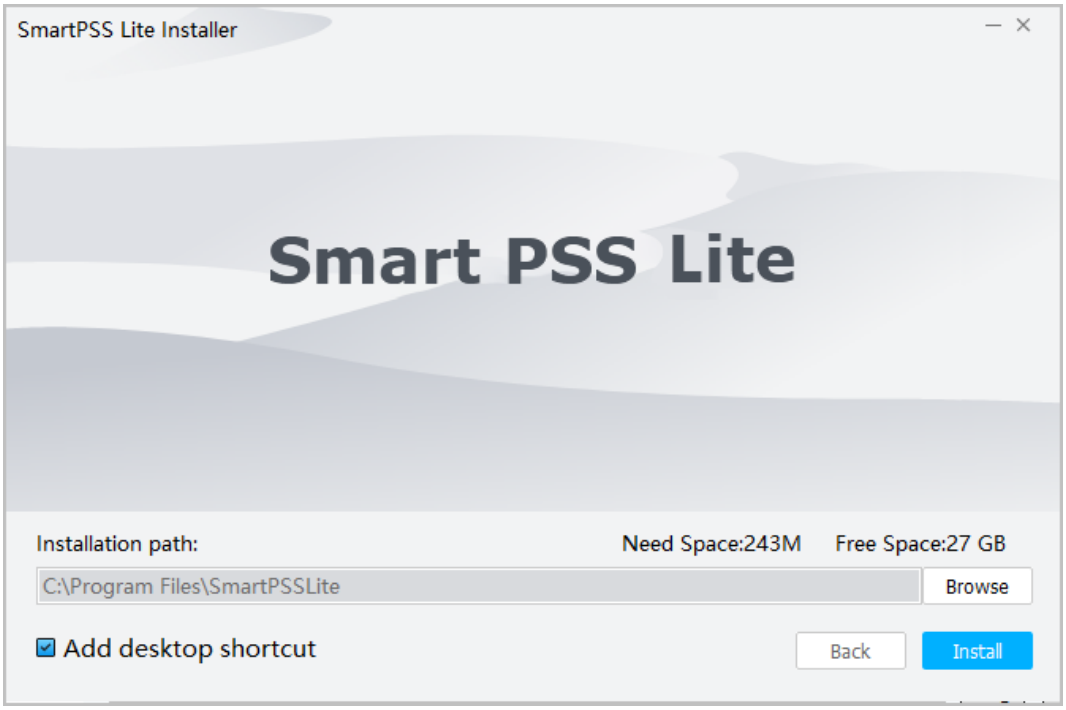
Step 1 Double-click SmartPSSLite.exe, or click **Open** next to the software icon in the ToolBox.

Step 2 Select the language from the drop-down list, select **I have read and agree the software agreement** , and then click **Next**.

Figure 2-1 Select language

Step 3 Click **Browse** to select installation path, and then click **Install**.

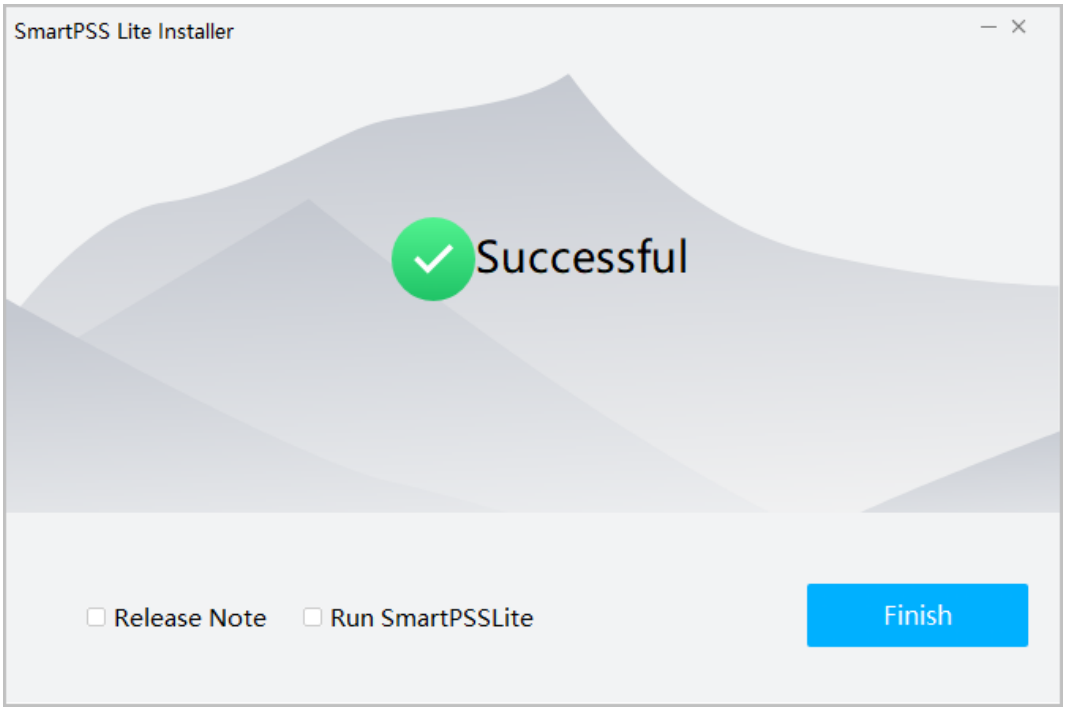
Figure 2-2 Select installation path



Step 4 Click **Finish** to complete the installation.

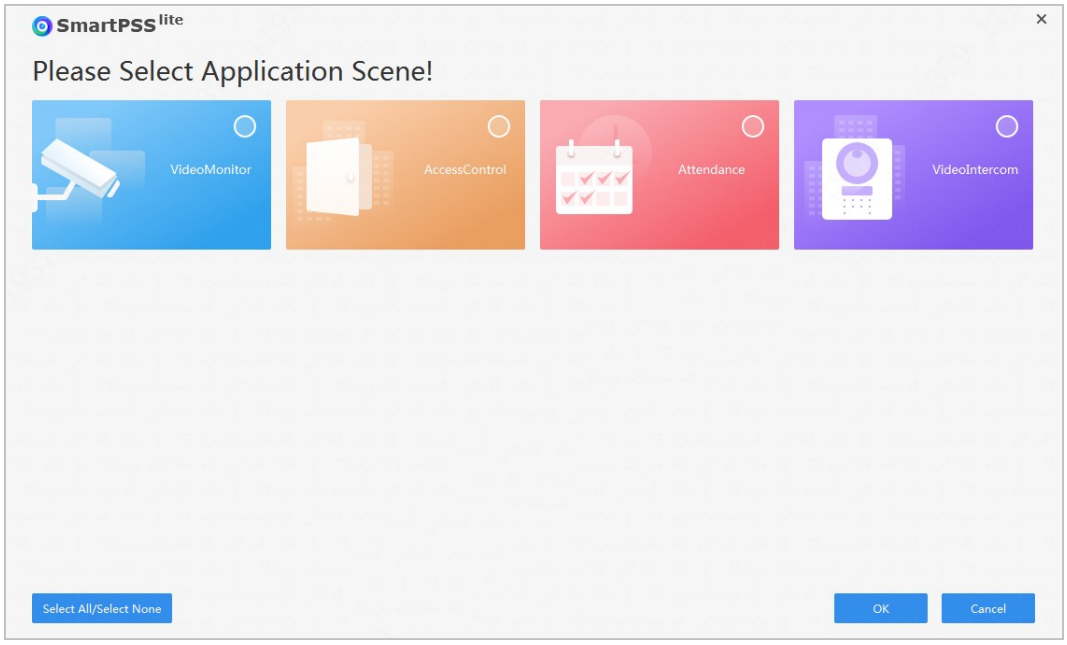
Select **Run SmartPSSLite** to start SmartPSS Lite.

Figure 2-3 Install complete



Step 5 Select the application scenes you want to add, and then click **OK**.

Figure 2-4 Select application scenes



Step 6 Click **Agree and Continue** to agree **Software License Agreement** and **Product Privacy Policy**.

Step 7 Set password on the **Initialization** page, and then click **Next**.

Figure 2-5 Set password

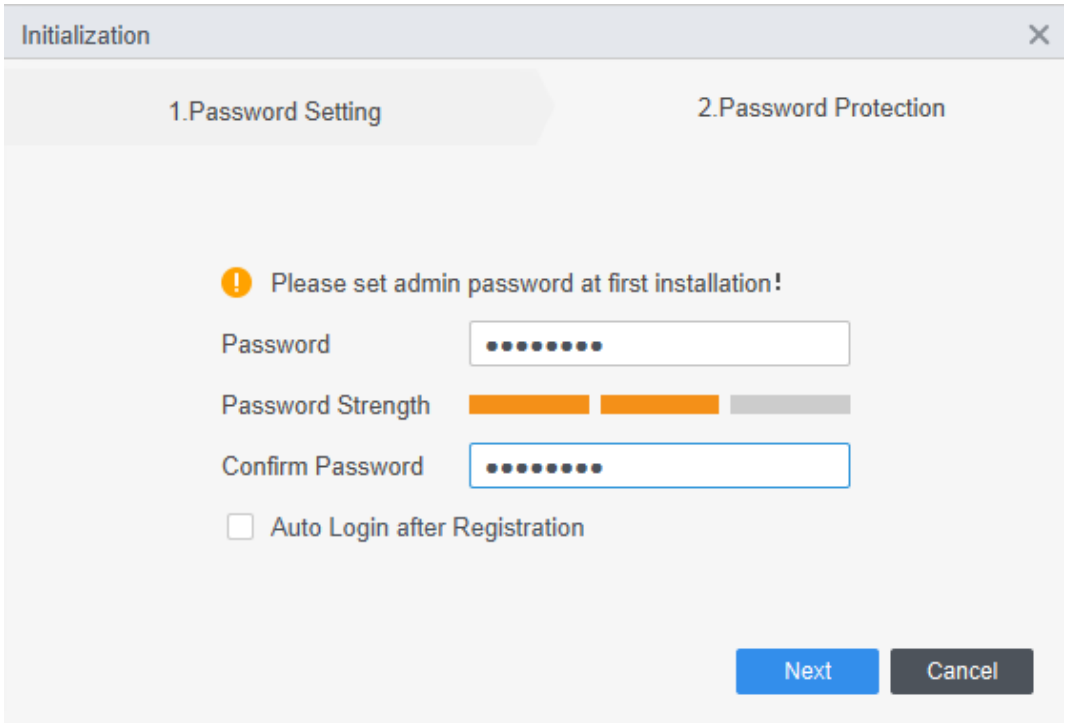
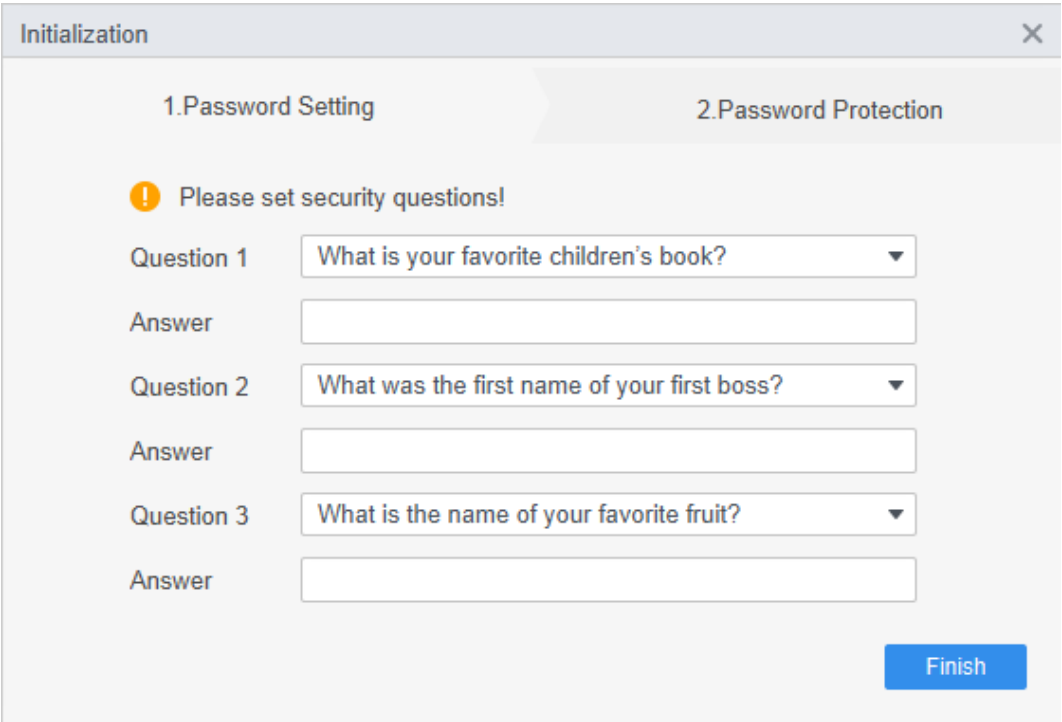


Table 2-1 Initialization parameters

Parameter	Description
Password	The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among uppercase, lowercase, number, and special character (excluding ' " ; : &).
Password Strength	Display the effectiveness of a password against guessing or brute-force attacks. Green means the password is strong enough, and red means less strong. Set a password of high security level according to the password strength prompt.
Confirm Password	Enter the password again to confirm the password.
Auto Login after Registration	Enable **Auto Login after Registration** so that the SmartPSS Lite will log in automatically after initialization; otherwise the login page is displayed.

