Focus®

user manual

N et L ocal

P / N : 2 0 2 1 0 1 0 3 A 0 1 Subject to version update without prior notice

Chapter 1 Account Login and Device Management

1. Introduction

The LAN management tool adopts multi-thread technology, which can quickly search and add all devices in the LAN, which is convenient for users to manage in a unified manner. Tube

In the management tool, operations such as adding and managing devices, viewing/recording video, arming and disarming can be performed.

NetLocal

2. Account login

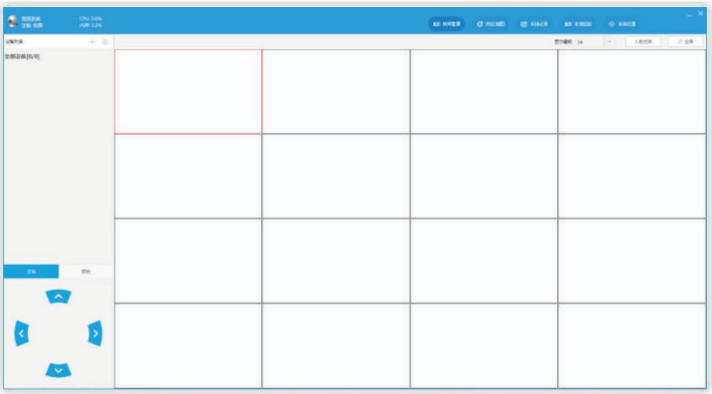
The default user account is admin, and the password is blank, just click "Login".

3. Device Management

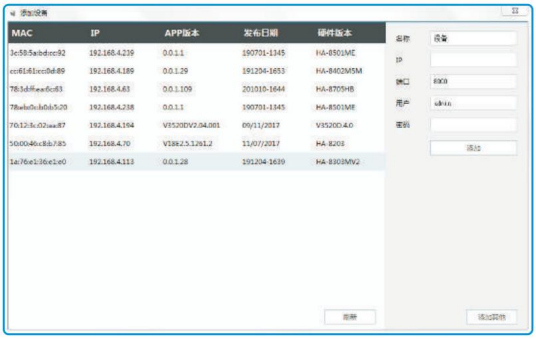
3.1 Device Addition and Deletion

Modify the IP address and gateway; select the device to be added - enter the user name and password of the device on the left side of the window, the default port of the video alarm host and camera is 8000, and the network alarm host is 18034 - click "Add" to enter the Find Devices in the submenu on the left. (The user name and password are detailed in the instruction manual. If there is any change, please refer to the changed one.)

Delete: Select the device in the submenu bar of the main page - click the right mouse button - select "Delete Device".



home page



add device

Icon Description

	NVR offline		camera offline		Control Panel Offline
	Device disarmed		Device Arming at Home	Device Arming	

3.2 Right-click on the

device, and the setting option will pop up. Some functions require the hardware support of the device. Please refer to the actual device for all functions. allow.

Play: Video playback, optional main stream, sub stream, face recognition camera optional AI stream. The main stream can be used for local transmission to obtain clearer storage video, and the sub-stream can be used for remote transmission to obtain smooth images and videos. The AI code stream is used to obtain the result of humanoid face recognition.

Close Video: Close video browsing.

Start recording all: Open all surveillance recordings under this device. Open

intercom: Intercom between the computer and the device, click the icon " " to cancel the intercom. Fisheye display: This

function requires the device to be a fisheye panoramic camera. Click to open the four panoramic images of the device, drag the right mouse button Or scroll the wheel to move or zoom in on the picture.

System arming: means the device is on alert. System stay-at-

home: When the host is in the fortified state, through artificial settings, some detectors work and some detectors do not work It is not only beneficial for people to move freely in the fortified prevention space, but also can play an effective prevention function.

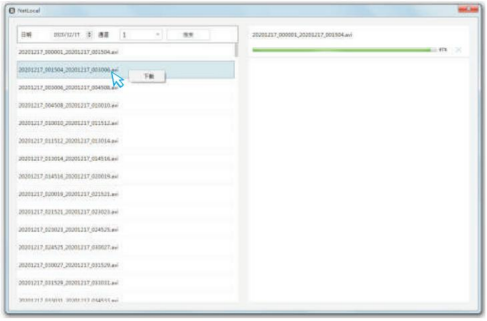
System disarm: means that the device is released from the alert state, and does not call the police when an alarm is triggered. (The dismantling alarm

is not affected by arming and disarming) System clear: Stop alarming after the device triggers the alarm. Parameter setting: see chapter three for

details. Defense area map: used to view the location of the defense area, click "Load map" to select a picture, "Add defense area" to load the added

detector in the map, drag the defense area in the map to the location, when the alarm is triggered, you can Enter the "Defense Area Map" in the main menu bar, double-click the alarm below to view the location of the red flashing defense area icon.

Download: Recording download, the default download path is C:/Program Files/ tech/NetLocal/Record in the location of the software, and the recording file name format is "recording start year, month, day_hour, minute, second_recording end year, month, day_hour, minute, second". Users can enter the "System Settings" in the main menu bar to modify. Select the recording date and channel, click "Search", select the recording you want to download in the search results and click the right mouse button - "Download".



Remote recording: view the recording in the hard disk or TF card. The green background in the date column on the right is recorded, select the recording date - select the channel -Click the icon "ÿ" to start playback, scroll the mouse wheel below the time to zoom in/out the time node.

remote recording

Device modification: The user name and password need to be modified according to the name and password of the actual device. Modify it.

Delete device: remove the device from the list. Face data setting:

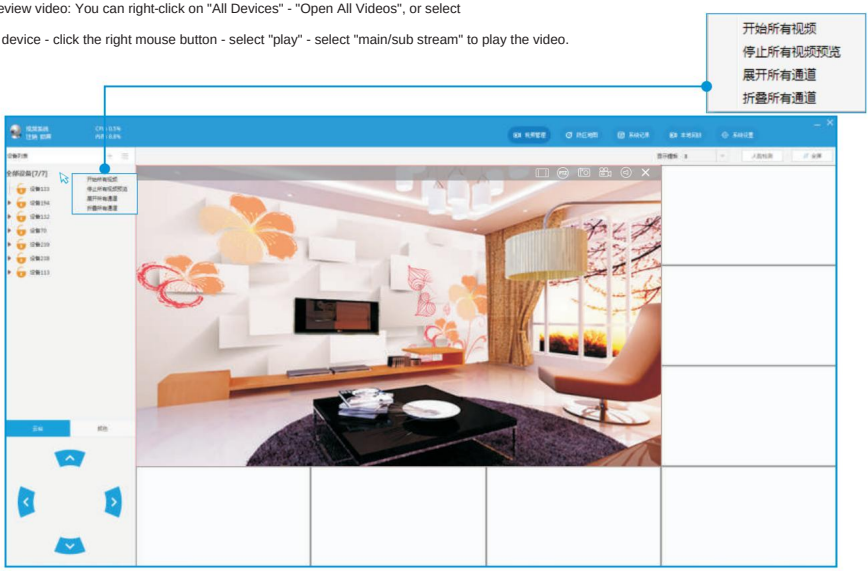
see Chapter 4 for details

Chapter 2 Function Introduction

1. Video management

Preview video: You can right-click on "All Devices" - "Open All Videos", or select

Select the device - click the right mouse button - select "play" - select "main/sub stream" to play the video.



