

Honeywell

Honeywell 35 Series

Network Video Recorder

HN35040100	HN35040101	HN35040102	HN35040104
HN35040106	HN35040108	HN35040110	HN35080200
HN35080202	HN35080204	HN35080208	HN35080210
HN35080216	HN35160200	HN35160204	HN35160208
HN35160210	HN35160216	HN35160220	HN35040100N
HN35080100N	HN35160200N	HN35080200C	HN35080202C
HN35080204C	HN35080208C	HN35080210C	HN35080216C
HN35160200C	HN35160204C	HN35160208C	HN35160210C
HN35160216C	HN35160220C	HN35160400C	HN35160404C
HN35160408C	HN35160410C	HN35160416C	HN35160420C
HN35320400	HN35320404	HN35320408	HN35320410
HN35320416	HN35320420	HN35320400N	

User Guide

Recommended

Find the latest version of this and other Honeywell 35 Series NVR documents on our website:
<https://buildings.honeywell.com/security>.

Copy Right

© 2023 Honeywell International Inc. All rights reserved. No part of this publication may be reproduced by any means without written permission from Honeywell. The information in this publication is believed to be accurate in all respects. However, Honeywell cannot assume responsibility for any consequences resulting from the use thereof. The information contained herein is subject to change without notice. Revisions or new editions to this publication may be issued to incorporate such changes. For patent information, see <https://buildings.honeywell.com/us/en/support/legal/patents>.

Revision

Issue	Date	Revisions
A	05/2022	New document.
B	06/2022	Add P2P. Add Web Mode.
C	10/2022	Add new SKUs. Add MPC settings.
D	12/2022	Add notes and update UI screenshots.
E	04/2023	Update MAXPRO Cloud page screenshots.

Cautions and Warnings

	CAUTION RISK OF ELECTRIC SHOCK DO NOT OPEN		 THIS SYMBOL INDICATES THAT DANGEROUS VOLTAGE CONSTITUTING A RISK OF ELECTRIC SHOCK IS PRESENT WITHIN THE UNIT.
CAUTION: TO REDUCE THE RISK OF ELECTRIC SHOCK, DO NOT REMOVE THE COVER. NO USER-SERVICEABLE PARTS INSIDE. REFER SERVICING TO QUALIFIED SERVICE PERSONNEL.			 THIS SYMBOL INDICATES THAT IMPORTANT OPERATING AND MAINTENANCE INSTRUCTIONS ACCOMPANY THIS UNIT.



Warning: Installation and servicing should be performed only by qualified and experienced technicians to conform to all local codes and to maintain your warranty.



Warning: Use only with the supplied power cable.
Power output: HN350401xx for 45W and HN350802xx/
HN351602xx for 130W, PoE 802.3at/af in total.



Caution: The Honeywell product uses a 3.3V CR2032 lithium battery as the power supply for its internal real-time clock (RTC). Low battery power affects the operation of the RTC, causing it to reset at every power-up.
Risk of explosion if the battery is incorrectly replaced.
Dispose of used batteries according to local regulations or the battery manufacturer's instructions.
Make sure the product is power-down before removal.
Then carefully remove the battery.
Replace only with an identical battery or a battery which is recommended by Honeywell.

Regulatory Statements

FCC Compliance Statement

Information to the User: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio

communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class A digital apparatus complies with Canadian ICES-003.

Manufacturer's Declaration of Conformance

North America

The equipment supplied with this guide conforms to UL 62368-1 and CSA C22.2 No. 62368-1.

Europe

The manufacturer declares that the equipment supplied is compliant with the European Parliament and Council Directive on the restriction of the use of certain hazardous substances in electrical and electronic equipment (2015/863/EU), the Low Voltage Directive (2014/35/EU) and the essential requirements of the EMC directive (2014/30/EU), conforming to the requirements of standards EN 55032/EN 61000-3-2/EN 61000-3-3/EN 61000-6-4 for emissions, EN 50130-4/EN 55024/EN 55035 for immunity, and EN 62368-1 for electrical equipment safety.

CAUTION This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

Waste Electrical and Electronic Equipment (WEEE)



Correct Disposal of this Product (applicable in the European Union and other European countries with separate collection systems).

This product should be disposed of, at the end of its useful life, as per applicable local laws, regulations, and procedures.

Check Local Waste Guidelines

Components of this product require separate waste collection. Check local waste guidelines for sorting rules.

General Data Protection Regulation

Please be aware that this product can store personal data.

Personal data is protected by the General Data Protection Regulation (2016/679) in Europe and therefore the owners of personal data have obtained certain rights thanks to this regulation.

We strongly advise you to be fully aware of these owner ("data subjects") rights as well as which limitations you have to obey regarding the use and distribution of this data.

Further details can be found on the GDPR website of the EU:
https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

Safety Instructions

Before installing or operating the unit, read and follow all instructions. After installation, retain the safety and operating instructions for future reference.

HEED WARNINGS - Adhere to all warnings on the unit and in the operating instructions.

INSTALLATION

- Install in accordance with the manufacturer's instructions.
- Installation and servicing should be performed only by qualified and experienced technicians to conform to all local codes and to maintain your warranty.
- Any wall or ceiling mounting of the product should follow the manufacturer's instructions and use a mounting kit approved or recommended by the manufacturer.

OPERATION REQUIREMENT

- Install the PoE front-end device indoors.
- The device does not support wall mount.
- Do not place and install the device in an area exposed to direct sunlight or near heat generating device.
- Do not install the device in a humid, dusty or fuliginous area.
- Keep its horizontal installation, or install it at stable places, and prevent it from falling.
- Do not drip or splash liquids onto the device; do not put on the device anything filled with liquids, to prevent liquids from flowing into the device.
- Install the device at well-ventilated places; do not block its ventilation opening.

- Use the device only within rated input and output range.
- Do not dismantle the device arbitrarily.
- Transport, use and store the device within allowed humidity and temperature range.

POWER SOURCES - This product should be operated only from the type of power source indicated on the marking label. If you are not sure of the type of power supplied to your facility, consult your product dealer or local power company.

MOUNTING SYSTEM - Use only with a mounting system recommended by the manufacturer, or sold with the product.

ATTACHMENTS/ACCESSORIES - Do not use attachments/accessories not recommended by the product manufacturer as they may result in the risk of fire, electric shock, or injury to persons.

CLEANING - Do not use liquid cleaners or aerosol cleaners. Use a damp cloth for cleaning.

SERVICING - Do not attempt to service this unit yourself. Refer all servicing to qualified service personnel.

REPLACEMENT PARTS - When replacement parts are required, be sure the service technician has used replacement parts specified by the manufacturer or have the same characteristics as the original part. Unauthorized substitutions may result in fire, electric shock or other hazards. Using replacement parts or accessories other than the original manufacturers may invalidate the warranty.

WASTE- Components of this product require separate waste collection. Check local waste guidelines for sorting rules.

Warranty and Service

Subject to the terms and conditions listed on the product warranty, during the warranty period Honeywell will repair or replace, at its sole option, free of charge, any defective products returned prepaid.

In the event you have a problem with any Honeywell product, please call Customer Service at 1.800.323.4576 for assistance or to request a **Return Merchandise Authorization (RMA)** number.

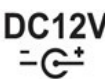
Be sure to have the model number, serial number, and the nature of the problem available for the technical service representative.

Prior authorization must be obtained for all returns, exchanges, or credits. **Items shipped to Honeywell without a clearly identified Return Merchandise Authorization (RMA) number may be refused.**

List of Symbols

The following is a list of symbols that might appear on the NVR.

Table 1 List of Symbols

Symbol	Explanation
	The WEEE symbol. This symbol indicates that when the end-user wishes to discard this product, it must be sent to separate collection facilities for recovery and recycling. By separating this product from other household-type waste, the volume of waste sent to incinerators or landfills will be reduced, and thus natural resources will be conserved.
	The UL compliance logo. This logo indicates that the product has been tested and is listed by UL (formerly Underwriters Laboratories).
	The FCC compliance logo. This logo indicates that the product conforms to Federal Communications Commission compliance standards.
	The direct current symbol. This symbol indicates that the power input/output for the product is direct current.
	The alternating current symbol. This symbol indicates that the power input/output for the product is alternating current.
	The LDPE symbol. This symbol indicates that this product is made of Low-Density Polyethylene (LDPE).
	The Direct Current symbol. This symbol indicates that the product operates from a 12 V direct current.
	The Lead-free symbol. This symbol indicates that the product does not contain lead (Pb).
	The CCC compliance logo. This logo indicates that the product conforms with the China Compulsory Certification guidelines.
	The Environment Friendly Use-period symbol. This symbol indicates the length of time that this electronic product can be used without harming the environment.
	The RCM Compliance symbol. This symbol indicates that the product conforms with the Australian RCM guidelines.

	The TVU Lab symbol. This symbol indicates that the product has been safety tested by the TUV Lab.
	The Direct Current symbol. This Direct Current symbol indicates that the product operates direct current.
	This symbol indicates that the product is to be used indoors.
	The CE Compliance logo. This logo indicates that the product conforms to the relevant guidelines/standards for the European Union harmonization legislation.
	The Protective Earth symbol. This symbol indicates that the marked terminal is intended for connection to the protective earth/grounding conductor.
	This symbol is used to direct attention to important information.
	This symbol warns that the corresponding action could result in an electric shock.
	This symbol indicates On/Standby functionality of the corresponding control/button/switch.

TABLE OF CONTENTS

Cautions and Warnings	i
Regulatory Statements	i
FCC Compliance Statement.....	i
Manufacturer's Declaration of Conformance	ii
Waste Electrical and Electronic Equipment (WEEE).....	ii
Check Local Waste Guidelines	ii
General Data Protection Regulation.....	iii
Safety Instructions.....	iii
Warranty and Service.....	iv
List of Symbols.....	iv
About This Document.....	i
Overview of Contents.....	i
1 Introduction.....	1
Overview.....	1
Key Features.....	1
Network Video Recorder Components.....	3
Front Panel and Rear Panel.....	3
Mouse Operation	16
2 Getting Started	17
Unpacking the NVR	17
Connecting External Devices	17
Devices Connection	18
Starting and Shutting Down the NVR.....	21
Starting the NVR.....	21
Shutting Down the NVR.....	21
Reset Button	22
Device Initialization.....	23
Device Wizard.....	25
Resetting Password.....	30
Enabling Password Reset Function	30
Resetting Password on Local Interface	30
Home Page	31

Mute Buzzer.....	32
Two-way Talk.....	33
Device-end to IPC.....	33
IPC-end to the Device-end.....	33
3 Local Basic Operation	35
Configuring Camera.....	35
Camera.....	35
Encode	41
Sensor Setting.....	42
OSD	43
POE Status	44
Configuring Storage Settings.....	45
Record Schedule	45
Disk.....	47
Storage Mode	48
S.M.A.R.T.....	49
Disk Detection	50
Disk Calculation	50
FTP/SFTP	51
Configuring Events Settings.....	53
General.....	53
Motion Detection	55
Camera Tampering	60
Video Loss.....	60
Intelligent Analysis.....	61
Alarm In.....	63
Abnormal Events.....	65
Alarm Out.....	66
Local Intelligent Analysis.....	67
Configuring Network Settings.....	68
Network.....	69
802.1X	72
DDNS	73
Port Mapping.....	74
Email.....	75
P2P	76
IP Filter.....	78
SNMP	79
Network Traffic.....	81
Access Platform.....	81

Configuring System Settings	82
Information	82
General.....	84
User Account	87
Security Center	91
Layout.....	93
Auxiliary Screen	94
Logs.....	95
Maintenance.....	97
Configuring MAXPRO Cloud.....	99
Configuring Live View Settings.....	100
Live View.....	100
Live View Control Interface	102
Playback.....	106
Time Interface	106
Picture Grid	109
Event Recording.....	110
Backup List.....	111
Setting MAXPRO Cloud	111
Register 35 Series NVR on the MAXPRO Cloud.....	111
Enable MPC Integration on the 35 Series NVR	113
Apply NVR Level Settings	114
Apply Camera Level Settings	115
View Recordings on the MAXPRO Cloud.....	117
Upgrade Firmware.....	118
Check Alarms.....	118
4 Web Operation	120
Network Connection.....	120
Web Login	121
Web Main Menu.....	122
Live View.....	122
Playback	123
Event Recording.....	125
Setting.....	126
5 FAQ	130

Figures

Figure 1 Front Panel (HN350401xx)	3
Figure 2 Rear Panel (HN350401xx)	4
Figure 3 Front Panel (HN35040100N & HN35080100N)	5
Figure 4 Rear Panel (HN35040100N & HN35080100N)	5
Figure 5 Front Panel (HN350802xx)	6
Figure 6 Rear Panel (HN350802xx)	7
Figure 7 Front Panel (HN351602xx)	8
Figure 8 Rear Panel (HN351602xx)	8
Figure 9 Front Panel (HN350802xxC)	9
Figure 10 Rear Panel (HN350802xxC)	9
Figure 11 Front Panel (HN351602xxC)	10
Figure 12 Rear Panel (HN351602xxC)	11
Figure 13 Front Panel (HN351604xxC/HN353204xx)	12
Figure 14 Rear Panel (HN351604xxC/HN353204xx)	12
Figure 15 Front Panel (HN35160200N)	13
Figure 16 Rear Panel (HN35160200N)	14
Figure 17 Front Panel (HN35320400N)	14
Figure 18 Rear Panel (HN35320400N)	15
Figure 19 Devices Connection (HN350401xx)	19
Figure 20 Devices Connection (HN35040100N/HN35080100N)	19
Figure 21 Devices Connection (HN350802xx)	20
Figure 22 Devices Connection (HN351602xx)	20
Figure 23 Devices Connection (HN35160200N)	21
Figure 24 Reset Button	22
Figure 25 Device Activation	23
Figure 26 Question (Recovery the Password)	24
Figure 27 Set Unlock Pattern	24
Figure 28 Recover the Password	25
Figure 29 Startup Wizard	25
Figure 30 Network	26
Figure 31 Setup Wizard – Date and Time	26
Figure 32 Setup Wizard –Time Zone	27
Figure 33 Setup Wizard –DST	27
Figure 34 Setup Wizard –Camera	28
Figure 35 Setup Wizard – Disk	28
Figure 36 Setup Wizard – P2P	29
Figure 37 Setup Wizard – Resolution	29
Figure 38 Reset Password	30
Figure 39 Password Reset 1	31
Figure 40 Password Reset 2	31
Figure 41 Home Page (Without MAXPRO Cloud)	32
Figure 42 Home Page (With MAXPRO Cloud)	32
Figure 43 Enable Two-way Talk	33
Figure 44 Device to IPC	33
Figure 45 IPC to Device	34
Figure 46 Add Camera	36
Figure 47 Manually Add Devices	37
Figure 48 Update Interface	38
Figure 49 Select File	39

Figure 50 Operating Online Channel.....	40
Figure 51 Protocol Management.....	40
Figure 52 Encode	41
Figure 53 Image.....	43
Figure 54 OSD.....	44
Figure 55 PoE Status	45
Figure 56 Record Schedule	46
Figure 57 Record Type.....	46
Figure 58 Set Period by Drawing.....	47
Figure 59 Disk Interface.....	48
Figure 60 Storage Mode	49
Figure 61 S.M.A.R.T Interface.....	49
Figure 62 Disk Detection Interface.....	50
Figure 63 Disk Calculation	51
Figure 64 Computation time.....	51
Figure 65 FTP	52
Figure 66 SFTP	52
Figure 67 General Page	54
Figure 68 IO Control Push	54
Figure 69 Motion Detection	55
Figure 70 Copy Dialog Box	56
Figure 71 Region Setting.....	57
Figure 72 Schedule Setting.....	57
Figure 73 Smart Motion.....	58
Figure 74 Smart Motion – Detection Area.....	59
Figure 75 Smart Motion – Schedule.....	59
Figure 76 Camera Tamper	60
Figure 77 Video Loss.....	61
Figure 78 Intrusion	62
Figure 79 Multi Loitering	62
Figure 80 Crowd Detection.....	63
Figure 81 Alarm In.....	64
Figure 82 Camera Alarm in Port.....	65
Figure 83 Abnormal Events.....	65
Figure 84 Alarm Out.....	66
Figure 85 Local Intelligent Analysis.....	67
Figure 86 Intrusion Event Actions	68
Figure 87 Detection Area.....	68
Figure 88 Networks - IP.....	69
Figure 89 Port Interface.....	70
Figure 90 POE.....	71
Figure 91 IPv4 CCTV.....	72
Figure 92 802.1X Interface.....	73
Figure 93 DDNS Interface.....	73
Figure 94 Port Mapping Interface	74
Figure 95 NAT Port Interface	75
Figure 96 Email Interface.....	76
Figure 97 P2P Interface.....	77
Figure 98 IP Filter	78
Figure 99 Add IP to Filter.....	78
Figure 100 SNMPv1/2	79
Figure 101 SNMPV3.....	80

