

 VITEK® VT-TNR Series Network
Video Recorders with
Advanced Analytics

**Transcendent 8MP / 12MP
Real Time PoE NVRs with
Programmable / Advanced
Analytics**

PRODUCT MANUAL



THIS MANUAL IS APPLICABLE FOR MODELS:

VT-TNR414PN, VT-TNR818PN, VT-TNR818PFN, VT-TNR1626PN,
VT-TNR1646PFN, VT-TNR3216PFN, VT-TNR3280E1N

KEY FEATURES



- 4 / 8 / 16 / 32 Channel Stand-alone Real-time IP Network Video Recorders
- Full 8MP Recording ("PN" Models) / 12MP Resolution ("PFN" Models)
- 4K HDMI & VGA Video Outputs
- H.265S / H.265+ / H.265 / H.264 Video Compression
- Programmable Analytics including Face Detection & Target Counting (PFN "GEN IV" Models only), License Plate Recognition & Fisheye De-warping (through IE / App), Object Removal, Line Crossing, and Area and More!
- Plug and Play & Auto configuration for many leading ONVIF compliant IP Cameras
- Internal PoE Switches (Model Dependant)
- Single / Dual 1 Gigabit LAN Port, USB Ports
- Pentaplex: Live Display / Record / Playback / Backup / Remote Access
- SATA2 / SATA3 HDD Slots [up to 160TB - model dependent]
- Applications for iOS® & Android®
- Remote Viewing over the Internet via Web Browser or LAN
- Free VMS (Video Management Software)
- Control locally via USB Mouse or with the Included IR Remote control
- 3 Year Warranty



PLEASE NOTE:

Complete User Guide, Software, Tools, and Updates are available online. Scan the QR Code or visit:
<https://www.vitekccv.com>

Manual Notes

- Please read this user manual carefully to ensure that you understand how to use the device correctly and safely.
- There may be several technical or printing errors in this manual. Updates will be added to newer versions of this manual. Contents are subject to change without notice.
- This device should be operated only from the type of power source indicated on the label. The voltage of the power must be verified before using. It is recommended to 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. Ensure proper ventilation around the recorder.
- Always follow proper shutdown procedures.
- This recorder is for indoor use only. Do not expose the recorder to rain or moist environments. In case any solid or liquid gets inside the recorder'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 backup and clear the personal data stored in the device before the device is returned to us for repair or replacement other than data that is 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 multiple models. All examples and pictures used in the manual are from one of the models for reference purposes.

Disclaimer

- For products with internet access, the use of the product shall be wholly at your own risk. Vitek will not be responsible for abnormal operation, privacy leakage, or other damages resulting from cyber-attack, hacker attacks, viruses, 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 responsibility for any consequences resulting from illegal operations. In the event of any conflicts between this manual and the applicable law, the latter prevails.
- The storage of 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. Vitek shall not be responsible for data loss.

Cybersecurity Recommendations

- Use a strong password with at least 8 characters, a combination of numbers, and upper- and lower-case letters.
- Set a 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, please update it to ensure the system is current with the latest security patches and fixes. This feature is coming soon.
- 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 your system.
- It is recommended to set up 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 a public network. When it is necessary to be exposed to a public network, please configure an external hardware firewall and a corresponding firewall policy.
- It is not recommended to use the v1 and v2 functions of SNMP.
- To enhance the security of WEB client access, please create a TLS certificate to enable HTTPS.
- Use the block and allow list to filter IP addresses. 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 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 required.
- Check the log if you want to know whether your device has been accessed by unauthorized users or not. The system log will show you which IP addresses were used to log in to your system and what was accessed.

Regulatory Information

1.1 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 to 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.

1.2 CE Information

 The products have been manufactured to comply with the following directives.

EMC Directive 2014/30/EU

1.3 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.

***The models covered in this manual are manufactured in compliance with the Terms of the 2019 John S. McCain National Defense Authorization Act, using approved chipsets.**



1.4 Table of Contents

MANUAL NOTES	1
DISCLAIMER.....	1
CYBERSECURITY RECOMMENDATIONS.....	2
REGULATORY INFORMATION	2
1.1 FCC INFORMATION.....	2
1.2 CE INFORMATION	3
1.3 RoHS	3
1.4 TABLE OF CONTENTS.....	4
2 INTRODUCTION.....	10
2.1 FEATURES	10
2.2 FRONT PANEL DESCRIPTIONS	14
2.3 REAR PANEL DESCRIPTIONS.....	14
2.4 CONNECTIONS	19
3 BASIC OPERATION GUIDE	21
3.1 STARTUP & SHUTDOWN.....	21
3.1.1 Startup.....	21
3.1.2 Shutdown.....	21
3.2 REMOTE CONTROL	21
3.3 MOUSE CONTROL	23
3.4 TEXT-INPUT INSTRUCTION.....	24
3.5 COMMON BUTTON OPERATION.....	24
4 WIZARD & MAIN INTERFACE.....	25
4.1 STARTUP WIZARD.....	25
4.2 MAIN INTERFACE.....	32
4.2.1 Main Interface Introduction.....	32
4.2.2 Setup Panel	35
4.2.3 Main Functions	36
5 CAMERA MANAGEMENT	38
5.1 ADD/EDIT CAMERA	38
5.1.1 Add Camera	38
5.1.2 Edit Camera.....	40
5.2 ADD/EDIT CAMERA GROUP	41
5.2.1 Add Camera Group.....	41
5.2.2 Edit Camera Group.....	43

5.2.3	IP Planning	43
6	LIVE VIEW INTRODUCTION	44
6.1	LIVE VIEW INTERFACE INTRODUCTION	44
6.2	VIEW MODE.....	45
6.2.1	Preview by Display Mode	45
6.2.2	Quick Sequence View	48
6.2.3	Camera Group View in Sequence	48
6.2.4	Scheme View in Sequence	49
6.3	POS SETTINGS.....	51
6.4	PREVIEW IMAGE CONFIGURATION	54
6.4.1	OSD Settings	54
6.4.2	Image Settings	55
6.4.3	Mask Settings	56
6.4.4	Fisheye Settings	56
6.4.5	Image Adjustment.....	57
7	PTZ.....	60
7.1	PTZ CONTROL INTERFACE INTRODUCTION	60
7.2	PRESET SETTINGS	65
7.3	CRUISE SETTINGS	66
7.4	CRUISE GROUP SETTINGS	67
7.5	TRACE SETTINGS	67
7.6	TASK SETTINGS	68
7.7	SMART TRACKING	69
8	RECORD & DISK MANAGEMENT	72
8.1	RECORD CONFIGURATION.....	72
8.1.1	Mode Configuration.....	72
8.1.2	Schedule Settings	74
8.1.3	Advanced Configuration	77
8.2	ENCODE PARAMETERS SETTINGS	77
8.3	RECORD MODE.....	78
8.3.1	Manual Recording.....	78
8.3.2	Schedule Recording.....	78
8.3.3	Motion Based Recording.....	78
8.3.4	Sensor Based Recording	78
8.3.5	AI Event Recording	78
8.4	DISK	79
8.4.1	Disk Management	79
8.4.2	Storage Mode Configuration	82
8.4.3	View Disk Information	83
9	PLAYBACK & BACKUP.....	85

9.1 INSTANT PLAYBACK.....	85
9.2 PLAYBACK INTERFACE INTRODUCTION	85
9.3 SMART PLAYBACK	90
9.3.2 <i>Smart Playback Settings</i>	91
9.3.3 <i>Smart Playback Based on Motion Detection</i>	91
9.3.4 <i>Smart Playback by Face Search</i>	92
9.3.5 <i>Smart Search by License Plate</i>	94
9.3.6 <i>Smart Search by Object Attributes</i>	95
9.4 RECORD SEARCH, PLAYBACK & BACKUP.....	95
9.4.1 <i>Search, Playback & Backup by Time-sliced Image</i>	96
9.4.2 <i>Search, Playback & Backup by Time</i>	98
9.4.3 <i>Search, Playback & Backup by Event</i>	98
9.4.4 <i>Search & Playback by Tag</i>	99
9.4.5 <i>Image Management</i>	100
9.4.6 <i>View Backup Status</i>	100
10 AI EVENT MANAGEMENT	101
10.1 FACE RECOGNITION.....	101
10.1.1 <i>Face Detection Settings</i>	101
10.1.2 <i>Face Database Management</i>	103
10.1.3 <i>Face Recognition Settings</i>	105
10.2 LICENSE PLATE RECOGNITION.....	107
10.2.1 <i>License Plate Detection Settings</i>	107
10.2.2 <i>Plate Database Management</i>	108
10.2.3 <i>License Plate Recognition Settings</i>	109
10.3 LINE CROSSING DETECTION	110
10.4 INTRUSION DETECTION.....	112
10.5 ABANDONED/MISSING OBJECT DETECTION	112
10.6 CROWD DENSITY DETECTION.....	113
10.7 TARGET COUNTING	114
10.8 EXCEPTION DETECTION.....	117
10.9 FIRE DETECTION.....	117
10.10 TEMPERATURE DETECTION.....	118
10.11 VIDEO METADATA	119
11 INTELLIGENT ANALYTICS.....	121
11.1 TARGET DETECTION VIEW	121
11.1.1 <i>Human Body/Vehicle Detection View</i>	121
11.1.2 <i>Face Detection/Match View</i>	121
11.1.3 <i>License Plate Detection/Recognition View</i>	125
11.1.4 <i>Object Attribute View</i>	127
11.2 SMART SEARCH	128
11.2.1 <i>Face Search</i>	128

11.2.2 Track Playback.....	131
11.2.3 Face Search by Snapshot	134
11.2.4 Human Body Search.....	134
11.2.5 Vehicle Search	135
11.2.6 Combination Search.....	137
11.3 VIEW STATISTICAL INFORMATION	137
11.4 ENABLING AI MODE.....	139
12 GENERAL EVENT MANAGEMENT	140
12.1 SENSOR ALARM.....	140
12.2 MOTION ALARM.....	141
12.2.1 Motion Configuration	141
12.2.2 Motion Alarm Handling Configuration	142
12.3 COMBINATION ALARM	143
12.4 EXCEPTION ALARM	144
12.4.1 IPC Offline Settings	144
12.4.2 Exception Alarm Settings	144
12.5 ALARM EVENT NOTIFICATION	145
12.5.1 Alarm-out	145
12.5.2 E-mail.....	145
12.5.3 Display.....	145
12.5.4 Buzzer.....	146
12.5.5 Push Text.....	146
12.5.6 Audio	146
12.5.7 Light.....	148
12.5.8 Alarm Server	148
12.6 MANUAL ALARM.....	149
12.7 VIEW ALARM STATUS.....	149
12.8 SYSTEM DISARMING.....	150
13 APPLICATION.....	152
13.1 FACE ATTENDANCE.....	152
13.2 FACE CHECK-IN.....	153
13.3 PARKING LOT SETTINGS	154
13.3.1 Basic Settings.....	154
13.3.2 Parking Space Settings	154
13.3.3 Entrance/Exit Management	155
13.3.4 Parking Lot Management	155
13.3.5 Search Vehicle Entry/Exiting Records.....	156
13.4 ACCESS CONTROL MANAGEMENT.....	157
13.4.1 Access Control Settings.....	157
13.4.2 Open a Door Manually.....	158
14 ACCOUNT & PERMISSION MANAGEMENT	159

14.1 ACCOUNT MANAGEMENT	159
14.1.1 Add User	159
14.1.2 Edit User	160
14.2 USER LOGIN & LOGOUT	162
14.3 PERMISSION MANAGEMENT	162
14.3.1 Add Permission Group	162
14.3.2 Edit Permission Group	163
14.4 BLOCK AND ALLOW LIST	163
14.5 PREVIEW ON LOGOUT	164
14.6 NETWORK SECURITY	164
14.7 PASSWORD SECURITY	165
14.8 VIEW ONLINE USER	165
15 DEVICE MANAGEMENT	166
15.1 NETWORK CONFIGURATION	166
15.1.1 TCP/IP Configuration	166
15.1.2 Port Configuration	168
15.1.3 PPPoE Configuration	171
15.1.4 DDNS Configuration	172
15.1.5 E-mail Configuration	174
15.1.6 UPnP Configuration	175
15.1.7 802.1X	176
15.1.8 NAT Configuration	176
15.1.9 FTP Configuration	177
15.1.10 SNMP	178
15.1.11 Cloud Upgrade	179
15.1.12 Platform Access	179
15.1.13 UPnP Report Access	180
15.1.14 ONVIF	180
15.1.15 Network Status	181
15.2 BASIC CONFIGURATION	181
15.2.1 Common Configuration	181
15.2.2 Date and Time Configuration	182
15.2.3 Recorder OSD Settings	183
15.2.4 PoE Power Management	183
15.3 FACTORY DEFAULT	184
15.4 DEVICE SOFTWARE UPGRADE	184
15.5 BACKUP AND RESTORE	184
15.6 RESTART AUTOMATICALLY	185
15.7 VIEW LOG	185
15.8 VIEW SYSTEM INFORMATION	186
16 REMOTE SURVEILLANCE	187

16.1 MOBILE CLIENT SURVEILLANCE.....	187
16.2 WEB LAN ACCESS	187
16.3 WEB WAN ACCESS	188
16.4 WEB REMOTE CONTROL.....	189
16.4.1 Remote Preview.....	191
16.4.2 Remote Playback.....	194
16.4.3 Remote Search and Backup.....	195
16.4.4 Intelligent Analysis.....	195
16.4.5 Application.....	195
16.4.6 Remote Configuration.....	196
APPENDIX A FAQ	197
APPENDIX B: CALCULATE RECORDING CAPACITY	202
APPENDIX C COMPATIBLE DEVICE LIST.....	204
APPENDIX D: COMMUNICATION PORT LIST	205
APPENDIX E: PERSONAL DATA COLLECTION DESCRIPTION...	206
APPENDIX F: DEFAULT ACCOUNT LIST.....	208
APPENDIX G: COMMAND LIST.....	209

2 Introduction

2.1 Features

Basic Functions

- Supports network device access including IP cameras and Onvif IP cameras
- Some NVRs support H.265S/H.265+/ H.265 and H.264S/H.264+/ H.264 IP cameras
- Supports standard ONVIF protocol
- Supports dual stream recording of each camera
- Supports quickly or manually adding IP cameras
- Supports collective or individual configuration of the cameras' OSD, video parameters, mask, motion etc.
- Supports smart detection access and linkage, 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 the default Administrator, Advanced, and Ordinary permission groups.
- Supports the creation of multiple users, the ability to have multiple web clients logged in using one username at the same time, and the enabling or disabling of user permission controls.
- Supports multiple web client logins at the same time (depending on models)
- Supports binding the NVR to an account on 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
- Some models support face capture view, face match view, license plate recognition view, and human/motor vehicle /non-motor vehicle view
- Supports auto adjustment of the camera's image display proportion
- Supports enabling or disabling audio monitoring for each camera
- Supports manually snapshotting the live view of a camera
- Supports adjustment of the sequence of the preview cameras
- Supports saving and recalling custom display modes
- Supports operation of the preview window using the quick tool bar
- Supports group view, sequence view scheme, quick sequence view, and dwell time settings for the cameras
- Supports motion detection and video mask
- Supports multiple popular P.T.Z. control protocols and the setup of the preset and cruise
- Supports direct mouse control in order to rotate, zoom, focus, and so on for cameras

- Supports sliding the mouse wheel to zoom for a single camera image
- Supports zooming in on any area of the image up to 16 times the current size
- Supports image and lens adjustment (only available for some cameras)
- Supports quickly adding cameras from the live preview interface
- The live camera sequence of the web client will keep consistent with that of the NVR after adjusting the live camera sequence of the NVR, but the live camera sequence of the NVR will not be changed if that of the web client is changed

Disk Management

- NVRs with a 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 of the NVR supports HDDs with a max capacity of 10TB. Some models may support 12TB capacity
- Supports disk hot swapping
- 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 working status
- Supports batch formatting of disks

Record Configuration

- Supports mainstream and sub stream recording at the same time and batch or single configuration of the record stream
- Supports automatic and custom recording modes
- Supports scheduled recording, sensor alarm recording, and motion detection recording, etc
- Supports smart playback using drawn lines, quadrilaterals, or rectangles.
- Supports scheduled recording and event recording having different encoding settings
- Supports recording schedule setting and recycling recordings
- Supports pre-recording and post-recording configuration for event recordings

Recording Playback

- Supports timeline operation during quick playback and playback date and time being set randomly by scrolling the mouse; the time interval of the timeline can be zoomed in and out
- Supports recording searching by time slice/time/event/tag
- Supports smart playback by drawing a grid, line, or quadrilateral and vehicle smart playback (some models also support smart playback by face)
- Supports time view and camera view when searching using the time slice mode
- Supports searching by month, day, hour, or minute when using time slice searching and displaying camera thumbnails when using time slice mode
- Supports a maximum view of 16 cameras when searching recordings by time
- Supports using manual/motion/sensor/intelligent events when searching by event
- Supports manually adding and searching tags in recordings
- Supports instant playback for selected cameras in the live preview interface
- Supports a maximum of playing back 16 synchronous cameras

- Supports speeding up (maximum 32 times of the normal speed), slowing down (minimum 1/32 times of the normal speed), and jumping forward or back 30 seconds during recordings

Record Backup

- Supports record to be backed up through USB (U disk, mobile HDD) interface
- Supports backing up recordings by time/event/image searching
- Supports cutting time out of the timeline to back up recordings during playback
- Supports multiple backup tasks in the background and viewing the backup status

Event Management

- Supports configuring the schedule settings for alarm functions
- Supports enabling or disabling motion detection, external sensor alarm input, combination alarm, intelligence 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 etc., alarm linkage configuration is supported
- Supports linking an IPC offline alarm to a PTZ event, snapshotting on a camera, bringing up a pop-up window with a camera's video, etc.
- Supports event notifications triggering alarm-out, pop-up video, pop-up message box, buzzer, e-mail and so on
- Snapshots of cameras can be attached to an e-mail when alarm linkage is triggered
- Supports viewing the alarm status of alarm-in, alarm-out, motion detection, and exception alarm
- Supports triggering and clearing alarms manually
- Supports auto rebooting the system when an exception alarm happens
- Supports alarm linkage based on face detection, vehicle detection and license plate recognition
- Some models support triggering an alarm when there is a face match

Face Recognition

- 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 search by image, track playback, and database management
- Supports face information statistics
- Supports face match alarm

LPR Function

- Supports registering 50,000 license plates (some models only support registering 1,000 license plates)
- Supports license plate detection, match, and search
- Supports vehicle information statistics
- Supports triggering an alarm when there is a license plate match

Application

- Supports parking lot management
- Supports access control management
- Supports face attendance and face check in (depending on models)

Network Functions

- Supports TCP/IP and PPPoE, DHCP, DNS, DDNS, UPnP, NTP, SMTP protocols and so on
- Supports block and allow list function and blocking/allowing based on the IP address/IP segment/MAC address
- Supports multiple browsers including Microsoft Edge, Firefox, Opera, Chrome (available only for the versions lower than 45) and Safari in MAC system. Units on certain firmware versions must use Edge Browser in Internet Explorer mode
- Supports remote achievement, configuration, import and export of the NVR parameters and other system maintenance operations including remote upgrading and system restart
- Supports remote configuring cameras remotely through the NVR including video parameters, image quality, and so on
- Supports remotely searching, viewing playback, and backing up footage on the NVR
- Supports manually triggering/clearing alarms remotely
- Supports adjustment of auto-focusing cameras through the web client (supports zoom in/out, but one key focus is not currently supported)
- Supports the VMS or other platform management software accessing the NVR and managing it
- Supports the NAT function and QRCode scanning by mobile phones and tablets
- Supports mobile surveillance on phones or tablets with iOS or Android OS
- If one camera recording is enabled or disabled manually through web client, it will be simultaneously enabled or disabled in the NVR
- Supports direct jumping from NVR web client to IPC web client in a local network
- The installation mode and display mode of a fisheye camera can be set via the Web client

Other Functions

- The NVR can be controlled and operated by the buttons on the front panel, the remote control, and the mouse where applicable
- Setting interfaces can be switched to one another conveniently by clicking the main menus on the top of the setting interfaces
- Supports viewing the NVR's information including basic info, camera status, alarm status, record status, network status, disk info, and backup status
- Supports factory restoring, importing and exporting the system configuration, viewing activity logs, and exporting and local upgrading by a USB storage device
- Supports auto recognition of a monitor's resolution
- You can click the right mouse button at any interface to go back to the upper interface
- You can click the middle mouse button 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 reserved if you reset the NVR to factory default
- Press and hold the right mouse button for 5 seconds in any interface to switch the resolution the NVR is outputting to the monitor

2.2 Front Panel Descriptions

The following descriptions are for reference only.

Type I:

Name	Descriptions
REC	When recording, the light is blue
Net	The light turns blue when it is able to access the network
Power	Power indicator, when connected , the light is blue
Fn	No function temporarily

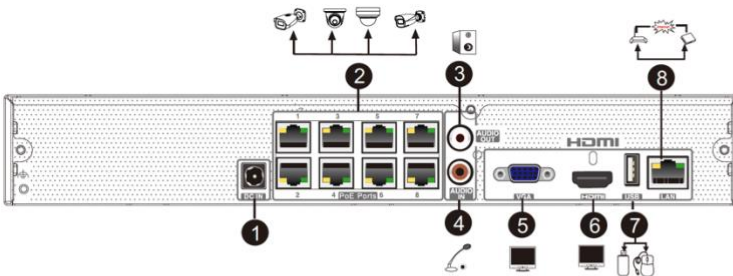
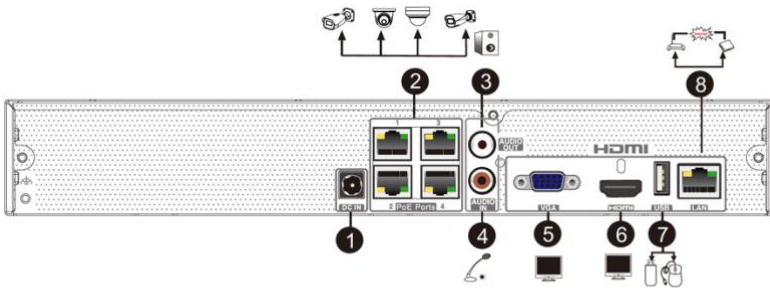
Type II:

Name	Descriptions
Power	Power Indicator, when connected, the light is blue
HDD	The light turns blue when reading/writing HDD
Net	The light turns blue when it is able to access the network
Backup	The light turns blue when backing up files and data
Play	The light turns blue when playing video
REC	Power Indicator, when connected, the light is blue
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 the Menu from live view
INFO	Check the information of the device
BACKUP	Enter backup mode from live view
SEARCH	Enter search mode from live view
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

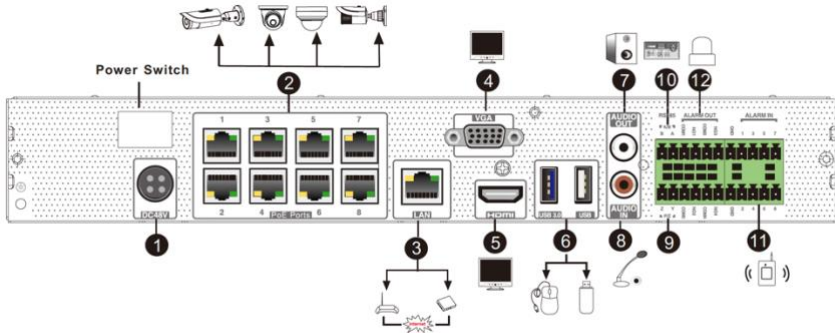
2.3 Rear Panel Descriptions

Here we use mock-up pictures of panels as an example to introduce their interfaces and connections. The interfaces and locations of the interfaces are only for reference. The real recorder's layout may vary.

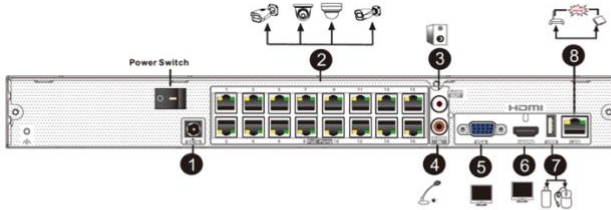
VT-TNR414PN & VT-TNR818PN



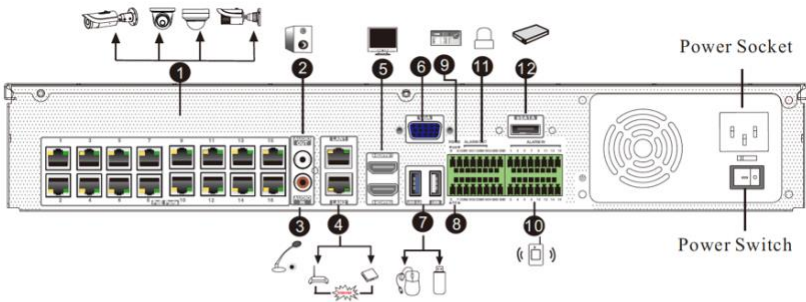
Number	Name	Description
1	DC IN	Connector for power input
2	PoE Ports	PoE network ports; connect to PoE IP cameras
3	AUDIO OUT	Audio output
4	AUDIO IN	Audio input
5	VGA	Connect to monitor
6	HDMI	Connect to high definition display device
7	USB	Connector for USB device (like USB mouse, USB storage device for backup or upgrade, etc.)
8	LAN	Ethernet port

VT-TNR818PFN

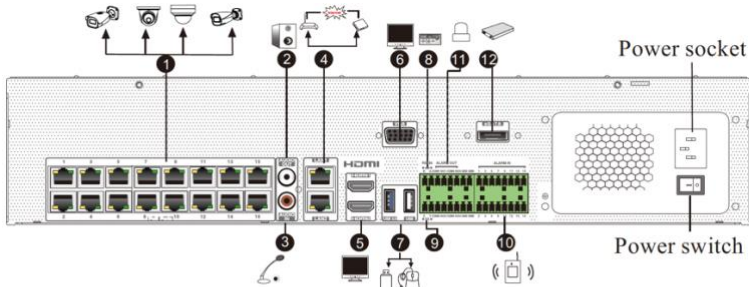
Number	Name	Description
1	DC48V	Connector for power input
2	PoE Ports	8 PoE network ports; connect to PoE IP cameras
3	LAN	Ethernet port
4	VGA	Connect to monitor
5	HDMI	Connect to high definition display device
6	USB3.0/USB	Connectors for USB devices (like USB mouse, USB storage device for backup or upgrade, etc.)
7	AUDIO OUT	Audio output
8	AUDIO IN	Audio input
9	P/Z	Currently no function
10	K/B	Connector for a keyboard. A is TX+, B is TX-
11	GND & ALARM IN	Connectors for alarm input devices, like sensors
12	ALARM OUT	Relay output; connectors for external alarm output devices

VT-TNR1626PN

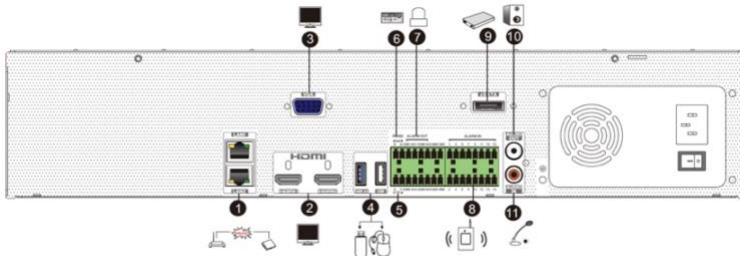
Number	Name	Description
1	DC IN	Connector for power input
2	PoE Ports	PoE network ports; connect to PoE IP cameras
3	AUDIO OUT	Audio output
4	AUDIO IN	Audio input
5	VGA	Connect to monitor
6	HDMI	Connect to high definition display device
7	USB	Connector for USB device (like USB mouse, USB storage device for backup or upgrade, etc.)
8	LAN	Ethernet port

VT-TNR1646PFN

Number	Name	Description
1	PoE Ports	16 PoE network ports; connect to PoE IP cameras
2	AUDIO OUT	Audio output connector
3	AUDIO IN	Audio input connector
4	LAN1/2	2 RJ45 10/100/1000Mbps self-adaptive Ethernet ports
5	HDMI1/2	HDMI video output connector
6	VGA	VGA connector, to connect to VGA monitor
7	USB/USB3.0	Connector for USB devices (like USB mouse, USB storage device)
8	P/Z	Connector for a PTZ device. Y is TX+, Z is TX-
9	K/B	Connector for a keyboard. A is TX+, B is TX-
10	GND & ALARM IN	Connectors for alarm input devices, like sensors
11	ALARM OUT	Relay output; connectors for external alarm output devices
12	E-SATA	Connector for the external HDD with E-SATA interface

VT-TNR3216PFN

Number	Name	Description
1	PoE Ports	16 PoE network ports; connect to PoE IP cameras
2	AUDIO OUT	Audio output connector
3	AUDIO IN	Audio input connector
4	LAN1/2	Ethernet port
5	HDMI/2	Connect to high definition display device
6	VGA	Connect to monitor
7	USB/USB3.0	Connector for USB devices (like USB mouse, USB storage device)
8	K/B	Connector for a keyboard; (A is TX+, B is TX-)
9	P/Z	Currently no function
10	GND & ALARM IN	Connectors for alarm input devices, like sensors
11	ALARM OUT	Relay output; connectors for external alarm output devices
12	E-SATA	Connector for the external HDD with E-SATA interface

VT-TNR3280E1N

Number	Name	Description
1	LAN1/2	Ethernet port
2	HDMI/2	Connect to high definition display device
3	VGA	Connect to monitor
4	USB/USB3.0	Connector for USB devices (like USB mouse, USB storage device)
5	P/Z	Currently no function
6	K/B	Connector for a keyboard; (A is TX+, B is TX-)
7	ALARM OUT	Relay output; connectors for external alarm output devices
8	GND & ALARM IN	Connectors for alarm input devices, like sensors
9	E-SATA	Connector for the external HDD with E-SATA interface
10	AUDIO OUT	Audio output connector
11	AUDIO IN	Audio input connector

2.4 Connections

- Video Connections

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

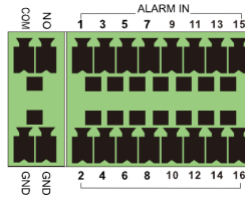
- Audio Connections

Audio Input: Connect to microphone, pickup, etc.

Audio Output: Connect to headphones, sound box or other audio output devices.

- Alarm Connections

Some models may not support this function. An interface with 16 CH alarm inputs and 1 CH alarm output is shown as an example.



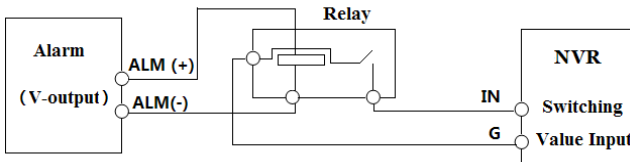
Alarm Input:

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 sensors to the device is shown below:



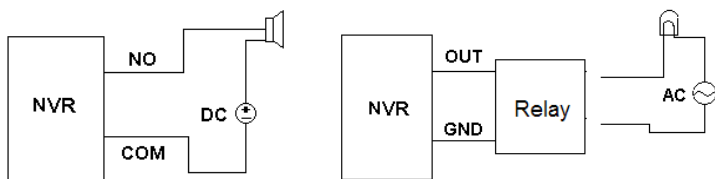
The alarm input is an open/closed relay. If the input is not an open/closed relay, please refer to the following connection diagram:



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 shown in the following figures:



3 Basic Operation Guide

3.1 Startup & Shutdown

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

3.1.1 Startup

- ① Connect the output display device to the VGA/HDMI interface of the NVR.
- ② Connect a mouse and the power. Flip the power switch on. The device will boot up and the power LED will turn blue.
- ③ After you read the privacy statement, a WIZARD window will pop up (you should select your display language the first time you use the NVR). Refer to [3.1 Startup Wizard](#) for details.

3.1.2 Shutdown

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

Using the remote control:

- ① Press the Power button. This will take you to a shutdown window. The unit will power off after clicking the “OK” button.
- ② Disconnect the power.

1. Using a mouse:

- ① Click Start→Shutdown to bring up 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.

3.2 Remote Control

- ① Two AAA size batteries are required for the remote.
- ② Open the battery cover of the remote control.
- ③ Place the batteries into the remote. Please observe the polarity (+ and -).
- ④ Replace the battery cover.

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

1. Check the batteries' polarity.
2. Check the remaining charge in the batteries.
3. Check the IR control sensor for anything covering it.

If it still doesn't work, please change to a new remote control, or contact your dealer. You can turn the IR sensor of the remote control toward the IR receiver of the NVR to control it when you are controlling multiple devices using a remote control.

There are two kinds of remote controls. The interface of remote control is shown below.

1. Type I:

VT-TNR1646PFN

VT-TNR3216PFN

VT-TNR3280E1N



Button	Function
Power Button	Switch off—to stop the device
Record Button	To start recording
-/-- /0-9	Input number or choose camera
Fn1 Button	Unavailable temporarily
Multi Button	To choose multi screen display mode
Next Button	To switch to the next camera in the live view
SEQ	To go to sequence view mode
Audio	To enable audio output in live view mode
SPOT	No function temporarily
Direction button	To move the cursor in setup or pan/tilt PTZ
Enter Button	To confirm choices in the setup menus
Menu Button	To go to the main menu
Exit Button	To exit the current interface
Focus/IRIS/Zoom/PTZ	To control PTZ cameras
Preset Button	To enter into preset settings for PTZ mode
Cruise Button	To go to cruise settings for PTZ mode
Track Button	No track function temporarily
Wiper Button	No function temporarily
Light Button	No function temporarily
Clear Button	No function temporarily
Fn2 Button	No function temporarily
Info Button	Get information about the device
	To control playback. Play(Pause)/Stop/Previous Frame/Next Frame/Speed Down/Speed Up
Snap Button	To take snapshots manually
Search Button	To go to the search and backup interface
Cut Button	No function temporarily
Backup Button	To go to the search and backup interface
Zoom Button	To zoom in on the camera's image in live view
PIP Button	No function temporarily

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

Password input: Move to the password entry box by pressing ▲ ▼ ◀ ▶ and then press the digital numbers to enter the password; press “Exit” to delete the inputted digital number; You cannot enter a password using digital numbers +

letter using the remote control. You will need to input it with a mouse.

Playback control: Press  to enter the playback interface. Press  or  to speed down or up the recorded video; press “Next” to switch the currently playing 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 a PTZ camera using the direction buttons and then press the “PTZ” button to go into PTZ control mode. Press the direction buttons to move the PTZ camera; press “Preset”+ “digital number” (eg. 3) to call the corresponding preset; press “Cruise” + “digital number” (eg.1) to call the corresponding cruise event. Note that the corresponding preset and cruise must be set using a mouse in advance, or they cannot be called.

2. Type II: VT-TNR414PN/PFN, VT-TNR818PN/PFN, VT-TNR1626PN



Button	Function
REC	Record manually
Search	To enter the search and backup interface
MEUN	To enter the main menu
Exit	To exit the current interface
ENTER	To confirm a choice in the setup menu
Direction button	To move the cursor in the setup menu
ZOOM	To zoom in
PIP	No function temporarily
  	To control playback. Play(Pause)/Next Frame/Speed Up/Stop/Previous Frame/Speed Down
  	
Multi	To choose multi screen display mode
Next	To switch camera
SEQ	To 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 control without digital numbers, you need to log into the device with a mouse first. Then point the IR sensor of the remote control towards the IR receiver of the NVR to control it.

3.3 Mouse Control

- Mouse control in Live Display & Playback interface

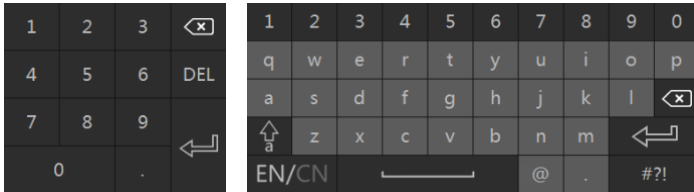
In the live display & playback interface, double click on any camera window to show the window in single screen mode; double click the window again to restore it to the previous size. In the live display & playback interface, if the interface is

displayed in full screen, move the mouse to the bottom of the interface to bring up a tool bar. 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 bring 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.

3.4 Text-input Instruction



The system includes two input boxes. Refer to the above pictures. The left box is the number input box and the right box is the input box which 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 to punctuation characters
	Delete Key		Enter key
	Switch between uppercase and lowercase letters		Space key

3.5 Common Button Operation

Button	Meaning
	Click to show the menu list.
	Click to change the sequence of the list.
	Click to change the camera display mode.
	Click to close the current interface.
	Click to go to the earliest date of camera recording.
	Click to go to the latest date of camera recording.

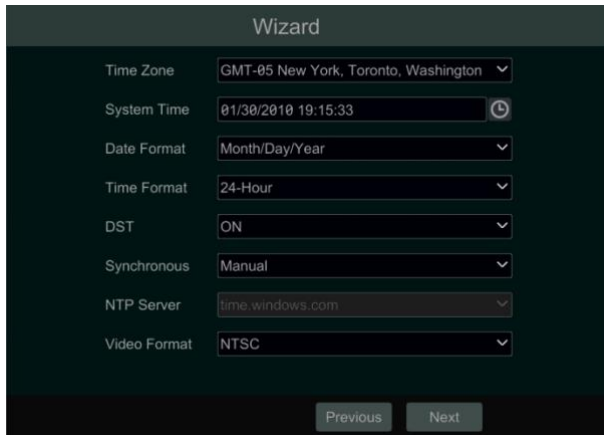
4 Wizard & Main Interface

4.1 Startup Wizard

The disk icons are 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 DVR using the setup wizard. You can configure settings with the wizard when you start the DVR for the first time (click “Skip” to use the wizard next time you reboot). Different versions may have different wizard steps. The following wizard steps are for reference only.

- ① Choose your language and locality if it is the first time using 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 when using the wizard for the first time. Refer to the below picture. Set the time zone, system time, date format, time format, and video format. DST will be enabled by default if the time zone selected uses DST. Click “Next” to continue.



The screenshot shows a 'Wizard' configuration window with the following settings:

Setting	Value
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

At the bottom of the window are two buttons: 'Previous' and 'Next'.

- ③ **System Login.** Set your own password when you use the wizard for the first time (the default username of the system is ***admin***); you'll use this password to log into the admin account next time you start up the machine.

Wizard

Admin Password Setup

Username: admin

New Password: 123456

Confirm Password: 123456

☒ Display Password ☐ Log In Automatically

Pattern Lock: ☐ Enable Edit

Previous Next

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

Pattern Lock

Click “Next” to set security questions and answers that can be used to reset the admin password. 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 number of disks, disk capacity, disk serial number, and the R&W status of the disk. Click “Format” to format the disk. Click “Next” to continue. Then click “Wizard Setup”.
- ⑤ **Network Settings.** Check “Obtain an IP address automatically” and “Obtain DNS automatically” to get the IP address and DNS automatically (DHCP must be enabled on the router being used in the local network), or manually enter them. Enter an HTTP port, HTTPS port, and Server port (please see [14.1.2 Port Configuration](#) for details). Click “Next” to continue.

Wizard

Network Settings > Add Camera > Report Settings > QoS Setup > User Upgrade

Ethernet Port 1 (Online)

☒ Obtain an IP address automatically

Address: 10 . 15 . 1 . 168

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

Previous Next Cancel

1. **Note:**

- If you use an NVR with PoE network ports, the online state of the internal Ethernet ports will be shown on the interface. Refer to the picture below. Please refer to [14.1.1 TCP/IP Configuration](#) for a detailed introduction of the internal Ethernet port.

Wizard

Network Settings > Add Camera > Report Settings > QoS Setup > User Upgrade

Subnet Mask: 255 . 255 . 0 . 0 Gateway: 10 . 20 . 0 . 1 ☐ Obtain DNS automatically Preferred DNS: 8 . 8 . 8 . 8 Alternate DNS: . . .	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

Default Route: Ethernet Port 1

Port

HTTP Port: 80 HTTPS Port: 443

Server Port: 6036

Previous Next Cancel

- If the NVR has two network ports or more, you can select the network work pattern (depending on models) as needed. The work patterns “Network Fault Tolerance” and “Multiple Address Setting” are available. Refer to the pictures below. Please refer to

14.1.1 TCP/IP Configuration for more detailed information.

Wizard

Network Settings > **Add Camera** > Network Settings > **IP Code** > **Check 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

Previous Next Cancel

Wizard

Network Settings > **Add Camera** > **Network Settings** > **IP Code** > **Check 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

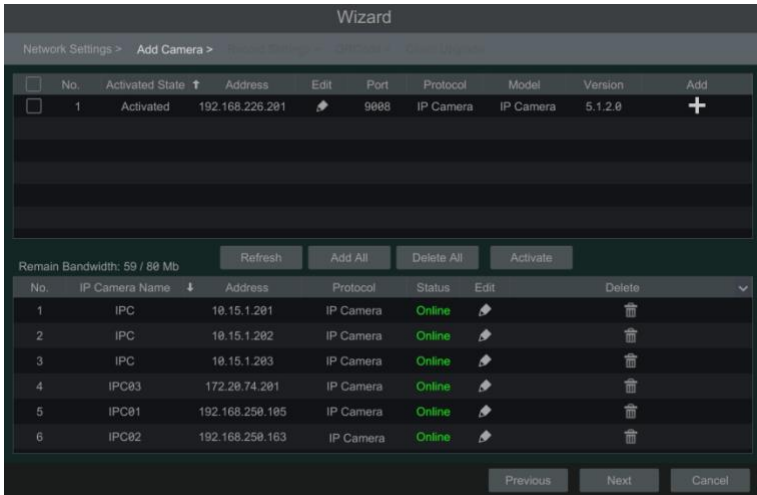
Ethernet Port 2 (Offline)

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

Port: _____

Previous Next Cancel

- ⑥ **Add Camera.** Click “Refresh” to refresh the list of online IP cameras which are in the same local network as the NVR.

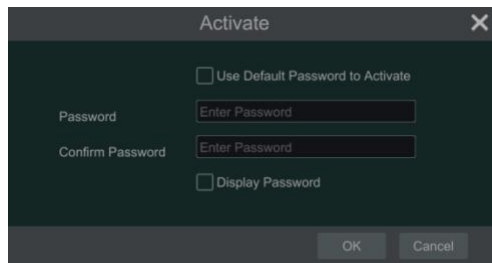


In the above interface, the device activation state can be viewed. For activated devices, you can click to add the searched camera. Click “Add All” to add all the cameras in the list.

If the default password is not used by the activated device, you will need to modify it manually.

Click to delete an added camera. Click “Delete All” to delete all the added cameras.

For un-activated devices, you can activate them one by one or in batches. Check the un-activated device, click “Activate” to bring up an activation box.



You can use the default password to activate.

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

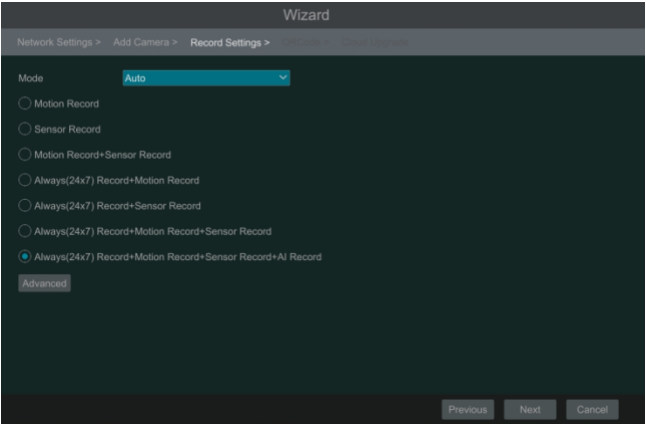
Click to edit searched IP cameras as shown on the below left. Enter a new IP address, subnet mask, gateway, username and the password for the camera. Click “OK” to save the settings.

Click  to edit added cameras as shown on the above right. Enter a new camera name, IP address, port, username, and the password for the camera. You can check “Sync to IPC” to modify the IP address of the IPC from a different network segment to match the network segment of the NVR. Then, click “Test” to test the connection. Click “OK” to save the settings. You can change the IP camera’s name only when the added camera is online. Click “Next” to continue.

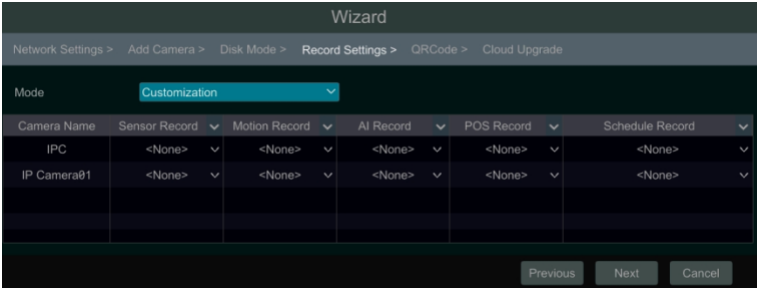
Tips: Please skip Step ⑦ and ⑧ if the NVR does not support RAID function.
THE ONLY MODEL IN THIS MANUAL THAT SUPPORTS RAID IS VT-TNR3280E1N

- 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 includes RAID0, RAID1, RAID5, RAID6 and RAID10. Global hot spares and array capacity can also be viewed here. See [7.4 Disk](#) for details. Click “Next” to continue.
- ⑨ **Record Settings.** Two recording modes are available: auto and customization.

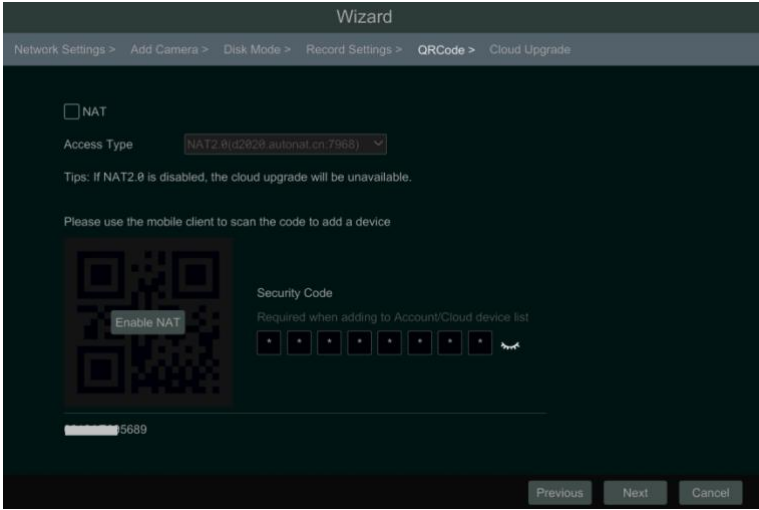
Auto: Select an auto mode option in the interface as shown below and then click “Next” to save the settings. Click “Advanced” to customize what modes the system will record with. See [7.1.1 Mode Configuration](#) for details.



Customization: Set “Sensor Record”, “Motion Record”, “AI Record”, “POS Record,” and “Schedule Record” for each camera. Click “OK” to save the settings. See [7.1.1 Mode Configuration](#) for details.