Step 8 Set security questions, and then click **Finish**.

Figure 2-6 Set security questions



2.3 Login

Procedure

Step 1 Double-click SmartPSSLite.exe, or click **Open** next to the software icon in the ToolBox.

Step 2 Enter username and password, and then click **Login**.

If multiple networks are available on your computer, you can select one from them.

Figure 2-7 Login

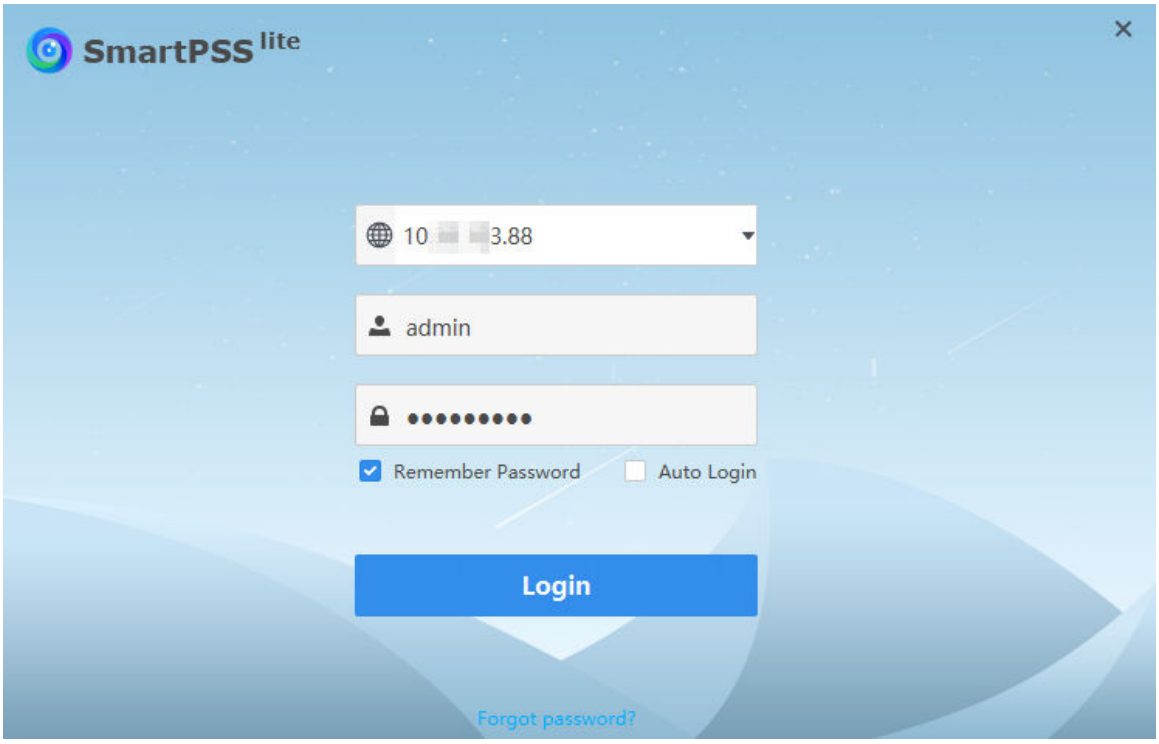


Table 2-2 Parameters of login

Parameter	Description
Remember Password	Enable **Remember Password** so that you do not need to enter the password again when logging in next time.
Auto Login	Enable **Auto Login** so that the SmartPSS Lite will log in automatically the next time when you use the same user account.
Forgot password?	Click **Forgot password?** to reset password through security questions when you forget the password.

2.4 Password Reset

You can reset the password by answering the security questions.

Procedure

Step 1 Double-click SmartPSSLite.exe, or click **Open** next to the software icon in the ToolBox.

Step 2 Click **Forgot password?** on the login page.

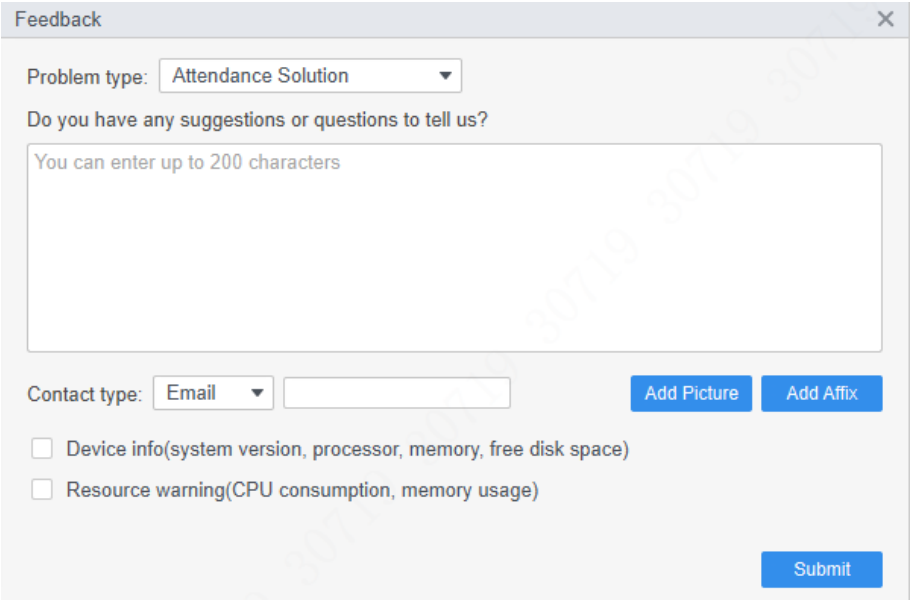
Step 3 Answer the security questions, and then click **Next**.

Step 4 Reset password according to page instructions.

2.5 Feedback

If you have any suggestion, on the upper right corner of the page, select > **Feedback** , and then you can enter suggestions (words), upload pictures and attachments, and then click **Submit**.

Figure 2-8 Feedback



3 Home Page

The homepage consists of 9 parts.

Figure 3-1 Home page

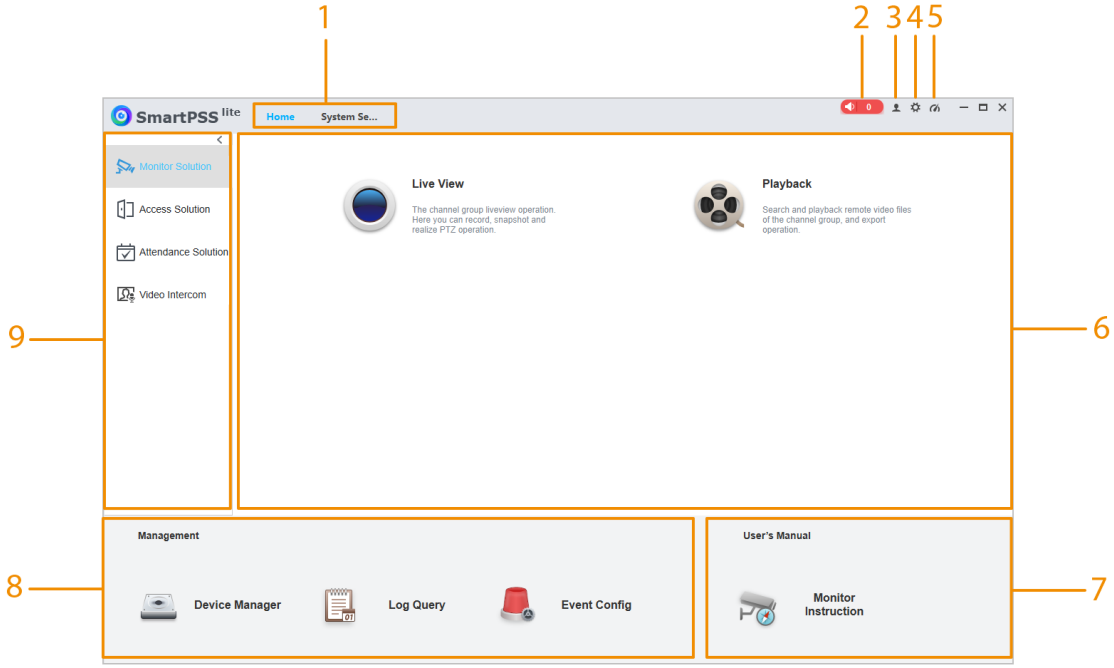


Table 3-1 Parameters of home page

No.	Parameter	Description
1	Function tab	Display the home page by default. When you click on a function for the first time, the function tab is added here.
2	Alarm sound	Click or to turn on or turn off the alarm sound. The number on the icon means the number of alarm events that are reported but unprocessed. Click the number to open the **Event Center** to view the details of alarm events. For details, see “8 Event Center”.
3	User management	• Click , and then select **User Manager** to manage users, such as add role/user, delete role/user and set permissions. • Click , and then select **Lock Screen** to lock screen. Enter password of login account when you want to unlock. • Click , and then select **Switch User** to return to the login page. You can log in with new account. • Click , and then select **Help Manual** to get the user’s manual.

No.	Parameter	Description
		• Click , and then select **About** to view the system version, date, **Opensource Statement** and **Software license agreement**. Enable **Open Debugging Log** so that the debugging logs are saved automatically to a local path, for locating and problems solving.
4	System configuration	Configure basic setting, monitoring setting and other parameters. For details, see “4 System Configurations”.
5	System status	Click to view the using status of CPU and RAM. If the CPU usage is high, the icon turns red.
6	Function module	Click the function icon to go to the function page.
7	User's Manual	Click the icon to get the user's manual of the corresponding solution.
8	Management	• **Device Manager** : You can add devices, remotely configure the device, modify IP address and more. • **Log Query** : You can query and export the log information of the platform and device. • **Event Config** : Configure alarm linkage actions.
9	Solution module	Select the needed solution. Click > or < to display or hide solutions.

4 System Configurations

4.1 Basic Setting

Configure the time, language, theme and other functions of the platform.

Procedure

Step 1 Select ⚙ > **System Config** > **Basic setting** .

Step 2 Configure basic setting parameters.

Figure 4-1 Basic setting

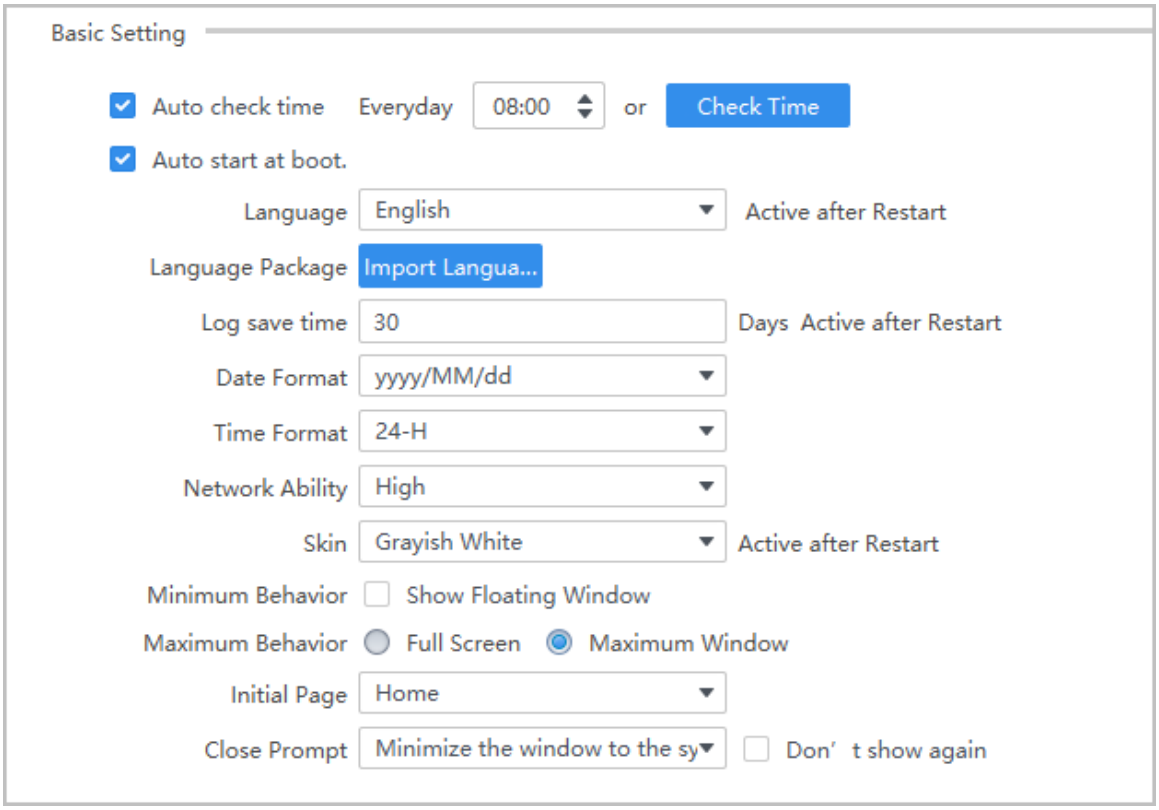


Table 4-1 Description of basic setting parameters

Parameters	Description
Timing	Enable **Auto Check Time Everyday** , set **Check Time**, the device will automatically check the time automatically at the scheduled time.
Auto start at boot	Automatically opens the platform at startup.
Language	Display the language of the platform after it restarts.
Language Package	Import the language packages. Restart the platform after the language package is imported.

