

# SmartPSS-AC\_General

User's Manual








# Foreword

## General

This manual introduces the general functions and operations of the SmartPSS-AC (hereinafter referred to as "the SmartPSS-AC").

## Safety Instructions

The following categorized signal words with defined meaning might appear in the manual.

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

## Revision History

Version	Revision Content	Release Time
V1.0.1	Modify log query function.	June 2020
V1.0.0	First release.	May 2020

## Privacy Protection Notice

As the device user or data controller, you might collect personal data of others such as face, fingerprints, car plate number, email address, phone number, GPS and so on. You need to be in compliance with the local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures include but not limited to: providing clear and visible identification to inform data subject the existence of surveillance area and providing related contact.

## About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.

- The manual would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our 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 the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

# Table of Contents

<b>Foreword</b> .....	<b>I</b>
<b>1 Overview</b> .....	<b>1</b>
<b>2 Installation and Login</b> .....	<b>2</b>
2.1 Installation .....	2
2.2 Login.....	2
2.2.1 Initialization .....	2
2.2.2 Daily Login .....	3
2.3 Password Reset.....	4
<b>3 Homepage</b> .....	<b>5</b>
<b>4 Device Management</b> .....	<b>8</b>
4.1 Adding Device .....	8
4.1.1 Adding Device by Auto Search .....	8
4.1.2 Adding Device Manually .....	9
4.1.3 Importing Device in Batches.....	11
4.2 Deleting Device .....	11
4.3 Exporting Device .....	12
4.4 Modifying Device.....	12
4.4.1 Modifying Device Information .....	12
4.4.2 Initialization .....	12
4.4.3 Modifying IP Address .....	14
4.4.4 Device Configuration .....	15
4.4.5 Alarm Configuration .....	17
<b>5 Log Query</b> .....	<b>18</b>
<b>Appendix 1 Cybersecurity Recommendations</b> .....	<b>19</b>

# 1 Overview

SmartPSS-AC is a client software developed for those 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-AC. You can get the ToolBox on the official website of Dahua.

