Market America New Platform Operation Manual

CMS

Table of contents

Chapter 1 Account Registration 4
1.1 Retail Account Registration 4
1.2 Operation User Registration 5
Chapter 2 Interface Introduction 6
1. User 6
2. Device Search 7
3. Add device 7
4. Refresh list 8
5. Filter device list 8
6. Equipment List 8
6.1 Host settings 8
6.2 Camera settings 17
7. Alarm information 18
8. PTZ control 19
9. Color Settings 19
10. Display Template 20
11. Local Settings 20
12. Icon Explanation 23
Chapter 3 Parameter Setting 23
3.1 Video Settings 24
3.1.1 Video equipment 24
3.1.2 Video scheduling 27
3.1.3 PTZ settings 28
3.1.4 Color Timing 29
3.2 Alarm settings 30
3.2.1 Alarm panel settings 30
3.2.2 Scheduled arming and disarming 36
3.2.3 Zone setting 37
3.2.4 Remote control settings 41
3.3 System Settings 42
3.3.1 Basic settings 43
3.3.2 Log query 44
3.3.3 Hard disk management 44
3.3.4 Factory settings 44
3.3.5 Regular maintenance 45
3.3.6 Update backup 46
3.3.7 Equipment installation 46
3.4 Network Settings 47
3.4.1 Basic settings 47
3.4.2 Advanced Settings 49
3.4.3 Platform Settings 51

3.4.4 IP filtering 52
3.5 Version Information 53
Chapter 4 Function List 53
4.1 User Management 53
4.1.1 Add 55
4.1.2 User modification 57
4.1.3 User deletion 57
4.1.4 User search 57
4.2 Device Management 58
4.2.1 Handling preallocation 58
4.2.2 Device Allocation 58
4.2.3 De-allocation of devices 59
4.2.4 Bind or unbind 60
4.3 Territory Management 61
4.4 Diary query 62
4.4.1 Alarm information 62
4.4.2 Operation Statistics 63
4.4.3 User logs 63
4.5 Map notation 63
4.6 Help panel 64

第一章 account registration

1.1 retail registration

Individual users (retail accounts): Individuals purchase and install the company's equipment, without the operator or its centralized management, the equipment is managed and configured by itself, mostly for shops, small and medium-sized companies and households.

There are two ways to obtain a retail account.

method one:

Step 1. Double-click the CMS icon , the login interface pops up, as shown in Figure 1-1;

Step 2. Click "Register Account", the user ID is the user's mobile phone number, and the password is set by yourself. Click to get the verification code and fill in the verification code obtained from the mobile phone into the verification code input field, and click "Submit";

Step 3. Fill in the user ID and password into the user account and user password respectively, and click "Login" to enter the main interface.

Figure 1-1Figure 1-2

Method Two:

Step 1. Scan the QR code as shown in Figure 1-3 to download and install the APP;

Step 2. Open the APP, select "User Registration" on the login interface (as shown in Figure 1-4), the service code is 1, enter the corresponding information and click "Register".

The successfully registered account and password can be used to log in to the CMS platform.

Note: If multiple people share a device, the account can be shared (the account can be found in Simultaneous login on different mobile phones), since the device can only belong to one user, You cannot use another account to scan and add repeatedly.

图 1-3

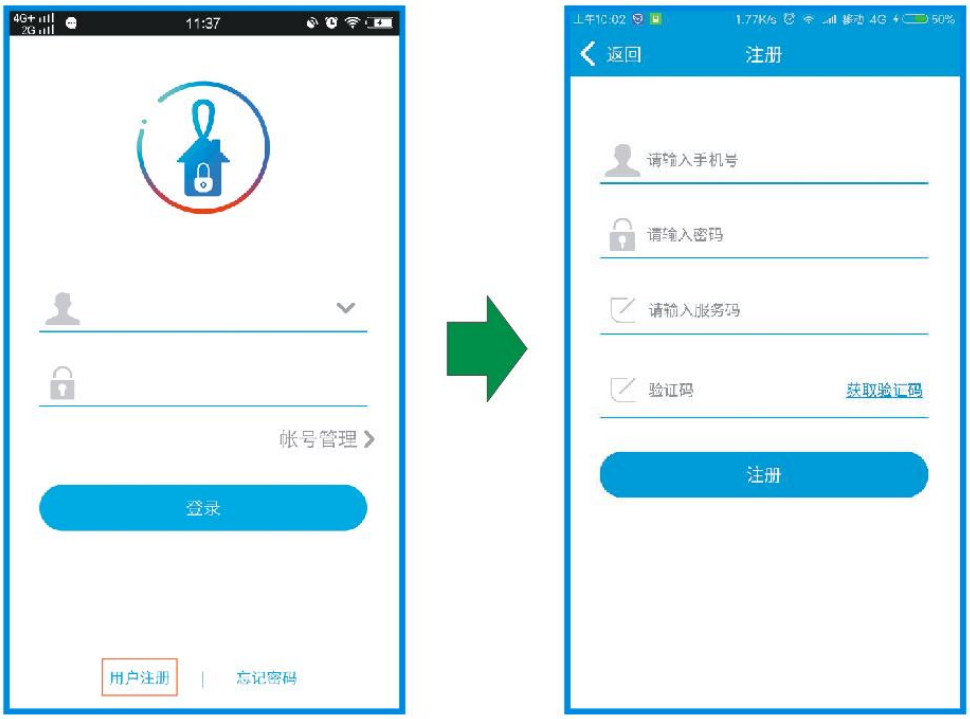


Figure 1-4

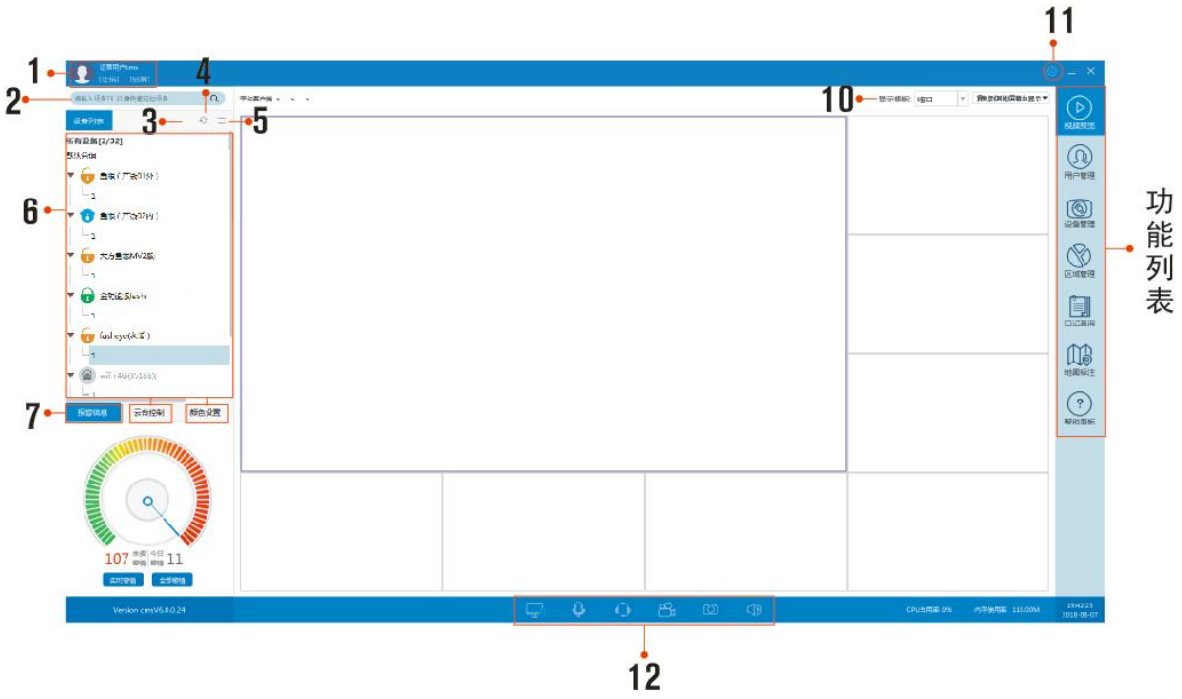
1.2 Operational user registration

Operating users: unified installation, management and maintenance by the operator, mostly schools, hospitals, banks, community security kiosks
and other public places. The operating user account is provided by the operator, and the operator is responsible for device viewing allocation and setting permissions.
If you have any questions, please call our customer service phone for consultation. Here we only introduce how an operation user can create a subordinate operation user
(operation), alarm receiving user (operation), individual user (operation), maintainer (operation).

For details on user registration, see "Chapter 4 Function List 4.1 User Management" on page 48 .

第二章 interface introduction

After entering the platform interface, the screen display is as shown in Figure 2-1:



1. user

Display the type of logged-in user. [Logout] is to log out of the platform. Click on the pop-up window as shown in Figure 2-2. After the screen is locked, you must unlock it to operate the platform. Click on the pop-up window as shown in Figure 2-3.

Figure 2-2 Figure 2-3

2. device search

Enter the device name to quickly find the device in the device list.

3. add device

Add the device to the device list of the current operating user,
The operation user can assign the added equipment to the area, add
method:
A. Make sure that the device is connected to the external network and connected to the service normally
In the case of the device, click to add a device window, click " "
Select an area (see the function list in Chapter 3 for details on adding an area
4. Territory management);
B. Enter the ID number of the device to be added (or use the scan
Barbarian gun to scan) press the Enter key;
C. As shown in Figure 2-4, the device to be added appears in the list
, select the device, click "Add", the status bar prompts
The addition is successful, and the device appears in the device list.
Clear list: Clear all devices in the list.

The equipment added by the operating user can be assigned to the alarm receiving user,
For end users, maintainers and retail investors, see "Chapter 4 Function List 2. User Management" for details.

图 2-4

4. refresh the list

Refresh all device information in the list.

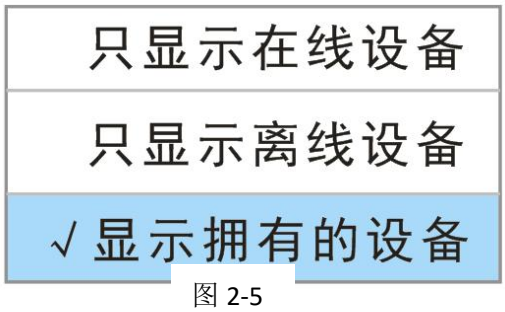


图 2-5

5. Filter device list

Click to pop up the prompt window in Figure 2-5, and the user can set it according to actual needs.

6. Device List

Display all device information, users can only operate on online devices, related icons and their meanings are shown in the table below.

图 标	含 义	图 标	含 义
	撤防		在家布防
	上线		外出布防
	离线		

注：为报警主机，为摄像机，为DVR。

6.1 host settings

Point the cursor at the online device (host) and right-click, and the setting options shown in Figure 2-6 will pop up.

6.1.1 preview

Preview all channel videos.

6.1.2 Close device streams (all)

Close all previews.

6.1.3 Start local recording (all channels of the device)

Record all videos. The video download path can be modified in "System Configuration" - "Other Settings".

6.1.4 Modify device information

The pop-up window is shown in Figure 2-7. The device ID, device password, owner name and owner ID cannot be changed. Items marked with "*" are required, and the expiration time is the device's service life.

Figure 2-6 Figure 2-7

Baidu longitude and latitude can be used to determine the coordinates of the device by clicking "Coordinate Picking" (as shown in Figure 2-8). The user can enter the correct address to query or use the mouse to determine the specific location. After completion, click "Save" to automatically return to the data modification interface Then click "Modify" to take effect.

Figure 2-8

6.1.5 parameter configuration

See "Chapter 3 Parameter Setting" for details.

6.1.6 start intercom

It means that voice dialogue can be carried out when both the host and the platform are equipped with pickups and speakers.

6.1.7 Zone map

The defense area map is used to view the specific location of the defense area. When the defense area map and the defense area are set up to trigger the alarm, the "real-time alarm" will display the name of the defense area, and the alarm receiver can find the location of the alarm through the defense area name. (as shown in Figure 2-9)

Figure 2-9

Regional map: Click "Set Map" to select a picture;

Logical partition: the partition of the defense zone map, the default is the living room, double-click the partition name to modify, up to

Add 40 partitions, click "+" to add, select a partition and click "-" to delete;

Logical defense area: the defense area of the logic partition to which it belongs, the defense area can be added when the host has been configured with accessories, and the maximum

Set 255 defense zones, click "+" to pop up the window shown in Figure 2-10,

Device ID: host ID number;

Defense zone number: the defense zone where the accessory is located. Note that when selecting the defense zone serial number, it should correspond to the defense zone where the accessory is located;

Zone name: set by the user;

Defense zone type: Click the drop-down window to select infrared, door sensor, keypad, emergency, broken, smoke, vibration and others.

After setting, click "Add" to enter the next defense area to add, and click "Return" to return to the defense area map setting interface.

Figure 2-10

6.1.8 Away arming

It mainly means that all detectors are set to be on alert.

6.1.9 Arming at home

Also known as staying behind. When the host is in the fortified state, through artificial setting, some detectors work and some detectors do not work, which is not only conducive to people's free movement in the fortified prevention space, but also can play an effective preventive function.

6.1.10 disarm

It is to set the alarm host controller to disarm, the alarm host will cancel the alert state, and the defense zone will not trigger an alarm.

6.1.11 Equipment Maintenance Order Management

It is used to record equipment maintenance information and contact information of relevant maintenance personnel. As shown in Figure 2-11, the start/end time is the search time period;

Add: Click "Add" to pop up a window as shown in Figure 2-12. The date of billing can be selected by clicking the drop-down window or manually input. Click "Save" and a pop-up window will prompt that the addition is successful (Figure 2-13).