Parameters	Description
Log save time	Set the save time for logs. This function will be activated after the system is restarted. For example, set the save time as 30, then the logs of the last 30 days will be saved.
Data Format	Select the format data is displayed in.
Time Format	Select the format time is displayed in.
Network Ability	Select the network ability according to your network conditions. For example, when the network connection is strong, you can select **High**.
Skin	Select the skin which is activated after restart. The default setting is grayish white. If we can change this to Theme, then set use theme for all of these. But if we can't, then leave it as Skin.
Minimum Behavior	Select **Show Floating Window**, and after the platform is minimized, will be displayed showing the number of alarm events.
Maximum Behavior	Select **Full Screen** to hide the taskbar; select **Maximum Window** to show the taskbar.
Initial Page	Select the function tab that is opened by default when the platform starts. You can select **Home** or **Resume last page**.
Close Prompt	A prompt will automatically pop up when the platform is closed. Select **Don't show again** if you do not need the prompt.

Step 3 Click **Apply**.

4.2 Monitor Setting

Configure default system type, instantly replay time, local record time and other functions.

Procedure

Step 1 Select > **System Config** > **Monitor setting** .

Step 2 Configure monitor setting parameters.

Figure 4-2 Monitor setting

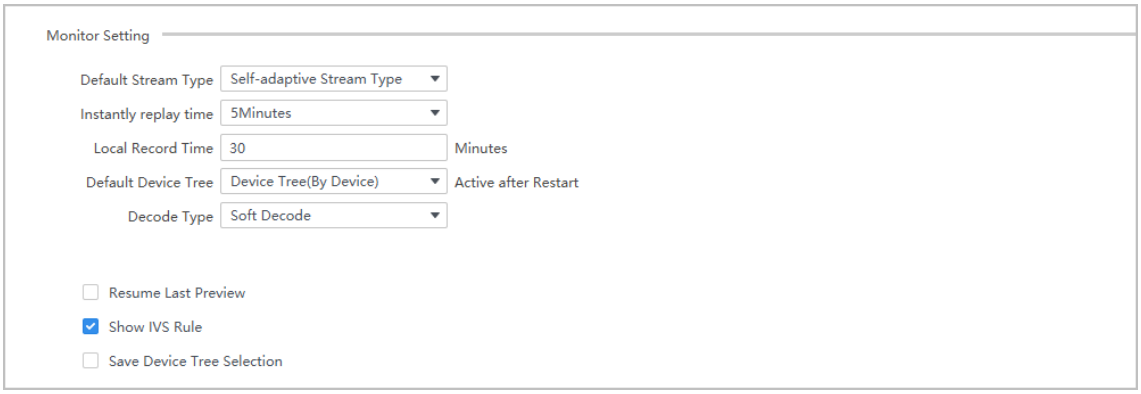


Table 4-2 Description of monitor setting parameters

Parameter	Description
Default Stream Type	Select the real-time default stream type. You can select from **Self-adaptive Stream Type** , **Sub Stream** and **Main Stream**.
Instantly replay time	Select the instantly replay time. For example, if the value is set to 5 minutes, the previous 5 minutes will be played back.
Local Record Time	Select the local record time. For example, if the value is set to 30 minutes, the system records a video for 30 minutes and then automatically saves the video to the default path on the computer. The default path is \Data\User\Record.
Default Device Tree	• Device Tree (By device): Display with the device as a node. • Region Tree (By Channel): Display with the channel as a node.
Decode Type	• **Soft Decode** : Decode through CPU. • **Hardware Decode** : Decode videos through graphics cards.
Resume Last Preview	After enabling this function, the platform automatically open the last preview after restarting the platform.
Show IVS Rule	After enabling this function, the IVS rules will be displayed on the monitoring screen.
Save Device Tree Selection	This function is not supported currently.

Step 3 Click **Apply**.

4.3 Device Setting

Select **System Settings** > **Device Settings** , and then click **Auto Login Device (Active after Restart)** to automatically log in to the platform when you start it.

4.4 Event Setting

Configure the alarm sound and link the sender and receiver of the email.

Procedure

Step 1 Select ⚙ > **System Config** > **Event** .

Step 2 Configure event setting parameters.

Figure 4-3 Event setting

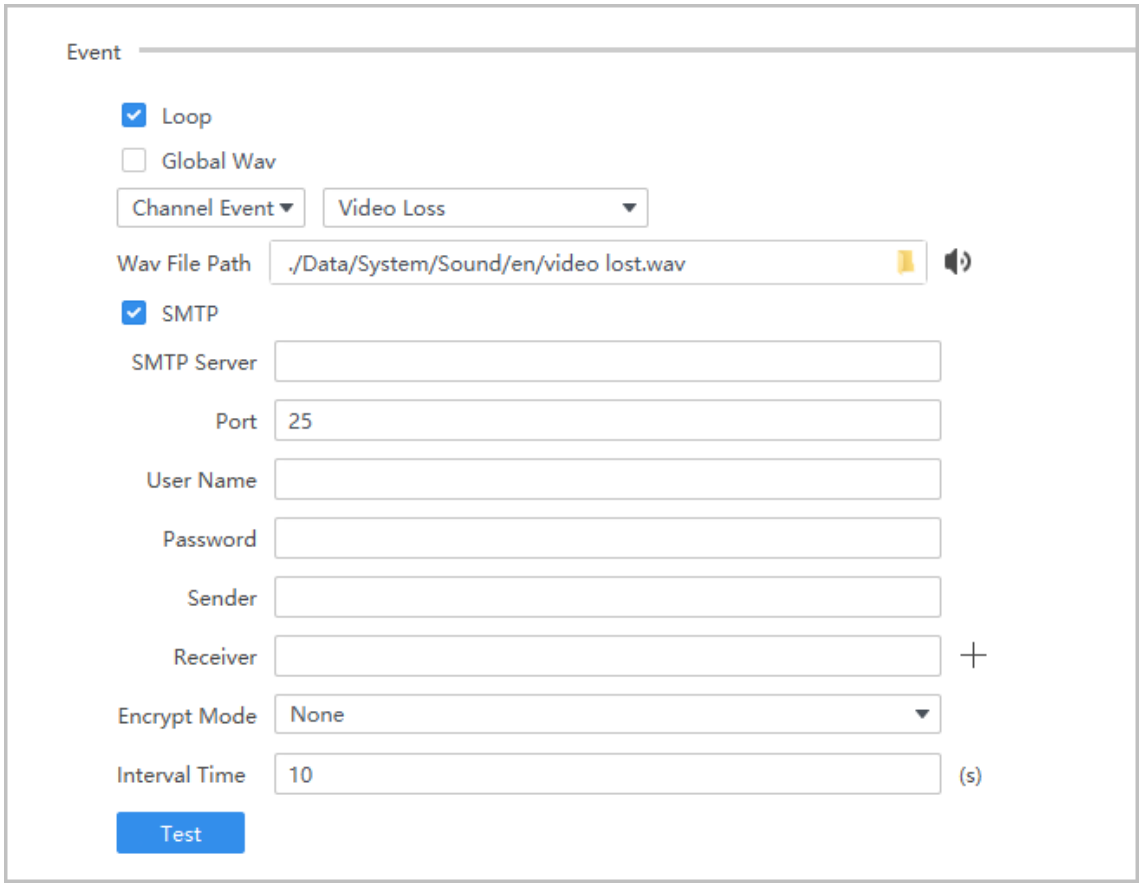


Table 4-3 Description of event setting parameters

Parameter	Description
Loop	After enabling this function, the alarm sound will be looped once an event occurs.
Global Wav	• Select **Global Wav** , and then select the sound file in the **Wav File Path**. The sound will be played after the corresponding event is triggered. • Do not select **Global Wav,** and then select the event type and sound type in the drop-down list or select the sound file in the **Wav File Path**. The sound will be played after the corresponding event is triggered.
SMTP	When you need to link email sending, enable SMTP function. • SMTP Server: SMTP (Simple Mail Transfer Protocol) server address. • Port: The port number of the SMTP server. • User Name: The account of SMTP server. • Password: The password of SMTP server. • Sender: The email address of the sender. • Receiver: The email address of the receiver. Supports 5 addresses at most. After entering the receiver's email address, click **Test** to test whether the emails can be sent and received.

Parameter	Description
	• Encrypt Mode: Select from **None** , **SSL** (Secure Sockets Layer) and **TLS** (Transport Layer Security). • Interval Time: The platform sends alarm information according to the set interval time.

Step 3 Click **Apply**.

4.5 Local Path

Set the save path for the pictures, videos and other data collected by the platform.

Procedure

Step 1 Select ⚙ > **System Config** > **Local Path** .

Step 2 Set the local path.

Figure 4-4 Set local path

Step 3 Click **Apply**.

4.6 Data Management

Periodically extract the attendance data from devices, and periodically clear the data, pictures and videos saved on the computer.

Procedure

Step 1 Select ⚙ > **System Config** > **Data Management** .

Step 2 Configure data management parameters.

Figure 4-5 Data management

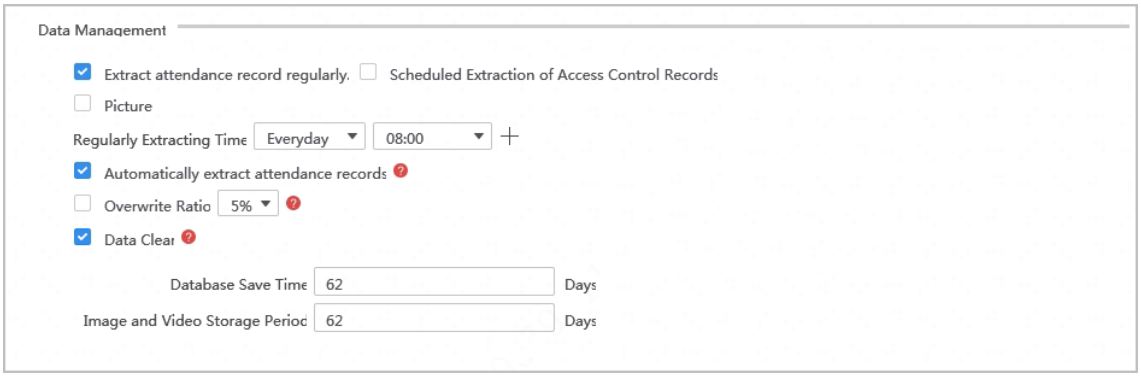


Table 4-4 Description of data management parameters

Parameter	Description
Extract attendance record regularly	The platform automatically extracts attendance and access control records and pictures according to the setting time. ● For attendance devices, extract the attendance data directly. For access controllers, set the device as attendance point in advance and then extract the attendance data. For details, see *SmartPSS Lite Attendance Solution User's Manual*. ● If you set **Regularly Extracting Time** as **Everyday**, you can select five time points. ● If you set **Regularly Extracting Time** as **Every Week**, you can select a certain time point on a certain day.
Scheduled Extraction of Access Control Records	
Auto extraction	Enable **Auto extraction** function, and then the platform will automatically extract attendance records or access control records.
Overwrite Ratio	Enable **Overwrite Ratio** function, and then configure the ratio. When the disk is full, the system will automatically overwrite the oldest images and videos according to the ratio.
Data Clear	Configure the save time of database, pictures and videos according to actual requirements. The platform automatically clears data and pictures that exceed the saving time. It triggers at 00:00 each day or when the software is started. This data does not include temperature monitoring data.

Step 3 Click **Apply**.

4.7 Attendance Setting

You need to enable **Attendance Summary SMTP Setting** function if you want to regularly send attendance summary to your email.

Procedure

Step 1 Select ⚙ > **System Config** > **Attendance Setting** .

Step 2 Configure the attendance settings.