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

## 2.2 Login

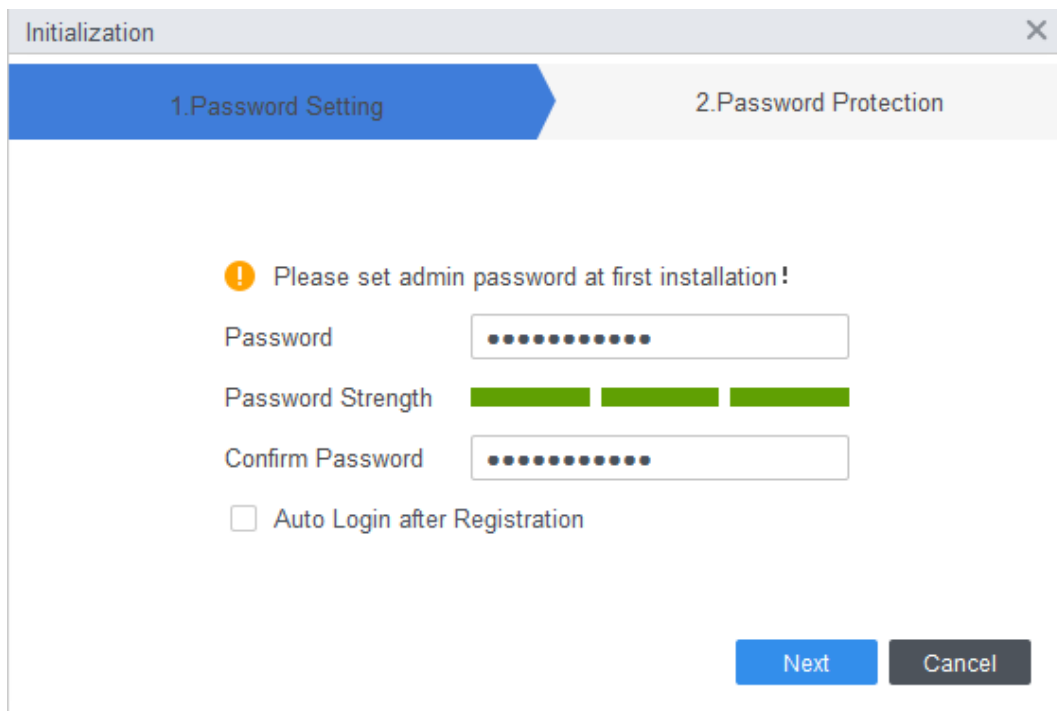
### 2.2.1 Initialization

Initialize SmartPSS-AC when you log in for the first time, including setting password and security questions. Password is for login, and security questions are for password resetting.

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

Step 2 Set password on the **Initialization** interface and then click **Next**.

Figure 2-1 Set password



Initialization

1.Password Setting

2.Password Protection

! Please set admin password at first installation!

Password

Password Strength

Confirm Password

Auto Login after Registration


Next Cancel

Table 2-1 Parameters of initialization

Parameter	Description
Password	The password should 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 with strong power, 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 <b>Auto Login after Registration</b> so that the SmartPSS-AC will log in automatically after initialization; otherwise, the login interface is displayed.

Step 3 Set security questions and then click **Finish**.

## 2.2.2 Daily Login

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

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

Figure 2-2 Login

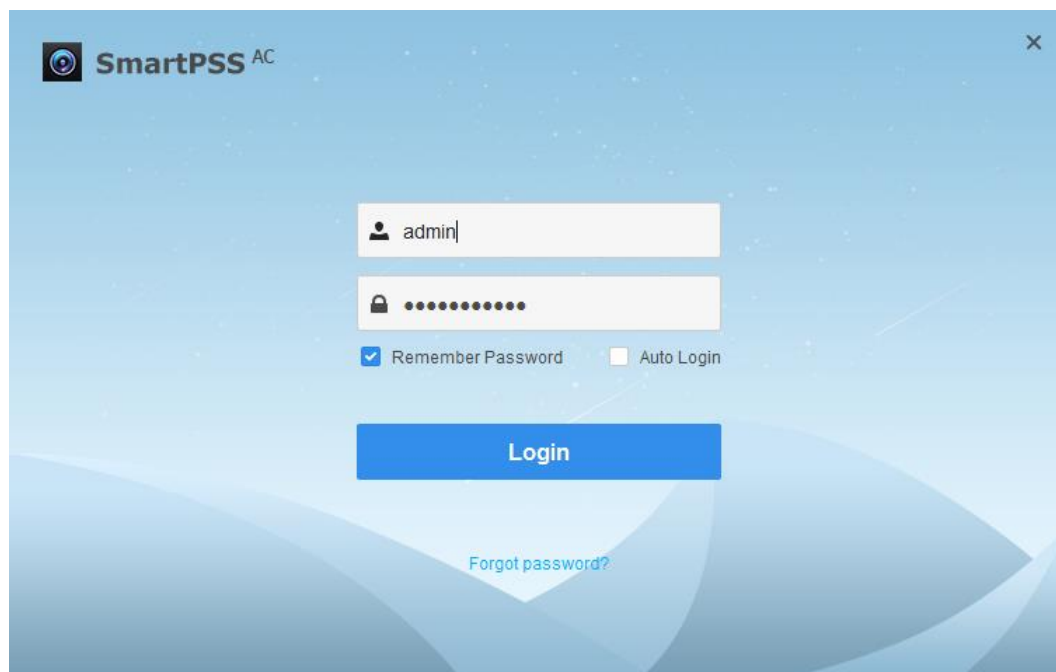



Table 2-2 Parameters of login

Parameter	Description
Remember Password	Enable <b>Remember Password</b> so that you do not need to enter the password again when logging in next time.