Modify: Select the maintenance order to be modified and click "Modify" to modify the maintenance order;

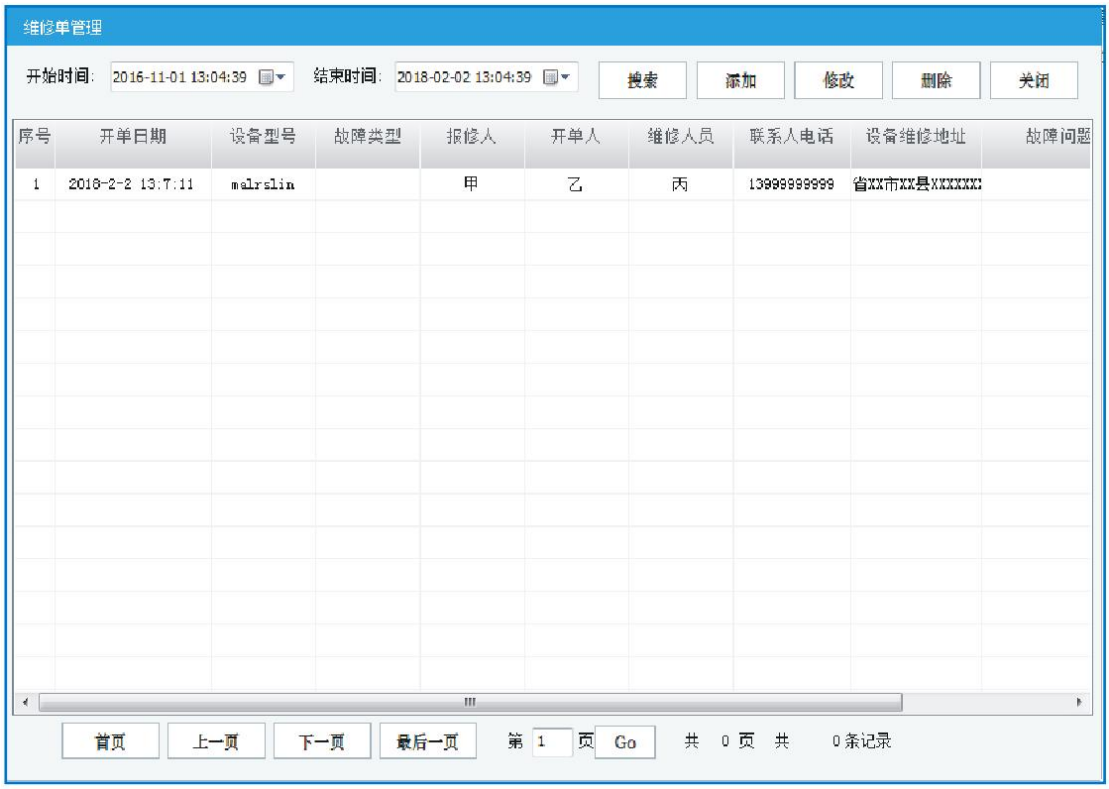


Figure 2-11

Figure 2-1 2 Figure 2-1 3

Delete: delete the selected maintenance order. As shown in Figure 2-14, click "Yes" to confirm the deletion.

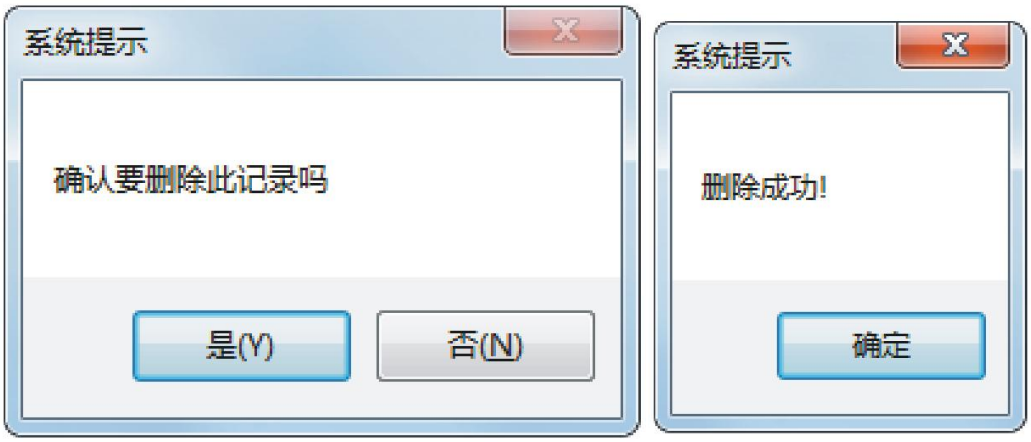


Figure 2-14 Figure 2-15

6.1.12 Electrical switch control

Electrical switches (such as light control switches, smart sockets, etc.) automatically return to the closed state according to the set time after they are turned on. As shown in Figure 2-16, select the electrical switch, check the "Auto" pop-up window as shown in Figure 2-17, the range of settings is 0~255 seconds, enter the time and click "OK" to take effect.

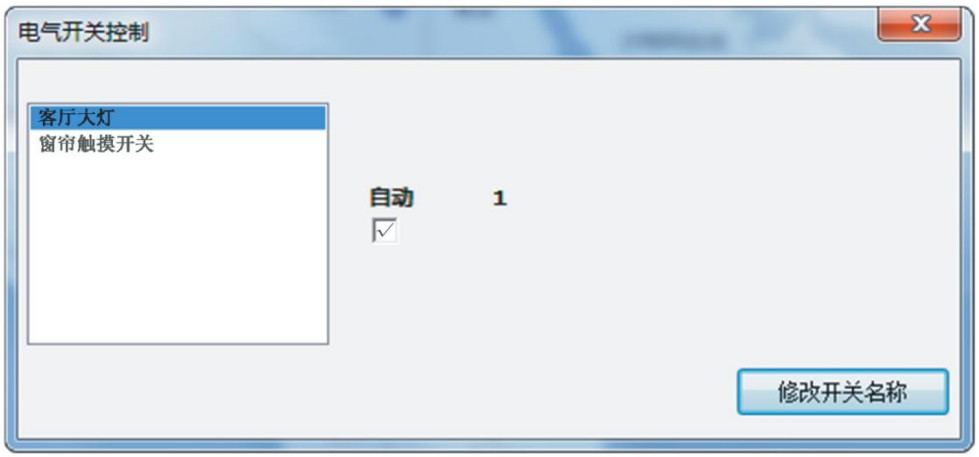


Figure 2-16

Figure 2-1 7

6.1.13 remote download

That is to download the device video through the platform, search for the video by selecting the channel, start time and end time, the default download path is the folder where the platform is located, click "Browse" to modify the download path.

Splicing time segments into the same file: refers to merging multiple recordings into one, and the merged recording will be played continuously for multiple recordings and the time displayed on the screen is still the recording time during playback.

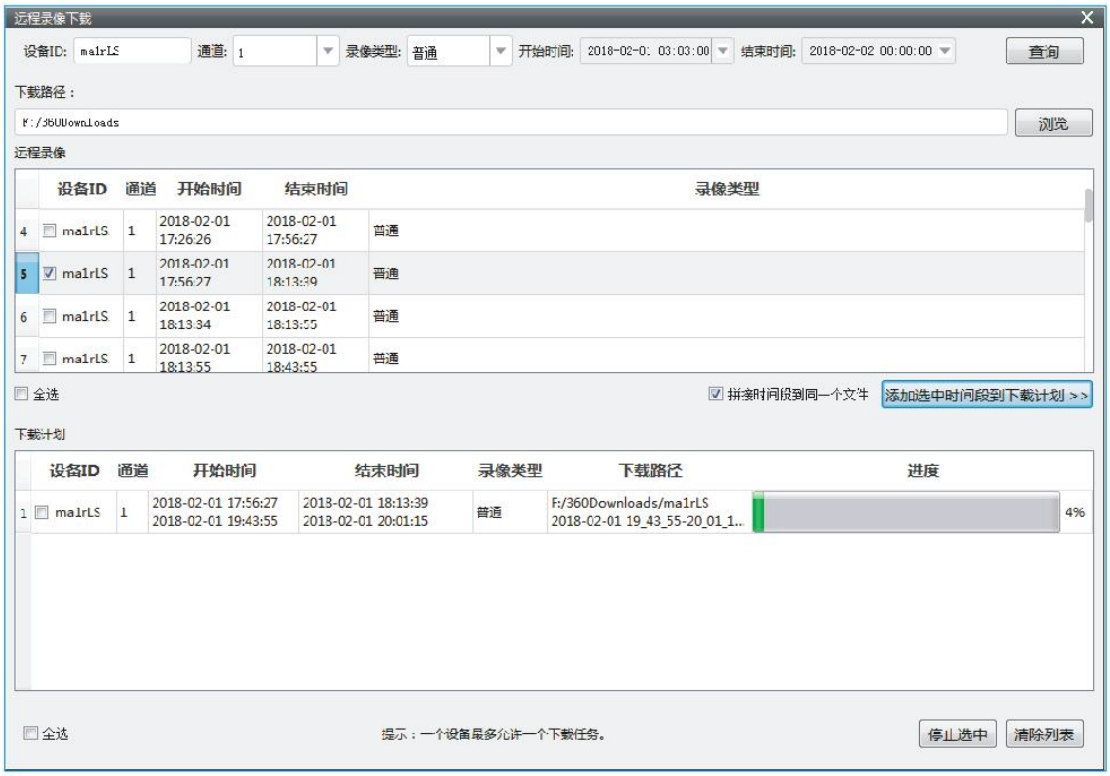


Figure 2-18

Add the selected time period to the download plan: download the selected video, if there are multiple download tasks, the selected video will be downloaded in sequence.

Stop selected: Stop downloading the selected video.

Clear List: Clear all downloads in the download plan.

6.1.14 map positioning

As shown in Figure 2-19, the map location of the device is displayed. Select the " " tool to drag the map, click " " to mark the map location, and click other icons in the lower left corner to view device information.

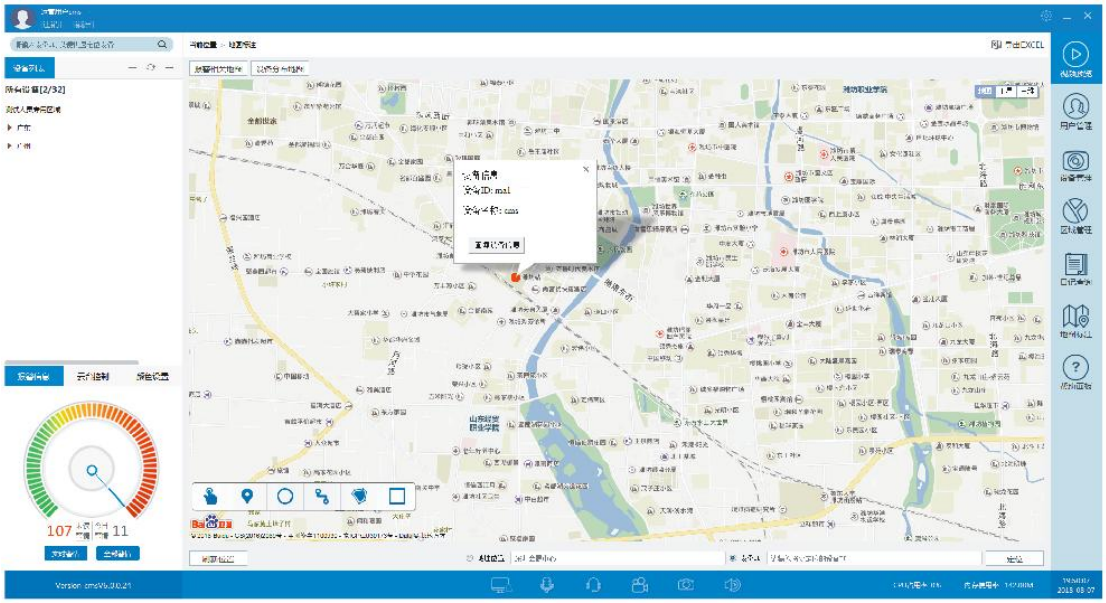


Figure 2-19

6.2 camera settings

Point the cursor at the camera under the online device (host) and right-click, and the setting options shown in Figure 2-20 will pop up.

Start channel local recording: record the channel, the video download path can be modified in "System Configuration" - "Other Settings".

Local Playback: Play back locally recorded video, as shown in Figure 2-21, the red covered area in the calendar column at the upper right corner indicates that the video recorded on that day can be played back.

Rescan video files: rescan local video files.

Number of recording time periods: the number of videos recorded in one day.

图 2-20

Figure 2-21

Example of video playback operation: select the date to be played back, place the mouse on the time axis and roll the wheel to zoom in/
Zoom out the time, the red part of the time axis is the recording time, use the mouse to drag into the graph bar to align the time point to be played with the central long line, click the icon " " to start playback, click " " to stop playback .

Remote playback: Play back all the videos stored in the hard disk of the device. For the operation method, please refer to video playback.

7. Alarm information

Real-time alarm: click to the right to expand the detailed information of the alarm, including device ID, device name, alarm information, device
Longitude and latitude etc. Click the cursor on the alert pop-up window as shown in Figure 2-22.

Figure 2-21

The user can click "receive alarm" in the lower right corner to deal with it. Fog control means that when the camera carries a fog

After triggering, it will automatically return to the closed state according to the set time. For the setting method, please refer to "6.1.12 Electrical switch control".

All alarms: click to jump to "Diary Query" in the function list, see "Chapter 4 Function List" for details.

8. PTZ control

This setting requires the support of the camera pan/tilt, as shown in Figure 2-23, open the video preview and select the video, and click the direction button according to the desired setting direction.

9. color settings

Color setting is the adjustment of the screen display effect, as shown in Figure 2-24, the user can set according to the actual situation, and click "Save" - "Refresh" after setting.

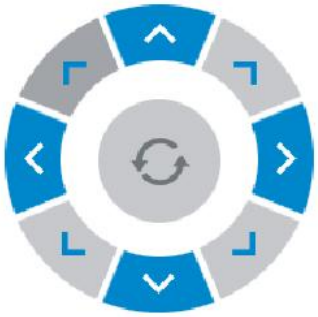


图2-23

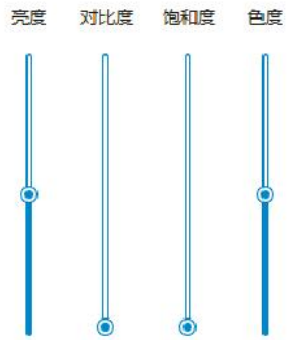


图2-24

图2-25

10. display template

The display template is the number of channel windows displayed on the display screen. Click the drop-down window " ▼ " to set the number of channel windows as 1, 4, 8, 9, 10, 12, and 16 windows. When the number of video previews exceeds the number of display windows on the display screen If the number exceeds the number, it cannot be displayed. At this time, the user must change the number of display windows.