Figure 4-6 Attendance settings

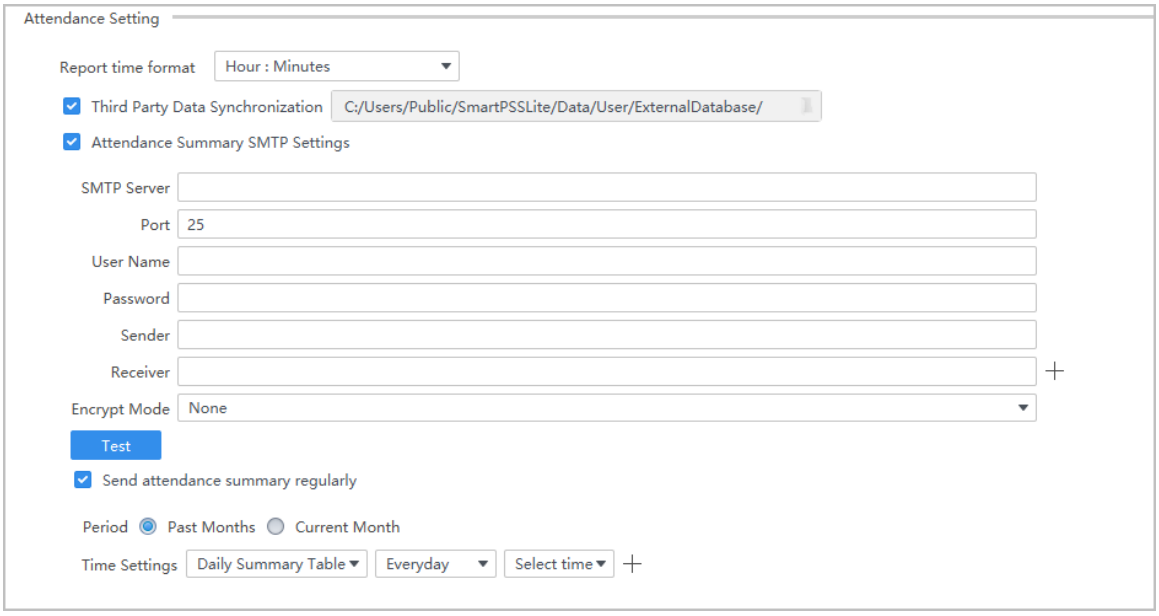


Table 4-5 Attendance setting parameters

Parameters	Description
Attendance Setting	● Report Time Format: Define the time format of attendance reports. For example, if it is set as **Hour: Minutes**, the time of attendance in a report will be displayed in the format of hour and minutes. ● Third Party Data Synchronization: Synchronize the attendance data to the defined file path. ● Attendance Summary SMTP Settings: Send attendance summary to the email that was set. Click **Test** to send a test email to the designated address. ● Third Party Data Synchronization: Synchronize attendance data to the defined file path. ● Attendance Summary SMTP Settings: Send attendance reports to the email that was set. ◇ Test: Test whether the email address is working. ◇ Send attendance summary regularly: Sends the attendance summary regularly to the set email address.

Step 3 Click **Apply**.

4.8 Video Intercom Settings

Procedure

Step 1 Select ⚙ > **System Config** > **Video Intercom** .

Step 2 Configure the attendance settings.

Figure 4-7 Video intercom

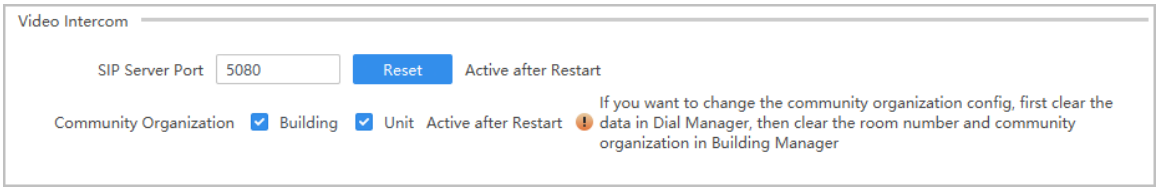


Table 4-6 Video intercom parameters

Parameters	Description
Server Port	The server port of the platform when it functions as the SIP server. The server port can be customized.
Community Organization	Set the organization level. ● Building: The organization only includes buildings. ● Unit: The organization includes buildings and units. The configuration will take effect after the platform is restarted. If you want to change the level of the organization, but the organization was already created before, go to **Video Intercom** > **Intercom Config** > **Dial Management** and clear the existing data from there, and then go to **Building Manager** to clear the remaining data.

Step 3 Click **Apply**.

4.9 Backing up and Restoring

Backup and restore platform configuration.

Procedure

Step 1 Select ⚙ > **System Config** > **Backup and Restore** .

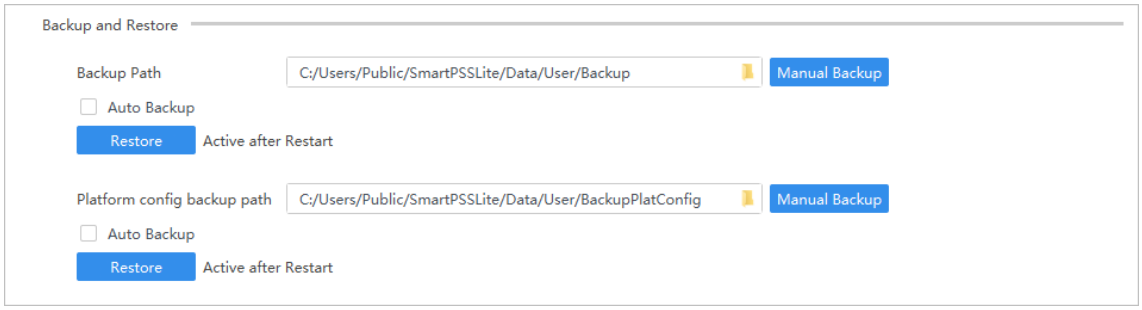
Step 2 Backup configurations and platform configurations to the computer. The platform supports to backup automatically and manually.

- Backup manually: Back up all data of the platform, including configuration, events, logs and more. Select the backup path, and then click **Manual Backup**.
- Backup automatically: Only back up the configuration information set by the users. Select the backup path, and then enable **Auto Backup**.

Step 3 Click **Restore**, and then select the backup file that you need.

Configurations will restore the file configurations.

Figure 4-8 Backup and restore



Step 4 Click **Apply**.

5 Device Management

The SmartPSS Lite allows for adding devices. You can remotely configure and operate the devices after adding by the SmartPSS Lite.

5.1 Adding Devices

There are several methods available to add devices.

- Automatically search
- Manually adding
- Import in batches

5.1.1 Adding Device by Auto Search

Background Information

- We recommend you add devices by automatically search when you need to add devices in batches within the same network segment, or when the network segment is known but the exact IP addresses of devices are not known.
- Close ConfigTool and DSS when you configure devices; otherwise, you may not be able to find all devices.

Procedure

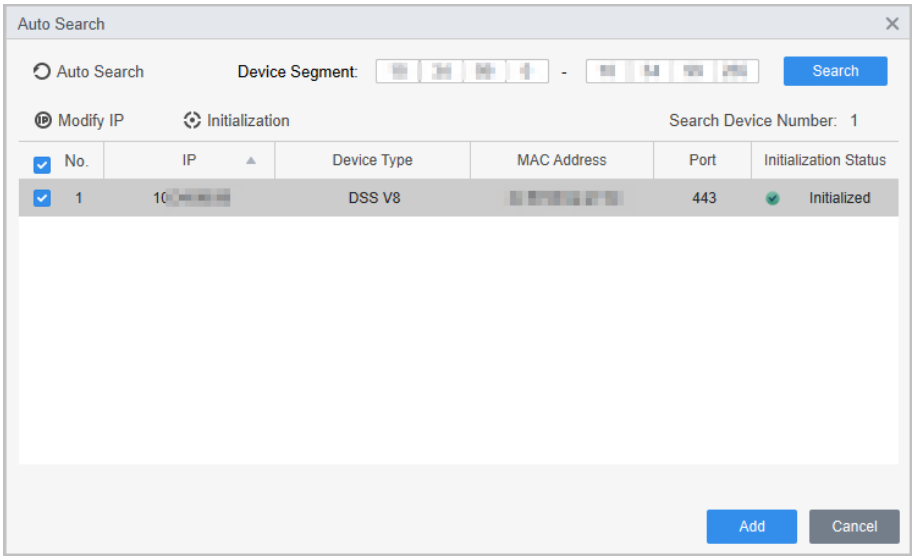
Step 1 Click **Auto Search** on the **Device Manager** page.

Step 2 Set the range of network segment, and then click **Search**.

The list of searched devices is displayed.

- Click **Auto Search** to refresh the search results.
- Click one needed device and then click **Modify IP** to change the IP address, subnet mask and gateway. For details, see “5.4.3 Changing IP Addresses”.
- Click one uninitialized device and then click **Initialization**. You can reset IP address, sub mask, gateway and login password. For details, see “5.4.2 Initializing Devices”.

Figure 5-1 Search results



Step 3 Click the devices, and then click **Add**.

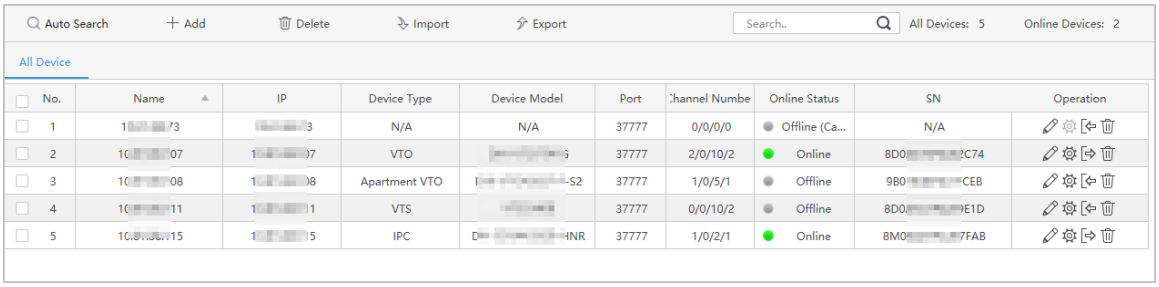
Step 4 Enter the login user name and password, and then click **OK** to confirm.

- The **Auto Search** page is still displayed after adding devices. You can continue to add or click **Cancel** to exit.
- Devices will be logged in automatically after adding. If the login is successful, the status displays as online; otherwise it is offline.

Results

After the devices are successfully added, they are displayed on this page.

Figure 5-2 Added devices



5.1.2 Adding Device One by One

We recommend you add devices manually when you need to add one single device with a known IP address or domain name.

Procedure

Step 1 Select **Add** on the **Device Manager** page.

Step 2 Set device parameters.

- Add devices through IP/Domain.

Figure 5-3 Add device manually

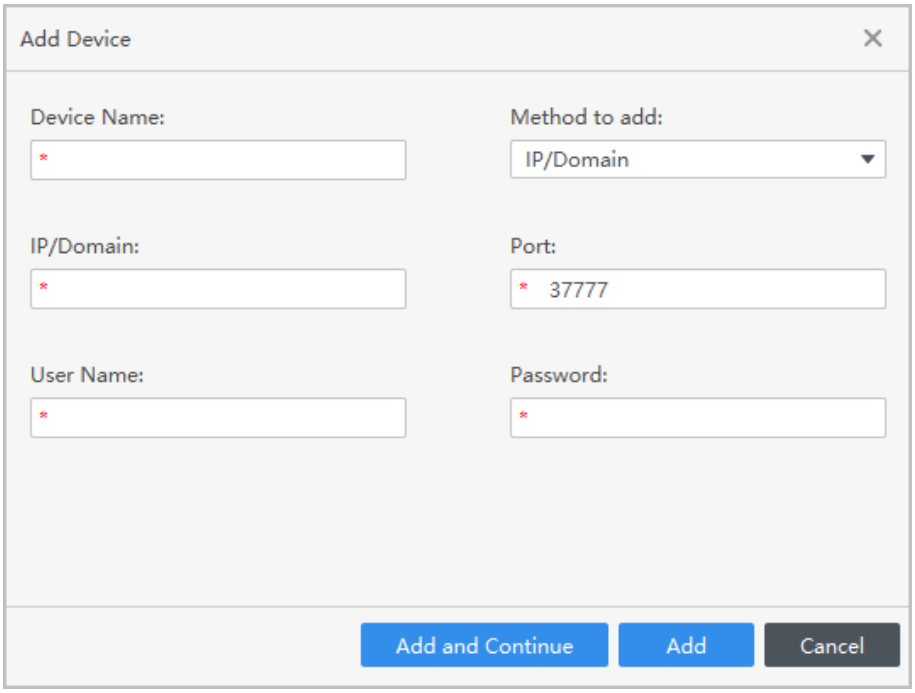


Table 5-1 Parameters of IP adding

Parameter	Description
Device Name	We recommend you name devices with the monitoring area for easy identification.
Method to add	Select **IP/Domain**.
IP/Domain	Enter the IP address or domain name of the device.
Port	Enter the port number, and the port number is 37777 by default. The actual port number might differ according to different models.
User Name	Enter the login user name.
Password	Enter the login password.

