User Manual

Network Video Recorder

Please read this manual carefully before operating the unit and keep it for further reference

Notes

- Please read this user manual carefully to ensure that you can use the device correctly and safely.
- There may be several technically incorrect places or printing errors in this manual. The updates will be added into the new version of this manual. The contents of this manual are subject to change without notice.
- This device should be operated only from the type of power source indicated on the marking label. The voltage of the power must be verified before using the same. Kindly remove the cables from the power source if the device is not to be used for a long period of time.
- Do not install this device near any heat sources such as radiators, heat registers, stoves or other devices that produce heat.
- Do not install this device near water. Clean only with a dry cloth.
- Do not block any ventilation openings and ensure proper ventilation around the machine.
- Do not power off the device at normal recording condition.
- This machine is for indoor use only. Do not expose the machine in rain or moist environment. In case any solid or liquid get inside the machine's case, please turn off the device immediately and get it checked by a qualified technician.
- Do not try to repair the device by yourself without technical aid or approval.
- In this manual, the trademarks, product names, service names, company names, products that are not owned by our company are the properties of their respective owners.
- It is recommended to back up and clear the personal data stored in the device before the device is returned to us for repair or replacement except those data that are essential for purposes of repair or replacement. The device will be restored to the default factory settings and all personal data will be cleared after repair or replacement. Our company ensures that the customer's data is not made available to third parties if the device is exchanged.
- This manual is suitable for many models. All examples and pictures used in the manual are from one of the models for reference purpose.
- The local language versions of this manual will be provided to users in the corresponding regions and countries.

Disclaimer

- With regard to the product with internet access, the use of product shall be wholly at your own risks. Our company shall be irresponsible for abnormal operation, privacy leakage or other damages resulting from cyber attack, hacker attack, virus inspection, or other internet security risks; however, our company will provide timely technical support if necessary.
- Surveillance laws vary from country to country. Check all laws in your local region before using this product for surveillance purposes. We shall not take the responsibility for any consequences resulting from illegal operations. In the event of any conflicts between this manual and the applicable law, the later prevails.

- The storage of the personal data depends on the capacity of the storage devices the users use and all data stored in the device shall be handled by themselves. Our company shall not be responsible for the data loss.

Cybersecurity Recommendations

- Use a strong password. At least 8 characters or a combination of characters, numbers, and upper and lower case letters should be used in your password.
- Set the password expiration time and regularly change the passwords of your devices to ensure that only authorized users can access the system. (recommended time is 90 days).
- The system will automatically check the latest firmware version once a day. Once the latest version is checked, you’d better update it to ensure the system is current with the latest security patches and fixes.
- It is recommended to change the service default ports (like HTTP-80, HTTPS-443, etc.) to reduce the risk of outsiders being able to access.
- It is recommended to set the firewall of your router. But note that some important ports cannot be closed (like HTTP port, HTTPS port, Data Port).
- It is not recommended to expose the device to the public network. When it is necessary to be exposed to the public network, please set the external hardware firewall and the corresponding firewall policy.
- It is not recommended to use the v1 and v2 functions of SNMP.
- In order to enhance the security of WEB client access, please create a TLS certificate to enable HTTPS.
- Use black and white list to filter the IP address. This will prevent everyone, except those specified IP addresses from accessing the system.
- If you add multiple users, please limit functions of guest accounts.
- If you enable UPnP, it will automatically try to forward ports in your router or modem. It is really very convenient for users, but this will increase the risk of data leakage when the system automatically forwards ports. Disabling UPnP is recommended when the function is not used in real applications.
- Check the log. If you want to know whether your device has been accessed by unauthorized users or not, you can check the log. The system log will show you which IP addresses were used to log in your system and what was accessed.

Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

1. FCC compliance

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

2. FCC conditions:

- This device complies with part 15 of the FCC Rules. Operation of this product is subject the following two conditions:
- This device may not cause harmful interface.
- This device must accept any interference received, including interference that may cause undesired operation.

CE Information

CE The products have been manufactured to comply with the following directives.
EMC Directive 2014/30/EU

RoHS

The products have been designed and manufactured in accordance with Directive EU RoHS Directive 2011/65/EU and its amendment Directive EU 2015/863 on the restriction of the use of certain hazardous substances in electrical and electronic equipment.

2012/19/EU (WEEE directive): The Directive on waste electrical and electronic equipment (WEEE Directive). To improve the environmental management of WEEE, the improvement of collection, treatment and recycling of electronics at the end of their life is essential. Therefore, the product marked with this symbol must be disposed of in a responsible manner.

Directive 94/62/EC: The Directive aims at the management of packaging and packaging waste and environmental protection. The packaging and packaging waste of the product in this manual refers to must be disposed of at designated collection points for proper recycling and environmental protection.

REACH(EC1907/2006): REACH concerns the Registration, Evaluation, Authorization and Restriction of Chemicals, which aims to ensure a high level of protection of human health and the environment through better and earlier identification of the intrinsic properties of chemical substances. The product in this manual refers to conforms to the rules and regulations of REACH. For more information of REACH, please refer to DG GROWTH or ECHA websites.

Table of Contents

1 Introduction

1.1 Summary

Based on the most advanced SOC technology and embedded system in the field, this series of the NVR adopt the new designed human interface and support the smart management of the IP camera and the record search of slice. This series of the NVR which are powerful and easy to use are provided with excellent image quality and stable system. They are centralized monitoring management products with high performance and high quality specially designed for network video monitoring field.

This series of the NVR can be widely used to security system of banks at home and abroad, schools, intelligent mansions, traffic, environmental protection, supermarkets, petrol service stations, residential quarters and factories and so on.

1.2 Features

✚ Basic Functions

- Supports network device access including our company's and third-party IP cameras
- Some NVRs support the H.265S/H.265+/ H.265 and H.264S/H.264+/ H.264 IP cameras
- Supports standard ONVIF protocol
- Supports dual stream recording for each camera
- Supports the addition of IP cameras both automatically and manually
- Support collective or individual configuration of the cameras' OSD, video parameters, mask, motion and so on
- Supports multiple smart detection access and linkage for IPC's, such as scene change, video color cast detection, video blur detection, intrusion detection (region entrance/exiting detection), target counting, abandoned object detection, missing object detection, crowd density detection, face detection, license plate detection, smart tracking, fire detection, temperature detection, video metadata, etc.
- Supports playback and backup
- Supports multiple user permission groups, including Administrator, Advanced and common, which are the default permission groups of the system
- Supports multiple web client logins by using one username at the same time and the ability to enable or disable user permissions
- Supports multiple web client logins at the same time
- Supports binding NVR to the account of the mobile APP
- Supports parking lot management

✚ Live View

- Supports 4K×2K/1920×1080/1280×1024 HDMI and 1920×1080/1280×1024 VGA high definition synchronous display
- Supports multi-screen modes such as 1/4/6/8/9/13/16/25/36 (varies by model)
- Some models support face capture view, face match view, license plate recognition view, human/motor vehicle /non-motor vehicle view

- Support auto adjustment of the camera's image display proportion
- Supports enabling or disabling audio monitoring of a camera
- Supports manual snapshot of a camera live view
- Supports camera sequence adjustment
- Supports adding and saving display modes, and saved modes can be recalled directly
- Supports quick tool bar operation from the preview window
- Supports camera group view and scheme view in sequence, quick sequence view and dwell time setting
- Supports motion detection and video masking
- Supports multiple popular PTZ control protocols and setup of preset and cruise
- Supports direct mouse control of the IP dome including rotating, zoom, focusing and so on
- Supports the zoom of a single camera image by sliding the scroll wheel of the mouse
- Supports the zoom of any area of a camera image up to a maximum of 16 times of the current size
- Supports image and lens adjustment (only available with some cameras)
- Supports quick camera addition in the camera window of the live view interface
- The live camera sequence of the web client will stay consistent with the NVR after adjusting the live camera sequence of the NVR, but the live camera sequence of the NVR will not be changed if the web client is changed

Disk Management

- The NVRs with the 3U case can add a maximum of 16 SATA HDDs; a maximum of 8 SATA HDDs with the 2U case, a maximum of 4 SATA HDDs with the 1.5U case, a maximum of 2 SATA HDDs with the 1U case and a maximum of 1 SATA HDD with the small 1U case
- Each SATA interface (varies by unit) on the NVR supports HDDs with a max storage capacity of 10TB. Some models may support a max storage capacity of 12TB per HDD
- Supports hot swap
- Supports disk group configuration and management and each camera can be added into different disk groups with different storage capacity
- Supports disk information and viewing of disk operating status
- Support formatting disks in batches

Record Configuration

- Supports main stream and sub stream recording, as well as collective or individual configuration of the recording stream
- Supports custom and auto recording modes
- Supports schedule recording, sensor alarm recording and motion detection recording, etc
- Supports schedule recording and event recording setting with different recording streams
- Supports recording schedule setting and recycle recording
- Supports pre-recording and delay recording configuration of an event

Record Playback

- Supports time scale operation in quick playback and the playback date and time can be set randomly by scrolling the mouse; the time interval of the time scale can be zoomed
- Support record searching by time slice/time/event/tag

- Support smart playback by drawing grid, line or quadrilateral and vehicle smart playback (some models also support smart playback by face)
- Supports time view and camera view in searching by time slice mode
- Supports time slice searching by month, by day, by hour and by minute and time slice to be displayed with camera thumbnail
- Supports a maximum of 4/8/16 cameras to be searched at a time (varies by unit channel size)
- Supports event search by manual/motion/sensor/intelligent events
- Supports tag searching by the manual added tags
- Supports instant playback of the selected camera in the live view interface
- Support a maximum of 16 synchronous playback cameras
- Support acceleration(to a maximum 32 times the normal speed), deceleration (to a minimum 1/32 times the normal speed) and 30s' addition or reduction to current playing time

Record Backup

- Supports backup of a recording through USB (U disk, mobile HDD)
- Supports backup of a recording by time/event/image search
- Supports record cutting for backing up when playing back
- Supports multiple backup tasks in background and backup status viewing

Event Management

- Supports alarm schedule setting
- Supports enabling or disabling of the motion detection, external sensor alarm input, combination alarm, intelligent alarm and exception alarms including IP address conflict alarm, disk IO error alarm, disk full alarm, no disk alarm, illegal access alarm, network disconnection alarm, IPC offline alarm and so on, alarm trigger configuration supportable
- Supports IPC offline alarm trigger configuration of PTZ, snap, pop-up video, etc.
- Supports event notification modes of alarm-out, pop-up video, pop-up message box, buzzer, e-mail and so on
- Captured images can be attached to an e-mail when an alarm is triggered
- Supports alarm status view of alarm-in, alarm-out, motion detection and exception alarm
- Supports triggering and clearing an alarm manually
- Supports auto-reboot of the system when an exception happens
- Support alarm linkage based on face detection, vehicle detection and license plate recognition
- Some models support face match alarm

Face Recognition (available for some models)

- Supports adding 5000 face pictures to the face database (some models support adding 10,000 face pictures to the face database)
- Supports face capture and face match
- Supports image search by image, track playback and database management
- Supports face information statistics
- Supports face match alarm

LPR Function

- Supports registration of up to 50,000 license plates (some models only support registration of 1,000 license plates)
- Supports license plate detection, matching and search
- Supports vehicle information statistics
- Supports license plate match alarm

Application

- Supports parking lot management
- Supports access control management
- Supports face attendance and face check in (varies by model)

Network Functions

- Supports TCP/IP and PPPoE, DHCP, DNS, DDNS, UPnP, NTP, SMTP protocol and so on
- Supports allow and block list function and the allow and block IP address/IP segment address can be set
- Supports multiple browsers including IE8/9/10/11, Firefox, Opera, Chrome and Safari on Macs
- Supports remote configuration, import and export of the NVR parameters and other system maintenance operations including remote upgrading and system restart
- Supports remote camera configuration through the NVR including video parameters, image quality and so on
- Supports remote search, playback and backup through the NVR
- Supports triggering and clearing manual alarms remotely
- Motorized zoom cameras can be adjusted through the web client
- Supports NVMS or other platform management software to access the NVR and manage it
- Supports NAT function and QR Code scanning by mobile phones and tablets
- Supports mobile surveillance by phones or tablets with iOS or Android OS
- If one camera recording is enabled or disabled manually through the web client, it will be simultaneously enabled or disabled on the NVR
- Supports direct jumping from NVR web client to IPC web client
- The installation mode and display mode of the fisheye camera can be set via Web client

Other Functions

- The NVR can be controlled and operated by the buttons on the front panel (on applicable models), the remote controller and the mouse
- Setup interfaces can be conveniently switched by clicking the main menus at the top
- Supports NVR information viewing including basic, camera status, alarm status, record status, network status, disk and backup status
- Support factory restore, import and export of the system configuration, log view and export and local upgrading by USB mobile device
- Supports auto recognition of the displayer’s resolution
- You can click the right mouse button at any interface to go back to the upper interface
- You can click the mouse wheel at any interface to go to the live view interface
- The display language and video format of the NVR will not be changed and the system logs will be preserved if you restore to the default parameters

- Press and hold the right mouse button for 5 seconds in any interface to switch the output cyclically.

1.3 Front Panel Descriptions

The following descriptions are for reference only.

Type I:

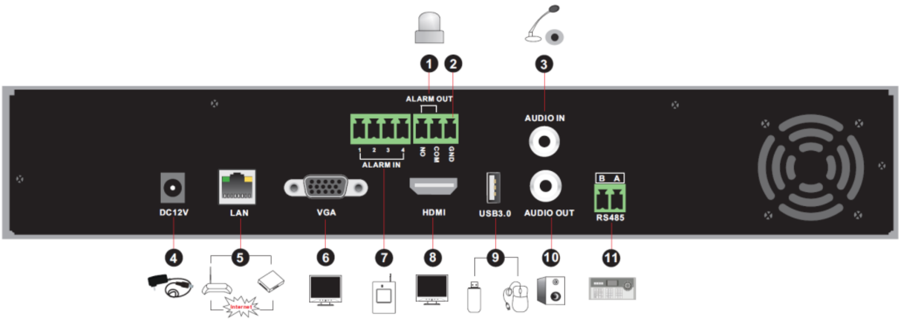
Name	Descriptions
REC	The light will be blue when recording
Net	The light will be blue when there is access to a network
Power	The light will be blue when there is power
Fn	Currently no function

Type II:

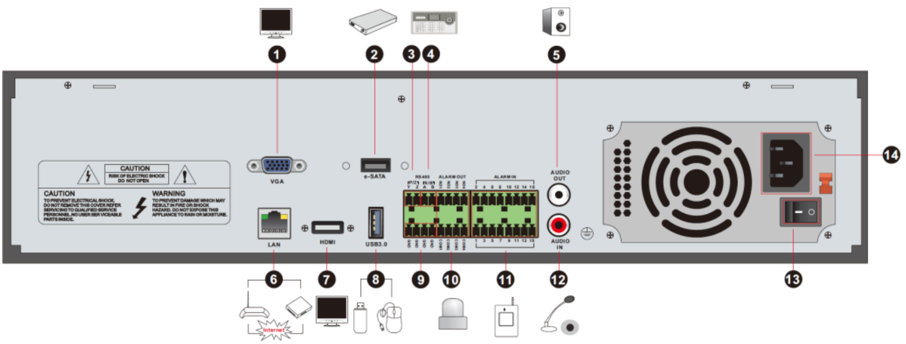
Name	Descriptions
Power	The light will be blue when there is power
HDD	The light will be blue when reading/writing HDD
Net	The light will be blue when there is access to a network
Backup	The light will be blue when backing up files and data
Play	The light will be blue when playing video
REC	The light will be blue when recording
AUDIO /+	1. Adjust audio 2. Increase the value in setup
P.T.Z / -	1. Enter PTZ mode 2. Decrease the value in setup
MENU	Enter Menu in live
INFO	Check the information of the device
BACKUP	Enter backup mode in live
SEARCH	Enter search mode in live
Exit	Exit the current interface
●	Manually record
▶❙	Play/Pause
◀◀	Speed down
▶▶	Speed up
1-9	Input digital number and select camera
0/--	Input number 0, the number above 10
Direction Key	Change direction
Multi-Screen Switch	Change the screen mode
Enter	Confirm selection
USB	To connect external USB device like USB mouse or USB flash

1.4 Rear Panel Descriptions

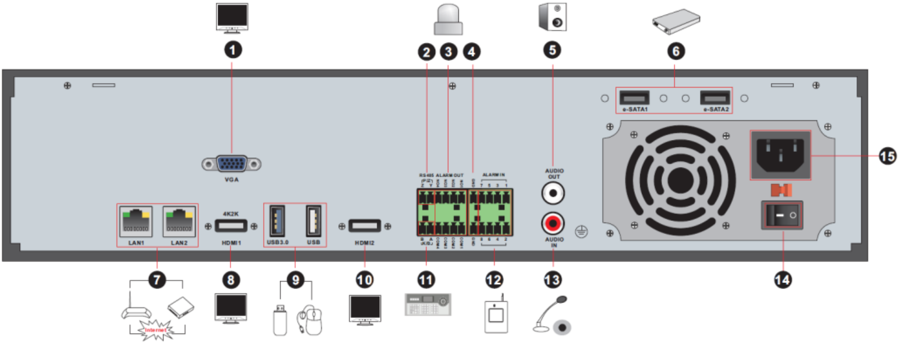
Here we only take a part of real panels for example to introduce their interfaces and connections. The interfaces and locations of the interfaces are only for references. Please take the real object as the standard.



No.	Name	Descriptions
1	ALARM OUT	Relay output; connect to external alarm
2	GND	Grounding
3	AUDIO IN	Audio input; connect to audio input device, like microphone, pickup, etc
4	DC12V	DC12V power input
5	LAN	Network port
6	VGA	Connect to monitor
7	ALARM IN	Alarm inputs for connecting sensors
8	HDMI	Connect to high definition display device
9	USB	Connect USB storage device or USB mouse
10	AUDIO OUT	Audio output; connect to sound box
11	RS485	Connect to keyboard. A is TX+; B is TX-

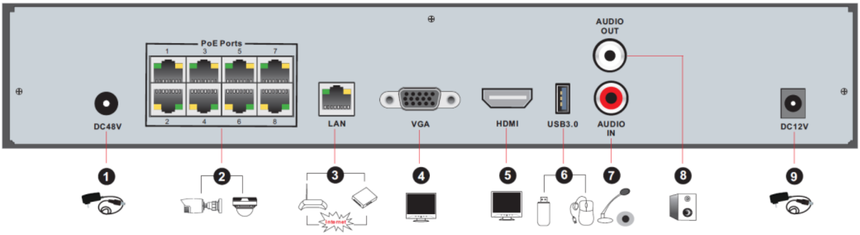


No.	Name	Descriptions
1	VGA	Connect to monitor
2	e-SATA	Connect to HDD with e-SATA interface
3	RS485 Y/Z interface	Connectors for speed dome. Y is TX+, Z is TX- (This interface of some models is unavailable.)
4	RS485 A/B interface	Connect to a keyboard. A is TX+; B is TX-
5	AUDIO OUT	Audio output; connect to sound box
6	LAN	Network port
7	HDMI	Connect to high definition display device
8	USB	Connect USB storage device or USB mouse
9	GND	Grounding
10	ALARM OUT	Relay output; connect to external alarm
11	ALARM IN	Alarm inputs for connecting sensors
12	AUDIO IN	Audio input; connect to audio input device, like microphone, pickup, etc
13	Power Switch	Press the switch to turn on/off the NVR
14	Power Supply	Power supply interface

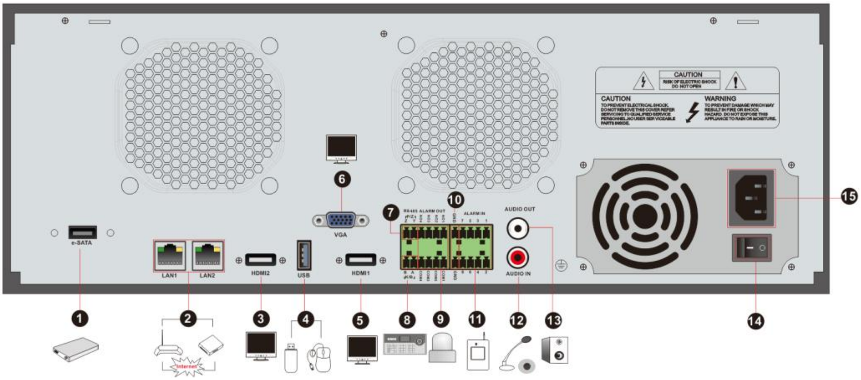


No.	Name	Descriptions
1	VGA	Connect to monitor
2	RS485 Y/Z interface	Connect to speed dome. Y is TX+, Z is TX- (This interface of some models is unavailable.)
3	ALARM OUT	Relay output; connect to external alarm
4	GND	Grounding
5	AUDIO OUT	Audio output
6	e-SATA1/ e-SATA2	Connect to HDD with e-SATA interface
7	LAN1/LAN2	Network port
8	HDMI1	Connect to 4K×2K high definition display device
9	USB3.0/USB	USB3.0 and USB 2.0 interface, connect USB storage

No.	Name	Descriptions
		device or USB mouse
10	HDMI2	Connect to 1920×1080 high definition display device. Connect to monitor as an AUX output channel by channel. Only video display, no menu show
11	RS485 A/B interface	Connect to a keyboard. A is TX+; B is TX-
12	ALARM IN	Alarm inputs for connecting sensors
13	AUDIO IN	Audio input
14	Power Switch	Press the switch to turn on/off the NVR
15	Power Supply	Power supply interface



No.	Name	Descriptions
1	Power Supply	DC48V power supply interface
2	PoE port	8 PoE network ports; connect to 8 PoE IP cameras
3	LAN	Network port
4	VGA	Connect to monitor
5	HDMI	Connect to 1920×1080 high definition display device
6	USB3.0	USB3.0 interface, connect USB storage device or USB mouse
7	AUDIO IN	Audio input; connect to audio input device, like microphone, pickup, etc
8	AUDIO OUT	Audio output; connect to sound box
9	Power Supply	DC12V power supply interface



No.	Name	Descriptions
1	e-SATA	Connect to HDD with e-SATA interface
2	LAN1/LAN2	Network port
3	HDMI2	Connect to 1920×1080 high definition display device. Connect to monitor as an AUX output channel by channel. Only video display, no menu show
4	USB	USB interface, connect USB storage device or USB mouse
5	HDMI1	Connect to 4K×2K high definition display device
6	VGA	Connect to monitor
7	RS485 Y/Z interface	Connect to speed dome. Y is TX+, Z is TX- (This interface of some models is unavailable.)
8	RS485 A/B interface	Connect to keyboard. A is TX+; B is TX-
9	ALARM OUT	Relay output; connect to external alarm
10	GND	Grounding
11	ALARM IN	Alarm inputs for connecting sensors
12	AUDIO IN	Audio input; connect to audio input device, like microphone, pickup, etc
13	AUDIO OUT	Audio output; connect to sound box
14	Power Switch	Press the switch to turn on/off the NVR
15	Power Supply	Power supply interface

1.5 Connections

- **Video Connections**

Video Output: Supports VGA/HDMI video output. You can connect to a monitor through these video output interfaces simultaneously or independently.

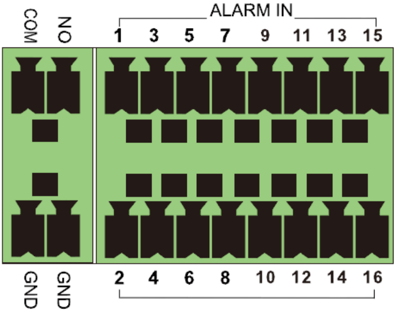
- **Audio Connections**

Audio Input: Connect to microphone, pickup, etc.

Audio Output: Connect to headphone, powered speaker (ex, ASPC20), amplifier, or other audio output devices.

- **Alarm Connections**

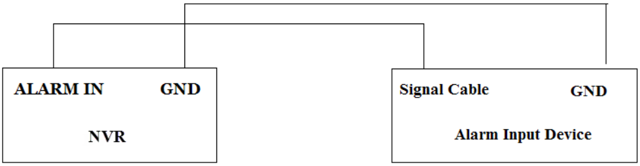
Some models may not support this function. Take 16 CH alarm inputs and 1 CH alarm output for example.



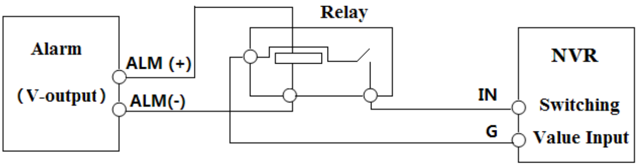
Alarm Input:

Alarm IN 1~16 are 16 CH alarm input interfaces. There are no type requirements for sensors. NO type and NC type are both available.

The way to connect sensor and the device is as shown below:



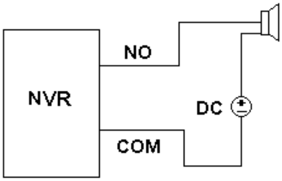
The alarm input is an open/closed relay. If the input is not an open/closed relay, please refer to the following connection diagram:

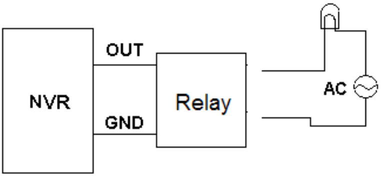


Alarm Output:

The way to connect alarm output device:

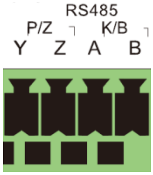
Pull out the green terminal blocks and loosen the screws in the alarm-out port. Then insert the signal wires of the alarm output devices into the port of NO and COM separately. Finally, tighten the screws. Provided that the external alarm output devices need power supply, you can connect the power supply as per the following figures.



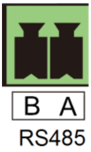


- **RS485 Connection**

There are two types of RS485 interfaces:



(Type 1)



(Type 2)

Type 1: The P/Z interfaces are unavailable temporarily. K/B interfaces are used to connect keyboard.

Type 2: The RS485 interfaces are used to connect keyboard. A is TX+; B is TX-.

2 Basic Operation Guide

2.1 Startup & Shutdown

Please make sure all the connections are done properly before you power on the unit. Proper startup and shutdown are crucial to extending the life of your device.

2.1.1 Startup

① Connect the output display device to the VGA/HDMI interface of the NVR.

② Connect the mouse and power. When powered on, the device will boot and the power LED would turn blue.

③ After you read the privacy statement, a WIZARD window will pop up (you should select the display language the first time you use the NVR). Refer to Startup Wizard for details.

2.1.2 Shutdown

You can power off the device by using remote controller or mouse.

By remote controller:

① Press Power button. This will take you to a shutdown window. The unit will power off after clicking the "OK" button and verifying the username and password.

② Disconnect the power.

By mouse:

① Click ***Start→Shutdown*** to open the Shutdown window. Select "Shutdown" in the window. The unit will power off after clicking the "OK" button and verifying the username and password.

② Disconnect the power according to the prompt shown on the screen.

2.2 Remote Controller

① Uses two AAA size batteries. (Not included)

② Open the battery cover of the remote controller.

③ Place batteries. Please note the polarity (+ and -) and insert properly.

④ Replace the battery cover.

Key points to check in case the remote doesn't work.

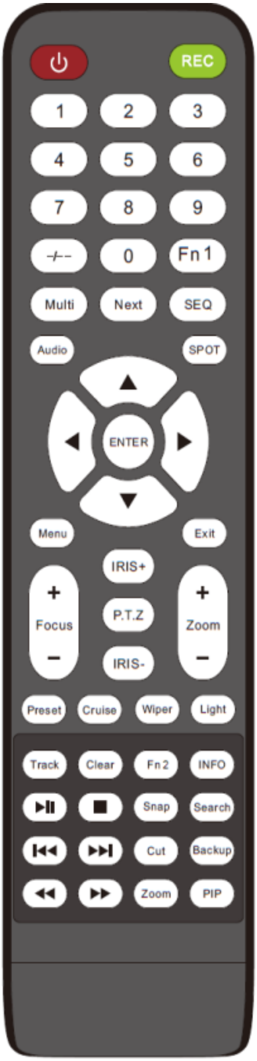
1. Check batteries polarity.
2. Check the remaining charge in the batteries.
3. Check IR controller sensor for any masking.

If it still doesn't work, please contact your distributor. Note that the remote control is the same for all units of the same model. Be sure to point the IR sensor of the remote control directly towards the IR receiver of the NVR you wish control if you have multiple devices.

It's also recommended to place the recorders away from each other if possible.

There are two kinds of remote controller. The interface of remote controller is shown as below.

Type I:



Button	Function
⏻ Power Button	Turn device on and off
Record Button	To start recording
-/-- /0-9	Input number or choose camera
Fn1 Button	Currently no function
Multi Button	Choose multi screen display mode
Next Button	Switch camera
SEQ	Go to sequence view mode
Audio	Enable audio output in live mode
SPOT	Currently no function
Direction button	Move cursor in setup or pan/title PTZ
Enter Button	Confirm a choice or setup
Menu Button	Go to the main menu
Exit Button	Exit the current interface
Focus/IRIS/Zoom/PTZ	Control PTZ camera
Preset Button	Enter into preset setting in PTZ mode
Cruise Button	Go to cruise setting in PTZ mode
Track Button	Currently no function
Wiper Button	Currently no function
Light Button	Currently no function
Clear Button	Currently no function
Fn2 Button	Currently no function
Info Button	Get information about the device
⏯ ⏹ ⏮ ⏭ ⏪ ⏩	Control playback. Play(Pause)/Stop/Previous Frame/Next Frame/Speed Down/Speed Up
Snap Button	Take snapshots manually
Search Button	Go to the search and backup interface
Cut Button	Currently no function
Backup Button	Go to the search and backup interface
Zoom Button	Zoom in
PIP Button	Currently no function

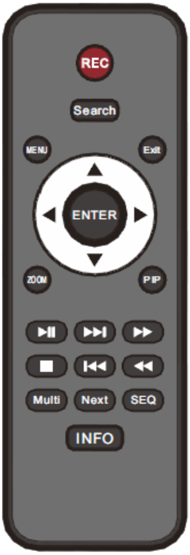
Calling login box: After the device starts successfully, the login box will appear by pressing "Menu" or "Enter" button.

Password input: Move to the password edition box by pressing ▲ ▼ ◀ ▶ and then press the digital numbers to enter the password; press “Exit” to delete the input digital number; But the “digital number + letter” password cannot be input by the remote controller. You need to input by mouse-click.

Playback control: Press ⏯ to enter the playback interface. Press ⏪ or ⏩ to speed down or up the recorded video; press “Next” to switch the playback camera (channel); press “Multi” to switch the screen display mode; press ⏹ to stop playing; press ⏯ to pause; after the playback pauses, press ⏮/⏭ to play the previous or next frame.

PTZ control: Select the PTZ camera through the direction buttons and then press “PTZ” button to go to the PTZ control mode. Press the direction buttons to move the PTZ camera; press “Preset”+ “digital number” (eg. 3) to call preset 3; press “Cruise” + “digital number” (eg.1) to call cruise 1. Note that the corresponding preset and cruise must be set by mouse-click in advance, or they cannot be called.

Type II:



Button	Function
REC	Record manually
Search	Enter the search and backup interface
MEUN	Enter the main menu
Exit	Exit the current interface
ENTER	Confirm the choice or setup
Direction button	Move cursor in setup
ZOOM	Zoom in
PIP	Currently no function
⏯ ⏭ ⏩ ⏹ ⏮ ⏪	Control playback. Play(Pause)/Next Frame/Speed Up/Stop/Previous Frame/Speed Down
Multi	Choose multi screen display mode
Next	Switch camera
SEQ	Go to sequence view mode
INFO	Get information about the device

Playback control: the operations are the same as above.

PTZ control: select the PTZ camera and then press “Enter” to go to the PTZ control mode. Press the direction buttons to move the PTZ camera.

Note: Before using the remote controller without digital numbers, you need to log in the device by mouse-click first. Then turn the IR sensor of the remote controller towards the IR receiver of the NVR to control it.

2.3 Mouse Control

- **Mouse control in Live Display & Playback interface**

In the live display & playback interface, double click on any camera window to show the window in single screen mode; double click the window again to restore it to the previous size.

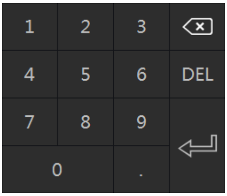
In the live display & playback interface, if the interfaces display in full screen, move the mouse to the top of the interface to have the tool bar appear. The tool bar will disappear automatically after you move the mouse away from it; move the mouse to the right side of the interface to pop up a panel and the panel will disappear automatically after you move the mouse away from it.

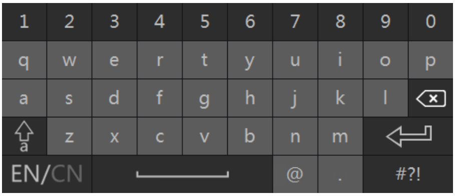
- **Mouse control in text-input**

Move the mouse to the text-input box and then click the box. The input keyboard will pop up automatically.

> *Note: Mouse is the default tool for all operations unless an exception is indicated.*

2.4 Text-input Instruction





The interface has two types of input boxes. Refer to the above pictures. The left box is the number-only input box and the right box provides inputs of numbers, letters and punctuation characters. The introductions of keys on the input boxes are shown below.

Button	Meaning	Button	Meaning
⌫	Backspace key	#?!	Switch keyboard to see more punctuation characters
DEL	Delete Key	↵	Enter key
⇧a	Switch between upper and lower letter	␣	Space key
EN/CN	Switch language		

2.5 Common Button Operation

Button	Meaning
⌄	Click to show the menu list.
↓ ↑	Click to change the sequence of the list.
🖼 ⊞ ☷ ☰	Click to change the camera displaying mode.
✕	Click to close the current interface.
Earliest	Click to go to the earliest date of camera recording.
Latest	Click to go to the latest date of camera recording.

3 Wizard & Main Interface

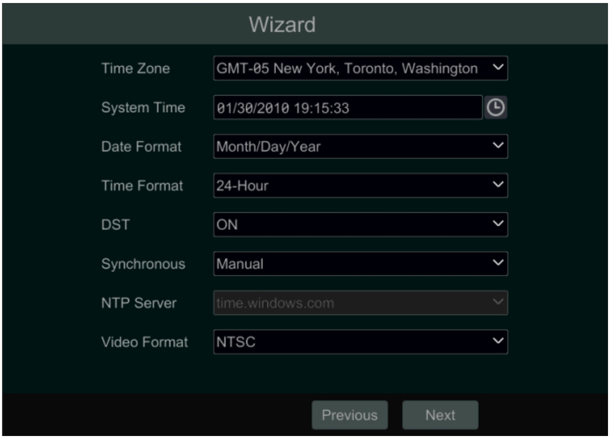
3.1 Startup Wizard

The disk icons will be shown on the top of the startup interface. You can view the number and status of each disk quickly and conveniently through these icons (: no disk; : unavailable disk; : RW available disk).

You can quickly configure the NVR by wizard setup to make the NVR work normally. You must configure the wizard if you start the NVR for the first time (or click “Skip” to cancel the wizard until the next time you login). Maybe different versions have different wizard steps. The following wizard steps are for reference only.

① Choose the language and locality as needed if it is the first time for you to use the wizard and then read the privacy statement, checkmark “***I have read and agree***” and click “OK”.

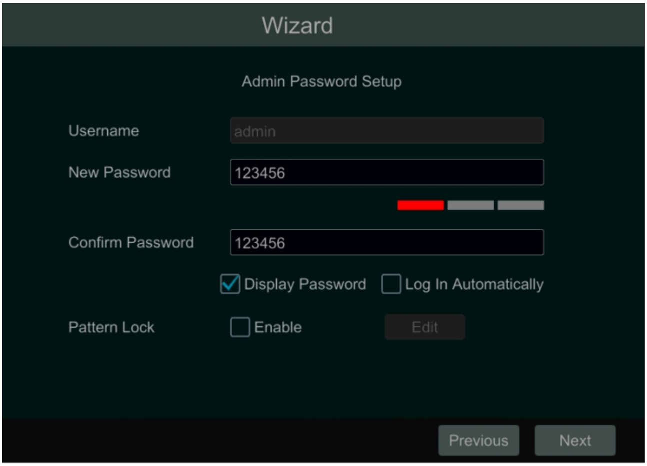
② ***Date and Time Configuration***. The date and time of the system need to be set up if you use the wizard for the first time. Refer to the following figure. Set the time zone, system time, date format, time format and video format. The DST will be enabled by default if the time zone selected includes DST. Click “Next” to continue.



Wizard

Time Zone	GMT-05 New York, Toronto, Washington
System Time	01/30/2010 19:15:33
Date Format	Month/Day/Year
Time Format	24-Hour
DST	ON
Synchronous	Manual
NTP Server	time.windows.com
Video Format	NTSC

③ ***System Login***. Set your own password when you use the wizard for the first time (the default username of the system is ***admin***); select the login username and enter the corresponding password next time.



Wizard

Admin Password Setup

Username: admin

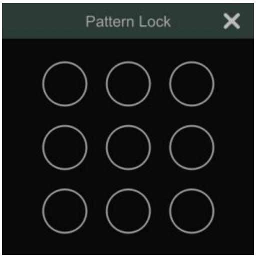
New Password: 123456

Confirm Password: 123456

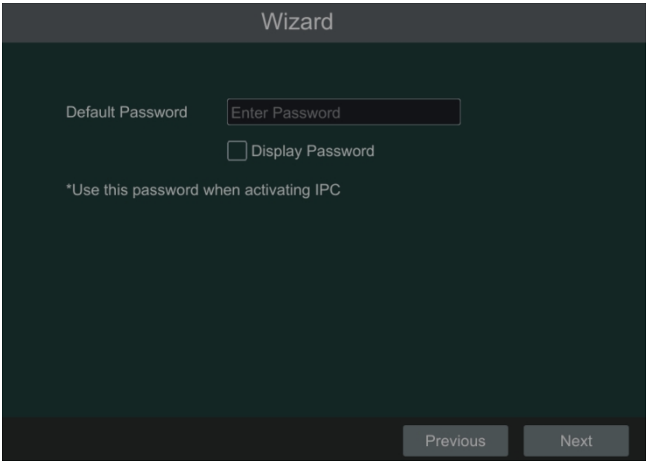
☑ Display Password ☐ Log In Automatically

Pattern Lock ☐ Enable

Enable pattern lock and click “Edit” to set the pattern lock.



Click “Next” to set the default password which is used to activate IPC.



Wizard

Default Password: Enter Password

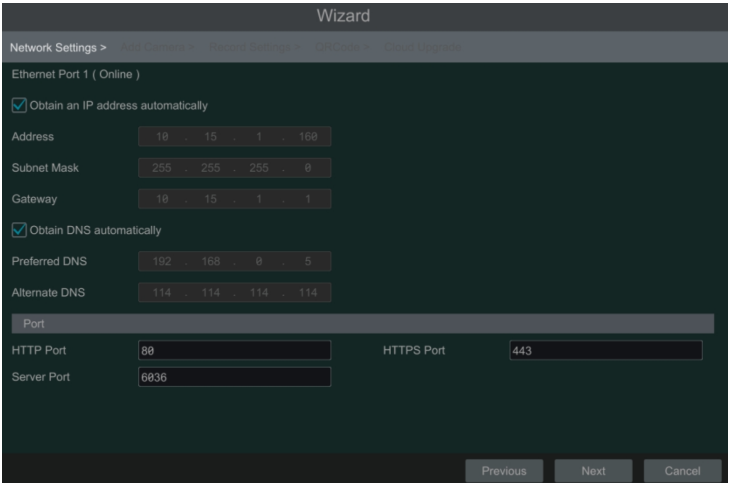
☐ Display Password

*Use this password when activating IPC

Click "Next" to set questions and answers for password security of admin. If you forget the password, please refer to Q4 in Appendix A FAQ for details.
Click "Next" to continue.

④ ***Disk Settings.*** You can view the disk number, disk capacity of the NVR and serial number, R&W status of the disk. Click "Format" to format the disk. Click "Next" to continue. Then click "Wizard Setup".

⑤ ***Network Settings***. Select the network parameters as required. Check "Obtain an IP address automatically" and "Obtain DNS automatically" to get the IP address and DNS automatically (the DHCP function of the router in the same LAN should also be enabled), or manually enter them. Enter the HTTP port, HTTPS port and Server port (please see Port Configuration for details). Click "Next" to continue.



Ethernet Port 1 (Online)

☑ Obtain an IP address automatically

Address 10 . 15 . 1 . 160

Subnet Mask 255 . 255 . 255 . 0

Gateway 10 . 15 . 1 . 1

☑ Obtain DNS automatically

Preferred DNS 192 . 168 . 0 . 5

Alternate DNS 114 . 114 . 114 . 114

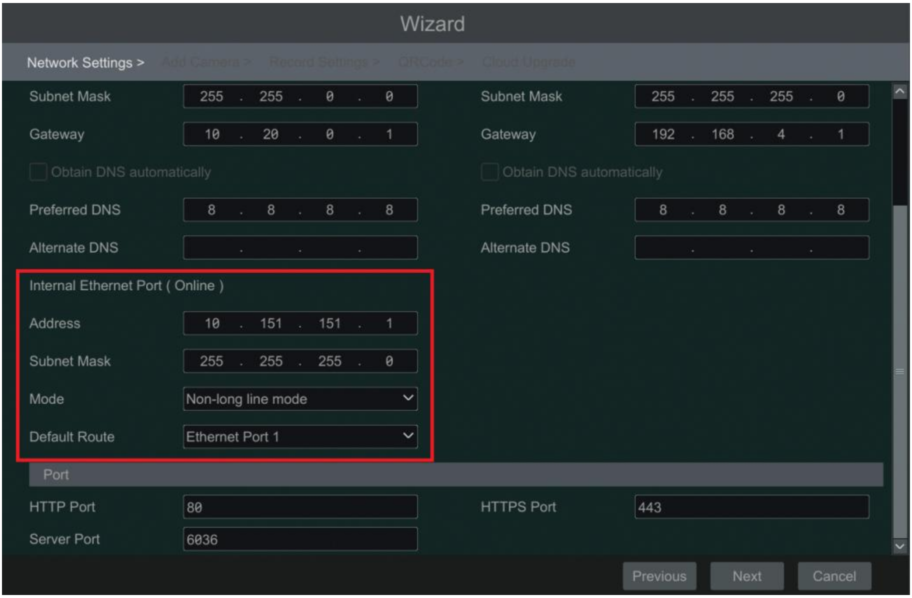
Port

HTTP Port 80 HTTPS Port 443

Server Port 6036

Note:

➢ If you use the NVR with the PoE network ports, the online state of the internal Ethernet port will be shown on the interface. Refer to the picture below. Please refer to TCP/IP Configuration for detail introduction of the internal Ethernet port.



Wizard

Network Settings > Add Camera > Record Settings > QRCode > Cloud Upgrade

Subnet Mask	255 . 255 . 0 . 0	Subnet Mask	255 . 255 . 255 . 0
Gateway	10 . 20 . 0 . 1	Gateway	192 . 168 . 4 . 1
□ Obtain DNS automatically		□ Obtain DNS automatically	
Preferred DNS	8 . 8 . 8 . 8	Preferred DNS	8 . 8 . 8 . 8
Alternate DNS	. . .	Alternate DNS	. . .

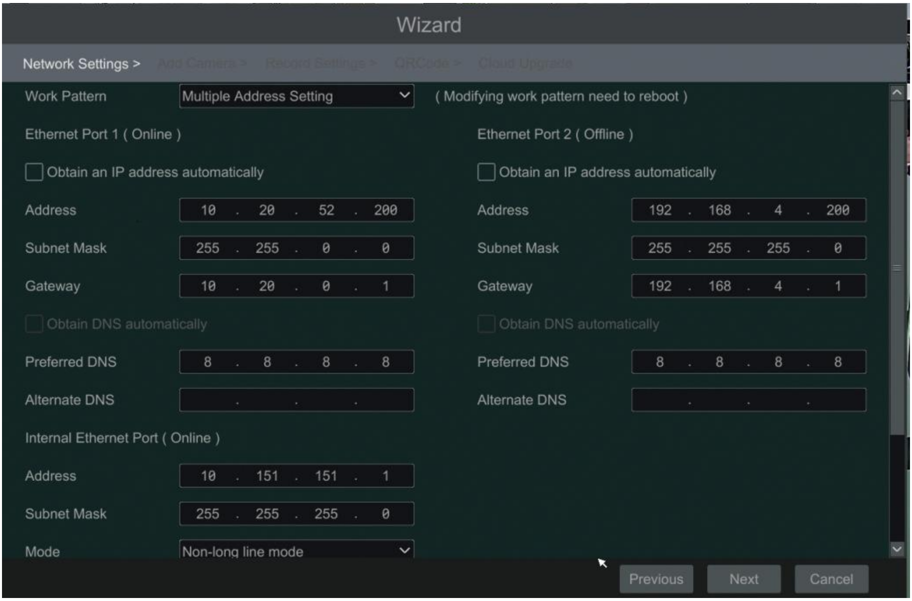
Internal Ethernet Port (Online)

Address	10 . 151 . 151 . 1
Subnet Mask	255 . 255 . 255 . 0
Mode	Non-long line mode
Default Route	Ethernet Port 1

Port

HTTP Port	80	HTTPS Port	443
Server Port	6036		

➢ If the NVR has two or more network ports, you can select TOE (varies by model) as needed. Select the work pattern: Network Fault Tolerance and Multiple Address Setting are available. Refer to the pictures below. Please refer to TCP/IP Configuration for more detailed information.



Wizard

Network Settings > Add Camera > Record Settings > QRCode > Cloud Upgrade

Work Pattern: Multiple Address Setting (Modifying work pattern need to reboot)

Ethernet Port 1 (Online)

□ Obtain an IP address automatically

Address: 10 . 20 . 52 . 200

Subnet Mask: 255 . 255 . 0 . 0

Gateway: 10 . 20 . 0 . 1

□ Obtain DNS automatically

Preferred DNS: 8 . 8 . 8 . 8

Alternate DNS: . . .

Ethernet Port 2 (Offline)

□ Obtain an IP address automatically

Address: 192 . 168 . 4 . 200

Subnet Mask: 255 . 255 . 255 . 0

Gateway: 192 . 168 . 4 . 1

□ Obtain DNS automatically

Preferred DNS: 8 . 8 . 8 . 8

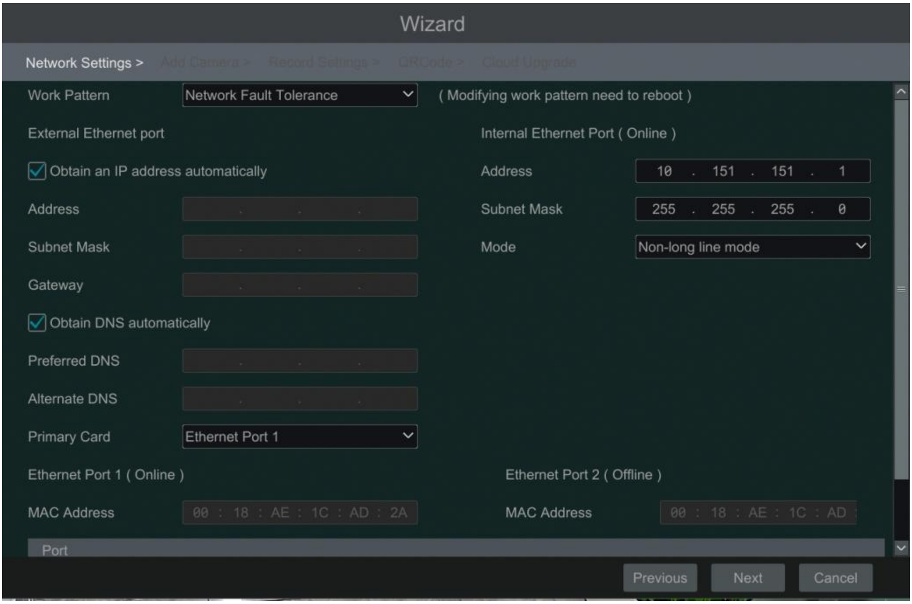
Alternate DNS: . . .

Internal Ethernet Port (Online)

Address: 10 . 151 . 151 . 1

Subnet Mask: 255 . 255 . 255 . 0

Mode: Non-long line mode



Wizard

Network Settings > Add Camera > Record Settings > QRCode > Cloud Upgrade

Work Pattern: Network Fault Tolerance (Modifying work pattern need to reboot)

External Ethernet port

☑ Obtain an IP address automatically

Address: . . .

Subnet Mask: . . .

Gateway: . . .

☑ Obtain DNS automatically

Preferred DNS: . . .

Alternate DNS: . . .

Primary Card: Ethernet Port 1

Internal Ethernet Port (Online)

Address: 10 . 151 . 151 . 1

Subnet Mask: 255 . 255 . 255 . 0

Mode: Non-long line mode

Ethernet Port 1 (Online)

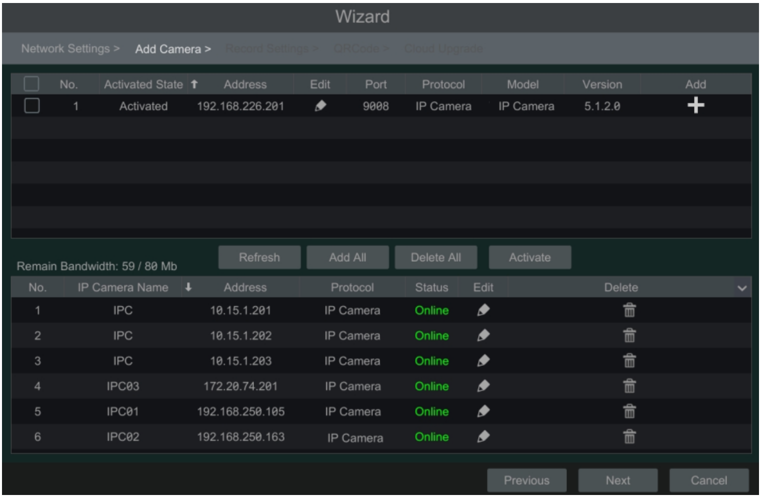
MAC Address: 00 : 18 : AE : 1C : AD : 2A

Ethernet Port 2 (Offline)

MAC Address: 00 : 18 : AE : 1C : AD

Port

⑥ ***Add Camera***. Click "Refresh" to refresh the list of online IP cameras which are in the same local network with NVR.



Wizard

Network Settings > Add Camera > Record Settings > QRCode > Cloud Upgrade

□	No.	Activated State	Address	Edit	Port	Protocol	Model	Version	Add
□	1	Activated	192.168.226.201	✎	9008	IP Camera	IP Camera	5.1.2.0	+

Remain Bandwidth: 59 / 80 Mb

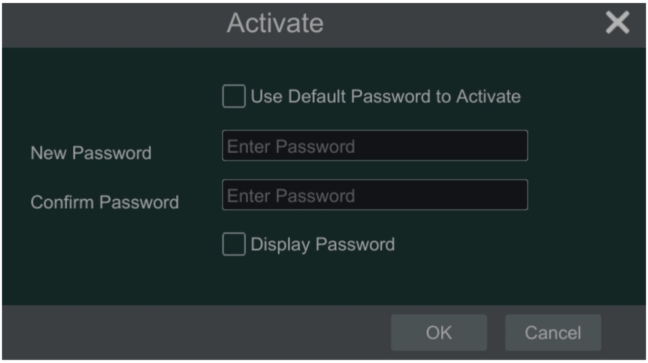
Refresh | Add All | Delete All | Activate

No.	IP Camera Name	Address	Protocol	Status	Edit	Delete
1	IPC	10.15.1.201	IP Camera	Online	✎	🗑
2	IPC	10.15.1.202	IP Camera	Online	✎	🗑
3	IPC	10.15.1.203	IP Camera	Online	✎	🗑
4	IPC03	172.20.74.201	IP Camera	Online	✎	🗑
5	IPC01	192.168.250.105	IP Camera	Online	✎	🗑
6	IPC02	192.168.250.163	IP Camera	Online	✎	🗑

Previous | Next | Cancel

In the above interface, the device activation state can be viewed. For the activated device, you can click + to add the searched camera. Click “Add All” to add all the cameras in the list. If the default password is not used by the activated device, you need to modify it manually. Click 🗑 to delete the added camera. Click “Delete All” to delete all the added cameras.

For the unactivated devices, you can activate one by one or in batches. Check the unactivated device and click “Activate” to pop up an activation box.



Activate ✕

□ Use Default Password to Activate

New Password: Enter Password

Confirm Password: Enter Password

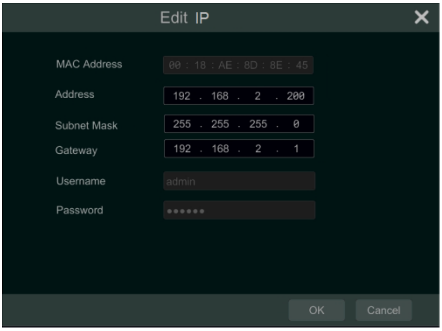
□ Display Password

OK | Cancel

You can use default password to activate.

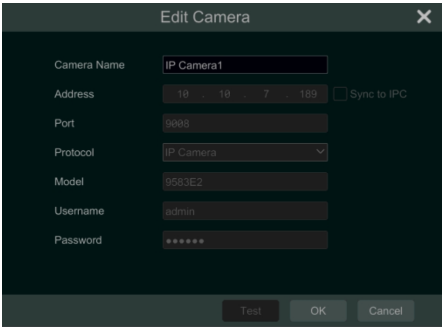
If your camera needs to be activated by self-defined password, you need to manually enter the password to activate.

Click ✎ to edit the searched IP camera as shown on the below left. Enter the new IP address, subnet mask, gateway, username and the password of the camera. Click “OK” to save the settings.



Edit IP

MAC Address 00 : 18 : AE : 8D : 8E : 45
Address 192 . 168 . 2 . 200
Subnet Mask 255 . 255 . 255 . 0
Gateway 192 . 168 . 2 . 1
Username admin
Password ••••••



Edit Camera

Camera Name IP Camera1
Address 10 . 10 . 7 . 189 □ Sync to IPC
Port 9008
Protocol IP Camera
Model 9583E2
Username admin
Password ••••••

Click ✎ to edit the added camera as shown on the above right. Enter the new camera name, IP address, port, username and the password of the camera. You can check "Sync to IPC" to modify the IP address of the IPC via different network segments for being in the same network segment with the NVR. Then click "Test" to test the connection. Click "OK" to save the settings. You can change the IP camera name only when the added camera is online. Click "Next" to continue.

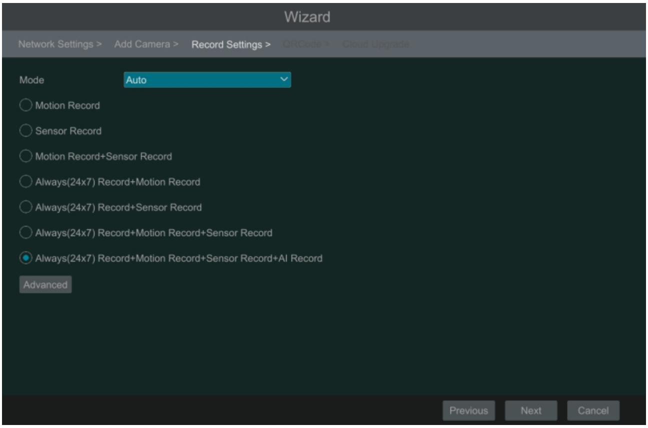
Tips： Please skip Step ⑦ and ⑧ if the NVR does not support RAID function.

⑦ ***Disk Mode.*** Click "Enable RAID" to enable the RAID function. Click "Next" to continue.

⑧ ***Create an array.*** Set the array name and select array type which including RAID0, RAID1, RAID5, RAID6 and RAID10. The global hot spares and array capacity can also be viewed here. See Disk for details. Click "Next" to continue.

⑨ ***Record Settings***. Two record modes are available: auto and customization.

Auto: Select one auto mode in the interface as shown below and then click the "Next" to save the settings. Click "Advanced" to self-define record mode. See Mode Configuration for details.



Wizard

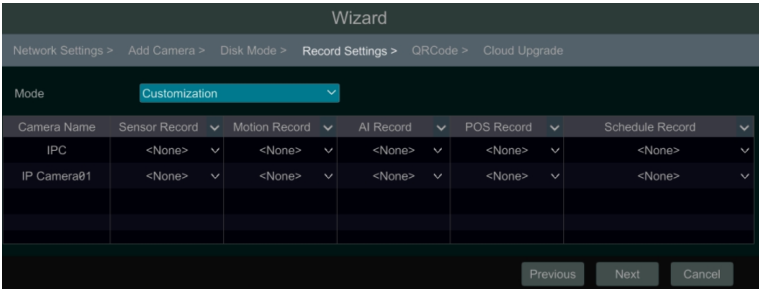
Network Settings > Add Camera > Record Settings > QRCode > Cloud Upgrade

Mode Auto

○ Motion Record
○ Sensor Record
○ Motion Record+Sensor Record
○ Always(24x7) Record+Motion Record
○ Always(24x7) Record+Sensor Record
○ Always(24x7) Record+Motion Record+Sensor Record
● Always(24x7) Record+Motion Record+Sensor Record+AI Record

Advanced
Previous
Next
Cancel

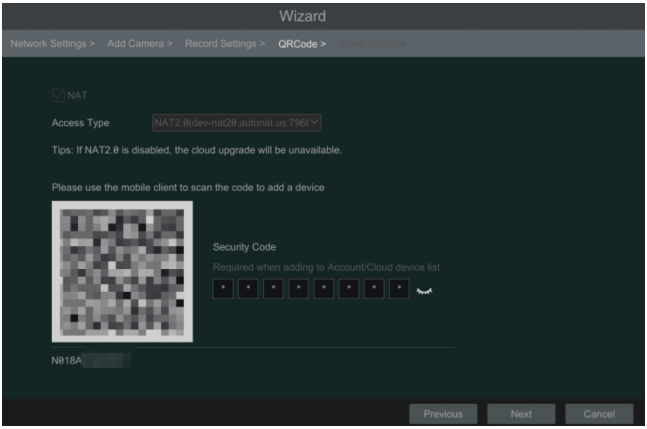
Customization: Set the “Sensor Record”, “Motion Record”, “AI Record”, “POS Record” and “Schedule Record” of each camera. Click “OK” to save the settings. See Mode Configuration for details.



Mode: Customization

Camera Name	Sensor Record	Motion Record	AI Record	POS Record	Schedule Record
IPC	<None>	<None>	<None>	<None>	<None>
IP Camera01	<None>	<None>	<None>	<None>	<None>

⑩ ***QRCode.*** Enable the NAT function in the interface or set it in the network configuration after exiting the wizard (please refer to NAT Configuration for details). You can scan the QRCode through mobile client which is installed in the mobile phone or tablet PC to log in the mobile client instantly. Please refer to Mobile Client Surveillance for details. Click “OK” to save the settings.



☑ NAT

Access Type: NAT2.0(dev-nat20.autonat.us:796

Tips: If NAT2.0 is disabled, the cloud upgrade will be unavailable.

Please use the mobile client to scan the code to add a device

Security Code

Required when adding to Account/Cloud device list

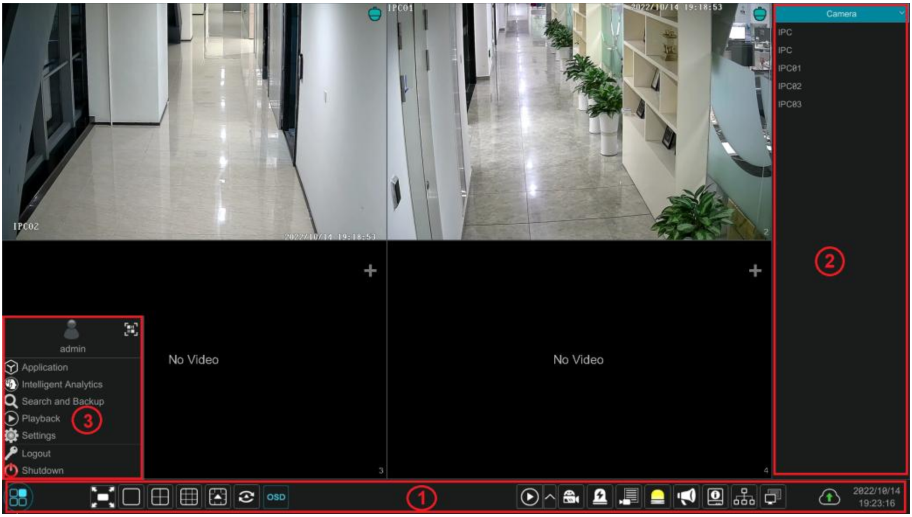
* * * * * * * *

N018A[redacted]

⑪ ***Cloud Upgrade.*** Enable “Cloud Upgrade” and then click “OK” to save. If this function is enabled, you can get the latest version from the cloud server. Please refer to Cloud Upgrade for details. Only user levels with “Network” access will be able to enable/disable cloud upgrades.

3.2 Main Interface

3.2.1 Main Interface Introduction

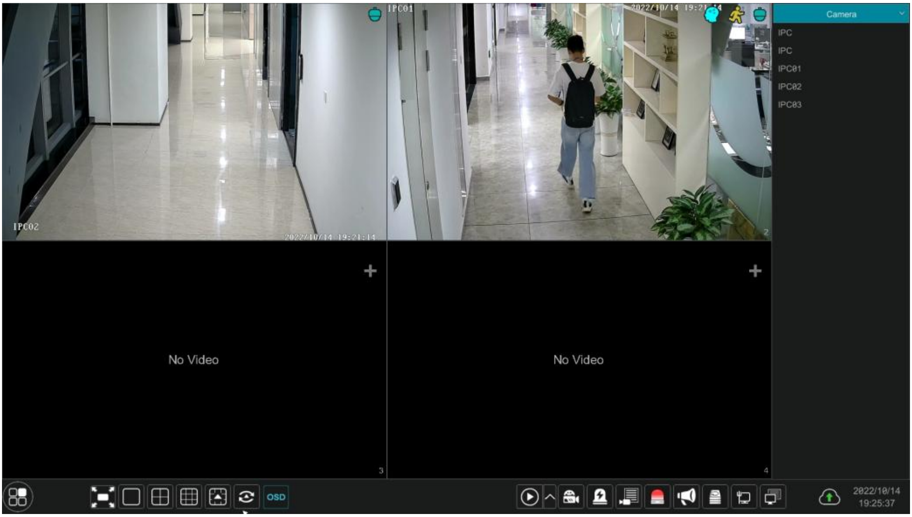


The buttons in area ① are described in the table below.

Button	Meaning
⊞	Start button. Click to pop up area ③.
⛶	Full screen button. Click to show full screen; click it again to exit the full screen.
□ ⊞ ▦ 16 ⏏	Screen mode button.
⟳	Dwell button (see Quick Sequence View and Scheme View In Sequence for details).
OSD	Click to enable OSD; click again to disable OSD.
▶ ^	Click ^ to set the default playback time before starting instant playback (Instant Playback) or going to the playback interface for playback operations (Playback Interface Introduction); click ▶ to go to the playback interface. For instance, if you choose “5 minutes ago” as the default playback time, you can playback the recording from the past five minutes.
🎥	Manual record button. Click to enable/disable record.
⚠	Manual alarm button. Click to trigger or clear the alarm-out manually in the popup window.
📄	Record status button. Click to view the record status.
🚨	Alarm status button. Click to view the alarm status.
📢	Voice broadcast button. Click to select the channel to broadcast.

Button	Meaning
🖴 / 🖴	Disk status button. Click to view the disk status and RAID status.
🖧 / 🖧	Network status button. Click to view the network status.
🖥	Information button. Click to view system information.
☁	Click to enable the cloud upgrade feature.

Note: Different models may have different buttons on the live view interface. See the following picture. All pictures in this manual are for reference only; the real product shall prevail.



Introduction of area ②:

Area ② is hidden by default. Move the cursor to the right to reveal this area. Click "Camera" to view all the added cameras in the camera list. Select one camera window on the left side of the interface and then double click one camera in the list to preview the camera image in the selected window.

Click ⌄ on the top right corner and then select "Single Channel Sequences" to view all the added groups in the group list; click one group in the list to view all the added cameras in the group (refer to Add/Edit Camera Group for detail configuration of the camera group). Select one camera window on the left side of the interface and then double click one group in the group list to preview the cameras' images one by one in the selected window.

Click ⌄ on the top right corner and then select "Customize Display Modes" to view all the display modes in the display mode list (refer to Preview by Display Mode for detail configuration of the display mode). Double click one display mode in the list to switch to the display mode for previewing.

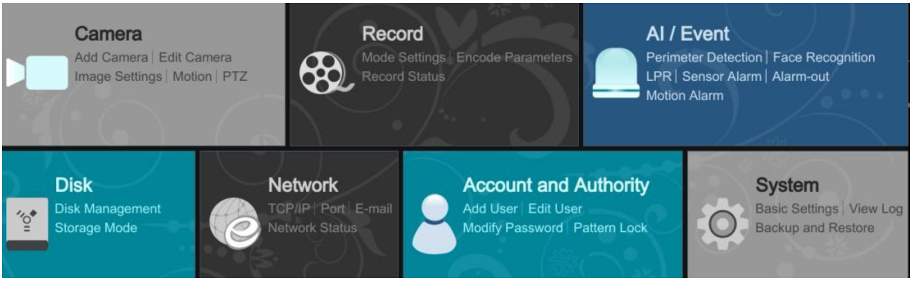
Click ⌄ on the top right corner and then select “Target Detection” to go to target detection interface. This tab will show the captured human, vehicles, license plates and face images. (This function is only available for some models). Note that only some models support multi-channel target detection display.

Introduction of area ③:

Icon / Button	Meaning
admin	It shows the current login user. Click the QR code icon to view the QR code and security code. User can quickly add the NVR to the server list of the mobile APP by scanning this QR code.
Intelligent Analytics	Click to go to the intelligent analytics interface.
Application	Click to set parking lot, access control, face attendance and face check-in (varies by models)
Search and Backup	Click to go to record search and backup interface, see Record Search, Playback & Backup for details.
Playback	Click to go to playback interface (click ▮ on the tool bar at the bottom of the live view interface to set the default playback time), see Playback Interface Introduction for details.
Settings	Click to open the setup panel, see Setup Panel for details.
Logout	Click to log out the system.
Shutdown	Click it and then select “Logout”, “Reboot” or “Shutdown” in the popup window.

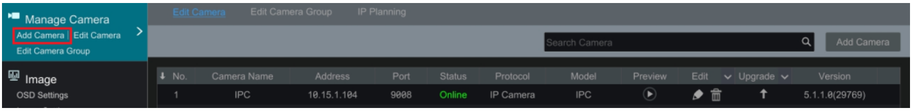
3.2.2 Setup Panel

Click ***Start→Settings*** to open the setup panel as shown below.



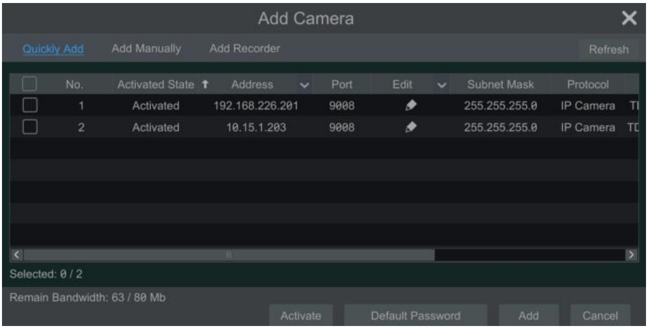
The setup panel includes seven modules. Each module provides some function entries with links for convenient operation.

Here we take ***Camera*** module as an example. The ***Camera*** module provides convenient links such as “Add Camera”, “Edit Camera”, “Image Settings”, “Motion” and “PTZ”. Click ***Camera*** to go to the camera management interface as shown below.



No.	Camera Name	Address	Port	Status	Protocol	Model	Preview	Edit	Upgrade	Version
1	IPC	10.15.1.104	9008	Online	IP Camera	IPC				5.1.1.0(29769)

There are some function items on the left side of the camera management interface. Click each item to go to corresponding interface or window. For instance, click “Add Camera” to open the window as shown below.

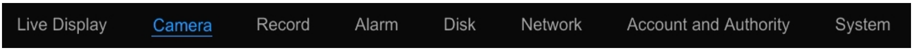


□	No.	Activated State	Address	Port	Edit	Subnet Mask	Protocol	
□	1	Activated	192.168.226.201	9008		255.255.255.0	IP Camera	TI
□	2	Activated	10.15.1.203	9008		255.255.255.0	IP Camera	TD

Selected: 0 / 2

Remain Bandwidth: 63 / 80 Mb

Click the main menus on the top of the camera management interface to go to corresponding interfaces. Refer to the picture below. For instance, you can go to system setup interface by clicking “System” tag.