11. local settings

Click the icon “ ” to display the setting items as shown in Figure 2-25.

Logout: Log out of the current account;

Settings: including alarm settings, other settings and version information.

①Alarm setting (as shown in Figure 2-26)

Real-time message prompt sound: hit " √ " in front of the switch to turn on the prompt sound; click "..." to select the prompt sound path.

Alarm automatic pop-up box: When the defense zone triggers an alarm, the system automatically pops up a window to prompt the alarm information.

Automatically locate the map when an alarm occurs: When the defense zone triggers an alarm, the system automatically pops up a map to prompt the location of the device.

Alarm message text color: Alarm messages include report, arm, disarm, fault, emergency, error, fire, robbery, burglary, alarm, remote control, access, deactivation, monitoring, bypass, test. The default report is lavender; arming and disarming are blue; emergency, fire, robbery, and burglary are red, and the rest are black. Click on a color to change it.

Unread alarm text color: the default is dark gray, click the color to change it.

After setting, click "Save" to take effect.

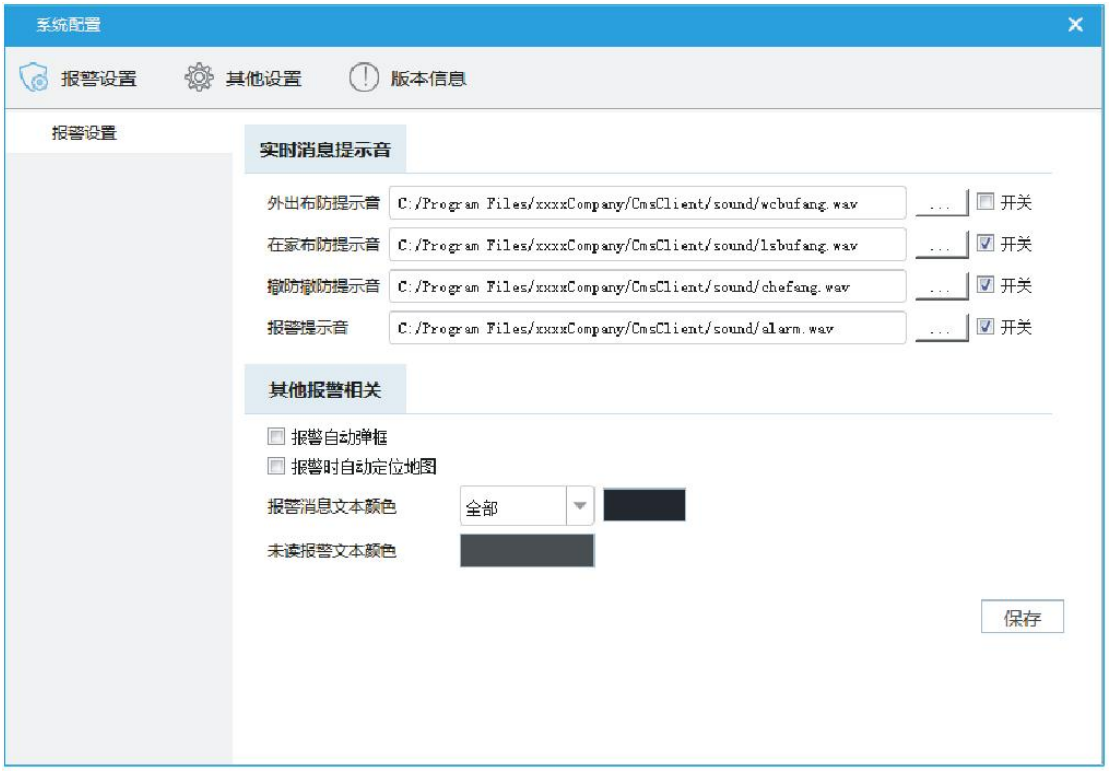


Figure 2-26

②Other settings (as shown in Figure 2-27)

Video path: The video is saved in the hard disk of the computer. If multiple hard disks are checked, the storage order is the selected alphabetical order. If D, E, and F disks are checked, the video will be saved in D disk. If D disk If the storage space is insufficient, the video will be saved in Disk E, and so on. After setting, click "Save", a pop-up window prompts to restart the client, click "OK" to restart, and "Cancel" will not save.

System prompt sound: refers to the prompt sound when the device is online and offline. After changing the setting, click "Save".

Figure 2-27

③version information

Client version, click "Update Check" to check the version, and update the version when there is a new version.

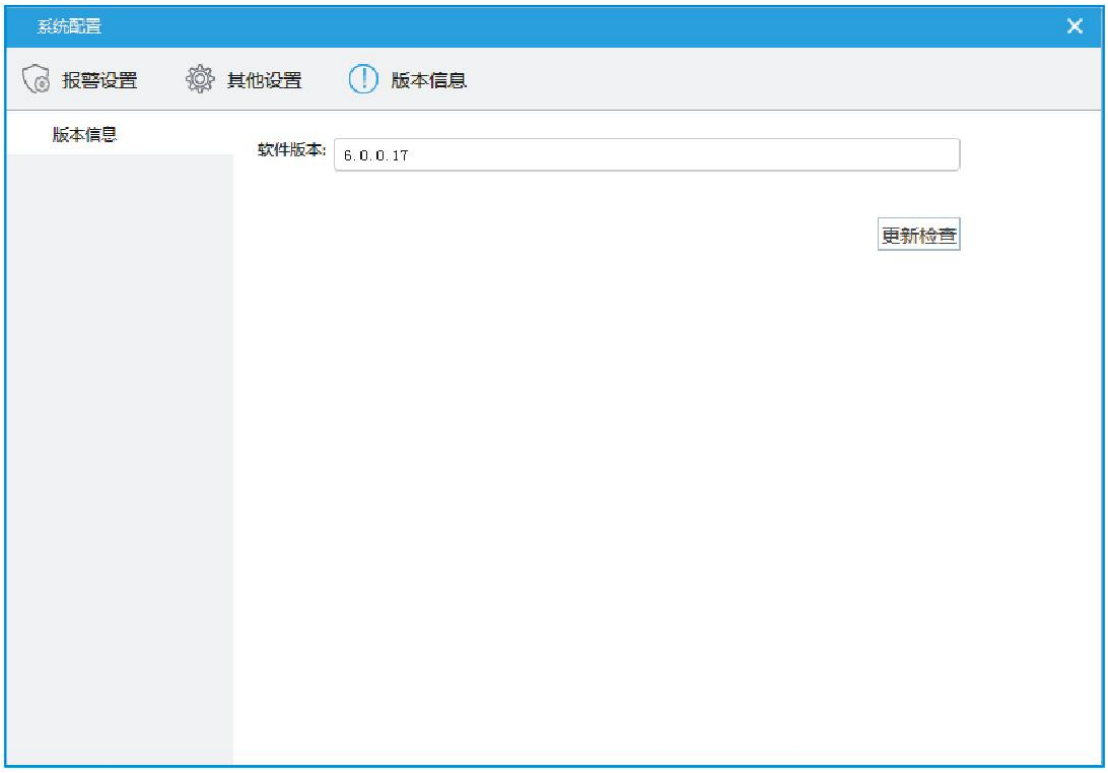


Figure 2-28

12. icon explanation

图 标	含 义	图 标	含 义
	锁屏		本地录像
	开始对讲		抓拍
	开始侦听		对讲音量

第三章 parameter settings

Parameter settings include video settings, alarm settings, smart home, system settings, network settings, version information,

As shown in Figure 3-1. Through parameter setting, operations such as video management, detector and remote control addition, arming and disarming can be performed on the device.

Figure 3-1

3.1 Video Settings

Including video equipment, video scheduling, PTZ settings, color timing.

3.1.1 Video equipment

Set the channel connected to the host (as shown in Figure 3-2).

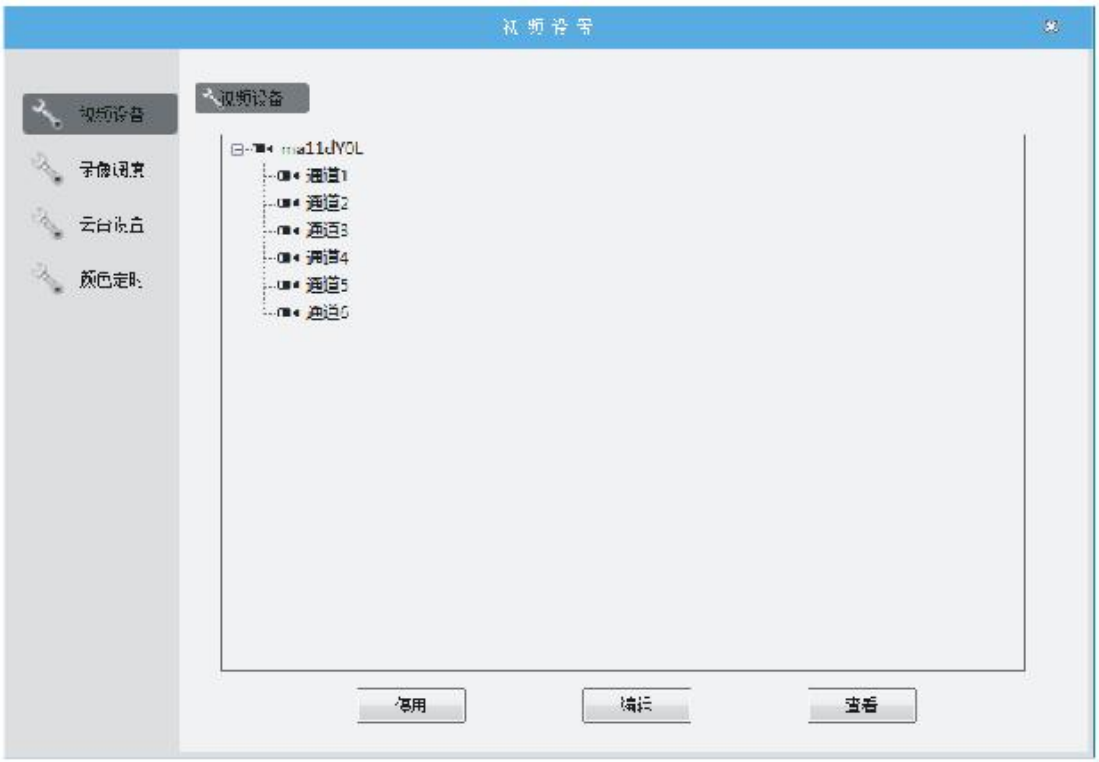


Figure 3-2

Disable: close the selected channel;

Edit: Select the channel and click "Edit", the pop-up window is shown in Figure 3-3.

Figure 3-3

View: As shown in Figure 3-4, view the IP addresses and connection status of all IPCs.

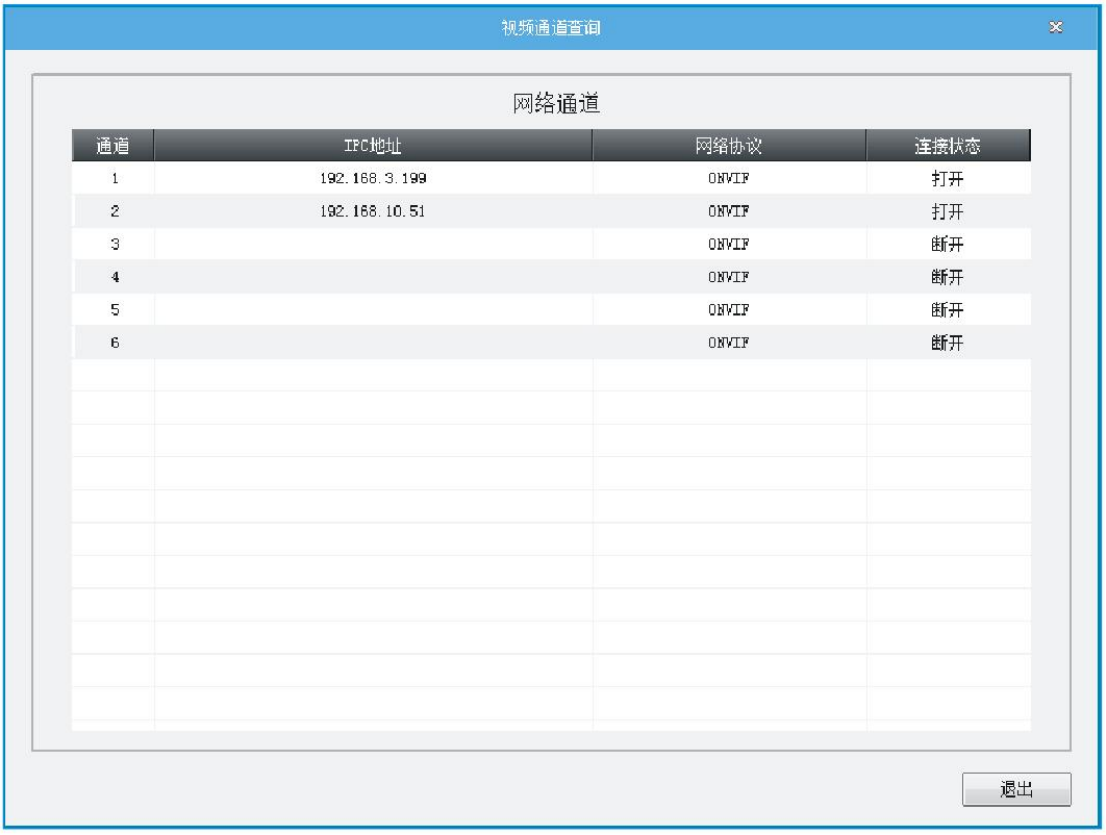


Figure 3-4

Click "Edit" to perform channel setting and IPC search and login.