Video settings: Click on the video, and the following icon will appear in the upper right corner.

icon meaning		explain
	Screen ratio 1:1 Click to	make the screen play according to 1:1
PTZ	screen zoom	You can use the mouse wheel to zoom, and after zooming in, press and hold the left mouse button to move the screen
	screenshot	Capture the entire video screen, the save path can be modified in "System Settings"
	video	Record the current video, the save path can be modified in "System Settings"
	Open the monitor to open	the current video sound
	Cancel preview——	

PTZ setting: This setting requires the device to support PTZ rotation. Select the video and click the direction button to rotate the PTZ.

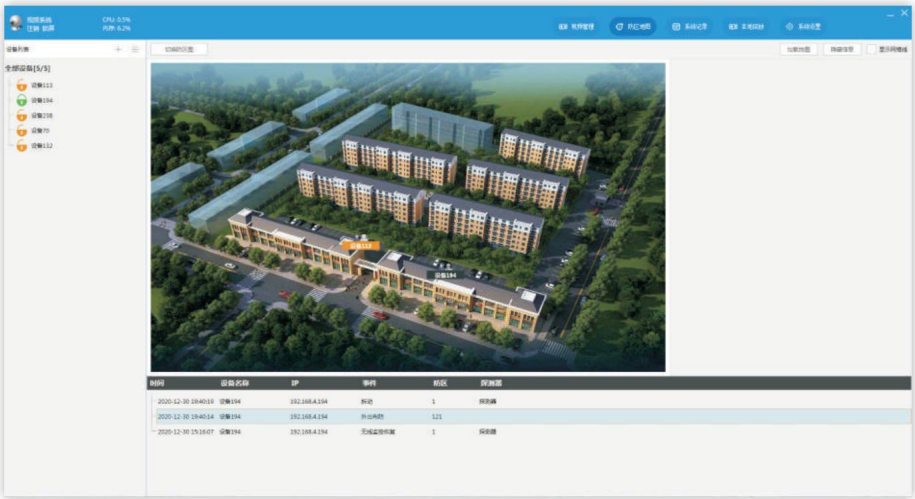
Color setting: screen color adjustment, the user can set according to the actual situation, select the video, move the setting item up and down and click

Click "Save" and "Refresh" to observe the color change of the screen. Display of

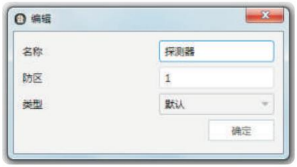
the number of videos: Click the drop-down window of "Display Template" on the upper right, and a maximum of 64 videos can be displayed.

2. Defense area map

The defense area map is used to view the location of the alarm area. Click "Load Map" to add a map, "Device Location Map" is the map location of the host/camera, and "Defense Zone Map" is the map location of the defense zone.



Add the device to the map: Click on the device - press and hold the right button and drag to the "Equipment Location Map".



Add defense area: Click "Switch defense area map", left click on the map - "Add defense area", the pop-up window displays the defense area name, defense area number and defense area type. If adding a wired defense zone, please fill in the equipment wiring defense zone number. Click on the zone icon and hold down the right button to drag.

When the device triggers an alarm, the alarm information is displayed at the bottom of the map, double-click to pop up the map where the device is located, and the alarm zone flashes red, allowing you to quickly find the alarm area.

3. System records

System records include alarm records and operation records.

Alarm record: display all equipment alarm time, alarm equipment IP, alarm events, etc. Operation record: Display the online time of all devices and the IP of the device.

4. Local playback

Play back the downloaded video, double-click the video file in the file list on the right to play it back. Select the video file and click the icon " "- " " to delete, click " " to select all, " " to cancel.

5. System settings

Alarm sound: voice prompts the device to arm or disarm or alarm, if it is turned off, there will be no prompt. Online

and offline sound: When the device is online/offline, it will prompt "device online"/"device offline", if it is closed, it will not prompt.

Alarm prompt: When the device goes offline, armes and disarms, or triggers an alarm, a window pops out at the lower right corner of the interface to prompt the device and the event.

Alarm pop-up box: When the device performs arming and disarming operations or an alarm is triggered, an alarm detail window will pop up and record in real time. Reality

The real-time recording function is enabled on the premise that the detector is bound to a camera.

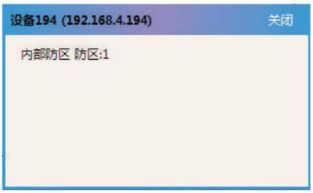
Full Screen: Maximizes the interface.

Taskbar: Display the current version number and time.

Video buffering: Play part of the downloaded video first during video playback, and you don't need to download all of it to watch it.

Modify password: modify the password of the local account, which is empty by default, and it will be effective after re-login after modification. Path:

Default screenshots and videos are saved in the C drive, click "..." to modify.



Alarm prompt window

Alarm Details Window

Chapter 3 Parameter Setting

The parameters include six items including system settings, video, alarm, network settings, smart home, and version.

1. System settings

System settings include basic settings, user settings, factory settings, timer, update, installation, hard disk.

1.1 Basic Settings

The date format and time format are video display time formats. If the modified date and time are earlier than the current time, the recording between before and after modification will be erased; there are two video formats, PAL and NTSC, and the default is PAL; The size is the length of a video. Hard disk: You can choose not to overwrite or overwrite; the condition for not overwriting recording is that the current working disk is being overwritten, or the current working disk has just

If the hard disk is full, but the next disk is not empty, the recording will stop. At this time, if the hard disk full abnormal alarm is turned on, a hard disk full alarm will be generated; the condition for overwriting is that the current working disk is just full, and the next disk is not empty. It will cycle overwrite the earliest video files

Resolution: the resolution of the VGA output interface

Rate.

Device language: Chinese and English are optional. After changing, click "Save", and the device will go offline. After the device restarts automatically, it will take effect and the device will go online again.

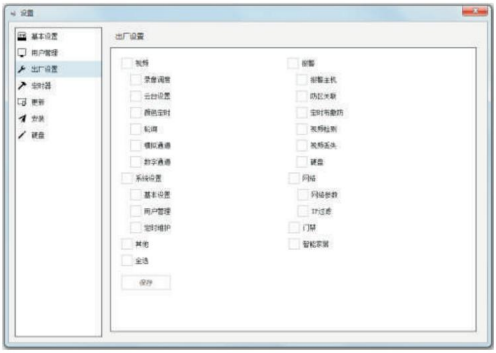
Boot screen: This function is limited to NVR Use, when the host is turned on and uses HDMI or VGA output, the interface will display the number of video images.

1.2 User Management

Display current user status.

1.3 Factory settings

Restore the settings to the factory defaults, and the user operates according to the actual situation. After restoring the factory settings, please re-set the parameters and zone added.



1.4 Timers

You can set a regular restart time, select the number with the mouse and click "ÿ"/"ý" to adjust it up or down, and check the work Click "Save" to take effect later.