Parameter	Description
Auto Login	Enable <b>Auto Login</b> so that the SmartPSS-AC will log in automatically the next time when you use the same user account.
Forgot password?	Click <b>Forgot password</b> to rest password through security questions when you forget the password.

## 2.3 Password Reset

You can rest the password by answering the security questions.

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

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

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

Step 4 Reset password according to interface instructions.



# 3 Homepage

The homepage consists of 6 parts.

Figure 3-1 Homepage

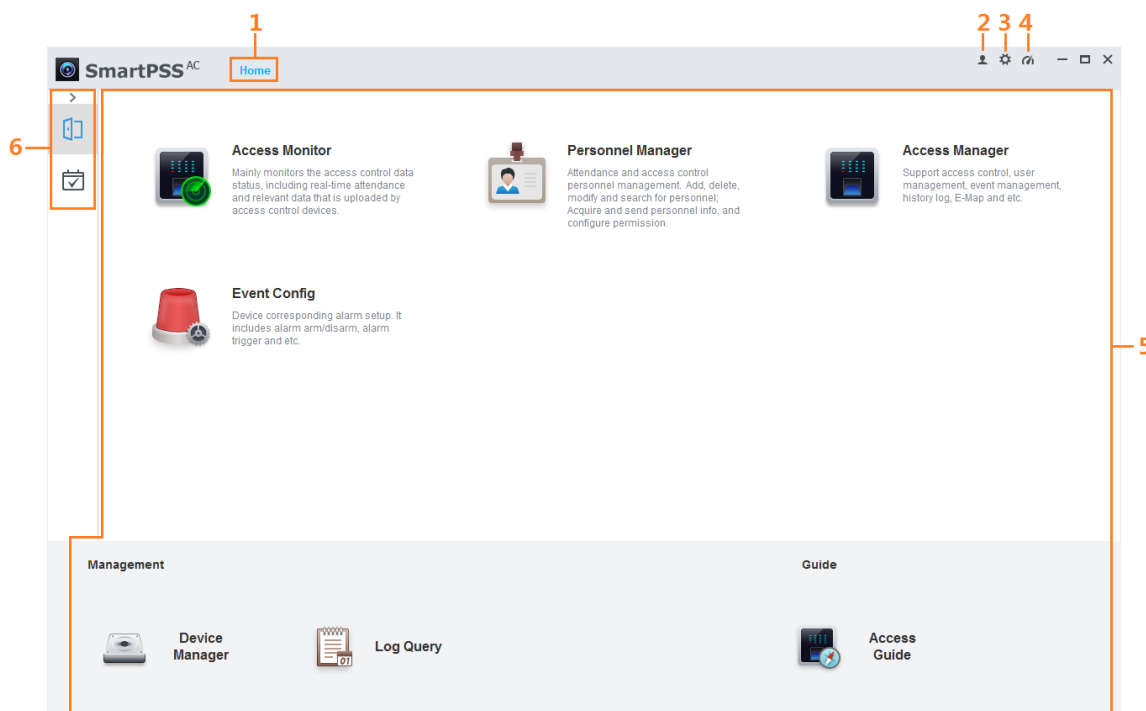









Table 3-1 Parameters of homepage

No.	Parameter	Description
1	Function tab	<p>Display the homepage by default.</p> <p>When you click on a function for the first time, the function tab is added here.</p>
2	User management	<ul style="list-style-type: none"> <li>Click  and select <b>User Manager</b> to manage users, such as add role/user, delete role/user and set permissions.</li> <li>Click  and select <b>lock Screen</b> to lock screen. Enter password of login account when you want to unlock.</li> <li>Click  and select <b>Switch User</b> to return to the login interface. You can log in with new account.</li> <li>Click  and select <b>Help Manual</b> to get the user's manual.</li> <li>Click  and select <b>About</b> to view the system version and date. Enable <b>Open Debugging Log</b> so that the debugging logs are saved automatically to a local path, for locating and problems solving.</li> </ul>
3	System configuration	<ul style="list-style-type: none"> <li>Basic Setting <ul style="list-style-type: none"> <li>◇ Timing: Enable <b>Auto Check Time Every day</b> and set <b>Check Time</b> so that the devices check time automatically at the set</li> </ul> </li> </ul>