1) Channel settings

Network protocol: There are three protocols to choose from, namely ONVIF, MA_PRIVATE, and

MA_CMS;
ONVIF: When using the ONVIF protocol, you need to enter the "IPC Search/Login" page first, search for the target IPC on this page, select the IPC, click the "OK" button to return to the "Channel Settings", enter the connection user name and Enter the connection password and click the "Connect" button to complete the IPC connection.
MA_PRIVATE: MA private protocol, the target IPC must be a MA IPC. When using, directly input the IP address, port, user name and user password of the target IPC.
MA_CMS: The application scenario of this protocol is: the user wants the device to be used as a decoder, and a certain video of a certain user on the CMS platform is used as the input of the channel, such as decoding to the wall; input in the box behind the network protocol It is the channel number of the channel where the video to be acquired comes from logging in to the CMS platform device. Please fill in according to the actual situation.
Stream type: The stream type of the IPC access device can be selected. By default, both the main stream and the sub stream are checked.
Note: a. Both main stream and sub stream are unchecked, IPC can be connected, but there will be no video stream.
b. If the main stream is checked and the sub stream is not checked, the IPC can be connected, and the device uses the main stream to record when video comes. However, when requesting the sub stream video from the IE or mobile client, Video data will not be requested.
c. If the main stream is unchecked and the sub stream is checked, the IPC can be connected, and the device uses the sub stream to record. At this time, when the IE or mobile client requests the main stream video from the device, the obtained It is actually a substream.

Domain name: The use of the domain name is related to the selected network protocol. When the network protocol is "ONVIF" and "MA_PRIVATE", the domain name refers to the domain name address of the target IPC; when the network protocol is "MA_CMS", the domain name refers to the CMS platform domain name address;
Port: The use of the port is related to the selected network protocol. When the network protocol is "ONVIF", the port is fixed at 554; when the network protocol is "MA_PRIVATE", the port is fixed at 8000; when the network protocol is "MA_CMS", the port It will vary depending on the server. If the device is automatically authenticated, it is a fixed port and does not need to be filled in. Manually fill in is generally 7809;
Username: The use of the user name is related to the selected network protocol. When the network protocol is "ONVIF" and "MA_PRIVATE", the user name refers to the user name used when connecting to the target IPC; when the network protocol is "MA_CMS", Username refers to the login ID of the user on the CMS platform;
Password: The use of the password is related to the selected network protocol. When the network protocol is "ONVIF" and "MA_PRIVATE", the password is the password used when connecting to the target IPC; when the network protocol is "MA_CMS", the user name refers to the CMS Login passwords of users on the Platform;

2) IPC search/login
As shown in Figure 3-4, select "IPC Search/Login" above, and click the "Search" button to search for all IPCs that support the ONVIF protocol in the LAN where the device is located.

Select the IPC to be added, click "Edit" to log in to the IPC for parameter setting, the login password is the password of the IPC, click "OK" to automatically synchronize the information of the IPC to the channel setting page.

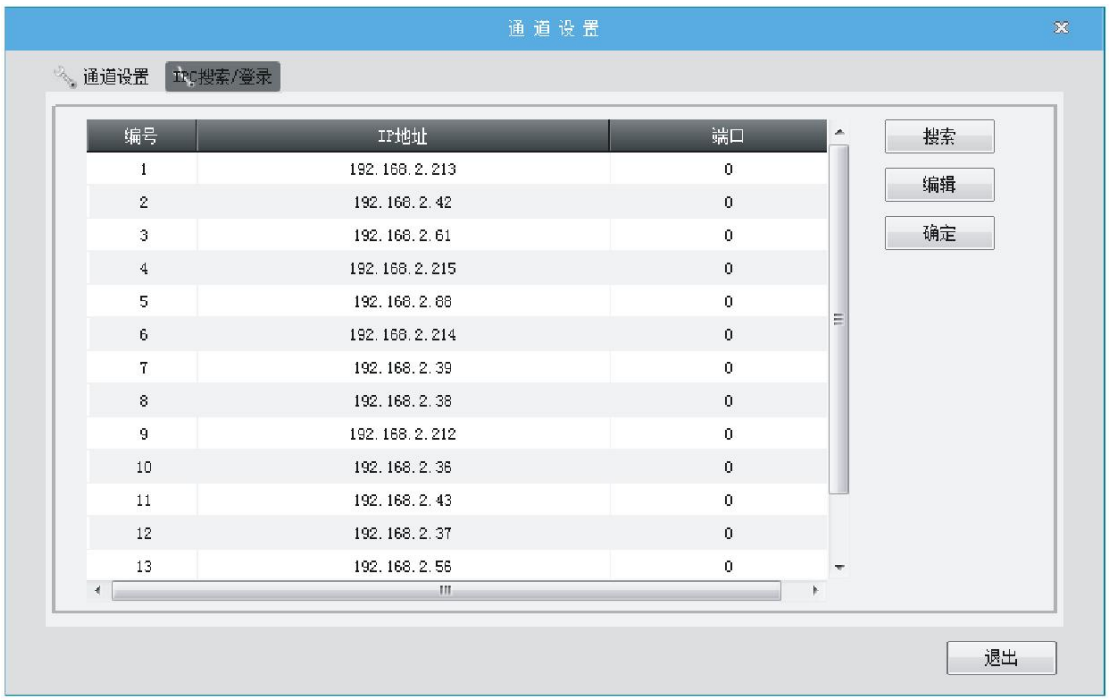


Figure 3-4

3.1.2 Video scheduling

In the video setting window, select "record scheduling" with the cursor, as shown in Figure 3-5.

Figure 3-5

Recording type: refers to the category of recording, which is divided into timing recording and alarm recording.

Timing setting: The user can set the channel, week and time period that need to be recorded according to the needs. Time period setting Each channel has four periods per working day. After setting the time period, you need to check the enable item behind the time period, otherwise the time period will not work.

Precautions:

In the time period, the recording type is only effective for one type. If the timed recording is set, the manual recording will not work in this time period. The priority of alarm recording is the highest, and the priority of scheduled recording is higher than that of manual recording.

3.1.3 PTZ Settings

In the video settings window, select "PTZ Settings" with the cursor, as shown in Figure 3-6.

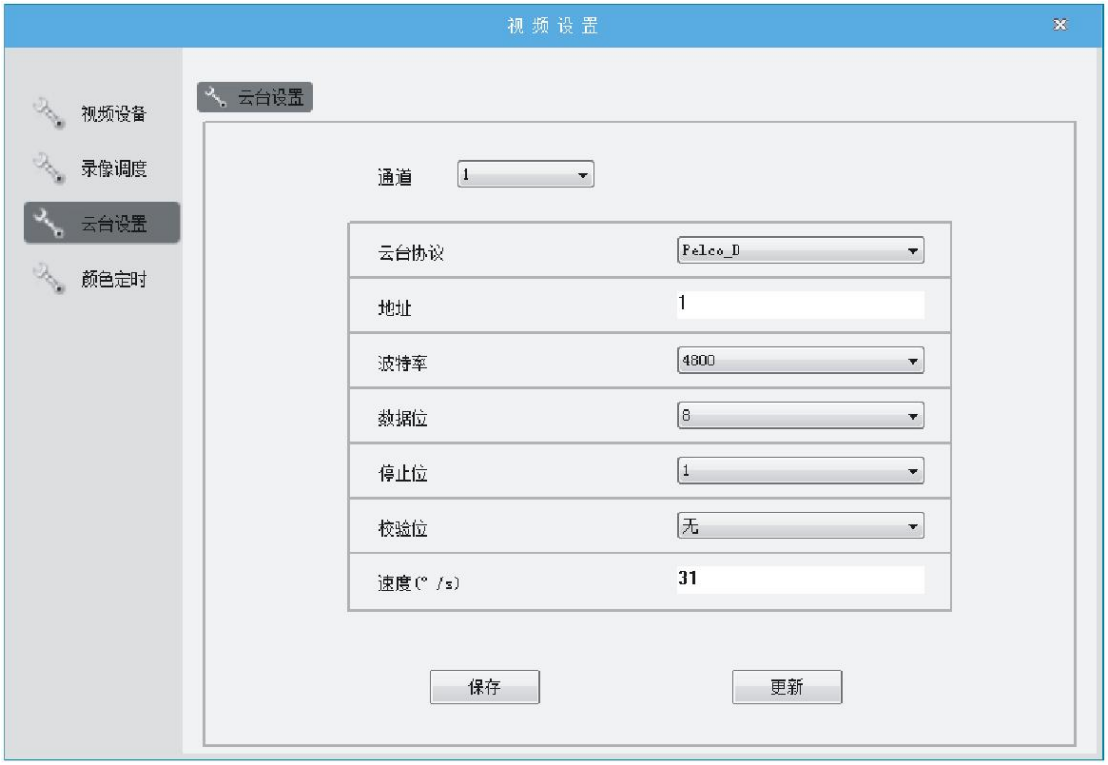


Figure 3-6

Channel: select the channel connected to the camera;

Protocol: Select the camera protocol (Pelco-d) of the corresponding brand model;

Address: set to the corresponding camera address, the default is 01;

Baud rate: Select the baud rate used by the corresponding camera to control the PTZ and camera of the corresponding channel, the default is 9600;

Data bits: 8 by default;

stopbit: 1 by default;

Check Digit: None by default;

Speed: The default is 01.

Note: The address here must be consistent with the address of the camera, otherwise the camera cannot be controlled!

3.1.4 Color Timing

As shown in Figure 3-7, the color timing is to adjust the color of the channel in different time periods.

Figure 3-7

3.2 Alarm Settings

Including alarm host setting, timing arming and disarming, zone setting, remote control setting, equipment alarm setting.

3.2.1 Alarm panel settings

Including system settings, alarm center settings, user dial settings, password settings, GSM settings, partition settings.

3.2.1.1 System Settings

By default, when entering the alarm setting window, it first displays "Alarm Host Settings" - "System Settings", as shown in Figure 3-8.

Figure 3-8

Entry delay: entry delay refers to the time period for the host to delay the alarm after triggering, 001~255 seconds, the default is 10s;

Exit Delay: Exit Delay refers to the time for the user to leave the defense zone before the main unit arming takes effect after the user manually arming or the remote control arming. It can be set between 001 and 255 seconds, and the default is 10s;

Siren time: The siren ringing time after the main unit alarms, it is recommended that the user set it not to exceed 15 minutes (default 5 minutes).

Telephone line detection: Telephone line drop detection, the options are divided into alarm, prompt and no detection. (default alarm)

Detector loss detection time: The time interval for detecting the loss or power failure of the wireless detector. When the host does not receive any signal from the detector within this time period, the host will upload the detector loss information to the alarm center. Default 0 is no detection;

Ringing and off-hook times: the user remotely operates the main unit, dials the main unit number, the number of ringing times when the main unit is off-hook, and the number of ringing and off-hook can be set from 0 to 99 times. When it is set to 00, the telephone remote control operation function is turned off. (default is 7 times)

AC power-down time: AC power-down detection, default 0 does not detect;

Arming and disarming report: Whether arming and disarming is uploaded to the alarm center, it is closed by default;

Prompt sound for arming and disarming: Whether the device emits a beep when arming and disarming;

Always upload to the alarm center: When an alarm occurs, the network will usually be used to upload the alarm information to the network alarm center. When the network fails or the

uploading of information fails, the PSTN will be used to upload the alarm information to the telephone alarm center. If this option is selected , the device will upload alarm information to the network and PSTN at the same time no matter what the situation is, and it is closed by default.

Forced arming: When the defense zone fails, the device is forced to arm, and it is turned on by default;

Alarm limit: If alarm limit is selected, when there are three or more alarms in the same defense area within a period of time, the system will consider this alarm as a false alarm, and will no longer send alarm information to the platform, and it will be closed by default;

Emergency alarm prompt: whether to sound the siren at the scene when an emergency alarm occurs;

Door sensor detection: detect whether the door sensor is open or not, it is closed by default;

3.2.1.2 Alarm center setting

Click the cursor to "Alarm Center Settings", as shown in Figure 3-9.

Figure 3-9

Alarm center number: Two alarm center numbers can be set. When setting the alarm center number, you need to set the center user number at the same time. The two alarm center numbers share the same center user number. Be careful not to set the user phone number as the alarm center number;

Center user code: the number assigned uniformly by the alarm center to distinguish which user the alarm information comes from;

Number of calls from the center: the number of calls made by the device to the alarm center when the alarm center has not been connected for many times. If the number exceeds the number, the call will stop. (5 times by default)
Center test time: It is used for the heartbeat test time of this device and the alarm center, which can be set from 0 to 999 hours.
Line priority selection: When an alarm is triggered, which line will be used to upload the alarm information to the telephone alarm center first, there are two optional lines: GSM line and telephone line. (default GSM line)
After setting, click "Save" - "Update" to take effect.

3.2.1.3 User dial setting

Click the cursor on "User Dial Settings", as shown in Figure 3-10.

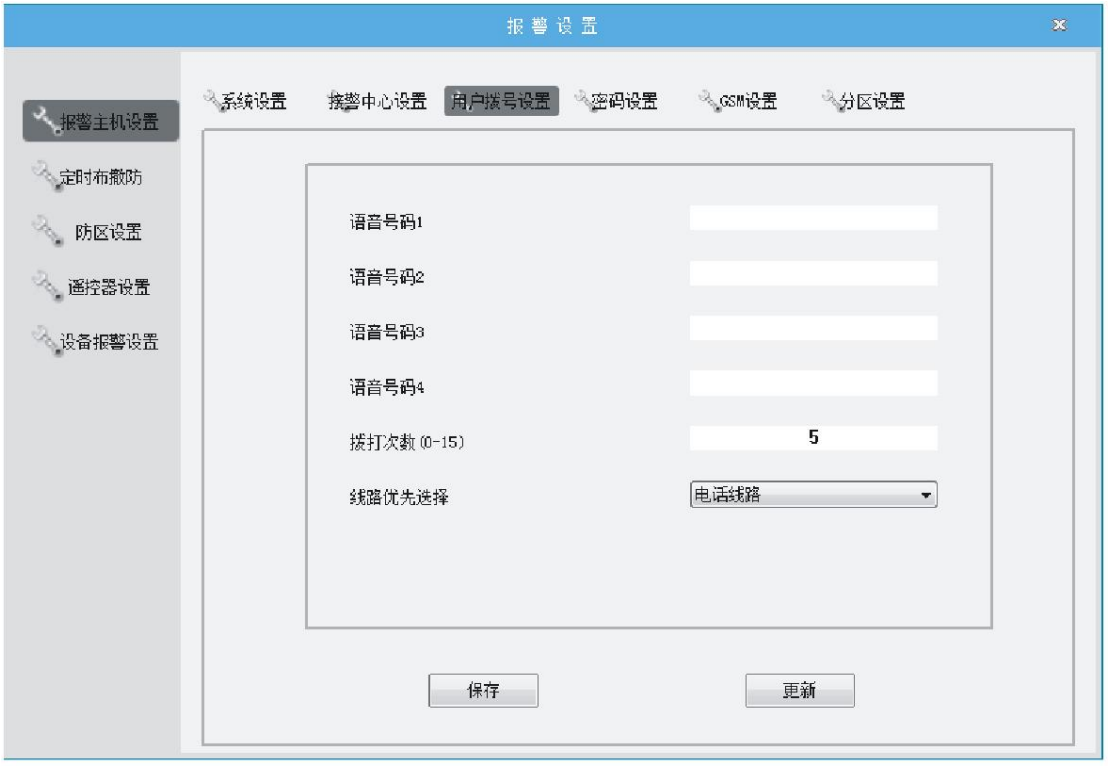


Figure 3-10

Voice number: refers to the phone number that calls the user when the device alarms, including fixed phone numbers and mobile phone numbers. Up to 4 user phone numbers can be set, and a phone number can be entered with a maximum of 17 digits.
Number of calls: refers to the number of calls made by this device to the user when the user's phone has not been connected for many times after the alarm is triggered. If the number exceeds the number, the call will stop. (5 times by default)
Line priority selection: When an alarm is triggered, which line will be used to make a call to the user first, there are two options: GSM line and telephone line. (default GSM line)
After setting, click "Save" - "Update" to take effect.