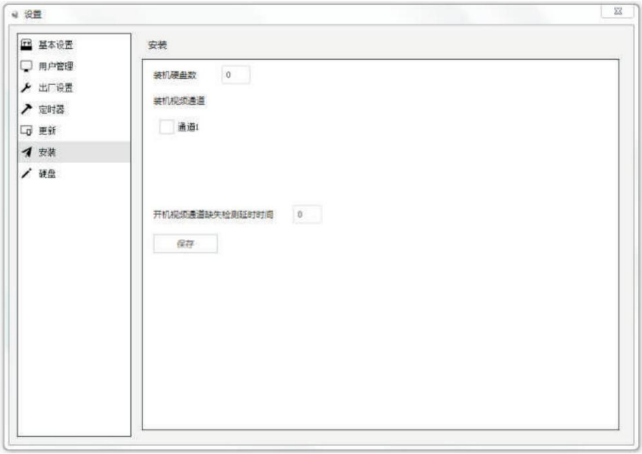
1.5 Update

Click "..." to select the upgrade file, click "Device Upgrade" to upgrade the system, and it will automatically restart after the upgrade is successful.

1.6 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 system When the number of detected hard disks is less than the number of installed hard disks and the hard disk loss alarm is enabled, the hard disk loss alarm is triggered.

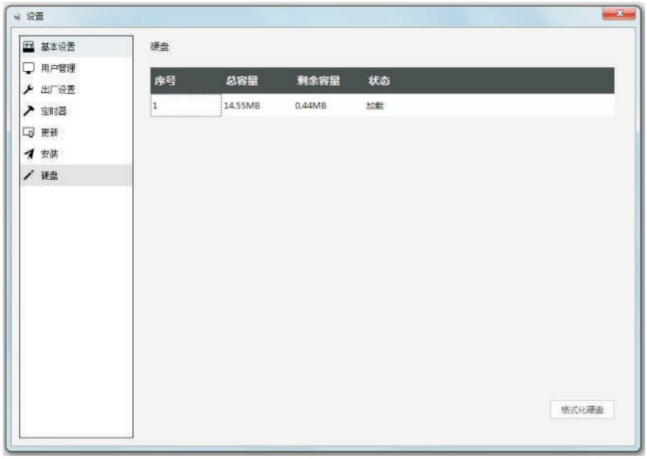
Installed video channel: The installed video channel refers to the video channel that the user actually accesses the device during installation. When the device is turned on, it detects the channel with video signal input, and triggers a video loss alarm when it detects that the channel is specified 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 from the system startup to the system starts to detect the installed analog video channel separated.

1.7 hard disk

Display the number and capacity of the hard disk, click "Format Hard Disk" to clear the hard disk, and the device will automatically restart after formatting.

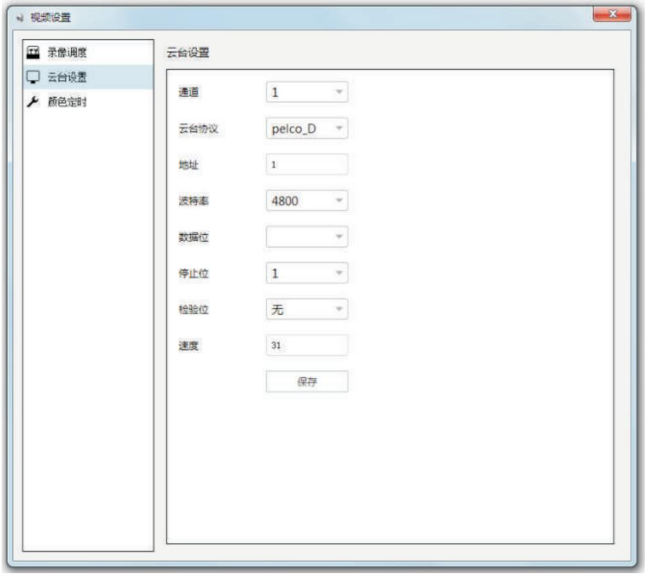


2. Video

2.1 Video scheduling

Each channel can set 4 timer records Image or alarm recording, regular recording means that the device records within the time period set by the user, and alarm recording means recording when the device triggers an alarm within the time period set by the user. Recording settings: select the channel and recording type, the user can set any working day or four time periods per day to record according to the actual situation, select the number of the hour/ minute/second in the time period with the mouse, and click "ÿ" /"ÿ" to adjust up/down, press and hold "ÿ"/"ÿ" to continue to increase or decrease, 00:00:00~23:59:59 is the whole day video, after the time is set, check "Use ", click "Save" to take effect. (If you don't check "Enable", the time period will not be enabled, and if you don't click "Save", the recording settings will be invalid)

Note: In the scheduled time period, the recording type is only effective for one type. If there is a scheduled recording, the time In-segment manual recording does not work. The priority of alarm recording is the highest, and the priority of scheduled recording is higher than that of manual recording.



2.2 Please use the default value for the PTZ setting, and non-professionals should not change it at will.

2.3 Color Timing

Color timing is to adjust the color of the channel in time intervals.

3. Alarm

3.1 Alarm host setting

3.1.1 Setting up the system

Entry delay: After the delay zone is triggered, the time for the host to delay the alarm can be set from 0 to 255 seconds; Exit delay: the user configures the host

The time from defense until the main unit enters the defense state can be set from 0 to 255 seconds;

Siren time: the siren ringing time after the host alarm, the alarm host can be set from 0 to 999 seconds, the NVR can be set from 0 to 30 minutes, the default is 5 minutes, it is recommended that users do not set more than 15 minutes;

Telephone line drop detection: detect whether the phone line is dropped, optional alarm, no prompt, no detection.

Detector loss detection: detect the time interval of wireless detector loss or power failure, if the host does not receive any signal from the detector, it will upload the detector loss information to the alarm center. The default is 0 for no detection. (in hours)

Ringing and off-hook times: the number of ringing times when the user remotely operates the main unit and the main unit is off-hook, which can be set from 0 to 15 times. The number of local communication automatic hangups is the maximum number. When it is set to 00, the remote control operation function of the phone is turned off. (default is 7 times)

AC power-off time: AC power-off detection, the default is 0 and no detection; Arm and

disarm report: Whether arm and disarm is uploaded to the alarm center, the default is off;

Arming and disarming reminder: Whether the device emits a prompt sound when arming and disarming;

Forced arming: When a fault occurs in the defense area, the device is forced to arm, and it is enabled by default; Alarm limit:

If alarm limit is selected, when three or more alarms occur 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, which is 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, the default is off;

3.1.2 Alarm center setting

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 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; Center call

times: the number of calls made by the device to the alarm center when the alarm center has not been connected for many times.

