Ossia WNVR

User Manual

Models:

- All Supporting Devices (NVR5)

Index

Index **2**

1. Terms & Conditions **9**

1. Introduction **11**

1.1 Summary 11

1.2 Features 11

1.3 Front Panel Description: 13

1.4 Rear Panel Description: 15

1.5 IPC Description 15

1.6 Connections 16

1.6.1 Alarm Input (Availability depends on model): 16

1.6.2 Alarm Output (Availability depends on model): 17

1.6.3 RS-485 (Availability depends on model): 17

2. Basic Operations Guide **18**

2.1 Startup & Shutdown 18

2.1.1 Startup 18

2.1.2 Shutdown 18

2.2 Mouse Control 18

2.3 Text Input 18

3. Wizard & Main Interface **19**

3.1 First Startup Wizard 19

3.1.1 Language and Region 19

3.1.2 Privacy Statement 20

3.1.3 Date and Time 20

3.1.4 Admin setting 20

3.1.5 IPC Activation Password 21

3.1.6 Channel IP Planning 21

3.1.7 Password Recovery Email 22

3.1.8 Password Recovery Question 22

3.2 Standard Startup Wizard 23

3.2.1 Network settings 24

3.2.2 Disk Setting 24

3.2.3 Record Settings: 25

3.2.4 QR Code / NAT: 26

3.2.5 Cloud Upgrade: 26

3.2.6 Disk Settings:.....27
3.3 Main Interface.....28
3.3.1 Main Interface Introduction.....28
4. Camera Management.....30
4.1 Add/Edit Camera.....30
4.1.1 Add Camera.....30
4.1.2 Quick Add Camera.....30
4.1.3 Editing IP Address of Specific Camera.....31
4.1.4 Editing IP Address of Several Cameras.....31
4.1.5 WI-FI Match.....31
4.1.6 Add Manually.....31
4.1.7 Add Recorder:.....32
4.1.8 Auto Report:.....33
4.2 Edit Camera's General Parameters.....33
4.2.1 Edit Camera's name:.....34
4.2.2 Change camera's password:.....34
4.2.3 Delete Cameras:.....34
4.2.4 Update IPC Firmware:.....34
4.3 "In-Channel Sequence".....35
4.3.1 Add "In-Channel Sequence".....35
4.3.2 Edit In-Channel Sequence.....35
4.4 IPC Networking.....36
4.4.1 IP Camera management.....36
4.4.2 Device Management.....36
4.5 Repeater.....37
5. Live View Introduction.....39
5.1 Live View Interfaces:.....39
5.2 Fish-Eye Display:.....40
5.3 Digital Zoom:.....40
5.4 Live-View Modes:.....41
5.4.1 Display Modes Tabs.....41
5.4.2 Customized Display Mode.....41
5.4.3 Sequence.....42
5.4.4 In Channel Sequence.....43
5.4.5 Object detection.....44
5.5 Cloud Update.....46
5.6 Emergency Live-View:.....46

5.7 Image Configuration 46
5.7.1 OSD Settings 46
5.7.2 Image Settings (Setting Interface) 47
5.7.3 Mask Settings 48
5.7.4 Smart Supplement Light 48
5.7.5 Fish-Eye 48
5.7.6 Image Adjustment (Live-View Interface) 49

6. PTZ 51

6.1 PTZ Control Interface: 51
6.2 Preset/Cruise (PTZ Live interface): 52
6.3 Preset/Cruise (PTZ Configuration Menu): 53
6.4 Auto Tracking: 54
6.5 Home Position (Park Action): 54

7. IP Speaker 55

7.1 Add IP Speaker: 55
7.2 Edit IP Speaker: 56
7.3 Delete IP Speaker: 56

8. Record & Disk Management 56

8.1 Record Configuration: 56
8.1.1 Mode Configuration: 56
8.1.2 Advanced Configuration 58
8.2 Encode Parameters Setting 59
8.2.1 Main Stream recording 59
8.2.2 Sub-Stream recording 59
8.3 Schedule Setting 60
8.3.1 Add Schedule 60
8.3.2 Record Schedule Configuration 61
8.4 Record Mode 61
8.4.1 Manual Recording 61
8.4.2 Scheduled Recording: 62
8.4.3 Motion Based Recording: 62
8.4.4 Sensor Based Recording: 62
8.5 Analytics Based Recording: 62
8.5.1 POS Based Recording: 62
8.6 Disk Management: 63
8.6.1 Storage Mode Configuration 63

8.6.2 Disk Mode (Models supporting RAID only):.....64
8.6.3 Physical Disk (Models supporting RAID only):.....64
8.6.4 Array (Models supporting RAID only):.....65
8.6.5 View Disk and S.M.A.R.T. Information:.....65

9. Standard Search, Playback & Backup.....65

9.1 Instant Playback.....65

9.2 Playback Interface Introduction.....66
9.2.1 Standard Playback.....66
9.2.2 Smart Playback.....69

9.3 Record Search, Playback & Backup.....71
9.3.1 Search & Playback by Time-sliced Image.....71
9.3.2 Search, Playback & Backup by Time:.....73
9.3.3 Search, Backup & Playback by Event.....74
9.3.4 Search & Playback by Tag.....74
9.3.5 Snapshots.....75
9.3.6 Backup Procedures.....75
9.3.7 View Backup Status.....75

10. Analytics Interface.....76

10.1 Local Analytics Engine (If applicable):.....76

10.2 Analytics Search.....76
10.2.1 Face.....76
10.2.2 Human.....77
10.2.3 Vehicle.....77
10.2.4 Combine.....78

11. Event Management.....78

11.1 Event Notification.....78
11.1.1 Alarm-out.....78
11.1.2 E-mail.....78
11.1.3 Display.....78
11.1.4 Buzzer.....78
11.1.5 Push Message.....78
11.1.6 Audio Message.....79
11.1.7 Light.....80
11.1.8 Alarm Server.....80

11.2 Analytics.....80
11.2.1 AI Type Selection (Applicable devices only).....81
11.2.2 Perimeter Monitoring (DDA):.....81
11.2.3 Line Crossing Configuration.....83
11.2.4 Face Recognition (Applicable devices only).....84

11.2.5 LPR (License Plate Recognition – For LPR Cameras only) 85
11.2.6 Video Metadata (Applicable devices only) 86
11.2.7 Thermal (Applicable devices only) 87
11.2.8 Others: 87
11.3 Databases 90
11.3.1 Face Database 90
11.3.2 LPR Database 91
11.3.3 Exporting databases: 92
11.3.4 Importing databases: 92
11.4 General Event Alarms 92
11.4.1 Motion Alarm 92
11.4.2 Motion Configuration 92
11.4.3 Motion Alarm Triggers Configuration 93
11.4.4 Sensor 93
11.4.5 Combined Alert 93
11.4.6 IPC Offline Settings 94
11.4.7 General Fault Settings 94
11.5 Manual Alarm 94
11.6 Burglar Alarm Linkage 94
11.7 Alert Status 95
11.8 Triggers: 96
11.8.1 Record: 96
11.8.2 Snap: 96
11.8.3 Push: 96
11.8.4 Alarm-out: 96
11.8.5 Preset: 96
11.8.6 IP Speaker: 96
11.8.7 Buzzer: 96
11.8.8 Pop-up Video: 96
11.8.9 Pop-up Message Box: 96
11.8.10 E-mail: 96
12. Account & Permission Management 97
12.1 Account Management 97
12.1.1 Add User 97
12.1.2 Edit User 98
12.2 Permission Management 98
12.2.1 Add Permission Group 98
12.2.2 Edit Permission Group 99
12.3 User Login & Logout 99

12.4 Security 99
12.4.1 Block and Allow Lists 99
12.4.2 Preview on Logout 99
12.5 Network Security 100
12.6 Password Security 100
12.7 Check Point Protection (If Applicable) 101
12.8 Password Recovery Settings 101
12.9 Double Verification 101
12.10 User Status: 102
12.10.1 Online Users 102

13. Device Management 103

13.1 Network Configuration 103
13.1.1 TCP/ IPv4/6 Configuration 103
13.1.2 Port Configuration 103
13.1.3 HTTPS Configuration 104
13.1.4 API Server 106
13.1.5 RTSP 106
13.1.6 DDNS Configuration 106
13.1.7 E-mail Configuration 107
13.1.8 UPnP Configuration 107
13.1.9 NAT Configuration 108
13.1.10 FTP Configuration (For supported device) 109
13.1.11 SNMP Configuration 109
13.1.12 Cloud Upgrade 109
13.1.13 WI-FI 110
13.2 Network Stream 111
13.2.1 Network Stream Settings 111
13.3 Integration 111
13.3.1 ONVIF 111
13.3.2 Auto-Report Configuration 111
13.4 Network Status 112
13.4.1 View Network Status 112
13.5 Basic Configuration 112
13.5.1 General Settings 112
13.5.2 Date and Time Configuration 113
13.5.3 Layout settings: 113
13.5.4 POS settings: 114
13.5.5 PoE Power Management: 114
13.5.6 OSD Settings: 114

13.6 Maintenance:.....115
13.6.1 View Log.....115
13.6.2 Factory Default.....115
13.6.3 Device Software Upgrade.....115
13.6.4 Backup and Restore.....116
13.6.5 Auto Maintenance:.....116
13.6.6 Diagnostic Data:.....116
13.6.7 View System Information.....116
13.6.8 WIFI Camera Maintenance.....117

14. Applications.....117

14.1 Parking Lot Management.....117
14.1.1 Configure.....117
14.1.2 Parking.....117
14.1.3 Entrance and Exit.....118
14.1.4 Monitoring.....118
14.2 Access Control Management.....118
14.3 Face Attendance.....118
14.4 Face Check-In.....118

1. Terms & Conditions

- We strongly advise users to read this manual and keep it for later use for proper and safe device usage.

- Please use the provided & authorized by Provision-ISR technician power supply and power source indicated on the marking label. The power voltage must be verified before use.

- Avoid improper operation, shock vibration, and heavy pressing that can cause product damage.

- Do not use corrosive detergents when cleaning. When necessary, please use a soft dry cloth to wipe the dirt off; use neutral detergents for problematic pollution & decay. Any cleanser for high-grade furniture is applicable.

- Keep away from heat sources such as radiators, heat registers, stoves, etc.

- Do not try to repair the device without technical aid or approval.
- For camera installations:
- Avoid aiming the camera directly towards extremely bright objects, such as the sun, which may damage the image sensor.
- Please abstain from reversing the camera. This will result in an inverted image. Please follow the instructions for proper camera installation.
- Do not operate the camera in extreme temperatures or extreme humidity conditions.
- For Recorder & server installations:
- Do not block any ventilation openings and ensure proper airing around the device.
- Perform a safe shutdown before disconnecting from power. Otherwise, HDD damage and configuration loss might occur.
- This device is for indoor use only.
- Do not install this device near water, nor expose it to rainy or moist environments. If any solids or liquids get inside the device's case, turn the device off immediately and have it checked by a qualified technician.

- The instructions in this manual are suitable for all models running Ossia OS. Models which do not support any of the features will have explicit markings.

- For devices with internal power supply, please ensure that the AC 220/110V input selector is set correctly.

- There may be incorrect info or printing errors in this manual. PROVISION-ISR reserves the right to change this manual and publish the revision online on our website (www.provision-isr.com); there may be inconsistencies with the latest

version, which apply to any software upgrades and product improvements, interpretation and modification added. Updates and corrections are subject to change without notice.

- All pictures and examples used in the manual are for reference purposes only.

- When this device is in use, the relevant contents of Microsoft, Apple and Google are involved. The ownership of trademarks, logos, and other intellectual properties related to Microsoft, Apple, and Google, belong to the companies mentioned above.

1. Introduction

1.1 Summary

This series of devices running Ossia OS are designed to provide unconditional security for homes, offices, banks, schools, supermarkets, petrol service stations, residential quarters, factories, Etc. In can be accessed from local or remote locations.
The Ossia OS was designed specifically to answer the user's needs. It is based on the most advanced SOC technology and adopts a new and intuitive human GUI. This series of the devices is more powerful than any older device produced by Provision-ISR. It is easy to use while providing excellent image quality and system stability.

1.2 Features

Basic Functions:

- Support live view, record and configuration of IP cameras
- All Ossia devices support the latest H.265 (HEVC) video coding stream and a mixture input of H.265 and H.264 IP cameras.
- Support standard ONVIF protocol*
- ONVIF Profile T/G Support (As ONVIF Device)
- ONVIF Profile S Support As Host
- Support dual stream recording of each camera
- Support IPC Quick add*
- Support batch or single configuration of IP cameras (OSD, video parameters, mask, motion, alarms, Etc.) *
- Support a maximum of 8 user permission groups including Administrator, Advanced and Ordinary which are the default permission groups of the system
- Support a maximum of 16 users.
- Support a numerous web client's login at the same time (According to device's specs)
- Analytics support*

Live Preview Features:

- 8K*/4K*/2K*/1920×1080/1280×1024 HDMI and 1920×1080/1280×1024 VGA high-definition synchronous display (This may vary according to your model. Please refer to your device technical specs for more information)
- Multi-screen modes such as 1/4/6/8/9/16/25/32 (depends on model)
- Auto adjustment of the camera's image display proportion
- IPC audio monitoring (can be enabled or disabled)*
- Manual snapshot of the previewed camera
- Customized setting the sequence pages
- Support saving of the display modes. The saved modes can be called directly
- One channel operation tool bar
- Camera group view and scheme view in sequence and quick sequence view
- Motion detection and video masking
- Full PTZ control including setting up the presets and cruises
- Direct mouse control over the PTZ cameras including movement, zoom and focus.

- Intuitive Digital-Zoom can be controlled directly from the mouse wheel
- Image adjustment (only available for some cameras)

HDD Support:

- 3U Case support up to 16 SATA HDDs
- 2U Case support up to 8 SATA HDDs
- 1.5U Case support up to 4 SATA HDDs
- 1U Case support up to 2 SATA HDDs
- Small 1U/MM Case support up to 1 SATA HDD
- Each SATA interface of the device supports the HDDs with max 10TB storage capacity Except of MM models whish support up to 6TB only)
- E-SATA HDD for Record/Backup*

Disk Management:

- The HDDs can be grouped for configuration and management.
- Each camera can be added into different disk group with different storage capacity
- RAID Support*
- The system allows batch formatting of the HDDs

Record Configuration:

- Support simultaneous main stream and sub-stream recording (Configurable).
- Batch or single configuration of the record stream
- Manual and auto record modes
- Schedule, sensor alarm, motion, analytics, POS recording
- Configure different record streams for schedule recording and event recording setting
- Support record duration setting and recycle recording
- Support pre-alarm recording and post alarm recording configuration for event recording

Playback:

- Time scale operation in quick playback. Also, the playback date and time can be set easily by scrolling the mouse wheel. The intervals of the time scale can be zoomed in/out.
- Record searching by Image-slice/time/event/tag
- Time image slice searching by month, by day, by hour and by minute and time. The slice is displayed by image thumbnail
- Up to 16 channels to be searched by time
- Event searching by manual/motion/sensor events
- Tag searching (for tags manually added by user)
- Instant playback of selected camera within the live preview interface
- Up to 16 synchronous playback channels (Depends on devices)

Record Backup

- Backup through USB (U-disk, mobile HDD) or E-SATA* interface
- Backup by time/event/image searching
- Customized backup selection while playing back
- Up to 10 backup tasks running in the background

Alarm Management:

- Alarm schedule setting

- Supports enabling or disabling of motion detection, external sensor alarm input and exception alarms including IP address conflict alarm, disk I/O error alarm, disk full alarm, no disk alarm, illegal access alarm, network disconnection alarm and IPC offline alarm.
- Configurable alarm trigger
- Alarms can trigger PTZ Operation, snapshots, pop-up videos and more.
- Event notification modes: Alarm-out, pop-up video, pop-up message box, buzzer and E-mail
- E-mail schedule support
- Snapped images can be attached to the e-mail when alarm triggered
- Alarm information status for alarm-in, alarm-out, motion detection and exception alarm
- Alarm can be triggered and cleared manually
- System auto reboot when HDD or I/O exception happens – in order to restart and recover the HDD

Network Functions:

- TCP/IP and PPPoE, DHCP, DNS, DDNS, UPnP, NTP, SMTP, RTSP protocols
- "Allow & Block" lists according to IP or MAC addresses
- Multiple browser support for Windows and Mac OS
- Remote configuration and maintenance including remote upgrading and remote system reboot
- Remote camera configuration of the device including video parameters, image quality, Etc.*
- Remote search, playback and backup.
- CMS or other management software can access the device and manage it.
- Support Cloud connection (NAT) and QR Code scanning by smart phones and tablets
- Support mobile surveillance by smart phones or tablets running iOS or Android OS
- Telnet function can be enabled or disabled by the user for remote maintenance

Other Functions:

- The device can be controlled and operated by the supplied mouse or remote controller
- Standard remote Mouse can be used (Not supplied)
- Quick device information view including basic details, camera status, alarm status, record status, network status, disk and backup status
- Support auto recognition of the display resolution

*Supported models only

1.3 Front Panel Description:

The following descriptions are for reference only.

Type I (MM/Small 1U/1.5U Models):

Name	Descriptions
REC	While recording, the light is blue
NET	When accessed by network the light is blue
PWR	When powered on, the light is blue

Type II (2U Models):

Name	Descriptions
Power	When powered on, the light is blue
HDD	The light turns blue when reading/writing HDD
Net	The light turns blue when the devices accesses the network
Backup	The light turns blue when backing up files and data
Play	The light turns blue when playing back video
REC	When recording, 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 Menu
INFO	Check the information of the device
BACKUP	Enter backup mode in live
SEARCH	Enter search mode in live
Exit	Exit the current interface
	Manual record
	Play/Pause
	Speed down
	Speed up
1-9	Input digital number and select camera
0/--	Input number 0, the number above 10
Direction Key	Change direction
Multi-Screen Switch	Change the screen mode
Enter	Confirm selection
USB	To connect external USB device like USB mouse or USB flash

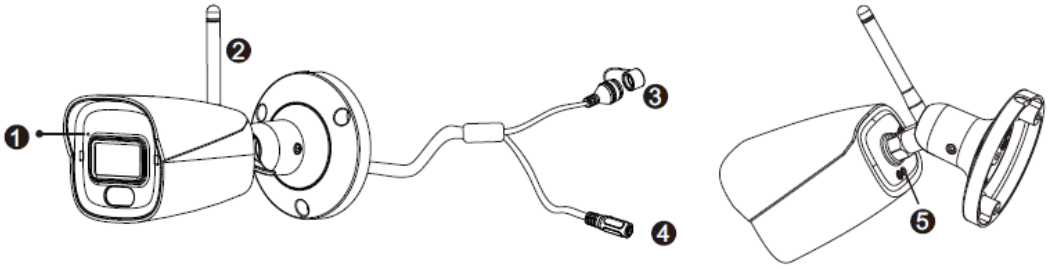
1.4 Rear Panel Description:

In this section we will introduce you to a few samples of rear panels. Of course, we cannot include all rear panels of all the available devices. Please take this manual as reference only.

No.	Name	Descriptions
1	Ground	Ground interface
2	Antennas	Connect antennas for WIFI comms to supported ipcs
3	DC12V	DC12V power input
4	LAN	Network port
5	VGA	Connect to VGA monitor
6	HDMI	Connect to HD display
7	USB	Connect USB storage device or USB mouse. USB3.0 interfaces will be colored in blue.
8	AUDIO OUT	Audio output

1.5 IPC Description

No.	Name	Descriptions
1	Microphone	Microphone for hearing sound
2	Antenna	Antenna for WIFI signal increase
3	Reset*	Reset: press and hold for 3s to reset to the factory default settings and then enter the Wi-Fi match mode (white led blinks).
4	Power input	DC12 v
5	Ground	Grounding for camera voltage discharge



1.6 Connections

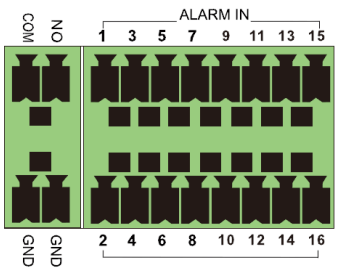
Video Output Connections:
Video Output: Supports VGA/1 HDMI or more. You can connect to monitor through these video output interfaces simultaneously or independently. (Depends on the mode)

Audio Connections:
Audio Input: Connect to microphone, etc.
Audio Output: Connect to headphone, Speaker or other audio output devices.

Alarm Connections:
Only selected models support this function. See below 16 CH alarm inputs and 1 CH alarm output for example.

1.6.1 Alarm Input (Availability depends on model):

Alarm IN 1~16 are 16CH alarm input interfaces. There are no type requirements for sensors. NO type and NC type are both available and can be configured from the device interface. The method to connect sensors to the device is as shown below:

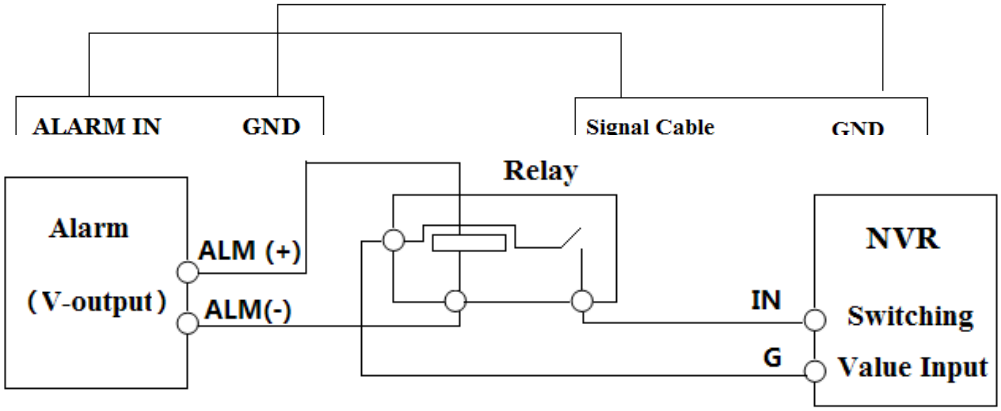


The alarm input is an open/close relay. If the input is not an open/close relay, please refer to the following connection diagram:

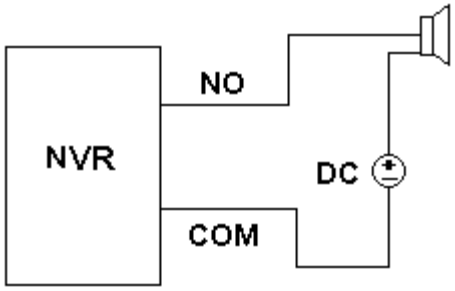
1.6.2 Alarm Output (Availability depends on model):

The way to connect alarm output device:

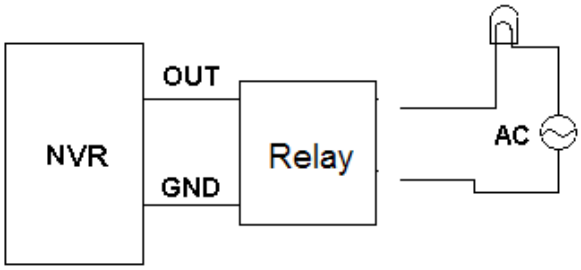
Pull out the green terminal blocks and loosen the screws in the alarm-out port. Then insert



the signal wires of the alarm output devices into the port of NO and COM separately. Finally, tighten the screws. Provided that the external alarm output devices need power supply, you can connect the power supply as per the following figures.



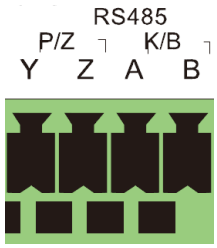
(Option 1)



(Option 2)

1.6.3 RS-485 (Availability depends on model):

There are two types of RS485 interfaces:



(Type 1)

(Type 2)

Type 1: The P/Z is for PTZ cameras – Not applicable for NVR devices. The K/B interface is used to connect the C06 control keyboard.

Type 2: The RS485 interface is used to connect control keyboard and PTZ cameras (This connector cannot be used for PTZ control in NVR devices. A is TX+; B is TX-.

2. Basic Operations Guide

2.1 Startup & Shutdown

Please make sure all the connections are done properly before you power on the device. Proper startup and shutdown are crucial for prolonging the lifespan of the device.

2.1.1 Startup

1. Connect the output display device to the VGA/HDMI interface of the device.
2. Connect the USB mouse and network cable
3. Connect the power. The device will boot and the power LED would turn blue.
4. A Wizard window will pop up (you should select the display language the first time you use the device).

2.1.2 Shutdown

1. Click Start→Shutdown to pop up the Shutdown window. Select “Shutdown” in the window. The unit will power off after a while by clicking “OK” button.
2. Disconnect the power.

2.2 Mouse Control

Mouse control in Live Preview & Playback interface:
In the live preview & playback interface, double click on any camera window to show the video in single screen mode; double click the window again to restore it to the previous split.

If the interfaces display in full screen, move the mouse to the bottom or to the right side of the interface to pop up the relevant tool bar. The tool bar 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 click the box. When required to input text the keyboard will pop up automatically.

2.3 Text Input

The system includes two input keyboard layouts as shown the above pictures. The left box is the number input keyboard and the right box is the general input keyboard which provides inputs of numbers, letters and punctuation characters as shown below

Button	Meaning	Button	Meaning
	Backspace key		Switch to punctuation characters
	Delete Key		Enter key
	Switch key between upper and lower-case letters		Space key

3. Wizard & Main Interface

3.1 First Startup Wizard

The first startup wizard will only appear on the initial startup of the device, or after the device has been reset to factory default. It takes the user through all the initial mandatory step required to prepare the system for use.

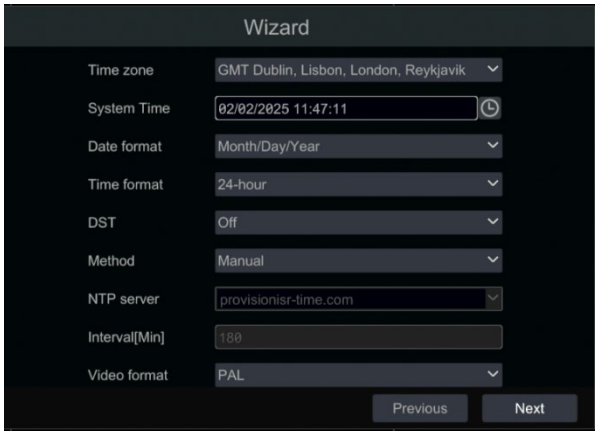
3.1.1 Language and Region

The first step is to set the system language and locality of the system. The language selection will not affect any setting except of the system language. The Locality selection will automatically set the following: Video System (PAL/NTSC), Time-zone, Time keeping settings, IP/TCP, Ports, NAT and recording settings according to your local requirements

3.1.2 Privacy Statement

The second step is to read and confirm Provision-ISR's and Check Point's user privacy statement and License agreement. Please read it thoroughly as it states all the information shared with Provision-ISR when using each one of the offered services (NAT, DDNS, Push Notification Etc.)

3.1.3 Date and Time

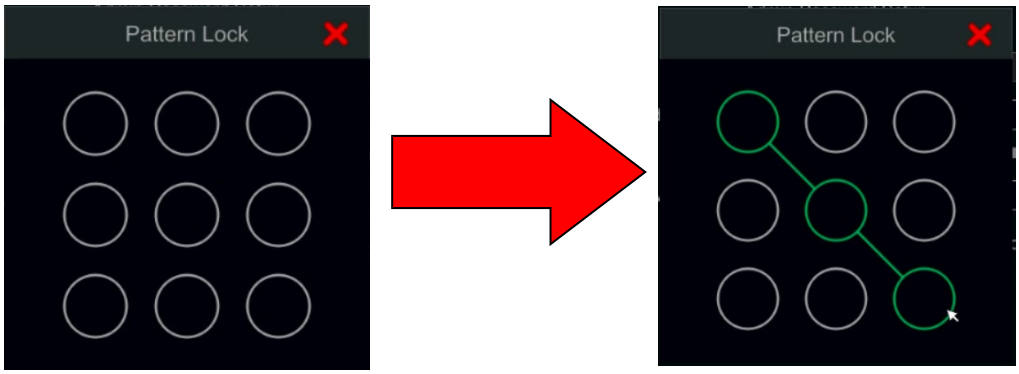


The date and time of the system must be configured when you use the wizard for the first time. It is automatically configured based on the locality settings you set on the first stage, but you can now edit it if required. Set the time zone, system time, date format and time format. The DST will be enabled by default if the time zone selected includes DST. The "Method" line allows you to change from manual setting to NTP (Network Time Protocol) setting which will synchronize the time with the configured NTP server with the set interval. The default NTP server is "provisionisr-time.com" and the interval is set to 180 minutes but you can change it to any other NTP server as you wish. Here you can also set the Video Format to PAL/NTSC as required. Changing this setting will reboot the system at the end of the wizard. Click "Next" to continue.

3.1.4 Admin setting

Set your own admin password. The default username is admin and cannot be changed. There are no default settings and this step cannot be skipped. The initial settings require a minimum of 8-character password that includes at least one letter, one digit, and one special character.

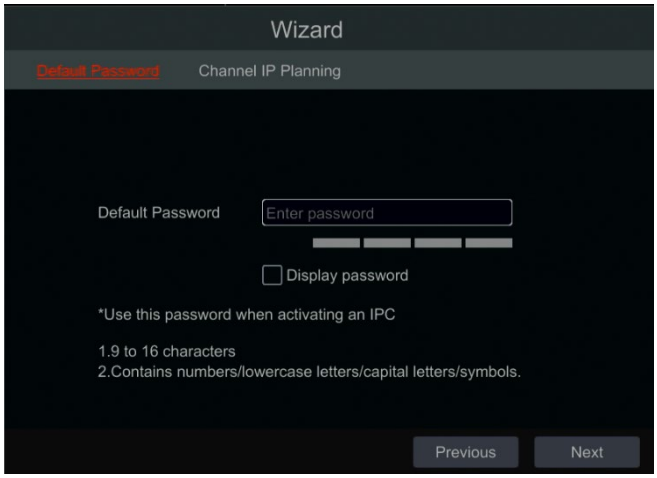
In this step you can also set a “Pattern” password that could be used for login into the device. It is simpler and more fluid to use the pattern lock when using a mouse and screen only (without a keyboard). If you wish to use pattern lock, enable it and click “edit” to set it as follows:



Click “Next” to continue.

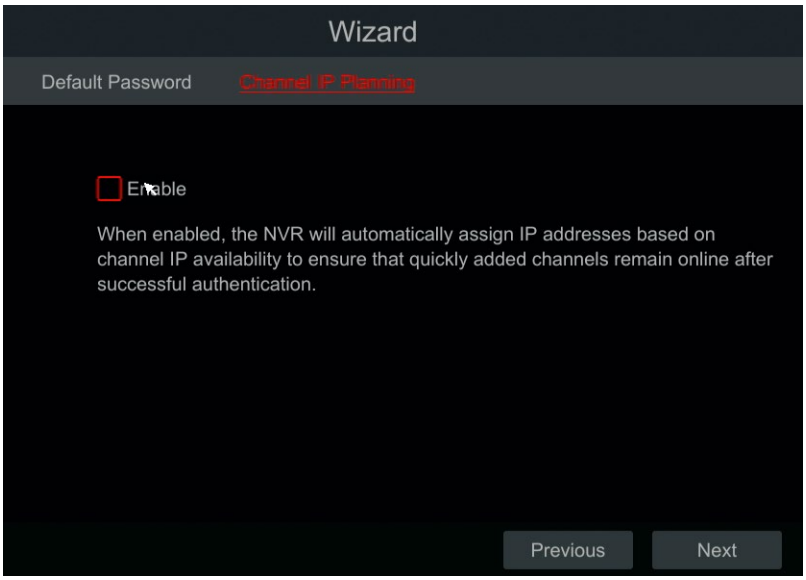
3.1.5 IPC Activation Password

Set up a unique password for IPC activation. This password can be used whenever an non-activated IPC is found on the LAN.



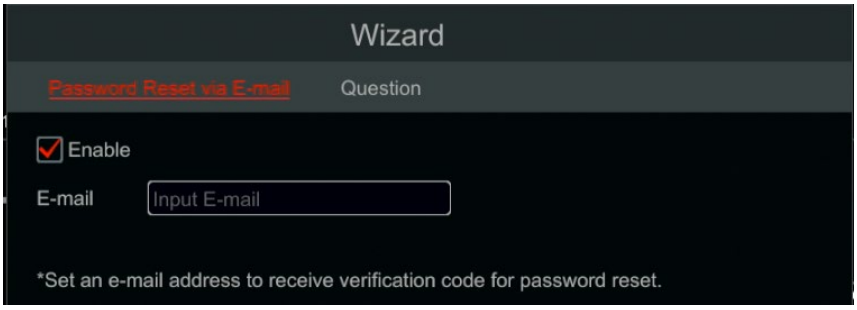
3.1.6 Channel IP Planning

When an IP camera is not on the same segment as the NVR, the NVR will change the IPC address to the same segment as his. Preventing cameras from being offline.



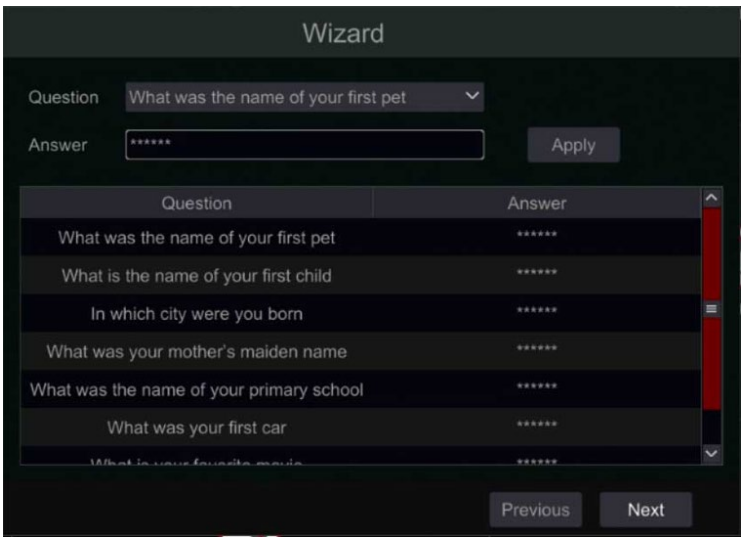
3.1.7 Password Recovery Email

Setting an Email for recovery will allow you to get a recovery password directly to your email without the need for any other details or the help of the support.

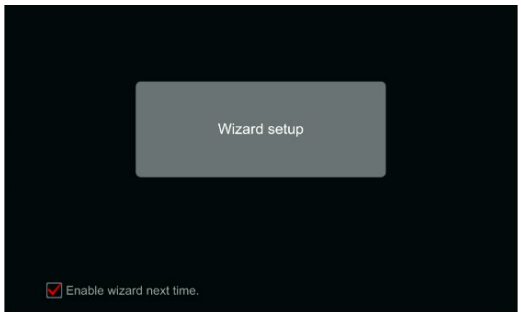


3.1.8 Password Recovery Question

In the “Password Recovery” you must set at least one question and answer for password recovery. If you will ever forget the password – these questions will be used to restore the password to factory default. Please refer to Q4 in Appendix A FAQ for details.
Choose the question you wish to answer. Input the answer and click on “Apply”. Only one question is required.



3.2 Standard Startup Wizard



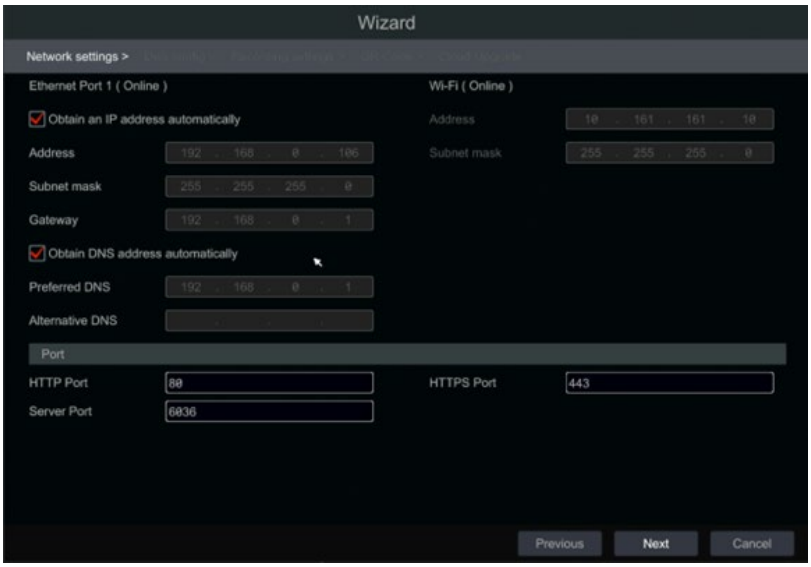
On each startup, the disk icons will be shown on the top of the interface. You can view the number and status of each disk quickly and conveniently through these icons

1. No disk
2. Unavailable disk
3. R/W available disk

You can quickly and easily configure the device using the setup wizard. The wizard can also be skipped and will be shown in the next startup unless the “Enable wizard next time” was unticked.

3.2.1 Network settings

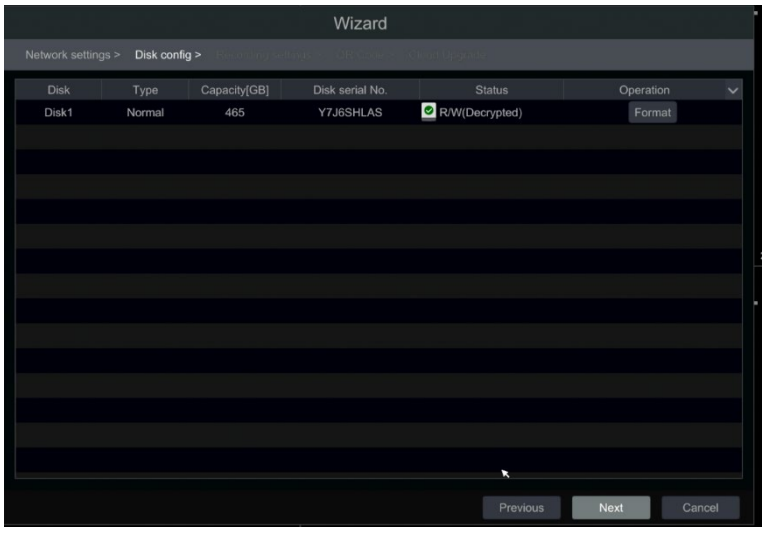
Check “Obtain an IP address automatically” and “Obtain DNS automatically” to get the IP address and DNS automatically (You must have a DHCP Service enabled in your network). Uncheck it in order to input it manually. Input the HTTP port, RTSP port and Server port.



WIFI: The WIFI section is enabled by default. It is used to connect the KIT's WIFI cameras to the NVR automatcially. The NVR does not onnect to other networks via WIFI. Only via ethernet cable.
Click next to continue.

3.2.2 Disk Setting

You can view the disk status, number, capacity and serial number. Click “Format” to format the disk. Click “Next” to continue.