3.2.1.4 Password setting

Click "Password Settings" with the cursor, as shown in Figure 3-11.

Figure 3-11

Move the cursor to the password setting, click the left mouse button to enter the password setting interface:

Password setting is mainly used to set keyboard operation administrator password and main user password.

Administrator password: refers to the access password for setting alarm panel parameters through the keyboard, and the default is 012345. (When using the keyboard, enter 012345# to enter the parameter setting);

Master user password: Set the user password, the default is 1234, which is used when the user performs arming and disarming and telephone dial-in control.

Ordinary user password: similar to the master user password, it should be noted that the master user password is applicable to all partitions, while the ordinary user password is only applicable to the specified partition.

3.2.1.5 GSM Settings

Click the cursor on "GSM Settings", as shown in Figure 3-12.

Figure 3-12

①GSM communication settings

Before enabling this function, please confirm whether your SIM card meets the requirements of the GSM module. The network supports China Mobile (GSM) and China Unicom (GSM), but does not support Telecom (CDMA)

GSM enabled: After enabling it, you can make calls and send and receive text messages;

GPRS enable: After opening, use GPRS flow for network alarm.

GSM APN: SIM card operator's access point;

GSM user name: the GSM user name of the SIM card, which is empty by default;

GSM password: the GSM password of the SIM card, which is empty by default;

After setting, click "Save" - "Update" to take effect.

② GPRS alarm server settings: see "3.4.2 Platform Settings" on page 34 for details.

3.2.1.6 Partition Settings

Click "Partition Settings" with the cursor, as shown in Figure 3-13.

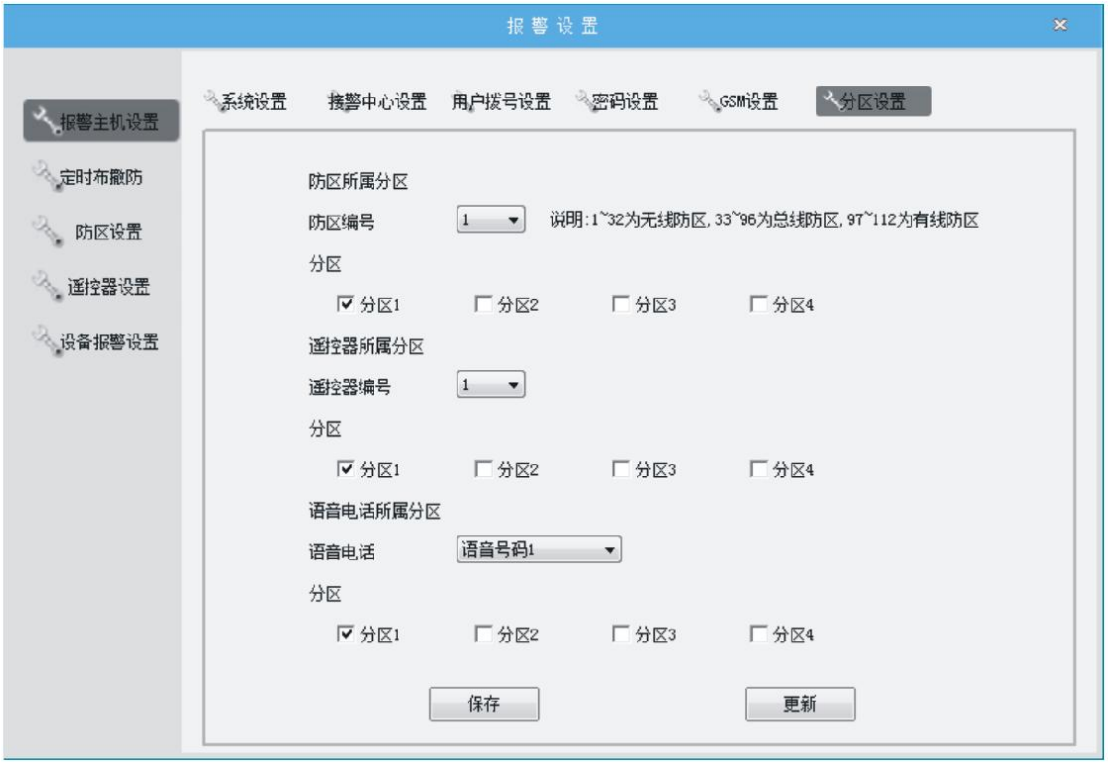


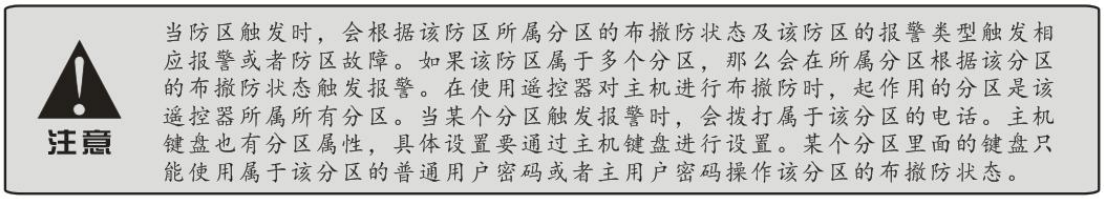
Figure 3-13

Zoning: In a certain area, you can independently enjoy arming, arming, disarming, and alarm without affecting other areas. The model supports a total of 4 partitions.

Partition to which the defense zone belongs: Each defense zone can be set to belong to a partition, which can belong to a single partition or to multiple partitions, but must belong to at least one partition. (By default it belongs to partition 1)

Partition to which the remote control belongs: Each remote control can be set to belong to a partition, which can belong to a single partition or to multiple partitions, but must belong to at least one partition. (By default it belongs to partition 1)

Partition to which the voice call belongs: Each defense zone can be set to belong to a partition, which can belong to a single partition or to multiple partitions, but it must belong to at least one partition. (By default it belongs to partition 1)



3.2.2 Scheduled arming and disarming

Click "Password Settings" with the cursor, as shown in Figure 3-14.

Figure 3-14

The user can set the timing period according to the needs, and ticking "Enable" means enabling it, otherwise, it is considered that this time period is not enabled. Under each time period, there is a partition that the time period applies to. Check a certain partition to indicate that the timing period will act on the partition. If you check multiple times, the time period will act on multiple minutes. , it will not affect any partitions. There are four timing periods in a day, and each period is composed of a timing arming time and a timing disarming time.

注意事项

1、若所设置的时间段的第一个参数大于第二个参数时，所对就在的时间段为第二个参数时间至次日的第一个参数时间。
如：所设时间段为“17：30-8：00”，对应的时间段为17：30至次日的8：00.
2、这些定时布撤防时间段的设置只对盗警和周边警情起作用，其他警情24小时有效。

3.2.3 Zone setting

Click the cursor to "Zone Setting", as shown in Figure 3-15.

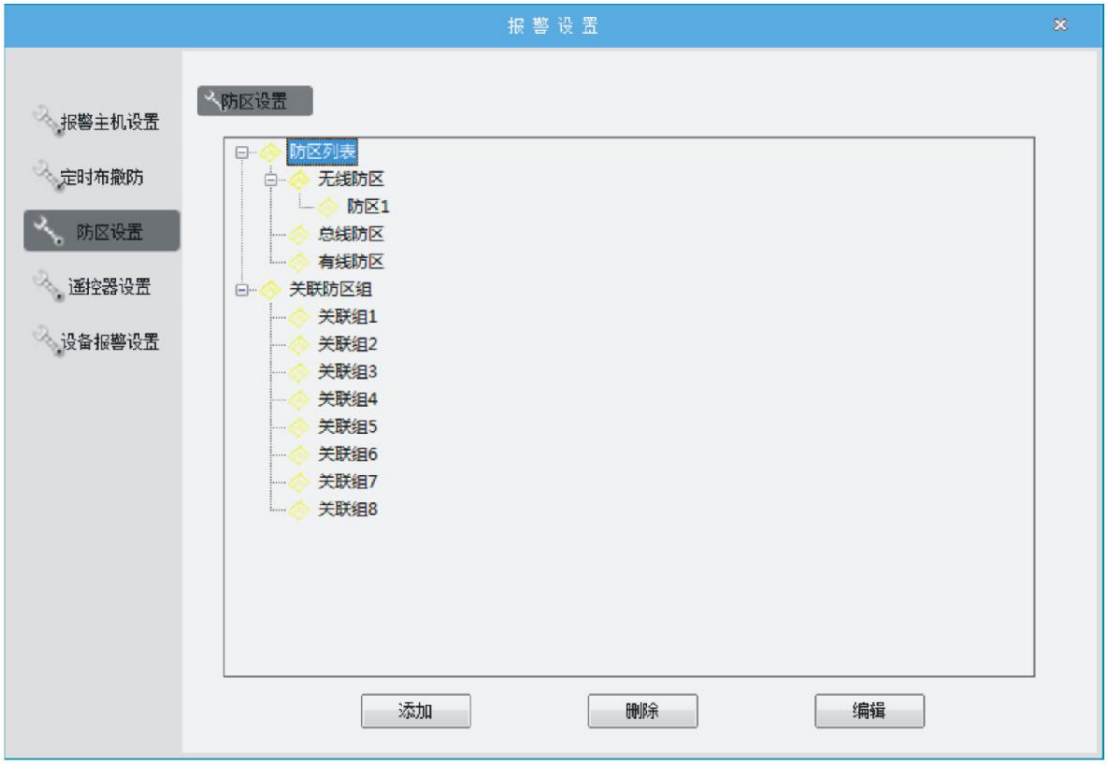


Figure 3-15

The defense zones of the equipment are divided into wireless defense zones (1~32), bus defense zones (33~96), and wired defense zones (97~112).

Zone list

① Defense zone setting

Click "Add" to pop up a window as shown in Figure 3-16, and you can set to add defense zones at this time.

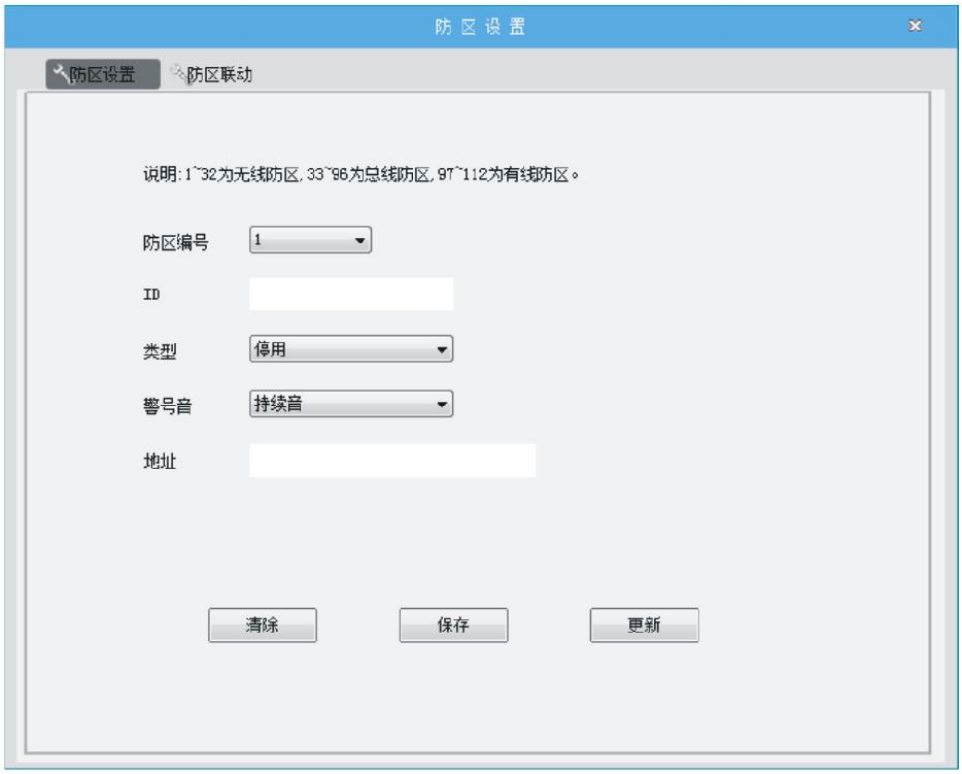


Figure 3-16

Defense zone number: the defense zone number to be added, you can click the drop-down window symbol "▼" to select (in the edit mode, it means the defense zone number currently being set, and it cannot be changed at this time).

ID: Refers to the unique code of the wireless device, which can be input directly against the nine-digit address code on the back of the device.

Type: the alarm type of the defense zone, click the drop-down window symbol "▼" to select ;

Disabled: do not use this zone;

Delay/Perimeter: When it is triggered in the stay or arm state, it will alarm;

Burglar/Emergency/24 Hours/Fire: Alarm will be triggered under any circumstances.

Siren Tone: Whether the siren will sound when the zone triggers an alarm.

Address: the address where the zone is located. In order to know the location of the alarm at the first glance when the alarm is made, the address of the defense zone can be set here.

After setting, click "Save" - "Update" to take effect.