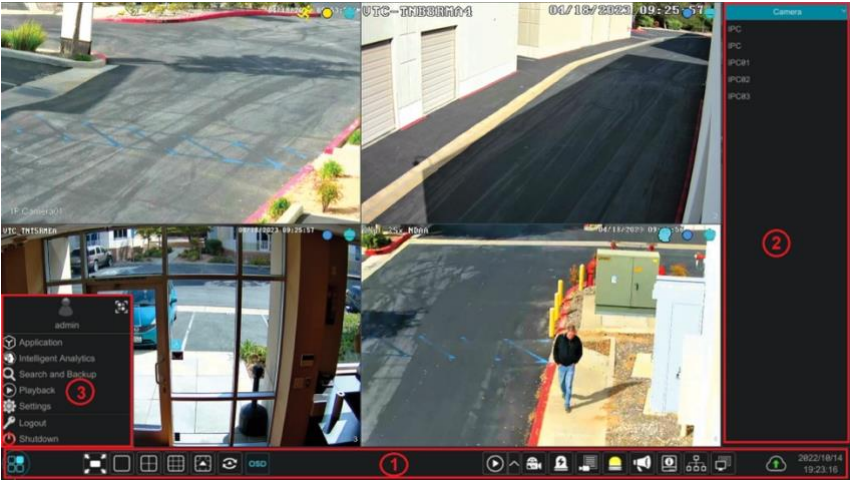
- ⑩ **QR Code.** Enable the NAT or NAT2.0 function in the interface or set it in the network configuration after exiting the wizard (please refer to [14.1.8 NAT Configuration](#) for details). You can scan the QR Code on the mobile client installed on a mobile phone or tablet PC to log in the mobile client instantly. Please refer to [15.1 Mobile Client Surveillance](#) for details. Click “OK” to save the settings.



- 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 [14.1.11 Cloud Upgrade](#) for details.

4.2 Main Interface

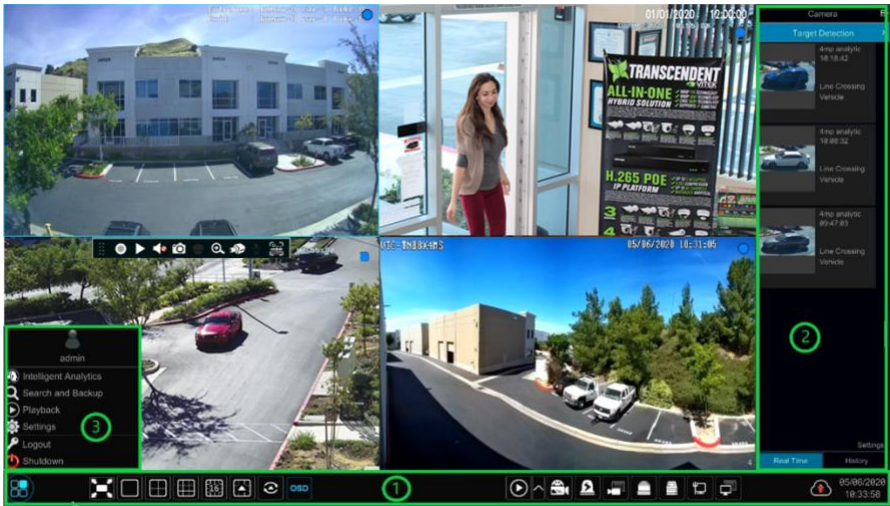
4.2.1 Main Interface Introduction



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

Button	Meaning
	Start button. Click it to pop up area ③.
	Full screen button. Click it to show full screen; click it again to exit the full screen.
	Screen mode button.
	Dwell button (see 5.2.2 Quick Sequence View and 5.2.4 Scheme View In Sequence for details).
	Click to enable OSD; click again to disable OSD.
	Click to set the default playback time before starting instant playback (8.1 Instant Playback) or going to the playback interface for playback operations (8.2 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 record from the past five minutes.
	Manual record button. Click to enable/disable manual recording.
	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.
	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 this button to enable cloud upgrade.

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 takes precedence.



Introduction of area ②:

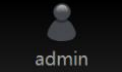
Area ② is hidden by default. Move the cursor to the right to reveal this area. Click “Camera” to view all the added cameras in the camera list. Select one camera window on the left side of the interface and then double click one camera in the list to preview the camera image in the selected window.

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 that group (refer to [4.2 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 [5.2.1 Preview by Display Mode](#) for a detailed 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 captured humans, 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.

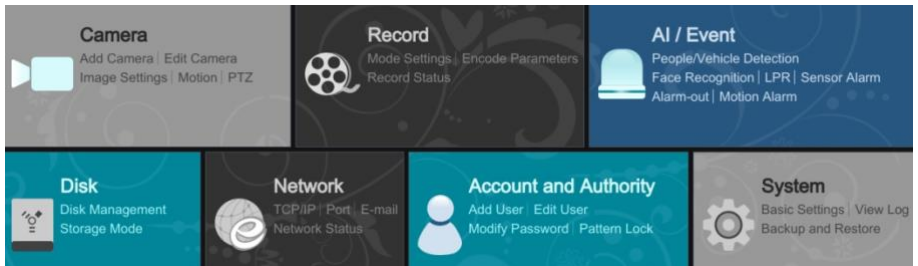
Introduction of area ③:

Icon / Button	Meaning
 	Shows the current user logged in. 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.

Icon / Button	Meaning
 Intelligent Analytics	Click to go to the intelligent analytics interface.
 Application	Click to configure parking lot management, access control, face attendance, and face check-in (depending on models)
 Search and Backup	Click to go to record search and backup interface, see 8.4 Record Search, Playback & Backup for details.
 Playback	Click to go to the playback interface (click  on the tool bar at the bottom of the live preview interface to set the default playback time), see 8.2 Playback Interface Introduction for details.
 Settings	Click to pop up the setup panel, see 3.2.2 Setup Panel for details.
 Logout	Click to log out the system.
 Shutdown	Click this button and then select “Logout”, “Reboot” or “Shutdown” in the popup window.

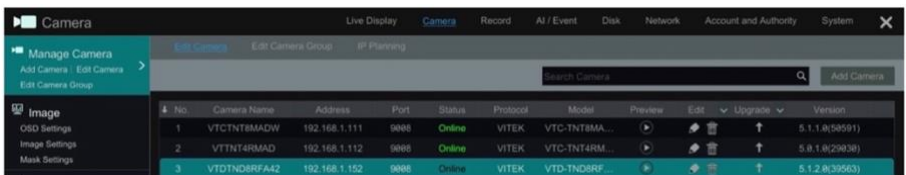
4.2.2 Setup Panel

Click Start→Settings to bring up the setup panel as shown below.



The setup panel includes seven modules. Each module provides a header for the main function with links for quickly moving to sub-menus.

Using the Camera module as an example, it provides convenient links to sub-menus such as “Add Camera”, “Edit Camera”, “Image Settings”, “Motion” and “PTZ”. Click Camera to go to the camera management interface as shown below.



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 bring up the window as shown below.



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 the "System" tag.



4.2.3 Main Functions

➤ Camera

This module covers **Camera Management** (see [Chapter 4 Camera Management](#) for details), **Image Settings** (see [5.4 Preview Image Configuration](#) for details), **Motion** (see [11.2 Motion Alarm](#) for details), and **PTZ** (see [Chapter 6 PTZ](#) for details.)

➤ Record

This module covers **Encode Parameters** and **Record Schedule**. Please see [Chapter 7 Record & Disk Management](#) for details.

➤ AI/Event

This module covers **Smart Event**, **Combination Alarm**, **Exception**, **Sensor and Motion Alarm Handling**, and **Alarm Out Settings**. Please see [Chapter 9 AI Event Management](#) and [Chapter 11 General Event Management](#) for details.

➤ Disk

This module covers **Disk Management**, **Storage Mode**, and **Disk Information**. Please see [Chapter 7 Record & Disk Management](#) for details.

➤ Network

This module covers **TCP/IP**, **DDNS**, **Port**, **E-mail**, **Network Status**, and so on. Please see [14.1 Network Configuration](#) for details.

➤ **Account and Authority**

This module covers **Account Management** (see [13.1 Account Management](#) for details), **Permission Management** (see [13.3 Permission Management](#) for details), and so on.

➤ **System**

This module covers **Basic Configuration** (see [14.2 Basic Configuration](#) for details), **Device Information** (see [14.8 View System Information](#) for details), **Log Information** (see [14.7 View Log](#) for details), **Configuration File Import & Export** (see [14.5 Backup and Restore](#) for details), and so on.

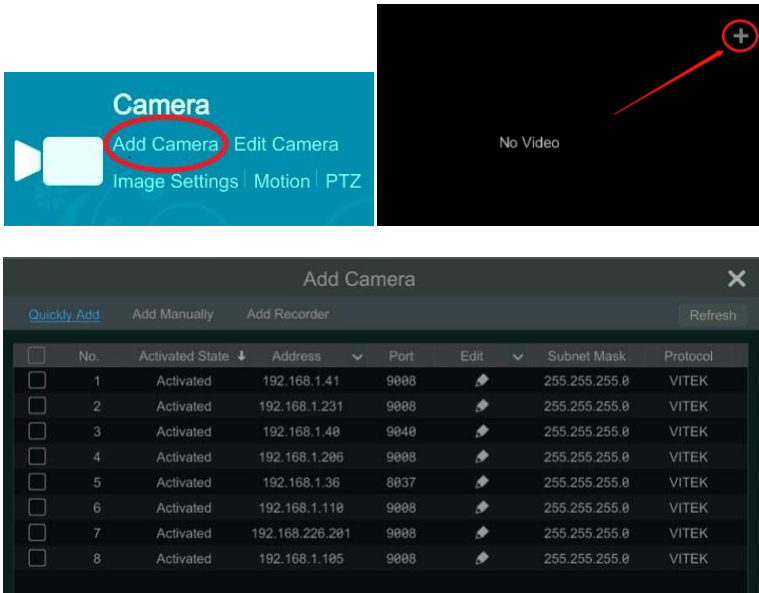
5 Camera Management

5.1 Add/Edit Camera

5.1.1 Add Camera

The network of the NVR should be set up before adding IP camera (see [14.1.1 TCP/IP Configuration](#) for details).

Refer to the pictures below. Click **Add Camera** in the setup panel or  in the top right corner of a preview window to bring up the “Add Camera” window as shown below. You can **quickly add** or **add manually** IP cameras.



➤ Quickly Add

Check the cameras you want to add and then click “Add” to add them. Click  to edit the camera’s IP address, username, and password and. 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

Default Password Add Cancel

➤ Add Manually

Enter the IP address or domain name (click in the IP address column to bring up the domain name input window, enter the domain name of the IPC in the window and then click “OK”), port, username, and password of the camera and then select the protocol. Click “Test” and then click the “Add” button (you can input a camera’s information such as IP address, username, and password before clicking the “Add” button). Click to delete a camera. Click “Default Password” to set the default username and password of each camera.

➤ Add Recorder

Add Camera ✕

Quickly Add Add Manually Add Recorder Refresh

No.	Device Name	Address	Port	Edit	Model	Serial No.
1	Vitek DVR	192.168.1.150	8019		VT-TR5HA...	1C:7C:45:10:79:33
2	Device Name	192.168.1.20	8021		VT-TR8NH...	1C:7C:45:16:B8:72
3	Device Name	192.168.1.38	9038		VT-TNR41...	1C:7C:45:13:C6:5D
4	Device Name	192.168.1.33	6036		VT-TNR41...	1C:7C:45:13:C6:53
5	Device Name	192.168.1.35	6036		VT-TNR81...	1C:7C:45:16:6E:6B
6	Device Name	192.168.1.37	6036		VT-TNR81...	1C:7C:45:13:35:23
7	My_TNR1616F	192.168.1.39	3660		VT-TNR16...	1C:7C:45:10:D9:92

Remain Bandwidth: 144 / 160 Mb

Default Password Manual Add Add Cancel

- Quickly Add: Select an NVR/DVR from the list of detected recorders on the local

network and click “Add” to add it.

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

Add Recorder Channel ✕

Address: ☐ Domain Name

Server Port: Channels:

Username: Password:

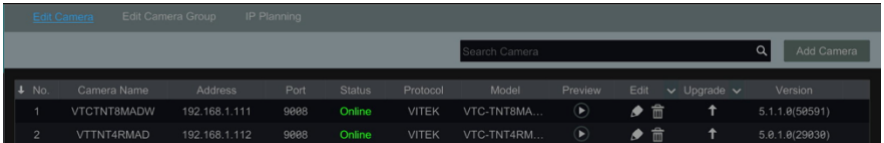
☐	Remote Channel No.	Camera Name	Model
☐	1	IP Camera	VT-TNR414PN
☐	2	IPCamera2	VT-TNR414PN
☐	3	IPCamera1	VT-TNR414PN
☐	4	det	VT-TNR414PN

Selected: 0 / 4 Test OK Cancel

Note: IP cameras from an NVR on the local network may only be added when the local NVR has unoccupied channels. The added IP cameras support previewing and recording.

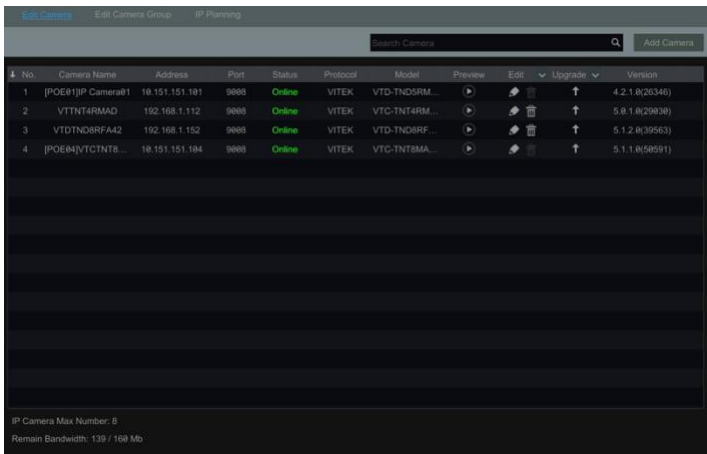
5.1.2 Edit Camera

Click “Edit Camera” in the setup panel to go to the interface shown below. Click to view the live image of that camera in a pop-up window. Click to edit the camera (see **Add camera** in [3.1 Startup Wizard](#) for details). Click to delete the camera. Click in the “Edit” header line and then click “Modify IPC Password” to bring up a window(check the cameras in the window, set a new password and then click “OK”; only online camera passwords can be modified. A batch of camera passwords can be modified at the same time). Click to upgrade an online camera (or click in the “Upgrade” header line and then click “IPC Batch Upgrade” to upgrade a batch of cameras), select the USB device where the upgrade file is stored in the “Device Name” section of the pop-up window and then choose the upgrade file in the list and then click “Upgrade” to start upgrading(the camera will restart automatically after the upgrade is completed successfully).



1. Note:

If you use an NVR with PoE network ports, 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 IP camera which occupies the PoE resource has a prefix shown before its camera name. The prefix consists of PoE plus PoE port number. IP cameras connected to PoE ports cannot be deleted from the camera list manually.



- IP cameras directly connected to the PoE port of the NVR through private protocol will be shown automatically in the camera list.
- One of two conditions must be met for a directly connected IP camera, using ONVIF protocol, to be shown automatically in the camera list.
- ✓ An IP camera directly connected to the PoE port on the NVR must be in same network segment as the internal Ethernet port.
- ✓ DHCP (obtain an IP address automatically) must be enabled on the ONVIF IP camera directly connected to the PoE port of the NVR.

If an IP camera connected to the PoE port is not displayed automatically in the camera list, please refer to Q6 in [Appendix A FAQ](#) for details.

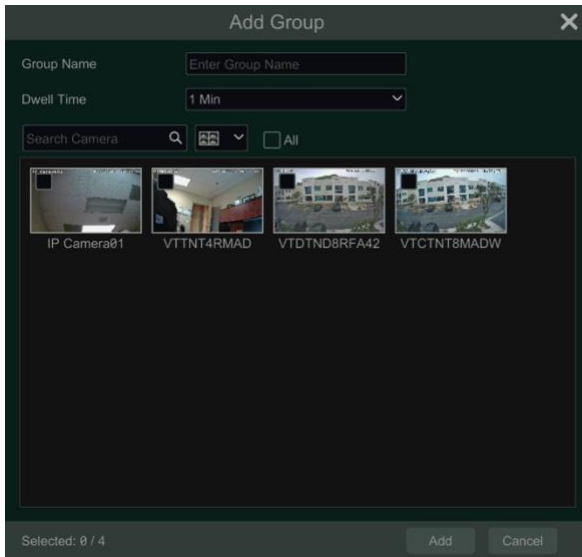
5.2 Add/Edit Camera Group

5.2.1 Add Camera Group

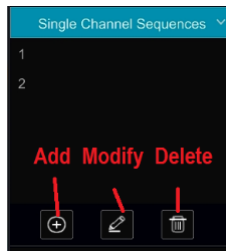
Click "Edit Camera Group" in the above interface to go to the interface shown below.



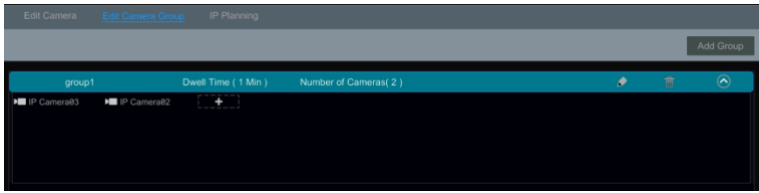
Click “Add Group” to bring up the window shown below. Set a group name and dwell time (the time that a camera group sequence view will dwell on screen) in the window. Check the cameras and then click “Add” to create a group. Click  to view the cameras in the group after adding a group.



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



5.2.2 Edit Camera Group



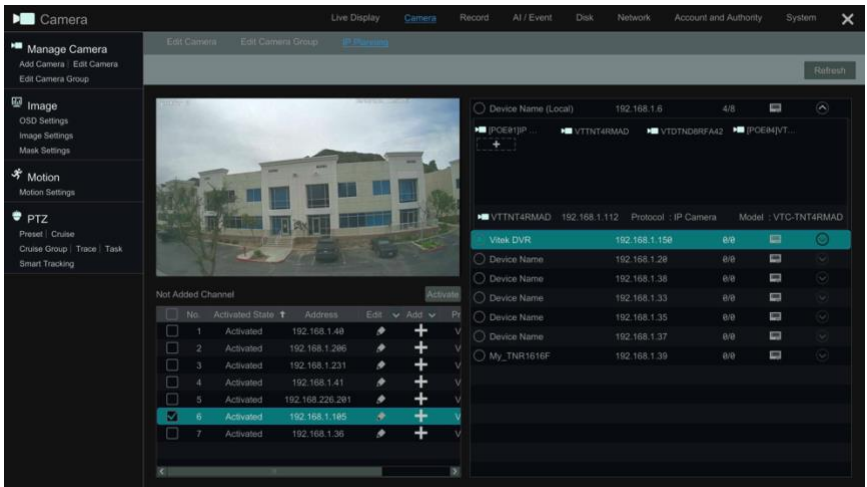
Click  to modify the group information such as group name and dwell time. Click  to delete the group. Click  to add cameras to the group.

5.2.3 IP Planning

Some models may not support this function.

Click “IP Planning” to go to the interface shown below. This function supports searching other NVRs/DVRs on the same local network as the NVR. You can add cameras from other NVRs/DVRs into the unoccupied channels of the local NVR.

For searched channels, if it is “unactivated”, you can activate it first and then add it.



Click  to edit the IP address, user name/password, and the NVR's other information.

Click  behind the “Add” button to add the selected camera. You can edit the IP address, user name, or password by clicking  behind the “Edit” button.

6 Live View Introduction

6.1 Live View Interface Introduction

First, you must add a camera after logging in to the system (see [4.1.1 Add Camera](#) for details). Refer to the interface shown below, drag one camera in the preview window to another window to swap cameras between windows. Click the **OSD** button to display recording symbols. The recording symbol colors in the live preview window refers to different recording types when recording: green stands for manual recording, red stands for sensor based recording, yellow stands for motion based recording, blue stands for schedule recording, and cyan stands for AI Event recording.

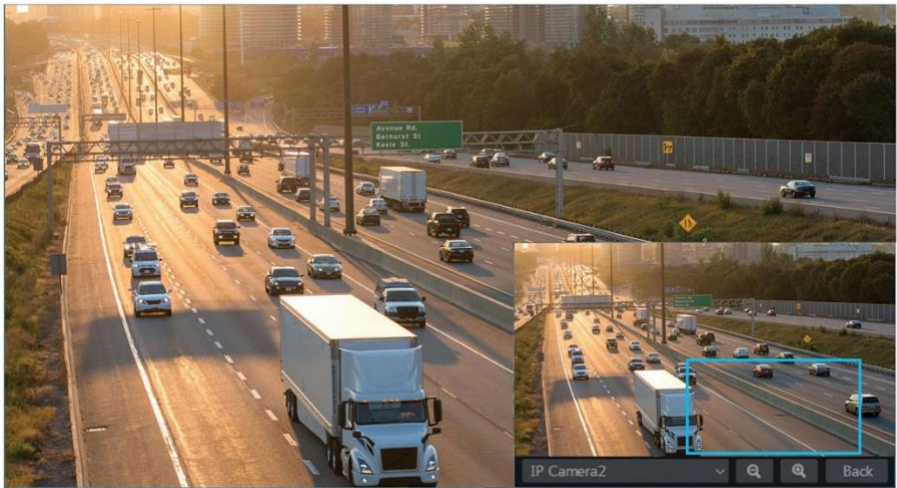


Click the preview window to show the tool bar as shown in area ①; right click the preview window to bring up the menu list. The tool bar and menu list are introduced in the table below.

Button	Menu List	Meaning
	--	Move tool. Click it to move the tool bar anywhere.
	Manually Record On	Click to start recording manually in highest possible quality.
	Instant Playback	Click  to playback the recording; click "Instant Playback" to select or self-define the instant playback time. See 8.1 Instant Playback for details.
	Enable Audio	Click to enable audio. You can listen to the camera's live audio by enabling audio.
--	Original Proportions/ Overspread window	Click it to select the display proportion of the window.

Button	Menu List	Meaning
	Snapshot	Click to bring up the snapshot window. Click “Save” in the window to save an image. Click “Export” to export an image.
	PTZ Control	Click to go to the PTZ control interface. See Chapter 6 PTZ for details.
	Zoom In	Click to go to the single channel Zoom interface.
	--	Click to go to the image adjustment interface. Refer to 5.4.5 Image Adjustment for details.
	Start/Close Talk	Click to start two-way-talk.
	Target detection	Click to go to the single channel target detection interface; targets include faces, human bodies, and vehicles. (Only applicable on some models)
--	Camera Info	Click to view camera information.

The single channel Zoom interface is shown below. Press and drag the blue box to select the zoom area. Click  /  to zoom into/out of the image. Click the camera selection box to select other cameras to zoom in on. Click “Back” to return to the live preview interface.



6.2 View Mode

6.2.1 Preview by Display Mode

You can set different screen modes and cameras display sequences as desired and save display modes classified by surveillance areas, priorities etc. Refer to the picture below. Double click a display mode in the display mode list to view the cameras in that mode.



➤ Add Display Mode

1. Method One:

- ① Click “Customized Display Modes” in the above interface.
- ② Click  to add a display mode name and then set the screen mode.
- ③ Add cameras and adjust the cameras’ display sequence as required.
- ④ Click  under the display mode list.

2. Method Two:

- ① Click Start→Settings→System→Basic→Output Settings to go to the interface and configure a 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 [5.2.4 Scheme View In Sequence](#) for detailed configuration info). The display mode will be saved and displayed in the display mode list in the live preview interface.

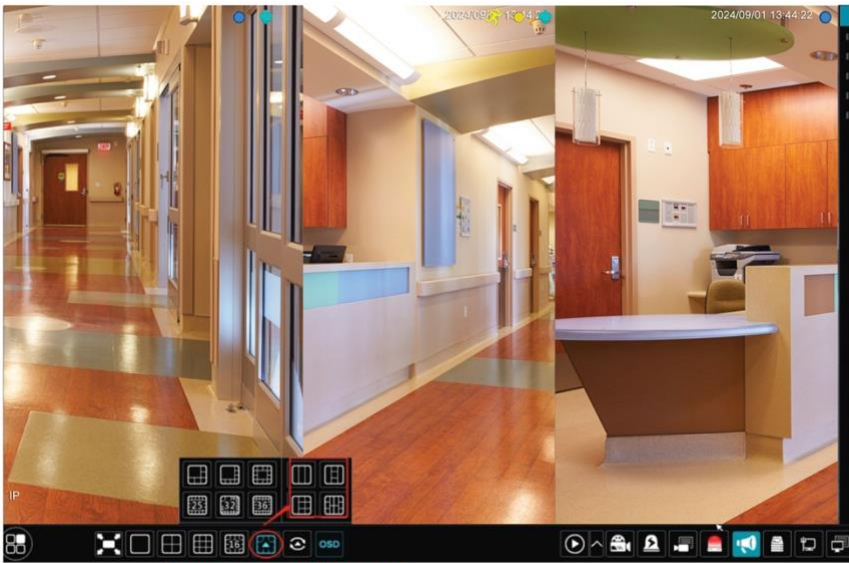
➤ Edit Display Mode

Click “Customize Display Modes” tab in the live preview 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 orientation of the video image by using this function in order to view more vertical space. Please refer to the User Manual of the relevant camera.



Change to corridor mode

➤ Fisheye Mode

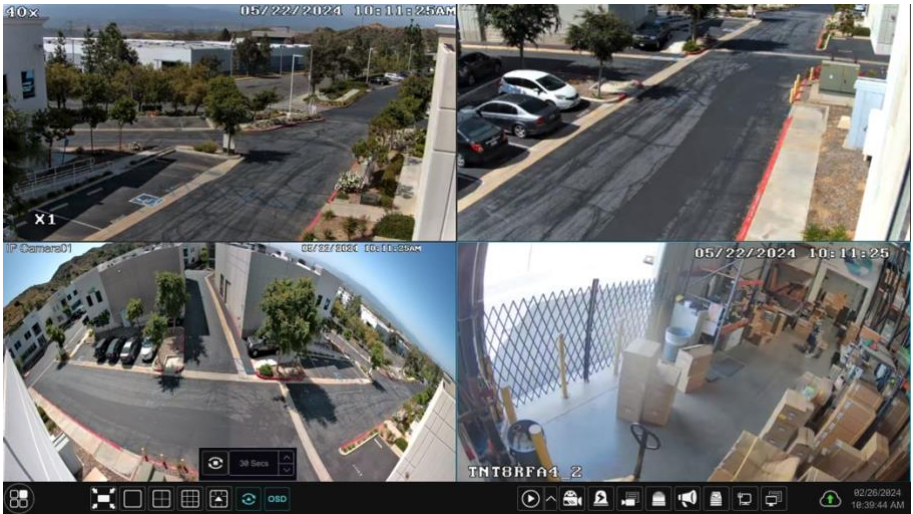
Some models may not support this function. While on the live preview interface, select a view mode corresponding to the installation and display mode of the fisheye camera. Please refer to the camera's User Manual for more details.



In addition, if this function is unavailable for this device, you can set the display mode and the installation mode via the Web Client. To log in to the web client, please refer to Chapter 14 for details.

6.2.2 Quick Sequence View

You cannot start a quick sequence view if a scheme has not been configured. If a scheme has been configured, please refer to [5.2.4 Scheme View in Sequence](#) for details.



Go to the live preview interface and then click to bring up a menu. 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.

6.2.3 Camera Group View in Sequence

You can start the camera group view in sequence if a camera group has been created (see [4.2.1 Add Camera Group](#) for details).

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



Double click one camera group on the right side of the interface. The cameras in the group will start rotating through camera group views 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.

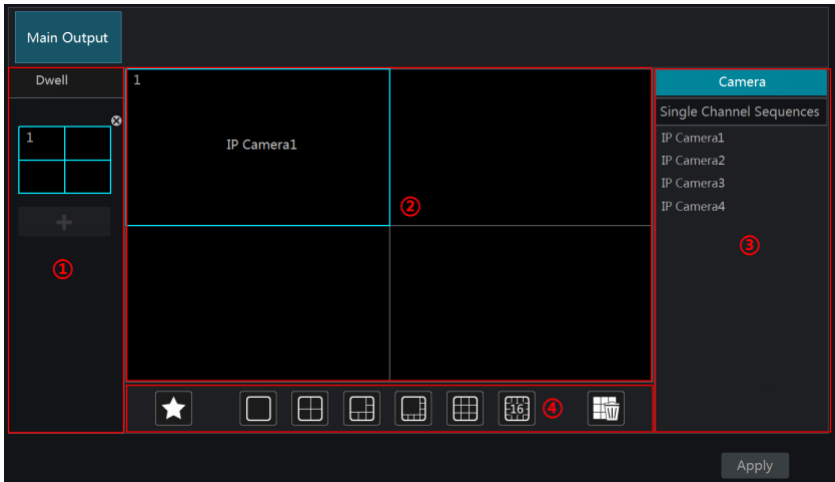
Click  to add a camera group. Select a group and click  to modify the group name and dwell time; Select a group and click  to delete the group.

6.2.4 Scheme View in Sequence

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

Area ① displays all the dwell schemes; area ② shows detailed information of the scheme.

Area ③ displays all the cameras and groups. Area ④ is the tool bar (: clear button; : favorite button, click it to bring up 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 in the top right corner of the scheme to delete it.

➤ **Configure Scheme**

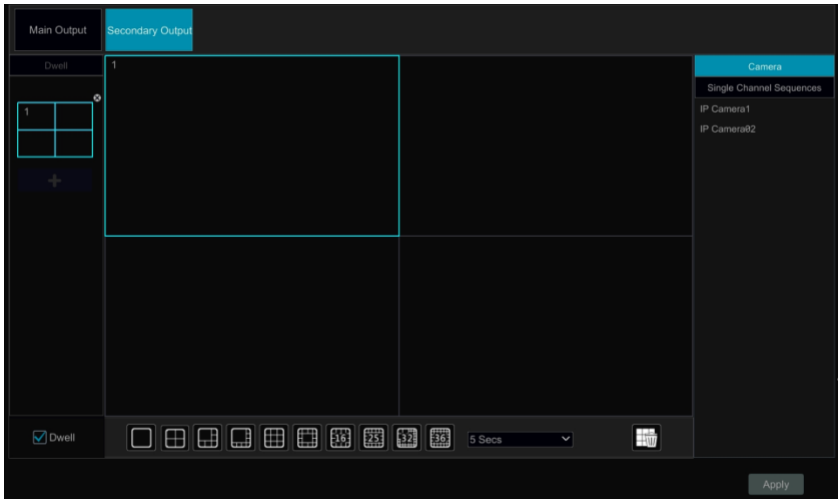
- a) Select a scheme in area ① and then click the screen mode button on the tool bar to set a screen mode for the scheme.
- b) Select a camera window in area ② and then double click the camera or group in area ③. The camera or group will be added into the selected window. One camera in the same scheme cannot repeat. You can right-click to make the “Clear” button appear in the camera window 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 preview interface and then click to bring up a window. Set the dwell time in the window and then click to start a 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.

1. **Note:**

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

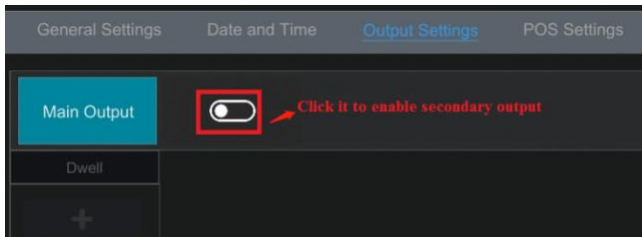


Check “Dwell” and then set the scheme view in sequence on the secondary output. The setting steps are similar to that of the main output.

Set a quick sequence view if “Dwell” is not checked. The steps to set this up 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.

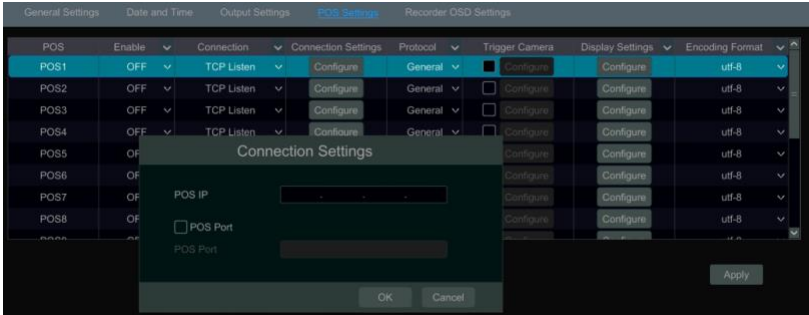
For devices with multi-output mode and AI mode, the secondary output will be unavailable when AI mode is enabled. If you want to enable a secondary output, please click Start→System→Output Settings.



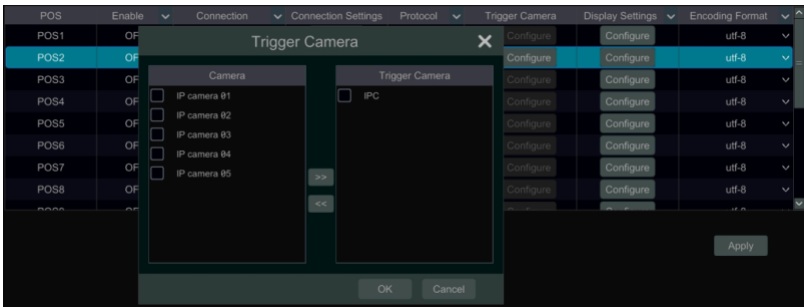
6.3 POS Settings

- ① Click Start→Settings→Basic→POS Settings to go to the POS interface.
- ② Enable POS and click “Configure” under “Connection Settings” to go to the following interface. The connections include TCP Listen, TCP Client, UDP, and Multicast.
- ③ Enter the IP address of the POS you want to add.

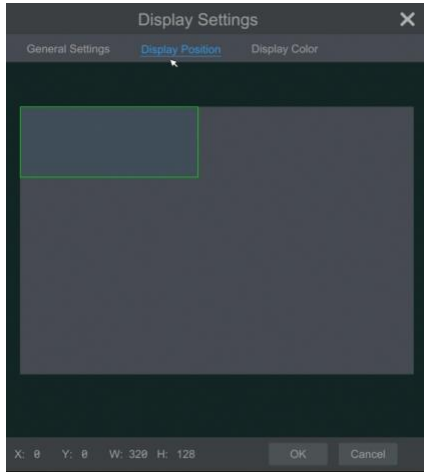
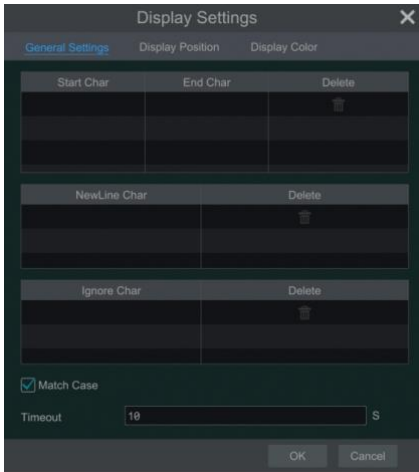
- ④ Check the “POS port” of your device and then enter it.



- ⑤ Select the POS protocol.
- ⑥ Check “Trigger Camera” and click “Configure” under it to bind the POS to that camera. One POS can be bound to multiple channels, but only one channel can be bound to one POS.



- 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.

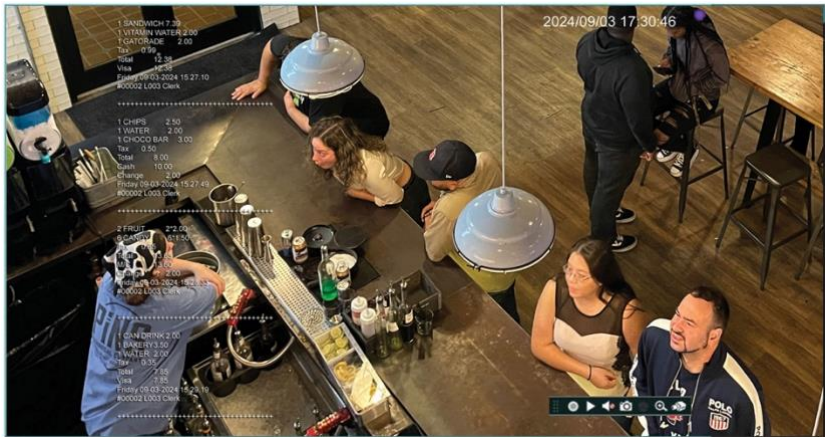


Click the “Display Color” tag and then choose the color you want to display on the screen. Multiple colors can be selected at the same time. In addition, the print method and preview display can be set here. If “Preview Display” is enabled, the POS contents will be displayed on the live view/playback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

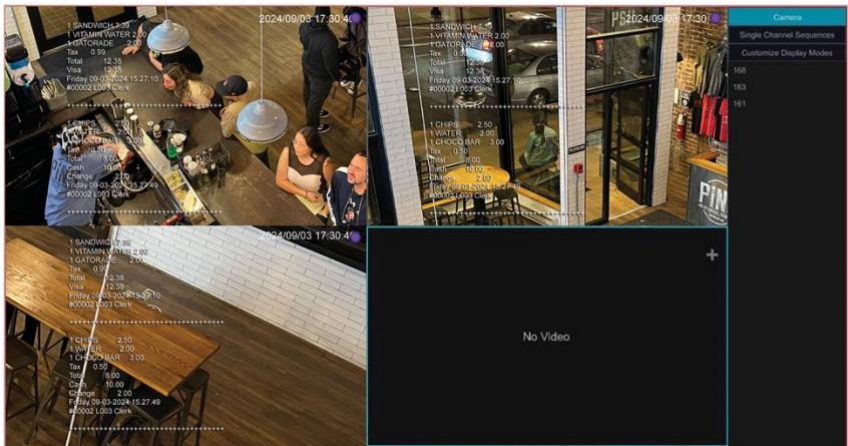


- ⑧ Select an encoding format as needed.
- ⑨ Choose the manufacturer of the POS device.
- ⑩ Click “Apply” to save the settings and then the transaction information will be displayed on the preview image in real-time.

One POS bound to one camera:



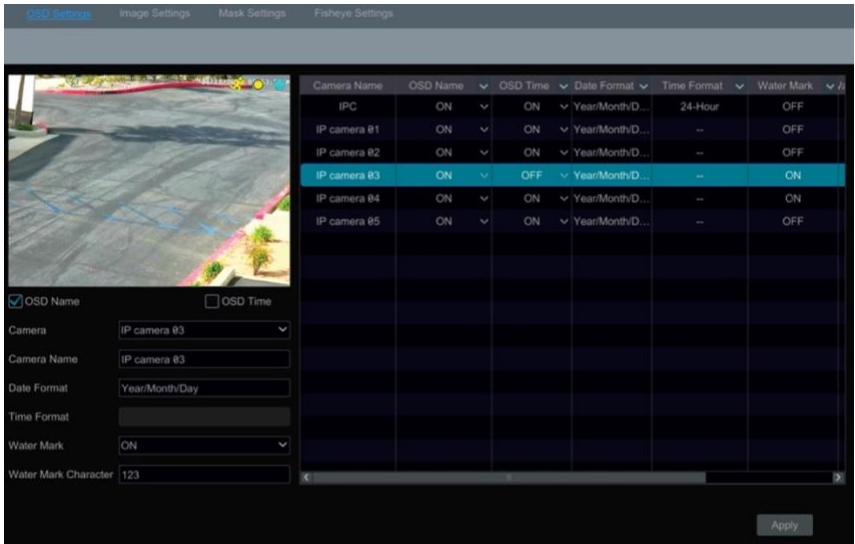
One POS bound to multiple cameras:



6.4 Preview Image Configuration

6.4.1 OSD Settings

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

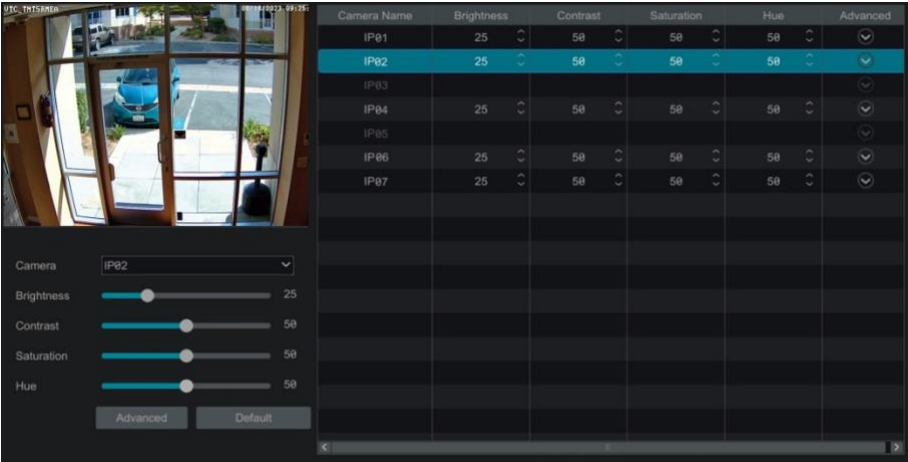


Select a camera, enter a camera name (or double click the camera name in the camera list to change the camera name), enable or disable the name and time displays (if enabled, drag the red name and time displays directly in the image view area to change the OSD's display position) and select the date and time format (24h or 12h). Additionally, the water mark function can be enabled or disabled here. If you have enabled the water mark function, you can enter the information for a water mark as needed. Finally, click "Apply" to save the settings.

6.4.2 Image Settings

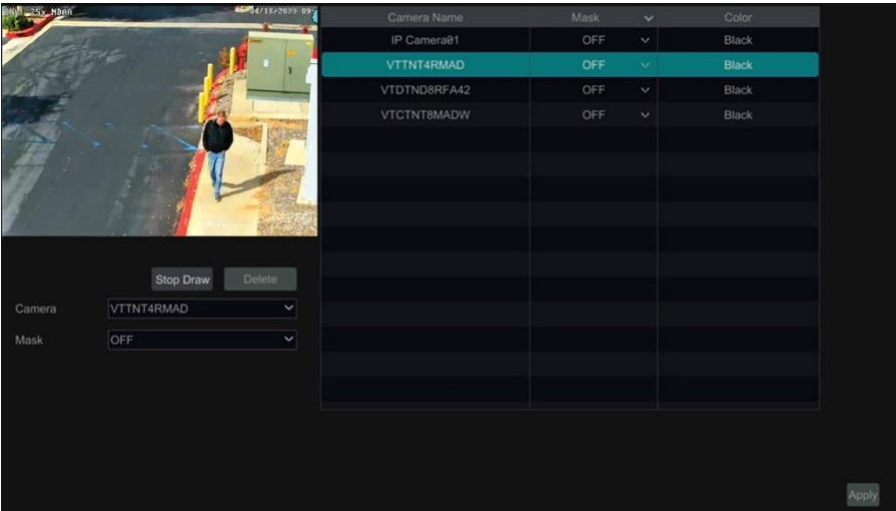
Click Start→Settings→Camera→Image→Image Settings to go to the following interface. Select a camera and then set the brightness, contrast, saturation, and hue of the camera. Click the "Advanced" button or  in the camera list on the right side of the interface to bring up the "Image Adjust" interface and then configure the relevant settings. Please refer to [5.4.5 Image Adjustment](#) for detailed explanations of these items.

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



6.4.3 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 below.

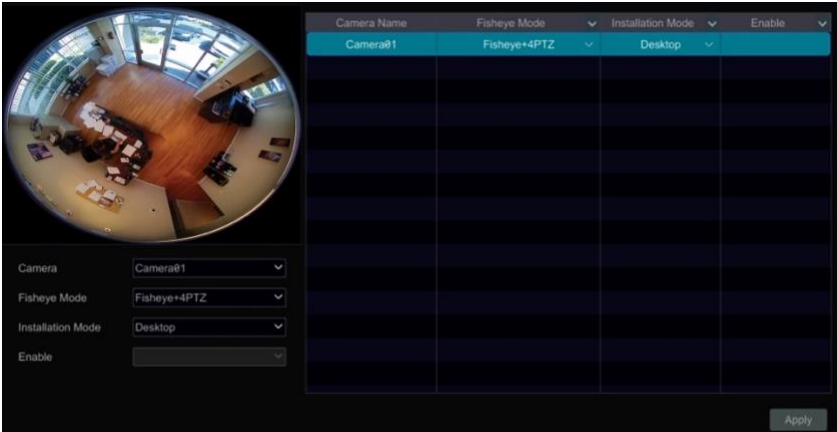


Select a camera and enable a mask. Click the “Draw” button and then drag the mouse on the image area to set a mask area; click the “Delete” button to delete mask areas; click “Apply” to save the settings.

6.4.4 Fisheye Settings

Some models may not support this function.

Click Start→Settings→Camera→Image→Fisheye Settings to go to the interface below. Select a camera and a mode for the fisheye as well as the installation style.



6.4.5 Image Adjustment

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



➤ Image Adjustment

Select a camera and then click “Image Adjustment” to go to the image adjustment tab. Refer to the above picture. Drag the slider to set the camera's brightness, contrast, saturation, and hue value. Check sharpen, wide dynamic, or denoise and drag the slider to set the values. Click “Default” to set these parameters to default values. The details of these parameters are as follows:

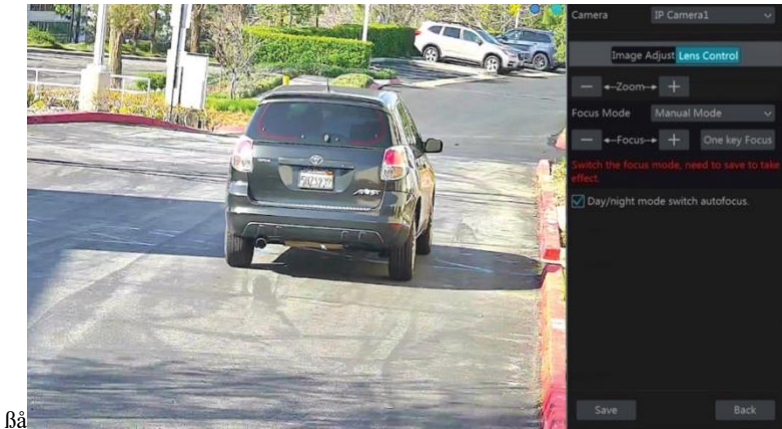
Parameter	Meaning
Brightness	The brightness level of the camera's image.

Parameter	Meaning
Contrast	The color difference between the brightest and darkest parts.
Saturation	The degree of color purity. The color is purer, the image is brighter.
Hue	Color temperature of the image
Sharpness	Resolution level of the image plane and the sharpness level of the image edge.
Wide Dynamic	Wide Dynamic Range (WDR) function helps the camera provide clear images even under backlight 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 heighten the noise reduction effect but 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 objects in the darkest area will be seen more clearly.
Corridor Pattern	Rotate camera image 0°, 90°, 180° or 270° for corridor areas. (Only some cameras support this function)
Image Mirror	Turn the current video image horizontally.
Image Flip	Turn the current video image vertically.
High FPS Mode	High frame rate mode, if enabled, the frame rate of a 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 is 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).

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

➤ Lens Control

Select a 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.



The details of these parameters and buttons are as follows.

Button/Parameter	Meaning
	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.
	Click / to increase/decrease the focal length.
	Click it to focus instantly.
Day/night mode switch autofocus	If checked, the lens will focus automatically when the camera is switching between day/night mode.
Time Interval	The time interval before a camera’s lens auto-focuses. The interval can be set in the drop-down list.