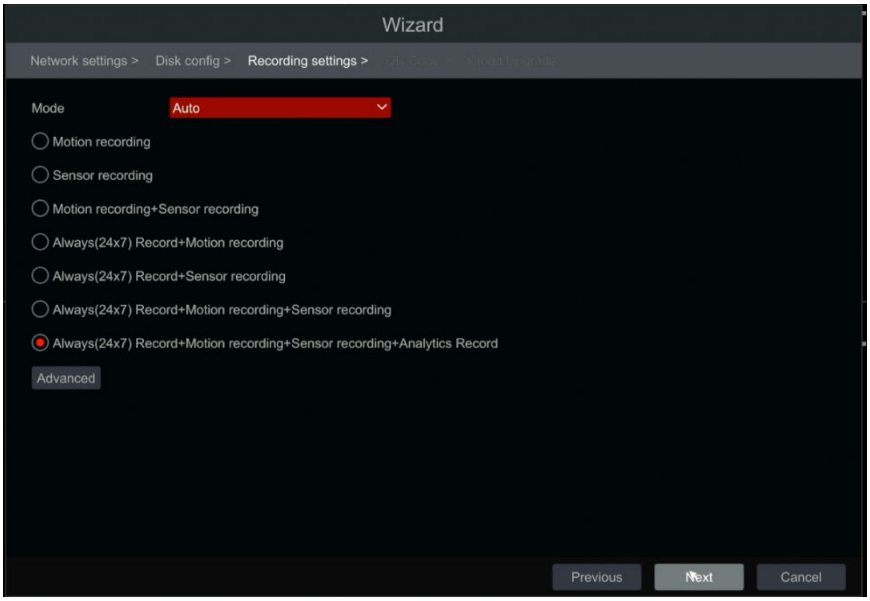


Please note:

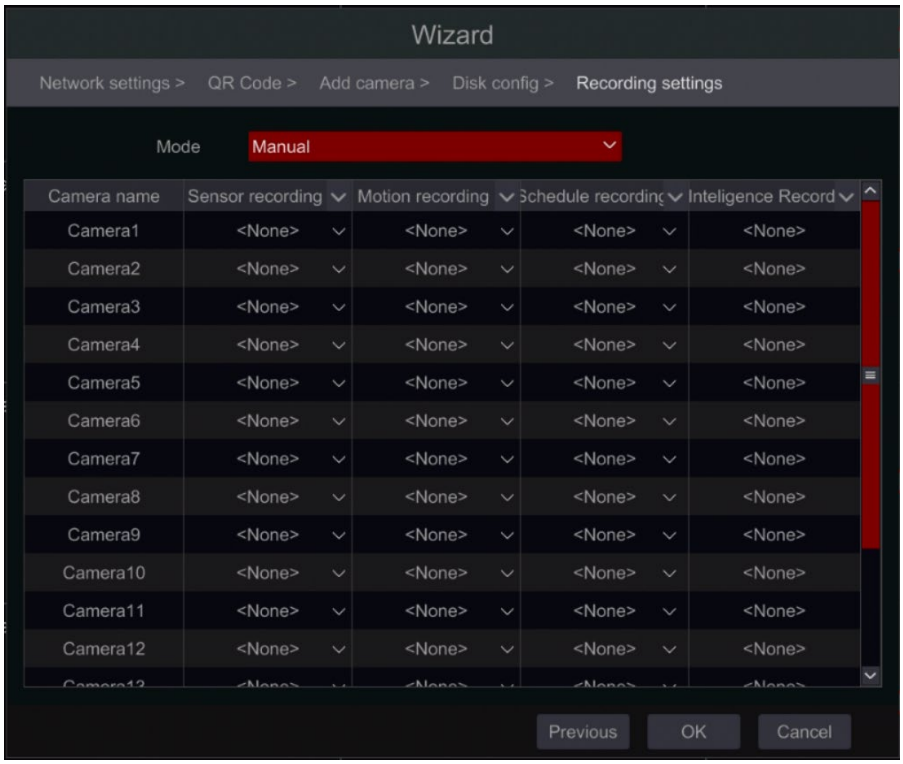
- Unformatted HDD will result in no records.

3.2.3 Record Settings:

Two record modes are available: Auto and Manual. See 7.1.1 Mode Configuration for details.
Auto: Select the desired auto mode in the interface as shown below and click "OK" button to save the settings. You can use the "Advanced" button to create new combinations for recording.

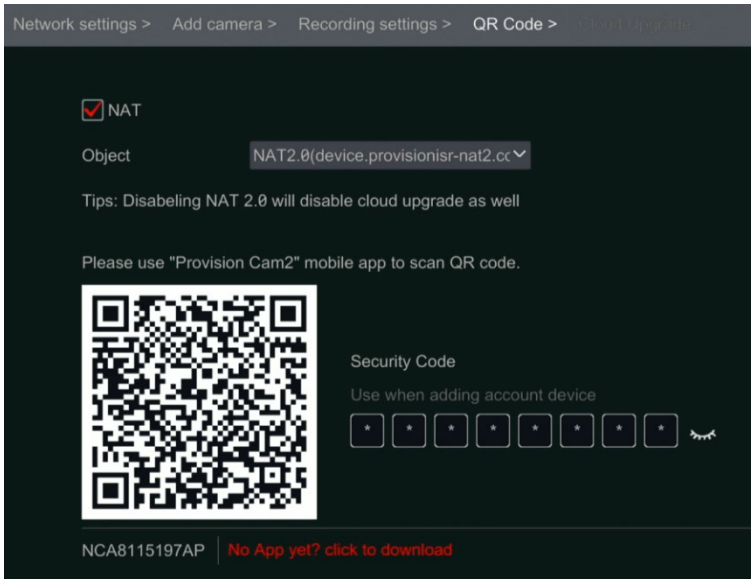


Manual: After switching to manual, set the schedule for "Sensor Record", "Motion Record" and "Schedule Record" of each camera. (You can choose all together by clicking on ⌄. Click "OK" to save the settings.



3.2.4 QR Code / NAT:

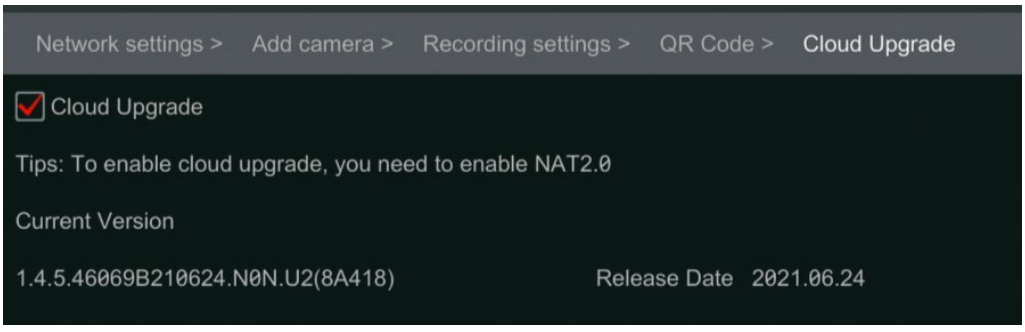
The QR code is designed for easy connection with Provision Cam2 Mobile app and Computer web browsers via P2P which is more reliable and secure than IP/DDNS connection. You can enable the NAT service and scan the QR Code using the “Provision Cam 2” mobile application to quickly connect to the device.
You can also use the dedicated QR codes to download the app from Google play and Apple App stores, by clicking on “click to download” and scanning the QR code applicable for your device.



On the Provision Cam2 mobile app, it is advised to use an account. When logged out of an account, you will need to connect to the device using username/password. When logged into an account you will have to use the Security Code. Click on the closed eye icon to display it.

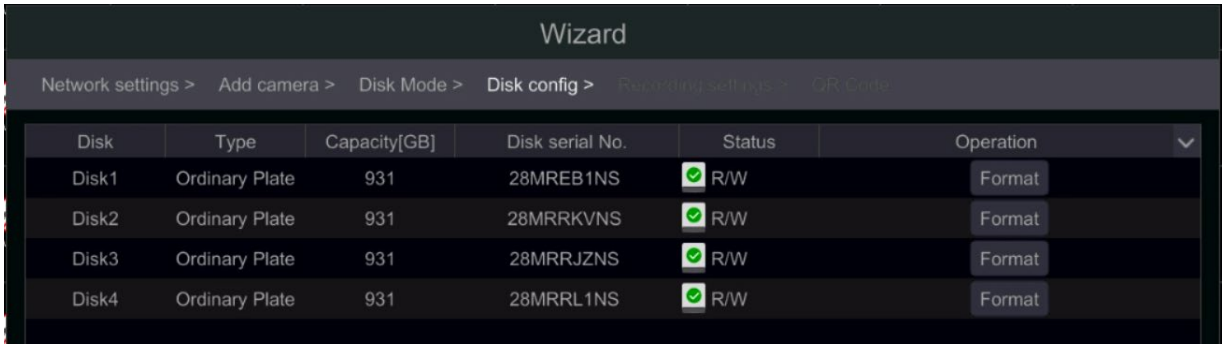
3.2.5 Cloud Upgrade:

Cloud upgrade allows the device to regularly check for updates and commence device update once there is an available update on the updater server. Enable this service if required.

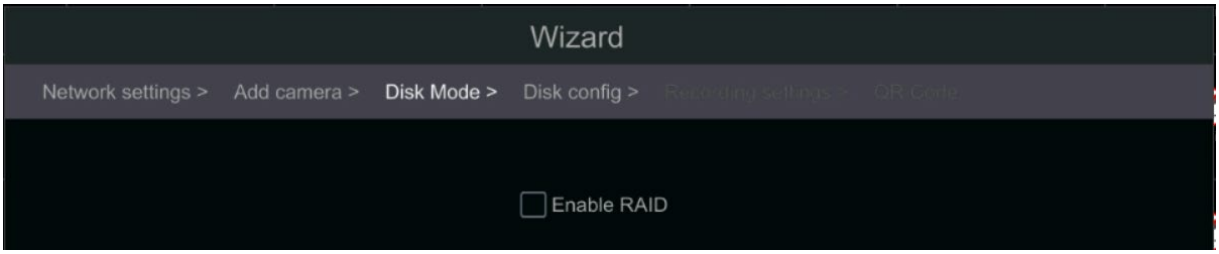


3.2.6 Disk Settings:

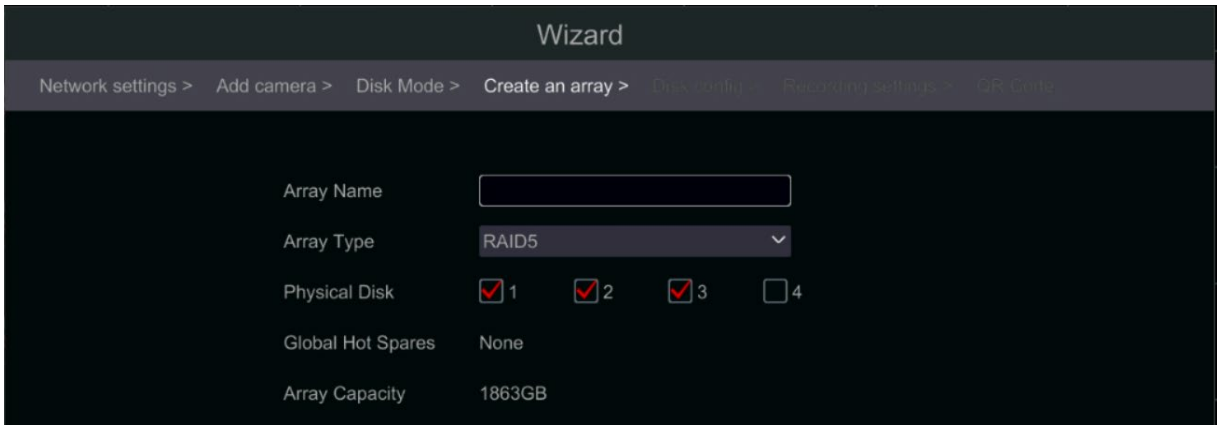
You can view the disk status, number, capacity and serial number. Click “Format” to format the disk. Click “Next” to continue.



Models Supporting RAID: These models will have another step – “Disk Mode”. Here you will be able to enable RAID.

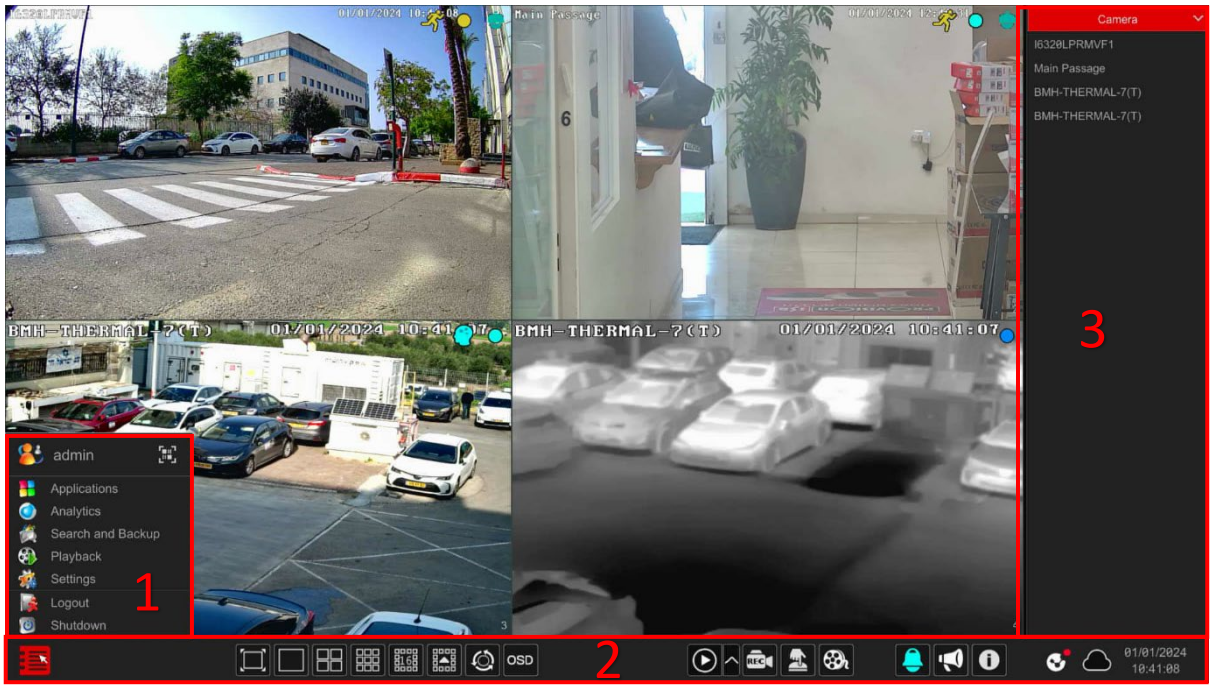


After confirmation – The device will prompt for a reboot.
After the reboot, there will be a new step in the wizard – “Create an array”
Set the array as you wish and click “next” to continue. You can find further explanation about RAID in the appendix at the end of this manual.



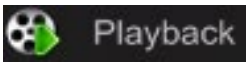
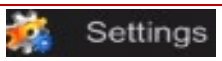
3.3 Main Interface

3.3.1 Main Interface Introduction

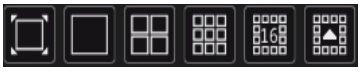


Menu (1) options descriptions:

Icon / Button	Meaning
admin	Show the current user name
	QR Code and Security Code Display for P2P Connection
Applications	Access “Special Applications” such as LPR Parking management.
Analytics	Advanced Analytics interface (Including DDA, LPR, Face Recognition and Smart Search).
Search and Backup	Record search and backup interface, see 8.3 Record, Search, Playback & backup for details.

	Playback interface. see 8.2 Playback Interface Introduction for details.
	Setup panel, see 3.2.2 Setup Panel for details.
	Log out of the system.
	Perform “Logout”, “Reboot” or “Shutdown”

Operations Bar (2) icon descriptions:

Button	Meaning
	Start button. Click it to pop up the menu (③).
	Full screen button. Click it to switch to full screen mode; click it again to exit the full screen mode.
	Screen split mode buttons.
	Dwell button (see 5.2.2 Quick Sequence View and 5.2.4 Scheme View in Sequence for details).
	Click it to enable OSD; click to disable OSD.
	Click to set the default playback time for in-channel instant playback; click to activate quick playback for all channels – going back to the specified time. 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 it to enable/disable manual record.
	Manual alarm button. Click it to manually trigger or clear the alarm-out
	Recording Status. Click it to see the recording status
	Alarm Status. Click it to see the alarm status. The icon will change its color based on the current alarms
	Public Announcement. Click it to set and broadcast audio messages to multiple supporting cameras
	System info and status. Click it to see a variety of system statuses including: Device info, Alarm, Disk, Backup, Etc.
	Check Point Status. This will indicate the status of the Check Point IoT Cyber Protection. (For supported devices)
	Cloud update interface

User Bar (3) description:

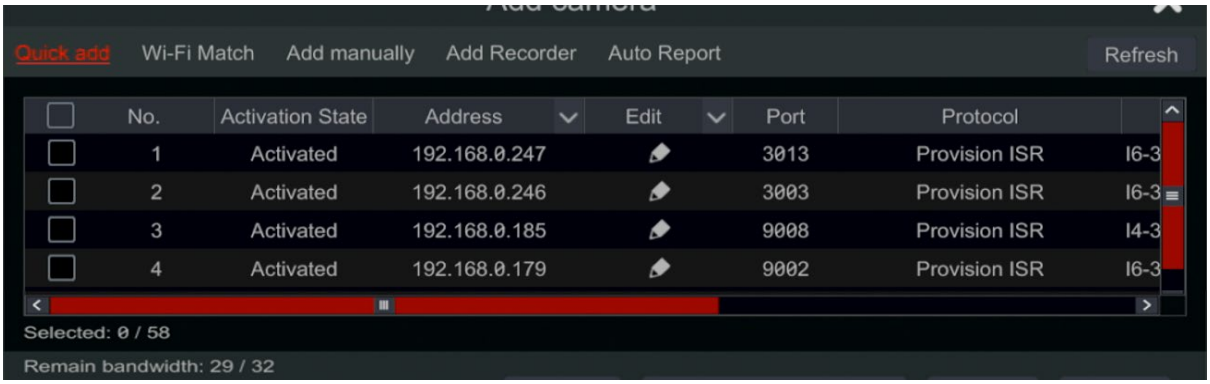
1. Choose “Camera” to view all the cameras available for display. Either select one window on the left side of the interface and double click on the camera name you wish to view in the selected window or drag a camera name from the right pane to the selected window on the left.
2. Choose “In-Channel Sequence” to view all the configured “In-Channel Sequence” groups list; Select a group in the list to view all the cameras related to that group. Either select one window on the left side of the interface and double click on the group you wish to view in the selected window or drag a group name from the right pane to the selected window on the left.
3. Choose “Customized Display Modes” to view your saved display layouts. Double click on the desired display preset from the list to activate it.
4. Choose “Object Recognition (DDA)” to see all Object recognition event snapshots (DDA, DDA2, Face Detection, Face Recognition, LPR).

4. Camera Management

4.1 Add/Edit Camera

4.1.1 Add Camera

The device’s network parameters should be configured before adding IP cameras (see TCP/IPv4 Configuration for details).
Referring to the pictures below, Click on ***Add Camera*** in the setup panel or in the top right corner of the preview window to pop up the “Add Camera” window as shown below. You can use the “quick add” interface to add an IP Camera or add it manually.

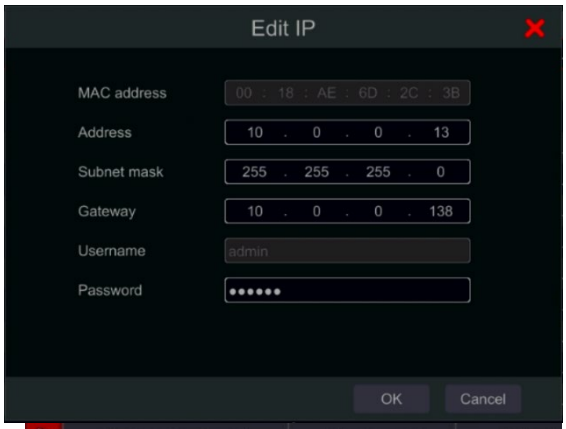


4.1.2 Quick Add Camera

Mark the desired cameras and click “Add” to add cameras.
Click on “Default Password” to set the default username and password per manufacturer.

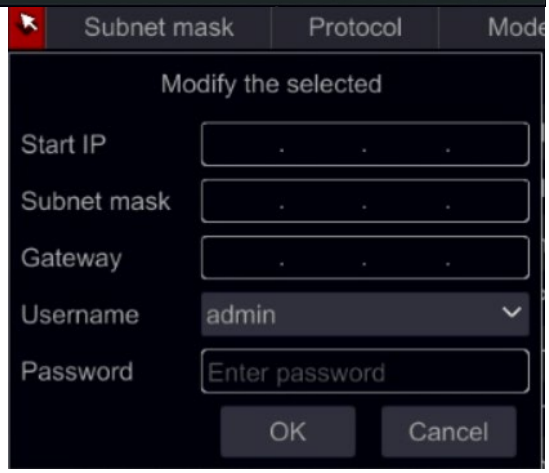
4.1.3 Editing IP Address of Specific Camera

Must be done prior to adding the IPC. From the "Quick Add" interface, Click to edit the IP of a specific IP camera. Set the IP new IP address, subnet mask and default gateway. Input the IPC password and confirm. After a few seconds, the camera IP address will change.



4.1.4 Editing IP Address of Several Cameras

Must be done prior to adding the IPC. From the "Quick Add" interface, Click next to the "Edit" tab and choose "Batch IP Settings". Choose the target cameras, set the first IP Address, Subnet Mask and Default Gateway and confirm. The IPC Addresses will be set in consecutive order. Make sure that all the target IP addresses are free (For example: If you configure 32 cameras and the starting IP is 192.168.1.1, then you need to make sure that all the addresses from 192.168.1.1 to 192.168.1.32 are free)



4.1.5 WI-FI Match

The wireless cameras are pre-paired with the NVR before delivery, so no pairing is required.

Once the NVR and cameras are powered on, live video will appear automatically on the NVR's live view.

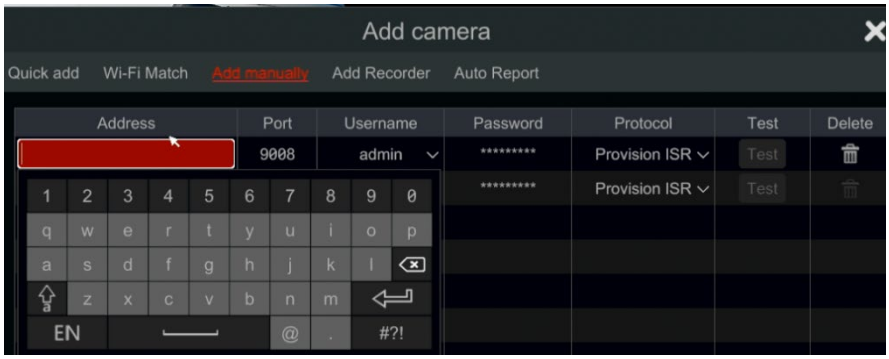
To add a new wireless camera (that fit to the kit), go to Settings > Manage Camera > Edit Camera, remove an existing camera if needed, and then follow these steps:

a. From the edit camera menu, click the "+" icon in the top-right corner and select "Wi-Fi Match."
b. 2. After powering on the camera, press and hold the Reset button for 3 seconds to go to "pairing mode" – when the camera white light flickers 3 times it is in pairing mode
c. 3. After the camera is matched, the NVR will output the image.
   Note: If the camera is in paring mode for more than 2 minutes the process will stop

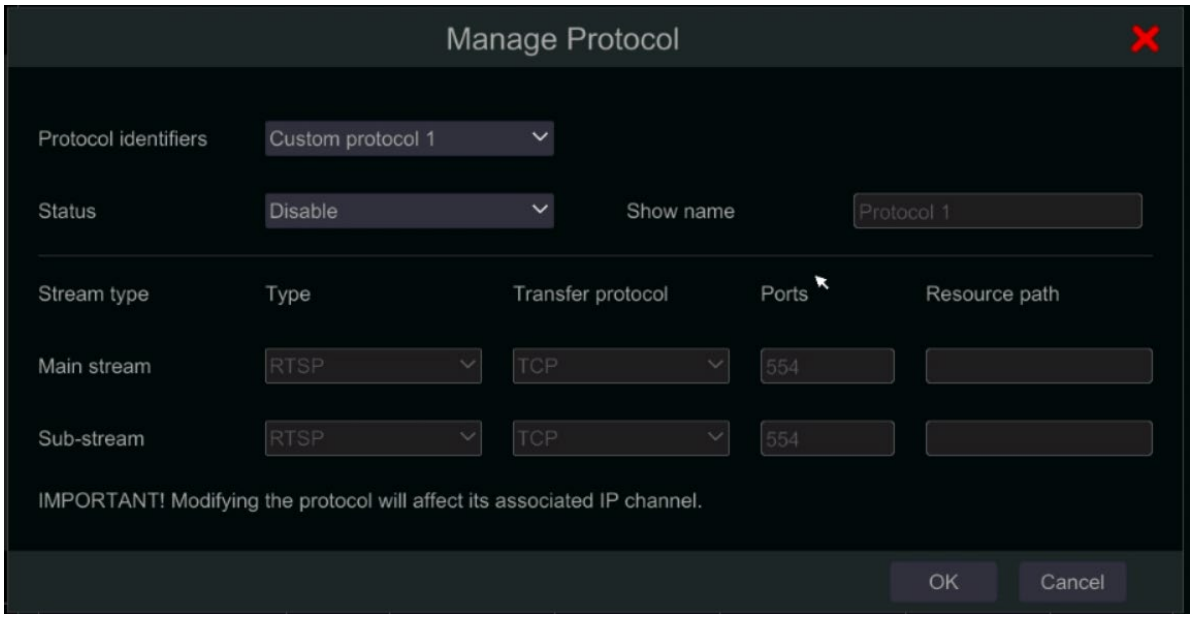
4.1.6 Add Manually

IPv4/IPv6 Input: Input the IP address, port, username, password and protocol of the camera and click "Test" to confirm the settings are correct and that connection can be made with the camera.

Domain Input: If you are using DDNS to connect with the camera, click on the arrow next to the IP address to switch the connection mode from IP to domain.
Once finished, click the “Add” button.



Protocol / RTSP Input: The system has several built-in communication protocols with the camera (Provision-ISR, ONVIF, Hikvision, Dahua). If you wish to add a channel using RTSP, click on the drop-down menu arrow next to the chosen protocol (Default is “Provision-ISR”) and choose “Manage Protocol”. The following window will appear.

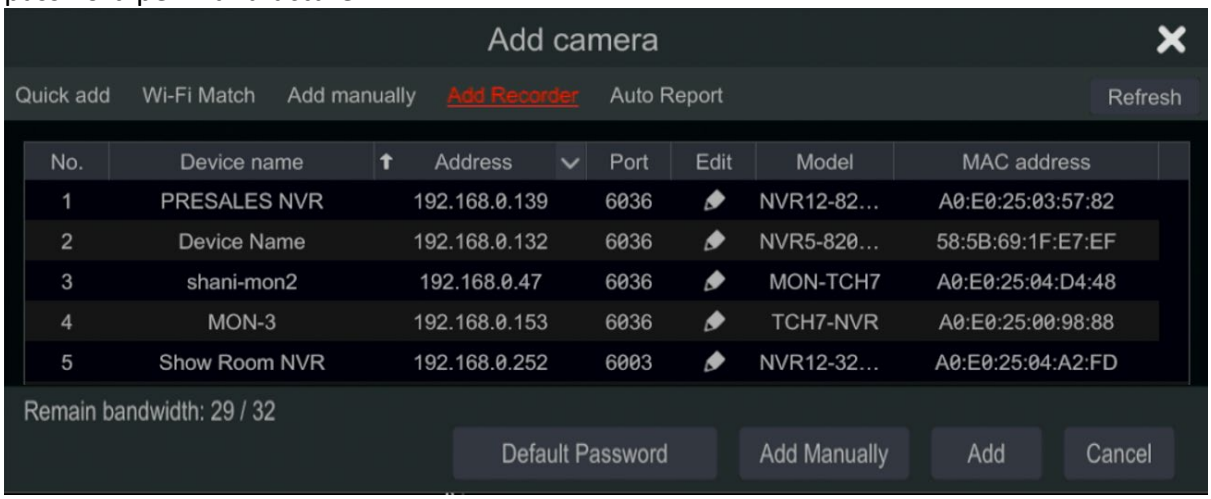


Set a name for the protocol, enable it and set the values as required (Both master-stream and sub-stream values must be entered). Click OK to continue.

4.1.7 Add Recorder:

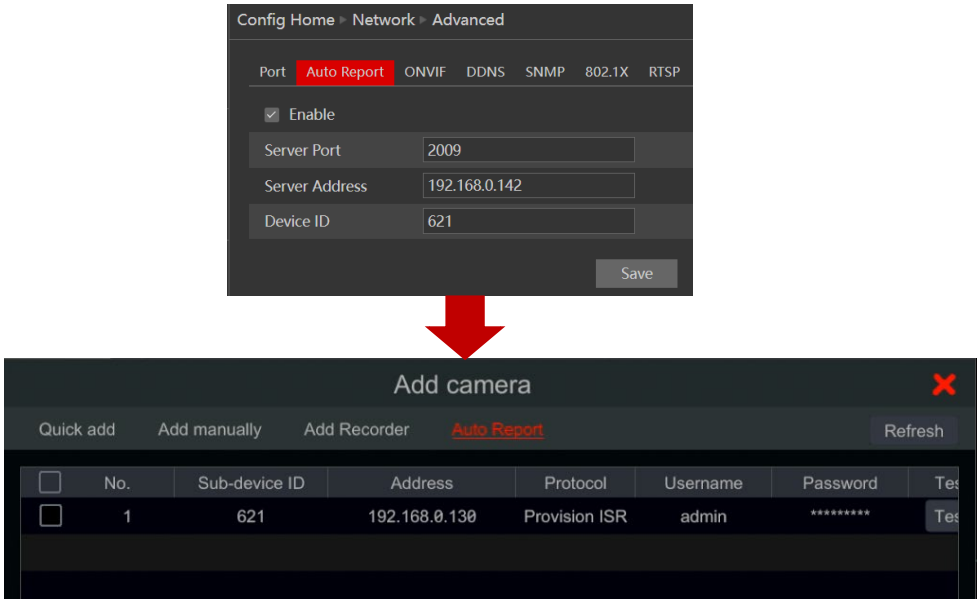
f you wish to view/record channels from another Provision-ISR device on the network you can use this option. Click on “Add Recorder”. The following window will appear.
The NVR will display automatically all the supported devices found on the LAN with its details. If you wish to add a channel from any of the displayed devices, double click on it and then double click on the channel you wish to add.
If you wish to add a channel from a recorder located on another network, click on “Add Manually” and input the IP address, port and login credentials for the device, then click on “Test Device” if the connection is well, you will get a list of available channels. Double click on the channel you wish to add.

Click to delete the camera. Click “Default Password” to set the default username and password per manufacturer.



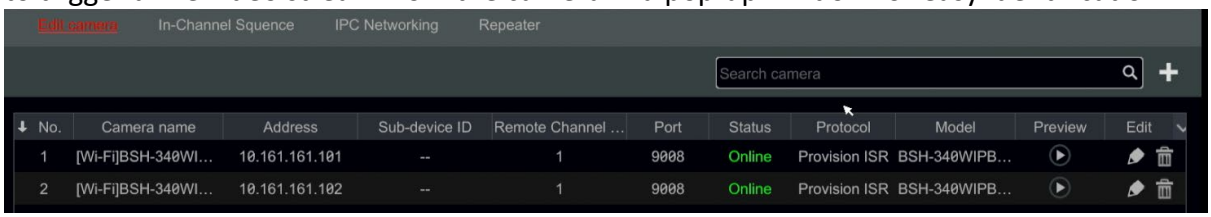
4.1.8 Auto Report:

Strating version 1.4.12, you can add IP cameras to the NVR using the “Auto Report” method. This means that you need to configure the IP camera to communicate with the NVR directly. Please refer to the IP camera user manual for the settings. In the example below, the IP Camera address is 192.168.0.130 and the NVR IP address is 192.168.0.142.
After setting the camera to communicate over Auto report with the NVR, the result will be as follows:



4.2 Edit Camera’s General Parameters

This can be done only when there are active video channels. You can use Preview button to trigger a live video stream from the camera in a pop-up window for easy identification.

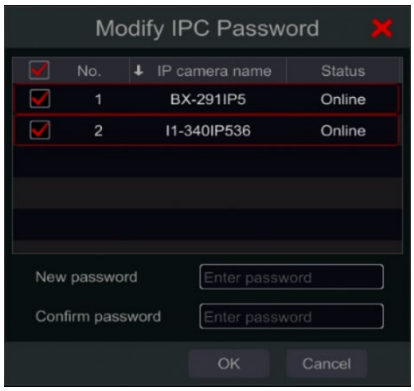


Click “Edit Camera” in the setup panel to go to the edit interface.

4.2.1 Edit Camera’s name:

Click to edit the camera’s name. Set the new name and confirm.

4.2.2 Change camera’s password:



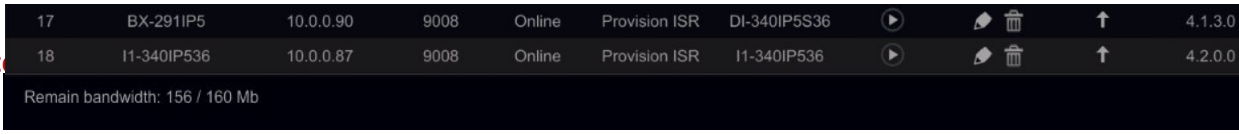
Note: WIFI camera password cannot be changed

Click on the button next to “Operation” and then choose “Modify IPC Password”. In the opened window choose the desired cameras, input the new password and reenter it for confirmation.

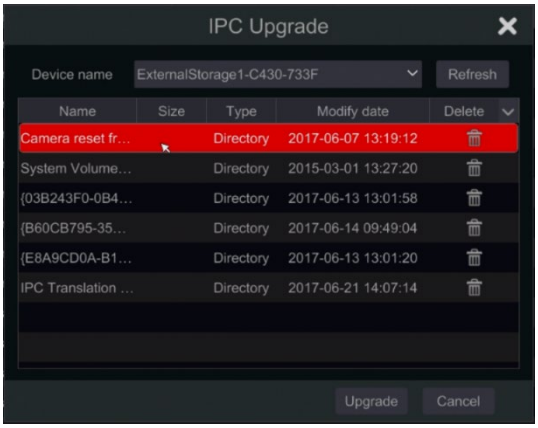
4.2.3 Delete Cameras:

Click on to delete the camera.

4.2.4 Updat



Click on cameras and firmware version from the opened window and confirm.



Note:

If a PoE NVR is used, the IP cameras (with PoE function) which connect directly to the PoE port of the NVR will be displayed automatically in the camera list. The IP camera which occupies the PoE port has a prefix shown before its camera name. The prefix consists of PoE plus PoE port number. Cameras connected to PoE ports cannot be deleted from the camera list.

IP cameras that connect directly to the PoE port of the NVR using “Provision-ISR” private protocol will be shown automatically in the camera list.

One of the two conditions must be met for an IP camera that connect directly to the PoE port of the NVR using “ONVIF” protocol to be shown automatically in the camera list.

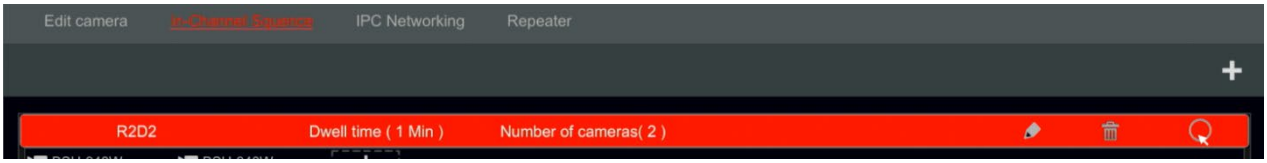
- ✓ The IP camera is in the same network segment with the NVR internal ethernet port.
- ✓ The DHCP (Assigning IP Address automatically) of the IP camera is enabled.

4.3 “In-Channel Sequence”

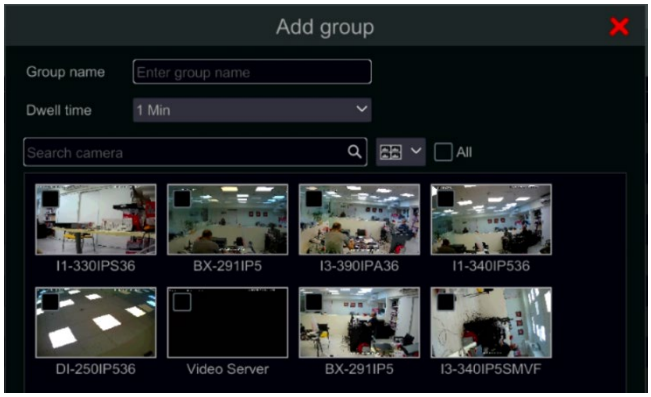
In channel sequence will run a sequence of specified cameras within a single window while in split mode. It can also be used on full screen, but will be less effective.

4.3.1 Add “In-Channel Sequence”

Click “In-Channel Sequence” in the interface to go to the configuration area as shown below.