警情内容	盗警	延时	周界	24小时	紧急	火警	停用
外出布防时状态	√	√	√	√	√	√	X
在家布防时状态	X	√	√	√	√	√	X
撤防时状态	X	X	X	√	√	√	X

注意

“√”表示该警情被触发时主机产生报警;
“X”表示该警情被触发时主机不产生报警;
无线防区默认情况下为有效，有线防区均处于停用状态;
警号音可以根据需要设置，建议在警情不同的情况下有所区分，如紧急报警可以设置为静音。

② Defense zone linkage

In the defense zone setting window, the cursor clicks "Defense Zone Linkage", as shown in Figure 3-17.

Figure 3-17

For example: link channel 1 pan/tilt to defense zone 03, channel 2 video to defense zone 03, channel 3 snapshot to defense zone 03, smart switch 1 to defense zone 03, check email notification, and check upload CMS alarm center. When the defense area 03 alarms, the host will link the 1-channel PTZ; send the alarm information and the alarm picture of the 3-channel to the designated mailbox; upload the alarm information, the alarm video of the 02 channel and the alarm picture of the 03 channel to the alarm platform; open smart switch1.

The operation steps are as follows:

1) Add 3 defense zones referring to "①Defense Zone Setting";

2) If the alarm mailbox has not been set before, please refer to 3.4.2.3 Mailbox Settings on page 34 to set it;

3) If the alarm platform has not been set before, please refer to 3.4.3 Platform Settings on page 34 to set it;

4) Select email notification;

5) Select the upload center;

6) Set the gimbal linkage, link channel 1 to defense zone 3;

7) Set video linkage, link channel 2 to zone 3;

8) Set up snapshot linkage, link channel 3 to defense zone 3;

9) Set up smart device linkage, and associate electrical switch 1 with defense zone 3;

10) Click Save.

Associated zone group

In order to prevent false alarms, associate two adjacent detectors as needed. When two detectors are triggered within the set time range, the controller will give an alarm. Only one of the defense zones is triggered, and the defense zone will give an early warning. , playing the warning recording "You have entered private territory, please leave quickly".

Click "Association Group 1" - "Edit", the pop-up window is shown in Figure 3-18,

Figure 3-18

Enable: hit " √ " means enable;

Associated time: The maximum time interval between when a member of an associated zone group is triggered and when another zone in the associated zone group is triggered to cause an alarm for this zone group. When the time interval between the triggering of two member defense zones of the associated defense zone group is greater than the associated time, the defense zone group will not

An alarm will be generated.

The device has a total of 8 associated defense zone groups. When using it, click 'Select Defense Zone' to select members of the associated defense zone group, set the associated time, check the associated defense zone group enable, and click "Save" to complete the setting of an associated defense zone group.

3.2.4 Remote control settings

Click "Remote Control Settings" with the cursor to enter the remote control setting interface.

Click the 'Add' button to enter the remote control setting interface, or select a remote

control and click the 'Edit' button to enter the remote control setting interface, as shown in Figure 3-19.

Figure 3-19

Remote control number: In the edit mode, it indicates the remote control number currently being set, which cannot be selected at this time; in the add mode, it indicates the remote control number to be added, and you can click the drop-down window symbol "▼" to select.

Enable: turn on the remote control;

ID: the identification of the communication between the wireless detector and the alarm host;

Wireless code pairing: Click the "Wireless code pairing" button, the device enters the ID learning mode, trigger the target remote control, you can get the target ID, click "OK" to complete the wireless code pairing. (Note: In order to prevent the wrong ID code from being learned due to external interference, do not rush to click Confirm after obtaining the ID code, first confirm whether the obtained ID is the target ID)

Username: The user of the remote control, mainly for the convenience of knowing who is operating when arming and disarming.

Emergency associated channel: when the emergency alarm button on the remote control is pressed, the channel associated with the alarm.

After setting, click "Save" - "Update" to take effect.

Note: The emergency associated channel is different from the zone associated channel. The associated channel is only popped up on the platform client, IE, intranet client, and local interface when an emergency alarm is triggered on the remote control.

3.3 System Settings

Including basic settings, log query, hard disk management, factory settings, scheduled maintenance, update backup, and device installation.

Figure 3-20

3.3.1 Basic Settings

By default, the system first enters the basic settings when entering the system settings.

System time: used to modify the current date and time of the device; (Note: If the modified system time is earlier than the current time, the recording between the modified and before the modified will be erased.)

Date format: The format used to select the date display includes year-month-day and day-month-year;

Time format: The format used to select the time display includes "24 hours" and "12 hours";

Video format: used for video signal formats, including PAL and NTSC, the system defaults to PAL;

Package size: used to set the video package time length, divided into 15 minutes, 30 minutes, 45 minutes, 60 minutes;

HDD overwrite type: You can choose not to overwrite or overwrite; the conditions for not overwriting recording are: the current working disk is being overwritten, or the current working disk is just full, and the next disk is not empty, and the recording will stop. If the hard disk is full at this time, it will be abnormal When the alarm is turned on, a hard disk full alarm will be generated; the condition for overwriting is: the current working disk is just full, and the next disk is not empty, and the earliest video file will be cyclically overwritten;

Resolution: The resolution of the VGA output interface, the existing VGA(1024*768), VGA(1280*1024), VGA1440*900, HDMI1920*1080;

Device language: There are two interfaces, Chinese and English, for selection;

3.3.2 Log query

Date: the date of the log to be queried;

Log type: the type of log to be queried, there are alarm log, operation log and system log to choose from;

search: start searching logs;

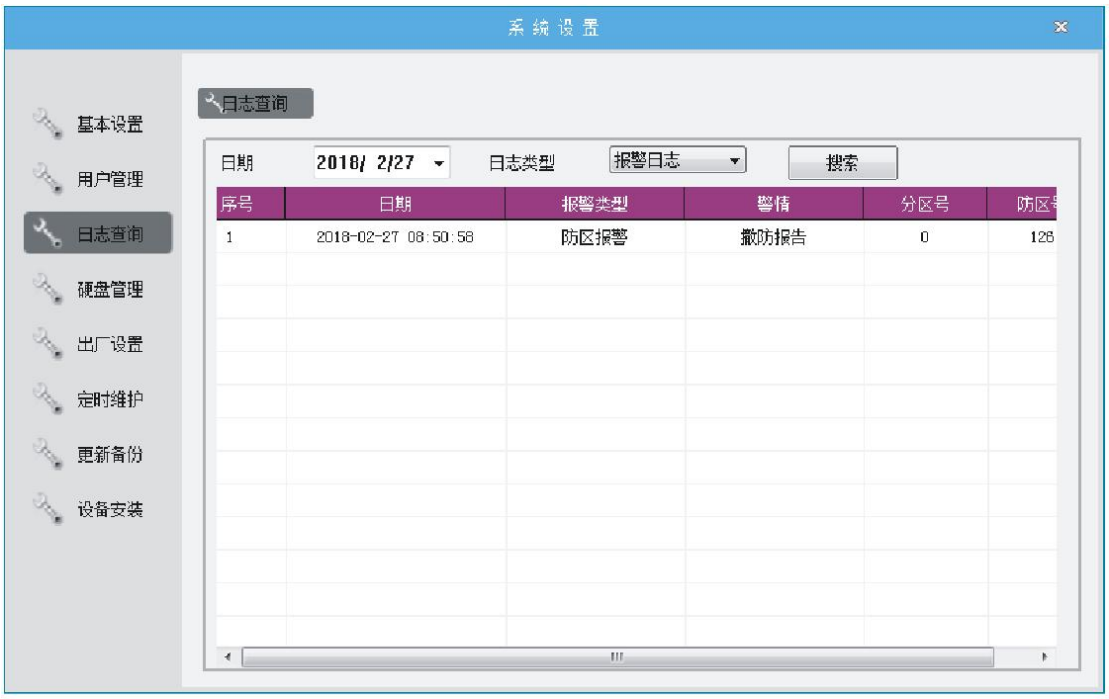


Figure 3-21

3.3.3 Hard disk management

View the hard disk connection and capacity information, or click "Format" to clear the hard disk.

3.3.4 Factory settings

As shown in Figure 3-22, the user selects the setting items that need to be restored according to the needs. If this function is used, the previous corresponding settings will be restored to the factory settings. Please use it with caution.

Figure 3-22

3.3.5 Scheduled maintenance

As shown in Figure 3-23, set the automatic restart date and time of the system, and you can select multiple options. Once selected and saved, restarts occur at the same time every week.

Figure 3- 23

3.3.6 Update backup

As shown in Figure 3-24, click " ··· " to select the upgrade file, click "Device Upgrade" to upgrade the system, and the system will restart after the upgrade is successful.

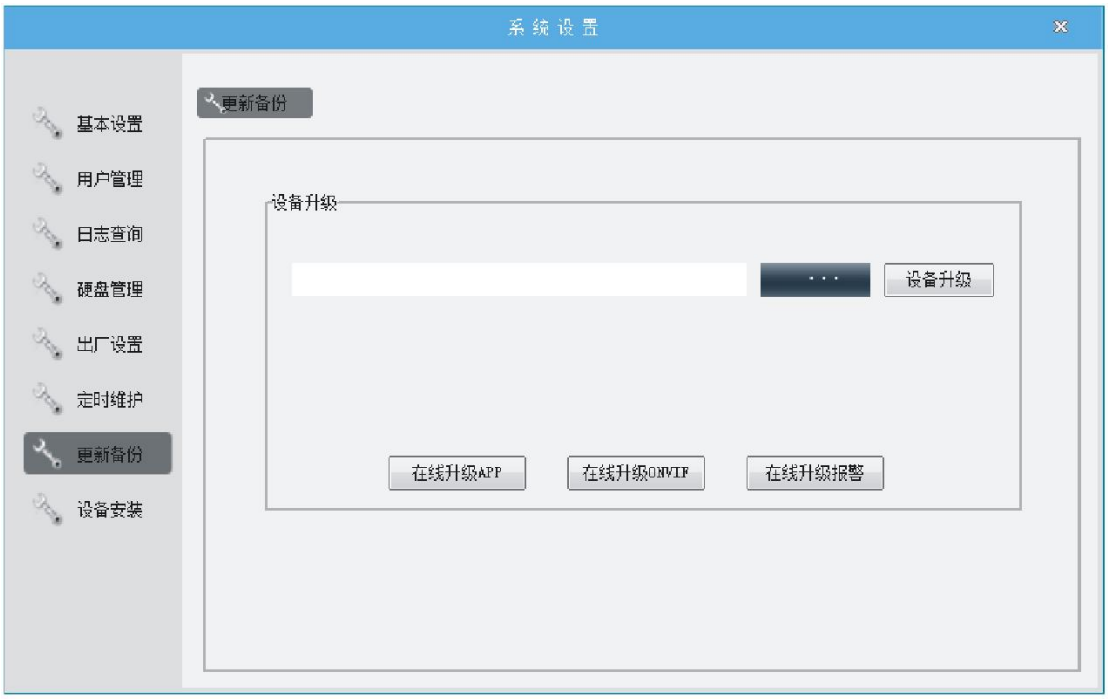


Figure 3-24

3.3.7 Equipment installation

Click "Device Installation" with the cursor, as shown in Figure 3-25.

Figure 3-25

Number of installed hard disks: The number of installed hard disks refers to the number of hard disks actually placed in the device by the user during installation. When the number of hard disks detected by the system is less than the number of installed hard disks and the hard disk loss alarm is enabled, the hard disk loss alarm is triggered.

Installed video channel: The installed video channel refers to the video channel that the user actually accesses the device during installation. When the device is turned on, it detects the channel with video signal input, and triggers a video loss alarm when it detects that the channel is specified for installation but no video input signal is detected and the video loss alarm is enabled. This function is a supplement to the video loss alarm.

Start-up video channel missing detection delay time: refers to the time interval from the system startup to the system starts to detect the installed video channel.

3.4 Network settings

Including basic settings, advanced management, platform settings, IP filtering.

3.4.1 Basic Settings

By default, click the "Network Settings" pop-up window to enter the basic settings first.

Figure 3-2 6

3.4.1.1 Network Settings

Obtain IP automatically: Obtain IP address dynamically from the router.

Static IP address: Use the IP address given by the user.

Default IP: 192.168.1.106
Subnet mask: 255.255.255.0
Default Gateway: 192.168.1.1
Primary DNS: the IP of the local primary domain name server of the network used by the host;
Secondary DNS: the IP of the local secondary domain name server of the network used by the host;
The MAC address is assigned by the manufacturer;
Users can modify IP and MAC addresses as needed.

3.4.1.2 Port Settings

UPNP settings: UPnP (Universal Plug and Play), Universal Plug and Play, is a collective name for a set of protocols, and a simple understanding is UPnP = "automatic port mapping".
If you need to map the port in the LAN, UPNP is enabled by default for WEB mapping port, video mapping port, platform alarm mapping port and mobile phone browsing mapping port, and the port number is set according to the requirement. It is recommended to set the port number between 1024--65500 .
Port mapping is actually a kind of NAT address translation that is often said. Its function is to translate the address on the public network into a private address. The ADSL broadband router using routing mode has a dynamic or fixed public network IP. ADSL is directly connected to the On the HUB or switch, all computers share the Internet.

The listening port refers to the local area network. If some routers are blocked or other devices need to use the default ports of this machine, such as port 80, port 8000, port 9000, etc., you need to use the listening port when browsing in the local area network. To listen to port settings, the device needs to be restarted.

Figure 3-2 7

For example: the internal network IP of this machine: 192.168.1.69, applied for an external network IP: test.3322.org, set the WEB port number as 2001, the video mapping port as 2002, the mobile phone browsing mapping port as 2003, and the WEB listening port It is 3000, the video listening port is 3001, and the mobile phone listening port is 3002. How should I browse the internal/external network?

答： 外网浏览： WEB浏览：http://test.3322.org：2001（IE端浏览）
视频浏览：http://test.3322.org：2002（客户端浏览）
手机浏览：http://test.3322.org：2003（手机需在支持的型号之内）
内网浏览： WEB浏览：192.168.1.69：3000（IE端浏览）
视频浏览：192.168.1.69：3001（客户端浏览）
手机浏览：192.168.1.69：3002（首先手机需在所支持的型号之内，
其次使得手机在内网以内，如手机支持WIFI，路由器具有无线功能）

3.4.2 Advanced Settings

3.4.2.1 PPPOE setting

PPPOE (on\off): Define whether PPPOE is enabled, and the general system defaults to "off"
Account: for the username provided by the ISP
Password: The password corresponding to the username provided by the ISP.