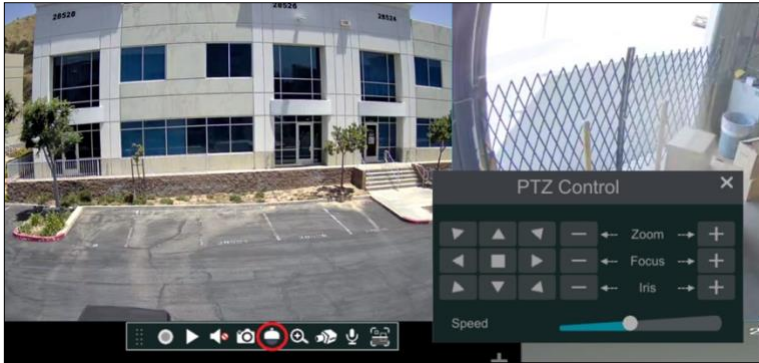
Note: if the a camera has a fixed lens, the lens control function is unavailable.

7 PTZ

7.1 PTZ Control Interface Introduction

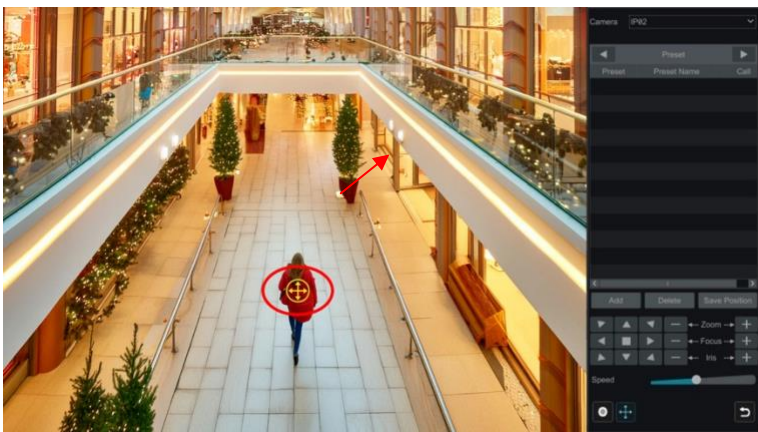
You can control the pan, tilt, and zoom of a PTZ camera and the zoom and focus of a motorized varifocal lens camera.

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

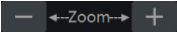
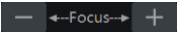
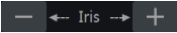
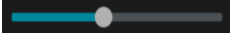


The direction, zoom, focus, iris, and speed can be controlled in the small PTZ control window.

Right click the PTZ/speed dome camera window and select “PTZ Control” to go to the PTZ control panel as shown below.



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

Button	Meaning
	Click  /  /  /  /  /  /  /  to rotate a PTZ camera. Click  to stop rotating the dome.
	Click  /  to zoom in / out on the camera image.
	Click  /  to increase / decrease the focal length.
	Click  /  to increase / decrease the iris of the dome.
	Drag the slider to adjust the rotating speed of a PTZ camera.
	Click  /  to start / stop recording.
	Click  /  to hide / show an analog joystick.
	Click to return to the live preview interface.

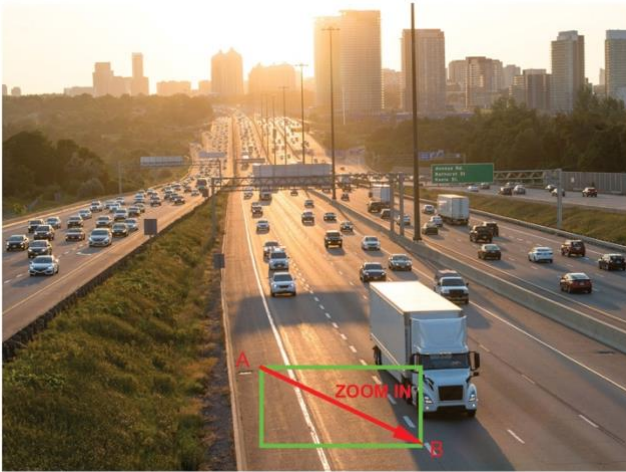
➤ Analog Joystick Control

The analog joystick on the left side of the interface provides quick PTZ control. The 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 PTZ will rotate. The dome or PTZ will stop rotating when you stop dragging the analog joystick.

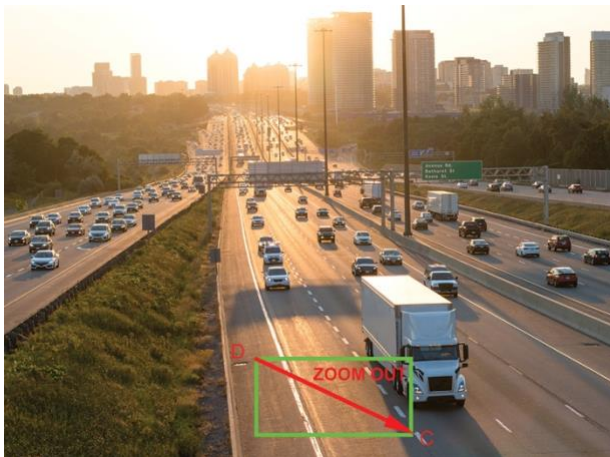
➤ 3D Control

Click anywhere on a camera image and the image will center on the clicked point.

Refer to the picture shown below. Drag the mouse from A to B to draw a green rectangle and it will zoom in on the selected area.



Refer to the picture shown below. Drag the mouse from C to D to draw a green rectangle and it will zoom out from the selected area.



➤ Advanced 3D Control

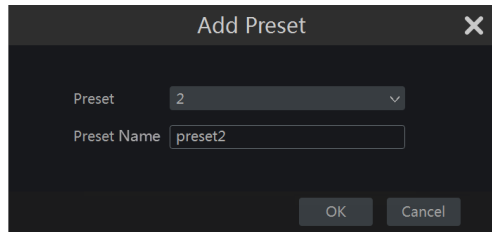
Double click the left button of the mouse on any area of the camera image and the image size will be doubled and centered on the clicked point.

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

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

➤ Preset Settings

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

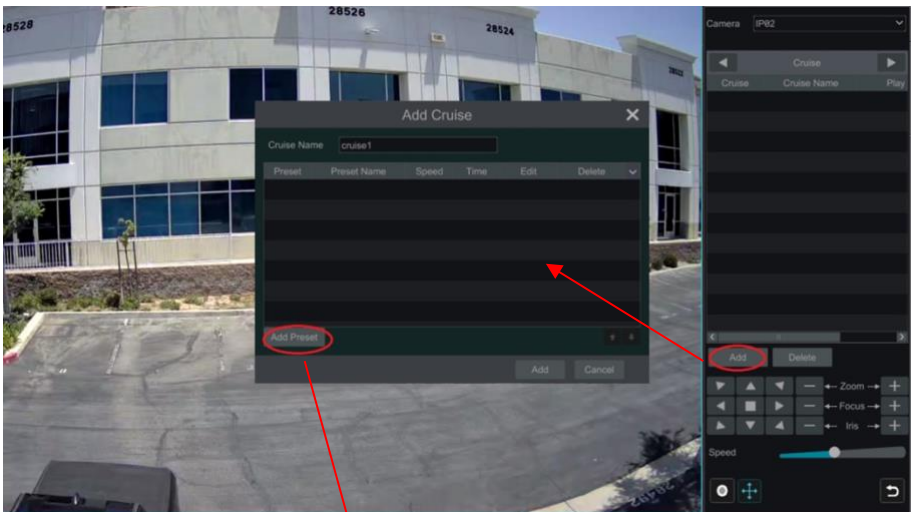


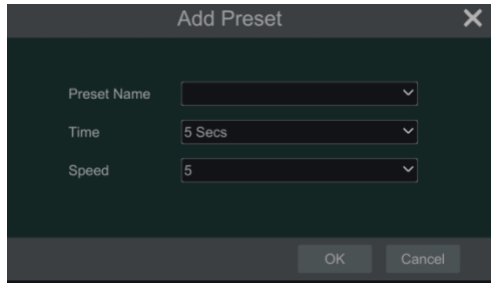
Adjust the PTZ's direction and click “Save Position” to save the current preset position (you can also click another preset in the preset list and then save the preset position after adjusting the dome's direction); click  in the preset list to call a preset; click “Delete” to delete the selected preset.

You can also go to the preset setting interface for setting presets, see [6.2 Preset Setting](#) for details.

➤ Cruise Settings

On the right panel, click  to go to the cruise operation tab and click “Add” to open the window shown to the left in the below image. You can add up to 8 cruise configurations for each PTZ.





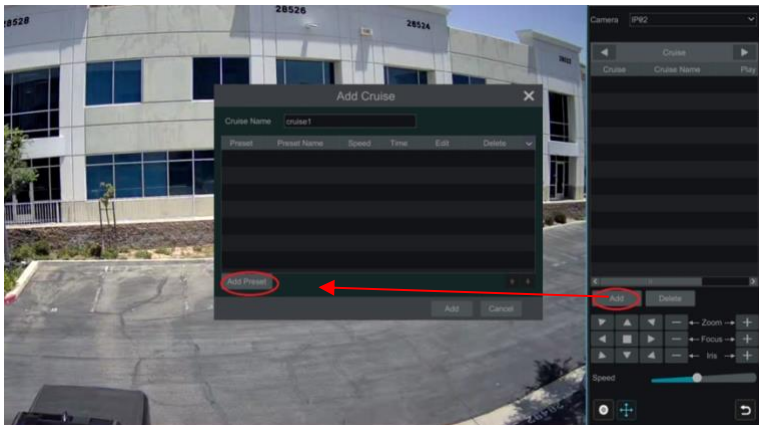
- ① Enter a cruise name in the “Add Cruise” window and then click “Add preset” to bring up the “Add Preset” window (Before adding presets to the cruise, please create presets for the PTZ first).
- ② In the “Add Preset” window, select a preset name, preset time, and preset speed and click “OK”.
- ③ In the “Add Cruise” window, you can click  to reselect a preset, then change the preset time and speed. Click  to delete a preset. Click “Add” to save the cruise.

Click  to start the cruise and click  to stop the cruise in the cruise list on the cruise operation tab; click “Delete” to delete the selected cruise.

You can also go to the cruise setting interface for setting up cruises, see [6.3 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.

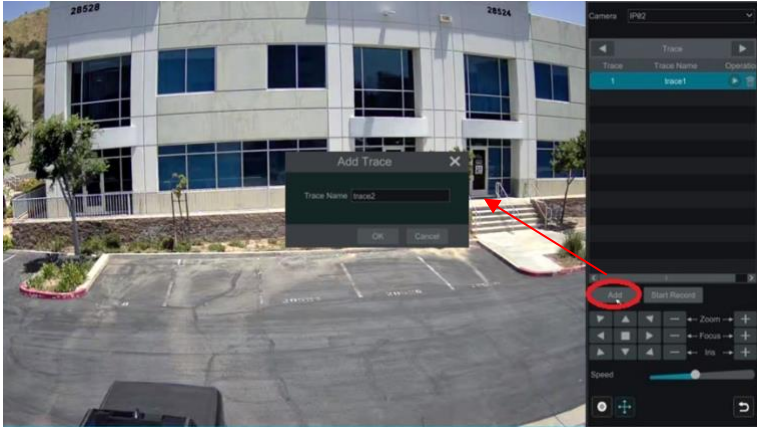


In the “Add Cruise” window, select a cruise line name. Then click “Play” to play

the cruise lines in sequence.

➤ Trace Settings

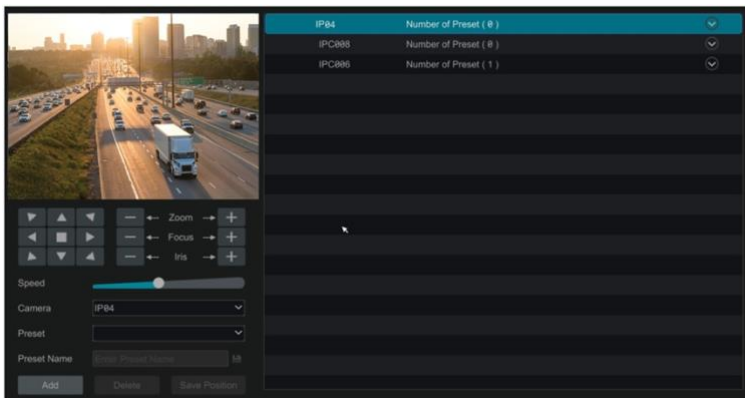
On the right panel, click  to go to the trace setting tab. Click “Add” to add a trace name. Then click “OK” to save this name. Please refer to the following picture.



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.

7.2 Preset Settings

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



➤ Add preset

Select a camera and then click “Add” to add a preset; or click  in the camera list on the right side of the interface to display the preset information of the PTZ and then click  to add a preset. The operations of the “Add Preset” window are similar to that of the PTZ control interface; please see [6.1 PTZ Control Interface Introduction](#) for details.

➤ Edit preset

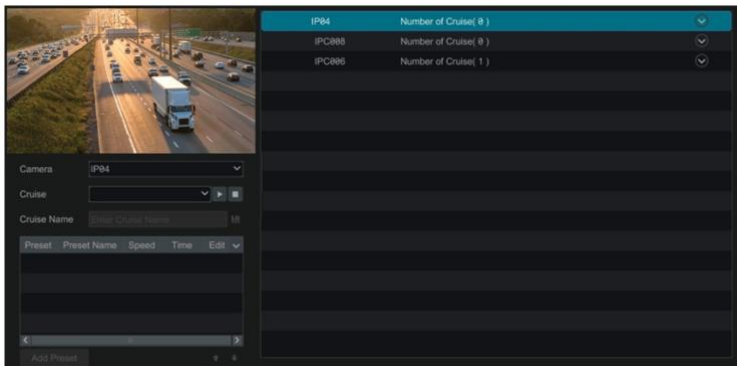
Select a camera and a preset. You can enter a new name for the preset and then click  to save the new preset name. Adjust the rotating speed, position, zoom, focus, and iris of the preset and then click “Save Position” to save the preset.

➤ Delete Preset

Select camera and preset and then click “Delete” to delete that preset.

7.3 Cruise Settings

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



➤ Add Cruise

Click  in the camera list on the right side of the interface to display the cruise information of a PTZ and then click  to add a cruise. The operations of the “Add Cruise” window are similar to that of the PTZ control interface; please see [6.1 PTZ Control Interface Introduction](#) for details.

➤ Edit Cruise

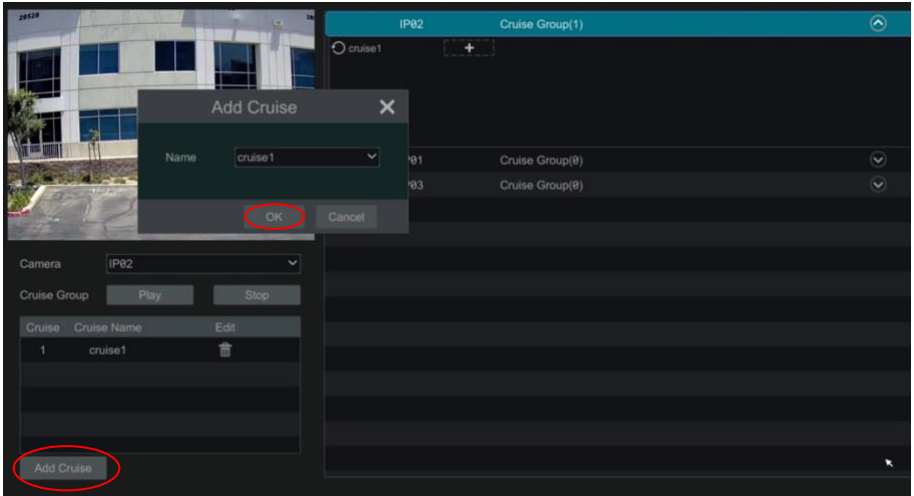
Select a camera and cruise in the “Cruise” interface. Enter a new cruise name and then click  to save the cruise name. Click “Add Preset” to add a preset to the cruise. Click  to edit that preset. Click  to delete the preset from the cruise. Click one preset in the preset list and then click  to move the preset down the list  to move the preset up the list. 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 cruise information for a PTZ and then click  on the top right corner of the cruise to delete the cruise.

7.4 Cruise Group Settings

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



➤ Add Cruise Group

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

➤ Delete Cruise

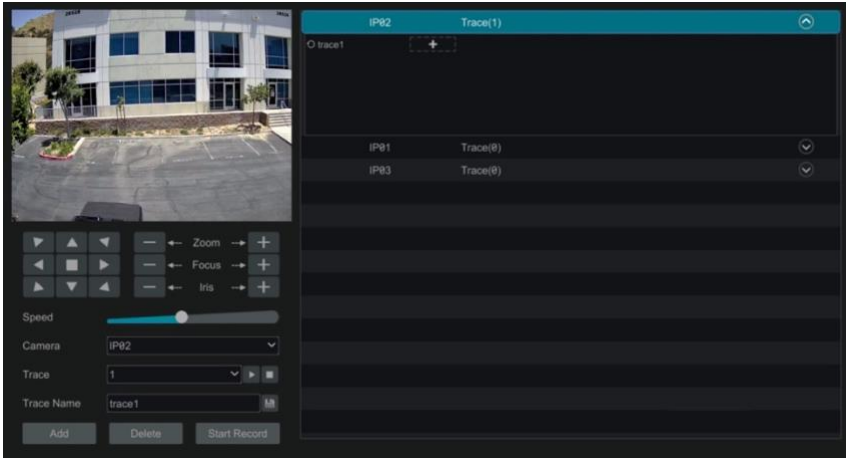
In the cruise list, click  to delete a cruise.

7.5 Trace Settings

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

➤ Trace Record

Select a PTZ camera and then click “Add” or extend the camera 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.



➤ Play or Stop Trace

Select a trace and click  to play that trace; click  to stop that trace.

➤ Modify the Trace Name

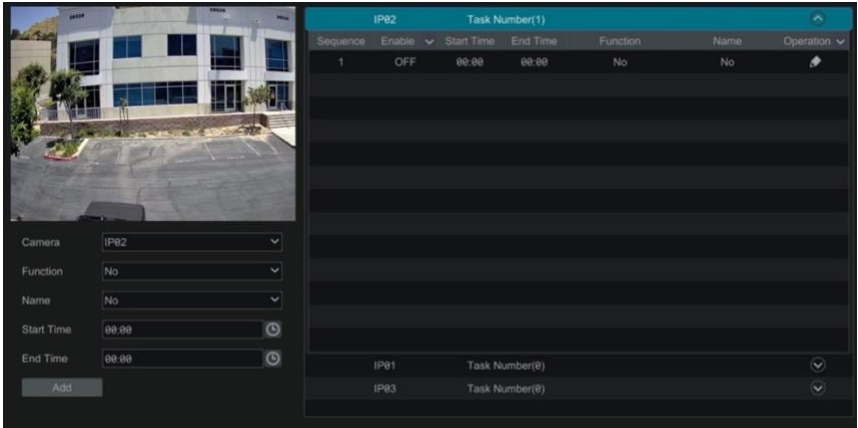
On the left panel, enter a new trace name and click  to modify and save that trace name.

➤ Delete the Trace

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

7.6 Task Settings

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



- ① Select a PTZ camera.
- ② Select a function, such as preset, cruise, trace, random scanning, etc.
- ③ Select a name, such as preset name, cruise name, etc.
- ④ Select a start and end time.
- ⑤ Click “Add” to add the task.
- ⑥ Click  to extend the tasks of a 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.

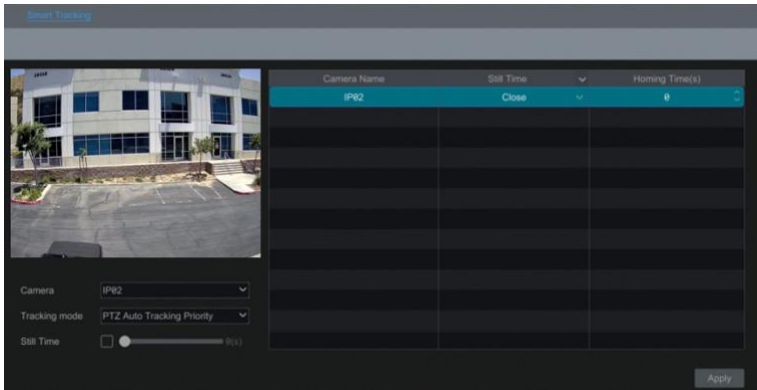
7.7 Smart Tracking

This function is only available for AI PTZ cameras. Please add an AI PTZ camera to the NVR first.

Smart Tracking: When a person or vehicle crosses the alarm line or intrudes into a predefined area, the PTZ camera will automatically track them, it will automatically zoom in and center on the target until the target disappears from the screen. After that, the PTZ camera will return to its tracking start position.

To set smart tracking:

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



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

Tracking Mode: You can choose PTZ Auto Tracking Priority or Manual PTZ Control Priority.

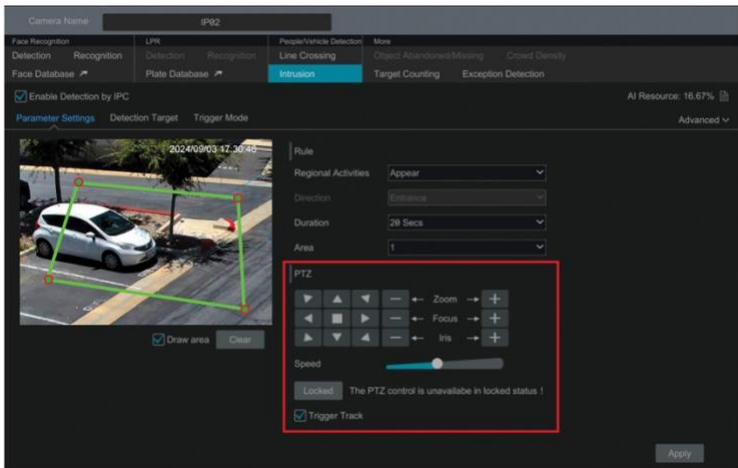
PTZ Tracking Priority: if this mode is selected, after enabling “Trigger track” for one of the following events, you cannot control the PTZ by clicking the buttons on the PTZ control panel in the live view interface.

Manual PTZ Control Priority: if this mode is selected, after enabling “Trigger track” for one of the following events, you can control the 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 a target is detected.

Still time: If enabled and you’ve set a time, when a target stops or hides behind an obstacle, or the target tracking is complete and no target appears in the detection area during the set time, the PTZ camera will return to the tracking start position. Of course, 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: in a crossroad, if a car is waiting for the red light for 30 seconds, and the still time is set to 20 seconds, then the tracking will stop following; but if the still time is set to 40 seconds, after the red light changes to a green light, and the car starts to move, the PTZ will continue to track the car.

3. Click Settings→AI/Event→AI Event. Select an AI PTZ camera and the type of event as needed (Line Crossing/Intrusion). For example: intrusion.



4. Enable an event, set a 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 PTZ must be locked, or the smart tracking cannot take effect.

5. Click “Draw area” and then draw an intrusion region on the screen. After that, check “Trigger Track” and click “Apply” to save the settings.

6. Set a detection target.

7. Click “Apply” to save settings.

8 Record & Disk Management

8.1 Record Configuration

8.1.1 Mode Configuration

Please format HDDs before recording (refer to [7.4.1 Disk Management](#) for details). Click Start→Settings→Record→Mode Settings to go to the mode settings interface. You can set the recording time under the “Manual Record Settings” and then click “Apply” to save the settings. There are two record modes: auto mode and manual mode.

The screenshot displays the 'Record Mode' configuration window. At the top, the title 'Record Mode' is shown. Below it, the 'Mode' is set to 'Auto' in a dropdown menu. A list of recording modes follows, each with a radio button: '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', and 'Always(24x7) Record+Motion Record+Sensor Record+AI Record'. The last option is selected, indicated by a blue dot and a mouse cursor. An 'Advanced' button is located below the radio buttons. The bottom section, titled 'Manual Record Settings', contains a 'Record Time' dropdown set to 'Manual' and an 'Apply' button.

➤ Auto Mode

Motion Record: Motion alarm recording will trigger when motion is detected.

Sensor Record: Sensor alarm recording will trigger when a sensor alarm happens.

Motion Record+Sensor Record: Motion/sensor alarm recording will be enabled when motion/sensor events happen.

Always(24 x 7) Record+Motion Record: Normal recording is enabled all the time; motion alarm recording will start when motion is detected.

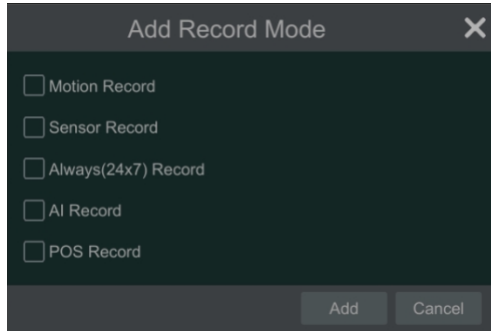
Always(24 x 7) Record+Sensor Record: Normal recording is enabled all the time; sensor alarm recording will trigger when a sensor alarm happens.

Always(24 x 7) Record+Motion Record+Sensor Record: Normal recording is enabled all the time; motion/sensor alarm record will be enabled when motion/sensor events happen,

Always(24 x 7) Record+ Motion Record + Sensor Record + AI Record: Normal

recording is enabled all the time; AI recording will be enabled when an AI event happens.

You can customize what events to record on, including POS recording. Click “Advanced” to bring up the window shown below. Check the modes in the window you wish to use and then click “Add” to create a list of events to record on (in the window, the modes you check will trigger recording, the ones you do not check won’t trigger recording.)



Select an auto mode to bring up the corresponding window. Set encode, GOP, resolution, FPS, bitrate type, quality, max bitrate, and audio for each camera and then click “OK” to save the settings. Please adjust the parameters according to your needs.



Video Encode: the available options are H.265S, H.265+, H.265 and H.264. If the connected IP camera doesn’t support H.265s, H.265+, or H.265, then those options will not be shown.

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

FPS: the higher the frame rate is, the more fluid the video is. However, more storage will be used.

Bitrate Type: CBR and VBR can be selected. 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 to 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 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: you can choose between 32Kbps ~10240Kbps.

GOP: group of pictures.

➤ Customization Mode

If custom mode is selected, you set the recording schedules for each camera individually. See [7.1.2 Schedule Settings](#) for details.

The screenshot shows the 'Record Mode' interface with 'Customization' selected in the 'Mode' dropdown. Below is the 'Schedule Config' section with a 'Schedule Management' button. It contains a table with columns: Camera Name, Sensor Record Schedule, Motion Record Schedule, AI Record Schedule, POS Record Schedule, and Timed Record. There are four rows for IP camera 01, IP camera 02, IP camera 03, and IP camera 04. Each row has dropdown menus for the first five columns, all currently set to '<None>'. Below the table is a 'Manual Record Settings' section with a 'Record Time' dropdown set to 'Manual' and an 'Apply' button.

Camera Name	Sensor Record Schedule	Motion Record Schedule	AI Record Schedule	POS Record Schedule	Timed Record
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

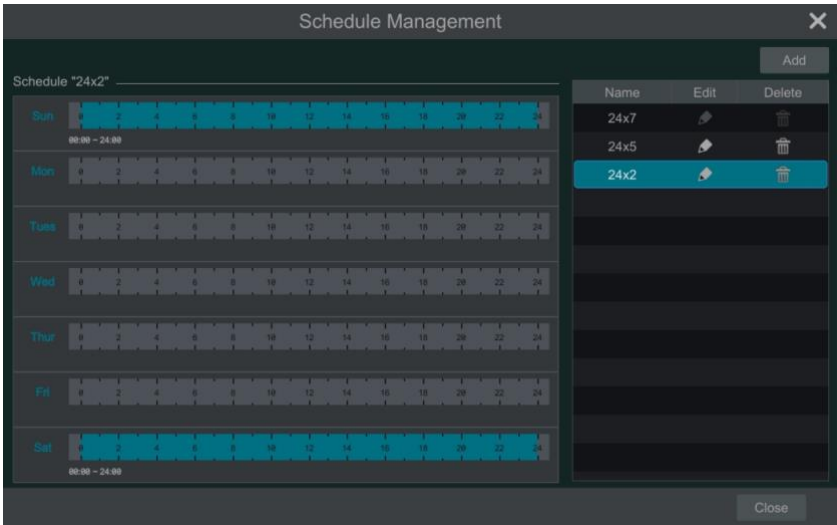
Apply

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

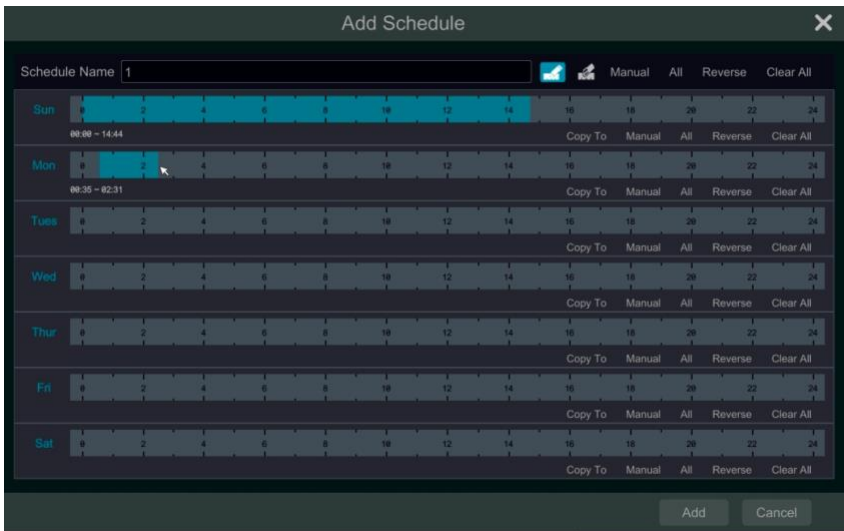
8.1.2 Schedule Settings

➤ 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. The default options are “24 x 7”, “24 x 5” and “24 x 2”; you cannot edit or delete “24 x 7” while “24 x 5” and “24 x 2” can be edited and deleted. Click the schedule name to display detailed schedule information on the left side of the interface. The seven rows stand for the days in a week and each row stands for 24 hours in a day. Blue stands for time you have selected and gray stands for unselected time.



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

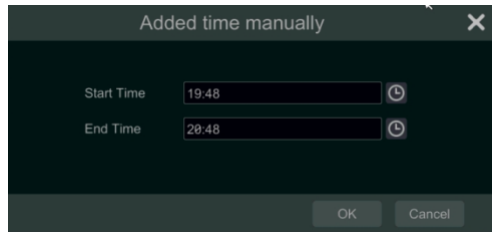


Set a schedule name and schedule time and then click “Add” to save the schedule. You can set a day schedule or a week schedule. : add button; : delete button.

➤ Set Day Schedule

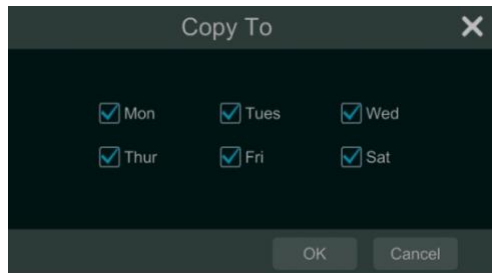
Click  and then drag the cursor on the time scale to set the recording time; click  and then drag the cursor on the time scale to delete the selected area.

You can manually set the record start time and end time. Click  or  and then click “Manual” on each day to bring up the window shown below. Set the start and end time in the window and then click “OK” to save the settings.



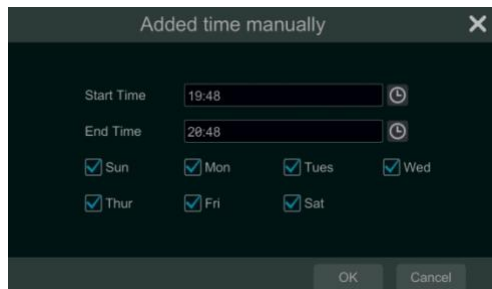
Click “All” to set all day recording; click “Reverse” to swap the selected and unselected time in a day; click “Clear All” to clear all the selected areas in a day.

Click “Copy To” to copy the schedule from the day to other days. Refer to the picture below. Check the days in the window and then click “OK” to save the settings.



➤ Set Week Schedule

Click  or  and then click “Manual” beside  to set a 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.



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.

8.1.3 Advanced Configuration

Click Start→Settings→Record→Advanced to go to the following interface. Enable or disable cycle record (the earliest recording data will be deleted and replaced by the latest when the disks are full). Choose what streams will be recorded, Main Stream, Sub Stream, or both streams. Set up the pre-alarm record time, post-alarm record time, and expiration time of each camera and then click “Apply” to save the settings.

Mode Settings **Advanced**

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 Camera2	5 Secs ▼	10 Secs ▼	Never Expire ▼
name109	5 Secs ▼	10 Secs ▼	Never Expire ▼
IPC	5 Secs ▼	10 Secs ▼	Never Expire ▼

Apply

Pre-alarm Record Time: set the time to save recording footage before the recording event began.

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

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

8.2 Encode Parameters Settings

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

Additionally, you can view the recording sub stream settings of each camera. Click “Apply” to save these settings. You can set the recording stream of each camera one by one or set them in bulk for all cameras.

Event Recording Settings									
Schedule Recording Settings									
Record Substream									
Camera Name	Stream Type	Encode	Resolution	FPS	Bitrate Type	Quality	Max Bitrate	Bitrate Limit Recommendation	
IP#1	Main Stream	H.265	1920x1080	25	VBR	Higher	2048Kbps	2350~3930Kbps	
IP#5	Main Stream	H.265	1920x1080	25	VBR	Higher	2048Kbps	2350~3930Kbps	
IP#3	Main Stream	H.265	1920x1080	25	VBR	Higher	2048Kbps	2350~3930Kbps	
IP#4	Main Stream	H.265	3840x2160	30	VBR	Higher	5120Kbps	5632~19338Kbps	

Remain Bandwidth: 54 / 80 Mb

Apply

8.3 Record Mode

8.3.1 Manual Recording

Method One: Click  on the tool bar at the bottom of the live preview interface to manually start recording all cameras in highest quality.

Method Two: Go to live preview 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.

8.3.2 Schedule Recording

Schedule Recording: the system will record automatically according to a set schedule.

Set the recording schedule for each camera. See [7.1.2 Schedule Settings](#) for details.

8.3.3 Motion Based Recording

Motion Based Recording: the system will start motion based recording when motion occurs in the field of view. The setup steps are as follows:

- ① Set a motion based recording schedule for each camera. See [7.1.2 Schedule Settings](#) for details.
- ② Enable motion and set a motion area for each camera. See [11.2 Motion Alarm](#) for details.

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

8.3.4 Sensor Based Recording

- ① Set the schedule for sensor based recording for each camera. See [7.1.2 Schedule Settings](#) for details.
- ② Select NO(normally open) or NC(normally closed) for each sensor, enable the sensor alarm and then check and configure the “Record”. See [11.1 Sensor Alarm](#) for details.

8.3.5 AI Event Recording

- ① Set a schedule for intelligent recording for each IP camera. See [7.1.2 Schedule Settings](#) for details.
- ② Enable intelligent detection (object detection, exception, line crossing, intrusion, or face detection) and draw an alert surface or warning area for each IP camera. See [9](#)

[AI Event Management](#) for details.

The camera will start AI recording once you finish the above settings. This function is only available for some cameras.

8.4 Disk

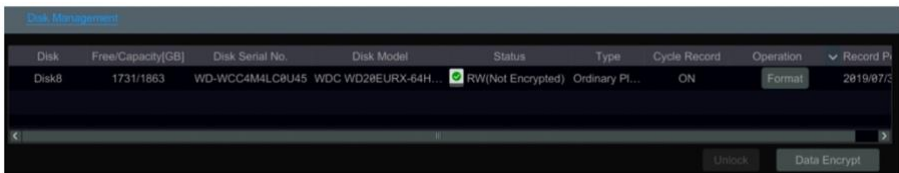
8.4.1 Disk Management

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

For models 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) for recording.

➤ Disk Management

Click Start→Settings→Disk→Disk Management to go to the disk management interface. You can view an NVR's disk capacity, disk status, and so on in this interface. Click “Format” to format HDDs.



Data Encryption:

- ① Click “Data Encrypt”.
- ② Enter the username and password used to log into the NVR. The account used must have disk management permissions.
- ③ Check the disk you want to encrypt and then enter a password.

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

Data Decryption:

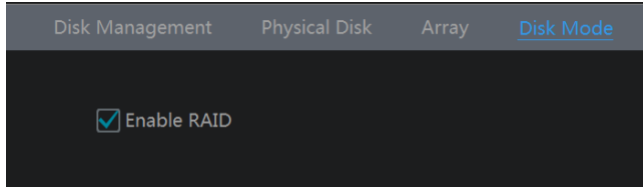
- ① Click “Change Encrypt”.
- ② Enter the username and password used to log in the NVR. The account used must have disk management permissions.
- ③ Check the disk you want to decrypt and then enter the password.
- ④ Click “Close Encrypt”.

Unlock the disk: when one encrypted disk is transferred from another NVR to this NVR, it will be in a locked status. 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 it cannot be written to.

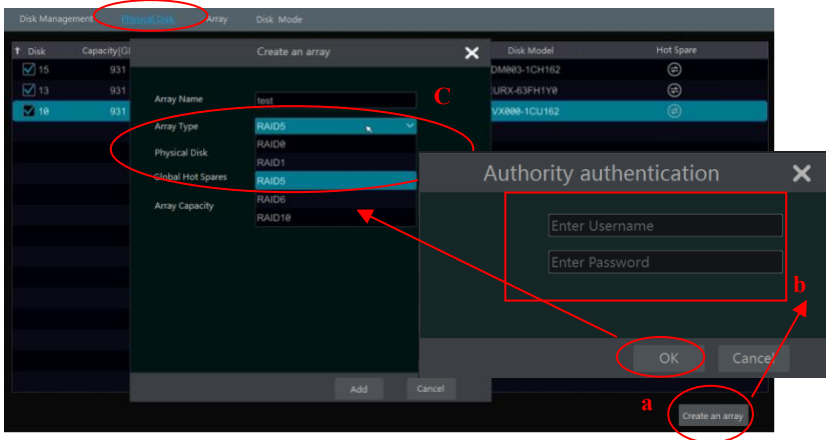
Some models do not support the RAID function. The settings of RAID are as follows. Please skip the settings of physical disk, array, and disk mode if the NVR doesn't support this function.

- RAID ① Enable RAID (Go to Start→Settings→Disk→Disk Mode) Click Enable Raid.



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

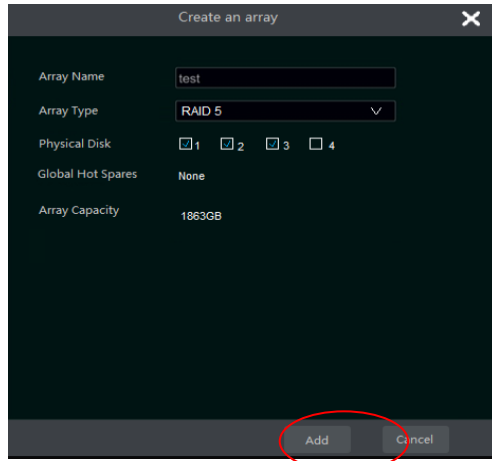
- Click “Physical Disk” tab and then click “Create an array”.
- Enter a username and password for an account with Disk Management permissions. If you don't have one, you can use the username and password that you login with (the default username: admin; the default password: 123456).
- Enter an array name and select an array type (such as RAID5).



- Select physical disk.

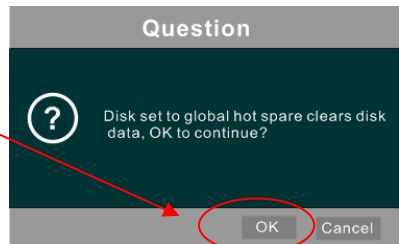
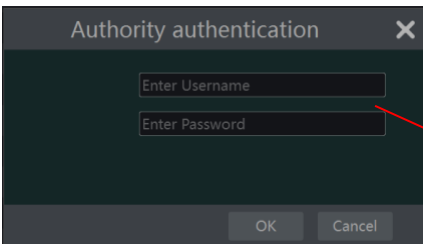
If you have 16 disks, please choose 15 disks. The remaining one will set as a hot spare.

If higher data security is needed, you can decrease physical disks and increase hot spare disks. Please set them up as needed.



- e. Select a hot spare. In the physical disk interface, select a 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	



● RAID Rebuilding

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

Disk Management Physical Disk Array Disk Mode

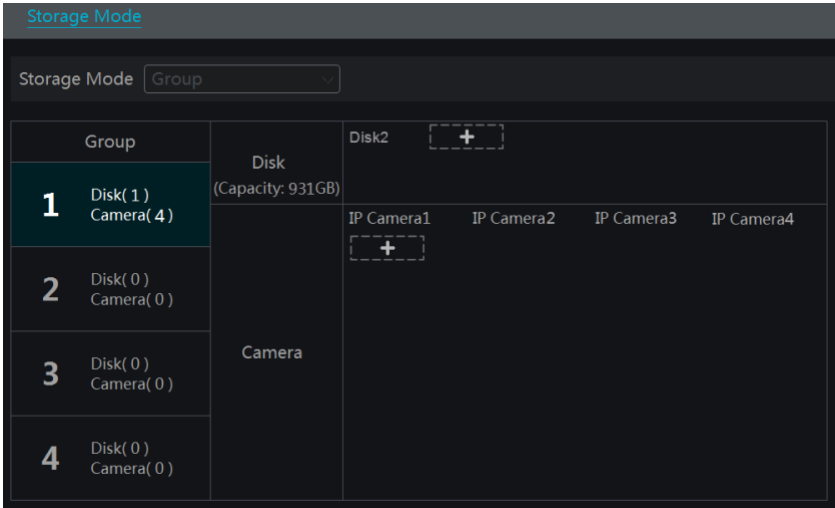
No.	Name	Capacity[GB]	Physical Disk	Hot Spare Position	Status	Type	Rebuild
1	test	1862	2 3	4	Degraded	RAID5	

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



8.4.2 Storage Mode Configuration

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

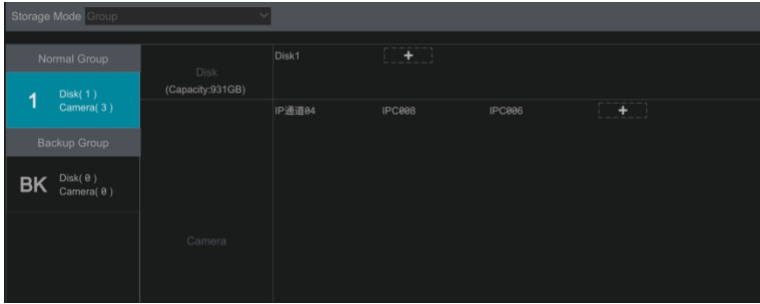


For example, there are four disk groups. By using the disk group function, you can correspond cameras to specific disks (the recording data of each camera in a group will be stored on the disks in the same group). NVRs with an e-SATA interface support recording on e-SATA connected disks.

Disks and cameras are added into group one by default. Disks and cameras not in group one can be deleted (select a disk group and then click  on the top right corner of the added disk or camera to delete it from the group). 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 bring up a window. Check the disks or cameras in the window and then click "Add".

For models with 2 or 4 HDD slots, backup groups can be added as shown below.



Click  to add a 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 move it to a 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.

8.4.3 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.

View Disk Information						
S.M.A.R.T. Information						
Health Status Check						
Disk	Disk1					
Disk Serial No.	Z3T9QMCM					
Disk Model	ST5800M002-1BD142					
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	100	99	0	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	656989752	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 plugging-in or pulling-out details of a HDD from the logs to check if someone removed your HDD or not. Click Start→Settings→System→View Log.

[View Log](#)

Factory Default

Upgrade

Backup and Restore

Auto Maintenance

Main Type

All

Alarm

Operation

Settings

Exception

Start Time

2021/01/04 00:00:00

End Time

2021/01/06 23:59:59

Search

Export

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	—

9 Playback & Backup

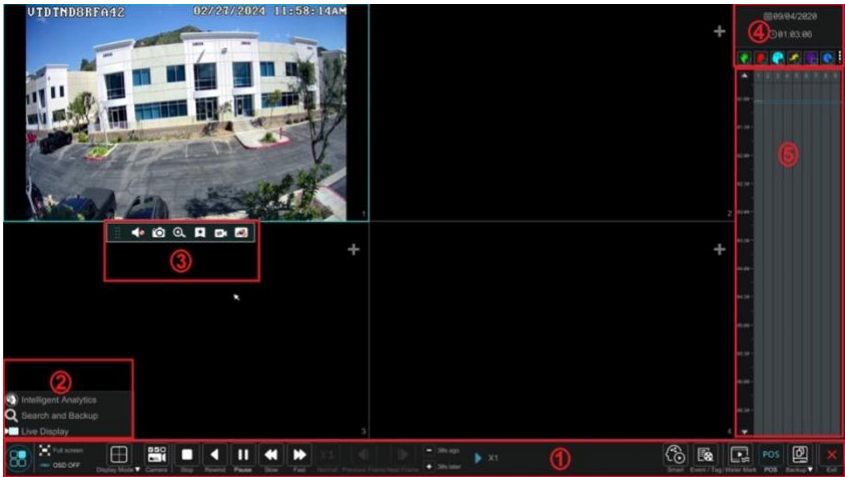
9.1 Instant Playback

Click  on the tool bar at the bottom of the preview camera window to play back the recording (click  on the tool bar at the bottom of the live preview 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 right-click in the camera window and hit “Instant Playback” and then set the instant playback time to play back recordings.



9.2 Playback Interface Introduction

Click  on the tool bar at the bottom of the live preview 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 preview interface to set default playback time).



On the panel on the right you will see the channel number and the recorded data coded by color. The bar that runs across them represents the playback time being viewed. You can click around this bar to change what time is being played back. 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 records in the playback interface automatically. You can also add a playback camera manually. Click **+** in the playback window to bring up the “Add Camera” window. Check the cameras in the window and then click “Add” to add a playback camera. The system supports a maximum of 16 playback cameras at once.

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 it to bring up area ②.
	Full screen button. Click it to show full screen; click it again to exit the full screen.
	Screen display mode button. 1/4/9/16 screen display mode can be selected (depending on models); in addition, the playback channel will switch when the same screen display mode button is clicked, 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 ON button. Click it to enable OSD; click it again to disable OSD.
	Quick channel selection button
	Stop button.
	Rewind button. Click it to play video backward.

Button	Meaning
	Play button. Click it to play video forward.
	Pause button.
	Slow Play button. Click it to decrease the playing speed.
	Fast Play button. Click it 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.
	Click  to step backward 30s and click  to step forward 30s.
	Click to enter the smart playback interface
	Event list/tag button. Click it to view the event record of manual/schedule/sensor/ motion and the tag information.
	Watermark button. Click it to enable a watermark; click it again to disable a watermark.
	Open/close POS information.
	 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 it to view the backup status.
	Back button. Click it to return.

Note: Some models may not support face search and face smart playback.
Introduction of area ②:

Button	Meaning
 Intelligent Analytics	Click it to go to the intelligent analytics interface.
 Search and Backup	Click it to go to record search and backup interface; see 8.4 Record Search, Playback & Backup for details.
 Live Display	Click it to go to the live preview interface; see Chapter 5 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 it to move the tool bar anywhere.
	Enable Audio	Click it to enable audio. You can listen to the camera audio by enabling audio.