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

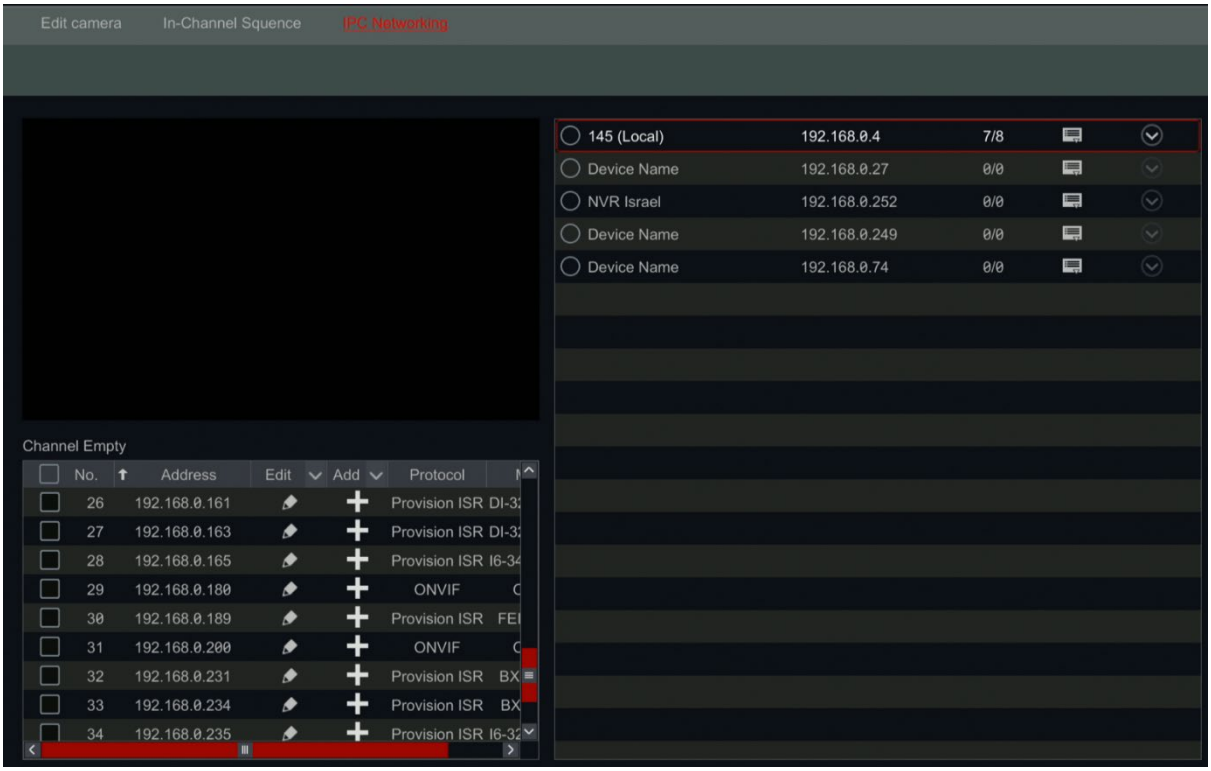


4.3.2 Edit In-Channel Sequence

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

4.4 IPC Networking

IPC networking will allow you to remotely configure IP cameras and basic network parameters of other devices. This is applicable only for devices running Ossia v1.1 and up. Below you will be able to learn about the different options of this feature.



4.4.1 IP Camera management

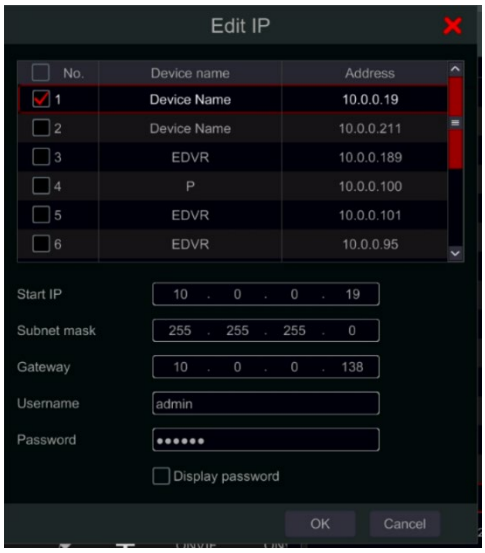
The IP Camera management is identical to the “Add/edit camera” Interface. You can set the IP parameters and the name of the camera through it.

4.4.2 Device Management

Here you will be able to remotely set the general network parameters of the device and configure the IPC cameras connected to the device. The following information is available: Device name, Device current IP Address, Cameras and availability.

Clicking on will open the device menu You wll have the following options:

- Edit IP – Set the device's IP address, subnet mask and gateway.
  Tick the devices you wish to configure and set the start IP address. The device will set automatically the rest of the IP address. Make sure that the whole segment is available before running this procedure.
  Set the subnet mask and gateway – this will be set for all devices.
  Set the username and password for the devices. If any of the devices have a different password, it should be set independently otherwise the procedure will fail.
  Click OK to start the process.



- Edit user – set the admin address for the specified device. This is only required if the device password is different than the default password (admin / 123456).
  Tick all the relevant devices and set the user name and password
- Buzzer – the buzzer will help you identifying the device you wish to configure by activating the buzzer on the unit itself.
- Delete all – will delete all IP cameras set on the device.
  Click on to open a list of all cameras connected to the device. Click on to hide it.
  Once the list is open, you can delete specific IP cameras by pointing on it and clicking on the icon that appears. To add a specific camera to the device, choose the device and add cameras from the IPC interface on the left. Make sure that you set the user credentials beforehand.

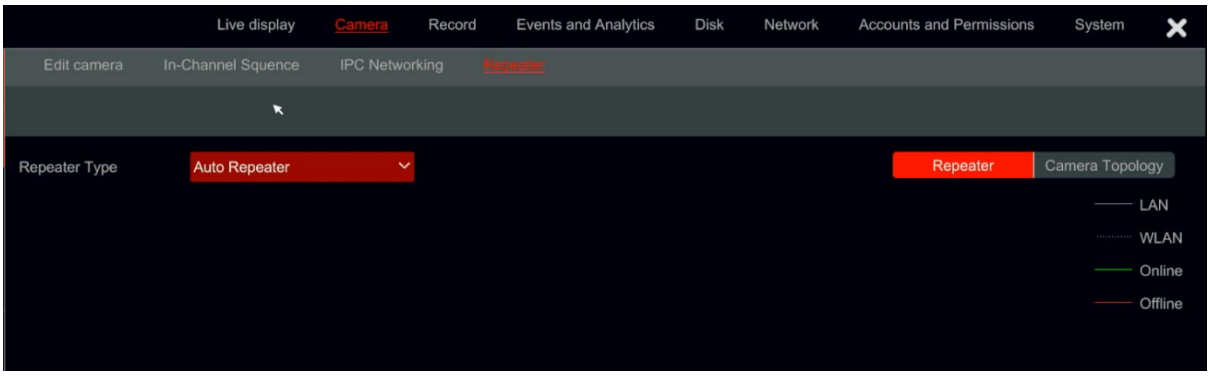
4.5 Repeater

In complex environments, wireless signals may weaken when passing through obstacles. Proper repeater configuration can help extend the transmission distance.

Note:

- The repeater function does not strengthen the signal; it extends the transmission range.
- Proper camera placement can improve wireless performance.

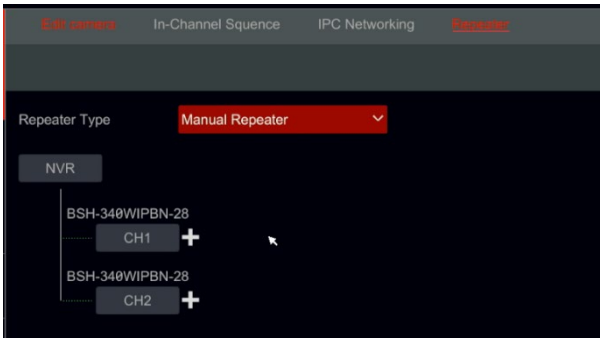
Repeater setup requires a stable connection. For best results, plan the repeater configuration based on the actual environment. It is recommended to place the camera near the NVR and configure the repeater before final installation.



Repeater types:

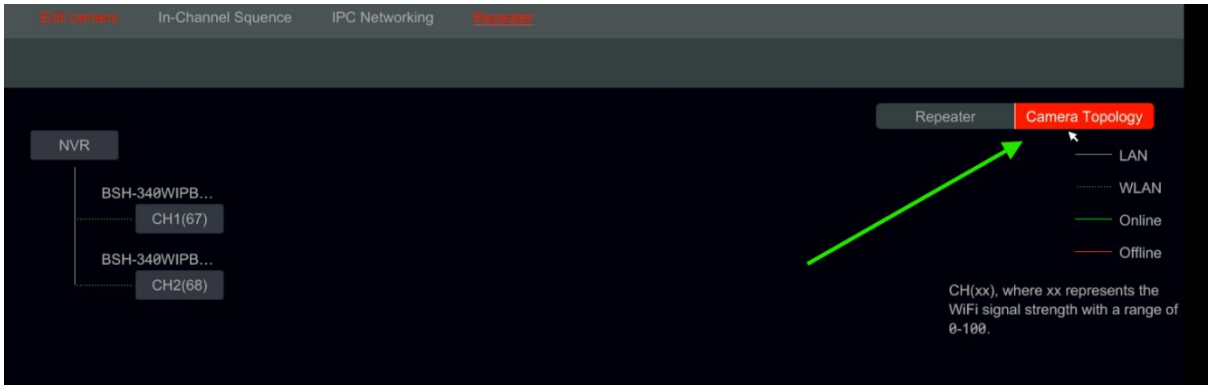
- Manual repeater:

Configure the repeater based on the camera's installation location. Click "+" to add the camera you want to link, then click "Apply" to save the settings.



- Auto repeater:

In the interface above, select "Auto Repeater" and click "Apply" to enable the feature. Once enabled, the system will automatically search for nearby cameras and choose the optimal relay path when a camera's signal is weak. Then, click "Camera Topology" (Below) to view the repeater details.



5. Live View Introduction

5.1 Live View Interfaces:

You must have active video channels for this interface to be active.

Live view indicators (Will appear only when a channel is active)

Indicator	Meaning
	Active Motion detection
	Active Analytics detection
	POS Recording
	Motion Recording
	Schedule Recording
	Sensor Recording
	Manual Recording
	Analytics Recording
	Indicating that the channel support PTZ operations
	Indication that the audio stream for the channel is enabled
	“No Signal” for Analog Cameras. “Not Available” for IP Cameras

Click on the live-view window to show the channel tool bar as shown in area ① . Right click on the preview window to show the channel menu list. The tool bar and menu list are explained in the table below.

Button	Menu List	Meaning
	--	Move tool. Click and drag it to move the tool bar.
	Manual Record On	Start/Stop manual recording for the specific channel.
	Instant Playback	Start Instant playback for the specified channel. The playback will commence within the selected window.

*	**Enable Audio + Volume Control***	Enable/disable audio from the selected cannel (Requires camera/channel to support of this feature). Once enabled, a volume slider will appear to control the output volume.
	Snap	Take a snapshot and open a snapshot pop-up. Click “Save” in the window to save the image. Click “Export” to export the image.
*	**PTZ Control***	Switch to the PTZ control interface.
	Zoom In	Switch to the digital zoom interface. Digital Zoom can also be achieved by placing the mouse cursor on the required object and using the mouse scroll wheel to zoom in & out.
*	**Fish Eye**	Open Fish-Eye display controls.
	--	Switch to the image adjustment interface.
*	--	Open audio out (Talk)
*	**Object Detection***	**Supporting Devices Only** will display Face+Object detection. If the camera doesn’t support face detection, this icon will be grey.
--	**Camera Info**	View the camera information.

*Supporting Devices only.

5.2 Fish-Eye Display:

Fish eye cameras are usually installed to cover large areas and provide a 360° view. In order to dewarp the image properly, you need to set the installation method and the view you wish to get. Click on the “Fish Eye” Icon to get the following pop up:
Choose the installation mode out of Ceiling, Wall and Desktop. Setting the installation mode wrong will result in wrong view of the video.
Now choose the display mode out of the following:

1. Fish-Eye: Normal view of the warped fish eye sphere view.
2. Panorama: A stretched view of the sphere removing all the black borders.
3. 360° view: See 2 180° views side by side
4. Fish-Eye + 3PTZ: Normal view of the warped fish eye sphere view + 3 Digital PTZ that can be dragged and moved using the mouse.

Please note:

3. Note: Changing the Fish-Eye display mode doesn’t affect the recording of the camera.

5.3 Digital Zoom:

Digital Zoom can be achieved by one of two methods: The first and more intuitive one is the mouse scroll wheel. Just left click on the channel you wish to control, point the mouse cursor on the object you want to zoom on and scroll the mouse wheel up or down to zoom in or out.

The second method is by the digital zoom interface. The digital zoom interface is shown below. Press and drag the red box to select the zoom area. Click / to zoom the image. Click the camera selection box to select other cameras for amplification. Click “Back” to return to the live preview interface.

5.4 Live-View Modes:

5.4.1 Display Modes Tabs

The system offers several display modes. In the latest version, the only available tab is “Camera” by default. If you wish to edit the view option tabs, click on the “” button at the top right corner of the screen and choose which tabs you wish to activate/disactivate.

5.4.2 Customized Display Mode

Set different screen split modes and camera layouts as required and save the display to create a preset. Refer to the picture below. Double click on the display preset from the list to activate it.
Customized display mode is also used to control the secondary monitor display (On supported devices)

Adding Customized Display:

Method One:

1. Click “Customized Display Modes” in the main interface
2. Set the screen split mode.
3. Add and organize the cameras as desired.
4. Click the “Save” button under the display presets list
5. Enter the display preset name in the popup window and click “OK” to save it.

Method Two:

1. Click Start→Settings→System→Basic→Layout Settings
2. Click to add a new layout.
3. Choose the screen split mode from the bottom.

4. Double click the camera or camera group in the list to add them to the selected window.
5. Click ★ to save the defined output as a preset (refer to 5.2.4 Scheme View In Sequence for detailed configurations). The saved preset will be displayed in the display preset list in the live-view interface.

Using method two will affect the sequence settings – please refer to 5.3.2 Sequence for additional information.

Editing Customized Displays

Click “Customized Display” tab in the live-view interface. Select the required display from the list. Click “Rename” to edit the display mode name; click “Delete” to delete the display mode.

Using Customized Displays with 2 Screens (Requires model supporting independent displays):

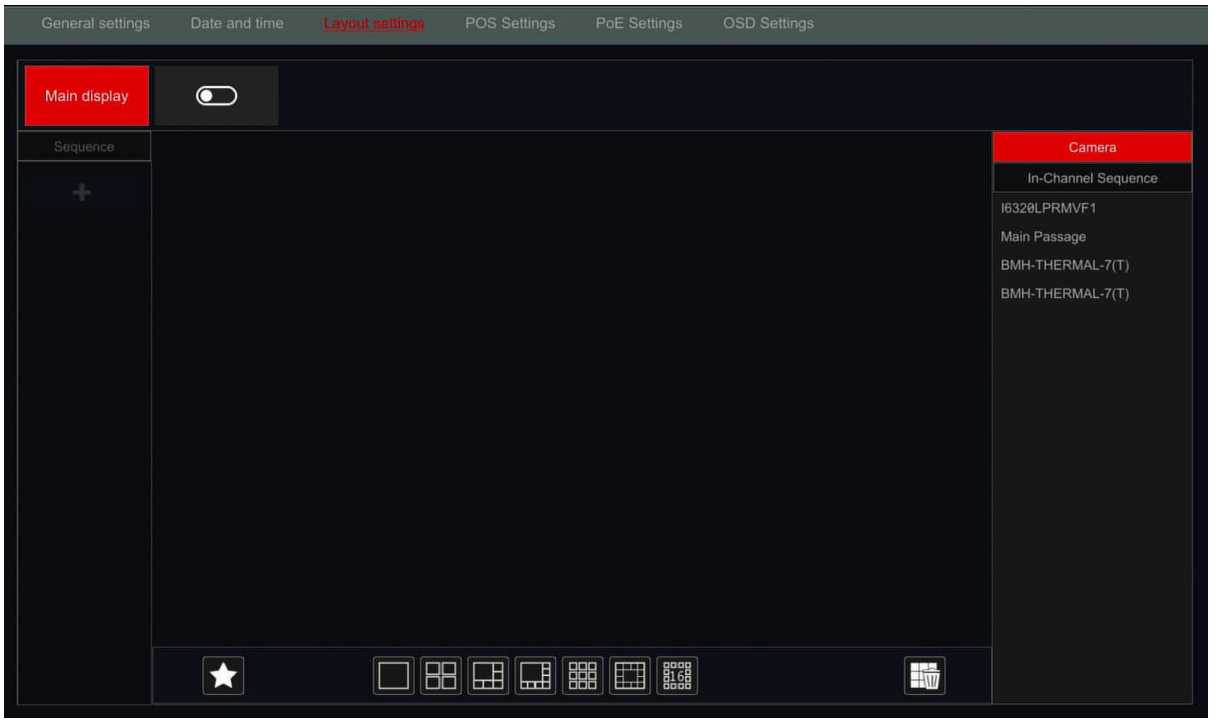
Click “Customized Display” tab in the live-view interface. Right click on the required display from the list and choose “Send to Main Screen” or “Send to Secondary Screen”.

5.4.3 Sequence

The sequence view will automatically switch between cameras in specified times.
If a customized scheme has not been created, it will keep the split layout and go through all of the available cameras. If the scheme has been created – the sequence will run through the created scheme. Controlling the sequence will be done from the sequence control icon as shown below.

Sequence Scheme Settings

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



Add Scheme

Click on the left pane to create a new scheme. Click on the top right corner of the scheme to delete it.

Configure Scheme

1. Select a scheme on the left pane and the screen split mode button from the bottom pane
2. Drag cameras from the camera list to the desired window from the right pane. The camera or group will be added into the selected window.
3. You can click the right-click on a camera and click “Clear” to remove a single camera or click to remove all the cameras.
4. Click “Apply” to save the settings.

Start Sequence View

Go to the live-view interface and click to pop up a little window. Set the dwell time for each window and click to start the sequence. Double click the sequence view interface to pause the view; double click again to restore the view. Click to stop the view.

5.4.4 In Channel Sequence.

You can start “In-Channel Sequence” only if a camera group was created.

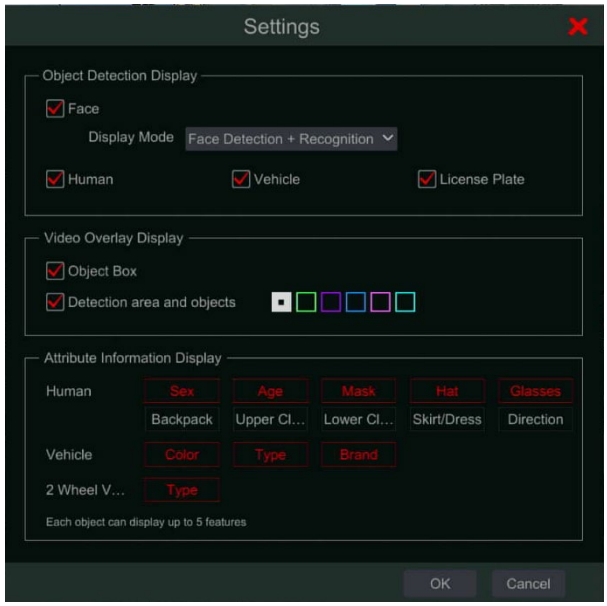
1. Go to the live-view interface and select a camera window.
2. Double click one the “In-channel Sequence” group on the right side of the interface. The cameras in the group will start sequencing one by one in the selected camera window.
3. You can also drag the group directly to any preview window.

4. Right click on the view window and click “Close Dwell” button to stop the sequence.

5.4.5 Object detection.

The Object detection tab will open the object detection **and** face recognition display for all face detection cameras configure d on the system. The pane and its controls are as follows (DDA Object detection marked in Green. Face Detection and Recognition marked in Red):

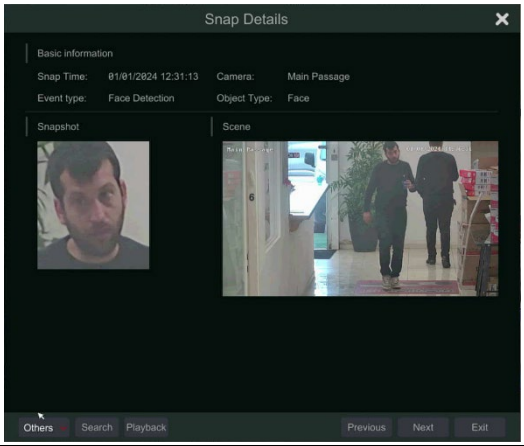
Controls and settings: The object detection interface has 3 important settings that can be configured by clicking on “Settings” on the bottom right of the panel:



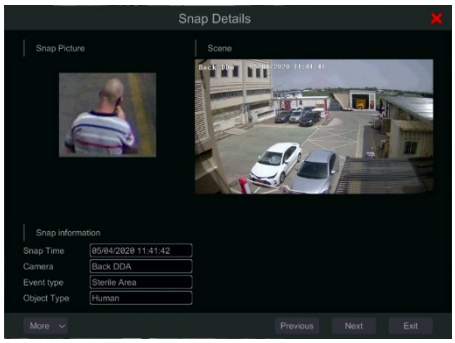
1. Object detection Display: Here you can choose which detections will be displayed (Face, Human, Vehicle, LPR). Moreover, for Face detection, you can choose whether to display Face Detection + Recognition (Meaning that unrecognized faces will be displayed as well), or only face recognition.
2. Video Overlay Settings: Choose if to see the object/face detection on the live image in real-time. Object Box shows the detection object with a rectangle in the chosen color around it. Detection area and objects show the detection ROI in white. It will color red once alarm is triggered by it. This setting has no effect on the detection capabilities and it will work with this option enables or disabled.
3. Attribute Information Display: Metadata analytics (Part of DDA2) contains many attributes. The object detection pane can only display 5 attributes. Choose the ones you want to see in the object detection pane (All other attributes will be saved but not displayed)

Face detection/recognition interface controls:

Button	Menu List Meaning
	Add to Database: Add a person to the database
	Search: Search for the person in the past day
	Instant Playback: Playback the detection moment

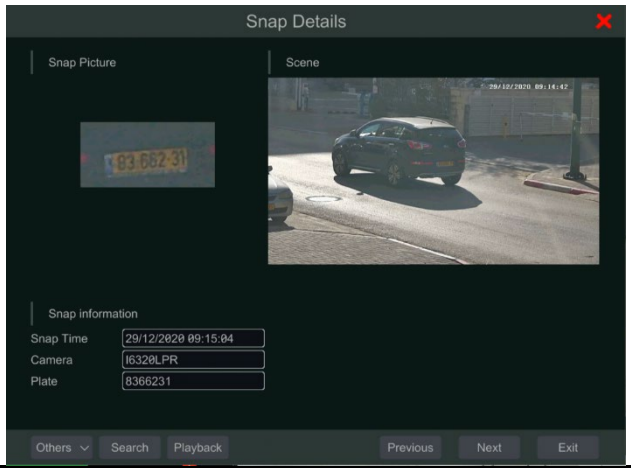
	General Info: Get the detection info 

Object detection interface controls:

Button	Menu List Meaning
	Search: Search for similar objects in the past day
	Instant Playback: Playback the detection moment
	General Info: Get the detection info 

LPR interface controls:

Button	Menu List Meaning
	Add to Database: Add a license plate to the database
	Search: Search for the person in the past day
	Instant Playback: Playback the detection moment

	General Info: Get the detection info 

5.5 Cloud Update

Starting from v1.4.4, cloud update is available for the system. Click on the cloud icon ( ) to check the cloud update status. If the icon is marked with a red “No entry” sign ( ) it means that there is an error. This can be caused by 3 reasons:

1. The cloud update server cannot be reached (Network issue). Please check your network connection and try again.
2. The cloud update is disabled. Please enable it by clicking on the cloud icon and ticking “Cloud Upgrade”.
3. NAT2.0 interface is disabled. When enabling the cloud update, the following Prompt will appear. Please confirm it by pressing on “OK”

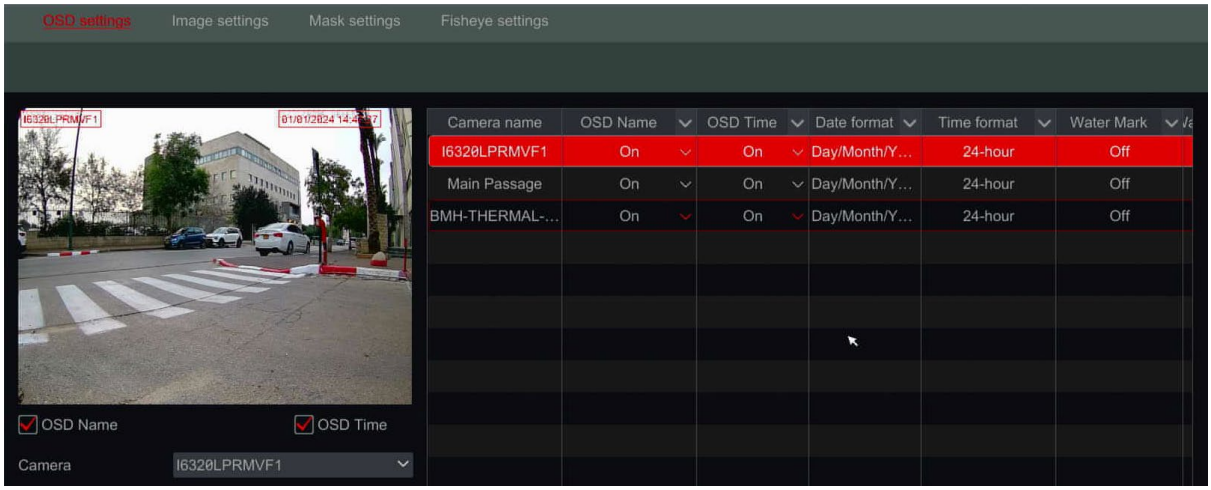
5.6 Emergency Live-View:

In some cases, you will have to go back to the live-view interface as soon as possible. Doesn’t matter where you are in the system or what you are currently doing. The “Emergency Live-View” was designed just for that.
From any place in the system, click on the middle mouse button to activate the “Emergency Live-View”. This will take you back to the last live view display you were viewing.
Please note: Using the “Emergency Live-View” during configuration will exit the configuration window and discard any unsaved changed you have made.

5.7 Image Configuration

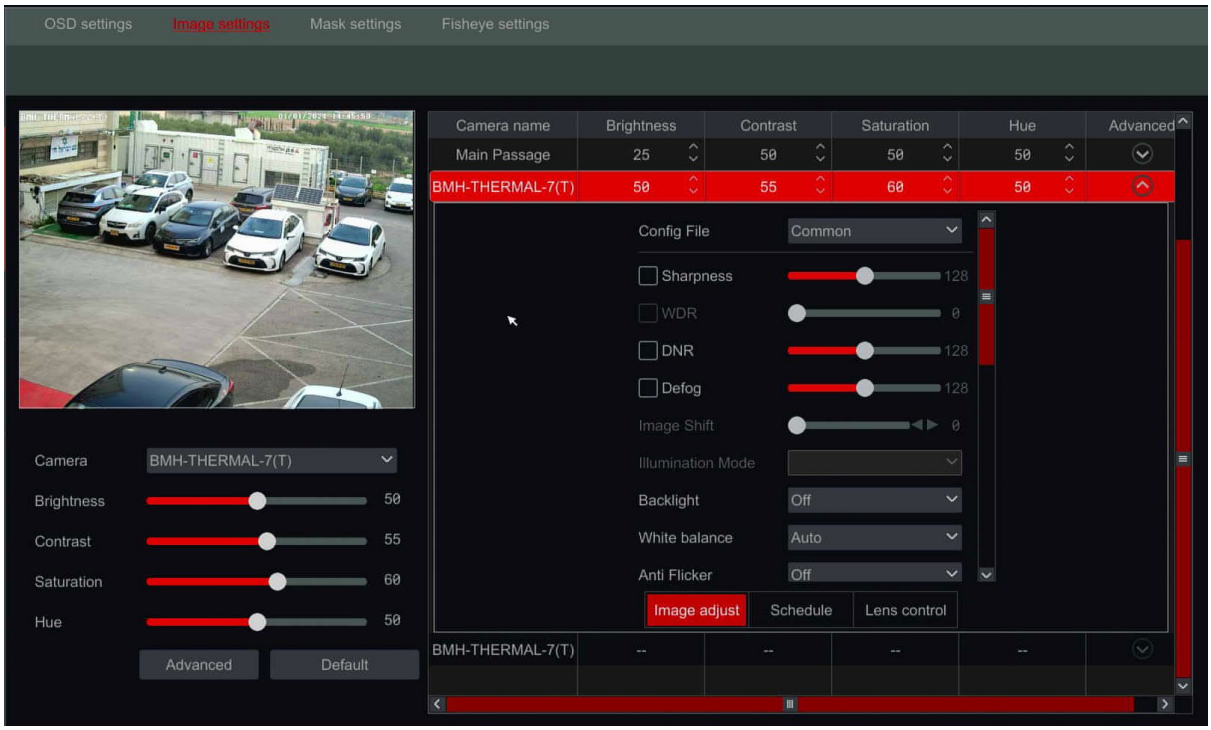
5.7.1 OSD Settings

Click Start→Settings→Camera→Image→OSD Settings to go to the interface shown below. Select the camera, input the camera name (or double click the camera name in the camera list to edit the camera’s name), enable or disable the name and time OSD (if enabled, drag the red name and time OSDs in the image view area to change the OSDs’ display position) and select the date and time formats. Click “Apply” to save the settings.



5.7.2 Image Settings (Setting Interface)

Click Start→Settings→Camera→Image→Image Settings.
Select the camera and set the image brightness, contrast, saturation and hue. For advanced settings you click on the arrow under the “Advanced” tab. Only cameras connected by “Provision-ISR” protocol will support advanced features.
You can click “Default” button to restore the image settings to the default factory settings.



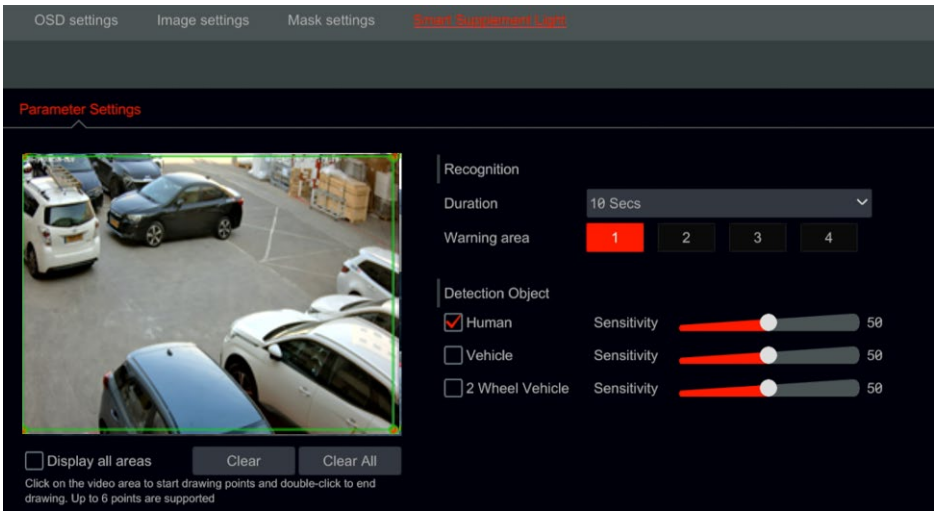
Please note:
Different IPC models/versions will support different image settings and features.

5.7.3 Mask Settings

Some areas of the image can be masked for privacy. Up to four mask areas can be set for each camera. (Only for Provision-ISR Cameras non-ONVIF cameras).
Click Start→Settings→Camera→Image→Mask Settings to open the interface as shown below. Select the camera and enable the mask. Click “Draw” button and drag the mouse on the image area to set the mask area; click “Delete” button to delete the mask areas; click “Apply” to save the settings.

5.7.4 Smart Supplement Light

Click Start→Settings→Camera→Image→Smart Supplement Light to open the interface as shown below. Select the camera you wish to configure. Set the conditions under which the camera will switch from IR light/B&W to Visible LED/Color image

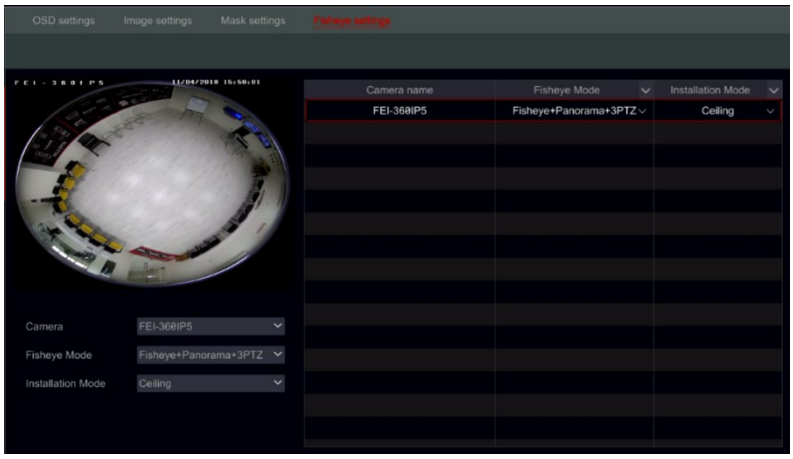


Please note:
Only Hybrid camera models support Smart Supplement Light configuration.

5.7.5 Fish-Eye

Fish-Eye Settings will allow you to set the installation way of the fish-eye camera in order to get the proper dewarping.

1. Click Start→ Settings→ Camera→Image→Fish Eye.



Here you can set the installation mode and your preferred view mode. Make sure that the installation mode is set properly for the image to be displayed correctly.

5.7.6 Image Adjustment (Live-View Interface)

Go to live-view interface. Choose the channel by clicking on the desired and click on button from the tool bar under the camera window to switch to the image adjustment interface.

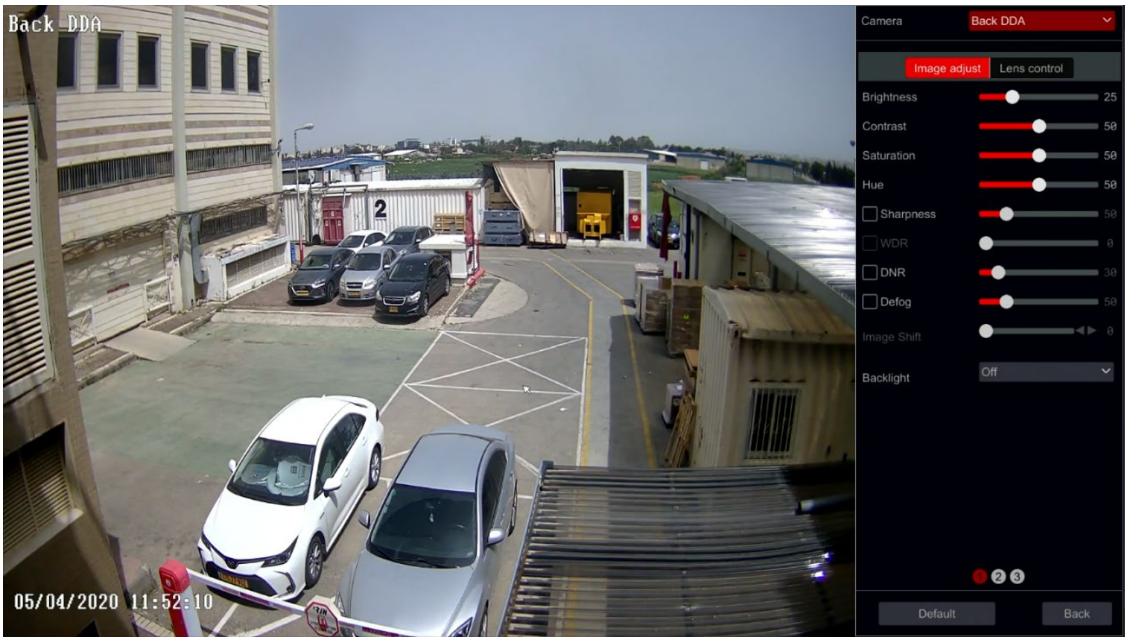


Image Adjustment

Drag the slider to set the image brightness, contrast, saturation and hue values. Check Sharpness, WDR and DNR to enable it and drag the slider to set their values. Click “Default” button to set these parameters to their default values.

The introductions of these parameters are as follows:

Parameter	Meaning
Brightness	Image brightness level
Contrast	The color difference between the brightest and darkest parts.
Saturation	The intensity of colors, expressed as the degree to which it differs from white.
Hue	Color levels of the image.
Sharpness	Relates to the sharpness level of the image and the image edges.
WDR	This refers to **Digital WDR.** For True-WDR (if supported the camera, please refer to “Backlight”
DNR	DNR (Digital Noise Reduction): decreases the noise levels and making the image smoother. Increasing the value will increase the noise reduction but it will reduce the image resolution and details.
Defog	Adding contrast and reducing the brightness of the camera

Backlight	Backlight, HLC and WDR (Wide Dynamic Range) function helps the camera provide clear images even under extreme light conditions. When there are both bright and dark areas in the field of view, WDR balances the brightness level of the whole image and provide clearer image. If enabled, there will be new control for the enhancement level
White Balance	Automatically adjust the color temperature according to the environment. Can also be set manually.
Anti-Flicker	Reducing flickering on the video
Exposure Mode	Settings the exposure of the camera. If “Manual” will be set, a new line will appear where the exposure value can be set.
Gain Mode	Set the Gain Mode of the camera
Gian Limit	Set the Gain Limit of the camera
Corridor Mode	Set the corridor mode of the camera
Image Mirror	Mirror the video image right and left.
Image Flip	Flip the video image upside down.
High FPS Mode	Switch the camera to work in 50/60FPS instead of 25/30FPS (Comes on the account of True WDR + Maximum resolution of 2MP)
Smart IR	Enable Smart IR
Day/Night Mode	Set the camera to Day / Night / Auto mode
Sensitivity	Sensitivity for switching day/night modes
Delay Time	How many seconds to delay before switching to day/night
IR Mode	Set the IR Mode (Auto/On/Off)

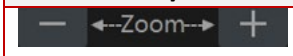
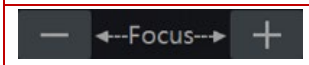
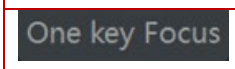
Please note:

1. Different IP Cameras will support different Image configuration features.
2. Some cameras have more than one settings page. You need to switch pages in the bottom of the image adjustment area.

Lens Control:

Select the camera and 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 introductions of these parameters and buttons are as follows:

Button/Parameter	Meaning
	Click + / − to zoom in/out.
Focus Mode	If manual mode is selected, focus button, “One Key Focus” and “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.
	Instant Focus
Re-focus when camera switches between day/night	If checked, the lens will focus automatically when the camera switches between day/night modes.

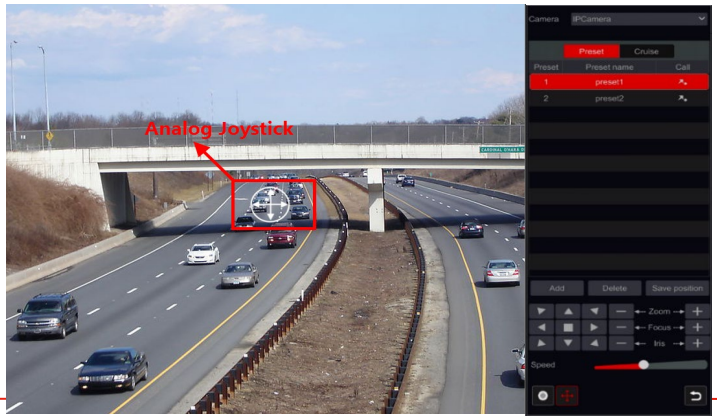
Please note:
This function is only available for the models with motorized VF (MVF) lens.

6. PTZ

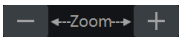
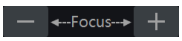
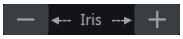
6.1 PTZ Control Interface:

The device supports full control over PT or PTZ cameras. Click on the desired camera and on the icon from the channel tool bar. A Basic PTZ control will pop up. Using this interface, you can move the camera.