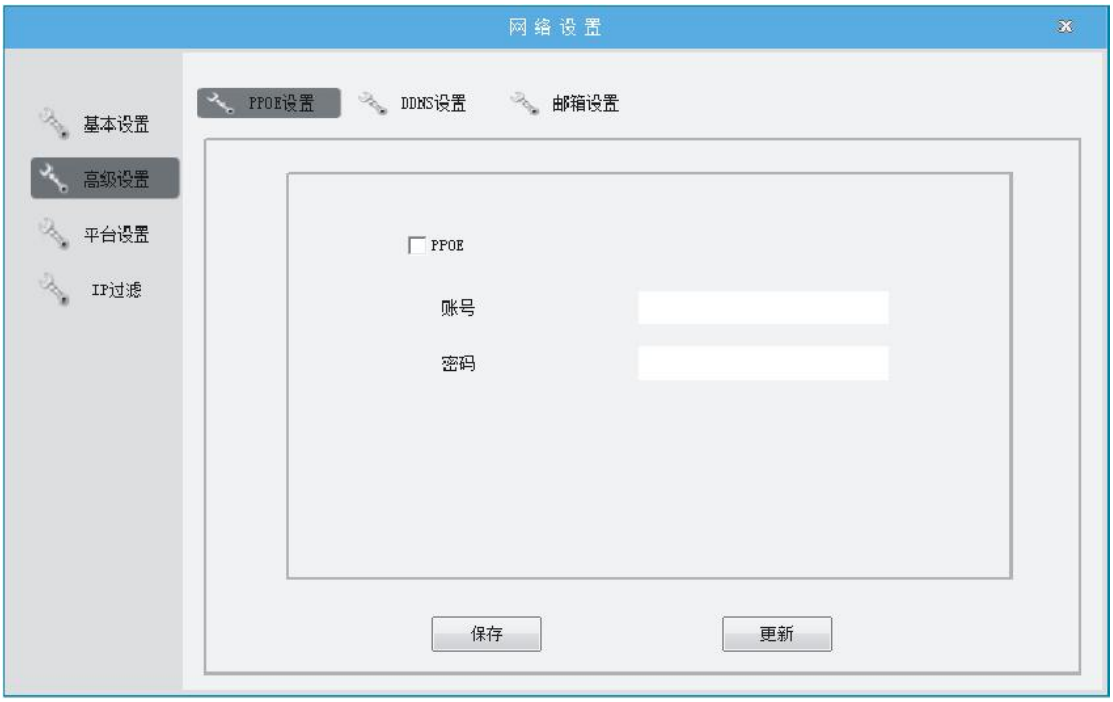


Figure 3-2 8

注意事项

当启用PPPoE拨号上网时，输入用户名和密码后，点击保存退出，等1分钟后再进入网络设置界面，可以在PPPoE的IP栏看到获取到的IP；另外当设备重新启动后，设备会自动重新拨号，获取新的IP地址。

3.4.2.2 DDNS settings

Click "Advanced Settings" - "DDNS Settings" with the cursor, as shown in Figure 3-29 .

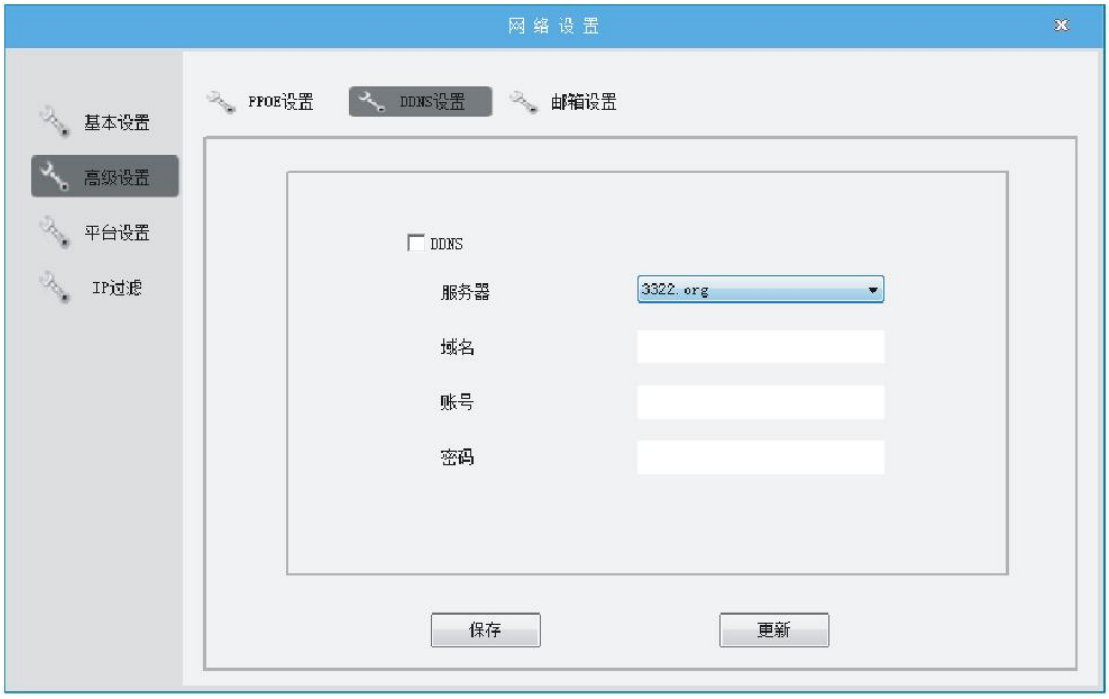


Figure 3-29

DDNS maps the user's dynamic IP address to a fixed domain name resolution service. Every time the user connects to the network, the client program will transmit the host's dynamic IP address to the server program on the service provider's host through information transfer. , the server program is responsible for providing DNS services and realizing dynamic domain name resolution. That is to say, DDNS captures the IP address that users change each time, and then corresponds it to the domain name, so that other Internet users can communicate through the domain name.

If you need to browse videos in the WAN, first set forwarding in the router, and then you need to apply for a free domain name on the Xiwang server, and then fill in the domain name, account number and password at the time of application under this setting item, save and pass WAN browsing.

3.4.2.3 Email Settings

Mailbox setup steps:

1) Find and fill in the domain name of the SMTP server for sending emails;

2) Fill in the receiving email address;

3) Fill in the sending email address, which can be consistent with the receiving email address;
4) Fill in the sending email password;
5) Click Save.

3.4.3 Platform Settings

3.4.3.1 Server Settings

Under this setting item, you can set the IP of the alarm platform/registration platform. If you need to upload the alarm information to the platform, you need to apply for a registration ID before you can upload the information; the opening and closing of the platform will restart the machine.

Use authentication server: After checking and saving, the device will automatically find the corresponding server to log in. After checking, manually setting the platform will not be enabled.

Heartbeat time: refers to the time interval for the device to send a heartbeat message to the platform according to the last message sent. Every heartbeat interval, the device will send heartbeat information to the platform. After the platform receives the heartbeat information, it will record the time of receiving the heartbeat this time. If the heartbeat information of the device is not received for 4 consecutive heartbeat intervals, it will be considered that the device is offline or offline, and this time will be recorded in the platform data. offline.

Synchronize to the GPRS alarm receiving platform: refers to synchronizing the address port information of the platform server, user ID and password information to the GPRS alarm receiving server settings.

Figure 3-30

3.4.3.2 FTP Settings

FTP is used for bi-directional transfer of control files over the Internet. Through it, users can connect their devices to all servers running the FTP protocol around the world, and access a large number of programs and information on the servers. The main function of FTP is to allow users to connect to a remote computer (the FTP server program is running on these computers) to view the files on the remote computer, and then copy the files from the remote server to the local device, or send the files of the local device to remote server.

Figure 3-31

3.4.4 IP filtering

Under this setting item, you can set which IP addresses are allowed to access the machine or which IP addresses are not allowed to access the machine. IP filtering has two working modes: whitelist filtering and blacklist filtering. In the white list filtering mode, only the IP addresses in the IP list are allowed to access the machine; in the black list filtering mode, all IP addresses except the IP addresses listed in the IP list can access the machine.

Figure 3-32

3.5 Version Information

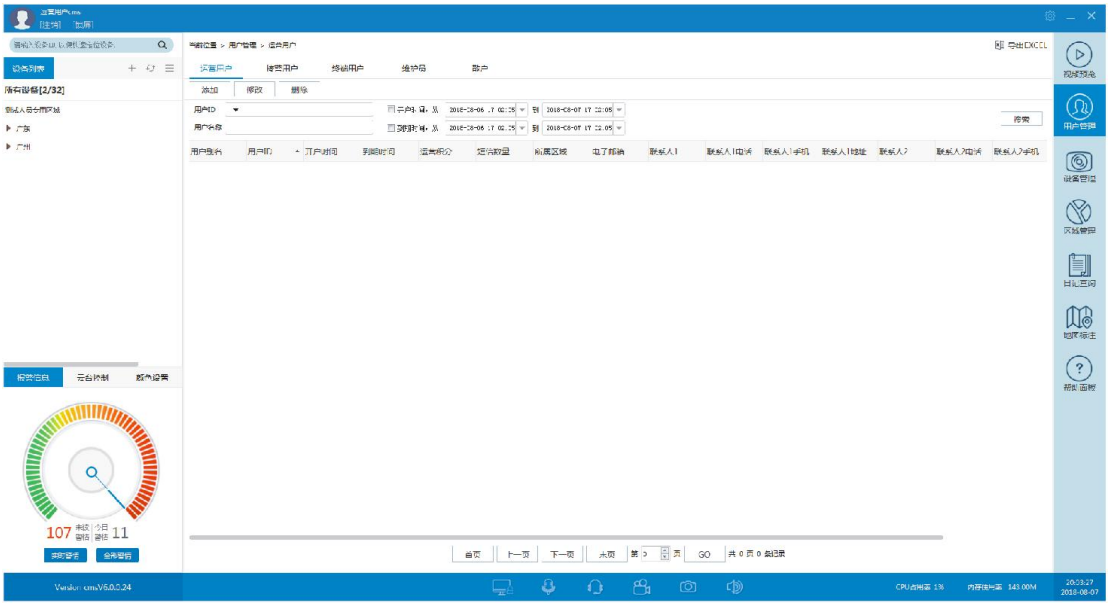
View information such as the number of device channels, the number of defense zones, software and hardware versions, etc.

第四章 function list

The function list includes "video preview", "user management", "device management", "area management", "diary query", "map annotation", "order scheduling", "work order management", "statistical analysis", "Help Panel" ten items. "Video preview" is the user's video viewing item, right click on the device - "Preview" will display the video to be previewed. The functions of "Send Order Scheduling", "Work Order Management", and "Statistical Analysis" in the list have not yet been opened, so stay tuned.

4.1 User Management

Click "User Management" with the cursor, as shown in Figure 4-1.



Pic 4-1

User categories are divided into super users, operation users, alarm users, end users, maintenance personnel and retail investors. The operating users are installed, managed and maintained by the operator in a unified manner. Most of them are public places such as schools, hospitals, banks, and community security kiosks. Retail investors purchase and install the company's equipment for individuals. Without the operator or its centralized management, the equipment is managed and managed by itself. The configuration is mostly used by shops, small and medium-sized companies and families; this manual uses operating users as an example to describe various functions, and other types of users please refer to it.

Various user descriptions are shown in the table below:

用户类型	权　限	管理区域	帐号创建者
超级用户	所有权限	所有区域	美安公司
运营用户	管理接警/终端用户/维护	所分配区域	运营商或美安公司
接警用户	处理终端用户的警情	所分配区域	运营用户
终端用户	设备所属个人帐号，设备	设备所在区域	运营用户
维护员	临时安装设备，无操作权	————————	运营用户
散　户	设备所属个人帐号，设备	设备所在区域	自行注册或运营商

Different user types have different functions after login, as shown in the table below, tick " √ " for the functions that the user has, and tick "×" for the functions that do not have.

功能 / 用户类型	视频预览	用户管理	日记查询	地图标注
接警用户	√	√	√	√
终端用户	√	√	√	√
维护员	√	√	×	√
散　户	√	√	√	√

The "User Management" function after the alarm receiving user, terminal user, maintainer and retail account log in only displays the current user information, as shown in Figure 4-2, the user can click the input column to modify information other than the category, login user name, and account opening time.

The login password must be consistent with the confirmation password;

Account opening time: when the account was created;

Rights Management: View the rights assigned to users.

After modifying, click "Modify" to save.

Figure 4-2Figure 4-3

Super users and operating users can add, modify, and delete other accounts (including operating users). They can also double-click the retail account to enter the user profile of the retail account, and click "Change User Type to Operation" to convert the retail account into an operating user.

4.1.1 User Addition

For example: to add an operation user, please follow the steps below:

Click "Operation User" - "Add" with the cursor, and the pop-up window is as shown in Figure 4-4.

Figure 4-4

Operation credits: credits assigned by super users or operators to operating users. 1 credit is 1 year. When the account expires, the user needs to pay and recharge before continuing to use it. If operating user A creates operating user B, the operating points assigned to operating user B will be deducted from operating user A. (Only the operation user needs to set this item)

Number of text messages: the number of all text messages sent by the system to the user's contacts, up to 16 digits can be entered.

Region: The region managed by the operating user. The region needs to be set in the "Regional Settings" in advance, and click " " to select.

Account Opening Time: The time the user was created.

Expiration time: The expiration time of the device, the default is one year, the user can click the button "▼" in the drop-down window to modify it.

Items with "*" are required. After inputting, click "Add" to complete. For other user additions, please refer to the operation user addition method.

4.1.2 User modification

Select a user, click "Modify" to pop up the user profile of the user, you can modify information other than the type, login user name and account opening time, and click "Modify" to complete the modification.

4.1.3 User deletion

Select a user, click "Delete" to pop up a window as shown in Figure 4-5, click "OK" to delete, and the deleted user will not be able to log in to the platform.