- Add devices through SN.

Figure 5-4 Add devices through SN

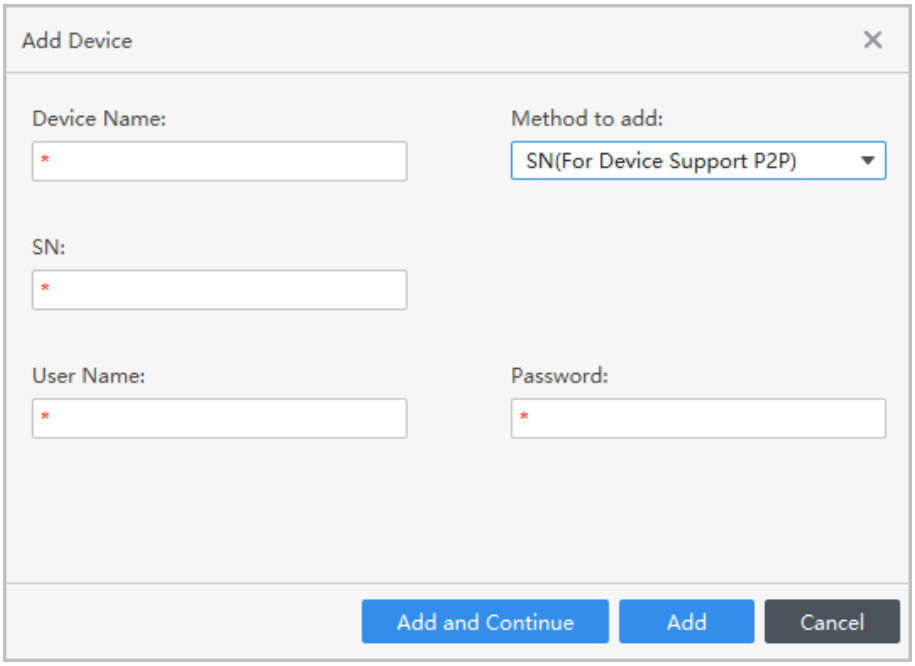


Table 5-2 Parameters of SN adding

Parameter	Description
Method to add	Select **SN (For Device Support P2P)**.
SN	Enter the serial number of the device.

Step 3 Click **Add** to add the device, and then close the **Add Device** page; or click **Add and Continue** to add the device and stay on the **Add Device** page so that you can add another device conveniently.

5.1.3 Importing Device in Batches

When you need to add devices in batches but they are not on the same network segment, we recommend you add devices by importing them to the platform. Organize the device information as a file in .xml format, and then import the file. You can export the template of device information. Select a device and click **Export**.

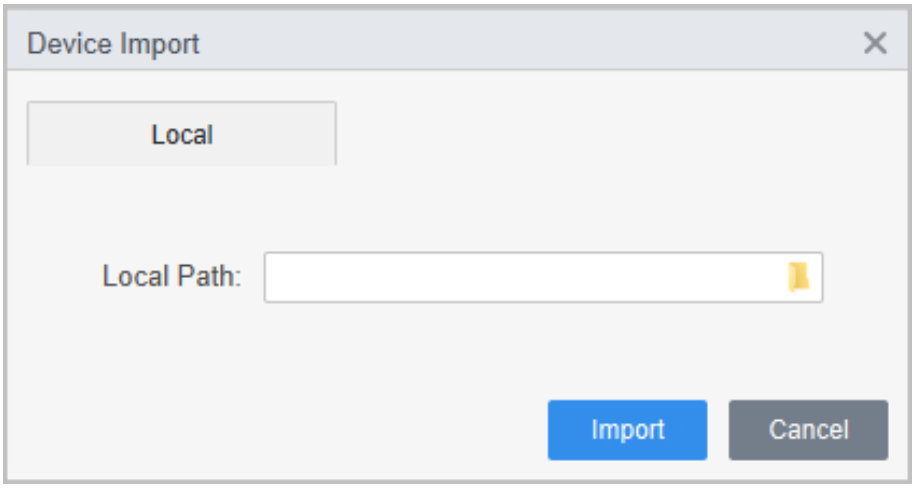
Procedure

Step 1 Click **Device Manager** > **Import** .

Step 2 Select the information file, and then click **Import**.

Devices will be logged in automatically after adding. If the login is successful, the status displays as online; otherwise it is offline.

Figure 5-5 Import device information in .xml format



5.2 Deleting Devices

Procedure

Step 1 Select **Device Manager** on the home page.

Step 2 Select the device that you do not need any more, and then click **Delete** or on the right side of device.

Step 3 (Optional) select **At the same time delete the device snapshot and video** if you do not need those snapshots and videos.

Step 4 Click **OK**.

5.3 Exporting Devices

You can export device information to local.

Procedure

Step 1 Select **Device Manager** on the home page.

Step 2 Select the device which needs to be exported, and then click **Export** on the **Device Manager** page.

Step 3 Select the local path of export, and then click **Export**.

5.4 Editing Devices

5.4.1 Editing Devices

You can modify the information of added device.

Procedure

Step 1 Select **Device Manager** on the home page.

Step 2 Click on the right side of the selected device or double-click the device.

Step 3 Edit device information.

Step 4 Click **Save**.

5.4.2 Initializing Devices

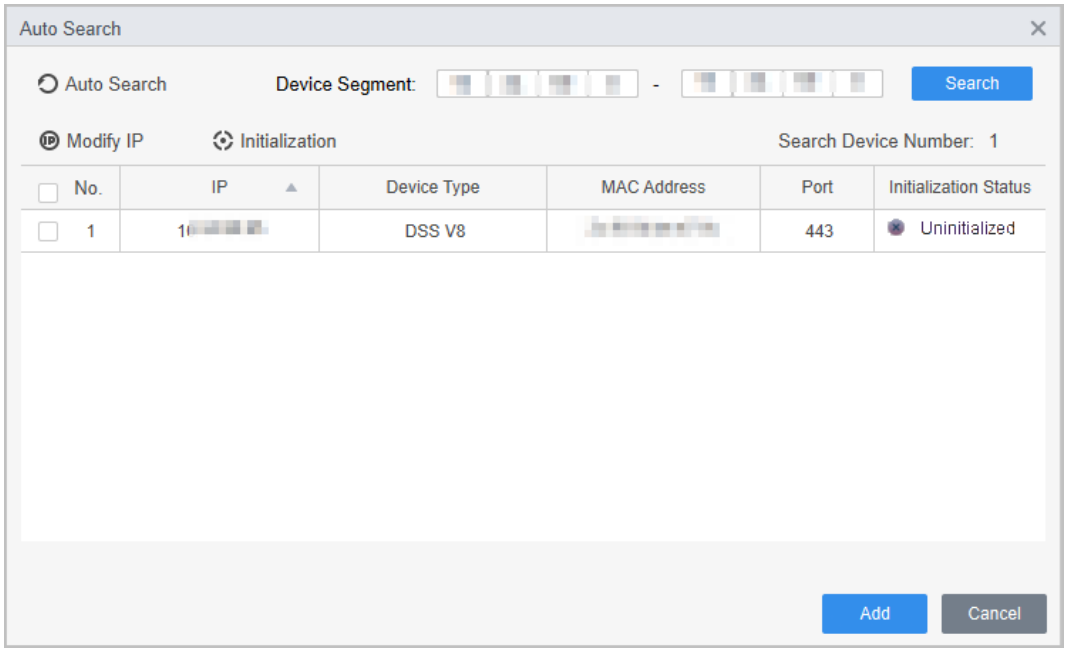
You can only initialize devices which are on the same network segment as the computer.

Procedure

Step 1 Click **Device Manager** > **Auto Search** .

Step 2 Set the range of network segment, and then click **Search**.

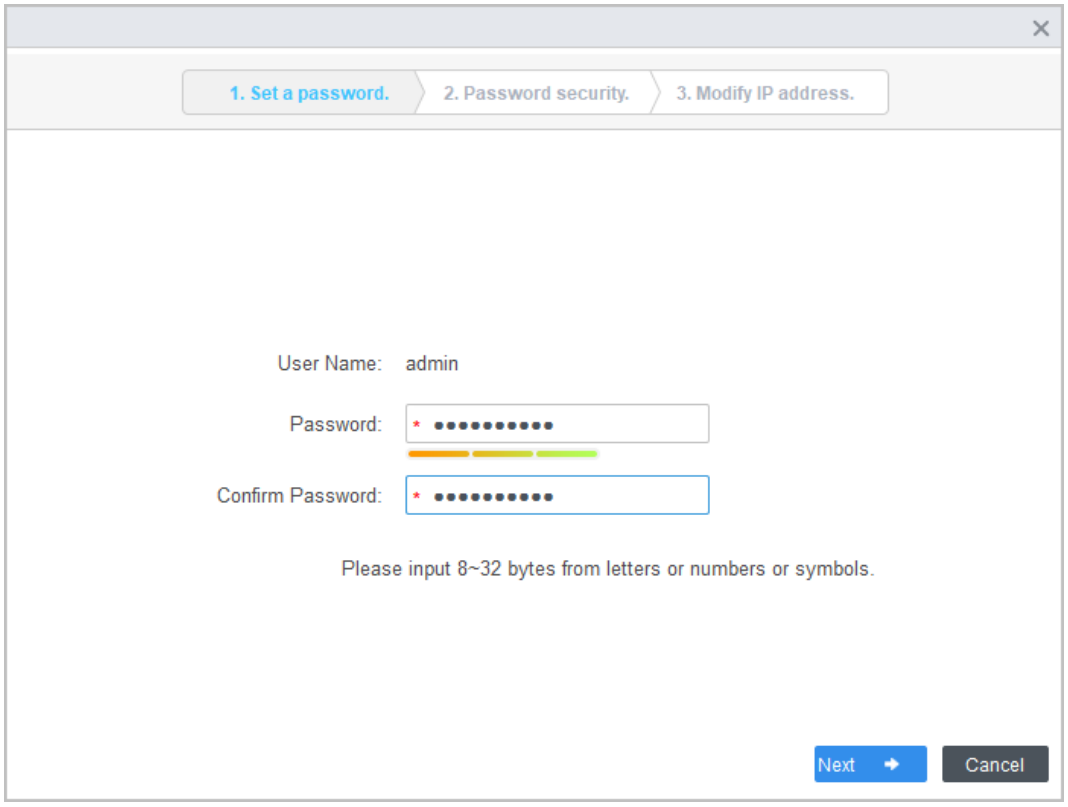
Figure 5-6 Device list



Step 3 Select the uninitialized device, and then click **Initialization**.

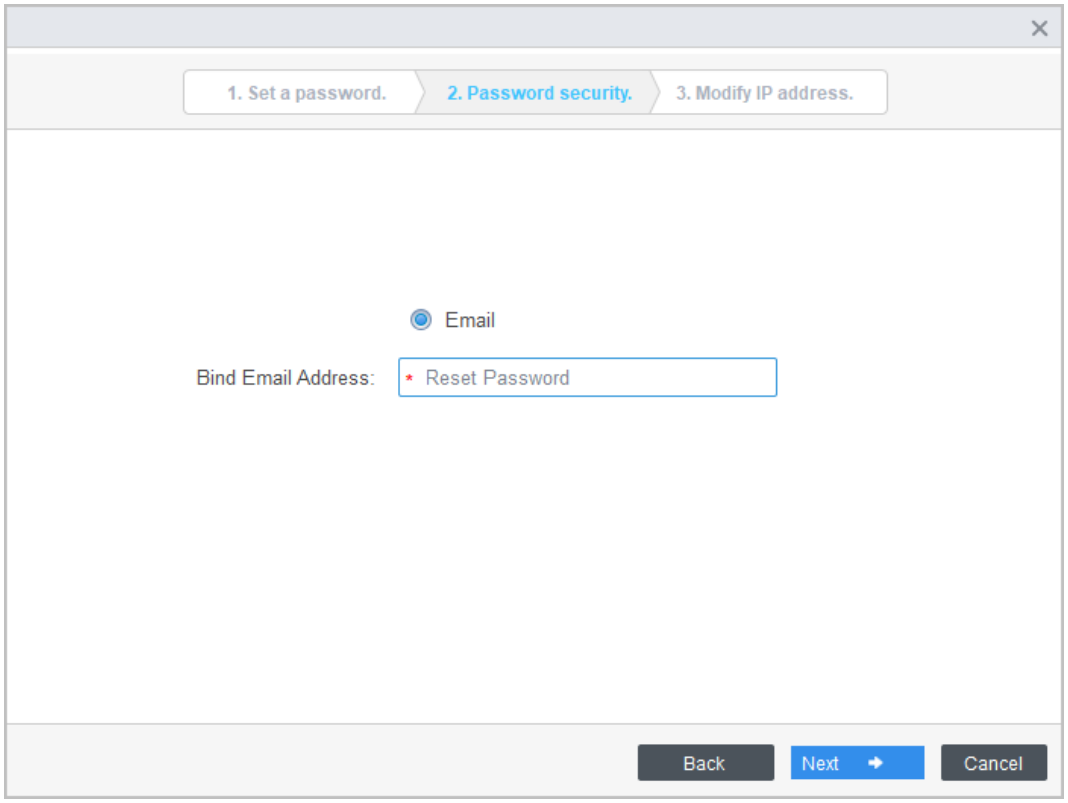
Step 4 Set password, and then click **Next**.