Figure 102 Network Traffic Interface.....	81
Figure 103 Access Platform Interface.....	82
Figure 104 Network Status.....	82
Figure 105 System Status.....	83
Figure 106 Channel Status.....	83
Figure 107 Disk Usage.....	83
Figure 108 Alarm Status.....	84
Figure 109 System.....	84
Figure 110 Date and Time.....	85
Figure 111 Time Zone.....	86
Figure 112 DST.....	86
Figure 113 Sync Camera Time.....	87
Figure 114 User.....	87
Figure 115 Edit User.....	88
Figure 116 Add User.....	88
Figure 117 Permission.....	89
Figure 118 Advance Setting.....	90
Figure 119 App Verification.....	90
Figure 120 Input Security Code on App.....	91
Figure 121 Password.....	92
Figure 122 Unlock Pattern.....	92
Figure 123 Security Question.....	93
Figure 124 Layout.....	93
Figure 125 Auxiliary Screen.....	94
Figure 126 Auxiliary Screen – Layout.....	95
Figure 127 Logs - System Log.....	96
Figure 128 Event Log.....	96
Figure 129 Maintenance.....	97
Figure 130 Update Interface.....	98
Figure 131 Network Packet Capture interface.....	99
Figure 132 MAXPRO Cloud Interface.....	99
Figure 133 Live View Interface.....	100
Figure 134 Manual Alarm.....	101
Figure 135 Events List Pop-up Window.....	102
Figure 136 Live View Control Bar.....	102
Figure 137 Instant Replay Interface.....	103
Figure 138 PTZ Control Panel.....	104
Figure 139 Add Patrol Panel.....	105
Figure 140 Digital Zoom Interface.....	105
Figure 141 Camera Picture Parameter Interface.....	106
Figure 142 Playback.....	107
Figure 143 Picture Grid Interface.....	109
Figure 144 Replay Interface.....	110
Figure 145 Event Recording Page.....	110
Figure 145 Backup Interface.....	111
Figure 147 MAXPRO Cloud Sign in Page.....	112
Figure 148 Add New Controllers.....	112
Figure 149 Add Controller.....	113
Figure 150 MAXPRO Cloud.....	113
Figure 151 Select Connected Devices.....	114
Figure 152 Devices.....	115
Figure 153 Live Preview.....	116

Figure 154 Device Tab-Camera List.....	117
Figure 155 Search Firmware.....	118
Figure 156 Alarm List	119
Figure 157 Security Problem	121
Figure 158 Login	122
Figure 159 Liveview Page	122
Figure 160 Playback Page	124
Figure 161 Event Recording page	125
Figure 162 Setting Page.....	126
Figure 163 IPC Login Page.....	127
Figure 164 HTTPS	127
Figure 165 Certificate Request	128
Figure 166 Certificate Page	128
Figure 167 Upload Files Page	128
Figure 168 Uploaded Files.....	129
Figure 169 CA Certificate Page.....	129

Tables

Table 1 List of Symbols	v
Table 2 NVR Front Panel Description (HN350401xx)	3
Table 3 NVR Rear Panel Description (HN350401xx)	4
Table 4 NVR Front Panel Description (HN35040100N & HN35080100N)	5
Table 5 NVR Rear Panel Description (HN35040100N & HN35080100N)	5
Table 6 NVR Front Panel Description (HN350802xx)	6
Table 7 NVR Rear Panel Description (HN350802xx)	7
Table 8 NVR Front Panel Description (HN351602xx)	8
Table 9 NVR Rear Panel Description (HN351602xx)	8
Table 10 NVR Front Panel Description (HN350802xxC)	9
Table 11 NVR Rear Panel Description (HN350802xxC)	9
Table 12 NVR Front Panel Description (HN351602xxC)	10
Table 13 NVR Rear Panel Description (HN350802xxC)	11
Table 14 NVR Front Panel Description (HN351604xxC/HN353204xx)	12
Table 15 NVR Rear Panel Description (HN351604xxC/HN353204xx)	12
Table 16 NVR Front Panel Description (HN35160200N)	13
Table 17 NVR Rear Panel Description (HN35160200N)	14
Table 18 NVR Front Panel Description (HN35320400N)	15
Table 19 NVR Rear Panel Description (HN35320400N)	15
Table 20 Mouse Operation Instruction	16
Table 21 Remote Channel Parameters	37
Table 22 Audio/Video Parameters	41
Table 23 Image Parameters	43
Table 24 FTP/SFTP Parameters	52
Table 25 Motion Detection Parameters	55
Table 26 Detection Area Setting Parameters	59
Table 27 Alarm-in Port Parameters	64
Table 28 Abnormal Alarm Parameters	65
Table 29 Alarm Out Parameters	66
Table 30 Local Intelligent Analysis Parameters	67
Table 31 IP Parameters	69
Table 32 Port Parameters	71
Table 33 Port Mapping Parameters	74
Table 34 Email Parameters	76
Table 35 SNMP Parameters	80
Table 36 Data and Time Parameters	85
Table 37 Add Interface Parameters	89
Table 38 Navigation Bar Icons	100
Table 39 Live view Control Icons	102
Table 40 PTZ Control Panel Parameters	104
Table 41 Event Recording Parameters Description	110
Table 42 Liveview Icons & Parameters	123
Table 43 Playback Icons & Parameters	124
Table 44 Event Recording Icons & Parameters	125
Table 45 Setting Symbols	126

ABOUT THIS DOCUMENT

This document introduces the Honeywell 35 Series Network Video Recorder. It explains how to install and operate the 35 Series Network Video Recorder.

This document is intended for installers and users.

Overview of Contents

This document contains the following chapters and appendixes:

Chapter [1 Introduction](#), describes the front and rear panel layout of the NVR.

Chapter [2 Getting Started](#), describes how to connect the NVR and log on to its user interface.

Chapter [3 Local Basic Operation](#), describes the NVR's local operations.

Chapter [4 Web Operation](#), describes how to configure the web operations.

Chapter [5 FAQ](#), describes Q&A for resolving issues that you may encounter when operating the NVR.

INTRODUCTION

Overview

The 35 Series NVR is a high-performance network video recorder. This series product supports local live view, multiple-window display, recorded file local storage, remote control and mouse shortcut menu operation, and remote management and control function.

The 35 Series NVR supports center storage, front-end recording and client-end recording. The monitor zone in the front-end can be set in anywhere. Working with other front-end devices such as IPC, NVR, this series product can establish a strong surveillance network through the HSV. In the network system, there is only one network cable from the monitor center to the monitor zone in the whole network. There is no audio/video cable from the monitor center to the monitor zone. The whole project is featured by simple connection, low-cost, low maintenance work.

The 35 Series NVR can be widely used in areas such as public security, water conservancy transportation and education.

Key Features

Real-Time Surveillance

- VGA, HDMI port: Connect to monitor to realize real-time surveillance. Support VGA/HDMI output at the same time.
- Shortcut menu for preview.
- Support multiple popular PTZ decoder control protocols. Support preset and patrol.

Playback

- Support independent real-time recording for each channel. At the same time, it supports functions such as network monitor, record search and download.
- Support various playback modes: slow play, fast play, backward play and frame-by-frame play.

- Support time title overlay so that you can view the event accurate occurred time.
- Support specified zone enlargement.

User Management

Users can be added to user groups for management. Each group has a set of permissions that can be individually edited.

Storage

- With corresponding settings (such as alarm settings and schedule settings), you can back up related audio/video data in the network video recorder.
- You can take records via the web and the record files are saved on the PC in which the client locates.

Alarm

- Respond to external alarm simultaneously (within 200 ms). Based on user's pre-defined relay settings, the system can process the alarm input correctly and sends user screen or voice prompts (supporting pre-recorded audio).
- Support settings of the central alarm server, so that the system can automatically notify users of the alarm information. Alarm input can be derived from various connected peripheral devices.
- Alert you of alarm information via email.

Network Surveillance

- Send audio/video data compressed by IPC or HSV to client-ends through the network, and then the data will be decompressed and displayed.
- Transmit audio/video data by protocols such as HTTP, TCP, UDP, MULTICAST and RTP/RTCP.
- Transmit some alarm data or alarm info by SNMP.
- Support web access in WAN/LAN.

Window Split

Adopt video compression and digital processing to display several windows in one monitor. Support 1/4/8/9/16 window split in preview and 1/4/9/16 window split in playback.

Record

Support schedule record, manual record and event record. Save the recorded files in the HDD, USB device, client-end PC or network storage server and you can search or playback the saved files at the local-end or via the Web/USB devices.

Backup

Support network backup and USB record backup. You can back up the record files in devices such as network storage server, peripheral USB2.0 device and USB 3.0 device.

Network Management

- Supervise NVR configuration and control power via Ethernet.
- Support web management.

Peripheral Equipment Management

- Support peripheral device control and you can freely set the control protocol and connection port.

Auxiliary

- Support real-time display of system resources information and running status.
- Support log record.
- Local GUI output. Shortcut menu operation with the mouse.
- Support to play the video/audio files from remote IPC.

Network Video Recorder Components

Front Panel and Rear Panel

Note: The following front panel and rear panel figures are for reference only. The actual product shall prevail.

HN350401xx

Figure 1 Front Panel (HN350401xx)

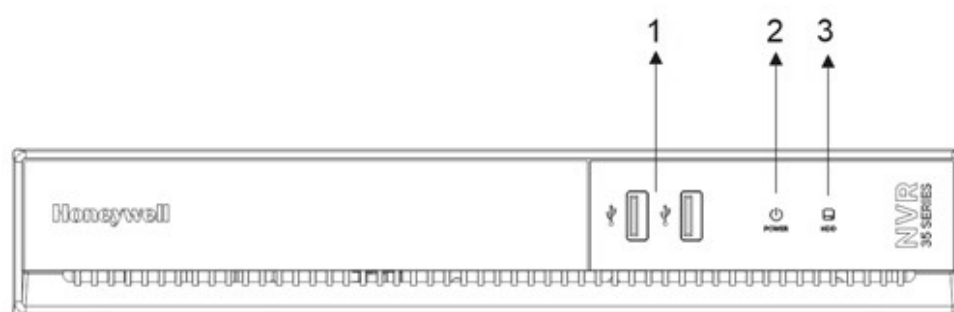


Table 2 NVR Front Panel Description (HN350401xx)

No.	Name	Description
1	USB port	Connect to peripheral USB 2.0 storage device, mouse and so on.
2	POWER	The light is on when the power connection is OK.

No.	Name	Description
3	HDD	The green light is flash when the device is recording, if the disk is not working, light is always bright. The light is off without disk.

Figure 2 Rear Panel (HN350401xx)

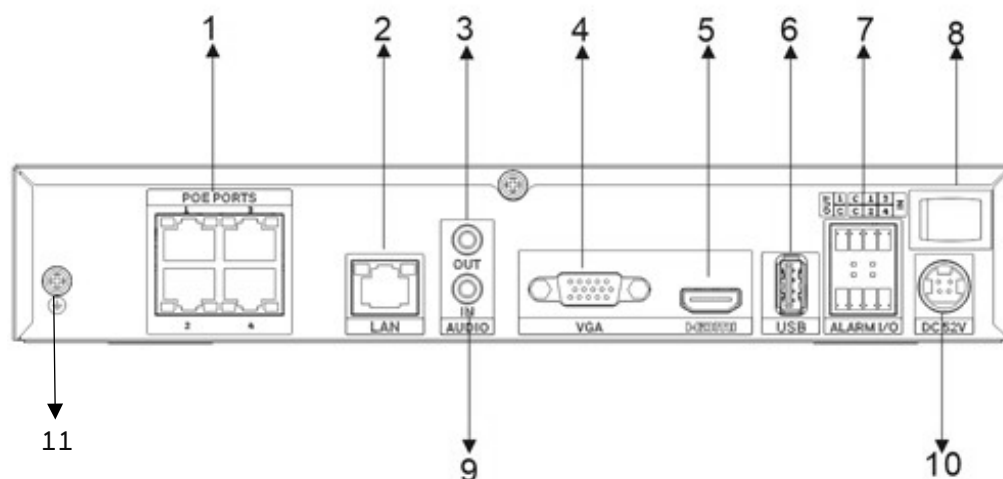


Table 3 NVR Rear Panel Description (HN350401xx)

No.	Name	Description
1	PoE port	Built-in switch. Support PoE function. For PoE series product, you can use this port to provide power to the network camera.
2	Network port	10M/100Mbps self-adaptive Ethernet port. Connect to the network cable.
3	AUDIO OUT	Audio output port. It is to output the analog audio signal to the devices such as the sound box. - Bidirectional talk output. - Audio output on 1-window video monitor. Audio output on 1-window video playback.
4	VGA	VGA video output port. Output analog video signal. It can connect to the monitor to view analog video.
5	HDMI	High definition audio and video signal output port. It transmits uncompressed high definition video and multiple-channel data to the HDMI port of the display device. HDMI version is 1.4.
6	USB port	USB port. Connect to mouse, USB storage device and etc.
7	ALARM I/O	They receive signals from external alarm source. C is COM port. There is one channel of alarm in; there are four channels of alarm out. When your alarm input device is using external power, make sure the device and the NVR have the same GND.
8	Power switch	Power on/off button.
9	AUDIO IN	Bidirectional talk input port. It is to receive the analog audio signal output from the devices such as microphone, pickup.
10	Power input port	Power socket.
11		GND

HN35040100N & HN35080100N

Figure 3 Front Panel (HN35040100N & HN35080100N)

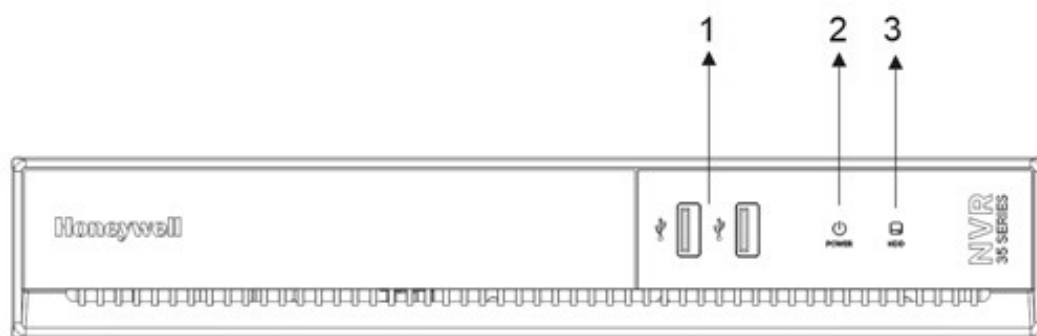


Table 4 NVR Front Panel Description (HN35040100N & HN35080100N)

No.	Name	Description
1	USB port	Connect to peripheral USB 2.0 storage device, mouse and so on.
2	POWER	The light is on when the power connection is OK.
3	HDD	The green light is flash when the device is recording, if the disk is not working, light is always bright. The light is off without disk.

Figure 4 Rear Panel (HN35040100N & HN35080100N)

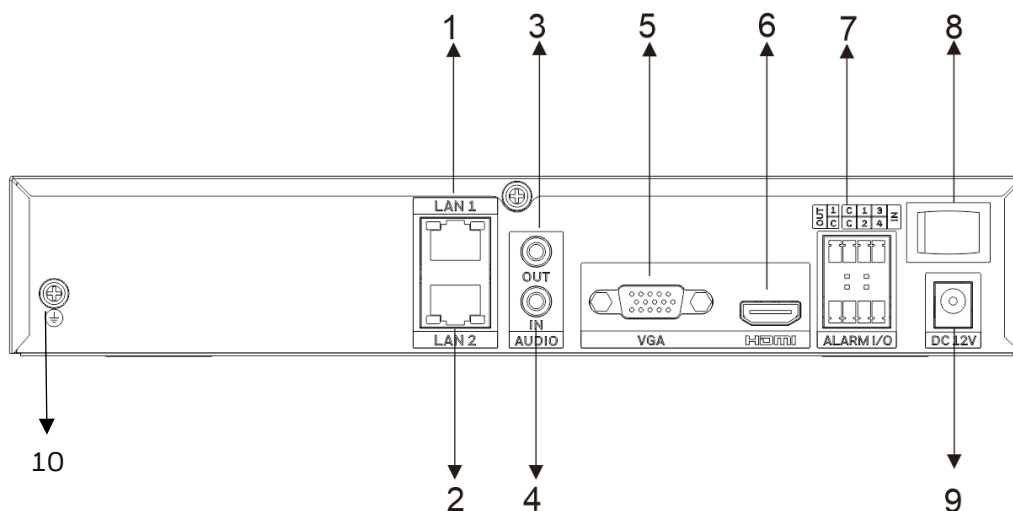


Table 5 NVR Rear Panel Description (HN35040100N & HN35080100N)

No.	Name	Description
1	LAN1	Network port. 10M/100Mbps self-adaptive Ethernet port. Connect to the network cable.
2	LAN2	Connect to the network cable, LAN2 port is only allowed to connect cameras, cannot to connect to Internet.
3	AUDIO OUT	Audio output port. It is to output the analog audio signal to the devices such as the sound box. - Bidirectional talk output. - Audio output on 1-window video monitor. Audio output on 1-window video playback.