If you need the full PTZ interface, Wither click on the icon positioned on the top left of the PTZ mini menu, or right click on the camera and choose “PTZ Control”. The live view will switch to the PTZ control interface as shown below. You can select another IP dome or PTZ from the dropdown menu on the top right of the PTZ interface.



Introductions of the interface buttons:

Button	Meaning
	/ / / / / / / / to rotate the dome. Click to stop rotating the dome.
	/ to zoom in / out.
	/ to increase / decrease the focal length.
	/ to increase / decrease the aperture.
	Drag the slider to adjust the movement speed.
/	/ to start / stop manual recording.
/	/ to hide / show the analog joystick.
	Return to the live view interface.

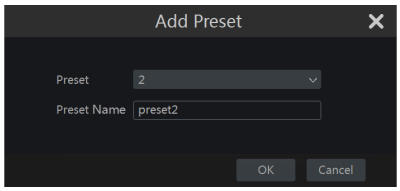
Analog Joystick Control

1. The analog joystick on the left side of the interface provides quick PTZ control. The dome or PTZ will move when you drag the analog joystick. The further you drag the analog joystick from the middle of the image, the faster the dome or PTZ will move. The dome or PTZ will stop rotating when you release the analog joystick or move it to the middle.
2. Click and hold the left mouse button to zoom in
3. Click and hold the right mouse button to zoom out

6.2 Preset/Cruise (PTZ Live interface):

Preset Settings (PTZ Live interface)

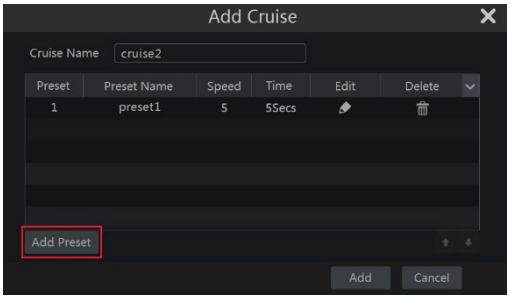
Presets can be used to save important locations and recalling it quickly when needed.
As default, the preset list is empty so you will have to add and configure the presets that are important to you.

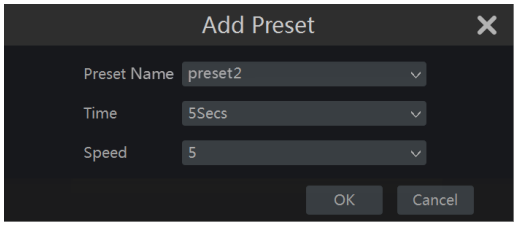


1. Click “Preset” to go to preset operation tab and click “Add” button to pop up a setting window as shown below. Select the desired preset number and input the preset name. Click “OK” to save the settings.
2. Adjust the camera direction and click “Save Position” to save the current preset position on the selected preset. You can also go to preset setting interface for preset setting.
3. Click in the preset list to call the preset; click “Delete” button to delete the selected preset.
4. You can add up to 255 presets for each supported camera.

Cruise Settings

Cruises are built from a sequence of presets and are used for creating a specified patrol between presets for an endless duration (Cruise will run until you will stop it, or move the camera). Therefore, you must save the desired presets before creating a cruise.





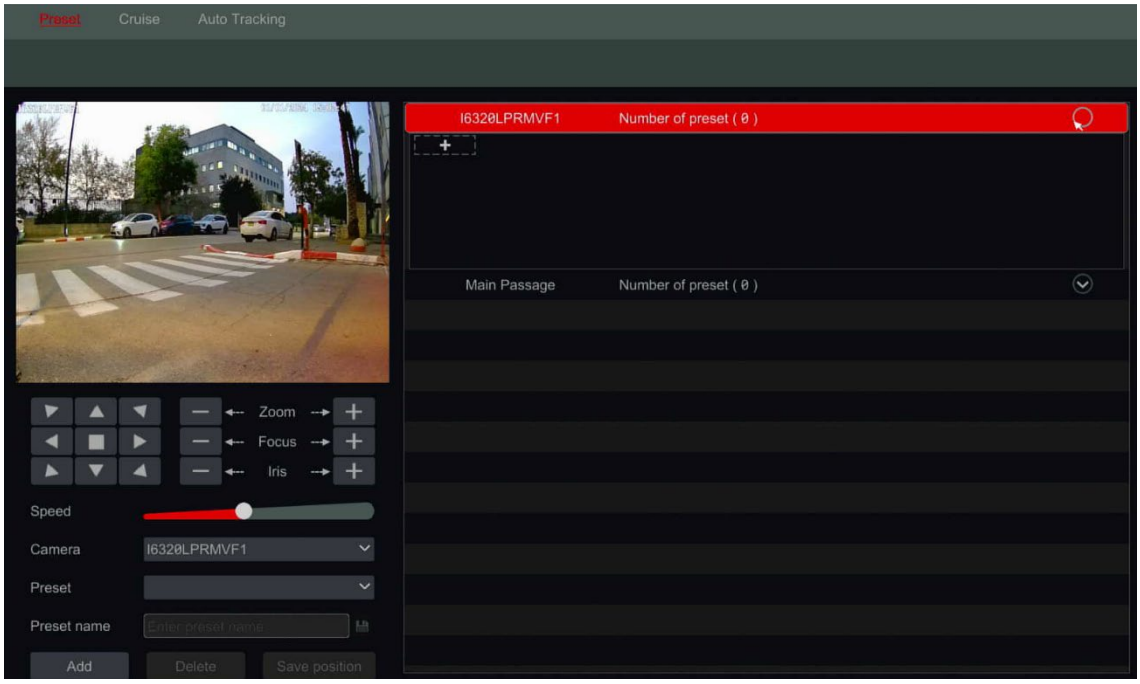
1. Click “Cruise” to go to cruise operation tab and click “Add” button to open the settings window as shown on the right.
2. Input the cruise name and click “Add preset” to pop up the “Add Preset” window as shown above on the right.
3. Select the preset name, dwell time and preset speed and click “OK”.
4. In the “Add Cruise” window, you can click to redefine the checkpoint. Click to delete the preset.
5. Click “Add” button to save the cruise.
6. You can also go to cruise setting interface for cruise setting.
7. You can add 8 cruises for each dome at most.

In order to activate the cruise, click to start the cruise and click to stop the cruise. Any movement or other command sent to the camera from the PTZ interface will stop the cruise as well.

Click “Delete” button to delete the selected cruise.

6.3 Preset/Cruise (PTZ Configuration Menu):

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



Add preset

Select the desired camera and click “Add” button to add preset; or click in the camera list on the right side of the interface to display the preset information of the camera and

click to add preset. The operations of the “Add Preset” window are similar to that of the PTZ control interface.

Edit preset

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

Delete Preset

Select camera and preset and click “Delete” to delete the preset.

Cruise Setting

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 the camera and click to add cruise. The operations of the “Add Cruise” window are similar to that of the PTZ control interface.

Edit Cruise

Select the camera and cruise in the “Cruise” interface. Input the new cruise name and click to save the cruise name. Click “Add Preset” to add preset to the cruise. Click to delete the preset from the cruise. Click a preset in the preset list and click to move the preset down the list and click 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 the cruise information of the dome and click on the top right corner of the cruise to delete it.

6.4 Auto Tracking:

Smart Tracking allows the camera to track detected DDA object. There are several related configurations:

Tracking Priority:

Once tracking is enabled, there are 2 options:

1. Manual Priority: Meaning that the operator can take control over the camera in any given moment and bypass the auto tracking algorithm, even during active tracking
2. PTZ Priority: Meaning that as long that auto tracking is enabled, the operator cannot control it. The auto tracking algorithm is the sole controller.

Still Time:

Once enabled, the auto tracking will cease active tracking and return back to the hope position after the set duration. If disabled, the auto tracking will remain on the position of the static object until another object will enter the scene.

Please note:

Only Z# cameras support Smart Tracking.

6.5 Home Position (Park Action):

Home Position (Park Action) configures the camera’s action when it is not in use by the operator for an x amount of time.

Enable it if needed, set the wait time, choose the action out of Preset, Cruise, Trace, Random Scanning, Boundary Scanning and set the command number if needed (For example, preset number 71)

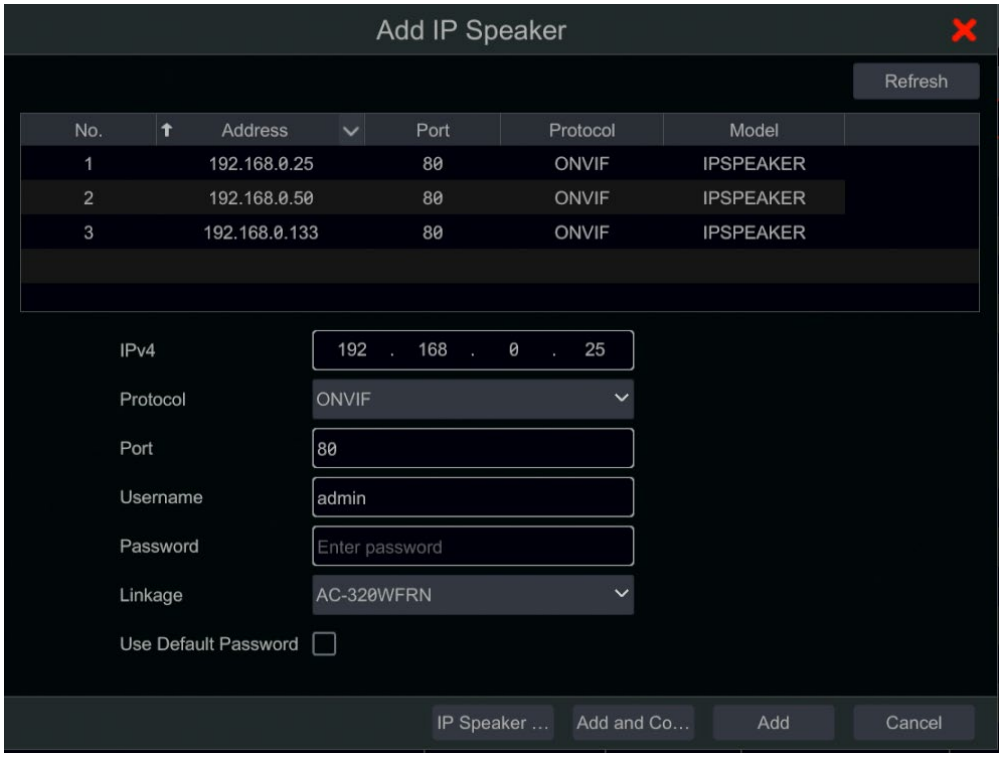
Please note:
Only Z# cameras support Home position configuration.

7. IP Speaker

Starting v1.4.12, the Ossia NVRs support integration with Provision-ISR's IP Speaker.

7.1 Add IP Speaker:

Since the IP Speaker integration is done using ONVIF protocol, the IP Speaker **must** be in the same network segment of the NVR, otherwise it will not be found automatically and will remain offline if added manually.



The detected IP Speakers will be listed in the top window. Since each IP speaker needs to be bound with a channel, it cannot be added in bulks, but only one by one.
Click on the IP Speaker you with to connect to, set the username/password manually or set "Use Default Password". Choose the bound channel through the "Linkage" drop down. Note that bound channels will be hidden from the list.
You can also choose from the list "NVR" which means that the IP Speaker will be used for 2 Way communication with the NVR.
Click "Add" to add the IP Speaker and close the adding interface.
Click "Add and Continue" to add the IP Speaker and keep the adding interface to add additional speakers.

Please note:
Bounding an IP Speaker to IP Channel will override the IP camera audio when using the NVR.

7.2 Edit IP Speaker:

Click on to change the IP Speaker details/credentials and/or replace the bound channel.

7.3 Delete IP Speaker:

Click on to delete the IP Speaker.

8. Record & Disk Management

8.1 Record Configuration:

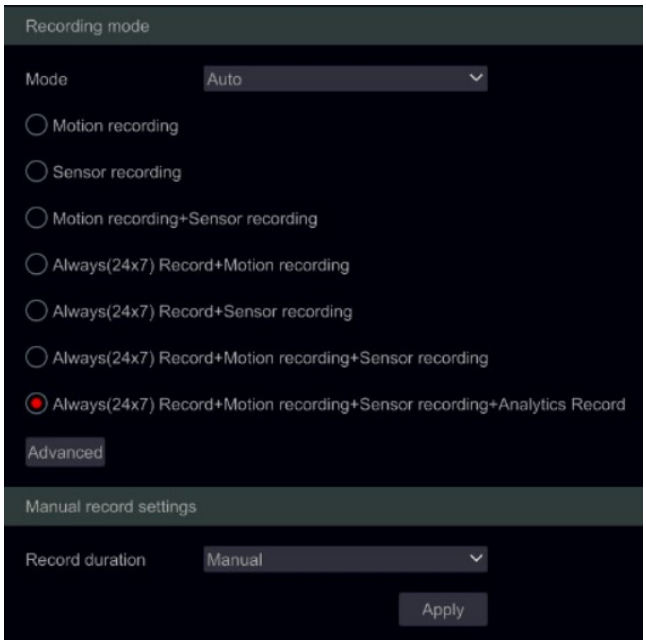
8.1.1 Mode Configuration:

Please format the HDDs to enable recording

The Ossia recording interface was redesigned to be clearer and easier to configure. It is based on statistics showing that most users configure the recording to work all year long in 24x7 schedule – the "Auto" mode is the best choice for these users. "Manual" mode is for users who wish to customize the recording/schedule configuration.

Click Start→Settings→Record→Mode Settings to go to the mode settings interface.

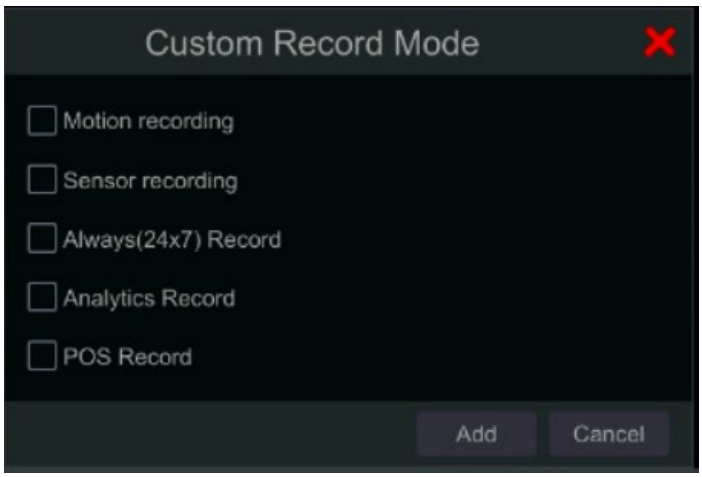
Auto Mode: The standard setting will include the following presets:



Motion Record: Record will start upon *Motion Alarm* under 24x7 schedule for all channels.
Sensor Record: Record will start upon *Sensor Alarm* under 24x7 schedule for all sensors.
Motion Record + Sensor Record: Record will start upon *Motion or Sensor Alarms* under 24x7 schedule for all channels and sensors.
Always (24 X 7) Record + Motion Record: All the channels will be recorded continuously. *Motion alarms* will be marked in the event list and trigger "Event Record".
Always (24 X 7) Record + Sensor Record: All the channels will be recorded continuously. *Sensor alarms* will be marked in the event list and trigger "Event Record".
Always (24 X 7) Record + Motion Record + Sensor Record: All the channels will be recorded continuously. *Motion and sensor alarms* will be marked in the event list and trigger "Event Record".

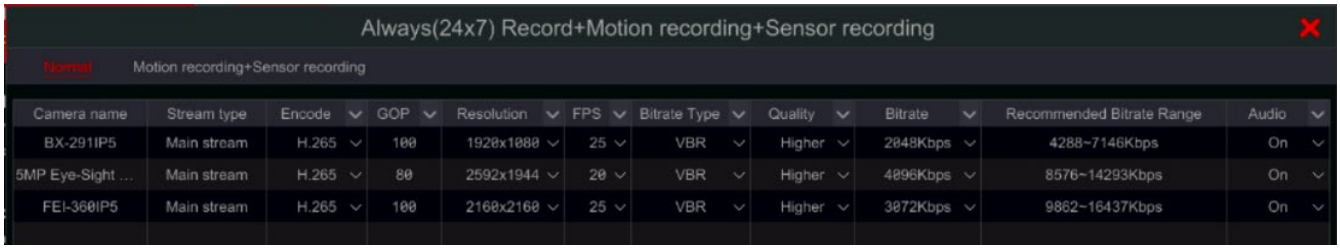
Always (24 X 7) Record + Motion Record + Sensor Record + ***Analytics Record:*** All the channels will be recorded continuously. *Motion, sensor and analytics alarms* will be marked in the event list and trigger "Event Record".

If you wish to create a personalized combination, click on the "advanced button to open the advanced menu: The advanced menu allows you to create any combination you require (As long as it is not currently available in the standard menu). Tick the recording triggers you wish for the combination to have and click on "add" to continue. The new combination will be added as a new line to the standard menu. Only one customized combination can be used. If you wish to edit it, click on the advanced button once again and change the selected triggers.



Selecting one of the auto modes will pop up the stream settings window as shown below. Set the video encode type, resolution, FPS, bit-rate type, bitrate and audio for each of the camera and click "OK" to save the settings. It is recommended to follow the bit-rate recommended by the system in the "Bit-Rate Limit Recommended Range" Tab.

Important: In case you chose one of the continuous modes, make sure to configure both "Normal" and "Event" settings.



Camera name	Stream type	Encode	GOP	Resolution	FPS	Bitrate Type	Quality	Bitrate	Recommended Bitrate Range	Audio
BX-291IP5	Main stream	H.265	100	1920x1080	25	VBR	Higher	2048Kbps	4288~7146Kbps	On
5MP Eye-Sight ...	Main stream	H.265	80	2592x1944	20	VBR	Higher	4096Kbps	8576~14293Kbps	On
FEI-360IP5	Main stream	H.265	100	2160x2160	25	VBR	Higher	3072Kbps	9862~16437Kbps	On

Encode: This will set the video encoding type based on the support of the connected device. Most devices support H264 and H265, but some devices can support more efficient encoding such as H265+ and H265S.

GOP: Stands for "Group of Pictures" and required for efficient decoding. Keep as configured unless required otherwise.

Resolution: the higher the resolution, the bigger the image.

FPS: Higher frame rate delivers more fluency. However, more storage space will be required.

Bitrate Type: Choose between CBR (Constant Bit-Rate) and VBR (Variable Bit-Rate).

Bitrate: bitrate stands for the compression aggressiveness. The lower the bitrate, the higher the compression. High compression means lower bandwidth and storage space usage, but also decreasing the video quality.

Recommended Bitrate Range: The system will show a range of bitrates that balances between quality and bandwidth/storage consumption according to the configuration you set. It is recommended to follow this recommendation.

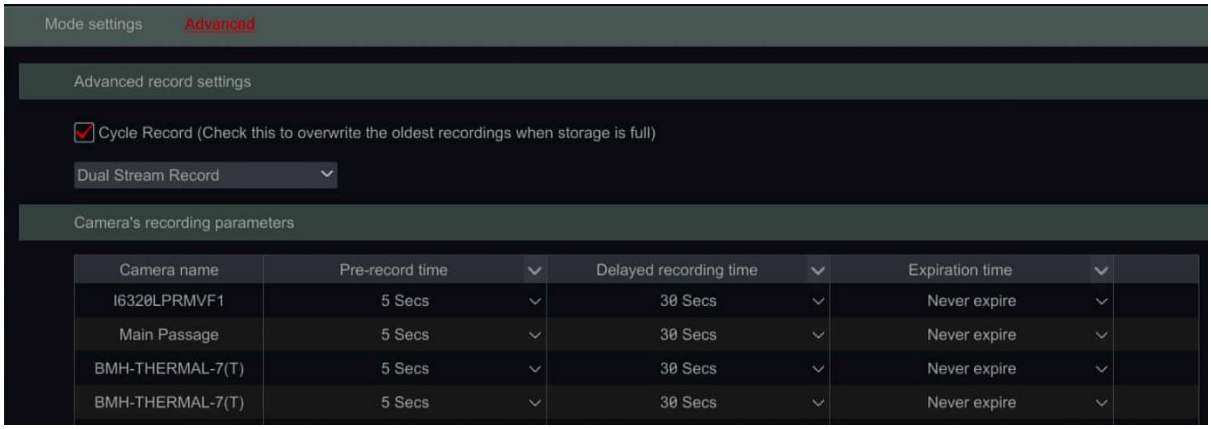
Audio: Select weather to record audio or not for the chosen channel.

Manual Mode

If *manual mode* is selected, you will need to set the encode parameters and schedules for each of the cameras. Failing to do so will result in recording inconsistency or complete lack of recording.

8.1.2 Advanced Configuration

Click Start→Settings→Record→Advanced to go to the following interface. Enable or disable cycle and sub-stream recording, set the pre-alarm record time, post-alarm record time and expiration time of each camera and click "Apply" to save the settings.



Cycle record: The recording will work in FIFO method – First in first out – meaning that the oldest recording will be overwritten by new recording once the HDD is full.
Dual Stream Recording: Enable/Disable the sub-stream recording of the device.

Please note:

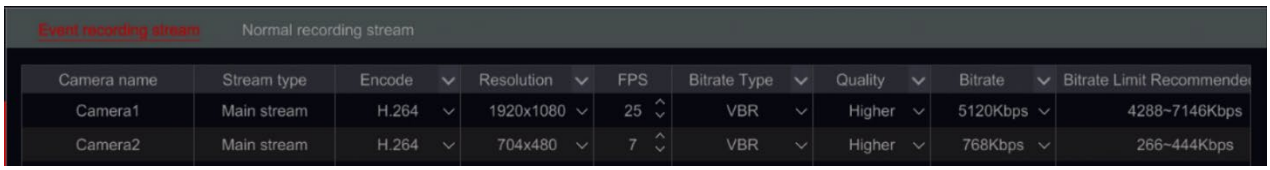
Disabling sub-stream recording will increase the duration of main stream recording but will dramatically reduce system performance and disable many features that rely on the sub-stream recording in order to work.

Pre-alarm Record Time: set the record time duration before the alarm event started.
Post-alarm Record Time: set the record time duration after the alarm event ended.
Expiration Time: set the expiration time for recorded video. Recordings will not be kept longer than the specified duration even if the HDD is not full.

8.2 Encode Parameters Setting

8.2.1 Main Stream recording

Click Start→Settings→Record→Encoding Parameters to access the interface shown below. Set the video encode, resolution, FPS, bitrate type, bitrate and audio of main stream for each of the cameras.



Important: this interface offers both “Event Recording Stream” and “Normal Recording Stream” configurations. Make sure to configure both. You can set the record stream for each camera set all cameras together by clicking on . Click “Apply” to save the settings.

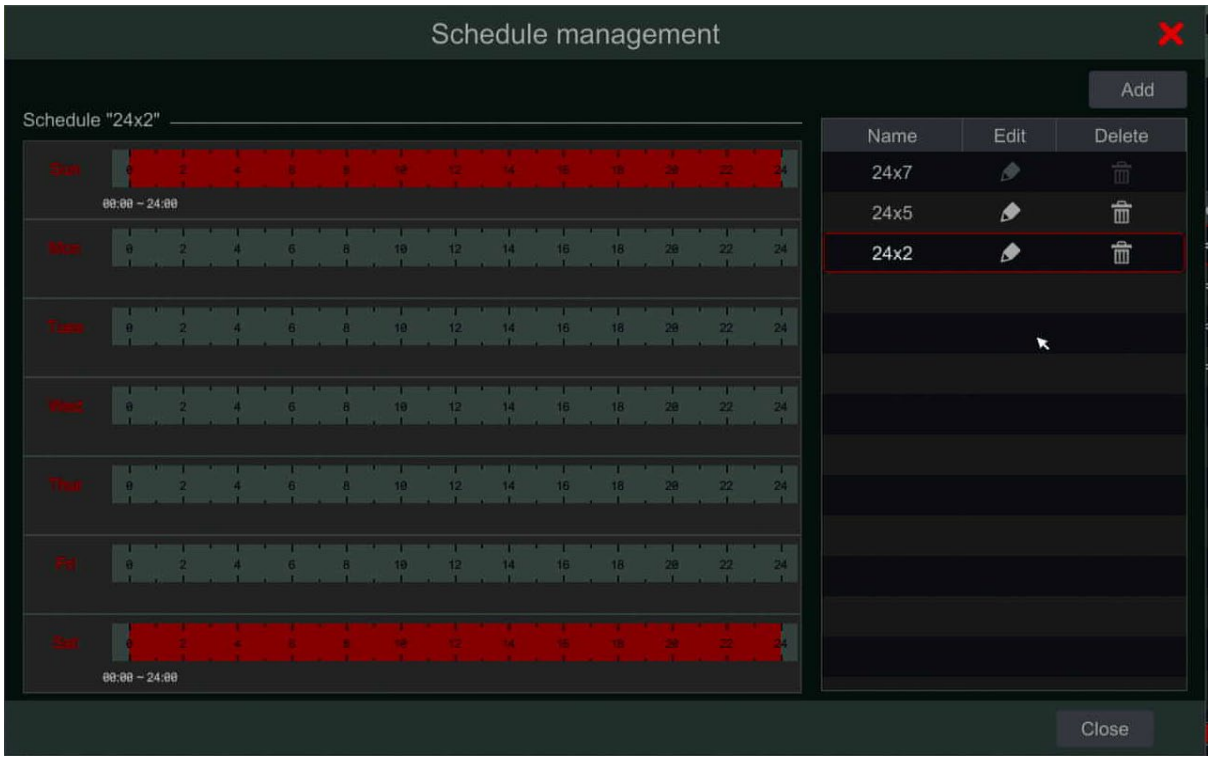
8.2.2 Sub-Stream recording

Click Start→Settings→Record→Encoding Parameter→Record Substream Settings to go to “Sub-stream” interface.

The default Mode is “Auto” which will record in D1/25Fps/512Kbps. You can switch the Mode to Manual and set the sub-stream video encode type, resolution, FPS, Bitrate type and bitrate for each camera or for all cameras together by clicking on . Click “Apply” to save the settings.

8.3 Schedule Setting

Interfaces that include schedules will have “Schedule Management” button. This button will open the following interface:



8.3.1 Add Schedule

The pre-set schedules are “24 x 7” (All week), “24 x 5” (Weekdays - Monday to Friday) and “24 x 2” (Weekends – Saturday & Sunday). “24 x 7” schedule cannot be deleted or modified while “24 x 5” and “24 x 2” can be edited or deleted.

Click the schedule name to display the detailed schedule information on the left side of the interface. The lines on the left stand for the seven days of the week. Each line stands for the daily 24 hours. Red marks the active selection and grey marks inactive selection.

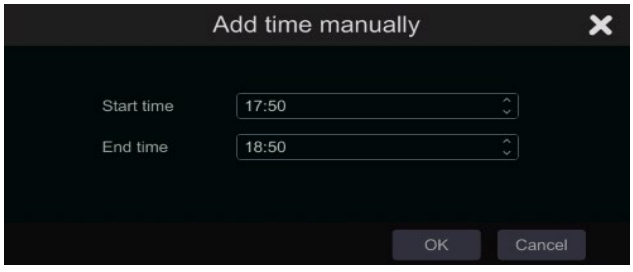
Click to add a new schedule or to edit an existing one. Refer to the picture below.

Input the schedule name, set the schedule times and click “Add” to save the schedule. You can set day schedule or week schedule. -Active duration button -Inactive duration button.

Set Single Day Schedule

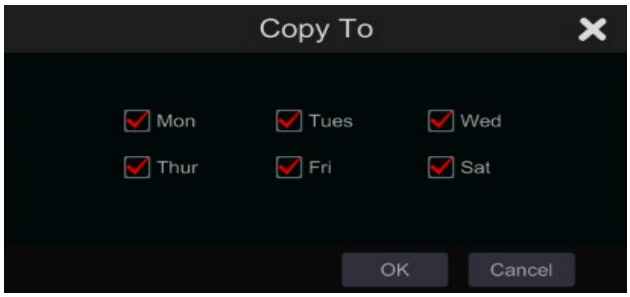
Free Editing: Click and drag the mouse cursor on the time scale of a specific day to mark the active duration. Click and drag the cursor on the time scale of a specific day to make a selected area inactive.

Manual Editing: You can manually set the record start time and end time: select “Manual” from beneath the day bar and set the desired time. Click “Ok” to confirm.



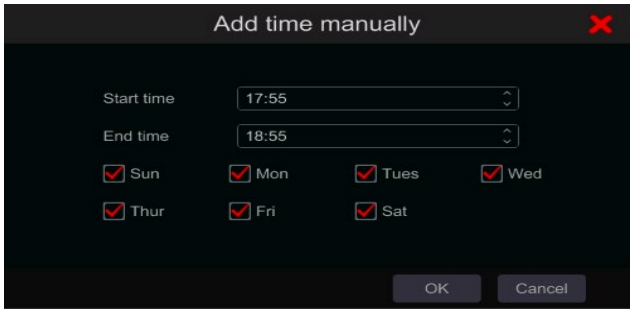
Click “All” to set all day recording; click “Reverse” to swap the marked and unmarked areas; Click “Clear All” to clear all the selected area in a day.

Copying Schedules: After completing a setting for any day, you can click “Copy To” from beneath the day bar to copy the selected schedule to other days. Refer to the picture below. After clicking on “Copy To” from the source day, check the destination days in the window and click “OK” to save.



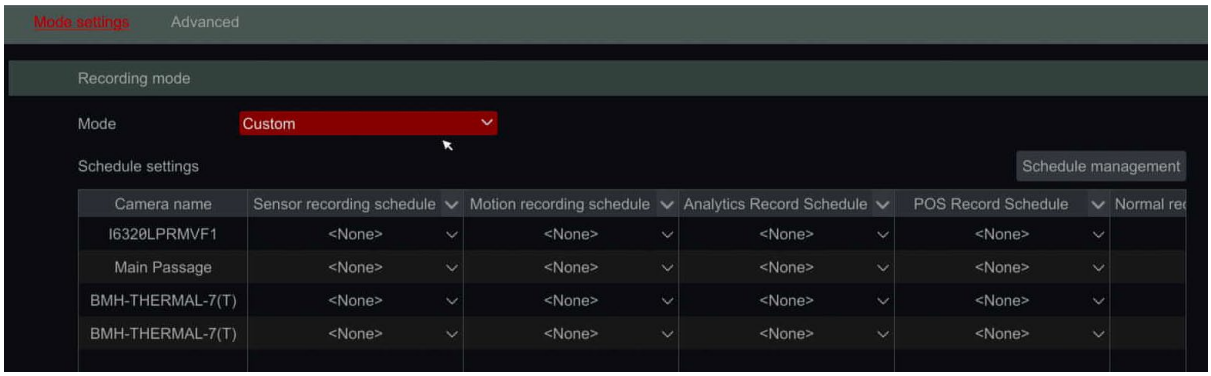
Set Multi-Day Schedule

Use “Manual” beside to set the weekly schedule. Refer to the picture below. Set the start and end time, check the days in the window and 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.



8.3.2 Record Schedule Configuration

Click Start→Settings→Record→Mode Settings. If switching to “Custom” mode, schedule management will become available



Define the schedule for sensor, motion, analytics, POS and normal recording. Click “None” in the drop-down menu to clear the selected schedule.
Click “Apply” to save the settings.

8.4 Record Mode

8.4.1 Manual Recording

Method One –Manual record for all channels: Click on the tool bar at the bottom of the live-view interface to enable manual recording for all cameras.
Method Two –Manual record for single channel: In the live-view interface – either right click on the desired camera and choose “Manual Record On” or left click on the desired camera window and click on the channel tool bar.

Please note:

Click Start→Settings→Record→Mode Settings and set the manual record duration in the referred menu. Click “Apply” to save the settings. Default settings is “Manual”

8.4.2 Scheduled Recording:

Scheduled Recording: the system will record automatically according to the schedule weather there is an additional alarm or not.

8.4.3 Motion Based Recording:

The system will start recording based on motion alarms. You can use the default settings or create customized setting for each camera as follows:

1. Set the motion alarm schedule for each camera.
2. Enable the motion and set the motion area of each camera.

The camera will start motion-based recording as soon as the above settings are applied.
Enable Motion Icon: In some cases, the motion detection on the camera is disabled. In such a case, even with “Motion Recording” on, there will be no recording. Click on the “Motion On” icon ( ) in order for the system tto automatically go through all the cameras, enable motion detection, set the detection area to full scene and the detection schedule to 24x7.

8.4.4 Sensor Based Recording:

The system will start recording based on sensor alarms. Configure the recording parameters as follows:

1. Set the sensor alarm schedule for each camera/alarm input.
2. Set the NO/NC type of the sensor, enable the sensor alarm and check and configure the “Record”.

8.5 Analytics Based Recording:

The system will start recording based on analytics alarms. Configure the recording parameters as follows:

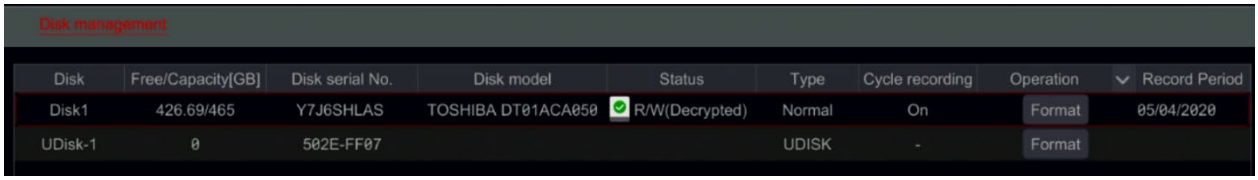
1. Set the analytics alarm schedule for each camera.
2. Set each one of the available analytics alarms and check and configure the “Record”.

8.5.1 POS Based Recording:

The system will start recording based on POS events. POS Recording enables 24x7 schedule recording automatically.

8.6 Disk Management:

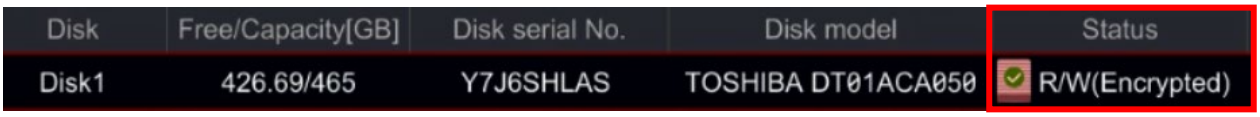
Click Start→Settings→Disk→Disk Management. On this interface you can view the device's disk numbers, status and recording dates stored on each drive. Click "Format" button to format the desired HDD or click on to format all drives together.



Please note:

New HDD/s should be formatted before it can be used by the system.

v1.4 Allows encryption of the HDDs. Encrypted HDD will require the encryption password if trying to access the recorded data using another recording device or by the RPAS PC player. Click on "Encrypt Data" (Supported by v1.4 and up). Choose the HDDs you wish to encrypt and set an encryption password. Click on "Encrypt Data" to finish. You will have to enter the admin credentials again to confirm your identity. After the process is done. The HDD will appear as "Encrypted".



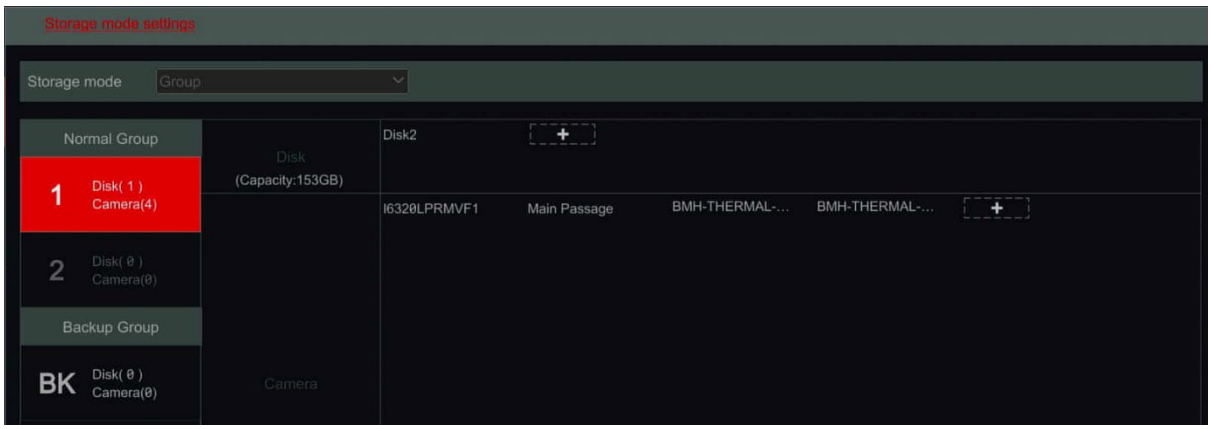
If you wish to decrypt the HDD, repeat the process.

Please note:

1. Encrypting the HDD requires format (Data cannot be encrypted retroactively)
2. Decrypting the HDD formats the HDD. All data will be erased.
3. The encryption password cannot be restored in any way or matter. Forgetting it will make the data unusable in case it will be required by any external source. In such a case, the HDD will have to be formatted to become useable again.

8.6.1 Storage Mode Configuration

Click Start→Settings→Disk→Storage Mode.



There are four available disk groups. By using disk group, you can allocate a specific camera to a specific disk (the recorded data from the grouped cameras will be stored in the disks allocated for that group).
Newly added disks and cameras will be joined into group one as default. The disks and cameras in the different groups can be deleted except of group one (select a disk group and click ⊗ on the top right corner of the added disk or camera to delete it from the group). The deleted disks and cameras will be moved into group one automatically.
Each group can receive disks and cameras from other groups. Each disk/camera can be allocated to one group only.

Edit Disk/Camera Groups:
Select a disk group and click + in the disk or camera row to pop up a window. Check the disks or cameras in the window and click "Add".

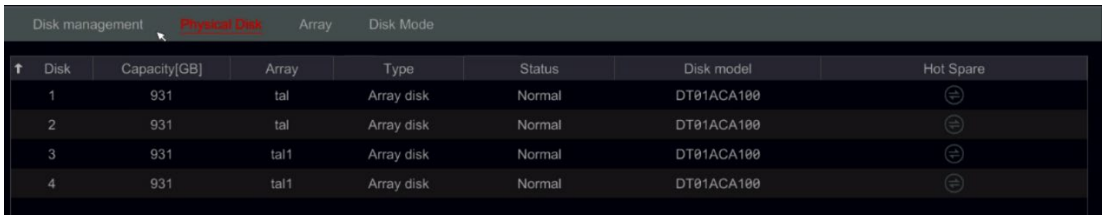
Please note:
Changing group allocation for a disk/camera will result in losing data of the changed disk/camera.

8.6.2 Disk Mode (Models supporting RAID only):

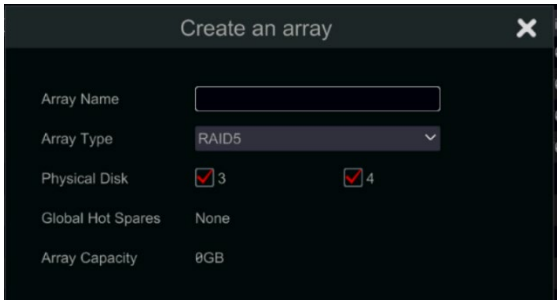
Disk mode allows you to enable RAID (If supported by the device). Once the RAID is enabled, the device will reboot and new options will be available.