3.2.3 Main Functions

- **Camera**

The module covers the functions such as ***Camera Management*** (see Camera Management for details), ***Image Settings*** (see Preview Image Configuration for details), ***Motion*** (see Motion Alarm for details), and ***PTZ*** (see PTZ for details) and so on.

- **Record**

The module covers the functions such as ***Encode Parameters*** and ***Record Schedule*** and so on. Please see Record & Disk Management for details.

- **AI/Event**

The module covers the functions such as ***Smart Event, Combination Alarm, Exception, Sensor and Motion Alarm Handling*** and ***Alarm Out Settings***. Please see AI Event Management and General Event Management for details.

- **Disk**

The module covers the functions such as ***Disk Management***, ***Storage Mode*** and ***Disk Information*** and so on. Please see Record & Disk Management for details.

- **Network**

The module covers the functions such as ***TCP/IP***, ***DDNS***, ***Port***, ***E-mail*** and ***Network Status*** and so on. Please see Network Configuration for details.

- **Account and Authority**

The module covers the functions such as ***Account Management*** (see Account Management for details) and ***Permission Management*** (see Permission Management for details) and so on.

- **System**

The module covers the functions such as ***Basic Configuration*** (see Basic Configuration for details), ***Device Information*** (see View System Information for details), ***Log Information*** (see View Log for details) and ***Configuration File Import & Export*** (see Backup and Restore for details) and so on.

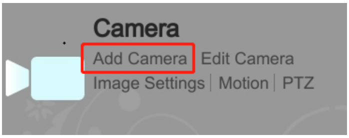
4 Camera Management

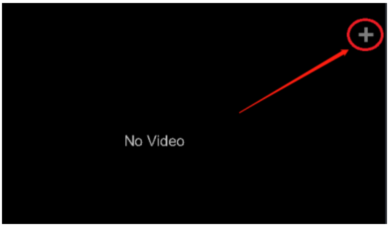
4.1 Add/Edit Camera

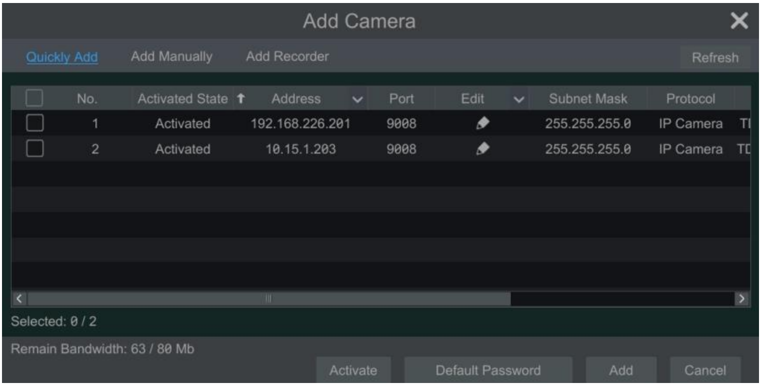
4.1.1 Add Camera

The network parameters of the NVR should be set before adding an IP camera (see TCP/IP Configuration for details).

Refer to the pictures below. Click ***Add Camera*** in the setup panel or + in the top right corner of the preview window to open the "Add Camera" window as shown below. You can quickly add from a list, or add the IP camera manually.







☐	No.	Activated State	Address	Port	Edit	Subnet Mask	Protocol	
☐	1	Activated	192.168.226.201	9008	✎	255.255.255.0	IP Camera	TI
☐	2	Activated	10.15.1.203	9008	✎	255.255.255.0	IP Camera	TI

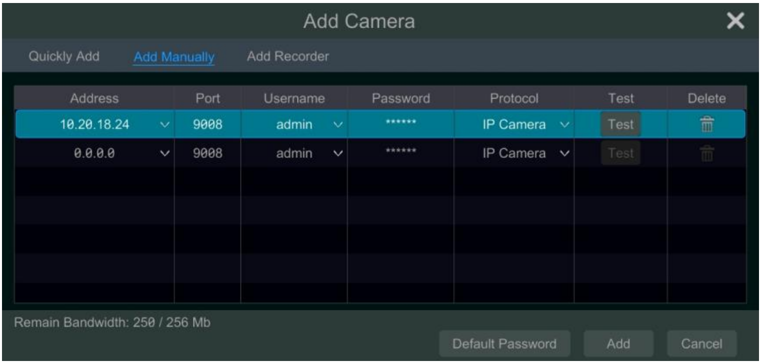
Selected: 0 / 2

Remain Bandwidth: 63 / 80 Mb

- **Quickly Add**

Check the cameras and then click "Add" to add cameras. Click ✎ to edit the camera's IP address, username and password and so on. Click "Refresh" to refresh the device list. Click "Default Password" to set the default username and password of each camera.

If the activation state is "Unactivated", you can check the device and click "Activate" to activate it.



Add Camera

Quickly Add | Add Manually | Add Recorder

Address	Port	Username	Password	Protocol	Test	Delete
10.20.18.24 ⌄	9008	admin ⌄	******	IP Camera ⌄	Test	🗑
0.0.0.0 ⌄	9008	admin ⌄	******	IP Camera ⌄	Test	🗑

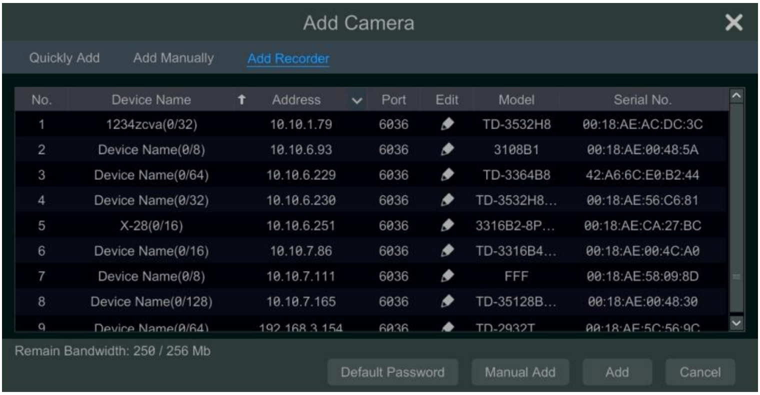
Remain Bandwidth: 250 / 256 Mb

➢ **Add Manually**

Enter the IPv4/IPv6 address or domain name (click ⌄ in the IP address column to open the IPv4/IPv6/domain name input window), port, username and password of the camera and then select the protocol. Click "Test" to test the accuracy of the input information and then click the "Add" button (you can input one camera's information or above such as IP address, username and password before clicking the "Add" button). Click 🗑 to delete the camera. Click "Default Password" to set the default username and password of each camera.

Note: Some models may not support this function.
Click ***Start→Settings→System→Basic→General Settings*** to check "Enable Add IPC by Zero Operation". If the NVR has unoccupied channels, it can add IPC without any operation by restarting.

➢ **Add Recorder**



Add Camera

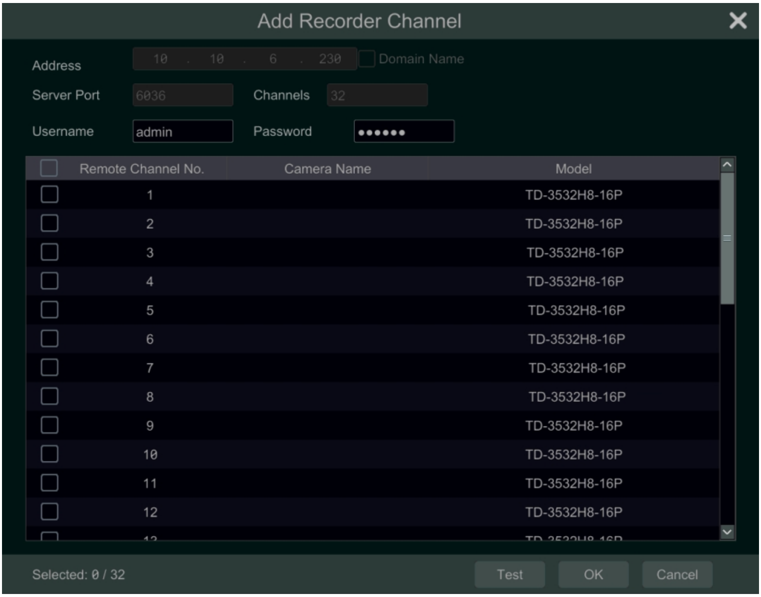
Quickly Add | Add Manually | Add Recorder

No.	Device Name	Address	Port	Edit	Model	Serial No.
1	1234zcva(0/32)	10.10.1.79	6036	✎	TD-3532H8	00:18:AE:AC:DC:3C
2	Device Name(0/8)	10.10.6.93	6036	✎	3108B1	00:18:AE:00:48:5A
3	Device Name(0/64)	10.10.6.229	6036	✎	TD-3364B8	42:A6:6C:E0:B2:44
4	Device Name(0/32)	10.10.6.230	6036	✎	TD-3532H8...	00:18:AE:56:C6:81
5	X-28(0/16)	10.10.6.251	6036	✎	3316B2-8P...	00:18:AE:CA:27:BC
6	Device Name(0/16)	10.10.7.86	6036	✎	TD-3316B4...	00:18:AE:00:4C:A0
7	Device Name(0/8)	10.10.7.111	6036	✎	FFF	00:18:AE:58:09:8D
8	Device Name(0/128)	10.10.7.165	6036	✎	TD-35128B...	00:18:AE:00:48:30
9	Device Name(0/64)	192.168.3.154	6036	✎	TD-2932T	00:18:AE:5C:56:9C

Remain Bandwidth: 250 / 256 Mb

- Quickly Add：Select the searched NVR/NVR and the click "Add" to add NVR in the same local network.

- Manually Add： Click “Manual Add” and then enter the IP address or domain name, port, username and password of the NVR/NVR. Check the added remote channel number and click “Test”. Then click “OK” to return to the previous interface.



Add Recorder Channel

Address 10 . 10 . 6 . 230 □ Domain Name

Server Port 6036 Channels 32

Username admin Password ••••••

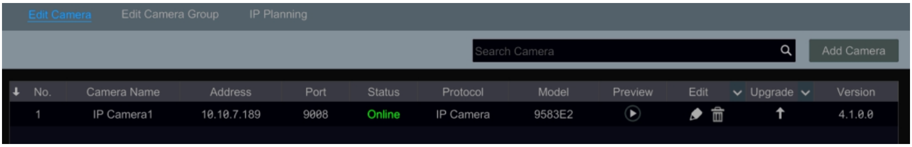
□ Remote Channel No.	Camera Name	Model
□ 1		TD-3532H8-16P
□ 2		TD-3532H8-16P
□ 3		TD-3532H8-16P
□ 4		TD-3532H8-16P
□ 5		TD-3532H8-16P
□ 6		TD-3532H8-16P
□ 7		TD-3532H8-16P
□ 8		TD-3532H8-16P
□ 9		TD-3532H8-16P
□ 10		TD-3532H8-16P
□ 11		TD-3532H8-16P
□ 12		TD-3532H8-16P
□ 13		TD-3532H8-16P

Selected: 0 / 32

Note: IPC from other NVR/DVR on the same local network can only be added if your NVR has open channels and the added IPCs support previewing and recording.

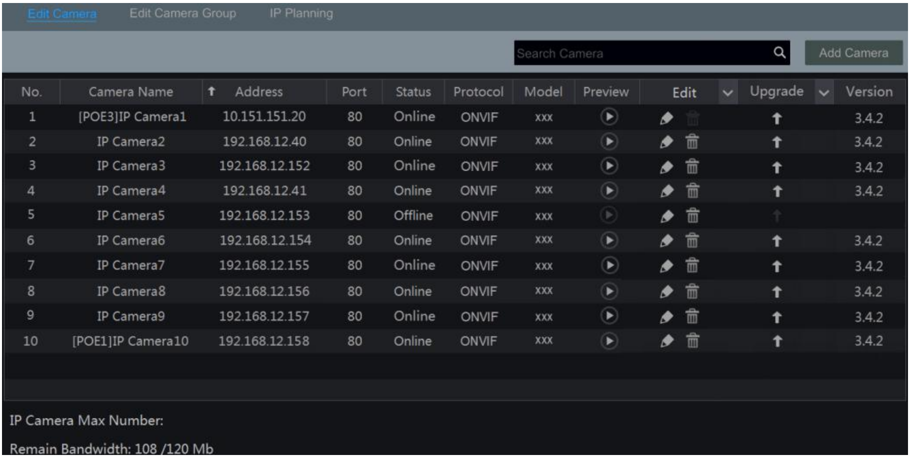
4.1.2 Edit Camera

Click “Edit Camera” in the setup panel to go to the interface as shown below. Click ▶ to view the live image of the camera in the popup window. Click ✎ to edit the camera (see ***Add camera*** in Startup Wizard for details). Click 🗑 to delete the camera. Click ∨ in the “Edit” header line and then click “Modify IPC Password” to open a window(check the IPCs in the window, set the new password and then click “OK”; only the online IPCs’ passwords can be modified and a batch of IPCs’ passwords can be modified at the same time). Click ⬆ to upgrade an online IPC (or click ∨ in the “Upgrade” header line and then click “IPC Batch Upgrade” to upgrade a batch of IPCs), select the device which stores the upgrade file in the “Device Name” item of the popup window and the upgrade file in the list(you should select the upgrade IPC model in the window if a batch of IPCs’ passwords need to be modified) and then click “Upgrade” to start upgrading(the IPC will restart automatically after the upgrade is completed successfully).



No.	Camera Name	Address	Port	Status	Protocol	Model	Preview	Edit	Upgrade	Version
1	IP Camera1	10.10.7.189	9008	Online	IP Camera	9583E2	▶	✎ 🗑	↑	4.1.0.0

Note:
If you use the NVR with the PoE network ports, the IP cameras (with PoE function) which are directly connected to the PoE port of the NVR will be displayed automatically in the camera list. Refer to the picture below. The PoE camera directly connected to the PoE port has a prefix shown before its camera name. The prefix consists of PoE plus PoE port number. A PoE camera directly connected to the PoE port cannot be deleted from the camera list manually.



No.	Camera Name	Address	Port	Status	Protocol	Model	Preview	Edit	Upgrade	Version
1	[POE3]IP Camera1	10.151.151.20	80	Online	ONVIF	xxx	▶	✎ 🗑	↑	3.4.2
2	IP Camera2	192.168.12.40	80	Online	ONVIF	xxx	▶	✎ 🗑	↑	3.4.2
3	IP Camera3	192.168.12.152	80	Online	ONVIF	xxx	▶	✎ 🗑	↑	3.4.2
4	IP Camera4	192.168.12.41	80	Online	ONVIF	xxx	▶	✎ 🗑	↑	3.4.2
5	IP Camera5	192.168.12.153	80	Offline	ONVIF	xxx	▶	✎ 🗑	↑	
6	IP Camera6	192.168.12.154	80	Online	ONVIF	xxx	▶	✎ 🗑	↑	3.4.2
7	IP Camera7	192.168.12.155	80	Online	ONVIF	xxx	▶	✎ 🗑	↑	3.4.2
8	IP Camera8	192.168.12.156	80	Online	ONVIF	xxx	▶	✎ 🗑	↑	3.4.2
9	IP Camera9	192.168.12.157	80	Online	ONVIF	xxx	▶	✎ 🗑	↑	3.4.2
10	[POE1]IP Camera10	192.168.12.158	80	Online	ONVIF	xxx	▶	✎ 🗑	↑	3.4.2

IP Camera Max Number:

Remain Bandwidth: 108 /120 Mb

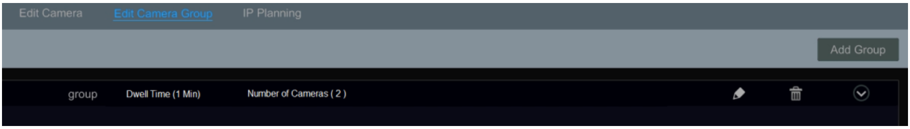
- An IP camera directly connected to the PoE port of the NVR through private protocol will be shown automatically in the camera list.
- One of the two conditions must be met if an IP camera directly connected to the PoE port of the NVR through ONVIF protocol to be shown automatically in the camera list.
  - ✓ The IP camera which is directly connected to the PoE port is in the same network segment with the internal Ethernet port.
  - ✓ The DHCP (obtain an IP address automatically) of the IP camera which is directly connected to the PoE port is enabled.

If the IP camera which is connected to the PoE port cannot be displayed automatically in the camera list, please refer to Q6 in Appendix A FAQ for details.

4.2 Add/Edit Camera Group

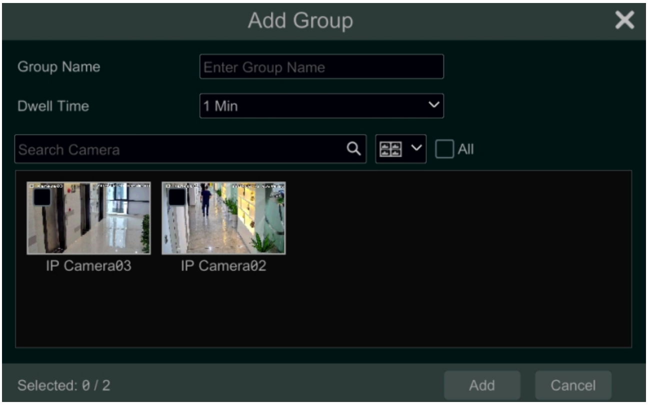
4.2.1 Add Camera Group

Click “Edit Camera Group” in the above interface to go to the interface as shown below.



group Dwell Time (1 Min) Number of Cameras (2)

Click “Add Group” to open the window as shown below. Set the group name and dwell time (the dwell time of the camera group sequence view) in the window. Check the cameras and then click “Add” to add group. Click to view the cameras in the group after adding group.

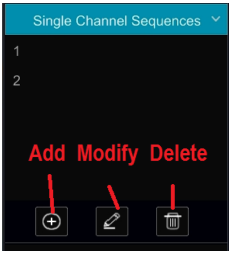


Group Name: Enter Group Name

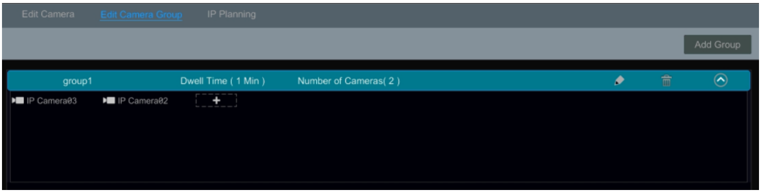
Dwell Time: 1 Min

Selected: 0 / 2

You can also add the camera group in the live view interface. Click on the top right corner of the live view interface and then select “Single Channel Sequences”. Click to add the camera group



4.2.2 Edit Camera Group



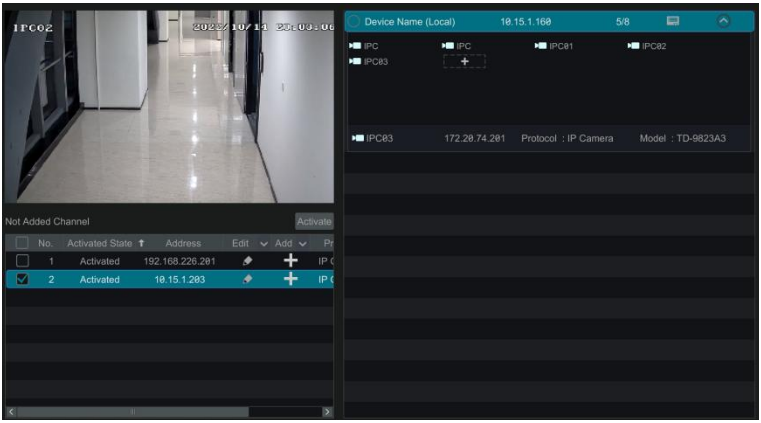
Click ✎ to modify the group information such as group name and dwell time. Click 🗑 to delete the group. Click + to add cameras to the group.

4.2.3 IP Planning

Some models may not support this function.

Click “IP Planning” to go to the interface as shown below. This function supports searching other NVRs/DVRs that is in the same local network as the local NVR. You may add the IPC of other NVRs/DVRs into the unoccupied channels of the local NVR.

For the searched channel, if its state is “unactivated”, you can activate it first and then add it.



IPC03 172.20.74.201 Protocol : IP Camera Model : TD-9823A3

□	No.	Activated State	Address	Edit	Add	Pr
□	1	Activated	192.168.226.201	✎	+	IP
☑	2	Activated	10.15.1.203	✎	+	IP

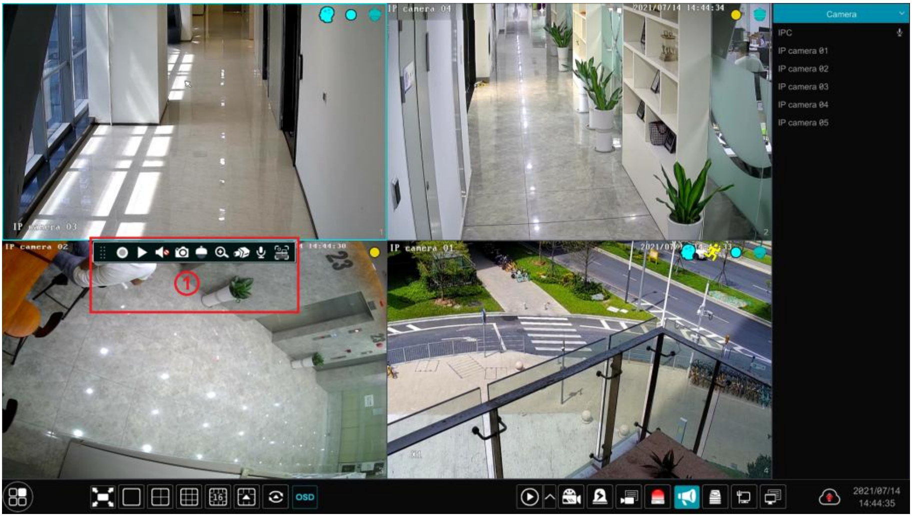
Click 🖥 to edit the IP address, user name or password and other information of the NVRs.

Click ⌄ behind the “Add” button to add the IPC selected and the user may edit the IP address, user name or password by clicking ⌄ behind the “Edit” button.

5 Live View Introduction

5.1 Live View Interface Introduction

You should add a camera when first logging on to the system (see Add Camera for details). Refer to the interface as shown below and drag one camera in the preview window to another window to exchange windows. Click OSD button and then you can view the record symbols. The record symbols with different colors in the live view window refer to different record types when recording: green stands for manual record, red stands for sensor based record, yellow stands for motion-based record, blue stands for schedule record and cyan stands for intelligent record, sky-blue stands for AI record.

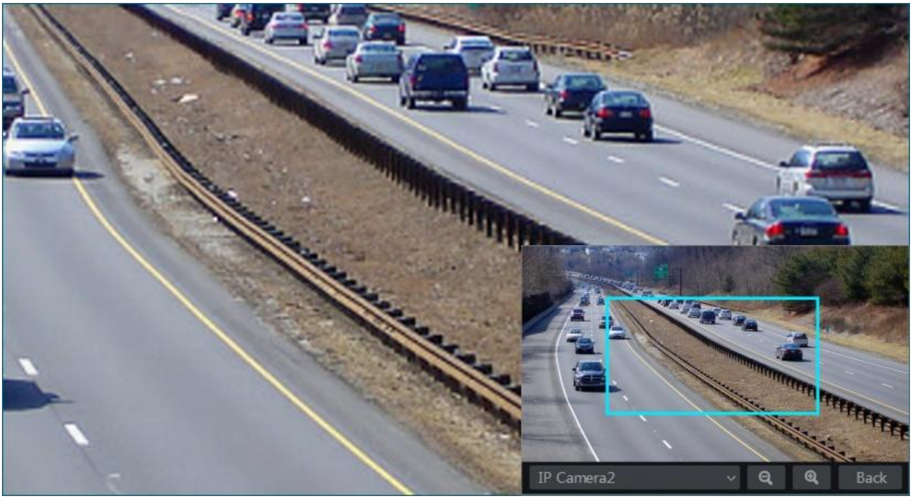


Click the preview window to show the tool bar as shown in area ①; right click the preview window to show the menu list. The tool bar and menu list are introduced in the table below.

Button	Menu List	Meaning
⋮⋮	--	Move tool. Click to move the tool bar anywhere.
◉	**Manually Record On**	Click to start recording.
▶	**Instant Playback**	Click ▶ to playback the record; click “Instant Playback” to select or self-define the instant playback time. See Instant Playback for details.
🔇	**Enable Audio**	Click to enable audio. You can listen to the camera audio by enabling audio.
--	**Original Proportions/ Overspread window**	Click to select the display proportion of the window.

Button	Menu List	Meaning
📷	**Snapshot**	Click to pop up the snap window. Click “Save” in the window to save the image. Click “Export” to export the image.
◒	**PTZ Control**	Click to go to PTZ control interface. See PTZ for details.
🔍	**Zoom In**	Click to go to single channel amplification interface.
▶	--	Click to go to image adjustment interface. Refer to Image Adjustment for details.
🎤	**Start/Close Talk**	Click to start talk.
⛶	**Target detection**	Click to go to single channel target detection interface; the target includes faces, human bodies and vehicles. (**only some models support**)
--	**Camera Info**	Click to view the camera information.

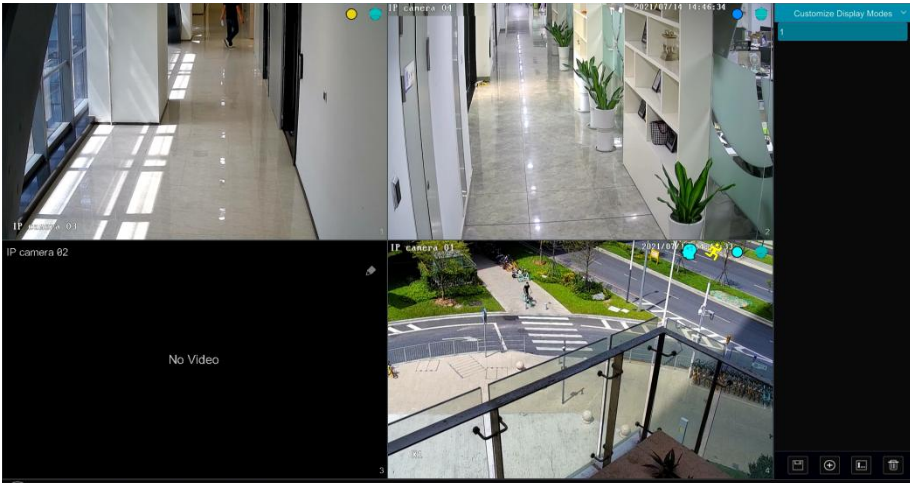
The single channel zoom amplification interface is as shown below. Press and drag the blue box to select the area to zoom in. Click 🔍 / 🔍 to zoom the image. Click the camera selection box to select other cameras for amplification. Click “Back” to return to the live view interface.



5.2 View Mode

5.2.1 Preview by Display Mode

Set different screen modes and camera display sequences as needed and then save the display modes classified by surveillance areas, priorities and so on. Refer to the picture below. Double click one display mode in the display mode list to view the live images in this mode.



➢ Add Display Mode

Method One:

① Click "Customize Display Modes" in the above interface

② Click ⊕ to add a display mode name and then set the screen mode.

③ Add the cameras and adjust the cameras' display sequence as required.

④ Click 💾 under the display mode list.

Method Two:

① Click ***Start→Settings→System→Basic→Output Settings*** to go to the interface and then set the screen mode.

② Double click the camera or camera group in the list to add them to the selected window.

③ Click ★ to save the current display mode (refer to Scheme View In Sequence for detail configurations). The display mode will be saved and displayed in the display mode list in the live view interface.

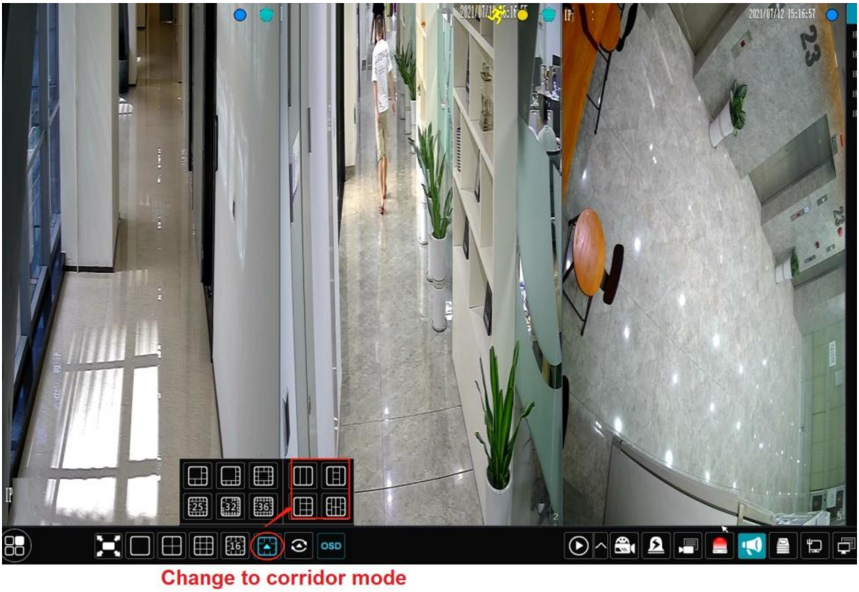
➢ Edit Display Mode

Click "Customize Display Modes" tab in the live view interface and then select one display mode in the list. Click ✎ to edit the display mode name; click 🗑 to delete the display mode.

➢ Corridor Pattern

Some models may not support this function.

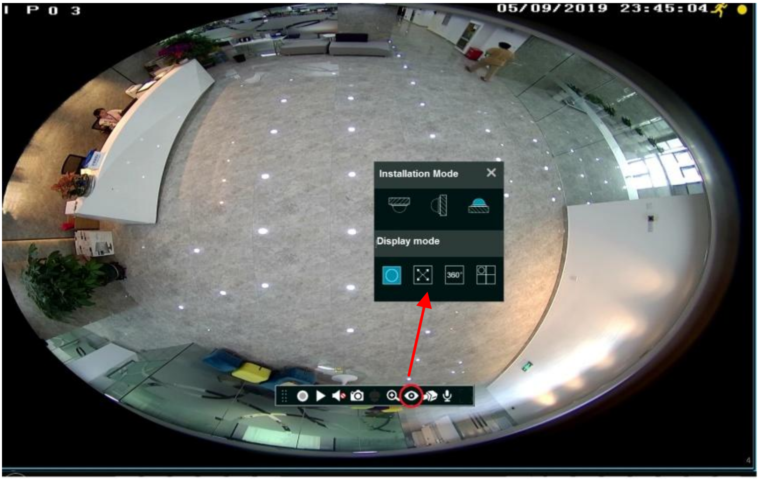
Select corridor pattern in display mode. You can change the direction of the video image by using this function. Please refer to User Manual of relevant camera.



- **Fisheye Mode**

Some models may not support this function.

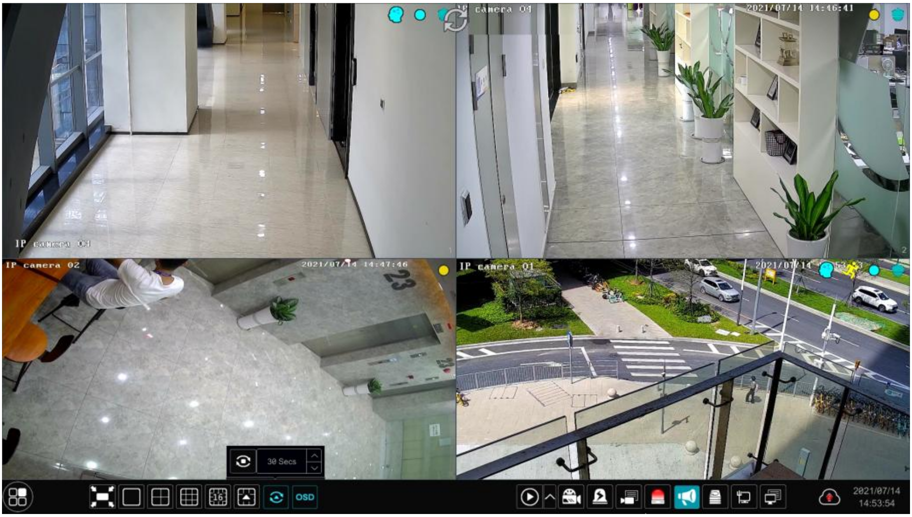
In the live view interface, select the view mode according to the installation mode and display mode of the fisheye camera. Please refer to User Manual of the relevant fisheye camera.



In addition, if this function is unavailable in the device, you can set the display mode and the installation mode via Web Client. To log in the web client, please refer to Remote Surveillance for details.

5.2.2 Quick Sequence View

You can start quick sequence view if the scheme has not been created. If the scheme has been created, please refer to Scheme View in Sequence for details.

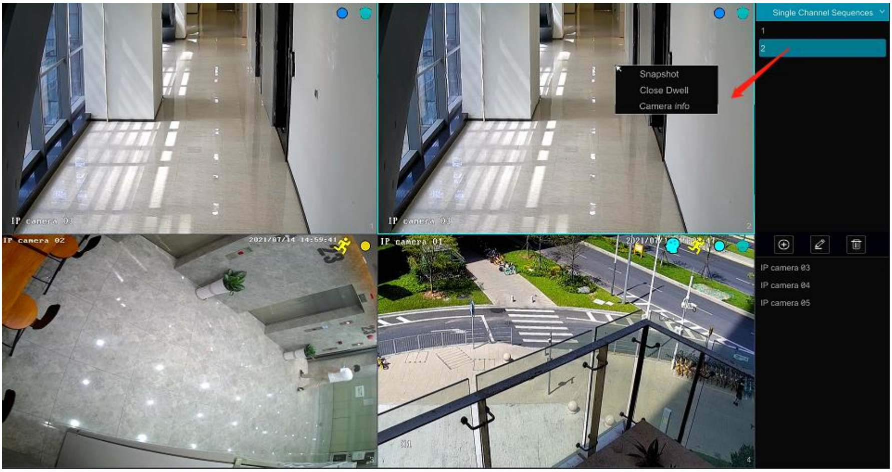


Go to the live view interface and then click ⟳ to open a small window. Set the dwell time in the window and then click ⟳ to view the live group by group according to the camera number of the current screen mode. Double click the sequence view interface to pause the view; double click again to restore the view. Click ⟳ to stop the view.

5.2.3 Camera Group View in Sequence

You can start camera group view in sequence if camera group has been created (see Add Camera Group for details).

① Go to the live view interface and then select a camera window.



② Double click one camera group on the right side of the interface. The cameras in the group will start camera group view one by one in the selected camera window.

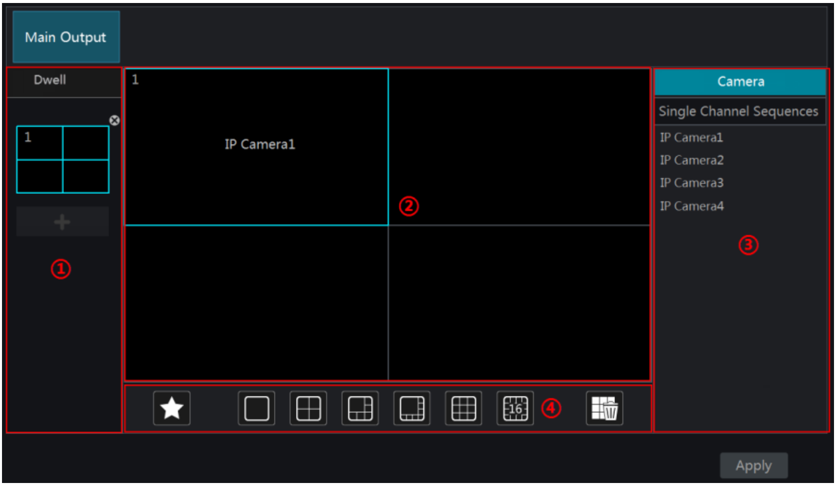
You can also drag the group directly to any preview window. Right click on the group view window and then click “Close Dwell” to stop the view.

Click ⊕ to add camera group. Select a group and click ✎ to modify the group name and dwell time; Select a group and click 🗑 to delete the group.

5.2.4 Scheme View in Sequence

Click ***Start→Settings→System→Basic→Output Settings*** to go to the interface as shown below.

Area ① displays all the dwell schemes; area ② shows the detailed information of the scheme; area ③ displays all the cameras and groups; area ④ is the tool bar (🗑: clear button; ★: favorite button, click to open a window, enter the display mode name in the window and then click “OK” to save the current display mode; other buttons are screen mode buttons).



➢ Add Scheme

Click in area ① to create a new scheme. Click on the top right corner of the scheme to delete it.

➢ Configure Scheme

a) Select a scheme in area ① and then click the screen mode button on the tool bar to set the screen mode of the scheme.

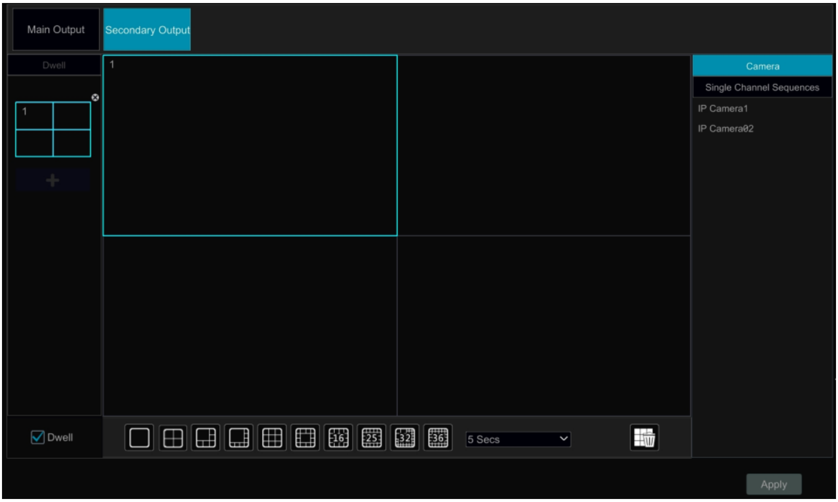
b) Select a camera window in area ② and then double click the camera or group in area ③. The camera or group will be added into the selected window. You cannot repeat a camera in the same scheme. You can click the right-click menu "Clear" in area ② to remove a single camera or click to remove all the cameras.

c) Click "Apply" to save the settings.

➢ Start Sequence View

Go to the live view interface and then click to open a window. Set the dwell time in the window and then click to start scheme view in sequence. Double click the sequence view interface to pause the view; double click again to restore the view. Click to stop the view.

Note:
You can set the secondary output preview if the NVR has dual outputs. Refer to the interface as shown below.



Check "Dwell" and then set scheme view in sequence of the adjuvant output. The setting steps are similar to that of the main output.

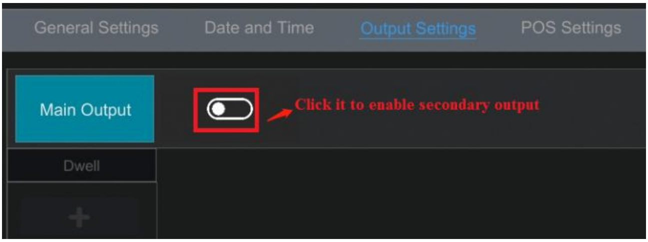
Set quick sequence view if "Dwell" is not checked. The setting steps are as follows:

① Set screen mode by clicking the relevant buttons on the tool bar.

② Select one window and then double click one camera or group in the list.

③ Click "Apply" to save the settings after adding cameras or groups to the windows.

For the device with multi-output mode and AI mode, the secondary output will be unavailable after AI mode is enabled. If you want to enable secondary output, please click Start→System→Output Settings.



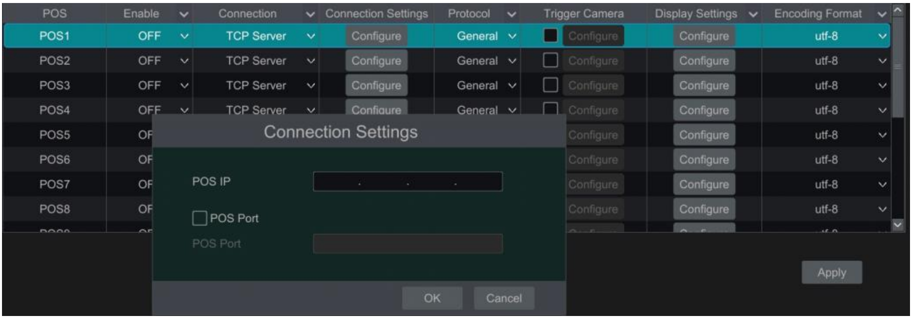
5.3 POS Settings

① Click ***Start→Settings→Basic→POS Settings*** to go to the interface.

② Enable POS and click "Configure" under "Connection Settings" to go to the following interface. The connection way includes TCP Server, TCP Client, UDP and Multicast.

③ Enter IP address of the POS you want to add.

④ Check "POS port" and then enter POS port.



POS	Enable	Connection	Connection Settings	Protocol	Trigger Camera	Display Settings	Encoding Format
POS1	OFF	TCP Server	Configure	General	■ Configure	Configure	utf-8
POS2	OFF	TCP Server	Configure	General	□ Configure	Configure	utf-8
POS3	OFF	TCP Server	Configure	General	□ Configure	Configure	utf-8
POS4	OFF	TCP Server	Configure	General	□ Configure	Configure	utf-8
POS5	OF				Configure	Configure	utf-8
POS6	OF				Configure	Configure	utf-8
POS7	OF				Configure	Configure	utf-8
POS8	OF				Configure	Configure	utf-8

Connection Settings

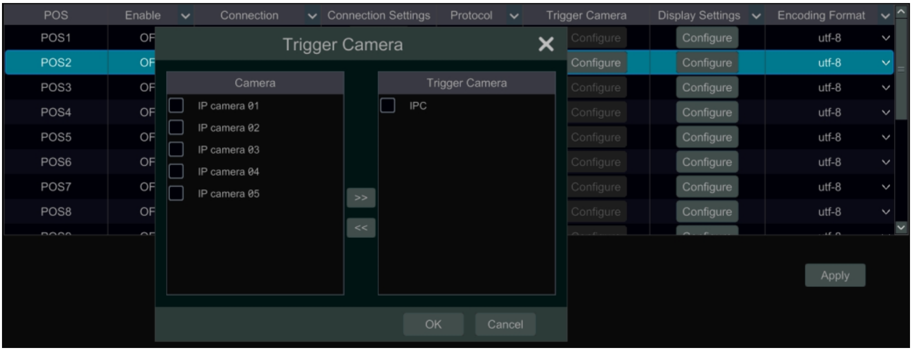
POS IP . . .

□ POS Port

POS Port

⑤ Select the POS protocol.

⑥ Check "Trigger Camera" and click "Configure" under it to bind POS to the camera. One POS can be bound to multiple channels, but one channel can only be bound to one POS.

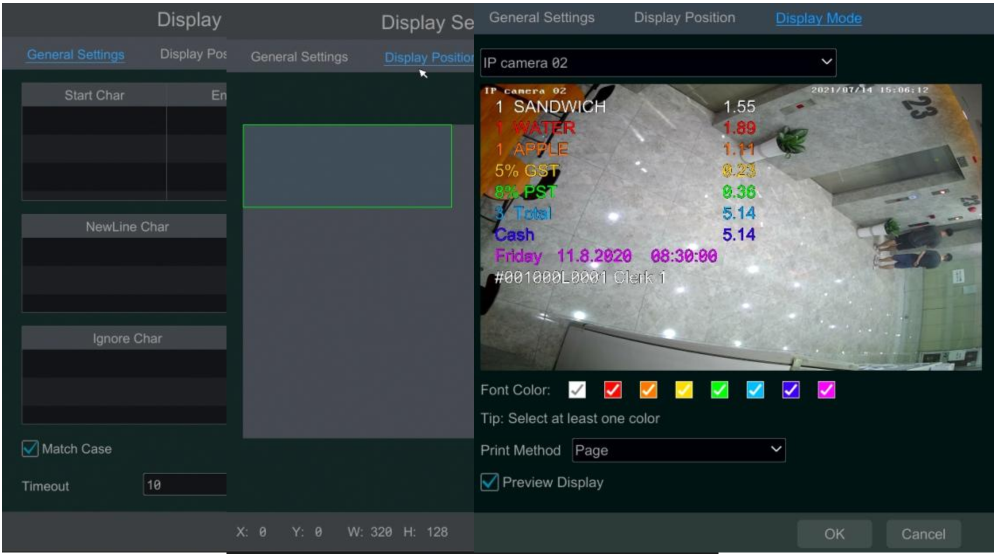


POS	Enable	Connection	Connection Settings	Protocol	Trigger Camera	Display Settings	Encoding Format
POS1	OF				Configure	Configure	utf-8
POS2	OF				Configure	Configure	utf-8
POS3	OF				Configure	Configure	utf-8
POS4	OF				Configure	Configure	utf-8
POS5	OF				Configure	Configure	utf-8
POS6	OF				Configure	Configure	utf-8
POS7	OF				Configure	Configure	utf-8
POS8	OF				Configure	Configure	utf-8

Trigger Camera

Camera	Trigger Camera
□ IP camera 01	□ IPC
□ IP camera 02	
□ IP camera 03	
□ IP camera 04	
□ IP camera 05	

⑦ Click "Configure" under "Display Settings" to set the general settings, the position and display color of the POS information. Set the start character and the end character and display time-out period in the general settings interface. Drag your mouse to set the position of the POS information in the display position interface. Then click "OK" to confirm your settings.



☑ Match Case

Timeout 10

X: 0 Y: 0 W: 320 H: 128

IP camera 02

Font Color: ☑ ☑ ☑ ☑ ☑ ☑ ☑ ☑

Tip: Select at least one color

Print Method Page

☑ Preview Display

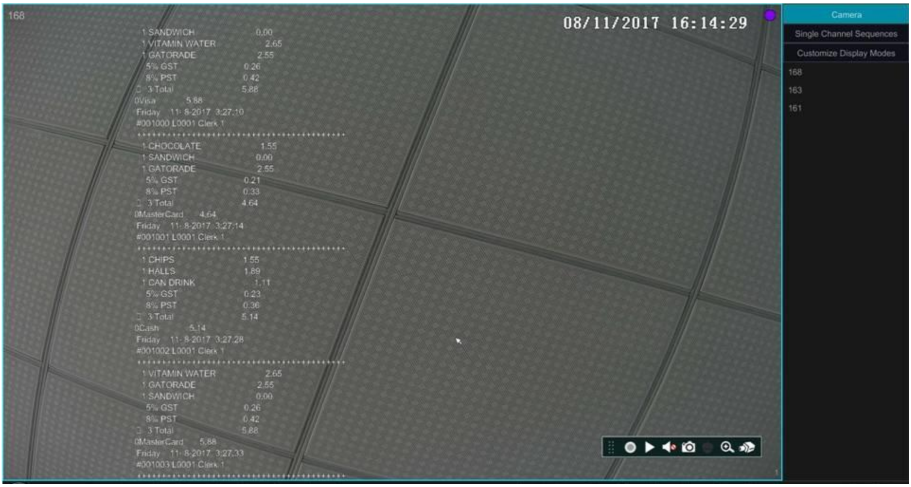
Click the "Display Color" tag and then choose the color you want to display on the screen. Multi-color can be selected at the same time. In addition, print method and preview display can be set here. If "Preview Display" is enabled, the POS contents can be displayed on the live view/playback interface.

⑧ Select the encoding format as needed.

⑨ Choose the manufacturer of the POS device.

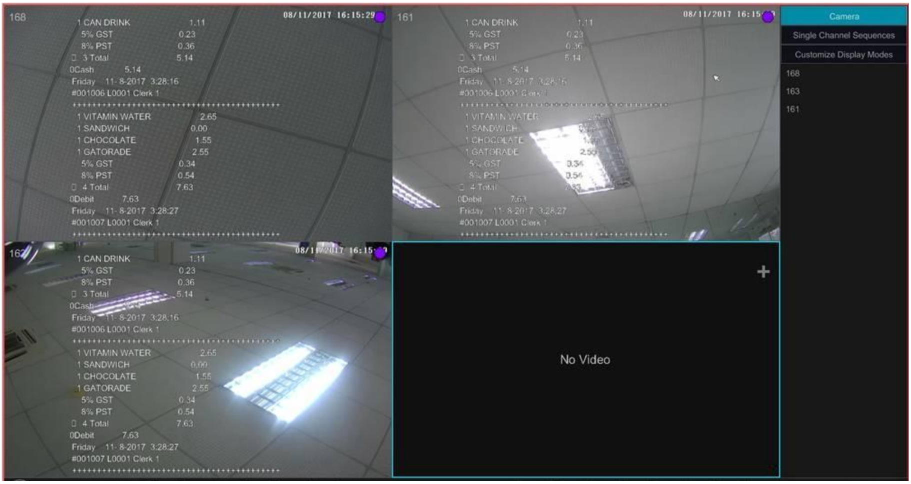
⑩ Click "Apply" to save the settings and then the transaction information will be displayed on the preview image in real-time.

One POS is bound to one camera:



```
 1 SANDWICH            0.00
 1 VITAMIN WATER          2.65
 1 GATORADE            2.55
  5% GST            0.26
  8% PST            0.42
 3 Total            5.88
0Visa        5.88
Friday   11-8-2017  3:27:10
#001000 L0001 Clerk 1
++++++++++++++++++++++++++++++++++++++++++++
 1 CHOCOLATE             1.55
 1 SANDWICH            0.00
 1 GATORADE            2.55
  5% GST            0.21
  8% PST            0.33
 3 Total            4.64
0MasterCard     4.64
Friday   11-8-2017  3:27:14
#001001 L0001 Clerk 1
++++++++++++++++++++++++++++++++++++++++++++
 1 CHIPS            1.55
 1 HALLS            1.89
 1 CAN DRINK            1.11
  5% GST            0.23
  8% PST            0.36
 3 Total            5.14
0Cash         5.14
Friday   11-8-2017  3:27:28
#001002 L0001 Clerk 1
++++++++++++++++++++++++++++++++++++++++++++
 1 VITAMIN WATER          2.65
 1 GATORADE            2.55
 1 SANDWICH            0.00
  5% GST            0.26
  8% PST            0.42
 3 Total            5.88
0MasterCard     5.88
Friday   11-8-2017  3:27:33
#001003 L0001 Clerk 1
++++++++++++++++++++++++++++++++++++++++++++
```

One POS is bound to multiple cameras:

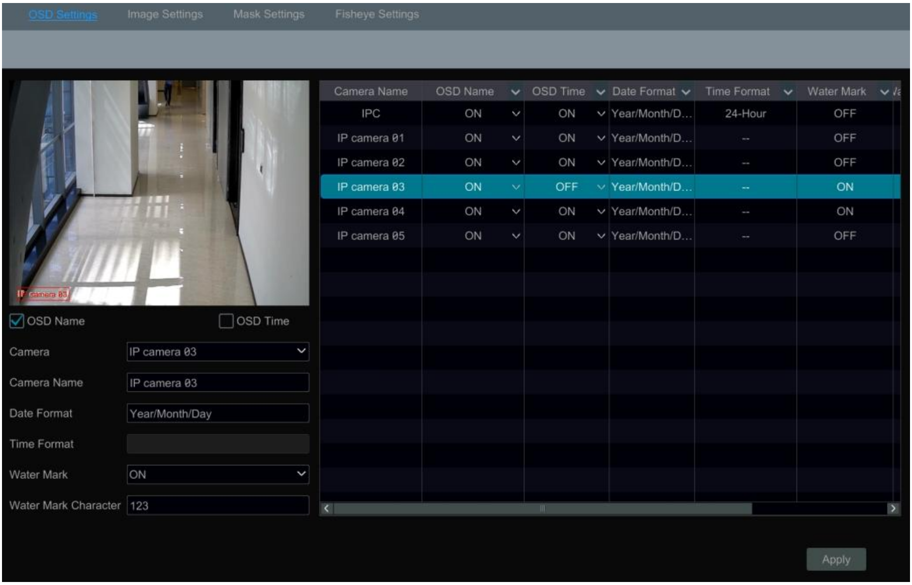


```
 1 CAN DRINK            1.11
  5% GST            0.23
  8% PST            0.36
 3 Total            5.14
0Cash         5.14
Friday   11-8-2017  3:28:16
#001006 L0001 Clerk 1
++++++++++++++++++++++++++++++++++++++++++++
 1 VITAMIN WATER          2.65
 1 SANDWICH            0.00
 1 CHOCOLATE            1.55
 1 GATORADE            2.55
  5% GST            0.34
  8% PST            0.54
 4 Total            7.63
0Debit        7.63
Friday   11-8-2017  3:28:27
#001007 L0001 Clerk 1
++++++++++++++++++++++++++++++++++++++++++++
```

5.4 Preview Image Configuration

5.4.1 OSD Settings

Click ***Start→Settings→Camera→Image→OSD Settings*** to go to the interface as shown below.



Camera Name	OSD Name	OSD Time	Date Format	Time Format	Water Mark
IPC	ON	ON	Year/Month/D...	24-Hour	OFF
IP camera 01	ON	ON	Year/Month/D...	--	OFF
IP camera 02	ON	ON	Year/Month/D...	--	OFF
IP camera 03	ON	OFF	Year/Month/D...	--	ON
IP camera 04	ON	ON	Year/Month/D...	--	ON
IP camera 05	ON	ON	Year/Month/D...	--	OFF

☑ OSD Name □ OSD Time

Camera: IP camera 03

Camera Name: IP camera 03

Date Format: Year/Month/Day

Time Format:

Water Mark: ON

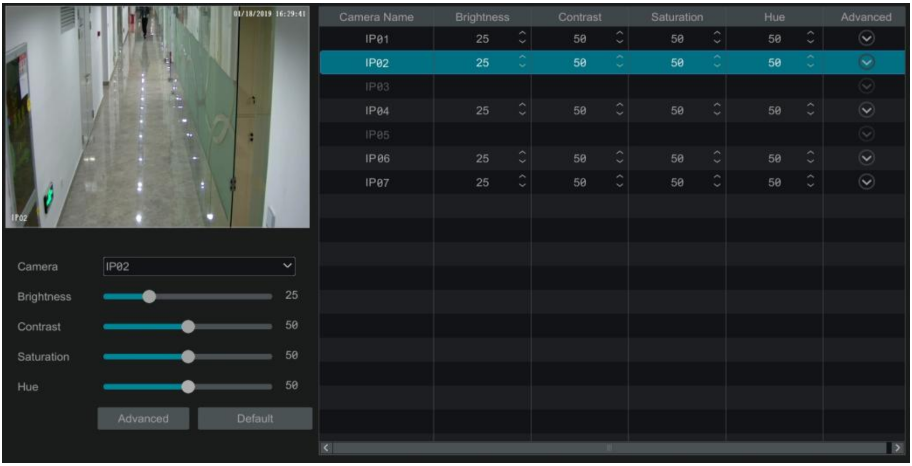
Water Mark Character: 123

Select the camera, enter the camera name (or double click the camera name in the camera list to change the camera name), enable or disable the name and time OSDs (if enabled, drag the red name and time OSDs directly in the image view area to change the OSDs' display position) and select the date and time format (24h or12h is optional). Additionally, water mark can be enabled or disabled here. Having enabled the water mark function, you can enter the information of the water mark as needed. Finally, click "Apply" to save the settings.

5.4.2 Image Settings

Click ***Start→Settings→Camera→Image→Image Settings*** to go to the following interface. Select the camera and then set the brightness, contrast, saturation and hue of the camera. Click the "Advanced" button or ⌄ in the camera list on the right side of the interface to open the "Image Adjust" interface and then set the relevant setting items. Please refer to Image Adjustment for detailed introductions of these items.

You can click "Default" to restore the image settings to the default factory settings.

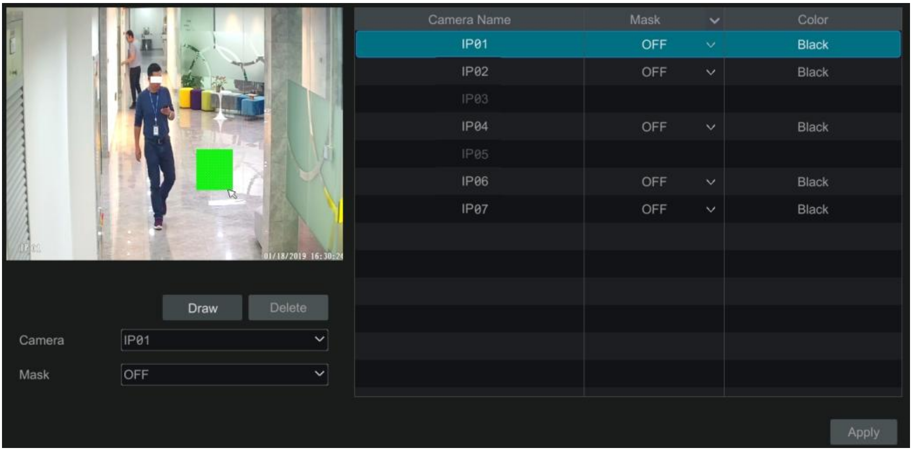


Camera Name	Brightness	Contrast	Saturation	Hue	Advanced
IP01	25	50	50	50	⌄
IP02	25	50	50	50	⌄
IP03					⌄
IP04	25	50	50	50	⌄
IP05					⌄
IP06	25	50	50	50	⌄
IP07	25	50	50	50	⌄

Camera IP02
Brightness 25
Contrast 50
Saturation 50
Hue 50

5.4.3 Mask Settings

Some areas of the image can be masked for privacy. Up to four mask areas can be set for each camera. Click ***Start→Settings→Camera→Image→Mask Settings*** to go to the interface as shown below.



Camera Name	Mask	Color
IP01	OFF	Black
IP02	OFF	Black
IP03		
IP04	OFF	Black
IP05		
IP06	OFF	Black
IP07	OFF	Black

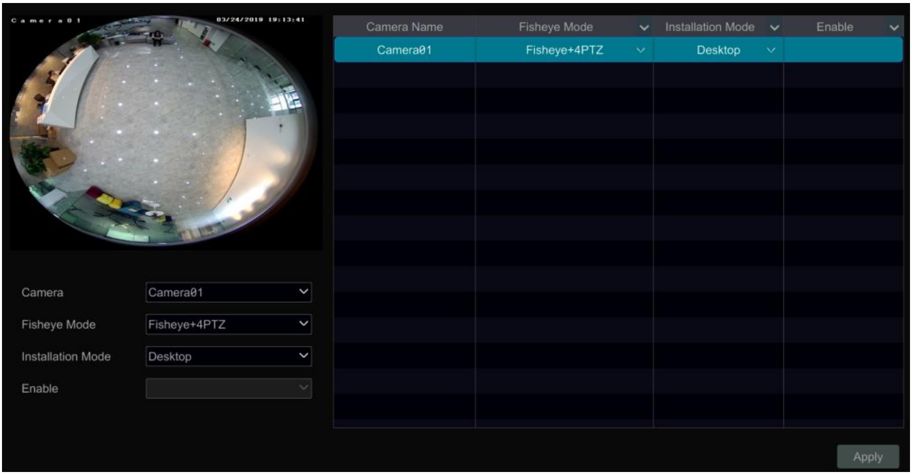
Camera IP01
Mask OFF

Select the camera and enable the mask. Click the "Draw" button and then drag the mouse on the image area to set the mask area; click the "Delete" button to delete the mask areas; click "Apply" to save the settings.

5.4.4 Fisheye Settings

Some models may not support this function.

Click ***Start→Settings→Camera→Image→Fisheye*** Settings to go to the interface as shown below. Select the camera and the mode of fisheye and installation.



Camera Name	Fisheye Mode	Installation Mode	Enable
Camera01	Fisheye+4PTZ	Desktop	

Camera: Camera01

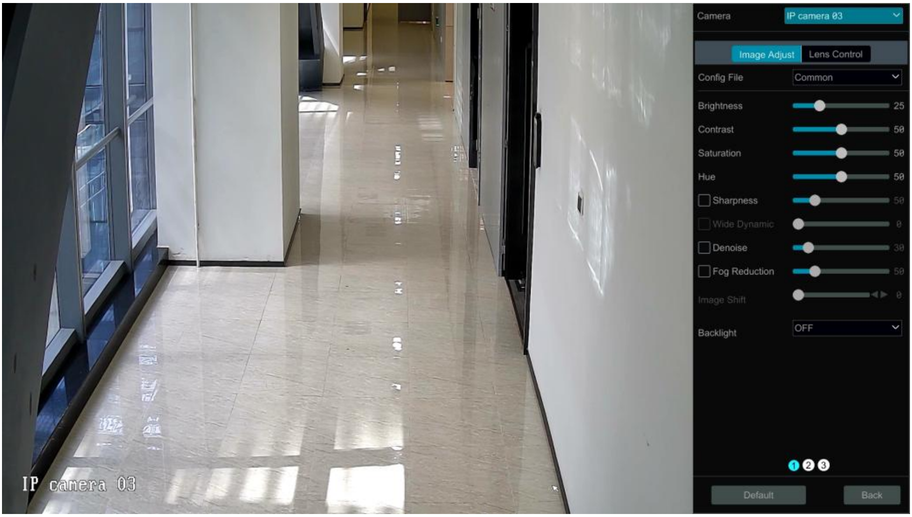
Fisheye Mode: Fisheye+4PTZ

Installation Mode: Desktop

Enable:

5.4.5 Image Adjustment

Go to the live view interface and then click button on the tool bar under the camera window to go to the image adjustment interface.



Camera: IP camera 03

Config File: Common

Brightness 25

Contrast 50

Saturation 50

Hue 50

□ Sharpness 50

□ Wide Dynamic 0

□ Denoise 30

□ Fog Reduction 50

Image Shift 0

Backlight: OFF

➢ **Image Adjustment**

Select the camera and then click “Image Adjustment” to go to image adjustment tab. Refer to the picture above. Drag the slider to set the camera’s brightness, contrast, saturation and hue value. Check sharpness, wide dynamic and denoise and then drag the slider to set the value.

Click “Default” button to set these parameters to default values.

Note: For some IPCs, if you have set HWDR in the NVR, these IPCs will automatically reboot after setting the following image parameters, including exposure/shutter mode, gain mode, gain, corridor pattern or smart IR. After these IPCs successfully reboot, HWDR will be disabled.

The introductions of these parameters are as follows:

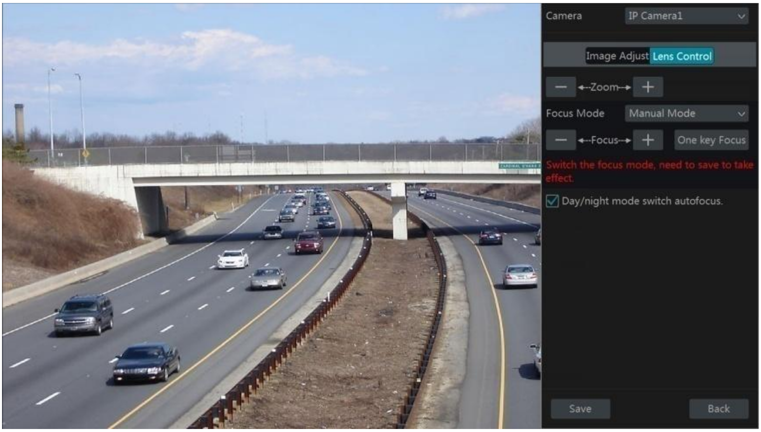
Parameter	Meaning
Brightness	The brightness level of the camera’s image.
Contrast	The color difference between the brightest and darkest parts.
Saturation	The degree of color purity. The image appears brighter the purer the color is.
Hue	Relates to the total color degree of the image.
Sharpness	Relates to the resolution level of the image plane and the sharpness level of the image edge.
Wide Dynamic	The wide dynamic range (WDR) function helps the camera provide clear images even under back light circumstances. When there are both very bright and very dark areas simultaneously in the field of view, WDR balances the brightness level of the whole image and provide clear images with details.
Denoise	Decrease the noise and make the image more thorough. Increasing the value will make the noise reduction effect better but it will reduce the image resolution.
White Balance	Adjust the color temperature according to the environment automatically.
BLC	HLC: lowers the brightness of the entire image by suppressing the brightness of the image’s bright area and reducing the size of the halo area. BLC: If enabled, the auto exposure will activate according to the scene so that the object of the image in the darkest area will be seen clearly.
Corridor Pattern	0 °, 90 °, 180 ° or 270 ° can be selected. (Only some cameras support this pattern)
Image Mirror	Turn the current video image horizontally.
Image Flip	Turn the current video image vertically.
High FPS Mode	High frame rate mode, if is it enabled, the frame rate of the camera’s main stream can be set to 1080P/720P @60fps/50fps. (Only some cameras support this mode)
Gain Mode	Choose “Auto” or “Manual”. If “Auto” is selected, the gain value will be automatically adjusted according to the actual situation. If “Manual” is selected, the gain value shall be set manually. The higher the value is, the brighter the image is.
Infrared Mode	Choose “Auto”, “On” or “Off” as needed.
Shutter Mode	Choose “Auto” or “Manual”. If manual is chosen, the digital shutter speed can be adjusted.
Day & Night Mode	Choose “Auto”, “Day”, “Night” or “Timing” as needed.
White Light Mode	“Auto”, “Manual” or “Off” can be selected. (Only some cameras support this mode).

Parameter	Meaning
EIS	Electronic image stabilization; increase the stability of video image by using jitter compensation technology (only some IPCs support this function)
Digital Zoom	Please select it as needed (only some PTZ cameras support this function)
Supplement Light Mode	Choose “White Light”, “Infrared Light” or “Smart Supplement Light” as needed (this function is only available for dual-illumination cameras)

Note: The above-mentioned descriptions of the image parameters are for reference only. The cameras made by different manufacturers may have different parameter settings.

➢ Lens Control

Select the camera and then click “Lens Control” to go to lens control tab. Click − or + to adjust the zoom and focus parameters of the camera’s lens. Click “Save” to save the settings.



Camera: IP Camera1

Focus Mode: Manual Mode

Switch the focus mode, need to save to take effect.

☑ Day/night mode switch autofocus.

The introductions of these parameters and buttons are as follows.

Button/Parameter	Meaning
− ←Zoom→ +	Click + / − to zoom in/out the image.
Focus Mode	If manual mode is selected, focus button & “One Key Focus” & “Day/night mode switch autofocus” will be available; if auto mode is selected, the time interval setup will be available.
− ←Focus→ +	Click + / − to increase/decrease the focal length.
One key Focus	Click to focus instantly.
Day/night mode switch autofocus	If checked, the lens will focus automatically when the camera is switching day/night mode.

Button/Parameter	Meaning
Time Interval	It is the time interval when camera lens is auto focusing. The interval can be set in the drop-down list.

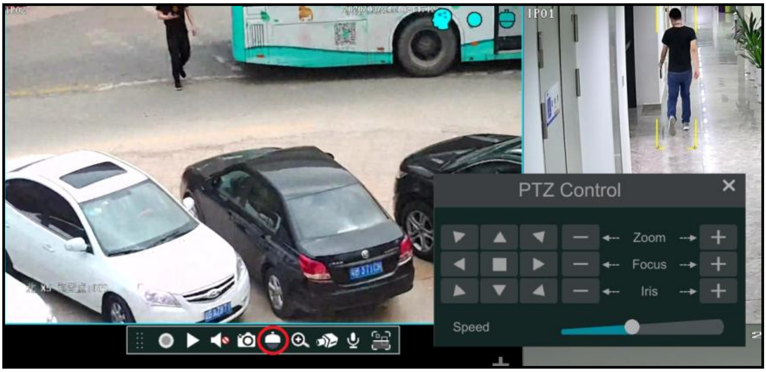
Note: This function is only available for motorized zoom cameras.

6 PTZ

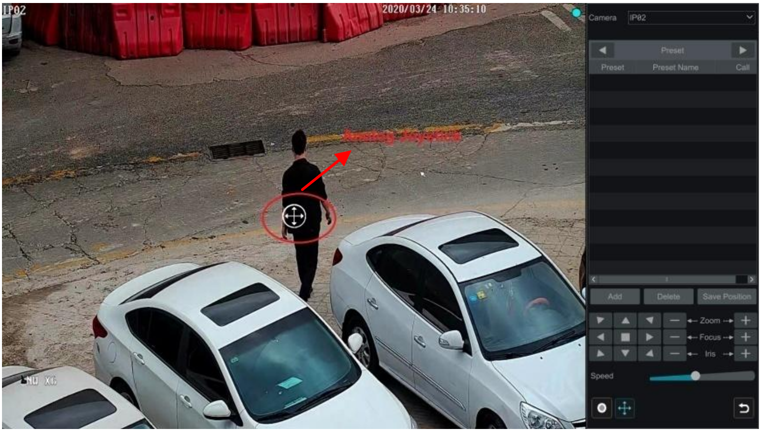
6.1 PTZ Control Interface Introduction

You can control the IP dome or PTZ connected to the IP camera for PTZ control.