No.	Name	Description
4	AUDIO IN	Bidirectional talk input port. It is to receive the analog audio signal output from the devices such as microphone, pickup.
5	VGA	VGA video output port. Output analog video signal. It can connect to the monitor to view analog video.
6	HDMI	High definition audio and video signal output port. It transmits uncompressed high definition video and multiple-channel data to the HDMI port of the display device. HDMI version is 1.4.
7	ALARM I/O	They receive signals from external alarm source. C is COM port. There is one channel of alarm in; There are four channels of alarm out. When your alarm input device is using external power, make sure the device and the NVR have the same GND.
8	Power switch	Power on/off button.
9	Power input port	Power socket.
10		GND

HN350802xx

Figure 5 Front Panel (HN350802xx)

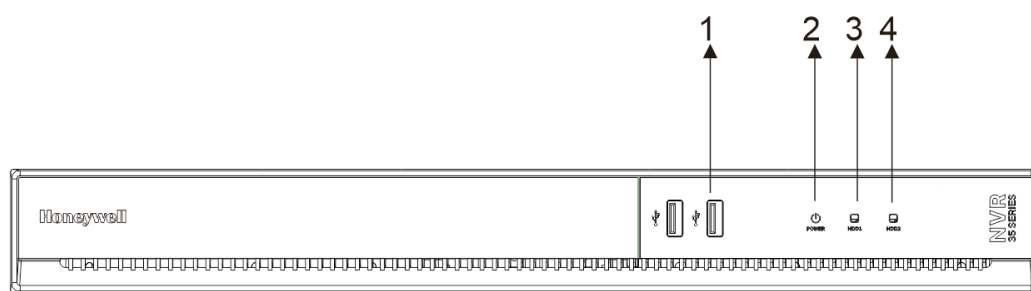


Table 6 NVR Front Panel Description (HN350802xx)

No.	Name	Description
1	USB port	Connect to peripheral USB 2.0 storage device, mouse and so on.
2	POWER	The light is on when the power connection is OK.
3-4	HDD1/HDD2	The green light is flash when the device is recording, if the disk is not working, light is always bright. The light is off without disk.

Figure 6 Rear Panel (HN350802xx)

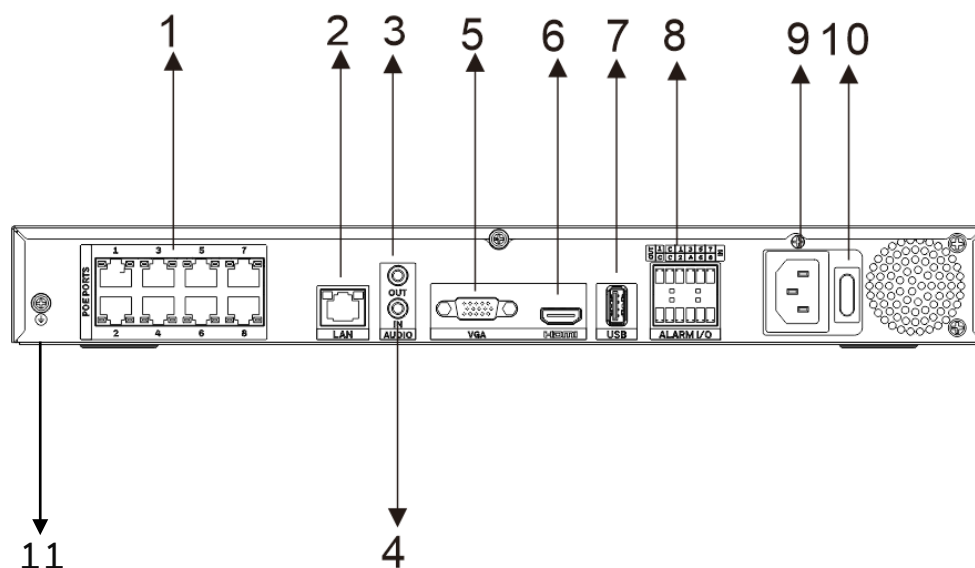


Table 7 NVR Rear Panel Description (HN350802xx)

No.	Name	Description
1	PoE port	Built-in switch. Support PoE function. For PoE series product, you can use this port to provide power to the network camera.
2	Network port	10M/100Mbps self-adaptive Ethernet port. Connect to the network cable.
3	AUDIO OUT	Audio output port. It is to output the analog audio signal to the devices such as the sound box. - Bidirectional talk output. - Audio output on 1-window video monitor. Audio output on 1-window video playback.
4	AUDIO IN	Bidirectional talk input port. It is to receive the analog audio signal output from the devices such as microphone, pickup.
5	VGA	VGA video output port. Output analog video signal. It can connect to the monitor to view analog video.
6	HDMI	High definition audio and video signal output port. It transmits uncompressed high definition video and multiple-channel data to the HDMI port of the display device. HDMI version is 1.4.
7	USB port	USB port. Connect to mouse, USB storage device and etc.
8	ALARM I/O	They receive signals from external alarm source. C is COM port. There is one channel of alarm in; There are eight channels of alarm out. When your alarm input device is using external power, make sure the device and the NVR have the same GND.
9	Power input port	Power socket.
10	Power switch	Power on/off button.
11		GND

HN351602xx

Figure 7 Front Panel (HN351602xx)

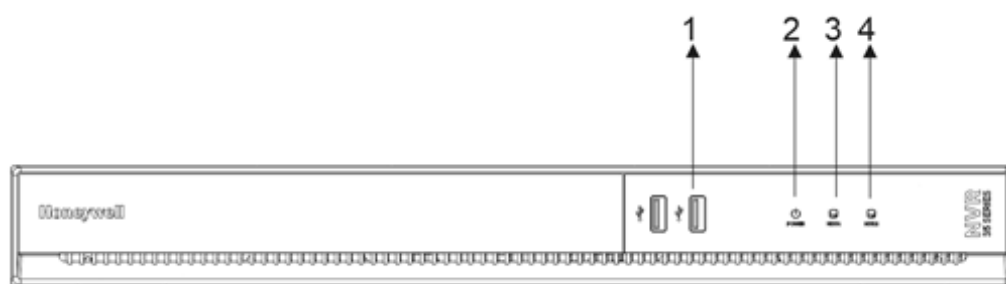


Table 8 NVR Front Panel Description (HN351602xx)

No.	Name	Description
1	USB port	Connect to peripheral USB 2.0 storage device, mouse and so on.
2	POWER	The light is on when the power connection is OK.
3-4	HDD1/HDD2	The green light is flash when the device is recording, if the disk is not working, light is always bright. The light is off without disk.

Figure 8 Rear Panel (HN351602xx)

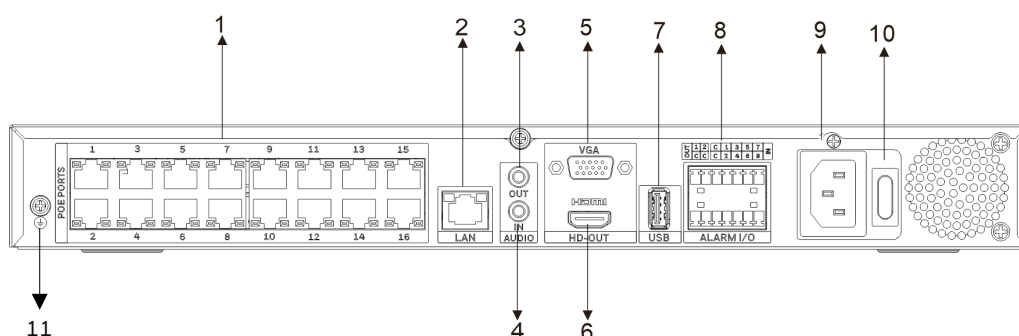


Table 9 NVR Rear Panel Description (HN351602xx)

No.	Name	Description
1	PoE port	Built-in switch. Support PoE function. For PoE series product, you can use this port to provide power to the network camera.
2	Network port	100M/1000Mbps self-adaptive Ethernet port. Connect to the network cable.
3	AUDIO OUT	Audio output port. It is to output the analog audio signal to the devices such as the sound box. - Bidirectional talk output. - Audio output on 1-window video monitor. Audio output on 1-window video playback.
4	AUDIO IN	Bidirectional talk input port. It is to receive the analog audio signal output from the devices such as microphone, pickup.
5	VGA	VGA video output port. Output analog video signal. It can connect to the monitor to view analog video.

No.	Name	Description
6	HDMI	High definition audio and video signal output port. It transmits uncompressed high definition video and multiple-channel data to the HDMI port of the display device. HDMI version is 1.4.
7	USB port	USB port. Connect to mouse, USB storage device and etc.
8	ALARM I/O	They receive signals from external alarm source. C is COM port. There is one channel of alarm in; There are eight channels of alarm out. When your alarm input device is using external power, make sure the device and the NVR have the same GND.
9	Power input port	Power socket.
10	Power switch	Power on/off button.
11		GND

HN350802xxC

Figure 9 Front Panel (HN350802xxC)

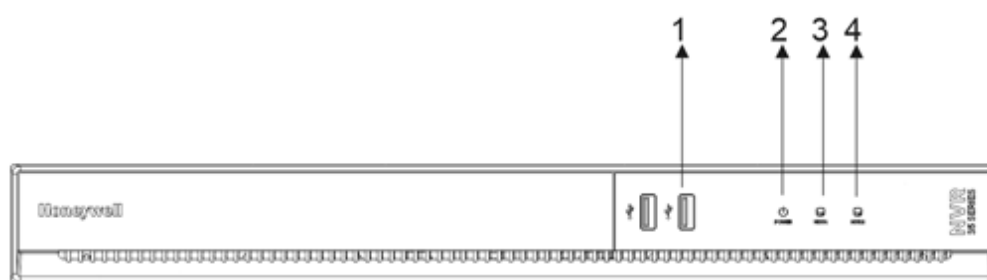


Table 10 NVR Front Panel Description (HN350802xxC)

No.	Name	Description
1	USB port	Connect to peripheral USB 2.0 storage device, mouse and so on.
2	POWER	The light is on when the power connection is OK.
3-4	HDD1/HDD2	The green light is flash when the device is recording, if the disks are not working, lights are always bright. The light is off without disk.

Figure 10 Rear Panel (HN350802xxC)

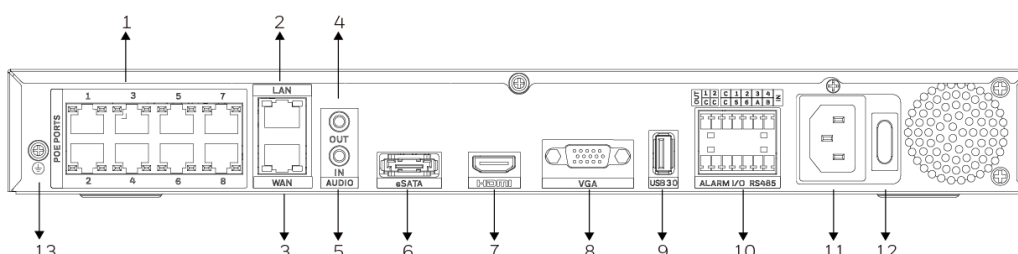


Table 11 NVR Rear Panel Description (HN350802xxC)

No.	Name	Description
1	PoE port	Built-in switch. Support PoE function. For PoE series product, you can use this port to provide power to the network camera.

No.	Name	Description
2~3	Network port	10M/100Mbps self-adaptive Ethernet port. Connect to the network cable.
4	AUDIO OUT	Audio output port. It is to output the analog audio signal to the devices such as the sound box. - Bidirectional talk output. - Audio output on 1-window video monitor. Audio output on 1-window video playback.
5	AUDIO IN	Bidirectional talk input port. It is to receive the analog audio signal output from the devices such as microphone, pickup.
6	eSATA	Hard disk port
7	HDMI	High definition audio and video signal output port. It transmits uncompressed high definition video and multiple-channel data to the HDMI port of the display device. HDMI version is 1.4.
8	VGA	VGA video output port. Output analog video signal. It can connect to the monitor to view analog video.
9	USB port	USB port. Connect to mouse, USB storage device and etc.
10	ALARM I/O	They receive signals from external alarm source. C is COM port. There is one channel of alarm in; There are eight channels of alarm out. When your alarm input device is using external power, make sure the device and the NVR have the same GND.
11	Power input port	Power socket.
12	Power switch	Power on/off button.
13		GND

HN351602xxC

Figure 11 Front Panel (HN351602xxC)

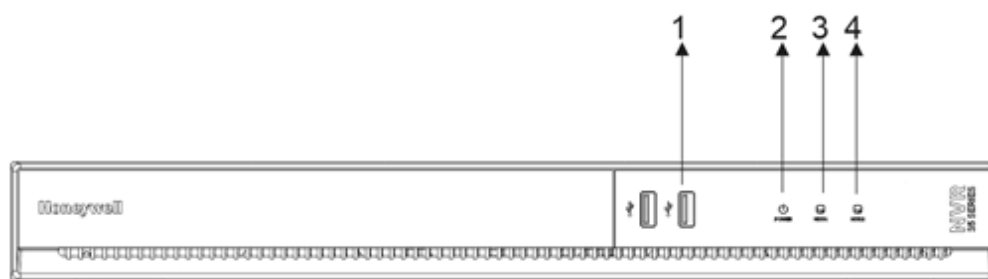


Table 12 NVR Front Panel Description (HN351602xxC)

No.	Name	Description
1	USB port	Connect to peripheral USB 2.0 storage device, mouse and so on.
2	POWER	The light is on when the power connection is OK.
3-4	HDD1/HDD2	The green light is flash when the device is recording, if the disks are not working, lights are always bright. The light is off without disk.

Figure 12 Rear Panel (HN351602xxC)

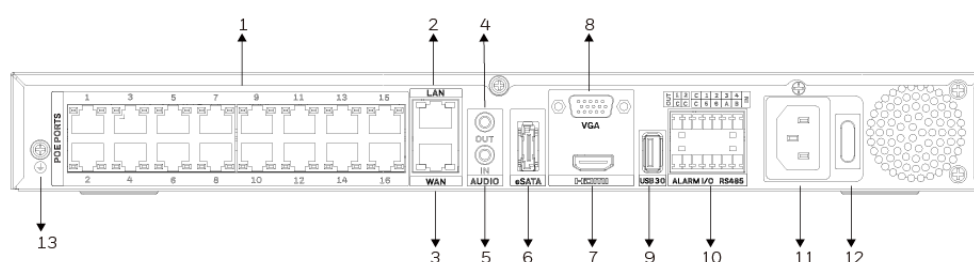


Table 13 NVR Rear Panel Description (HN350802xxC)

No.	Name	Description
1	PoE port	Built-in switch. Support PoE function. For PoE series product, you can use this port to provide power to the network camera.
2~3	Network port	10M/100Mbps self-adaptive Ethernet port. Connect to the network cable.
4	AUDIO OUT	Audio output port. It is to output the analog audio signal to the devices such as the sound box. - Bidirectional talk output. - Audio output on 1-window video monitor. Audio output on 1-window video playback.
5	AUDIO IN	Bidirectional talk input port. It is to receive the analog audio signal output from the devices such as microphone, pickup.
6	eSATA	Hard disk port
7	HDMI	High definition audio and video signal output port. It transmits uncompressed high definition video and multiple-channel data to the HDMI port of the display device. HDMI version is 1.4.
8	VGA	VGA video output port. Output analog video signal. It can connect to the monitor to view analog video.
9	USB port	USB port. Connect to mouse, USB storage device and etc.
10	ALARM I/O	They receive signals from external alarm source. C is COM port. There is one channel of alarm in; There are eight channels of alarm out. When your alarm input device is using external power, make sure the device and the NVR have the same GND.
11	Power input port	Power socket.
12	Power switch	Power on/off button.
13		GND

HN351604xxC/HN353204xx

Figure 13 Front Panel (HN351604xxC/HN353204xx)

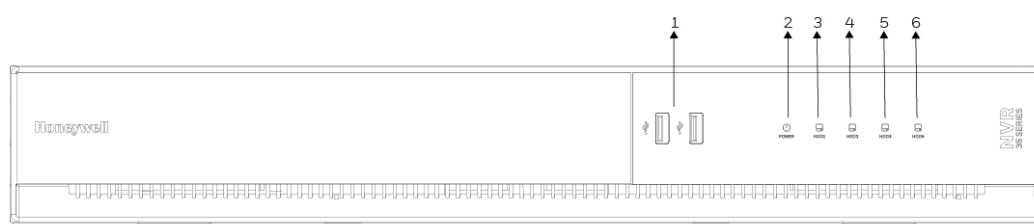


Table 14 NVR Front Panel Description (HN351604xxC/HN353204xx)

No.	Name	Description
1	USB port	Connect to peripheral USB 2.0 storage device, mouse and so on.
2	POWER	The light is on when the power connection is OK.
3~6	HDD1/HDD2/HDD3/HDD4	The green light is flash when the device is recording, if the disks are not working, lights are always bright. The light is off without disk.