8.6.3 Physical Disk (Models supporting RAID only):

This menu is available only if RAID is enabled. Here you will see all the disks and their current status. Before you can start recording, you will need to assign the disks to RAID groups or assign it as "Hot Spare".



Creating an array:



In order to assign disks, click on "Create Array". The following window will appear. Set a name to the new array and choose the array type. The available options are RAID0, RAID1, RAID5, RAID6, RAID10. (For more information about RAID types, please refer to appendix 2 at the end of the manual).
Choose the disks that you want the array to include (Note that different RAID types require different number of disks.
Click "Add" to finalize the process.

Please note:

1) All the data stored on the HDD will be deleted.

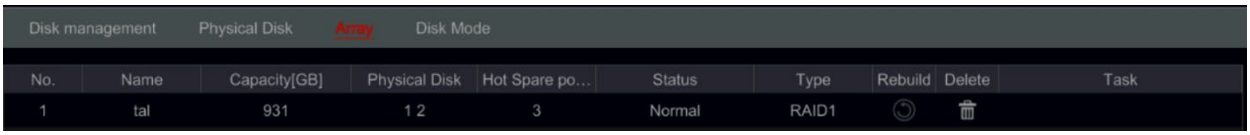
2) Up to 2 RAIDs can be configured.

Setting a "Hot Spare"

In terms of RAID, "Hot Spare" is a backup disk that is ready for use in case that an active array disk has failed. In such case, the hot spare will replace the failed array disk automatically and rebuilt its data (a process that takes time). The "Hot spare" of the system is global meaning that it will be used for all RAIDs configured on the system.
In order to assign a disk to perform as "Hot Spare", click on the icon next to it and confirm the process. Repeat the process to change it back to normal state.

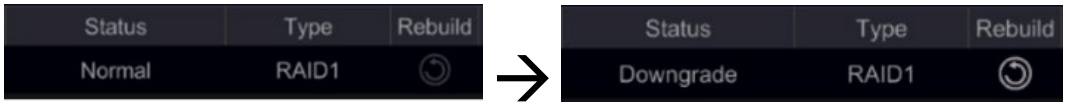
8.6.4 Array (Models supporting RAID only):

This menu is available only if RAID is enabled. Here you will see all the created RAID groups and their current status (Name, Capacity, Assigned Disks, Hot Spares, Status). Also, you will be able to delete the arrays and rebuilt it if required.



Rebuilding an array:

In case one of the disks of the array failed – the array state will change to "downgraded" and the rebuild button will become active as follows.



Once the faulty disk was replaced with a new one, click on the "rebuild" to restore the array state to normal.

Deleting an array:

If you wish to delete an array, click on the icon and confirm the process.

8.6.5 View Disk and S.M.A.R.T. Information:

Click Start→Settings→Disk→View Disk Information; click "S.M.A.R.T. Information" to view the working status of the HDD. Refer to the picture below.

9. Standard Search, Playback & Backup

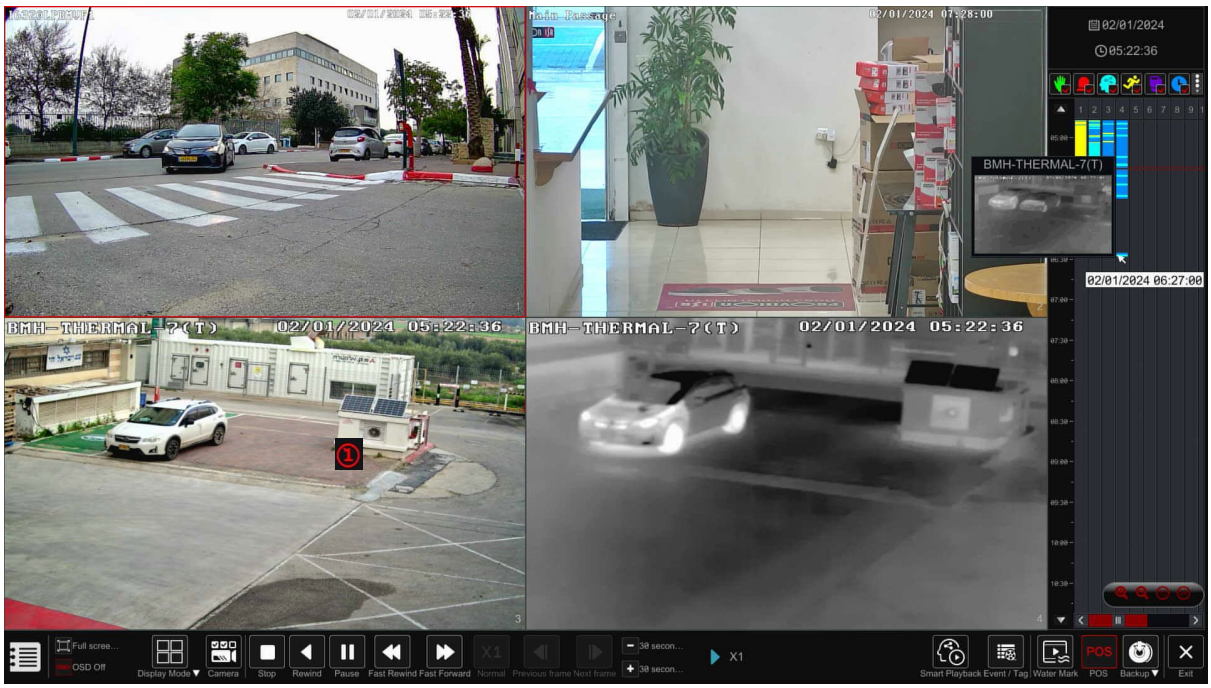
9.1 Instant Playback

Click on the channel tool bar at the bottom of the live-view camera window to play back the record (click on the general tool bar at the bottom of the live-view interface to set the default playback time). Drag the playback progress bar to change the playback time. You can also click the right-click menu "Instant Playback" in the camera window and set the instant playback time to play back the record.

9.2 Playback Interface Introduction

9.2.1 Standard Playback

Click on the general tool bar at the bottom of the live-view interface or click Start→Playback. (Click on the general tool bar at the bottom of the live-view interface to set the default playback time).



The interface will switch from live-view to playback and the cameras from the live-view will be played back automatically. You can add the playback cameras manually by clicking on + in the playback window to open the “Add Camera” window. Mark the cameras you wish to add and click “Add”. The system supports a maximum of 16 synchronous playback cameras.

The buttons of the main tool bar are introduced in the table below:

Button	Meaning
	Start menu button.
	Full screen button. Click it to show full screen. Click it again to exit the full screen.
	Screen split modes.
/	“OSD ON/OFF” button. Click it to enable/disable the OSD
	Change the displaying cameras
	Stop button.
	Rewind button. Click it to play video backward.
	Play button. Click it to play video forward.
	Pause button.
	Decelerate button. Click it to decrease the playing speed.

	Acceleration button. Click it to increase the playing speed.
X1	Return to normal playback speed (x1)
	Previous frame button. It works only when the forward playing is paused in single screen mode.
	Next frame button. It works only when the forward playing is paused in single screen mode.
30S	Click − to step backward 30s and click + to step forward 30s.
	Enable/Disable Watermark appearance
POS	Enable/Disable POS data appearance
	Smart Playback Icon.
	Event list/tag button. Click it to view the event records of manual / schedule / sensor / motion and the tag information.
	Backup button. Drag the mouse on the time scale to select the time periods and cameras and click the backup button to back up the record. (After marking the area for backup, you can also click on the right mouse button)
	View the backup status.
	Back button. Click it to return.

Click on the playback window to show the channel tool bar. Right click on the window to show the menu list. The tool bar and menu list are introduced in the table below.

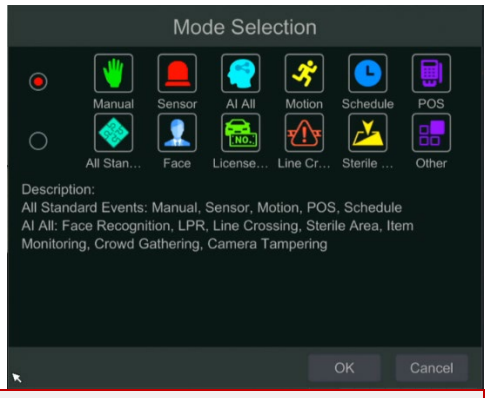
Button	Menu List	Meaning
	--	Move tool. Click it to move the tool bar.
	Enable Audio	Click it to enable audio and listen to the camera's audio channel.
	Snap	Click it to take a snapshot. Not supported by "X" models when playback is paused.
	Digital Zoom In	Click it to go to the digital zoom. The playback digital zoom interface is similar to live-view digital zoom interface. Click to pause the playback. When the record is paused while in forward playing mode, you can click to view the previous frame and click to view the next frame.
	Fish Eye	Click it to open controls for Fish-Eye cameras (If applicable) as described in the "Live-View" Chapter.
	Add Tag	Save a tag of the exact date and time you wish to save. You can use the tag later to go back quickly to the tagged point. When adding a new tag, the system will name it with the saved time automatically. You can change the name or edit it later.
	Switch Camera	Click it to switch the playback camera to a different camera that will playback the exact date and time. Click it and choose the new camera in the window. Click "OK" to change the camera.

	Close Camera	Click it to close the playback camera.

Time Bar introduction:

Button	Meaning
	Set/Change the playback date
	Set/Change the playback time
* *	Manual Record markings. Uncheck it to remove manual record display
* *	Sensor Alarm Record markings. Uncheck it to remove manual record display
* *	Analytics Alarm Record markings. Uncheck it to remove manual record display
* *	Motion Alarm Record markings. Uncheck it to remove manual record display
* *	Schedule Record markings. Uncheck it to remove manual record display
* *	POS Record markings. Uncheck it to remove manual record display

With the introduction of advanced analytics, you can now switch from “Standard” playback markers to “Analytics” Playback markers. Click on the menu marker ( ) to open the interface on the right. Choose between “Standard” and “analytics” and click OK to confirm. The new icons and color markers will be as follows:



Button	Meaning
* *	All pixel-based analytics
* *	Face Detection/Recognition
* *	LPR (License Plate Recognition)
* *	Line Crossing Analytics
* *	Sterile Area Analytics
* *	Other Analytic Types

** Playback must be stopped completely before these icons can be used. After stopping the playback use icon to add the desired cameras for search/playback.

Introduction of the record time scale:

Button	Meaning

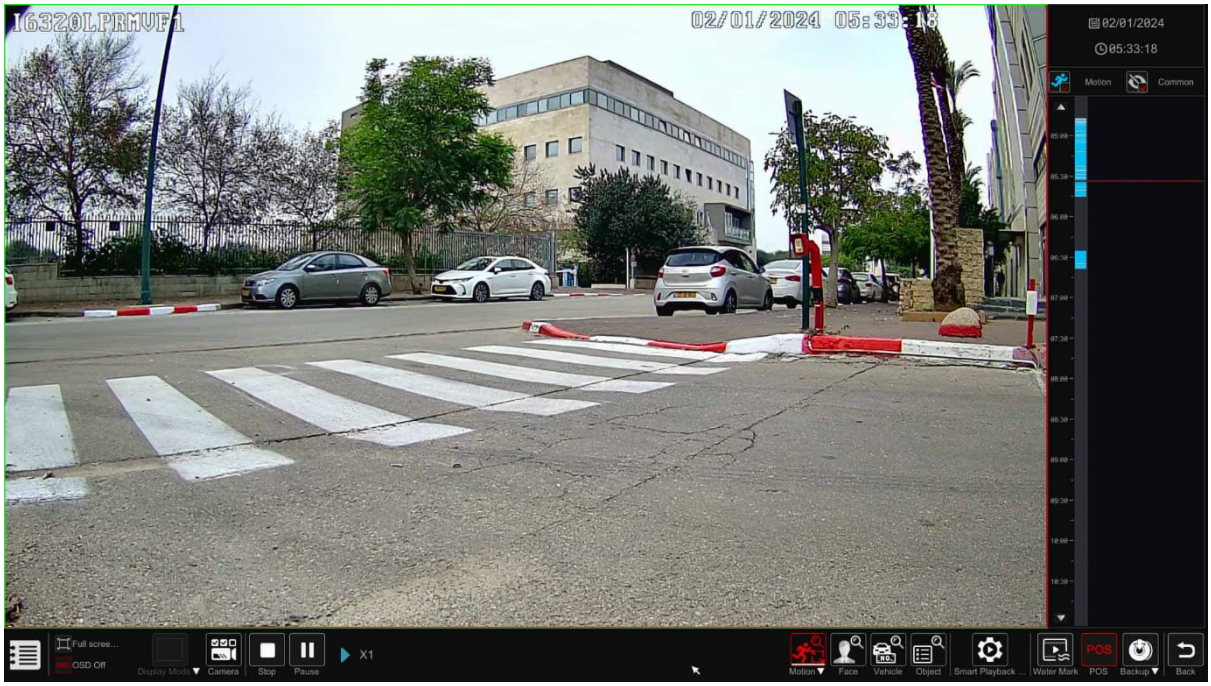
	The time-scale default view is 24 hours. Click on this icon to return to 24 hours view
/	Zoom in/out within the playback time scale
	Move up the time scale (The mouse wheel can also be used)
	Move down the time scale (The mouse wheel can also be used)

The record time scale shows different record types with different colors. The green color stands for manual record, red color stands for sensor alarm record, yellow color stands for motion alarm record and blue color stands for schedule record. Click the time scale to set the playback exact location.
Drag the mouse cursor on the time scale to select the backup area and right click on the marked area or click to pop up a backup information window. Select the destination device, backup path and backup format and click “Backup” to start the backup process.

9.2.2 Smart Playback

Click on the smart playback icon to switch the playback interface from “Standard” to “Smart”.
Smart Playback allows you to perform simple analysing of recorded video while playing it back, saving a lot of time and efforts. It only works on a single channel and cannot work on multiple channels simultaneously.

The Smart playback will display all the filtered results and play it as you wish.



We will only touch the differences between the “Standard” and “Smart”

9.2.2.1 Motion Based Smart Playback

The options for Motion Detection Smart analytics as follows:

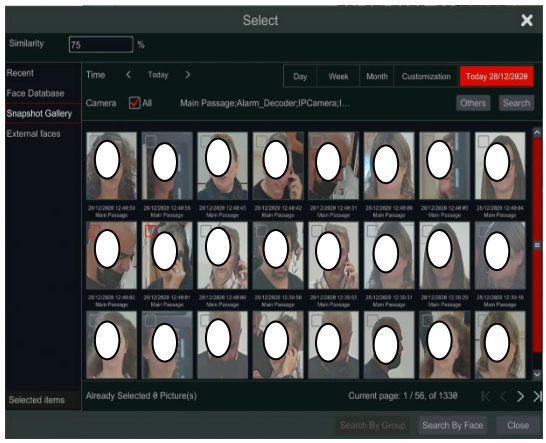
Button	Meaning
	Full screen motion search
	Square selection motion search
	Line Crossing (Bi-Directional)
	Polygon selection (up to 4 Corners)

9.2.2.2 Analytic Based Smart Playback

The system allows you to apply additional analytic filters such as face recognition or LPR to the smart search, click on the desired icon to open the filter interface.

Face Recognition Filter: In the following interface click on in order to activate the face filter and set the similarity value.

You can choose face/faces from the following options:



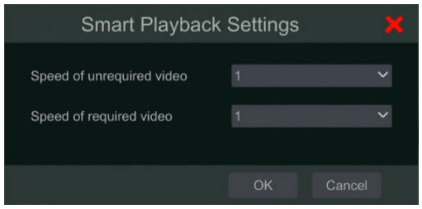
1) Face database – Search from faces already in the database.
   A) Here you can choose from the thumbnails or search by name. Click on “More” to narrow down groups or tick “All” to search/display within all groups.
   B) Tick the face/faces you wish to search for and click on Search by face/group as needed.
2) Snapshot Gallery – Search within snapshots taken by the system
   A. Set the time range for the face snapshot search. (Day to choose a day, Week to choose a week, Month to choose a month, customization to set a unique time range and Today to choose the date of today starting at midnight).
   B. Choose the camera/cameras that took the face snapshot. Click on “More” to choose specific cameras or tick “All” to choose all cameras.
   C. Choose whether you like to see recognized and unrecognized faces in the search.
   D. Tick the face/faces you wish to search for and click on Search by face/group as needed.
3) External Faces – Choose a picture file that contain a single face from a USB storage.
   A. Select the USB storage under the “Device Name”
   B. Select the relevant file (Must contain a single clear face).
   C. Click on Search face.

LPR Filter: In the following interface click on in order to activate the LPR filter.

You can choose face/faces from the following options:

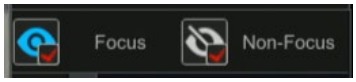
1. Vehicle database – Search from plates already in the database.
2. Customization – Input the license plate you wish to search for in a free text form:

Smart Search Settings: Click on the icon to open the settings menu: Here you can set if to skip unrequired video or play it.
You can set the playback speed for required video and unrequired video (if requested).



After applying smart playback filter you will see that the time bar will display the original time bar next to the filtered time bar as follows:

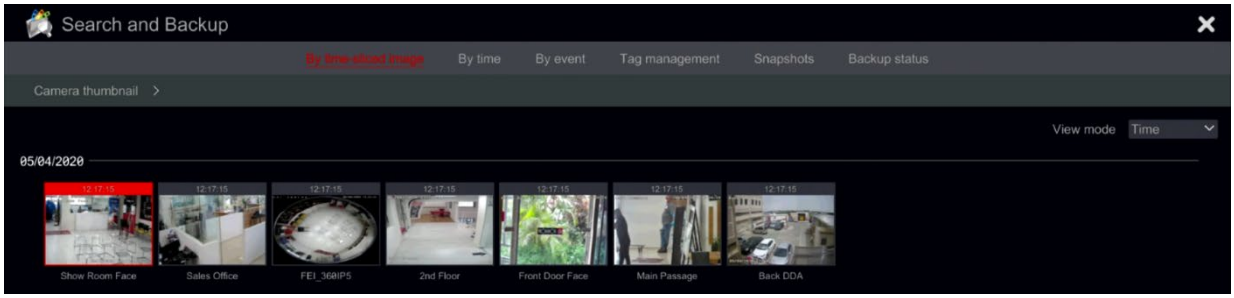
Use the top controllers to choose if to view the required video only, or both required and unrequired video.



9.3 Record Search, Playback & Backup

9.3.1 Search & Playback by Time-sliced Image

Click Start→Search & Backup→By Time-sliced Image.
The "Time-Sliced Image" search is designed to quickly find a change in the scene. Mainly missing or appearing object. If the duration of the searched event is shorted than 1 minute, this is not the right interface for it.

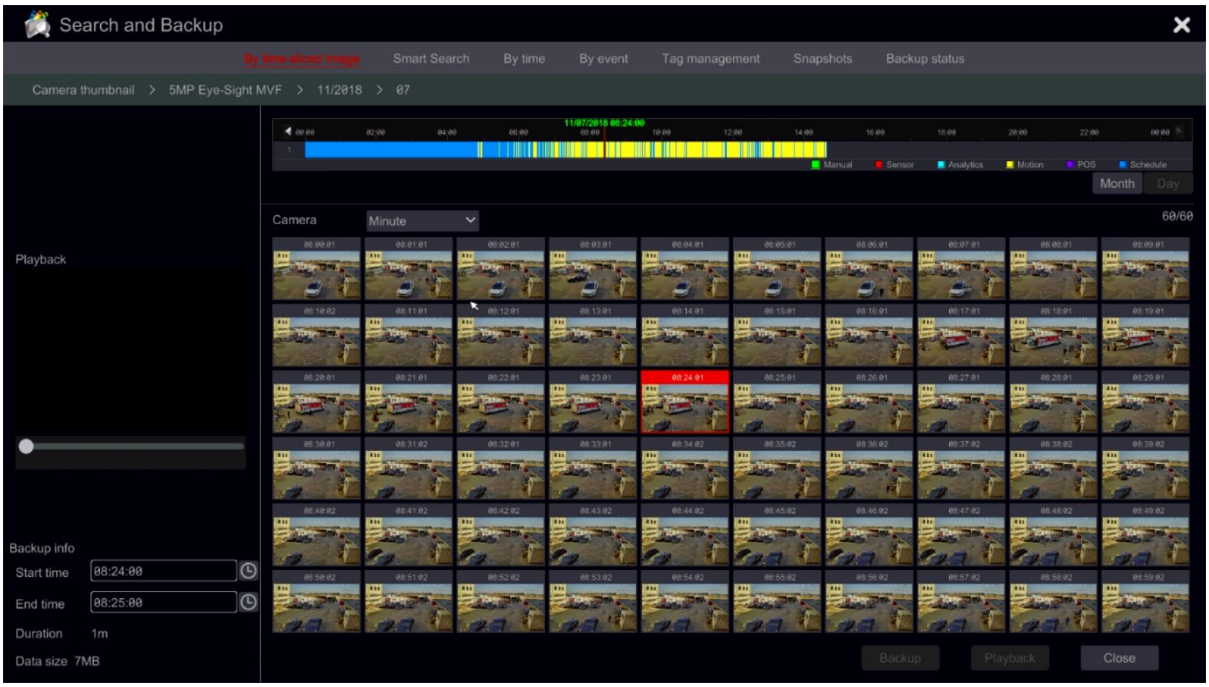


There are two view modes: by time and by camera. In the time view mode, a maximum of 64 camera thumbnails can be showed. If the camera thumbnail number is greater than 64, the cameras will be listed by their camera name, and not as a thumbnail. A maximum of 196 camera names can be listed. If the camera name number is more than 196, the time view mode will be disabled and only the camera view mode will be available.

1. Double click on the selected camera or select one camera and click the "Open" button. The camera will refine from "Day" view to "Hour" view. Repeat this stage to refine from "Hour" view to "Minute" View.
2. You can also click once on the thumbnail to commence playback on the left window. This will help you to confirm if you are in the right camera/time.
3. Once in "Minute" view, double clicking on any image thumbnail will open the full playback interface and commence playback for the selected camera at the specific time and date.
4. You can click once on the image box to play the record in the small playback box on the left side of the interface (If the thumbnail is blackened out – it means there is no

record data available)

5. You can perform backup directly from this interface in two methods:
   A. Left click and drag the mouse on the time scale to select the segment for playback and click “Backup” button to continue; select the device, backup path and backup format in the opened window and click “Backup” button to start the backup.
   B. After choosing the channel, click on “Set Backup Time” and input the start and end times. Confirm by clicking on “OK” and start the backup process using the “Backup” button.
6. Click “Playback” button (Or double click on the thumbnail) to commence playback in the playback interface.
7. Click “Close” to close the interface.



9.3.1.1 Time Slice Mode Working methods:

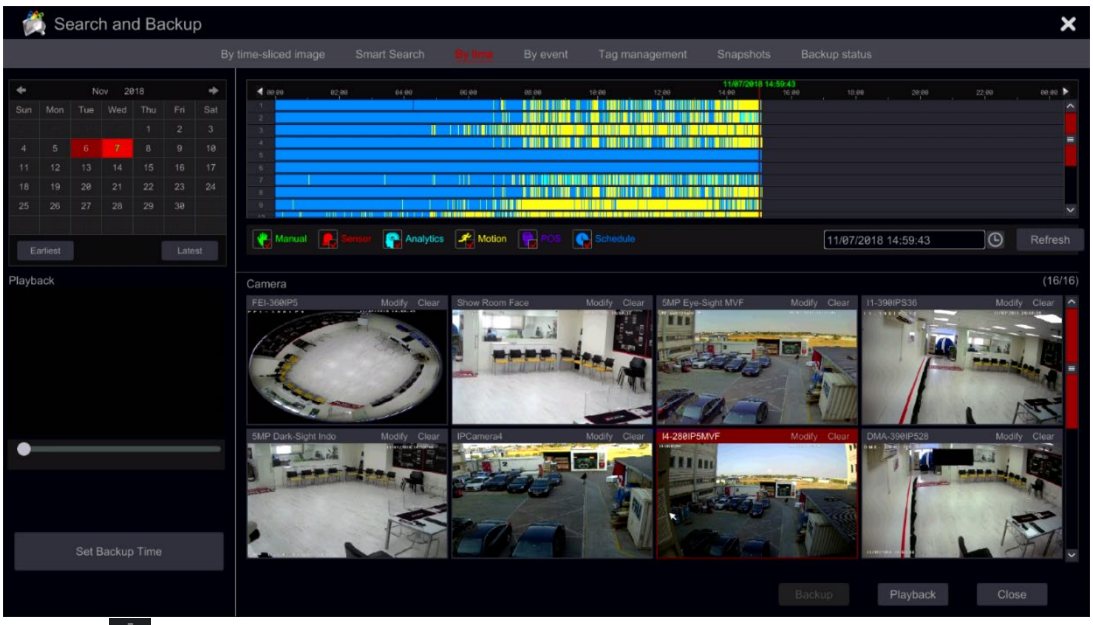
Method One: Click “Year”, “Month” or “Day” button under the record time scale to select the time slice mode. In “Day” mode, click / on the left/right side of the time scale to jump to the next/previous day; click “Minute” in the “Picture” option under the time scale to select “Minute” mode (in “Minute”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

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

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

9.3.2 Search, Playback & Backup by Time:

1. Click Start→Search & Backup→By Time.



2. Click on the bottom of the interface to choose the cameras (A maximum of 16 cameras can be added). Click “Modify” on the top right corner of the camera window to change the camera or click “Clear” to remove the camera.

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

4. Single click on the time bar to set the time for playback. The camera thumbnails will be updated automatically and show a snapshot from the chosen time.

5. You can perform backup directly from this interface. Left click and drag the mouse on the time scale to select the segment for playback and click “Backup” button to continue; select the device, backup path and backup format in the opened window and click “Backup” button to start the backup.

6. You can perform backup directly from this interface in two methods:
   - **a)** Left click and drag the mouse on the time scale to select the segment for playback and click “Backup” button to continue; select the device, backup path and backup format in the opened window and click “Backup” button to start the backup.
   - **b)** After choosing the channel, click on “Set Backup Time” and input the start and end times. Confirm by clicking on “OK” and start the backup process using the “Backup” button.

7. Click “Playback” button (Or double click on the thumbnail) to commence playback in the playback interface (refer to 8.2 Playback Interface Introduction for details). Click “Close” to close the interface.

9.3.3 Search, Backup & Playback by Event

1. Click Start→Search & Backup→By Event.

2. Mark the required event type in the interface (Manual, Sensor, Motion or Analytics).
3. Click to set the start time and end time on the top left of the interface.
4. Mark the desired cameras on the left side of the interface and click to search the database. The searched records will be displayed in the list.
5. Click in the list to playback the record in a popup window. You can also select one record data from the list and click “Backup” button instant backup.
6. Select one record data from the list and click “Playback” button to play the record in the playback interface.

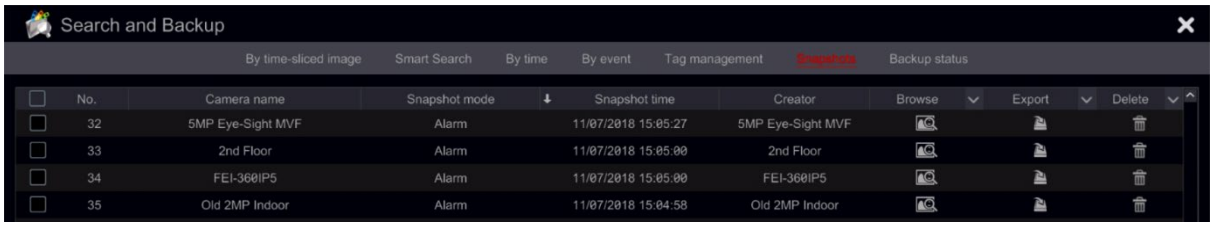
9.3.4 Search & Playback by Tag

You have to save tags prior to using this interface. While playing back click on one of the camera windows to open the camera menu bar and click on .
Click Start→Search & Backup→Tag Management

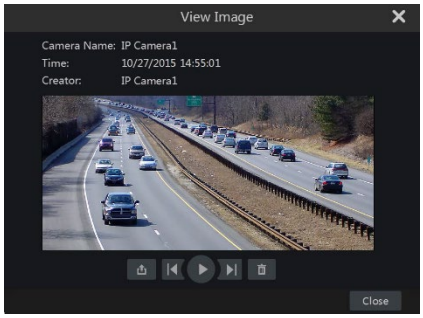
Click in the interface to play the record. Click to edit the tag name. Click to delete the tag.

9.3.5 Snapshots

Click Start→Search & Backup→Snapshots. The system will display all the snapped images.

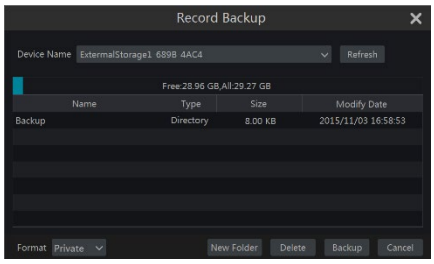


Click to delete an image. Click to open the "Export" window. Select the device name and save path in the window and click "Save" button.
Click to open a view window. Click to export the image. Click to view the previous image or click to view the next image. Click to delete the image; click to play all the images automatically one by one.



9.3.6 Backup Procedures

The recorded data and the snapped pictures can be backed up locally to USB (U-disk or external USB HDD) or by e-SATA (only available in selected models) it can also be backed up through network (only to AVI format). The file system of the backup devices must be FAT32 format or it will not be useable by the system.



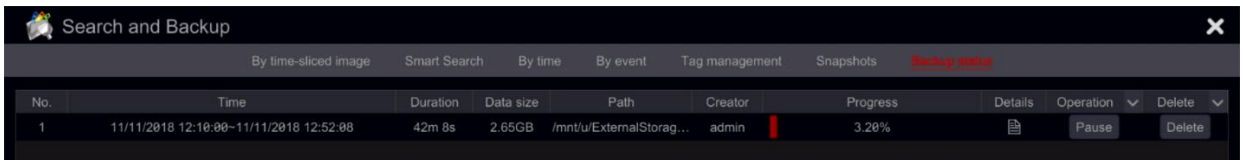
1. Refer to any of the Search & Backup methods and use the applicable backup methods.
2. Once selecting the backup duration, click "Backup" button to open the "Record Backup" window. Select the device name, backup format and path and click "Backup" button to start the backup.

Please note:

There are two backup formats available: AVI is a common video file that can be played by any video player. "Private" format can be played by "RPAS player" only. The RPAS player will be added to on the USB device automatically.

9.3.7 View Backup Status

Click Start→Search & Backup→Backup Status or click on the tool bar at the bottom of the playback interface to view the backup status.
This will show all the active backup procedures. From here you will be able to see the general progress of the backup tasks and pause or delete any of it.



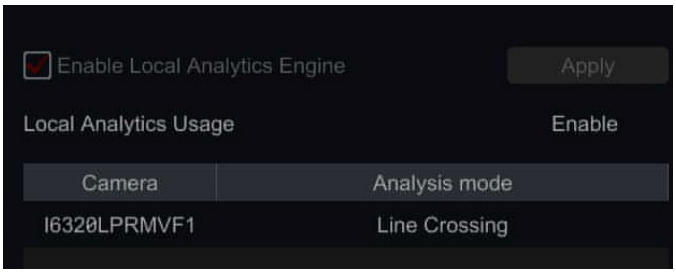
10. Analytics Interface

The main analytics search, playback and backup is “Analytics”. It can be accessed from Start Menu→Analytics:

10.1 Local Analytics Engine (If applicable):

Some NVR models have their own analytics engine. This engine can perform DDA, Face detection and face recognition analytics. This interface allows you to monitor which analytic tasks the NVR is performing.

Click Start→Analytics→Local Analytics Engine. In the example on the right, the NVR is performing a DDA Line Crossing task on an LPR camera that ordinarily doesn’t support this type of analytics



10.2 Analytics Search

10.2.1 Face

If face recognition is enabled by any IPC channel or the NVR analytics engine you can perform this search. Click Start→Analytics→Search and choose “Face” on the left pane.

10.2.1.1 Search Face by Event:

Searching by event is the default option. You can search by all events, Successful recognition or unrecognized events

After the search was performed and results are showing you can perform several actions:

1. Click on an image to view a quick playback on the left preview window.
2. Click on the “…” icon on the top right of the image to open the recognition window. The recognition window allows additional searches and the ability to add the person to the database

10.2.1.2 Search Face by Face:

Searching by face should be used when the desired person is known. In many cases searching by face will start as event search and be refined from there. Click on the “+”. The selection window will open. You can choose face/faces from the following options:

1. Face database – Search from faces already in the database.
    a. Here you can choose from the thumbnails or search by name. Click on “More” to narrow down groups or tick “All” to search/display within all groups.
    b. Tick the face/faces you wish to search for and click on Search by face/group as needed.
2. Snapshot Gallery – Search within snapshots taken by the system
    a. Set the time range for the face snapshot search. (Day to choose a day, Week to choose a week, Month to choose a month, customization to set a unique time range and Today to choose the date of today starting at midnight).
    b. Choose the camera/cameras that took the face snapshot. Click on “More” to choose specific cameras or tick “All” to choose all cameras.

   c. Choose whether you like to see recognized and unrecognized faces in the search.
   d. Tick the face/faces you wish to search for and click on Search by face/group as needed.
3. External Faces – Choose a picture file that contain a single face from a USB storage.
   a. Select the USB storage under the “Device Name”
   b. Select the relevant file (Must contain a single clear face).

Click on Search face.

10.2.2 Human

Human search is related to all DDA analytics. It can be refined to more accurate search by the video metadata DDA2 analytics.

1. Click Start→Analytics→Search and choose “Human”
2. Select the required date or range of dates.
3. Select the required DDA event.
4. If any of the required cameras is also running video metadata DDA2 analytics, you can choose “Object” and select the required attributes from the opened window.
5. Click Search to run the search

10.2.3 Vehicle

Vehicle search is related to all DDA analytics. It can be refined to more accurate search by LPR cameras analytics.

10.2.3.1 Search Vehicle by Event:

1. Click Start→Analytics→Search and choose “Vehicle”
2. Select the required date or range of dates.
3. Select the required DDA event.
4. If any of the required cameras is also running video metadata DDA2 analytics, you can choose “Object” and select the required attributes from the opened window.
5. If any of the required cameras is an LPR camera, you can set the car license plate number on the “Plate” input text box.
6. Click Search to run the search

10.2.3.2 Search Vehicle by Entry/Exit:

If there is a parking lot configured and managed by the NVR, you can also search a vehicle by the entry/exit.

4. Click Start→Analytics→Search and choose “Vehicle”
5. Switch to “By Entry/Exit”
6. Select the required date or range of dates.
7. Select the camera
8. Select entry or exit
9. You can set the car license plate number on the “Plate” input text box.
10. Click Search to run the search

10.2.4 Combine

Combine is a combination search of Face, Human and Vehicle.

11. Event Management

11.1 Event Notification

11.1.1 Alarm-out

Ossia devices will integrate with any device that has alarm output and display it on the alarm out list (together with any integral alarm outputs available on the device itself).

1. Click Start→Settings→Alarm→Alarm Out to access the following interface.
2. Set the delay time and the schedule of each alarm-out.
3. Set the alarm out NO/NC. (Cannot be mixed)
4. Click “Apply” to save the settings. You can click “Test” to test the alarm output.

11.1.2 E-mail

Click Start→Settings→AI/Event→Event Notification→E-mail to go to the e-mail configuration interface.

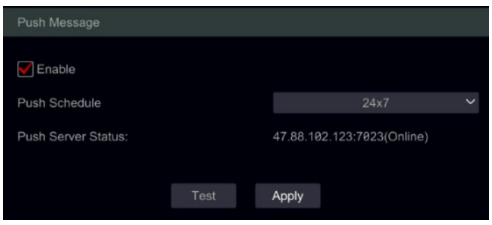
11.1.3 Display

Click Start→Settings→ AI/Event →Event Notification→Display to set the duration of the pop-up video and pop-up message box. Click “Apply” to save the settings.

11.1.4 Buzzer

Click Start→Settings→ AI/Event →Event Notification→Buzzer to set the holding time of the buzzer and click “Apply” to save the setting. You can click “Test” to test the buzzer.

11.1.5 Push Message

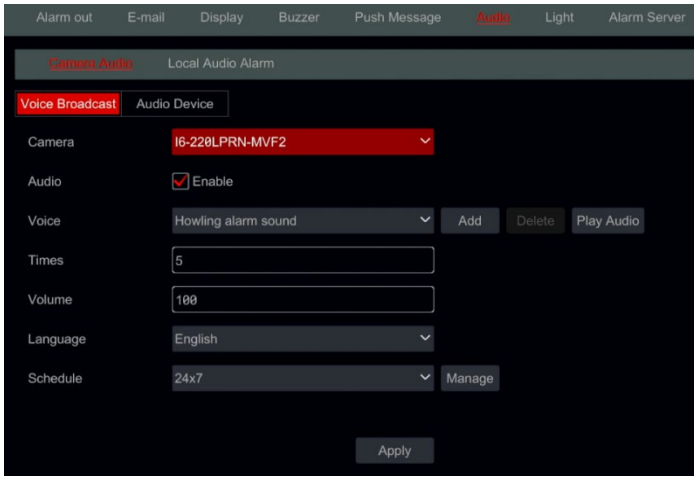


Click Start→Settings→ AI/Event →Event Notification→Push Message. Enable the push message service and wait for the Push server status to change from “Disabled” to xxx.xxx.xxx.xxx:xxxx (Online). The IP Address of the Push server might vary according to your location and the availability of the server. All of the Push notification configuration will be done on your mobile phone through the “Provision Cam2” App. You can also set the “Push Schedule” which will define the days and times that push notifications will be sent by the device to the mobile app.

11.1.6 Audio Message

Click Start→Settings→ AI/Event →Event Notification→Audio.

Audio from IP Cameras → Camera Audio



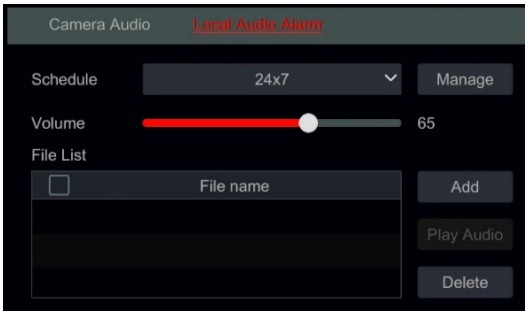
The Camera Audio Audio Divides into 2 sections:

1. Voice Broadcast: For Active Deterrence audio control
2. Audio Device: For audio input/output control

Below, we have the schedule setting for Audio Alerts. No audio alerts will be triggered outside of this schedule.