Figure 5-7 Set password



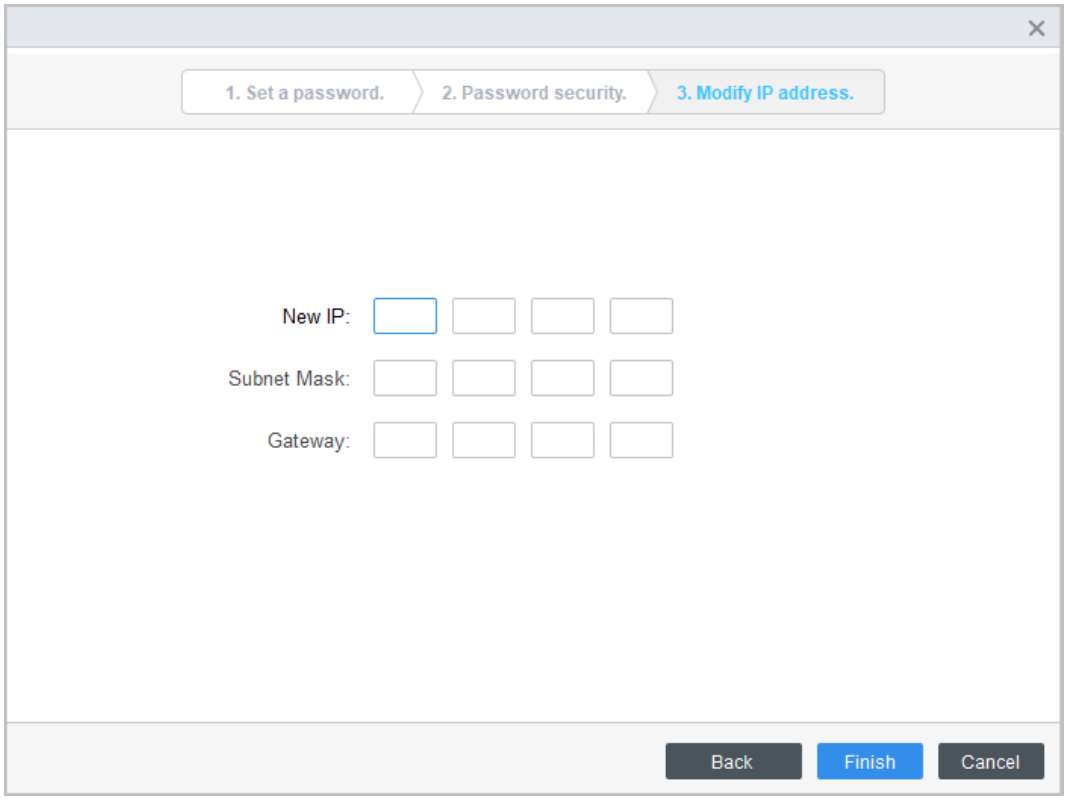
Step 5 Enter email address for password resetting.

Figure 5-8 Reserve email address



Step 6 Enter new IP address, subnet mask and gateway, and then click **Finish**. If they are not entered, the three parameters will be the default values.

Figure 5-9 Modify IP address



5.4.3 Changing IP Addresses

After initializing remote device, you can change the IP address of initialized devices.

Procedure

Step 1 Click **Auto Search** on the **Device Manager** page.

Step 2 Set the range of network segment, and then click **Search**.

Step 3 Select the needed devices, and then click **Modify IP**.

Step 4 Change the IP address, subnet mask and gateway of the device, and then click **OK**. You can change IP of a single device or of devices in batches.

- For batch change, the new IP will be assign to the top-most device, and other IP addresses will increase by 1 from top to bottom. For example, if you select two devices and set the new IP as 192.168.1.10, then the IP address of top device on the list will be changed as 192.168.1.10, and the next device will be changed as 192.168.1.11.
- For batch change, the subnet mask and gateway will be assigned to all selected devices.

Figure 5-10 Change IP of a single device

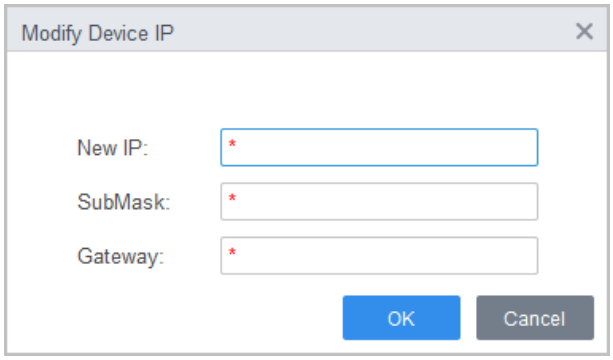


Figure 5-11 Change IP of devices in batches

Step 5 Enter the login username and password, and then click **OK** to confirm.

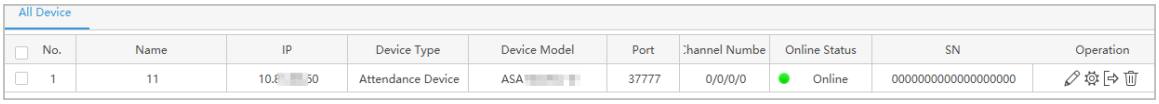
5.4.4 Configuring Devices

For some access control devices, you can make configuration, including time setting, firmware upgrade, device restart, personnel extraction and attendance record extraction.

Procedure

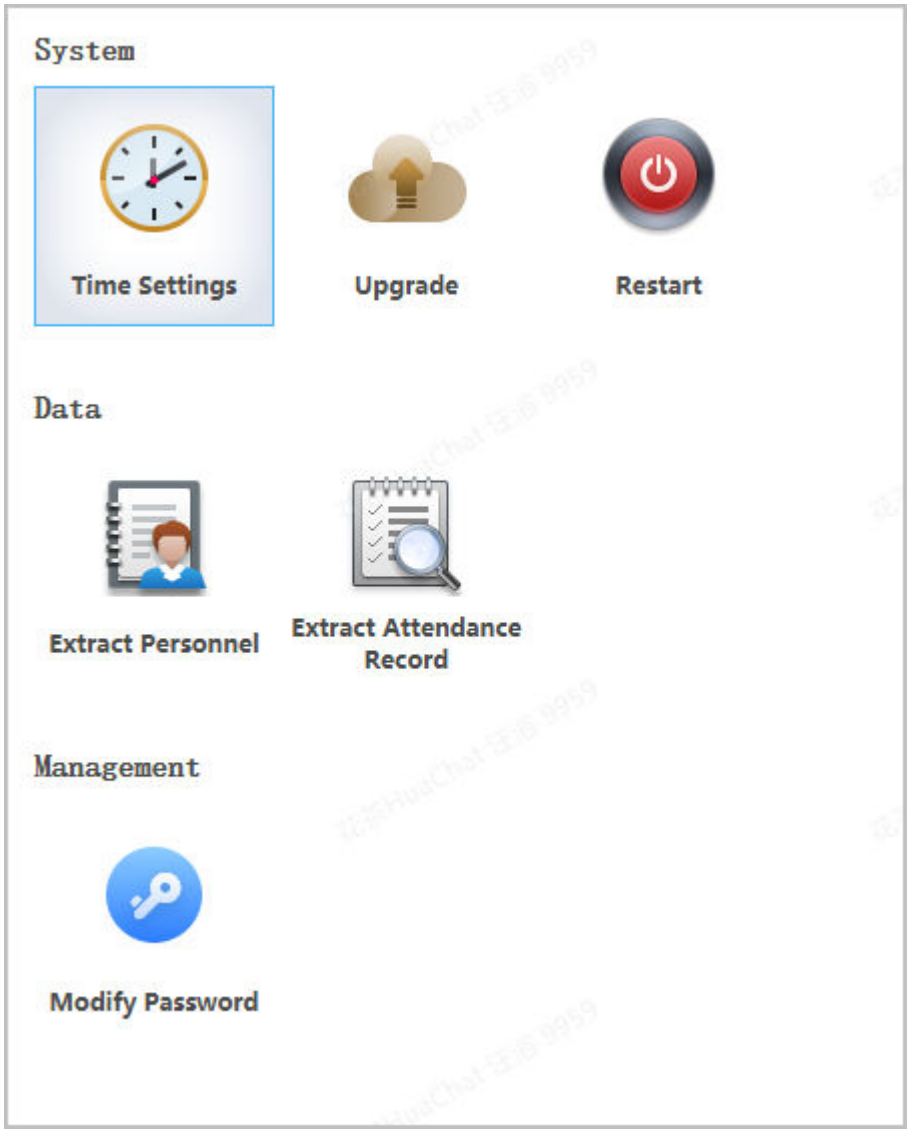
Step 1 Select **Device Manager**, and then click ⚙.

Figure 5-12 Configure device



Step 2 Click ⚙ to configure the device.

Figure 5-13



- Time settings

Figure 5-14 Modify IP of devices in batches

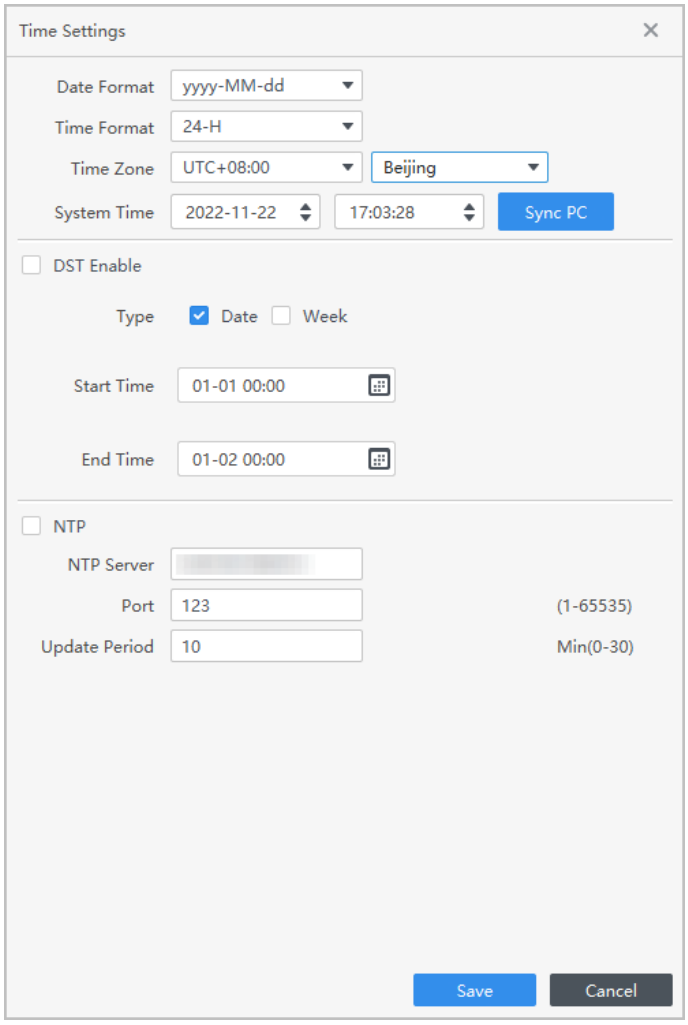
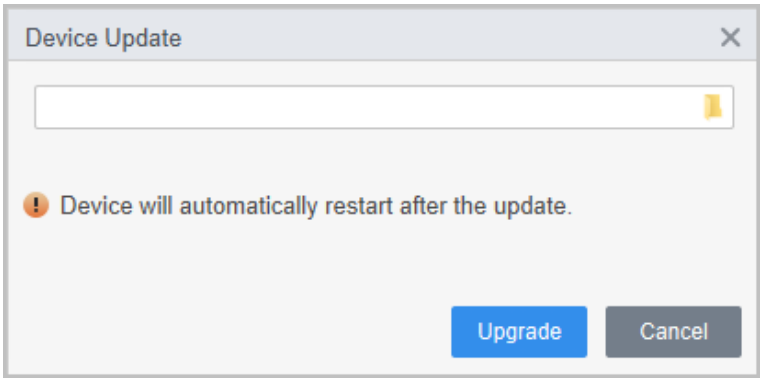


Table 5-3 Parameters of time setting

Parameter	Description
Date Format	Set the date display format.
Time Format	Set the time display format.
Time Zone	Set the time zone.
System Time	Set the system time. You can also click **Sync PC** to set the system time as the same as PC time.
DST	Enable DST as needed. Set the DST type, start time and end time.
NTP	Enable NTP server if you need to sync system time as the same as NTP time. Enter the server address, port and update period.