No.	Parameter	Description
		<p>point in time.</p> <ul style="list-style-type: none"> <li>◇ Language: Display the language which is activated after restart.</li> <li>◇ Log save time: Set the save time of log and then logs from today to the set time will be saved. This function is activated after restart. For example, set the save time as 30, and then the logs of the last 30 days will be saved.</li> <li>◇ Data format: Select data display format.</li> <li>◇ Time format: Select time display format.</li> <li>◇ Network ability: Select network ability according to your network condition. For example, when network condition is fluent, you are recommended to select <b>High</b>.</li> <li>◇ Skin: Select the skin which is activated after restart. The default setting is grayish white.</li> </ul> <ul style="list-style-type: none"> <li>● Event <ul style="list-style-type: none"> <li>◇ Enable the loop of event sound.</li> <li>◇ Select event sound. You can select the needed sound or add the customized sounds in the path.</li> <li>◇ Enable and configure SMTP.</li> </ul> </li> <li>● Local path <p>The storage paths.</p> </li> <li>● Data management <ul style="list-style-type: none"> <li>◇ Extract regularly: Set the regularly extracting time so that the attendance data of devices will be extracted on pre-defined time. For example, if you set 8:00 of everyday as regularly extracting time, the SmartPSS-AC will auto extract the attendance data from 8:00 the previous day to 8:00 today at 8:00 every morning.</li> </ul> <p> For attendance devices, extract the attendance data directly. For access controllers, set the device as attendance point and then extract the attendance data.</p> <ul style="list-style-type: none"> <li>◇ Clear regularly: Set saving time for data and pictures. SmartPSS-AC auto clears data and pictures that exceed the saving time. It triggers at 00:00 everyday or when the software is started.</li> </ul> </li> <li>● Backup: Support to back up automatically and manually. <ul style="list-style-type: none"> <li>◇ Manual: Select the backup path and click <b>Manual Backup</b>.</li> <li>◇ Auto: Select the backup path and enable <b>Auto Backup</b>.</li> </ul> </li> <li>● Restore: Click <b>Restore</b> and select the backup file that you need. Configurations will restore the file configurations.</li> </ul>
4	System status	Click  to view the using status of CPU and RAM. If the CPU usage is high, the icon turns red.

No.	Parameter	Description
5	Function module	Click the function icon to go to the function interface.
6	Solution module	Select the needed solution. Click > to display or hide solutions.

# 4 Device Management

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

## 4.1 Adding Device

There are various methods to add devices. Select the most suitable method according to the situations, such as IP address and network segment.

- Auto search
- Manually adding
- Import in batches

### 4.1.1 Adding Device by Auto Search



Close ConfigTool and DSS when you configure devices; otherwise, you may not be able to search all devices.

It is recommended to add devices by auto search when you need to add devices in batches within the same network segment, or when the network segment is clear but the device IP address is unclear.

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

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

The list of searched devices is displayed.



- Click **Refresh** 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 "4.4.3 Modifying IP Address."
- Click one uninitialized device and then click **Initialization**. You can reset IP address, sub mask, gateway and login password. For details, see "4.4.2 Initialization."