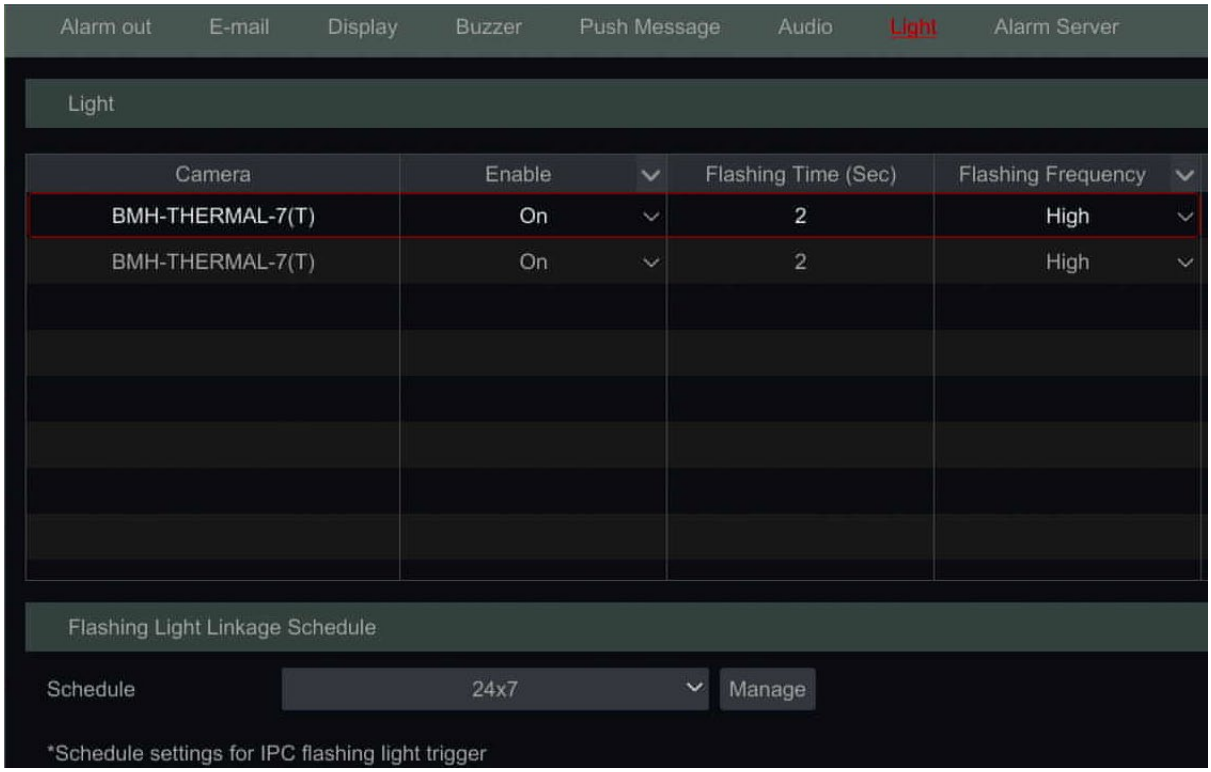
Audio from the NVR → Local Audio Alarm

You can upload wav files to the NVR and trigger it when as a response to events.
Click on “Add” to add a file, Select a file and click “Delete” to delete it.
If needed, you can set the volume of the output.



11.1.7 Light

Click Start→Settings→ AI/Event →Event Notification→Light.



The light section relates to future cameras with built-in strobe light (Smart Sight PA Series, Thermal, Etc.). Here you will be able to set the strobe light features.
Below, we have the schedule setting for Strobe Light Alerts. No strobe light alerts will be triggered outside of this schedule

11.1.8 Alarm Server

Click Start→Settings→ AI/Event →Event Notification→Alarm Server.
The alarm server allows you to send events to a listening server in XML event format.

1. Set the server IP and port
2. Choose if to send a heartbeat and its intervals
3. Set the alarm server event sending schedule. No events will be sent to the server outside this schedule.
4. Set the required events. Only the selected events will be sent to the server.

11.2 Analytics

Click Start→Settings→Analytics→**Desired Analytics** to access the interface.
There are several types of Analytics alarms. You will need to configure the ones that applies to your needs. Select the camera, and choose the type of analytics you wish to set.

Please note:
Some NVR models can perform analytics even if the IPC doesn't support it.
"Enable Detection by NVR" means that the NVR CPU will perform the analytics
"Enable Detection by IPC" means that the IPC will perform the analytics
Refer to the NVR specs to learn which analytics are supported by the NVR and for how many channels

11.2.1 AI Type Selection (Applicable devices only)

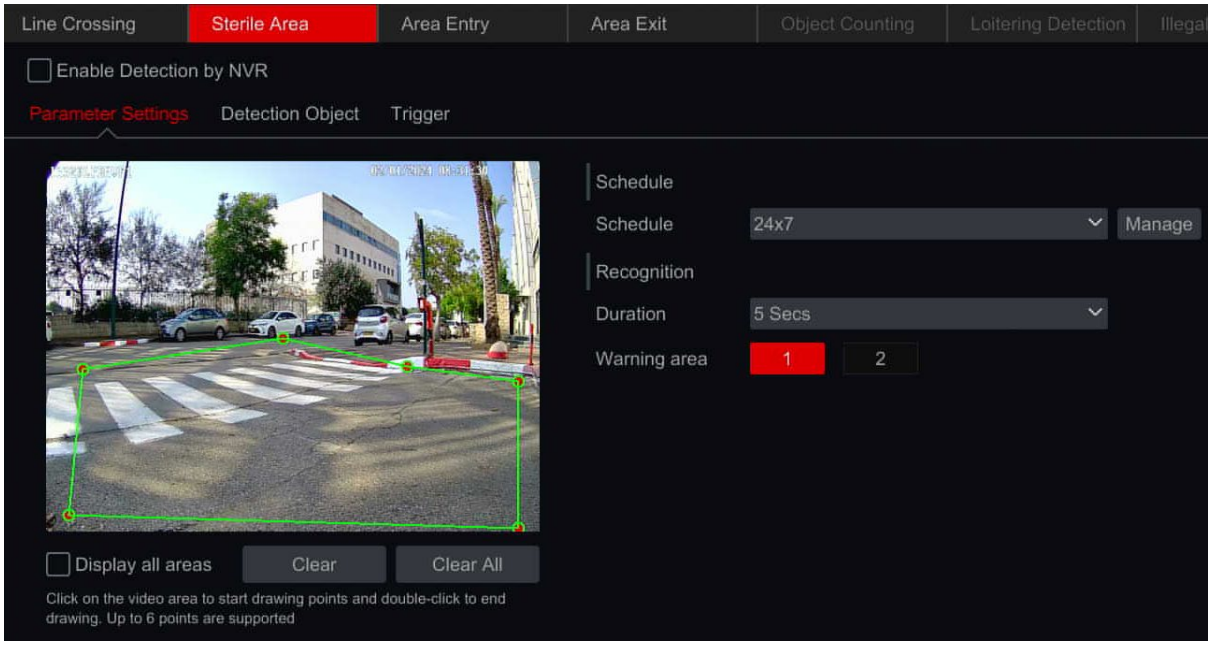
Starting v5.1.2, The Analytics on the IPC are divided to groups: Face Detection, DDA, Metadata. This interface allows you to define which mode the IPC will work in.

11.2.2 Perimeter Monitoring (DDA):

AI Perimeter detection includes 7 types of analytics: We will touch each one below:

11.2.2.1 Sterile Area Configuration

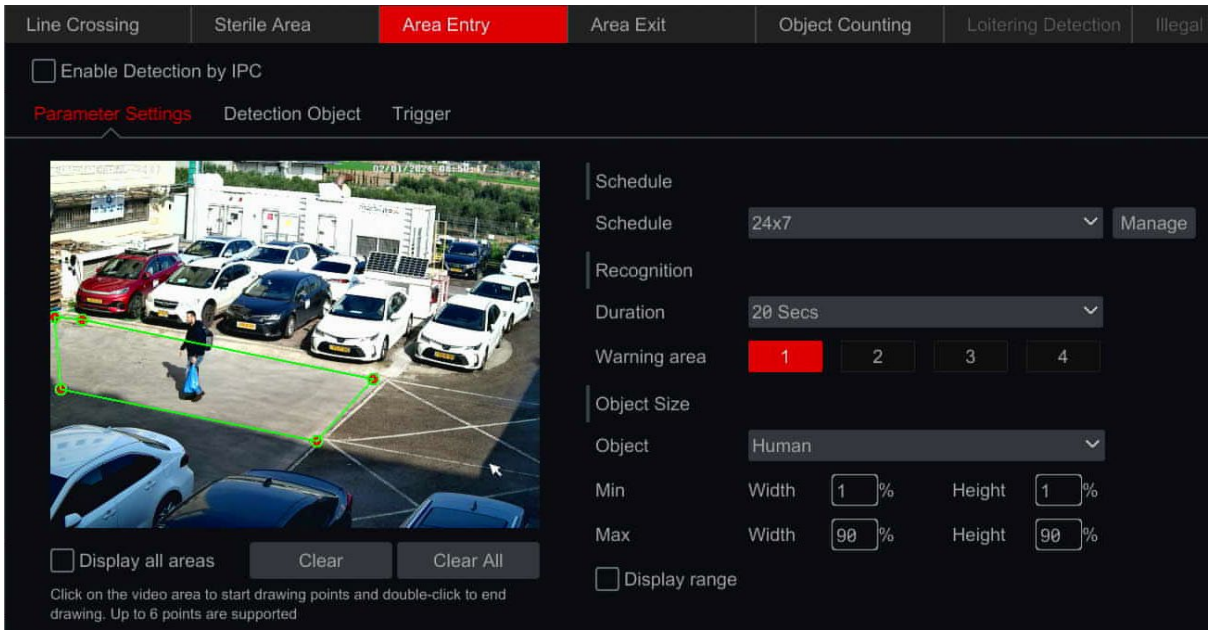
DDA Sterile Area will detect configured objects (Humans / 4 Wheel vehicles / 2 Wheel Vehicles) that move in a specified area.
Click Start→Settings→Events and Analytics→Analytics→Perimeter Monitoring(DDA)
Select the camera from the top (Camera name), then select Sterile Area to access the following interface.



1. Enable/Disable the alarm.
2. Set the Duration for detection (5sec-2mins)
3. Set the alert area (The number of available areas varies between different models).
4. Create an area by clicking and on the image to set the corners of the polygon.
5. Switch to the "Detection Object" and choose which objects should be detected, and its detection sensitivity.
6. Switch to the "Trigger" Interface and set the required triggers.

11.2.2.2 Area Entry/Exit Configuration

DDA Area Entry/Exit will detect configured objects (Humans / 4 Wheel vehicles / 2 Wheel Vehicles) that enter/exit from a specified area.
Click Start→Settings→Events and Analytics→Analytics→Perimeter Monitoring(DDA)
Select the camera from the top (Camera name), then select Area Entry/Exit to access the following interface.



1. Enable/Disable the alarm.
2. Set the Duration for detection (5sec-2mins)
3. Set the alert area (The number of available areas varies between different models).
4. Create an area by clicking and on the image to set the corners of the polygon.
5. Switch to the “Detection Object” and choose which objects should be detected, and its detection sensitivity.
6. Switch to the “Trigger” Interface and set the required triggers.

Please note:
When setting “Area Entry”, the object box of the recognized object must meet the detection area from the outside. Painting the polygon too close to the image edges will result in missed events.

11.2.2.3 Loitering Configuration

DDA Loitering will detect configured Humans that staying in a specified area for a selectable specific time limit (10-3600 seconds).
Click Start→Settings→Events and Analytics→Analytics→Perimeter Monitoring(DDA)
Select the camera from the top (Camera name), then select Loitering Detection to access the interface.

1. Enable/Disable the alarm.
2. Set the Duration for detection (5sec-2mins)
3. Set the alert area (The number of available areas varies between different models).
4. Create an area by clicking and on the image to set the corners of the polygon.
5. Switch to the “Detection Object” and choose which objects should be detected, and its detection sensitivity.
6. Switch to the “Trigger” Interface and set the required triggers.

11.2.2.4 Illegal Parking Configuration

DDA illegal parking will detect configured objects (Humans / 4 Wheel vehicles / 2 Wheel Vehicles) that enter/exit from a specified area.
Click Start→Settings→Events and Analytics→Analytics→Perimeter Monitoring(DDA)
Select the camera from the top (Camera name), then select Loitering Detection to access the interface.

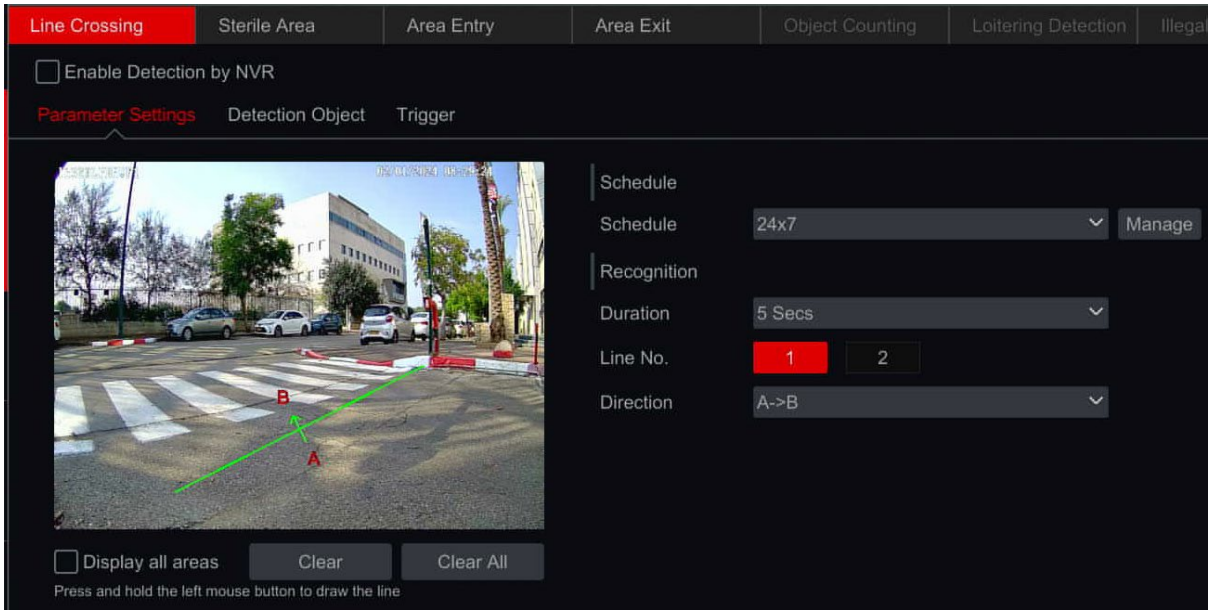
1. Enable/Disable the alarm.
2. Set the Duration for detection (5sec-2mins)
3. Set the alert area (The number of available areas varies between different models).
4. Create an area by clicking and on the image to set the corners of the polygon.
5. Switch to the “Detection Object” and choose which objects should be detected, and its detection sensitivity.
6. Switch to the “Trigger” Interface and set the required triggers.

11.2.3 Line Crossing Configuration

DDA Line crossing will detect configured objects (Humans / 4 Wheel vehicles / 2 Wheel Vehicles) that cross a specified line. Line crossing can work in 3 ways:

1. Left to Right (A→B)
2. Right to Left (B→A)
3. Any side to the other side (A←→B)

Click Start→Settings→Events and Analytics→Analytics→Perimeter Monitoring(DDA)
Select the camera from the top (Camera name), then select Line Crossing to access the following interface.



1. Enable/Disable the alarm.
2. Set the Duration for detection (5sec-2mins)
3. Set the alert line (The number of available lines varies between different models).
4. Create a line by clicking and dragging the mouse cursor on the image.
5. Set the detection direction as specified on the line.
6. Switch to the “Detection Object” and choose which objects should be detected, and its detection sensitivity.
7. Switch to the “Trigger” Interface and set the required triggers for line crossing.

11.2.4 Face Recognition (Applicable devices only)

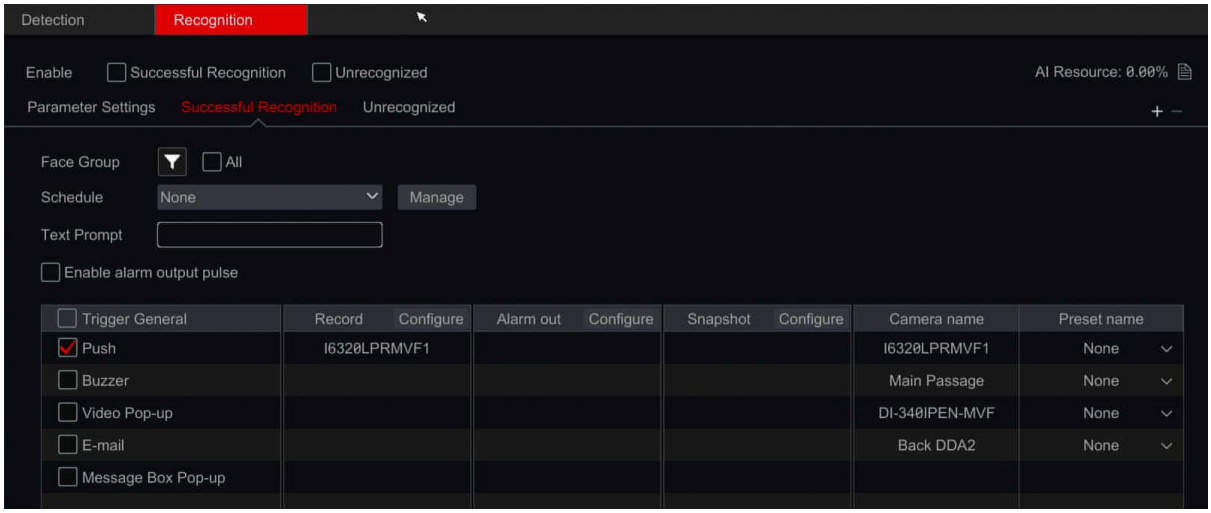
11.2.4.1 Face detection

The system will trigger an alarm upon a **detection** of any face on the detection area. Please note that the alarm is not related to recognition.
Click Start→Settings→Events and Analytics→Analytics→Face Recognition
Select the camera from the top (Camera name), then select Detection to access the interface.

1. Enable/Disable the alarm.
2. Set the Duration for detection (5sec-2mins)
3. Create an area by clicking and on the image to set the corners of the polygon.
4. Switch to the “Trigger” Interface and set the required triggers.

11.2.4.2 Face Recognition

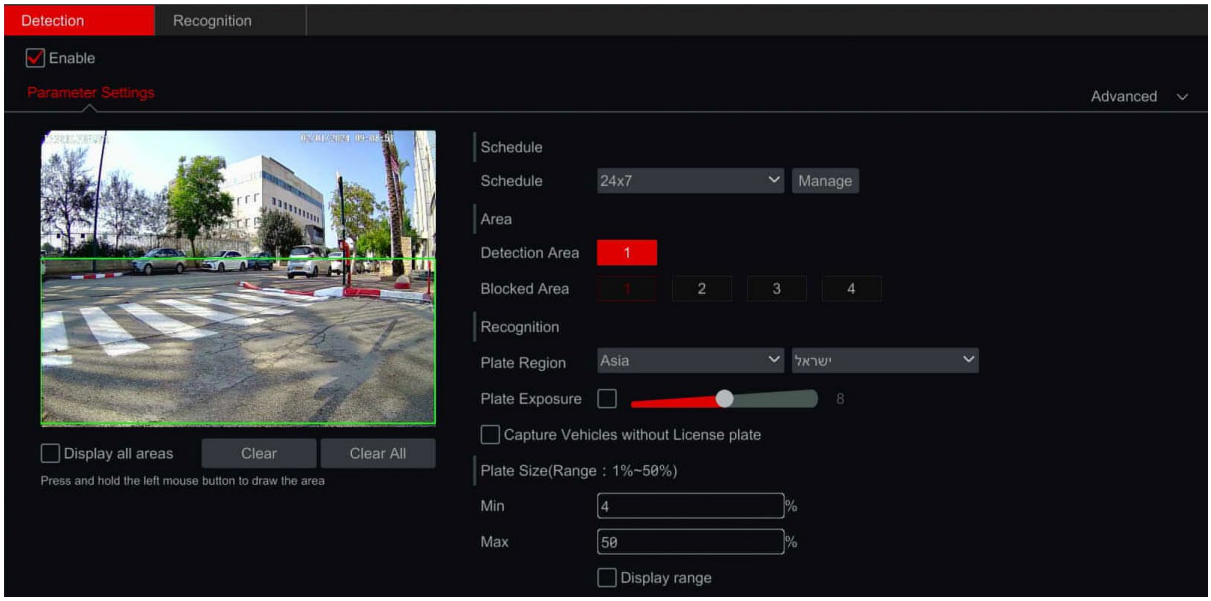
Face recognition cannot work without enabling and properly configuring the face detection. (Without detection there cannot be any recognition). Therefore, the recognition includes triggers only.
Click Start→Settings→Events and Analytics→Analytics→Face Recognition
Select the camera from the top (Camera name), then select Recognition to access the interface.



1. Enable the types of triggers you wish to activate:
   a) Successful recognition: Trigger response to a recognized person (You can set different triggers to differed groups)
   b) Unmatched: triggers for all unsuccessful recognitions
2. For successful recognition, choose the group related to the trigger by clicking on the filter button ( ) or choose all by ticking “All”.
3. Set the schedule for the trigger.
4. For unmatched, there is no group relation. Set the schedule for the trigger.
5. Set the desired system triggers.
6. You can also set a text/voice prompt that will be attached to the recognition.
7. Enabling “Enable alarm output pulse” will trigger 2 alarm outputs within a few seconds (As required by some alarm systems for verification).
8. You can add/remove triggers groups based on different groups by clicking on the + − icons

11.2.5 LPR (License Plate Recognition – For LPR Cameras only)

Detection: LPR detects vehicles in the frame, reads its license plate and recognizes it. It can trigger based on successful/unsuccessful detections.
Click Start→Settings→Events and Analytics→Analytics→LPR
Select the camera from the top (Camera name), then select LPR to access the interface.



1. Enable/Disable the alarm.
2. Set the detection schedule
3. Create an area by clicking and on the image and dragging to create a rectangle.
4. Set a Blocked area if needed. License plates will not be searched in a blocked area.
5. Set the license plate region and country
6. Set the Plate size range. License plates sizes outside limit range will be ignored.
7. Switch to the Recognition tab to continue the setting

Recognition: LPR recognition cannot work without enabling and properly configuring the LPR detection. (Without detection there cannot be any recognition). Therefore, the recognition includes triggers only.

1. Enable the types of triggers you wish to activate:
   a) Successful recognition: Trigger response to a recognized license plate group (You can set different triggers to differed groups)
   b) Unrecognized Plate: triggers for all recognitions not found in the database
2. For successful recognition, choose the group related to the trigger by clicking on the filter button ( ) or choose all by ticking “All”.
3. Set the schedule for the trigger.
4. For Unrecognized, there is no group relation.
5. Set the schedule for the trigger.
6. You can also set a text/voice prompt that will be attached to the recognition.

11.2.6 Video Metadata (Applicable devices only)

Video Metadata is mainly used for post event search. It will recognize additional details from detected objects. Note that Metadata does not create any system triggers.
Click Start→Settings→Events and Analytics→Analytics→Video Metadata
Select the camera from the top (Camera name), then select Video Metadata to access the interface.

1. Enable/Disable the alarm.
2. Set the detection schedule
3. Create an area by clicking and on the image to set the corners of the polygon.

4. Set a Blocked area if needed. Objects will not be detected in a blocked area.
5. Switch to the “Detection Object” and choose which objects should be detected, and its detection sensitivity.
6. Switch to the “Image Overlay” and choose which attributes will be included for each object.

11.2.7 Thermal (Applicable devices only)

11.2.7.1 Fire Detection

Fire detection will detect fire on the whole scene.
Click Start→Settings→Events and Analytics→Analytics→Thermal
Select the camera from the top (Camera name), then select Fire Detection to access the interface.

1. Enable/Disable the alarm.
2. Switch to the “Trigger” Interface and set the required triggers.

11.2.7.2 Temperature Detection

Temperature detection will detect object temperatures based on line, point or area and trigger an event once a rule was breached.
Click Start→Settings→Events and Analytics→Analytics→Thermal
Select the camera from the top (Camera name), then select Temperature Detection to access the interface.

1. Enable/Disable the alarm.
2. Set each required rule. The setting should include:
3. Enabling/Disabling the rule
4. Setting a rule name.
5. Set the rule Type (Point/Line/Area)
6. Marking the Point/Line/Area on the video preview window.
7. Setting the emissivity, distance and reflected temperature of the object
8. Setting the alarm rule
9. Setting the alarm temperature.
10. Click Apply and switch to the “Trigger” Interface and set the required triggers.

11.2.8 Others:

“Others” include all the rest of the analytics including all the old “Pixel Based” Analytics

11.2.8.1 Item Monitoring Configuration

Object monitoring will check that no items were left behind in a specified area (Left Object) or check that a monitored item was not taken (Missing Object). It is based on “Pixel Change”
Click Start→Settings→Events and Analytics→Others→Item monitoring (Must be supported by the IP Camera) to access the following interface.

1. Enable/Disable the alarm.
2. Set the Duration for detection (5sec-2mins)
3. Choose the type of detection:
   a) Missing object will monitor a specific object to prevent it from being taken.
   b) Left object will monitor an area to prevent from items to be left over.

4. Set the warning area. Up to 4 areas can be configured.
5. On the left side of the interface tick “Draw warning area” and create a polygon by clicking on the corners of the area you wish to mark. If you chose “missing object” then the polygon should be marked around a specific object. If you chose “left object” then the polygon should be marked around the monitored area.
6. Set the area’s name.
7. If you need to set additional areas, switch to area 2-4 and repeat stages 3-8

11.2.8.2 Camera Tampering Configuration

Camera tampering will check that the camera hasn’t been tampered in a way that will prevent it from providing a decent video image. Camera tampering monitors:

1) Camera Shifting: In case the camera was shifted and it does not point at the area that was set during the installation.
2) Lens Tampering: In case the Zoom/Focus of the lens was tampered and the image became blurry.
3) Camera Masking: In case that the camera was covered or blocked by a foreign object that blocks the majority of its view.

Click Start→Settings→ Events and Analytics→Others→Camera Tampering (Must be supported by the IP Camera) to access the following interface.

1. Select the camera.
2. Enable/Disable the alarm.
3. Set the Duration for detection (5sec-2mins)
4. Set the sensitivity.
5. Switch to the “Trigger” Interface and set the required triggers.

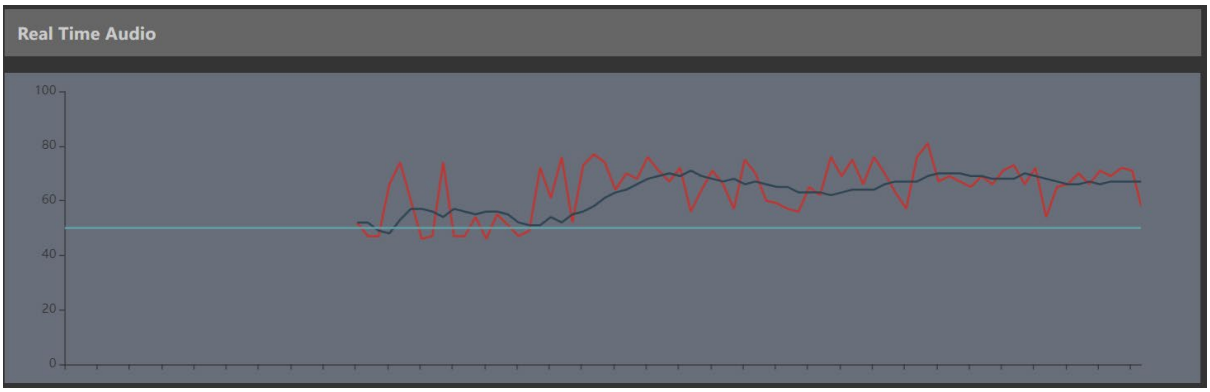
11.2.8.3 Audio Exception Configuration

Audio Exception notices unusual audial behavior such as sudden increase or drop of baseline audio.

Click Start→Settings→ Events and Analytics→Others→Audio Exception (Must be supported by the IP Camera) to access the following interface.

1. Select the camera.
2. Enable/Disable the alarm.
3. Set the schedule.
4. Set the recognition duration (How long should the audio exception take before the trigger of event)

5. Enable the required detection: Sudden increase of sound or Sudden deacrese of sound. Use the realtime audio bar to set the audio threshold.



6. Set the sensitivity.
7. Switch to the "Trigger" Interface and set the required triggers.

Please note:
Audio must be enabled on the IPC for this feature to work.

11.2.8.4 Object Counting by Line/Area

Object counting Analytics will count the number of objects that crossed a defined line. Once the number of object passed the defined treshold, an alert will be triggered.

1. Click Start→Settings→ Events and Analytics→Others→ "Object Counting / by Area"
2. Enable the Alarm if required.
3. Under the "Rule Settings" set the schedule and duration between alarms.
4. Set time treshold between counter violation and alarm triggering.
5. Set the Line counter direction if needed
6. Set the alerting objects, detection sensitivity (Objects not marked will be ignored) and counter treshold for each object.
7. For advances settings, click on the "Advanced" button.
   - Set whether to save the scene image (Image) or the object image to the IP camera SD card.
   - Set if to send email report on a daily/weekly/monthly basis.
   - Set the counter reset rule. It is advised to reset the counter at least once a day. You can also reset the counter manually.
8. Switch to the OSD Overlay and set the Image overlay as required.
9. Set the triggers and click "Save" to confirm

11.2.8.5 Heatmap

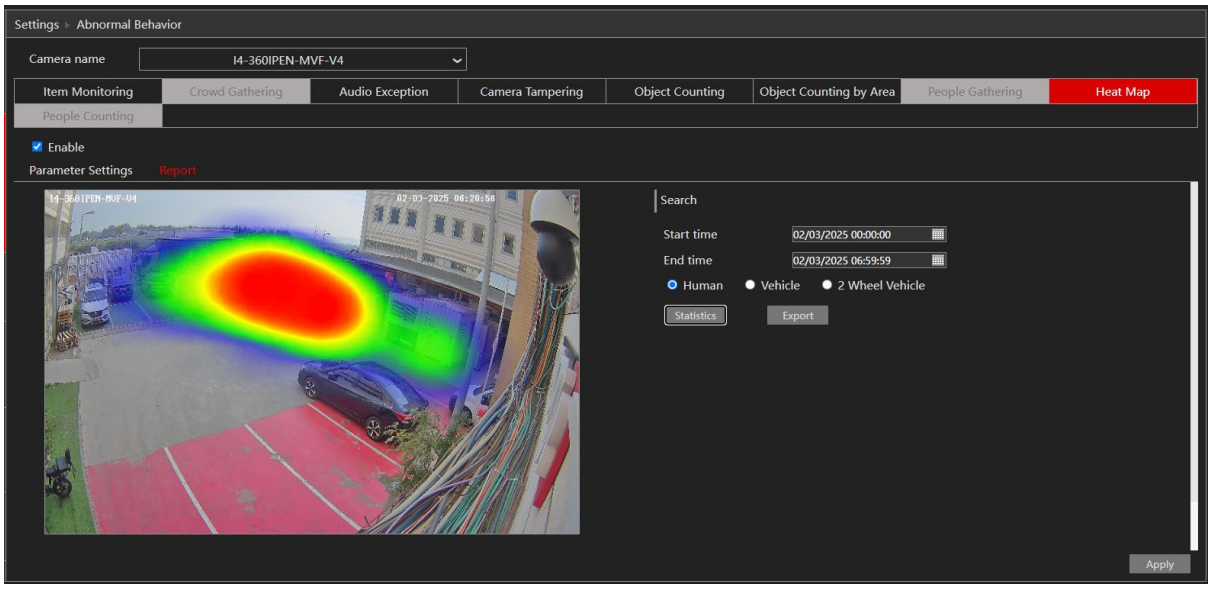
Heat map analytics gathers movement information of defined objects and shows it visually when required. It can be used for statistics and better understanding the flow and paths of movement. It doesn't generate any triggers.

1. Click Start→Settings→ Events and Analytics→Others→ "Heatmap"
2. Enable the detection if required.

3. Set the schedule.
4. Set the area for detection
5. Set the objects for tracking, detection sensitivity (Objects not marked will be ignored) and counter treshold for each object.

Viewing the report is only possible through the web interface.

1. Login to the NVR and browse to Settings→Analytics→Others→Heatmap→Report
2. Set the report duration and required object and click on “Statistics”
3. Export if needed. The file will be downloaded to your computer.



11.3 Databases

In This section you will be able to create, edit and manage your face database. By default, the databases are completely empty. You should create groups before you can add new objects to the databases (Faces or LPR)

You can create new groups by clicking on “Add Group”. You can configure “Permitted” time for members of customized groups.

Click on to edit a group name and on to delete a group (The default groups cannot be deleted).

Click on to open a group.

11.3.1 Face Database

11.3.1.1 Adding a new person to the database:

Click on “Add” to add a new person. If there are no groups configured, the system will ask for a new group name and set a group, then you will have to click “Add” again.

1. Input the data and click on “Select Face”.
2. Choose the source of the face snapshot. Snapshot Gallery – Search within snapshots taken by the system or External Faces – Choose a picture file that contain a single face from a USB storage.
3. If you chose “Snapshot Gallery”:
   A. Set the time range for the face snapshot search. (Day to choose a day, Week to choose a week, Month to choose a month, customization to set a unique time

range and “Today” to choose the date of today starting at midnight).

B. Choose the camera/cameras that took the face snapshot. Click on “More” to choose specific cameras or tick “All” to choose all cameras.
C. Click on “Search”
D. Choose the face you wish to input to the database. Click on “OK”
E. Fill the rest of the details in the form. (Only the name is mandatory. All the other fields are optional)

4. If you choose “External Faces:
   A. A. Choose a picture file that contain a single face from a USB storage.
   B. Select the USB storage under the “Device Name”
   C. Select the relevant file (Must contain a single clear face).
   D. Click on Select face.

Please note:

For good recognition results, the face must be well lit, looking straight to the camera with as many visible face features

11.3.1.2 Modifying a person in the database:

1. Click on to open a group.
2. Select a person and click on “Modify”
3. The person’s card will open. You will be able to edit any of the details and change the assigned group of the person.

11.3.1.3 Deleting a person from the database:

1. Click on to open a group.
2. Select a person and click on “Delete”
3. The system will prompt for deletion.
4. Clicking on “Clear All” will delete all the people in the specified group.

11.3.2 LPR Database

11.3.2.1 Adding a new Licesne Plate to the database:

1. Click on “Add” to add a new person. The following interface will open.
2. Fill all the data and click on “Ok”.

11.3.2.2 Modifying a License Plate in the database:

1. Click on to open a group.
2. Select a plate and click on “Modify”
3. The LPR card will open. You will be able to edit any of the details and change the assigned group of the plate.

11.3.2.3 Deleting a License Plate from the database:

1. Click on to open a group.
2. Select a plate and click on “Delete”
3. The system will prompt for deletion.

Clicking on “Clear All” will delete all the plates in the specified group.

11.3.3 Exporting databases:

1. Click on Export and Import to open the following interface.
2. Click on “Export” to export the database. Set the database name and target location.
3. Set a password
4. The database will be encrypted and exported to the target location.

11.3.4 Importing databases:

1. Click on Export and Import to open the following interface.
2. Choose the database file and click on “Import”
3. Inpit the database password to initialize the import procedure
4. The database will be created on the device. The device will reboot automatically at the end of this procedure.

Please note:

The Face database is stored on the HDD. The LPR database is stored on the flash memory. Formatting the HDD will delete the database as well. Importing a database will automatically overwrite the existing database.

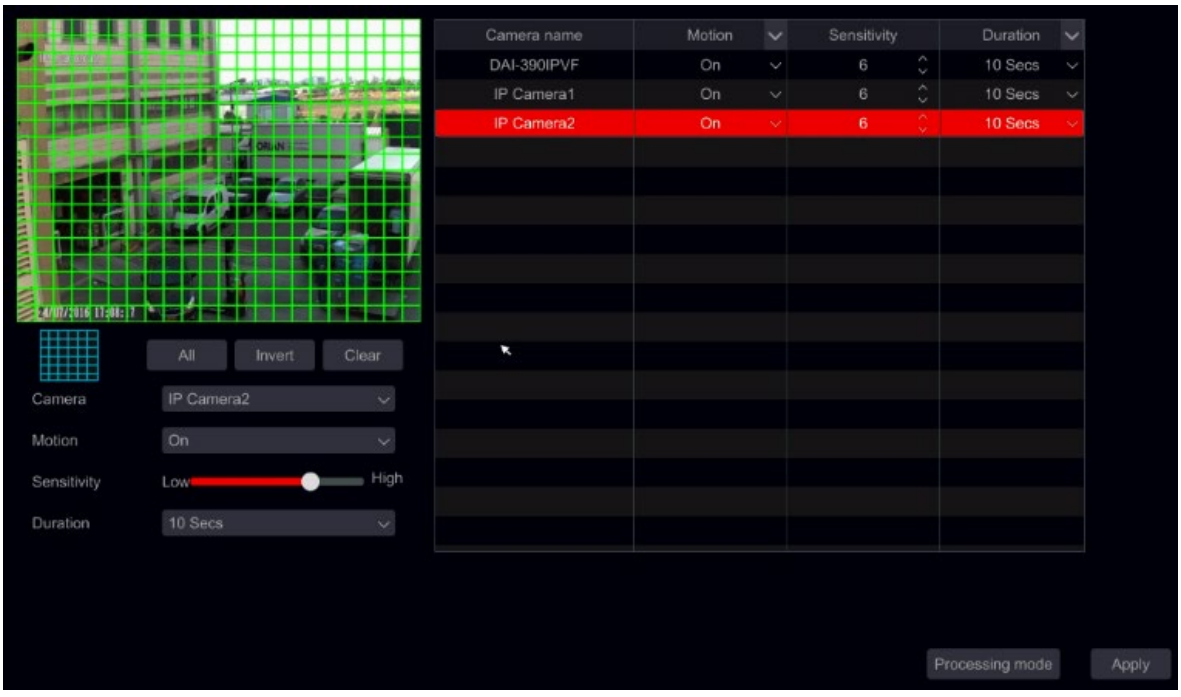
11.4 General Event Alarms

11.4.1 Motion Alarm

When motion appears in the specified area, it will trigger the motion alarm. Remember that the motion alarm is based on VMD which translates pixel color changes as motion, therefore might trigger false alarms.
You should enable and configure the motion detection for each of the cameras first and set the alarm handling to complete the motion alarm configuration.

11.4.2 Motion Configuration

Click Start→Settings→Camera→Motion→Motion Settings to access the following interface.