Click on the tool bar at the bottom of the live preview window to go to the PTZ control interface as shown below.



The direction, zoom, focus, iris and speed can be controlled in the small PTZ control window. Right click the PTZ/speed dome camera window and select "PTZ Control" to go to the PTZ control panel as shown below.



Introductions of the buttons on the bottom right of the interface:

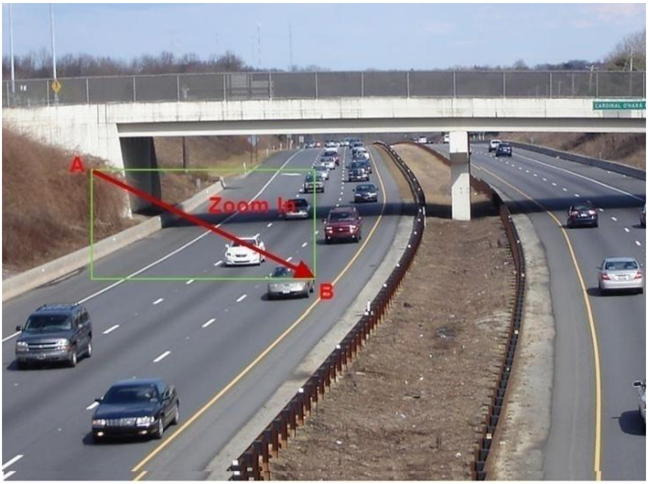
Button	Meaning
◤ ▲ ◥ ◀ ■ ▶ ◣ ▼ ◢	Click ▲ / ◤ / ◥ / ▼ / ◣ / ◢ / ◀ / ▶ to rotate the dome. Click ■ to stop rotating the dome.
— ←-Zoom-→ +	Click + / — to zoom in / out the camera image.
— ←-Focus-→ +	Click + / — to increase / decrease the focal length.
— ←-- Iris --→ +	Click + / — to increase / decrease the iris of the dome.
	Drag the slider to adjust the rotating speed of the dome.
⚪ / 🔴	Click ⚪ / 🔴 to start / stop recording.
✥ / ✥	Click ✥ / ✥ to hide / show the analog joystick.
↺	Click to return to the live view interface.

➢ Analog Joystick Control

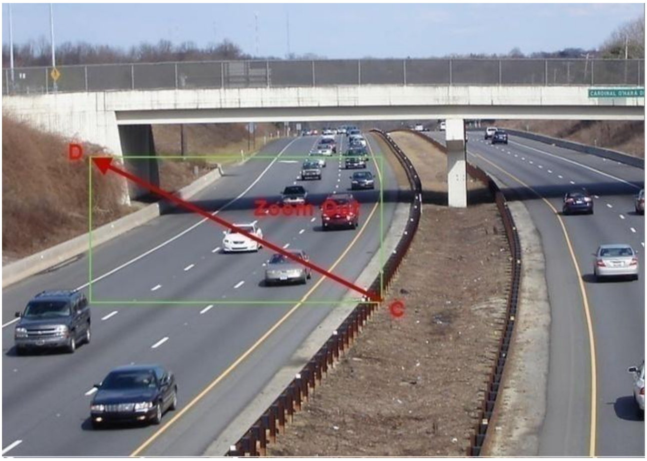
The analog joystick on the left side of the interface provides quick PTZ control. The dome or PTZ will rotate when you drag the analog joystick. The farther you drag the analog joystick from the middle of the image, the faster the dome or PTZ rotates. The dome or PTZ will stop rotating when you stop dragging the analog joystick.

➢ 3D Control

Click the camera image on any area and then the image will be centered on the clicked point. Refer to the picture as shown below. Drag the mouse from A to B to get a green rectangle and the rectangle area will be zoomed in.



Refer to the picture as shown below. Drag the mouse from C to D to get a green rectangle and the rectangle area will be zoomed out.



- **Advanced 3D Control**

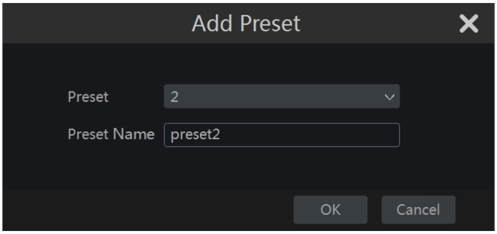
Double click the left button of the mouse on any area of the camera image and then the image size will be doubled and centered on the clicked point.

Press and hold the left button of the mouse on any area of the camera image to zoom in the image; press and hold the right button to zoom out the image.

Move the cursor of the mouse to the camera image and then slide the scroll wheel of the mouse forward to zoom in the image, slide the scroll wheel of the mouse backward to zoom out the image.

➢ Preset Settings

Click “Preset” to go to preset operation tab and then click “Add” to open the window as shown below. Select the preset and then enter the preset name in the window; finally click “OK” to save the settings. You can add up to 255 presets for each dome.



Add Preset

Preset: 2

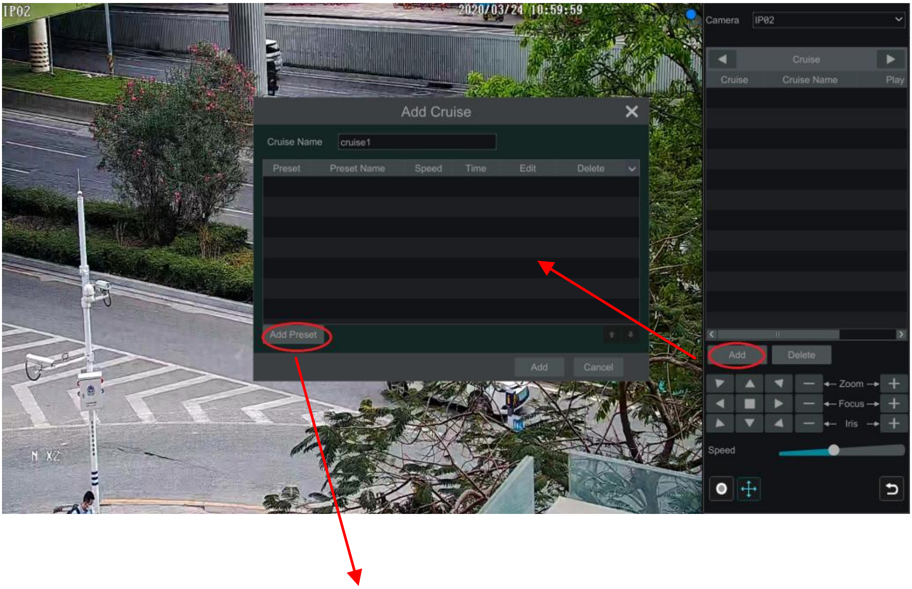
Preset Name: preset2

Adjust the dome’s direction and then click “Save Position” to save the current preset position (you can also click another preset in the preset list and then save the preset position after adjusting the dome’s direction); click ↗ in the preset list to call the preset; click “Delete” to delete the selected preset.

You can also go to preset setting interface for preset setting, see Preset Setting for details.

➢ Cruise Settings

On the right panel, click ▶ to go to cruise operation tab and then click “Add” to open the window as shown below. You can add up to 8 cruises for each dome.



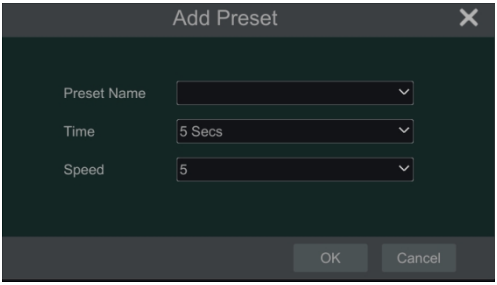
Add Cruise

Cruise Name: cruise1

Preset	Preset Name	Speed	Time	Edit	Delete

Camera: IP02

Cruise	Cruise Name	Play



Add Preset

Preset Name

Time: 5 Secs

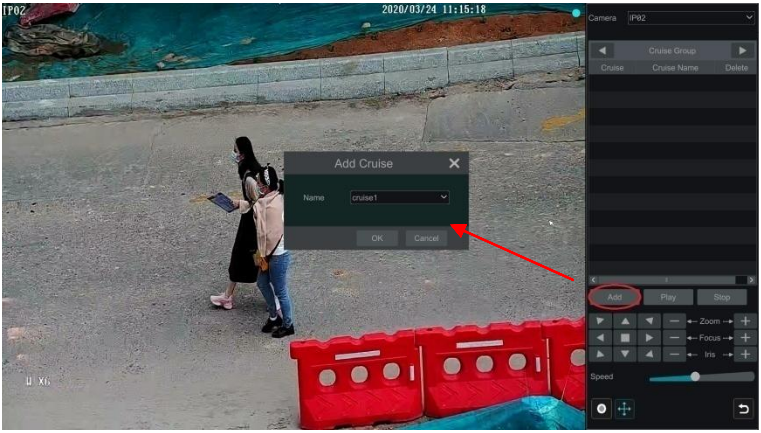
Speed: 5

① Enter the cruise name in the “Add Cruise” window and then click “Add preset” to open the “Add Preset” window (Before adding preset to the cruise, please add preset of the dome first).
② In the “Add Preset” window, select the preset name, preset time and preset speed and then click “OK”.
③ In the “Add Cruise” window, you can click ✎ to reselect the preset, then change the preset time and speed. Click 🗑 to delete the preset. Click “Add” to save the cruise.

Click ▶ to start the cruise and click ⏹ to stop the cruise in the cruise list of the cruise operation tab; click “Delete” to delete the selected cruise.
You can also go to cruise setting interface for cruise setting, see Cruise Setting for details.

➢ **Cruise Group Settings**

On the right panel, click ▶ to go to the cruise group setting tab. Click “Add” to add a cruise group as shown below.



IP02 2020/03/24 11:15:18

Camera: IP02

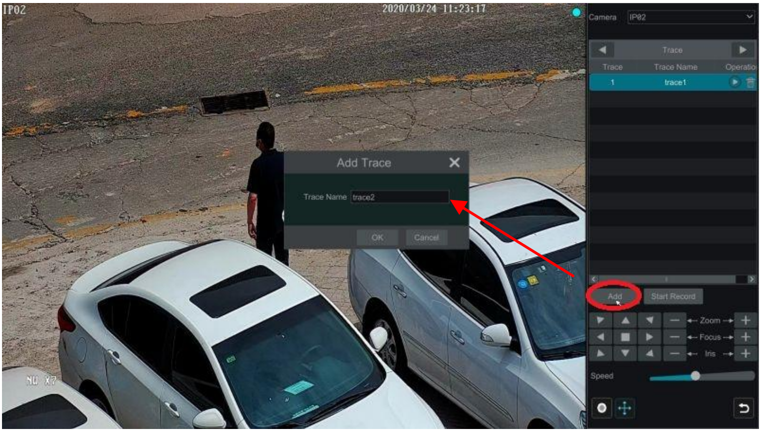
Add Cruise

Name: cruise1

In the “Add Cruise” window, select the cruise group name. After that, click “Play” to play the cruise groups in sequence.

➢ Trace Settings

On the right panel, click ▶ to go to the trace setting tab. Click "Add" to add the trace name. Then click "OK" to save this name. Please refer to the following picture.



Camera: IP02

Trace	Trace Name	Operation
1	trace1	

Add Trace

Trace Name: trace2

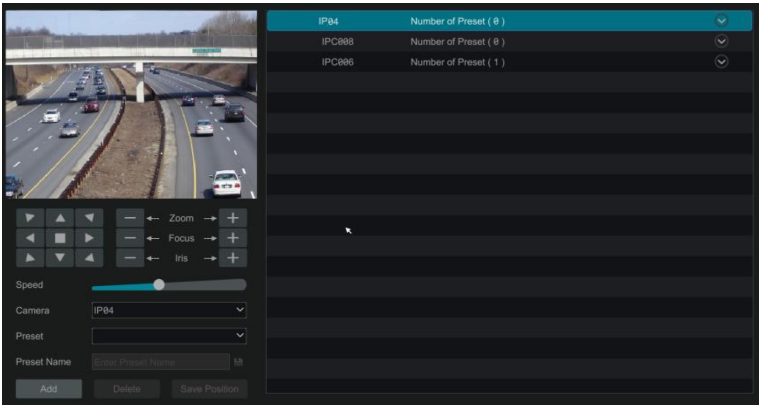
OK Cancel

Add Start Record

After that, click "Start Record" to record the trace. Then click "Stop Record" to finish recording. Click ⏵ to play the recorded trace. Click 🗑 to delete the trace.

6.2 Preset Settings

Click ***Start→Settings→Camera→PTZ→Preset*** to go to the interface as shown below.



IP04	Number of Preset (0)
IPC008	Number of Preset (0)
IPC006	Number of Preset (1)

Camera: IP04

Preset:

Preset Name: Enter Preset Name

Add Delete Save Position

➢ Add preset

Select camera and then click "Add" to add preset; or click ⌄ in the camera list on the right side of the interface to display the preset information of the dome and then click + to add preset. The operations of the "Add Preset" window are similar to that of the PTZ control interface; please see PTZ Control Interface Introduction for details.

- **Edit preset**

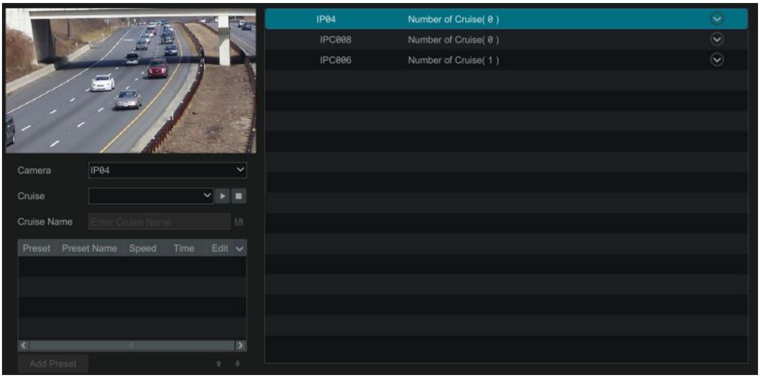
Select camera and preset. You can enter the new name of the preset and then click 💾 to save the new preset name. Adjust the rotating speed, position, zoom, focus and iris of the preset and then click "Save Position" to save the preset.

- **Delete Preset**

Select camera and preset and then click "Delete" to delete the preset.

6.3 Cruise Settings

Click ***Start→Settings→Camera→PTZ→Cruise*** to go to the interface as shown below.



IP04	Number of Cruise(0)	⌄
IPC008	Number of Cruise(0)	⌄
IPC006	Number of Cruise(1)	⌄

Camera: IP04

Cruise

Cruise Name: Enter Cruise Name

Preset	Preset Name	Speed	Time	Edit

- **Add Cruise**

Click ⌄ in the camera list on the right side of the interface to display the cruise information of the dome and then click + to add cruise. The operations of the "Add Cruise" window are similar to that of the PTZ control interface; please see PTZ Control Interface Introduction for details.

- **Edit Cruise**

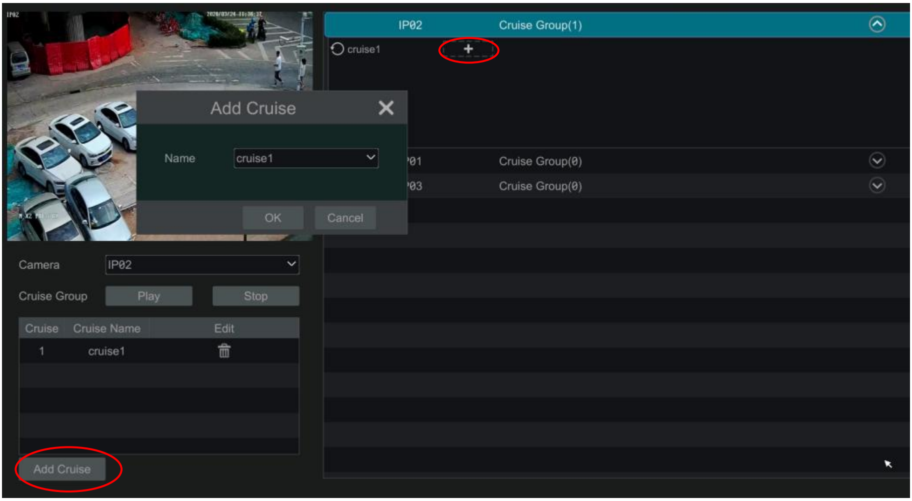
Select the camera and cruise in the "Cruise" interface. Enter the new cruise name and then click 💾 to save the cruise name. Click "Add Preset" to add preset to the cruise. Click ✎ to edit the preset. Click 🗑 to delete the preset from the cruise. Click one preset in the preset list and then click ⬇ to move down the preset and click ⬆ to move up the preset. Click ▶ to start the cruise and click ■ to stop it.

- **Delete Cruise**

Click ⌄ in the camera list on the right side of the interface to display the cruise information of the dome and then click ⊗ on the top right corner of the cruise to delete the cruise.

6.4 Cruise Group Settings

Click ***Start→Settings→Camera→PTZ→Cruise Group*** to go to the interface as shown below.



- **Add Cruise Group**

Click "Add Cruise" to add the cruise, or click ⌄ to extend the cruise list and then click + to add the cruise. After that, click "Play" on the left panel as shown below to play the cruise lines in sequence.

- **Delete Cruise**

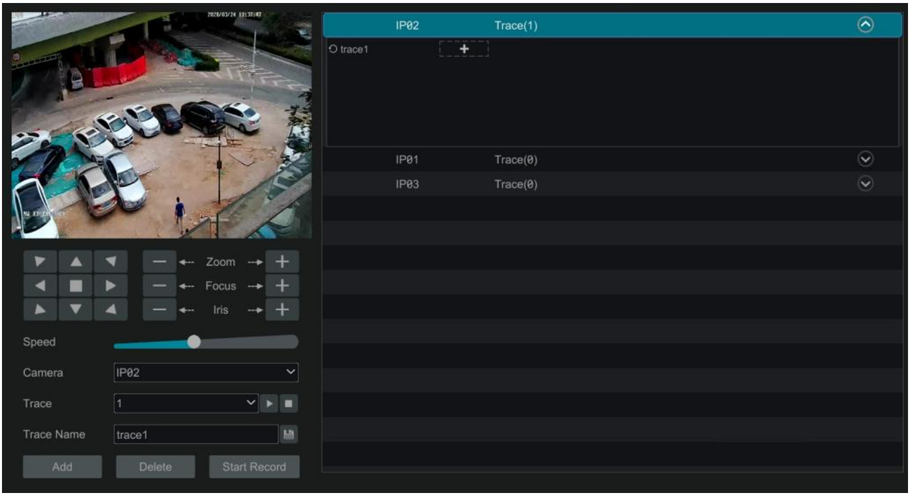
In the cruise list, click 🗑 to delete the cruise.

6.5 Trace Settings

Click ***Start→Settings→Camera→PTZ→Trace*** to go to the interface as shown below.

- **Trace Record**

Select the PTZ camera and then click "Add" or extend the IPC information by clicking ⌄ and then click + to add a trace name. After that, click "Start Record" and move the speed dome to change its position and set its trace. Then click "Stop Record" to complete the trace record.



Speed

Camera: IP02

Trace: 1

Trace Name: trace1

IP02	Trace(1)
trace1	
IP01	Trace(0)
IP03	Trace(0)

- **Play or Stop Trace**

Select the trace and click ▶ to play the trace; click ■ to stop the trace.

- **Modify the Trace Name**

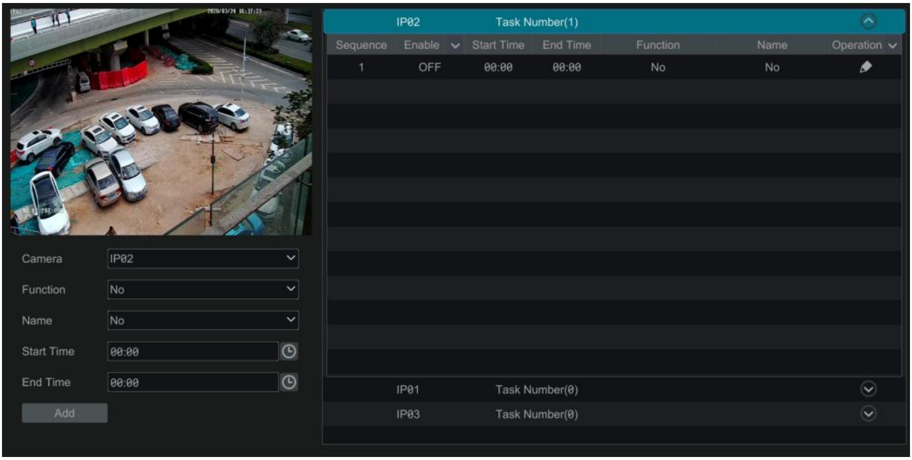
On the left panel, enter new trace name and click 💾 to modify and save the trace name.

- **Delete the Trace**

Click 🗑 to delete the trace. Or put the cursor on the trace name (right panel) and then ⊗ will appear on the right corner of the trace name; click to delete this trace.

6.6 Task Settings

Click ***Start→Settings→Camera→PTZ→Task*** to go to the interface as shown below.



Camera: IP02
Function: No
Name: No
Start Time: 00:00
End Time: 00:00
Add

IP02 Task Number(1)

Sequence	Enable	Start Time	End Time	Function	Name	Operation
1	OFF	00:00	00:00	No	No	✎

IP01 Task Number(0)

IP03 Task Number(0)

① Select a PTZ camera.
② Select function, such as preset, cruise, trace, random scanning, etc.
③ Select a name, such as preset name, cruise name, etc.
④ Select the start and end time.
⑤ Click "Add" to add the task.
⑥ Click ⌄ to extend the tasks of the PTZ camera. Click ⌄ beside "Enable" to enable the task. After the task is enabled, the PTZ camera will start the specific task at the specified time.

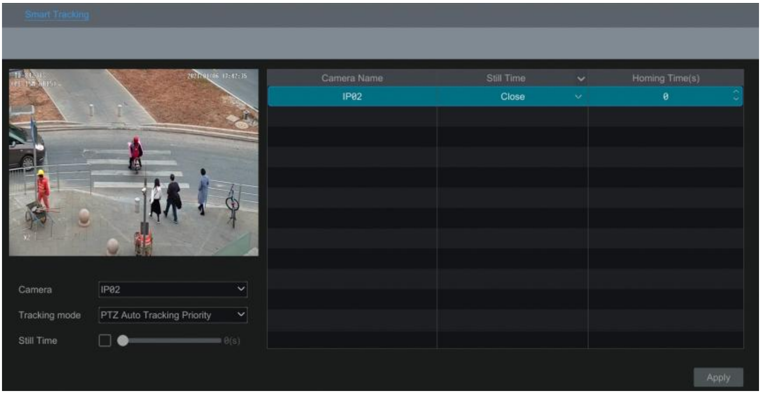
6.7 Smart Tracking

This function is only available for AI PTZ camera. Please add an AI PTZ camera to the NVR for this function to take effect.

Smart Tracking: When people or vehicle cross the alarm line or intrude the predefined area, the PTZ camera can automatically track them and the target image will be automatically zoomed in and centered on the screen until the target disappears from the screen. After that, the PTZ camera will return to the tracking start position.

To set smart tracking:

1. Click ***Settings→Camera→Smart Tracking*** to go to the smart tracking interface.



Smart Tracking

Camera Name	Still Time	Homing Time(s)
IP02	Close	0

Camera: IP02

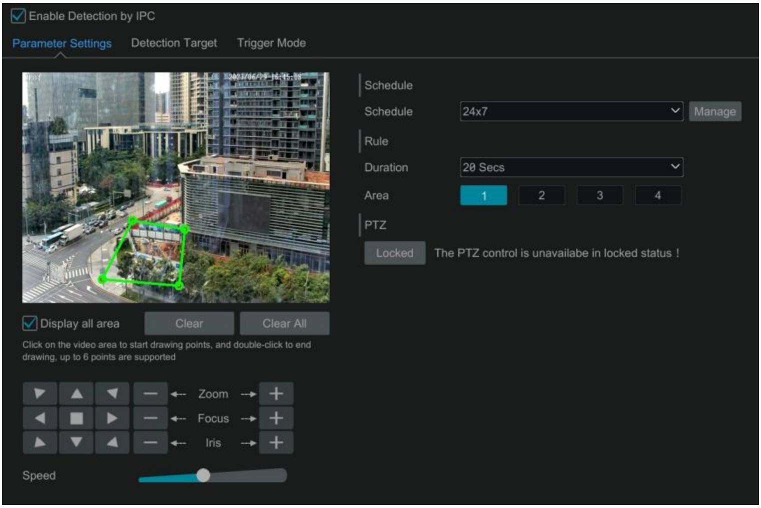
Tracking mode: PTZ Auto Tracking Priority

Still Time: □ 0(s)

2. Select the tracking mode and set the "still time" as needed.

Tracking Mode: choose **"**PTZ Auto Tracking Priority" or "Manual PTZ Control Priority"
PTZ Tracking Priority: if this mode is selected, after enabling "Trigger track" in one of the following events, you cannot control PTZ by clicking the buttons on the PTZ control panel in the live view interface.
Manual PTZ Control Priority: if this mode is selected, after enabling "Trigger track" in one of the following events, you can control PTZ by clicking the buttons on the PTZ control panel in the live view interface during the process of smart tracking. After you stop controlling for 5 seconds, the PTZ camera will return to the pre-defined detection area and start tracking again when detecting a target.
Still time: If it is enabled and the time is set, when the target stops or hides behind an obstacle, or the target tracking is complete and there is no target appearing in the detection area during the set time, the PTZ camera will return to the tracking start position after the set time expires. During this time, if there are targets moving, the PTZ will continue tracking. If it is not enabled, when the target stops or there is no target appearing in the detection area for 5 seconds, the PTZ camera will return to the start tracking position.
For example: At the stoplight, if a car is waiting for the red light for 30 seconds, and the still time is set as 20 seconds, the tracking will stop following; however, if the still time is set as 40 seconds, when the red light changes to green and the car starts to move, the PTZ will continue tracking this car.

3. Click ***Settings→AI/Event→AI Event***. Select the AI PTZ camera and the event as needed For example: Region intrusion.



☑ Enable Detection by IPC

Parameter Settings | Detection Target | Trigger Mode

Schedule

Schedule: 24x7 | Manage

Rule

Duration: 20 Secs

Area: 1 | 2 | 3 | 4

PTZ

Locked | The PTZ control is unavailabe in locked status !

☑ Display all area | Clear | Clear All

Click on the video area to start drawing points, and double-click to end drawing, up to 6 points are supported

4. Enable the event, set the rule and then click "Locked". This button will be changed to "Unlock". Now the PTZ control panel in the above interface will be activated. Set the detection area by clicking the directional buttons in the above interface. After that, click "Unlock" to lock the detection area.

Note: The home position of the PTZ must be locked, or the smart tracking cannot take effect.

5. Click "Draw area" and then draw the area of the region intrusion on the screen.

6. Set the detection target.

7. Click "Apply" to save settings.

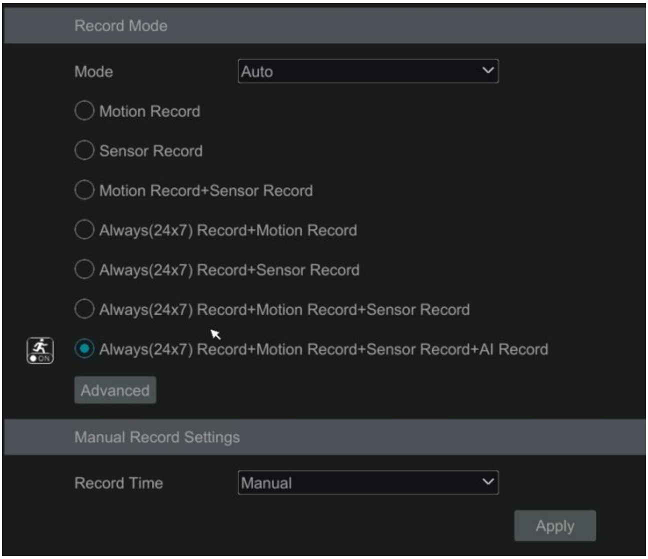
Additionally, you also need to check "Trigger Track" in the PTZ camera.

7 Record & Disk Management

7.1 Record Configuration

7.1.1 Mode Configuration

Please format the HDDs before recording (refer to Disk Management for details). Click ***Start→Settings→Record→Mode Settings*** to go to the mode settings interface. You can set the record time under the "Manual Record Settings" and then click "Apply" to save the settings. There are two record modes: auto mode and customization mode.



Record Mode

Mode: Auto

○ Motion Record

○ Sensor Record

○ Motion Record+Sensor Record

○ Always(24x7) Record+Motion Record

○ Always(24x7) Record+Sensor Record

○ Always(24x7) Record+Motion Record+Sensor Record

● Always(24x7) Record+Motion Record+Sensor Record+AI Record

Advanced

Manual Record Settings

Record Time: Manual

Apply

➢ **Auto Mode**

Motion Record: Motion alarm record will be enabled when motion alarm happens.

Sensor Record: Sensor alarm record will be enabled when sensor alarm happens.

Motion Record+Sensor Record: Motion/sensor alarm record will be enabled when motion/sensor alarm happens.

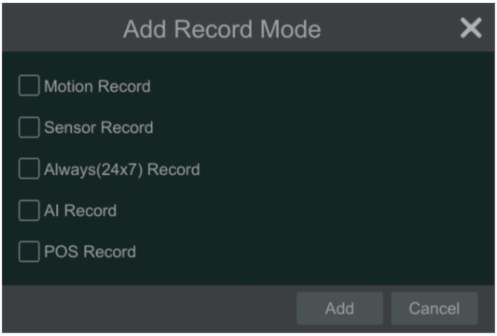
Always(24x7) Record+Motion Record: Normal record is enabled all the time; motion alarm record will be started when motion alarm happens.

Always(24x7) Record+Sensor Record: Normal record is enabled all the time; sensor alarm record will be started when sensor alarm happens.

Always(24x7) Record+Motion Record+Sensor Record: Normal record is enabled all the time; motion/sensor alarm record will be enabled when motion/sensor alarm happens.

Always(24x7) Record+ Motion Record + Sensor Record + AI Record: Normal record is enabled all the time; AI record will be enabled when AI event happens.

You can add more auto modes on analytics record. Click "Advanced" to pop up a window as shown below. Check the modes in the window and then click "Add" to show the modes in the record mode list (in the window, the checked modes can be shown in the record mode list while the unchecked modes cannot).



Add Record Mode

☐ Motion Record

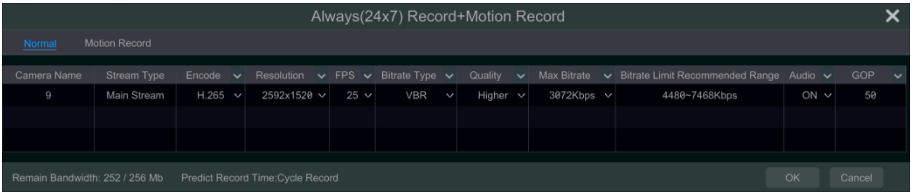
☐ Sensor Record

☐ Always(24x7) Record

☐ AI Record

☐ POS Record

Select one auto mode for the corresponding window to open. Set the encode, GOP, resolution, FPS, bitrate type, quality, max bitrate and audio of each camera and then click "OK" to save your settings. Please adjust the parameters according to the actual condition.



Always(24x7) Record+Motion Record

Camera Name	Stream Type	Encode	Resolution	FPS	Bitrate Type	Quality	Max Bitrate	Bitrate Limit Recommended Range	Audio	GOP
9	Main Stream	H.265	2592x1520	25	VBR	Higher	3072Kbps	4480~7468Kbps	ON	50

Remain Bandwidth: 252 / 256 Mb Predict Record Time:Cycle Record

Video Encode: the available options will be H.265S, H.265+, H.265 and H.264 depending on what the camera supports.

Resolution: the higher the resolution is, the clearer the image is.

FPS: the higher the frame rate is, the more fluency the video has, with the tradeoff of using more storage.

Bitrate Type: CBR and VBR are optional. CBR means that no matter how much change is seen in the video scene, the compression bitrate will be kept constant. VBR means that the compression bitrate will be adjusted according scene changes. For example, for scenes that do not have much movement, the bitrate will be kept at a lower value. This will help to optimize the network bandwidth.

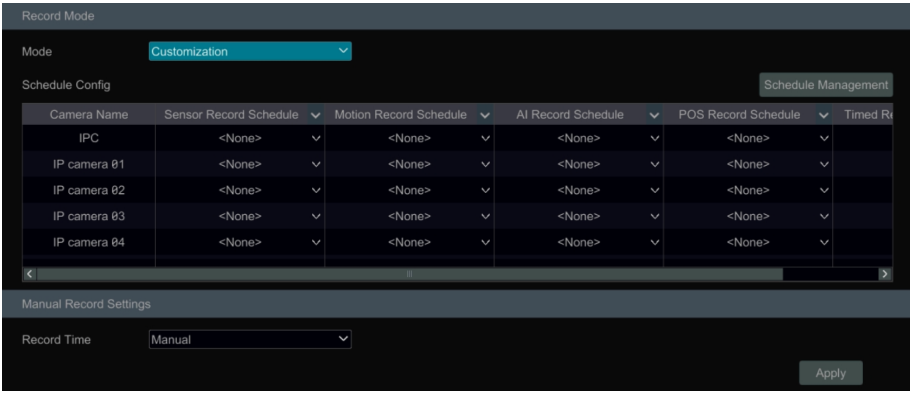
Quality: when VBR is selected, you need to choose image quality. The higher the image quality you choose, the more bitrate will be required.

Max Bitrate: 32Kbps ~10240Kbps are optional.

GOP: group of pictures.

- **Customization Mode**

If the customization mode is selected, you need to set the record schedules of each camera. See Schedule Settings for details.



Record Mode

Mode: Customization

Schedule Config

Camera Name	Sensor Record Schedule	Motion Record Schedule	AI Record Schedule	POS Record Schedule	Timed Re
IPC	<None>	<None>	<None>	<None>	
IP camera 01	<None>	<None>	<None>	<None>	
IP camera 02	<None>	<None>	<None>	<None>	
IP camera 03	<None>	<None>	<None>	<None>	
IP camera 04	<None>	<None>	<None>	<None>	

Manual Record Settings

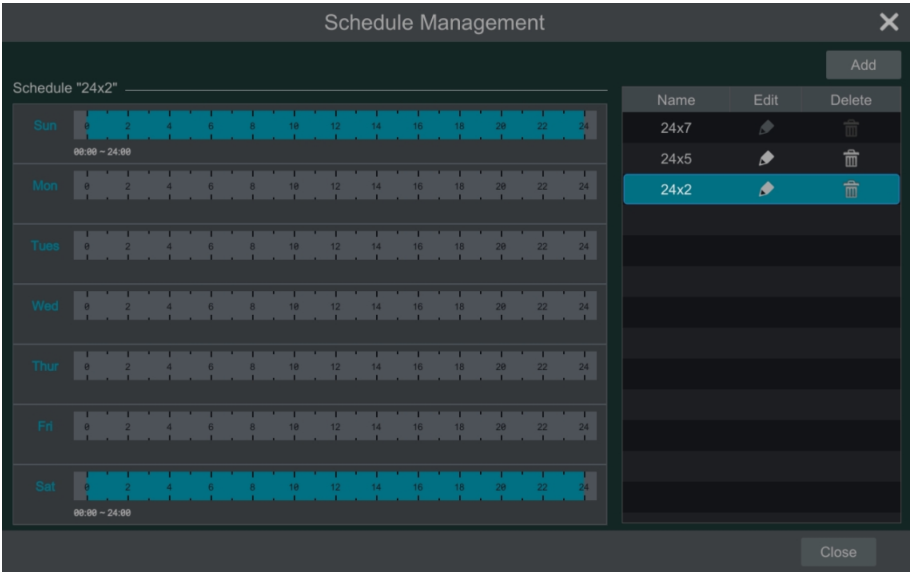
Record Time: Manual

In this interface, you can also set the record period of the manual record in the live view interface.

7.1.2 Schedule Settings

- **Add Schedule**

Click ***Start→Settings→Record→Mode Setting*** to go to the mode setting interface. Then select "Customization" mode and click "Schedule Management" to set the schedule as shown below. "24x7", "24x5" and "24x2" are the default schedules; you cannot edit or delete "24x7" while "24x5" and "24x2" can be edited and deleted. Click the schedule name to display the detailed schedule information on the left side of the interface. The seven rows stand for the seven days in a week and each row stands for 24 hours in a day. Blue stands for the selected time and gray stands for unselected time.



Schedule Management

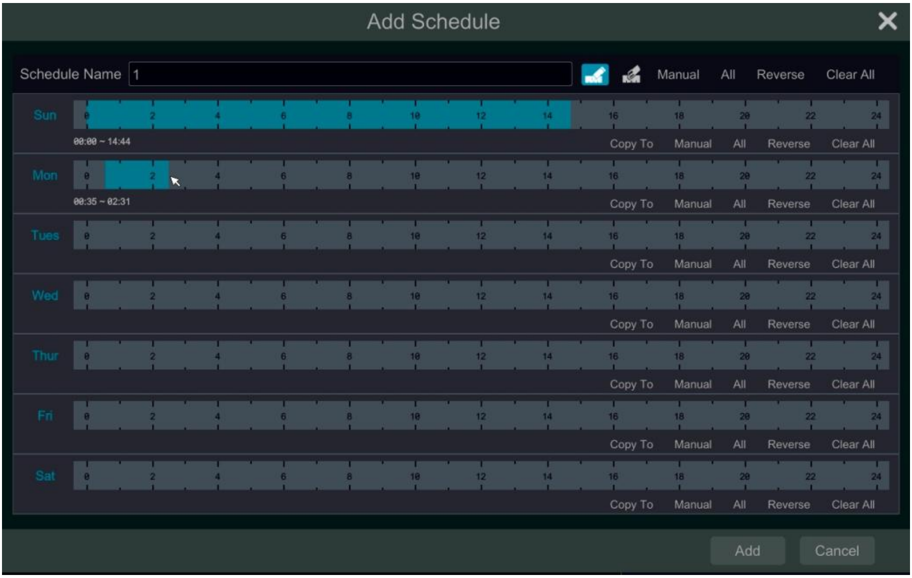
Schedule "24x2"

Name	Edit	Delete
24x7		
24x5		
24x2		

Sun 00:00 ~ 24:00

Sat 00:00 ~ 24:00

Click “Add” to add a new schedule. Refer to the picture below.



Add Schedule

Schedule Name: 1

Sun 00:00 ~ 14:44

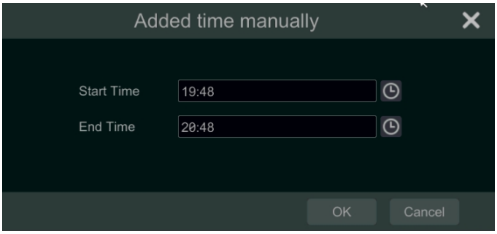
Mon 00:35 ~ 02:31

Set the schedule name and schedule time and then click “Add” to save the schedule. You can set day schedule or week schedule. : add button; : delete button.

➢ Set Day Schedule

Click and then drag the cursor on the time scale to set record time; click and then drag the cursor on the time scale to delete the selected area.

You can manually set the record start time and end time. Click or and then click "Manual" on each day to open a window as shown below. Set the start and end time in the window and then click "OK" to save the settings.

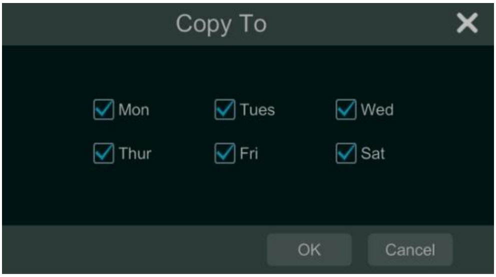


Added time manually

Start Time 19:48

End Time 20:48

Click "All" to set all day recording; click "Reverse" to swap the selected and unselected time in a day; click "Clear All" to clear all the selected area in a day.
Click "Copy To" to copy the schedule of the day to other days. Refer to the picture below. Check the days in the window and then click "OK" to save the settings.



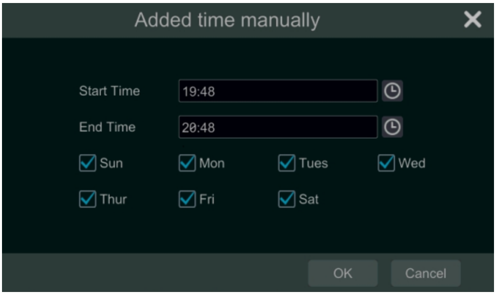
Copy To

☑ Mon ☑ Tues ☑ Wed

☑ Thur ☑ Fri ☑ Sat

➢ Set Week Schedule

Click or and then click "Manual" beside to set the week schedule. Refer to the picture below. Set the start and end time, check the days in the window and then click "OK" to save the settings.



Added time manually

Start Time 19:48

End Time 20:48

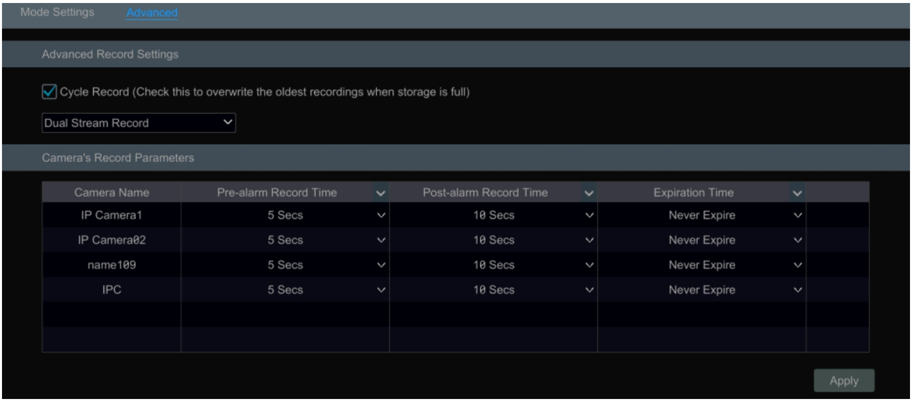
☑ Sun ☑ Mon ☑ Tues ☑ Wed

☑ Thur ☑ Fri ☑ Sat

Click "All" to set all week recording; click "Reverse" to swap the selected and unselected time in a week; click "Clear All" to clear all the selected area in a week.

7.1.3 Advanced Configuration

Click ***Start→Settings→Record→Advanced*** to go to the following interface. Enable or disable cycle record (cycle record: the earliest record data will be replaced by the latest when the disks are full). Choose the record stream. Set the pre-alarm record time, post-alarm record time and expiration time of each camera and then click "Apply" to save the settings.



Advanced Record Settings

☑ Cycle Record (Check this to overwrite the oldest recordings when storage is full)

Dual Stream Record

Camera's Record Parameters

Camera Name	Pre-alarm Record Time	Post-alarm Record Time	Expiration Time
IP Camera1	5 Secs	10 Secs	Never Expire
IP Camera02	5 Secs	10 Secs	Never Expire
name109	5 Secs	10 Secs	Never Expire
IPC	5 Secs	10 Secs	Never Expire

Pre-alarm Record Time: set the time to record before the actual recording begins.

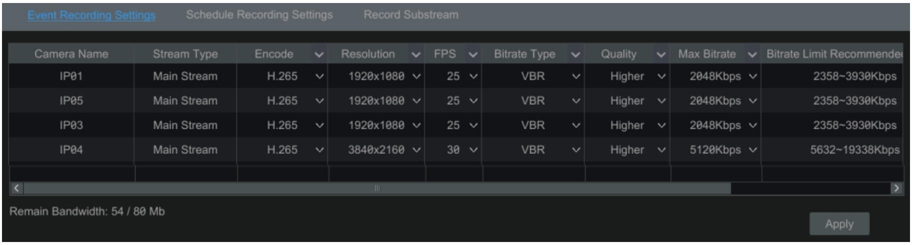
Post-alarm Record Time: set the time to record after the actual recording is finished.

Expiration Time: set the expiration time for recorded video. If the set date is overdue, the recorded data will be deleted automatically.

7.2 Encode Parameters Settings

Click ***Start→Settings→Record→Encode Parameters*** to go to the interface as shown below. Set the encode, resolution, FPS, GOP, bitrate type, quality, max bitrate and audio of main stream for each camera in "Event Recording Settings" and "Schedule Recording Settings" interfaces.

Additionally, the record sub stream of each camera can be viewed. Click “Apply” to save the settings. You can set the record stream of each camera one by one or set them in batches for all cameras.



Camera Name	Stream Type	Encode	Resolution	FPS	Bitrate Type	Quality	Max Bitrate	Bitrate Limit Recommende
IP01	Main Stream	H.265	1920x1080	25	VBR	Higher	2048Kbps	2358~3930Kbps
IP05	Main Stream	H.265	1920x1080	25	VBR	Higher	2048Kbps	2358~3930Kbps
IP03	Main Stream	H.265	1920x1080	25	VBR	Higher	2048Kbps	2358~3930Kbps
IP04	Main Stream	H.265	3840x2160	30	VBR	Higher	5120Kbps	5632~19338Kbps

Remain Bandwidth: 54 / 80 Mb

7.3 Record Mode

7.3.1 Manual Recording

Method One: Click on the tool bar at the bottom of the live view interface to enable recording of the camera.

Method Two: Go to the live view interface and then click the right-click menu “Manually Record On” in the camera window or click on the tool bar under the camera window to start recording.

> *Note: Click Start→Settings→Record→Mode Settings and then set the manual record time in the interface. Click “Apply” to save the settings.*

7.3.2 Timing Recording

Timing Recording: the system will record automatically according to the schedule.
Set the timing record schedule of each camera. See Schedule Settings for details.

7.3.3 Motion-based Recording

Motion-based Recording: the system will start motion-based recording when the motion object appears in the setup schedule. The setup steps are as follows:

① Set the motion-based recording schedule of each camera. See Schedule Settings for details.

② Enable the motion and set the motion area of each camera. See Motion Alarm for details.

The camera will start motion-based recording once you finish the above settings.

7.3.4 Sensor Based Recording

① Set the sensor based recording schedule of each camera. See Schedule Settings for details.

② Set the NO/NC type of the sensor, enable the sensor alarm and then check and configure the “Record”. See Sensor Alarm for details.

7.3.5 AI Event Recording

① Set the analytics recording schedule of each IP camera. See Schedule Settings for details.

② Enable the intelligent alarm detection (object detection, exception, line crossing, intrusion or face detection) and draw alert surface or warning area of each IP camera. See AI Event Management for details.

The camera will start analytic recording once you finish the above steps. This function is only available for some IPCs.

7.4 Disk

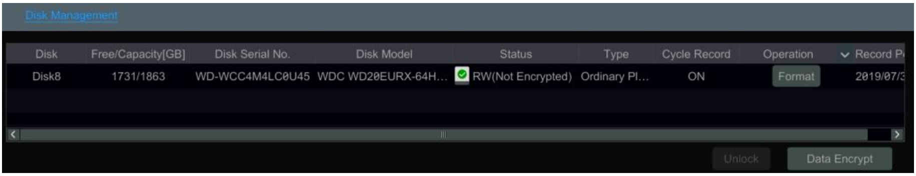
7.4.1 Disk Management

The HDD can be plugged in or pulled out when the NVR is on. When the HDD is in abnormal status, the abnormal information will be prompted on the screen (such as “No HDD”, “Only read”, “Unformatted”, “The HDD is unavailable”, etc.)

For the model with 8HDDs or more, in order to avoid video frame loss, it is recommended to use 7200RPM HDDs or above and add cameras to different disk groups or create one or more RAIDs (if applicable) to record.

➢ Disk Management

Click ***Start→Settings→Disk→Disk Management*** to go to disk management interface. You can view the NVR’s disk number and disk status and so on in the interface. Click “Format” to format the HDD.



Disk Management

Disk	Free/Capacity[GB]	Disk Serial No.	Disk Model	Status	Type	Cycle Record	Operation	Record P
Disk8	1731/1863	WD-WCC4M4LC0U45	WDC WD20EURX-64H...	✓ RW(Not Encrypted)	Ordinary Pl...	ON	Format	2019/07/3

Data Encryption:

① Click “Data Encrypt”.

② Enter the username and password used to log into the NVR. This username and password must have the permission of disk management.

③ Check the disk you want to encrypt and then enter the password.

After you encrypt the data of a disk, this disk cannot be read by other NVRs unless it is unlocked.

Data Decryption:

① Click “Change Encryption”.

② Enter the username and password used to log into the NVR. This user must have the permission of disk management.

③ Check the disk you want to decrypt and then clear the password.

④ Click “Close Encryption”.

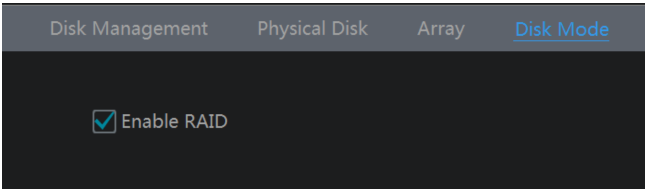
Unlock the disk: when one encrypted disk is transferred from another NVR to this NVR, it will be locked. You can select this locked disk and click “Unlock”. After you enter the password of its data encryption, its status will be “Read Only”. Now you can read the data of this disk but nothing can be written to it.

Some models may not support RAID function. RAID settings are as follows. Please skip the settings of physical disk, array and disk mode if the NVR doesn’t support this function. Check the datasheet for your model to confirm if it supports RAID.

➢ RAID

① Enable RAID

(Go to ***Start→Settings→Disk→Disk Mode***)



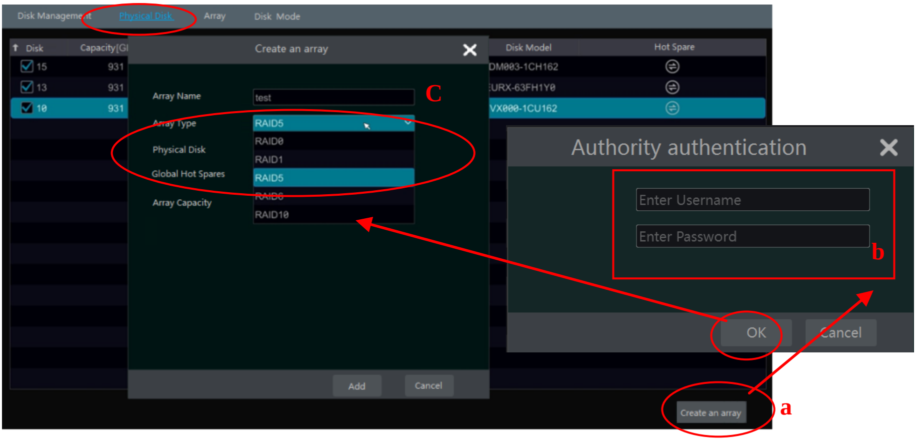
☑ Enable RAID

② Create an array. (Go to ***Start→Settings→Disk→Physical Disk***)

a. Click “Physical Disk” tab and then click “Create an array”.

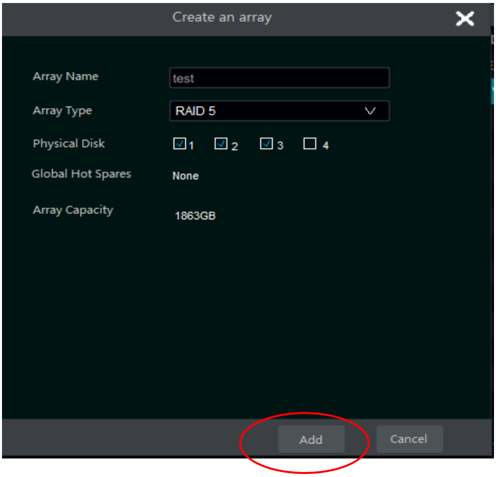
b. Enter the user name and password which has the authority of Disk Management. If you don’t have one, you can use the user name and password for system login(the default username: admin).

c. Enter array name and select array type (like RAID5).



d. Select physical disk.

If you have 16 disks, please check 15 disks. The remaining one should be set to a hot spare. If higher data security is needed, you can decrease physic disks and increase hot spare disks. Please set them as needed.


Create an array

Array Name: test

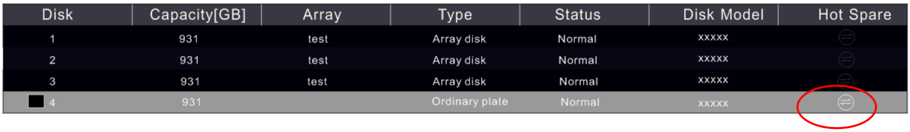
Array Type: RAID 5

Physical Disk: ☑1 ☑2 ☑3 □4

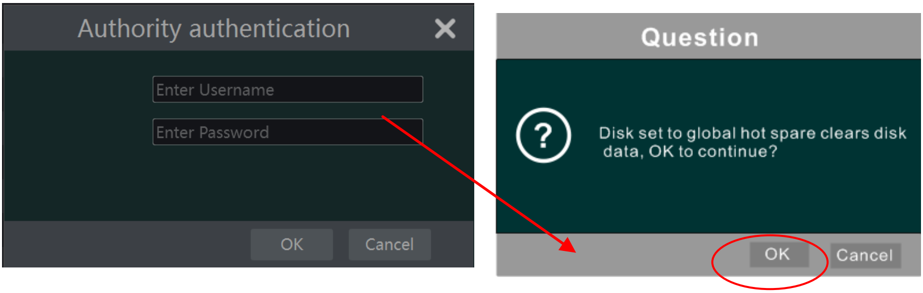
Global Hot Spares: None

Array Capacity: 1863GB

e. Select a hot spare. In the physical disk interface, select the disk that is not in the array and click ⊜ as shown in the following pictures.



Disk	Capacity[GB]	Array	Type	Status	Disk Model	Hot Spare
1	931	test	Array disk	Normal	xxxxx	⊜
2	931	test	Array disk	Normal	xxxxx	⊜
3	931	test	Array disk	Normal	xxxxx	⊜
■ 4	931		Ordinary plate	Normal	xxxxx	⊜



Authority authentication

Enter Username

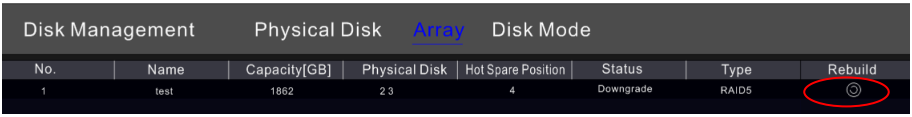
Enter Password

Question

Disk set to global hot spare clears disk data, OK to continue?

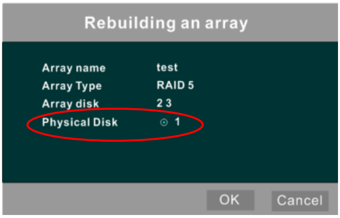
- RAID Rebuilding

If one of your disks is defective, the disk indicator on the front panel will turn red. A warning tip will pop up if the relevant HDD exception alarm is set. You need to rebuild the RAID after you replace the broken disk with a new one.



No.	Name	Capacity[GB]	Physical Disk	Hot Spare Position	Status	Type	Rebuild
1	test	1862	2 3	4	Downgrade	RAID5	◎

Click the above circled icon and then select the physical disk to rebuild.



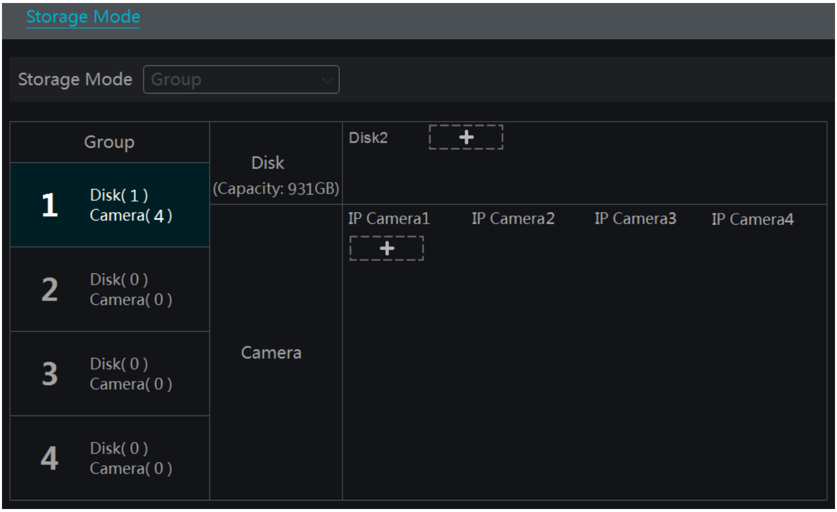
Rebuilding an array

Array name	test
Array Type	RAID 5
Array disk	2 3
Physical Disk	⊙ 1

Note: If the HDD you want to install has been used in a RAID of another device, it is recommended to install it after the device starts up. Having installed the HDD, you can set it as a hot spare disk or add it to a new RAID. If you have installed the HDD in shutdown state, the RAID you have created before is unavailable after the device runs. Now, you need to reboot your device to solve this problem.

7.4.2 Storage Mode Configuration

Click ***Start→Settings→Disk→Storage Mode*** to go to the interface as shown below.



Storage Mode

Storage Mode: Group

Group		

1	Disk(1)
	Camera(4)	

2	Disk(0)
	Camera(0)	

3	Disk(0)
	Camera(0)	

4	Disk(0)
	Camera(0)	

Disk (Capacity: 931GB): Disk2 +

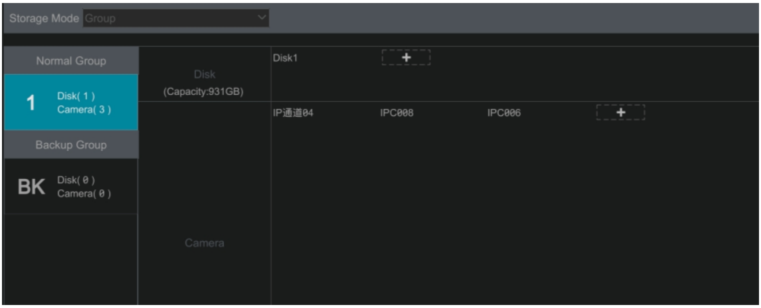
Camera: IP Camera1, IP Camera2, IP Camera3, IP Camera4 +

By using disk group, you can correspond a camera to disk (the record data of the camera in the group will be stored into the disks in the same group). The NVR with e-SATA interface supports e-SATA recording.

The added disks and cameras will be added into group one automatically. The disks and cameras in the groups can be deleted except group one (select a disk group and then click ⊗ on the top right corner of the added disk or camera to delete it from the group). The deleted disks and cameras will be moved into group one automatically.

Each group can add disks and cameras from other groups. Each disk and camera can only be added into one group. Select a disk group and then click + in the disk or camera row to open a window. Check the disks or cameras in the window and then click “Add”.

For the model with 2 or 4 HDD slots, BK group can be added as shown below.



Storage Mode: Group

Normal Group

1 Disk(1) Camera(3)

Backup Group

BK Disk(0) Camera(0)

Disk (Capacity:931GB): Disk1 +

Camera: IP通道04, IPC008, IPC006 +

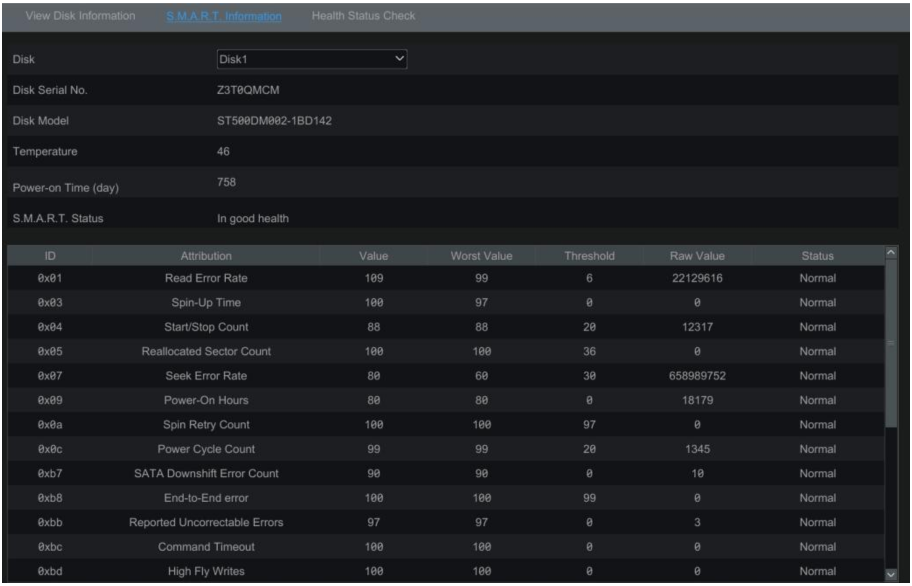
Click + to add the backup HDD. After account verification, select a HDD and then this HDD will be removed from the normal group to the backup group. Simultaneously, it will be formatted. Please back up all data of this HDD in advance when you want to remove it to the backup group.

You can add cameras to this HDD. The added cameras can exist and be recorded both in one HDD of the normal group and the backup group.

Note: Each HDD only can exist in one group.

7.4.3 View Disk Information

Click ***Start→Settings→Disk→View Disk Information*** to view the HDD information; click "S.M.A.R.T. Information" to view the working status of the HDD (refer to the picture below); click "Health Status Check" to check the western digital purple disks' health status.



Disk: Disk1

Disk Serial No.: Z3T0QMCM

Disk Model: ST500DM002-1BD142

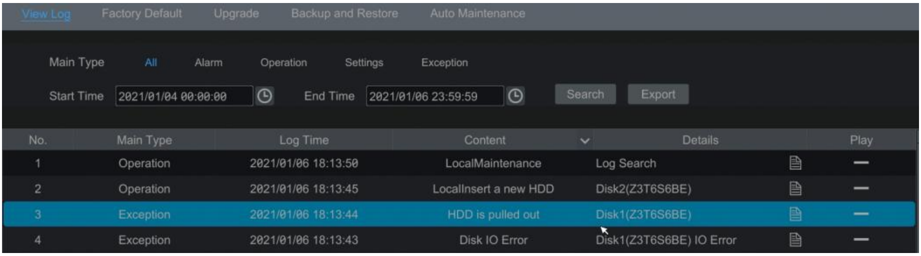
Temperature: 46

Power-on Time (day): 758

S.M.A.R.T. Status: In good health

ID	Attribution	Value	Worst Value	Threshold	Raw Value	Status
0x01	Read Error Rate	109	99	6	22129616	Normal
0x03	Spin-Up Time	100	97	0	0	Normal
0x04	Start/Stop Count	88	88	20	12317	Normal
0x05	Reallocated Sector Count	100	100	36	0	Normal
0x07	Seek Error Rate	80	60	30	658989752	Normal
0x09	Power-On Hours	80	80	0	18179	Normal
0x0a	Spin Retry Count	100	100	97	0	Normal
0x0c	Power Cycle Count	99	99	20	1345	Normal
0xb7	SATA Downshift Error Count	90	90	0	10	Normal
0xb8	End-to-End error	100	100	99	0	Normal
0xbb	Reported Uncorrectable Errors	97	97	0	3	Normal
0xbc	Command Timeout	100	100	0	0	Normal
0xbd	High Fly Writes	100	100	0	0	Normal

In addition, you can view the plug-in or pull-out details of the HDD from the logs to check whether someone moves your HDD or not. Click ***Start→Settings→System→View Log***.



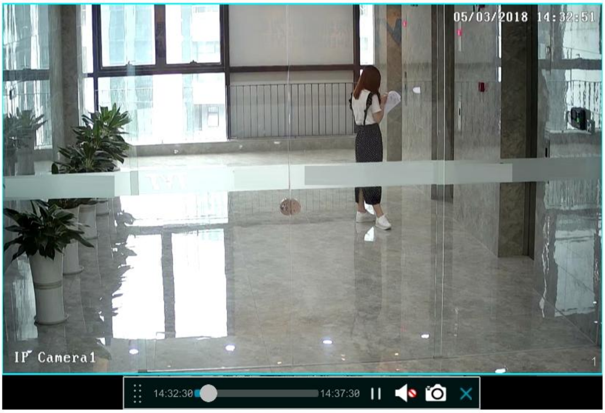
Start Time: 2021/01/04 00:00:00 End Time: 2021/01/06 23:59:59

No.	Main Type	Log Time	Content	Details	Play
1	Operation	2021/01/06 18:13:50	LocalMaintenance	Log Search	—
2	Operation	2021/01/06 18:13:45	LocalInsert a new HDD	Disk2(Z3T6S6BE)	—
3	Exception	2021/01/06 18:13:44	HDD is pulled out	Disk1(Z3T6S6BE)	—
4	Exception	2021/01/06 18:13:43	Disk IO Error	Disk1(Z3T6S6BE) IO Error	—

8 Playback & Backup

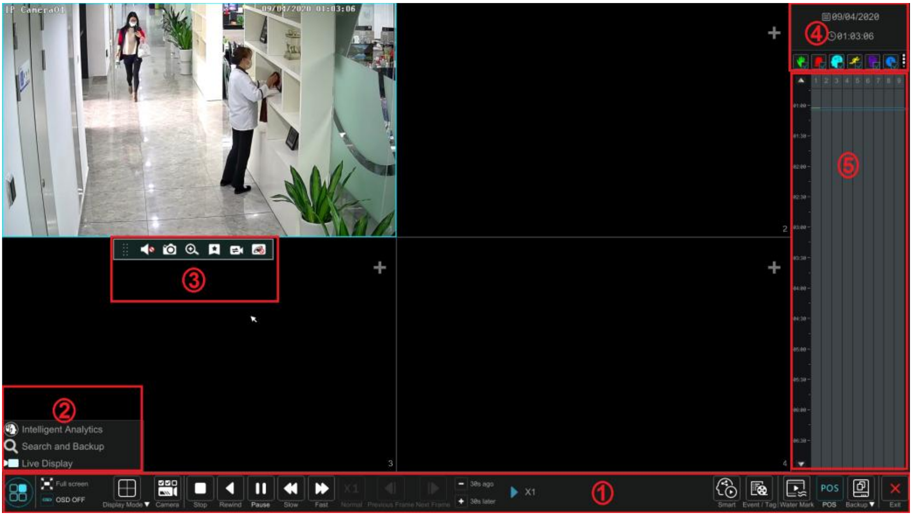
8.1 Instant Playback

Click ▶ on the tool bar at the bottom of the preview camera window to play back the record (click ⌃ on the tool bar at the bottom of the live view interface to set the default playback time). Refer to the picture below. Drag the playback progress bar to change the playback time. You can also click the right-click menu “Instant Playback” in the camera window and then set the instant playback time to play back the record.



8.2 Playback Interface Introduction

Click ⊙ on the tool bar at the bottom of the live view interface or click ***Start→Playback*** to go to the playback interface as shown below (click ⌃ on the tool bar at the bottom of the live view interface to set the default playback time).



The panel on the right will show you the channel number and the recorded data coded by color. The bar that runs across them represents the playback time being viewed. You can move this bar around. To export, highlight a section of the desired recording, click export and follow the prompts. You can export single or multiple channels at the same time.

The added cameras will playback their recordings in the playback interface automatically. You can also add the playback camera manually. Click + in the playback window to open the "Add Camera" window. Check the cameras in the window and then click "Add" to add playback camera. The system supports a maximum of 16 synchronous playback cameras.

The buttons on the tool bar (area ①) at the bottom of the playback interface are introduced in the table below.

Button	Meaning
⊞	Start button. Click to pop up area ②.
⛶	Full screen button. Click to show full screen; click again to exit the full screen.
⊞ Display Mode ▼	Screen display mode button. 1/4/9/16 screen display mode can be selected (depending on models); in addition, the playback channel will be switched by continuous selection of the same screen display mode, for example, after selecting 1-screen display mode, click this mode again and then the current playback channel will switch to the next playback channel.
OSD	OSD ON button. Click to enable OSD; click again to disable OSD.
Camera	Quick channel selection button
■	Stop button.