Figure 14 Rear Panel (HN351604xxC/HN353204xx)

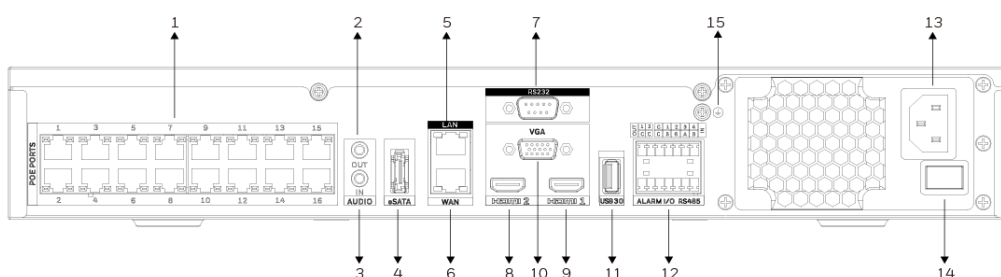


Table 15 NVR Rear Panel Description (HN351604xxC/HN353204xx)

No.	Name	Description
1	PoE port	Built-in switch. Support PoE function. For PoE series product, you can use this port to provide power to the network camera.
2	AUDIO OUT	Audio output port. It is to output the analog audio signal to the devices such as the sound box. - Bidirectional talk output. - Audio output on 1-window video monitor. Audio output on 1-window video playback.
3	AUDIO IN	Bidirectional talk input port. It is to receive the analog audio signal output from the devices such as microphone, pickup.
4	eSATA	Hard disk port
5~6	Network port	10M/100Mbps self-adaptive Ethernet port. Connect to the network cable.
7	RS232	RS232 port

No.	Name	Description
8~9	HDMI 2/ HDMI 1	High definition audio and video signal output port. It transmits uncompressed high definition video and multiple-channel data to the HDMI port of the display device. HDMI version is 1.4.
10	VGA	VGA video output port. Output analog video signal. It can connect to the monitor to view analog video.
11	USB port	USB port. Connect to mouse or USB storage device.
12	ALARM I/O	They receive signals from external alarm source. C is COM port. There is one channel of alarm in; There are eight channels of alarm out. When your alarm input device is using external power, make sure the device and the NVR have the same GND.
13	Power input port	Power socket.
14	Power switch	Power on/off button.
15		GND

HN35160200N

Figure 15 Front Panel (HN35160200N)

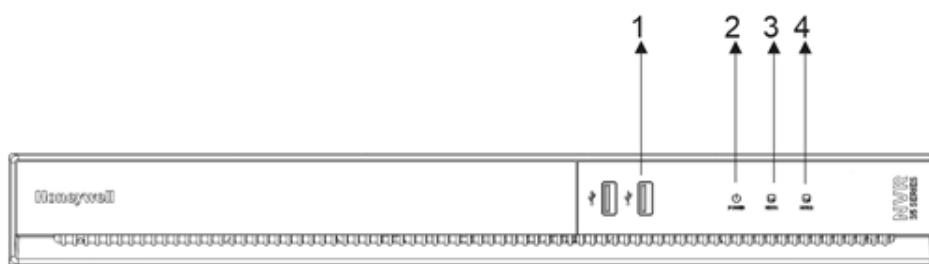


Table 16 NVR Front Panel Description (HN35160200N)

No.	Name	Description
1	USB port	Connect to peripheral USB 2.0 storage device, mouse and so on.
2	POWER	The light is on when the power connection is OK.
3~4	HDD1/HDD2	The green light is flash when the device is recording, if the disks are not working, lights are always bright. The light is off without disk.

Figure 16 Rear Panel (HN35160200N)

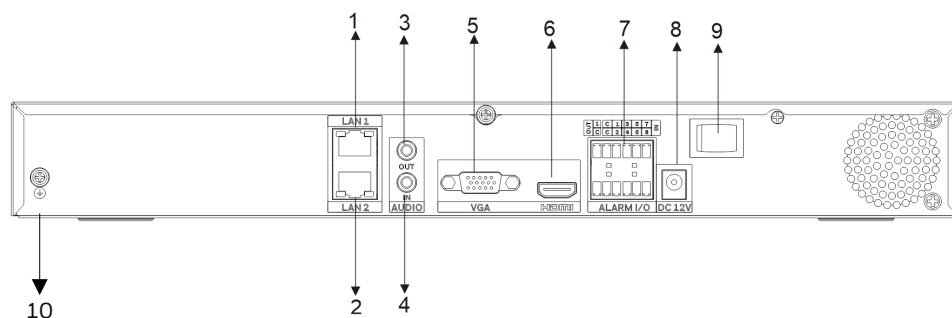


Table 17 NVR Rear Panel Description (HN35160200N)

No.	Name	Description
1	LAN1	Network port. 10M/100Mbps self-adaptive Ethernet port. Connect to the network cable.
2	LAN2	Connect to the network cable, LAN2 port is only allowed to connect cameras, cannot to connect to Internet.
3	AUDIO OUT	Audio output port. It is to output the analog audio signal to the devices such as the sound box. - Bidirectional talk output. - Audio output on 1-window video monitor. Audio output on 1-window video playback.
4	AUDIO IN	Bidirectional talk input port. It is to receive the analog audio signal output from the devices such as microphone, pickup.
5	VGA	VGA video output port. Output analog video signal. It can connect to the monitor to view analog video.
6	HDMI	High definition audio and video signal output port. It transmits uncompressed high definition video and multiple-channel data to the HDMI port of the display device. HDMI version is 1.4.
7	ALARM I/O	They receive signals from external alarm source. C is COM port. There is one channel of alarm in; There are eight channels of alarm out. When your alarm input device is using external power, make sure the device and the NVR have the same GND.
8	Power input port	Power socket.
9	Power switch	Power on/off button.
10		GND

N35320400N

Figure 17 Front Panel (HN35320400N)



Table 18 NVR Front Panel Description (HN35320400N)

No.	Name	Description
1	USB port	Connect to peripheral USB 2.0 storage device, mouse and so on.
2	POWER	The light is on when the power connection is OK.
3~6	HDD1/HDD2/ HDD3/HDD4	The green light is flash when the device is recording, if the disks are not working, lights are always bright. The light is off without disk.

Figure 18 Rear Panel (HN35320400N)

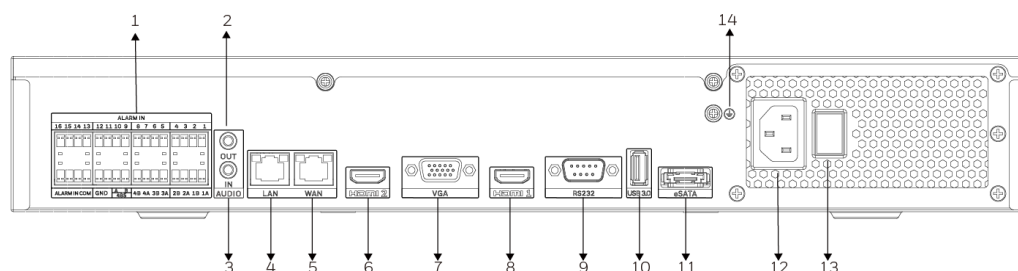


Table 19 NVR Rear Panel Description (HN35320400N)

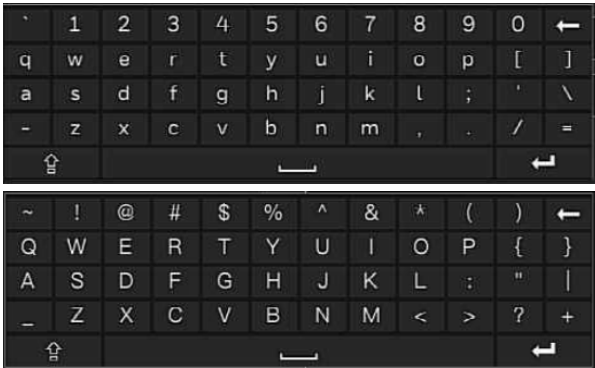
No.	Name	Description
1	Alarm Input/Output	They receive signals from external alarm source. C is COM port. There is one channel of alarm in; There are eight channels of alarm out. When your alarm input device is using external power, make sure the device and the NVR have the same GND.
2	AUDIO OUT	Audio output port. It is to output the analog audio signal to the devices such as the sound box. - Bidirectional talk output. - Audio output on 1-window video monitor. Audio output on 1-window video playback.
3	AUDIO IN	Bidirectional talk input port. It is to receive the analog audio signal output from the devices such as microphone, pickup.
4~5	Network port	10M/100Mbps self-adaptive Ethernet port. Connect to the network cable.
6	HDMI 2	High definition audio and video signal output port. It transmits uncompressed high definition video and multiple-channel data to the HDMI port of the display device. HDMI version is 1.4.
7	VGA	VGA video output port. Output analog video signal. It can connect to the monitor to view analog video.
8	HDMI 1	High definition audio and video signal output port. It transmits uncompressed high definition video and multiple-channel data to the HDMI port of the display device. HDMI version is 1.4.
9	RS232	RS232 port
10	USB port	USB port. Connect to mouse or USB storage device.
11	eSATA	Hard disk port
12	Power input port	Power socket.
13	Power switch	Power on/off button.

No.	Name	Description
14		GND

Mouse Operation

Refer to the following sheet for mouse operation instruction.

Table 20 Mouse Operation Instruction

Operation	Description
Left click mouse	When you have selected one menu item, left click mouse to view menu content.
	Modify checkbox or motion detection status.
	Click combo box to pop up drop-down list
	In input box, you can select input methods. Left click the corresponding button on the panel you can input numeral/English character (lower case/upper case).  stands for space button,  stands for deleting the previous character.  switch the case and special character, as shown in figure. 
Double left click mouse	Implement special control operation such as double click one item in the file list to playback the video.
	In multiple-window mode, double left clicks one channel to view in full-window. Double left clicks current video again to go back to previous multiple-window mode.
Right click mouse	In real-time monitor mode, goes back to home menu.
	Exit current menu without saving the modification.
Slide middle button	Switch the items in the check box, such as switch languages.
	Page up or page down, such as add cameras.
Move mouse	Select current control or move control.
Drag mouse	Select motion detection zone/ intelligent analysis zone.
	Select schedule manually.
	Select privacy mask zone.

GETTING STARTED

This chapter contains the following sections:

- [Unpacking the NVR](#), page 17
- [Connecting External Devices](#), page 17
- [Starting and Shutting Down the NVR](#), page 21
- [Device Initialization](#), page 23
- [Device Wizard](#), page 25
- [Resetting Password](#), page 30
- [Home Page](#), page 31
- [Mute Buzzer](#), page 32
- [Two-way Talk](#), page 33

Unpacking the NVR

Before you set up the NVR, make sure that you have received the following items:

- | | |
|--|---|
| • Quick Installation Guide | • Power adapter and cable |
| • Quick Certificate Installation Guide | • Terminal block connectors (The actual product shall prevail.) |
| • Mouse | • Screws |

If any of the items listed above are missing or damaged, contact your Honeywell dealer immediately.

Connecting External Devices

1. Connect the cameras

Connect the network cables from the cameras to the PoE port (The NVR need to support PoE port) or router.

Note: *The router cannot be directly connected to the PoE port.*

2. Connect the monitor

Connect a VGA cable (not supplied) to the VGA interface and/or an HDMI cable (not supplied) to the HDMI interface. Connect the other end to a monitor (do not use a TV). Simultaneous VGA and HDMI output is supported.

3. Connect the mouse

Connect the supplied USB mouse to the USB 2.0 interface.

4. Connect the Ethernet cable

Connect the supplied CAT5e Ethernet cable to the network port. Connect the other end to a router on your network.

5. Connect audio devices (if applicable)

To record audio, connect the audio sources to the AUDIO IN connectors. To play audio, connect an audio output device (low-impedance headphones, speaker, or amplifier) to the AUDIO OUT connector.

6. Connect alarm devices (if applicable)

Connect alarm devices to the alarm in/out interface. If the alarm inputs use external power, the device must have the same ground as the NVR.

7. Connect a PTZ camera (if applicable)

Your embedded NVR communicates with PTZ cameras through the Network. Ensure that your camera is correctly connected to the Network.

8. Connect the power cable

Connect the supplied 12 V DC (Depend on models, DC12V(3A) /DC 52V /AC 220V please refer to actual product) power adapter to the power input. Use of an uninterruptible power supply (UPS) is strongly recommended.

Devices Connection

The following diagram shows a typical NVR connection:

Figure 19 Devices Connection (HN350401xx)

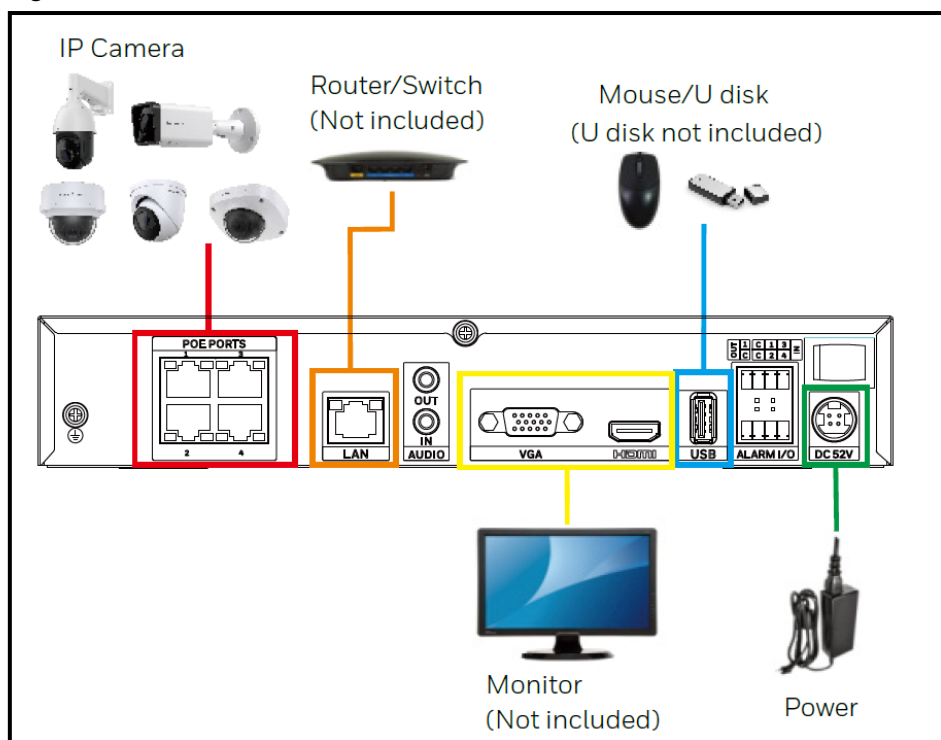


Figure 20 Devices Connection (HN35040100N/HN35080100N)

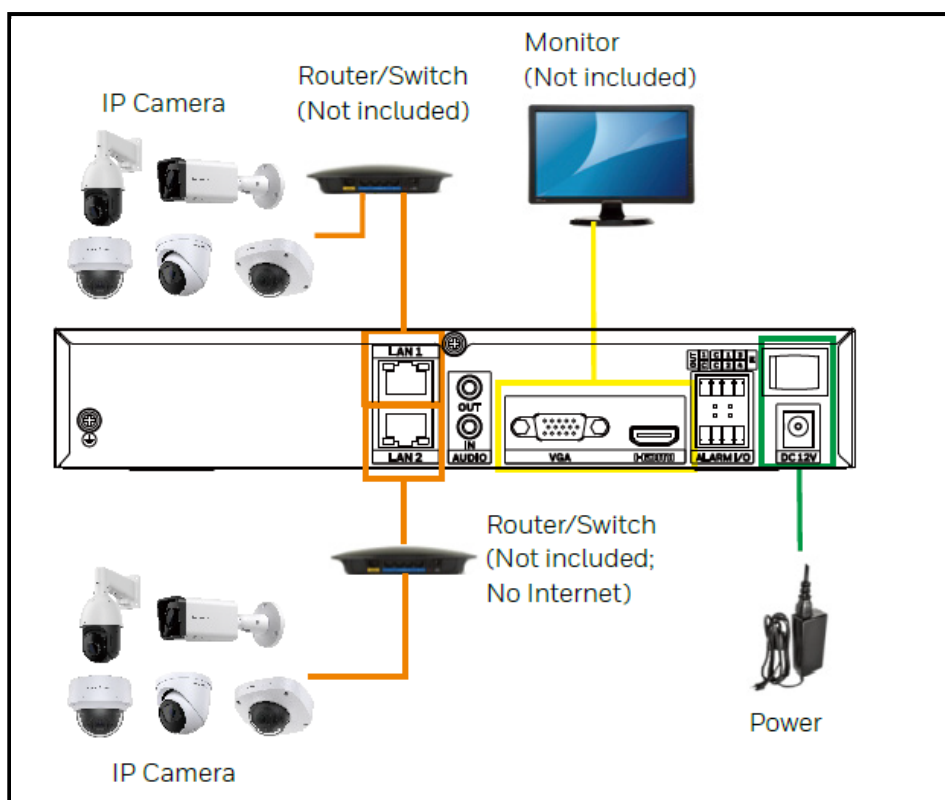


Figure 21 Devices Connection (HN350802xx)