Figure 4-1 Search results

The screenshot shows the 'Auto Search' window with a search bar at the top containing 'Device Segment' and a 'Search' button. Below the search bar are three buttons: 'Refresh', 'Modify IP', and 'Initialization'. To the right of these buttons, it says 'Search Device Number: 5'. The main area contains a table with the following data:

No.	IP	Device Type	MAC Address	Port	Initialization Status
1	192.168.1.1	AS17214Y-C-V3	0800201680000001	37777	Initialized
2	192.168.1.2	DHI-IVSS7008-1T	0800201680000002	37777	Initialized
3	192.168.1.3	ITC902-RF2D	0800201680000003	37777	Initialized
4	192.168.1.4	IPC-HDBW3230R-Z	0800201680000004	37777	Initialized
5	192.168.1.5	IPC-HDPW5421E	0800201680000005	37777	Initialized

At the bottom right of the window are 'Add' and 'Cancel' buttons.

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

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



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

## 4.1.2 Adding Device Manually

It is recommended to add devices manually when you need to add one single device with certain IP address or domain name.

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

**Step 2** Set device parameters.

Figure 4-2 Add device manually

Table 4-1 Parameters of manually adding

Parameter	Description
Device Name	It is recommended to name devices with the monitoring area for easy identification.
Method to add	Select the method to add.
IP	Enter the device IP address here when you select IP as the method to add.
Port	Enter the port number, and the port number is 37777 by default. The actual port number shall prevail.
User Name	Enter the login user name.
Password	Enter the login password.

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

## 4.1.3 Importing Device in Batches

It is recommended to add devices by importing when you need to add devices in batches but they are not on the same network segment. 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**.

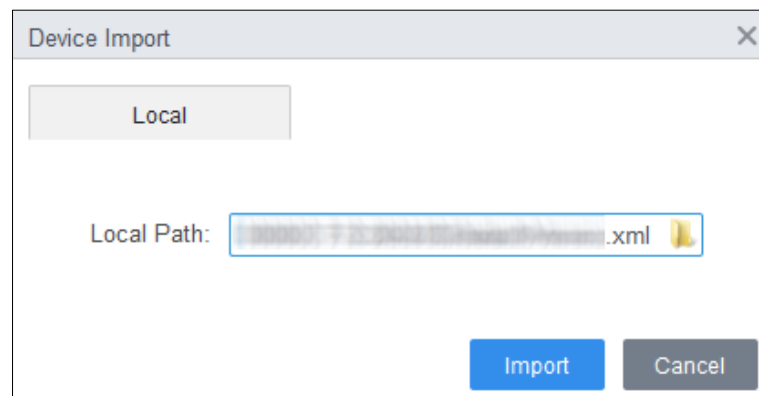
**Step 1** Click **Device Manager > Import**.

**Step 2** Select the information file and 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 4-3 Import device information in .xml format



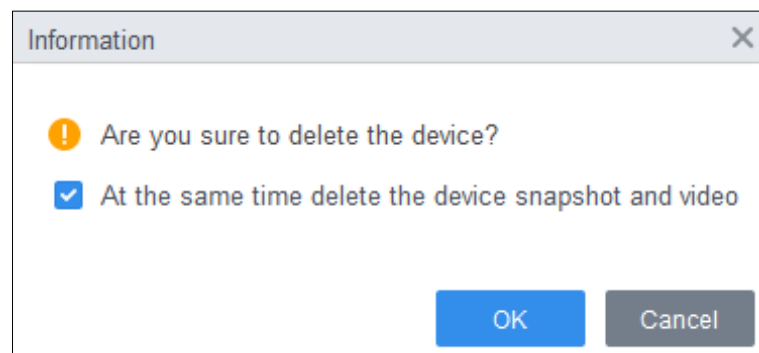
## 4.2 Deleting Device

**Step 1** Select **Device Manager** on the homepage.

**Step 2** Select the device that you do not need any more, and then click **Delete** or  which is 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; otherwise, do not check it.