Button	Meaning
◀	Rewind button. Click to play video backward.
▶	Play button. Click to play video forward.
⏸	Pause button.
⏪	Slow Play button. Click to decrease the playing speed.
⏩	Fast Play button. Click to increase the playing speed.
◀‖	Previous frame button. It works only when the forward playing is paused in single screen mode.
‖▶	Next frame button. It works only when the forward playing is paused in single screen mode.
− 30s ago + 30s later	Click − to step backward 30s and click + to step forward 30s.
⟳	Click to enter the smart playback interface
☰	Event list/tag button. Click to view the event recording of manual/schedule/sensor/ motion and the tag information.
▣	Watermark button. Click to enable watermark; click it again to disable watermark.
POS	Open/close POS information.
⏻/Backup ▾	⏻ Backup button. Drag the mouse on the time scale to select the time periods and cameras, and then click the button to back up the record. ▣: Backup status button. Click to view the backup status.
✕	Back button. Click to return.

Note: Some models may not support face search and face smart playback.

Introduction of area ②:

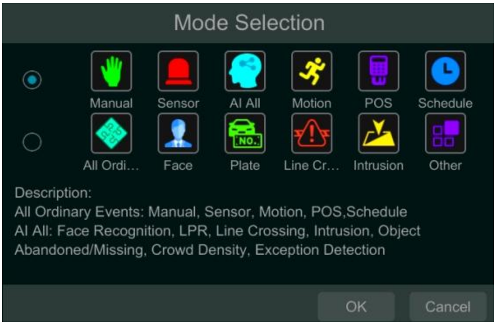
Button	Meaning
Intelligent Analytics	Click to go to the intelligent analytics interface.
Search and Backup	Click to go to record search and backup interface; see Record Search, Playback & Backup for details.
Live Display	Click to go to the live view interface; see Live View Introduction for details.

Click on the playback window to show the tool bar as shown in area ③; right click on the window to show the menu list. The tool bar and menu list are introduced in the table below.

Button	Menu List	Meaning
⋮	--	Move tool. Click to move the tool bar anywhere.
🔇	**Enable Audio**	Click to enable audio. You can listen to the camera audio by enabling audio.
📷	**Snap**	Click to take a snapshot.
🔍	**Zoom In**	Click to go to the zoom in interface. The zoom in interface is similar to that of the camera window in the live view interface. Click ⏸ to pause the record playing; click ▶ to play the record. When the record is paused in forward playing mode, you can click ◀ to view the previous frame and click ▶ to view the next frame.
★	**Add Tag**	Click to add tag. You can play back the record by searching the added tag. Click and then enter the tag name in the popup window. Click “Add” to add tag.
⇄	**Switch Camera**	Click to switch the playback camera. Click it and then check the camera in the popup window. Click “OK” to change the camera.
⊘	**Close Camera**	Click to close the playback camera.

Introduction of area ④:

Click 📅 to set the date; click 🕒 to set the time and then the playback camera will play the record from the time you set. You can check the record type as needed for record playback; first you should click ■ on the tool bar at the bottom of the interface to clear all the playback camera, then check the record type (✋: manual record; 🚨: sensor based record; 🏃: motion-based record; 🕒: schedule record; 🧠: AI record; ▨: POS record, if you want view the detailed smart playback icons, click ⋮ to switch, as shown below). Finally, click ➕ in the playback window to add camera for playback (the record time scale will show the record data of the checked record type only after the above operations).



Description:
All Ordinary Events: Manual, Sensor, Motion, POS,Schedule
AI All: Face Recognition, LPR, Line Crossing, Intrusion, Object Abandoned/Missing, Crowd Density, Exception Detection

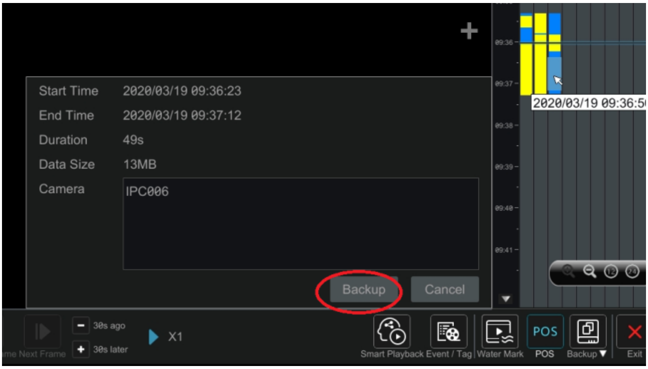
Introduction of the record time scale (area ⑤):

A tool bar will appear after moving the mouse to the record time scale. Click ⊕ / ⊖ to zoom the timeline; click ㉔ to recover the timeline to 24 hours' ratio. Drag the timeline or slide the scroll wheel of the mouse on the time scale to show the hidden time on the top or bottom of the timeline. You can also click ▲ to show the hidden time on the top of the timeline or click ▼ to show the hidden time on the bottom of the timeline. Drag the slider at the bottom of the time scale to show the hidden playback cameras.

The record time scale shows different record types with different colors. The green block stands for manual record, red block stands for sensor based record, yellow block stands for motion-based record, blue block stands for schedule record and cyan block stands for intelligence record. Click the record block to set the time and then the playback camera will play the record from the time you set.

Backup Introduction:

Insert the storage device into the device. Drag the color block on the time scale to select the backup area and then right click the area or click ⏺ to pop up a backup information window. Click the "Backup" button in the window to pop up the backup window. Select the device, backup path and backup format and then click the "Backup" button.

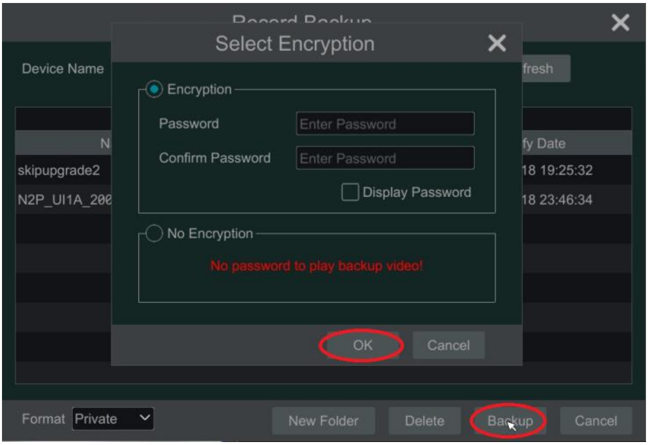


Start Time	2020/03/19 09:36:23
End Time	2020/03/19 09:37:12
Duration	49s
Data Size	13MB
Camera	IPC006

In the backup window, you can select backup path and format. Then click "Backup".

Backup format: Private, AVI or MP4.

Please select "Encryption" or "No Encryption" as needed. After that, click "OK".



Record Backup

Select Encryption

● Encryption

Password: Enter Password

Confirm Password: Enter Password

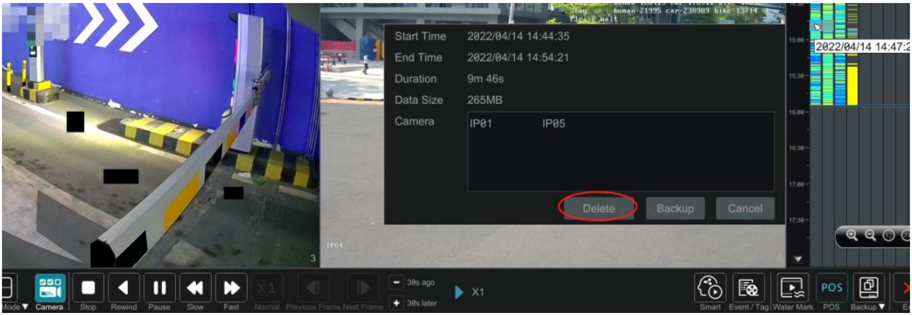
□ Display Password

○ No Encryption

No password to play backup video!

Delete the video record of backup disk group

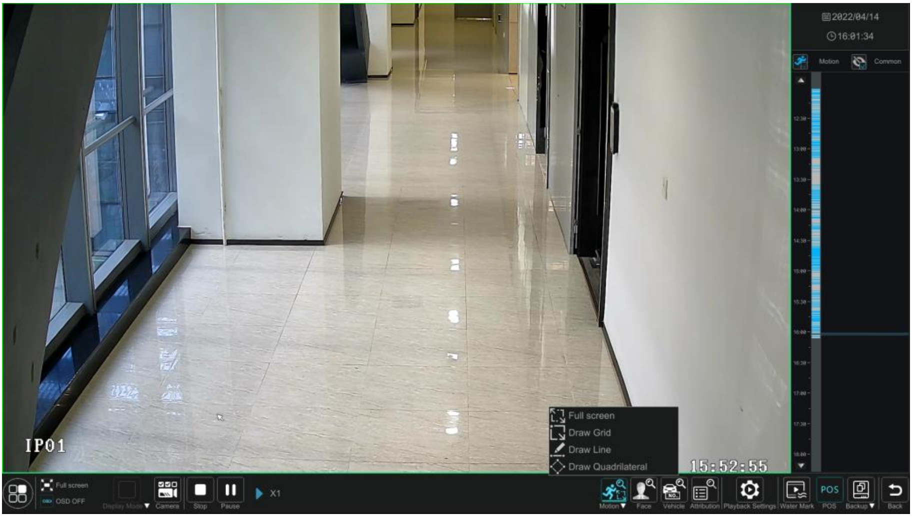
In the playback interface, click to select the backup disk group. Then use the left mouse button to drag on the timetable to select the records you want to delete. Then right click and select [Delete] to delete it.



Start Time	2022/04/14 14:44:35
End Time	2022/04/14 14:54:21
Duration	9m 46s
Data Size	265MB
Camera	IP01 IP05

8.3 Smart Playback

In the playback interface, click to go to the smart playback interface as shown below.



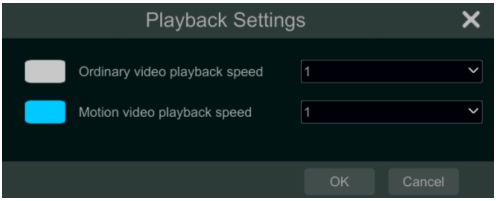
The descriptions of buttons in the smart playback interface

Button		Description
Motion ▼	⛶	Full screen motion button.
	⛶	Draw grid. You can search the record of motion detection in the pre-defined area.
	✎	Draw line. You can search the record of crossing the line after drawing the line.
	◇	Draw quadrilateral. You can search the record in this quadrilateral after drawing it.
Face		Search by face (only some models support)
Vehicle		Search by license plate number
Attribution		Search by human/vehicle attributes
⚙		Playback settings button
↩		Return button. Click to return to the previous interface.

8.3.1 Smart Playback Settings

Click ⚙ to set “Motion/Face/Vehicle video playback speed”, “Ordinary video playback speed”.

You can disable “Common” to view motion/face vehicle video playback in the right corner of the smart playback interface.



Playback Settings

Ordinary video playback speed: 1

Motion video playback speed: 1

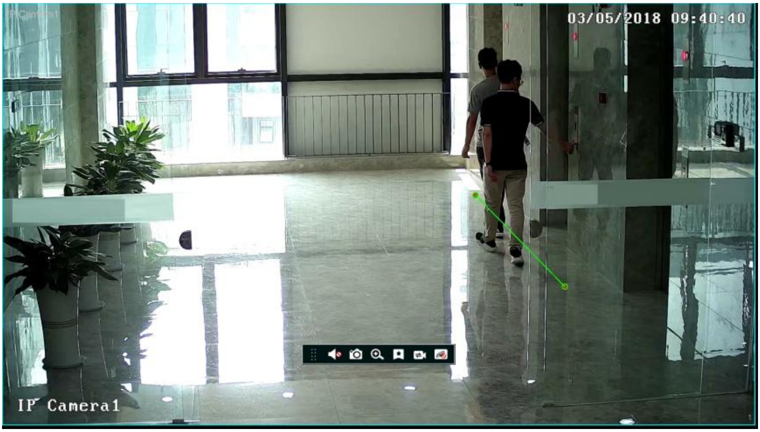
8.3.2 Smart Playback Based on Motion Detection

- **Smart Playback by Drawing Grid**

Click and draw a rectangle in the desired area. The system will automatically search the record files of this area. The cyan blocks indicate that there are intelligent recording files. Move the cursor to such block and click to play the recording.

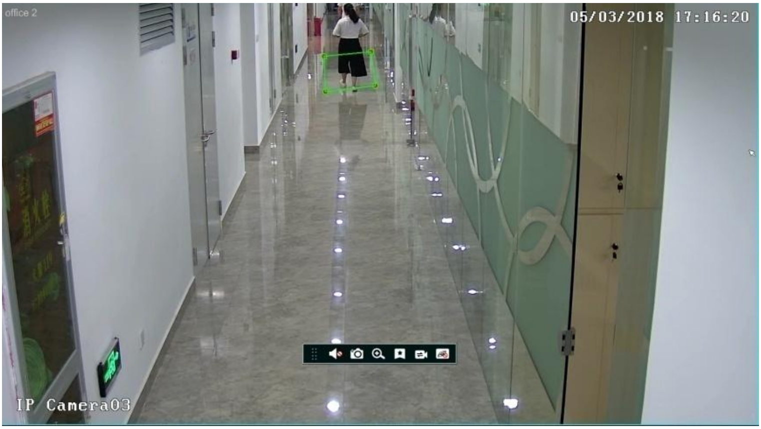
- **Smart Playback by Drawing Line**

Click and draw a line in the desired area. Then the system will automatically search for the record files where this line was crossed. The cyan blocks indicate that there are intelligent recording files. Move the cursor to such block and click to play the recording.



- **Smart Playback by Drawing Quadrilateral**

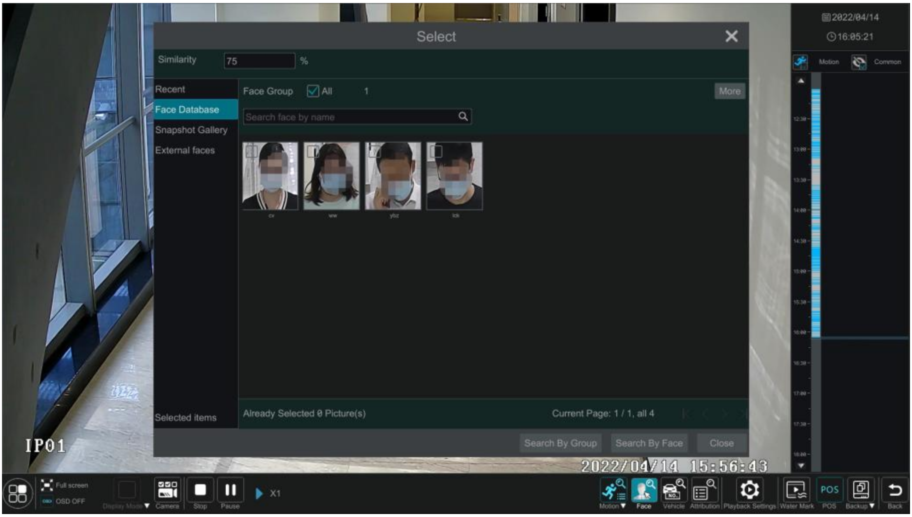
Click and draw a quadrangle in the desired area. Then the system will automatically search the record files of this area. The cyan blocks indicate that there are intelligent recording files. Move the cursor to such block and click to play the recording.



8.3.3 Smart Playback by Face Search

Before starting this function, the face recognition function must be enabled. Please see Face Recognition for details. If your device doesn't support such a function, please skip the following instructions.

① In the smart playback interface, click Face to open the following window.


Similarity 75 %

Already Selected 0 Picture(s)

Current Page: 1 / 1, all 4

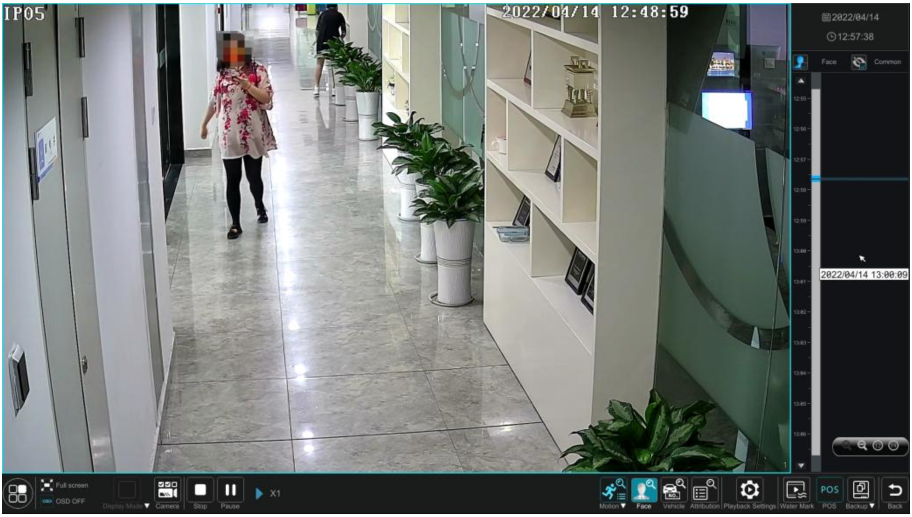
② Set similarity. The higher the sensitivity value is, the lower the searching accuracy is, and vice versa.

③ Select targets. You can select targets from recent, face database, snapshot gallery or external faces.

④ Select search mode. There are two search modes: search by group and search by face.

Search by group: Choose “Face Database” and then click “More” to choose one or more groups.

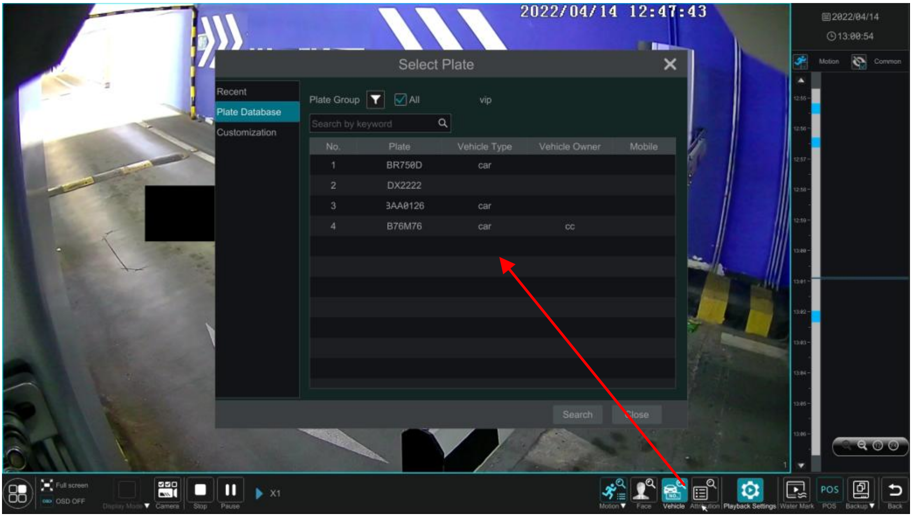
Move the cursor to the time block where the record exists and click to play those records. You can only check “Face” to view the face records.



8.3.4 Smart Search by License Plate

Before starting smart search by plates, please add ANPR cameras first and enable the LPR function. Please refer to License Plate Recognition section for details.

Click Vehicle button to go to the following interface.


[redacted]

Select Plate

Recent
Plate Database
Customization

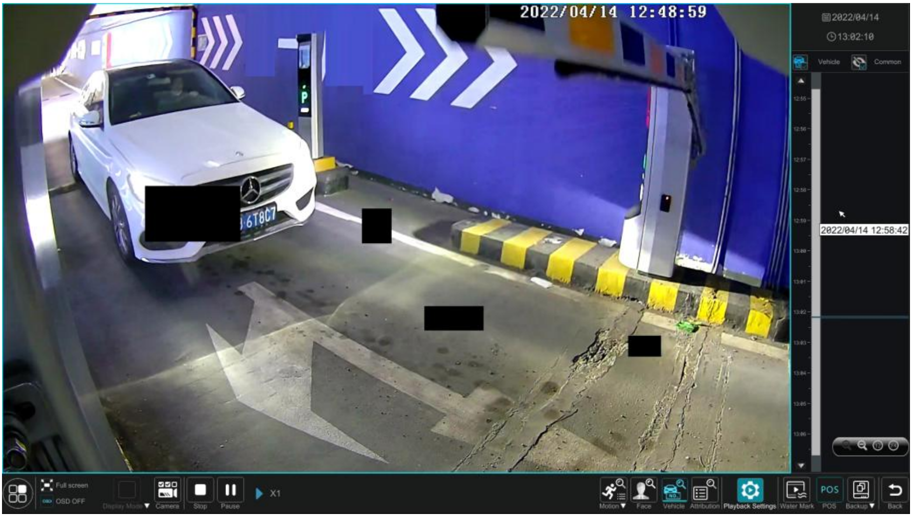
Plate Group ☑ All vip

Search by keyword

No.	Plate	Vehicle Type	Vehicle Owner	Mobile
1	BR750D	car		
2	DX2222			
3	3AA0126	car		
4	B76M76	car	cc	

Select the plate from “Recent”, “Plate Database” or “Customization” and then click “Search” to search recorded files and play. Here is an example of plate search from “Plate Database”.

Click ▼ to choose a group. Then plates will be listed in the table automaticaly. Click “Search” to play.

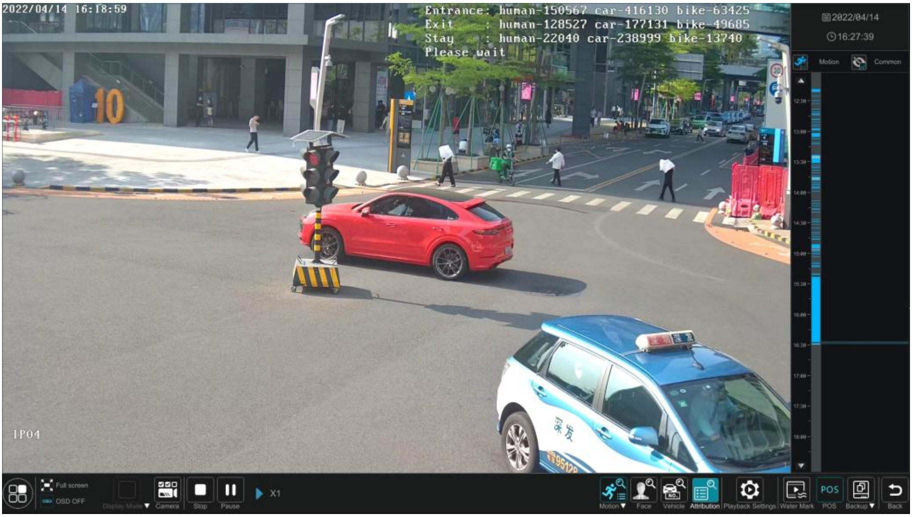

[redacted]
[redacted]
[redacted]
[redacted]

8.3.5 Smart Search by Object Attributes

Before searching objects by attributes, please enable video metadata function of cameras. ***Please note that this function will only work with specific cameras running the newest***

firmware. Click to select the attributes.

Select the attributes of human/motor vehicle/non-motor vehicle as needed to search the results.



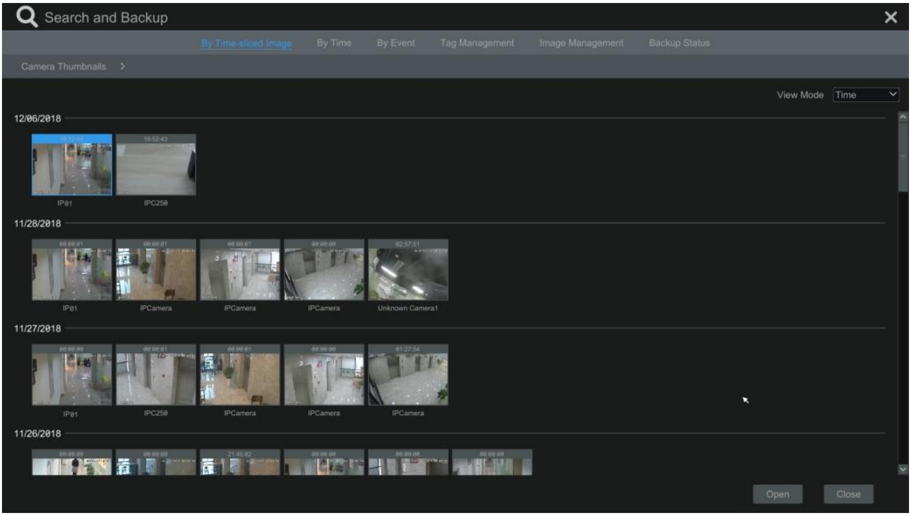
```
2022/04/14 16:18:59
Entrance: human-150567 car-416130 bike-63425
Exit    : human-128527 car-177131 bike-49685
Stay    : human-22040 car-238999 bike-13740
Please wait
```

8.4 Record Search, Playback & Backup

The record data and the captured pictures can be backed up through the network or USB (U disk or USB mobile HDD). The file system of the backup devices should be FAT32 format.

8.4.1 Search, Playback & Backup by Time-sliced Image

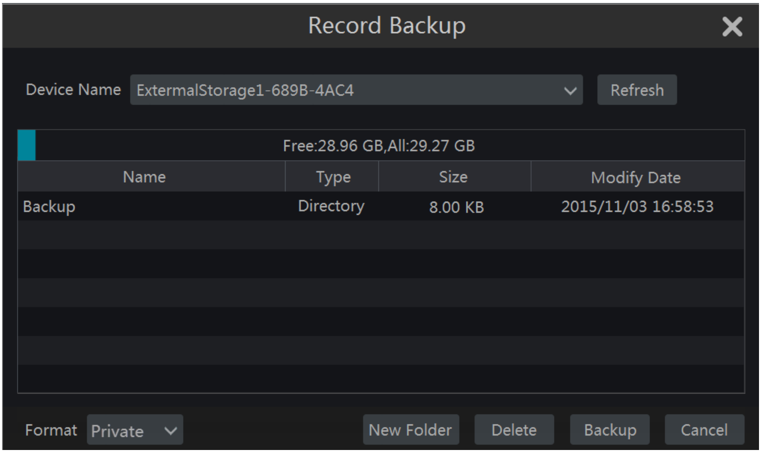
① Click ***Start→Search and Backup→By Time-sliced Image*** to go to “By Time-sliced Image” tab. There are two view modes: by time and by camera. In the time view mode, a maximum of 64 camera thumbnails can be shown. If the camera thumbnail number is more than 64, the cameras will be listed directly by their camera name, not the thumbnail. A maximum of 196 camera names can be listed. If the camera names exceed 196, the time view mode will be disabled and only the camera view mode will be available.



② Select one camera in the interface and then click the “Open” button.

③ Click the image box to play the recording in the small playback box on the left side of the interface (the box which has image inside indicates that the recording data exist).

④ Refer to the picture below. Drag the color blocks on the time scale to select the recording data and then click the “Backup” button to open the “Record Backup” window as shown below. Select the device name, backup format and path and then click the “Backup” button to start the backup.


Record Backup

Device Name ExternalStorage1-689B-4AC4

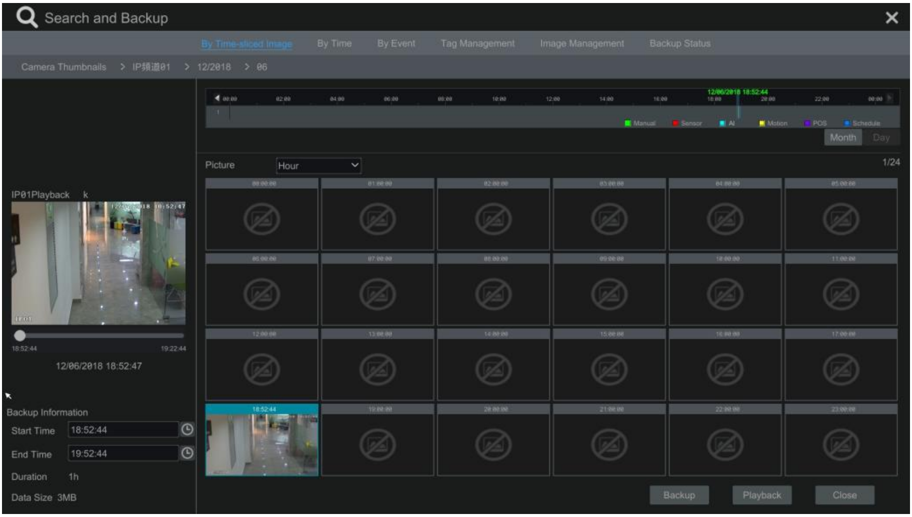
Free:28.96 GB,All:29.27 GB

Name	Type	Size	Modify Date
Backup	Directory	8.00 KB	2015/11/03 16:58:53

Format Private

Note: If you back up the record in private format, the system will back up a RPAS player to USB device automatically. The private format record can be played by RPAS player only.

⑤ Click “Playback” to play the record in the playback interface (refer to Playback Interface Introduction for details). Click “Close” to close the interface.



Picture: Hour

12/06/2018 18:52:47

Backup Information

Start Time 18:52:44

End Time 19:52:44

Duration 1h

Data Size 3MB

Time Slice Search:

Method One: Click “Year”, “Month” or “Day” button under the record time scale to select the time slice mode. In “Day” mode, click ◀ / ▶ on the left/right side of the time scale to view the record of the last/next day; click “Minute” in the “Picture” option under the time scale to select “Minute” mode (in “Minute” mode, click the time scale to change the time of the 60 display windows) and click “Hour” to select “Hour” mode.

Method Two: Click > beside “Camera Thumbnail” on the left top corner of the interface to select the time slice mode.

Method Three: Right-click the mouse on any area of the time-sliced interface to go back to the upper interface.

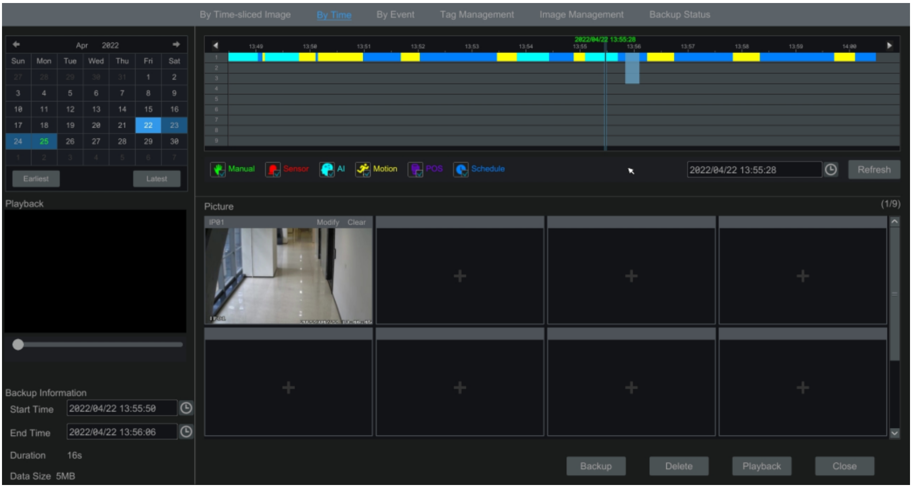
8.4.2 Search, Playback & Backup by Time

① Click ***Start→Search and Backup→By Time*** to go to “By Time” tab as shown below.

② Click + on the bottom of the interface to add playback camera. A maximum of 16 cameras can be added for playback. Click “Modify” on the top right corner of the camera window to change the camera and click “Clear” to remove the camera.

③ Click the camera window to play the recording in the small playback box on the left side of the interface. You can set the date on the top left of the interface, check the event type as needed and click the time scale or click 🕒 under the time scale to set the time. The camera window will play the recording according to the time and event type you set.

④ Drag the color blocks on the time scale to select the record data (or click “Set Backup Time” on the bottom left corner of the interface to set the backup start time and end time) and then click “Backup” for record backup. Click “Playback” to play the recording in the playback interface. Click “Delete” to delete the selected record file.



By Time-sliced Image | By Time | By Event | Tag Management | Image Management | Backup Status

Backup Information
Start Time 2022/04/22 13:55:50
End Time 2022/04/22 13:56:06
Duration 16s
Data Size 5MB

Picture (1/9)

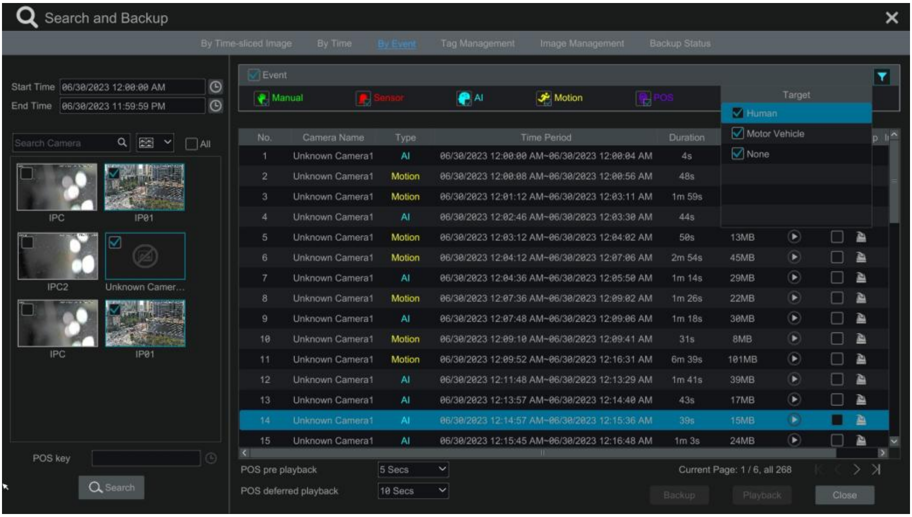
2022/04/22 13:55:28 Refresh

Backup | Delete | Playback | Close

8.4.3 Search, Playback & Backup by Event

Some models may support searching POS event.

① Click ***Start→Search and Backup→By Event*** to go to “By Event” tab as shown below.



Search and Backup

By Time-sliced Image | By Time | By Event | Tag Management | Image Management | Backup Status

Start Time 06/30/2023 12:00:00 AM
End Time 06/30/2023 11:59:59 PM

☑ Event: Manual, Sensor, AI, Motion, POS

Target: ☑ Human ☑ Motor Vehicle ☑ None

No.	Camera Name	Type	Time Period	Duration	
1	Unknown Camera1	AI	06/30/2023 12:00:00 AM~06/30/2023 12:00:04 AM	4s	
2	Unknown Camera1	Motion	06/30/2023 12:00:08 AM~06/30/2023 12:00:56 AM	48s	
3	Unknown Camera1	Motion	06/30/2023 12:01:12 AM~06/30/2023 12:03:11 AM	1m 59s	
4	Unknown Camera1	AI	06/30/2023 12:02:46 AM~06/30/2023 12:03:30 AM	44s	
5	Unknown Camera1	Motion	06/30/2023 12:03:12 AM~06/30/2023 12:04:02 AM	50s	13MB
6	Unknown Camera1	Motion	06/30/2023 12:04:12 AM~06/30/2023 12:07:06 AM	2m 54s	45MB
7	Unknown Camera1	AI	06/30/2023 12:04:36 AM~06/30/2023 12:05:50 AM	1m 14s	29MB
8	Unknown Camera1	Motion	06/30/2023 12:07:36 AM~06/30/2023 12:09:02 AM	1m 26s	22MB
9	Unknown Camera1	AI	06/30/2023 12:07:48 AM~06/30/2023 12:09:06 AM	1m 18s	30MB
10	Unknown Camera1	Motion	06/30/2023 12:09:10 AM~06/30/2023 12:09:41 AM	31s	8MB
11	Unknown Camera1	Motion	06/30/2023 12:09:52 AM~06/30/2023 12:16:31 AM	6m 39s	101MB
12	Unknown Camera1	AI	06/30/2023 12:11:48 AM~06/30/2023 12:13:29 AM	1m 41s	39MB
13	Unknown Camera1	AI	06/30/2023 12:13:57 AM~06/30/2023 12:14:40 AM	43s	17MB
14	Unknown Camera1	AI	06/30/2023 12:14:57 AM~06/30/2023 12:15:36 AM	39s	15MB
15	Unknown Camera1	AI	06/30/2023 12:15:45 AM~06/30/2023 12:16:48 AM	1m 3s	24MB

POS pre playback 5 Secs
POS deferred playback 10 Secs
Current Page: 1 / 6, all 268

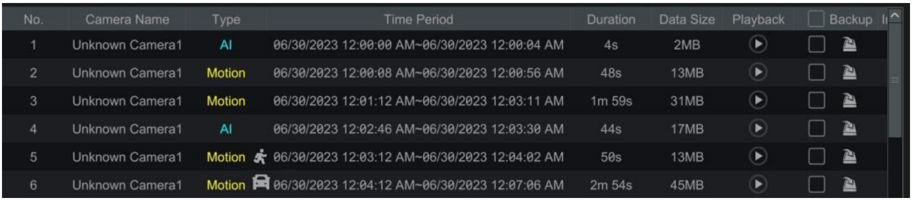
Backup | Playback | Close

② Check the event type in the interface as required.

③ Click 🕒 to set the start time and end time on the top left of the interface. Click ▼

to filter targets. Select “Human” or “Motor Vehicle” to show motion (human) or (motor vehicle) as shown below. If “None” is selected, all events will be searched except motion (human) or (motor vehicle).

Note: Only the camera with SMD function has the data of motion (human/vehicle classification).



No.	Camera Name	Type	Time Period	Duration	Data Size	Playback	□ Backup
1	Unknown Camera1	AI	06/30/2023 12:00:00 AM~06/30/2023 12:00:04 AM	4s	2MB	▶	□
2	Unknown Camera1	Motion	06/30/2023 12:00:08 AM~06/30/2023 12:00:56 AM	48s	13MB	▶	□
3	Unknown Camera1	Motion	06/30/2023 12:01:12 AM~06/30/2023 12:03:11 AM	1m 59s	31MB	▶	□
4	Unknown Camera1	AI	06/30/2023 12:02:46 AM~06/30/2023 12:03:30 AM	44s	17MB	▶	□
5	Unknown Camera1	Motion	06/30/2023 12:03:12 AM~06/30/2023 12:04:02 AM	50s	13MB	▶	□
6	Unknown Camera1	Motion	06/30/2023 12:04:12 AM~06/30/2023 12:07:06 AM	2m 54s	45MB	▶	□

④ Check cameras on the left side of the interface or check “All” to select all the cameras and then click 🔍 Search to search the record. The searched record will be displayed in the list.

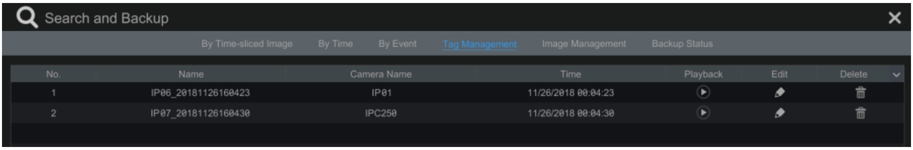
⑤ Click ▶ in the list to play back the record in the popup window. Click to back up one record data or check multiple record data in the list and then click “Backup” for record batch backup.

⑥ Select one record data in the list and then click “Playback” to play the record in the playback interface.

8.4.4 Search & Playback by Tag

Only if you add the tags can you play the record by tag search. Click ***Start→Playback*** to go to the playback interface and then click ★ on the bottom of the camera window to add tag when you want to mark the playback time point of the selected camera.

Click ***Start→Search and Backup→Tag Management*** to go to “Tag Management” tab.

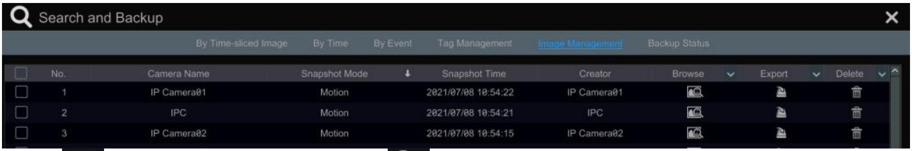


No.	Name	Camera Name	Time	Playback	Edit	Delete
1	IP06_20181126160423	IP01	11/26/2018 00:04:23	▶	✎	🗑
2	IP07_20181126160430	IPC250	11/26/2018 00:04:30	▶	✎	🗑

Click ▶ in the interface to play the record. Click ✎ to edit the tag name. Click 🗑 to delete the tag.

8.4.5 Image Management

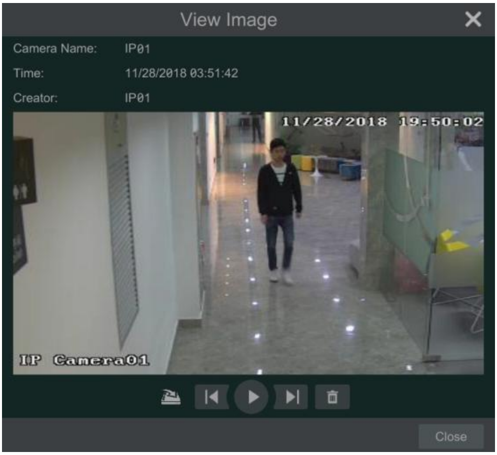
Click ***Start→Search and Backup→Image Management*** to go to “Image Management” tab. The system will display all the snapped images automatically in the list.


Search and Backup

□	No.	Camera Name	Snapshot Mode	Snapshot Time	Creator	Browse	Export	Delete
□	1	IP Camera01	Motion	2021/07/08 10:54:22	IP Camera01			
□	2	IPC	Motion	2021/07/08 10:54:21	IPC			
□	3	IP Camera02	Motion	2021/07/08 10:54:15	IP Camera02			

Click to delete the image. Click to open the “Export” window. Select the device name and save path in the window and then click the “Save” button.

Click to pop up the “View Image” window. Click to export the image. Click to view the previous image; click to view the next image; click to delete the image; click to play all the images.


View Image

Camera Name: IP01

Time: 11/28/2018 03:51:42

Creator: IP01

8.4.6 View Backup Status

Click ***Start→Search and Backup→Backup Status*** or click on the tool bar at the bottom of the playback interface to view the backup status.

9 AI Event Management

9.1 Face Recognition

Only some models support alarm trigger based on face comparison. If your device doesn't support face recognition function, please skip the face database and face recognition instructions.

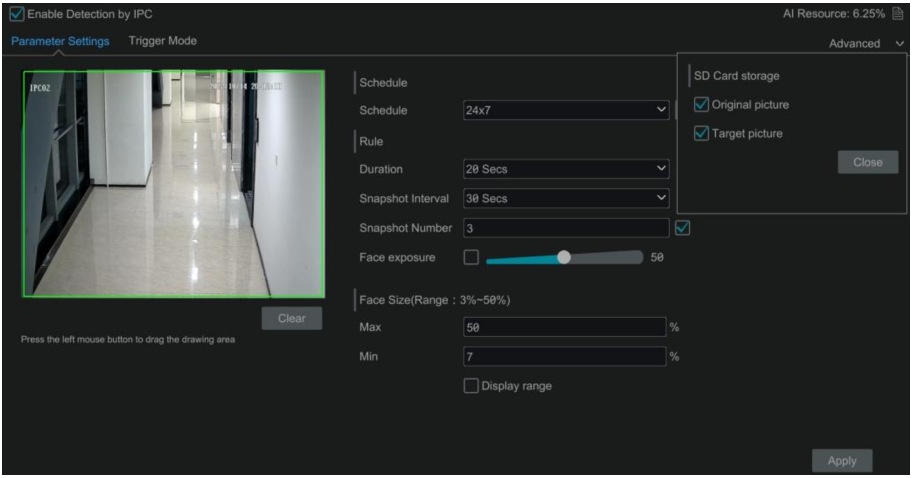
The following are instructions on how to set up the Face Recognition function for the first time:

Set face detection and alarm linkage → Add face group → Add faces to the face group → Enable and set successful recognition (or stranger) → Set successful recognition (or stranger) alarm linkage

9.1.1 Face Detection Settings

Face Detection: Alarms will be triggered if someone intrudes into the pre-defined alarm areas.

① Click ***Start→Settings→AI/Event→AI Event→Face Recognition→ Detection*** to go to the following interface.



☑ Enable Detection by IPC

AI Resource: 6.25%

SD Card storage

☑ Original picture

☑ Target picture

Schedule

Schedule: 24x7

Rule

Duration: 20 Secs

Snapshot Interval: 30 Secs

Snapshot Number: 3 ☑

Face exposure: □ 50

Face Size(Range : 3%~50%)

Max: 50 %

Min: 7 %

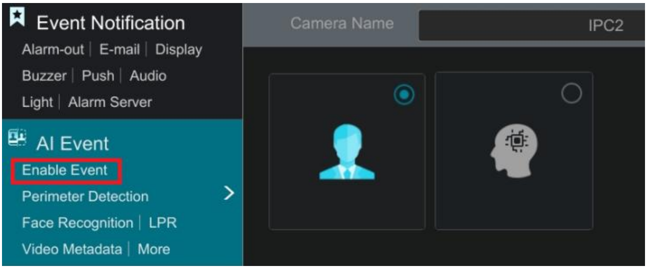
□ Display range

Press the left mouse button to drag the drawing area

② Select the camera, check "Enable Detection by IPC" and set the duration.

Note: 1. Some models may support face detection by NVR. For these models, the camera without AI function also can be added and used to detect faces through NVR. However, if face detection by NVR is enabled for a camera (without AI), people/vehicle perimeter detection cannot be enabled simultaneously, and vice-versa.

2. Some AI cameras support event type classification. If the event type is not face event, you need to select face event by clicking Start→Setting→AI/Event→Enable Event. After the camera restarts, face detection of the IPC can be enabled.



③ Set the schedule. Click "Manage" to set the desired schedule. Please refer to Schedule Settings for details.

④ Set the snapshot interval and snapshot number. The snapshot interval refers to the time interval that the camera captures the same face during its continuous tracking period. The snapshot number refers to the picture number of the same face captured during its continuous tracking period (For example: the snapshot interval is set to "30 seconds" and the snapshot number is set to "3"; then the camera will capture the same face once every 30 seconds and it will capture this face 3 times at most during its continuous tracking period).

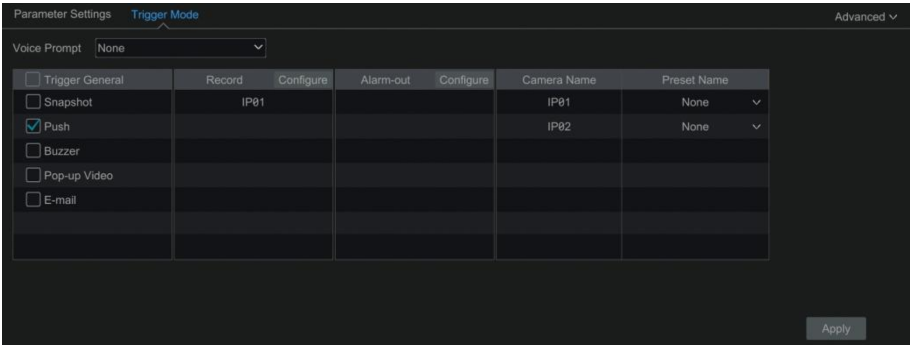
⑤ Enable face match exposure as needed. When the brightness of the captured face is not enough, it can be enabled. (Only some IPCs support this function)

⑥ Set the alarm area. Drag the mouse to draw a detection area. Click "Clear" to delete the alarm area. Then set the detectable face size by defining the maximum value and the minimum value (The default size range of a single face image occupies from 3% to 50% of the entire image).

⑦ Enable "Original picture" or/and "Target picture" as needed. If enabled, the system will automatically save the corresponding images on the SD card.

⑧ Click "Apply" to save the settings.

⑨ Click "Trigger Mode" to go to face detection alarm linkage setting interface:



Voice Prompt: None

☐ Trigger General	Record	Configure	Alarm-out	Configure	Camera Name	Preset Name
☐ Snapshot	IP01				IP01	None
☑ Push					IP02	None
☐ Buzzer						
☐ Pop-up Video						
☐ E-mail						

Face Detection Alarm Linkage Configuration:

- Trigger "Voice Prompt", "Record", "Snapshot", "Push", "Alarm-out", "Preset", "Buzzer", "Pop-up Video" and "E-mail" as needed.

Voice Prompt: Please upload the audio file in local audio alarm interface first (click Start→Settings→AI/Event→Event Notification→Audio). Please see Audio for details.

Record: Click the "Configure" button to open the window. Select a camera on the left side and then click >> to set the camera as the trigger camera. Select a trigger camera on the right side and then click << to cancel the trigger camera. Click "OK" to save the settings. The trigger cameras will record automatically when faces are detected.

Alarm-out: Click the "Configure" button to open the window. Then the "Trigger Alarm-out" window will pop up automatically. Configure the trigger alarm-out in the window. The system will trigger the alarm-out automatically when faces are detected. You need to set the delay time and the schedule of the alarm outputs. See Alarm-out for details.

Preset: Click ⌄ and then select the preset for each camera. To add presets, please see Preset Setting for details.

Snapshot: If it is enabled, the current camera will capture images automatically when faces are detected.

Push: If it is enabled, the system will send messages when faces are detected.

Buzzer: if it is enabled, the system will begin to buzz when faces are detected. To set the delay time of the buzzer, please see Buzzer for details.

Pop-up Video: if it is enabled, the system will open the corresponding video automatically when faces are detected. To set the duration time of the video, please see Display for details.

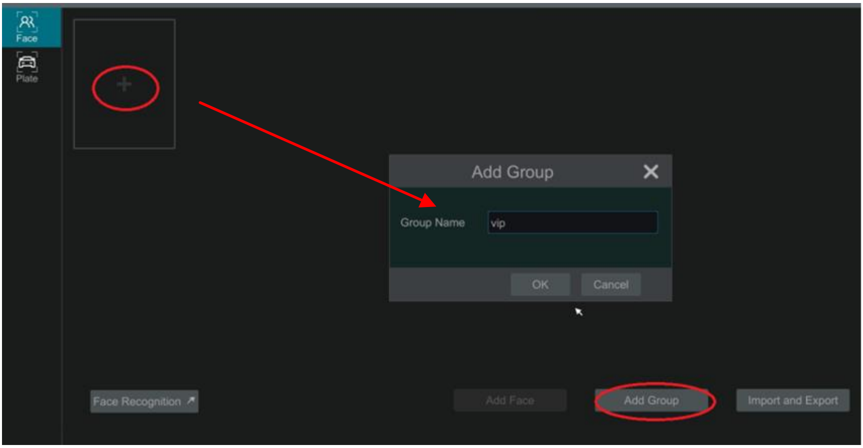
E-mail: if it is enabled, the system will send an e-mail when faces are detected. In the meanwhile, it will attach the captured face picture and the original picture so that you can view the whole scene when the alarm occurs. Before you enable the email, please configure the recipient's e-mail address first (see E-mail Configuration for details).

Enable "IPC_Audio" or "IPC_Light" as needed (only some IPCs support these two functions). To set the IPC voice and its times and volume, please refer to Audio for details. To set the light flashing time and frequency of the IPC, please refer to Light for details.

⑩ Click "Apply" to save the settings.

9.1.2 Face Database Management

① Click ***Start→Settings→AI/Event→AI Event→Face Recognition→Face Database*** to go to the following interface as shown below.

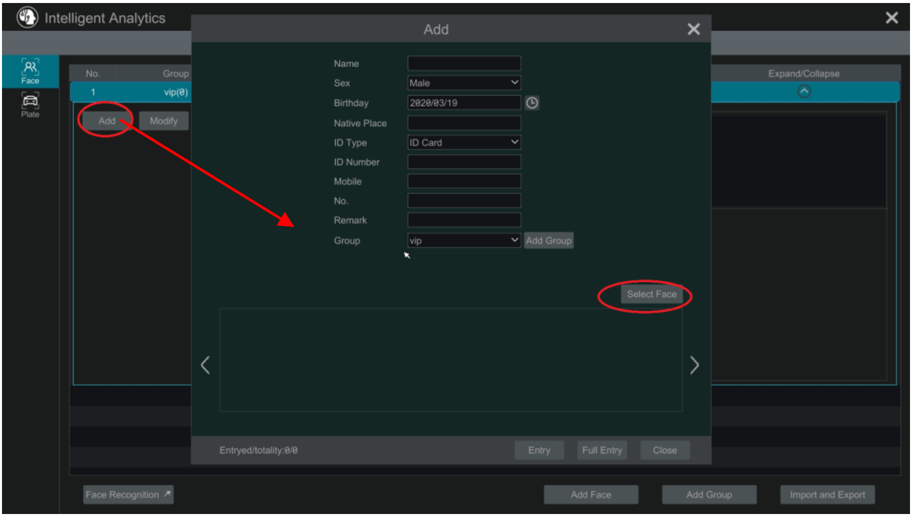


Group Name: vip

For the first time, you can click "+" or "Add Group" to add groups.

② To add targets for each group.

- Select a list and then click ⌄ to expand the list as shown below.



Add

No.	Group
1	vip(0)

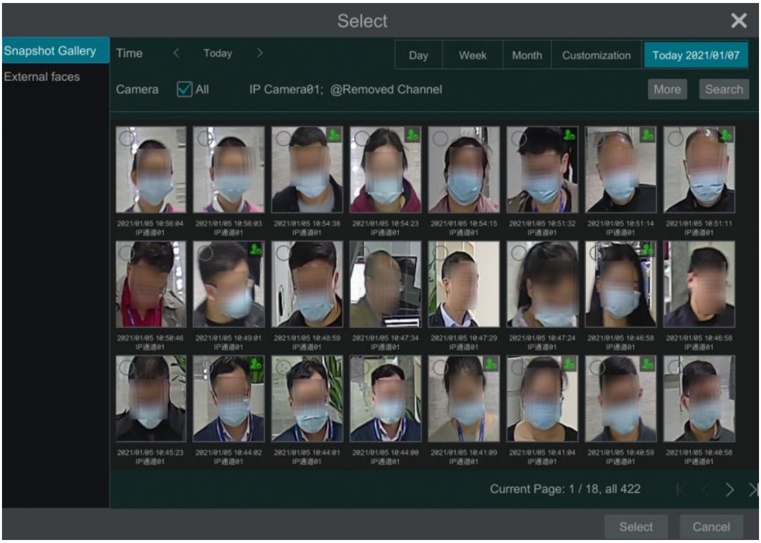
Name:
Sex: Male
Birthday: 2020/03/19
Native Place:
ID Type: ID Card
ID Number:
Mobile:
No.:
Remark:
Group: vip

Entryed/totality:0/0

- Click "Add" and then click "Select Face" to add face images. You can add faces from snapshot gallery or external faces.

  Adding faces from snapshot gallery: Select search time or self define the search time and then click "Search" to search target faces. Then select the desired faces and click "Select".

  Note: The picture marked with a green icon can be added to the face database. Those pictures can’t likely have resolution issues.



Add external faces

Save the face pictures on your USB storage device and then insert the USB storage device into the USB port of the NVR.

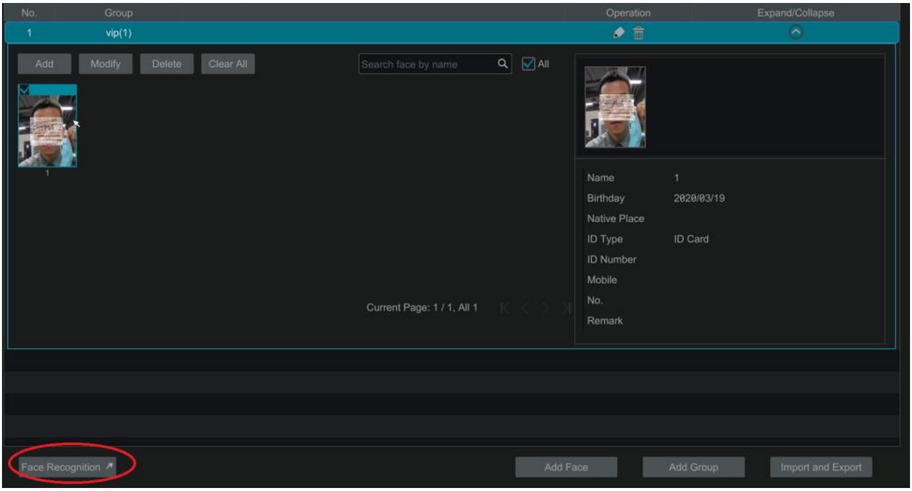
Go to the face database interface. Click to expand the group and then click “Add”. Select “External faces” to select face pictures. You can select one face to add or multiple faces to add.

To add multiple faces: a. put face pictures and the description file (.csv or .txt) to one specific folder (please edit the detailed descriptions of these pictures according to the personal information description); b. click “All” to select all face pictures; c. click “Full Entry”.

Note: the added image must be less than 70KB and the image format shall be “.jpg” and “.jpeg”.

- After that, add the corresponding information, like name, gender, birthday, ID number, phone number and so on.

Having saved the target image, click the image and then the detailed information will be listed on the right.



No.	Group	Operation	Expand/Collapse
1	vip(1)		

Current Page: 1 / 1, All 1

Name 1
Birthday 2020/03/19
Native Place
ID Type ID Card
ID Number
Mobile
No.
Remark

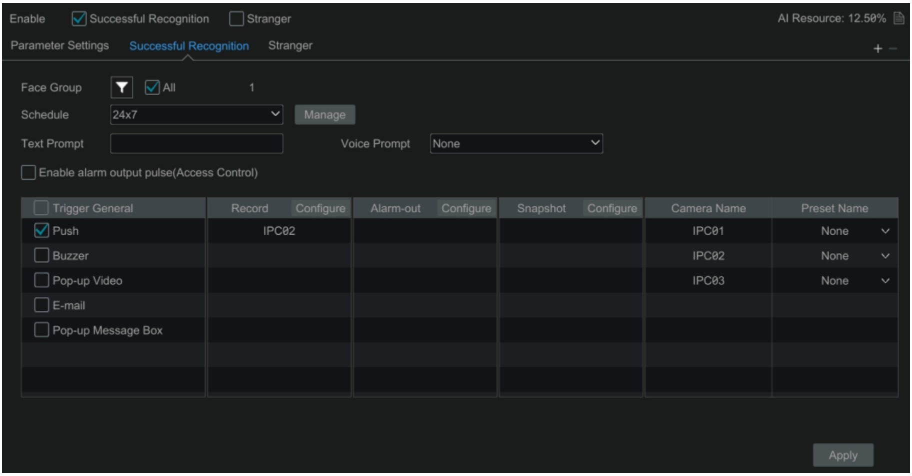
- Import and Export Face database

Insert your mobile storage device into the USB interface of the NVR and then click "Import and Export" to import or export the face database settings.

The exported face database file (cvs+jpg) can be directly imported to the face database to make it very convenient for you to transfer one NVRs face database file to other NVRs.

9.1.3 Face Recognition Settings

After the face database and face pictures are added, click "Face Recognition" to return to the face recognition setting interface. Click the "Recognition" tab to go to the following interface.



Enable ☑ Successful Recognition □ Stranger

AI Resource: 12.50%

Face Group ☑ All 1

Schedule 24x7

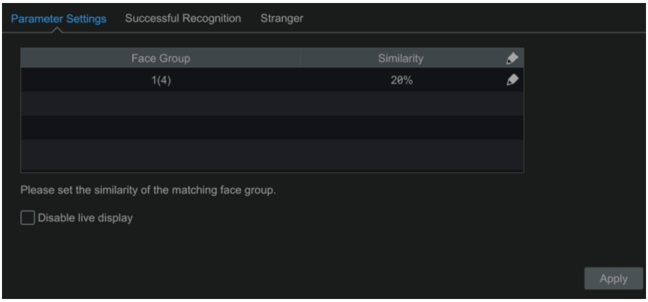
Text Prompt

Voice Prompt None

□ Enable alarm output pulse(Access Control)

□ Trigger General	Record	Configure	Alarm-out	Configure	Snapshot	Configure	Camera Name	Preset Name
☑ Push	IPC02						IPC01	None
□ Buzzer							IPC02	None
□ Pop-up Video							IPC03	None
□ E-mail								
□ Pop-up Message Box								

① Enable "Successful Recognition" or "Stranger". Click "Parameter Settings" to set the similarity of the matching face group.



Face Group	Similarity
1(4)	20%

Please set the similarity of the matching face group.

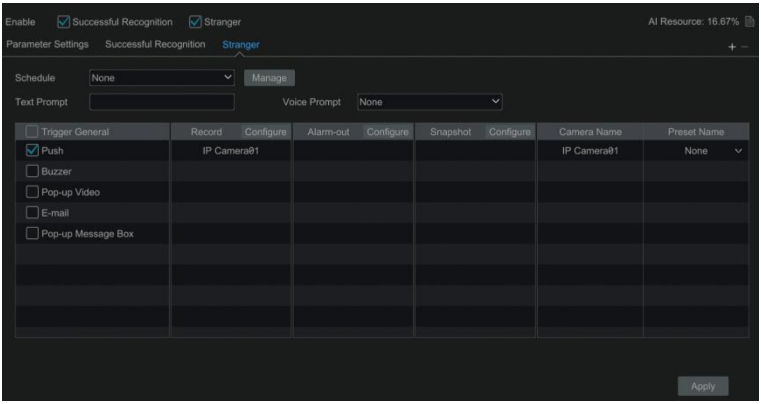
□ Disable live display

Disable live display: if checked, the live view interface (target detection tab) will not display captured faces in real time.

② Set the alarm linkage items for successful recognition.

- Select one or more face groups and then choose the schedule. Click "Manage" to set the schedule.
- Set the text prompt and voice prompt. When the captured face is matched successfully, the text will appear on the right of the live view interface and broadcast the audio.
- Enable alarm output pulse (access control).
- Trigger record, snapshot, alarm-out, buzzer, push, pop-up video, E-mail and pop-up message box as needed. The alarm linkage settings are similar to the face detection alarm (see Face Detection Settings for details).
- Click "Apply" to save the settings.

③ Set the stranger alarm linkage items. When the captured face picture doesn't match the face pictures in the face database or their similarity is lower than the set value, the captured person will be regarded as a stranger.


Enable ☑ Successful Recognition ☑ Stranger

AI Resource: 16.67%

Schedule: None

Text Prompt:

Voice Prompt: None

□ Trigger General	Record	Configure	Alarm-out	Configure	Snapshot	Configure	Camera Name	Preset Name
☑ Push	IP Camera01						IP Camera01	None
□ Buzzer								
□ Pop-up Video								
□ E-mail								
□ Pop-up Message Box								

- Configure the schedule
- Set the text prompt and voice prompt. The text will show on the captured picture and the voice will be broadcasted when detecting a stranger.
- Trigger record, snapshot, alarm-out, buzzer, push, pop-up video, E-mail, Preset and pop-up message box as needed. The alarm linkage settings are similar to the face detection alarm (See Face Detection Settings for details).
- Click “Apply” to save the settings.

④ Click “+” to add more successful recognition tasks. Select the added task and then click “–” to delete it.

9.2 License Plate Recognition

Please add an ANPR camera before you using this function. If your camera doesn’t support this function, please skip the following instructions.

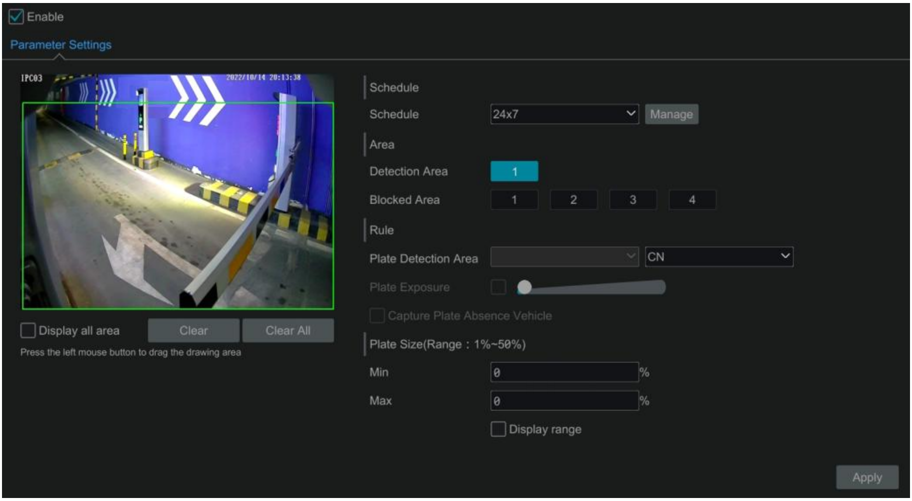
When setting up an LPR for the first time, please use the following procedures:

Enable and set plate detection → Add plate group → Add plates to the plate group →

Enable license plate recognition → Set successful recognition (or strange plate) alarm linkage

9.2.1 License Plate Detection Settings

Click ***Start→AI/Event→AI Event→LPR*** to go to the following interface. Select an ANPR camera and click the “Detection” tab as shown below.



☑ Enable

Parameter Settings

□ Display all area

Press the left mouse button to drag the drawing area

Schedule

Schedule 24x7

Area

Detection Area 1

Blocked Area 1 2 3 4

Rule

Plate Detection Area CN

Plate Exposure □

□ Capture Plate Absence Vehicle

Plate Size(Range : 1%~50%)

Min 0 %

Max 0 %

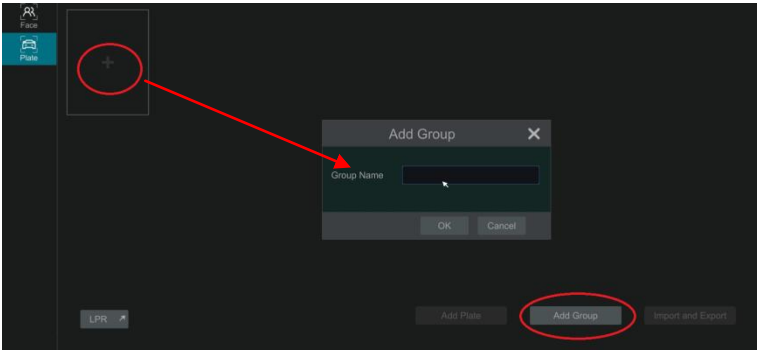
□ Display range

- Set the schedule.
- Set the area and plate exposure as needed.
  Set the alarm area. Drag the mouse to draw a detection area. Click “Clear” to delete the alarm area.
  Set the blocked area. Select the number and then draw a blocked area. Up to 4 areas can be set up. After you set the blocked area, this area will not be detected.
  Click “Display all area” to view all blocked and detection areas.
  Click “Clear All” to clear all blocked and detection areas.
- Check “Capture plate absence vehicle” as needed.
- Set the plate size by defining the maximum value and the minimum value (The default size range of a single plate occupies from 5% to 50% of the entire image).
- Display range: if enabled, the set maximum detection box and the minimum detection box can be displayed on the left window.
- Click “Advanced” to set the recognition mode as needed (only some LPR cameras support).

9.2.2 Plate Database Management

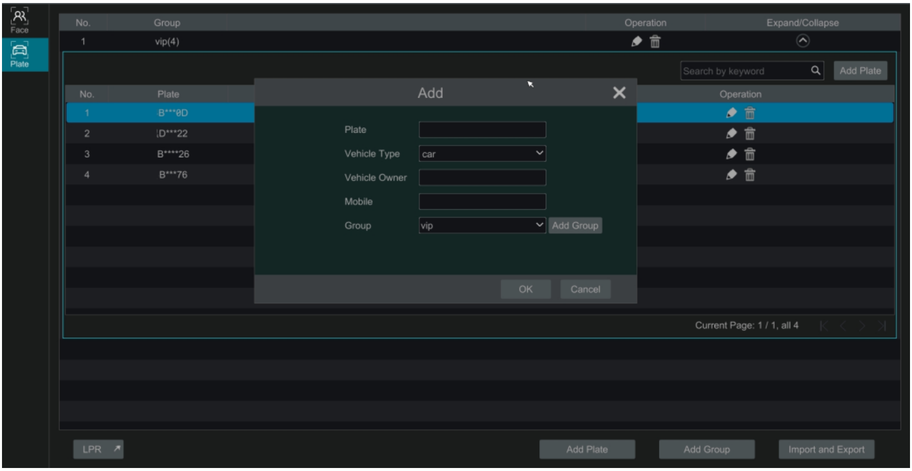
In the LPR interface, click the “Plate Database” tab to go to the plate database management interface as shown below.

For the first time, you can click “+” or “Add Group” to add groups.



Add plates to each group:

① Click ⌄ to extend the group. Click “Add Plate” to display the following window.