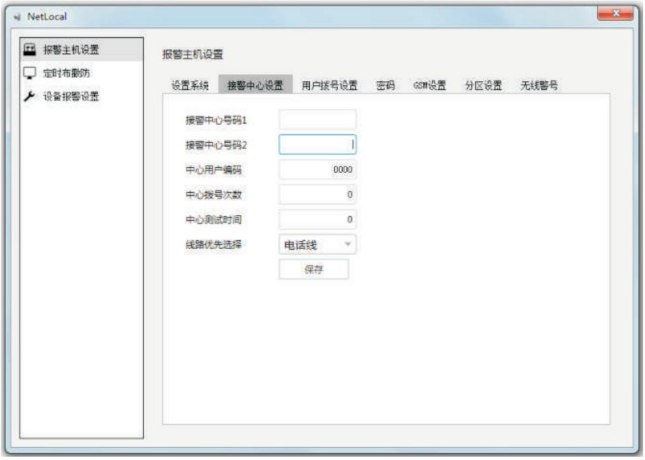
Calls will stop after the number of calls is exceeded. (5 times by default)

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 the alarm information be uploaded to the telephone alarm center first, and there is a GSM line

Road and telephone lines are optional. (Default GSM line) After setting, click

"Save" to take effect.



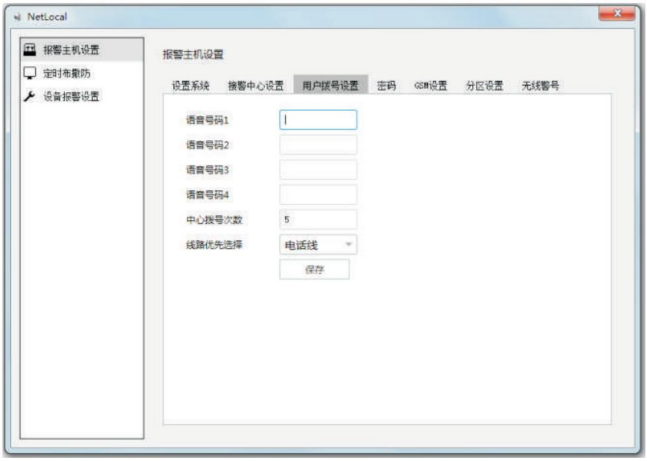
3.1.3 Voice number set by user

dialing: refers to the phone number that the device dials to the user when the device alarms, including landline and mobile phone numbers. up to

Set up 4 user phone numbers, the phone number can be input up to 17 digits. Number of calls: refers to the number

of times the device makes calls 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. (Default 5 times) Line priority selection: When an alarm is triggered, which line will be

used to make a call to the user first, there are two optional lines: GSM line and telephone line. (default GSM line)



After setting, click "Save" to generate

effect.

3.1.4 Password

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

Admin password: means through the keyboard Set the access password of the alarm panel parameters, 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.

3.1.5 GSM settings

GSM communication settings

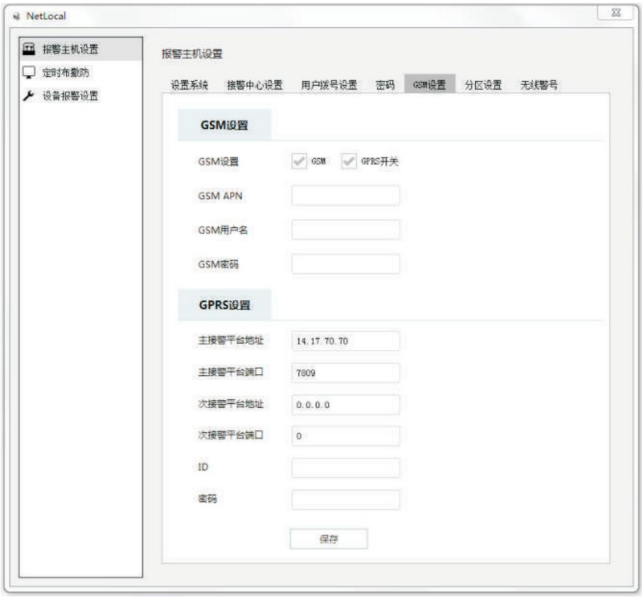
Before enabling this function, please confirm whether your SIM card meets the requirements of the GSM module. The network supports China Mobile and China Unicom, but does not support China Telecom. (CDMA)

GSM settings: After turning on GSM, you can make calls and send and receive text messages; after checking GPRS enable, you can use GPRS traffic Network alarm.

GSM APN: SIM card operator's access point;

GSM user name: SIM card GSM username;

GSM password: SIM card's GSM password;



GPRS settings

After setting the platform information, use GPRS traffic to carry out network alarm. Please refer to "4.3.1 Server Settings" for details on alarm platform settings.

After setting, click "Save" to generate effect.

3.1.6 Partition setting

Partition: In a certain area, it can independently enjoy arming when going out, arming by staying, disarming, and alarming without affecting other areas. The model supports a total of 4 partitions. When the defense zone is triggered, it will trigger the corresponding alarm or defense zone failure according to the arming and disarming status of the partition to which the defense zone belongs and the alarm type of the defense zone. If the defense zone belongs to multiple partitions, an alarm will be triggered in the partition to which it belongs according to the arming and disarming status of the partition. When using the remote control to arm and disarm the main unit, the effective partitions are all partitions to which the remote control belongs. When a partition triggers an alarm, the phone belonging to that partition will be dialed. The host keyboard also has partition attributes, and the specific settings should be set through the host keyboard. The keypad in a partition can only operate the arming and disarming status of the partition with the common user password or master user password belonging to the partition.

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

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

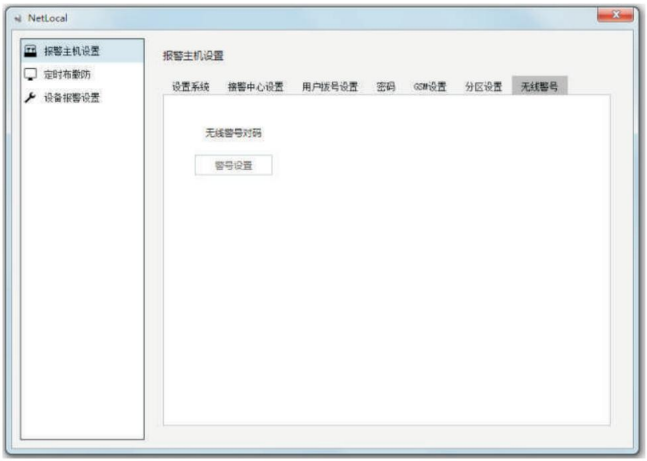
Partition to which the voice call belongs: Each defense zone can be set to belong to a partition, which can belong to a single partition or to multiple partitions, but it must belong to at least one partition. (By default it belongs to partition 1)

3.1.7 Wireless siren

Trigger the siren and click "Siren Settings" to perform code matching. Wireless siren code pairing:

When the local siren cannot achieve the corresponding effect and needs to be connected to an external wireless siren, use this button to pair the code so that the wireless siren is associated with the host.

Use: Trigger the wireless siren to be paired, left-click on the "Siren Settings" on the interface, and it will prompt whether the siren is associated with the host after the code is successfully paired.



3.2 Timed arming and

disarming The user can set the timing period according to the needs, and check "Enable" to enable it, otherwise the time period will not be considered to be enabled. Under each time period, there are partitions 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 partitions. Does 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.