	Snap	Click to take a snapshot of the camera recording.
	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 preview 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 a tag. You can play back the recording by searching the added tag. Click it and then enter the tag name in the popup window. Click “Add” to add a tag.
	Switch Camera	Click it to switch to another playback camera. Click it and then check the camera in the popup window. Click “OK” to change the camera.
	Close Camera	Click it 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 its recording from the time you set. You can check the recording type as desired; first, click  on the tool bar at the bottom of the interface to clear all the playback cameras, then check the recording type (: manual recording; : sensor based recording; : motion based recording; : schedule recording; : AI recording; : POS recording, if you want to view detailed smart playback icons, click  to switch, as shown below). Finally, click  in the playback window to add camera for playback (the recording time scale will show the record data of the checked recording type only after the above operations).



Introduction of the recording time scale (area ⑤):

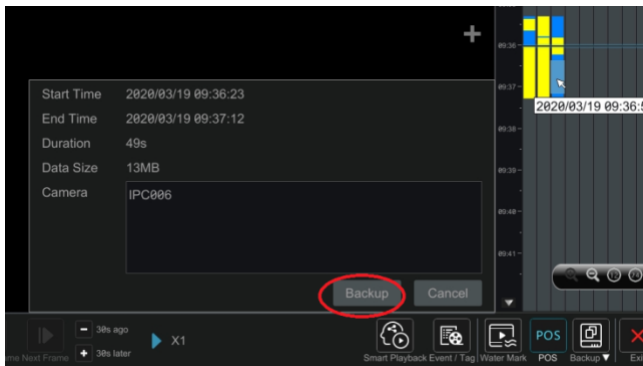
A tool bar will appear after moving the mouse to the recording time scale. Click  /  to zoom in on the timeline; click  to return the timeline to a 24-hour view. Drag the timeline or slide the scroll wheel of the mouse to scroll through the time that's not

visible above or below the current view. You can also click ▲ or ▼ to scroll through the time above or below what's visible currently on the timeline. Drag the slider at the bottom of the time scale to show more cameras on the time scale.

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

1. Backup Introduction:

Insert a storage device into the recorder. Click and drag a selection over the color block on the time scale to select a backup time and then right click the area or click 📄 to bring up a backup information window. Click the "Backup" button in the window to bring up the backup window. Select the storage device, backup path, and backup format and then click the "Backup" button.



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

Backup formats can include: Private, AVI, or MP4.

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



9.3 Smart Playback

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



1. The descriptions of buttons in the smart playback interface

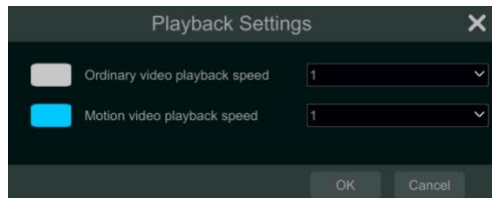
Button	Description
	Full screen motion button.
	Draw grid. You can search recordings of motion detected in the area drawn.
	Draw line. You can search recordings of times the line was crossed after drawing the line.

Button	Description
	Draw quadrilateral. You can search recordings in this quadrilateral after drawing it.
	Search by face
	Search by license plate number
	Search by human/vehicle detection
	Playback settings button
	Return button. Click to return to the previous interface.

9.3.2 Smart Playback Settings

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

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



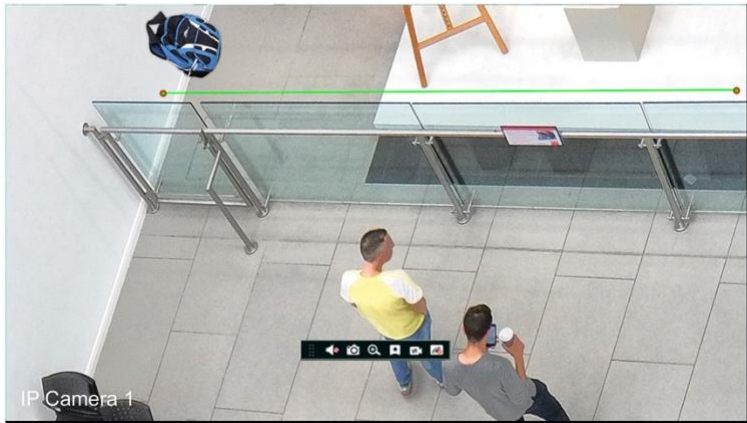
9.3.3 Smart Playback Based on Motion Detection

- Smart Playback by Drawing a Grid

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

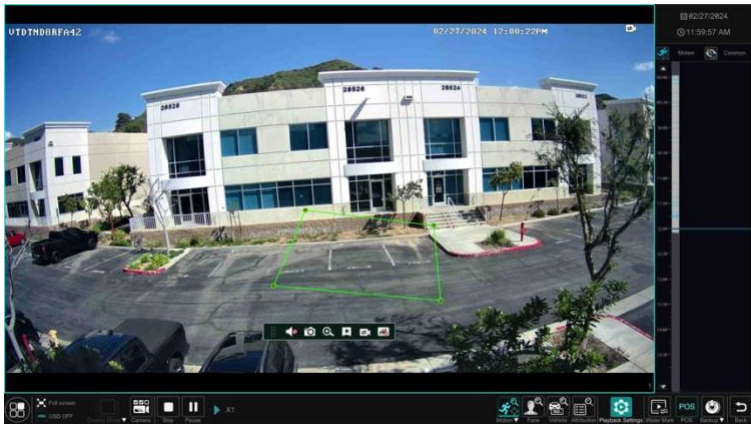
- Smart Playback by Drawing Line

Click  and draw a line in the desired area. The system will automatically search the recordings where a line crossing was detected. The cyan blocks indicate that there are intelligent recordings. Move the cursor to that block and click to play the recording.



- Smart Playback by Drawing Quadrilateral

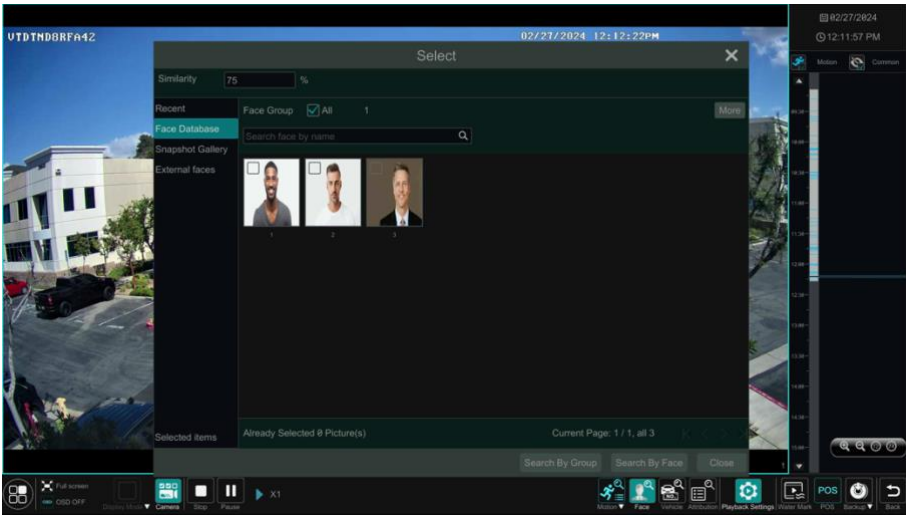
Click  and draw a quadrilateral in the desired area. Then the system will automatically search the recordings of this area. The cyan blocks indicate that there are intelligent recordings. Move the cursor to that block and click to play the record.



9.3.4 Smart Playback by Face Search

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

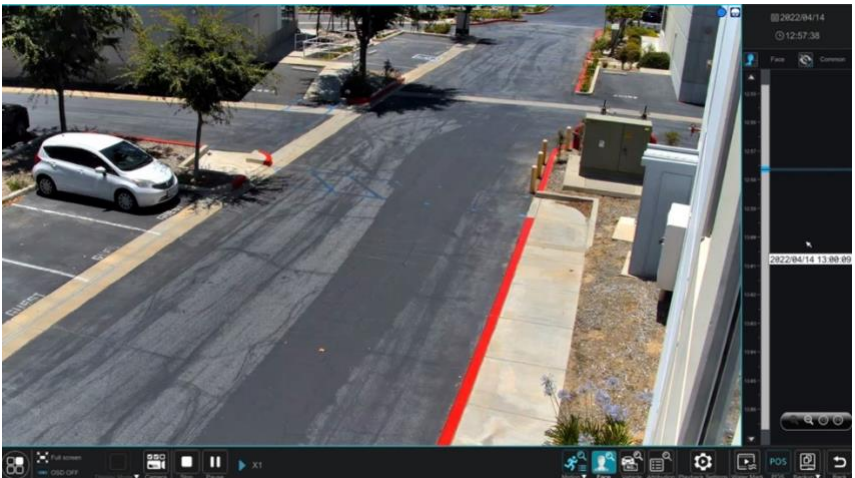
- ① In the smart playback interface, click  to bring up the following window.



- ② Set similarity. The higher the sensitivity value is, the lower the searching accuracy will be, and vice versa.
- ③ Select targets. You can select targets from recent recordings, the face database, the snapshot gallery, or external faces (from pictures stored on an inserted drive.)
- 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 recording exists and click to play those recordings.

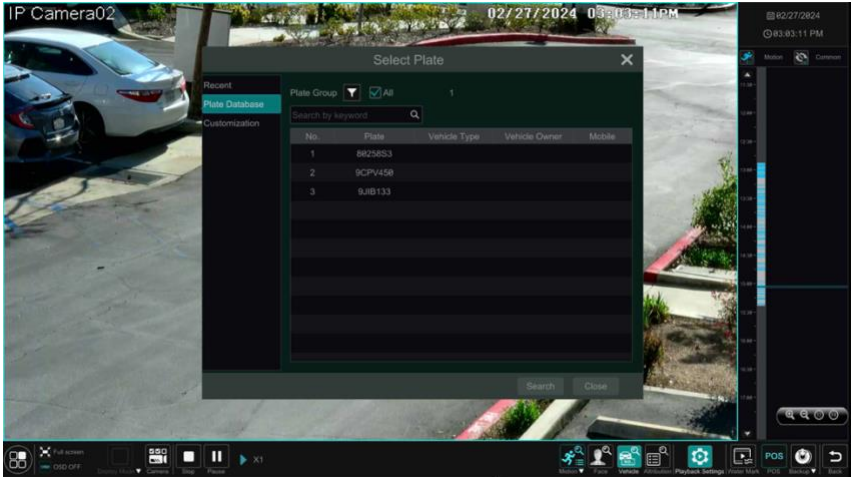
You can only check "Face" to view the face records.



9.3.5 Smart Search by License Plate

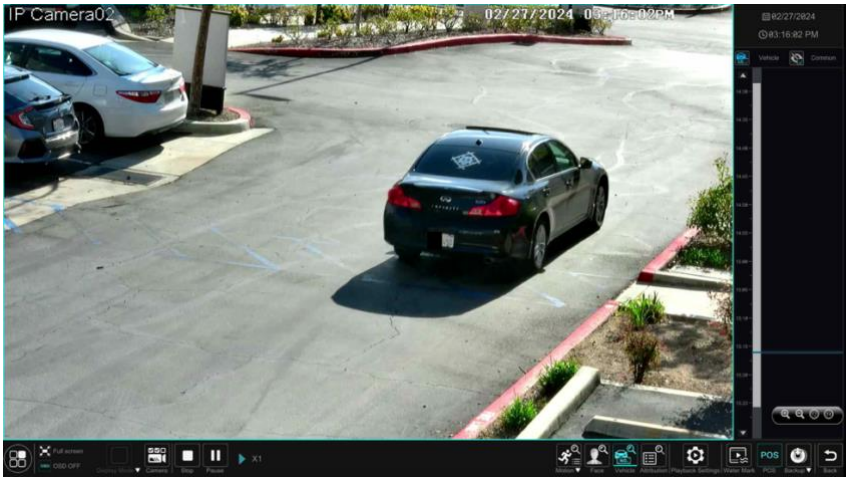
Before starting smart search by plates, please add LPR cameras first and enable the LPR function. Please refer to License Plate Recognition for details.

Click the  button to go to the following interface.



To search for plates, select from “Recent”, “Plate Database” or “Customization” and then click “Search” to search recordings and play them. Here we use an example of searching a plate from the “Plate Database”.

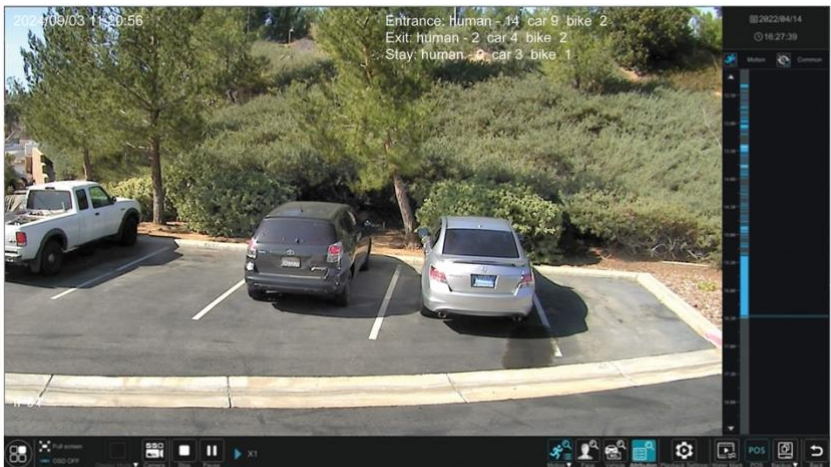
Click  to choose a group. Then plates will be listed in the table automatically. Click “Search” to play.



9.3.6 Smart Search by Object Attributes

Before searching objects by attributes, please enable the video metadata function of cameras. Click  to select attributes.

Select attributes of humans/motor vehicles/non-motor vehicles as desired to search the results.

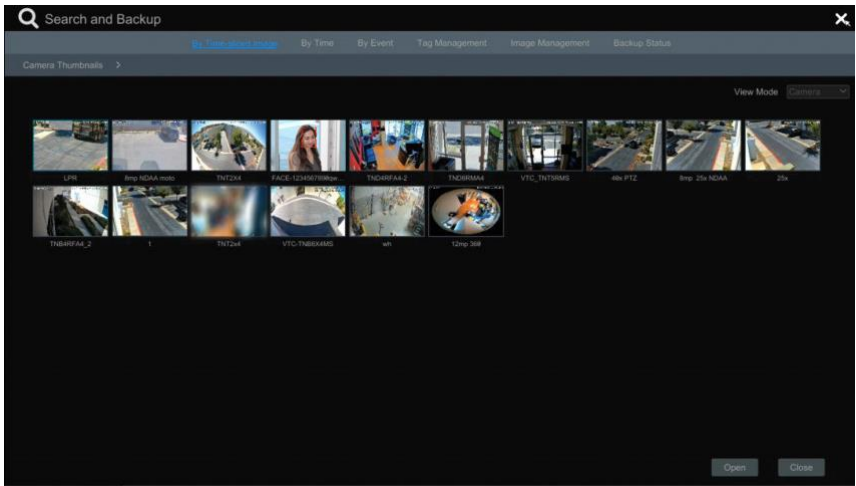


9.4 Record Search, Playback & Backup

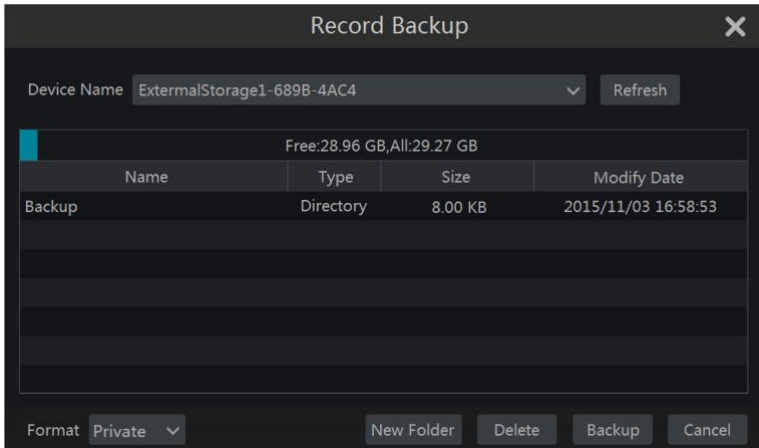
The recording data and the snapshotted pictures can be backed up through the network or a USB (U disk or USB mobile HDD). The file system of the backup devices should be FAT32 format.

9.4.1 Search, Playback & Backup by Time-sliced Image

- ① Click Start→Search and Backup→By Time-sliced Image to go to the “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 a thumbnail. A maximum of 196 camera names can be listed. If there are more than 196 camera name, then the time view mode will be disabled and only the camera view mode will be available.

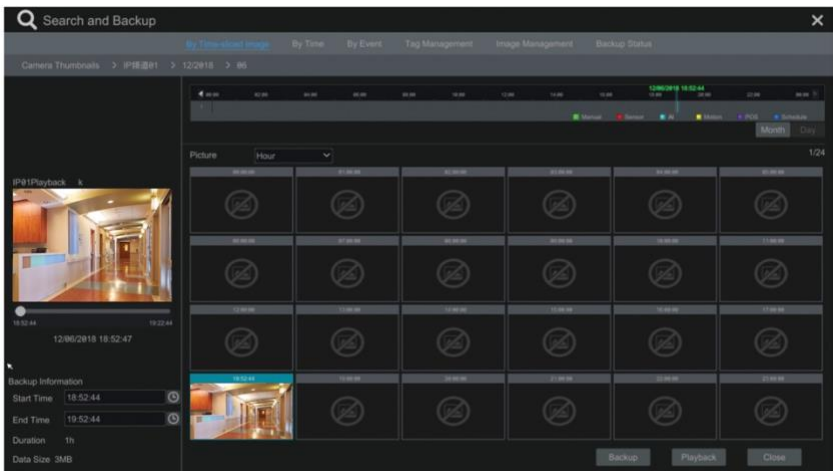


- ② Select one camera in the interface and then click the “Open” button.
- ③ Click the image box to play the recording in a small playback box on the left side of the interface (the box with images inside indicate that a recording exists).
- ④ Refer to the picture below. Drag the color blocks on the time scale to select the recording and then click the “Backup” button to bring up 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.



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 a recording in the playback interface (refer to [8.2 Playback Interface Introduction](#) for details). Click “Close” to close the interface.



1. Time Slice Mode Selecting:

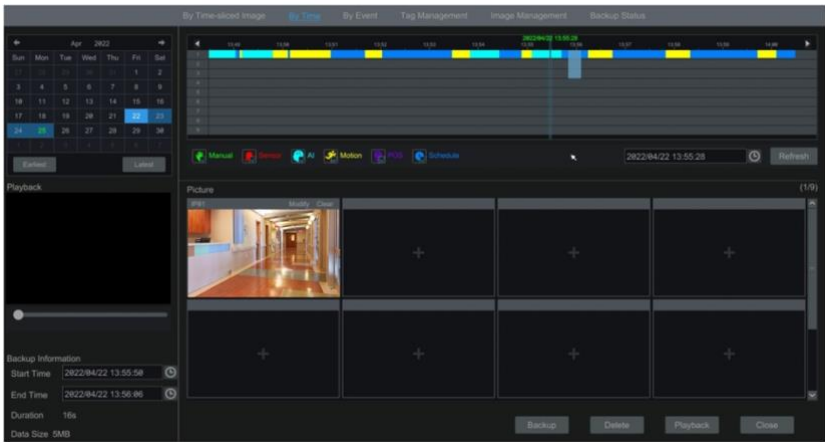
Method One: Click “Year”, “Month” or “Day” button under the recording time scale to select time slice mode. In “Day” mode, click ◀ / ▶ on the left/right side of the time scale to view recordings of the last/next day; click “Minute” in the “Picture” option under the time scale to select “Minute” mode (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 from the different time slice modes.

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

9.4.2 Search, Playback & Backup by Time

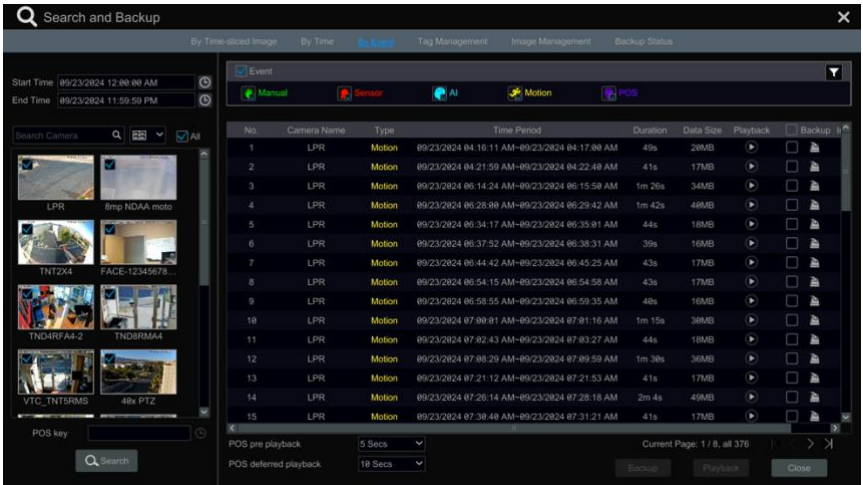
- ① Click Start→Search and Backup→By Time to go to the “By Time” tab shown below.
- ② Click  on the bottom of the interface to add a playback camera. A maximum of 16 cameras can be added for playback. Click “Modify” on the top right corner of the camera window to change the camera and click “Clear” to remove the camera.
- ③ Click the camera window to play the recording in a 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 desired and click the time scale or click  under the time scale to set the time. The camera window will play recordings based on the time and event type you set.
- ④ Drag the color blocks on the time scale to select recording 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” to start a record backup. Click “Playback” to play the recording in the playback interface. Click “Delete” to delete the selected record file.



9.4.3 Search, Playback & Backup by Event

Some models may support searching by POS events.

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

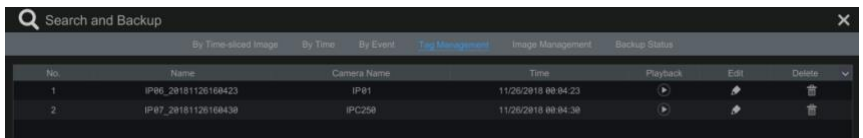


- ② Check the event type in the interface as desired.
- ③ Click to set the start time and end time on the top left of the interface.
- ④ Check cameras on the left side of the interface or check "All" to select all the cameras and then click to search the recordings. The searched recording will be displayed in the list.
- ⑤ Click in the list to play back the recording in a popup window. Click to back up one recording file or check multiple recording files in the list and then click "Backup" for batch backup.
- ⑥ Select one recording file in the list and then click "Playback" to play the recording in the playback interface.

9.4.4 Search & Playback by Tag

You can play back recordings that you previously tagged. Click Start→Playback to go to the playback interface and then click on the bottom of the camera window to add a tag when you want to mark the playback time point of a selected camera.

Click Start→Search and Backup→Tag Management to go to "Tag Management" tab.



Click in the interface to play the recording. Click to edit the tag name. Click to delete the tag.

9.4.5 Image Management

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

Q

Search and Backup

X

By Time-sliced Image

By Time

By Event

Tag Management

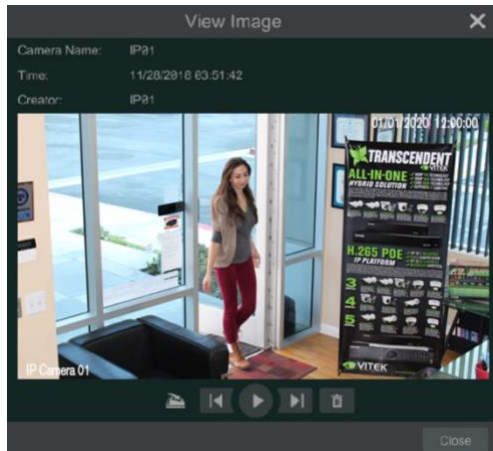
Image Management

Backup Status

☐	No.	Camera Name	Snapshot Mode	Snapshot Time	Creator	Browse	Export	Delete
☐	1	IP Camera#1	Motion	2021/07/08 18:54:22	IP Camera#1			
☐	2	IPC	Motion	2021/07/08 18:54:21	IPC			
☐	3	IP Camera#2	Motion	2021/07/08 18:54:15	IP Camera#2			

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

Click to bring 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.



9.4.6 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 status of backed up files.

10 AI Event Management

10.1 Face Recognition

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

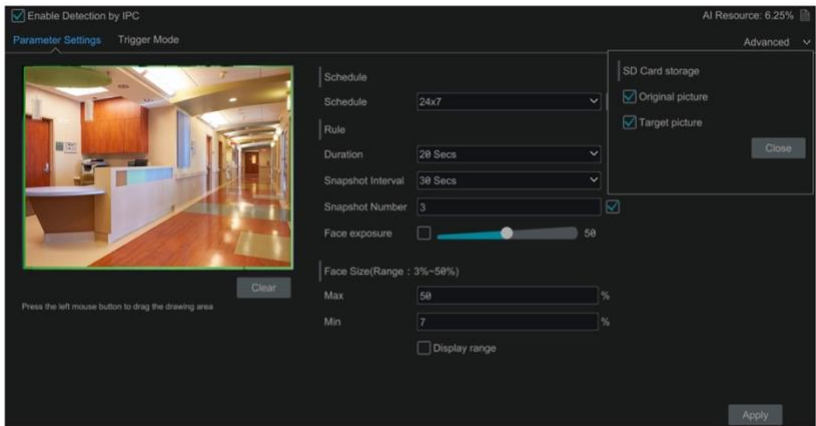
Please use the following steps to set up the face recognition function for the first time.

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

10.1.1 Face Detection Settings

Face Detection: Alarms are 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.



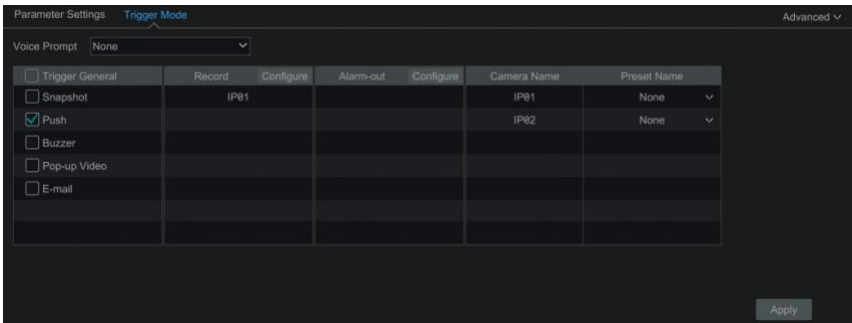
- ② Select a camera, check “Enable Detection by IPC” and set the duration.

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

- ③ Set the schedule. Click “Manage” to set the desired schedule. Please refer to [7.1.2 Schedule Settings](#) for details.
- ④ Set the snapshot interval parameter and snapshot number. The snapshot interval

refers to the amount of time before a camera captures the same face again. The snapshot number setting refers to the number of pictures of the same face that will be captured during the snapshot interval (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 if needed. It can help when the brightness of a detected face is too low. (Only some cameras support this function)
- ⑥ Set up the alarm area. Drag the mouse to draw a detection area. Click “Clear” to delete the alarm area. Then, set the face detection size by defining a maximum and minimum value (The default size range of a single face image occupies from 3% to 50% of the entire image).
- ⑦ Enable “Save Source Information” and/or “Save Face Information” as desired. If enabled, the system will automatically save the corresponding images on an SD card.
- ⑧ Click “Apply” to save the settings.
- ⑨ Click “Trigger Mode” to go to face detection alarm linkage setting interface:



1. Face Detection Alarm Linkage Configuration:

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

Voice Prompt: Please upload an audio file in the local audio alarm interface first (click Start→Settings→AI/Event→Event Notification→Audio). Please see [11.5.6 Audio](#) for details.

Record: Click the “Configure” button to bring up a window. Select a camera on the left side and then click  to set the camera to record. Select a camera on the right side and then click  to cancel disable recording on that camera. Click “OK” to save the settings. The selected cameras will record automatically when faces are detected.

Alarm-out: Click the “Configure” button to bring up the “Trigger Alarm-out” window. You can configure the trigger alarm-out settings here. The system will trigger alarm-out events automatically when faces are detected. You need to set a delay time and the schedule of the alarm outputs. See [11.5.1 Alarm-out](#) for details.

Preset: Click  and then select a preset for each PTZ camera. To add presets,

please see [6.2 Preset Setting](#) for details.

Snapshot: The current camera will capture images automatically when faces are detected.

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

Buzzer: if enabled, the system will begin to buzz when faces are detected. To set the delay time of the buzzer, please see [11.5.4 Buzzer](#) for details.

Pop-up Video: if enabled, the system will bring up a pop-up window of the corresponding video automatically when faces are detected. To set the duration time of the video, please see [11.5.3 Display](#) for details.

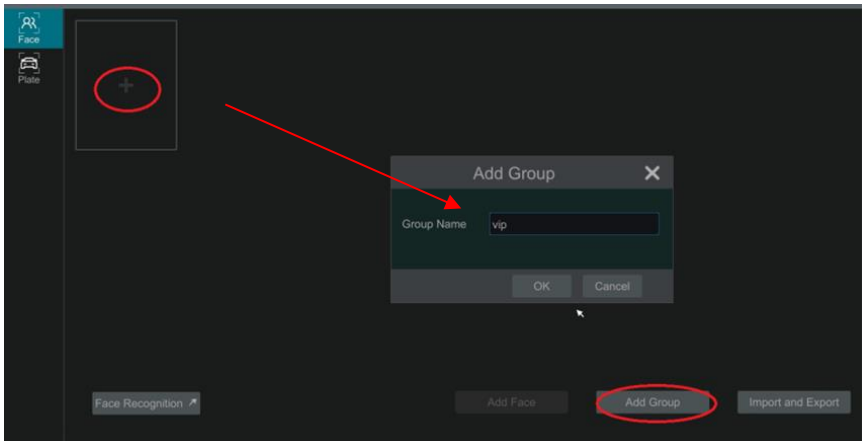
E-mail: if enabled, the system will send an e-mail when faces are detected. It will attach a zoomed-in captured face picture and an original full picture so that you can view the whole scene when the alarm occurs. Before you enable the email, configure the recipient's e-mail address first (see [14.1.5 E-mail Configuration](#) for details).

Enable "IPC_Audio" or "IPC_Light" as desired (only some cameras support these two functions). To set up the camera's audio, number of times it will go off, and volume, please refer to [11.5.6 Audio](#) for details. To set the flashing time and frequency of the camera's lights, please refer to [11.5.7 Light](#) for details.

- ⑩ Click "Apply" to save the settings.

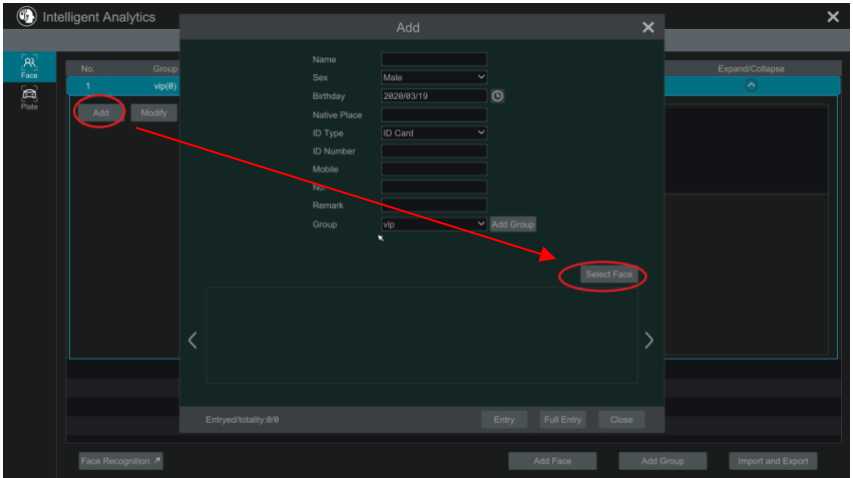
10.1.2 Face Database Management

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



The first time you open this, you can click "+" or "Add Group" to add groups.

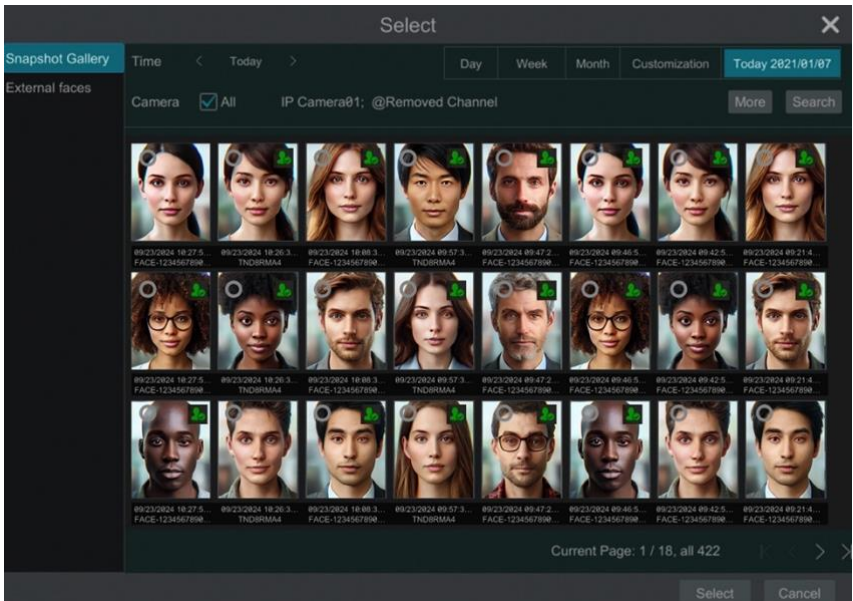
- ② To add targets for each group.
- Select a list and then click  to expand the list as shown below.



- Click “Add” and then click “Select Face” to add face images. You can add faces from the snapshot gallery or an external source.

Adding faces from the snapshot gallery: Select a search time or self-define a search time and then click “Search” to search for detected faces, then select the desired face pictures, and click “Select”.

Note: Pictures marked with a green icon can be added to the face database.



1. Add an external face

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

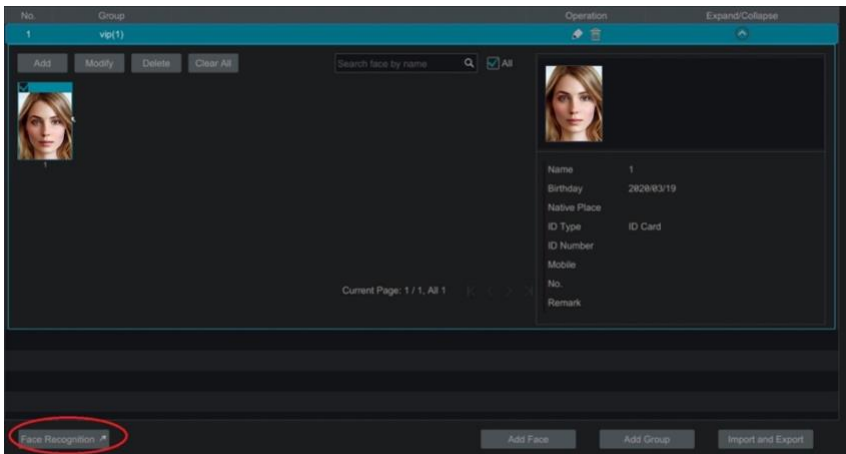
Go to the face database interface. Click  to expand the group and then click "Add". Select "External faces" to select face pictures. You can select one face or multiple faces to add.

To add multiple faces: A. Put face pictures and the description file (.csv or .txt) in 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 must be ".jpg" or ".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 detailed information will be listed on the right.



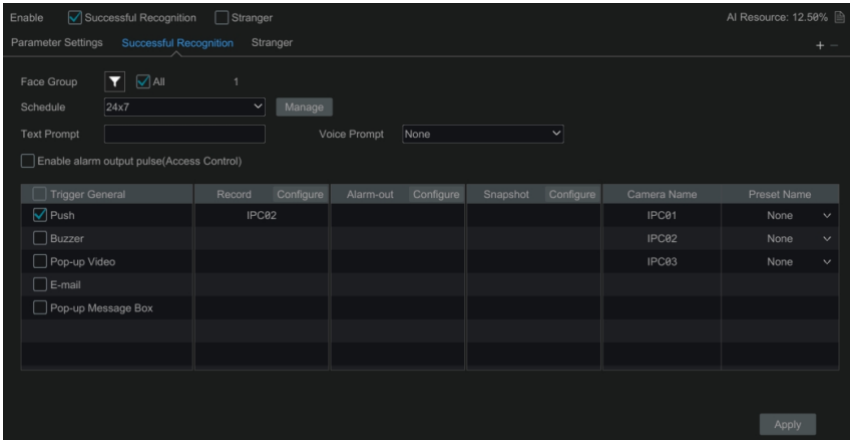
- Import and Export Face databases

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

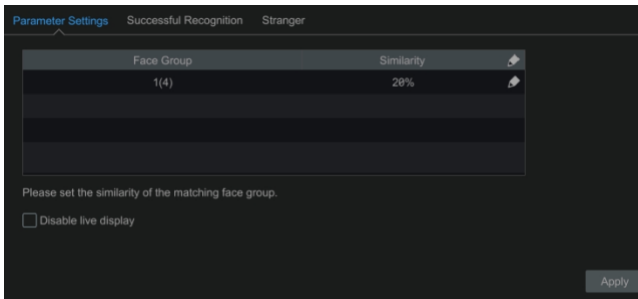
The exported face database file (csv+jpg) can be directly imported to the face database. This makes it is very convenient for you to transfer face database files to other devices.

10.1.3 Face Recognition Settings

After a 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.

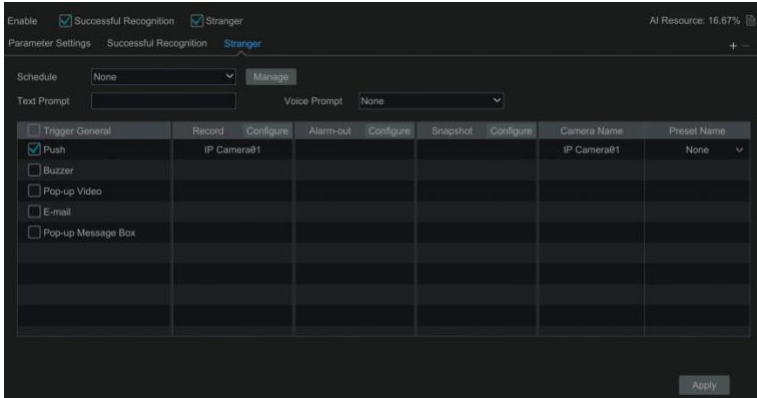


- ① Enable “Successful Recognition” or “Stranger”. Click “Parameter Settings” to set the similarity percentage for matching to the face group.



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

- ② Set alarm linkage items for successful recognition.
 - Select one or more face groups and then choose a schedule. Click “Manage” to set the schedule.
 - Set the text prompt and voice prompt. When a captured face is matched successfully, the text will appear on the right of the live view interface and broadcast the audio.
 - Enable the alarm output pulse (access control).
 - Trigger record, snapshot, alarm-out, buzzer, push alert, pop-up video, E-mail, and pop-up message box as desired. The alarm linkage settings are similar to the face detection alarm settings. (see [9.1.1 Face Detection Settings](#) for details).
 - Click “Apply” to save the settings.
- ③ Set up the stranger alarm linkage items. When a captured face picture doesn’t match any face pictures in the face database or their similarity is lower than the set value, the captured person will be regarded as a stranger.

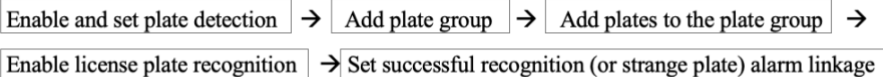


- Configure a schedule.
 - Set the text prompt and voice prompt. The text will show on the captured picture and the voice will be broadcasted when a stranger is detected.
 - Trigger record, snapshot, alarm-out, buzzer, push alert, pop-up video, E-mail, Preset, and pop-up message box as needed. The alarm linkage settings are similar to the face detection alarm settings (See [9.1.1 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.

10.2 License Plate Recognition

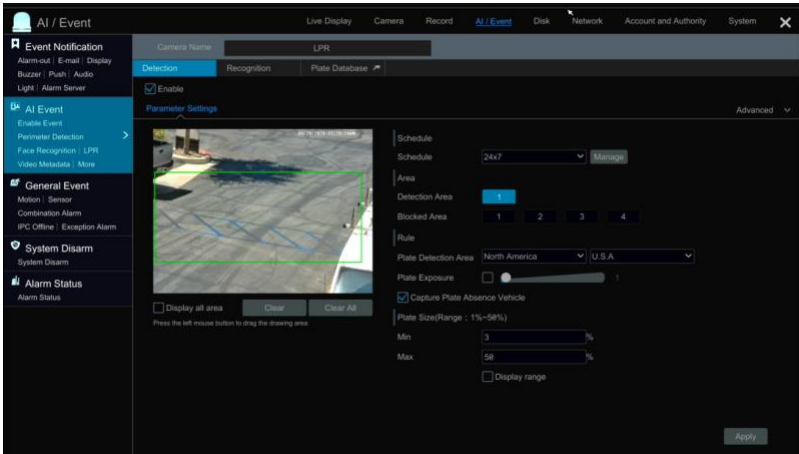
Please add an LPR camera before using this function. If your camera doesn't support this function, please skip the following instructions.

Please follow these steps to set up the license plate recognition function.



10.2.1 License Plate Detection Settings

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

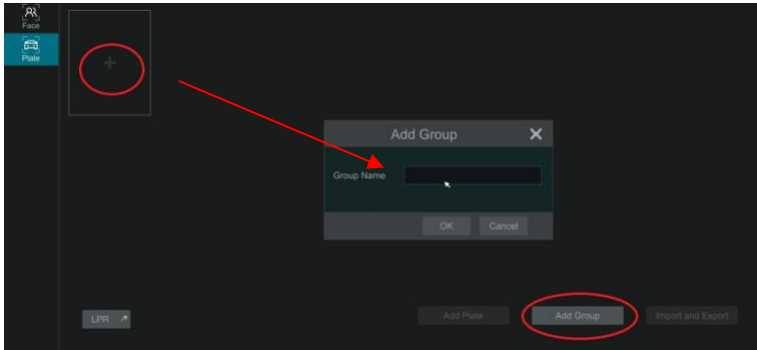


- Select a schedule.
- Set up the area and plate exposure as needed.
- Set up the alarm area. Drag the mouse to draw a detection area. Click “Clear” to delete the alarm area.
- Set up blocked areas. Select the number of areas needed and then draw a blocked area. Up to 4 areas can be set up. After you set up blocked areas, they will not be included in the detection area.
- Click “Display all areas” to view all blocked and detection areas.
- Click “Clear All” to clear all blocked and detection areas.
- Check “Capture plate absence vehicle” if needed, this will detect if a license plate is missing from a vehicle.
- Set the plate size by defining the maximum and minimum values (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” will be displayed on the left window.
- Click “Advanced” to set the recognition mode as needed (only some LPR cameras support).

10.2.2 Plate Database Management

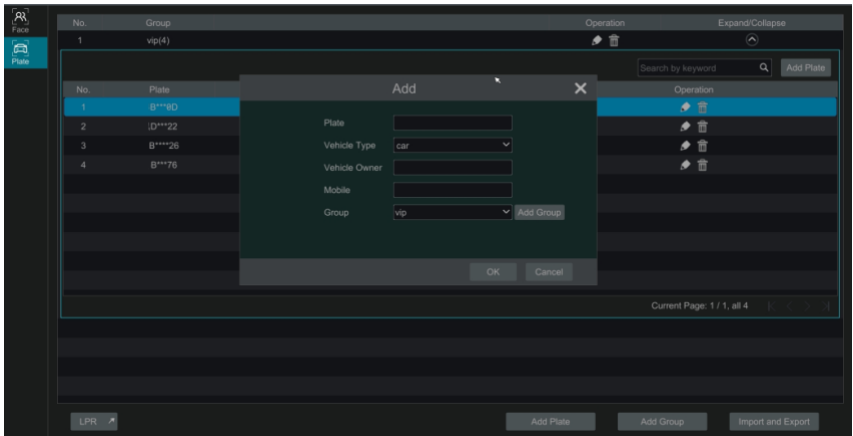
In the LPR interface, click the “Plate Database” tab to go to the plate database management interface shown below.

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



1. Add plates to each group:

- ① Click to extend the group. Click “Add Plate” to bring up the following window.



- 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 detailed information about how to import or export the plate list.

10.2.3 License Plate Recognition Settings

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

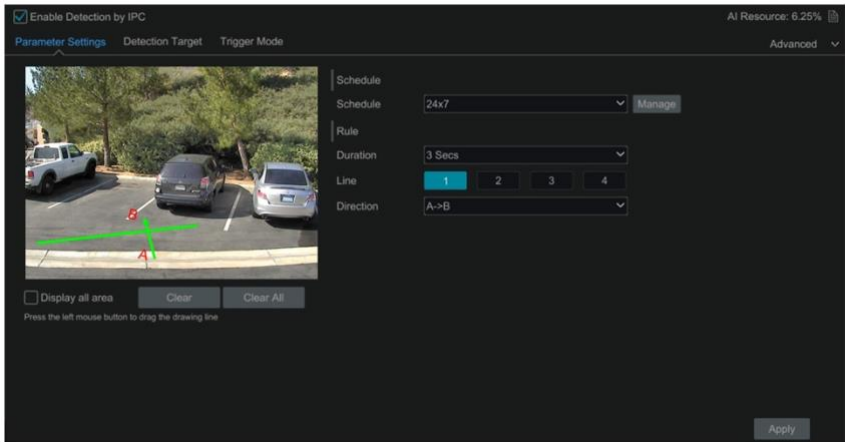
The screenshot shows the configuration interface for 'Successful Recognition' and 'Strange Plate' settings. At the top, there are checkboxes for 'Enable', 'Successful Recognition' (checked), and 'Strange Plate'. Below this, there are tabs for 'Successful Recognition' and 'Strange Plate'. The 'Successful Recognition' tab is active. It includes a 'Plate Group' dropdown set to 'All' with a count of '1', a 'Schedule' dropdown set to '24x7' with a 'Manage' button, a 'Text Prompt' input field, and a 'Voice Prompt' dropdown set to 'None'. There is also an unchecked checkbox for 'Enable alarm output pulse(Access Control)'. Below these settings is a table with columns for 'Trigger General', 'Record', 'Configure', 'Alarm-out', 'Configure', 'Snapshot', 'Configure', 'Camera Name', and 'Preset Name'. The table has four rows of settings: 'Push' (checked), 'Buzzer' (unchecked), 'Pop-up Video' (checked), and 'E-mail' (unchecked). The 'Pop-up Message Box' is also unchecked. The table lists three cameras: IPC01, IPC02, and IPC03, each with a 'None' preset name. An 'Apply' button is located at the bottom right.

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								

- ② Set the successful recognition alarm linkage.
 - Select one or more plate groups and then choose a 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 message, pop-up video, E-mail, and pop-up message box as needed. The alarm linkage settings are similar to the face detection alarm (See [9.1.1 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.