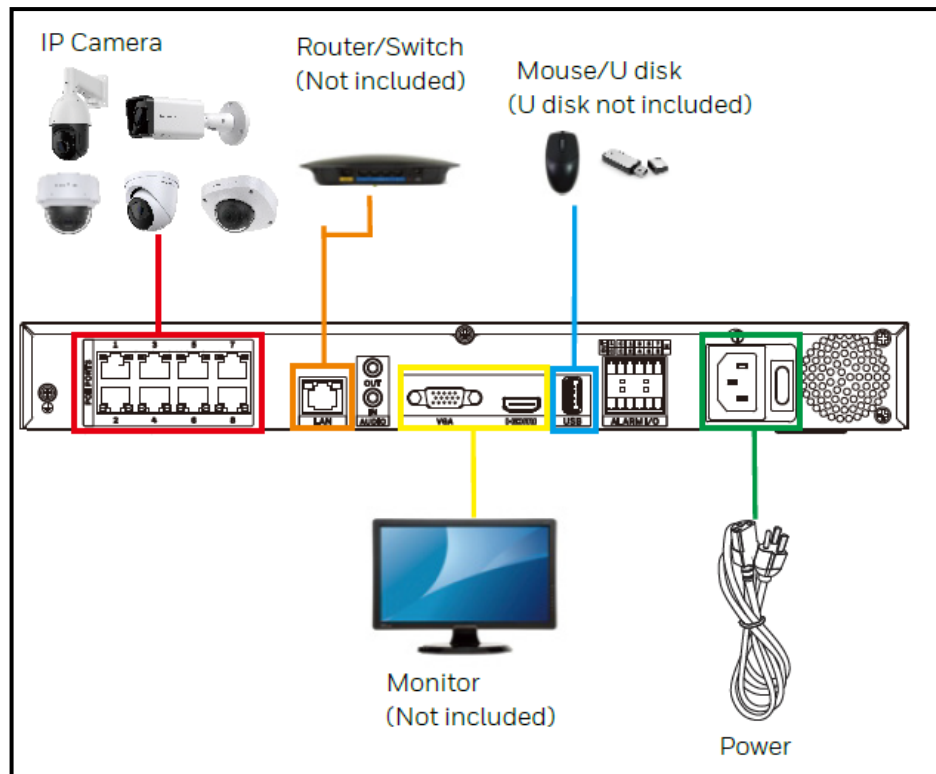


Figure 22 Devices Connection (HN351602xx)

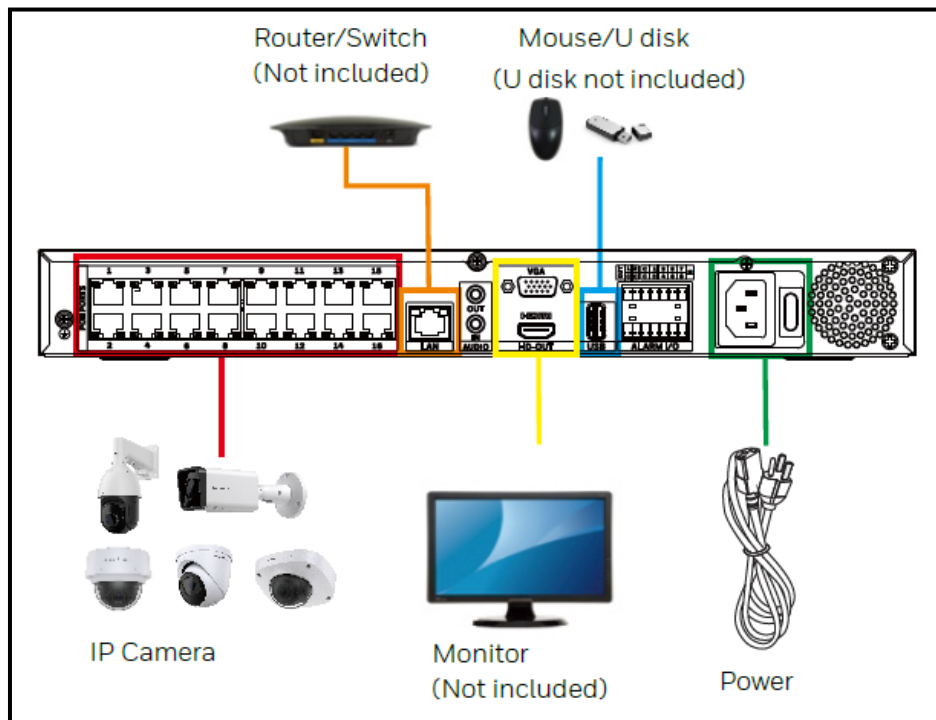
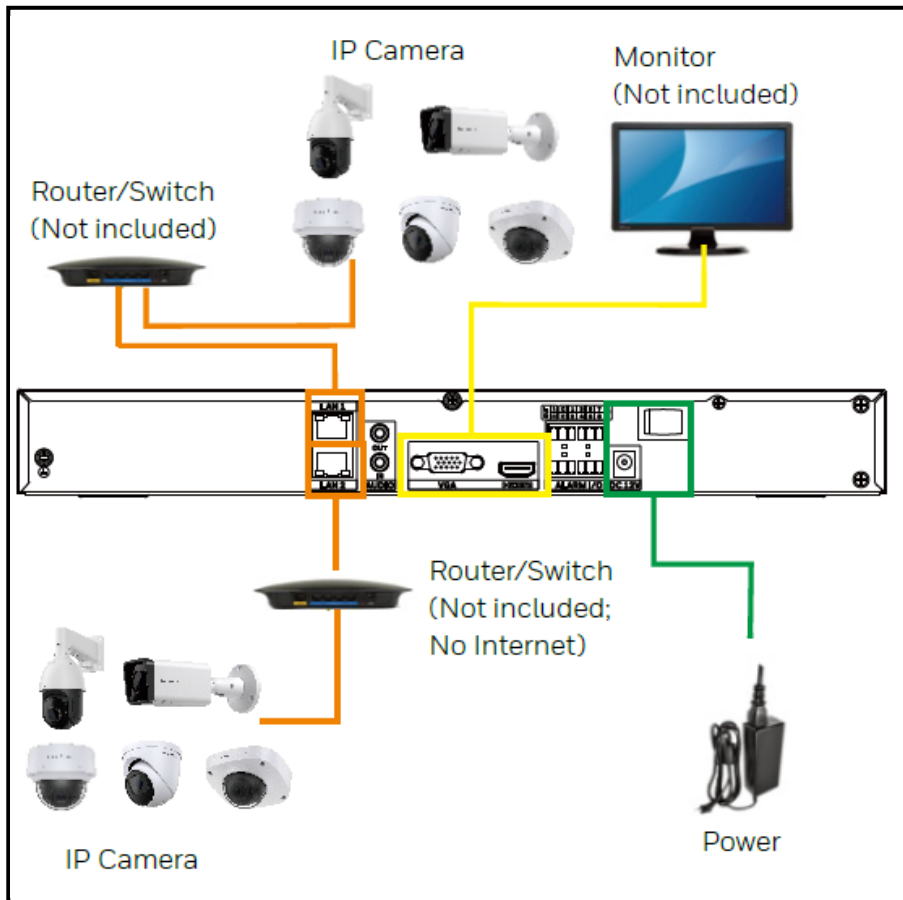


Figure 23 Devices Connection (HN35160200N)



Starting and Shutting Down the NVR

Starting the NVR

1. Make sure that the NVR is connected to an appropriate power source.
2. Turn on the power switch on the rear panel to start the NVR.

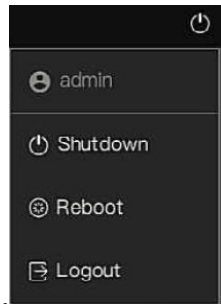
Note: The beep at startup is normal.

Shutting Down the NVR

Note: To shut down the NVR, you must be logged in as the admin user or have shutdown privileges assigned to you.

To prevent damage to the hard drive, follow these steps to shut down the NVR:

1. In live view mode, right-click anywhere on the screen to display Main Menu. Or click home menu icon at bottom of live view page to enter the Main Menu page.
2. Go to Main Menu > System > Maintenance, click Shutdown. Or click  in the upper right corner and click Shutdown.



3. In the Shutdown window, click OK.

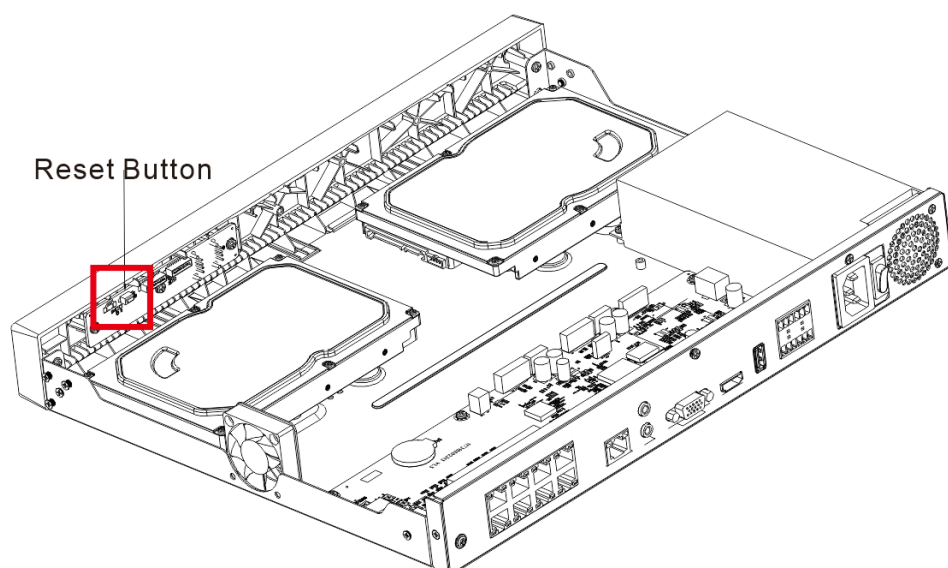
Reset Button

You can use the reset button on the light PCB board to reset the device to the factory default settings.

1. Disconnect the device from power source, and then remove the cover panel.
2. Find the reset button on the light PCB board.
3. Connect the device to the power source again and long press the reset button for 5 to 10 seconds.

The device restarts automatically.

Figure 24 Reset Button



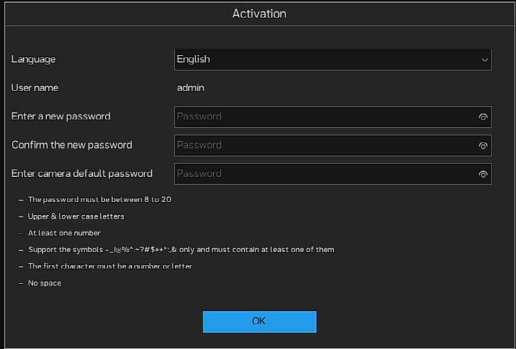
After the device is restarted, the settings have been restored to the factory default. You can start resetting the password.

Device Initialization

- If it is your first time to use the device, set a login password of admin (system default user) and a channel default password. You can select to use unlock pattern to login as needed.
- Input the ask to recovery the password, there are many questions you can choose three questions to ask.
- For your device safety, keep your login password of admin well after the initialization steps, and change the password regularly.

1. Activate NVR.

Figure 25 Device Activation



The screenshot shows a 'Device Activation' window with the following fields and options:

- Language:** A dropdown menu set to 'English'.
- User name:** A text field containing 'admin'.
- Enter a new password:** A password input field with a strength indicator icon.
- Confirm the new password:** A password input field with a strength indicator icon.
- Enter camera default password:** A password input field with a strength indicator icon.

Below the input fields, there are password requirements:

- The password must be between 8 to 20
- Upper & lower case letters
- At least one number
- Support the symbols "_!@%*~?&\$+~&" only and must contain at least one of them
- The first character must be a number or letter
- No space

An 'OK' button is located at the bottom right of the window.

- ### 2. Answer question to recover password. When you forget the password, answer the setting question to enter the password resetting page.

Note: If you don't want to set the question, you can skip the steps and the login window will not show the Forget password button. Honeywell recommends user to set the questions in case you forget the password.

Figure 26 Question (Recovery the Password)

Question (Recovery The Password)

Question one: What was your childhood nickname? ✓

Question one answer: [Input field]

Question two: In what city or town was your first job? ✓

Question two answer: [Input field]

Question three: What is your best friend's birthday month and year? ✓

Question three answer: [Input field]

– Please enter at least 1 characters for the answer
– Please enter up to 32 characters for the answer

SKIP THIS STEP OK

3. Set the Unlock Pattern.

Figure 27 Set Unlock Pattern

Unlock Pattern

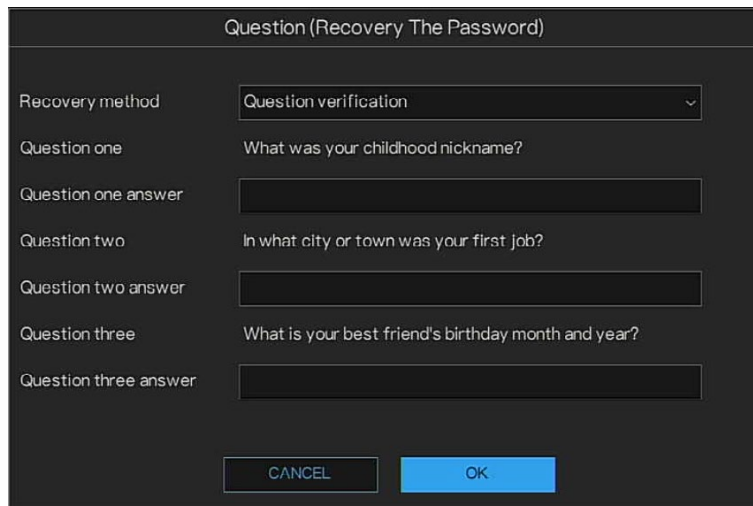
Please draw a pattern

REDRAW SKIP THIS STEP OK

After setting **Question (Recovery Password)**, the **Unlock Pattern** interface is displayed

- If you do not want to configure the unlock pattern, click **SKIP THIS STEP**.
- Once you have configured the unlock pattern, the system will require the unlock pattern as the default login method. If you skip this setting, enter the password for login.

Figure 28 Recover the Password



Question (Recovery The Password)

Recovery method: Question verification

Question one: What was your childhood nickname?

Question one answer:

Question two: In what city or town was your first job?

Question two answer:

Question three: What is your best friend's birthday month and year?

Question three answer:

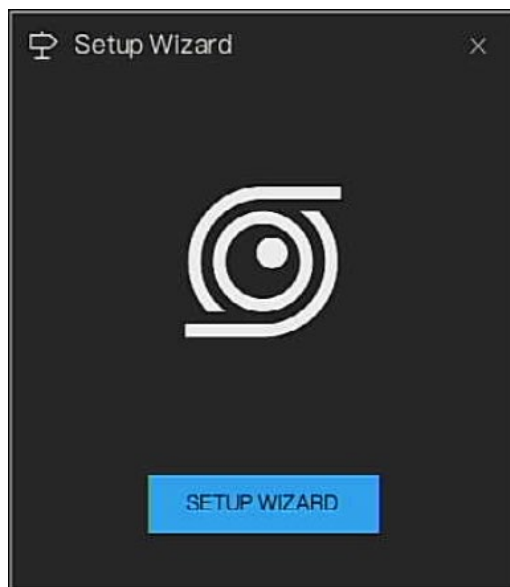
CANCEL OK

After answering three questions correctly, you can enter the reset password window.

Device Wizard

After the device initialization, the **Setup Wizard** opens.

Figure 29 Startup Wizard



Using the wizard, you can:

- Configure the network settings
- Configure date and time, time zone DST
- Configure P2P
- Search for and add IP cameras
- Configure Disk Manager

- Set resolution
1. Click SETUP WIZARD in the Setup Wizard window. Set Network according to the actual environment on the Network page, and then click Next.