If the first parameter of the set time period is greater than the second parameter, the corresponding time period is from the time of the second parameter to the time of the first parameter of the next day. For example, if the set time period is "17:30-8:00", the corresponding time period is from 17:30 to 8:00 of the next day.

The setting of these timing arming and disarming time periods is only effective for burglary alarms and surrounding alarms, and other alarms are valid for 24 hours.

3.3 Device alarm settings 3.3.1

Motion detection When the screen

changes, the system will do corresponding processing. According to the actual needs, you can set the certain detection alarm of the channel to be associated with the arming and disarming status of the partition, or directly set the working time of the motion detection alarm.

Channel: The channel where the motion detection alarm parameters will be set.

Enable: Whether to enable the "Motion Detection" function for this channel. Arming and disarming

association: When this function is selected, the "movement detection" of this channel will only work when partition 1 is armed. If this function is not selected, it has nothing to do with the arming and disarming status of partition 1.

Timing switch: When this function is selected, only when the current time is within the set time range, the 'dynamic detection' of this channel will be kick in. If this function is not selected, it has nothing to do with the set time period. Sensitivity:

Define the sensitivity of "Motion Detection". There are 7 types of high and low, and users can choose according to their needs.

Siren Sound: Whether to enable the sound alarm when the channel triggers the motion detection alarm.

Capture picture: When the channel triggers a motion detection alarm, whether to capture a picture of the channel. Alarm center setting: When the channel triggers a motion detection alarm, whether to upload the alarm information to the alarm center. Send email: When this channel triggers a motion detection alarm, it will send an email to the user.

3.3.2 Video loss Video loss:

When the device switches from signal to no signal input, the device will trigger a video loss alarm.

(When a channel is set as the channel with video by default in the "System Settings-Installation" setting page, and the device detects that there is no video signal input to the channel after startup, it will trigger the video loss alarm of the channel) The device will follow the following settings A good way to call the police. Channel: The channel where the video loss alarm parameters will be set.

Timing switch: When this function is selected, the "video loss detection" of this channel will only work if the current time is within the set time range. If this function is not selected, it has nothing to do with the set time period.

Arming and disarming association: When this function is selected, only when partition 1 is armed, the "video loss detection" of this channel will work. If this function is not selected, it has nothing to do with the arming and disarming status of partition 1. Central test time: the interval between the last triggering of video loss and the next triggering of video loss for this channel. Siren sound: When the channel triggers the "video loss" alarm, whether to enable the siren alarm. Send email: When the channel triggers the "video loss" alarm, whether to send a message to the user's mailbox. Buzzer: When the channel triggers the "video loss" alarm, whether to enable the buzzer alarm prompt. Upload to CMS platform: When this channel triggers a "video loss" alarm, whether to send information to the CMS platform.

3.3.3 Hard Disk Abnormal

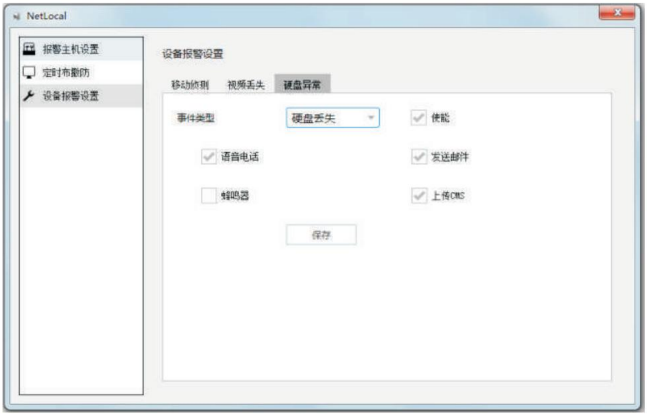
Hard disk abnormality is divided into three types: hard disk loss, hard disk error, and hard disk full;

Hard disk loss: When it is detected that the number of hard disk connections of the device is less than the number of installed hard disks set in "System Settings-Installation", the

A hard disk loss event will be triggered. If the hard disk loss alarm is enabled, a hard disk loss alarm will be triggered. (Before using this function, you must set the number of installed hard disks on the "System Settings-Installation" page. When the number of installed hard disks is 0, this function is invalid)

Hard disk error: When the hard disk is in use, a hard disk error event will occur when the communication between the hard disk and the device fails due to various reasons. If the hard disk error alarm is enabled, the hard disk error alarm will be triggered.

The hard disk is full: when the hard disk recording is full and the "HDD overwrite type" is not overwritten, a hard disk full event will be generated, if If the hard disk full alarm is enabled, the hard disk full alarm will be triggered.



Enable: Whether to enable the abnormal alarm function. Voice

call: Whether to make a set voice call when an abnormal alarm is triggered. Send email: When the abnormal alarm is

triggered, whether to send the alarm information to the user mailbox.

Upload to CMS center: Whether to upload the alarm information to the CMS platform when the abnormal alarm is triggered.

Buzzer: When the abnormal alarm is triggered, whether to enable the buzzer alarm prompt. After setting,

click "Save" to take effect.

4. Network settings

4.1 Basic Settings

4.1.1 Network Settings

Users can choose two ways: "automatic acquisition" or "manual modification". Automatically obtained as a dynamic IP obtained from the router, such as Manually modify the IP address, please ensure that the IP addresses in the LAN do not conflict.

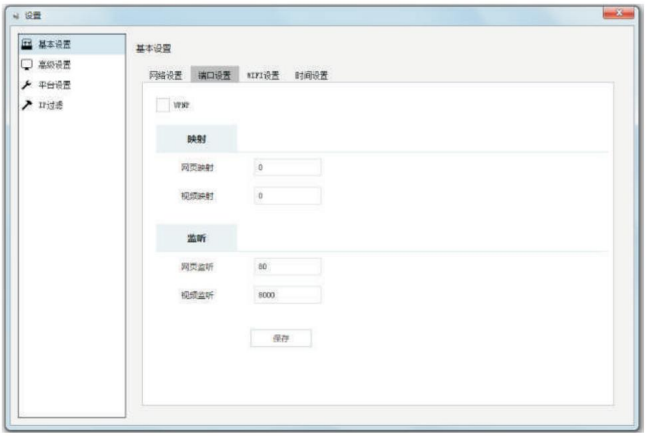
Primary DNS: It is the IP of the local primary domain name server of the network used by the host.

Secondary DNS: It is the IP of the local secondary domain name server of the network used by the host.

The MAC address is assigned by the manufacturer.

After setting, click "Save", and the device is offline at this time, please add it again in the device list column.

4.1.2 Port Settings



UPNP setting: UPNP (Universal Plug and Play), Universal Plug and Play, is a collective name for a set of protocols, and the simple understanding is that UPNP = "automatic port mapping".

If you need to map the ports in the LAN, WEB mapping port, video mapping port, platform alarm mapping port and mobile phone browsing mapping port, the port number should be set according to the requirements, and the recommended port number is between 1024--65500.

Port mapping is actually often said A kind of NAT address translation, its function is to translate the address in the public network into a private address. The ADSL broadband router with routing mode has a dynamic or fixed public network IP, and the ADSL is directly connected to the HUB or switch. All Computer sharing online.

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. settings, the device needs to be restarted. 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?