10.3 Line Crossing Detection

1. Tripwire/Line Crossing Detection Configuration:
Alarms will trigger if people or vehicles cross the pre-defined alarm line.
 - ① Click Start→Settings→AI/Event→AI Event →Line Crossing to go to the following interface.



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

Note: Some models may support line crossing detection using the NVR.

- ③ Set a schedule.
- ④ Select the direction.

Direction: You can select A<->B, A->B and A<-B. This represents the direction that the target 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 shown above. Drag the mouse in the image to draw an alert line. Click “Clear” to delete the alert line.
- ⑥ Click “Detection Target” to choose a detection target and the sensitivity of detection. Detection targets include humans, motor vehicles, and non-motor vehicles. Only some cameras can detect humans or vehicles separately. If the camera doesn’t support this function, please skip this step.
- ⑦ 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).
- ⑧ Click “Trigger Mode” to configure the type of alarms triggered by a line-crossing event.
 - Enable or disable “Record”, “Snapshot”, “Push Message”, “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 [11.5.6 Audio](#) for details. To set the light flashing time and frequency of the IPC, please refer to [11.5.7 Light](#) for details.
- ⑨ Click “Apply” to save the settings.

10.4 Intrusion Detection

1. Intrusion Detection Configuration:

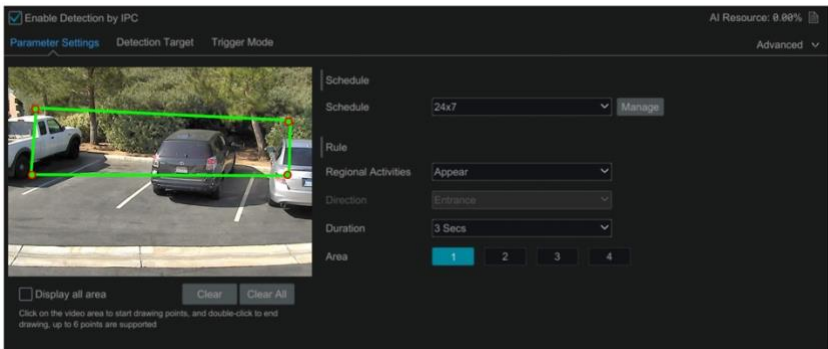
Alarms will trigger if people or vehicles intrude into a pre-defined area.

- ① Click Start→Settings→AI/Event →AI Event→Intrusion to go to the following interface.

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

Note: Some models may support line crossing detection using the NVR.

- ③ Set a schedule.
- ④ Select regional activities. “Appear” or “Cross” can be selected (if your camera doesn’t support region entrance/exiting detection, “Cross” will not be enabled). If “Cross” is selected, you can choose the crossing direction.
- ⑤ Select alarm areas. Up to 4 alarm areas can be set up.
- ⑥ Draw an alarm area for intrusion detection. Refer to the interface shown below. Click around the area where you want to set as the alarm area in the image (the alarm area must be a closed area).



- ⑦ Click “Detection Target” to choose a detection target and set up sensitivity. Detection targets include humans, motor vehicles, and non-motor vehicles.
- Click “Trigger Mode” to configure the type of alarms triggered by an intrusion event.
- Enable or disable “Record”, “Snapshot”, “Push Message”, “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 [11.5.6 Audio](#) for details. To set the light flashing time and frequency of the IPC, please refer to [11.5.7 Light](#) for details.
- ⑧ Click “Copy To” to copy all settings to other cameras.
- ⑨ Click “Apply” to save the settings.

10.5 Abandoned/Missing Object Detection

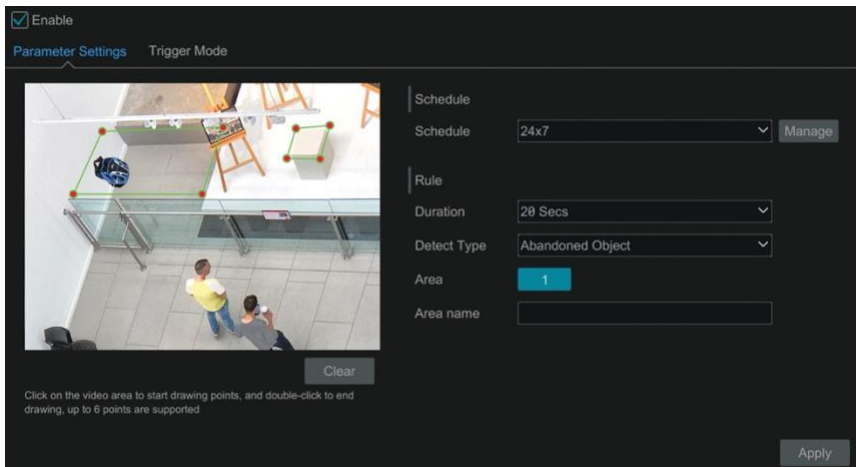
- ① Click Start→Settings→AI/Event→AI Event→Object Abandoned/Missing to go to the following interface.

- ② Set a schedule.
- ③ Select a camera, enable object detection, and set the duration and detection type. There are two detection types: Abandoned object and missing object.

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

Missing object: Alarms will trigger if there are articles missing in the detection area drawn by the user.

- ④ Select an alarm area and area name. A maximum of 4 alarm areas can be set.
- ⑤ Draw an alarm area for object detection. Refer to the interface shown below. Click around the area you want to set as the alarm area in the image (the alarm area should be a closed area). Click the “Clear” to delete an alarm area.



- ⑥ Click “Trigger Mode” to configure the type of alarms triggered by missing/abandoned object detection.
- ⑦ Enable or disable “Record”, “Snapshot”, “Push Message”, “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).
- ⑧ Click “Apply” to save the settings.

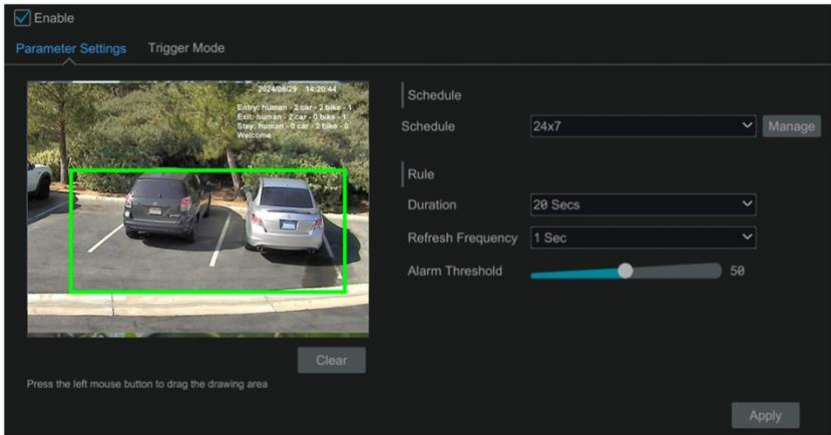
10.6 Crowd Density Detection

Only some cameras may support this function.

1. Crowd Density Configuration:

Alarms will trigger if a crowd's density exceeds the set threshold value in a pre-defined area.

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



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

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

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

- ③ Select an alarm area. Draw an alarm area for crowd density detection. Refer to the interface shown above. Drag the mouse to draw a rectangle area. Click the “Clear” to delete an alarm area.
- ④ Click  to configure the type of alarms triggered by crowd density detection events. Enable or disable “Record”, “Snapshot”, “Push Message”, “Alarm-out”, “Preset”, “Buzzer”, “Pop-up Video,” and “E-mail”. The alarm linkage settings are the same as for face detection alarm (see [9.1.1 Face Detection Settings](#) for details).
- ⑤ Click “Apply” to save the settings.

10.7 Target Counting

Only some IPCs may support this function.

- People counting in a pre-defined area:

This function is used to calculate the number of people entering or exiting a detected area on the video by detecting, tracking and counting the head shapes of people.

Note: Only some specific IPCs may support this function.

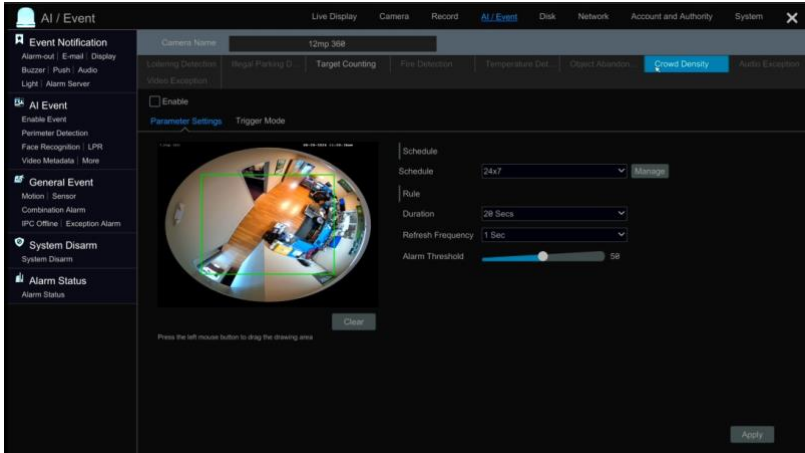
- ① Click Start→Settings→AI/Event→AI Event→Target Counting to go to the following interface.
- ② Select a camera, enable target counting detection, and set a schedule, duration, sensitivity, statistic cycle, enter threshold, departure threshold, and retention threshold.

Statistic cycle: Sets statistic reports to happen Always, Daily, Weekly, or Monthly.

Manual Reset: Click the “Manual Reset” button and the current number of people

counted will be cleared and the statistic cycle will restart.

③ Set an alarm area and entrance direction. Click “Draw Area” and drag the mouse to draw a rectangle area. Drag the rectangle to change its position. Uncheck the “Draw Area” when you finish the drawing. Click “Clear” to clear the area. Click and drag the arrow or the other end of the arrow line to change the people entrance direction.



⑤ Click “Apply” to save the settings.

● Human/Motor Vehicle/Non-Motor Vehicle Counting

The information of humans/motor vehicles/non-motor vehicles can be calculated and sent daily, weekly, and monthly, so that you can receive and analyze these statistics as needed.

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

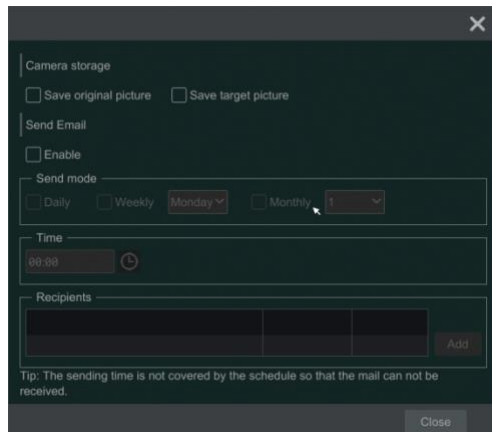
① Click Start→Settings→AI/Event→AI Event→Target Counting to go to the following interface.



- ② Enable line crossing counting.
- ③ Set a schedule.
- ④ Drag the mouse on the small window to draw a crossing line. Click “Clear” to delete the alert line.

Direction: The options are A->B and A<-B. This is the direction of a target crossing over the alert line.

- ⑤ Check “Statistical OSD”, and the statistical information will be displayed on the live view interface.
- ⑥ Set reset information. You can set reset information manually or enable “Auto Reset” as needed.
- ⑦ Click the “Detection Target” tab to set detection targets, this includes humans, motor vehicles, and non-motor vehicles.
- ⑧ Click “Advanced” to bring up the following window. You can select “Save original picture” or “Save target picture”.



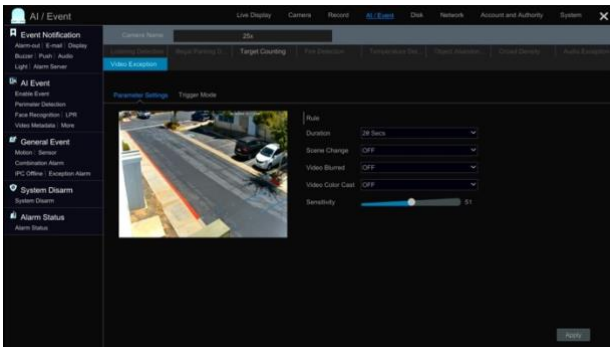
In the above interface, you can send an Email to a specified person daily/weekly/monthly with target counting statistics. Click “Add” to add a recipient”, and then enable “Send Email” and select “Send mode” and time.

- ⑨ Click “Apply” to save the settings.

10.8 Exception Detection

1. Exception Detection Configuration:

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



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

Scene Change: Alarms will be triggered if the view of the camera drastically changes.

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

Video Color Cast: Alarms will be triggered if a rapid color change is detected.

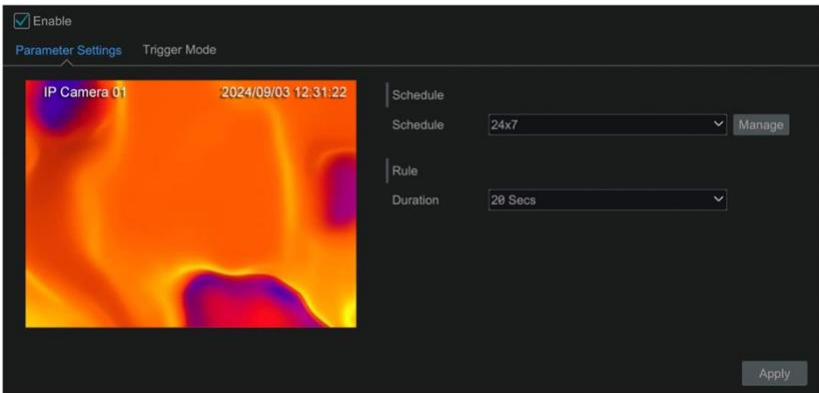
- ③ Set the sensitivity for the exception detection.
- ④ Click “Trigger Mode” to configure exception alarm linkage items. Enable or disable “Record”, “Snapshot”, “Push Message”, “Alarm-out”, “Preset”, “Buzzer”, “Pop-up Video,” and “E-mail”. The alarm linkage settings are the same as the face detection alarm (see [9.1.1 Face Detection Settings](#) for details).
- ⑤ Click “Apply” to save the settings.

10.9 Fire Detection

Fire detection is available when security thermal cameras are connected.

Fire Detection: Alarms will trigger when the camera detects a fire source.

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



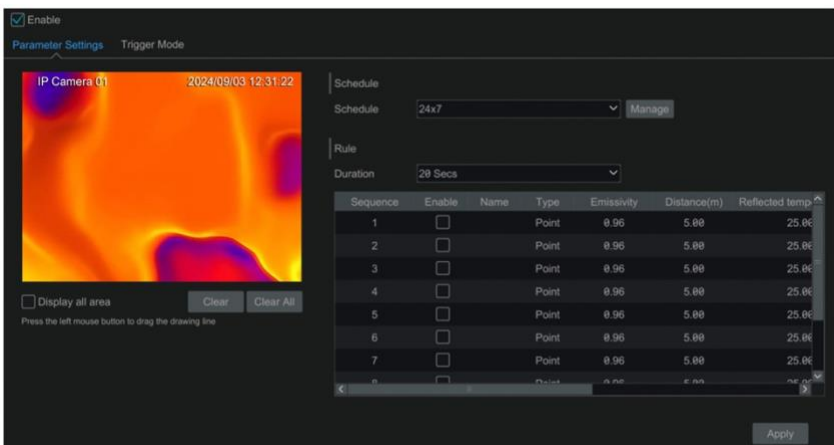
- ② Set the schedule and the alarm duration time.
- ③ Click “Trigger Mode” to configure exception alarm linkage items. Enable or disable “Record”, “Snapshot”, “Push Message”, “Alarm-out”, “Preset”, “Buzzer”, “Pop-up Video”, “Pop-up Message Box,” and “E-mail”. The alarm linkage settings are the same as the face detection alarm (see [11.1 Sensor Alarm](#) for details).
- ④ Click “Apply” to save the settings.

10.10 Temperature Detection

Temperature detection is available when security thermal cameras are connected.

Temperature Measurement: When the temperature of a pre-defined point/line/area exceeds the configured threshold an alarms will trigger.

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



- ② Set the schedule and the alarm duration time.

- ③ Set the thermography rule. Select a 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°C and check alarm output. Then alarms will be triggered when the average temperature of the target is higher than 100°C.

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

Point setting: 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 setting: 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.

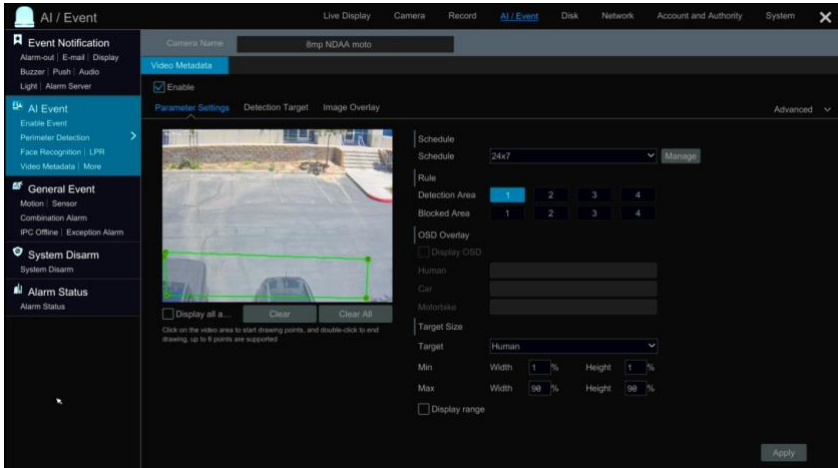
Area setting: Click around the area where you want to set as the alarm area on the image (the alarm area should be a closed area). To ensure the accuracy of temperature measurement, it is recommended to set not more than two areas at the same time.

- ⑤ Click "Trigger Mode" to configure exception alarm linkage items. Enable or disable "Record", "Snapshot", "Push Message", "Alarm-out", "Preset", "Buzzer", "Pop-up Video", "Pop-up Message Box" and "E-mail". The alarm linkage settings are the same as the face detection alarm (see 11.1 Sensor Alarm for details).
- ⑥ Click "Apply" to save the settings.

10.11 Video Metadata

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.



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 in the pre-defined detection area will be counted and captured.

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

To set detection area: Select the number of areas and then set up a detection area. Click around to make a closed box on the area you want to set as the alarm area.

To set blocked areas: Select the number of blocked areas and then set the blocked area up using the same method as above.

Display OSD: If enabled, the statistical information of humans, motor vehicles, and non-motor vehicles will be displayed on the screen. The statistical OSD information can be customized as needed.

④ Set the reset information. You can choose auto reset or manual reset as needed.

⑤ Advanced settings. Click “Advanced” to enter the advanced setting interface. Select the recognition mode as needed. You can select interval mode or instant mode.

Interval mode: the system will push captured pictures to the live view interface according to a set time interval.

Instant mode: the system will push captured pictures immediately once a target is detected.

⑥ Set a detection target and sensitivity.

⑦ Select the attribute information for the target. When a target is detected, the information you select will be displayed under the captured image.

⑧ Click “Apply” to save the settings

11 Intelligent Analytics

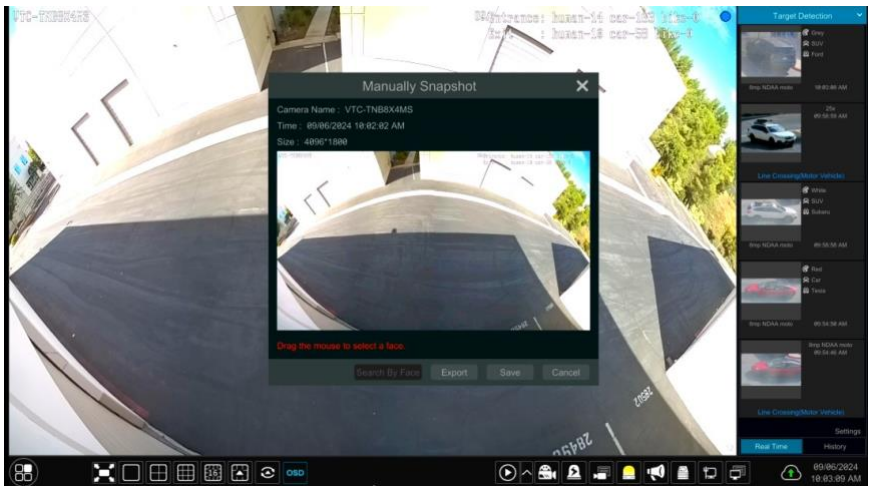
11.1 Target Detection View

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

11.1.1 Human Body/Vehicle Detection View

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

- ① Enable the Line crossing/Intrusion/Target counting function of cameras or the NVR, draw a line or area and choose a detection target (see [9.3 Line Crossing Detection](#), [9.4 Intrusion Detection](#) and [9.7 Target Counting](#) for details).
- ② Go to the 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 multiple channels as shown below. Click a captured picture on the right of the live interface to see snapshot detail information, such as snapshot time, camera, event type, and target type.



Click “More” to bring up a dropdown list. You can export 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.

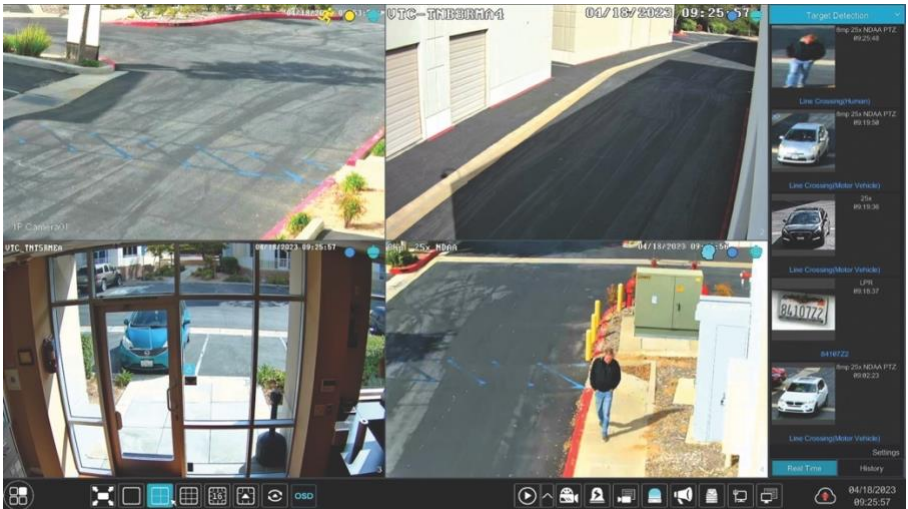
11.1.2 Face Detection/Match View

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

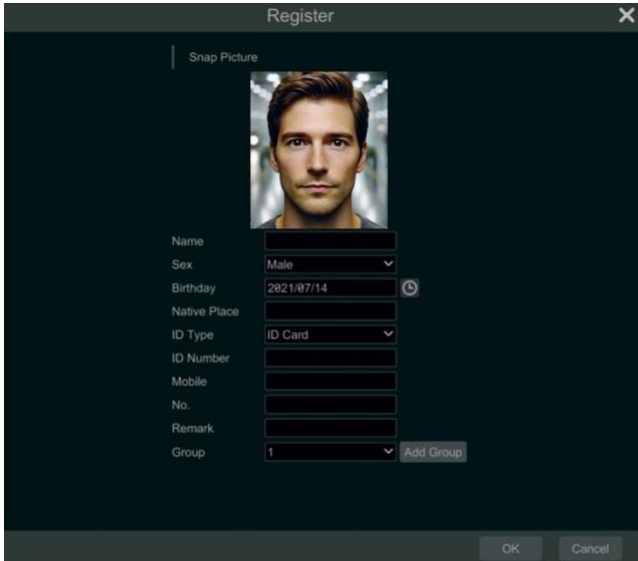
The setting steps are as follow:

- ① Enable the face detection function (see [9.1.1 Face Detection Settings](#) for details).
- ② Enable the face recognition function and set up alarm linkage items (see [9.1.3 Face Recognition Settings](#) for details).
- ③ Go to the live view interface and click on a channel with face detection enabled. This will bring a toolbar under the channel. Then click  to go to the target detection interface for 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 multiple channels as shown below.

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



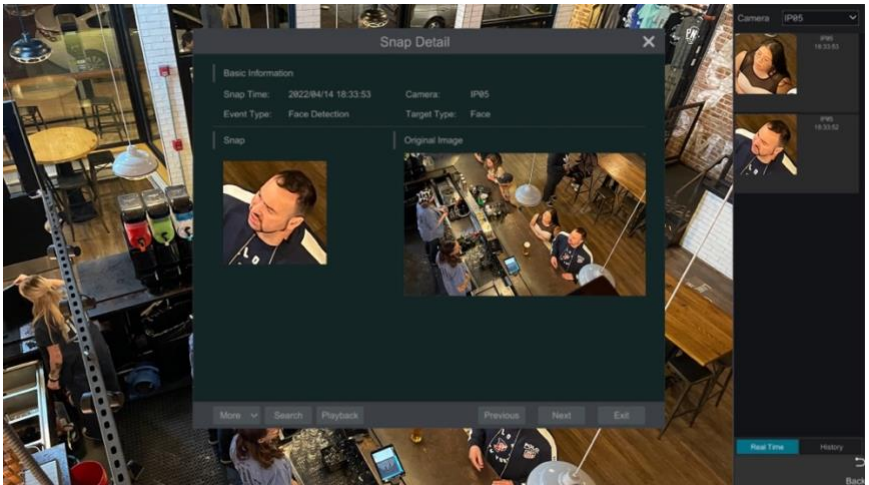
For unknown faces, you can select the captured face picture and click  under it to register the face to the database (see the following picture); click  to quickly go to the smart face search interface where you can search for matching face picture information; click  to quickly go to the smart face playback interface; click  to view snapshot details.



The 'Register' dialog box is used for adding a new face to the system. It features a 'Snap Picture' section with a preview of a man's face. Below this, there are several input fields: Name, Sex (set to 'Male'), Birthday (2021/07/14), Native Place, ID Type (set to 'ID Card'), ID Number, Mobile No., Remark, and Group (set to '1'). An 'Add Group' button is located next to the Group field. At the bottom right, there are 'OK' and 'Cancel' buttons.

Before registering target face pictures, please add groups for them in advance (see [9.1.2 Face Database Management](#) for details).

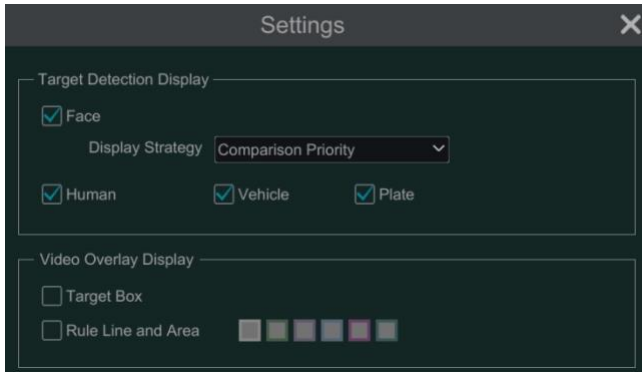
After face pictures are registered, the system will compare them automatically once the corresponding faces are captured next time. Refer to the following picture.



Double click a face picture to see its snapshot details, such as the zoomed in snapshot of the face, the original full image, time of the snapshot, and the camera the face picture came from. Click "more" and then a dropdown list will appear.

Click “Register” to register the current snapshot. Click “Search” to go to the face search interface. Click “Playback” to go to the playback interface. Click “Export” to export the snapshot’s details. Click “Information” to view the face ID.

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

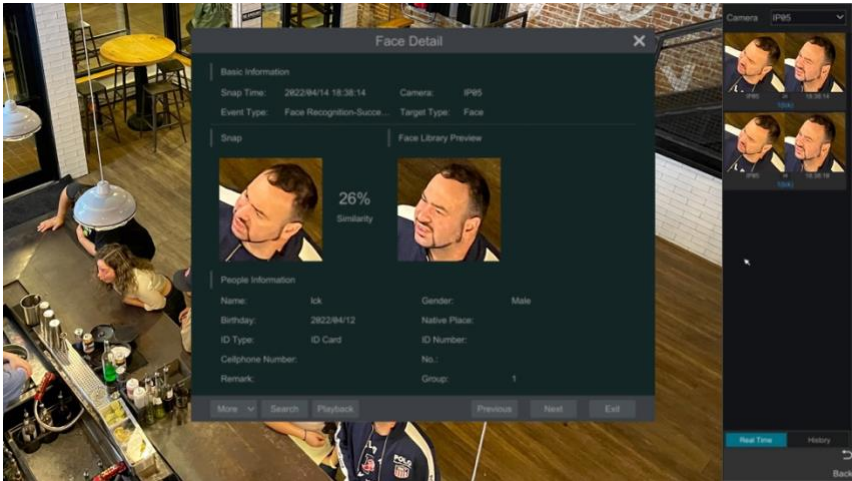


Target Detection Display: You can enable Face, human body, vehicle, or license plate event detection. If disabled, captured target pictures for that type of event will not be displayed under the target detection tab in the live view interface.

Display Strategy: There are two options, Comparison priority and only comparison

1. **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 configured for line crossing detection and the detection area of an intrusion detection setup displayed on the screen. You can select the color of the rule line and area as needed.



When captured face pictures are successfully recognized, click the picture on the right to bring up a face detail window as shown above. In this window, you can see the captured face picture, the picture it was matched against from the face library, and other relevant information. You also can view the original image, search image by snapshot, playback by snapshot, and export the face details by clicking the “More” button.

Additionally, you can view a historical list of captured face pictures and face match information in the face match interface by clicking the “History” tab. Besides registering face pictures in the live view interface, you can also add target face pictures in the face database interface.

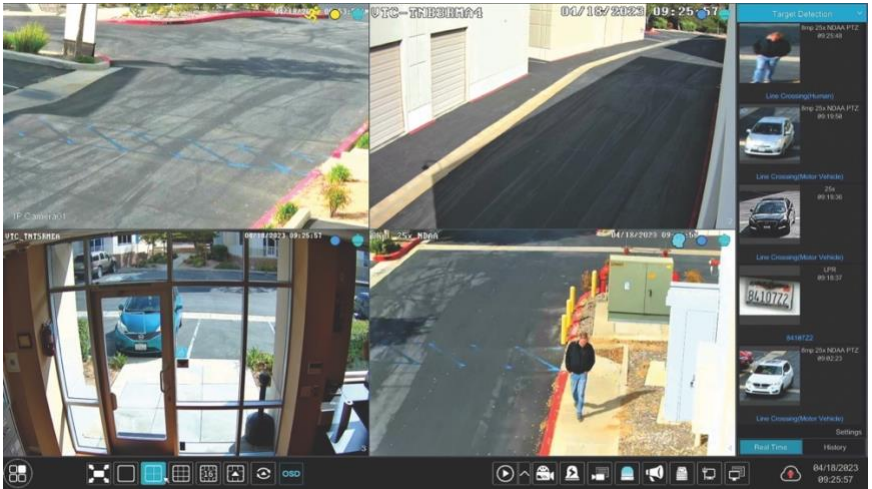
Note: if you enter a remark when adding a face picture to the face database, instead of the name, the remark information will be shown under the face library picture after successful recognition.

11.1.3 License Plate Detection/Recognition View

You can only capture and match license plates when a LPR camera is added and enabled. The setting steps are as follows.

- ① Enable the plate detection function (See [9.2.1 License Plate Detection Settings](#) for details).

Then you can see 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.

The 'Add' dialog box is shown with the following fields and options:

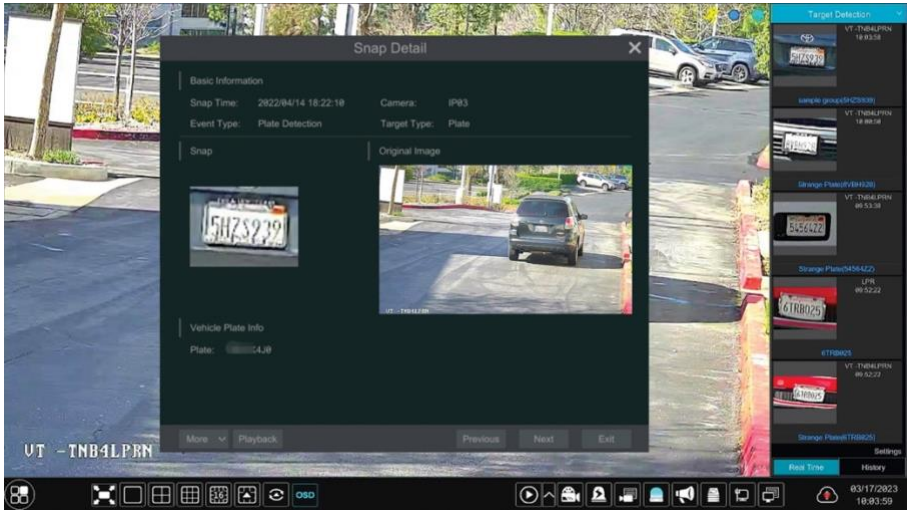
- Plate:
- Vehicle Type:
- Vehicle Owner:
- Mobile:
- Group: 1

At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Click  to view captured information. Click  to quickly go to the vehicle search interface. You can search for matched plate information in this interface.

Click  to go to the smart playback interface.

- ② Enable the license plate recognition function and set alarm linkage items (see [9.2.3 License Plate Recognition Settings](#) for details).
- ③ Go to the 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 for multiple channels as shown below. When a plate is captured, it will be displayed on the right panel.

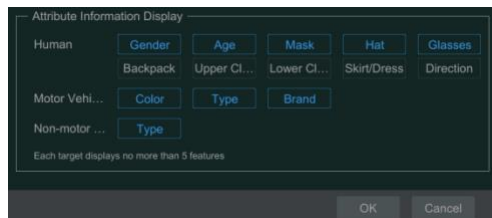


Click a captured plate picture and it will bring up a window with detailed information. You can view snapshot pictures, original pictures, snapshot time, camera, etc. Click “More” to view the ID information of the target and export the captured picture. Click “Search” to go to the vehicle search interface.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

11.1.4 Object Attribute View

- ① Enable the video metadata function and then select a detection target and display attributes (see [9.11 Video Metadata](#) for details).
- ② Go to the live view interface and click on an AI camera channel (video metadata function is supported). This will bring up 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 for multiple channels.

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.



Click a captured picture to view details. In the detail interface, you can view

captured pictures, original pictures, object attributes, etc.

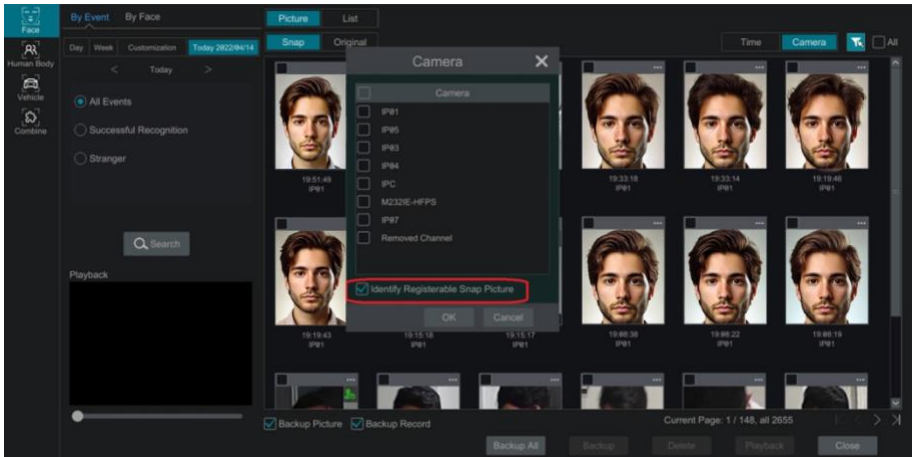
11.2 Smart Search

11.2.1 Face Search

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

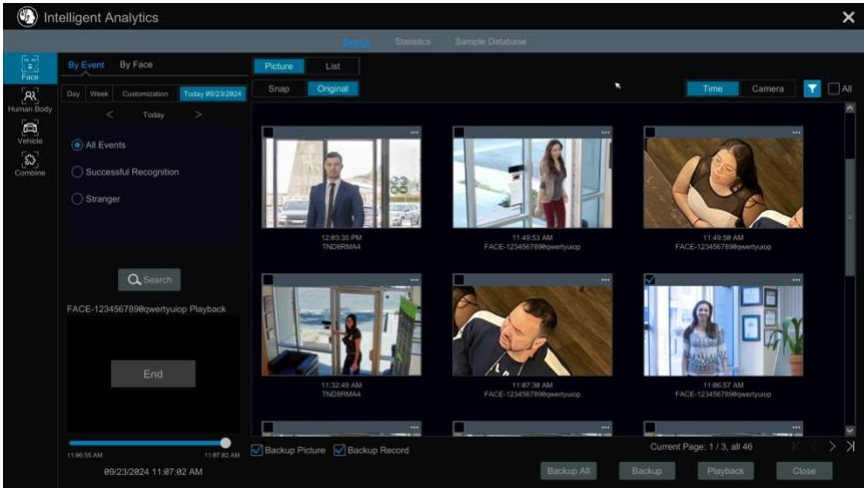
➤ Face Search by Event

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.” Pictures that can be added to the face database will be marked with a green icon **after clicking “OK”**.
- ③ Select either “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 a searched face picture to play it back in a small window; select a face picture and click “Backup” to export it.

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

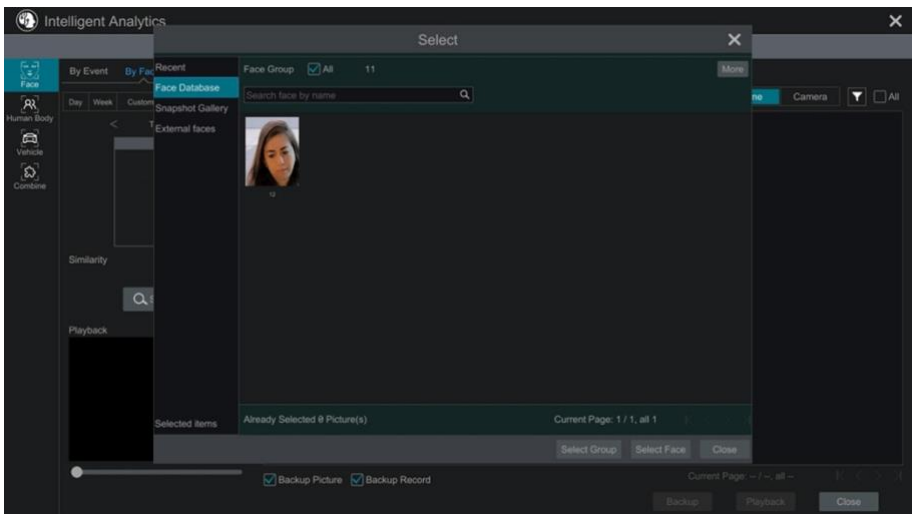


Click “List” to view the snapshot information list. Click  to view detailed information; click  to back up the image.

➤ Face Search by Face

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

① Click  to add a target face that has been added from either recently added faces, the face database, the snapshot gallery, or external faces. You can add and search one or multiple face pictures. (Below shows a single face picture as an example)



To add target faces that were recently added:

- a. Choose the face.
- b. Click “Select Face”.

To add target faces from the face database:

- a. Click “More” to choose groups.
- b. Select a target face and click “Select Face”.

To add target faces from the snapshot gallery:

- a. Select time and click “More” to choose cameras.
- b. Click “Search”.
- c. Check a face and click “Select Face”.

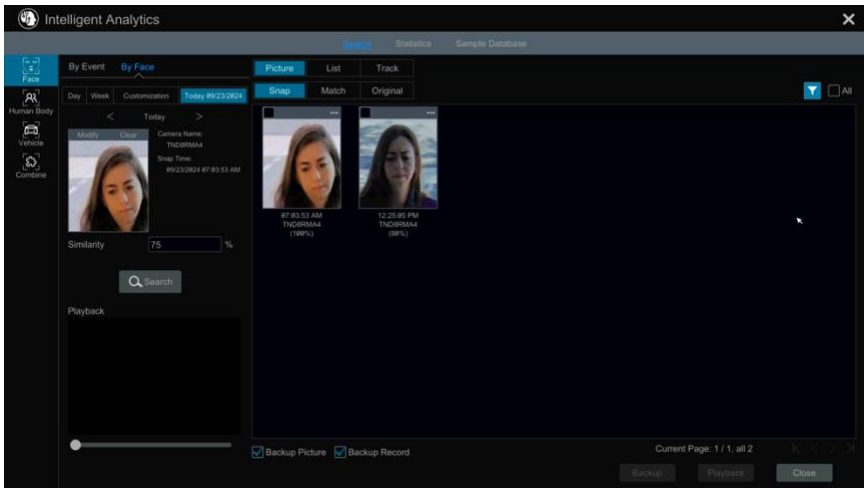
To add target faces from an external storage source:

- a. Save a target face to a USB storage device and insert the device into the USB interface on the NVR.
- b. Select “External Face” to import the face in this interface.

② Set similarity and then click “Search”.

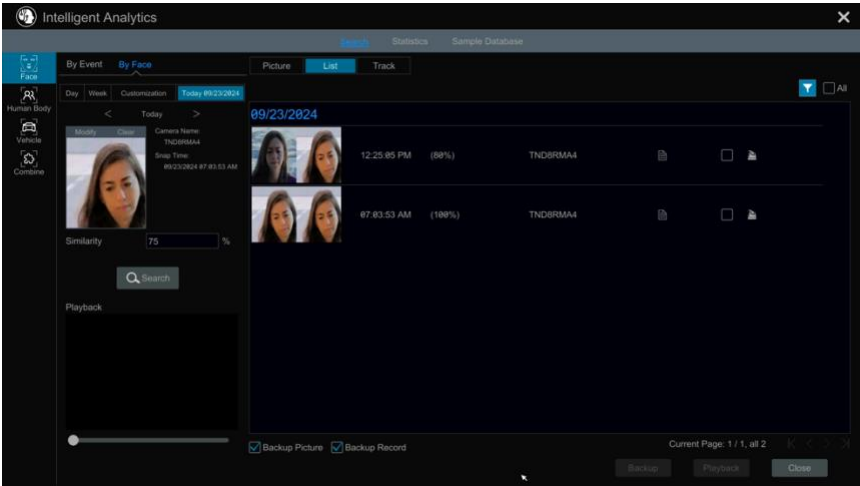
③ Click the searched image to play the recordings in a small window.

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



● View Image by List

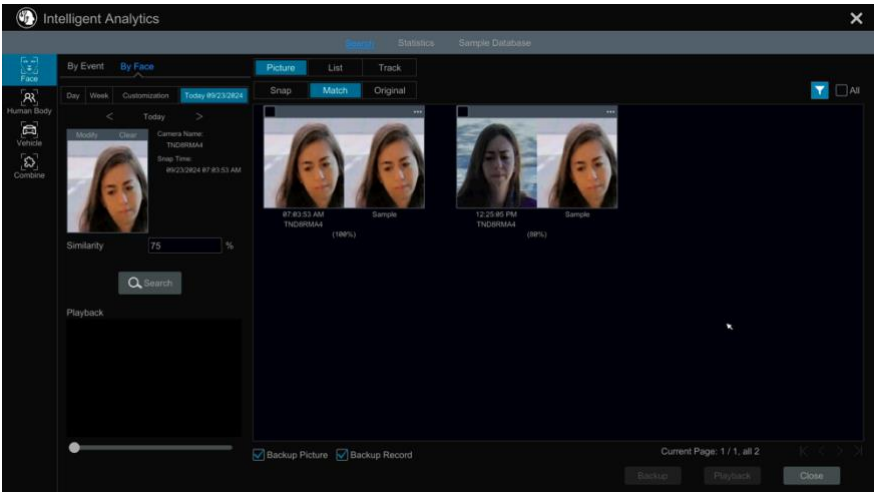
Click the “List” tab to view images by time as shown below.



Click an image to play its recording. Click  to view detailed information related to the compared target face.

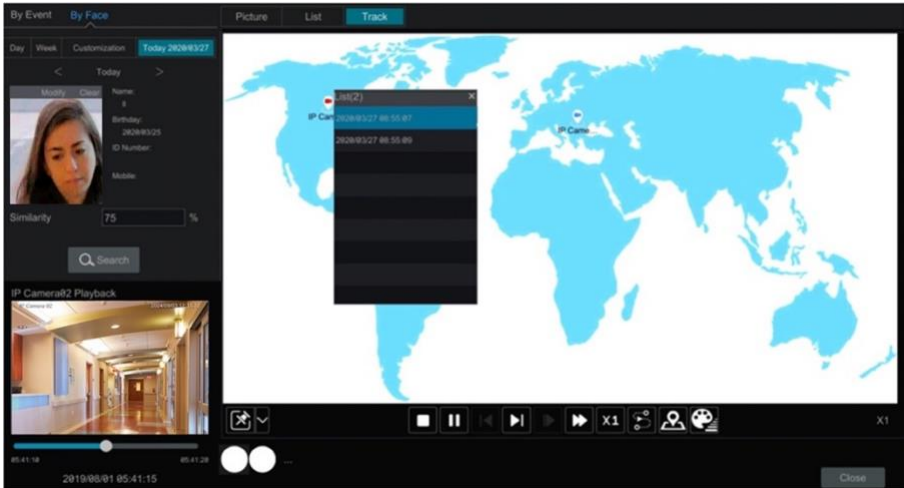
- View Match Images

Click the “Match” tab to view matched images as shown below.



11.2.2 Track Playback

Select “Track” to go to the following interface.



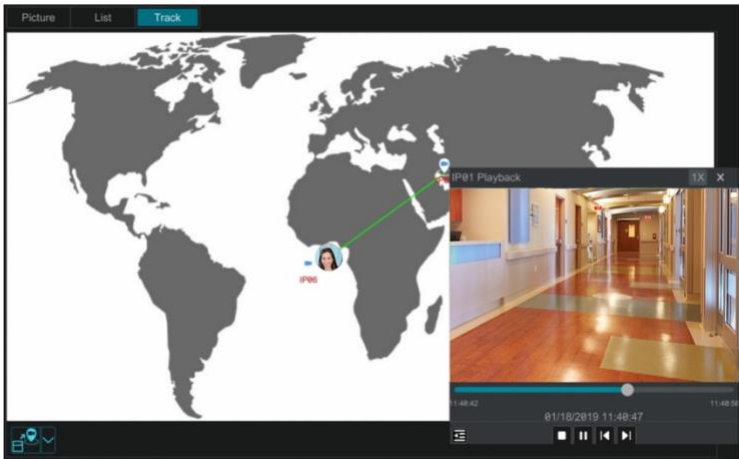
Note: Tracking information only works when a person was detected by two or more cameras.

Descriptions of buttons on the track interface

	Fixed Window		Frame
	Followed Window		Fast Forward (x2;x4)
	Exchange Window		Normal Speed
	Stop		Start/Stop Track
	Play		Edit Map
	Previous		Edit Color
	Next		

Click on the camera name and then an event list will appear. Click an item to play its recording.