1. Select the camera, enable the motion and set the sensitivity and duration of the alarm.
2. Sensitivity: the higher the value is, the more sensitive it is to motion. You should adjust the value according to the practical conditions since the sensitivity is influenced by color and time (day or night).
3. Duration: it refers to the interval time between two motion detections. For instance, if the duration time is set to 10 seconds, once the system detects a motion, it will trigger the alarm and disregard all other motions for 10 seconds (specific to camera). If there is another motion detected during this period, it will be considered as continuous movement, otherwise it will be considered as a single motion.
4. To select the area of interest, click and drag the mouse cursor on camera image from the top left to the bottom right. You can set more than one motion area. Click “All” to set the whole camera image as the motion detection area. Click “Reverse” to swap the selected area and the unselected area. Click “Clear” to clear all the motion areas. To delete a specified area click and drag the mouse cursor on the camera image from the bottom right to the top left.
5. Click “Apply” to save the settings. Click “Processing Mode” to go to the alarm handling configuration interface of the motion alarm.

11.4.3 Motion Alarm Triggers Configuration

1. Click Start→Settings→Events and Analytics→General Alarm→Motion Alarm to access the interface.
2. Set the required triggers
3. Click “Apply” to save the settings. You can click “Motion Settings” to return to the motion configuration interface.

11.4.4 Sensor

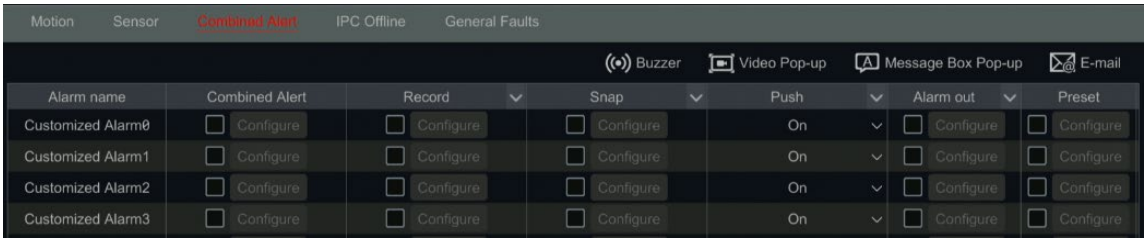
To fully configure the sensor alarm settings, you should enable the sensor alarm and set up the alarm handling for each camera/channel.
Click Start→Settings→ Events and Analytics →General Event → Sensor Alarm to access the following interface.

1. Select the alarm type (NO or NC) according to trigger type of the sensor.
2. Enable the sensor alarm for the desired cameras/channels.
3. Mark the and configure the desired response for sensor alarm out of “Record”, “Snap”,,” Push Notification”, “Alarm-out” and “Preset”, and enable/disable “Buzzer”, “Pop-up Video”, “Pop-up Message Box” and “E-mail”.
4. Click “Apply” to save the settings.

11.4.5 Combined Alert

Combined alert allows you to trigger an alarm only when a combination of 2 different alerts takes place.

Click Start→Settings→→ Events and Analytics →General Event → Combined Alert to access the following interface (Originally containing 16 customized combinations)



1. Click on “Configure” for the desired line. The following interface will open.
2. Here you can set a combination of 2 out of 5: Motion, Sensor, Face Recognition, Sterile Area, and Line Crossing. After choosing the combination you desire, set the cameras that originate the original single alarm.
   You need to make sure the the analytic is active on the selected camera.
3. Set a firendly name for you to identify this combination by clicking on the alarm name editing it.
4. Set the combined alarm triggers.

11.4.6 IPC Offline Settings

Click Start→Settings→→ Events and Analytics →General Event → IPC Offline Settings to open the interface.
Mark the and configure the desired triggers

11.4.7 General Fault Settings

The system monitors its general health and the general condition of the HDD and network connection. The available alarms in this sector are: IP address conflict, Disk I/O error, Disk full, No disk, Illegal access, Network disconnected, HDD removed. (Fault list can vary according to your device model and features).
Click Start→Settings→ Events and Analytics →General Event → General Faults Settings
Mark the and configure the desired trigger for each fault and click “Apply” to save the settings.

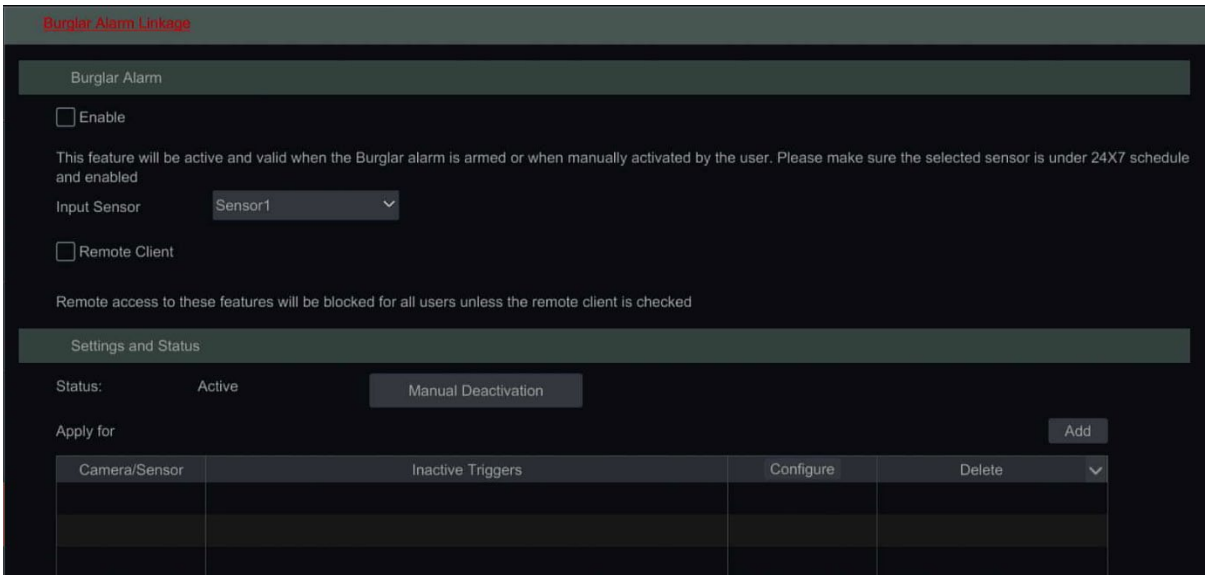
11.5 Manual Alarm

Click on the general tool bar at the bottom of the live-view interface to open the window as shown below. Click “Trigger” to start alarm. Click “Clear” to stop alarm. (The device must support alarms or have IPC which support alarm out connected to it in order to support this feature). If you wish for the alarm to be cleared automatically, set the delay timer according to your needs. “Manual” settings mean that the alarm will stay active until you will clear it.

11.6 Burglar Alarm Linkage

The system can change it behavior and triggers based on the status of your burglar alarm. You can also control it manually through the local/remote interfaces and through the mobile app (Remote Client authorization must be granted).

Click Start→Settings→ Events and Analytics →Burglar Alarm Linkage to open the following interface:



1. Enable/Disable the feature as required.
2. Set the sensor connected to the Burglar Alarm System. This sensor schedule must be set to 24x7.
3. If you with to allow control or override the burglar alarm status remotely, you should enable the “Remote Client”. If disabled, you cannot control this feature remotely.
4. You can see the status of the burglar alarm. “Active” means that the burglar alarm is armed. “Inactive” means that the burglar alarm is disarmed.
5. You can manually activate or deactivate it as require (Will override the burglar alarm true status).
6. Click on “Add” to add a channel/sensor to deactivate while the burglar alarm is disarmed.
7. Click on “Configure” to exclude triggers from the selected channel/sensor. The default value is “All” which means that all triggers will not be active while the burglar alarm is disarmed.

Please note:

Configuring the “Burglar Alarm Linkage” wrongly will result in system lack of triggers and might cause the system not to record events. Please use with caution.

11.7 Alert Status

Click Start→Settings→ Events and Analytics →General Event → Alarm Status or click on the general tool bar at the bottom of the live-view interface and click “Alarm Status”. Click “Clear” button to stop the buzzer if the buzzer is on. Click to view detailed information as shown below.

If the exception information is more than one page, you can input the number in the box and click to jump to the specified page. Click / to view the exception alarm information in the previous/next pages. Click to play the alarm record (if available).

11.8 Triggers:

11.8.1 Record:

When enabling “record” a “Trigger Record” window will pop up (you can also click “Configure” button to open the window manually). Select camera/s on the left side and click to set the camera as a triggered camera. Select a triggered camera from the right side and click to remove the triggered camera. Click “OK” button to save the settings. The triggered camera/s will commence recording in case of alarm.

11.8.2 Snap:

When enabling “Snap” a “Trigger Snapshot” window will pop up (you can also click “Configure” button to open the window manually). Select camera/s on the left side and click to set the camera as a triggered camera. Select a triggered camera from the right side and click to remove the triggered camera. Click “OK” button to save the settings. The triggered camera/s will take a snapshot in case of a sensor alarm.

11.8.3 Push:

Send a push notification to the relevant Provision Cam2 Mobile app (Needs to be configured on the mobile app)

11.8.4 Alarm-out:

When enabling “Alarm-Out” a “Trigger alarm-out” window will pop up (you can also click “Configure” button to open the window manually). Select alarm/s on the left side and click to set the alarm as a triggered alarm. Select a triggered alarm from the right side and click to remove the triggered alarm. Click “OK” button to save the settings. The triggered alarm will commence in case of a sensor alarm. You need to set the delay time and the schedule of the alarm outputs.

11.8.5 Preset:

Once enabling “Preset” a “Trigger Preset” window will pop up (Requires a PTZ camera with configured presets).

11.8.6 IP Speaker:

Set the Audio file to be played (Must be configured through the Audio Interface beforehand)

11.8.7 Buzzer:

If enabled, the system will buzz using the internal buzzer when alarm is triggered.

11.8.8 Pop-up Video:

Once enabling “Pop-up Video” a “Set Camera” window will pop up. Select a camera from the list as the triggered channel. Click “OK” button to save the settings. The triggered camera will open in a single channel live-view in case of sensor alarm

11.8.9 Pop-up Message Box:

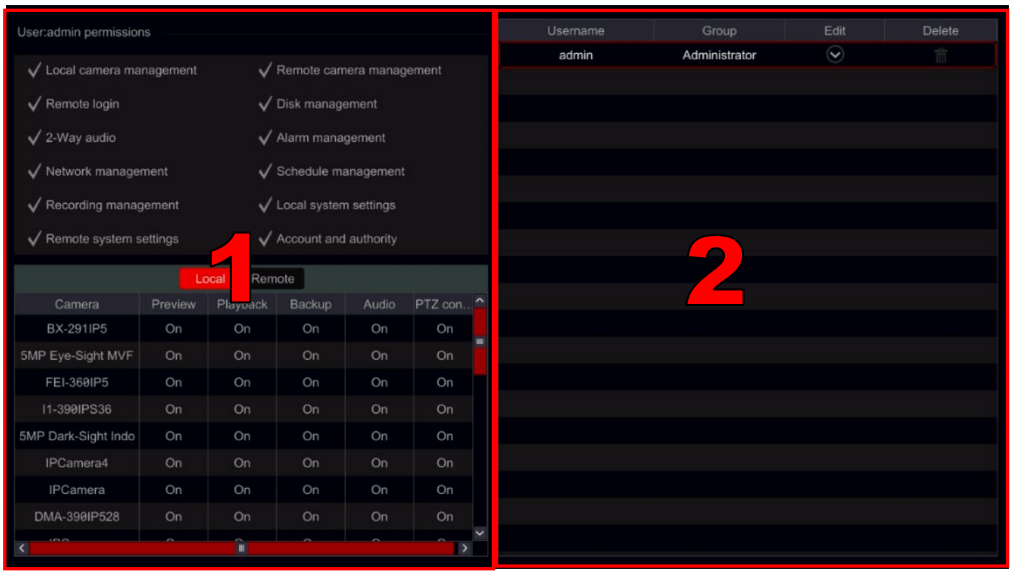
If enabled, the system will pop up the corresponding alarm message box automatically when alarm is triggered.

11.8.10 E-mail:

If enabled, the system will send an e-mail when alarm is triggered. Before you enable the email, please configure the e-mail addresses first.

12. Account & Permission Management

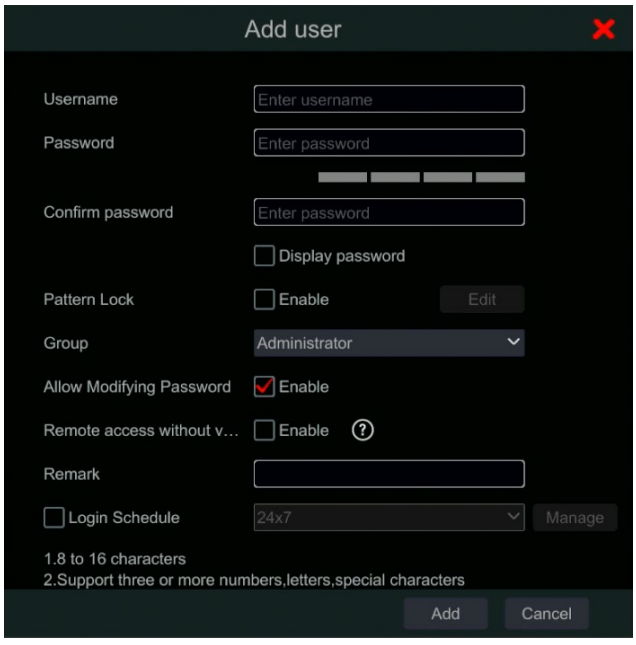
12.1 Account Management



Click Start→Settings→Account and Permissions→Account
Area 1 displays the user permissions. Area 2 displays the user list. Click on a user in area 2 to display its user permissions in area 1.
There are three default permission groups ("Administrator", "Advanced" and "Common") available when adding accounts. You can manually add new permission group.
The user ***admin*** has all system permissions and it can manage the device's accounts. Group "Administrator" owns all the permissions displayed in area 1 and its permissions can never be changed or edited while the permissions of "Advanced" and "Common" can be changed.

12.1.1 Add User

1. Click Start → Settings → Account and Permissions → Account → Add User or click + beside the search box.



2. Set the username, password and permission group. Try to choose a complicated password that will be hard to guess. It is optional to set pattern lock. You can also set if the user is allowed to change his password.
3. You can set 1 user that can bypass the “Security Access” mechanism by marking the “Remote access without verification code”
4. Set the login schedule. The user will not be permitted to login outside the selected schedule.
5. Click “Add” to confirm and add the user.

12.1.2 Edit User

Click Start→Settings→Account and Permissions →Account→Edit User. Click in the user list or double click the user to edit its information. Click to delete the user (the user ***admin*** cannot be deleted). If ***admin*** is edited, its permission control is closed and permission group cannot be changed. You can enable or disable other users (if disabled, the user will be invalid), open or close their permission control (if closed, the user will get all the permissions which the administrator permission group has) and set their permission groups. Click “OK” to save the settings.

12.1.2.1 Modify Password

Only the password of ***admin*** can be modified. Click “Modify Password”. Input the current password and set new password. Click “OK” to save the settings.

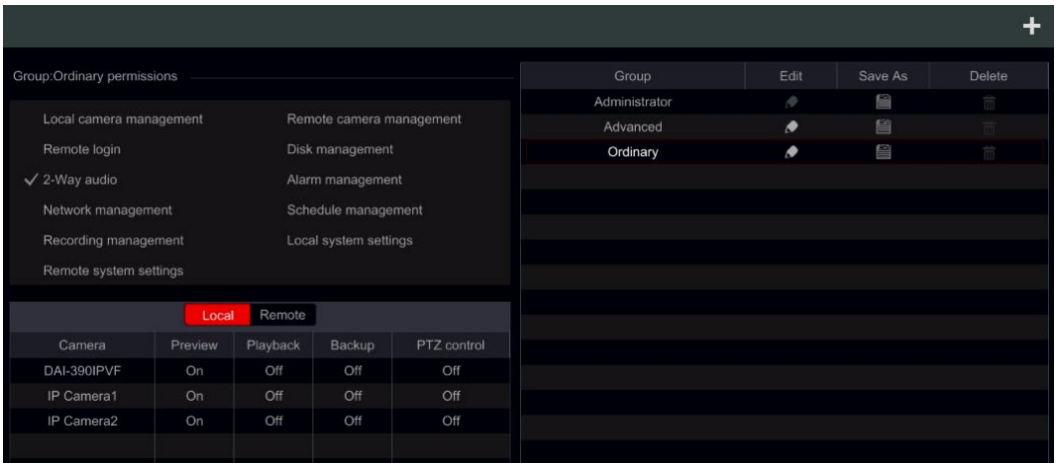
12.1.2.2 Edit User

Click “Edit User” to open the window as shown below.

12.2 Permission Management

12.2.1 Add Permission Group

Click Start→Settings→Account and Permissions →Account→Edit Permission Group to open the interface as shown below.



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

12.2.2 Edit Permission Group

Go to “Edit Permission Group” interface and click in the group list to edit the permission group. Click to save the group as another group. Click to delete the permission group. The three default permission groups (“Administrator”, “Advanced” and “Common”) cannot be deleted.

12.3 User Login & Logout

Login: Click Start→Login or directly click the live-view interface, then input the username and the password. Click “Login” button to log in the system. If “Auto Login” is marked – the system will not ask for password again until logout.
Logout: Click Start→Logout or click Start→Shutdown. Select “Logout” in the window and click “OK” button to log out the system.

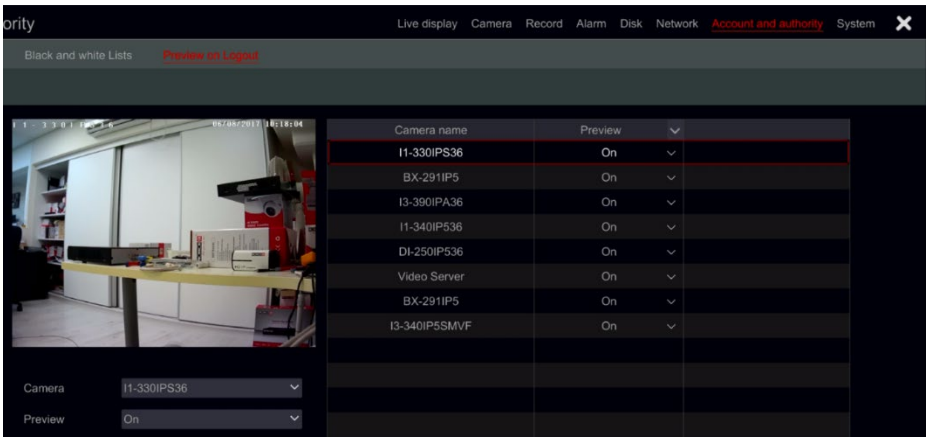
12.4 Security

12.4.1 Block and Allow Lists

Click Start→Settings→Account and Permissions →Security→Block and Allow List
Check “Enable” if required and and choose the relevant usage. Note that allow list and block list cannot work simultaneously.
Allow List: Only IP/MAC on the list can log into the device.
Block List: Any IP/MAC on the list cannot log into the device.
Add IP/IP segment/MAC. Click “Add IP” or “Add MAC” button and check “Enable” in the popup window (only if you check it can the IP/IP segment/MAC you add be effective). Enter the IP/IP segment/MAC and click “OK” button. In the above interface, click to edit IP/IP segment/MAC, click to delete it. Click “Apply” to save the settings.

12.4.2 Preview on Logout

Preview on logout configuration will set which channels will be available for view while no user is logged into the system only channels marked as “on” will be available. The default setting is “on” for all channels. To configure:
Click Start→Settings→Account and Permissions →Security→Preview on Logout to go to the following interface.



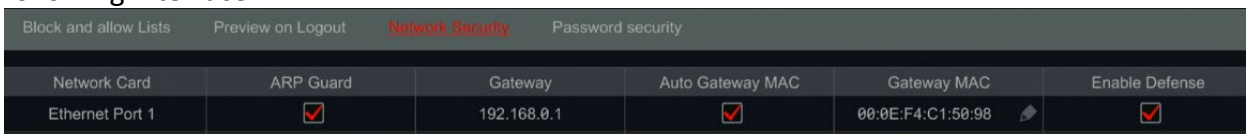
Choose which channels can be viewed and which are not when all local users are logged out.

12.5 Network Security

The network security feature adds a layer of security against MiTM cyber attacks (Man in the middle) which means that the hacker can see any data being sent and received by the NVR. The most common method of applying MiTM attack is by impersonating the hacker computer to the router by changing the NVR/Router ARP Tables which stores all the LAN IPs and their corresponding MAC Addresses. The IP will not change, but the MAC address will change. After the ARP poisoning was done, the NVR will send data to the hacker instead of to the Router.

The Network Security feature protects the NVR by securing its ARP value for the router.

Click Start→Settings→Account and Permissions →Security→Network Security to go to the following interface.



1. Click on “ARP Guard” to activate it
2. The gateway is set automatically by the Network IPv4 setting.
3. There are 2 options to set the router’s MAC address: Automatically and Manually.
   a) Automatically: If you are sure that no MiTM attack is taking place, you can use the “Auto Gateway MAC” option. The NVR will copy the MAC address from its ARP table to the interface.
   b) Manually: You can check and confirm the MAC address of the router by yourself and then input it to the interface by clicking on the icon under “Gateway MAC”
4. Click on “Enable Defence” and “Apply” to finish the process.

Please note:

After enabling network security, the NVR will only communicate through the provided MAC address, meaning that any change of the network/router will require updating this setting.

12.6 Password Security

Password security can force the user to change the password after given time and also can force the user to choose a password with defined strength

Click Start→Settings→Account and Permissions →Security→Password Security interface.

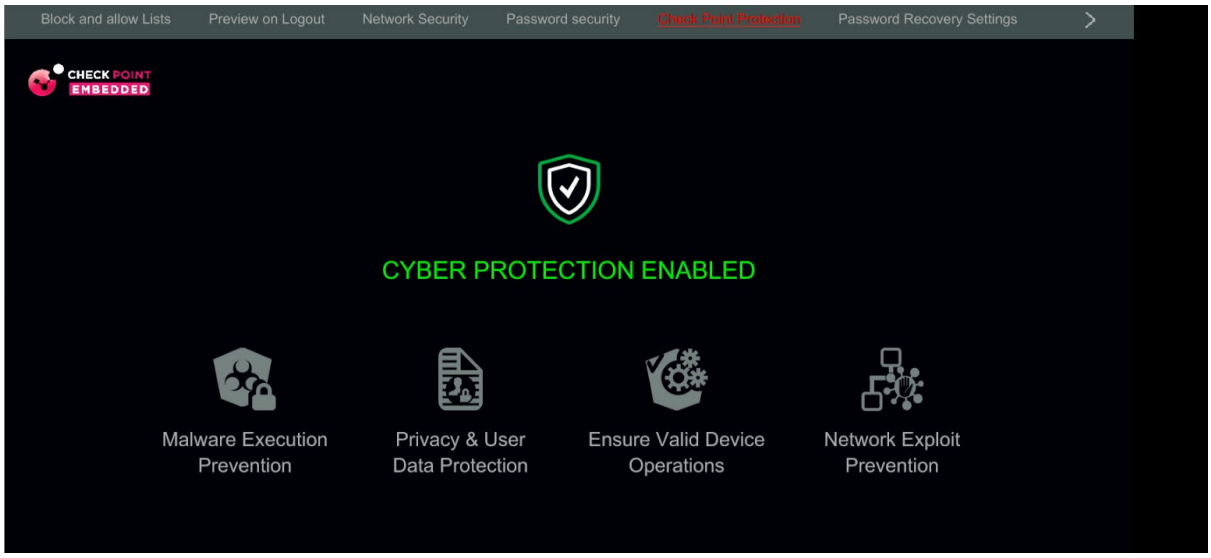
Set the password level as follows:

1. Weak: Any password will be allowed
2. Medium: Password must be minimum 8 characters long and include at least 1 letter and 1 number
3. Strong: Password must be minimum 8 characters long and include at least 1 letter , 1 capital letter and 1 number
4. Stronger: Password must be minimum 8 characters long and include at least 1 letter , 1 capital letter, one special character and 1 number.

Choose Expiration time out of: Never / 30 Days / 60 Days / 90 Days. When the password will expire, the user will have to set a new password according to the set password level.

12.7 Check Point Protection (If Applicable)

Device with Check Point Protection are running Check Point's IoT workload protection agent that is monitoring all activities and incoming/outgoing traffic. This provides an extra layer of cyber security for the device.
Click Start→Settings→Account and Permissions →Security→Check Point Protection.



Enable/Disable the WLP Agent as required. Changing the Check Point agent status requires administrator authentication.

Please note:
It is highly advisable to keep the Check Point agent enabled.

12.8 Password Recovery Settings

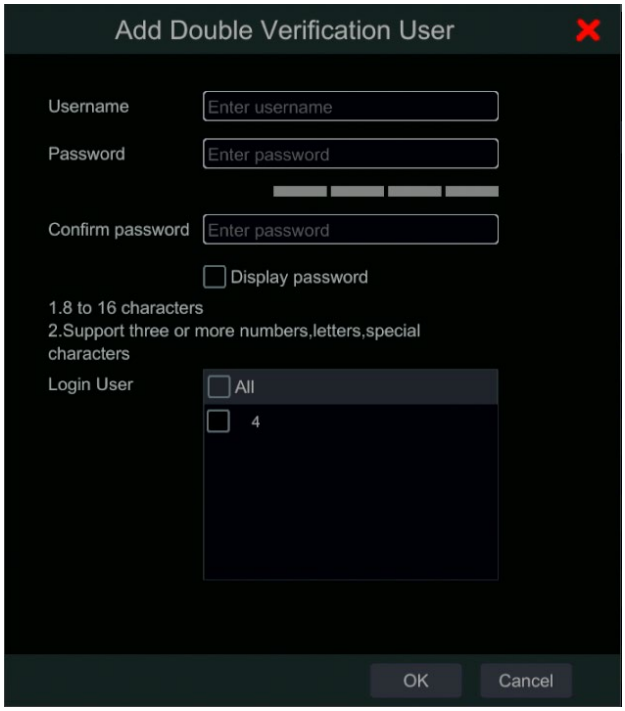
There are 2 password recovery options: Email and Questions.
Email: Enable the option and set the email account that will receive the temporary ***admin*** password when needed.
Questions: You can set password security question only for ***admin***. Select the question you want to answer, input the reply and click on "Apply" to save it, then apply to save the new configuration.

12.9 Double Verification

Double Verification allows to set a condition that will require 2 accounts in order to login to the NVR.
Click Start→Settings→Account and Permissions →Security→Double Verification

1. Enable the feature if needed.
2. Click on "Add" to setup the double verification rule

3. Set up the username and password for the supervisor or authenticating user. This user is not part of the NVR user list and cannot login to the system with these credentials.
4. Choose the authenticated user. Once confirmed, the selected user will not be able to login to the system without the username and password of the authenticating user.
5. Click OK to save the settings.
6. Click Apply to apply.



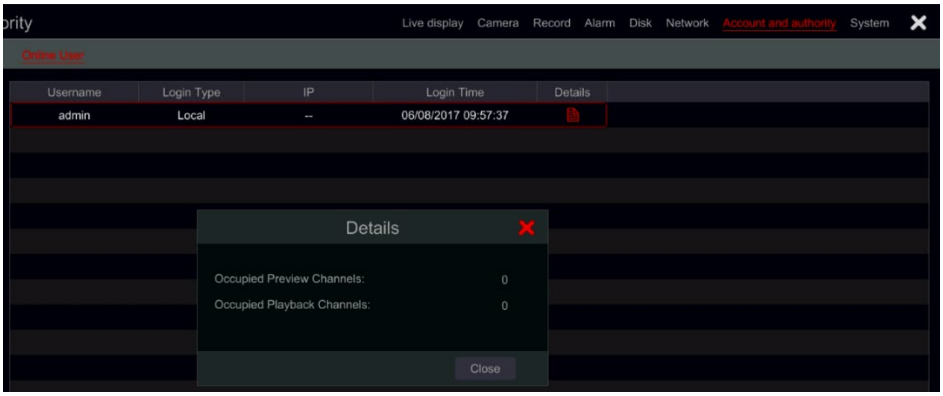
12.10 User Status:

12.10.1 Online Users

Click Start→Settings→Account and Permissions →User Status→Online Users to go to the following interface.

In the list you will find all the users who are currently connected to the system including their IP addresses and the number of live/playback channels they occupy

Click on to see detailed information about the channel usage by the selected user.



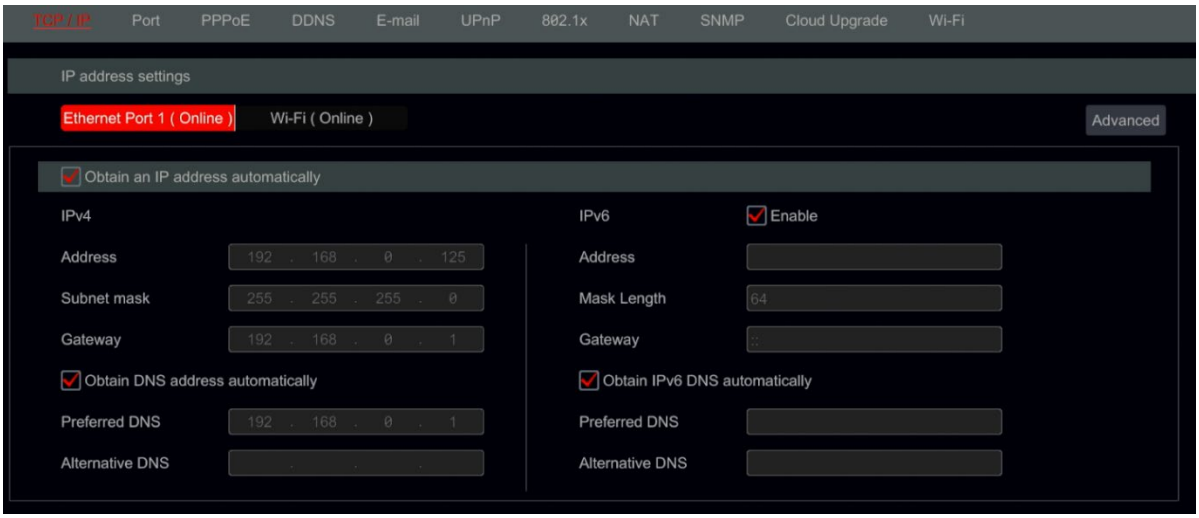
13. Device Management

13.1 Network Configuration

13.1.1 TCP/ IPv4/6 Configuration

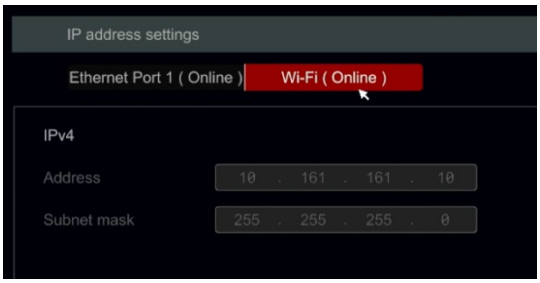
13.1.1.1 IP Address Settings

Click Start→Settings→Network→TCP/ IP.
Mark “Obtain an IP address automatically” and “Obtain DNS automatically” to get the IP address and DNS automatically, or input the IP address, subnet mask, gateway, preferred DNS and alternate DNS manually. Click “Apply” to save the settings. If your network support IPv6 you can set it here as well. The default setting is “Obtain an IPv6 address automatically”



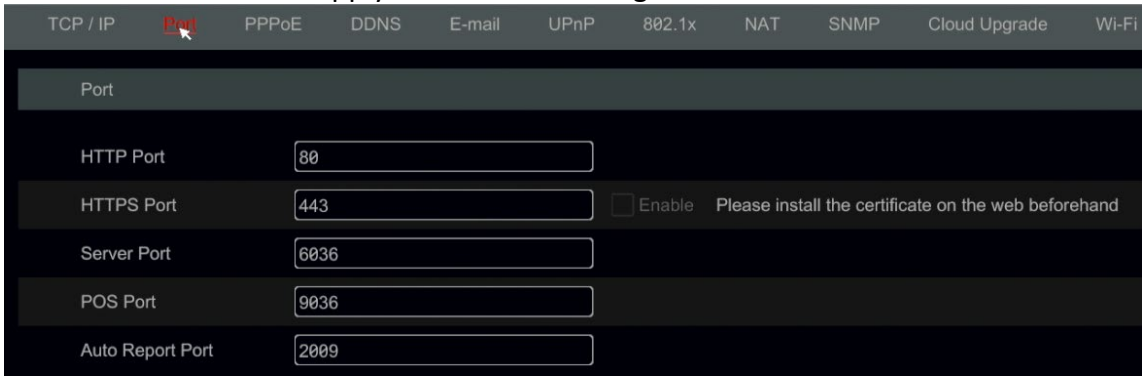
13.1.1.2 Internal Ethernet Port (PoE) – If Applicable:

WIFI: The WIFI section is enabled by default. It is used to connect the KIT's WIFI cameras to the NVR automatcially. The NVR does not onnect to other networks via WIFI. Only via ethernet cable.



13.1.2 Port Configuration

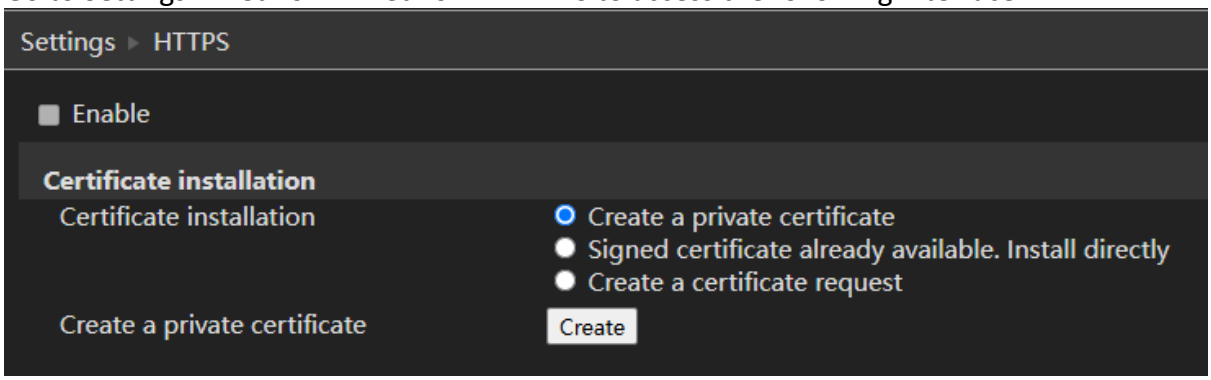
Click Start→Settings→Network→Port. Input the HTTP, HTTPS, Server, RTSP and POS ports of the device and click “Apply” to save the settings.



HTTP Port: the default HTTP port of the device is 80. The port number can be changed. The port is mainly used for direct IE and mobile application remote access via static IP or DDNS. To access the device through IE, input the IP address plus HTTP port in the address bar for example: http://192.168.11.61:81. (If the HTTP port is 80 – there is no need to input it)
HTTPS Port: HTTPS will allow you to create an encrypted communication between the device and any web browser connected to it.The default is 443 and must be enabled from this interface in order to use it. Before enabling it, you must set the certificates through the web.
Once enabled, you will be able to access the device using HTTPS address. For example: https://192.168.11.61. If you don't change the default port (443) there is no need to input it in the address line.
Server Port: the default server port of the device is 6036 and it can be changed as required. The port is mainly used in network video management system like CMS.
POS Port: POS (Point Of Sale) is used to connect cash registered to the device in order to compare the cash register output with the video recordings. The default port is 9036.
Auto Report Port: This port is used when using the NVR as the auto report server. The default is 2009.

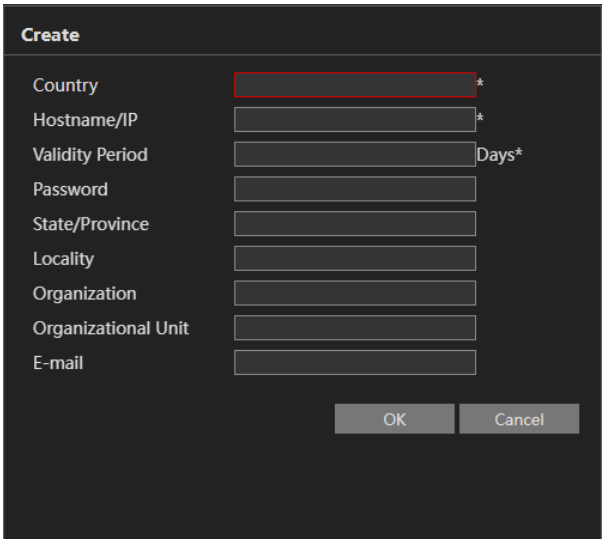
13.1.3 HTTPS Configuration

Before the HTTPS could be used, the user must set the encryption certificates. This can only be done through the device web interface. Login to the device through a web browser.
Go to Settings→Network→Network→HTTPS to access the following interface.



There are 3 options:
Create a private certificate.
The NVR will create a certificate using its own algorithm.
1. Click "Create" to open the following page.

2. Set the country as a 2 letter code (For example: IL for Israel, US, for United States of America, Etc.)
3. Set the protected hostname/IP which will appear in the certificated details
4. Set the certificate validity in days (1-5000)
5. Click on Ok to create and install the certificate



Signed certificate already available. Install directly:

If you already have a signed certificate, it should be in "crt" format. The certificate allows the NVR to encrypt data, but it will also need the private key in order to decrypt data. Please follow the steps below to avoid errors with the certificate.

1. Open your certificate (*.crt) file using a text editor such as Notepad or Notepad++
2. Open your private key (*.key) file using a text editor such as Notepad or Notepad++
3. Copy the content of the private key file and paste it **above** the content of the certificate file.
4. Save the edited certificate file as a copy and close both files.
5. Choose "Signed certificate already available. Install directly", click on "Browse" and select the edited certificate file.
6. Click on "Import" to import the file.
7. If the certificate is protected by a password select "Encryption", input the password and click on "OK". Otherwise keep the selection on "Decrypted" and click on Ok.
8. Once you see the installed certificate with its details, click on "Apply"

Create a certificate request:

Certificate request is used to initiate the process of creating a signed certificate. The certificate request file will later be used by other services to create a signed certificate.

1. Choose "Create a certificate request" and click on "Create"
2. Set the country as a 2 letter code (For example: IL for Israel, US, for United States of America, Etc.)
3. Set the protected hostname/IP which will appear in the certificated request details
4. Click on "Ok"
5. Click on "Browse" next to "Certificate download request", choose the destination folder and click on "Export" to download the request.
6. Use this request file by any signed certificate service you wish in order to generate a signed certificate.
7. Once the Signed certificate is ready, click on "Browse" next to "Install the generated certificate" and import.
8. Once you see the installed certificate with its details, click on "Apply"

13.1.3.1 Enabling/Disabling HTTPS

Once a certificate is successfully installed, you can enable/disable the HTTPS through either the local or the web interfaces. Note that once enabled, all HTTP communication will be blocked.

If HTTPS is not working through the web interface, there might be something wrong with the certificate configuration. Disable the HTTPS from the local interface and login to the web interface through normal HTTP to reconfigure the certificate.