Answer: Extranet browsing: WEB browsing: http://test.3322.org: 2001 (IE-side browsing) Video browsing: http:// test.3322.org: 2002 (client browsing) Mobile browsing: http:/ /test.3322.org: 2003 (mobile phone must be within the supported model) Intranet browsing: WEB browsing: 192.168.1.69:3000 (IE end browsing)

Video browsing: 192.168.1.69:3001 (client browsing) Mobile phone browsing: 192.168.1.69:3002 (first, the mobile phone must be within the supported model,

Secondly, make the mobile phone within the internal network, such as the mobile phone supports WIFI, and the router has wireless function)

4.1.3 WIFI settings

Mode: optional off, client, server. Off to not use WiFi; select client for existing host connections WiFi; if the server is selected, the device can be used as a hotspot to connect to the camera (the device needs to support the hotspot function).

Encryption: Automatic acquisition, NONE, WEP, WPA/WPA2-PSK are optional. The security capabilities of the encryption types vary, and the transfer rates vary depending on the technology supported by the wireless device. NONE means no encryption; WEP is an old-fashioned encryption method, which uses IEEE 802.11 technology, and now wireless routing devices basically use IEEE 802.11n technology, so when using WEP encryption, it will affect the transmission of wireless network devices If the old-fashioned equipment only supports IEEE 802.11, then no matter which encryption is used, it is compatible and has no effect on the wireless transmission rate. WPA-PSK/WPA2-PSK is the encryption type we often set up now. This encryption type has high security performance and is quite simple to set up. All branches of Meian Technology

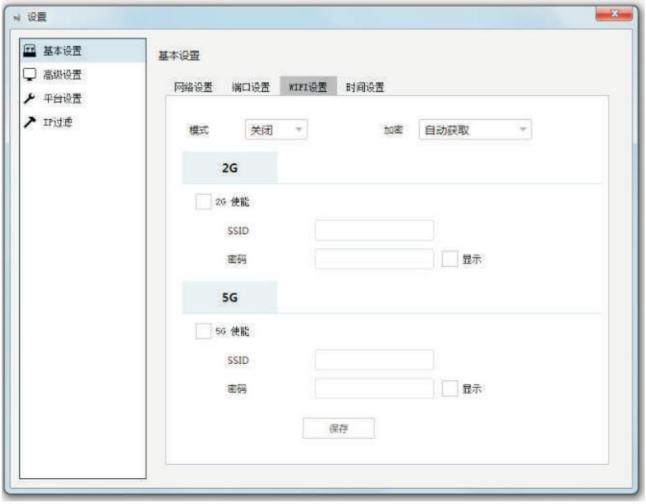
Devices that support hotspots all adopt IEEE 802.11n/b/g technology. The default is to get it automatically.

2G enable: check to enable;

SSID: WiFi name, choose guest

In client mode, please refer to the hotspot name in the device manual to fill in;

Password: WiFi password, when selecting the client mode, please refer to the device manual hotspot password to fill in; 5G function is not supported for now.

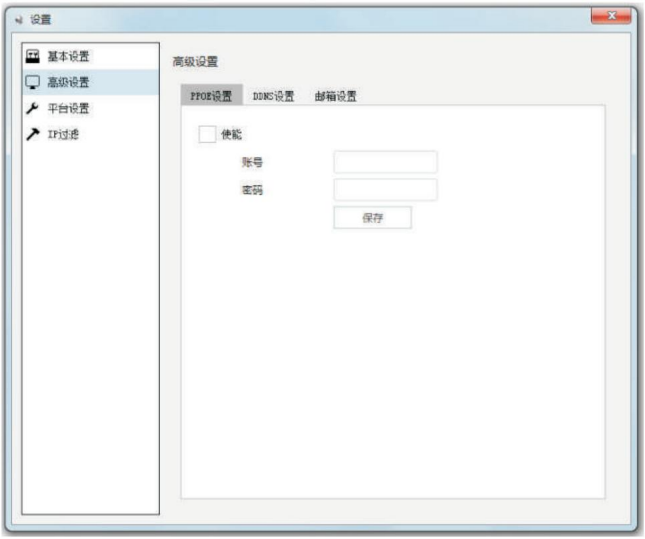


4.1.4 Time setting Under

this setting item, you can set automatic network time synchronization, time zone selection, time server, port number and time interval.

4.2 Advanced Settings

4.2.1 PPOE setting



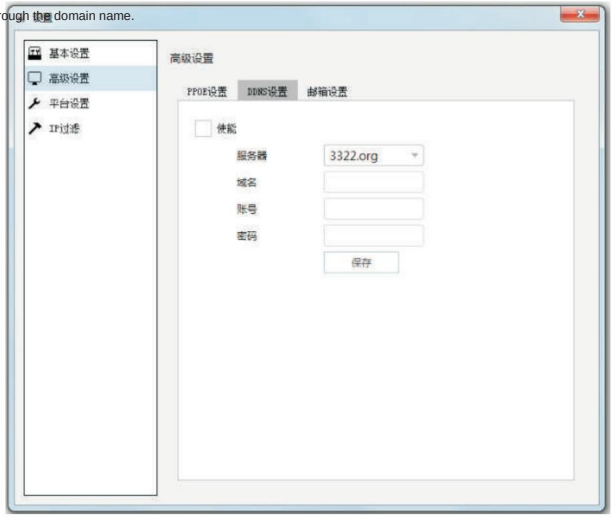
Enable: define whether PPOE is enabled Generally, the system defaults to "off";

Account: for the username provided by the ISP; Password: for the password corresponding to the username provided by the ISP;

When PPOE dial-up is enabled, enter the user name and password, click Save to exit, wait for 1 minute and then enter the network setting interface, you can see the obtained IP in the PPOE IP column; in addition, when the device is restarted, the device will automatically Re-dial to obtain a new IP address.

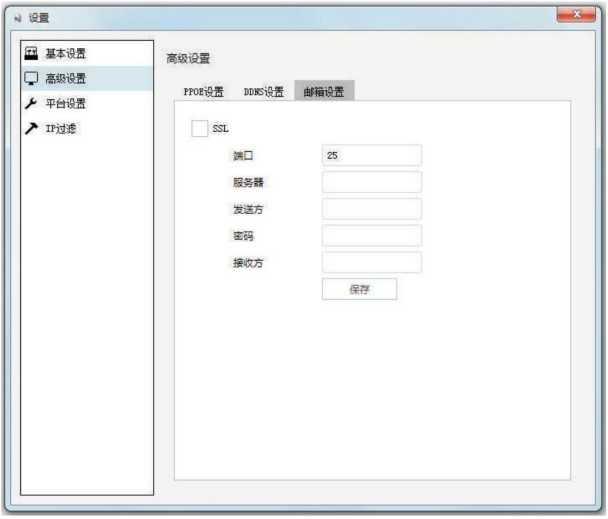
4.2.2 DDNS settings

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 you can pass WAN browsing.

4.2.3 Email Settings



SSL: A mature and reliable email security technology, which can most effectively protect the confidential information of users and completely eliminate the phenomenon of illegal theft and tampering of passwords from the browser to the server. Check it to enable it.