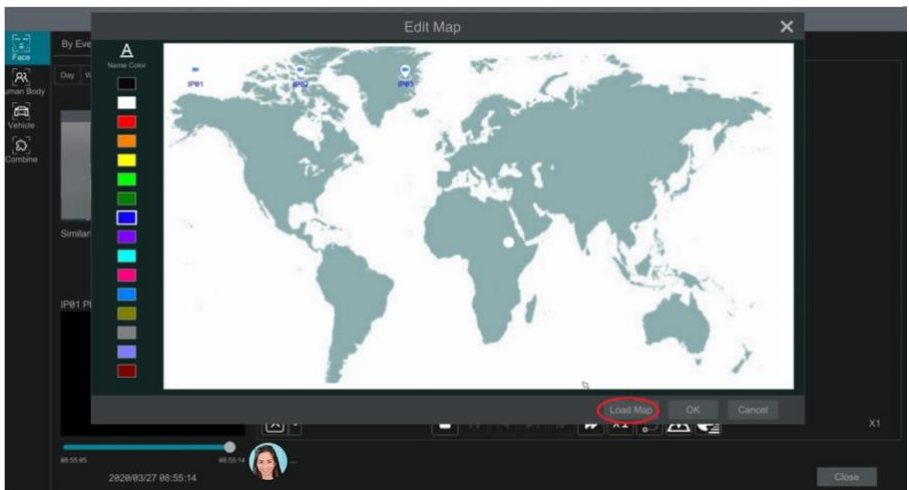
Click the button beside the fixed window icon to show the “Followed Window” and “Exchange Window” icons. A small playback window will float on the map window by clicking “Followed Window” as shown below.



Click **1X** to switch play speed between 1x and 2x. Click  to view the event list. Click an item to play the 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 on the map to change their locations. Choose a color on the left color list to set your favorite color for camera names.

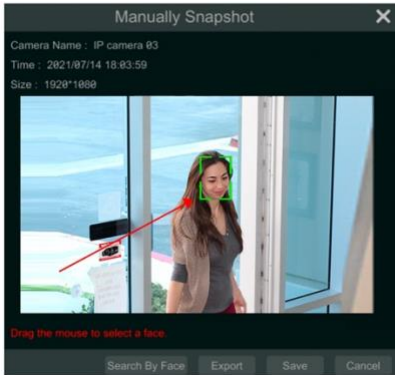
Load Map: ① Save the map to a USB storage device and then insert the USB

storage device into the NVR. ② Click the “Load Map” button to upload the map.

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

11.2.3 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.

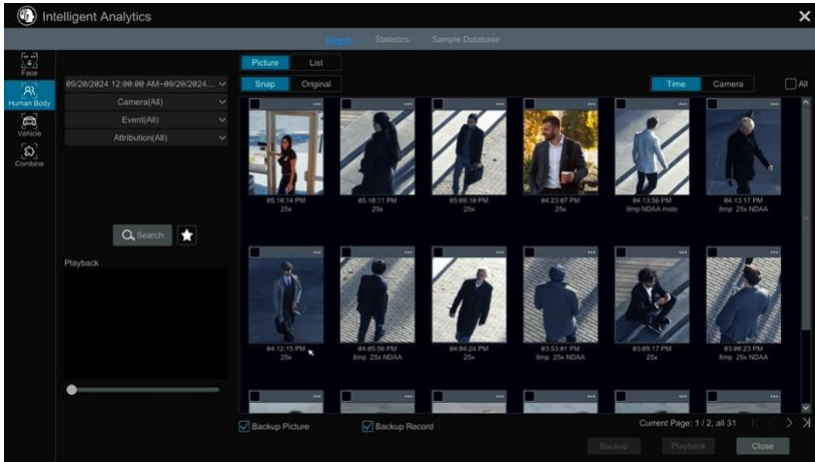


Drag the mouse to select a face and then click “Search by Face” to go to the search by face interface. You can see its snapshots, matched pictures, original pictures, and so on by clicking the corresponding tab.

11.2.4 Human Body Search

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

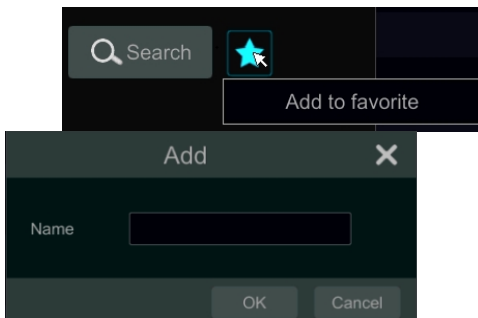
Select the search time, camera, and event and then click “Search” to view the searched pictures.



You can also select attributes to help filter people (like gender, age, mask-wearing status, glasses-wearing status, color of clothes, etc.)

Click a searched picture to play its recording in a 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 “Original” to view the captured full size original picture. 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 that favorite group. Then, you can quickly view these pictures by clicking  and choosing the group name.



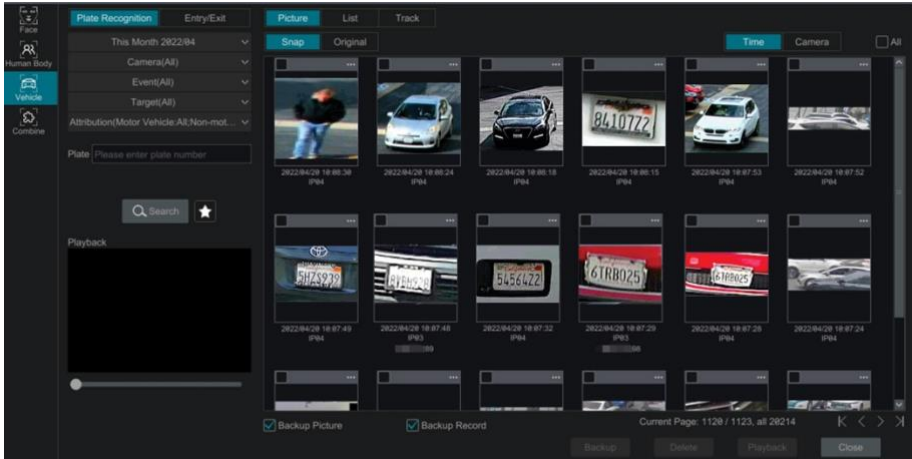
11.2.5 Vehicle Search

- ① Click Start→ Intelligent Analytics→Smart 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: You can select Intrusion, Line Crossing, Target Counting, Plate Detection, Plate Match-Successful Recognition, and Plate Match-Strange Plate.

Attribution: Vehicle or non-vehicle attributes can be selected as needed. For example, you can search vehicles according to the color, brand or type.

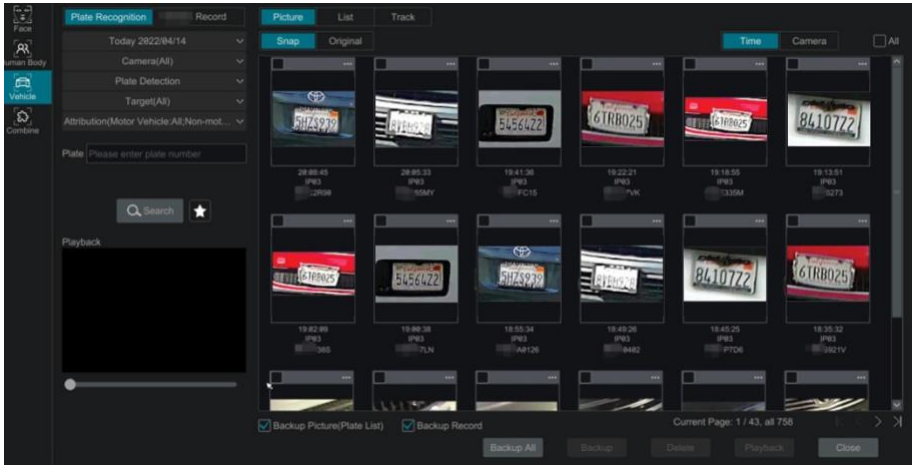
You can view face pictures by time or by camera.



Click a searched vehicle picture to play its recording in a small window. 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 original full-size pictures; click “List” to view the snapshot information list. Click  to view detailed information; click  to back up the image.

Select “Plate Detection” or “Plate Recognition” to view plate images. You can also enter a plate number to search through plate pictures. You can track vehicles this way.



Click “Track” to view tracking information for a vehicle.

Note: Only one plate can be tracked at a time and two or more LPR cameras must have detected this license plate to track it.

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

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

11.2.6 Combination Search

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

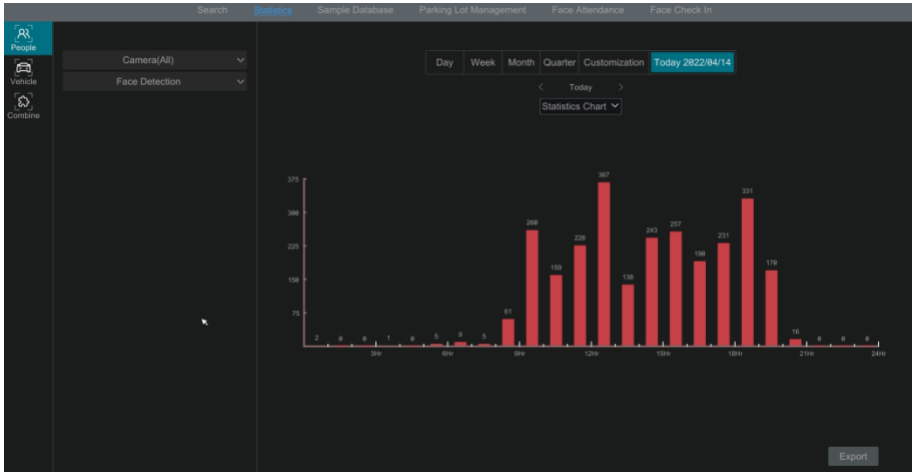
- ① Click “Combine”.
- ② Select from search time, camera, event, and vehicle as needed.

Click a searched picture to play its recording in a 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.

11.3 View Statistical Information

Click Start→ Intelligent Analytics→Statistics to go to the following interface. In this interface, you can view the people and vehicle statistical information or you can customize the statistical information.



View People Information:

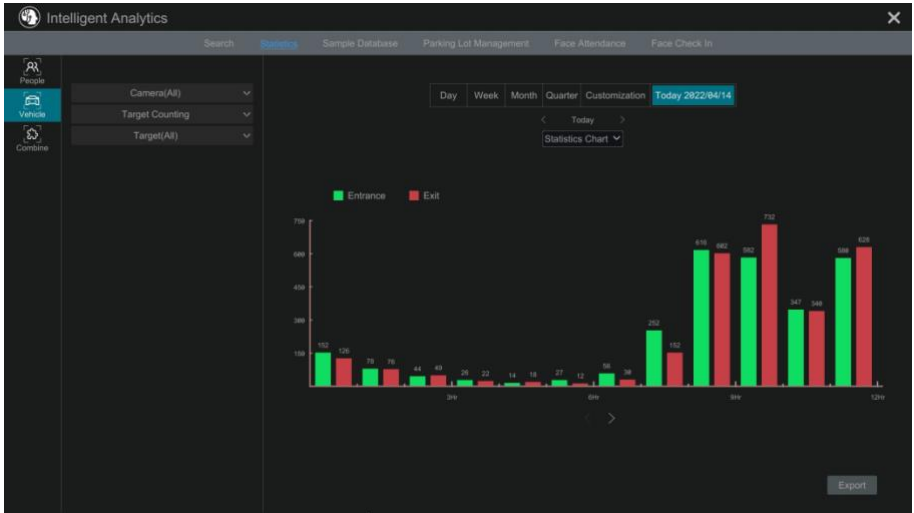
Note: People Information includes face and full-body information.

- ① Select a time.
- ② Select cameras.
- ③ Select events as needed, such as face detection, face recognition, intrusion, 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 this information.

View Vehicle Information:

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



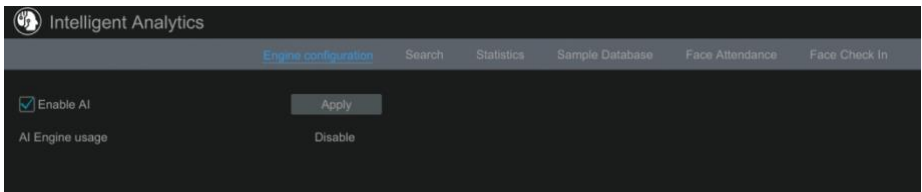
If “Remove duplicate license plate numbers” is checked, duplicate details of the same license plate in the same day will not be displayed in the chart.

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

11.4 Enabling AI Mode

Only some models support this function.

For these models, an IP camera without AI functionality added to the NVR may utilize AI functions like face detection, line crossing, and 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.



12 General Event Management

12.1 Sensor Alarm

To completely configure sensor alarm settings, enable sensor alarms for each camera and then set up the alarm handling of each 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	☐ Configure
Local-2	Sensor2	24x7	NO	ON	30 Secs	☐ Configure	☐ Configure	ON	☐ Configure
Local-3	Sensor3	24x7	NO	ON	30 Secs	☐ Configure	☐ Configure	ON	☐ Configure
Local-4	Sensor4	24x7	NO	ON	30 Secs	☐ Configure	☐ Configure	ON	☐ Configure
Local-5	Sensor5	24x7	NO	ON	30 Secs	☐ Configure	☐ Configure	ON	☐ Configure
Local-6	Sensor6	24x7	NO	ON	30 Secs	☐ Configure	☐ Configure	ON	☐ Configure
Local-7	Sensor7	24x7	NO	ON	30 Secs	☐ Configure	☐ Configure	ON	☐ Configure
Local-8	Sensor8	24x7	NO	ON	30 Secs	☐ Configure	☐ Configure	ON	☐ Configure

- ② Select an alarm type (NO or NC) according to the trigger type of the sensor.
- ③ Enable sensor alarms for each camera and select a 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 desired.
- ⑤ Click “Apply” to save these settings.

Configuration steps for the above-mentioned alarm linkages are as follows.

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

Record: Enable this and then the “Trigger Record” window will pop up automatically (you can also click the “Configure” button to bring up the window). Select a camera on the left side and then click  to set the camera as a trigger camera. Select a trigger camera on the right side and then click  to cancel the trigger camera. Click “OK” to save settings. The trigger cameras will record automatically when the sensor alarm is triggered.

Snapshot: Enable this and then the “Trigger Snapshot” window will pop up automatically. Configure the trigger camera in this window. Trigger cameras will capture images automatically when the sensor alarm is triggered.

Push: Enable this and choose ON or OFF. If it is ON, the system will send

messages when the sensor alarm is triggered.

Alarm-out: Enable this and the “Trigger Alarm-out” window will pop up automatically. Configure trigger alarm-out settings in this window. The system will trigger an alarm-out automatically when the sensor alarm is triggered. You need to set up the delay time and schedule for the alarm outputs. See [11.5.1 Alarm-out](#) for details.

Preset: Enable this and the “Trigger Preset” window will pop up automatically. Configure the trigger preset of each camera. To add presets, please see [6.2 Preset Setting](#) for details.

Buzzer: if enabled, the system will begin to buzz when a sensor alarm is triggered. To set the delay time of the buzzer, please see [11.5.4 Buzzer](#) for details.

Pop-up Video: After enabling, the system will bring up the corresponding video automatically when a sensor alarm is triggered. To set the duration time of the video, please see [11.5.3 Display](#) for details.

Pop-up Message Box: if enabled, the system will bring up a message box with information on the corresponding alarm automatically when a sensor alarm is triggered. To set the duration time of the message box, please see [11.5.3 Display](#) for details.

E-mail: if enabled, the system will send an e-mail when the sensor alarm is triggered. Before you enable the email, please configure the recipient's e-mail address first (see [14.1.5 E-mail Configuration](#) for details).

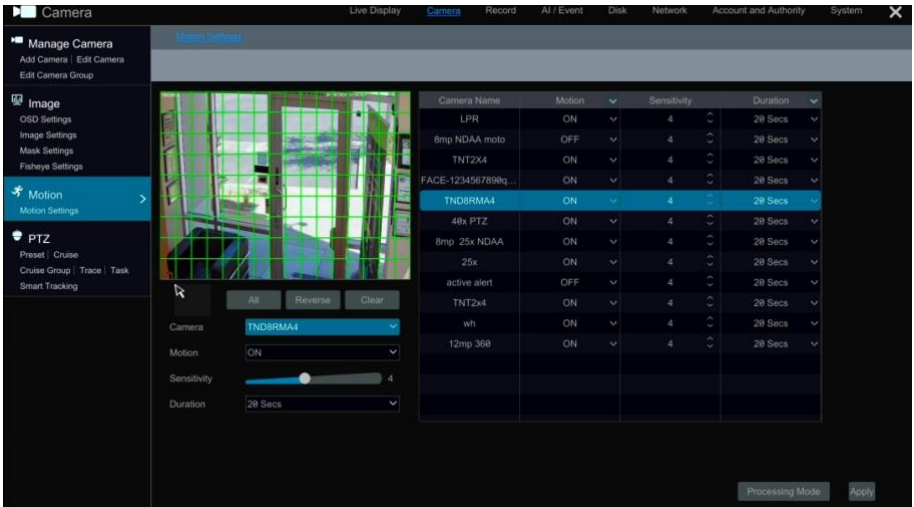
Virtual alarm: This function should be used with an API server. If you want to enable it, please make sure the API Server is enabled first (Start→Network→Port) and then set the authentication as “Digest”.

12.2 Motion Alarm

Motion Alarm: when there is motion in a specified area, it will trigger an alarm. You must enable motion detection for each camera and then set the alarm handling for each camera to complete configuration.

12.2.1 Motion Configuration

- ① Click Start→Settings→Camera→Motion Settings to go to the following interface.



- ② Select a camera, enable motion detection, and set the sensitivity/duration for the camera.

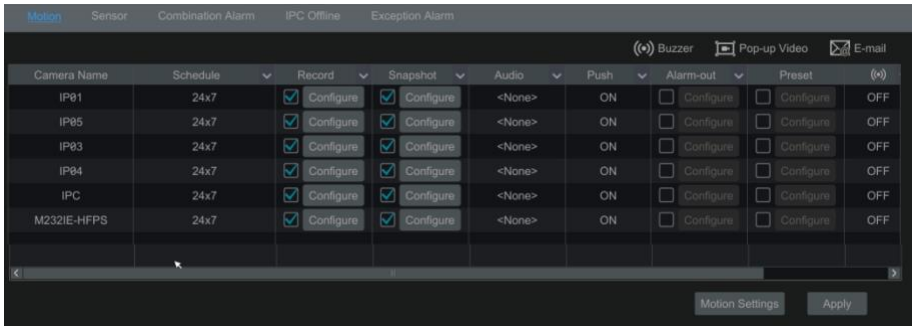
Sensitivity: the higher the value is, the more sensitive it is to motion. You should adjust the value according to the conditions of the scene since the sensitivity is influenced by color and time (day or night).

Duration: refers to the interval of time between adjacent motion detections. For instance, if the duration is set to 10 seconds, once the system detects motion, it will trigger the alarm and won't detect any other motion (specific to that camera) for 10 seconds. If there is another motion event during this period, it will be considered continuous movement; otherwise, it will be considered as a single motion event.

- ③ Drag across a camera image to set up its motion area. You can set multiple motion areas. Click “All” to set the whole camera image as the motion area. Click “Reverse” to swap motion areas with non-motion areas. Click “Clear” to clear all motion areas.
- ④ Click “Apply” to save settings. Click “Processing Mode” to go to the alarm handling configuration interface for motion alarms.

12.2.2 Motion Alarm Handling Configuration

- ① Click Start→Settings→Alarm→Motion Alarm to go to the following interface.

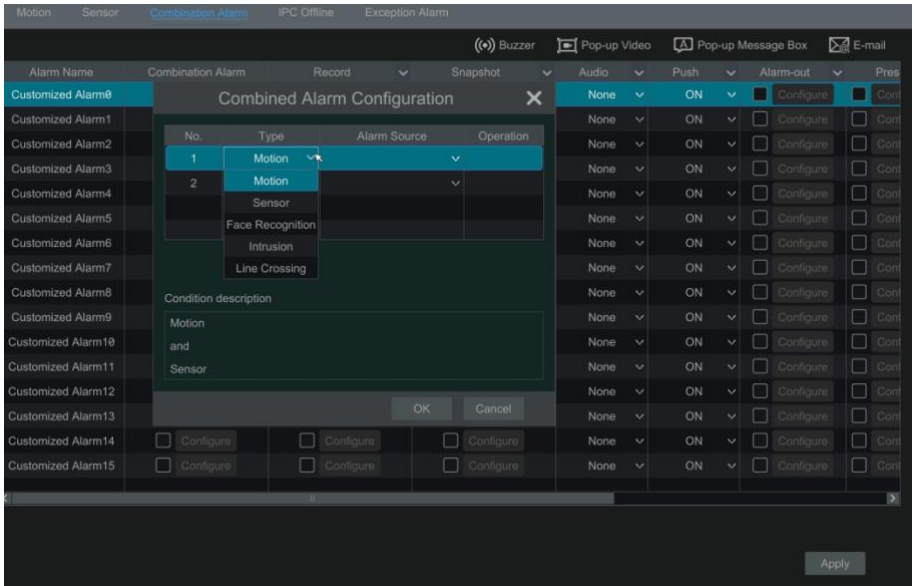


- ② Enable or disable “Record,” “Snapshot,” “Push,” “Alarm-out,” “Audio,” “Preset,” “Buzzer,” “Pop-up Video,” and “E-mail”. The alarm handling settings for motion alarms is similar to that of sensor alarms (see [11.1 Sensor Alarm](#) for details).
- ③ Click “Apply” to save the settings. You can click “Motion Settings” to go to the motion configuration interface.

12.3 Combination Alarm

- ① Click Start→Settings→Alarm →Combination Alarm to go to the following interface.
- ② Customize combination alarms. Set an alarm name and click “Configure” under the Combined Alarm Configuration item (motion/sensor/intrusion/face recognition/line crossing). Then select an alarm type and alarm source. Finally, click “OK” to save the settings.

(Only some models support face recognition)



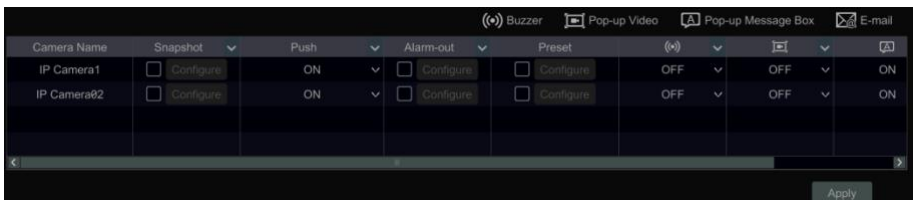
③ Enable or disable “Record”, “Snapshot”, “Push”, “Alarm-out”, “Preset”, “Buzzer”, “Audio”, “Pop-up Video,” and “E-mail”. The alarm handling setting of combination alarm is similar to that of sensor alarms (see [11.1 Sensor Alarm](#) for details).

Click “Apply” to save the settings.

12.4 Exception Alarm

12.4.1 IPC Offline Settings

- ① Click Start→Settings→AI/Event→IPC Offline Settings to go to the interface shown below.
- ② Enable or disable “Snapshot”, “Push”, “Alarm-out”, “Preset”, “Buzzer”, “Pop-up Video”, “Pop-up Message Box,” and “E-mail”. IPC Offline Settings are similar to that of sensor alarms (see [11.1 Sensor Alarm](#) for details).
- ③ Click “Apply” to save the settings.



12.4.2 Exception Alarm Settings

- ① Click Start→Settings→AI/Event→Exception Alarm to go to the interface shown below.

Event Type	Push	Alarm-out	Buzzer	Pop-up Message Box	E-mail
IP Address Conflict	ON	☐ Configure	ON	ON	OFF
Disk IO Error	ON	☐ Configure	ON	ON	OFF
Disk Full	ON	☐ Configure	ON	ON	OFF
No Disk	ON	☐ Configure	ON	ON	OFF
Illegal Access	ON	☐ Configure	ON	ON	OFF
Network Disconnection	ON	☐ Configure	ON	ON	OFF
HDD is pulled out	ON	☐ Configure	ON	ON	OFF
Alarm Server Offline	ON	☐ Configure	ON	ON	OFF

Apply

- ② Enable or disable “Push”, “Alarm-out”, “Buzzer”, “Pop-up Message Box,” and “E-mail”. Exception handling settings are similar to that of sensor alarms (see [11.1 Sensor Alarm](#) for details).
- ③ Click “Apply” to save the settings.

12.5 Alarm Event Notification

12.5.1 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 a delay time, the schedule, and the type of each alarm-out. You can click “Edit Schedules” to edit the schedules (see [7.1.2 Schedule Settings](#) for details).
- ③ Click “Apply” to save the settings. You can click “Test” to test the alarm output.

12.5.2 E-mail

Click Start→Settings→AI/Event→Event Notification→E-mail to go to the e-mail configuration interface. Set up e-mail addresses for recipients. See [14.1.5 E-mail Configuration](#) for details.

12.5.3 Display

Click Start→Settings→AI/Event→Event Notification→Display to go to the display configuration interface. Set the duration desired for pop-up video windows and pop-up message boxes. If your device supports two outputs, please set the output you want the video or message window to pop up on. After that, click “Apply” to save the settings.

The screenshot shows two configuration sections. The top section, titled "Pop-up Video", has a "Duration" dropdown set to "10 Secs" and an "Output" dropdown set to "Main Output". The bottom section, titled "Pop-up Message Box", has a checked checkbox for "Don't show later" and a "Duration" dropdown set to "10 Secs". An "Apply" button is located at the bottom right of the interface.

12.5.4 Buzzer

Click Start→Settings→AI/Event→Event Notification→Buzzer to go to the buzzer configuration interface. Set the delay time desired for the buzzer and then click “Apply” to save the setting. You can click “Test” to test the buzzer.

The screenshot shows the "Buzzer" configuration interface. It features a "Delay" dropdown menu set to "5 Secs". At the bottom, there are two buttons: "Test" and "Apply".

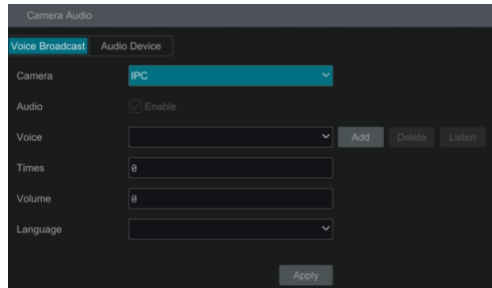
12.5.5 Push Text

Click Start→Settings→ AI/Event →Event Notification→Push Text to go to the interface shown below. Check “Enable”, select a schedule, and then click “Apply” to save your settings. If the Push Server is online, it will push alerts to mobile app users according to a set schedule.

The screenshot shows the "Push Text" configuration interface. It includes a checked checkbox for "Enable" and a "Push Schedule" dropdown menu set to "24x7". At the bottom, there are three buttons: "Schedule Management", "Test", and "Apply".

12.5.6 Audio

Click Start→Settings→ AI/Event →Event Notification→Audio to go to the interface shown below.



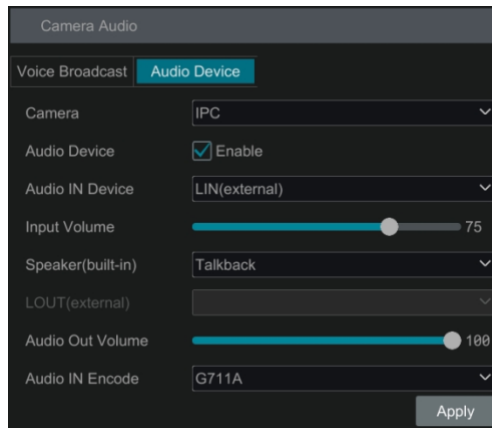
1. Camera audio settings:

Voice broadcast can be set up for perimeter alert cameras. Select a 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 line you set.

Audio: Enable or disable as desired. If your camera doesn’t support this function, the checkbox will not be displayed.

Voice: click “Add” to add an alarm audio file in .wav format. Click “Listen” to listen to the uploaded audio.

Click “Audio Device” to configure audio for the camera.



Select a camera and then enable its audio by checking the “Audio Device” box.

Audio IN Device: Select according to the device’s capabilities (built-in mic or Line-In external mic.)

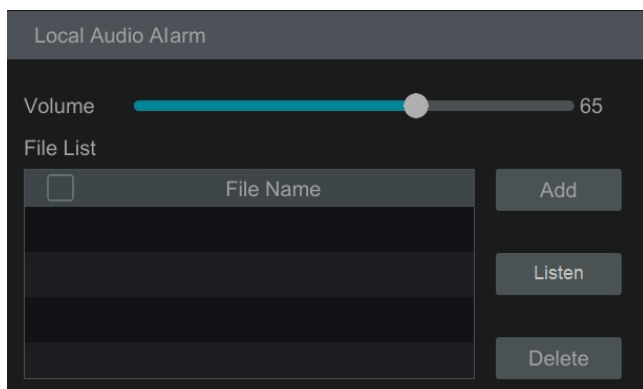
Speaker (built-in): Select according to the device’s capabilities.

LOUT: Select if your camera has a line-out configuration.

Audio Input Encode: Select G711A/G711U based on your location. G711U is commonly used in North America.

2. Local Audio Alarm

Set an audio alarm for the NVR that plays locally from the HDMI output.



In this interface, you can set the volume for the local audio. Click “Add” to upload an audio file. Choose the uploaded audio file and then click “Listen” to listen to it; click “Delete” to delete this file.

12.5.7 Light

Click Start→Settings→Alarm→Event Notification→Light to go to the interface shown below. In this interface, you can enable and set the light’s flashing time and frequency when an alarm is triggered.

Camera	Enable	Flashing Time(s)	Flashing Frequency
IPC	ON	20	Low

12.5.8 Alarm Server

Go to Alarm→Alarm Server interface as shown below.

Enable the alarm server and enter a server address and the port of the alarm server. Then, select protocol. If “Send Heartbeat” is enabled, set interval times. Set a schedule and alarm type as needed. After that, test the effectiveness of the alarm server. Having tested successfully, please click “Apply”. When the relevant 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

Port

Protocol

☐ Send Heartbeat

Interval Time[s]

Schedule Manage

Alarm Type

Configure

Motion Alarm

Sensor Alarm

IPC Offline

Object Abandoned/Missing

Exception Detection

Line Crossing

Test

Apply

12.6 Manual Alarm

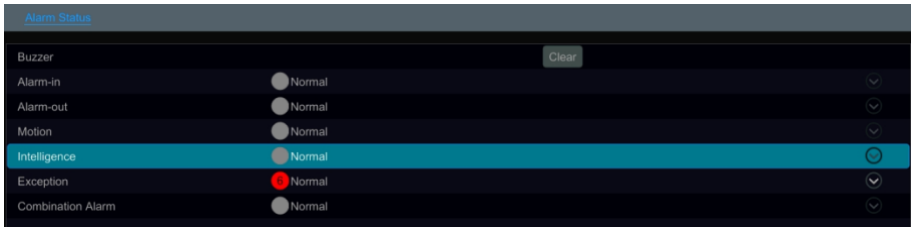
Click  on the tool bar at the bottom of the live preview interface to bring up a window. Click “Trigger” to start an alarm. Click “Clear” to stop the alarm.

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 Camera82_AlarmOut1	Normal	Trigger	Clear

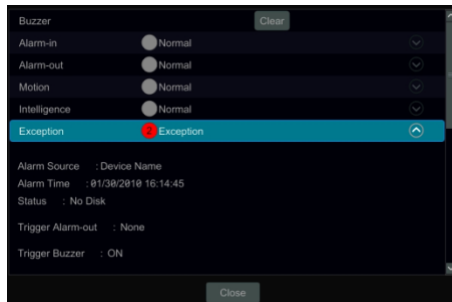
Close

12.7 View Alarm Status

Click Start→Settings→Alarm→Alarm Status or click  on the tool bar at the bottom of the live preview interface to view the alarm status.



Click “Clear” to stop the buzzer when the buzzer alarm goes off. Click  to view detailed information as shown below.



If the exception information has more than one page, you can enter the page number in the box and then click  to jump to that specified page. Click  /  to view exception alarm information in the previous/next page.

12.8 System Disarming

You can quickly disarm devices through the alarm host and remote client (like 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 parameters setting is valid when the remote switch is enabled

Disarm Set

Status : Arming One Key Disarm

Disarm Channel/Sensor Add

Channel/Sensor	Disarm Link Item	Configure	Delete

*At the State of disarm, the parameters of channel and sensor is invalid

Apply

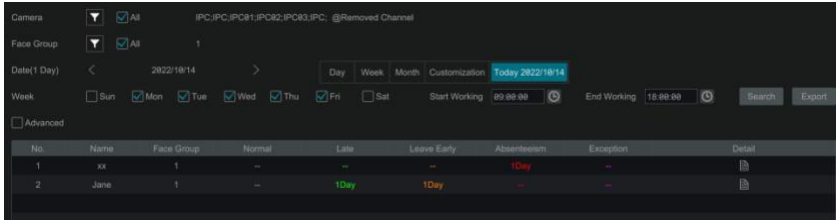
All alarm linkages for all channels and sensor alarms will be turned off after clicking “One Key Disarm” by default. You can also self-define the channels and sensors you want to disarm by clicking “Add”. Only the selected channels and sensors will be disarmed when you click “One Key Disarm”.

13 Application

13.1 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.



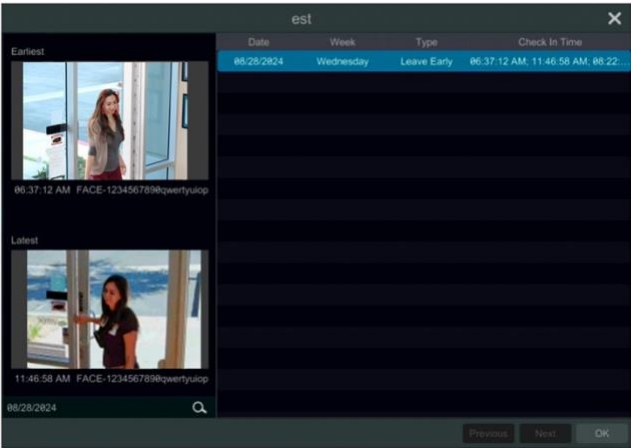
1. To search attendance information

- ① Click next to a camera and group to choose the desired cameras and groups.
- ② Set attendance days. You can choose a day, a week, a month, today, or customize the time period.
- ③ Set the start time and the end time of the work day.
- ④ Click “Search” to view the attendance state.

If some specific person's attendance state needs to be known, you can click “Advanced” and then enter their name and choose the type.

Click “Export” to export searched attendance information.

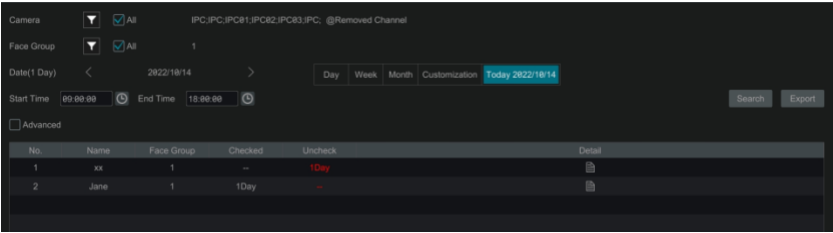
Click to view detailed information on attendance. In this interface, click to go to the face search interface.



13.2 Face Check-In

Click Start→Intelligent Analytics→Face Attendance to go to the following interface.
The search steps of face check-in are as follows.

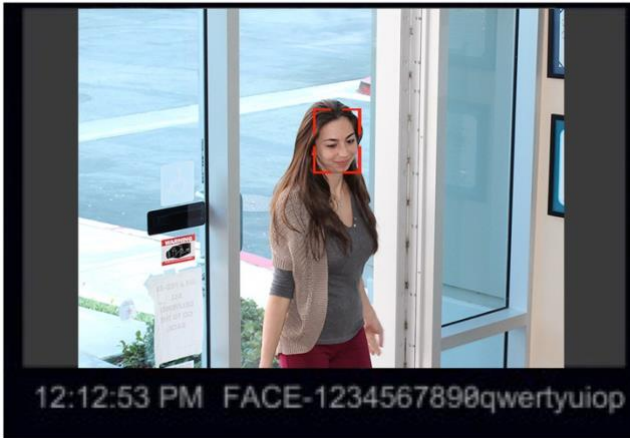
- ① Click  next to a camera and group to choose the desired cameras and groups.
- ② Set the check-in date. You can choose a day, a week, a month, today, or can customize the time period.
- ③ Set the start time and the end time for face check-in.
- ④ Click “Search” to view the check-in state.



If you want to know detailed check-in information for someone, click “Advanced” and then enter the name and choose the type to search.

Click  to view detailed information. In this interface, the checked image can be viewed.

Click  to view registered face picture for this person.



You can manage the parking lot through the NVR. Before using this function, please add a professional LPR camera.

13.3 Parking Lot Settings

Click Start→Intelligent Analytics→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
Total Parking Space	100
Remaining Parking Space	82
Apply	

13.3.1 Basic Settings

The system only supports one parking lot management. Please enter the parking lot name, total parking spaces, and remaining parking spaces. To ensure an accurate count of parking spaces, please enter parking space information when there is no vehicle entering or exiting.

13.3.2 Parking Space Settings

Only vehicles added into the plate database are allowed to pass through automatically. You can set parking spaces according to the vehicle group or directly use the total parking spaces. For the block-list, you can set “No parking allowed”. After that, set a schedule and Email as needed.



No.	Parking Group Name	Parking Options	Total Parking	Remaining Pa.	Schedule
1	vip	Use the total parking space to park			24x7

13.3.3 Entrance/Exit Management

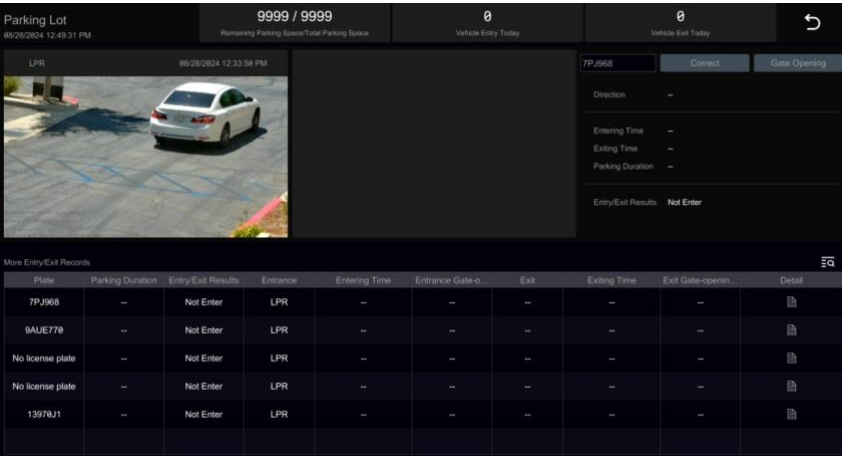
Set the passing direction of vehicles and bind LED screens as needed.



No.	Lane Name	Direction	Camera	Status	Enable LED screen	Associated LED screen
1	IP83	Enter	IP83(172.28.74.281)	Online	☒	LED display

13.3.4 Parking Lot Management

After the above settings are configured, click “Parking Lot” on the left menu to go to the following interface.



Parking Lot
8/28/2024 12:43:31 PM

9999 / 9999
Remaining Parking Space/Total Parking Space

0
Vehicle Entry Today

0
Vehicle Exit Today

↺

LPR
8/28/2024 12:33:58 PM



7PJ968

Correct

Gate Opening

Direction: --

Entering Time: --

Exiting Time: --

Parking Duration: --

Entry/Exit Results: Not Enter

More Entry/Exit Records

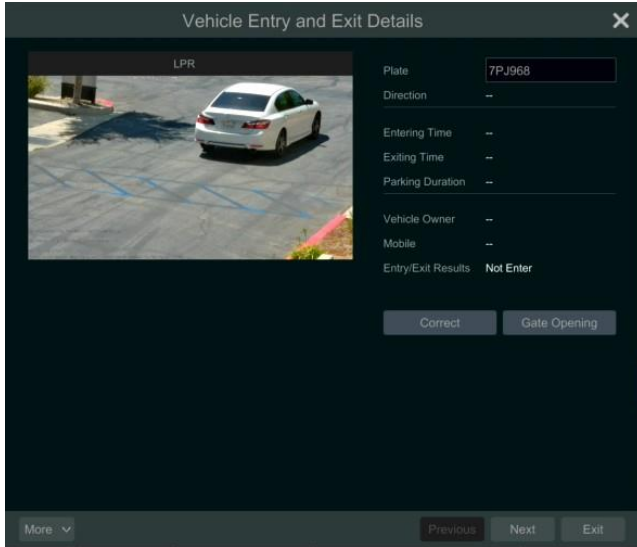
Plate	Parking Duration	Entry/Exit Results	Entrance	Entering Time	Entrance Gate-o...	Exit	Exiting Time	Exit Gate-open...	Detail
7PJ968	--	Not Enter	LPR	--	--	--	--	--	
9AUE778	--	Not Enter	LPR	--	--	--	--	--	
No license plate	--	Not Enter	LPR	--	--	--	--	--	
No license plate	--	Not Enter	LPR	--	--	--	--	--	
13078J1	--	Not Enter	LPR	--	--	--	--	--	

In this interface, you can view detailed information about the parking lot, including the total number of parking spaces, remaining parking spaces, number of vehicles entering today, number of vehicles 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. You can release it manually by clicking “Gate Opening”. If the plate number captured is not matched with the one seen in the live view, you can click “Correct” to correct it.

Click  to view detailed information for vehicles entering/exiting.
Click “More” to register a license plate or view ID information.

Click  to search the records of vehicles entering/exiting.

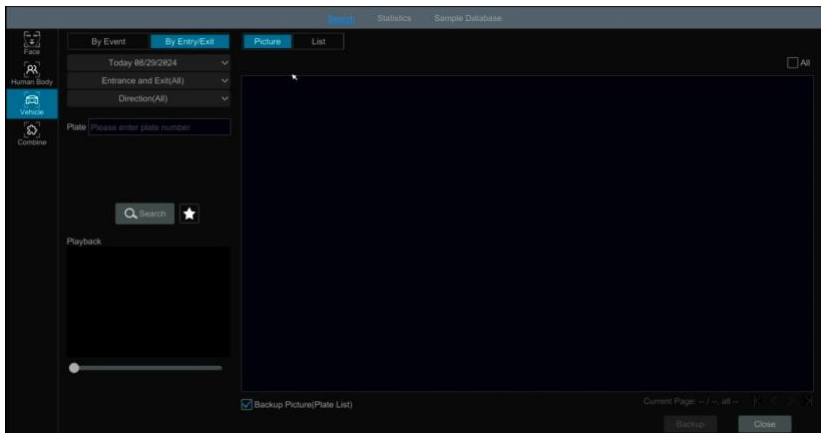


Click  to return to the live view interface.

13.3.5 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 filter conditions (including time/direction/license plate). Click  in the right corner of the searched picture to view details; click "Backup" to export searched pictures.



13.4 Access Control Management

This system 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.

13.4.1 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)

Apply

Select the access control device you want to configure the parameters of.

Lock: Choose the lock you want to control.

Unlocking Mode: if “Mask On” is selected, the door will open when the matched person is 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, if the unlocking mode is “Face only” and the delay time is set to “2” seconds; the door will be opened 2 seconds after face recognition.

Unlocking Duration: If the door has been unlocked for a period that exceeds the duration, the door will automatically lock. The time range is from 0 to 10 seconds. For example, if the unlocking mode is “Face only” and the duration is set to “3” seconds; the unlocked door will be automatically locked after 3 seconds.

Door Lock Setting: Choose “Auto”, “NO,” or “NC” according to your door lock type.

Alarm Linkage Type: Open/close the door

Wiegand Config: You can select Wiegand Input, Wiegand Output, or Off. If the

card reader is connected to a Wiegand interface, please select “Wiegand Input”. If the access control is connected to a Wiegand interface, please select “Wiegand Output”.

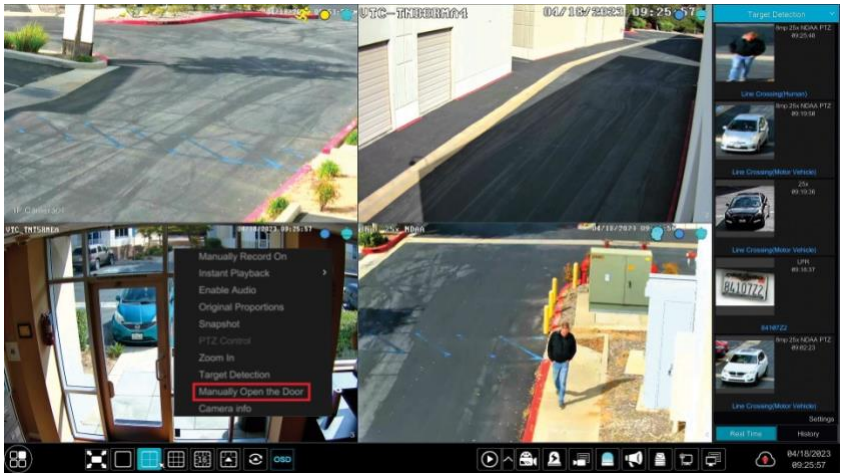
Wiegand Mode: You can select 26bit(8), 26bit(10), 34bit, 37bit, 42bit, 46bit, 58bit, or 66bit.

After clicking “Apply”, configuration will be synchronized with the camera.

When someone wants to enter, the access control device will open the door according to set conditions.

13.4.2 Open a Door Manually

In the live view interface, select an access control camera. Right click on the window to bring up a dropdown list. Select “Manually Open the Door” to open the door via the NVR.

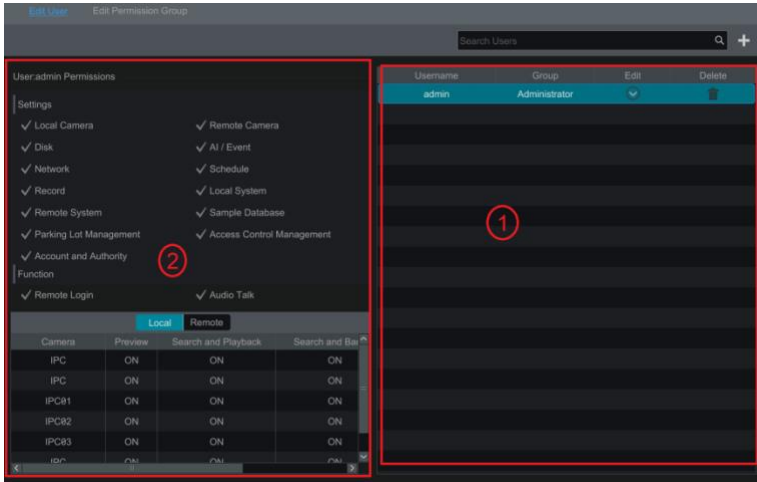


If you want to view real-time face snapshots and comparison of access control devices, please enable face detection or comparison function as needed. The corresponding results will display under the target detection tab in the live interface.

14 Account & Permission Management

14.1 Account Management

Click Start→Settings→Account and Authority→Account→Edit User to go to the interface shown below.



Area ② displays user permissions. Area ① displays the user list. Click the user in the list to display its user permissions in area ②.

There are three default permission groups (“Administrator”, “Advanced” and “Common”) available when adding accounts. You can also manually add new permission groups (see [13.3.1 Add Permission Group](#) for details).

Only the **admin** account and users that have the “Account and Authority” permissions can manage the system’s accounts. The group “Administrator” owns all the permissions displayed in area ② except “Account and Authority” and its permissions cannot be changed while the permissions of “Advanced” and “Common” can be changed.

14.1.1 Add User

- ① Click Start→Settings→Account and Authority→Account→Add User or click beside the search box to bring up the window shown below.