Face | Plate

No.	Group	Operation	Expand/Collapse
1	vip(4)	✎ 🗑	⌃

Search by keyword | Add Plate

No.	Plate	Operation
1	B***0D	✎ 🗑
2	D***22	✎ 🗑
3	B****26	✎ 🗑
4	B***76	✎ 🗑

Add

Plate:

Vehicle Type: car

Vehicle Owner:

Mobile:

Group: vip | Add Group

OK | Cancel

Current Page: 1 / 1, all 4

LPR | Add Plate | Add Group | Import and Export

② Enter the plate, vehicle owner and mobile phone number.

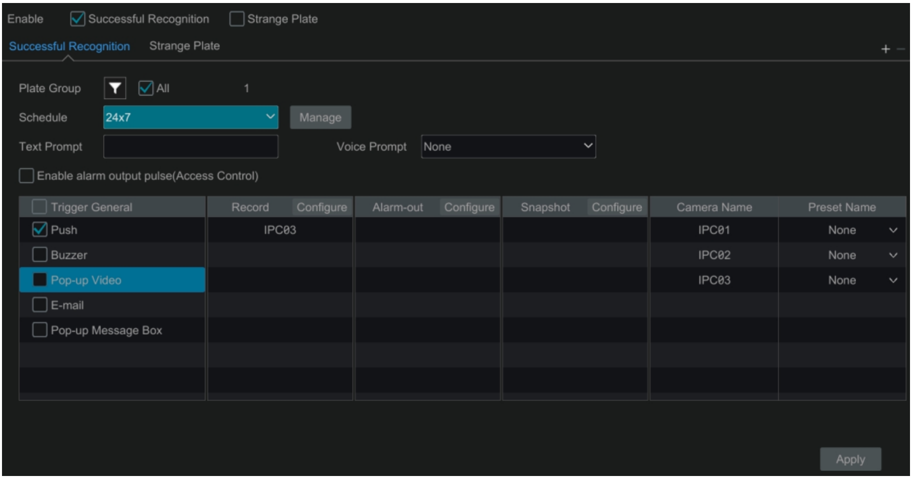
③ Select the vehicle type and group.

④ Finally, click “OK” to complete.

Select the added plate and then click ✎ to modify its information; click 🗑 to delete this plate. The plates can be imported and exported in bulk by clicking “Import and Export”. You can click “Plate Information Description” to view the detailed information about how to import or export the plate list.

9.2.3 License Plate Recognition Settings

① In the LPR interface, click the “Recognition” tab. Then enable “Successful Recognition” or “Strange Plate”.



Enable ☑ Successful Recognition ☐ Strange Plate

Successful Recognition | Strange Plate

Plate Group ☑ All 1

Schedule: 24x7 | Manage

Text Prompt:

Voice Prompt: None

☐ Enable alarm output pulse(Access Control)

☐ Trigger General	Record	Configure	Alarm-out	Configure	Snapshot	Configure	Camera Name	Preset Name
☑ Push	IPC03						IPC01	None
☐ Buzzer							IPC02	None
☐ Pop-up Video							IPC03	None
☐ E-mail								
☐ Pop-up Message Box								

Apply

② Set the successful recognition alarm linkage.

- Select one or more plate groups and then choose the schedule. Click “Manage” to set the schedule.
- Set the text prompt. When the captured plate is matched successfully, the text will appear on the right of the live view interface.
- Enable alarm output pulse (access control).
- Trigger record, snapshot, alarm-out, buzzer, push, pop-up video, E-mail and pop-up message box as needed. The alarm linkage settings are similar to the face detection alarm (See Face Detection Settings for details).

③ Set the strange plate alarm linkage. When the captured plate picture doesn’t match the plates in the plate database or their similarity is lower than the set value, the captured plate will be regarded as a strange plate.

9.3 Perimeter Detection

Note:

1. Some models may support perimeter detection (line crossing, region intrusion/entrance/exiting) by NVR. For these models, the camera without AI function also can be added and used to detect line crossing, region intrusion, region entrance and region exiting events through NVR. However, if perimeter detection by NVR is enabled for a camera (without AI), face detection cannot be enabled simultaneously, and vice-versa.

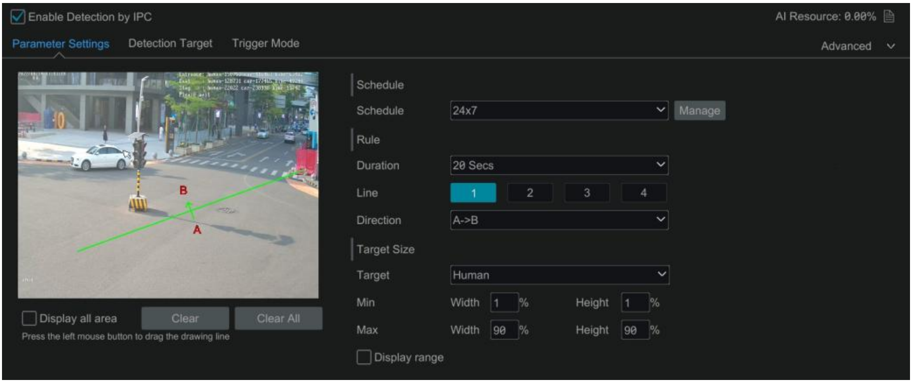
2. Some AI cameras support event type classification. If the event type is face event, you need to select by clicking Start→Setting→AI/Event→Enable Event. After the camera restarts, perimeter detection of the IPC can be enabled.

9.3.1 Line Crossing Detection

Tripwire/Line Crossing Detection Configuration:

Alarms will be triggered if the people or vehicles cross the pre-defined alarm line.

① Click ***Start→Settings→AI/Event→AI Event →Perimeter Detection→Line Crossing*** to go to the following interface.



☑ Enable Detection by IPC

AI Resource: 0.00%

Schedule

Schedule: 24x7

Rule

Duration: 20 Secs

Direction: A->B

Target Size

Target: Human

Min Width 1 % Height 1 %

Max Width 90 % Height 90 %

□ Display range

□ Display all area

Press the left mouse button to drag the drawing line

② Select the camera, enable line crossing detection by IPC and set the duration.

Note: Some models may support line crossing detection by NVR.

③ Set the schedule.

④ Select the direction.

Direction: A<->B, A->B and A<-B optional. It is the crossing direction of the target that crosses over the alert line.

A<->B: the alarm triggers when the target crosses over the alert line from B to A or from A to B.

A->B: the alarm triggers when the target crosses over the alert line from A to B.

A<-B: the alarm triggers when the target crosses over the alert line from B to A.

⑤ Draw line. Refer to the interface as shown above. Drag the mouse in the image to draw an alert line. Click the "Clear" to delete the alert line.

⑥ Set target size. Check "Display range" and then select target. Enter the width and height value to set the size; click the set min./max. box and then four dots will be shown at the four corners of the min./max. box. Now, drag one of the four lines of the min./max to change its position. Note that only some IPCs support target size settings. If the added camera doesn't support this function, please skip this step.

⑦ Click "Detection Target" to choose the detection target and the sensitivity. The detection target includes human, motor vehicle and non-motor vehicle. Only some IPCs can detect human or vehicle separately. If the camera doesn't support this function, please skip this step.

⑧ Click "Advanced" to choose "Save original picture" or "Save target picture" on the SD card of the camera. (If your camera doesn't support this function, please skip this step).

⑨ Click "Trigger Mode" to configure line crossing alarm linkage items.

● Enable or disable "Record", "Snapshot", "Push", "Alarm-out", "Preset", "Buzzer", "Pop-up Video" and "E-mail". The alarm linkage settings are the same as the face detection alarm (see 9.1.1 Face Detection Settings for details).

● Enable "IPC_Audio" or "IPC_Light" as needed (only some IPCs support these two functions). To set the IPC voice and its times and volume, please refer to Audio for details. To set the light flashing time and frequency of the IPC, please refer to Light for details.

⑩ Click “Apply” to save the settings.

9.3.2 Region Intrusion Detection

Region Intrusion Detection Configuration:

Alarms will be triggered if the people or vehicles intrude into the pre-defined area.

① Click ***Start→Settings→AI/Event →AI Event→Perimeter Detection→Region Intrusion*** to go to the following interface.

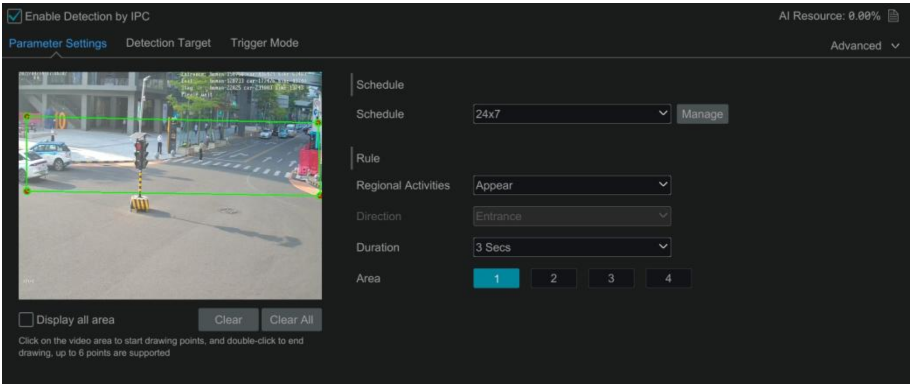
② Select the camera, enable region intrusion detection by IPC and set the duration.

Note: Some models may support region intrusion detection by NVR.

③ Set the schedule.

④ Select the alarm area. Up to 4 alarm areas can be set up.

⑤ Draw the alarm area of region intrusion detection. Refer to the interface as shown below. Click around the area where you want to set as the alarm area in the image (the alarm area should be a closed area).



Schedule

Schedule: 24x7

Rule

Regional Activities: Appear

Direction: Entrance

Duration: 3 Secs

Area: 1 2 3 4

Click on the video area to start drawing points, and double-click to end drawing, up to 6 points are supported

⑥ Set target size. Please refer to the target size setup of line crossing for details. Note that only some IPCs support target size settings. If the added camera doesn’t support this function, please skip this step.

⑦ Click “Detection Target” to choose the detection target and the sensitivity. The detection target includes human, motor vehicle and non-motor vehicle.

⑧ Click “Trigger Mode” to configure intrusion detection alarm linkage items.

- Enable or disable “Record”, “Snapshot”, “Push”, “Alarm-out”, “Preset”, “Buzzer”, “Pop-up Video” and “E-mail”. The alarm linkage settings are the same as the face detection alarm (see Face Detection Settings for details).
- Enable “IPC_Audio” or “IPC_Light” as needed. (only some IPCs support these two functions). To set the IPC voice and its times and volume, please refer to Audio for details. To set the light flashing time and frequency of the IPC, please refer to Light for details.

⑨ Click “Copy To” to copy all settings to other cameras.

⑩ Click “Apply” to save the settings.

9.3.3 Region Entrance Detection

Region Entrance: Alarms will be triggered if the target enters the pre-defined areas.

Click ***Start→Settings→AI/Event→AI Event →Perimeter Detection→Region Entrance.*** The setup steps are the same as Region Intrusion. See Region Intrusion Detection for details.

9.3.4 Region Exiting Detection

Region Exiting: Alarms will be triggered if the target exits from the pre-defined areas.

Click ***Start→Settings→AI/Event→AI Event →Perimeter Detection→Region Exiting.*** The setup steps are the same as Region Intrusion. See Region Intrusion Detection for details.

9.4 Abandoned/Missing Object Detection

① Click ***Start→Settings→AI/Event→AI Event→ More→ Object Abandoned/Missing*** to go to the following interface.

② Set the schedule.

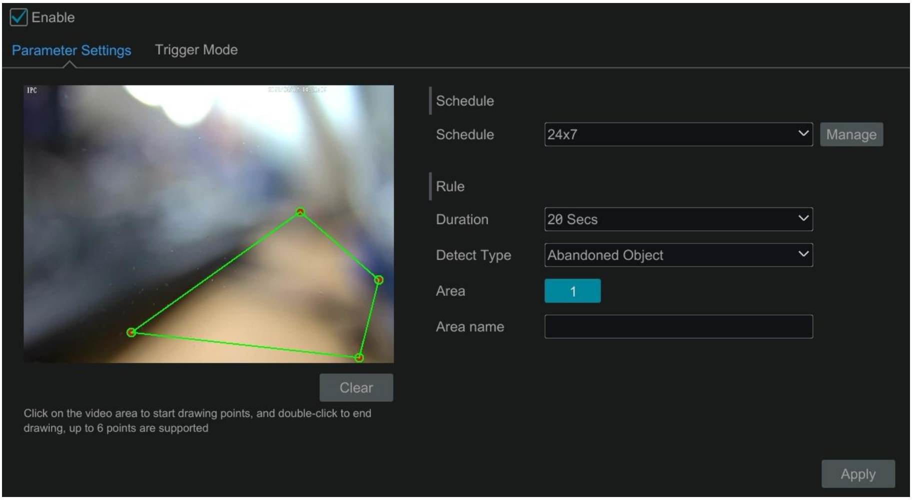
③ Select the camera, enable the object detection and set the duration and detect type. There are two detection types: Abandoned object and missing object.

Abandoned object: Alarms will be triggered if there are articles left in the pre-defined detection area.

Missing object: Alarms will be triggered if there are articles missing in the detection area drew by the users.

④ Select the alarm area and area name. A maximum of 4 alarm areas can be set.

⑤ Draw the alarm area of the object detection. Refer to the interface as shown below. Click around the area where you want to set as the alarm area in the image (the alarm area should be a closed area). Click the “Clear” to delete the alarm area.



☑ Enable

Click on the video area to start drawing points, and double-click to end drawing, up to 6 points are supported

Schedule

Schedule: 24x7

Rule

Duration: 20 Secs

Detect Type: Abandoned Object

Area: 1

Area name:

⑥ Click "Trigger Mode" to configure abandoned/missing object detection alarm linkage items. Enable or disable "Record", "Snapshot", "Push", "Alarm-out", "Preset", "Buzzer", "Pop-up Video" and "E-mail". The alarm linkage settings are the same as the face detection alarm (see Face Detection Settings for details).

⑦ Click "Apply" to save the settings.

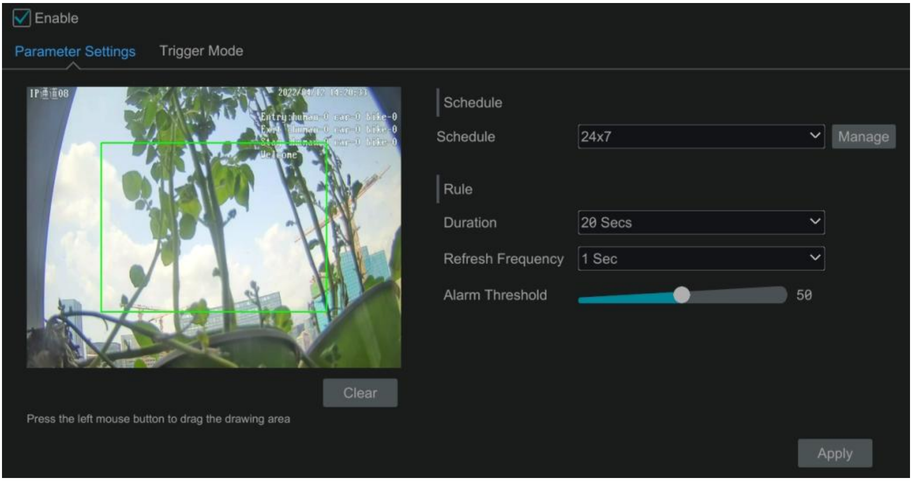
9.5 Crowd Density Detection

Only some IPCs may support this function.

Crowd Density Configuration:

Alarms will be triggered if the crowd density exceeds the set threshold value in the pre-defined area.

① Click ***Start→Settings→AI/Event→AI Event→More→Crowd Density*** to go to the following interface.



☑ Enable

Parameter Settings　Trigger Mode

Schedule

Schedule: 24x7 　Manage

Rule

Duration: 20 Secs

Refresh Frequency: 1 Sec

Alarm Threshold: 50

Clear

Press the left mouse button to drag the drawing area

Apply

② Select the camera, enable crowd density detection and set the schedule, duration, refresh frequency and alarm threshold.

Refresh Frequency: Refers to the refresh time of the detection result report.

Alarm Threshold: Alarms will be triggered once the percentage of the crowd density in a specified area exceeds the pre-defined threshold value.

③ Select the alarm area. Draw the alarm area for the crowd density detection. Refer to the interface as shown above. Drag the mouse to draw a rectangle area. Click the “Clear” to delete the alarm area.

④ Click to configure crowd density detection alarm linkage items. Enable or disable “Record”, “Snapshot”, “Push”, “Alarm-out”, “Preset”, “Buzzer”, “Pop-up Video” and “E-mail”. The alarm linkage settings are the same as the face detection alarm (see Face Detection Settings for details).

⑤ Click “Apply” to save the settings.

9.6 Target Counting

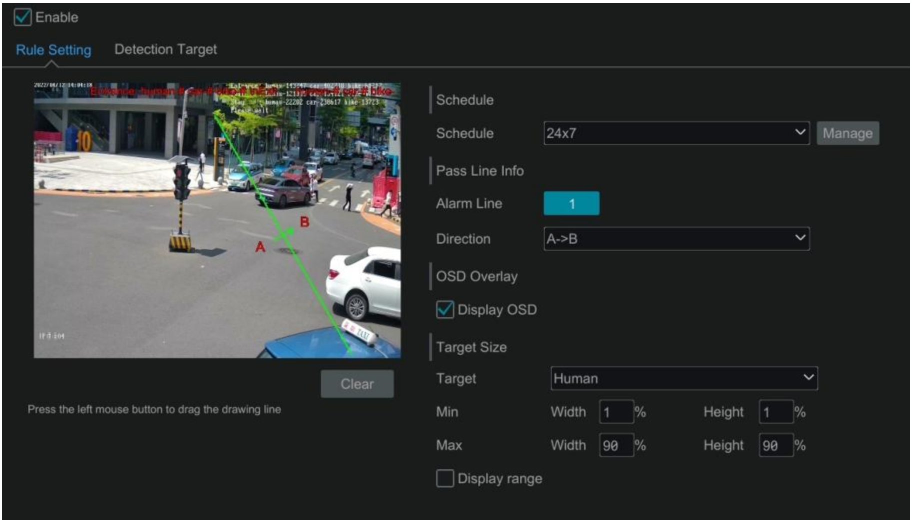
Only some IPCs may support this function.

- **Human/Motor Vehicle/Non-Motor Vehicle Counting**

The information of human/motor vehicle/non-motor vehicle can be calculated and sent by day, by week and by month, so that you can receive and analyze these statistics on time.

Only some IPCs support this function. If your camera doesn’t support this function, please skip the following instructions.

① Click ***Start→Settings→AI/Event→AI Event→More→Target Counting*** to go to the following interface.



☑ Enable

Rule Setting   Detection Target

Clear

Press the left mouse button to drag the drawing line

Schedule

Schedule: 24x7 Manage

Pass Line Info

Alarm Line: 1

Direction: A->B

OSD Overlay

☑ Display OSD

Target Size

Target: Human

Min Width 1 % Height 1 %

Max Width 90 % Height 90 %

□ Display range

② Enable line crossing counting.

③ Set the schedule.

④ Drag the mouse on the small window to draw the crossing line. Click “Clear” to delete the alert line.

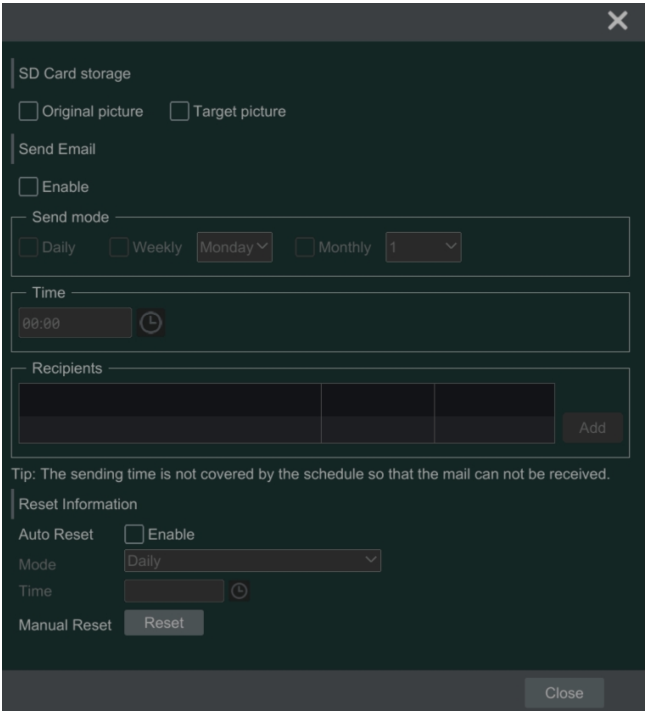
Direction: A->B and A<-B are optional. It is the crossing direction of the target that crosses over the alert line.

⑤ Check “Display OSD”, the statistical information will be displayed on the live view interface.

⑥ Set target size. Please refer to the target size setup of line crossing for details. Note that only some IPCs support target size settings. If the added camera doesn’t support this function, please skip this step.

⑦Click the “Detection Target” tab to set the detection target, including human, motor vehicle and non-motor vehicle.

⑧ Click “Advanced” to open the following window. You can select “Save original picture” or “Save target picture”, and set reset information manually or enable “Auto Reset” as needed.



SD Card storage

□ Original picture □ Target picture

Send Email

□ Enable

Send mode

□ Daily □ Weekly Monday □ Monthly 1

Time

00:00

Recipients

Tip: The sending time is not covered by the schedule so that the mail can not be received.

Reset Information

Auto Reset □ Enable

Mode Daily

Time

Manual Reset

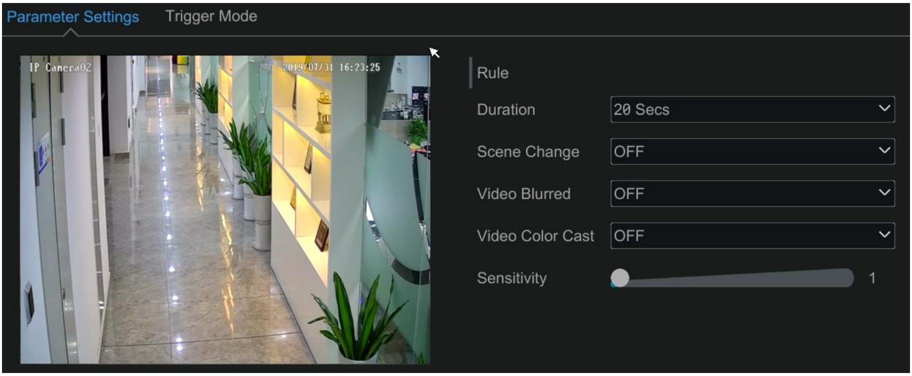
In the above interface, you can send Email to a specified person on a daily/weekly/monthly basis regarding the target counting. Click “Add” to add the recipient”, and then enable “Send Email” and select “Send mode” and time.

⑨ Click “Apply” to save the settings.

9.7 Exception Detection

Exception Detection Configuration:

① Click ***Start→Settings→AI/Event→AI Event→More→Exception Detection*** to go to the following interface.



Rule

Duration: 20 Secs

Scene Change: OFF

Video Blurred: OFF

Video Color Cast: OFF

Sensitivity: 1

② Select the camera and detection duration and then enable the relevant detection as needed.

Scene Change: Alarms will be triggered if the scene of the monitor video has changed.

Video Blurred: Alarms will be triggered if the video becomes blurry.

Video Color Cast: Alarms will be triggered if the image is abnormal caused by color deviation.

③ Set the sensitivity of the exception detection.

④ Click "Trigger Mode" to configure exception alarm linkage items. Enable or disable "Record", "Snapshot", "Push", "Alarm-out", "Preset", "Buzzer", "Pop-up Video", and "E-mail". The alarm linkage settings are the same as sensor alarm (see Face Detection Settings for details).

⑤ Click "Apply" to save the settings.

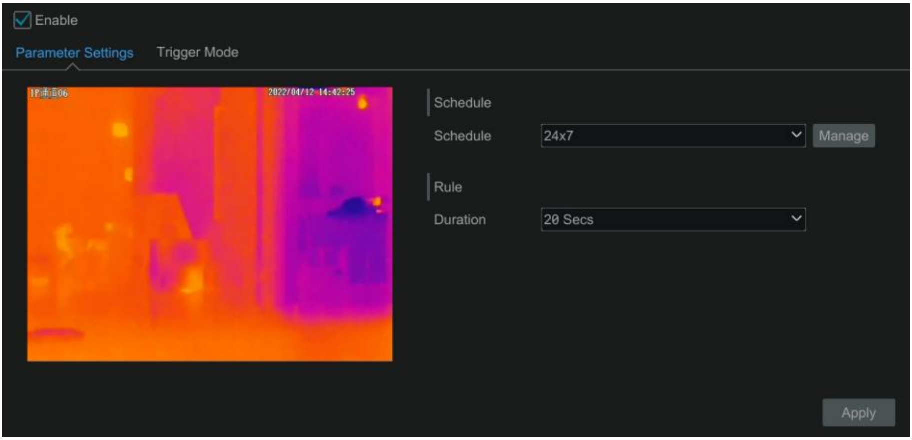
9.8 Fire Detection

Only when the security thermal cameras are connected, can the fire detection be available.

Please note this is only intended as a supplement to official fire detection methods and should not be relied on as a primary alert source.

Fire Detection: Alarms will be triggered when the camera detects a fire source through the thermal imaging.

① Click ***Start→Settings→AI/Event→AI Event→More→Fire Detection*** to go to the following interface.



☑ Enable

Parameter Settings Trigger Mode

Schedule

Schedule 24x7 Manage

Rule

Duration 20 Secs

Apply

② Set the schedule and the alarm duration time.

③ Click “Trigger Mode” to configure alarm linkage items. Enable or disable “Record”, “Snapshot”, “Push”, “Alarm-out”, “Preset”, “Buzzer”, “Pop-up Video”, and “E-mail”. The alarm linkage settings are the same as sensor alarm (see Face Detection Settings for details).

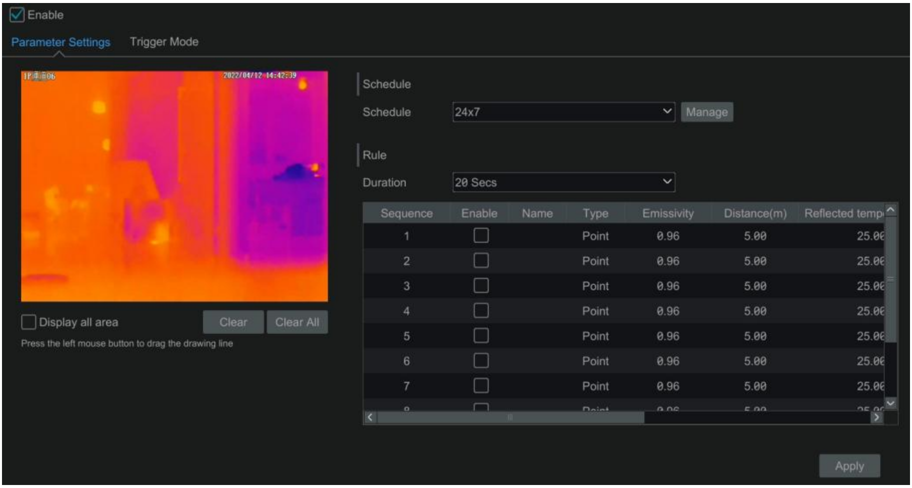
④ Click “Apply” to save the settings.

9.9 Temperature Detection

Only when the security thermal cameras are connected, can the temperature detection be available.

Temperature Measurement: When a temperature of the pre-defined point/line/area exceeds the temperature threshold value, alarms will be triggered.

① Click ***Start→Settings→AI/Event→AI Event→More→Temperature Detection*** to go to the following interface.



☑ Enable

Parameter Settings Trigger Mode

Schedule

Schedule: 24x7 Manage

Rule

Duration: 20 Secs

Sequence	Enable	Name	Type	Emissivity	Distance(m)	Reflected temp
1	□		Point	0.96	5.00	25.0
2	□		Point	0.96	5.00	25.0
3	□		Point	0.96	5.00	25.0
4	□		Point	0.96	5.00	25.0
5	□		Point	0.96	5.00	25.0
6	□		Point	0.96	5.00	25.0
7	□		Point	0.96	5.00	25.0
8	□		Point	0.96	5.00	25.0

□ Display all area Clear Clear All

Press the left mouse button to drag the drawing line

Apply

② Set the schedule and the alarm duration time.

③ Set thermography rule. Select the rule type, including Point, Line and Area.

Emissivity: Set the emissivity of the target. The emissivity of each object is different.

Distance: The distance between the target and the camera.

Reflected temperature: If there is any object with high emissivity in the scene, set the reflective temperature to correct the ambient temperature. The reflective temperature should be set the same as the temperature of the high emissivity object.

Set the alarm rule, alarm temperature and alarm output. For example, select Alarm Rule as Above (Average Temperature), set the alarm temperature to 100 ℃ and check alarm output. Alarms will be triggered when the average temperature of the target is higher than 100 ℃.

④ Set the point, line or area on the small window.

Point setup: After the type is set to "Point", click on the image to set the point. Up to 10 points can be set in the above interface.

Line setup: After the type is set to "Line", drag the mouse on the image to draw a line. To ensure the accuracy of temperature measurement, it is recommended to set not more than two lines at the same time.

Area setup: Click around the area where you want to set as the alarm area on the image (the alarm area should be a closed area). To ensure the accuracy of temperature measurement, it is recommended to set not more than two areas at the same time.

⑤ Click "Trigger Mode" to configure alarm linkage items. Enable or disable "Record", "Snapshot", "Push", "Alarm-out", "Preset", "Buzzer", "Pop-up Video", and "E-mail". The alarm linkage settings are the same as sensor alarm (see Face Detection Settings for details).

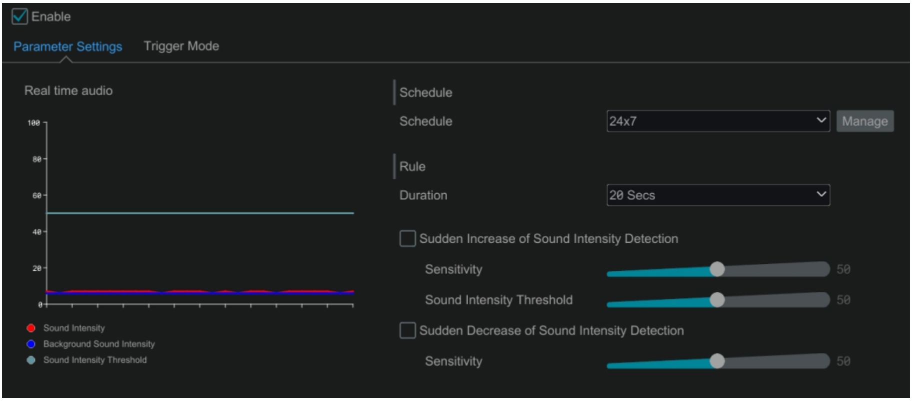
⑥ Click "Apply" to save the settings.

9.10 Audio Exception

Only some IPCs support this function. If the camera you added doesn't support this function, please skip the following instructions.

Audio Exception: Alarms will be triggered when the abnormal sound is detected in the surveillance scene, such as the sudden increase/decrease of the sound intensity.

① Click ***Start→Settings→AI/Event→AI Event→More→ Audio Exception*** to go to the following interface.



☑ Enable

Parameter Settings   Trigger Mode

Real time audio

Schedule

Schedule: 24x7 Manage

Rule

Duration: 20 Secs

□ Sudden Increase of Sound Intensity Detection

Sensitivity: 50

Sound Intensity Threshold: 50

□ Sudden Decrease of Sound Intensity Detection

Sensitivity: 50

② Set the schedule and alarm duration.

Sudden Increase of Sound Intensity Detection: Detect sudden increase of sound intensity. If enabled, sensitivity and sound intensity threshold are configurable. Alarms will be triggered when the detected sound intensity exceeds the sound threshold.

Sensitivity: The higher the value is, the easier the alarm will be triggered.

Sound Intensity Threshold: It is the sound intensity reference for the detection. The lower the value is, the easier the alarm will be triggered. It is recommended to set as the average sound intensity in the environment. The louder the environment sound, the higher the value should be. Please adjust it according to the actual environment condition.

Sudden Decrease of Sound Intensity Detection: Detect sudden decrease of sound intensity. Please set the sensitivity as needed. The higher the value is, the easier the alarm will be triggered.

Real-time audio graphic:

Red wavy line stands for the current detected sound intensity.

Navy blue line stands for the environment (background) sound intensity.

Green line stands for the sound intensity threshold.

In order to reduce false alarm, it is recommended to set the sensitivity and sound intensity threshold according to the real-time audio graphic.

③ Click "Trigger Mode" to configure audio exception alarm linkage items. Enable or disable "Record", "Snapshot", "Push", "Alarm-out", "Preset", "Buzzer", "Pop-up Video", and

"E-mail". The alarm linkage settings are the same as the face detection alarm (see Face Detection Settings for details).

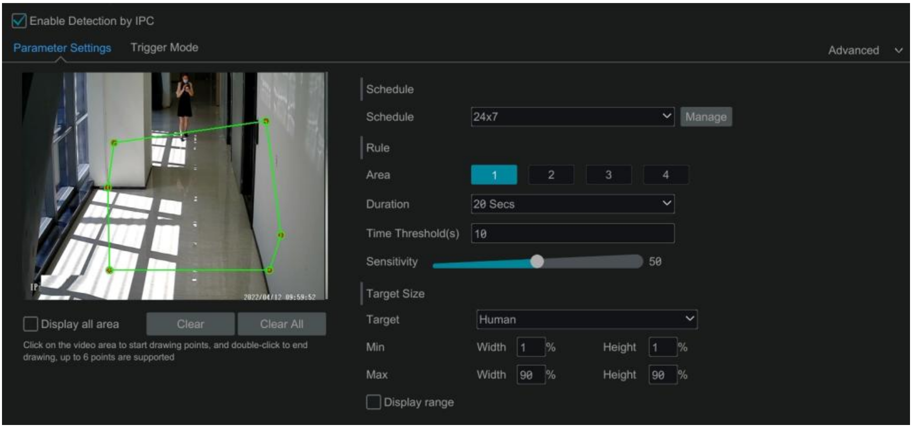
④ Click "Apply" to save the settings.

9.11 Loitering Detection

Only some IPCs support this function. If the camera you added doesn't support this function, please skip the following instructions.

Loitering Detection: when someone entering and loitering in a pre-defined area exceeds the threshold, alarms will be triggered until the object leaves this area.

① Click ***Start→Settings→AI/Event→AI Event→More→Loitering Detection*** to go to the following interface.



☑ Enable Detection by IPC

Schedule

Schedule: 24x7

Rule

Area: 1 2 3 4

Duration: 20 Secs

Time Threshold(s): 10

Sensitivity: 50

Target Size

Target: Human

Min Width 1 % Height 1 %

Max Width 90 % Height 90 %

□ Display range

□ Display all area

Click on the video area to start drawing points, and double-click to end drawing, up to 6 points are supported

② Set the schedule, duration, time threshold and sensitivity.

Sensitivity: The higher the value is, the easier the alarm can be triggered.

Time Threshold: the time that a person is allowed to stay in the area. If a person staying and moving in the specified area exceeds the threshold, alarms will be triggered until this person leaves or stops moving.

For example: Set the threshold to "60seconds; when a person staying and moving in the specified area exceeds 60seconds, an alarm is triggered and continues. 2 minutes later, this person stops moving in the specified area, and then the alarm stops. However, the alarm will continue once this person moves again in the specified area unless the person leaves this area.

③ Set the alarm area. Up to four alarm areas can be set. Click around the area where you want to set as the alarm area in the image (the alarm area should be a closed area).

④ Set target size. Please refer to the target size setup of line crossing for details. Note that only some IPCs support target size settings. If the added camera doesn't support this function, please skip this step.

⑤ Click "Trigger Mode" to configure loitering detection alarm linkage items. Enable or disable "Record", "Snapshot", "Push", "Alarm-out", "Preset", "Buzzer", "Pop-up Video", and

"E-mail". The alarm linkage settings are the same as the face detection alarm (see Face Detection Settings for details).

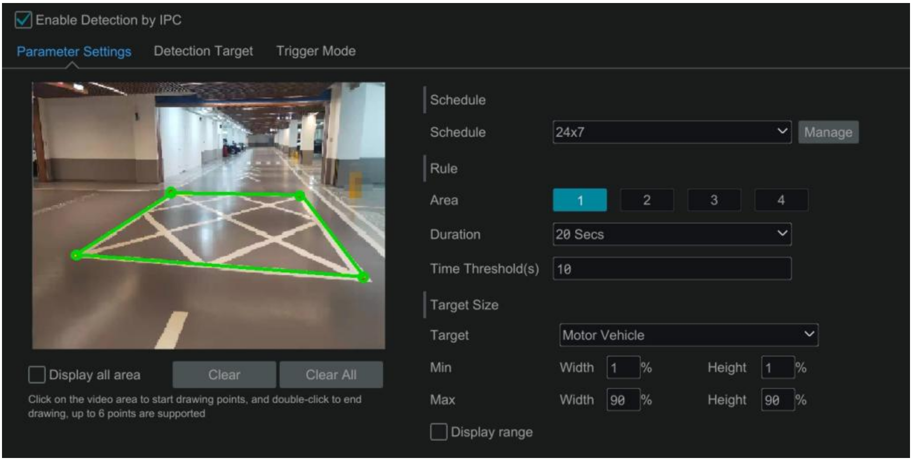
⑥ Click "Apply" to save the settings.

9.12 Illegal Parking Detection

Only some IPCs support this function. If the camera you added doesn't support this function, please skip the following instructions.

Illegal Parking Detection: when a vehicle (like a car, truck, motorcycle, etc.) staying in a no-parking zone exceeds the threshold, alarms will be triggered until the vehicle is driven away.

① Click ***Start→Settings→AI/Event→AI Event→More→ Illegal Parking Detection*** to go to the following interface.



☑ Enable Detection by IPC

Parameter Settings | Detection Target | Trigger Mode

Schedule

Schedule: 24x7

Rule

Area: 1 | 2 | 3 | 4

Duration: 20 Secs

Time Threshold(s): 10

Target Size

Target: Motor Vehicle

Min Width 1 % Height 1 %

Max Width 90 % Height 90 %

□ Display range

□ Display all area

Click on the video area to start drawing points, and double-click to end drawing, up to 6 points are supported

② Set the schedule and alarm duration.

Sensitivity: the higher the value is, the easier the alarm can be triggered.

Time Threshold: the time that a vehicle is allowed to stay in the specified area. If a vehicle staying in the area exceeds the threshold, alarms will be triggered until it is driven away. For example, the time threshold is set to 30s. When the system detects a vehicle stopping in the set no-parking zone, it will start counting. Alarms will be triggered after it stays for more than 30s. And the illegal parking alarm will not stop until the vehicle is driven away from the non-parking zone.

Duration: it is the time that the alarm extends for after the overstaying vehicle leaves.

③ Set the alarm area. Up to four alarm areas can be set. Click around the area where you want to set as the alarm area in the image (the alarm area should be a closed area).

④ Set target size. Please refer to the target size setup of line crossing for details. Note that only some IPCs support target size settings. If the added camera doesn't support this function, please skip this step.

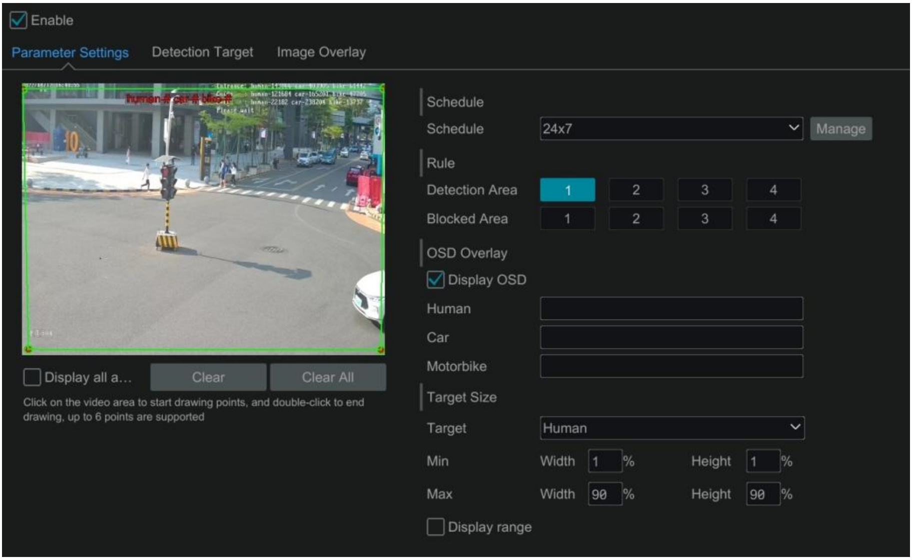
⑤ Click “Trigger Mode” to configure exception alarm linkage items. Enable or disable “Record”, “Snapshot”, “Push”, “Alarm-out”, “Preset”, “Buzzer”, “Pop-up Video”, and “E-mail”. The alarm linkage settings are the same as the face detection alarm (see Face Detection Settings for details).

9.13 Video Metadata

Only some IPCs support this function. If the camera you added doesn’t support this function, please skip the following instructions.

Video Metadata: Human, motor vehicle and non-motor vehicle in the video can be classified, counted and captured and the relevant features can be extracted and displayed on the live interface.

① Click ***Start→Settings→AI/Event→AI Event→Video Metadata*** to go to the following interface.



☑ Enable

Parameter Settings | Detection Target | Image Overlay

□ Display all a… | Clear | Clear All

Click on the video area to start drawing points, and double-click to end drawing, up to 6 points are supported

Schedule

Schedule: 24x7 | Manage

Rule

Detection Area: 1 2 3 4

Blocked Area: 1 2 3 4

OSD Overlay

☑ Display OSD

Human:

Car:

Motorbike:

Target Size

Target: Human

Min: Width 1 % Height 1 %

Max: Width 90 % Height 90 %

□ Display range

② Enable video metadata and then set the schedule.

③ Set the detection area and blocked area.

Detection Area: 4 detection areas can be set. Targets that enter the pre-defined detection area will be counted and captured.

Blocked Area: 4 blocked areas can be set. Targets that enter the pre-defined blocked area will not be counted and captured.

To set detection area: Select the number and then set the detection area. Then click around the area where you want to set as the alarm area on the image (the alarm area should be a closed area).

To set blocked area: Select the number and then set the blocked area. The setting steps are the same as detection area settings.

Display OSD: If enabled, you can see the statistical information of human, motor vehicle and non-motor vehicle on the screen. The statistical OSD information can be customized as needed.

④ Advanced settings. Click “Advanced” to enter the advanced setting interface. Select SD card storage type and the reset information. Auto reset or manual reset can be set as needed.

⑤ Set the detection target and sensitivity.

⑥ Select the attribute information of the target. When the target is detected, the information you select will be displayed under the captured image.

⑦ Click “Apply” to save the settings

10 Intelligent Analytics

10.1 Target Detection View

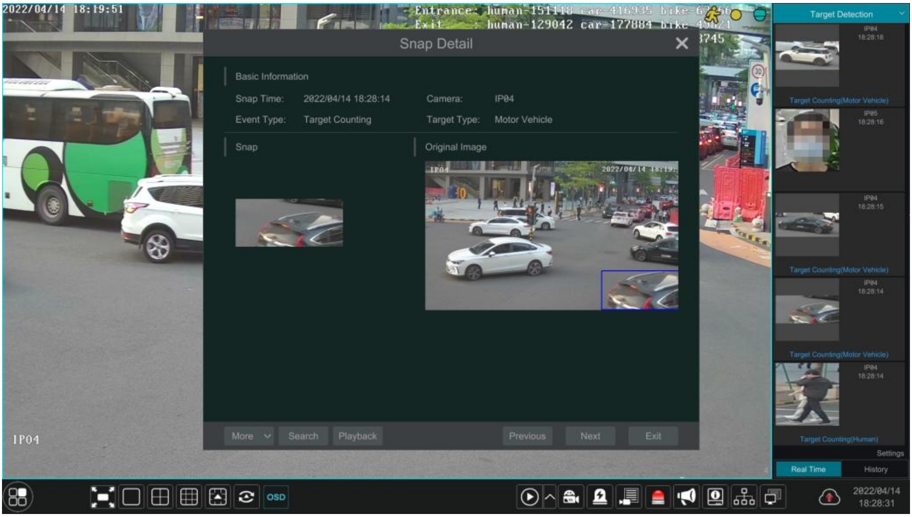
Only some models support target detection view. If your device doesn't support it, please skip the following instructions.

10.1.1 Human Body/Vehicle Detection View

Only when the camera supports human body/vehicle detection, can you view the real-time captured people or vehicle pictures. The setting steps are as follow:

① Enable the Line crossing/Region Intrusion/Region Entrance/Region Exiting/Loitering Detection/Target counting/Video Metadata function of IPCs/NVR, draw the line or area and choose the detection target (see the corresponding sections for details).

② Go to live view interface and then click to go to the target detection interface of this channel. In this interface, you can switch the channel on the top right. You can also click on the top right corner of the live view interface and then choose the target detection tab to go to the target detection interface of multi-channel as shown below. Note that only some models support multi-channel target detection function. Click the captured picture on the right of the live interface to see the snapshot detailed information, such as snapshot time, camera, event type and target type.



Snap Detail

Basic Information

Snap Time: 2022/04/14 18:28:14 Camera: IP04

Event Type: Target Counting Target Type: Motor Vehicle

Click "More" to see a dropdown list. You can export the captured pictures by clicking "Export" or view the target ID by clicking "Information". Click "Search" to go to smart human body/vehicle search interface. The system will automatically search captured people/vehicles. Click "Playback" to go to the playback interface.

10.1.2 Face Detection/Match View

Only the face recognition NVR supports the following functions. If your NVR doesn't support them, please skip the following instructions.

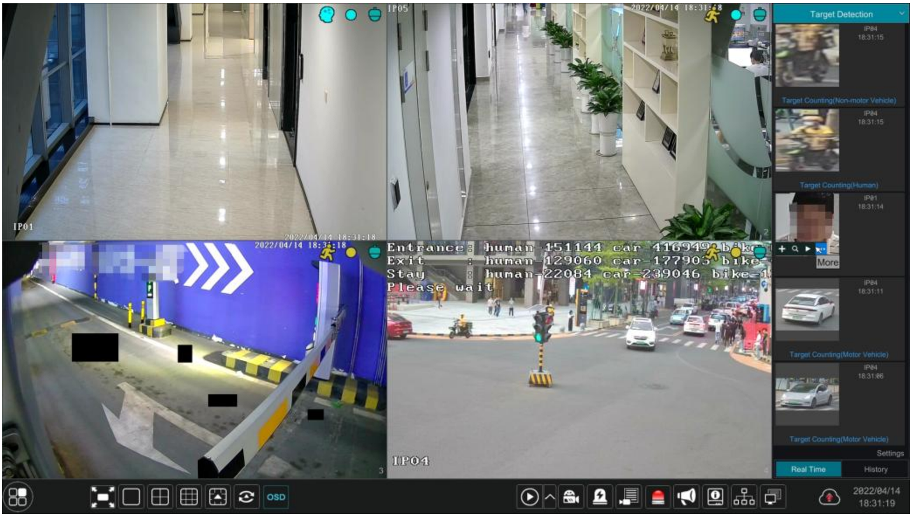
The setting steps are as follow:

① Enable face detection function (see Face Detection Settings for details).

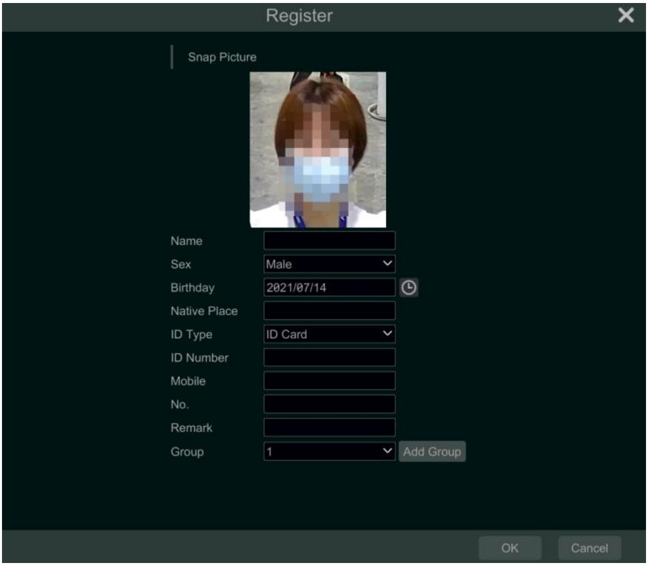
②Enable face recognition function and set the alarm linkage items (see Face Recognition Settings for details).

③ Go to live view interface and click on a face detection channel. This will bring a toolbar under the channel. Then click ⊡ to go to the target detection interface of this channel. In this interface, you can switch the channel on the top right. You can also click ⌄ on the top right corner of the live view interface and then choose the target detection tab to go to the target detection interface of multi-channel as shown below.

Note: Multi-channel target detection function is only available for some models.



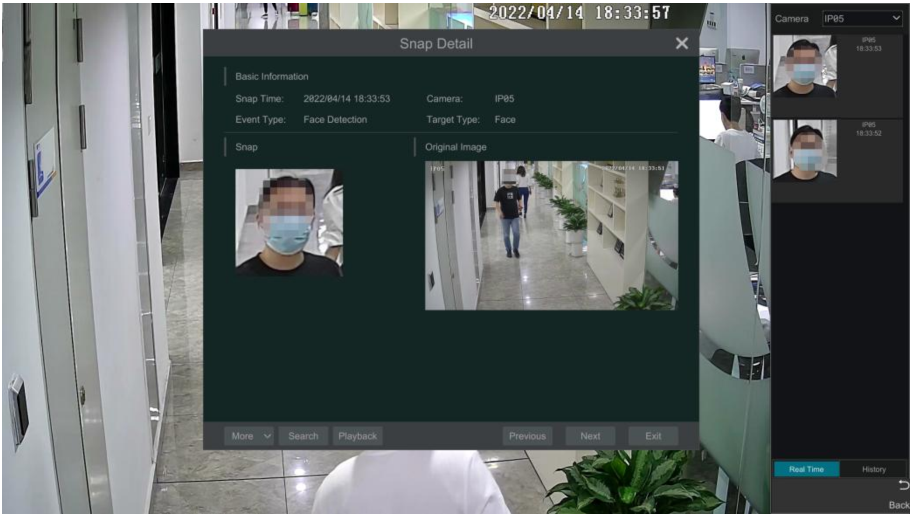
For unknown faces, you can select this face and click + under the captured face to register this face (see the following picture); click 🔍 to quickly go to the smart face search interface where you can search the matching facial information; click ▶ to quickly go to the smart face playback interface; click ••• to view snapshot details.



Name
Sex: Male
Birthday: 2021/07/14
Native Place
ID Type: ID Card
ID Number
Mobile
No.
Remark
Group: 1

Before registering face pictures, please add groups for them in advance (see Face Database Management for details).

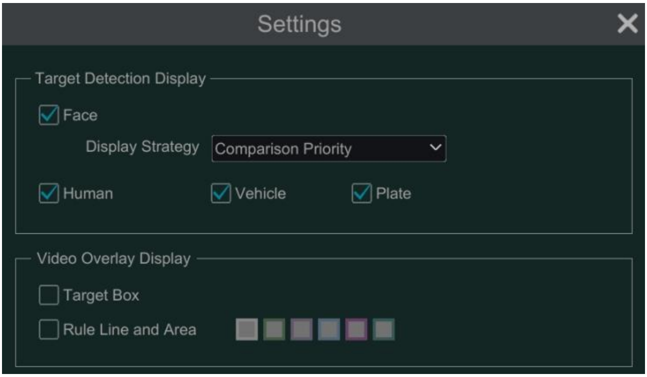
After the face pictures are registered, the system will compare them automatically the next time the corresponding faces are captured. Refer to the following picture.



Basic Information
Snap Time: 2022/04/14 18:33:53 Camera: IP05
Event Type: Face Detection Target Type: Face

Double click a face picture to see the snapshot details, such as snapshot picture, original image, snapshot time and camera. Click "more" and then a dropdown list will display with more options. Click "Register" to register the current snapshot. Click "Search" to go to face search interface. Click “Playback” to go to the playback interface. Click “Export” to export this snapshot details. Click “Information” to view face ID.

In the face match interface, click “Settings” to open the following window.



Target Detection Display

☑ Face

Display Strategy: Comparison Priority

☑ Human ☑ Vehicle ☑ Plate

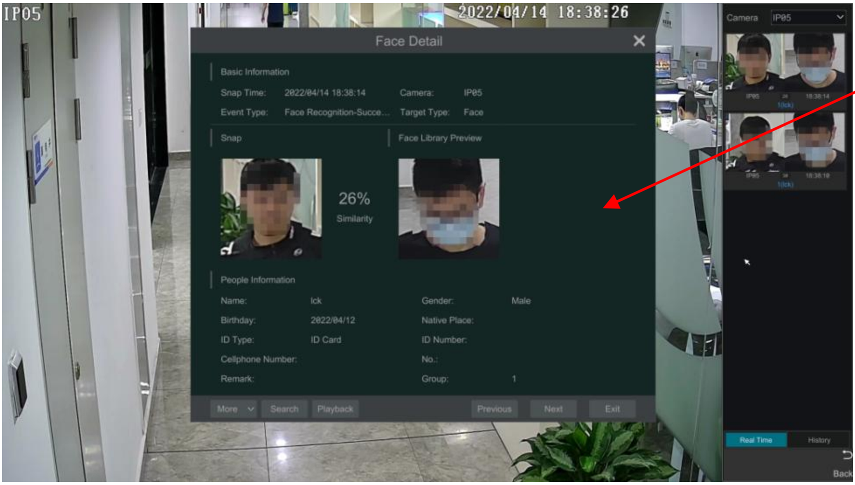
Video Overlay Display

☐ Target Box

☐ Rule Line and Area

Target Detection Display: Face, human body, vehicle or plate can be enabled. If disabled, the captured target picture will not be displayed under the target detection tab in the live view interface.
Display Strategy: Two options: Comparison priority and only comparison

Video Overlay Display:
If “Target box” is clicked, you will see the target traced by a little red box.
If “Rule Line and Area” is checked, you will see the rule line of line crossing detection and detection area of intrusion detection displayed on the screen. You can select the color of the rule line and area as needed.



Basic Information

Snap Time: 2022/04/14 18:38:14 Camera: IP05

Event Type: Face Recognition-Succe... Target Type: Face

Snap

Face Library Preview

26% Similarity

People Information

Name: Ick Gender: Male

Birthday: 2022/04/12 Native Place:

ID Type: ID Card ID Number:

Cellphone Number: No.:

Remark: Group: 1

When a captured face picture is successfully recognized, click the picture on the right to open a face detail window as shown above. In this window, you can see the captured face picture, the matched picture from face library and the relevant information. You also can view the original image, search image by snapshot, play back by snapshot and export the face details by clicking "More" button.

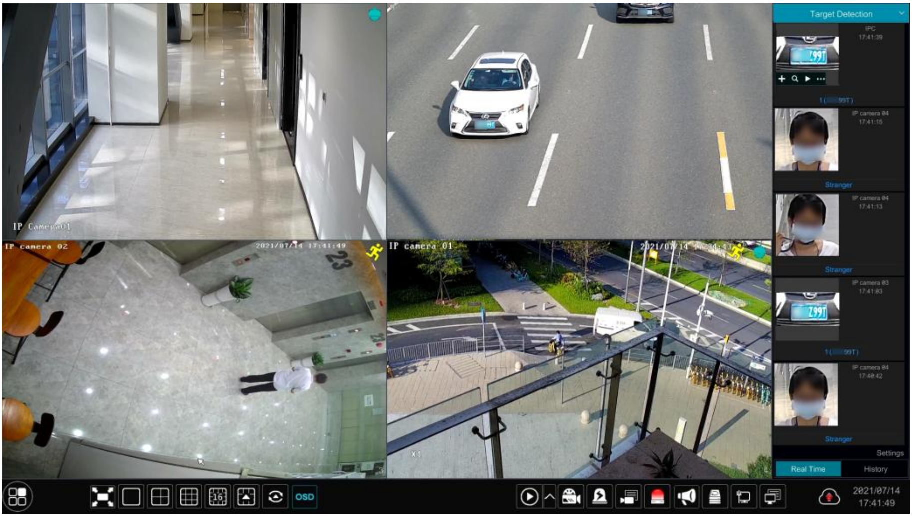
Additionally, you can view the history of captured face pictures and face match information in the face match interface by clicking "History" tab. Besides registering face pictures in the live view interface, you can also add target face pictures in the face database interface.

Note: if you enter a remark when adding a face picture to the face database, the remark information (instead of the person's name) will be shown under the picture after a successful recognition.

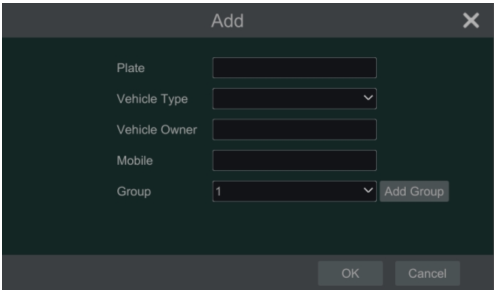
10.1.3 License Plate Detection/Recognition View

Only when the ANPR camera is added and enabled, can license plates be captured and matched. The setting steps are as follows

① Enable the plate detection function (See License Plate Detection Settings for details). Then you can see the captured plates displayed in the live view interface as shown below.



Put the cursor on the captured plate picture and then click ✚ to register this plate as shown below.



Add

Plate

Vehicle Type

Vehicle Owner

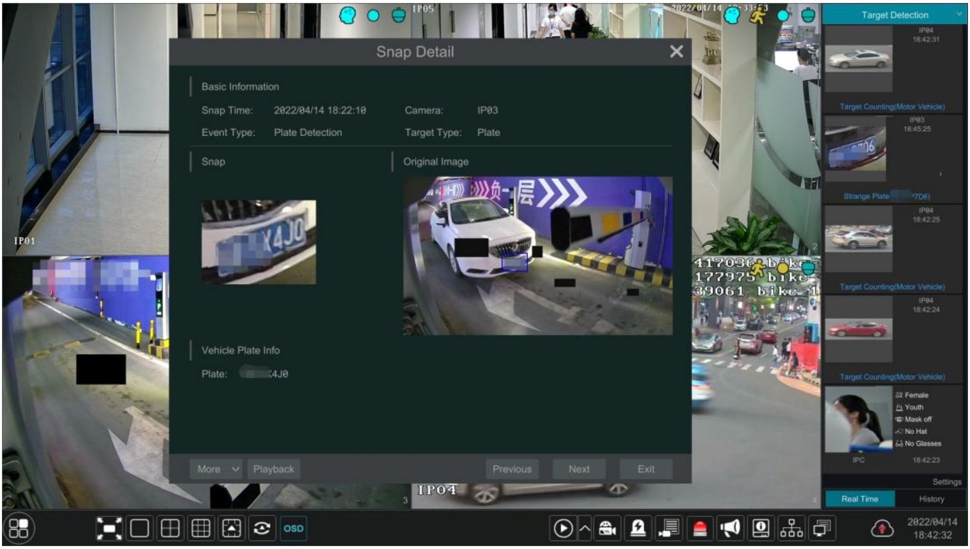
Mobile

Group: 1

Click ••• to view the captured detail information. Click 🔍 to quickly enter the vehicle search interface. You can search the matched plate information in this interface. Click ▶ to go to the smart playback interface.

② Enable license plate recognition function and set the alarm linkage items (see License Plate Recognition Settings for details).

③ Go to live view interface and click ⌄ on the top right corner of the live view interface and then choose the target detection tab to go to the target detection interface of multi-channel as shown below. When a plate is captured, it will be displayed on the right panel. A strange plate will show "Strange plate" under the plate picture.



Snap Detail

Basic Information

Snap Time: 2022/04/14 18:22:10   Camera: IP03

Event Type: Plate Detection   Target Type: Plate

Snap   Original Image

Vehicle Plate Info

Plate: [redacted]4J0

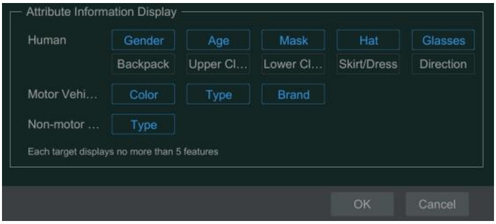
Click the captured plate picture and then it will open a detailed information window. You can view the snapshot picture, original picture, snapshot time, camera, etc. Click "More" to view the ID information of the target and export the captured picture. Click "Search" to go to the vehicle search interface. Click “Playback” to go to the playback interface.

10.1.4 Object Attribute View

①Enable video metadata function and then select the detection target and display attributes (see Video Metadata for details).

②Go to live view interface and click on an AI camera channel (which supports video metadata function). This will bring a toolbar under the channel. Then click to go to the target detection interface of this channel. In this interface, you can switch the channel on the top right. You can also click on the top right corner of the live view interface and then choose the target detection tab to go to the target detection interface of multi-channel.

Click “Settings” at the bottom right to select the attribute information of people/motor vehicle/non-motor vehicle you want to view under the captured picture.



Attribute Information Display

Human: Gender, Age, Mask, Hat, Glasses, Backpack, Upper Cl..., Lower Cl..., Skirt/Dress, Direction

Motor Vehi...: Color, Type, Brand

Non-motor ...: Type

Each target displays no more than 5 features

Click the captured picture to view the details. In the detail interface, you can view the captured picture, original picture, object attributes, etc.

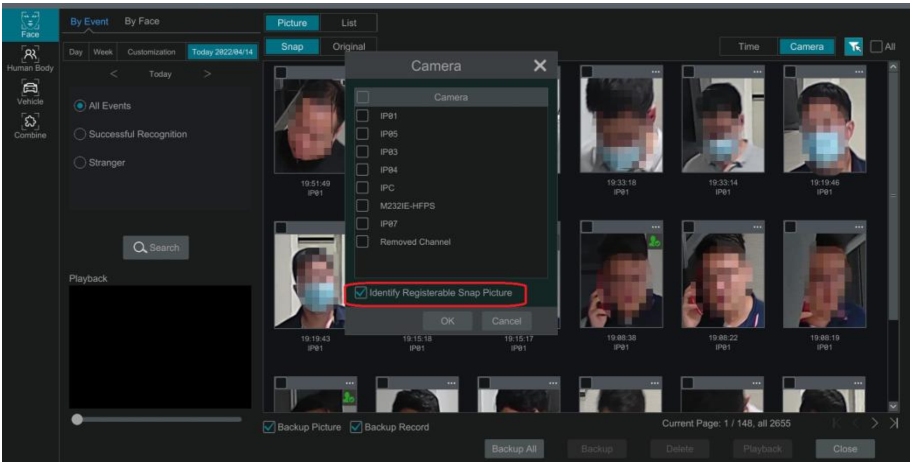
10.2 Smart Search

10.2.1 Face Search

Only some models support this function. If your device doesn’t support it, please skip the following instructions.

➢ **Face Search by Event**

① Click ***Start→ Intelligent Analytics → Search→Face*** to go to the following interface.



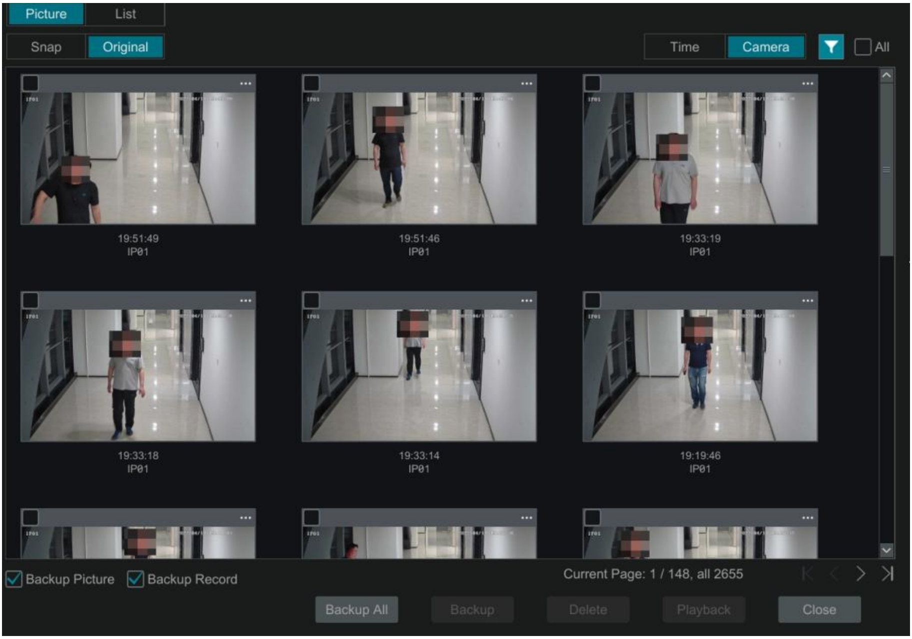
② Click ▼ to choose face detection cameras. You can enable “Identify Registerable Snap Picture”. Then the picture which can be added to the face database will be marked with a green icon.

③ Select all events, successful recognition or stranger.

④ Click “Search” to search face pictures. You can view face pictures by time or by camera.

⑤ Click the searched face picture to play in the small playback window; select a face picture and click “Backup” to export it.

Click “Original” to see the original image as shown below.

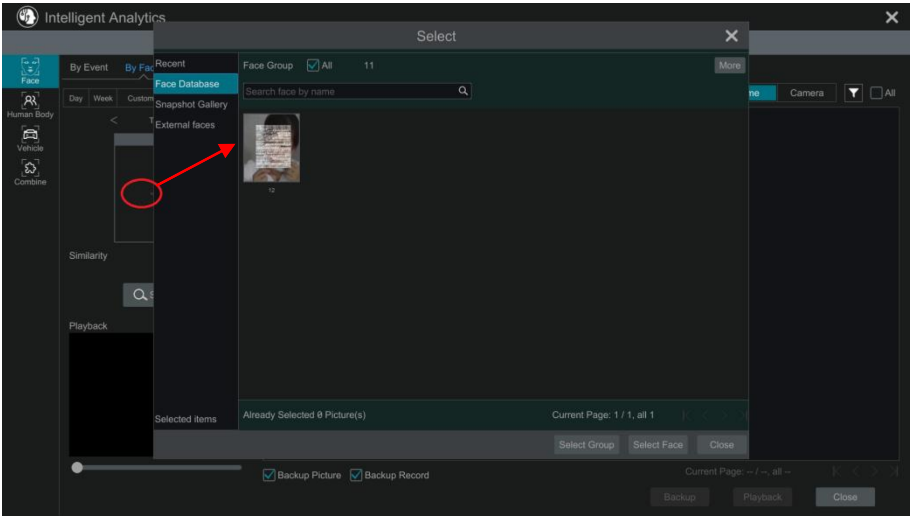


Click “List” to view the snapshot information list. Click 🗎 to view the detail information; click ⬇ to back up the image.

➢ Face Search by Face

In the face picture search interface, click “By Face” to go to the following interface.

① Click ➕ to add the target face which can be searched and added from recent, face database, snapshot gallery and external faces. A single face picture or multiple face pictures can be added and searched. (Taking a single face picture for example)



To add a single target face from recent faces

a. Choose the face.

b. Click “Select Face”.

To add a single target face from the face database:

a. Click “More” to choose groups.

b. Select a target face and click “Select Face”.

To add a single target face from the snapshot gallery:

a. Select time and click “More” to choose cameras.

b. Click “Search”.

c. Check a face and click “Select Face”.

To add a single target face from external faces:

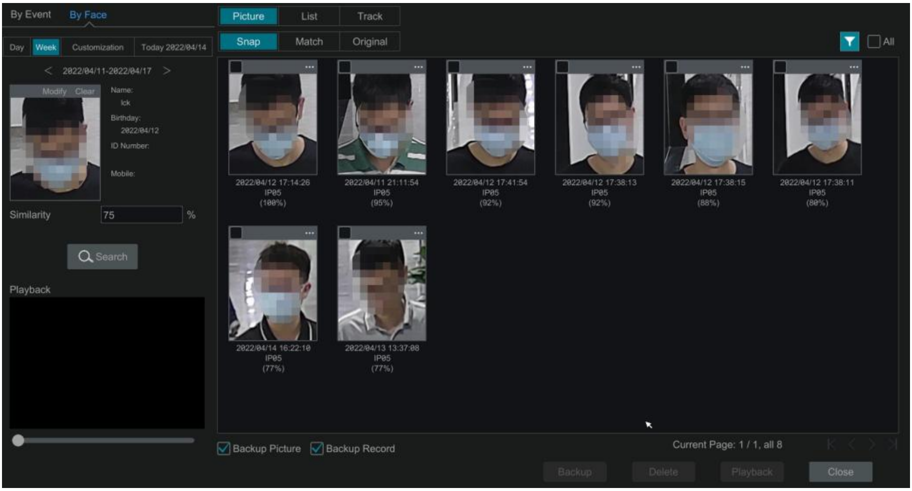
a. Save the target face to the mobile storage device and then insert this device into the USB interface of NVR.

b. Select “External Face” to import the face in this interface.