Port: Different servers correspond to different port numbers, please fill in according to the mailbox server type.

Server: Mailbox server name. Sender: The email address of the sending email.

Password: The password of the email sender.

Recipient: Email recipient's mailbox Number.

After setting, click "Save".

4.3 Platform Settings

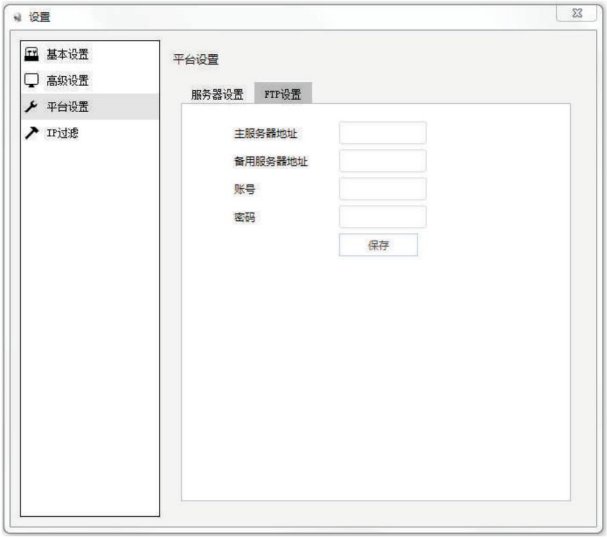
4.3.1 Server settings Under this setting item, you can set the IP of the alarm platform/ registration platform. After opening, the alarm information can be uploaded to the platform. If you choose manual setting, you need to apply for a registration ID before you can upload information; the opening and closing of the platform will restart the device.

Use authentication server: Check it to automatically obtain server address, port number, ID and other information and connect to the platform. Check it and click "Save" to restart the device to go online on the CMS platform.

Platform connection: manually fill in the server address, port, ID, and password. 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 3 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.

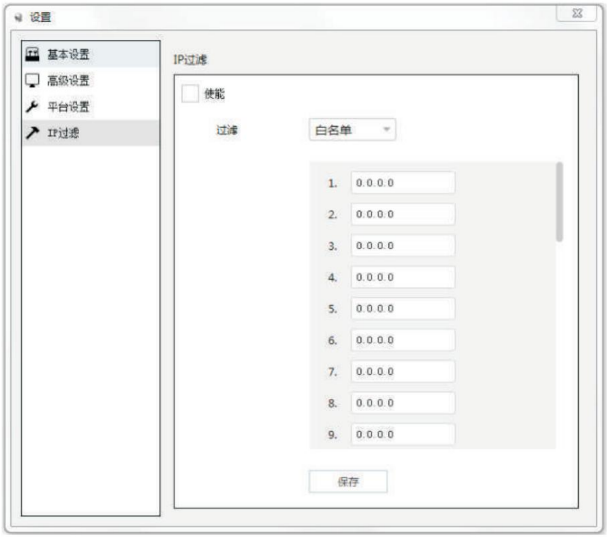
4.3.4 FTP settings

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 (these computers are running FTP server program) to check what files the remote computer has, and then copy the files from the remote server to the local device, or send the files of the local device to the remote server. If you set up FTP, you must first have a server with FTP service, and apply for an account number and password. Fill in these contents under this setting item, and then you can upload via FTP, and upload the alarm video to the server. If you are using the free platform provided by our company, you don't need to set it, the account number and password uploaded by FTP are already embedded in the software; if you use another platform, please set the server IP, account number, password here, only the setting Only after these and the platform are completed can the alarm video and pictures be uploaded to the platform, and the alarm pictures and alarm videos can be browsed on the platform. The FTP of this machine cooperates with the platform to upload alarm video and alarm pictures. In addition, if you use the platform, please pay attention to the settings FTP account and password.



4.4 IP filtering

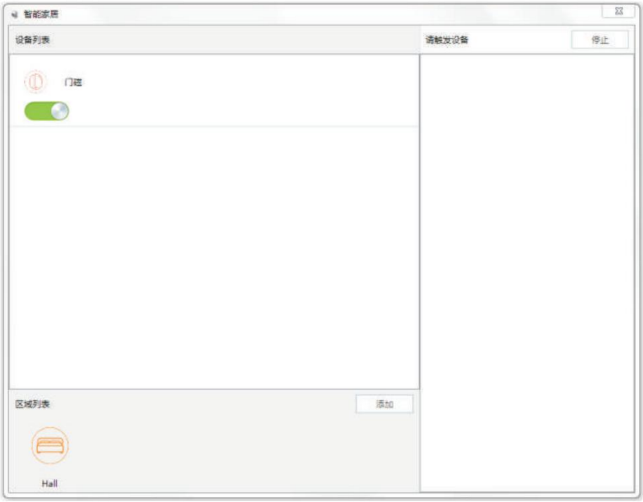
Under this setting item, you can set which IP addresses are allowed to access the machine or which IP addresses are not allowed to access the machine. IP filtering has two modes: whitelist filtering and blacklist filtering. In the white list filtering mode, only the IP addresses in the IP list are allowed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



5. Smart home

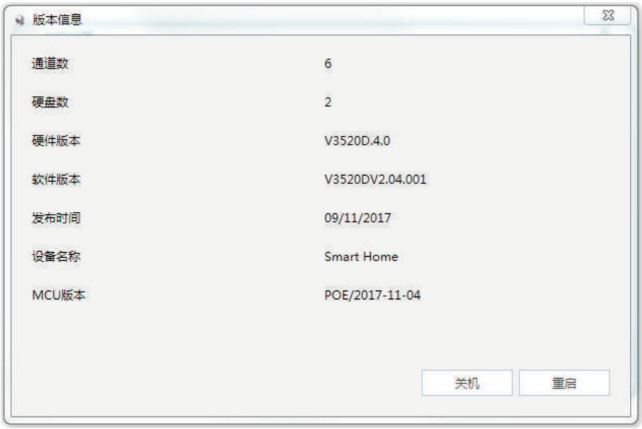
Under this function setting, the wired defense area is automatically obtained, and wireless devices can be added: click "Add" on the right side of the "Device List", and the right column will prompt "Please trigger the device" to trigger the wireless device to be paired. Find the device in the list bar. Select the device and right-click to modify the area where the device is located.

Area list: Divide the equipment into different areas, right click on the area to arm and disarm all the devices in the area.



6. Version

Under this item, you can view the channel information of the machine, the maximum number of hard disks, the number of defense zones, the number of alarm outputs, the number of smart devices, the number of alarm outputs, hardware version, software version, release date, device name and MCU version, etc. You need to be familiar with this information when upgrading and consulting customer service.