Add User

Username:

Password:

Confirm Password:

☐ Display Password

☒ Allow Modify Password

Pattern Lock: ☐ Enable

E-mail:

Group:

- ② Set a username, password, and group. The user can also set a pattern lock here. The e-mail address box is optional. Click “Add” to add the user.

14.1.2 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's 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 a password security question for **admin** only. 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. Passwords of other users can be recovered by the **admin** account or users that have “Account and Authority” permissions.

➤ Modify Password

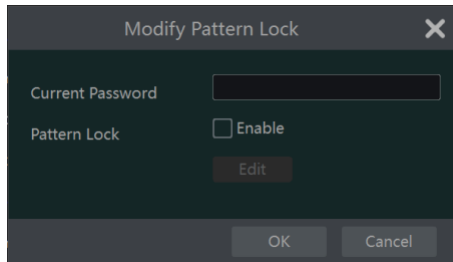
You can modify the **admin** account password. Click “Modify Password” to bring up a window. Enter the current password and then set a new password. Click “OK” to save the settings.

In addition, the admin user can modify common/advanced user's passwords.

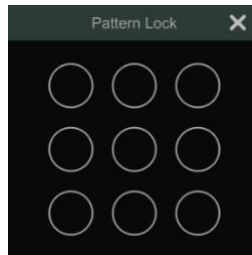
➤ Modify Pattern Lock

Some models may not support this function.

Click “Modify Pattern Lock” to bring up a window.

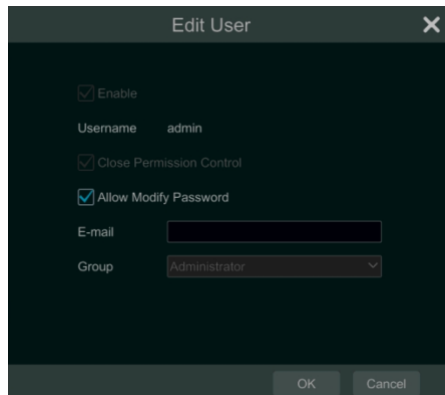


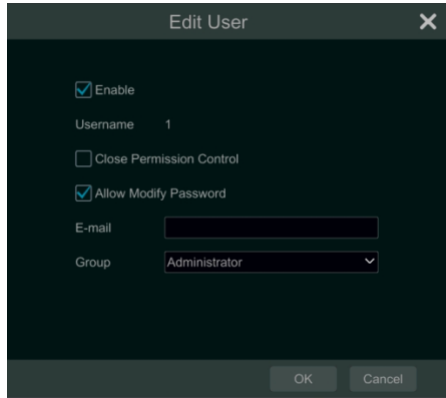
Input the current password and then check “Enable” to set a pattern lock.



➤ Edit User

Click “Edit User” to bring up the window shown below. The **admin** account can’t be disabled, its permission control is closed, and its permission group cannot be changed by default. You can enable or disable other users, 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 these settings.





14.2 User Login & Logout

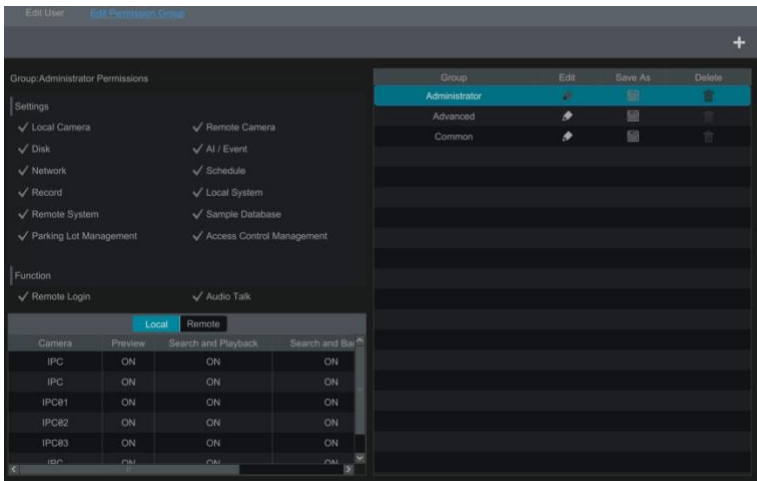
Login: Click Start→Login, or directly click the preview interface, and then select a username and enter its password in the window. Click the “Login” button to log in to the system.

Logout: Click Start→Logout or click Start→Shutdown to bring up the “Shutdown” window. Select “Logout” in this window and then click “OK” to log the system out.

14.3 Permission Management

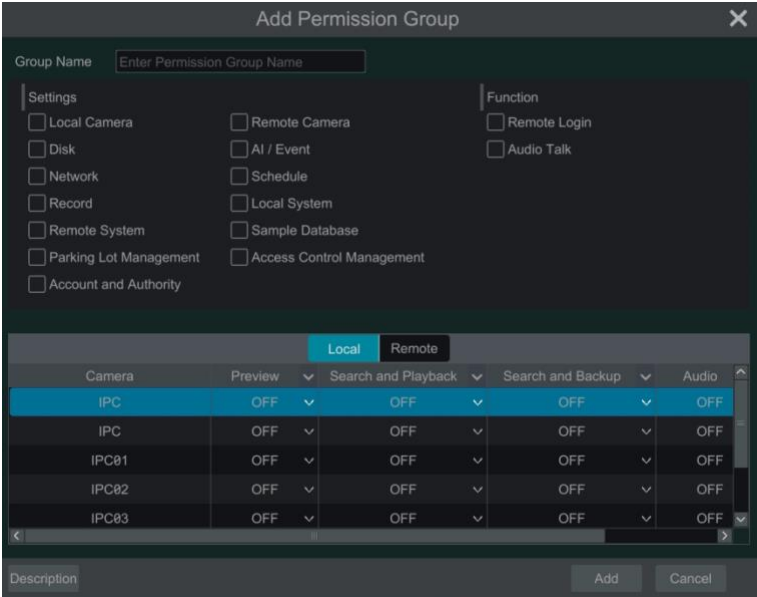
14.3.1 Add Permission Group

Click Start→Settings→Account and Authority→Account→Edit Permission Group to go to the interface shown below.



Click  to add a permission group. Set a group name, check the permissions as required, and then set the “Local” and “Remote” permissions. Click “Add” to save

the settings.

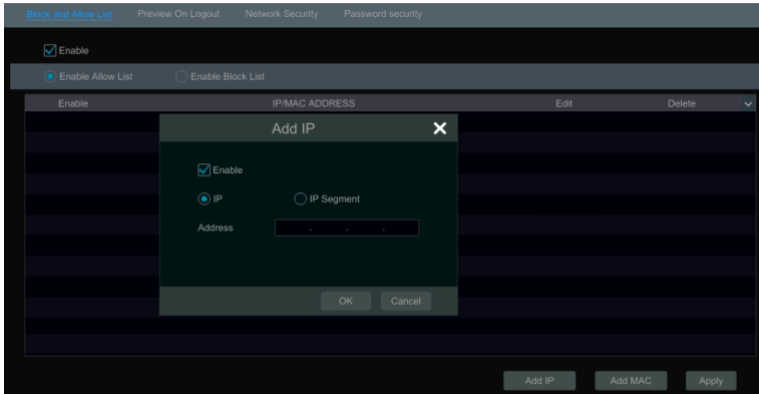


14.3.2 Edit Permission Group

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 [13.3.1 Add Permission Group](#) for details). Click  to save the group as a new group. Click  to delete the permission group. The three default permission groups (“Administrator”, “Advanced” and “Common”) cannot be deleted.

14.4 Block and Allow List

- ① Click Start→Settings→Account and Authority→Security to go to the following interface.

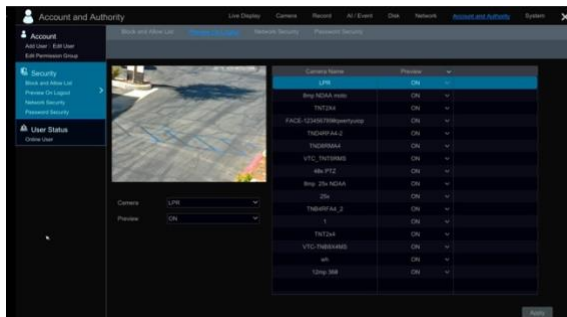


- ② Check “Enable” and then choose “Enable Allow List” or “Enable Block List” (PC clients using the configured IP address in the allow list can access the NVR remotely while PC clients in the block list cannot).
- ③ Add IP/IP segment/MAC. Click “Add IP” or “Add MAC” and then check “Enable” in the popup window (The IP/IP segment/MAC can only be configured if you check this option). Enter an IP/IP segment/MAC and then click “OK”. In the above interface, click  to edit an IP/IP segment/MAC, click  to delete it. Click “Apply” to save the settings.

14.5 Preview on Logout

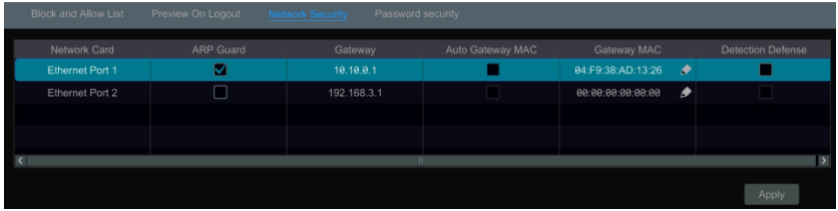
Click Start→Settings→Account and Authority→Security→Preview on Logout to go to the following interface.

Select a camera and then enable or disable the preview permission on logout as desired. If a camera's preview permission on logout is “ON”, you can view the camera's live image when the system is logged out, if “OFF” you cannot see it while logged out.



14.6 Network Security

Click Start→Settings→Account and Authority→Security→Network Security to go to the following interface. You can enable ARP Guard.



ARP Guard: Address Resolution Protocol Guard. This function can protect the LAN from ARP attacks. If enabled, you can enable auto gateway MAC or manually set the gateway MAC. Additionally, detection defense can also be enabled as desired.

14.7 Password Security

Click Start→Settings→Account and Authority→Security→Password Security to go to the following interface.



In this interface you can set the difficulty level and expiration time for passwords.

14.8 View Online User

Click Start→Settings→Account and Authority→User Status to view online user information (you can view the online user name, login type, IP address, and login time; click  to bring up a window showing the preview occupied channel number and playback occupied channel number).

15 Device Management

15.1 Network Configuration

15.1.1 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 an IPv4/IPv6 (if IPv6 is enabled) address automatically, or manually enter network addresses. You can click “Advanced” to 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 the settings.

The screenshot shows the 'IP Address Settings' window for 'Ethernet Port 1 (Online)'. It has an 'Advanced' button in the top right. A toggle 'Obtain an IP address automatically' is checked. Below, there are two columns for IPv4 and IPv6 settings. IPv4 settings include Address (192.168.2.100), Subnet Mask (255.255.0.0), Gateway (192.168.0.1), and DNS (Preferred: 8.8.8.8, Alternate: empty). IPv6 settings include a checked 'Enable' box, Address (fe80::f12:168:2:100), Mask Length (64), Gateway (fe80::f12:168:2:1), and DNS (Preferred and Alternate are empty). A 'Default Route' dropdown is set to 'Ethernet Port 1'. An 'Apply' button is at the bottom right.

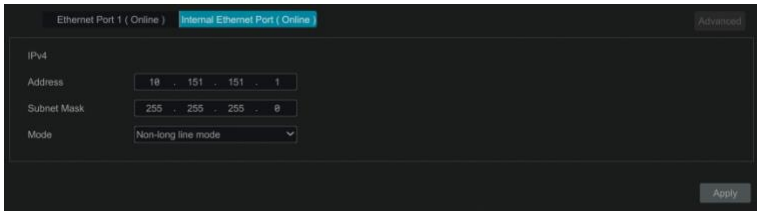
Note:

1. Internal Ethernet Port

If you use the NVR with built-in PoE network ports, click “Internal Ethernet Port” to go to the following interface.

The internal Ethernet Port settings are used to configure the PoE ports on the back of the NVR. If the internal Ethernet Port is shown to be offline, all the PoE ports will be unavailable, it's possible for the internal Ethernet Port to be broken. The Internal Ethernet Port's network address can be changed to match the IP addresses of IP cameras that are directly connected to the PoE ports on the back of the NVR. However, it is **not** recommended to change the Internal Ethernet Port's address.

Mode: You can select Non-Long Line Mode or Long Line Mode. Long-Line mode can extend the transmission distance of long network cables from 100 meters(about 300 ft) to 200 meters(about 600 ft.) This will lower the data throughput from 100Mbps to 10Mbps.



- Multiple Ethernet Ports Setting

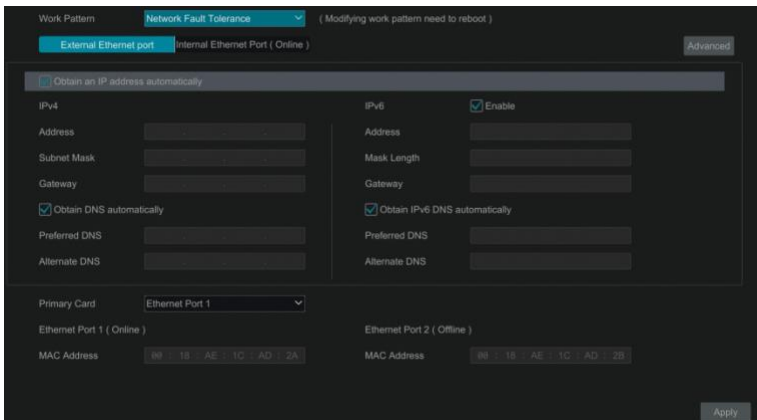
If the NVR has two network ports or more, you can set it to the network work pattern needed.

TOE: Some models may support TOE mode. It is a technology for improving network transmission speeds. You can enable it if your network supports it. If TOE is enabled, it will be in high-speed mode. Then, you can choose and configure the multiple address settings or set it to network fault tolerance mode. If TOE is not enabled, then network fault tolerance cannot be selected and set up.

2. Network Fault Tolerance:

The two network ports will be bound to one IP address if you select “Network Fault Tolerance.” The advantages of this setting are: 1. increases bandwidth; 2. It will form a network redundant array to share the load. When one network port fails, the other port will take over the entire load immediately. The takeover process is seamless, and network service will not be interrupted.

Refer to the figure shown below. If “Network Fault Tolerance” is selected, check “Obtain an IPv4 address automatically”, and “Obtain DNS automatically” to get a network address automatically, or manually enter IPv4/IPv6(if IPv6 is enabled) addresses and select one Ethernet port as the primary card and then click “Apply” to save the settings.



3. Multiple Address Setting:

If “Multiple Address Setting” is selected, the IP addresses of the two Ethernet ports will be set separately. Refer to the picture shown below.

Check “Obtain an IP address automatically” and “Obtain DNS automatically” to get the network address automatically, or manually enter a 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) | Advanced

☒ Obtain an IP address automatically

IPv4

Address: 192.168.2.298

Subnet Mask: 255.255.0.0

Gateway: 192.168.2.1

☐ Obtain DNS automatically

Preferred DNS: 8.8.8.8

Alternate DNS:

IPv6

☒ Enable

Address: fe80::192:168:2:298

Mask Length: 64

Gateway: fe80::192:168:2:1

☐ Obtain IPv6 DNS automatically

Preferred DNS:

Alternate DNS:

Default Route: Ethernet Port 1

Apply

15.1.2 Port Configuration

Click Start→Settings→Network→Port to go to the interface shown below. Enter the HTTP port, HTTPS port, server port, and POS port you'd like the NVR to use, and then click “Apply” to save the settings. You can also enable and set the RTSP port (please check “Anonymous” if needed).

Port

HTTP Port: 80

HTTPS Port: 443 ☐ Enable Please install the certificate on the web beforehand

Server Port: 6636

POS Port: 9836

API Server

☐ Enable

Authentication: Digest

RTSP

☐ Enable

Authentication: Digest

RTSP Port: 554 ☐ Anonymous

Apply

HTTP Port: the default HTTP port of the NVR is 80. The port number can be changed to others like 81. The port is mainly used for web client access. If you

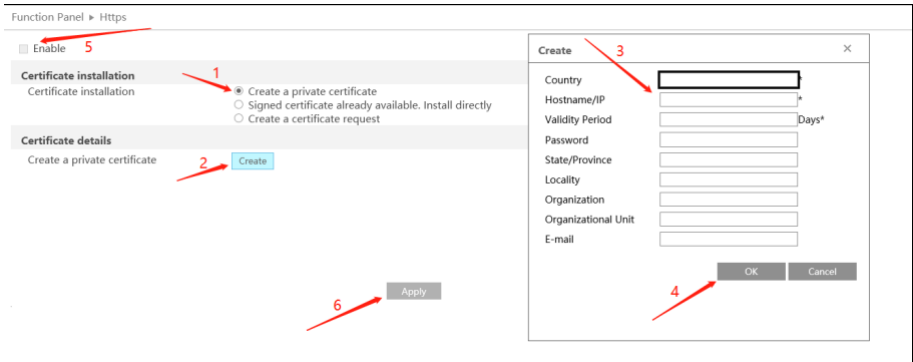
want to access the NVR through a web browser, you must enter the IP address plus HTTP port in the address bar of the web browser like so: <http://192.168.11.61:81>.

Note: The HTTP port and server port of the NVR must be mapped in the router before you can access the NVR via WAN.

HTTPS Port: the default HTTPS port of the NVR is 443.

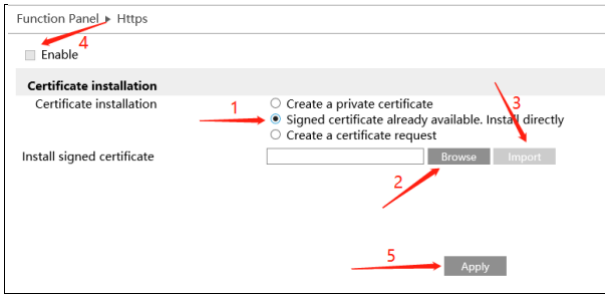
HTTPS provides authentication on the web portal and protects the user's privacy. You can enter the IP address plus HTTP port in the address bar of the web browser. Then enter the username and password to log in. Click Function Panel→Network→HTTPS to go to the following interface. There are three ways 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 period, 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



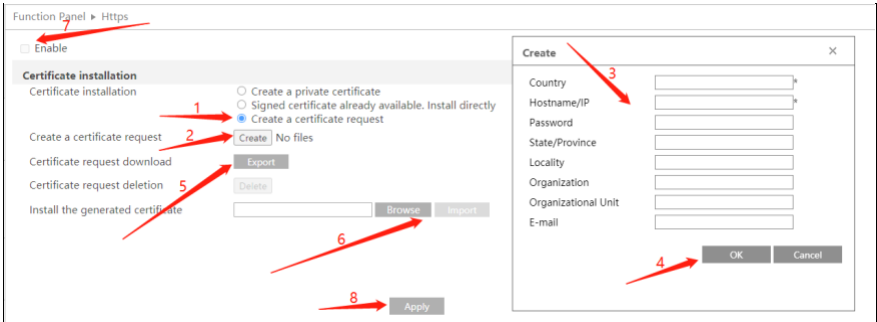
- ① Check “Signed certificate already...”.
- ② Click “Browse” to select the certificate you want to import.
- ③ Click “Import”.
- ④ Check “Enable”.
- ⑤ Click “Apply” to save the settings.

Please note that the certificate uploaded here must be a certificate with a private key.

How 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



- 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 period, 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 a 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](https://IP:https port via the web browser) 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 for the Video Management System program.

POS Port: the default POS port of the NVR is 9036. Used for connection to Point-of-Sale devices.

API Server: You can log in to a media player that supports the RTSP protocol. Moreover, a third-party can further develop features through the API service.

Authentication: You can choose either basic authentication or digest authentication.

RTSP Port: RTSP real-time stream protocol can be used to control the sending of real-time data. Using a media player (like VLC player) which supports RTSP real-time streaming protocol, you can view live video 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 indicates main stream; sub indicates sub stream; chID indicators channel ID).

Examples: Enable RTSP and “Anonymous”. Then open VLC player and enter the address (for example: <rtsp://192.168.1.88:554/chID=1&streamType=main>) in the network address bar of VLC player. Then you can view the video of channel 1.

15.1.3 PPPoE Configuration

Click Start→Settings→Network→PPPoE to go to the interface shown below. Check “Enable” in “PPPoE Settings” and then enter the username and password obtained from the dealer. Click “Apply” to save the settings.

15.1.4 DDNS Configuration

DDNS is used to connect to an NVR on a network with a dynamic IP address using a domain name. You can access the NVR easily if DDNS is enabled and configured.

Click Start→Settings→Network→DDNS to go to the interface shown below.

The screenshot shows the DDNS configuration window. It has a title bar 'DDNS'. Below it is a checkbox labeled 'Enable' which is checked. Then there is a dropdown menu for 'DDNS Type' with 'www.dvrdyns.com' selected. Below that are input fields for 'Server Address', 'Domain Name', 'Username', and 'Password', each with a placeholder text 'Enter Address', 'Enter Domain Name', 'Enter Username', and 'Enter Password' respectively. There is a 'Heartbeat Interval' field with a placeholder 'Enter heartbeat interval' and a unit 's' (Range : 5~3600). At the bottom, there is a 'Connection Status' field showing 'Failure'. At the very bottom are two buttons: 'Test' and 'Apply'.

Check “Enable” and then select a DDNS type. Enter a server address, domain name, username, and password based on to the selected DDNS type. Click “Test” to test the entered information. Click “Apply” to save settings. After that, the connection status will show “success” if it’s working.

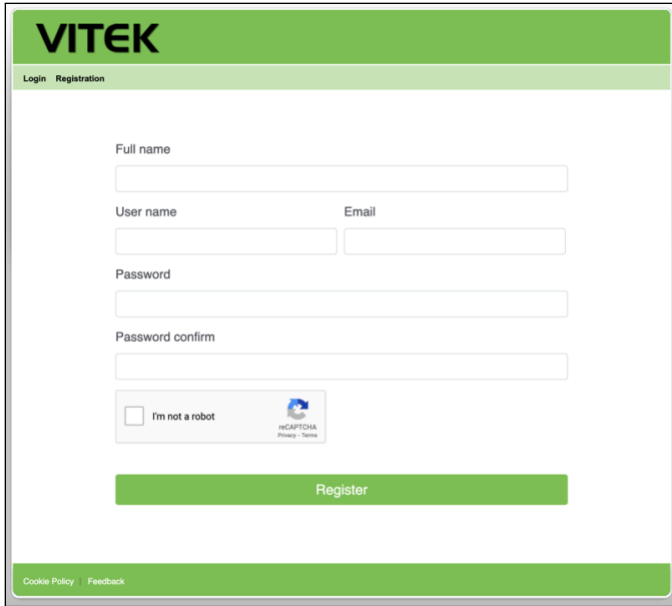
Note: The heartbeat interval can only be configured when the DDNS type is “dyndns.”

You will have to enter a server address and domain name when using some DDNS types. Go to the relative DNS website to register a domain name and then enter the registered domain information here).

Enter <http://www.vitekiyppddns.com/> in the address bar to visit its DNS website.

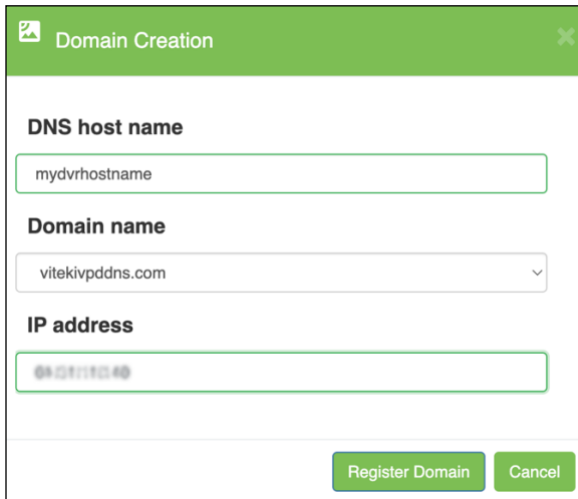
The screenshot shows the VITEK website login page. It has a green header with the 'VITEK' logo. Below the header is a navigation bar with 'Login' and 'Registration' links. The main content area has a 'User name or email' input field, a 'Password' input field, and a 'Password lookup' link. Below these is a checkbox labeled 'I'm not a robot' next to a CAPTCHA image. At the bottom of the main content area is a green 'Login' button. At the very bottom is a green footer with 'Cookie Policy' and 'Feedback' links.

- ① Click **Registration** to go to the interface shown below. Set up the DDNS account information (username, password and so on) and then click **Submit** to save the account.



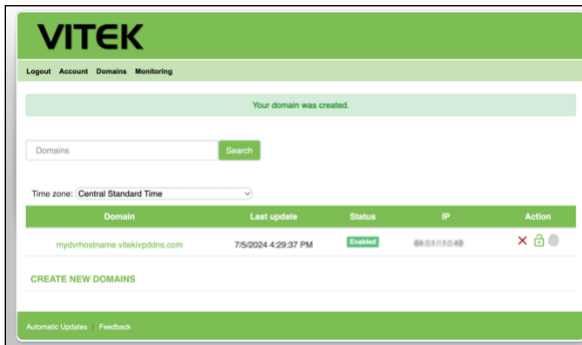
The image shows the VITEK registration interface. At the top is a green header with the VITEK logo. Below the header is a navigation bar with 'Login' and 'Registration' links, where 'Registration' is highlighted. The main form area contains several input fields: 'Full name', 'User name', 'Email', 'Password', and 'Password confirm'. Below these fields is a CAPTCHA section with a checkbox labeled 'I'm not a robot' and a CAPTCHA image. At the bottom of the form is a large green 'Register' button. The footer of the page contains links for 'Cookie Policy' and 'Feedback'.

- ② Create a domain name and then click **Request Domain**.



The image shows the 'Domain Creation' form. It has a green header with a close button (X) in the top right corner. The form contains three main sections: 'DNS host name' with a text input field containing 'mydvhostname'; 'Domain name' with a dropdown menu showing 'vitekivddns.com'; and 'IP address' with a text input field containing '04.01.110.40'. At the bottom right of the form are two buttons: 'Register Domain' and 'Cancel'.

- ③ After you successfully request your domain name, you will see your domain name information in the list.



- ④ Click Start→Settings→Network→DDNS to go to DDNS setting interface. Enable DDNS and then select the <http://www.vitekipddns.com/> DDNS type. Enter the registered username, password, and domain name and then click “Apply”.
- ⑤ Forward the HTTP and Server ports to the NVR’s IP address in the router (you can skip this step if UPnP function is enabled).
- ⑥ Enter the registered domain name plus HTTP port like so: <http://www.xxx.vitekipddns.com:81/> in the address bar and then press Enter key to go to the web client.

15.1.5 E-mail Configuration

Click Start→Settings→Network→E-mail to go to the following interface.

Sender

Sender Name

Email Address

SMTP Server

SMTP Port Default

Security

Attaching Image

☐ Anonymous Login

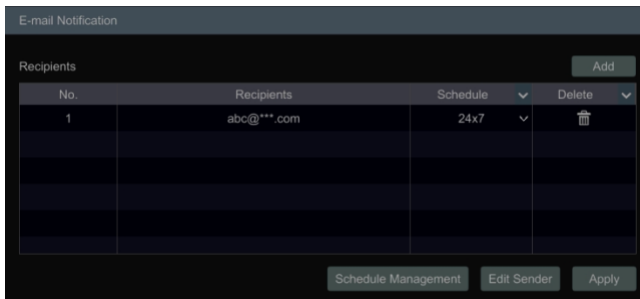
Username

Password

Edit Recipient Test Apply

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 SSL and the attaching image setting. Enter the username and password for the sender and then click "Apply" to save the settings (you don't have to enter the username and password if "Anonymous Login" is enabled). Click "Test" to bring up a window. Enter the e-mail address of the recipient in the window and then click "OK". The Sender e-mail address will send an e-mail to the recipient. If the e-mail is sent successfully, it indicates that the Sender e-mail address is configured correctly.

Click "Edit Recipient" to go to the following interface.



Click "Add" and then enter a recipient's e-mail address and select a schedule (if a schedule is selected, the system will only send alarm emails and the recipient will only receive it during 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 from the list. Click "Apply" to save the settings. Click "Edit Sender" to go to the e-mail configuration interface of the sender.

15.1.6 UPnP Configuration

With UPnP you can access the NVR's web client via WAN without doing port mapping in the router.

- ① Click Start→Settings→Network→UPnP to go to the following interface.
- ② Make sure the router supports UPnP function and that 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 shown below and then click "Apply".

Click the "Refresh" button to refresh the UPnP status. If the UPnP status is "Invalid UPnP" after refreshing it a few times, the port number may be 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 following picture. You can view the external IP address of the NVR. Enter the external IP address plus port in the address bar to access the NVR such as <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	6836		6836	Not Ready	
RTSP Port	554		554	Not Ready	

Test Apply

15.1.7 802.1X

If enabled, the NVR's data can be protected. When the NVR is connected to a 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

Apply

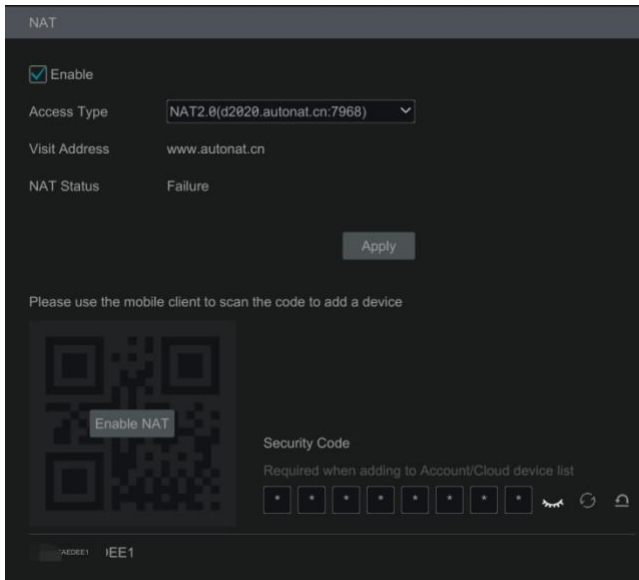
To use this function, the NVR must be connected to a switch supporting the 802.1x protocol. The switch will be considered as an authentication system to identify the device in a local network. If the NVR connected to the network interface of the switch has passed the authentication of the switch, it can be accessed via the local network.

Protocol type and EAPOL version: Please use the default settings.

Username and password: The user name and password must be the same as the user name and password applied for and registered in the authentication server.

15.1.8 NAT Configuration

Click Start→Settings→Network→NAT to go to the interface for NAT configuration.



Check “Enable” and then select the NAT server address. Click “Apply” to save the settings.

You can scan the QRCode through the mobile APP installed on a mobile phone or tablet PC to quickly add the device to the server list of the mobile APP.

Access Type: NAT 1.0 or NAT2.0 are available.

Note:

1. If you want to use cloud upgrade, you must enable NAT2.0.
2. After NAT is enabled, use the mobile APP to scan the QRcode and add the NVR to the server list of the mobile APP.
3. When Nat 2.0 is enabled, the device can be added to a specific account created in the mobile APP. When enabled you’ll add the system to the mobile APP using the Account section rather than the Server List section and enter the Security Code from the NAT settings section on the NVR.

After the device is bound to that specific account on the mobile APP, blue binding information will be shown under the QRcode. Click this blue information to unbind it.

NAT access can only be shared from the account on the mobile APP it was originally bound to.

15.1.9 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 a server name, port, username and password, max file size, and remote directory.

Please enable “Resume Uploading” if needed.

After that, choose a camera, set a schedule, and then select video records, images, and alarm information you want to upload in this interface.

FTP

☒ Enable

Server Address Port

Username Password ☐ Anonymous

Max File Size 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

No.	Camera Name	Schedule	Uploading record				Uploading Image	Uploading File(txt)
			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

Schedule Management Test Apply

15.1.10 SNMP

- ① Click Start→Settings→Network→SNMP to go to the interface for SNMP configuration.

SNMP

☒ Enable SNMPv1

☒ Enable SNMPv2

SNMP Port

Read Community

Write Community

Trap Address

Trap Port

Apply

- ② Check SNMPv1 or SNMPv2 to enable this function.
- ③ Set the port for SNMP.
- ④ Set the trap address and the trap port.
- ⑤ Click “Apply” to save the settings.

Trap Address: The SNMP host's IP address.

Trap Port: The SNMP host's port.

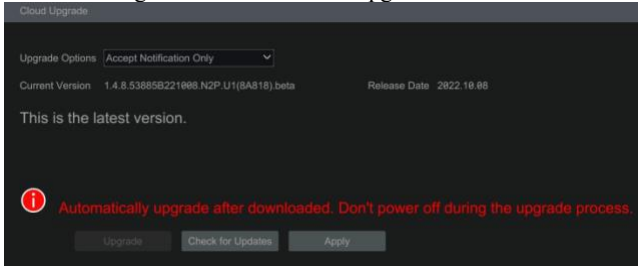
Tips: Before setting up SNMP, please download SNMP software and configure it to receive device information via the SNMP port. By setting the trap address, the

device is allowed to send alarm events and exception messages to the monitoring center.

15.1.11 Cloud Upgrade

Note: NAT 2.0 must be enabled before you can use the cloud upgrade feature.

- ① Click Start→Settings→Network→Cloud Upgrade as shown below.



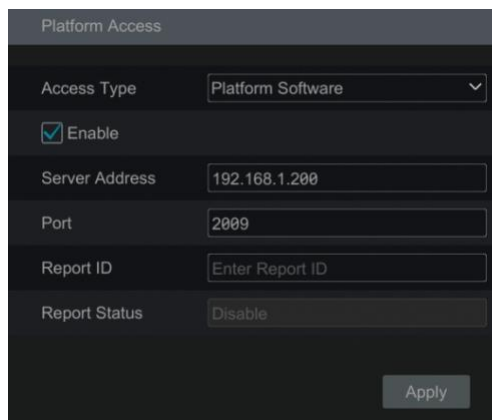
- ② Select “Accept Notification Only” or click “Check for Updates” to check whether the current version is the latest. If your software version is not the latest, click “Upgrade” to download and upgrade from the cloud server.
- ③ Please don't power off during the upgrade process.

15.1.12 Platform Access

Some models may not support this function.

This function is mainly used for connecting to Video Management Software. The setting steps are as follows.

Click Start→Settings→Network→Integration→Platform Access to go to the interface.



1. Platform Access

- ① Set “Access Type” to “Platform Software” and select “Enable” as shown above.

- ② Check the IP address and port for the transfer media server in the VMS software. The default server port for auto reporting is 2009. If it is modified, please go to the transfer media interface to check.
- ③ Enable auto report in the VMS software when adding a new device. Then, add a self-defined device ID and complete the remaining information for the device in the VMS software.
- ④ Enter the above-mentioned server address, port and report ID in the server interface. Then click “Apply” to save the settings. Now the NVMS system will automatically connect to this device.

15.1.13 UPnP Report Access

In this interface, you can also access a third-party platform by using UPnP Report. Click **Start→Settings→Network→Integration→UPnP Report**. If this is enabled, please enter the server address, port, and manufacturer ID.

UPnP Report

☒ Enable

Server Address

Port

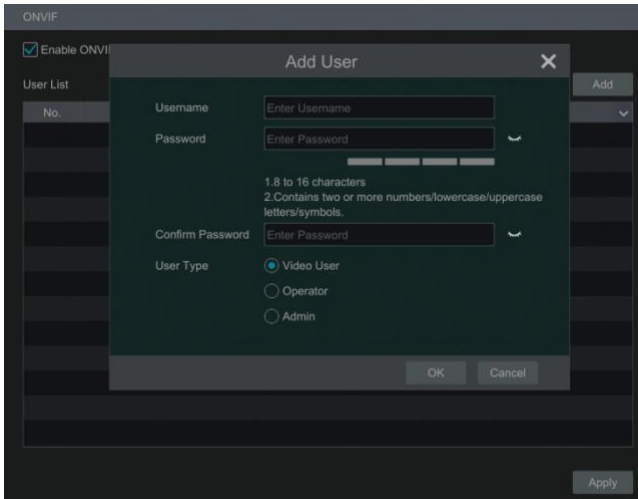
Manufacturer ID

Apply

15.1.14 ONVIF

This device supports ONVIF (Profile G/T/S). The model's name can be searched on ONVIF's official website for details. After ONVIF is enabled, it can be detected and connected to third-party platforms via the ONVIF protocol.

Click **Start→Settings→Network→Integration →ONVIF** to enter the following interface.



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.

15.1.15 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 preview interface to view network status quicker.

Click **Start**→**Settings**→**Network**→**Network Status Detection**. Enter an IP address and then click “Test” to check the network connection status (like network delay or packet loss).

15.2 Basic Configuration

15.2.1 Common Configuration

Click **Start**→**Settings**→**System**→**Basic**→**General Settings** to go to the following interface. Set a 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 No.

Language

Video Format

☒ Fixed Display Resolution

Main Output

Secondary Output

☒ Enable Wizard

☒ Log In Automatically

☒ Log Out Automatically

Wait Time

☒ App Live Self-adaption

☐ Dwell Automatically

Wait Time

☒ Live preview full screen time display

Apply

Device Name: The name of the device. It will display on the client end or VMS to help users recognize the device remotely.

Video Format: Two modes: PAL and NTSC. Select the video format according to the region, NTSC is for North America, PAL is for Europe.

Main Output: Enable “Fixed display resolution” to manually select the resolution that the NVR outputs to your monitor.

Note: You can set the resolutions of the main output and secondary output separately if the NVR has dual outputs. Refer to the picture shown below.

Dwell Automatically: Switch automatically. Check it and set the “wait time”. The system will switch images automatically if it is not operated during the time you set.

15.2.2 Date and Time Configuration

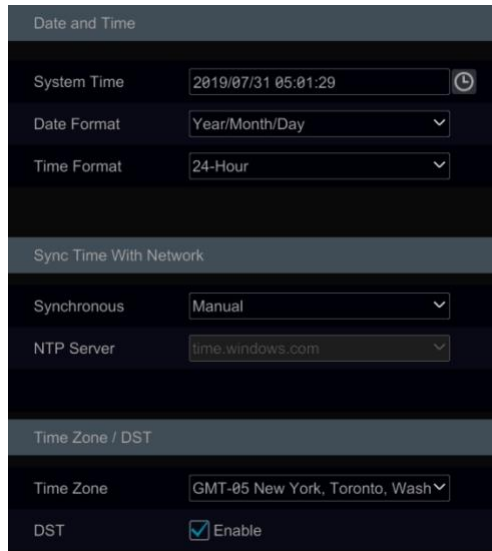
Click Start→Settings→System→Basic→Date and Time to go to the interface shown below.

Set the time, date format, time format, and time zone for the NVR. If the selected time zone uses Daylight Saving Time, the DST of the time zone will change automatically. Click “Apply” to save the settings.

You can manually set the system time or synchronize system time using the 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 an NTP server.



15.2.3 Recorder OSD Settings

Click Start→Settings→System→Basic→Recorder OSD settings to go to recorder OSD setting interface. You can enable or disable the visibility of OSD name and icons here.

15.2.4 PoE Power Management

Click Start→Settings→System→Basic Settings→PoE Power Management to go to the following interface. This function is only available for POE devices.

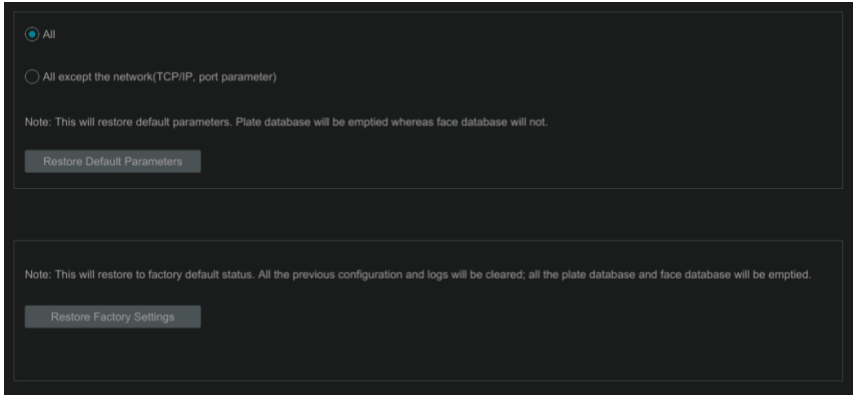
Poe Port	Enable	Current Power
Poe[01]	ON	0.00W
Poe[02]	ON	0.00W
Poe[03]	ON	0.00W
Poe[04]	ON	0.00W
Poe[05]	ON	0.00W
Poe[06]	ON	0.00W
Poe[07]	ON	0.00W
Poe[08]	ON	0.00W

In this interface, you can view the current power consumption of added POE

cameras. You can enable or disable the PoE power supply per port for PoE cameras by selecting “ON” or “OFF.”

15.3 Factory Default

Click Start→Settings→System→Maintenance→Factory Default to go to the following interface. You can restore specific default parameters or reset the device to factory settings.



Note: Restoring default parameters will not change the time zone or video format, other than that, only the admin account password will be kept.

15.4 Device Software Upgrade

● Upgrade

You can click Start→Settings→System→Information→Basic to view the MCU, kernel version, firmware version, and so on. Before upgrading, please acquire the correct upgrade file from your dealer.

The upgrade steps are as follows:

- ① Copy the upgrade software (.tar) onto a USB storage device formatted to FAT32.
- 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 exists. Select the upgrade software and then click “Upgrade”. The system may automatically restart during this process. Please wait for a while and do not power the NVR off during the upgrade.

Note: The file system of the USB mobile device used for upgrading, backing up, and restoring must be FAT32/NTFS format.

15.5 Backup and Restore

You can back up a configuration file containing the NVR’s settings by exporting the file to an external storage device; you can recover the configuration or apply

it to other NVRs of the same model by importing the configuration file on that NVR for quick setup and restoration of settings.

Insert a USB storage device into the USB interface of the NVR and then click Start→Settings→System→Maintenance→Backup and Restore to go to the interface.

- **Backup**

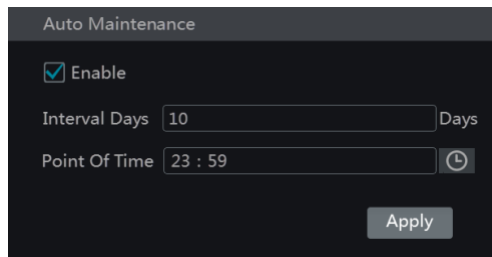
Select the USB device in “Device Name” option; go to the path where you want to store the configuration backup file and then click “Backup”; finally click “OK” in the popup window.

- **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.

15.6 Restart Automatically

You can set an automatic restart time for the NVR to maintain it regularly. Click Start→Settings→System→Maintenance→Auto Maintenance to go to the interface 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 selected time every interval of days.



Auto Maintenance

☒ Enable

Interval Days Days

Point Of Time 

15.7 View Log

Click Start→Settings→System→Maintenance→View Log to go to the log view interface. Select the log main type, click  to set a 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 a log file in the list and then click the “Export” button to export the log file. Click on the “Content” title bar to bring up a menu list. Check contents in the menu list and then the log list will show only the checked log contents. Click to play a video log.

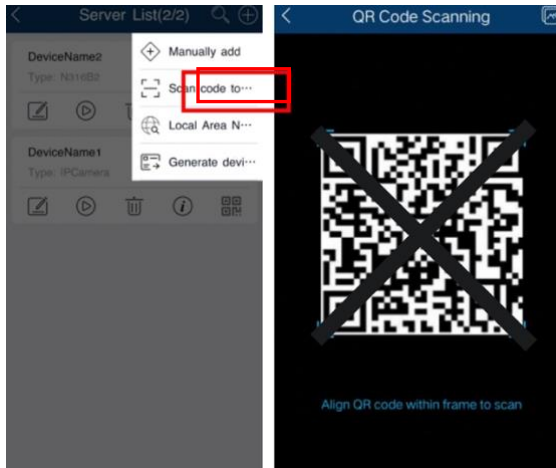
15.8 View System Information

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.

16 Remote Surveillance

16.1 Mobile Client Surveillance

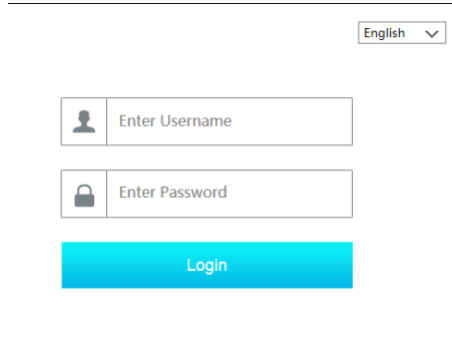
- ① Enable NAT in the NVR. Refer to [14.1.8 NAT Configuration](#) for details.
- ② Download and install the mobile client “Transcendent” on an Android or IOS mobile device.
- ③ Run the mobile client, go to the “Server List” interface, hit the top-right button, or hit the top left menu button and then “Server List”, and hit “Scan code to add” 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 and bind a device to an account in the mobile APP, you must enable NAT2.0 and enter the security code listed on the NAT page. Please refer to the mobile surveillance user manual for details.

16.2 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 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 preview interface.



English ▾

Enter Username

Enter Password

Login

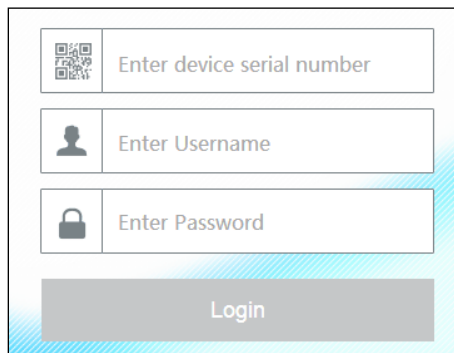
Notes: 1. Please make sure that the IP address of the NVR and the computer are both in the same local network segment. For example, supposing that the IP address of the computer is 192.168.1.41, the IP address of the NVR shall be set to 192.168.1.XXX.

2. If the HTTP port of the NVR is not 80, but other number instead, you need to enter the IP address plus port number in the address bar when accessing the NVR over network. For example, the HTTP port is 81. You should enter `http://192.168.1.42:81` in the address bar.

16.3 Web WAN Access

➤ NAT Access

- ① Set the network of the NVR. Please refer to [14.1.1 TCP/IP Configuration](#) for details.
- ② Enable NAT and then set the NAT server address. Please refer to [14.1.8 NAT Configuration](#) for details.
- ③ Open a web browser on your computer, enter the NAT server address www.autonat.com in the address bar and then press enter to go to the interface shown below (download and install the relative plug-in according to the tip if you are accessing the NVR through NAT for the first time).



Enter device serial number

Enter Username

Enter Password

Login

Enter the serial number (Go to Settings -> Network -> NAT to see the Nat serial

number), user name (the user name of the NVR, **admin** by default) and password of the NVR, select a display language on the top right corner of the interface, and then click “Login” to go to the web client interface.

➤ 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 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.XXX> 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 preview 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 in use by other devices on your network) and enable the 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 your router for details.
- ③ Get the WAN IP address of the NVR from the router or Google. Open a web browser on your computer, enter the WAN IP address plus HTTP port like so: <http://XXX.308.215:100> 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 preview 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.dvrddns.com:100> to access the NVR via internet.

16.4 Web Remote Control

The NVR supports web client access with plug-in or without plug-in.

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		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 browsers for the first time, the browser will need to download and install components for normal preview and playback.