Figure 4-4 Delete device



**Step 4** Click **OK**.

## 4.3 Exporting Device

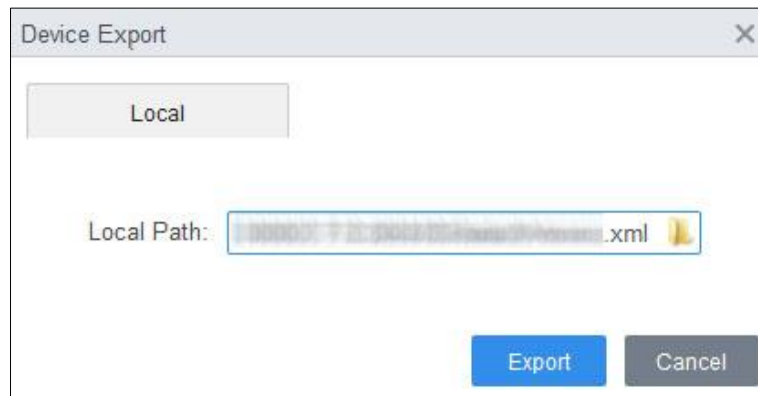
You can export device information to local.

Step 1 Select **Device Manager** on the homepage.

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

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

Figure 4-5 Export device information




## 4.4 Modifying Device

### 4.4.1 Modifying Device Information

You can modify the information of added device, such as name, login user name and password.

Step 1 Select **Device Manager** on the homepage.

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

Step 3 Modify device information.

Step 4 Click **Save**.

### 4.4.2 Initialization

Only support initializing devices which are within the same network segment as the PC.

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

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

The list of searched devices is displayed.



Figure 4-6 Device list

No.	IP	Device Type	MAC Address	Port	Initialization Status
<input checked="" type="checkbox"/> 1	192.168.1.101		08:00:27:0000:0000	37777	Uninitialized
<input type="checkbox"/> 2	192.168.1.102	VTT201	08:00:27:0000:0000	37777	Initialized
<input type="checkbox"/> 3	192.168.1.103	DH-SPS0116	08:00:27:0000:0000	37777	Initialized
<input type="checkbox"/> 4	192.168.1.104	DH-NVR4232-HDS2_T...	08:00:27:0000:0000	37777	Initialized
<input type="checkbox"/> 5	192.168.1.105	IPC-HFW1230M-I1-V2	08:00:27:0000:0000	37777	Initialized
<input type="checkbox"/> 6	192.168.1.106	IPC-HFW1230TP-ZS-28...	08:00:27:0000:0000	37777	Initialized
<input type="checkbox"/> 7	192.168.1.107	IPC-HDW1230T1-ZS-S4	08:00:27:0000:0000	37777	Initialized
<input type="checkbox"/> 8	192.168.1.108	IPC-HDBW1230R-ZS-S4	08:00:27:0000:0000	37777	Initialized

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

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

Figure 4-7 Set password

1. Set a password. 2. Password security. 3. Modify IP address.

User Name: admin

Password: \*

Confirm Password: \*

Please input 8-32 bytes from letters or numbers or symbols.