- Firmware upgrade: Select the bin for update, and then operate according to instructions.

Figure 5-15 Firmware upgrade



- Restart: Click to restart device.
- Local alarm linkage: Click to configure the alarm linkage information, and then click **Save**.

Figure 5-16 Local alarm linkage

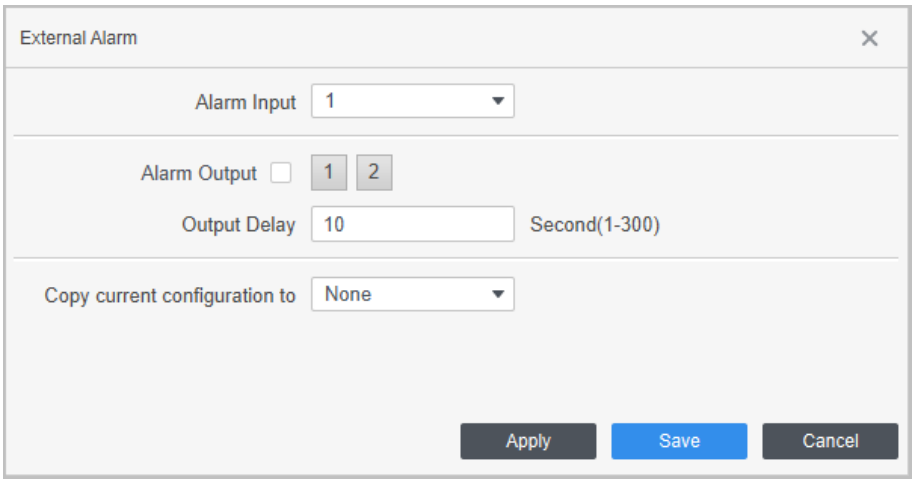


Table 5-4 Parameters of external alarm

Parameter	Description
Alarm input	Select an alarm input channel number as needed.
Alarm output	Select an alarm output channel number as needed.
Output delay	Alarms will be output after the duration you have set.
Copy current configuration to	You can copy the current configuration to other devices as needed.

- Extract personnel information: Select the needed personnel and extract personnel information from device to the computer.
- Extract attendance record: Set the time period and extract attendance records manually.
- Modify Password: Change password of admin account. This function is only available on select models of time attendance devices.

Make sure that you have set access controllers as attendance points before extraction. For details of attendance point setting, see *SmartPSS Lite_Attendance Solution_User's Manual*.

Related Operations

For some devices, you can click ⚙ to go to the device web client.

5.4.5 Alarm Configuration

Devices whose models are ASC2202B-D can be connected to external alarm devices. Go to the **External Alarm** page, and then configure the parameters.

Figure 5-17 External alarm

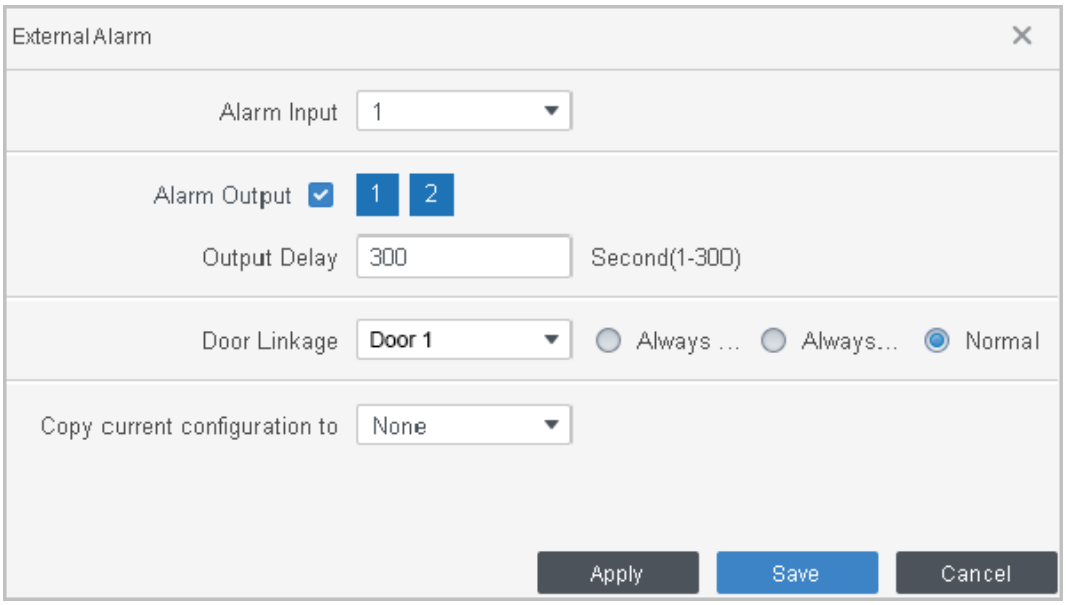


Table 5-5 Parameters of time setting

Parameter	Description
Alarm Input	Select an alarm input channel number as needed.
Alarm Output	Select an alarm output channel number as needed.
Output Delay	Alarms will be delayed after the defined duration.
Copy current configuration to	You can copy the current configurations to other devices as needed.

6 Log Query

You can query for alarm events, client logs and device logs.

Procedure

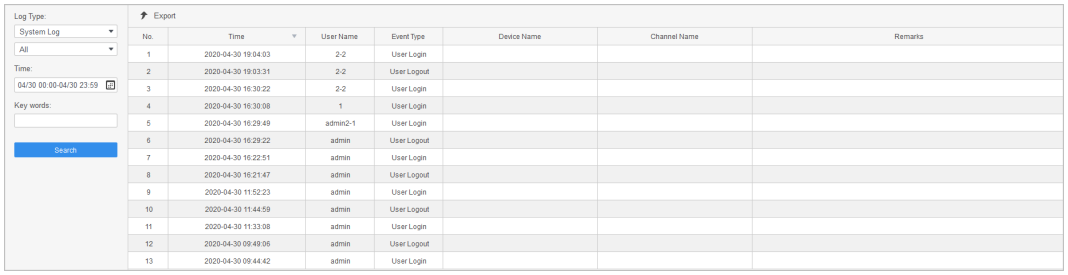
Step 1 Select **Log Query**.

Step 2 Select log type and log time, and then enter key words if needed.

Step 3 Click **Search**.

Step 4 (Optional) Click **Export** to export logs to local device.

Figure 6-1 Query for logs



No.	Time	User Name	Event Type	Device Name	Channel Name	Remarks
1	2020-04-30 19:04:03	2-2	User Login			
2	2020-04-30 19:03:31	2-2	User Logout			
3	2020-04-30 16:30:22	2-2	User Login			
4	2020-04-30 16:30:08	1	User Login			
5	2020-04-30 16:29:49	admin2-1	User Login			
6	2020-04-30 16:29:22	admin	User Logout			
7	2020-04-30 16:22:51	admin	User Login			
8	2020-04-30 16:21:47	admin	User Logout			
9	2020-04-30 11:52:23	admin	User Login			
10	2020-04-30 11:44:59	admin	User Logout			
11	2020-04-30 11:33:08	admin	User Login			
12	2020-04-30 09:49:06	admin	User Logout			
13	2020-04-30 09:44:42	admin	User Login			

7 Event Configuration

By configuring event, you can set event linkages, such as alarm sound, email sending and alarm linkages.

Background Information

- Configure external alarm linkages connected to the access controllers (such as smoke alarm), cameras and storage devices.
- Different devices support different alarm linkages, and the actual page might vary depending on different devices.
- Configure linkages of access controller events.
  - Alarm event
  - Abnormal event
  - Normal event

Procedure

Step 1 Click **Event Config** on the home page.

Step 2 Select the needed device, and then select **Alarm Event** > **Intrusion Event** .

Step 3 Click on the right side of **Intrusion Alarm** to enable the function.

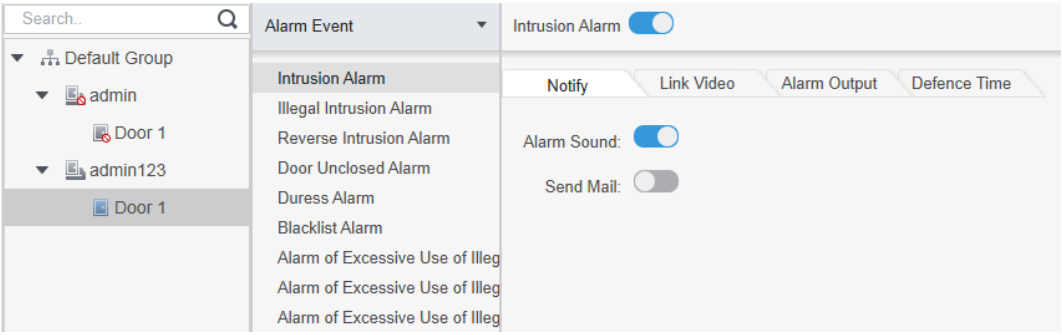
Step 4 Configure linkage actions of the intrusion alarm.

- Enable alarm sound.
- Send alarm email.

1. Enable **Send Mail** and confirm to set SMTP, you will automatically go to the **System Settings** page.
2. Configure SMTP parameters, such as server address, port number, and encryption mode.

   When intrusion event occurs, the system automatically sends alarm emails to the specified receiver.

Figure 7-1 Configure intrusion alarm



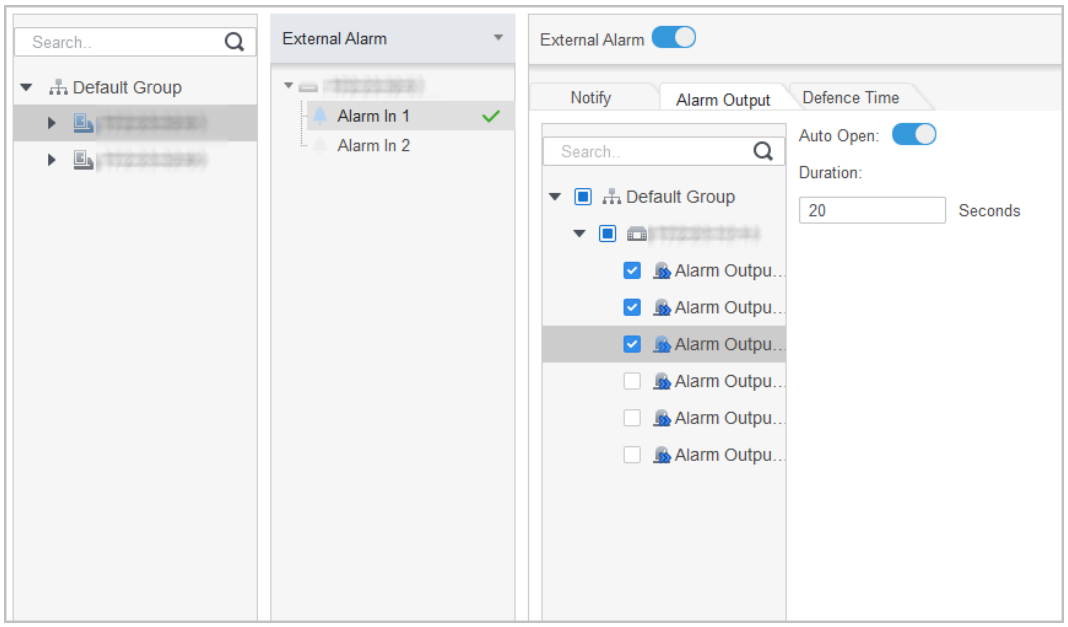
- Configure linkage video.

  Click **Link Video**, select video layout as needed. Once intrusion alarm is triggered, videos will be automatically displayed on the page.
- Configure alarm I/O.

  a. Click the **Alarm Out put** tab.
  b. Select the device which supports alarm input, select the alarm input channel, and then enable **External Alarm**.
  c. Select the device which supports alarm output, then select alarm-out page.

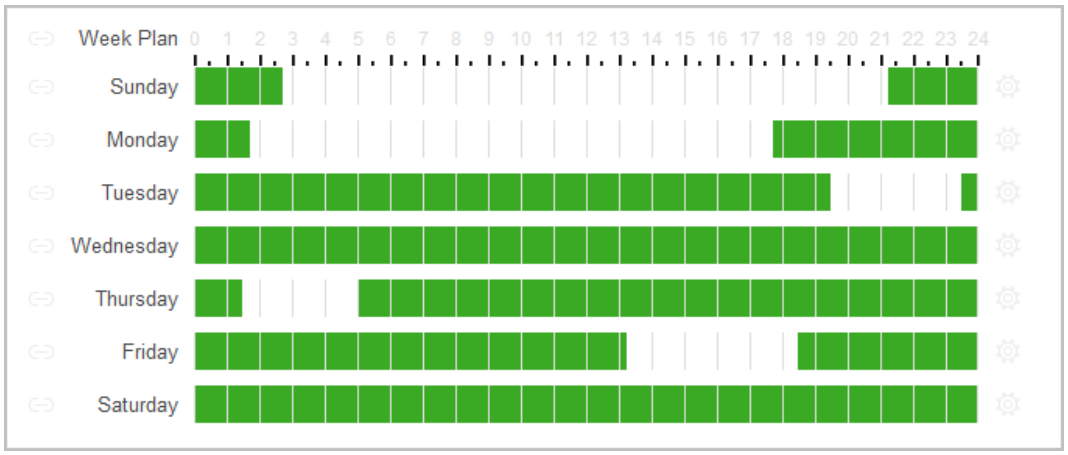
d. Enable **Auto Open** for the alarm linkage.
e. Set the duration.