② Set similarity and then click “Search”.

③ Click the searched image to play records in the small window.

④ Select the searched image and click “Backup Picture” or “Backup Record”. Then click “Backup” to build backups for pictures or records.



Name: lck

Birthday: 2022/04/12

ID Number:

Mobile:

Similarity 75 %

2022/04/12 17:14:26 IP05 (100%)

2022/04/11 21:11:54 IP05 (95%)

2022/04/12 17:41:54 IP05 (92%)

2022/04/12 17:38:13 IP05 (92%)

2022/04/12 17:38:15 IP05 (88%)

2022/04/12 17:38:11 IP05 (80%)

2022/04/14 16:22:10 IP05 (77%)

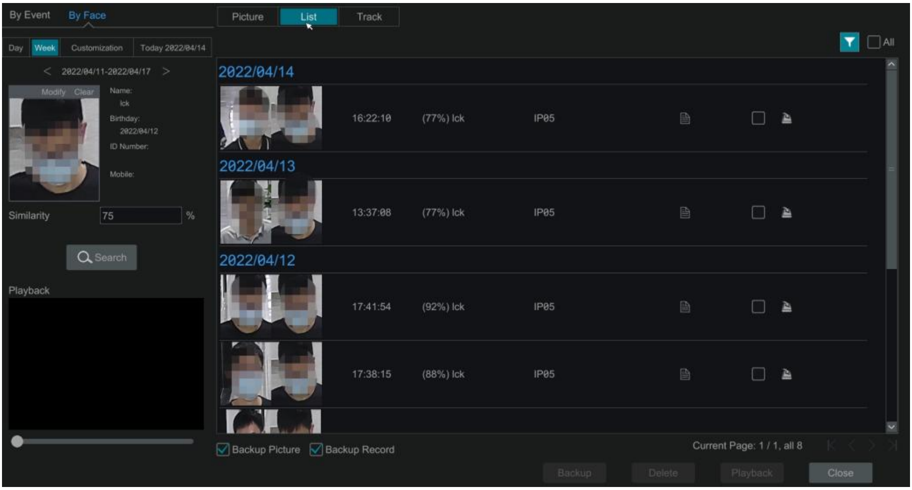
2022/04/13 13:37:08 IP05 (77%)

☑ Backup Picture ☑ Backup Record

Current Page: 1 / 1, all 8

- **View Image by List**

Click "List" tab to view images by time as shown below.



Name: lck

Birthday: 2022/04/12

ID Number:

Mobile:

Similarity 75 %

2022/04/14

16:22:10 (77%) lck IP05

2022/04/13

13:37:08 (77%) lck IP05

2022/04/12

17:41:54 (92%) lck IP05

17:38:15 (88%) lck IP05

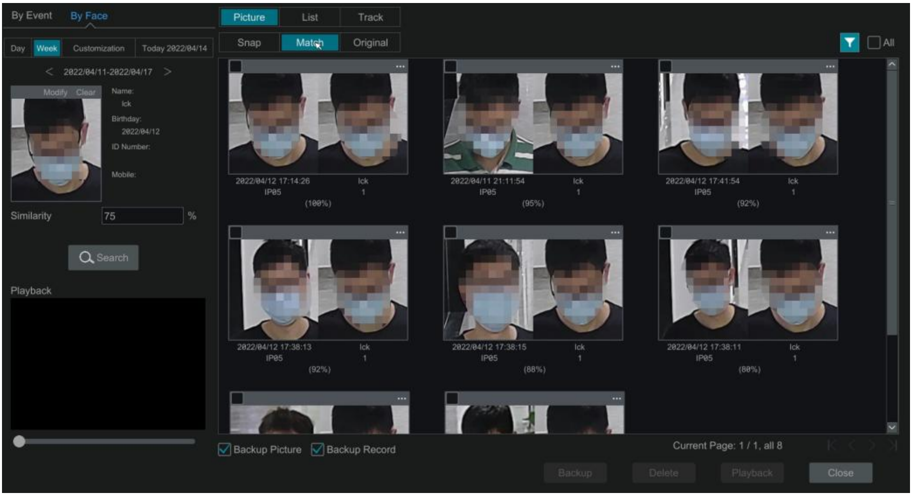
☑ Backup Picture ☑ Backup Record

Current Page: 1 / 1, all 8

Click the searched image to play a clip. Click 🗎 to view the detail information of the comparisons to the target face.

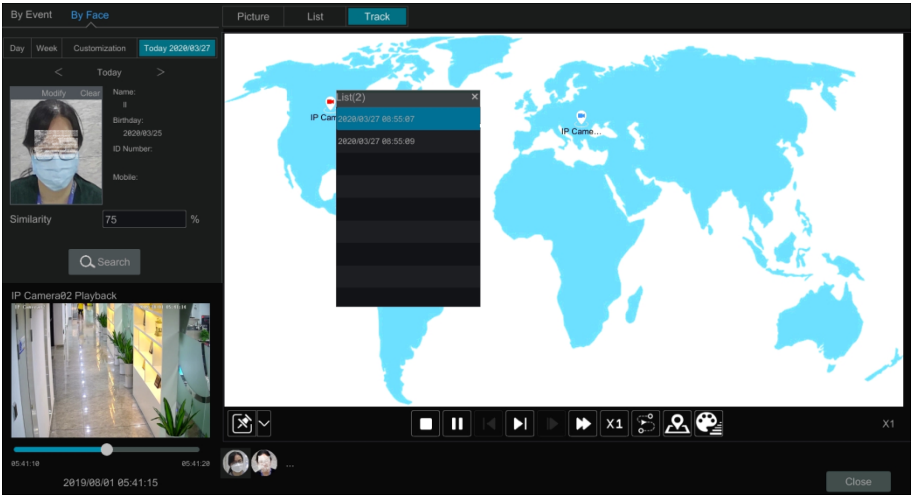
- **View Match Images**

Click "Match" tab to view matching images as shown below.



10.2.2 Track Playback

Select "Track" to go to the following interface.



Note: Tracking will only work if two or more cameras have viewed and recorded the subject.

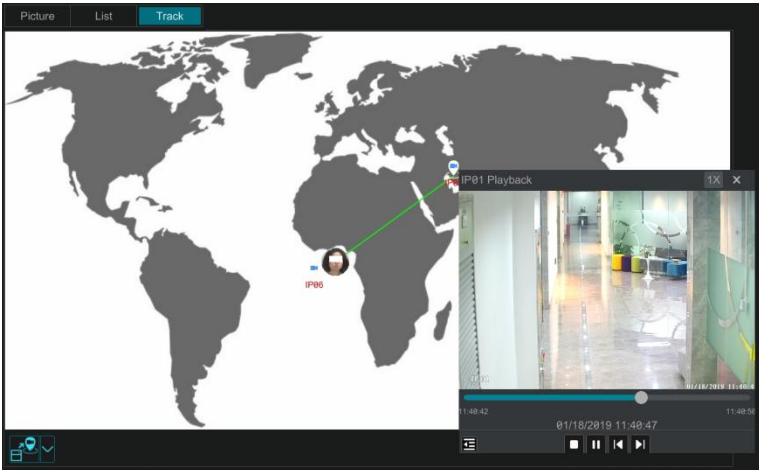
Descriptions of buttons on the track interface

	Fixed Window	▶	Frame
	Followed Window	⏩	Fast Forward（x2;x4）
	Exchange Window	X1	Normal Speed

■	Stop		Start/Stop Track
▶	Play		Edit Map
⏮	Previous		Edit Color
⏭	Next		

Click on a camera name and then an event list appears. Click one item to play the recording.

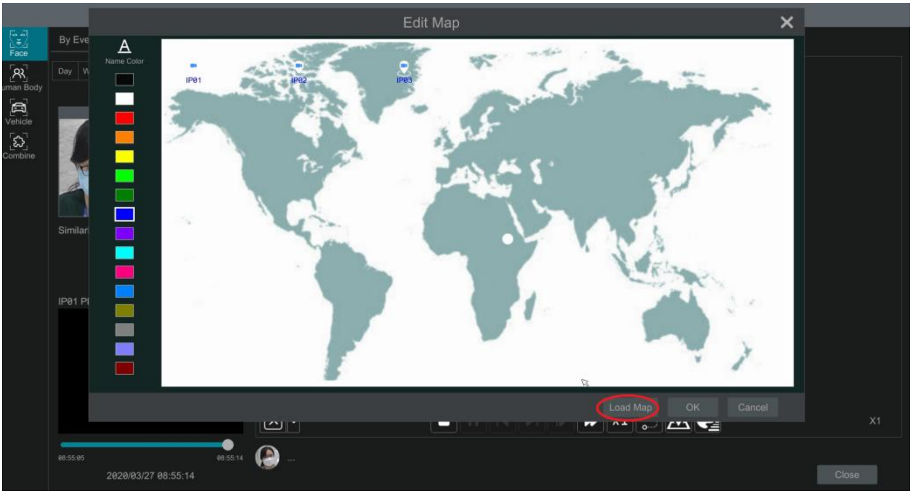
Click ⌄ button beside the fixed window icon to show “Followed Window” and “Exchange Window” icons. The small playback window will float on the map window by clicking “Followed Window” as shown below.



Click 1X to switch play speed. 1x and 2x can be switched. Click ☰ to view event list. Click one item to play this event.

Click “Exchange Window” to switch the position of the map window and the playback window.

Click button to go to the following interface.



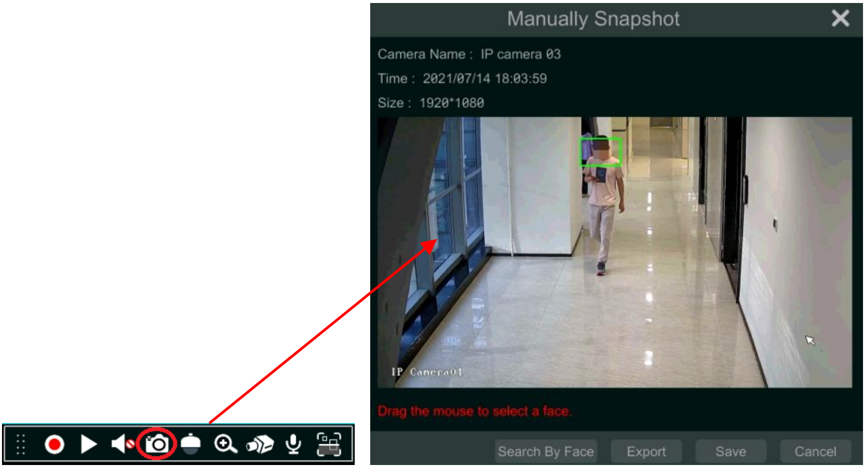
Click “Load Map” to add a map. Then drag the camera names onto and around the map to change their locations. Choose a color from the left color list to set your favorite color for camera names.

Load Map: ① Save the map to the USB storage device and then insert the USB storage device into the NVR. ② Click “Load Map” button to upload the map.

Click 🎨 button to modify the colors of camera names and track lines and set the line width.

10.2.3 Face Search by Snapshot

In the live or playback interface, click on a face detection camera and then select 📷 on the toolbar. This will bring the following window.



Camera Name : IP camera 03

Time : 2021/07/14 18:03:59

Size : 1920*1080

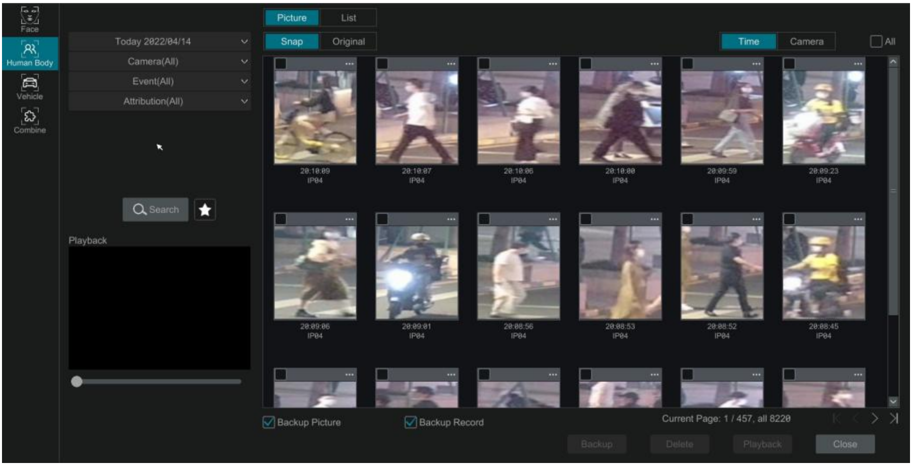
Drag the mouse to select a face.

Drag the mouse to select a face and then click "Search by Face" to go to the face search by face interface. You can see its snapshot pictures, match pictures, original pictures and so on by clicking the corresponding tab.

10.2.4 Human Body Search

Click ***Start→ Intelligent Analytics→Search→Human Body*** to go to the human body search interface.

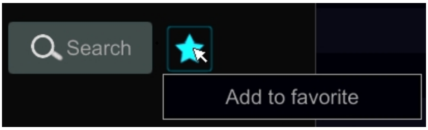
Select the search time, camera and event and then click "Search" to view the searched pictures.

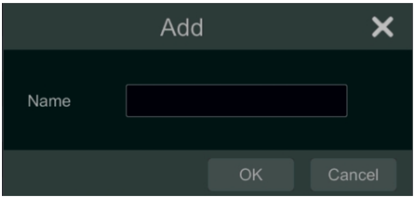


You can also select the attributes of people to filter (like gender, age, mask-wearing status, glasses-wearing status, color of clothes, etc.). Note that only the searched camera with video metadata function can filter attributes.

Click a searched picture to play the recording in the small window on the left. Select pictures and check "Backup Picture" and/or "Backup Record" and then click "Backup" to back up the pictures and /or records. Click "Original" to view the captured original pictures. Click "List" to view the file list of the captured pictures.

Click ★ and select "Add to favorite" to add a favorite group and save the current searched pictures to the favorite group. Then you can quickly view these figure pictures by clicking ★ and choosing the group name.



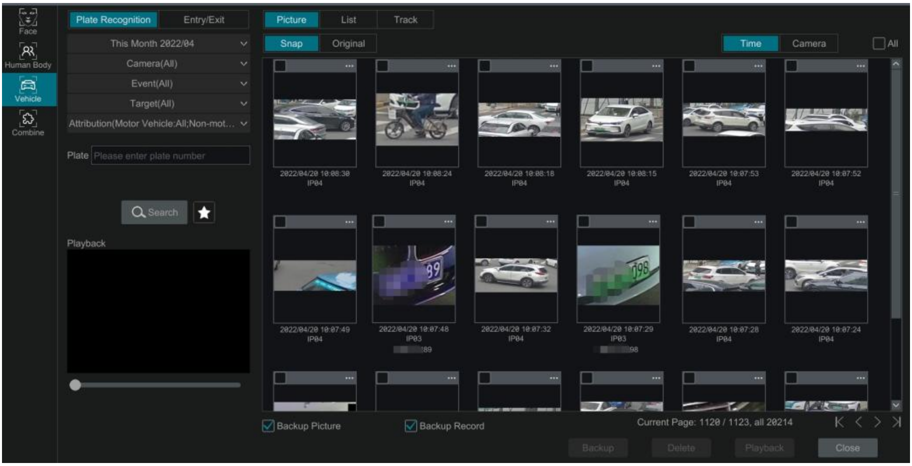


10.2.5 Vehicle Search

① Click ***Start→ Intelligent Analytics→ Search →Vehicle*** to go to the vehicle search interface.

② Select the time, camera, event and vehicle type. Then click "Search" to search vehicles.

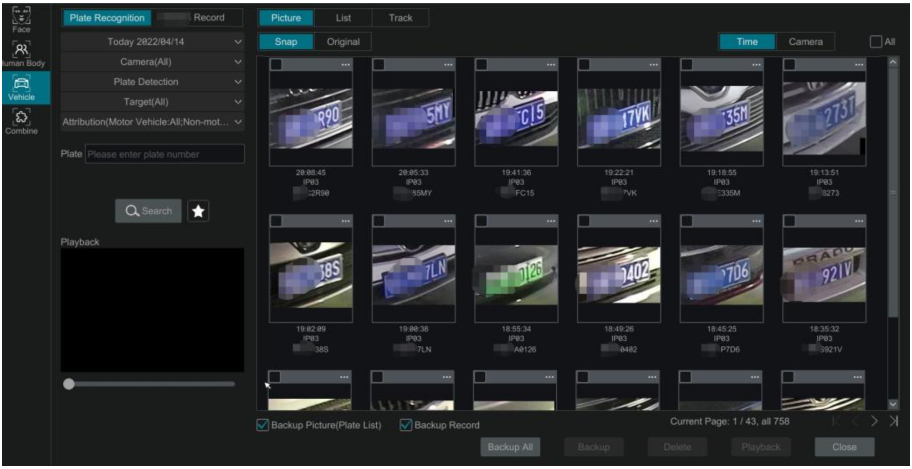
Event: Intrusion, Line Crossing, Target Counting, Plate Detection, Plate Match-Successful Recognition and Plate Match-Strange Plate can be selected.
Attribution: Vehicle or non-vehicle attributes can be selected as needed. For example, you can search vehicles according to the color, brand or type. Note that only the searched camera with video metadata function can filter attributes.
You can view face pictures by time or by camera.



Click a searched vehicle picture to play the clip in the small window on the left. Select vehicle pictures and check "Backup Picture" and/or "Backup Record" and then click "Backup" to back up the pictures and /or records.

③ Click "Original" to see the original pictures; click "List" to view the snapshot information list. Click 🗎 to view the detail information; click 💾 to back up the image.

Select "Plate Detection" or "Plate Recognition" to view plate image. You can also enter the plate number to search the plate pictures. Then you can view the track of this vehicle.



Click “Track” to view the track of the vehicle.

Note: Only one plate can be traced at a time and two or more ANPR cameras must have detected this vehicle to create a track to follow.

The track setting steps are similar to the face track setup steps. Please refer to face track settings for details.

Click ★ to add a favorite group and save the current searched pictures to the favorite group. Then you can quickly view these vehicle pictures by clicking ★ and choosing the group name.

10.2.6 Combination Search

If you want to view the human body, vehicle or face pictures simultaneously, you can choose combination search.

① Click “Combine”.

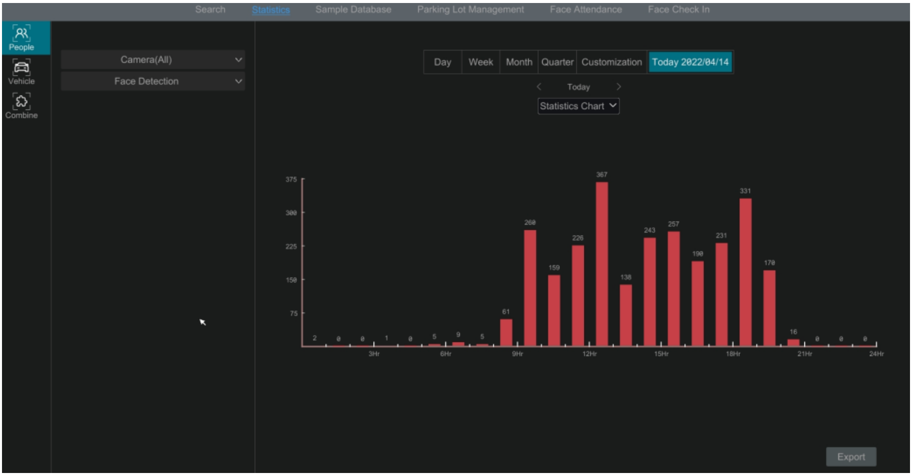
② Select the search time, camera, event and vehicle as needed.

Click a searched picture to play it in the small window. Select pictures and check “Backup Picture” and/or “Backup Record” and then click “Backup” to back up the pictures and /or records.

Click ★ to add a favorite group and save the current searched pictures to the favorite group. Then you can quickly view these pictures by clicking ★ and choosing the group name.

10.3 View Statistical Information

Click ***Start→ Intelligent Analytics→Statistics*** to go to the following interface. Through this interface, you can view the statistical information for people and vehicles, and you can customize the statistical information.



View People Information:

Note: The person information includes face information and figure information.

① Select the time.

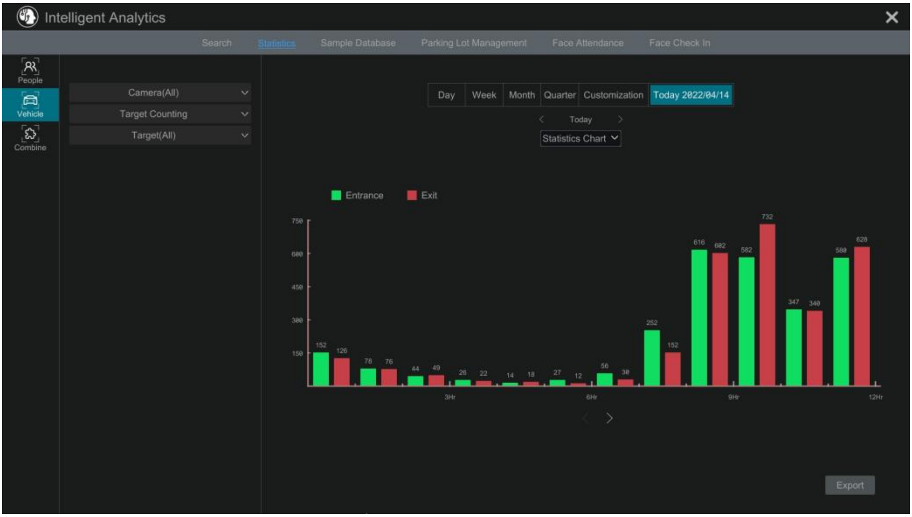
② Select cameras.

③ Select events as needed, such as face detection, face recognition, region intrusion, region entrance, region exiting, loitering detection, line crossing, target counting, etc.

Note: Face recognition events (successful recognition & stranger) are available for some models. If Face Recognition-Successful Recognition event is selected, you can choose “Detail Chart” to view.

View Vehicle Information:

- Click “Vehicle”
- Select the time and cameras.
- Select events as needed.
- Select the vehicle attribution.

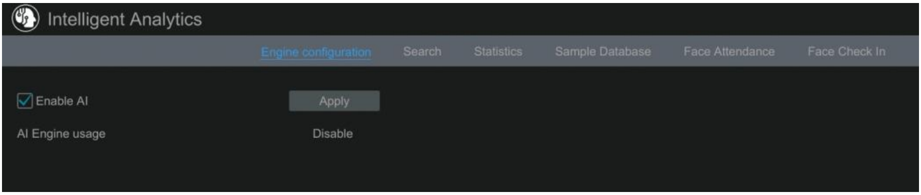


If “Remove duplicate license plate numbers” is checked, the duplicate statistics of the same license plate in the same day will not be displayed in the chart.

To customize statistical information:
Click “Combine” and then select events, people and vehicle as needed. For target counting, you can view the human, motor vehicle and non-motor vehicle information from the exported file.

10.4 Enabling AI Mode

Only some models support this function.
For these models, the IP camera without AI function added to the NVR may realize AI functions, like face detection, line crossing and region intrusion by enabling AI mode in the NVR. If AI mode is enabled, the secondary output will be disabled. Click Start→Intelligent Analytics→Engine Configuration.



☑ Enable AI

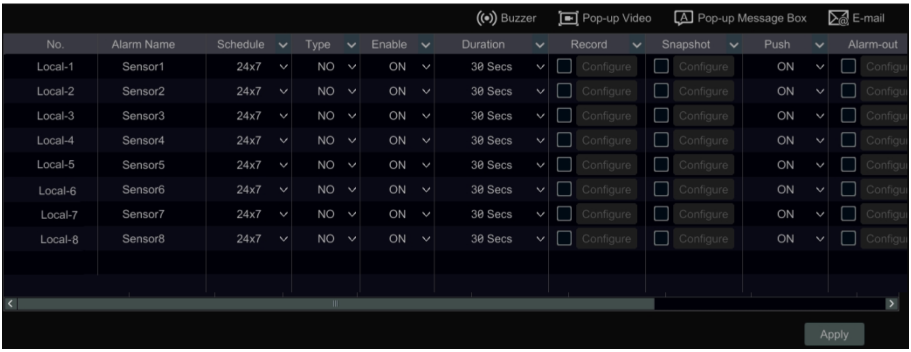
AI Engine usage Disable

11 General Event Management

11.1 Sensor Alarm

To ensure complete setup of the Sensor Alarm function, you should enable the sensor alarm of each camera and then immediately set up the alarm handling for that camera.

① Click ***Start→Settings→Alarm→Sensor*** to go to the following interface.



No.	Alarm Name	Schedule	Type	Enable	Duration	Record	Snapshot	Push	Alarm-out
Local-1	Sensor1	24x7	NO	ON	30 Secs	□ Configure	□ Configure	ON	□ Configu
Local-2	Sensor2	24x7	NO	ON	30 Secs	□ Configure	□ Configure	ON	□ Configu
Local-3	Sensor3	24x7	NO	ON	30 Secs	□ Configure	□ Configure	ON	□ Configu
Local-4	Sensor4	24x7	NO	ON	30 Secs	□ Configure	□ Configure	ON	□ Configu
Local-5	Sensor5	24x7	NO	ON	30 Secs	□ Configure	□ Configure	ON	□ Configu
Local-6	Sensor6	24x7	NO	ON	30 Secs	□ Configure	□ Configure	ON	□ Configu
Local-7	Sensor7	24x7	NO	ON	30 Secs	□ Configure	□ Configure	ON	□ Configu
Local-8	Sensor8	24x7	NO	ON	30 Secs	□ Configure	□ Configure	ON	□ Configu

② Select the alarm type (NO or NC) according to trigger type of the sensor.

③ Enable the sensor alarm of each camera and select the schedule.

④ Check the "Duration", "Record", "Snapshot", "Push", "Alarm-out" and "Preset" and enable or disable the "Buzzer", "Pop-up Video", "Pop-up Message Box" and "E-mail" as required.

⑤ Click "Apply" to save the settings.

The configuration steps of the above mentioned alarm linkages are as follows.

Duration: it refers to the interval time between the adjacent motion detections. For instance, if the duration time is set to 10 seconds, once the system detects a motion, it will go to alarm and would not detect any other motion (specific to camera) in 10 seconds. If there is another motion detected during this period, it will be considered as continuous movement; otherwise it will be considered as a single motion.

Record: If checked, the "Trigger Record" window will open automatically (you can also click the "Configure" button to open the window). Select a camera on the left side and then click >> to set the camera as the trigger camera. Select the trigger camera on the right side or click << to cancel the trigger camera. Click "OK" to save your settings. The trigger camera will record automatically when the sensor alarm is triggered.

Snapshot: If checked, the "Trigger Snapshot" window will open automatically. You can configure the trigger camera in this window. The trigger camera will capture images automatically when the sensor alarm is activated.

Push: If checked, choose ON or OFF. If ON, the system will send messages when the sensor alarm is triggered.

Alarm-out*:* If checked, the “Trigger Alarm-out” window will open automatically. The system will trigger the alarm-out automatically when the sensor alarm is tripped. You need to set the delay time and the schedule of the alarm outputs. See Alarm-out for details.

Preset*:* If checked, the “Trigger Preset” window will open automatically. Here you can configure the trigger preset for each camera. To add presets, please see Preset Setting for details.

Buzzer*:* if enabled, the system will emit an audible buzz when the sensor alarm is triggered. To set the delay time of the buzzer, please see Buzzer for details.

Pop-up Video*:* After camera setup, the corresponding video will pop up automatically when the sensor alarm is triggered. To set the duration time of the video, please see Display for details.

Pop-up Message Box: if enabled, the system will pop up the corresponding alarm message box automatically when the sensor alarm is triggered. To set the duration time of the message box, please see Display for details.

E-mail*:* if enabled, the system will send an e-mail when the sensor alarm is triggered. Before you enable email, please configure the recipient’s e- mail address first (see E-mail Configuration for details).

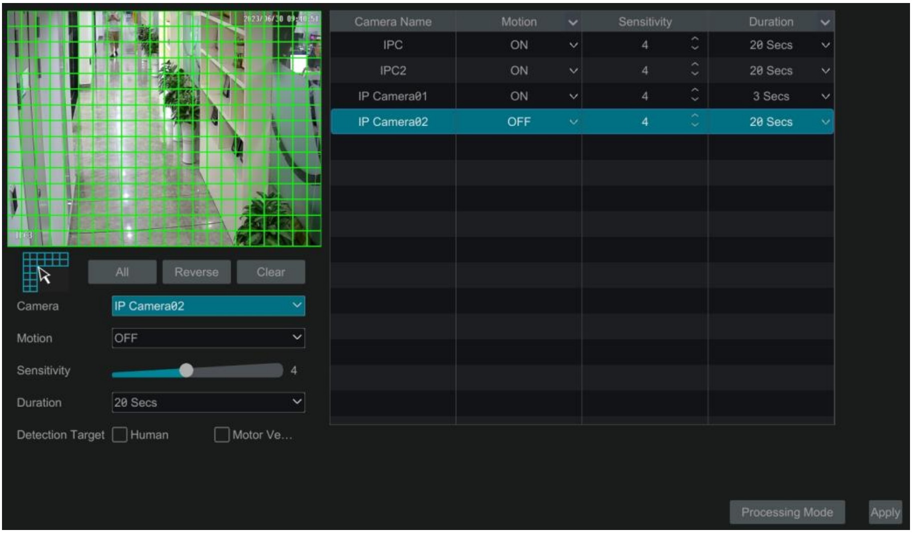
Virtual alarm: This function should be used with API server. If you want to enable it, please make sure the API Server is enabled first (Start→Network→Port) and then set the authentication as “Digest”.

11.2 Motion Alarm

Motion Alarm: when a motion object appears in the specified area, it will trigger the alarm. You should enable the motion of each camera first and then set the alarm handling of the camera to complete the whole configuration of the motion alarm.

11.2.1 Motion Configuration

① Click ***Start→Settings→Camera→Motion Settings*** to go to the following interface.



Camera Name	Motion	Sensitivity	Duration
IPC	ON	4	20 Secs
IPC2	ON	4	20 Secs
IP Camera01	ON	4	3 Secs
IP Camera02	OFF	4	20 Secs

Camera: IP Camera02

Motion: OFF

Sensitivity: 4

Duration: 20 Secs

Detection Target □ Human □ Motor Ve...

② Select a camera, enable motion and set the sensitivity and duration of the camera.

Sensitivity: the higher the value is, the more sensitive it will be to motion. You should adjust the value according to the practical conditions since the sensitivity is influenced by background color and time (day or night).

Duration: The interval time between adjacent motion detections. For instance, if the duration time is set to 10 seconds, once the system detects a motion, it will trigger the alarm and will not detect any other motion (specific to that camera) for 10 seconds. If there is another motion detected during this period, it will be considered as continuous movement.

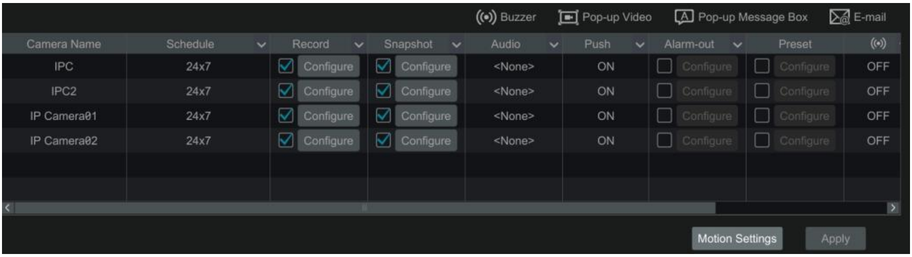
Detection Target: For the camera with SMD function, you can check the detection target as needed. If "Human/Motor Vehicle" is enabled, the camera will only detect the movement of human/motor vehicle. If no target is enabled, alarms will be triggered when the moving object appears on the image, including human, vehicle or other moving objects.

③ Drag the camera image to set the motion area. You can set more than one motion area. Click "All" to set the whole camera image as the motion area. Click "Reverse" to swap the motion area and the non-motion area. Click "Clear" to clear all the motion areas.

④ Click "Apply" to save the settings. Click "Processing Mode" to go to the alarm handling configuration interface of the motion alarm.

11.2.2 Motion Alarm Handling Configuration

① Click ***Start→Settings→Alarm→Motion Alarm*** to go to the following interface.



Camera Name	Schedule	Record	Snapshot	Audio	Push	Alarm-out	Preset	(•)
IPC	24x7	☑ Configure	☑ Configure	<None>	ON	☐ Configure	☐ Configure	OFF
IPC2	24x7	☑ Configure	☑ Configure	<None>	ON	☐ Configure	☐ Configure	OFF
IP Camera01	24x7	☑ Configure	☑ Configure	<None>	ON	☐ Configure	☐ Configure	OFF
IP Camera02	24x7	☑ Configure	☑ Configure	<None>	ON	☐ Configure	☐ Configure	OFF

② Enable or disable "Record", "Snapshot", "Push", "Alarm-out", "Audio", "Preset", "Buzzer", "Pop-up Video", "Pop-up Message Box" and "E-mail". The alarm handling setting of motion alarm is similar to that of the sensor alarm (see Sensor Alarm for details).

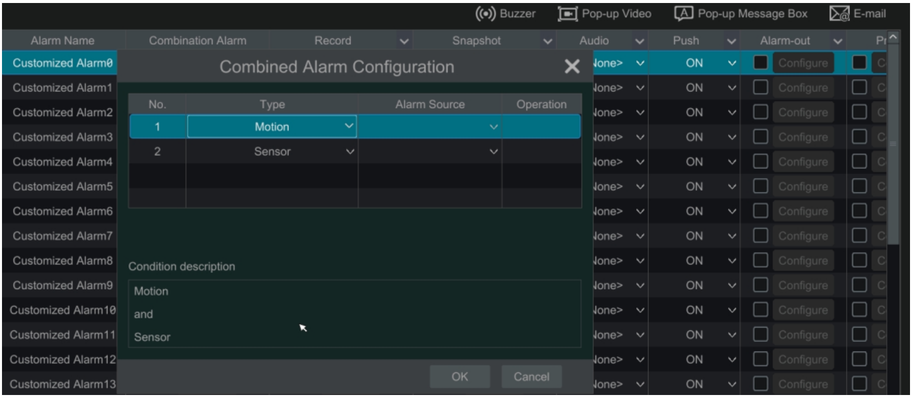
③ Click "Apply" to save the settings. You can click "Motion Settings" to go to the motion configuration interface.

11.3 Combination Alarm

① Click ***Start→Settings→Alarm →Combination Alarm*** to go to the following interface.

② Customize combination alarm. Set alarm name and click "Configure" under the Combined Alarm Configuration item (motion/sensor/intrusion/face recognition/line crossing). Then select alarm type and alarm source. Finally, click "OK" to save the settings.

(Only some models support face recognition)



Alarm Name	Combination Alarm	Record	Snapshot	Audio	Push	Alarm-out	Pr
Customized Alarm0				Jone>	ON	☐ Configure	☐ C
Customized Alarm1				Jone>	ON	☐ Configure	☐ C
Customized Alarm2				Jone>	ON	☐ Configure	☐ C
Customized Alarm3				Jone>	ON	☐ Configure	☐ C
Customized Alarm4				Jone>	ON	☐ Configure	☐ C
Customized Alarm5				Jone>	ON	☐ Configure	☐ C
Customized Alarm6				Jone>	ON	☐ Configure	☐ C
Customized Alarm7				Jone>	ON	☐ Configure	☐ C
Customized Alarm8				Jone>	ON	☐ Configure	☐ C
Customized Alarm9				Jone>	ON	☐ Configure	☐ C
Customized Alarm10				Jone>	ON	☐ Configure	☐ C
Customized Alarm11				Jone>	ON	☐ Configure	☐ C
Customized Alarm12				Jone>	ON	☐ Configure	☐ C
Customized Alarm13				Jone>	ON	☐ Configure	☐ C

Combined Alarm Configuration

No.	Type	Alarm Source	Operation
1	Motion		
2	Sensor		

Condition description

Motion
and
Sensor

③ Enable or disable "Record", "Snapshot", "Push", "Alarm-out", "Preset", "Buzzer", "Audio", "Pop-up Video", "Pop-up Message Box" and "E-mail". The alarm handling setting of combination alarm is similar to that of the sensor alarm (see Sensor Alarm for details).

Click "Apply" to save the settings.

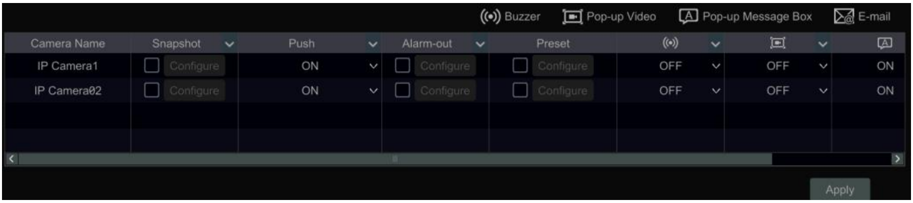
11.4 Exception Alarm

11.4.1 IPC Offline Settings

① Click ***Start→Settings→AI/Event→IPC Offline Settings*** to go to the interface as shown below.

② Enable or disable “Snapshot”, “Push”, “Alarm-out”, “Preset”, “Buzzer”, “Pop-up Video”, “Pop-up Message Box” and “E-mail”. The IPC Offline Settings are similar to that of the sensor alarm (see Sensor Alarm for details).

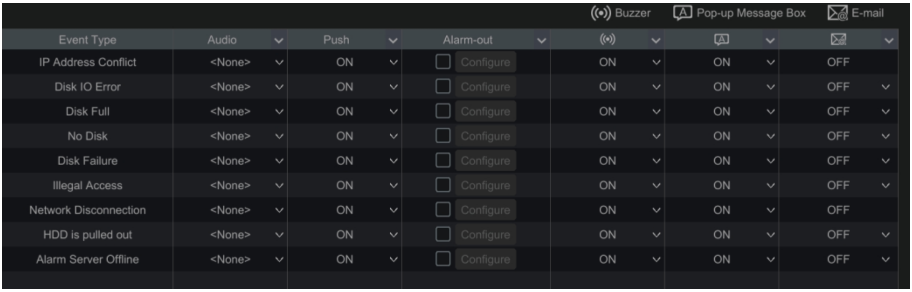
③ Click “Apply” to save the settings.



Camera Name	Snapshot	Push	Alarm-out	Preset			
IP Camera1	□ Configure	ON	□ Configure	□ Configure	OFF	OFF	ON
IP Camera02	□ Configure	ON	□ Configure	□ Configure	OFF	OFF	ON

11.4.2 Exception Alarm Settings

① Click ***Start→Settings→AI/Event→Exception Alarm*** to go to the interface as shown below.



Event Type	Audio	Push	Alarm-out			
IP Address Conflict	<None>	ON	□ Configure	ON	ON	OFF
Disk IO Error	<None>	ON	□ Configure	ON	ON	OFF
Disk Full	<None>	ON	□ Configure	ON	ON	OFF
No Disk	<None>	ON	□ Configure	ON	ON	OFF
Disk Failure	<None>	ON	□ Configure	ON	ON	OFF
Illegal Access	<None>	ON	□ Configure	ON	ON	OFF
Network Disconnection	<None>	ON	□ Configure	ON	ON	OFF
HDD is pulled out	<None>	ON	□ Configure	ON	ON	OFF
Alarm Server Offline	<None>	ON	□ Configure	ON	ON	OFF

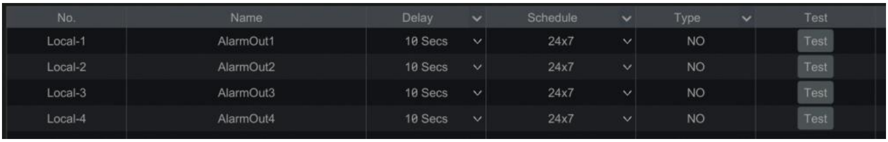
② Enable or disable “Push”, “Alarm-out”, “Buzzer”, “Pop-up Message Box” and “E-mail”. The exception handling settings are similar to that of the sensor alarm (see Sensor Alarm for details).

③ Click “Apply” to save the settings.

11.5 Alarm Event Notification

11.5.1 Alarm-out

① Click ***Start→Settings→AI/Event→Event Notification*** to go to the following interface.



No.	Name	Delay	Schedule	Type	Test
Local-1	AlarmOut1	10 Secs	24x7	NO	Test
Local-2	AlarmOut2	10 Secs	24x7	NO	Test
Local-3	AlarmOut3	10 Secs	24x7	NO	Test
Local-4	AlarmOut4	10 Secs	24x7	NO	Test

② Set the delay time the schedule and type of each alarm-out. You can click "Edit Schedules" to edit the schedules (see Schedule Settings for details).

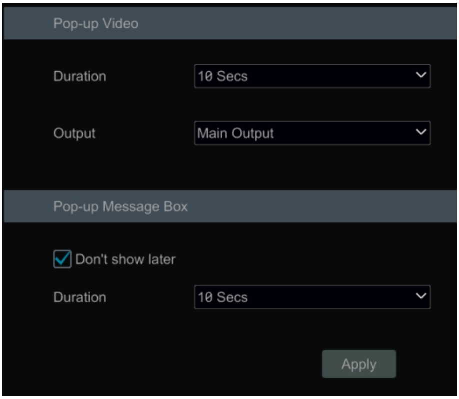
③ Click "Apply" to save the settings. You can click "Test" to test the alarm output.

11.5.2 E-mail

Click ***Start→Settings→AI/Event→Event Notification→E-mail*** to go to the e-mail configuration interface. Set the e-mail address of the recipients. See E-mail Configuration for details.

11.5.3 Display

Click ***Start→Settings→AI/Event→Event Notification→Display*** to go to the display configuration interface. Set the duration time of the pop-up video and the pop-up message box. If you device support two outputs, please set the output of the pop-up video as needed. After that, click "Apply" to save the settings.



Pop-up Video

Duration: 10 Secs

Output: Main Output

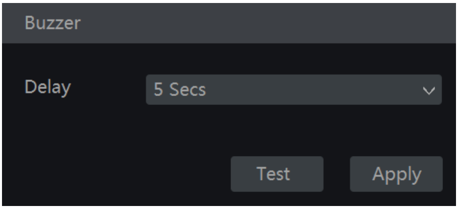
Pop-up Message Box

☑ Don't show later

Duration: 10 Secs

11.5.4 Buzzer

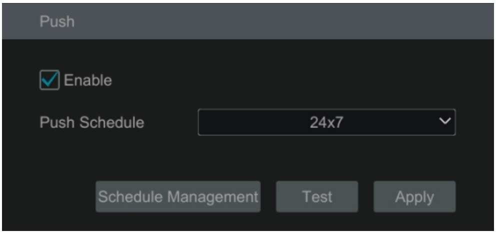
Click ***Start→Settings→AI/Event→Event Notification→Buzzer*** to go to the buzzer configuration interface. Set the delay time of the buzzer and then click "Apply" to save the setting. You can click "Test" to test the buzzer.



Delay: 5 Secs

11.5.5 Push

Click S***tart→Settings→ AI/Event →Event Notification→Push*** to go to the interface as shown below. Check "Enable", select the schedule and then click "Apply" to save the settings. If Push Server is online, it will push text to the mobile clients according to the set schedule.

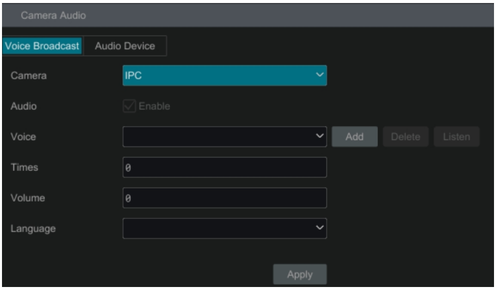


☑ Enable

Push Schedule: 24x7

11.5.6 Audio

Click ***Start→Settings→ AI/Event →Event Notification→Audio*** to go to the interface as shown below.



Camera: IPC

Audio: ☑ Enable

Voice:

Times: 0

Volume: 0

Language:

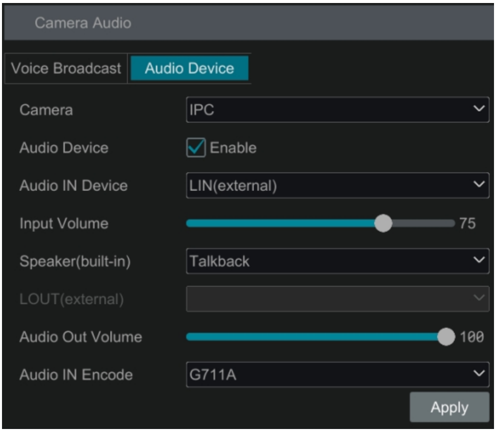
Camera audio settings:

For perimeter alert cameras, voice broadcast can be set up. Select the camera, voice, broadcast times, volume and language. Then click "Apply" to save the settings. When an alarm is triggered, the camera will broadcast the voice you set.

Audio: please enable or disable as needed. If your camera doesn't support this switch, this function is not available.

Voice: click "Add" to add the alarm voice in WAV format. Click "Listen" to listen to the uploaded audio.

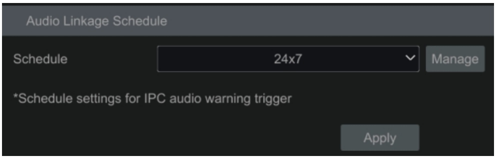
Click “Audio Device” to set the audio of the camera.



Camera	IPC
Audio Device	☑ Enable
Audio IN Device	LIN(external)
Input Volume	75
Speaker(built-in)	Talkback
LOUT(external)	
Audio Out Volume	100
Audio IN Encode	G711A

Select the camera and then enable audio device.
Audio IN Device: Please select it according to the actual device configuration.
Speaker (built-in): Please select its function as needed.
LOUT (Line Output): Select the function of the external audio device as needed.
Audio Input Encode: G711A/G711U
Note: The speaker (built-in) and LOUT (external) cannot be enabled simultaneously for some cameras. Please select it as needed.

Audio Linage Schedule: Set the schedule of audio linkage alarm. After the schedule is set, the audio alarm will be triggered by events within the schedule.



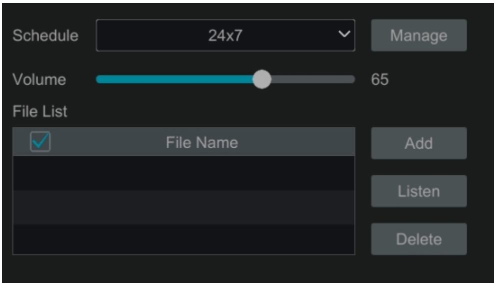
Schedule: 24x7

*Schedule settings for IPC audio warning trigger

Note: Only some perimeter alert cameras support schedule settings for audio alarm linkage.

Local Audio Alarm

Set the audio alarm of local NVR.



Schedule: 24x7

Volume: 65

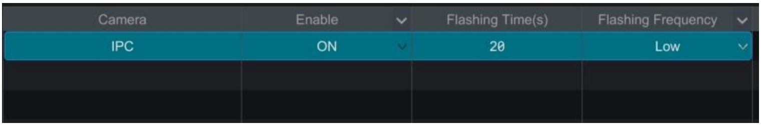
File List

☑	File Name

In this interface, you can set the schedule and volume of the local audio alarm. Click "Add" to upload the audio file (.mp3 format). Choose the uploaded audio file and then click "Listen" to listen to it; click "Delete" to delete this file.

11.5.7 Light

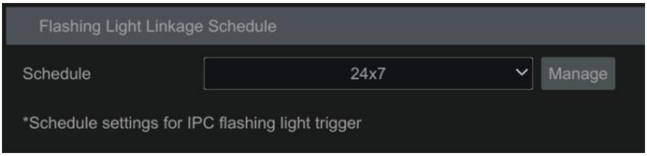
Click ***Start→Settings→Alarm→Event Notification→Light*** to go to the interface as shown below.



Camera	Enable	Flashing Time(s)	Flashing Frequency
IPC	ON	20	Low

In this interface, you can enable and set the light flashing time and frequency when an alarm is triggered.

Flashing light linkage schedule: Set the schedule of light linkage alarm. After the schedule is set, the light alarm will be triggered by events within the schedule.



Flashing Light Linkage Schedule

Schedule: 24x7

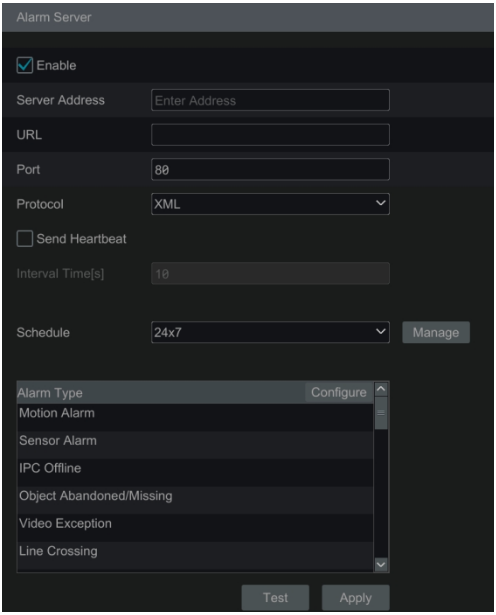
*Schedule settings for IPC flashing light trigger

Note: Only some perimeter alert cameras support schedule settings for light alarm linkage.

11.5.8 Alarm Server

Go to ***Alarm→Alarm Server*** interface as shown below.

Enable the alarm server and enter the server address, URL and port of the alarm server. Next, select the protocol. If "Send Heartbeat" is enabled, set the interval times. After that, test the effectiveness of the alarm server. After a successful test, please click "Apply". When an alarm occurs, the device will transfer the alarm event to the alarm server. If an alarm server is not needed, there is no need to configure this section.



Alarm Server

☑ Enable

Server Address: Enter Address

URL:

Port: 80

Protocol: XML

□ Send Heartbeat

Interval Time[s]: 10

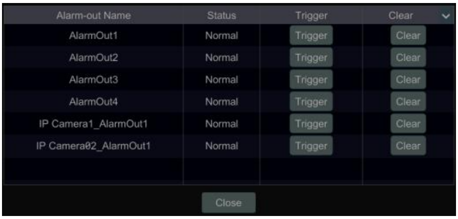
Schedule: 24x7 Manage

Alarm Type	Configure
Motion Alarm	
Sensor Alarm	
IPC Offline	
Object Abandoned/Missing	
Video Exception	
Line Crossing	

Test Apply

11.6 Manual Alarm

Click on the tool bar at the bottom of the live view interface to open a window. Click "Trigger" to start alarm. Click "Clear" to stop alarm.

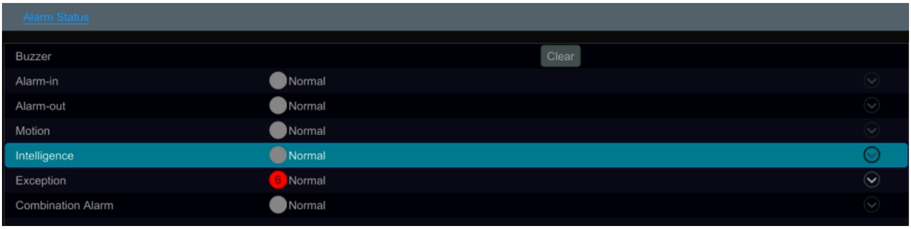


Alarm-out Name	Status	Trigger	Clear
AlarmOut1	Normal	Trigger	Clear
AlarmOut2	Normal	Trigger	Clear
AlarmOut3	Normal	Trigger	Clear
AlarmOut4	Normal	Trigger	Clear
IP Camera1_AlarmOut1	Normal	Trigger	Clear
IP Camera02_AlarmOut1	Normal	Trigger	Clear

Close

11.7 View Alarm Status

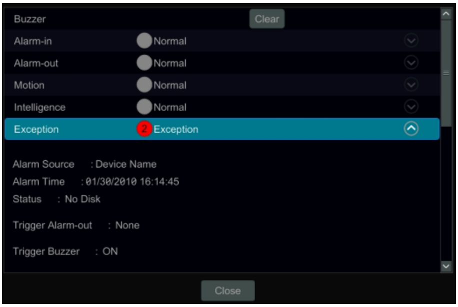
Click ***Start→Settings→Alarm→Alarm Status*** or click on the tool bar at the bottom of the live view interface to view the alarm status.



Alarm Status

Buzzer		Clear
Alarm-in	● Normal	⌄
Alarm-out	● Normal	⌄
Motion	● Normal	⌄
Intelligence	● Normal	⌄
Exception	6 Normal	⌄
Combination Alarm	● Normal	⌄

Click “Clear” to stop the buzzer when a buzzer alarm is triggered. Click ⌄ to view the detailed information as shown below.



Buzzer		Clear
Alarm-in	● Normal	⌄
Alarm-out	● Normal	⌄
Motion	● Normal	⌄
Intelligence	● Normal	⌄
Exception	2 Exception	⌃

Alarm Source : Device Name
Alarm Time : 01/30/2010 16:14:45
Status : No Disk

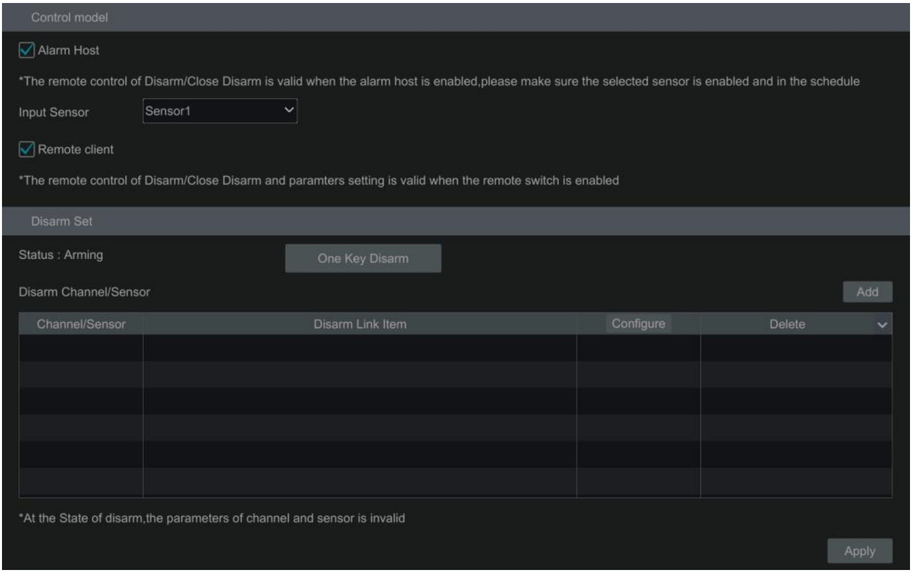
Trigger Alarm-out : None

Trigger Buzzer : ON

If the exception information is more than one page, you can enter the number in the box and then click ⇥ to jump to the specified page. Click < / > to view the exception alarm information in the previous/next page.

11.8 System Disarming

You can quickly disarm the device through the alarm host or a remote client (such as the mobile APP).



Control model

☑ Alarm Host

*The remote control of Disarm/Close Disarm is valid when the alarm host is enabled,please make sure the selected sensor is enabled and in the schedule

Input Sensor: Sensor1

☑ Remote client

*The remote control of Disarm/Close Disarm and paramters setting is valid when the remote switch is enabled

Disarm Set

Status : Arming

Disarm Channel/Sensor

Channel/Sensor	Disarm Link Item	Configure	Delete

*At the State of disarm,the parameters of channel and sensor is invalid

You can self-define the channels and sensors you want to disarm by clicking "Add". Only the selected channels and sensors can be disarmed by clicking "One Key Disarm".

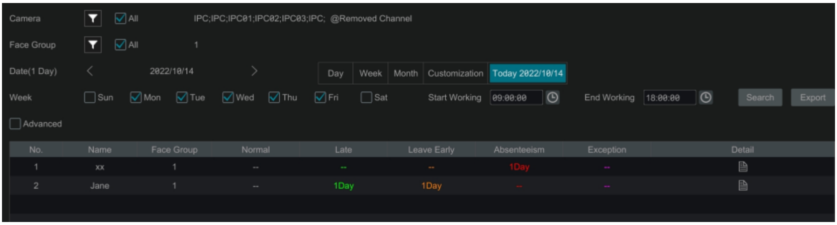
Note: If you want to control system disarm by a client, you must check "Remote client" in the above interface, or "One key disarm" function cannot be used in the client (like Web/APP client).

12 Application

12.1 Face Attendance

This function is only available for some models. If your device doesn't support it, please skip the following instructions.

Click ***Start→Application→Face Attendance*** to go to the following interface.



Camera ☑ All IPC;IPC;IPC01;IPC02;IPC03;IPC; @Removed Channel

Face Group ☑ All 1

Date(1 Day) < 2022/10/14 > Day Week Month Customization Today 2022/10/14

Week ☐ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☐ Sat Start Working 09:00:00 End Working 18:00:00 Search Export

☐ Advanced

No.	Name	Face Group	Normal	Late	Leave Early	Absenteeism	Exception	Detail
1	xx	1	--	--	--	1Day	--	📄
2	Jane	1	--	1Day	1Day	--	--	📄

To search attendance information

① Click behind camera and group to choose the desired cameras and groups.

② Set the attendance date. You can choose day, week, month and today or customize the time period.

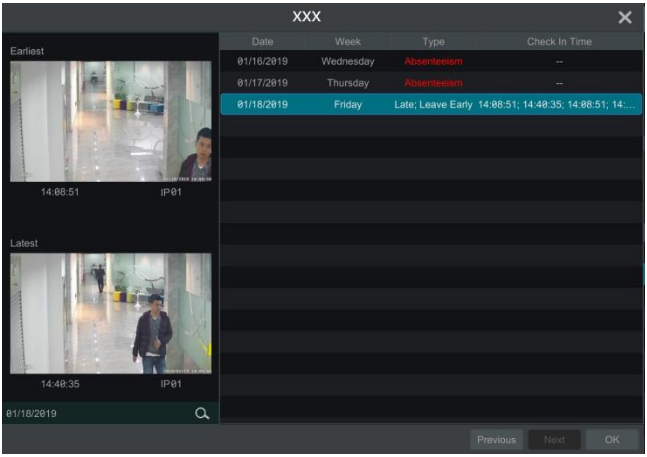
③ Set the start time and the end time of working.

④ Click "Search" to view the attendance state.

If you need to know the attendance status of a specific person, you can click "Advanced" and then enter the name and choose the type.

Click "Export" to export the searched attendance information.

Click to view the detailed information of attendance. In this interface, click to go to the face search interface.



XXX ✕

Earliest

14:08:51 IP01

Latest

14:40:35 IP01

01/18/2019

Date	Week	Type	Check In Time
01/16/2019	Wednesday	Absenteeism	--
01/17/2019	Thursday	Absenteeism	--
01/18/2019	Friday	Late; Leave Early	14:08:51; 14:40:35; 14:08:51; 14:...

12.2 Face Check-In

Click ***Start→Application→Face Check-In*** to go to the following interface.

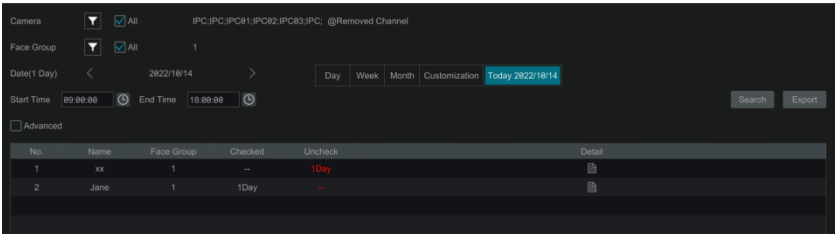
The search steps of face check-in are as follows.

① Click behind camera and group to choose the desired cameras and groups.

② Set the check-in date. You can choose day, week, month and today or customize the time period.

③ Set the start time and the end time of face check-in.

④ Click "Search" to view the check-in state.



Camera ☑ All IPC;IPC;IPC01;IPC02;IPC03;IPC; @Removed Channel

Face Group ☑ All 1

Date(1 Day) < 2022/10/14 >

Day | Week | Month | Customization | Today 2022/10/14

Start Time 09:00:00 End Time 18:00:00

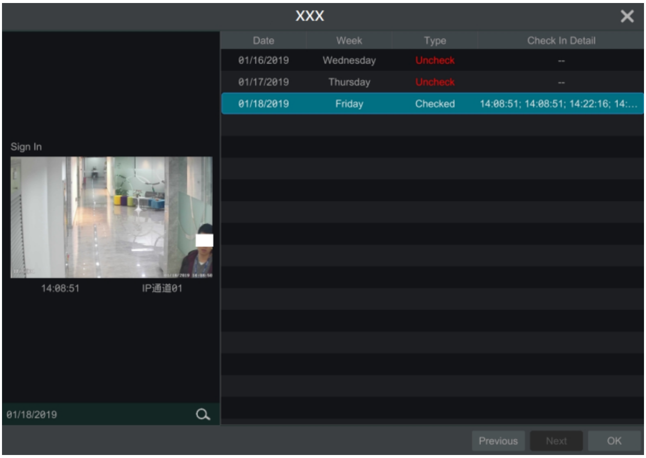
□ Advanced

No.	Name	Face Group	Checked	Uncheck	Detail
1	xx	1	--	1Day	🗎
2	Jane	1	1Day	--	🗎

If you want to know the check-in status of a specific person, please click "Advanced" and then enter the name and choose the type to search.

Click 🗎 to view the detailed information. In this interface, the checked image can be viewed.

Click 🔍 to view the registered face picture of this person.



XXX

Date	Week	Type	Check In Detail
01/16/2019	Wednesday	Uncheck	--
01/17/2019	Thursday	Uncheck	--
01/18/2019	Friday	Checked	14:08:51; 14:08:51; 14:22:16; 14:...

Sign In

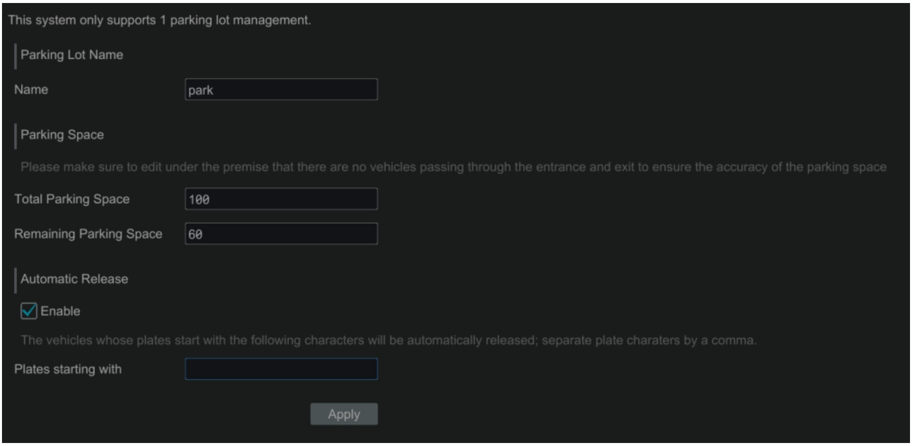
14:08:51 IP通道01

01/18/2019

12.3 Parking Lot Settings

You can manage the parking lot through the NVR. Before using this function, please add the professional ANPR camera.

Click ***Start→Application→Parking Lot Management*** to go to the parking lot setting interface.



This system only supports 1 parking lot management.

Parking Lot Name

Name: park

Parking Space

Please make sure to edit under the premise that there are no vehicles passing through the entrance and exit to ensure the accuracy of the parking space

Total Parking Space: 100

Remaining Parking Space: 60

Automatic Release

☑ Enable

The vehicles whose plates start with the following characters will be automatically released; separate plate charaters by a comma.

Plates starting with:

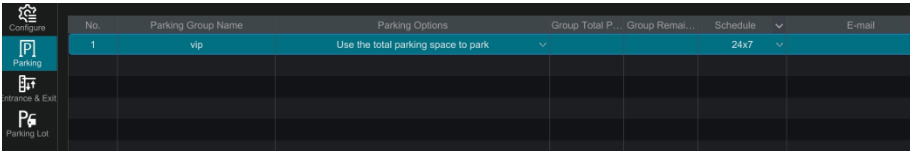
12.3.1 Basic Settings

The recorder only supports the management of one parking lot. Please enter the parking lot name, total parking spaces and remaining parking spaces as needed. To ensure the accuracy of the parking spaces, please enter the parking space information while there are no vehicles entering or exiting.

Automatic Release: The barrier gate can be automatically opened for special vehicles after enabling automatic release and enter the special characters. If you want to automatically release multiple vehicle types whose plates starting with special characters, you can enter and separate them with commas (,).

12.3.2 Parking Space Settings

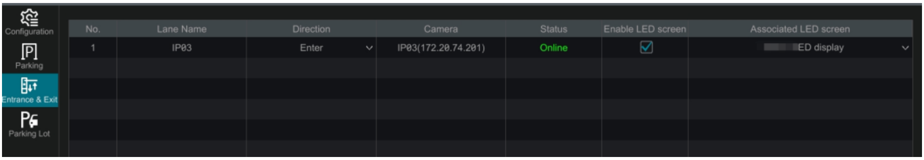
Only the vehicles added into the plate database with the proper permission are allowed to pass through automatically. You can set the parking spaces according to the vehicle groups or directly use the total parking spaces. For the block list, you can set "No parking allowed". After that, set the schedule and Email as needed.



No.	Parking Group Name	Parking Options	Group Total P...	Group Remai...	Schedule	E-mail
1	vip	Use the total parking space to park			24x7	

12.3.3 Entrance/Exit Management

Set the passing direction of vehicles (Enter/Exit/Enter and Exit) and bind LED screen as needed.



No.	Lane Name	Direction	Camera	Status	Enable LED screen	Associated LED screen
1	IP03	Enter	IP03(172.20.74.201)	Online	☑	[redacted]ED display

Direction: choose "Close", "Enter", "Exit" or "Enter and Exit" as needed.

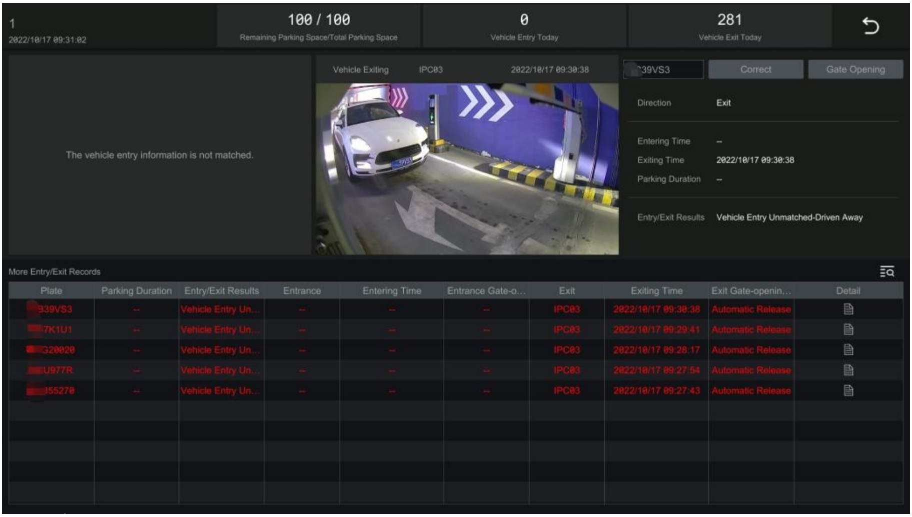
If "Close" is selected, the LPR/ANPR camera is only used to recognize plates and doesn't trigger the relevant parking management function.

If you want to manage vehicles entering and leaving a park by one LPR/ANPR camera, it is suggested to select "Enter and Exit". In this way, vehicles entering the park trigger alarms by default, but vehicles leaving the park don't trigger alarms. Vehicles entering/leaving are classified by recognition mode of the LPR/ANPR camera (recognizing when approaching or driving away). When there is a vehicle approaching, the LPR/ANPR camera captures and reports its license plate, the direction is recognized as "Enter" and the NVR analyzes whether the parking spaces are full. If there are remaining parking spaces, it will open the gate barrier and reduce a remaining parking space. If the parking spaces are full, the gate barrier will not be opened. When a vehicle is been driving away, the barrier gate is controlled by the ground sense coil, the LPR/ANPR camera captures and reports its license plate, the direction is recognized as "Exit/Leave" and the NVR increases a parking space.