Figure 30 Network

Setup Wizard

Networks

DHCP	☒
IP address	192 . 168 . 0 . 121
Subnet mask	255 . 255 . 255 . 0
Default gateway	192 . 168 . 0 . 1
Obtain DNS automatically	☒
Preferred DNS server	192 . 168 . 0 . 1
Alternate DNS server	8 . 8 . 8 . 8
Enable port mapping	☒
Mode	Auto
HTTP port	80
HTTPS port	443
Control port	30143

NEXT

2. Set Date and Time, Time Zone, DST according to actual environment, and then click Next.

Figure 31 Setup Wizard – Date and Time

Setup Wizard

Date And Time Time Zone DST

Date format	DD/MM/YY hh:mm:ss
Time format	24H
Enable NTP	☒
NTP server	time.windows.com
Sync time frequency (sec)	86400
Date	28/02/2022
Time	09:23:59

UPDATE TIME

PREVIOUS NEXT

Figure 32 Setup Wizard –Time Zone

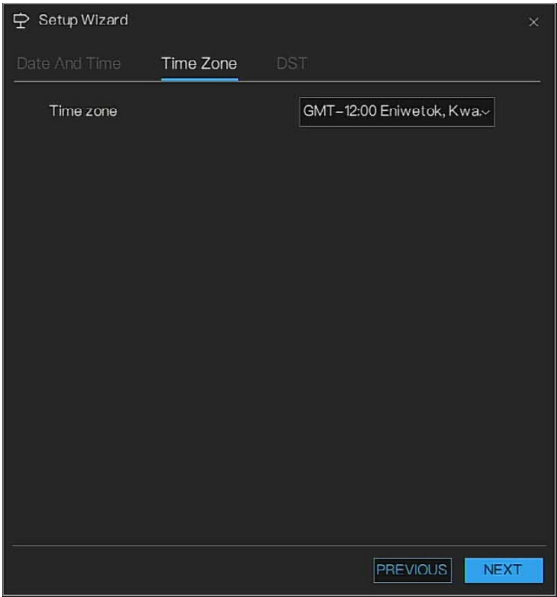
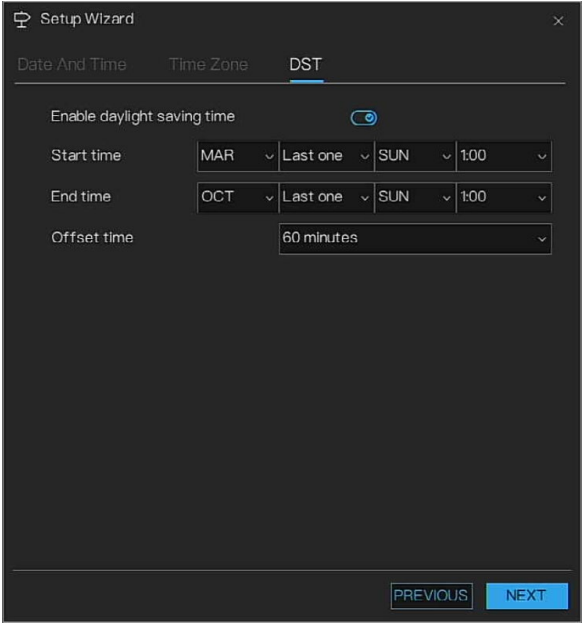


Figure 33 Setup Wizard –DST



3. Set Camera information.

Figure 34 Setup Wizard –Camera

Setup Wizard

Camera

☐	CHANN.	IP	MODEL	PROTOCOL	OPERATE
☐	Ch1	---	---	--	
☒	Ch2	---	---	--	
☐	Ch3	---	---	--	
☐	Ch4	---	---	--	

☐	IP	MODEL	PROTOCOL	FIRMWARE VERSION
☐	192.168.32.12:80		ONVIF	
☐	192.168.7.98:80	HC35WB8R.	ONVIF	
☐	192.168.7.95:80	HC35WE6R.	ONVIF	
☐	192.168.7.88:80	HC35WB8R.	ONVIF	

User name Password

Click **NEXT** directly if camera is connected to NVR with plug and play.

Or click **START SEARCH** to search cameras. Select the searched cameras and enter the user name and password to add cameras. Set the TLS mode. Click **NEXT**.

4. Format the disk.

Figure 35 Setup Wizard – Disk

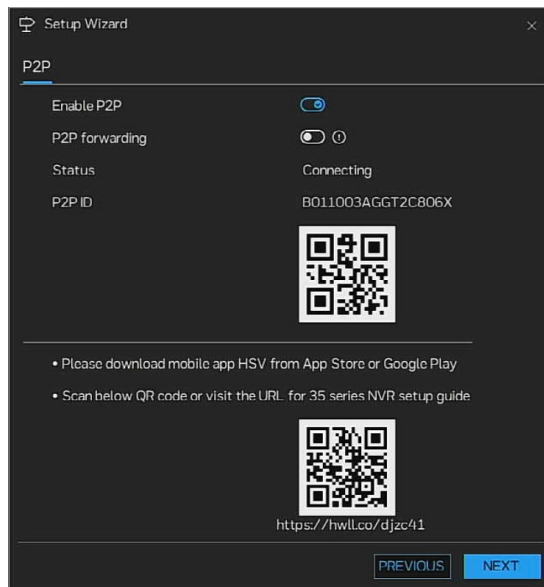
Setup Wizard

Disk

☐	DISK	CAPACIT.	USED	SN	DISK MODEL	STATUS
☐	Disk1	4 TB	0 MB	WD-WX62D31	WDC WD40EJ.	Format is n.
☐						
☐						
☐						
☐						
☐						
☐						

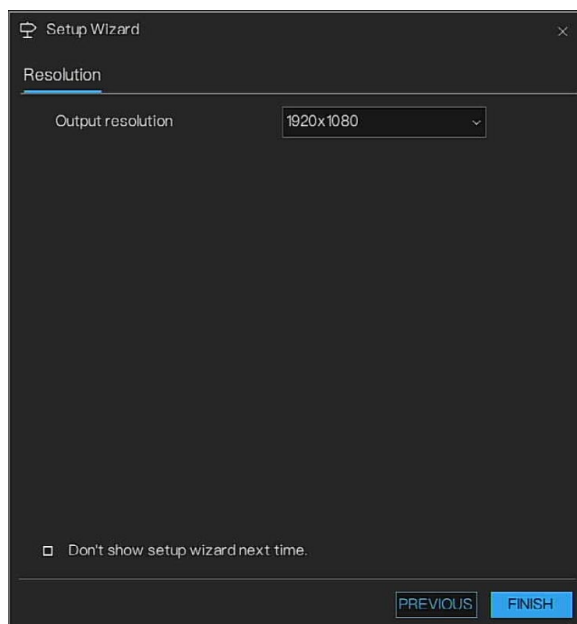
5. Click NEXT to view the P2P information. If the NVR is online, you can add the NVR to HSV by scanning the P2P ID.

Figure 36 Setup Wizard – P2P



6. Click NEXT. Set Resolution.

Figure 37 Setup Wizard – Resolution



Note: Check the checkbox for Don't show setup wizard next time, when users turn on the NVR enter Live view interface directly.

7. Click FINISH to save settings.

Resetting Password

If you forgot the admin password, you can reset the password by answering the security questions.

Note: To reset password by answering the security questions, you need configure this password resetting function in advance. Refer to [Device Initialization](#) or [Security Question](#).

Enabling Password Reset Function

1. Go to Main Menu > System > Security Center > Password.

The password reset interface is displayed.

Figure 38 Reset Password

The screenshot shows the 'Reset Password' interface in the Honeywell 35 Series Network Video Recorder's web interface. The interface is dark-themed. On the left is a sidebar with 'Setting' at the top, followed by 'Information', 'General', 'User Account', 'Security Center' (which is highlighted), 'Layout', 'Auxiliary Screen', 'Logs', and 'Maintenance'. The main content area has a top navigation bar with 'Camera', 'Storage', 'Events', 'Networks', 'System' (which is highlighted), and 'MAXPRO Cloud'. Below this is a sub-navigation bar with 'Password', 'Unlock Pattern', and 'Security Question'. The 'Password' tab is selected. It contains three input fields: 'Old password', 'New password', and 'Confirm password', each with a password icon. Below these fields are several password requirements: 'The password must be between 8 to 20', 'Upper & lower case letters', 'At least one number', 'Support the symbols ~, !, @, #, \$, %, ^, *, &, and must contain at least one of them', 'The first character must be a number or letter', and 'No space'. An 'APPLY' button is at the bottom right.

2. Input the old password, and create a new password and confirm it.
3. Click APPLY to set settings.

Resetting Password on Local Interface

1. Enter the Login interface.
 - If you have configured unlock pattern, the unlock pattern login interface is displayed. Click **Password**, the password login interface is displayed.
 - If you did not configure unlock pattern, the password login interface is displayed.
2. Click Forgot Password. Set the parameters according to the instruction on the pages.

Figure 39 Password Reset 1

Question (Recovery The Password)

Recovery method: Question verification

Question one: What was your childhood nickname?
Question one answer: [input field]

Question two: In what city or town was your first job?
Question two answer: [input field]

Question three: What is your best friend's birthday month and .
Question three answer: [input field]

CANCEL OK

3. Set new password.

In the New Password box, enter the new password and enter it again in the Confirm Password box.

Figure 40 Password Reset 2

Modify password

New password: Password [toggle]

Confirm password: Password [toggle]

Modify password

- The password must be between 8 to 20
- Upper & lower case letters
- At least one number
- Support the symbols - _ ! @ % ^ * - ? # \$ % + = , & only and must contain at least one of them
- The first character must be a number or letter
- No space

4. Click Modify password. The password resetting is complete.

Home Page

On live page, click  to enter home page, or right-click to enter home page directly.

Figure 41 Home Page (Without MAXPRO Cloud)

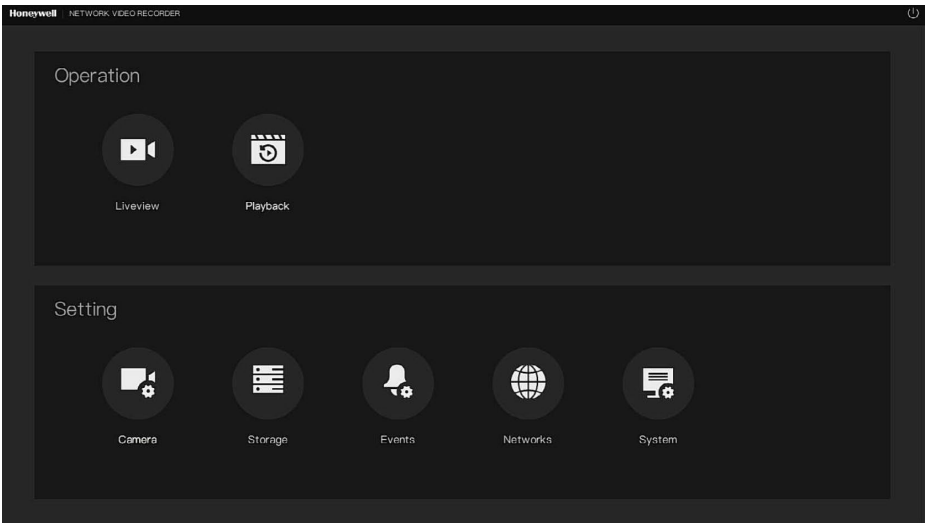
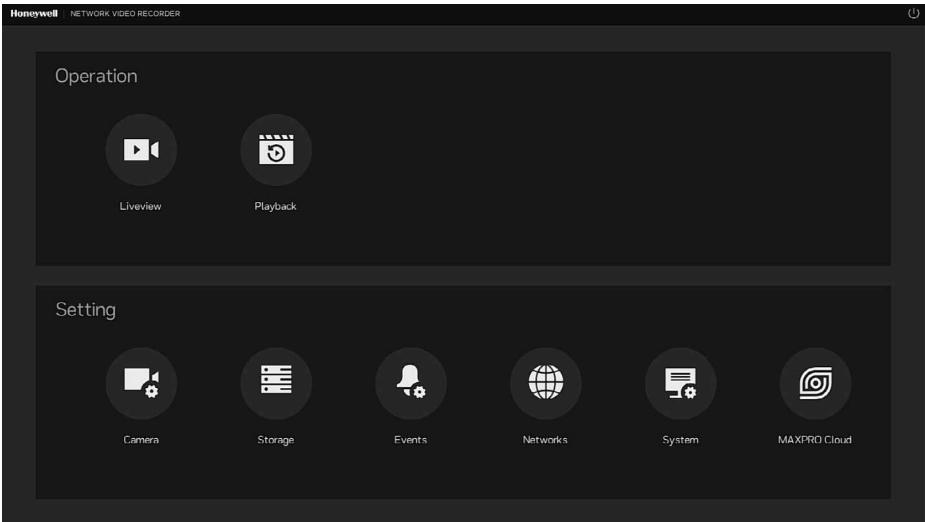


Figure 42 Home Page (With MAXPRO Cloud)



Mute Buzzer

On Setting interface, users can click  to mute the buzzer quickly when the buzzer is working.



Two-way Talk

Device-end to IPC

Please connect the speaker or the pickup to the first audio input port on the device rear panel. Then connect the earphone or the sound box to the audio output port in the IPC.

Click-left on live video, quick menu shows.

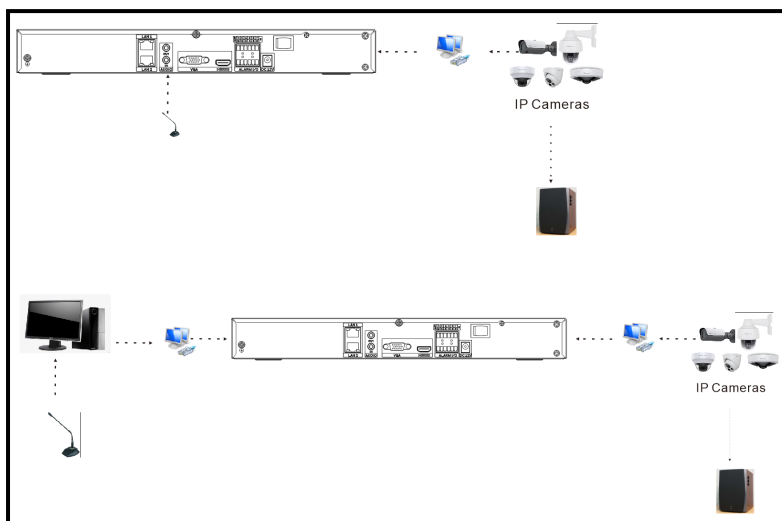
Figure 43 Enable Two-way Talk



Please refer to the following interface to enable two-way talk.

At the device end, speak by the speaker or the pickup, and then you can get the audio from the earphone or sound box at the IPC-end.

Figure 44 Device to IPC



IPC-end to the Device-end

Device Connection

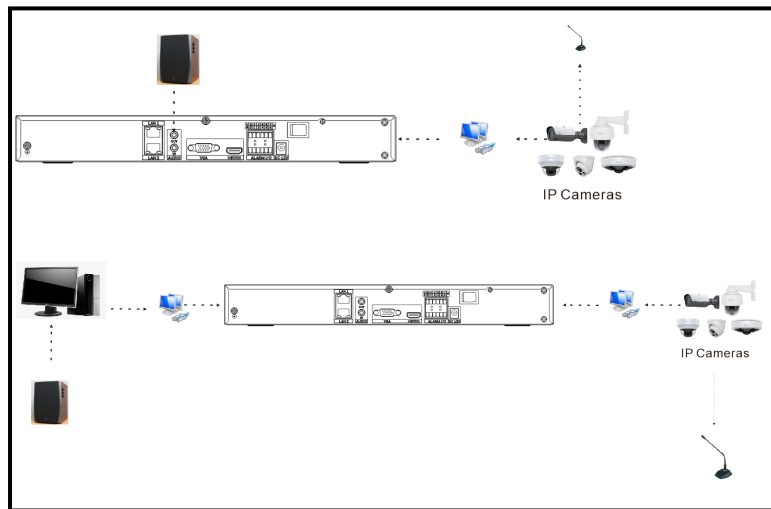
Connect the speaker or the pickup to the audio output port in the IPC and then connect the earphone or the sound box to the first audio input port in the device rear panel.

Login the Web and then enable the corresponding channel real-time monitor.

Listening Operation

At the IPC-end, speak by the speaker or the pickup, and then you can get the audio from the earphone or sound box at the device-end.

Figure 45 IPC to Device



LOCAL BASIC OPERATION

Note: Slight difference may be found on the user interface. The following figures are for reference only.

This chapter contains the following sections:

- [Configuring Camera](#), page 35
- [Configuring Storage Settings](#), page 45
- [Configuring Events Settings](#), page 53
- [Configuring Network Settings](#), page 68
- [Configuring System Settings](#), page 82
- [Configuring Live View Settings](#), page 100
- [Playback](#), page 106
- [Setting MAXPRO Cloud](#), page 111

Configuring Camera

Camera

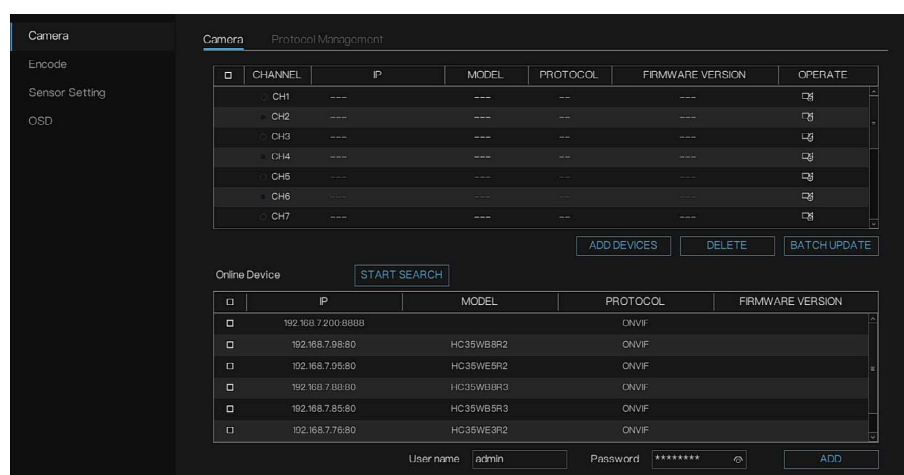
Adding Camera

When you connect a camera to the NVR via PoE port, NVR automatically initializes the camera. The NVR can activate and create new passwords for new cameras, the password is the same as the created channel password ([Figure 17 Device Activation](#)

By adding remote devices to the NVR, you can view the video on the NVR, and manage and storage the video file. Different series products support different remote device amount.