Next Cancel

**Step 5** Enter email address for password resetting.

Figure 4-8 Reserve email address

1. Set a password. 2. Password security. 3. Modify IP address.

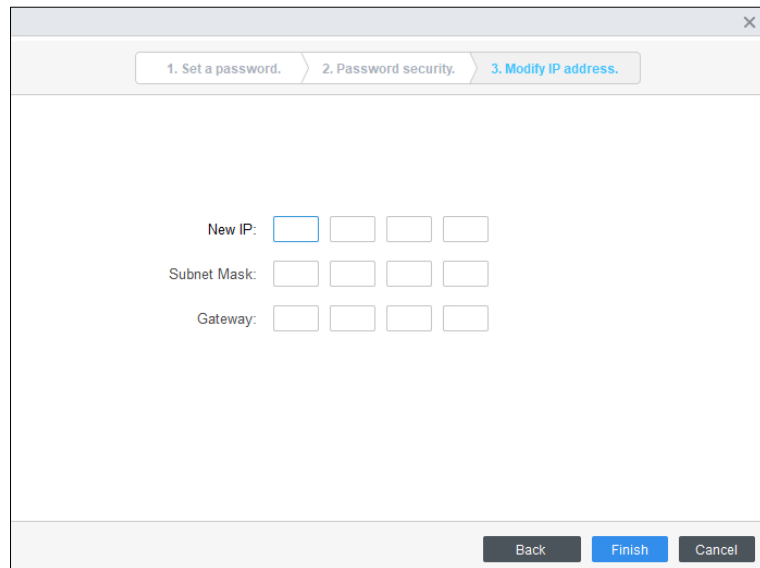
Email

Bind Email Address: \* Reset Password

Back Next Cancel

**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 4-9 Modify IP address



### 4.4.3 Modifying IP Address

After initializing remote device, you can change device IP address.

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

**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** Modify the IP address, subnet mask and gateway of the device, and click **OK**. You can modify IP of a single device or of devices in batches.



- For batch modify, 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 in the list will be modified as 192.168.1.10, and the next device will be modified as 192.168.1.11.
- For batch modify the subnet mask and gateway will be assigned to all selected devices.

Figure 4-10 Modify IP of a single device

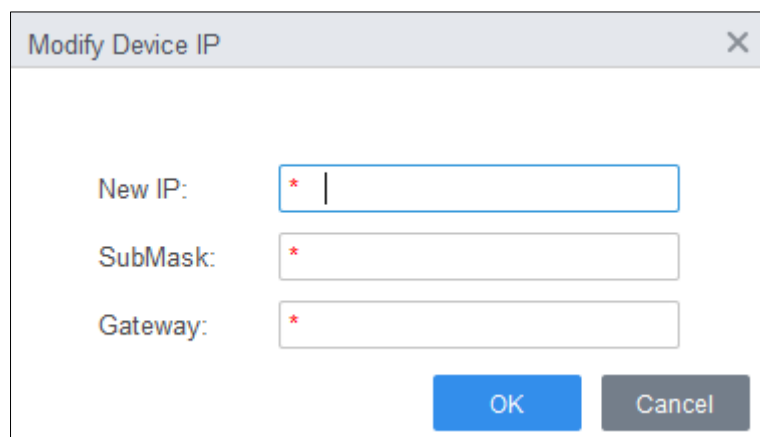


Figure 4-11 Modify IP of devices in batches

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




## 4.4.4 Device Configuration

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

**Step 1** Select **Device Manager**.

**Step 2** Click .

Figure 4-12 Configure device

<input type="checkbox"/>	No.	Name	IP	Device Type	Device Model	Port	Channel Numbe	Online Status	SN	Operation
<input type="checkbox"/>	1			Access Standalone	ASI8214Y-V3	37777	0/0/2/2	<span style="color: green;">●</span> Online		  

**Step 3** Configure device.

- Time setting

Figure 4-13 Modify IP of devices in batches

Table 4-2 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 <b>Sync PC</b> 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 upgrade bin and then operate according to instructions.
- Restart  
Click to restart device.
- Extract personnel  
Select the needed personnel and extract personnel info from device to the local.
- Extract attendance record.  
Set the time period and extract attendance records manually.



Make sure that you have set access controllers as attendance point before extraction. For details of attendance point setting, see *SmartPSS-AC\_Attendance Solution\_User's Manual*.

## 4.4.5 Alarm Configuration

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

Figure 4-14 External alarm

Table 4-3 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 output after the duration you have set.
Door Linkage	Once alarms are triggered, you can select Always Open, Always Close, or Normal for different doors.
Copy current configuration to	You can copy the current configuration to other devices as needed.

# 5 Log Query

You can query for client logs and devices logs. The two methods are similar, and here takes the system logs query of client as an example.