Note: Only some LPR/ANPR cameras can simultaneously manage the entry and exiting of vehicles. If "Enter" or "Exit" is selected, the set direction shall prevail.

12.3.4 Parking Lot Management

After the above settings are completed, click “Parking Lot” on the left menu to go to the following interface.



1
2022/10/17 09:31:02

100 / 100
Remaining Parking Space/Total Parking Space

0
Vehicle Entry Today

281
Vehicle Exit Today

The vehicle entry information is not matched.

Vehicle Exiting IPC03 2022/10/17 09:30:38

[redacted]39VS3 Correct Gate Opening

Direction Exit

Entering Time --
Exiting Time 2022/10/17 09:30:38
Parking Duration --

Entry/Exit Results Vehicle Entry Unmatched-Driven Away

More Entry/Exit Records

Plate	Parking Duration	Entry/Exit Results	Entrance	Entering Time	Entrance Gate-o...	Exit	Exiting Time	Exit Gate-openin...	Detail
[redacted]39VS3	--	Vehicle Entry Un...	--	--	--	IPC03	2022/10/17 09:30:38	Automatic Release	🗎
[redacted]7K1U1	--	Vehicle Entry Un...	--	--	--	IPC03	2022/10/17 09:29:41	Automatic Release	🗎
[redacted]G20020	--	Vehicle Entry Un...	--	--	--	IPC03	2022/10/17 09:28:17	Automatic Release	🗎
[redacted]U977R	--	Vehicle Entry Un...	--	--	--	IPC03	2022/10/17 09:27:54	Automatic Release	🗎
[redacted]55270	--	Vehicle Entry Un...	--	--	--	IPC03	2022/10/17 09:27:43	Automatic Release	🗎

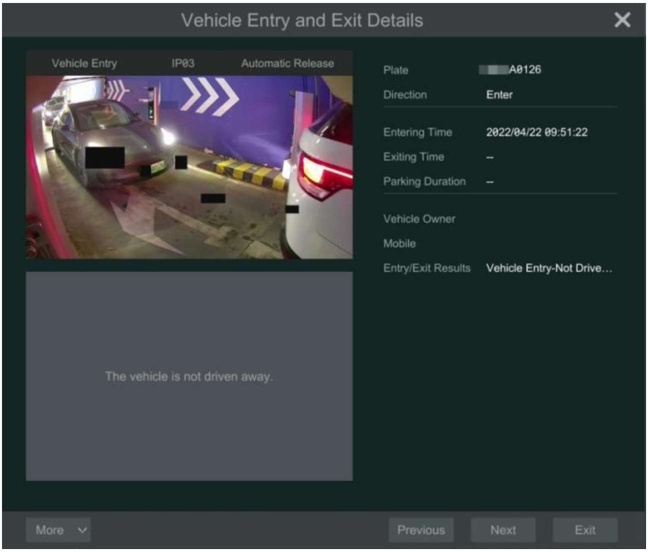
In this interface, you can view the detailed information of the parking lot, including the total parking space, remaining parking space, number of vehicle entering today, number of vehicle exiting today and vehicle entry/exit records.

Only vehicles added into the plate database are allowed to pass automatically. If the vehicle is a stranger/unknown vehicle, it will not be allowed to enter unless it is manually approved. You can release it manually by clicking “Gate Opening”. While entering, if the plate number captured is not matched with the actual one, you can click “Correct” to correct it manually.

Click 🗎 to view the detail information of vehicle entry/exiting.

Click “More” to register the license plate or view the ID information.

Click ☰🔍 to go to search the records of vehicles entering/exiting.



Vehicle Entry and Exit Details

Vehicle Entry IP03 Automatic Release

Plate [redacted]A0126
Direction Enter
Entering Time 2022/04/22 09:51:22
Exiting Time --
Parking Duration --
Vehicle Owner
Mobile
Entry/Exit Results Vehicle Entry-Not Drive...

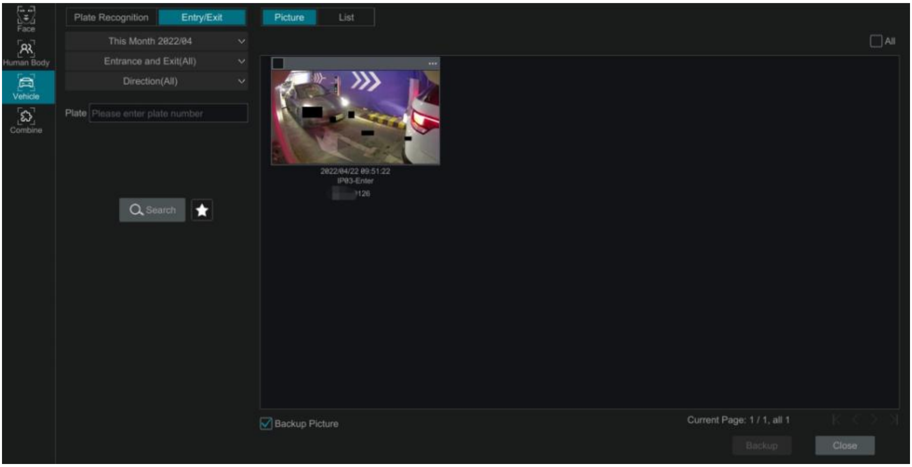
The vehicle is not driven away.

Click “⮌” to return to the live view interface.

12.3.5 Search Vehicle Entry/Exiting Records

In the parking lot management interface, click ☰🔍 to search the records of vehicles entering/exiting the park lot.

You can search these records by setting filtering conditions (including time/direction/license plate). Click ••• in the right corner of the searched picture to view the details; click “Backup” to export the searched picture.



This Month 2022/04
Entrance and Exit(All)
Direction(All)
Plate Please enter plate number

□ All

2022/04/22 09:51:22
IP03-Enter
[redacted]126

☑ Backup Picture

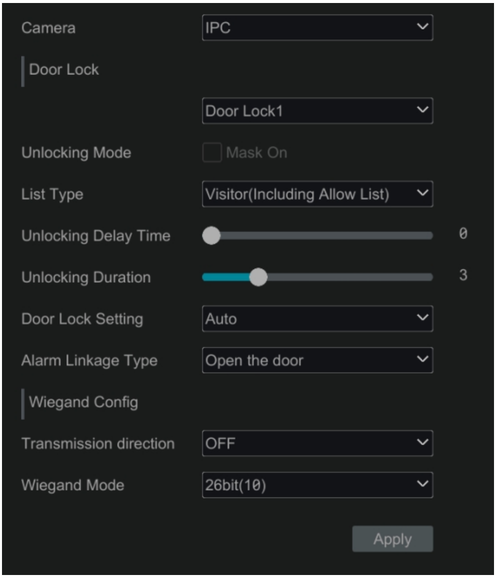
Current Page: 1 / 1, all 1

12.4 Access Control Management

The recorder supports access control parameter configuration and remote door opening. Before using the access control function, please add access control devices (face recognition & access control terminal/panel). Go to ***Start→Settings→Camera→Add Camera*** interface to add devices.

12.4.1 Access Control Settings

Click ***Start→Application→Access Control Management*** to go to the following interface.



Camera: IPC

Door Lock

Door Lock1

Unlocking Mode: □ Mask On

List Type: Visitor(Including Allow List)

Unlocking Delay Time: 0

Unlocking Duration: 3

Door Lock Setting: Auto

Alarm Linkage Type: Open the door

Wiegand Config

Transmission direction: OFF

Wiegand Mode: 26bit(10)

Select the access control device you want to configure the parameters.

Lock: Choose the lock you want to control.

Unlocking Mode: if "Mask On" is selected, the door will be opened when the matched person wearing a mask

List Type: Allow list, visitor (including allow list), stranger (including visitor and allow list).

Unlocking Delay Time: Set the door unlocking delay time. The time range is from 0 to 10 seconds. For example, the unlocking mode is "Face only" and the delay time is set to "2" seconds; the door will be opened 2 seconds later after face recognition.

Unlocking Duration: If the door has been unlocked for a period that exceeds the duration, the door will be automatically locked. The time range is from 0 to 10 seconds. For example, the unlocking mode is "Face only" and the duration is set to "3" seconds; the unlocking door will be automatically locked 3 seconds later.

Door Lock Setting: Choose "Auto", "NO" or "NC". Please select it according to your door lock type.

Alarm Linkage Type: Open/close the door

Wiegand Config: Wiegand Input, Wiegand Output or Off can be selected. If the card reader is connected to the Wiegand interface, please select “Wiegand Input”. If the access controller is connected to the Wiegand interface, please select “Wiegand Output”.

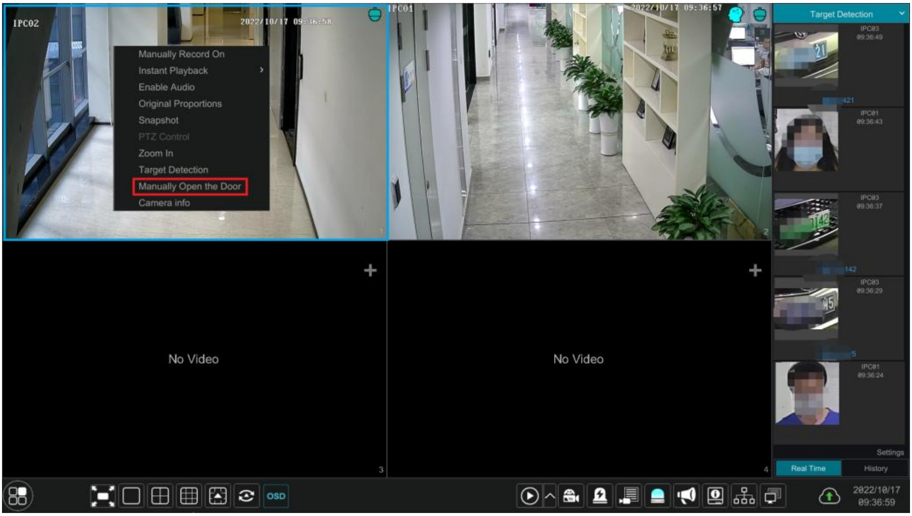
Wiegand Mode: 26bit(8), 26bit(10), 34bit, 37bit, 42bit, 46bit, 58bit or 66bit can be selectable.

After clicking “Apply”, the configuration will be synchronized with the camera.

When someone wants to enter, the access control device will open the door according to the set condition.

12.4.2 Open the Door Manually

In the live view interface, select an access control camera. Right click on the window to pop up a dropdown list. Select “Manually Open the Door” to open the door via the NVR.

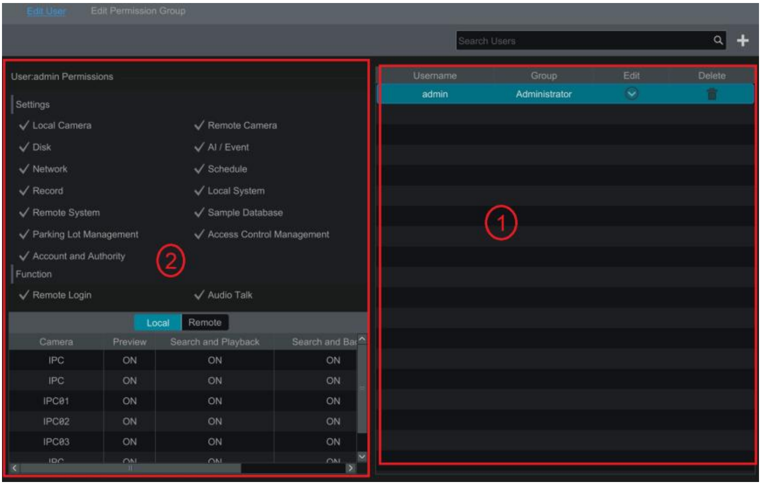


If you want to view the real-time face snapshots and comparison of access control devices, please enable face detection or comparison function as needed. Then the corresponding results will display under the target detection tab in the live interface.

13 Account & Permission Management

13.1 Account Management

Click ***Start→Settings→Account and Authority→Account→Edit User*** to go to the interface as shown below.



User:admin Permissions

Settings

- ✓ Local Camera
- ✓ Disk
- ✓ Network
- ✓ Record
- ✓ Remote System
- ✓ Parking Lot Management
- ✓ Account and Authority
- ✓ Remote Camera
- ✓ AI / Event
- ✓ Schedule
- ✓ Local System
- ✓ Sample Database
- ✓ Access Control Management

Function

- ✓ Remote Login
- ✓ Audio Talk

Local Remote

Camera	Preview	Search and Playback	Search and Ba
IPC	ON	ON	ON
IPC	ON	ON	ON
IPC01	ON	ON	ON
IPC02	ON	ON	ON
IPC03	ON	ON	ON
IPC	ON	ON	ON

Username	Group	Edit	Delete
admin	Administrator		

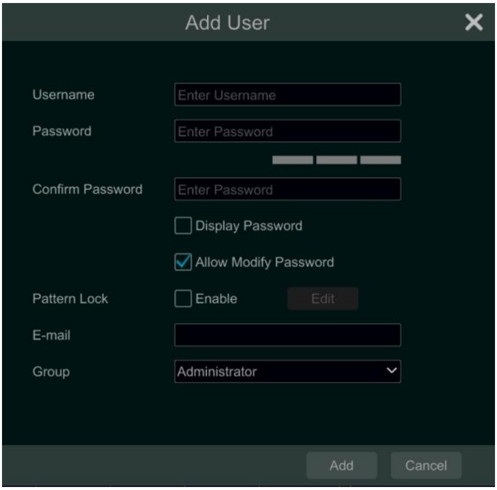
Area ① displays the user permissions. Area ② displays the user list. Click the user in the list to display its user permissions in area ①.

There are three default permission groups ("Administrator", "Advanced" and "Common") available when adding accounts. You can manually add new permission group (see Add Permission Group for details).

Only ***admin*** and the users that have the "Account and Authority" permission can manage the system's accounts. Group "Administrator" owns all the permissions displayed in area ① except "Account and Authority" and its permissions cannot be changed while the permissions of "Advanced" and "Common" can be changed.

13.1.1 Add User

① Click ***Start→Settings→Account and Authority→Account→Add User*** or click + beside the search box to open a window as shown below.



Add User

Username: Enter Username

Password: Enter Password

Confirm Password: Enter Password

□ Display Password

☑ Allow Modify Password

Pattern Lock: □ Enable Edit

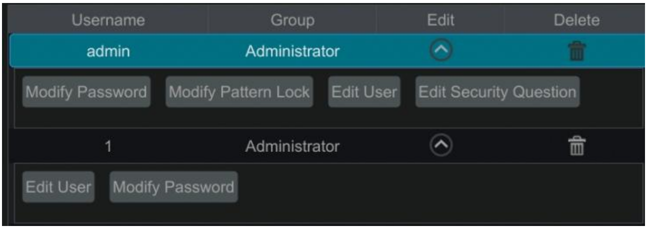
E-mail:

Group: Administrator

② Set the username, password and group. User can also set the pattern lock and e-mail address as needed. Click "Add" to add the user.

13.1.2 Edit User

Click ***Start→Settings→Account and Authority→Account→Edit User*** and then click ⌄ in the user list or double click the user to edit the user information. Click 🗑 to delete the user (the user ***admin*** cannot be deleted).



Username	Group	Edit	Delete
admin	Administrator	⌃	🗑
Modify Password Modify Pattern Lock Edit User Edit Security Question			
1	Administrator	⌃	🗑
Edit User Modify Password			

➢ **Edit Security Question**

You can set password security only for ***admin***. Click "Edit Security Question" and then set questions and answers in the popup window. If you forget the password for ***admin***, please refer to Q4 in Appendix A FAQ for details. The passwords of other users can be recovered by ***admin*** or the users that have the "Account and Authority" permission.

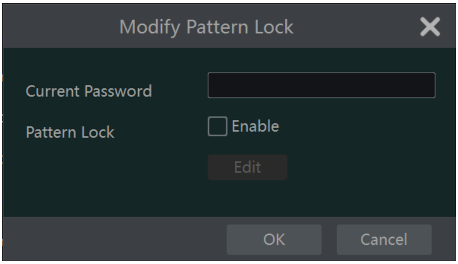
➢ **Modify Password**

The password of ***admin*** can be modified. Click "Modify Password" to pop up a window. Enter the current password and then set new password. Click "OK" to save the settings.

In addition, the admin user can modify the common/advanced user's password.

Modify Pattern Lock

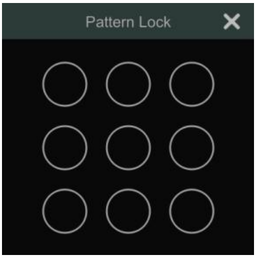
Some models may not support this function.
Click “Modify Pattern Lock” to pop up a window.



Current Password

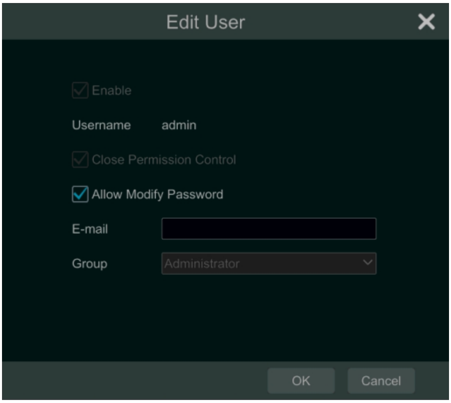
Pattern Lock □ Enable

Input current password and then check “Enable” to set pattern lock.



Edit User

Click “Edit User” to pop up the window as shown below. The ***admin*** is enabled, its permission control is closed and permission group cannot be changed by default. You can enable or disable other users (if disabled, the user will be invalid), open or close their permission control (if closed, the user will get all the permissions which ***admin*** has) and set their permission groups. Click “OK” to save the settings.



☑ Enable

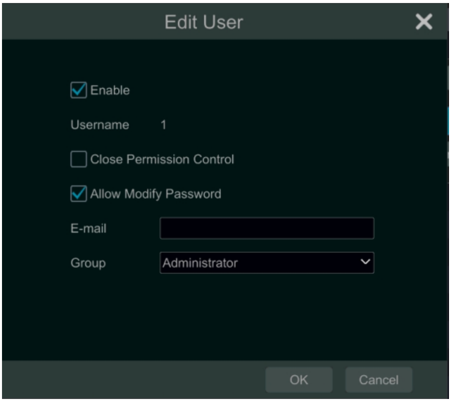
Username admin

☑ Close Permission Control

☑ Allow Modify Password

E-mail

Group Administrator



☑ Enable

Username 1

□ Close Permission Control

☑ Allow Modify Password

E-mail

Group Administrator

13.2 User Login & Logout

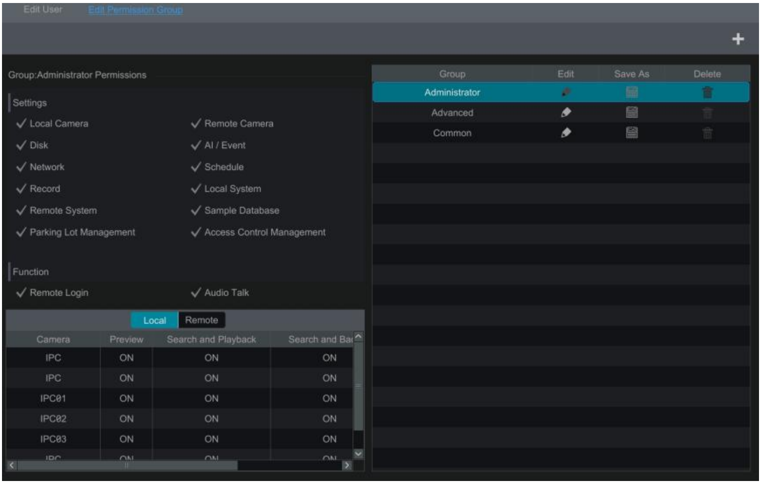
Login: Click ***Start→Login*** or directly click the preview interface and then select username and enter the password in the popup window. Click the "Login" button to log in the system.

Logout: Click ***Start→Logout*** or click ***Start→Shutdown*** to pop up the "Shutdown" window. Select "Logout" in the window and then click "OK" to log out the system.

13.3 Permission Management

13.3.1 Add Permission Group

Click ***Start→Settings→Account and Authority→Account→Edit Permission Group*** to go to the interface as shown below.



Group:Administrator Permissions

Settings

- ✓ Local Camera
- ✓ Disk
- ✓ Network
- ✓ Record
- ✓ Remote System
- ✓ Parking Lot Management
- ✓ Remote Camera
- ✓ AI / Event
- ✓ Schedule
- ✓ Local System
- ✓ Sample Database
- ✓ Access Control Management

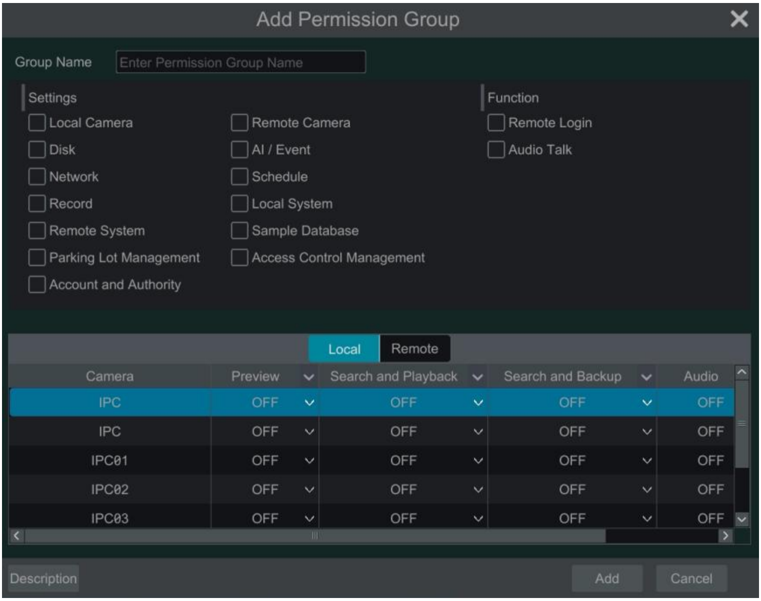
Function

- ✓ Remote Login
- ✓ Audio Talk

Camera	Preview	Search and Playback	Search and Ba
IPC	ON	ON	ON
IPC	ON	ON	ON
IPC01	ON	ON	ON
IPC02	ON	ON	ON
IPC03	ON	ON	ON
IPC	ON	ON	ON

Group	Edit	Save As	Delete
Administrator	✎	🖫	🗑
Advanced	✎	🖫	🗑
Common	✎	🖫	🗑

Click + to add permission group. Set the group name, check the permissions as needed and then set the "Local" and "Remote" permissions. Click "Add" to save the settings.



Add Permission Group ✕

Group Name: Enter Permission Group Name

Settings

- □ Local Camera
- □ Disk
- □ Network
- □ Record
- □ Remote System
- □ Parking Lot Management
- □ Account and Authority
- □ Remote Camera
- □ AI / Event
- □ Schedule
- □ Local System
- □ Sample Database
- □ Access Control Management

Function

- □ Remote Login
- □ Audio Talk

Local | Remote

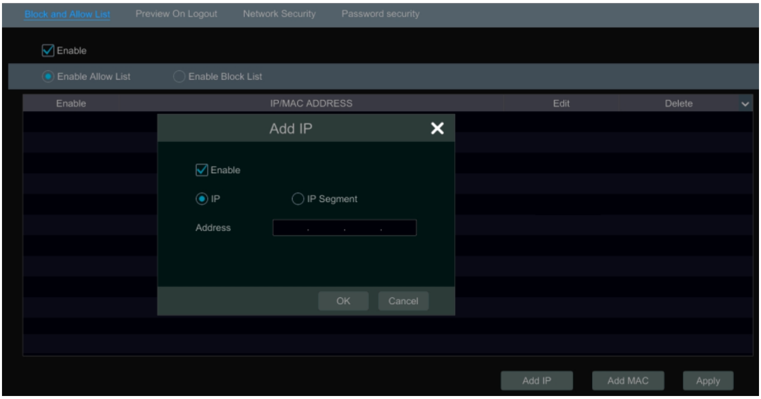
Camera	Preview	Search and Playback	Search and Backup	Audio
IPC	OFF	OFF	OFF	OFF
IPC	OFF	OFF	OFF	OFF
IPC01	OFF	OFF	OFF	OFF
IPC02	OFF	OFF	OFF	OFF
IPC03	OFF	OFF	OFF	OFF

13.3.2 Edit Permission Group

Go to "Edit Permission Group" interface and then click ✎ in the group list to edit the permission group (the operations of the "Edit Permission Group" are similar to that of the "Add Permission Group", please see Add Permission Group for details). Click 💾 to save the group as another group. Click 🗑 to delete the permission group. The three default permission groups ("Administrator", "Advanced" and "Common") cannot be deleted.

13.4 Black and White List

① Click ***Start→Settings→Account and Authority→Security*** to go to the following interface.



☑ Enable

● Enable Allow List ○ Enable Block List

Enable	IP/MAC ADDRESS	Edit	Delete

Add IP ✕

☑ Enable

● IP ○ IP Segment

Address: . . .

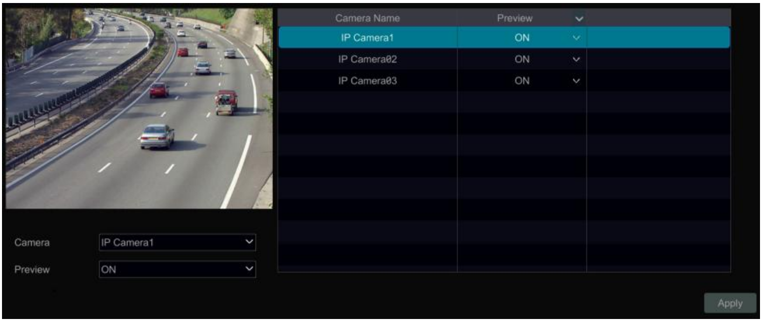
② Check “Enable” and then choose “Enable Allow List (white list)” or “Enable Block List (black list)” (the PC client of which the IP address is in the white list can access NVR remotely while the PC client in the black list cannot).

③ Add IP/IP segment/MAC. Click “Add IP” or “Add MAC” and then check “Enable” in the popup window (only if you check it can the IP/IP segment/MAC you add be effective). Enter the IP/IP segment/MAC and then click “OK”. In the above interface, click ✎ to edit IP/IP segment/MAC, click 🗑 to delete it. Click “Apply” to save the settings.

13.5 Preview on Logout

Click ***Start→Settings→Account and Authority→Security→Preview on Logout*** to go to the following interface.

Set a camera and then enable or disable the preview permission on logout as needed. If a camera’s preview permission on logout is “ON”, you can view the live image of the camera when the system is logged out, or the live image of the camera cannot be seen when logged out.



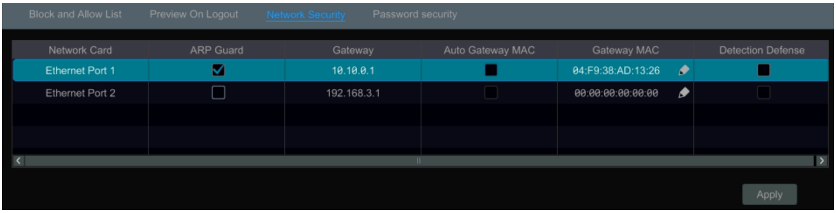
Camera Name	Preview
IP Camera1	ON
IP Camera02	ON
IP Camera03	ON

Camera: IP Camera1

Preview: ON

13.6 Network Security

Click ***Start→Settings→Account and Authority→Security→Network Security*** to go to the following interface. You can enable APR Guard.

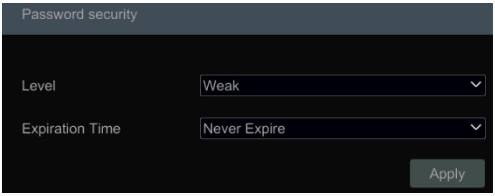


Network Card	ARP Guard	Gateway	Auto Gateway MAC	Gateway MAC	Detection Defense
Ethernet Port 1	☑	10.10.0.1	■	04:F9:38:AD:13:26 ✎	■
Ethernet Port 2	□	192.168.3.1	□	00:00:00:00:00:00 ✎	□

ARP (Address Resolution Protocol) Guard: This function can protect the LAN from ARP attacks and increase the network stability. If it is enabled, you can enable auto gateway MAC or manually set gateway MAC. Additionally, detection defense also can be enabled as needed.

13.7 Password Security

Click ***Start→Settings→Account and Authority→Security→Password Security*** to go to the following interface.



Password security

Level: Weak

Expiration Time: Never Expire

In this interface, you can set the security level and expiration time of the password. It's recommended to force a new password periodically to enhance system security.

13.8 View Online User

Click ***Start→Settings→Account and Authority→User Status*** to view the online user information (you can view the online user name, login type, IP address and login time; click 🗎 to open a window showing the preview occupied channel number and playback occupied channel number).

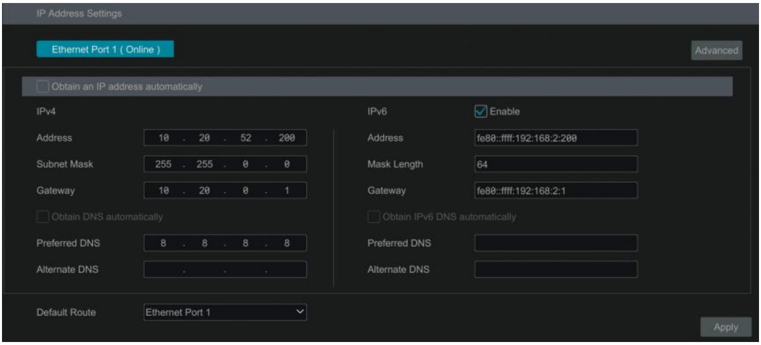
14 Device Management

14.1 Network Configuration

14.1.1 TCP/IP Configuration

Click ***Start→Settings→Network→TCP/IP*** to go to the following interface. Check “Obtain an IP address automatically”, and “Obtain DNS automatically” to get the IPv4/IPv6 (if IPv6 is enabled) address automatically, or manually enter the network addresses. You can modify the MTU value according to the network condition (MTU, Maximum Transmission Unit, can be modified according to network condition for higher network transmission efficiency). Click “Apply” to save your settings.

Additionally, if you want to configure multiple IP addresses for a single network card (for example: add devices from different network segments under the same switch), you can click “Advanced” to set a secondary IP address.



IP Address Settings

Ethernet Port 1 (Online) Advanced

□ Obtain an IP address automatically

IPv4		IPv6	☑ Enable
Address	10 . 20 . 52 . 200	Address	fe80::ffff:192:168:2:200
Subnet Mask	255 . 255 . 0 . 0	Mask Length	64
Gateway	10 . 20 . 0 . 1	Gateway	fe80::ffff:192:168:2:1
□ Obtain DNS automatically		□ Obtain IPv6 DNS automatically	
Preferred DNS	8 . 8 . 8 . 8	Preferred DNS	
Alternate DNS	. . .	Alternate DNS	

Default Route: Ethernet Port 1

Apply

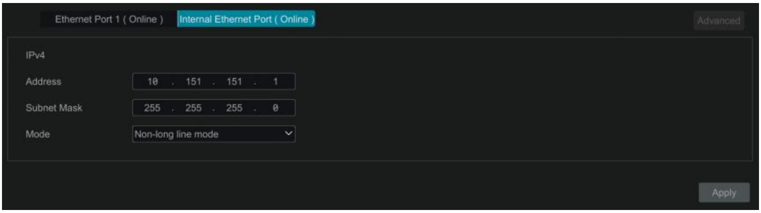
Note:

Internal Ethernet Port

If you use an NVR with PoE network ports, click “Internal Ethernet Port” to go to the interface below.

The internal Ethernet port is the port which connects all PoE ports with the NVR system. The PoE ports are available if the internal Ethernet port is online; if it is offline, all the PoE ports will be unavailable and it’s possible there’s an issue with the Ethernet port. The network address of the internal Ethernet port can be changed to be in the same network segment as IP cameras which are directly connected to the PoE ports of the NVR (Note that it is not recommended to change the network address of the internal Ethernet port).

Mode: Non-long line mode or long line mode can be selectable. The non-line mode is the default setting. If you want to run your PoE cameras longer than the standard 100M distance, you can choose long line mode. The tradeoff will be that your network speed on all PoE ports will drop to 10MBPs.


Ethernet Port 1 (Online) | Internal Ethernet Port (Online)

IPv4

Address: 10 . 151 . 151 . 1

Subnet Mask: 255 . 255 . 255 . 0

Mode: Non-long line mode

- **Multiple Ethernet Ports Setting**

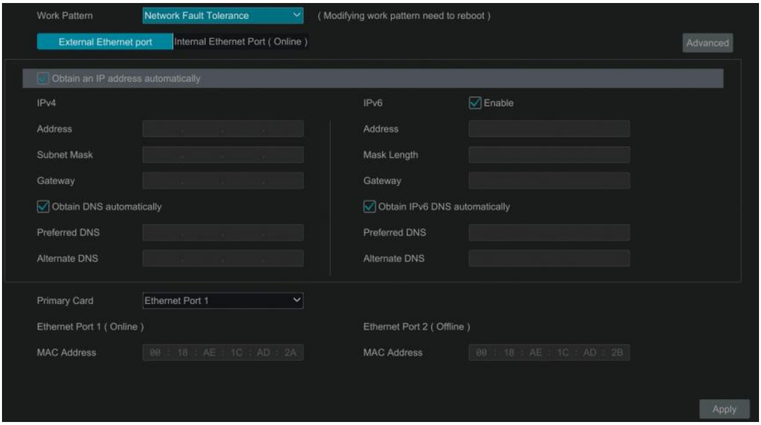
If the NVR has two network ports or above, you can select the network work pattern as required.

TOE: Some models may support TOE mode. It is a technology for improving the network transmission speed. Please enable it according to the actual network situation. If TOE is enabled, it shall be high speed mode. Then multiple address setting or network fault tolerance can be chosen and configured. If TOE is not enabled, it shall be compatible mode. Then the network fault tolerance cannot be selected and set up.

Network Fault Tolerance:

The two network ports will be bound to one IP address if you select the “Network Fault Tolerance” pattern. There are many advantages of this work pattern: 1. increase the bandwidth; 2. form a network redundant array to share the load. When a failure happens to one network port, the other port will take over the entire load immediately. The takeover process is seamless and the network service will not be broken off.

Refer to the figure as shown below. If “Network Fault Tolerance” is selected, check “Obtain an IPv4 address automatically”, and “Obtain DNS automatically” to get the network addresses automatically, or manually enter IPv4/IPv6(if IPv6 is enabled) address select one Ethernet port as the primary card and then click “Apply” to save the settings.


Work Pattern: Network Fault Tolerance (Modifying work pattern need to reboot)

External Ethernet port | Internal Ethernet Port (Online)

☑ Obtain an IP address automatically

IPv4

Address

Subnet Mask

Gateway

☑ Obtain DNS automatically

Preferred DNS

Alternate DNS

IPv6 ☑ Enable

Address

Mask Length

Gateway

☑ Obtain IPv6 DNS automatically

Preferred DNS

Alternate DNS

Primary Card: Ethernet Port 1

Ethernet Port 1 (Online)

MAC Address: 00 : 18 : AE : 1C : AD : 2A

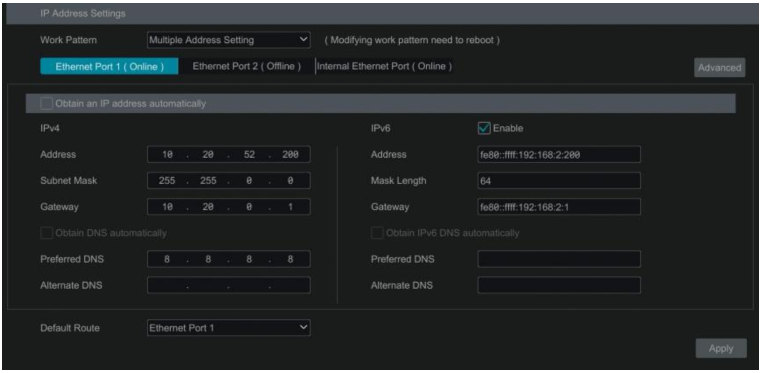
Ethernet Port 2 (Offline)

MAC Address: 00 : 18 : AE : 1C : AD : 2B

Multiple Address Setting:

If "Multiple Address Setting" is selected, the IP addresses of the two Ethernet ports should be set respectively. Refer to the picture as shown below.

Check "Obtain an IP address automatically" and "Obtain DNS automatically" to get the network addresses automatically, or manually enter IPv4/IPv6(if IPv6 is enabled) address; select one Ethernet port as the default route and then click "Apply" to save the settings.



IP Address Settings

Work Pattern: Multiple Address Setting (Modifying work pattern need to reboot)

Ethernet Port 1 (Online) | Ethernet Port 2 (Offline) | Internal Ethernet Port (Online)

□ Obtain an IP address automatically

IPv4
- Address: 10 . 20 . 52 . 200
- Subnet Mask: 255 . 255 . 0 . 0
- Gateway: 10 . 20 . 0 . 1
- □ Obtain DNS automatically
- Preferred DNS: 8 . 8 . 8 . 8
- Alternate DNS: . . .

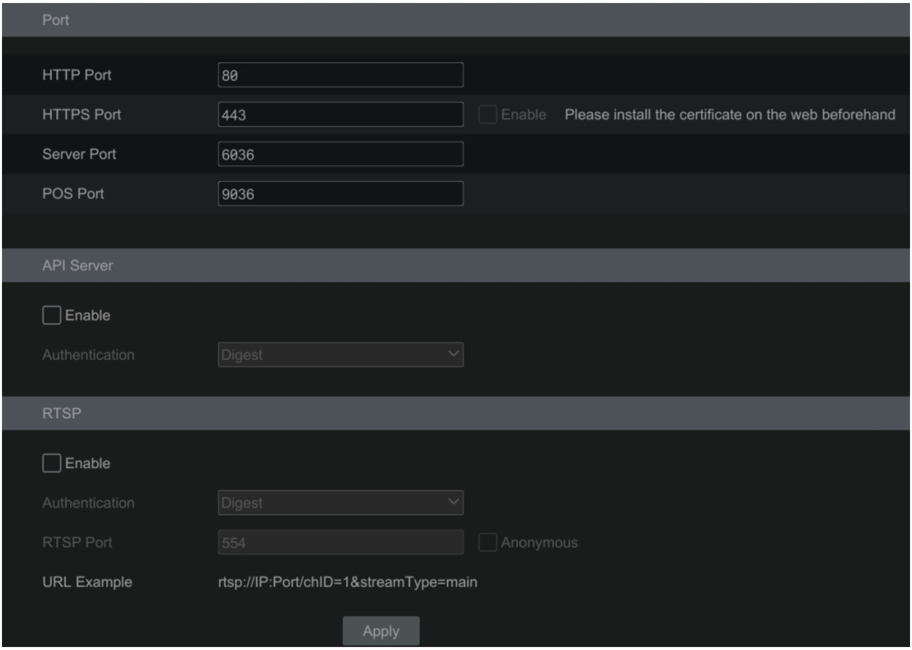
IPv6 ☑ Enable
- Address: fe80::ffff:192:168:2:200
- Mask Length: 64
- Gateway: fe80::ffff:192:168:2:1
- □ Obtain IPv6 DNS automatically
- Preferred DNS:
- Alternate DNS:

Default Route: Ethernet Port 1

Note: The above interface may be different for different models. The above picture are for reference only.

14.1.2 Port Configuration

Click ***Start→Settings→Network→Port*** to go to the interface as shown below. Enter the HTTP port, HTTPS port, server port and POS port of the NVR, and then click "Apply" to save the settings. You can also enable and set RTSP port (please check "Anonymous" as required).



Port

HTTP Port: 80

HTTPS Port: 443 □ Enable Please install the certificate on the web beforehand

Server Port: 6036

POS Port: 9036

API Server

□ Enable

Authentication: Digest

RTSP

□ Enable

Authentication: Digest

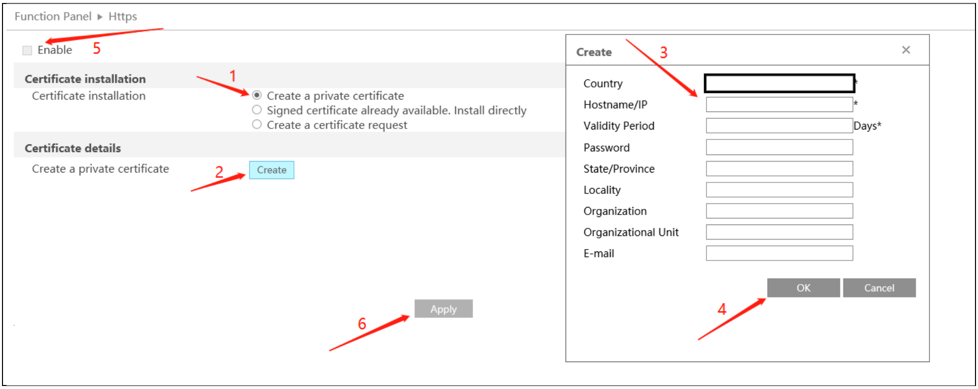
RTSP Port: 554 □ Anonymous

URL Example: rtsp://IP:Port/chID=1&streamType=main

HTTP Port: the default HTTP port of the NVR is 80. The port number can be changed to another number such as 81. The port is mainly used for web client access. If you want to access the NVR through a web browser, you should enter the IP address plus HTTP port in the address bar of the web browser like http://192.168.11.61:81.
Note: The HTTP port and server port of the NVR should be mapped to the router before you access the NVR via WAN.

HTTPS Port: the default HTTPs port of the NVR is 443.
HTTPs provides authentication of the web site and protects user privacy. You can enter IP address plus HTTPs port in the address bar of the web browser. Then enter username and password to log in. Click Functional Panel→Network→HTTPS to go to the following interface. There are three ways to enable HTTPs service.

A. Create a private certificate.



① Select "Create a private certificate".

② Click "Create".

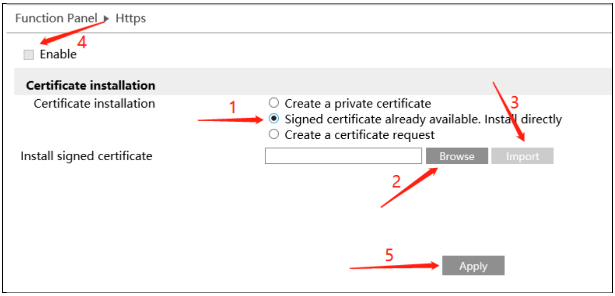
③ Fill out the corresponding information in the above creation box. Enter the country (only two letters available), domain (NVR's IP address/domain), validity date, password, province/state, region and so on.

④ Click "OK".

⑤ Check "Enable" checkbox.

⑥ Click "Apply" to save the setting.

B. Install a signed certificate


Function Panel ▸ Https
4
□ Enable
Certificate installation
Certificate installation
1
○ Create a private certificate
● Signed certificate already available. Install directly
○ Create a certificate request
3
Install signed certificate
Browse
Import
2
5
Apply

① Check "Signed certificate already….".

② Click "Browse" to select the certificate you want to import.

③ Click "Import".

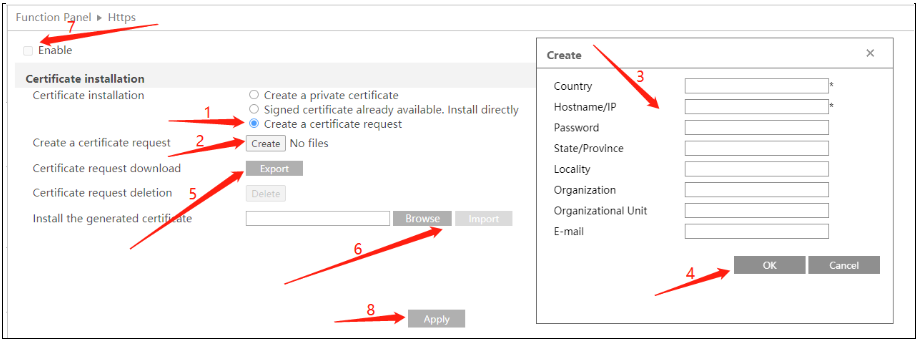
④ Check "Enable".

⑤ Click "Apply" to save the settings.

Please note that the certificate uploaded here shall be a certificate with private key.

To attach the private key to the certificate, please open the certificate and the private key files with an editor (like Notepad++) and then copy the private key to the certificate.

C. Create a certificate request



Function Panel ▸ Https

□ Enable

Certificate installation

Certificate installation: ○ Create a private certificate ○ Signed certificate already available. Install directly ● Create a certificate request

Create a certificate request: Create No files

Certificate request download: Export

Certificate request deletion: Delete

Install the generated certificate: Browse Import

Apply

Create ×

Country *

Hostname/IP *

Password

State/Province

Locality

Organization

Organizational Unit

E-mail

OK Cancel

① Check “Create a certificate request”.

② Click “Create”.

③ Fill out the corresponding information in the above creation box. Enter the country (only two letters available), domain (NVR’s IP address/domain), validity date, password, province/state, region and so on.

④ Click “OK”. Then a certificate request file (CSR) will be created.

⑤ Click “Export” to export the certificate request file. Then send this file to the trusted third-party CA to apply a signed certificate.

⑥ Click “Browse” and select the signed certificate issued by the CA and then import this certificate.

⑦ Click “Enable”.

⑧ Click “Apply” to save the settings.

After that, the device can be accessed by entering https://IP: https port via the web browser (eg. https://192.168.1.201:443).

Server Port: the default server port of the NVR is 6036. The server port number can be changed as required. The port is mainly used in network video management system.
POS Port: the default POS port of the NVR is 9036.

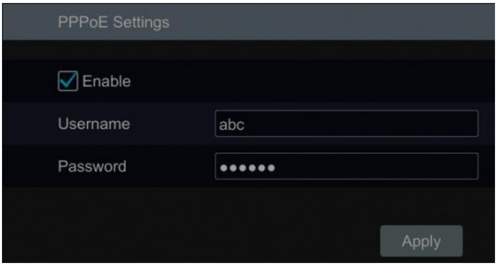
API Server: You can log into a media player which supports the RTSP protocol. Moreover, the third-party can further develop performance through an API service.
Authentication: Basic authentication and digest authentication are optional.

RTSP Port: RTSP real-time stream protocol can be used to control the transfer of real-time data. . Through a media player which supports the RTSP real-time stream protocol (Such as VLC player), you can view live images synchronously. The default RTSP port is 554 and it can be changed as needed. (The address format: rtsp://IP address:554/chID=1&streamType=main or rtsp://IP address:554/chID=1&streamType=sub; main indicators main stream; sub indicators sub stream; chID indicators channel ID).

Examples: Enable RTSP and "Anonymous". Then open the VLC player and enter the address (for example: rtsp://192.168.1.88:554/chID=1&streamType=main) in the network address bar of the VLC player. Then you can view the video of channel 1.

14.1.3 PPPoE Configuration

Click ***Start→Settings→Network→PPPoE*** to go to the interface as shown below. Check "Enable" in "PPPoE Settings" and then enter the username and password obtained from the dealer. Click "Apply" to save the settings.



PPPoE Settings

☑ Enable

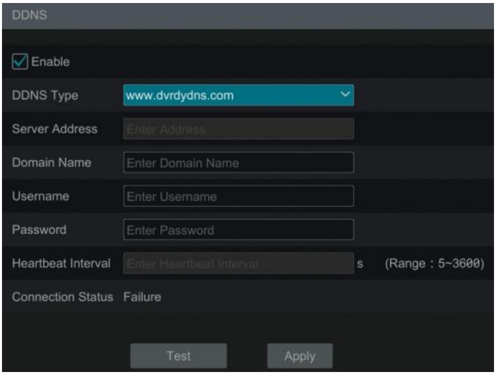
Username: abc

Password: ●●●●●●

14.1.4 DDNS Configuration

The DDNS is used to control the dynamic IP address through a domain name. You can access to the NVR easily if the DDNS is enabled and configured.

Click ***Start→Settings→Network→DDNS*** to go to the interface as shown below.



DDNS

☑ Enable

DDNS Type: www.dvrdydns.com

Server Address: Enter Address

Domain Name: Enter Domain Name

Username: Enter Username

Password: Enter Password

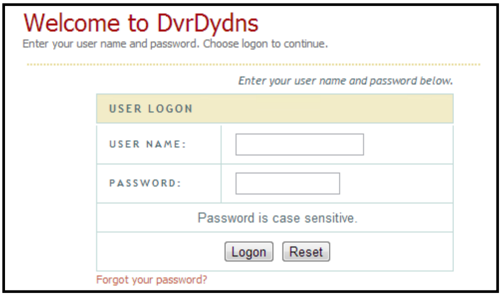
Heartbeat Interval: Enter Heartbeat Interval s (Range : 5~3600)

Connection Status: Failure

Check "Enable" and then select the DDNS type. Enter the server address, domain name, username and password according to the selected DDNS type. Click "Test" to test the effectiveness of the input information. Click "Apply" to save the settings. After that, the successful connection status can be viewed.

Note: Only when the DDNS type is "dyndns", can the heartbeat interval be configurable.
You will have to enter the server address and domain name if some DDNS types are selected. Go to the relative DNS website to register domain name and then enter the registered domain information here). Now we take ***www.NVRdydns.com*** for example.

① Enter ***www.NVRdydns.com*** in the address bar to visit its DNS website.



Welcome to DvrDydns

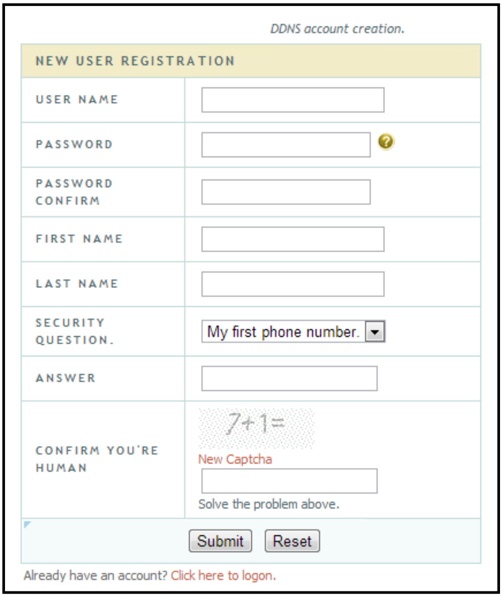
Enter your user name and password. Choose logon to continue.

Enter your user name and password below.

USER LOGON	
USER NAME:	
PASSWORD:	

Password is case sensitive.

② Click ***Registration*** to go to the interface as shown below. Set the DDNS account information (username, password and so on) and then click ***Submit*** to save the account.

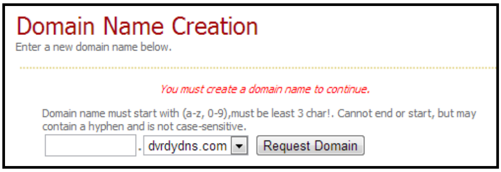


DDNS account creation.

NEW USER REGISTRATION	
USER NAME	
PASSWORD	
PASSWORD CONFIRM	
FIRST NAME	
LAST NAME	
SECURITY QUESTION.	My first phone number.
ANSWER	
CONFIRM YOU'RE HUMAN	7+1= New Captcha Solve the problem above.

Already have an account? Click here to logon.

③ Create domain name and then click ***Request Domain***.



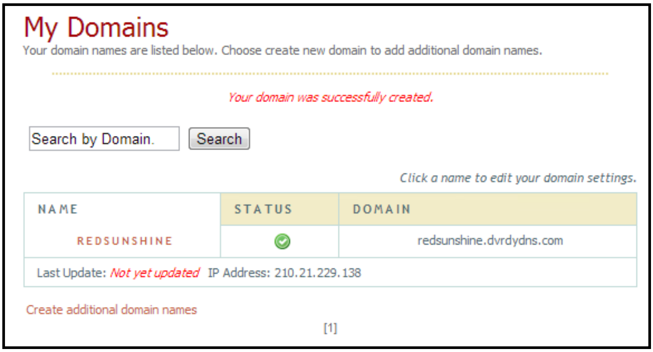
Domain Name Creation

Enter a new domain name below.

You must create a domain name to continue.

Domain name must start with (a-z, 0-9),must be least 3 char!. Cannot end or start, but may contain a hyphen and is not case-sensitive.

④ After you successfully request your domain name, you will see your domain name information in the list.



My Domains

Your domain names are listed below. Choose create new domain to add additional domain names.

Your domain was successfully created.

Click a name to edit your domain settings.

NAME	STATUS	DOMAIN
REDSUNSHINE	✓	redsunshine.dvrdydns.com
Last Update: *Not yet updated* IP Address: 210.21.229.138		

Create additional domain names

[1]

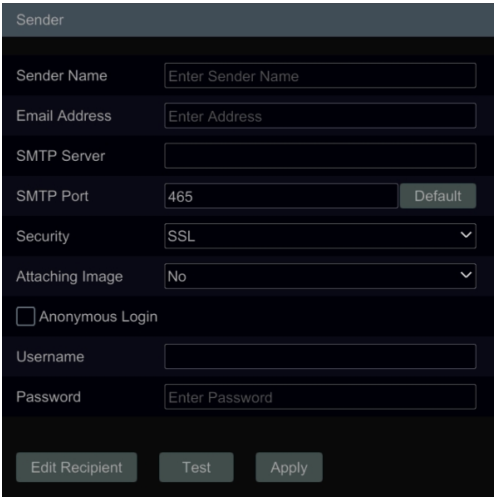
⑤ Click ***Start→Settings→Network→DDNS*** to go to DDNS setting interface. Enable DDNS and then select the ***www.NVRdydns.com*** DDNS type. Enter the registered username, password and domain name and then click "Apply".

⑥ Map the IP address and HTTP port in the router (you can skip this step if UPnP function is enabled).

⑦ Enter the registered domain name plus HTTP port like ***http://www.xxx.NVRdydns.com:81*** in the address bar and then press Enter key to go to the web client.

14.1.5 E-mail Configuration

Click ***Start→Settings→Network→E-mail*** to go to the following interface.



Sender

Sender Name: Enter Sender Name

Email Address: Enter Address

SMTP Server:

SMTP Port: 465

Security: SSL

Attaching Image: No

□ Anonymous Login

Username:

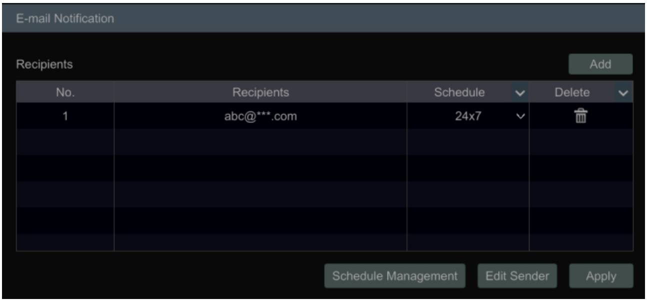
Password: Enter Password

Enter the sender’s name, e-mail address, SMTP server and SMTP port (you can click “Default” to reset the SMTP port to the default value) and then enable or disable the SSL and attaching image.

Attaching Image: Choose “NO”, “A Picture” or “Multiple Pictures”. If “A Picture” or “Multiple Pictures” is selected, snapshot image or original image can be selected to attach.

Select the username (the username list will be updated automatically according to the email address you input) and enter the password of the sender and then click “Apply” to save your settings (you don’t have to enter the username and password if “Anonymous Login” is enabled). Click “Test” to open a window. Enter the e-mail address of the recipient in the window and then click “OK.” The e-mail address of the sender will send an e-mail to the recipient. If the e-mail is sent successfully, it indicates that the e-mail address of the sender is configured correctly.

Click “Edit Recipient” to go to the following interface:



E-mail Notification

Recipients

No.	Recipients	Schedule	Delete
1	abc@***.com	24x7	🗑

Click “Add” and then enter the recipient’s e-mail address and select the schedule (if a schedule is selected, the system will send the alarm email and the recipient will receive it only in the selected schedule time) in the popup window. Click “Add” in the window to add the recipient. You can also change the recipient’s receiving schedule by clicking ∨ in the “Schedule” column. Click 🗑 to delete the recipient in the list. Click “Apply” to save your settings. Click “Edit Sender” to go to the e-mail configuration interface of the sender.

14.1.6 UPnP Configuration

By UPnP you can access the NVR through the web client which is on the WAN via a router without port mapping.

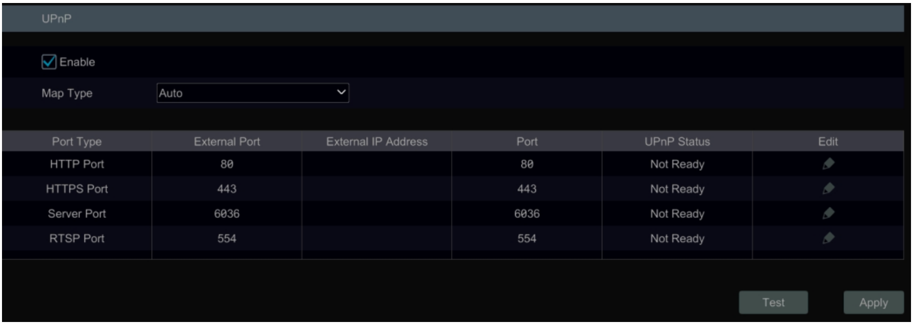
① Click ***Start→Settings→Network→UPnP*** to go to the following interface.

② Make sure the router supports UPnP function and the UPnP is enabled in the router.

③ Set the NVR’s IP address, subnet mask and gateway and so on corresponding to the router.

④ Check “Enable” in the interface as shown below and then click “Apply”.

Click “Refresh” button to refresh the UPnP status. If the UPnP status is still “Invalid UPnP” after refreshing, the port number is wrong. Please change the mapping type to “Manual” and then click ✎ to modify the port until the UPnP status turns to “Valid UPnP”. Refer to the picture below. You can view the external IP address of the NVR. Enter the external IP address plus port in the address bar of your browser to access the NVR (example: http://183.17.254.19:81).



UPnP

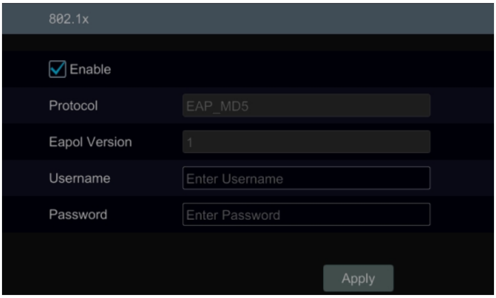
☑ Enable

Map Type: Auto

Port Type	External Port	External IP Address	Port	UPnP Status	Edit
HTTP Port	80		80	Not Ready	✎
HTTPS Port	443		443	Not Ready	✎
Server Port	6036		6036	Not Ready	✎
RTSP Port	554		554	Not Ready	✎

14.1.7 802.1X

If it is enabled, the NVR data can be protected. When the NVR is connected to the network protected by the IEEE 802.1X, user authentication is needed.



802.1x

☑ Enable

Protocol: EAP_MD5

Eapol Version: 1

Username: Enter Username

Password: Enter Password

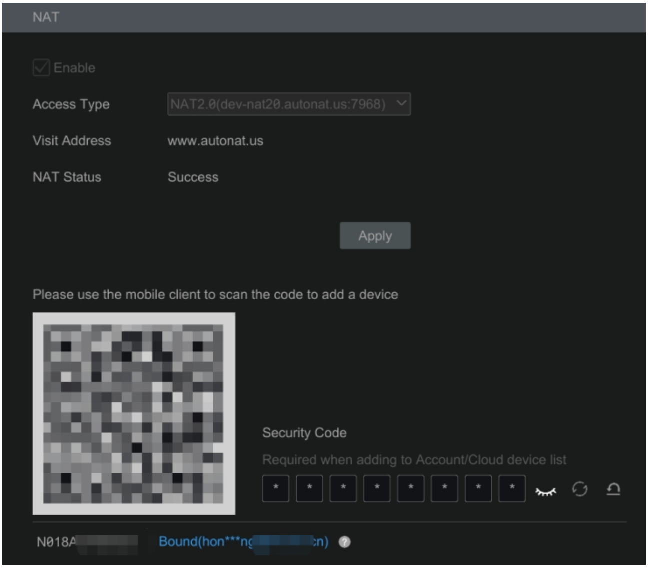
To use this function, the NVR shall be connected to a switch supporting the 802.1x protocol. The switch can be considered as an authentication system to identify the device in a local network. If the NVR connected to the network interface of the switch has passed the authentication of the switch, it can be accessed via the local network.

Protocol type and EAPOL version: Please use the default settings.

User name and password: The user name and password must be the same with the user name and password applied for and registered in the authentication server.

14.1.8 NAT Configuration

Click ***Start→Settings→Network→NAT*** to go to the interface for NAT configuration.



NAT

☑ Enable

Access Type: NAT2.0(dev-nat20.autonat.us:7968)

Visit Address: www.autonat.us

NAT Status: Success

Please use the mobile client to scan the code to add a device

Security Code

Required when adding to Account/Cloud device list

* * * * * * * *

N018A[redacted] Bound(hon***ng[redacted]cn)

Check “Enable” and then select the NAT server address. Click “Apply” to save the settings.

You can scan the QRCode through mobile APP which is installed on a mobile phone or tablet PC to quickly add the device to the server list of the mobile APP.

Access Type: NAT or NAT2.0 can be selected.
Click “Advanced” to select the area as needed.

Security Access: Only some models upgraded from a lower version can display this function. New models support this function by default. After this function is enabled, it reduces malware damage and enables NAT2.0 push function.

The setup steps of enabling NAT2.0 message push are as follow:
1. Enable NAT and security access. If “Security Access” is not displayed, it means this function is supported by default.
2. Select NAT2.0 access type.
3. Log in your APP account and add the device by scanning the QR code and entering the security code.
4. In the APP, select the device in the push setting interface and enable push message.

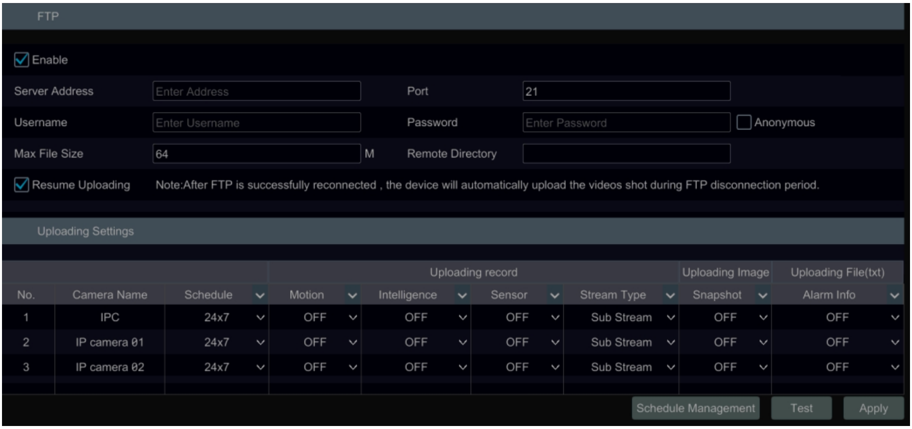
Web login by NAT2.0
After you bind the device to your APP account and enable NAT2.0, a verification code will be required when logging onto the web client by using the above visit address (different areas and regions maybe have different visit addresses). Please enter the correct verification code that getting from the APP.

Note:
1. If you want to use the cloud upgrade, you must enable NAT2.0.
2. After the NAT is enabled, use the mobile APP to scan the QRcode and then the device can be added to the server list of the mobile APP.
3. The device can be added to the account of the mobile APP only when NAT2.0 is enabled. After the NAT2.0 is enabled, when you add the device to the account of the mobile APP, you must enter the security code of the device here. Please refer to the mobile surveillance user manual for details.
4. Currently, only the latest APP version can receive the verification code.

After the device is bound to the account of the mobile APP, the blue binding information will be shown under the QR code. Click this blue information to unbind it.

14.1.9 FTP Configuration

Some models may not support this function.
Click ***Start→Settings→Network→FTP*** to go to the interface for FTP configuration. Check “Enable” and enter the server name, port, username and password, max file size and remote directory.
Please enable “Resume Uploading” as needed.
After that, you can choose the camera, set the schedule and then select the video records, images and alarm information to upload as needed in this interface.



FTP

☑ Enable

Server Address	Enter Address	Port	21
Username	Enter Username	Password	Enter Password □ Anonymous
Max File Size	64 M	Remote Directory	

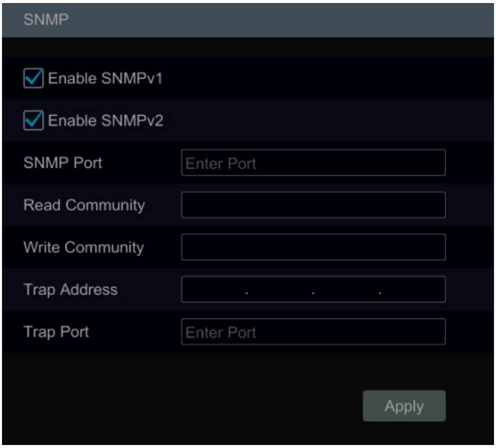
☑ Resume Uploading Note:After FTP is successfully reconnected , the device will automatically upload the videos shot during FTP disconnection period.

Uploading Settings

			Uploading record				Uploading Image	Uploading File(txt)
No.	Camera Name	Schedule	Motion	Intelligence	Sensor	Stream Type	Snapshot	Alarm Info
1	IPC	24x7	OFF	OFF	OFF	Sub Stream	OFF	OFF
2	IP camera 01	24x7	OFF	OFF	OFF	Sub Stream	OFF	OFF
3	IP camera 02	24x7	OFF	OFF	OFF	Sub Stream	OFF	OFF

14.1.10 SNMP

① Click ***Start→Settings→Network→SNMP*** to go to the interface for SNMP configuration.



SNMP

☑ Enable SNMPv1

☑ Enable SNMPv2

SNMP Port	Enter Port
Read Community	
Write Community	
Trap Address	. . .
Trap Port	Enter Port

② Check SNMPv1or SNMPv2 to enable this function.

③ Set the port of the SNMP.

④ Set the trap address and the trap port.

⑤ Click “Apply” to save the settings.

Trap Address: The IP address of SNMP host.

Trap Port: The port of SNMP host.

Tips: Before setting the SNMP, please download the SNMP software and manage to receive the device information via SNMP port. By setting the trap address, the device is allowed to send the alarm event and exception message to the monitoring center.

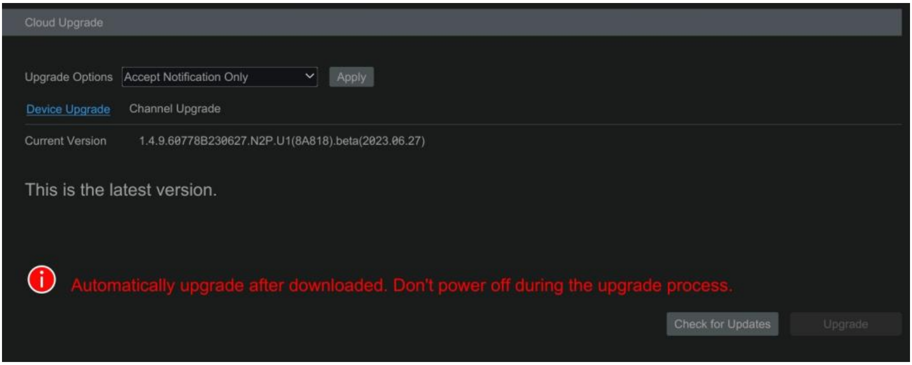
14.1.11 Cloud Upgrade

Note: Before you use cloud upgrade, please enable NAT2.0.

Click ***Start→Settings→Network→Cloud Upgrade*** as shown below.

Note: Only users with Network user authority can activate and use this feature. If the dealer does not wish to provide this capability to their users, they can ensure that only the main Admin login has network authority.

➢ **Device Upgrade**



Upgrade Options: Accept Notification Only

Current Version: 1.4.9.60778B230627.N2P.U1(8A818).beta(2023.06.27)

This is the latest version.

Automatically upgrade after downloaded. Don't power off during the upgrade process.

① Select "Accept Notification Only" or click "Check for Updates" to check whether the current version is the latest. If your software version is not the latest, click "Upgrade" to download and upgrade from the cloud server.

② Please don't power off during the upgrade process.