1. Go to Main Menu > Camera > Camera.

Figure 46 Add Camera



2. Add cameras.

a. Click START SEARCH.

The devices found are displayed at the upper pane. Devices already added do not show in the searched results.

b. Select the devices and click ADD Devices to register cameras on the online device list directly.

On the pop-up window, select YES/NO to use TLS connection or not for adding devices. If you use TLS connection, the total bitrate of all channels should be less than 40M. If the total bitrate exceeds 40M, the system will reminder “TLS bitrate exceeded” and you should choose NO for not using TLS on the pop-up window.

- Note:*
- The number of adding cameras should meet the captivity of NVR. When the cameras exceed the captivity, the channels will not be added.
 - The encrypted connection can support up to 40 Mbps. If the encrypted connection reaches 40 Mbps, the unencrypted connection can only support up to 40 Mbps.
 - The 30/60 series IP cameras cannot be connected to PoE port directly, you should set the password at IP cameras' web interface, and the password should be same as channel password of NVR.
 - Once the PoE cameras are added, they cannot be deleted manually at NVR UI interface. You can unplug the PoE network cables to delete.

Manually Add Devices

a. On the Channel list, click .

The Manually Add Devices interface is displayed.

Figure 47 Manually Add Devices

Manually Add Devices

CHANNEL	IP	PROTOCOL
CH1	192.168.32.144:80	ONVIF
CH2	192.168.32.123:80	ONVIF
CH3	192.168.32.58:80	ONVIF

Channel

10

IP address

Protocol

ONVIF

Port

0

User name

User name

Password

Password

Enable TLS

Unselected

RESET

CANCEL

OK

b. Configure parameters.

Table 21 Remote Channel Parameters

Parameter	Description
Channel	-
IP address	In the IP address box, enter the IP address of the remote device. The user can click the added channel to copy the channel information and then modify information, such as the remote channel.
Protocol	ONVIF /RTSP1-16
RTSP Port	The default value setting is 554. You can select the value according to your actual situation.
HTTP Port	The default value setting is 80. You can enter the value according to your actual situation. If you enter other value, for example 70, you should enter 70 after the IP address when logging in the device by browser.
User name	Enter the user name of the remote device.
Password	Enter the password of the user for the remote device.
Remote CH No.	Enter the remote channel number of the remote device that you want to add.

Parameter	Description
Enable TLS	If the remote device is added through the ONVIF protocol, enabling TLS will provide encryption protection to the data transmitted. Choose YES, the port will be 443; Choose NO, the port will be 80. To use this function, the HTTPS function should be enabled for the remote IP camera.

Note: Choose the protocol from the drop-down list, the protocol is set at protocol management interface. The cameras should be confirmed to the protocols.

c. Click OK.

The remote device information is displayed on the **Added Device** list.

You can click  to change the remote device information. Click  to delete remote device.

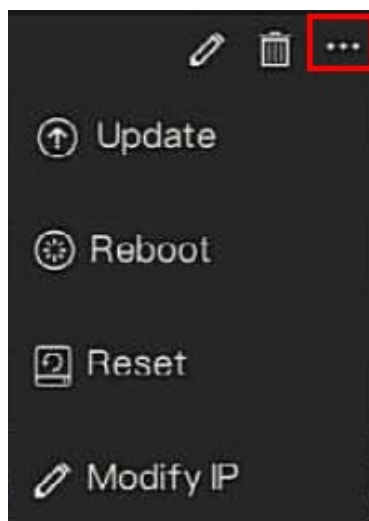
You can also add cameras on the live view interface by clicking  on the channel window.

UI local Update

You can upgrade the connected network camera firmware.

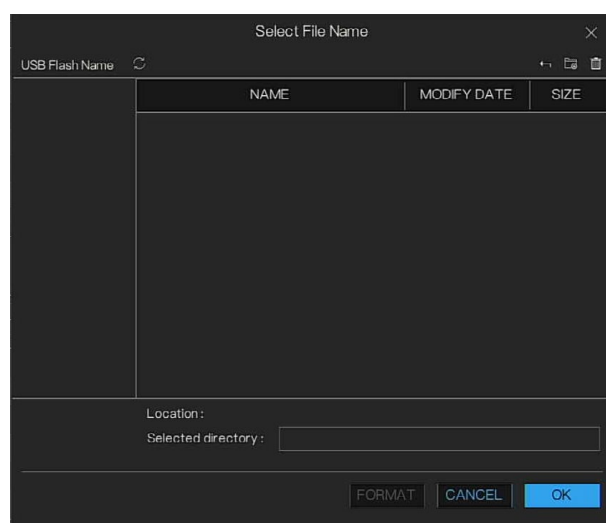
1. Plug in USB disk with the camera firmware.
2. Go to Main Menu > Camera > Camera. When the camera is online, click .

Figure 48 Update Interface



3. Update the firmware of the connected cameras.
 - a. Select update file on the pop-up interface.

Figure 49 Select File



- b. Select the update file and then click OK.

After successful operation, system prompts update successful dialogue box.

If there are too many same model cameras, select the cameras as needed, and click **BATCH UPDATE**. Choose firmware file in the pop-up interface.

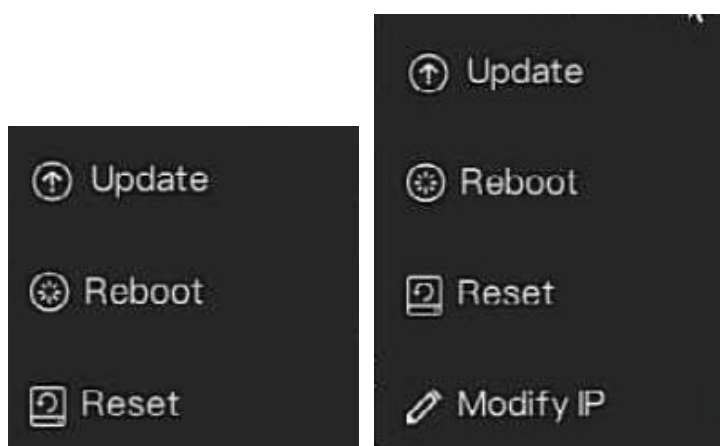
If you want to update the cameras remotely and the NVR can be accessed by Web, you can update cameras at remote port.

For cameras connected with NVR by non-PoE port, select the camera(s) on channel list and click **DELETE** to delete cameras in batch. Or click  to delete the selected cameras. Cameras added by PoE port of NVR cannot be delete here.

Operating online channel

1. Go to Main Menu > Camera > Camera. When the camera is online, click .
2. Click Update/Reboot/Reset to configure the cameras. For remote network added cameras, you can click Modify IP to set the IP information.

Figure 50 Operating Online Channel



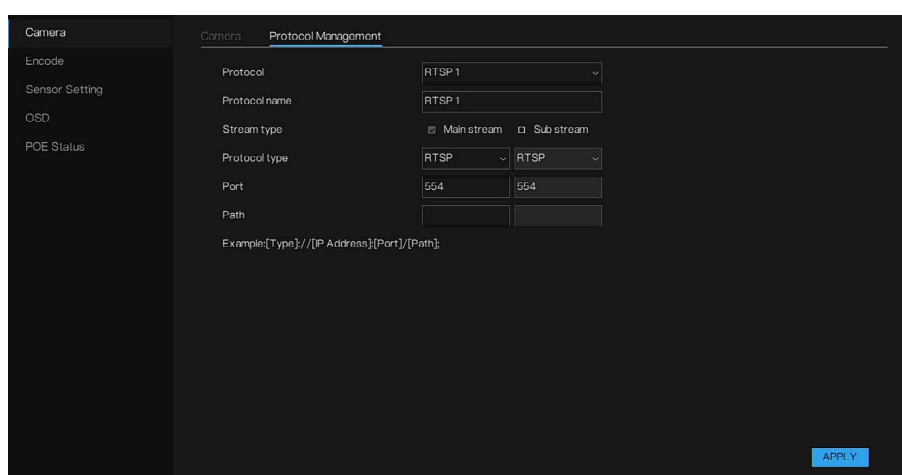
- Click Update to update the camera information.
- Click Reboot. In the pop-up window “Are you sure reboot”, click OK to reboot the camera.
- Click Reset. Enable or disable Reserve IP address. Click OK to reboot the camera.
- Click Modify IP. Enter the IP address and Subnet mask Click OK.

Protocol Management

If the user wants to add the different protocol cameras to NVR, you can set the protocol management, and add cameras one by one.

1. Go to Main Menu > Camera > Camera > Protocol Management. The Protocol Management interface is displayed.

Figure 51 Protocol Management



2. Choose the custom protocol from the drop-down list.
3. Input the protocol name.
4. Select main stream and sub stream. The main stream shows image on full screen live video. The sub stream shows image on split screen. If you only select main stream, the channel will not show image on split screen.

5. Choose the type of protocol. The default value is RTSP. Input the port which depends on the IP camera.
6. Input the path, it depends on the manufacturer of cameras.
7. Click APPLY to save the settings.

Encode

You can set video bit stream parameters such as video format, resolution, frame rate(fps), and so on.

Note: Some series products support three streams: main stream, sub stream 1, sub stream 2. The sub stream maximally supports 1080p.

1. Go to Main Menu > Camera > Encode.

The Encode interface is displayed.

Figure 52 Encode

Stream information	Main stream	Sub stream
Video format	H264	H264
Resolution	2560x1920	640x480
Frame rate(fps)	30	30
I frame interval(frame)	30	60
Bitrate type	VBR	CBR
Bitrate(kbps)	4000	2048
Quality	High	
Smart encode	☒	

2. Configure parameters.

Note: If you modify the Video format and Resolution, the device needs about 10 seconds to go online again and other operations during this period may result in failure for getting parameters.

Table 22 Audio/Video Parameters

Parameter	Description
Channel	In the Channel list, select the channel that you want to configure the settings for.

Parameter	Description
Smart encode	Enable the smart encode function to reduce the video bit stream for non-important recorded video to maximize the storage space. For some models, smart encode can be set for sub stream.
Video format	In the Compression list, select the encode mode. H.265: Main profile encoding. This setting is recommended. H.264: Main profile encoding.
Resolution	In the Resolution list, select resolution for the video. The maximum video resolution might be different dependent on your device model.
Frame rate (fps)	Configure the frames per second for the video. The higher the value is, the clearer and smoother the image will become. Frame rate changes along with the resolution. Generally, in PAL format, you can select the value from 1 through 25; in NTSC format, you can select the value from 1 through 30. However, the actual range of frame rate that you can select depends on the capability of the device. The NVR supports up to 30 fps, if the adding cameras' capability are over 30 fps, the NVR will degrade them to 30 fps.
I frame interval(frame)	The interval between two reference frames.
Bitrate type	In the Bit Rate Type list, select CBR (Constant Bit Rate) or VBR (Variable Bit Rate). If you select CBR , the image quality cannot be configured; if you select VBR , the image quality can be configured.
Bitrate(kbps)	Indicates the maximum value of the bit rate. You can input the value which can't be bigger than the biggest value from drop-down list), otherwise the value is invalid. Or you can choose value from drop-down list.
Quality	This function is available if you select VBR in the Bit Rate List. The bigger the value is, the better the image will become.

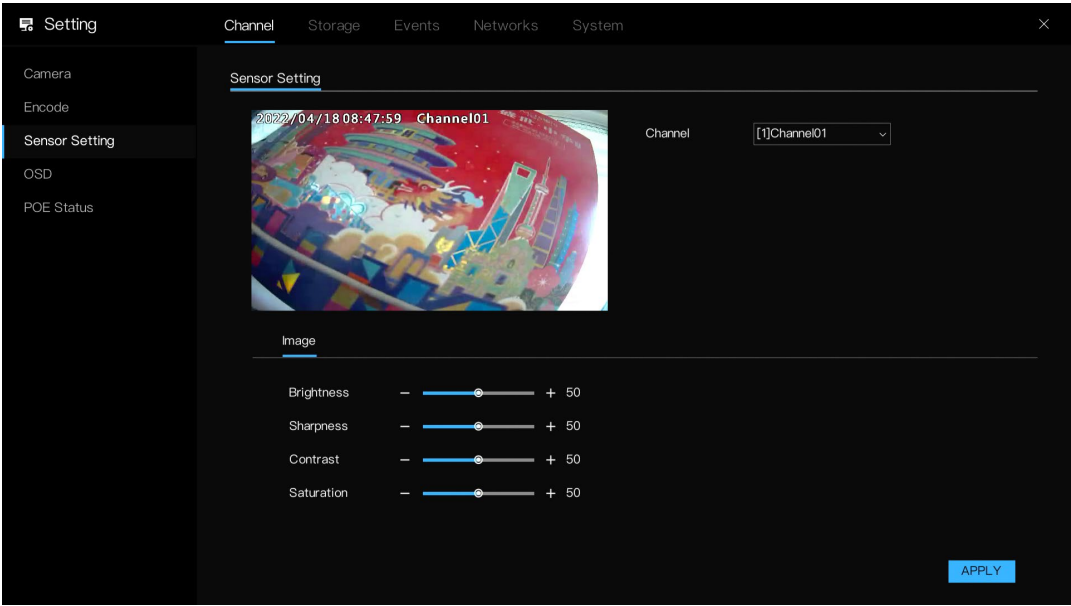
3. Click APPLY to complete settings.

Sensor Setting

1. Go to Main Menu > Camera > Sensor Setting.

The **Sensor Setting** interface is displayed

Figure 53 Image



2. Configure parameters.

Note: Different series network camera displays different parameters. The actual product shall prevail.

Table 23 Image Parameters

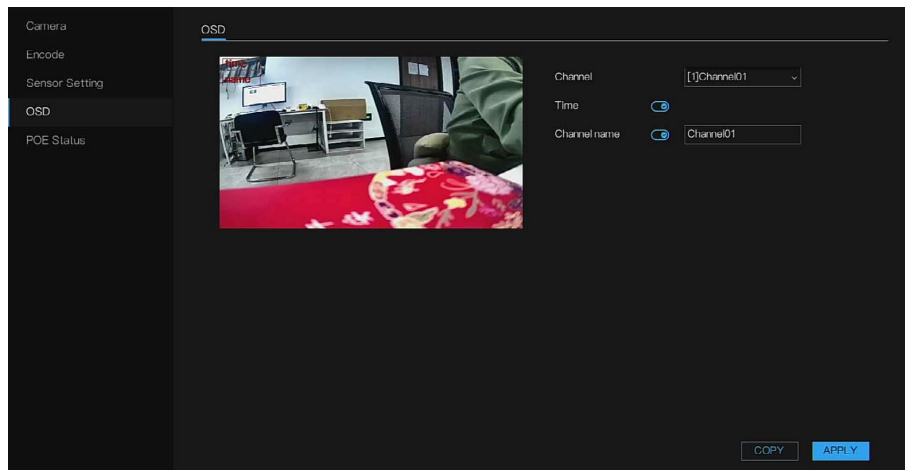
Parameter	Description
Channel	In the Channel list, select the channel that you want to configure.
Brightness	Adjusts the brightness according to actual environment.
Sharpness	Adjusts the sharpness according to actual environment.
Contrast	Adjusts the contrast according to actual environment.
Saturation	Adjusts the color shades. The bigger the value, the lighter the color will become. Adjusts the saturation according to actual environment.

3. Click APPLY.

OSD

1. Go to Main Menu > Camera > OSD. The OSD interface is displayed.

Figure 54 OSD



2. In the Channel list, select a channel to set OSD.
3. Enable Time to display. Enable Channel name to display and input the channel name to distinguish different locations' cameras.

The display box is displaying at top left of screen. Click and drag display box of time(channel) to move to a specified location.

Note: To modify the format of displaying time, go to Main Menu > SYSTEM > General > Date And Time to set. Refer to [Date And Time](#) for detailed information.