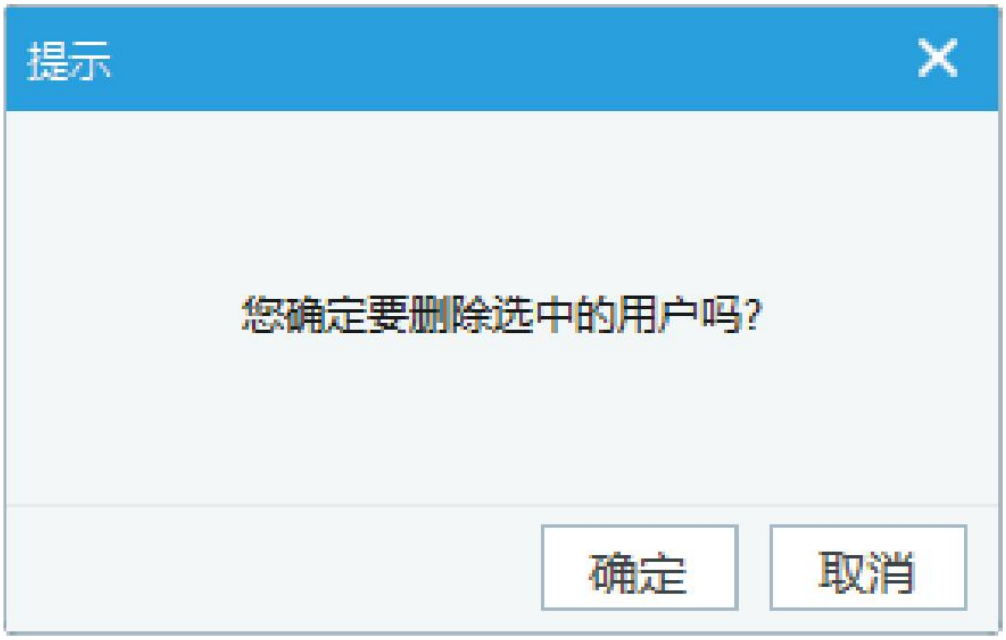


Figure 4-5

4.1.4 User Search

If no user ID, user name, account opening time and expiration time are not checked, select a certain category of users, such as "alarm users" and click "Search" to find all users of this category. If you search for a user according to the account opening time or expiration time, you need to tick " √ " before the account opening time or expiration time and click "Search".

4.2 Device Management

4.2.1 Handling preallocation

This item is set to add platform usage after the maintainer installs the device.

Specific steps are as follows:

A. Connect the device to power and network;

B. Use the maintenance account to log in to the APP and scan the QR code at the bottom of the device to add the device to the APP;

C. Long press the device icon in the APP, select "Pre-allocated device", and click "Submit" after setting the allocated device interface;

D. After the submission is successful, the device will be displayed in "Device Management" - "Processing Pre-allocation" in the operation user to which the maintainer belongs, as shown in Figure 4-6.

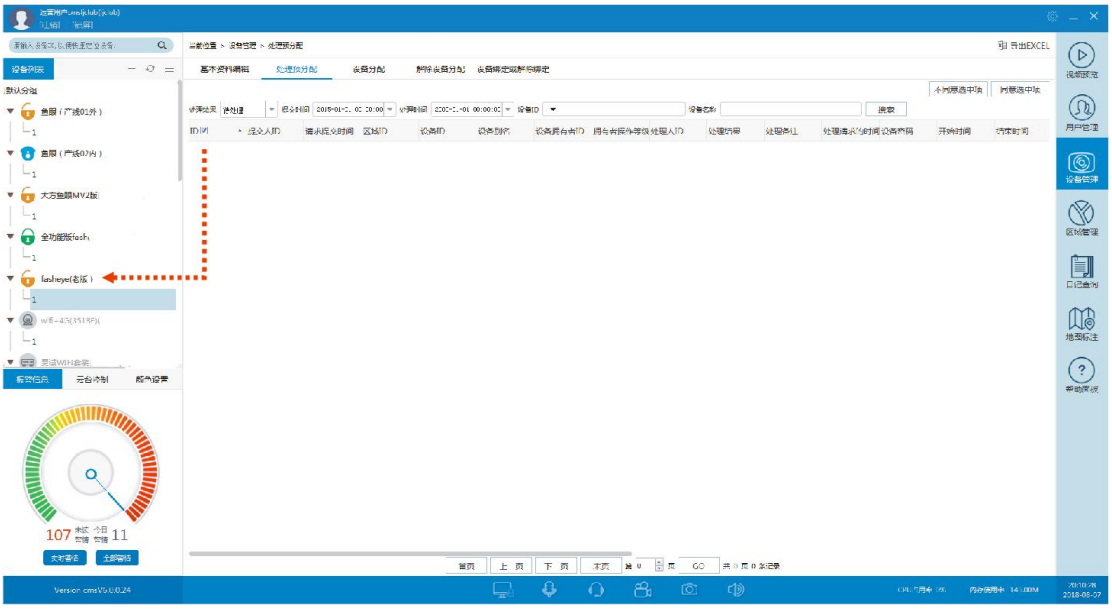


Figure 4-6

E. Put " √ " in front of the pre-allocated item and click "Agree to the selected item", and the device will appear in the device list.

4.2.2 Device Allocation

Device allocation is to assign devices in the device list to users. Click "Device Assignment", as shown in Figure 4-7.

Figure 4-7

Right-click the device in the device list on the left, and select "Modify Device Information" to view the device information. Users can fill in the information in "Modify Device Information".

The default permission type is advanced operation permission;

Assigned to User: The ID of the user who will manage the device.

After setting, click "Assign" to complete.

4.2.3 Deallocating a device

Click "Remove Device Allocation", as shown in Figure 4-8.

Figure 4-8

Enter the device ID and device owner and click "Deallocate".

4.2.4 Bind or unbind the alarm user equipment

Click "Device binding or unbinding" with the cursor, as shown in Figure 4-9.

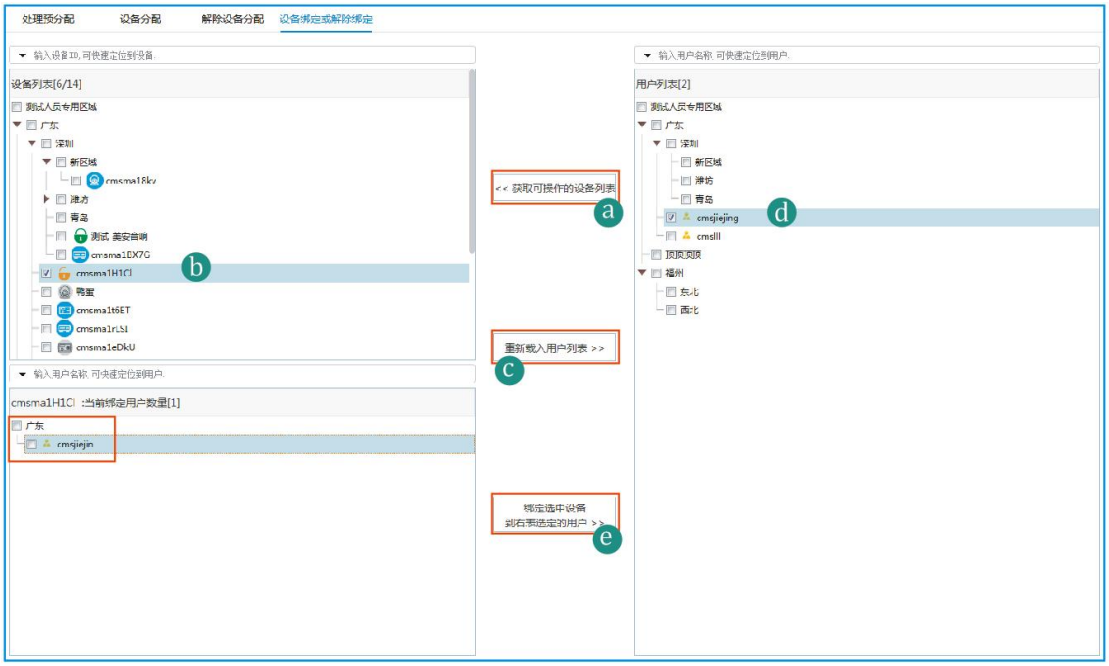


Figure 4-9

This function is applicable to alarm receiving users. When an alarm is triggered on the device bound to the alarm receiving user or maintenance personnel, the user can receive and handle the alarm.

device binding

The specific operation steps are as follows: (see Figure 4-9 mark)

a. Click "Get operable device list";

b. In the device list, tick " √ " before the device to be bound;

c. Click "Reload User List";

d. Put " √ " in front of the user to be bound;

e. Click "Bind the selected device to the user selected in the right table", and the bound user will appear in the bound user list, and the binding is completed.

unbind

The specific operation steps are as follows:

① Select the device to be unbound in the operable device list, and the user bound to the device will appear at the bottom left;

②Put " √ " in front of the user you want to unbind and right-click, a pop-up window will pop up "Unbind all users/Unbind selected users". After selection, a pop-up window will prompt whether to unbind, as shown in Figure 4-10 (all users) , click "OK" to complete.

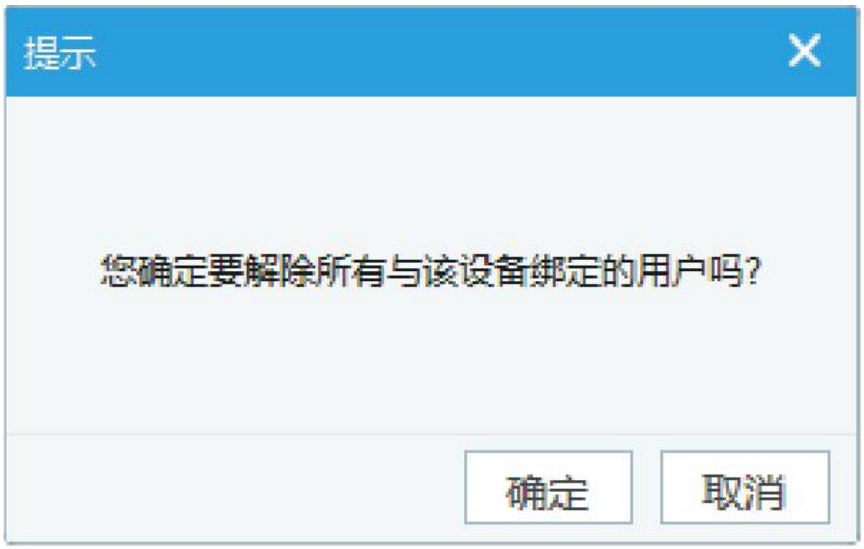


Figure 4-10

4.3 Territory Management

Areas can only be added by super users or operating users, as shown in Figure 4-11, right-click on the area and the item "Add/Delete/Modify Area" appears, and super users or operating users can add any area according to their needs.

Figure 4-11

4.4 Log query

The log query includes "alarm information", "operation statistics" and "user log". Users can view alarm information, user arming and disarming, device offline and other information through log query.

Figure 4-1 2

4.4.1 Alarm information

Unread alerts: Alerts that have not been read. Users can search by alarm type, alarm time period, device ID and device name, and click the drop-down window "▼" to select the device search method. Double-click the alert pop-up window as shown in Figure 4-13.

Figure 4-13

Real-time preview: click to view the current video of the alarm channel;

Alarm situation: alarm type;

Alarm status: the status of the current alarm information;

Alarm code: alarm code;
Time: alarm trigger time;
Channel: the video channel associated with the zone;
Picture: The picture captured when the alarm situation is triggered;
Defense zone: the defense zone where the alarm is located;
Recording: The video recorded by the channel when the alarm is triggered. In "Parameter Settings" - "Defense Zone Settings", check "Defense Zone Linkage" to automatically record when the defense zone is triggered;
Handling opinion: the precautions for handling the alarm, the user can set it by himself;
Previous/Next: Unread alarm information to switch;
Receiving an alarm: After receiving an alarm, it means that the alarm has been dealt with.
Unhandled alarms: Alarms that have been reported to the center but not received by the police officers.
In-progress police situation: The police receivers have already received the police, and currently dispatched personnel are processing the police situation.
Handled alarm situation: the alarm situation that the alarm receiver has received the alarm and has completed the processing of the incident.

4.4.2 Operation Statistics

Operational statistics record information such as user login, logout, arming and disarming, and payment. You can also select the alarm type, search time period, and enter ID or name in the drop-down window to search. Operational statistics include "arming diary", "disarming diary", "alarm diary", "device going online and offline", "expired equipment", and "payment log".

Arming diary: the information that the device enters the alert state when going out arming or staying arming;
Disarm diary: information about disarming the device and canceling the alert state;
Alarm log: information about the device triggering an alarm;
Device on and off line: information about device login/logout;
Expired equipment: equipment information that has reached the expiration date;
Payment log: the record of user renewal usage.

4.4.3 User logs

Record user login and logout information, including alarm receiving users, operating users, and end users.

4.5 Map labeling

The map label shows the location of the device on the map. You can also use the tool on the lower left to mark the location, or you can locate it by geographic location or device ID.

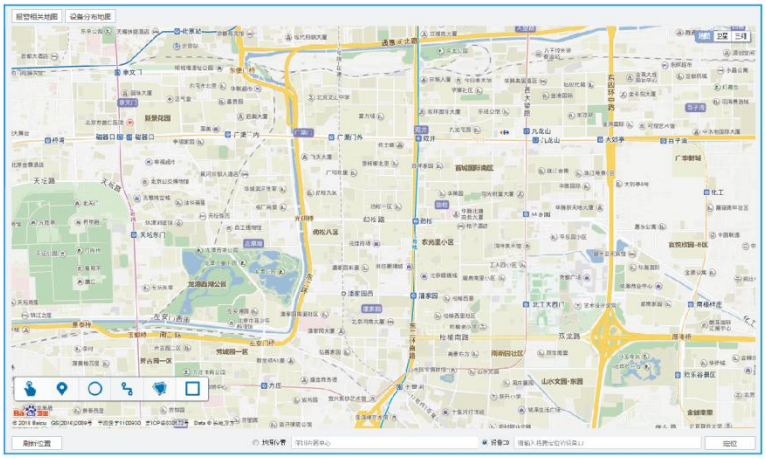


Figure 4-1 4

4.6 Help panel

Click "Help Panel" and a pop-up window will appear as shown in Figure 4-15. Users can complete the settings by following the prompts according to their needs.

Figure 4-1 5