➢ **Camera Upgrade**

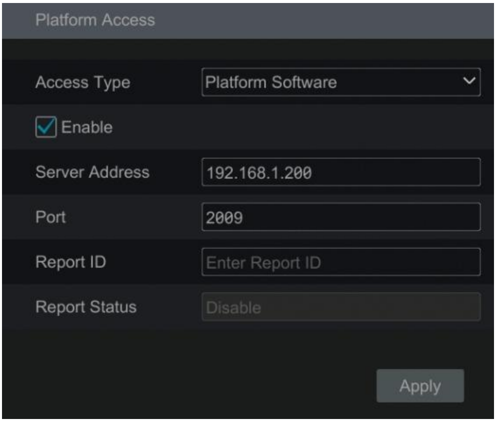
Click the "Channel Upgrade" tab to automatically check the added camera version. If cameras are not the latest version, click "Check for Updates" to get the latest version from the cloud server. You can upgrade cameras one by one or in batches as needed.

14.1.12 Platform Access

Some models may not support this function.

This function is mainly used for connecting ECMS/NVMS. The setting steps are as follows.

Click ***Start→Settings→Network→Integration→Platform Access*** to go to the interface.



Platform Access

Access Type: Platform Software

☑ Enable

Server Address: 192.168.1.200

Port: 2009

Report ID: Enter Report ID

Report Status: Disable

Platform Access

① Set “Access Type” as “Platform Software” and select “Enable” as shown below.

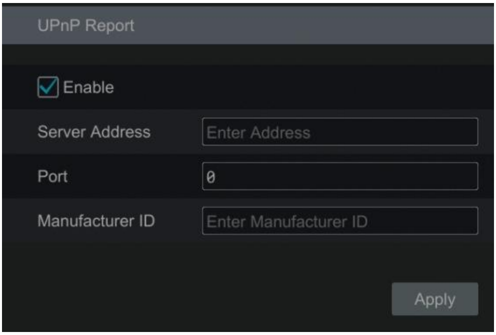
② Check the IP address and port of the transfer media server in the NVMS. The default server port for auto report is 2009. If it is modified, please go to the transfer media interface to check.

③ Enable the auto report in the NVMS when adding a new device. Then self-define device ID and complete the remaining information of the device in the NVMS.

④ Enter the above-mentioned server address, port and report ID in the server interface. Then click “Apply” to save the settings.

14.1.13 UPnP Report Access

In this interface, you can also access the third-party platform by UPnP Report. Click ***Start→Settings→Network→Integration→UPnP Report.*** If this one is enabled, please enter the server address, port and manufacturer ID.



UPnP Report

☑ Enable

Server Address: Enter Address

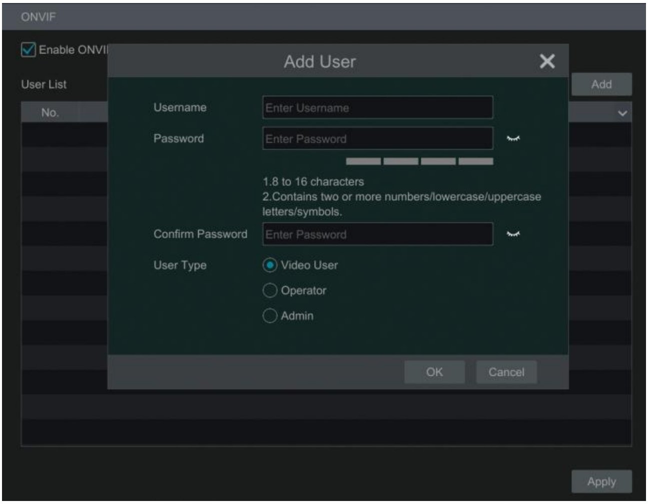
Port: 0

Manufacturer ID: Enter Manufacturer ID

14.1.14 ONVIF

The device supports ONVIF (Profile G/T/S) and the model name can be searched on the

ONVIF official website. After ONVIF is enabled, it can be searched and connected to a third-party platform via ONVIF protocol.
Click ***Start→Settings→Network→Integration →ONVIF*** to enter the following interface.



ONVIF

☑ Enable ONVI

User List

No.

Add

Add User ✕

Username: Enter Username

Password: Enter Password

1.8 to 16 characters
2.Contains two or more numbers/lowercase/uppercase letters/symbols.

Confirm Password: Enter Password

User Type: ● Video User ○ Operator ○ Admin

OK Cancel

Apply

Note: when adding the device to a third-party platform with ONVIF protocol, please check "Enable ONVIF" first and then enter the username and password created in the above interface.

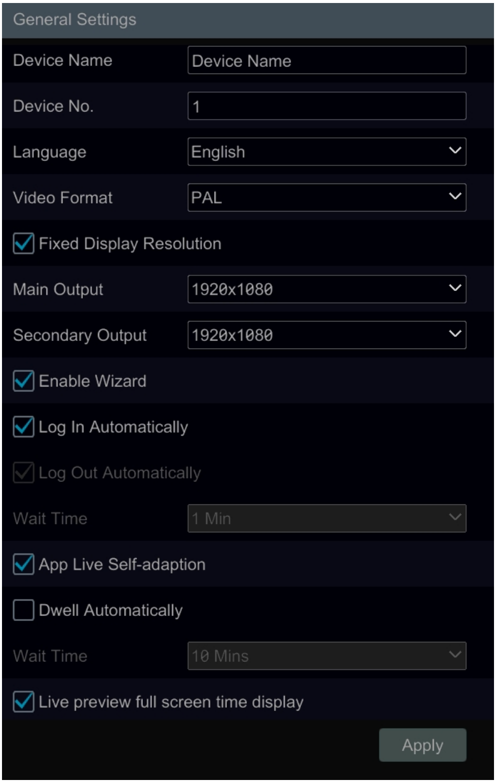
14.1.15 Network Status

Click ***Start→Settings→Network→Network Status*** to view the network status or click 🖧 on the tool bar at the bottom of the live view interface to view network status conveniently.
Click ***Start→Settings→Network→Network Status Detection***. Enter the IP address and then click "Test" to check the network connection status (like network delay, packet loss).

14.2 Basic Configuration

14.2.1 Common Configuration

Click ***Start→Settings→System→Basic→General Settings*** to go to the following interface. Set the device name, device No., language, video format and main output. Enable or disable wizard, "Log In Automatically", "Log Out Automatically" (if checked, you can set the wait time), "App Live Self-Adaption" and "Dwell Automatically" (if checked, you can set the wait time). Click "Apply" to save the settings.



General Settings

Device Name: Device Name

Device No.: 1

Language: English

Video Format: PAL

☑ Fixed Display Resolution

Main Output: 1920x1080

Secondary Output: 1920x1080

☑ Enable Wizard

☑ Log In Automatically

☑ Log Out Automatically

Wait Time: 1 Min

☑ App Live Self-adaption

□ Dwell Automatically

Wait Time: 10 Mins

☑ Live preview full screen time display

Device Name: The name of the device. It may display on the client end or CMS to help users to recognize the device remotely.

Video Format: Two modes: PAL and NTSC. Select the video format according to the camera.

Dwell Automatically: Switch automatically. Check it and set "wait time". The system will sequence automatically if it is not operated during the time you set.

Main Output: Enable "Fixed display resolution" and then select the main output as needed.

Note: You can set the resolutions of the main output, secondary output (varies by models) respectively if the NVR has multiple outputs.

You can check "Support 8K" as needed for some models.

14.2.2 Date and Time Configuration

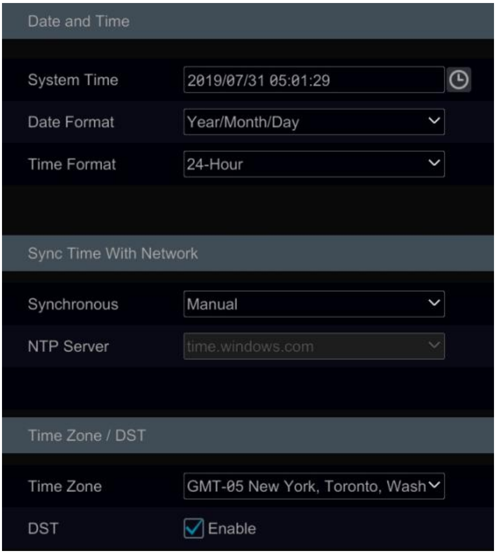
Click ***Start→Settings→System→Basic→Date and Time*** to go to the interface as shown below. Set the system time, date format, time format and time zone of the NVR. The default time zone is GMT+08 Beijing, Hong Kong, Shanghai, Taipei. If the selected time zone includes DST, the DST of the time zone will be checked by default. Click "Apply" to save the settings.

You can manually set the system time or synchronize system time with network through NTP.

Manual: select "Manual" in the "Synchronous" option and then click 🕒 after the "System

Time" option to set the system time.

NTP: select "NTP" in the "Synchronous" option and then enter the NTP server.



Date and Time

System Time: 2019/07/31 05:01:29

Date Format: Year/Month/Day

Time Format: 24-Hour

Sync Time With Network

Synchronous: Manual

NTP Server: time.windows.com

Time Zone / DST

Time Zone: GMT-05 New York, Toronto, Wash

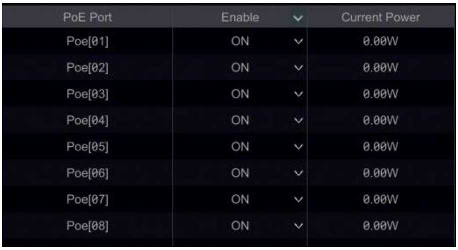
DST: ☑ Enable

14.2.3 Recorder OSD Settings

Click ***Start→Settings→System→Basic→Recorder OSD settings*** to go to recorder OSD setting interface. OSD name and icon can be enabled here.

14.2.4 PoE Power Management

Click ***Start→Settings→System→Basic Settings→PoE Power Management*** to go to the following interface. This function is only available for the POE device.



PoE Port	Enable	Current Power
Poe[01]	ON	0.00W
Poe[02]	ON	0.00W
Poe[03]	ON	0.00W
Poe[04]	ON	0.00W
Poe[05]	ON	0.00W
Poe[06]	ON	0.00W
Poe[07]	ON	0.00W
Poe[08]	ON	0.00W

In this interface, you can view the the current power consumption of the added POE camera/panel. The PoE power supply of the PoE camera/panel can be enabled or disabled by selecting "ON" or "OFF" as needed.

- PoE Plug-and-Play Settings

The PnP function of each PoE port is enabled by default. You can directly connect the PoE IPC to the PoE port of the NVR with a network cable.

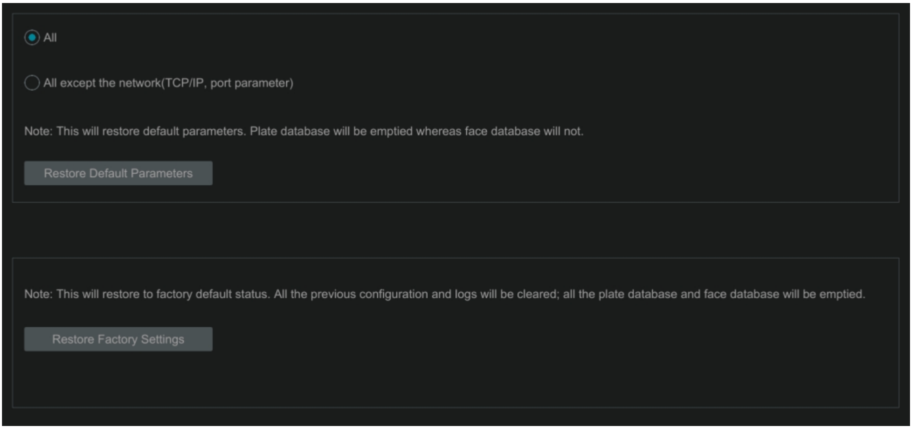
You can also connect the PoE IPC to the NVR via a PoE switch by referring to the following steps.

1. Go to Start→Settings→System→PoE Settings→PoE Pug-and-Play Settings interface. Disable the PnP function of a PoE Port.
2. Connect the PoE switch to this PoE port of the NVR with a network cable.
3. Connect the PoE IPCs to the PoE switch with network cables.
4. Go to Start→Settings→Network→Internal Ethernet Port interface. Set the IP address segment and mode as needed.
5. Go to Start→Settings→Camera→Edit Camera interface. Click "Add Camera" to add these PoE IPCs manually. Note that the IP address of these cameras must be in the same local network segment as the internal Ethernet port.

Note: If the above-mentioned PoE IPCs are added to the NVR successfully, the corresponding number of PoE ports will be occupied. For example, if the NVR has 16 PoE ports and one of them is used to connect a PoE switch which 8 PoE IPCs are connected to, then only 8 PoE ports of the NVR can be used to directly connect PoE cameras.

14.3 Factory Default

Click ***Start→Settings→System→Maintenance→Factory Default*** to go to the following interface. Please choose the item as needed.



● All

○ All except the network(TCP/IP, port parameter)

Note: This will restore default parameters. Plate database will be emptied whereas face database will not.

Note: This will restore to factory default status. All the previous configuration and logs will be cleared; all the plate database and face database will be emptied.

Note: Restoring default parameters will not change time zone and video format, except that, the password of the admin will be preserved.

14.4 Device Software Upgrade

- **Upgrade**

You can click ***Start→Settings→System→Information→Basic*** to view MCU, kernel version and firmware version and so on. Before upgrade, please get the upgrade file from your dealer. The upgrade steps are as follows:

① Copy the upgrade software onto the USB storage device.

② Insert the USB storage device into the USB interface of the NVR.

③ Click ***Start→Settings→System→Maintenance→Upgrade*** to go to "Upgrade" interface. Select the USB device in "Device Name" option and go to the path where the upgrade software resides. Select the upgrade software and then click "Upgrade". The system may automatically restart during upgrading. Please wait for the upgrade to finish and it's critical to not power off the NVR during the upgrade process.

Note: The file system of the USB mobile device which is used for upgrade, backup and restoration should be FAT32/NTFS format (only some models support NTFS format).

14.5 Backup and Restore

You can back up the configuration file of the NVR and export the file to other storage devices; in this way, you can implement the configuration to other NVRs of the same model and save setup time.

Insert the USB storage device into a USB interface on the NVR and then click ***Start→Settings→System→Maintenance→Backup and Restore*** to go to the interface.

- **Backup**

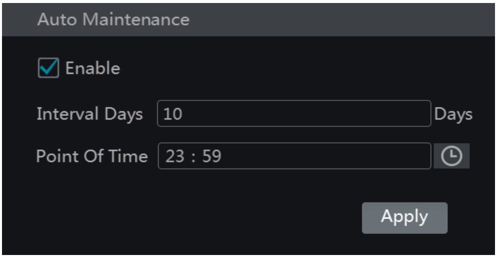
Select the USB device in "Device Name" option; go to the path where you want to store the configuration backup file and then click "Backup"; finally, click "OK" in the popup window.

- **Recover**

Select the USB device in "Device Name" option; find the configuration backup file and then click "Recover"; finally, click "OK" in the popup window.

14.6 Restart Automatically

You can set the automatic restart time for the NVR to maximize performance. Click ***Start→Settings→System→Maintenance→Auto Maintenance*** to go to the interface as shown below. Enable auto maintenance, set the interval days and point of time and then click "Apply" to save the settings. The NVR will restart automatically at the pointed time every *interval* days.



Auto Maintenance

☑ Enable

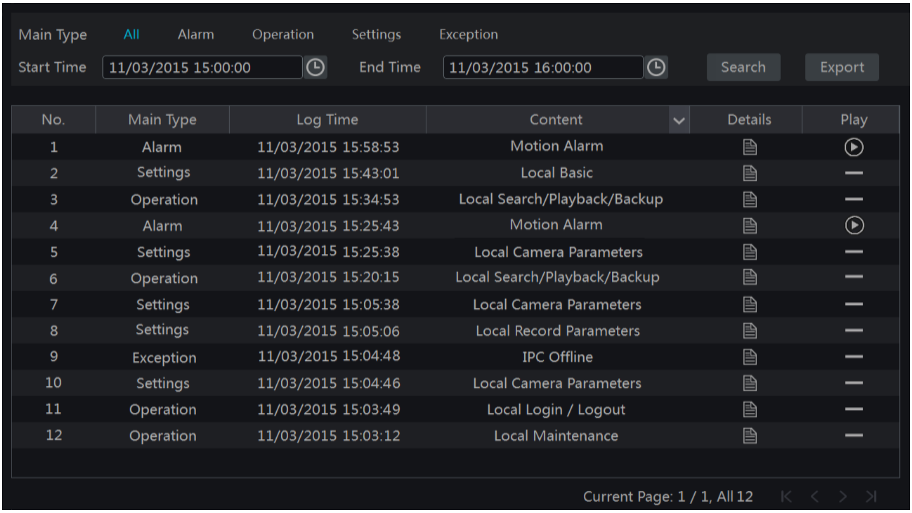
Interval Days 10 Days

Point Of Time 23 : 59 🕒

Apply

14.7 View Log

Click ***Start→Settings→System→Maintenance→View Log*** to go to the log view interface. Select the log main type, click 🕒 to set start time and end time and then click "Search". The searched log files will be displayed in the list.



Main Type All Alarm Operation Settings Exception

Start Time 11/03/2015 15:00:00 🕒 End Time 11/03/2015 16:00:00 🕒 Search Export

No.	Main Type	Log Time	Content ⌄	Details	Play
1	Alarm	11/03/2015 15:58:53	Motion Alarm	🗎	▶
2	Settings	11/03/2015 15:43:01	Local Basic	🗎	—
3	Operation	11/03/2015 15:34:53	Local Search/Playback/Backup	🗎	—
4	Alarm	11/03/2015 15:25:43	Motion Alarm	🗎	▶
5	Settings	11/03/2015 15:25:38	Local Camera Parameters	🗎	—
6	Operation	11/03/2015 15:20:15	Local Search/Playback/Backup	🗎	—
7	Settings	11/03/2015 15:05:38	Local Camera Parameters	🗎	—
8	Settings	11/03/2015 15:05:06	Local Record Parameters	🗎	—
9	Exception	11/03/2015 15:04:48	IPC Offline	🗎	—
10	Settings	11/03/2015 15:04:46	Local Camera Parameters	🗎	—
11	Operation	11/03/2015 15:03:49	Local Login / Logout	🗎	—
12	Operation	11/03/2015 15:03:12	Local Maintenance	🗎	—

Current Page: 1 / 1, All 12

Choose the log file in the list and then click "Export" button to export the log file. Click ⌄ on the "Content" title bar to pop up a menu list. Using the check box, check contents on the menu list and then the log list will show only the checked log contents. Click ▶ to play the video log.

14.8 View System Information

Click ***Start→Settings→System→Information*** and then click the corresponding menu to view the "Basic", "Camera Status", "Alarm Status", "Record Status", "Network Status" and "Disk" information of the system.

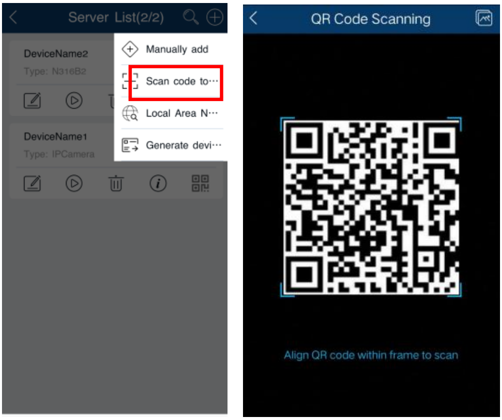
15 Remote Surveillance

15.1 Mobile Client Surveillance

① Enable NAT in the NVR. Refer to NAT Configuration for details.

② Download and install the mobile client "SuperLive Plus" into the mobile device with the Android or iOS system.

③ Run the mobile client, go to the "Server List" interface to scan the QRCode of the NVR (Go to Start→Settings→Network→NAT to view the QRCode of the NVR).

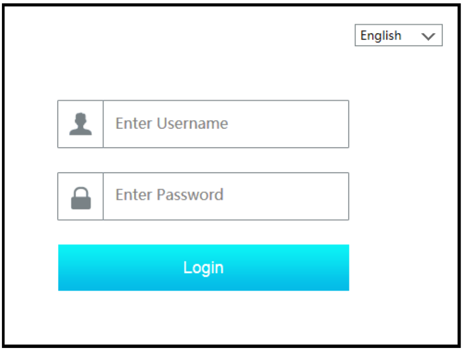


If you want to add the device to the account of the mobile APP, you must enable NAT2.0 and enter the security code. Please refer to the mobile surveillance user manual for details.

15.2 Web LAN Access

① Click ***Start→Settings→Network→TCP/IP*** to go to the "TCP/IP" interface. Set the IP address, subnet mask, gateway, preferred DNS and alternate DNS of the NVR.

② Open a web browser on your computer, enter the IP address of the NVR in the address bar and then press enter to go to the login interface as shown below. You can change the display language on the top right corner of the login interface. Enter the username and password of the NVR in the interface and then click "Login" to go to the live view interface.



Notes: 1. Please make sure that the IP address of the NVR and the computer are both in the same local network segment. For example, supposing that the IP address of the computer is 192.168.1.41, the IP address of the NVR shall be set to 192.168.1.XXX.
2. If the HTTP port of the NVR is not 80, but another number, you need to enter the IP address plus port number in the address bar when accessing the NVR over a network. For example, the HTTP port is 81. You should enter http://192.168.1.42:81 in the address bar.

15.3 Web WAN Access

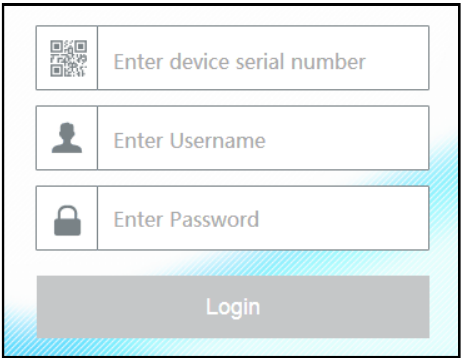
➢ **NAT Access**

① Set the network of the NVR. Please refer to TCP/IP Configuration for details.

② Enable NAT and then set the NAT server address. Please refer to NAT Configuration for details.

③ Open a web browser on your computer, enter the NAT server visit address (such as www.autonat.us) in the address bar and then press enter to go to the interface as shown below (download and install the relative plug-in according to the tip if you access the NVR through NAT for the first time).

Note: Different regions may have different visit addresses. Please go to the NAT interface to view the detailed visit address (click ***Start→Settings→Network→NAT***).



Enter the serial number (click 🖥 on the tool bar at the bottom of the live view interface to see the serial number of the NVR), user name (the user name of the NVR, ***admin*** by default) and password of the NVR, select the display language on the top right corner of the interface and then click "Login" to go to the web client interface.

Note: If your device is bound to the APP, the verification code that getting from the APP is needed.

➢ **PPPoE Access**

① Click ***Start→Settings→Network→PPPoE*** to go to the "PPPoE" interface. Check "Enable" in the "PPPoE settings" and then enter the username and password you get from your ISP. Click "Apply" to save the settings.

② Click ***Start→Settings→Network→Network Status*** to view the IP address of the NVR.

③ Open a web browser on your computer, enter the IP address of the NVR like http://210.21.229.138 in the address bar and then press enter to go to the login interface. Enter the username and password of the NVR in the interface and then click "Login" to go to the live view interface.

➢ **Router Access**

① Click ***Start→Settings→Network→TCP/IP*** to go to the "TCP/IP" interface. Set the IP address, subnet mask, gateway, preferred DNS and alternate DNS of the NVR.

② Set the HTTP port (it is suggested to modify the HTTP port because the default HTTP port 80 might be taken up) and enable UPnP function in both the NVR and the router. If the UPnP function is not available in the router, you need to forward the LAN IP address, HTTP port and server port of the NVR to the router. Port mapping settings may be different in different routers, so please refer to the user manual of the router for details.

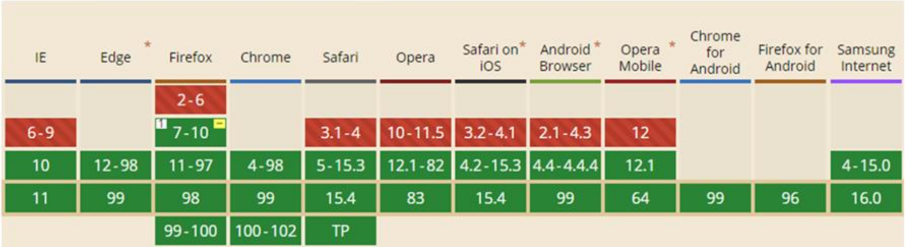
③ Get the WAN IP address of the NVR from the router. Open a web browser on your computer, enter the WAN IP address plus HTTP port like http://116.30.18.215:100 in the address bar and then press enter to go to the login interface. Enter the username and password of the NVR in the interface and then click "Login" to go to the live view interface.

> ***Note:*** *If the WAN IP address is a dynamic IP address, it is necessary for you to use the domain name to access the NVR. Click Start→Settings→Network→DDNS to set DDNS (see 14.1.4 DDNS Configuration for details). By using DDNS function you can use the domain name plus HTTP port like http://sunshine.NVRdydns.com:100 to access the NVR via the Internet.*

15.4 Web Remote Control

The NVR supports web client access with or without plug-in. The plug-in for HTLM5 browsers offers much improved features and performance.

The supported browsers (green color) for remote access with the plug-in are as follows. The red color versions are not supported.

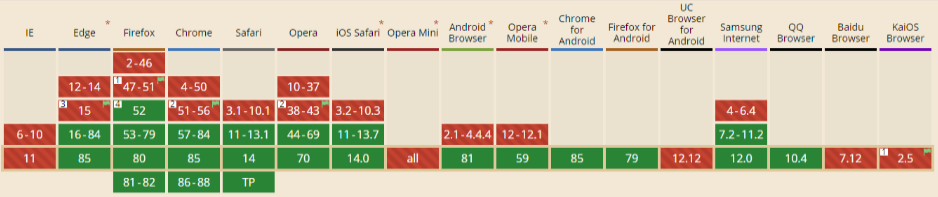


IE	Edge *	Firefox	Chrome	Safari	Opera	Safari on iOS *	Android Browser *	Opera Mobile *	Chrome for Android	Firefox for Android	Samsung Internet
		2-6									
6-9		[1] 7-10		3.1-4	10-11.5	3.2-4.1	2.1-4.3	12			
10	12-98	11-97	4-98	5-15.3	12.1-82	4.2-15.3	4.4-4.4.4	12.1			4-15.0
11	99	98	99	15.4	83	15.4	99	64	99	96	16.0
		99-100	100-102	TP							

When you access the NVR through the above web browser for the first time, the browsers need to download and install the relative components for normal preview and playback.

If your browser asks for permission on the configuration modifications after the plug-in runs, please allow it, or the interface will not display normally; if the relevant ports of the plug-in (port 11563; port 12863; port 13863) are occupied, the system will tell you which program currently occupies the port. Please stop the occupying program.

The supported browsers (green color) for remote access without the plug-in are as follows. The red color versions are not supported.



IE	Edge *	Firefox	Chrome	Safari	Opera	iOS Safari *	Opera Mini *	Android Browser *	Opera Mobile *	Chrome for Android	Firefox for Android	UC Browser for Android	Samsung Internet	QQ Browser	Baidu Browser	KaiOS Browser
		2-46														
	12-14	[1] 47-51	4-50		10-37											
	[3] 15	[4] 52	[2] 51-56	3.1-10.1	[2] 38-43	3.2-10.3							4-6.4			
6-10	16-84	53-79	57-84	11-13.1	44-69	11-13.7		2.1-4.4.4	12-12.1				7.2-11.2			
11	85	80	85	14	70	14.0	all	81	59	85	79	12.12	12.0	10.4	7.12	[1] 2.5
		81-82	86-88	TP												

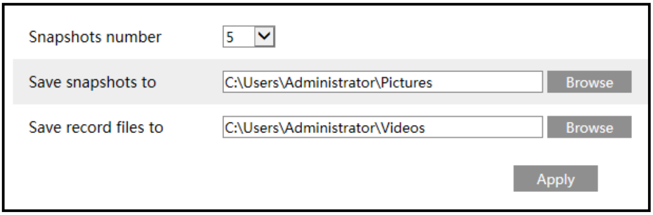
Please refer to the tips in the remote interfaces for details. The buttons and icons on the top right corner of the remote interface are introduced as follows.

admin: the current login username.

Logout: click to log out and return to the login interface.

Modify Password: click to change the password of the currently active user. Enter the current password and then set a new password in the popup window. Click "OK" to save the new password.

Local Settings: click to change the local settings. Set the snapshot number and click "Browse" to set the snapshot path and record path as shown below. Click "Apply" to save the settings.



Snapshots number 5

Save snapshots to C:\Users\Administrator\Pictures Browse

Save record files to C:\Users\Administrator\Videos Browse

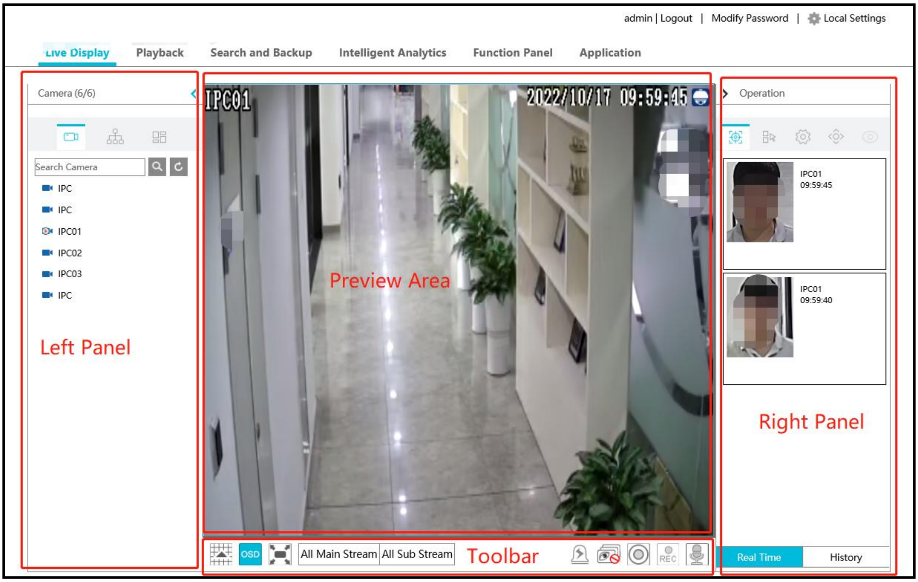
Apply

Below as an introduction is a web browser with the applicable plug-in installed.

15.4.1 Remote Preview

Click "Live Display" in the remote interface to go to the preview interface.

The preview interface consists of the four areas marked in the following picture.



➢ Start Preview

Select a window in the preview area and then click one online camera on the left panel to preview the camera in the window. You can click ◉ in the tool bar to preview all the cameras.

➢ Left Panel Introduction

Click < on the left panel to hide the panel and click > to show the panel. You can view all the added cameras and groups on the left panel.

● View Camera

Click ▭ to view the cameras. You can view the number of all the added cameras and the online cameras. For instance, the left number 3 in Camera (3/4) on the left panel stands for the number of online cameras; the right number 4 stands for the number of all the added cameras. Enter the camera name in the search box and then click 🔍 to search for the camera. Click ↻ to refresh the camera list.

● View Group

Click ☷ to view the groups. The top side of the left panel displays all the groups and the bottom displays all the cameras in the group.

● View Scheme

Click ▦ to view the scheme. All schemes can be shown in the left panel. Double click the scheme name to invoke it quickly.

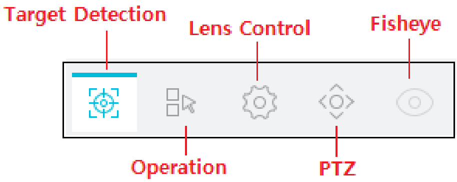
➢ Tool Bar Introduction

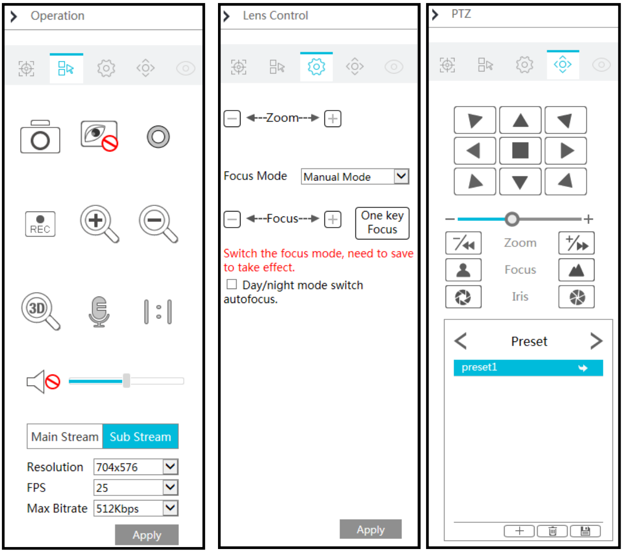
Button	Meaning
▦	Screen mode button.
OSD	Click to enable/disable OSD.
⛶	Click to show full screen. Right click on the full screen to exit full screen.
All Main Stream | All Sub Stream	Click “All Main Stream” or “All Sub Stream” to set the stream of all the cameras.
⚠	Manual alarm button. Click to open a window and then trigger and clear the alarm-out in the window manually.
◉	Click to preview all cameras.
⊘	Click to close all the preview cameras.
◎	Click to start recording for all cameras to computer. Click ● to stop recording.
REC	Click to start recording for all cameras to the NVR. Click REC to stop recording.

Button	Meaning
🎙	Click to enable talk through the NVR.

➢ Right Panel Introduction

Click ‹ on the right panel to show the panel and click › to hide the panel.





Resolution 704x576
FPS 25
Max Bitrate 512Kbps

Focus Mode Manual Mode

Switch the focus mode, need to save to take effect.

☐ Day/night mode switch autofocus.

Operation panel introduction:

Button	Meaning
📷	Click to take snapshots
◎	Click to start recording to computer
REC	Click to start recording to the NVR.
⊕	Click to zoom in the image of the camera and then drag the mouse on the camera image to view the hidden area.
⊖	Click to zoom out the image of the camera.

🎤	Click to start two-way talk.
3D	The 3D zoom in function is designed for P.T.Z. Click the button and then drag the image to zoom in or zoom out the image; click the image on different areas to view the image of the dome omni-directionally.
🚫	Click to close the preview camera.
1:1	Click to display original size
🔇	Click to enable audio and then drag the slider bar to adjust the volume. You can listen to the camera audio by enabling audio.

Click one camera window in the preview area and then click Main Stream to set the camera's live preview stream and record stream to main stream in manual record mode; click Sub-stream to set the camera's live preview stream and record stream to sub stream. In sub stream tab, set the resolution, FPS and bitrate and then click "Apply" to save the settings.

PTZ panel introduction:

Button	Meaning
◤ ▲ ◥ ◀ ■ ▶ ◣ ▼ ◢	Click ▲ / ▼ / ◥ / ▼ / ◤ / ◢ / ◀ / ▶ to rotate the dome; click ■ to stop rotating the dome.
− ○ +	Drag the slider to adjust the rotating speed of dome.
−◀◀ ←Zoom→ +▶▶	Click +▶▶ / −◀◀ to zoom in/out camera image.
👤 ←Focus→ ▲	Click ▲ / 👤 to increase/ decrease the focal length.
⊗ ← Iris → ⊛	Click ⊛ / ⊗ to increase/decrease the iris of the dome.
Preset	Click to view the preset list and then click the button in the list to call the preset. Click + to add a preset; click 💾 to save the preset setting; click 🗑 to delete the selected preset
Cruise	Click to view the cruise list. Click + to add a cruise; click ▶ to play the cruise; click ■ to stop cruise.
Cruise Group	Click to view the cruise group list. Click + to add a cruise group; click ▶ to play the cruise group; click ■ to stop cruise group.
Trace	Click to view the trace list. Click + to add a trace; click ▶ to play the trace click ■ to start record.

If the camera you added is motorized lens camera, click the lens control icon to adjust the lens. If the camera you added is a fisheye camera, click the fisheye icon to set the relevant parameters as needed.

15.4.2 Remote Playback

Click "Playback" in the remote interface to go to the playback interface.

① Check the record event types and cameras on the left panel. Set the record date on the calendar beside the time scale.

② Click 🔍 Search to search the record data and then click ▶ Play or directly click the time scale to play the record.

The operation of the playback time scale is similar to that of the time scale in the main program of the NVR. Please refer to Playback Interface Introduction for details.

Introduction of playback control buttons:

Button	Meaning
■	Stop button.
◀	Rewind button. Click to play video backwards.
▶	Play button. Click to play video forwards.
⏸	Pause button.
⏪	Deceleration button. Click to decrease the playing speed.
⏩	Acceleration button. Click to increase the playing speed.
◀❙	Previous frame button. It works only when the forward playing is paused in single screen mode.
❙▶	Next frame button. It works only when the forward playing is paused in single screen mode.
⊖30S⊕	Click ⊖ to step backward 30s and click ⊕ to step forward 30s.
[✂	Backup start time button. Click the time scale and then click to set the backup start time.
✂]	Backup end time button. Click the time scale and then click to set the backup end time.
⬇	Backup button.
💿	Backup tasks button. Click to view the backup status.
☰	Event list button. Click to view the event record of manual/schedule/sensor/motion.

15.4.3 Remote Search and Backup

Click "Search and Backup" in the remote interface to go to the backup interface. You can back up the record by event or by time.

- **By Event**

Check the record type on the left side of the interface and then click ▦ to set the start time and end time; check the cameras and then click 🔍 on the right side to search the record (the searched record data will be displayed in the list); check the record data in the list and then click "Backup" to backup the record.

- **By Time**

Click ▦ to set the start time and end time on the left side of the interface; check the cameras and then click on the right side to backup the record.

Image Management: Click “Image Management” to go to image management interface. The system will display all captured images automatically in the list. Click 🗑 to delete the image. Click to open the “Export” window. Click to open the “View Image” window. Click to export the image.

View Backup Status: Click “Backup Status” to view the backup status. Click “Pause” to pause; click “Resume” to continue the backup; click “Delete” to delete the task.

15.4.4 Intelligent Analysis

Click “Intelligent Analysis” in the remote interface to configure smart search, statistics and sample database. All of these settings are similar to that of the NVR. See the configurations of the NVR for details.

15.4.5 Application

The application of this system includes parking lot management, access control management, face attendance, face check-in and so on. Note that face attendance and face check-in functions are only available for some modes. All of these settings are similar to that of the NVR. See the configurations of the NVR for details.

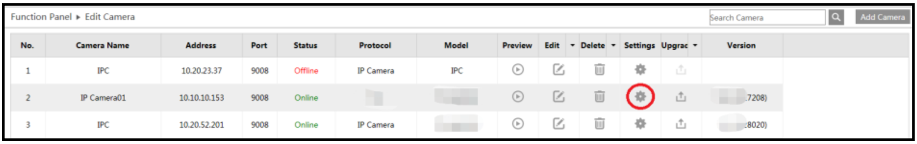
15.4.6 Remote Configuration

Click “Function Panel” in the remote interface and then configure the camera, record, alarm, disk, network, account and authority and system of the NVR remotely. All of these settings are similar to that of the NVR. See the configurations of the NVR for details.

- **Jumping to IPC Web Client**

Except for IPCs that access with RTSP protocol, the IPC can be directly jumped from the NVR web client to the IPC web client by clicking ⚙ in the above-mentioned interface.

1. Please login the Web Client of NVR (See Web LAN Access or Web WAN Access for details).
2. Click ***Function Panel→Camera→Edit Camera*** to go to the following interface.



No.	Camera Name	Address	Port	Status	Protocol	Model	Preview	Edit	Delete	Settings	Upgrac	Version
1	IPC	10.20.23.37	9008	Offline	IP Camera	IPC	▶	✎	🗑	⚙	⤴	
2	IP Camera01	10.10.10.153	9008	Online	[redacted]	[redacted]	▶	✎	🗑	⚙	⤴	[redacted]7208)
3	IPC	10.20.52.201	9008	Online	IP Camera	[redacted]	▶	✎	🗑	⚙	⤴	[redacted]8020)

3. Select the camera and click ⚙ to log into the web client of the camera. From there, you can set the parameters of the camera as needed.

Appendix A FAQ

Q1. Why can't I find the HDD?

a. Please check the power and SATA data cables of the HDD to make sure they are properly connected.

b. For some NVRs with the 1U or small 1U case, the power of the adapter may be not enough for operating your HDD. Please use the power adaptor supplied along with your specific NVR.

c. Please make sure the HDDs are compatible with the NVR. See Appendix C Compatible Device List for details.

d. The HDD could have gone bad.

Q2. Why are there no images in some or all the camera windows?

a. Please make sure the resolutions of the cameras are supported by the NVR.

b. Please make sure the network cables of the IP camera and NVR are both connected properly and the network parameters are set correctly.

c. Please make sure the network and the switch both work normally.

Q3. Why does my screen have no output after booting the NVR normally?

a. Please make sure the screen, HDMI or VGA cables are functioning and properly connected.

b. Please make sure the screen supports the resolution of 1280*1024, 1920*1080 or 3840*2160 (4K*2K). The NVR cannot self-adapt to a screen of which the resolution is lower than 1280*1024, In that event, the screen will remind you that the resolution is not supported by the NVR or just not display anything. Please change the screen to 1280*1024, 1920*1080 or 3840*2160 resolution before booting the NVR.

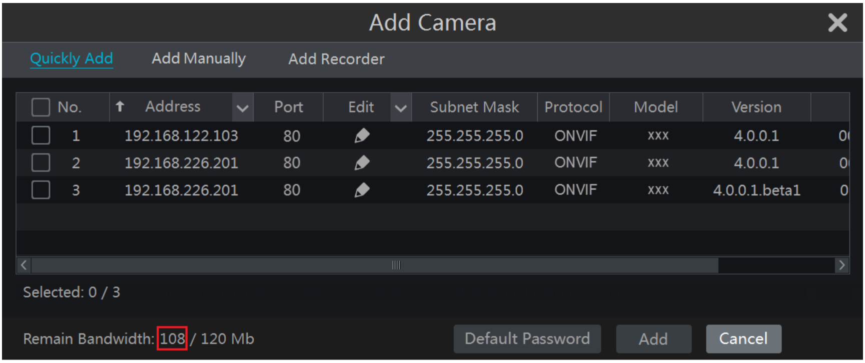
Q4. What do I do if I have forgotten my password?

a. The password for ***admin*** can be reset through the "Edit Security Question" function.
Click "Edit Security Question" in the login window and then enter the corresponding answer of the selected question in the popup window. After you correctly answer all questions, you can reset the password for ***admin***. If you forget the answers to these questions, there is no other way to restore the ***admin*** password, and you'll have to contact your dealer for assistance.

b. The passwords of other users can be reset by ***admin***, please refer to Edit User for details.

Q5. Why will my NVR not accept the maximum number of IP cameras?

Take a 16 CH NVR as an example. Some 16 CH NVRs support a maximum of 120Mbps bandwidth input (please take the real device as a standard). Refer to the picture below. The remaining bandwidth should be larger than the bandwidth of the IP camera you want to add, or you would fail to add an IP camera. You should lower the added cameras' bitrate to relieve the bandwidth. It is recommended to add cameras by "Quickly Add" for batch adding.



Add Camera

□ No.	↑ Address	Port	Edit	Subnet Mask	Protocol	Model	Version	
□ 1	192.168.122.103	80	✎	255.255.255.0	ONVIF	xxx	4.0.0.1	0
□ 2	192.168.226.201	80	✎	255.255.255.0	ONVIF	xxx	4.0.0.1	0
□ 3	192.168.226.201	80	✎	255.255.255.0	ONVIF	xxx	4.0.0.1.beta1	0

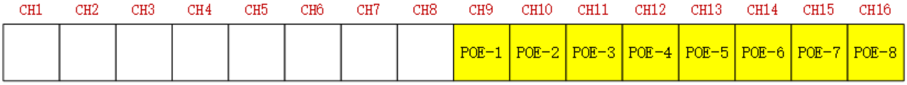
Selected: 0 / 3

Remain Bandwidth: 108 / 120 Mb

Q6. Why is an IP camera connected directly to the PoE port of my NVR not displayed automatically in the camera list?

a. Please check whether a PoE port is occupied by another IP camera that may have been added through the network (including a PoE switch).

- Take a 16 CH NVR with 8 PoE ports as an example. The resource distribution of the 16 CH IP cameras is shown in the picture below.

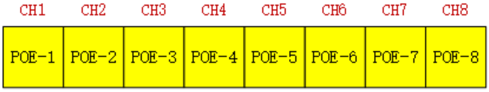


CH1	CH2	CH3	CH4	CH5	CH6	CH7	CH8	CH9	CH10	CH11	CH12	CH13	CH14	CH15	CH16
								POE-1	POE-2	POE-3	POE-4	POE-5	POE-6	POE-7	POE-8

When you add IP cameras through network, the IP cameras will occupy the resource from CH1, CH2, CH3, CH4…in the sequence they are added; if you directly connect IP cameras to the PoE ports of the NVR, the IP cameras will occupy ports from CH9 to CH16 according to the number of the PoE port each IP camera is connecting to.

Let's say 12 IP cameras have been added to the NVR through the network and no IP cameras have been directly connected to a PoE port. The 12 CH IP cameras occupy the 8 network resources from CH1 to CH8 and 4 PoE resources from CH9 to CH12 which otherwise would have been occupied by connecting the IP cameras directly. In this situation, if you directly connect one IP camera to PoE5, PoE6, PoE7 or PoE8, the IP camera will be displayed in the camera list automatically; if you connect it to PoE1, PoE2, PoE3 or PoE4, it won't be displayed in the camera list and will show a resource conflict; if you need to connect it to PoE1, PoE2, PoE3 or PoE4, you should first delete the IP camera which occupies the PoE port resource and then reconnect your camera to the PoE port.

- Take a 8 CH NVR with 8 PoE ports as another example. The resource distribution of the 8 CH IP cameras is shown in the picture below and the addition rules of the IP cameras are similar to the rules mentioned above. Please refer to the above for details.

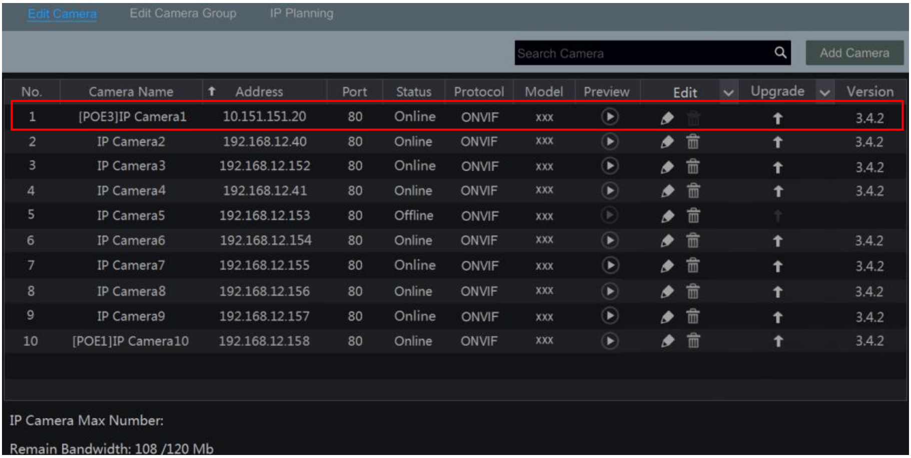


CH1	CH2	CH3	CH4	CH5	CH6	CH7	CH8
POE-1	POE-2	POE-3	POE-4	POE-5	POE-6	POE-7	POE-8

b. Please make sure that the internal Ethernet port and an IP camera which directly connects to a PoE port through the ONVIF protocol are in the same network segment, or you will fail to add the camera.
Log into the IP camera's Web client and then enable DHCP (to obtain an IP address automatically); or manually change the IP address of the IP camera to put it in the same network segment as the internal Ethernet port.
c. Check whether the number of the added IP camera exceeds the maximum allowed.
If the number of IP cameras exceeds the maximum allowed, the system will alert you that the IP camera count is exceeds the limit.

Q7. Why do I have no image output on an IP camera directly connected to the PoE port of my NVR using the ONVIF protocol, even though it's shown on the camera list?

Please make sure the username and password of the IP camera are correct. The IP camera's username and password can be modified through the two ways mentioned below.
① Click "Edit Camera" in the Camera module of the setup panel to go to the interface shown below. Click ✎ to modify the username and password of the IP camera (enter the correct username and password of the IP camera in the popup window and then click "OK").



No.	Camera Name	Address	Port	Status	Protocol	Model	Preview	Edit	Upgrade	Version
1	[POE3]IP Camera1	10.151.151.20	80	Online	ONVIF	xxx	▶	✎ 🗑	↑	3.4.2
2	IP Camera2	192.168.12.40	80	Online	ONVIF	xxx	▶	✎ 🗑	↑	3.4.2
3	IP Camera3	192.168.12.152	80	Online	ONVIF	xxx	▶	✎ 🗑	↑	3.4.2
4	IP Camera4	192.168.12.41	80	Online	ONVIF	xxx	▶	✎ 🗑	↑	3.4.2
5	IP Camera5	192.168.12.153	80	Offline	ONVIF	xxx	▶	✎ 🗑	↑	
6	IP Camera6	192.168.12.154	80	Online	ONVIF	xxx	▶	✎ 🗑	↑	3.4.2
7	IP Camera7	192.168.12.155	80	Online	ONVIF	xxx	▶	✎ 🗑	↑	3.4.2
8	IP Camera8	192.168.12.156	80	Online	ONVIF	xxx	▶	✎ 🗑	↑	3.4.2
9	IP Camera9	192.168.12.157	80	Online	ONVIF	xxx	▶	✎ 🗑	↑	3.4.2
10	[POE1]IP Camera10	192.168.12.158	80	Online	ONVIF	xxx	▶	✎ 🗑	↑	3.4.2

IP Camera Max Number:
Remain Bandwidth: 108 /120 Mb

② Go to the live view interface and then click ✎ in the preview window of the IP camera to edit the IP camera's username and password.

Q8. Why is my system not recording?

a. Make sure the HDD was formatted prior to use.
b. The recording schedule has not been set in customization mode. Please refer to <u>Schedule Settings</u> for details.
c. It's possible your HDD is full and the NVR is not able to record. Check HDD information from Disk Management and if required, please enable the recycle function (please see <u>Advanced</u>

Configuration for details).

d. There is no disk in the disk group, so please add at least one disk to the group. Refer to Storage Mode Configuration for details.

e. The HDD could have gone bad. Please change another one.

Q9. Fail to access the NVR remotely through IE.

a. Note that Internet Explorer is no longer supported by Microsoft and it's recommended to use another browser such as Chrome, Edge, Firefox, etc

b. Please make sure the IE version is IE8 or above.

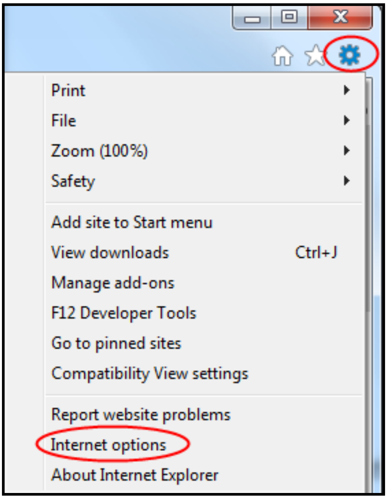
c. Please check whether the PC has enabled the firewall or installed the antivirus software. Please try to access the NVR again after you disable the firewall and stop the antivirus software.

d. Allow & block list may have been set in Account and Authority setting. The PC of which the IP address is in the block list or out of the allow list cannot access the NVR remotely.

Q10. ActiveX control cannot be downloaded. What can I do?

a. IE browser blocks ActiveX control. Please do setup as per the steps mentioned below.

① Open IE browser. Click ⚙ →Internet Options.

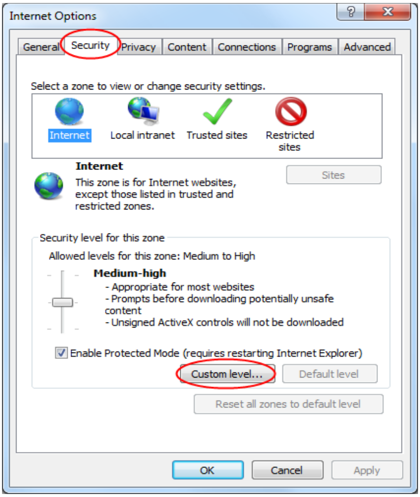


② Select ***Security→Custom Level***. Refer to Fig 10-1.

③ Enable all the sub options under "ActiveX controls and plug-ins". Refer to Fig 10-2.

④ Then click "OK" to finish setup.

b. Other plug-ins or anti-virus may block ActiveX. Please disable or do the required settings.



Select a zone to view or change security settings.

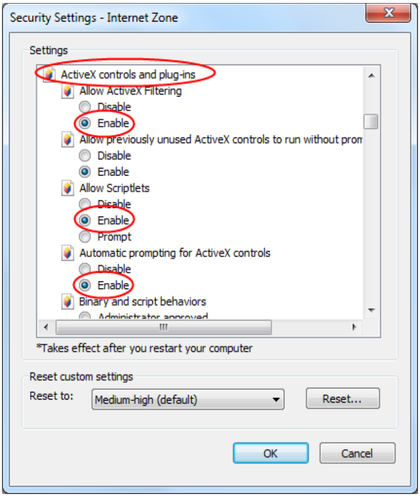
Internet
This zone is for Internet websites, except those listed in trusted and restricted zones.

Security level for this zone
Allowed levels for this zone: Medium to High

Medium-high
- Appropriate for most websites
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded

☑ Enable Protected Mode (requires restarting Internet Explorer)

Fig 10-1



Settings
ActiveX controls and plug-ins
Allow ActiveX Filtering
○ Disable
● Enable
Allow previously unused ActiveX controls to run without prom
○ Disable
● Enable
Allow Scriptlets
○ Disable
● Enable
○ Prompt
Automatic prompting for ActiveX controls
○ Disable
● Enable
Binary and script behaviors
○ Administrator approved

*Takes effect after you restart your computer

Reset custom settings
Reset to: Medium-high (default)

Fig 10-2

Q11. How do I play a backup file?

a. Recorded video backed up by NVR: insert the USB device with the recorded video backup files unto the USB interface of a PC, and then open the USB device path. The recorded video can be backed up in the private format and AVI format by NVR.

- If you select the private format when backing up recorded video by NVR, a RPAS compression package will be backed up to the USB device automatically along with the recorded video data. Uncompress the “RPAS.zip” and then click “RPAS.exe” to set up RPAS. After the setup is completed, open RPAS player and then click “Open Folder” in the middle of the interface to select the record data. Refer to Fig 11-1.

Select a camera in the resource tree on the left side of the interface to play the camera record. Click 🔇 on the tool bar under the camera image to enable audio. Refer to Fig 11-2.

> *Note: The record will not have audio output if you disable the audio when recording by NVR. Please see Mode Configuration and Encode Parameters Settings for details.*

- If you select the AVI format when backing up recorded video by NVR, the recorded video backup data can be played by a video player that supports this format.

b. Recorded video backed up through web. The recorded video can only be backed up using AVI format. The recorded video can be backed up to PC and played by the video player which supports this format.

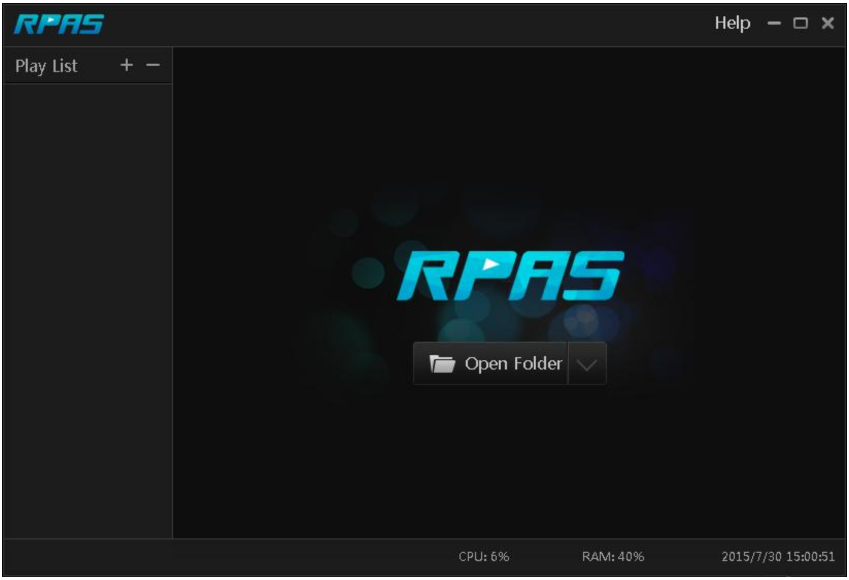


Fig 11-1

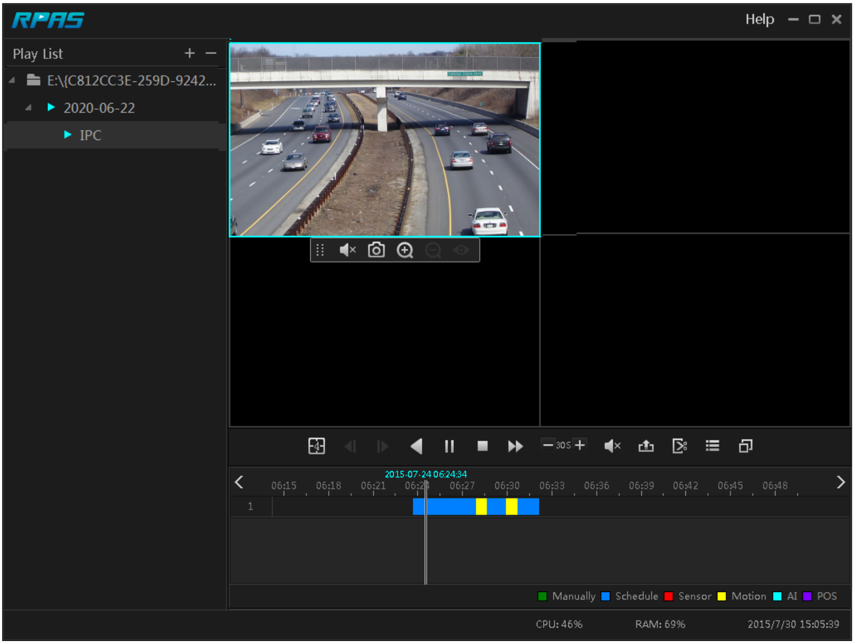


Fig 11-2

Q12. HTTPs service cannot work normally after directly installing the signed certificate.

a. When importing the certificate, the private key is not attached to the certificate.

b. When importing the certificate, the private key is attached to the certificate, but it is encrypted. At present, the NVR doesn’t support the certificate with the encrypted private key.

Q13. You are prompted with the unsafe statements/tips when using HTTPs service.

a. Please make sure your certificate is trusted.

b. Make sure whether the Common Name (domain information) of the certificate matches with the domain name of the visiting website.

c. Whether the certificate is within the period of validity.

Appendix B Calculate Recording Capacity

The recording capacity is mainly up to the record resolution, record stream and bitrate. Different image quality parameters decide different disk capacity occupation under equal circumstances. The higher the recording resolution, recording stream and recording bitrate is, the more disk capacity is taken up under equal circumstances. The calculation format of the recording capacity is shown as below.

Recording Capacity(MB) = Bitrate(Kbps) ÷1024 ÷8 ×3600 ×Recording hours per day × Record Storage Days ×channel numbers

3600 means record for an hour(1TB=1024GB，1GB=1024MB，1MB=1024KB，1Byte=8bit).

Record Bitrate (Kbps)	Used Space (MB/H)	Used Space (MB/D)
10240	4500	108000
8192	3600	86400
6144	2700	64800
4096	1800	43200
3072	1350	32400
2048	900	21600
1024	450	10800
768	337.5	8100
512	225	5400
384	168.75	4050
256	112.5	2700

The table below shows the recording capacity requirements for record storage in 30 days.

Record Bitrate (Kbps)	Recording Capacity(TB)					
	1CH	4CH	8CH	16CH	32CH	64CH
10240	3.09	12.36	24.72	49.44	98.88	197.76
8192	2.48	9.89	19.78	39.56	79.11	158.21
6144	1.86	7.42	14.84	29.67	59.33	118.66
4096	1.24	4.95	9.89	19.78	39.56	79.11
3072	0.93	3.71	7.42	14.84	29.67	59.33
2048	0.62	2.48	4.95	9.89	19.78	39.56
1024	0.31	1.24	2.48	4.95	9.89	19.78
768	0.24	0.93	1.86	3.71	7.42	14.84
512	0.16	0.62	1.24	2.48	4.95	9.89
384	0.12	0.47	0.93	1.86	3.71	7.42
256	0.08	0.31	0.62	1.24	2.48	4.95

For instance, there is a 32CH NVR recording 24 hours per day and the recordings are stored for 30 days and the NVR adopts dual stream recording. If the main stream is 4096Kbps and the sub stream is 1024Kbps, then the total recording capacity is 49.45TB (39.56TB + 9.89TB).

Considering the format loss of the disk is about 10%, the required disk capacity will be 55TB (49.45TB ÷(1-10%)).

Appendix C Compatible Device List

Compatible HDD list

Brand and Series		Capacity
Seagate	Barracuda Series	500GB /1TB /2TB /3TB
	SV35 Series (recommended)	1TB /2TB /3TB
	Surveillance HDD Series (recommended)	1TB /2TB /3TB /4TB /6TB/8TB/10TB
Western Digital	Blue Series	500GB /1TB
	Green Series	2TB /3TB /4TB
	Purple Series (recommended)	1TB /2TB /3TB /4TB /6TB/8TB/10TB

Compatible USB mobile device

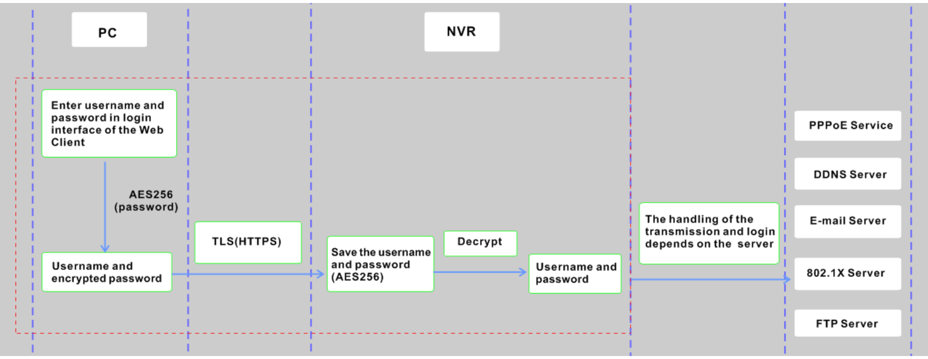
Brand	Capacity
SSK	2GB
Netac	4GB
Kingston	2GB/8GB/16GB/32GB
Aigo	2GB
Smatter vider	1GB
SanDisk	4GB/8GB/16GB/32GB

Appendix D Communication Port List

Port	Protocol (TCP/UDP)	Descriptions
80/443	TCP	HTTP/HTTPS communication port. It is opened by default and used to access the WEB client.
554	TCP	RTSP communication port. It is closed by default. After enabling RTSP function, this port will be opened and used to transfer audio and video stream.
6036	TCP	Private communication port. It is opened by default and used to transfer audio and video stream.
9036	TCP	This port is opened by default which is mainly used to receive the information sent by the POS terminal or printer. The information will be overlaid on the image of the IPC you have configured in previewing or recording mode.
41952-49156	TCP	This port is closed by default. After the UPnP or NAT function is enabled, this port is enabled too. It is mainly used to receive the request sent by other UPnP devices and communicate with other UPNP devices
1900	UDP	This port is opened by default which is used to enable, find and run SSDP. Additionally, it is also used to listen to and receive the multicast packets from other online UPnP devices.
6699	TCP	This port is closed by default. This port will be opened when adding cameras through ONVIF protocol for receiving event notifications.

Appendix E Personal Data Collection Description

There are five functions concerning the personal data collection under the network modules of the device, including PPPoE, DDNS, E-mail, 802.1x and FTP. In the device, these functions are used by the client-end of the device to communicate with the server of the customer's company (or service supplier). As the client-end, our device needs to keep the authentication credentials (username and password) used to connect the server. These credentials can be configured through the Web client of the device and then sent to the device. The process of the data transmission and storage are as follows.


PC
NVR
Enter username and password in login interface of the Web Client
AES256 (password)
Username and encrypted password
TLS(HTTPS)
Save the username and password (AES256)
Decrypt
Username and password
The handling of the transmission and login depends on the server
PPPoE Service
DDNS Server
E-mail Server
802.1X Server
FTP Server

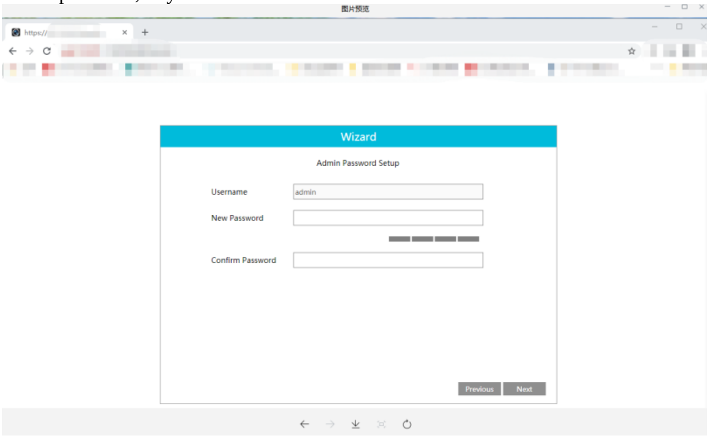
Function	Personal Data Type	Transmission Type	Storage Type	Authentication
PPPoE	Username, Password	TLS+AES256(password)	Password：AES256	Username/Password
DDNS	Username, Password	TLS+AES256(password)	Password：AES256	Username/Password
E-mail	Username, Password, E-mail address	TLS+AES256(password)	Password：AES256 The E-mail address will be desensitized before it is displayed on the page.	Username/Password
802.1x	Username, Password	TLS+AES256(password)	Password：AES256	Username/Password
FTP	Username, Password	TLS+AES256(password)	Password：AES256	Username/Password

Statement:

Except for service authentication when communicating with the server, we will never share these personal data stored on the device to the third-party or use them by ourselves without the client's authorization.

The log will record the operator's operation steps and change records, but will not contain any information about the collected personal data.

Appendix F Default Account List

Username	Default Password	Descriptions
admin	NO	Purpose：log onto the device and its clients Description： When you log in for the first time, a wizard will be displayed. You must set the password, or you cannot access the device.  Wizard Admin Password Setup Username admin New Password Confirm Password Previous Next
root	NO	Purpose：Test via serial port Description：The default password of “root” is null. It doesn’t mean you can log in the device without password. You must set the password of “admin” in the above-mentioned interface first. Then you can log in by using “root”.

Statement：

Remote testing/debugging doesn’t support for the device (Telnet/SSH unavailable). When an error occurs, the customer needs to send the device back to our company and tell us the password of “admin” used to log in the device and web client. Then the corresponding technician of our company will log in the serial port to find the problem. Without the customer’s identity verification information and the customer’s authentication, we cannot log in and do not have permission to log into the device.

Appendix G Command List

Command Type	Function	Command Contents
Operating Command	Hilinux Operating System Command	add-shell addgroup adduser arp ash awk basename blkid blockdev btools busybox cat chat chmod chpst cmp cp cut date dd delgroup deluser depmod devmem df diff dmesg dnsdomainname dos2unix du echo ed egrep eject env envdir envuidgid expr fbset fgrep find free fsck.vfat fsync getty grep groups halt head hexdump hiddrs himc himd himd.l himm hostname hwclock i2c_read i2c_write id ifconfig ifstat init insmod iostat ip ipaddr iplink iproute iprule iptables iptunnel kill killall killall5 ln login logname ls lsmod lsof lspci lsusb lzcat lzma md5sum mdev mkdir mkfifo mknod modinfo modprobe mount mountpoint mv netstat nice passwd pidof ping ping6 pmap poweroff pppd pppoe printf ps pstree pwd readlink reboot remove-shell renice restoreCFG_N9000.sh rm rmdir rmmod route sed setsid setuidgid sh shutdown_os.sh sleep softlimit stat stty sync tail tar test time top touch tty ubiattach ubidetach udevadm udevd udhcpc umount uname unix2dos unlzma uptime usleep vconfig vi watch wc xargs yes