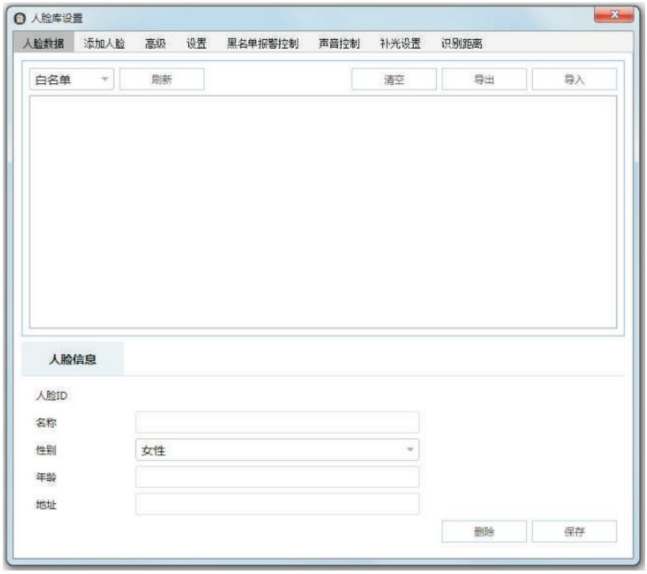


Chapter 4 Face Data Settings

The face recognition function requires the hardware support of the device, and the video should be played with "AI stream" when it is turned on. when the video appears When there is a face or a human figure, a blue frame will appear on the screen to capture it.

4.1 Face data Click

the drop-down window to select the whitelist/blacklist, and the corresponding face information in the whitelist/blacklist appears below the drop-down window, click Click the image in the list to view the face information below, click "Delete" to clear the face data, if you modify it, click "Save" to take effect.



White list: In the armed state, if the face information in the white list is detected, the voice will prompt "Welcome", and the voice broadcast can be set in "Voice Control";

Blacklist: In the armed state, if the face information in the blacklist is detected, it will prompt "Blacklist personnel, please pay attention"; Clear:

Delete all face data; Export: The default export path is C:\Program Files\tech\ NetLocal\Database, if the installation location of the LAN tool is not

in C:\Program Files, please refer to the actual installation location.

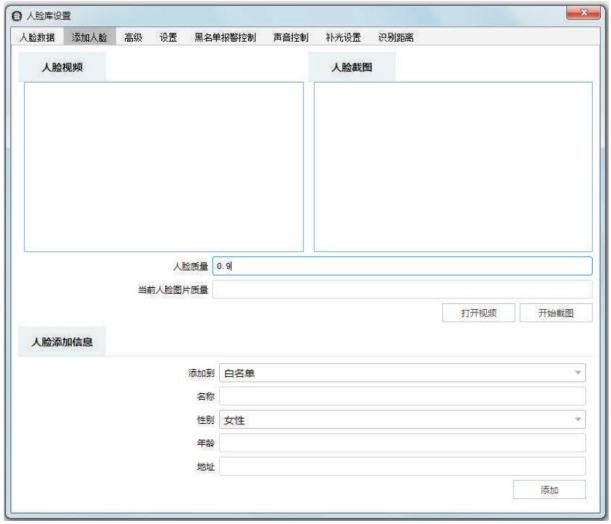
Import: import face data files.

4.2 Add face Add face

data through video screenshots.

Open video: open real-time video;

Start screenshot: Automatically screenshot the face that appears in the real-time video, click again to turn off automatic screenshot; Face quality: Face recognition degree of video detection, the range can be set from 0 to 1;



Current face image quality: automatic screenshot The quality of the face image in , the clearer the face, the higher the quality of the current face image;

Operation method: Click "Open Video" - "Start Screenshot", point the camera at the face for recognition, when the face is captured, it will automatically take a screenshot, set the quality of the face, and fill in the added information of the face, click "Add", Return to the face data interface to refresh to view the added face information.

4.3 Advanced

Under this setting item, images can be uploaded to add face information, and the user can operate according to the prompts.

4.4 Settings

Set the alarm interval time and alarm limit times for human figure recognition. In the armed state, when the camera with human shape recognition function

When a human figure is detected, the camera will push an alarm message to the platform.

Alarm time interval (seconds): The time interval between the triggering of human figure recognition alarm and the last time, can be set within 30~300 seconds; Alarm

limit times: The number of consecutive alarm triggers within the same time period, can be set 0~15 times.

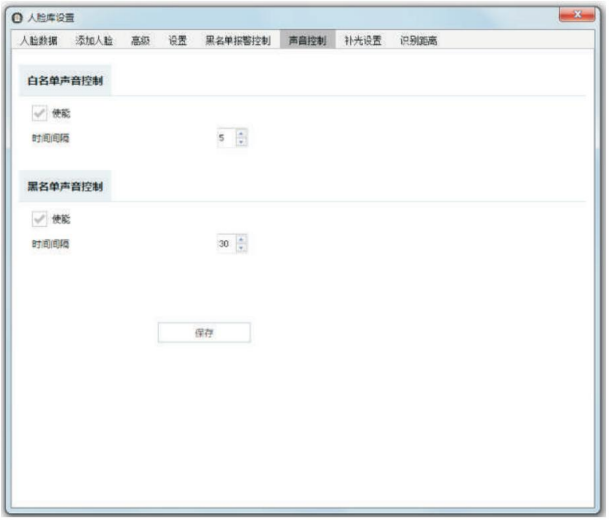
4.5 Blacklist alarm control Set the

alarm interval time and alarm limit times of face recognition. In the armed state, when the camera with face recognition function

When the face information in the blacklist is detected, the camera will push an alarm message to the platform.

4.6 Sound Control

When the AI face recognition camera detects the whitelist or blacklist, there will be a voice prompt "Welcome" or "Blacklist personnel, please pay attention", check "Enable" to open the voice broadcast, and the time interval is two voice broadcasts interval time, blacklist time interval does not work.

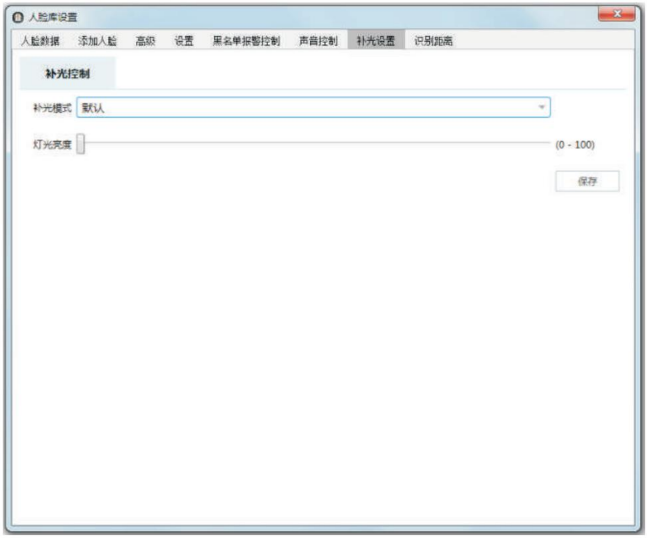


Click "Save" after setting to take effect.

4.7 Fill light settings

Fill light mode: optional default, automatic, normally open, normally closed, in automatic mode the camera will automatically fill light according to the light intensity, normally Closed is not enabled. The user selects the mode according to the actual scene. Light

brightness: used in normal open mode, adjustable from 0 to 100.



4.8 Recognition distance

The camera can recognize the distance between human faces and human figures. Users should choose according to the actual application; the minimum/large face ratio is the ratio of recognizable faces in the video, and the setting range is 0~1. The larger the ratio, the higher the recognition accuracy .