If permissions for configuration modification are needed after the plug-in runs, please allow it, or the interface cannot be displayed normally; if the relevant ports of plug-in (port 11563; port 12863; port 13863) are occupied, the system will tell you which program has occupied the port. Please stop the occupied 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	47-51	4-50		10-37											
	15	52	51-56	3.1-10.1	8-43	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	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 it to log out and return to the login interface.

Modify Password: click it to change the password of the current login user. Enter the current password and then set a new password in the popup window. Click "OK" to save the new password.

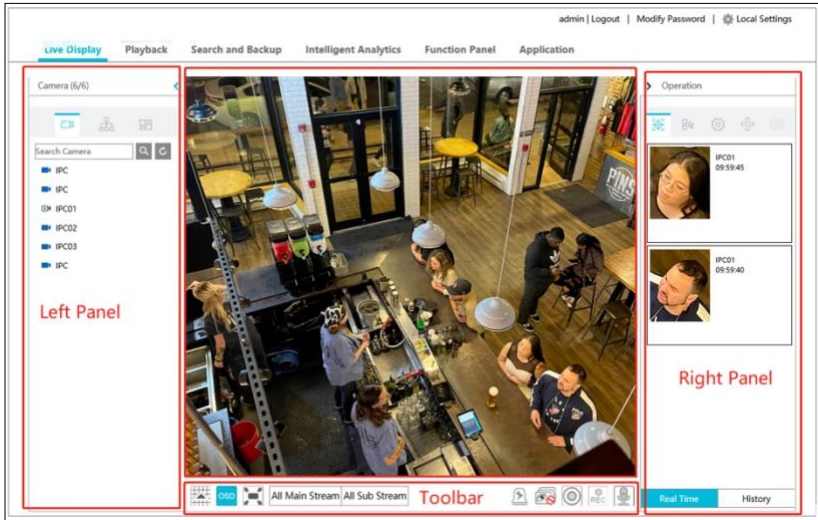
Local Settings: click it to change local settings. Set the snapshot number and click "Browse" to set a snapshot path and record path as shown below. Click "Apply" to save the settings.

Snapshots number	5	v
Save snapshots to	C:\Users\Administrator\Pictures	Browse
Save record files to	C:\Users\Administrator\Videos	Browse
Apply		

Here, web client access with the plug-in installed is used as an example.

16.4.1 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 play the camera in the window. You can click  on 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 amount of added cameras and the amount of 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 added cameras. Enter a camera name in the search box and then click  to search for that camera. Click  to refresh the camera list.

● View Group

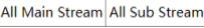
Click  to view groups. The top side of the left panel displays all the groups and the bottom side displays all the cameras in the group.

● View Scheme

Click  to view schemes. All schemes can be shown in the left panel. Double

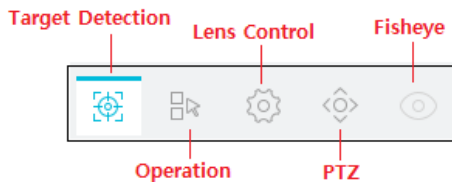
click the scheme name to display it.

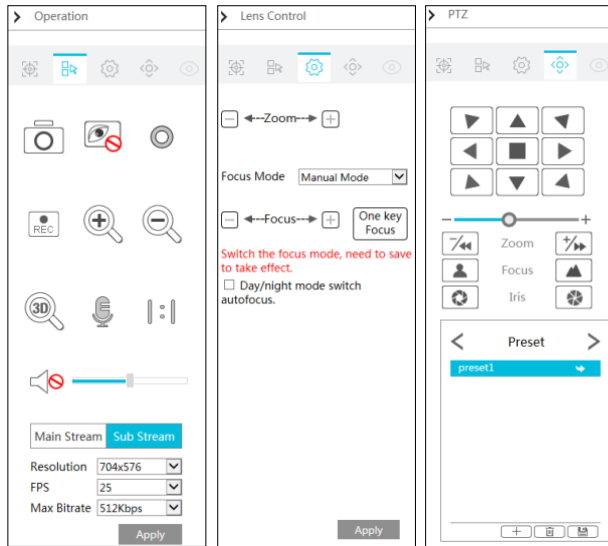
➤ Tool Bar Introduction

Button	Meaning
	Screen mode button.
	Click to enable/disable OSD.
	Click to show full screen. Right click on the full screen to exit full screen.
	Click “All Main Stream” or “All Sub Stream” to set the stream of all the cameras.
	Manual alarm button. Click to bring up a window and then trigger and clear the alarm-out in the window manually.
	Click to preview all the cameras.
	Click to close all the preview cameras.
	Click to start recording for all cameras to the computer. Click  to stop recording.
	Click it to start recording all the cameras to the NVR. Click  to stop recording.
	Click it to enable talk with the NVR.

➤ Right Panel Introduction

Click  on the right panel to show the panel and click  to hide the panel.





Click one camera window in the preview area and then click **Main Stream** to set the camera's live preview stream and recording stream to the main stream in manual recording mode; click **Sub-stream** to set the camera's live preview stream and recording stream to the sub stream. In the sub stream tab, set the resolution, FPS and bitrate and then click "Apply" to save the settings.

Operation panel introduction:

Button	Meaning
	Click to take a snapshot of the camera.
	Click to start recording to the computer
	Click to start recording to the NVR.
	Click to zoom in on the image of the camera and then drag the mouse on the camera image to view the other areas.
	Click to zoom out the image of the camera.
	Click to start two-way talk.
	The 3D zoom in function is designed for P.T.Z.s. Click it and then drag the image to zoom in or zoom out the image; click the image on different areas to move the image of the dome omni-directionally.
	Click to close the preview camera.
	Click to display the camera's original proportions
	Click to enable audio and then drag the slider bar to adjust the volume. You can listen to the camera audio by enabling audio.

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.
	Click / to zoom in/out the camera image.
	Click / to increase/ decrease the focal length.
	Click / to increase/decrease the iris of the dome.
Preset	Click to view the preset list and then click a button in the list to call that preset. Click to add a new 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 it 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 recording.

If the camera you added is a 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 decode the fisheye image.

16.4.2 Remote Playback

Click “Playback” in the remote interface to go to the playback interface.

- ① Check the recording event types and cameras on the left panel. Set a recording date on the calendar beside the time scale.
- ② Click Search to search the recording 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 interface of the NVR. Please refer to [8.2 Playback Interface Introduction](#) for details.

1. Introduction of playback control buttons:

Button	Meaning
	Stop button.
	Rewind button. Click it to play video backwards.
	Play button. Click it to play video forwards.
	Pause button.
	Deceleration button. Click it to decrease the playing speed.
	Acceleration button. Click it to increase the playing speed.

Button	Meaning
	Previous frame button. 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.
	Click  to step backward 30s and click  to step forward 30s.
	Backup start time button. Click the time scale and then click it to set the backup start time.
	Backup end time button. Click the time scale and then click it to set the backup end time.
	Backup button.
	Backup tasks button. Click it to view the backup download status.
	Event list button. Click it to view the event records of manual/schedule/sensor/motion recording.

16.4.3 Remote Search and Backup

Click “Search and Backup” in the remote interface to go to the backup interface. You can back up recordings by event or by time.

➤ By Event

Check the recording 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 recordings (the searched recording data will be displayed in the list); check the recording data in the list and then click “Backup” to back it up.

➤ 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 back up the recording.

Image Management: Click “Image Management” to go to image management interface. The system will display all captured images automatically in this list. Click  to delete an image. Click  to bring up the “Export” window. Click  to bring up the “View Image” window. Click  to export the image.

View Backup Status: Click “Backup Status” to view the backup download status. Click “Pause” to pause; click “Resume” to continue the backup; click “Delete” to delete the task.

16.4.4 Intelligent Analysis

1. This function is only available for models with VCA (video content analysis) functions.

Click “Intelligent Analysis” in the remote interface to configure smart search, statistics, face database, face attendance, and face check in. All these settings are similar to that of the NVR. See the configurations of the NVR for details.

16.4.5 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

these settings are similar to that of the NVR. See the configurations of the NVR for details.

16.4.6 Remote Configuration

Click “Function Panel” in the remote interface and then configure the camera, recording mode, alarm, disk, network, account and authority, and system of the NVR remotely. All these settings are similar to that of the NVR. See the configurations of the NVR for details.

➤ Jumping to an IPC Web Client

Other than IP cameras accessed with RTSP protocol, the IPC web client can be directly opened from the NVR web client by clicking  in the above-mentioned interface.

1. Please login to the Web Client of the NVR (See [14.2 Web LAN Access](#) or [14.3 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	Upgrade	Version
1	IPC	10.20.23.37	9008	Offline	IP Camera	IPC						
2	IP Camera01	10.10.10.153	9008	Online								7208
3	IPC	10.20.52.201	9008	Online	IP Camera							8020

3. Select the camera and click  to log in to the web client of the camera. Then you can set the parameters of the camera as needed.

Appendix A FAQ

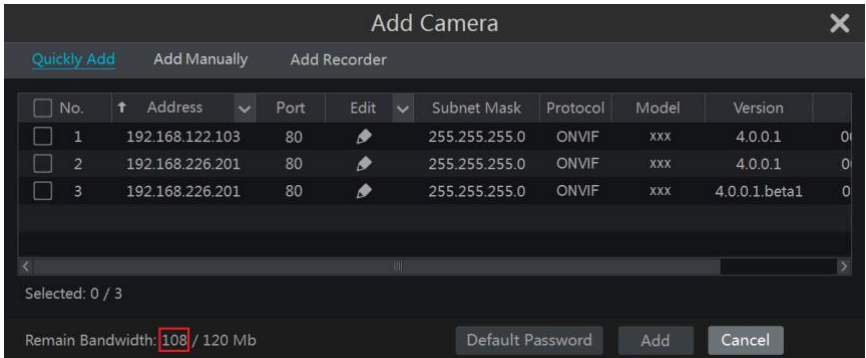
- Q1.** Why can't I see the hard drive in my unit?
- Please check the power and SATA data cables of the HDD to make sure they are well connected.
 - For some NVRs with a 1U or small 1U case, other power adapters may supply enough power to operate them. Please use the power adaptor supplied along with the NVR.
 - Please make sure the HDDs are compatible with the NVR. See [Appendix C Compatible Device List](#) for details.
 - The HDD could have gone bad.
- Q2.** Why are there no images output in some or all of the camera windows?
- Please make sure the resolutions of the cameras are supported by the NVR.
 - Please make sure the network cables of the IP cameras and NVR are connected properly and the network parameters are set correctly.
 - Please make sure the network and the switch both work normally.
- Q3.** What if the screen has no output after booting up the NVR normally?
- Please make sure the screen, HDMI cables, or VGA cables are good and connected properly.
 - Please make sure the screen supports one of the following resolutions: 1280*1024, 1920*1080 or 3840*2160 (4K*2K). The NVR cannot self-adapt to a screen with a resolution lower than 1280*1024, and then the screen will remind you that the screen resolution is not supported by the NVR or will simply have no display. Please change to a screen at least at the resolution 1280*1024, 1920*1080 or 3840*2160 before booting the NVR.
- Q4.** What if I have Forgotten my Password?
- The password for **admin** can be reset with the previously configured security question by selecting "Retrieve Password" from the login screen. Please go to the "Edit Security Question" function in Account and Authority to set this up.

Click an option in the drop-down menu under Question, and then enter the corresponding answer of the selected question in the Answer box below it. After you correctly answer the question, you can reset the password for **admin**. If you forgot the answers for the questions, or did not set a security question up, please contact your dealer for help.

- The passwords of other users can be reset by **admin**, please refer to [13.1.2 Edit User](#) for details.

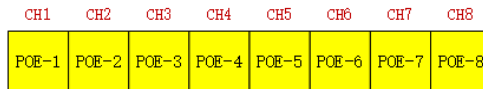
Q5. Why can't the NVR add the maximum number of IP cameras?

Take a 16 CH NVR as an example. Some 16 CH NVR support a maximum of 120Mbps bandwidth input (please refer the real device for details). Refer to the picture below. The remaining bandwidth should be larger than the bandwidth that the IP camera you want to add takes up or you cannot add the IP camera. You must lower the bitrate of the added cameras to lower the used bandwidth. It is recommended to add cameras by "Quickly Add" for batch adding.



Q6. An IP camera Connected to the PoE port of the NVR is not displaying automatically in the camera list, why?

- Please check whether the resource of the PoE port is occupied by another IP camera that is added through network.
- Take an 8 CH NVR with 8 PoE ports as an example. If an IP camera is added to the system through the network before any cameras are added by plugging directly into the back of the NVR, it will occupy channel 1. Now when you plug a camera into POE port 1 on the back of the NVR, it will cause a resource error. You'll want to add the cameras plugged into the back of the unit first and then start to add IP cameras through the network to take up the remaining channels.



- Please make sure that the internal Ethernet port and an ONVIF IP camera directly connected to the PoE port on the back of the NVR are in the same network segment or the camera will fail to be added to the system. Not all ONVIF cameras are fully compatible with our systems.

Log in the ONVIF IP camera's web client and then enable DHCP (obtain an IP address automatically); or manually change the IP address to match the IP scheme and address of the internal ethernet port it is being plugged into on the back of the NVR. By default, this will be 10.151.151.10X, with X = the number of the port on the back of the unit. Not all ONVIF cameras can be added by directly plugging them into the NVR and may need to be added through an external POE switch.

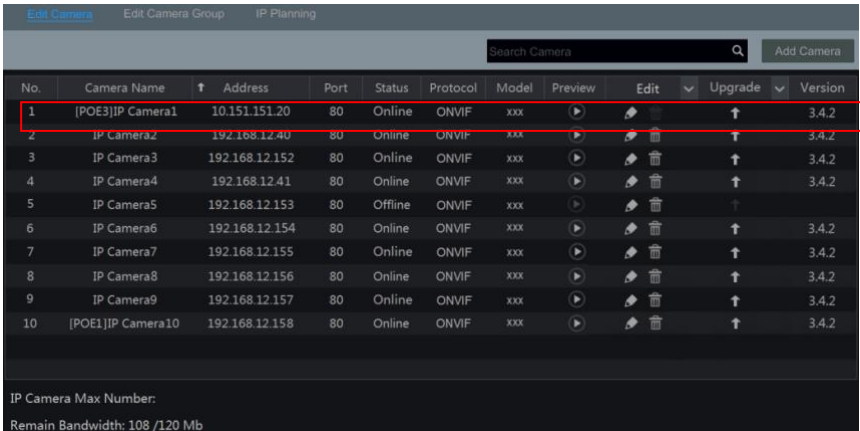
- Check whether the number of the added IP camera is at the maximum.

If the number of the added IP camera is at the maximum, the system will show you a message stating that the IP camera number is beyond the maximum when you directly connect another IP camera to the available PoE port and thus you will fail to add the IP camera.

Q7. A 3rd party IP camera directly connected to the PoE port of the NVR using the ONVIF protocol is shown in the camera list, but there is no image output, why?

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				3.4.2
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 preview interface and then click  in the preview window of the IP camera to edit the IP camera's username and password.

1. The system is not recording, why?

- Make sure the HDD was formatted prior to use.
- The recording schedule has not been set in customization mode. Please refer to [7.1.2 Schedule Settings](#) for details.
- The HDD may be full and thus the NVR is not able to record. Check HDD information from Disk Management and if required, please enable the recycle function (please see [7.1.3 Advanced Configuration](#) for details).
- There is no disk but cameras in a disk group, so please add at least one disk to that group. Refer to [7.4.2 Storage Mode Configuration](#) for details.
- The HDD could have gone bad. Please change to another one.

Q8. Why can't I access the NVR remotely through Edge Browser?

- Please make sure that Internet Explorer mode is turned on in Edge's settings and the tab is set to run in IE Mode. (Units above a certain firmware work without using IE mode, please contact your dealer for information if needed.)
- Please check whether the PC has a firewall enabled or antivirus software installed. Please try to access the NVR again after you disable the firewall and stop the antivirus software or allow the plugin through the firewall or antivirus rules, please refer to the manufacturer of the antivirus or firewall for instructions on how to do this.
- The allow & block list may have been set in Account and Authority setting. The PC's IP address may be in the block list or is not in allow list and cannot access the NVR remotely.

Q9. Why is the Plugin not being allowed to run?

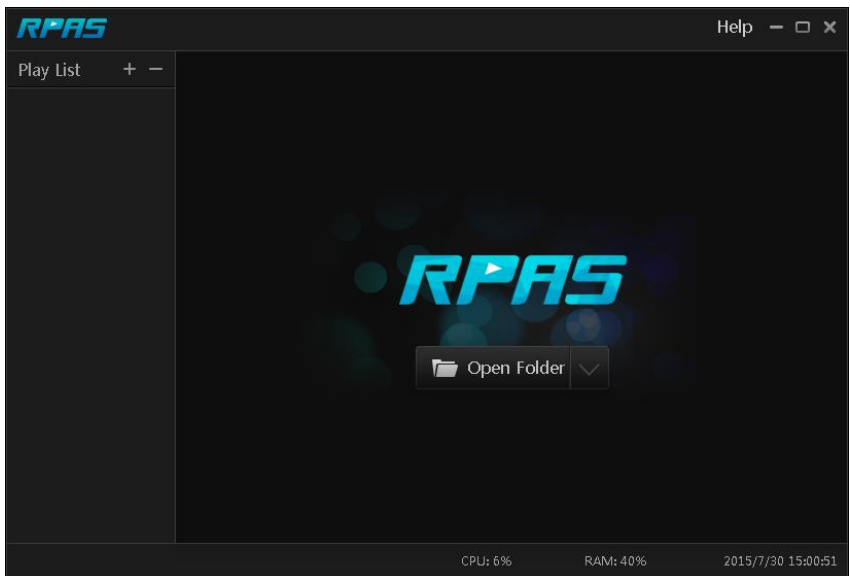
- a. Other plug-ins or anti-virus may be blocking the web interface plugin. Please disable or white list the plugin in the antivirus software or figure out what other plugin may be blocking it.

Q10. How do I play backup files?

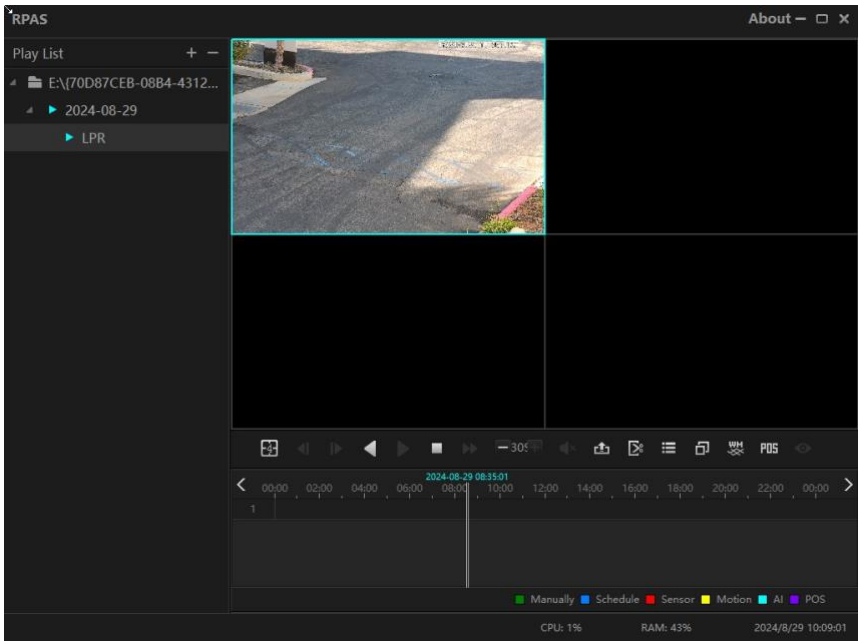
- a. Recorded video backed up by NVR: insert the USB device with the recorded video backup files saved on it to the USB interface of the PC and then open the USB device path. The recorded video can be backed up in the private format or the AVI format by NVR.
- If you select the private format when backing up recorded video by NVR, a RPAS Player will also 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 recording. Click  on the tool bar under the camera image to enable audio.

- If you select the AVI format when backing up recorded video from the NVR, the recorded video backup data can be played with a video player which supports this format. VLC Media Player is recommended.
- b. Recorded video backed up through web. Recorded video can only be backed up with AVI format through the web. The recorded video can be backed up to PC and played by a video player which supports this format.



2. Fig 11-1



3. Fig 11-2

Q11. HTTPs service aren't working normally after directly installing the signed certificate.

- When importing the certificate, the private key may not be attached to the certificate.
- When importing the certificate, the private key is attached to the certificate, but it is encrypted. At present, the NVR doesn't support certificates with an encrypted private key.

Q12. You are prompted with unsafe warnings when using HTTPs service.

- Please make sure your certificate is trusted.
- Make sure the Common Name (domain information) of the certificate matches with the domain name of the visiting website.
- Make sure the certificate is within the period of validity.

Appendix B: Calculate Recording Capacity

The recording capacity is mainly up to the recording resolution, recording stream, and bitrate. Different image quality parameters dictate different amounts of space needed to save the footage. The higher the recording resolution, recording stream, and recording bitrate is, the more disk capacity is taken for the same duration of footage. The calculation format of recording capacity is shown below.

Recording Capacity (MB) = Bitrate(Kbps) ÷ 1024 ÷ 8 × 3600 × Recording hours per day × Record Storage Days × channel numbers

3600 equals recording 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 30 days of recording storage.

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, a 32CH NVR is recording 24 hours per day and keeping the recordings for 30 days. The NVR adopts a dual stream recording. 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 ($49.45\text{TB} \div (1-10\%)$).

Appendix C Compatible Device List

4. 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

5. Compatible USB mobile device

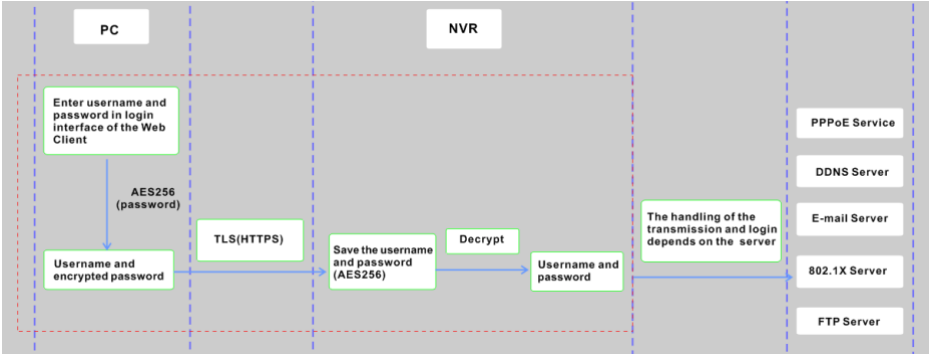
Brand	Capacity
SSK	2GB
Netac	4GB
Kingston	2GB/8GB/16GB/32GB
Aigo	2GB
Smatter vider	1GB
SanDisk	4GB/8GB/16GB/32GB

Appendix D: Communication Port List

Port	Protocol(TCP/UDP)	Descriptions
80	TCP	Description: HTTP communication port. It open by default and used to access the WEB client. Authentication: Username and password Encryption: NO
443	TCP	Description: HTTPS communication port. It is open by default and used to access the WEB client. Authentication: Username and password Encryption: TLS
554	TCP	Description: 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. Authentication: Username and password (Digest) Encryption: NO
6036	TCP	Description: Private communication port. It is opened by default and used to transfer audio and video stream. Authentication: Username and password (Digest) Encryption: AES
9036	TCP	Description: This port is opened by default which is mainly used to receive the information sent by a POS terminal or printer. The information will be overlaid on the image of the IPC you have configured in previewing or recording mode. Authentication: NO Encryption: NO
41952	TCP	Description: This port is open by default which is mainly used to receive requests sent by other UPnP devices and communicate with other UPnP devices. Authentication: NO Encryption: NO
41953	TCP	Description: This port is closed by default. After the UPnP function is enabled, this port is enabled too. It is mainly used to receive requests sent by other UPnP devices and communicate with other UPnP devices. Authentication: NO Encryption: NO
1900	UDP	Description: This port is open by default which is used to enable, find, and run SSDP. Additionally, it is also used to listen to and receive multicast packets from other online UPnP devices. Authentication: NO Encryption: NO

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.



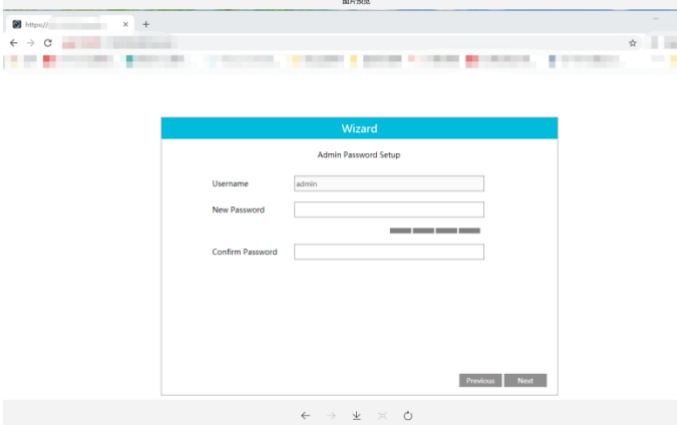
Function	Personal Data Type	Transmission Type	Storage Type	Authentication
PPPoE	Username, Password	TLS+AES256(password)	Password: AES256	Username/Password
DDNS	Username, Password	TLS+AES256(password)	Password: AES256	Username/Password
E-mail	Username, Password, E-mail address	TLS+AES256(password)	Password: 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:
Other than for service authentication when communicating

with the server, we will never share personal data stored on the device to a third-party or use them 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 a password, or you cannot access the device. 
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 a password. You must set the password for “admin” in the above-mentioned interface first. Then you can log in by using “root”.

6. Statement:

Remote testing/debugging isn't supported for this device (Telnet/SSH are 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 to 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 hime 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 rmdir 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

Specifications: VT-TNR414PN

Video Input / Resolution	4 IP Channels up to 8 MegaPixel (4K)
Main Monitor Output	1 × 4K HDMI / 1 × 1080P VGA
Multi Operation	Pentaplex: Live Display/Record/Playback/Backup/Remote Access
Recording Compression	H.265S / H.265+ / H.265 / H.264
Recording	120fps (30fps per channel)
Audio over IP Inputs	4 (IP Camera Dependent)
Local Audio In/Out	IN: RCA × 1CH / OUT: RCA × 1CH
Two-Way Audio*	YES
Recording Modes	Manual / Timer / Motion / Sensor
Analytics	License Plate Recognition, Tripwire, Intrusion, Object Detected / Missing, Exception, Crowd Density, People Counting, Human/Vehicle Classification
Search	Time sliced image search, Time/Calendar search, Event (Motion, External alarm), Tag search
Alarm Modes	Sensor, Motion, Video loss, IP conflict, Disk error, Illegal access, Network disconnection
Network Interface	RJ45 × 1 (LAN/WAN) + RJ45 × 4 with PoE
PoE Standard	802.3af 12W max per port
Total PoE Budget	48W all ports
Bit Rate (Per Camera)	512Kbps ~ 10 Mbps (Adjustable)
Total Bandwidth	40Mbps Incoming / 40Mbps Outgoing
Network Protocols	TCP/IP, UDP, DHCP, DNS, PPPOE, DDNS, Email, UPNP, NAT, Telnet
Remote Viewing	CMS / Web Browser / Mobile Platforms
Backup	Network, USB
SATA HDD	20TB Total (SATA × 1, Max 20TB each)
USB	USB 2.0 × 2 (for mouse and USB backup device)
Power Consumption, Supply	≤ 10W (Without HDD), 48V/1.25A
Dimensions (W × H × D)	11.81" × 1.77" × 9.80" (300mm × 45mm × 249mm)
Weight Net, Shipping w/o HDD	2.62, 4.74lbs (1.19, 2.15kg)

Specifications: VT-TNR818PN

Video Input / Resolution	8 IP Channels up to 8 MegaPixel (4K)
Main Monitor Output	1 × 4K HDMI / 1 × 1080P VGA
Multi Operation	Pentaplex: Live Display/Record/Playback/Backup/Remote Access
Recording Compression	H.265S / H.265+ / H.265 / H.264
Recording	240fps (30fps per channel)
Audio over IP Inputs	8 (IP Camera Dependent)
Local Audio In/Out	IN: RCA × 1CH / OUT: RCA × 1CH
Two-Way Audio*	YES
Recording Modes	Manual / Timer / Motion / Sensor
Analytics	License Plate Recognition, Tripwire, Intrusion, Object Detected / Missing, Exception, Crowd Density, People Counting, Human/Vehicle Classification
Search	Time sliced image search, Time/Calendar search, Event (Motion, External alarm), Tag search
Alarm Modes	Sensor, Motion, Video loss, IP conflict, Disk error, Illegal access, Network disconnection
Network Interface	RJ45 × 1 (LAN/WAN) + RJ45 × 8 with PoE
PoE Standard	802.3af 12W max per port
Total PoE Budget	72W all ports
Bit Rate (Per Camera)	512Kbps ~ 10 Mbps (Adjustable)
Total Bandwidth	80Mbps Incoming / 80Mbps Outgoing
Network Protocols	TCP/IP, UDP, DHCP, DNS, PPPOE, DDNS, Email, UPNP, NAT, Telnet
Remote Viewing	CMS / Web Browser / Mobile Platforms
Backup	Network, USB
SATA HDD	20TB Total (SATA × 1, Max 20TB each)
USB	USB 2.0 × 2 (for mouse and USB backup device)
Power Consumption, Supply	≤ 10W (Without HDD), 48V/1.8A
Dimensions (W × H × D)	11.81" × 1.77" × 9.80" (300mm × 45mm × 249mm)
Weight Net, Shipping w/o HDD	2.69, 5.1lbs (1.22, 2.34kg)

Specifications: VT-TNR1626PN

Video Input / Resolution	16 IP Channels up to 8 MegaPixel (4K)
Main Monitor Output	1 × 4K HDMI / 1 × 1080P VGA
Multi Operation	Pentaplex: Live Display/Record/Playback/Backup/Remote Access
Recording Compression	H.265S / H.265+ / H.265 / H.264
Recording	480fps (30fps per channel)
Audio over IP Inputs	16 (IP Camera Dependent)
Local Audio In/Out	IN: RCA × 1CH / OUT: RCA × 1CH
Two-Way Audio*	YES
Recording Modes	Manual / Timer / Motion / Sensor
Analytics	License Plate Recognition, Tripwire, Intrusion, Object Detected / Missing, Exception, Crowd Density, People Counting, Human/Vehicle Classification
Search	Time sliced image search, Time/Calendar search, Event (Motion, External alarm), Tag search
Alarm Modes	Sensor, Motion, Video loss, IP conflict, Disk error, Illegal access, Network disconnection
Network Interface	RJ45 × 1 (LAN/WAN) + RJ45 × 16 with PoE
PoE Standard	IEEE802.3AF/AT
Total PoE Budget	<150W
Bit Rate (Per Camera)	512Kbps ~ 10 Mbps (Adjustable)
Total Bandwidth	144Mbps Incoming / 144Mbps Outgoing
Network Protocols	TCP/IP, UDP, DHCP, DNS, PPPOE, DDNS, Email, UPNP, NAT, Telnet
Remote Viewing	VMS / Web Browser / Mobile Platforms
Backup	Network, USB
SATA HDD	40TB Total (SATA × 2, Max 20TB each)
USB	USB 2.0 × 2 (for mouse and USB backup device)
Power Consumption, Supply	≤ 10W (Without HDD), 48V/3.75A
Dimensions (W × D × H)	14.96" × 10.55" × 1.77" / 380mm × 268mm × 45mm
Weight Net (w/o HDD)	3.92lbs / 7.94lbs (1.78kg / 3.60kg)

Specifications: VT-TNR818PFN

Video Input / Resolution	8 IP Channels up to 12 MegaPixel
Main Monitor Output	1 × 4K HDMI / 1 × 1080P VGA
Multi Operation	Pentaplex: Live Display / Record / Playback / Backup / Remote Access
Recording Compression	H.265S / H.265+ / H.265 / H.264
OS	Embedded Linux
Recording	160fps @ 12MP (20fps/ch.), 240fps @ 8MP (30fps/ch.)
Audio over IP Inputs	8 (IP Camera Dependent)
Local Audio In/Out	IN: RCA x 1CH / OUT: RCA x 1CH
Two-Way Audio	YES
Decoding - Live View	1CH 12MP / 4CH 1080P
Recording Modes	Manual / Timer / Motion / Sensor
Local Playback	8CH
Gen. IV Analytics	Regional Entrance / Exit Detection, Line Crossing, Target Counting [Human / Motor Vehicle Classification] Face Detection [FD], Object Missing / Abandoned, Video Blur, Color Cast Detection, Abnormal Video + Supports LPR IP Cameras & Fisheye Dewarping
Search	Time sliced image search, Time/Calendar search, Event (Motion, External alarm), Tag search
Smart Search	Highlighted color to display certain time periods - colors refer to different recorded events
Alarm Modes	Sensor, Motion, Video loss, IP conflict, Disk error, Illegal access, Network disconnection
Alarm Inputs	8 CH local alarm input, 4 CH output
Alarm Triggering	Schedule Recording, NO / NC, Time Duration, Record Configuration, Snapshot, Presets, Push Notification, Alarm Out, Buzzer, Pop-up Video, Pop-up Message, Email
Network Interface	RJ45 × 1 (1000mbps)
PoE Ports / PoE Standard	RJ45 × 8, with PoE, Output Power <96W / IEEE802.3AF
Total PoE Budget	96W all ports
Bit Rate (Per Camera)	512Kbps ~ 10 Mbps (Adjustable)
Total Bandwidth	80Mbps Incoming / 80Mbps Outgoing
Dual-stream	Individual Network Video Stream and local recording stream, set separately
Network Protocols	TCP/IP, UDP, DHCP, DNS, PPPOE, DDNS, Email, UPNP, NAT
Remote Viewing	VMS / Web Browser / Mobile Platforms
RS 485	Yes (full-duplex), Connect to PTZ or Keyboard
Backup	Network, USB
SATA HDD	40TB Total (SATA × 2, Max 20TB each)
PTZ Protocol	Through Network
USB	USB 3.0 × 1, USB 2.0 × 2
Pwr Consumption / Supply	≤ 20W (Without HDD and PoE Power Supply) / 48V/2.5A
Working Environment	14°~122°F / -10°C ~ 50°C @ 10% ~ 90% RH
Dimensions (W × H × D)	11.81" × 1.77" × 9.78" (300mm × 45.0mm × 248.5mm)
Weight (Net / Shipping)	2.69lbs / 5.16lbs, 43.03oz / 82.54oz, 1.22kg / 2.34kg

Specifications: VT-TNR1646PFN

Video Input / Resolution	16 IP Channels up to 12 MegaPixel
Main Monitor Output (HDMI1, HDMI 2, VGA)	HDMI x 1 : 3840 × 2160 / 1920 × 1080 / 1280 × 1024, HDMI 2 & VGA x 1: 1920 × 1080 / 1280 × 1024 [*HDMI and VGA output the same Video Source]
Multi-Screen Display	Main Output: 1/4/6/8/9/13/16 (Live View), AUX output: 1/4/6/8/9 (live view) [Max. 16+9CH local live view]
Multi Operation	Pentaplex: Live Display / Record / Playback / Backup / Remote Access
Recording Compression	H.265S / H.265+ / H.265 / H.264
OS	Embedded Linux
Recording Resolution	240fps @ 12MP (20fps/ch), 480fps @ 8MP [4K] or less (30fps/ch)
Audio over IP Inputs	16 (Camera Dependent)
2-Way Audio, Local Audio In/Out	YES, IN: RCA × 1Ch. / OUT: RCA × 1Ch. G.711 (U/A Compression)
Encode	CBR / VBR
Recording Modes	Manual / Timer / Motion / Sensor / Alarm / AI
File Management	Reserving time, Redundancy, Dual Stream Recording
Local Playback	16Ch.
Gen. IV Advanced Analytics [Camera Dependent]	Regional Entrance/Exit, Line Crossing, Target Counting [All by Human/Motor Vehicle Classification] Face Detection [FD], Object Abandoned/Missing, Video Blur, Color Cast, Abnormal Video + License Plate Recognition & Fisheye Dewarping [WEB & APP]
Face Detection	16Ch., 32 Libraries (10,000 Face pics), 18 pics/sec Computing, Search by Pic, Add/Modify/Delete/Search Pics, Add pics w/ App, Web, Ext. Import, Supports Allow/Block Lists and Stranger Match Alarm, Track Display on Map, Bar Graph Stats by Time Period
License Plate Recognition	Supports Overview and Cut-Out of Plate, 10,000 Plate Database, 0-75mph (120kmph) Capture Speed (Installation Dependent)
360° Camera De-Warping	Multiple Views include 360° Overview, Quad, Overview + 3 Views, and Single View [Web & App]
Search	Time Sliced Image Search, Time/Calendar Search, Event (Motion, External Alarm), Tag Search
Smart Search	Highlighted Color to Display Certain Time Periods - Colors Refer to Different Recorded Events
Alarm Modes	Sensor, Motion, Video loss, IP conflict, Disk Error, Illegal access, Network Disconnection, Smart Events
Alarm In/Output & Triggering	16 CH Local Alarm Input, Supporting IPC Alarm Input / 4 CH Output, Record / Snap / PTZ Move, Alarm Out / E-mail
Network Interface	RJ45 10 / 100 / 1000 Mbps × 2
Total Bandwidth	160Mbps/160Mbps
Dual-stream	Individual Network Video Stream and local recording stream, set separately
Network Protocols	TCP/IP, PPPoE, DHCP, DNS, DDNS, UPnP, NTP, SMTP, RTSP, HTTP, HTTPS, 802.1x, SNMP, ONVIF
Remote Viewing	VMS / Web Browser / Mobile Platforms [iOS, Android]
Backup	Network, U Disk, USB Mobile HDD
SATA HDD	80TB Total (SATA x4, Max 20TB each)
USB	USB 3.0 × 1, USB × 2.0 × 2
RS485	RS485 (Full-Duplex), Connect to PTZ
PTZ Protocol, Support	Through Network or RS485 (Pelco D / Pelco P), PTZ Preset and Auto Cruise, up to 255 Presets and 8 Cruises
Power Consumption / Supply	≤ 20W (Without HDD) / AC 110/220V (ATX 300W)
Working Environment	14°F~122°F (-10°~50°C) / 10~90% RH
Dimensions (WxDxH)	17.32 × 15.35 × 2.76" (440 × 390 × 70mm)
Weight	Net: 9.59lb (4.35kg), Gross: 12.46lb (5.65kg)

Specifications: VT-TNR3216PFN

Video Input / Resolution	32 IP Ch. up to 12 MP: 12/8/6/5/4/3MP/1080P/1280x1024/960P/720P
Main Monitor Output (HDMI1, HDMI 2, VGA)	HDMI 1: 3840x2160 @60fps/30fps, 1080P/1280x1024/1024x768, HDMI 2: 1920x1080/1280x1024/1024x768, VGA: 1920x1080/1280x1024/1024x768
Multi-Screen Display	Main Output: 1/4/6/8/9/13/16/25/32/36 (Live View), AUX Output: 1/4/6/8/9 (Live View), Max. 32 + 9Ch. Local View
Multi Operation	Pentaplex: Live Display / Record / Playback / Backup / Remote Access
Recording Compression	H.265S / H.265+ / H.265 / H.264
OS	Embedded Linux
Recording Resolution	640fps @ 12MP (20fps per channel), 960 fps ≤8MP (30fps per channel)
Audio over IP Inputs	32 (Camera Dependent)
2-Way Audio, Local Audio In/Out	YES, IN: RCA × 1Ch. / OUT: RCA × 1Ch. G.711 (U/A Compression)
Encode	CBR / VBR
Recording Modes	Manual / Timer / Motion / Sensor / Alarm / AI
File Management	Reserving time, Redundancy, Dual Stream Recording
Local Playback	16Ch.
Gen. IV Advanced Analytics [Camera Dependent]	Regional Entrance/Exit, Line Crossing, Target Counting [All by Human/Motor Vehicle Classification] Face Detection [FD], Object Abandoned/Missing, Video Blur, Color Cast, Abnormal Video + License Plate Recognition & Fisheye Dewarping [WEB & APP]
Face Detection	32Ch., 32 Libraries (10,000 Face pics), 18 pics/sec Computing, Search by Pic, Add/Modify/Delete/Search Pics, Add pics w/ App, Web, Ext. Import, Supports Allow/Block Lists and Stranger Match Alarm, Track Display on Map, Bar Graph Stats by Time Period
License Plate Recognition	Supports Overview and Cut-Out of Plate, 10,000 Plate Database, 0-75mph (120kmph) Capture Speed (Installation Dependent)
360° Camera De-Warping	Multiple Views include 360° Overview, Quad, Overview + 3 Views, and Single View [WEB & APP]
Search	Time Sliced Image Search, Time/Calendar Search, Event (Motion, External Alarm), Tag Search
Smart Search	Highlighted Color to Display Certain Time Periods - Colors Refer to Different Recorded Events
Alarm Modes	Sensor, Motion, Video loss, IP conflict, Disk Error, Illegal access, Network Disconnection, Smart Events
Alarm In/Output & Triggering	16Ch. / 4Ch. / Record, Snap, Alarm out, E-mail
Network Interface	RJ45 10 / 100 / 1000 Mbps × 2
Total Bandwidth	192Mbps Incoming / 192Mbps Outgoing [384Mbps Total]
Dual-stream	Individual Network Video Stream and local recording stream, set separately
Network Protocols	TCP/IP, PPPoE, DHCP, DNS, DDNS, UPnP, NTP, SMTP, RTSP, HTTP, HTTPS, 802.1x, SNMP, ONVIF
Remote Viewing	VMS / Web Browser / Mobile Platforms [iOS, Android]
Backup	Network, U Disk, USB Mobile HDD
SATA HDD	160TB Total (SATA × 8, Max 20TB each)
USB	USB 3.0 × 1, USB 2.0 × 2
RS485	RS485 (Full-Duplex), Connect to PTZ
PTZ Protocol, Support	Through Network or RS485 (Pelco D / Pelco P), PTZ Preset and Auto Cruise, up to 255 Presets and 8 Cruises
Power Consumption / Supply	<30W (No HDD), ATX300W (PoE)
Working Environment	14°F~122°F (-10°~50°C) / 10~90% RH
Dimensions (W×D×H)	17.52 × 17.17 × 3.54" (445 × 436 × 90mm)
Weight	Net: 12.57 lbs (5.7kg), Gross: 16.13lbs (7.4kg)

Specifications: VT-TNR3280E1N

Video Input / Resolution	32 IP Ch. up to 12 MP: 12/8/6/5/4/3MP/1080P/1280×1024/960P/720P
Main Monitor Output (HDMI1, 2, VGA)	1: 3840×2160, 1080P/1280×1024/1024×768, 2: 1920×1080/1280×1024/1024×768, VGA: 1920×1080/1280×1024/1024×768
Multi Operation	Pentaplex: Live Display / Record / Playback / Backup / Remote Access
Multi Screen Display	Main: 1/4/6/8/9/13/16/25/32/36 (Live), AUX output: 1/4/6/8/9 (live view), Max. 32+9CH local live view
Recording Compression	H.265+ / H.265 / H.265S / H.264
OS	Embedded Linux
Recording Resolution	640fps @ 12MP (20fps per channel), 960 fps ≤8MP (30fps per channel)
Audio over IP Inputs	32 (Camera dependent)
2-Way Audio	Yes
Local Audio In/Out	IN: RCA × 1CH / OUT: RCA × 1CH
Audio Compression	G.711 (A/U)
Recording Stream	Dual stream recording
Recording Modes	Manual / Timer / Motion / Sensor
Simultaneous Playback	Max 16Ch
Playback Function	Play, pause, FF, FB, digital zoom
Smart Search	Highlighted color to display the camera recording in a certain period of time, different colors refer to different recording events
Decode: Live View/Playback	1CH 12MP@20fps / 4CH 1080P
GEN IV Analytics Support	Regional Entrance / Exit Detection, Line Crossing, Target Counting (All by Human / Motor Vehicle Classification) Face Detection, Crowd Density, Abandoned / Missing Object, Abnormal Video
Face Detection Support	32Ch, 32 Libraries (10,000 Face pics), 18 pics/sec Computing, Search by Pic, Add/Modify/Delete/Search Pics, Add pics w/ App, Web, Ext. Import, Supports Allow/Block Lists and Stranger Match Alarm, Track Display on Map, Bar Graph Stats by Day, Week, Month, Quarter, Custom
360° Camera De-Warping	Supports de-warping via Web Client or App: Multiple Views include 360° Overview, Quad, Overview + 3 Views, and Single View
License Plate Recognition	Yes (AI by IPC)
Search	Time sliced image search, Time/Calendar search, Event (Motion, External alarm), Tag search
Alarm Modes	Manual, sensor, motion, exception, smart events
Alarm In / Out / Triggering	16CH / 4CH / Record, Snap, Preset, Buzzer, E-mail
Network Interface	RJ45 x 2 (10/100/1000Mbps)
Total Bandwidth	320 Mbps / 256 Mbps (Incoming / Outgoing)
Dual-stream	Individual Network Video Stream and local recording stream, set separately
Network Protocols	TCP/IP, PPPoE, DHCP, DNS, DDNS, UPnP, NTP, SMTP, RTSP, HTTP, HTTPS, 802.1x, SNMP, ONVIF
Remote Viewing	VMS / Web Browser / Mobile Platforms (iOS, Android)
Remote Users	128 Simultaneous Online Users
Backup	Network, U Disk, USB Mobile HDD
SATA HDD	160TB Total (SATA × 8, Max 20TB each) + E-Sata × 1
USB	USB 2.0 × 2, USB 3.0 × 1
PTZ Protocol	Through Network
PTZ Support	PTZ Preset and Auto Cruise, up to 255 Presets and 8 Cruises
Remote Control	Yes
Power Consumption	<30W (No HDD)
Power Supply	ATX250W
Working Environment	14~122°F, 10% ~ 90% humidity
Dims. (W × D × H)	17.52 × 17.17 × 3.54" (445 × 436 × 89mm)
Weight	Net: 12.57 lbs (5.7kg) / Gross: 16.13lbs (7.4kg)
Certificates	CE, FCC
Environmental Protection	Directive EU RoHS, REACH and WEEE

LIMITED PRODUCT WARRANTY

This VITEK product carries a three (3) year limited warranty. VITEK warrants to the purchaser that products manufactured by VITEK are free of any rightful claim of infringement or the like, and when used in the manner intended, will be free of defects in materials and workmanship for a period of three (3) years, or as otherwise stated above, from the date of purchase by the end user. This warranty is nontransferable and extends only to the original buyer or end user customer of a VITEK Authorized Reseller.

The product must have been used only for its intended purpose, and not been subjected to damage by misuse, willful or accidental damage, caused by excessive voltage or lightning.

The product must not have been tampered with in any way or the guarantee will be considered null and void.

This guarantee does not affect your statutory rights.

Contact your local VITEK Reseller should servicing become necessary.

VITEK makes no warranty or guarantee whatsoever with respect to products sold or purchased through unauthorized sales channels. Warranty support is available only if product is purchased through a VITEK Authorized Reseller.

CLASS A DIGITAL DEVICE (INDUSTRIAL & COMMERCIAL ENVIRONMENT)

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to CE and FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.



28492 CONSTELLATION ROAD VALENCIA, CA 91355
WWW.VITEKCCTV.COM