**Step 1** Select **Log Query**.

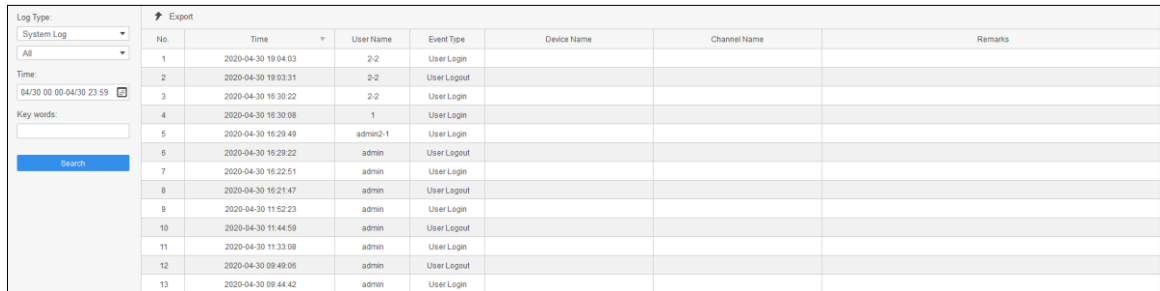
**Step 2** Select log type and log time, and enter key words if needed.

**Step 3** Click **Search**.

The results are displayed on the right side of interface.

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

Figure 5-1 Query for logs



The screenshot shows a web interface for querying logs. On the left, there is a search panel with the following elements:

- Log Type:** A dropdown menu set to "System Log".
- All:** A dropdown menu set to "All".
- Time:** A date and time range selector showing "04/30 00:00:00-04/30 23:59".
- Key words:** An empty text input field.
- Search:** A blue button.
- Export:** A link with a right-pointing arrow.

On the right, a table displays the search results. The table has the following columns: No., Time, User Name, Event Type, Device Name, Channel Name, and Remarks. The results are as follows:

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			

# Appendix 1 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations on how to create a more secured security system.

## **Mandatory actions to be taken for basic equipment network security:**

### **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. Update Firmware and Client Software in Time**

- According to the standard procedure in Tech-industry, we recommend to keep your equipment (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the equipment is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
- We suggest that you download and use the latest version of client software.

## **"Nice to have" recommendations to improve your equipment network security:**

### **1. Physical Protection**

We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable equipment (such as USB flash disk, serial port), etc.

### **2. Change Passwords Regularly**

We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

### **3. Set and Update Passwords Reset Information Timely**

The equipment supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

### **4. Enable Account Lock**

The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

### **5. Change Default HTTP and Other Service Ports**

We suggest you to change default HTTP and other service ports into any set of numbers between 1024~65535, reducing the risk of outsiders being able to guess which ports you are using.

#### **6. Enable HTTPS**

We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

#### **7. Enable Whitelist**

We suggest you to enable whitelist function to prevent everyone, except those with specified IP addresses, from accessing the system. Therefore, please be sure to add your computer's IP address and the accompanying equipment's IP address to the whitelist.

#### **8. MAC Address Binding**

We recommend you to bind the IP and MAC address of the gateway to the equipment, thus reducing the risk of ARP spoofing.

#### **9. Assign Accounts and Privileges Reasonably**

According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

#### **10. Disable Unnecessary Services and Choose Secure Modes**

If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

- SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
- SMTP: Choose TLS to access mailbox server.
- FTP: Choose SFTP, and set up strong passwords.
- AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

#### **11. Audio and Video Encrypted Transmission**

If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

Reminder: encrypted transmission will cause some loss in transmission efficiency.

#### **12. Secure Auditing**

- Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
- Check equipment log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

#### **13. Network Log**

Due to the limited storage capacity of the equipment, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

#### **14. Construct a Safe Network Environment**

In order to better ensure the safety of equipment and reduce potential cyber risks, we recommend:

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
- The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is



suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.

- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
- It is recommended that you enable your device's firewall or blacklist and whitelist feature to reduce the risk that your device might be attacked.