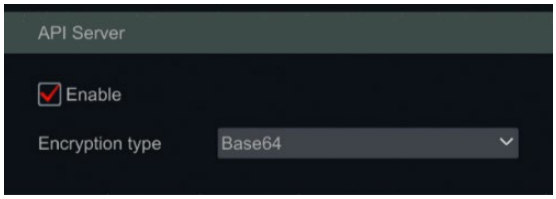
13.1.3.2 Deleting/Replacing the Certificate.

Login to the web interface through HTTPS and delete the certificate. Deleting the certificate will automatically disable the HTTPS, so you will need to login again through normal HTTP.

13.1.4 API Server

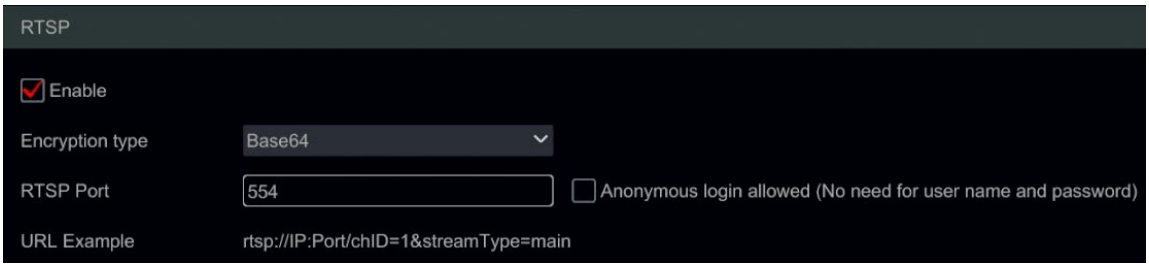
The API Server serves as an additional layer of protection for the end user. While disabled, All API/SDK connections to the system will be rejected.

Once enabled, you can choose your working mode: Base64/MD5.



13.1.5 RTSP

RTSP (Real-Time Stream Protocol) can be used to retrieve the video stream from the device by any media player which supports the RTSP. You can view the live stream synchronously. The default RTSP port is 554. It can be changed as required. Here you can also tick "Anonymous login allowed" to allow unauthenticated RTSP connections.

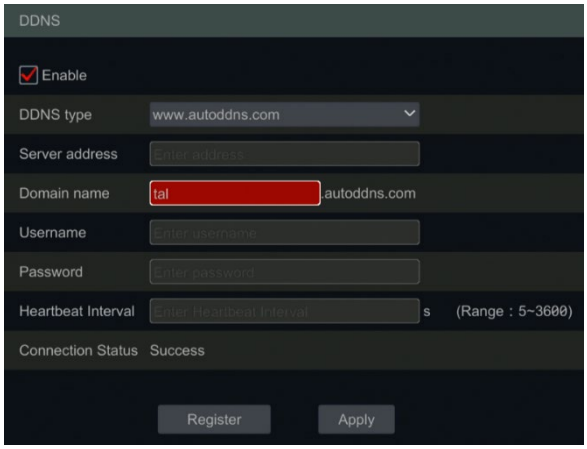


13.1.6 DDNS Configuration

The DDNS is used to control the dynamic IP address through a domain name. You can access to the device easily if the DDNS is enabled and properly configured.

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

Mark "Enable" and select the DDNS type. We advise on using www.autoddns.com which is free and simple to use. This manual is based on autoddns selection:

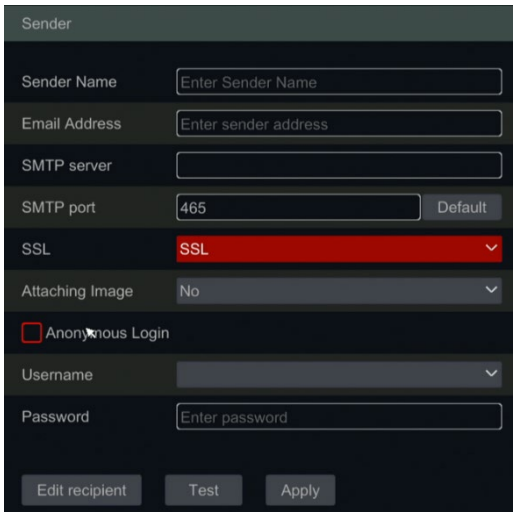


1. Input the desired "Domain Name".
2. Click ***Register*** button and wait for the prompt. If successful, continue to the next

step. If not, try another domain name and repeat.
3. After you successfully set your domain name, map the HTTP and Server ports on your router.
4. Browse to the DDNS domain you have set (for example: ***http://tal.autoddns.com:8081***)

13.1.7 E-mail Configuration

Click Start→Settings→Network→E-mail.

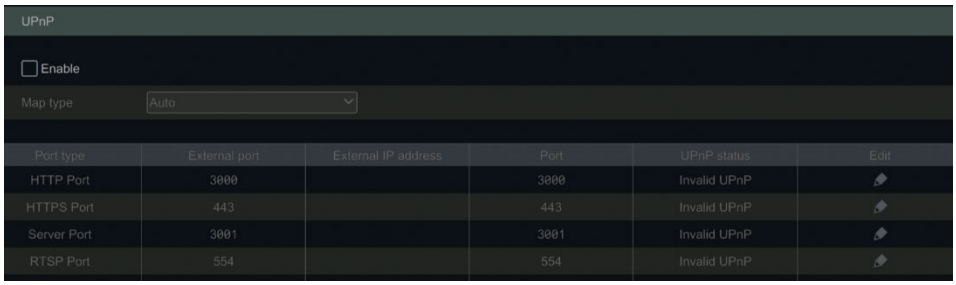


1. Input the sender's e-mail address, name, password, SMTP server and SMTP port (you can click "Default" to reset the SMTP port to the default value) and enable/disable the SSL and "attaching image". Click "Test". Input the e-mail address of the recipient in the window and click "OK" button. The e-mail address of the sender will send an e-mail to the recipient. If the e-mail was sent successfully, it indicates that the e-mail address of the sender is configured correctly. Click "Apply" to save the settings.
2. Click "Edit Recipient".
3. Click "Add" and input the recipient's e-mail address in the opened window. Set the schedule rule which you want to apply for the recipient and click "Add" to confirm. Click to delete a recipient from the list. Click "Apply" to save the settings. Click "Edit Sender" to go to the e-mail configuration interface of the sender.

13.1.8 UPnP Configuration

By using UPnP you can access the device through IE client in WAN via router without port mapping.

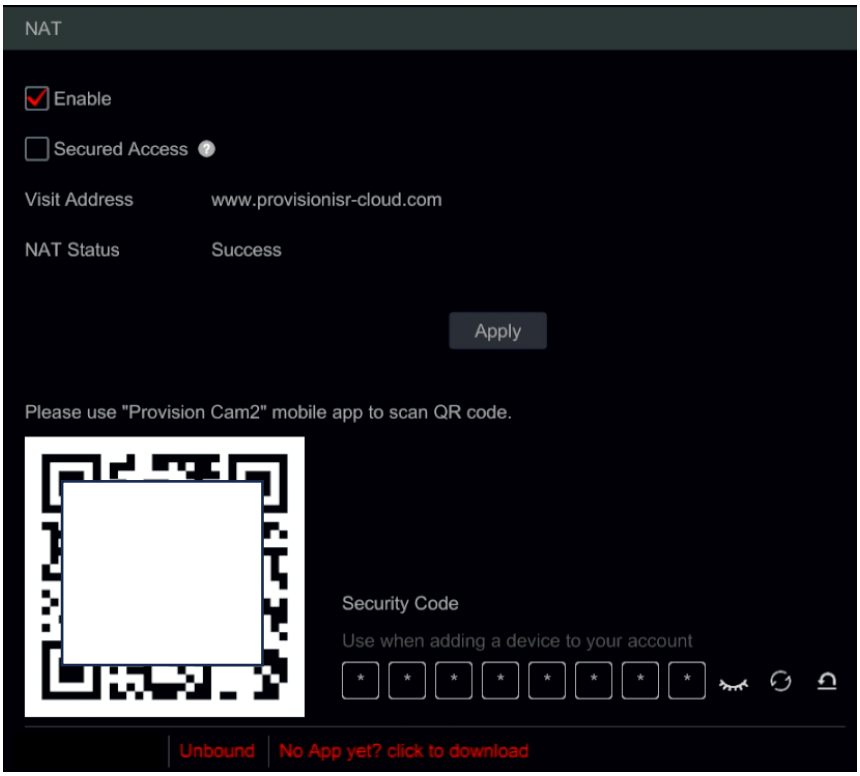
1. Click Start→Settings→Network→UPnP to go to the following interface.
2. Make sure the router supports UPnP function and the UPnP is enabled in the router.
3. Set the device's IP address, subnet mask and gateway and set the corresponding in the router interface.
4. Mark "Enable" and click "Apply" button.



Click "Refresh" button to refresh the UPnP status. If the UPnP status is still "Invalid UPnP" after refreshing, the port number is probably wrong. Please change the mapping type to "Manual" and 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 device. Input the external IP address plus port in the IE address bar to access the device.

13.1.9 NAT Configuration

NAT allows you to connect to the device using the P2P cloud platform. After enabling it, all you will have to do is to scan the QR code using the mobile app in order to remotely connect to your device.
Click Start→Settings→Network→NAT.
Mark “Enable” and click “Apply” to save the settings.



When using Provision Cam2 mobile app version >1.8 you have two options to add the device to the app by P2P:

1) The “old” method, by scanning the QR code and inputting the username/password. This method is considered less secure since anyone can perform this process (assuming that he has a username and password).
2) The “new” method – by adding the device to your account in the app. Scan the QR code from the App. This process will bind the device to the owner.

13.1.9.1 Security Access:

Secuirty access enhances the security of the user and limits connection to the device by P2P. Once enabled, any connection to the device via P2P will require the authorization of the bound account owner (Push message will be sent to Provision Cam2 Mobile app). The conditions for the Security Access to work:

1. Security Access is enabled
2. An account is bound to the device.

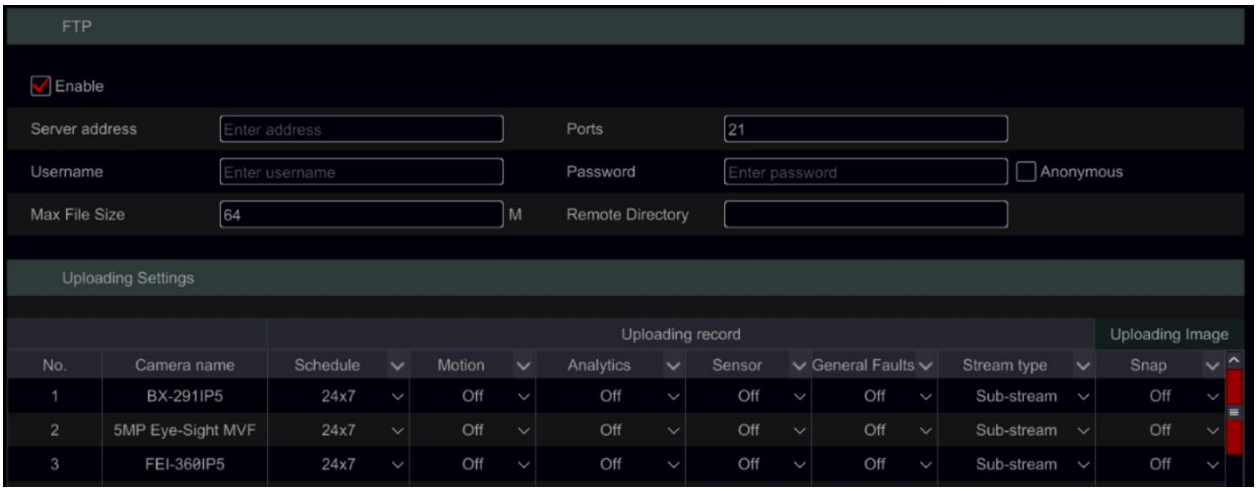
Once the security access is enabled, P2P access is possible through the following options:

1) Provision Cam2 Mobile app: Through device sharing only.
2) Web page (www.provisionisr-cloud.com): When trying to login, and after inputting the user credentials, there will be a need for an access code. The bound user will get this OTP to his Provision Cam2 app as a push message.

13.1.10 FTP Configuration (For supported device)

FTP allows you to **backup** recording to an FTP server based on set rules. The data is uploaded to the FTP from the HDD and cannot replace the HDD or perform as a “fail safe” to the HDD.

1. Click Start→Settings→Network→FTP.
2. Enable the FPT in order to activate the interface.
3. Input the FTP server address and port (default port is 21)
4. Input the login credentials for the server.
5. Set the maximum file size (in MB)
6. Set the remote directory path on the FTP
7. Choose which alarms will trigger the device to upload information to the FTP server and set the stream type (Main/Sub) and if to include snapshot.
8. Once done, click test. The system will confirm the connectivity and read/write permission on the FTP platform based on the given credentials.
9. If Test was successful, click “OK” to save.
10. If the test failed, repeat this process from stage 3 to 6.



13.1.11 SNMP Configuration

Simple Network Management Protocol (SNMP) is an Internet Standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behaviour.

Click Start→Settings→Network→SNMP

Set all information required for SNMP. This information should be provided by the site IT manager, or configured on the supported device (Managed Switch/Router Etc.)

13.1.12 Cloud Upgrade

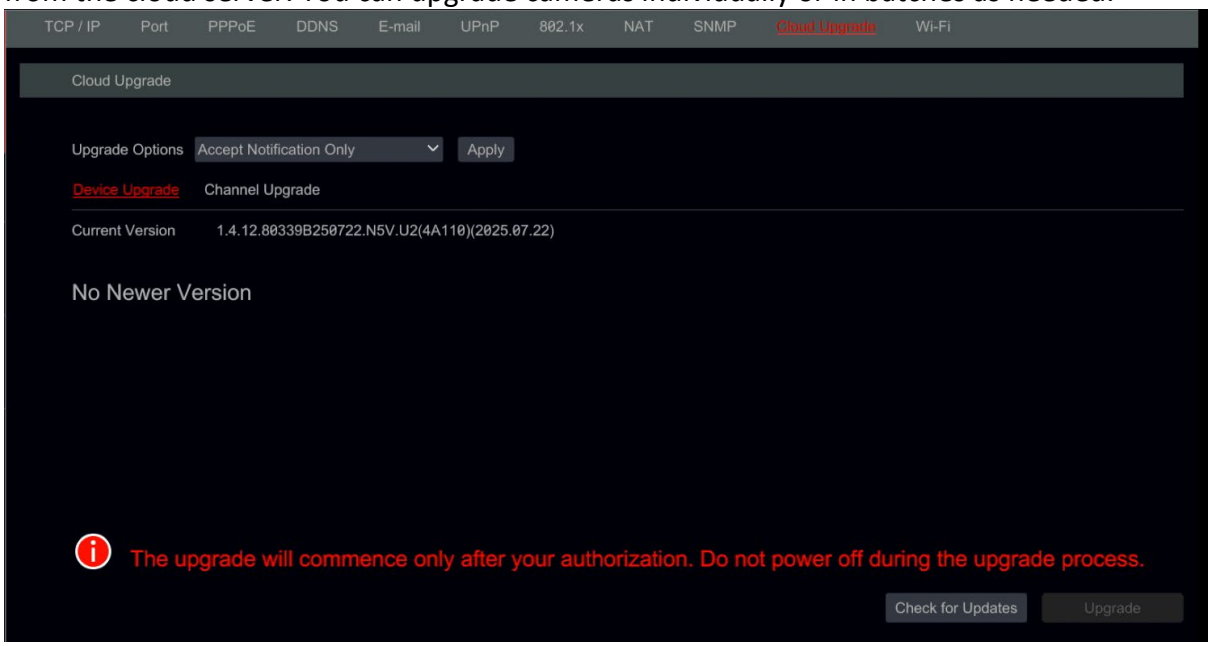
NVR Upgrade: Upgrade options allows you to receive notification upon detection of new firmware for the NVR and for IP cameras supporting the cloud update feature (Version >5.2). From here you can also check for updates manually and initiate the update procedure.

Click Start→Settings→Network→Cloud Upgrade.

To enable cloud upgrades, set the “Upgrade options” to “Accept notifications only” and apply.

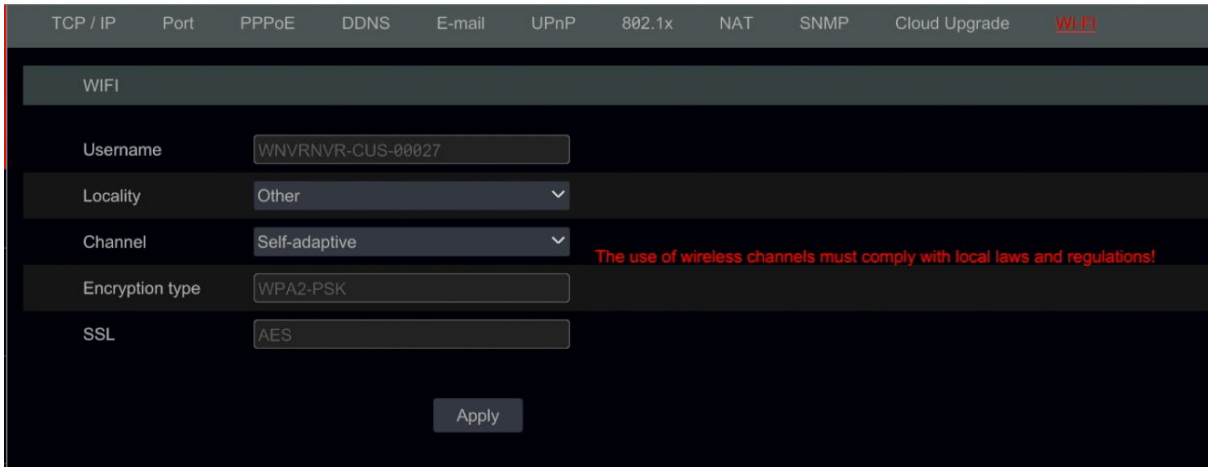
You can check for updates manually by clicking “Check for Updates”. If an update is available, click “Upgrade” to initiate the process.

IPC Upgrade:
Go to the “Channel Upgrade” tab to automatically check the versions of the added cameras. If any cameras are not up to date, click “Check for Updates” to retrieve the latest firmware from the cloud server. You can upgrade cameras individually or in batches as needed.



13.1.13 WI-FI

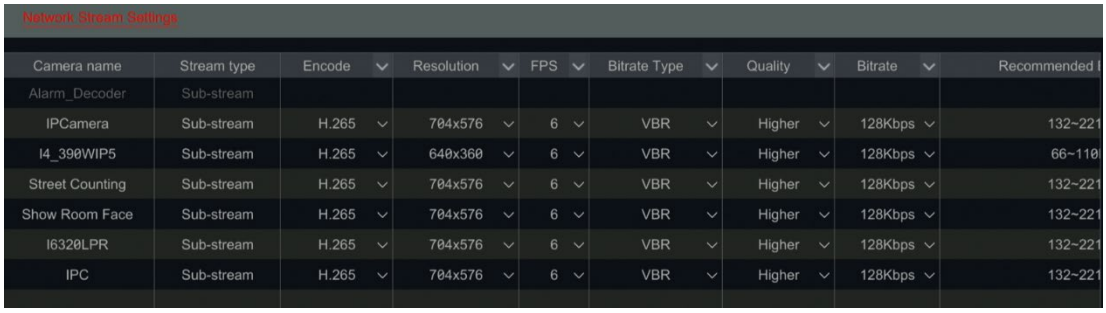
Click Start → Settings → Network → WiFi to access the interface. The WiFi port is enabled by default to allow connection of WiFi cameras. You can configure the region and channel as needed. When multiple WiFi NVR kits are used, you can either assign a separate channel for each system or select the self-adaptive channel option.



13.2 Network Stream

13.2.1 Network Stream Settings

Click Start→Settings→Network Stream→Network Stream Settings to go to the following interface.



From here you can set your network stream (Network Sub-Stream).

Please note:
Network Sub-Stream is not Record Sub-Stream. Please do not confuse between the two. For recording sub stream, refer to the recording section.

13.3 Integration

13.3.1 ONVIF

ONVIF allows you to connect to the NVR using 3rd party VMS software that support adding recording devices by ONVIF standard.
Click Start→Settings→Network→Integration→ONVIF to open the following interface

1) Enable ONVIF if required
2) Set a user for ONVIF by clicking on “Add”. Set a user name, password and user type.
3) Click “Apply” to confirm the setting.

Please note:
ONVIF user is also responsible for RTSP. If there is no ONVIF user, RTSP will be disabled.

13.3.2 Auto-Report Configuration

Auto Report allows the device to automatically report to the Ossia VMS server without port forwarding or static IP on the NVR side. Please refer to the Ossia VMS user manual for more information.
Click Start→Settings→Network→Auto Report.

1. Enable the service if needed.
2. Set the Ossia VMS server address + Port.
3. Set the device ID. Note that device IDs must be unique. Duplicated device IDs will cause conflicts.
4. Click on “Apply” and continue the configuration on the Ossia VMS server side.

13.4 Network Status

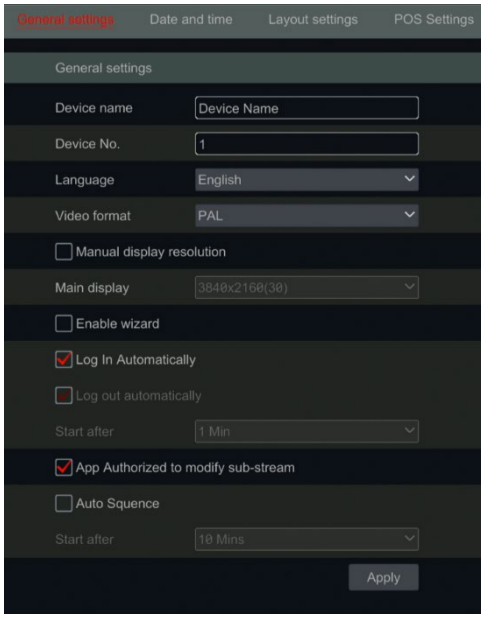
13.4.1 View Network Status

Click Start→Settings→Network→Network Status to view the network status / or click on the general tool bar at the bottom of the live-view interface and switch to “Network Status” to view network status.

13.5 Basic Configuration

13.5.1 General Settings

Click Start→Settings→System→Basic→General Settings to go to the following interface. Set the device name, device No., language, video format and resolution. Enable or disable the configuration wizard, “Log In Automatically” or “Log Out Automatically” (if marked, you can set the wait time before log out). Click “Apply” to save the settings.



Device Name: The name of the device. It may display on the client end or VMS and help the user to easily recognize the device.
Device No.: An address number used for controlling the device using C06 Controller (Joystick)
Language: Language Selection
Video Format: Two modes: PAL and NTSC. Select the video format according to the region / cameras.
Manual Display Resolution: Allowing the user to manually change the main display resolution.
Main Display: The device will automatically set the resolution when you turn on the device for the first time. If only VGA monitor is connected, the resolution will be set automatically to 1280x1024. If and HDMI monitor is connected, the resolution will be set automatically to 1920x1080. If both VGA and HDMI Monitors are connected, the HDMI will be the primary monitor and the resolution will be set to 1920x1080. In such case, you will have to reduce the resolution manually in case that the VGA monitor is not working well. Once the resolution has been set manually, the auto-configuration is disabled.
Secondary Output (Devices with 2 HDMI outputs only): Set the output for the secondary video output.
Enable Wizard: Enabling the configuration wizard to pop-up on each startup of the system.
Log in Automatically: The system will not request a login password until you will manually log out.
Log Out Automatically: The system will log out the system after the configured time duration.
App Authorized to modify Sub-Stream: The system will prevent from “Provision Cam2” mobile app from making any changes to the main/sub stream resolutions. This will

result in better performance on CMS and 3rd party applications on the expense of lower performance from the App side.

Auto Sequence + Wait Time: Start sequence when the system is not in use (mouse not moving) for a defined time.

13.5.2 Date and Time Configuration

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

Set the system time, date format, time format and time zone of the device. If the selected time zone includes DST, the DST of the time zone will be marked by default. Click "Apply" to save the settings.

You can manually set the system time or synchronize system time with network through NTP.

Manual: select "Manual" in the "Auto Time Sync." option and click after the "System Time" option to set the system time.

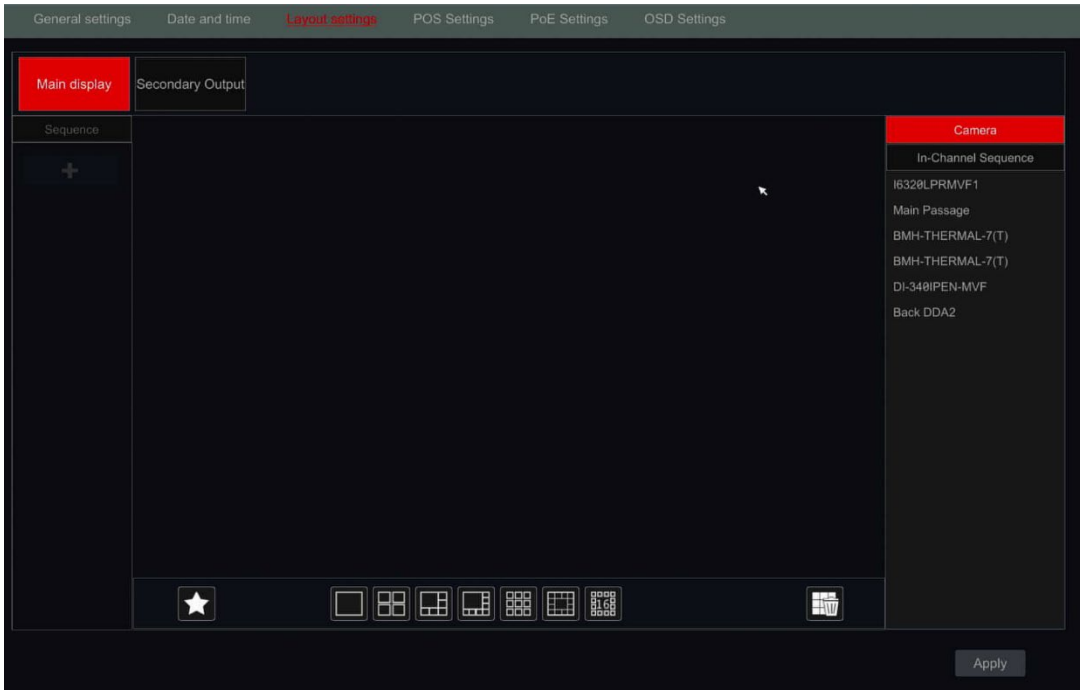
NTP: select "NTP" in the "Auto Time Sync." option and input the NTP server. (The default is www.provisionisr-time.com) and set the time adjustments interval.

13.5.3 Layout settings:

Click Start→Settings→System→Basic→layout settings to go to the interface as shown below.

The layout setting appearance and configuration options will be different depending on your device model. There are 3 options.

1) Standard NVR/PoE NVR – you will have only "Main Display" option. Here you will be able to set the layout for sequence or set your custmized display modes
2) Professional devices with 2 HDMI Outputs: In addition to the described above, you will also find here Secondary display. From here you will be able to set the layout for the second HDMI output. The secondary display does not show the main interface.
3) Professional devices with 1 HDMI Output + 1 VGA Output: In the layout settings, you

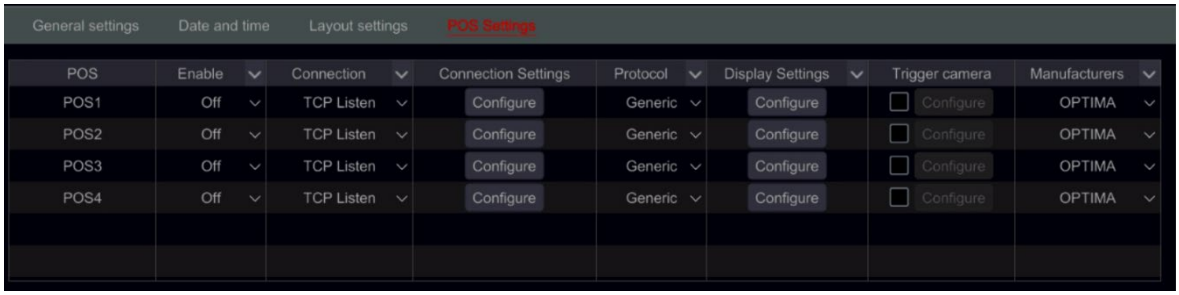


will be able to switch the VGA from Mirrored video output to auxiliary output.

The left pane displays all the schemes. The middle section shows the camera layout. The right pane displays all the cameras and groups. The bottom pane is the tool bar (: clear button; : favorite button. Click it to save the layout as preset – only available for main display).

13.5.4 POS settings:

Click Start→Settings→System→Basic→POS to go to the interface as shown below.
POS is used to integrate between the recorded video and the information coming from a supporting cash register. This section allows you to configure the POS and link it to the proper video channel. Up to 4 POS can be configured.



1) Enable the required POS channel.
2) Set the Connection Type
3) Set the connection settings as follows:
    a. POS IP: The IP of the required cash register.
    b. If you wish, you can set filters for ports and destinations.
4) Set the POS protocol as required.
5) Set the display settings as follows:
    a. Set the start and end characters
    b. Set the new line character.
    c. Set “ignore” character.
    d. Set connection timeout (Default is 10 seconds)
6) Switch to the “Display Position” Tab and set the required position for the text form the POS.
7) If you wish for the POS to trigger a camera record, tick that option and set the camera(s) you wish to record.
8) Set the manufacturer of the POS.

13.5.5 PoE Power Management:

Click Start→Settings→System→Basic→PoE Power Management. From this interface you can view the status of the PoE power bank as well as each PoE port and the current power output provided through it. If required, you can also disable the PoE port (Preventing only power output – the link will remain active).

13.5.6 OSD Settings:

Click Start→Settings→System→Basic→OSD Settings. This interface allows you to enable/disable the channel’s name and icons on the live view interface.

13.6 Maintenance:

13.6.1 View Log

Click Start→Settings→System→ View Log. Select the log type, click to set start time and end time and click “Search” button. The searched log files will be displayed as a list.
Choose the log file from the list and click “Export” button to export the log file.
Click on the “Content” title bar to create filters within the log entries. Click to play a video log if available.

13.6.2 Factory Default

Click Start→Settings→System→Maintenance→Factory Default. Now you have the option to choose between different types of factory default:

1) If you wish to keep the network settings, tick the “Reset all but Network Configuration” marker.
2) “Restore default parameters (Reboot)” will perform settings restore that will keep the device logs, face and LPR databases intact. Once complete the device will reboot

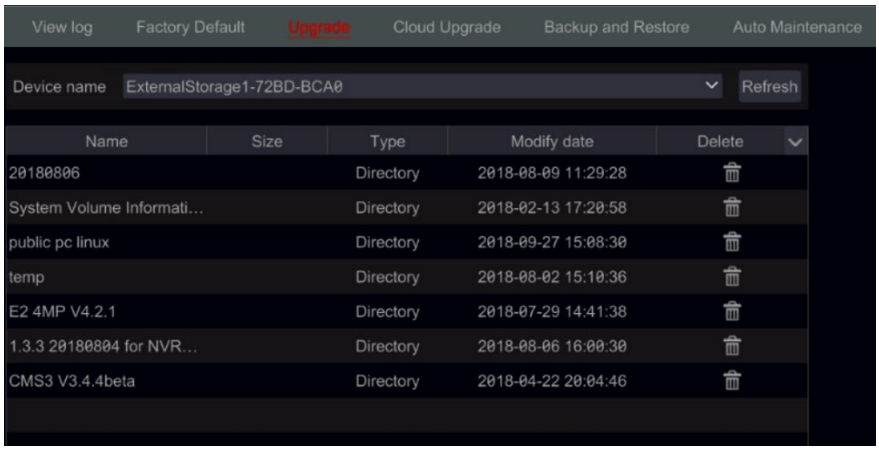
Please note:
When using “Restore default parameters” the admin settings will not be changed.

3) “Restore factory settings (Reboot)” will perform a full restore, clear the device logs, delete the LPR and face databases and reboot the device.

13.6.3 Device Software Upgrade

Before upgrading, download the correct update file from Provision-ISR’s website.
Click Start→Settings→System→ Maintenance →Upgrade.
The upgrade steps are as follows:

6. Copy the upgrade software into the USB storage device.
7. Insert the USB storage device into the USB slot of the device.
8. Select the USB device under the “Device Name” option and go to the path where the upgrade software exists. Select the upgrade software and click “Upgrade”. The system will automatically restart during the upgrade process. Do not power off the device during upgrading.



Please note:

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

13.6.4 Backup and Restore

You can back up the configuration file of the device by exporting the file to other storage devices; you can recover the configuration to other device which from the same model as the origin device importing the configuration file to other devices.

Insert the USB storage device into the USB interface of the device and click Start→Settings→System→Maintenance→Backup and Restore.

Backup: Select the USB device under “Device Name”, then go to the path where you want to store the configuration backup file and click “Backup”. Click “OK” to confirm.

Restore: Select the USB device under “Device Name” option. Find the configuration backup file and click “Recover”. Click “OK” to confirm.

13.6.5 Auto Maintenance:

You can set an interval of days/times for auto maintenance. This will reboot the device at the configured time to ensure that the memory, buffers and cache memory are always cleared.

Click Start→Settings→System→ Auto Maintenance. Tick “Enable”, set the days interval and the point of time during that day. It is highly advisable to choose a time where there is less chance for an incident to occur. During the auto maintenance procedure, the device will reboot so recording will not be available.

Click “Apply” – the next reboot date and time will appear in the interface.

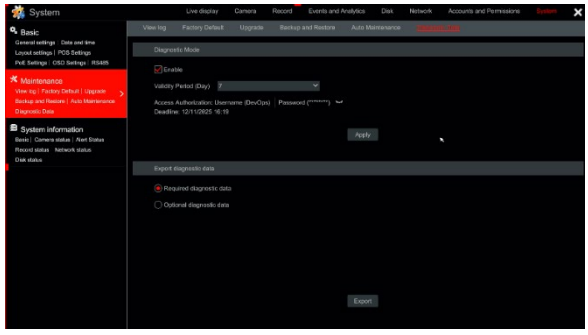
13.6.6 Diagnostic Data:

Click Start→Settings→System→Maintenance

The system can gather self diagnosis while running in order to recreate issues and exporting their diagnostic log to R&D dep.

Press Enable, choose "Validity Period" to determine how many days the system will gather information. Then press "Apply"

After the issue is recreated, you can export the diagnostic data into a USB drive.

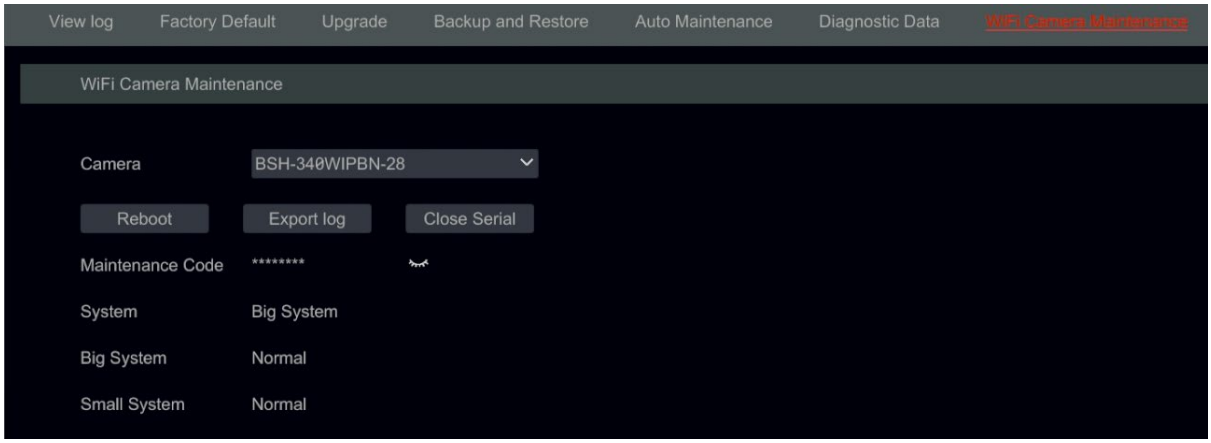


13.6.7 View System Information

Click Start→Settings→System→Information and choose the corresponding menu to view the “Basic”, “Camera Status”, “Alarm Status”, “Record Status”, “Network Status” and “Disk” information.

13.6.8 WIFI Camera Maintenance

Go to Start → Settings → System → WiFi Camera Maintenance. In this interface, you can reboot the Wi-Fi cameras connected to the NVR as needed.
Big and small system refers to the NVR and IPC correspondingly for upgrade status purposes.



14. Applications

14.1 Parking Lot Management

The NVR can manage a single Parking lot. The parking log can contain several entrances/exits with multi lanes

14.1.1 Configure

This is the basic configuration of the parking lot.

1. Click Start→Applications→Parking Lot Management. On the left pane choose Configure.
2. Set the parking name.
3. Set the total parking spaces and the currently vacant parking spaces.
4. You can choose license plate characters that will automatically allow exit.

14.1.2 Parking

This interface configures the parking lot groups and rules. You must have an active vehicle database to configure the parking.
Each LPR Database group can have its own selection out of the following 3 options:

1. No Parking Allowed: This group cannot park in this parking lot
2. User this group parking space: This group can enter the parking lot and has its own space allocation within the parking lot. When choosing this option, you will have to set the group's parking lot spaces and currently vacant spaces
3. Use the general parking space: This group can enter the parking lot and will take spaces out of the general vacant spaces.

You can also set the schedule for the group. The rule will only be applied during the set schedule.

14.1.3 Entrance and Exit

In this configuration you will see all the available LPR cameras. You will need to assign a role for each camera. The following options are:

1. Disabled: The camera is not used in this parking lot
2. Enter: This camera is designated for parking lot entrance only
3. Exit: This camera is designated for parking lot exit only
4. Enter and Exit: This camera is used for both entrance and exit

14.1.4 Monitoring

This is the main parking lot monitoring interface. In this interface you will see the latest events in the parking lot including vehicles entrance and exit. Once a vehicle reaches the gate, the operator can open the barrier even if the vehicle is not in the database. It will be registered in the log as manual entry.

14.2 Access Control Management

Use this interface to configure devices that are also used for Access control (For example the INT-320WIPN intercom unit).
The configuration is related to the door opening methods, door lock delay and holding time and Weigand configurations.
Access it via Click Start→Applications→Access Control Management

14.3 Face Attendance

The face attendance is a simple attendance application for small businesses. You need face database together with face recognition devices in the premises entrances and exits. You can set the Work times and get a full report for each one of the people in the database.
Access it via Click Start→Applications→Face Attendance

14.4 Face Check-In

Very similar to the face attendance, the face Check-In only indicates if a person was seen in a certain day or not.
Access it via Click Start→Applications→Face Check-In

Provision-ISR
11 Atir Yeda St, Kfar Saba,
Israel
Postal Code: 4442510
Tel: (972-9) 741 7511
Web: www.provision-isr.com