Figure 7-2 Configure alarm linkage



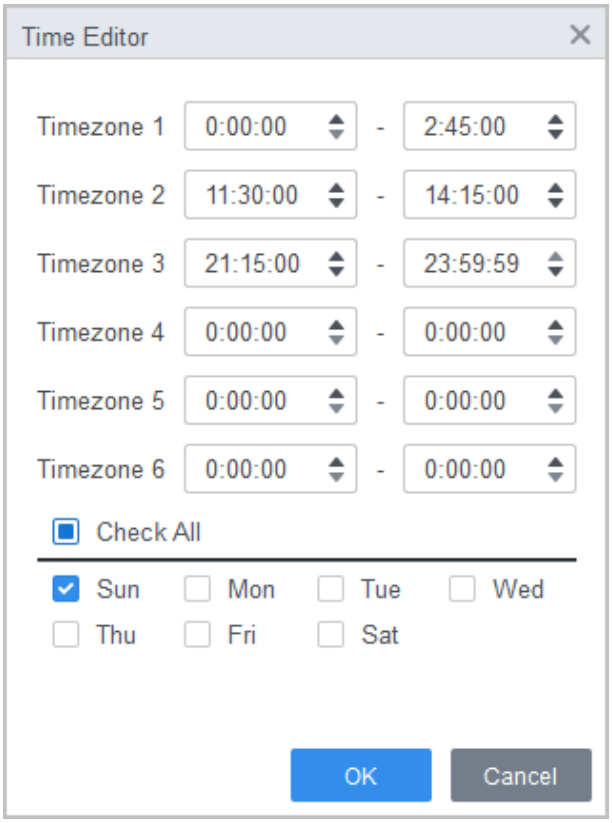
- Set arming periods. There are two methods.
  - Method 1: Move the cursor to set time periods. When the cursor turns to a pencil, click it to add periods; when the cursor turns to an eraser, click it to minus periods. The periods in green area are armed.

Figure 7-3 Set arming periods (method 1)



  - Method 2: Click ⚙ to set periods, and then click **OK**.

Figure 7-4 Set arming periods (method 2)



Step 5 (Optional) Click **Copy To** , select the access controller to be applied to, and then click **OK**.

Step 6 Click **Save**.

8 Event Center

You can view and process the real-time alarm events. Click the number on the upper-right corner of the page to enter the event center.

8.1 Overview

Figure 8-1 Event center

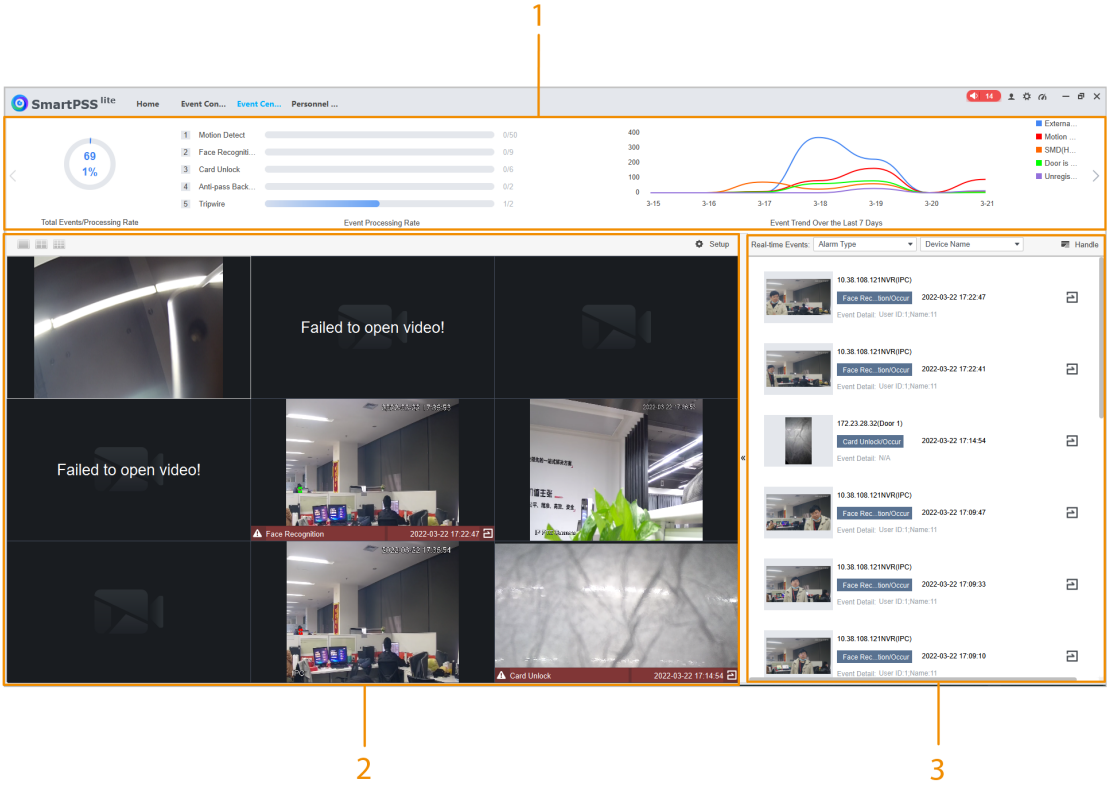


Table 8-1 Description of event center parameters

No.	Parameter	Description
1	Event statistics	• **Total Events/Processing Rate** : Display the pie chart of the total events and processing rate. Click the chart to view the information of unprocessed events. • **Event Processing Rate** : Display the processing rate of different event types in real time. • **Event Trend Over the Last 7 Days** : Display the graph of the top five event types in seven days (excluding today). Point to the graph to display the specific number of the alarm events. Click > to display the details of each alarm event.
2	Live View Video	Preview the configured channel video. Click « to the preview page.

No.	Parameter	Description
3	Real-time Events	View real-time alarm events. You can search event information according to alarm types and devices.

8.2 Configuring Live View Video

Configure live view video channels, and capture channel images, videos and video talks.

Procedure

Step 1 Click to select the screen number on the **Event Center** page.

It only supports 1, 4, 9 screen splits.

Step 2 Right-click the screen, click **Stream Type**, and then select the video channel that you want to live view.

Step 3 Click **Setup**, and then select the configuration according to actual needs.

Figure 8-2 Setup

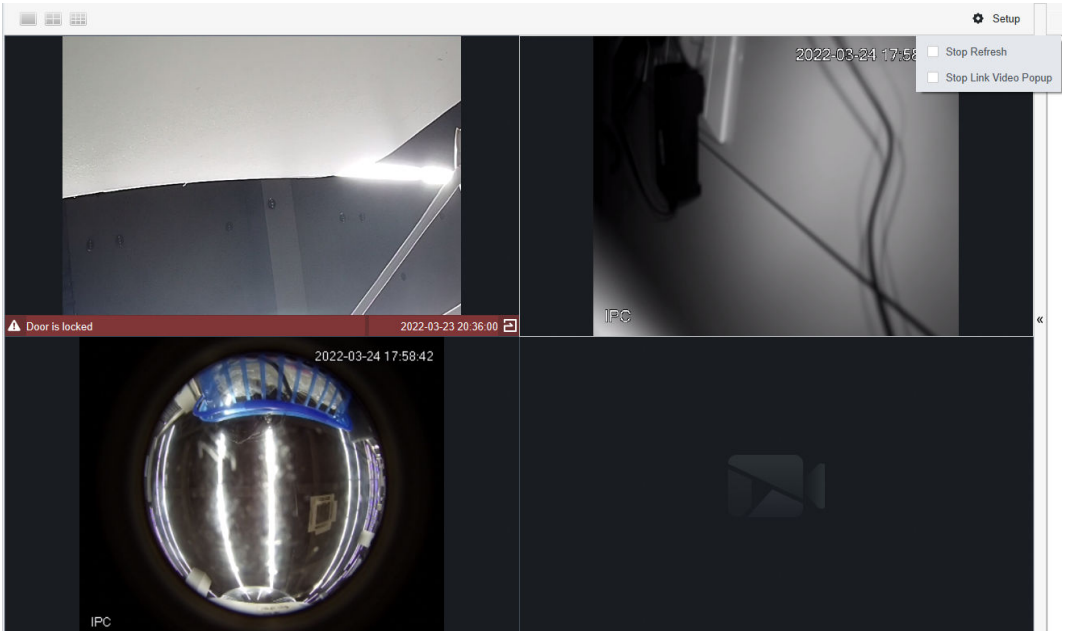


Table 8-2 Setup

Parameter	Description
Stop Refresh	Stop refreshing real-time alarm events
Stop Link Video Popup	Stop popping up event linkage video.

Related Operations

Live view video operations.

Point to the screen, and then the shortcut icons will be displayed on the upper-right corner of the window.

Table 8-3 Description of live view operation parameters

Icon	Parameter	Description
	Local Record	Click the icon to record videos in the current screen window. Click the icon again to stop recording and save the video to the computer. The default save path is "…/Data/User/Record". You can change the storage path through > **System Config** > **Local Path** > **Record Path** .
	Visitor Picture	Save the snapshot in the current video screen as an image on the computer (once at a time). The default save path is "…/Data/User/Picture/Capture". You can change the save path through > **System Config** > **Local Path** > **Pic Path** .
	Audio	Click the icon to open or close the audio of the camera.
	Audio Talk	Click the icon to open or close the audio talk of the corresponding camera.
	Instant Replay	Click the icon to open or close instant replay function. You can configure the replay time through > **System Config** > **Basic Setting** on the upper-right corner of the page. You need to have videos on the device before you enable instant replay function.
	Zoom In	Click the icon, and then scroll the mouse wheel to zoom in or out the screen.
	Close Video	Click the icon to close the video.

Appendix 1 Cybersecurity Recommendations

The necessary measures to ensure the basic cyber security of the platform:

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords:

   - The length should not be less than 8 characters.
   - Include at least two types of characters; character types include upper and lower case letters, numbers and symbols.
   - Do not contain the account name or the account name in reverse order.
   - Do not use continuous characters, such as 123, abc, etc.
   - Do not use overlapped characters, such as 111, aaa, etc.
2. **Customize the Answer to the Security Question**

   The security question setting should ensure the difference of answers, choose different questions and customize different answers (all questions are prohibited from being set to the same answer) to reduce the risk of security question being guessed or cracked.

Recommendation measures to enhance platform cyber security:

1. **Enable Account Binding IP/MAC**

   It is recommended to enable the account binding IP/MAC mechanism, and configure the IP/MAC of the terminal where the commonly used client is located as an allowlist to further improve access security.
2. **Change Passwords Regularly**

   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.
3. **Turn On Account Lock Mechanism**

   The account lock function is enabled by default at the factory, and it is recommended to keep it on to protect the security of your account. After the attacker has failed multiple password attempts, the corresponding account and source IP will be locked.
4. **Reasonable Allocation of Accounts and Permissions**

   According to business and management needs, reasonably add new users, and reasonably allocate a minimum set of permissions for them.
5. **Close Non-essential Services and Restrict the Open Form of Essential Services**

   If not needed, it is recommended to turn off NetBIOS (port 137, 138, 139), SMB (port 445), remote desktop (port 3389) and other services under Windows, and Telnet (port 23) and SSH (port 22) under Linux. At the same time, close the database port to the outside or only open to a specific IP address, such as MySQL (port 3306), to reduce the risks faced by the platform.
6. **Patch the Operating System/Third Party Components**

   It is recommended to regularly detect security vulnerabilities in the operating system and third-party components, and apply official patches in time.
7. **Security Audit**

   - Check online users: It is recommended to check online users irregularly to identify whether there are illegal users logging in.
   - View the platform log: By viewing the log, you can get the IP information of the attempt to log in to the platform and the key operation information of the logged-in user.
8. **The Establishment of a Secure Network Environment**

   In order to better protect the security of the platform and reduce cyber security risks, it is recommended that:

   - Follow the principle of minimization, restrict the ports that the platform maps externally by firewalls or routers, and only map ports that are necessary for services.

- Based on actual network requirements, separate networks: if there is no communication requirement between the two subnets, it is recommended to use VLAN, gatekeeper, etc. to divide the network to achieve the effect of network isolation.