The channel name supports up to 32 characters

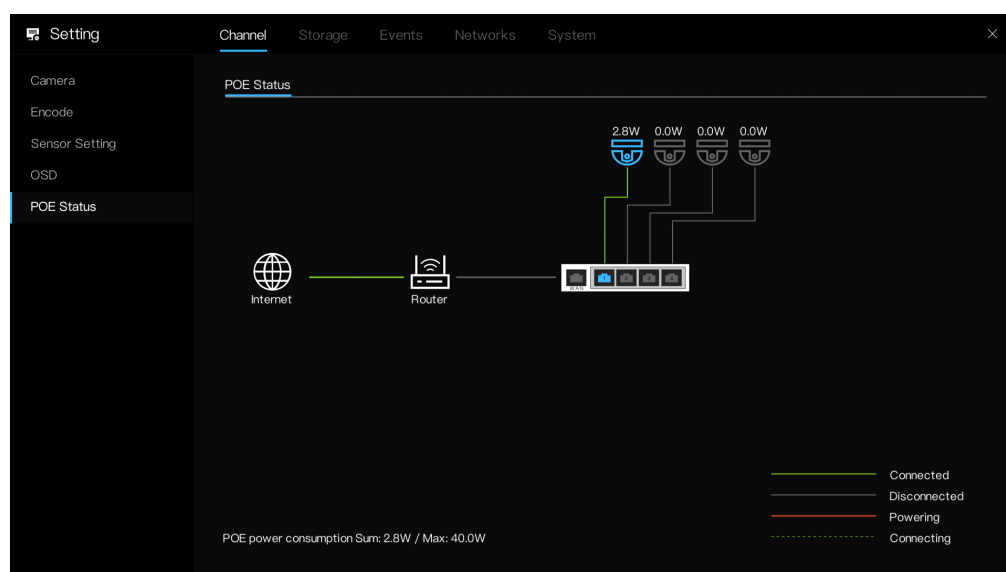
4. Click APPLY to complete settings.

POE Status

This function is only applicable for the PoE NVR.

1. Go to Main Menu > Camera > POE Status.
2. Check the status of POE. The POE Status interface is displayed.

Figure 55 PoE Status



Configuring Storage Settings

You can manage the storage resources (such as storage mode) and storage space. So that it is easy for you to use and enhance storage space usage.

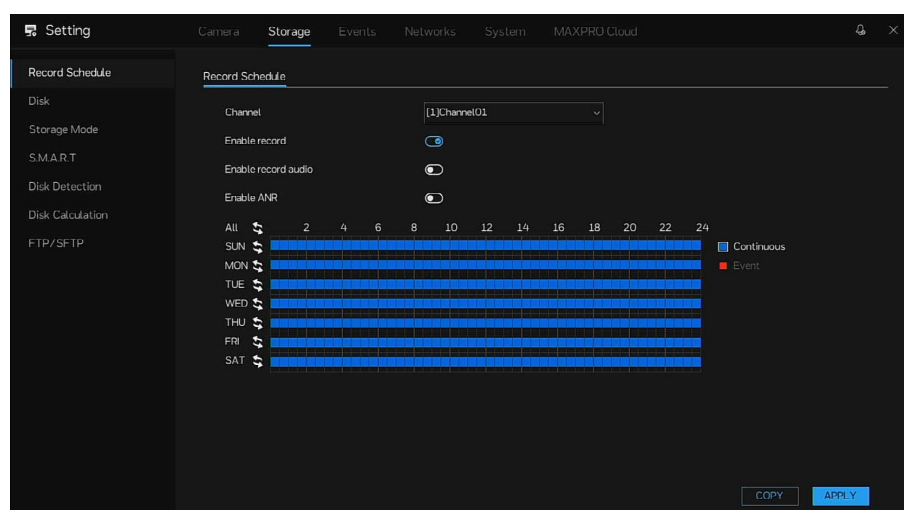
Record Schedule

After set schedule record, device can record video file according to the period you set here. For example, the alarm record period is from 6:00–18:00 Monday, device can record alarm video files during 6:00–18:00.

All channels are record continuously by default. You can set customized record period and record type.

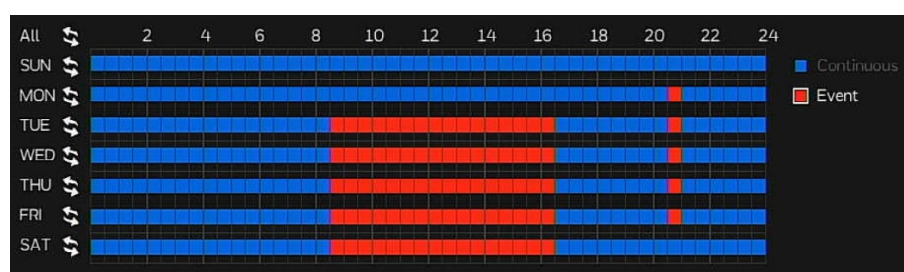
1. Go to Main Menu > Storage > Record Schedule.

Figure 56 Record Schedule



2. Select a channel from the drop-down list, you can set different record plans for different channels. Select COPY to copy settings for other channels.
3. Enable record and record audio.
4. Enable ANR (Auto Network Recording). If the camera is installed with an SD card and is disconnected from the network, the NVR can read the recording of camera and copy the lost video form the SD card when the network is recovered.
5. Set the schedule of recording.

Figure 57 Record Type



Define the period by drawing.

- a. Select a corresponding date to set.
- b. On the timeline, left click mouse and then drag to define a period.

In [Set Period by Drawing](#), users can set the continuous record or event record.

 - Blue stands for continuous record.
 - Red stands for event record.
 - Select a record type and then left-click to set or click  to set all day or all week. Left-click again to clear the corresponding period.

Note: The color schedule is only for view, the recording of disk cannot show these colors; There are only three types of recording



Figure 58 Set Period by Drawing



Method 1: Hold down the left mouse button, drag and release mouse to select the arming time within 00:00-24:00 from Monday to Sunday.

Method 2: Click  in the record schedule page to select the whole day or whole week.

Deleting record schedule: Click  again or inverse selection to delete the selected record schedule.

- When you select time by dragging the cursor, the cursor cannot move out of the time area. Otherwise, no time would be selected.
- The selected area is blue. The default is all week.
- User can choose alarm type to record, if the chosen alarm is happening at the setting time, it will record. So that it will using the disk effectively to avoid repeating useless recording.
- The ANR function can be used only for the cameras with supplementary recording function.
- User can set different alarms to record.

6. Click APPLY to complete the settings.

Enable auto record function so that the record plan can become activated. Refer to [Storage](#) for detailed information.

Disk

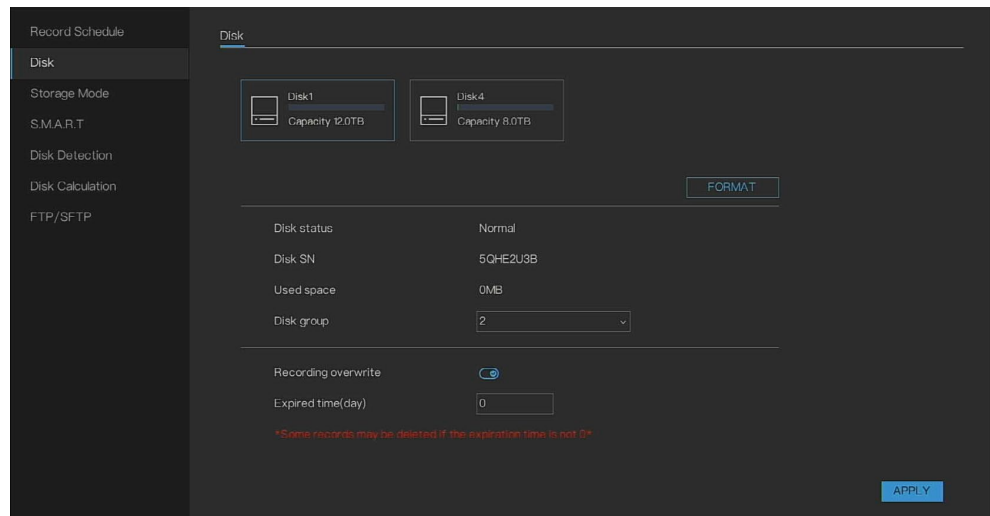
You can view and set HDD properties, format HDD and view current HDD type, status, capacity and etc. The operation includes format HDD, and change HDD property (read and write/read-only/redundancy).

To backup recorded video file, you can set HDD as redundant HDD.

1. Go to Main Menu > Storage > Disk.

The Disk interface is displayed.

Figure 59 Disk Interface



2. Select an HDD and then select disk group the drop-down list.
3. (Optional) Format an HDD.
 - a. Select an HDD and then click FORMAT.

Note: This operation will erase all data in the HDD. Proceed with caution. If you format the HDD, the data will be lost.

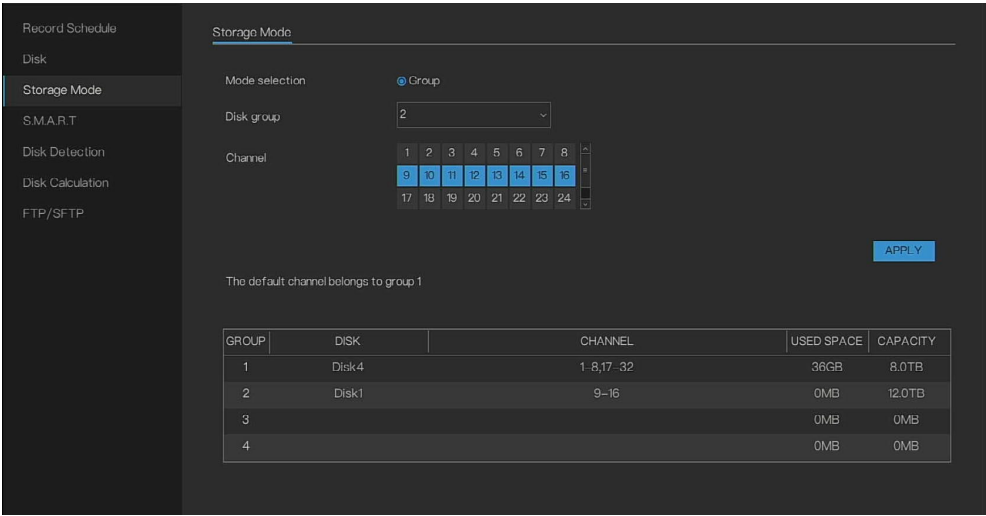
- b. Click OK.
4. Enable Recording overwrite, when the disk is full, it will overwrite.
5. Set Expired time(day), the expired time is not 0, the records will be deleted when the time is over the setting value.
6. Click APPLY to complete the setup.

Storage Mode

When the NVR is installed with several HDDs, you can configure the HDDs in different groups, and different HDDs can record different channels, so that users can access HDDs quickly and use the HDDs efficiently.

1. Go to Main Menu > Storage > Storage Mode.

Figure 60 Storage Mode



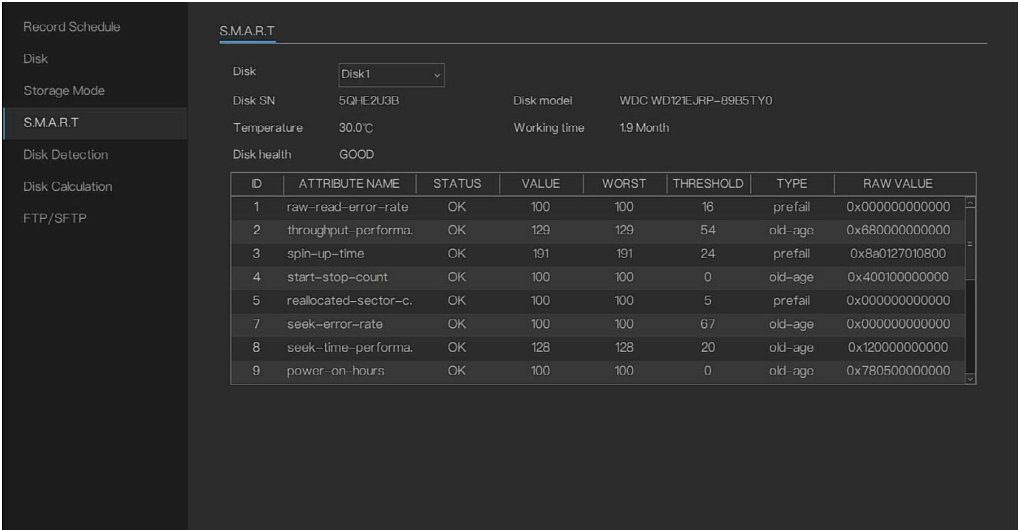
2. Choose the Disk group and Channels, the details of configuration are shown in list.
3. Click APPLY to complete settings.

Note: If the total bit rate for the channels in one group is more than 200 M, the channels need to be distributed to more than one group. For example, if the main stream rate for one channel is 8 M and sub stream rate (non-encrypted) is 2 M, the total bit rate for 32 channels is 320 M, and the 32 channels need to be distributed to 2 groups. The channels can be distributed to groups randomly.

S.M.A.R.T

S.M.A.R.T is Self-Monitoring Analysis and Reporting Technology with which user can view corresponding information. Replace the malfunction HDD in case there is data loss

Figure 61 S.M.A.R.T Interface



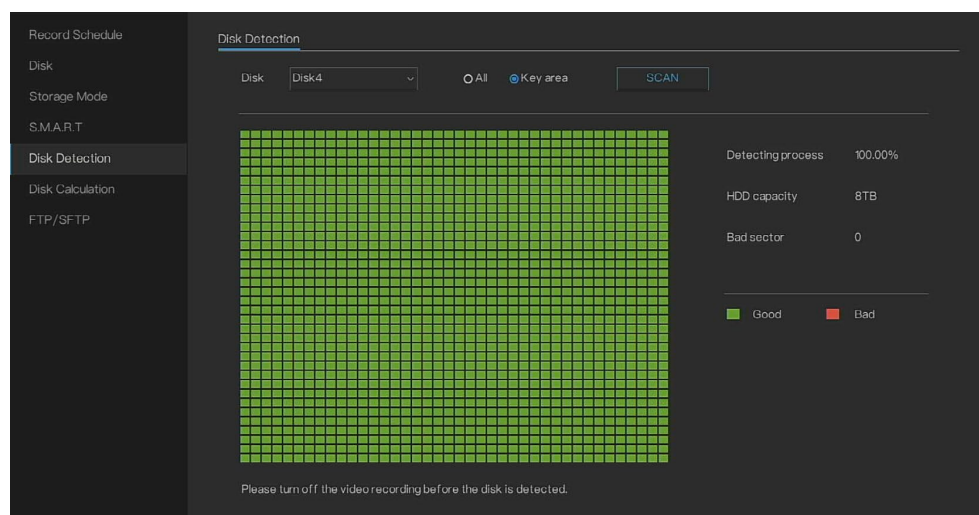
Disk Detection

HDD detect function can detect HDD current status to clearly understand the HDD performance and replace the malfunction HDD.

1. Go to Main Menu > Storage > Disk Detection.

The Disk Detection interface is displayed.

Figure 62 Disk Detection Interface



2. Choose Disk that you want to detect. Select All or Key area. Detecting All needs some time because it detects carefully and comprehensively; Detecting key section may need a few minutes.
3. Click SCAN.

The system starts detecting the HDD and displays the detection information.

- The green block means good, the red block means bad, if the red blocks are too much or at key section, please change the disk immediately
- Please turn off the video recording before the disk is detected, otherwise the recording of video maybe lost.

Note: When the system is detecting HDD, click CANCEL to stop current detection. When pop-up window shows “Would you like to stop disk detection?”, click OK to end detecting.

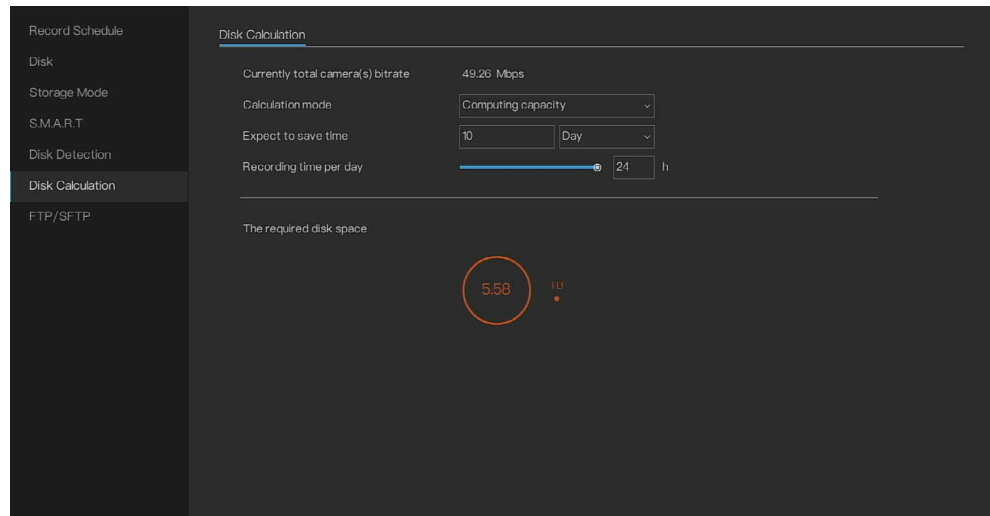
Disk Calculation

Record estimate function can calculate how long you can record video according to the HDD capacity, and calculate the required HDD capacity according to the record period.

1. Go to Main Menu > Storage > Disk Calculation.

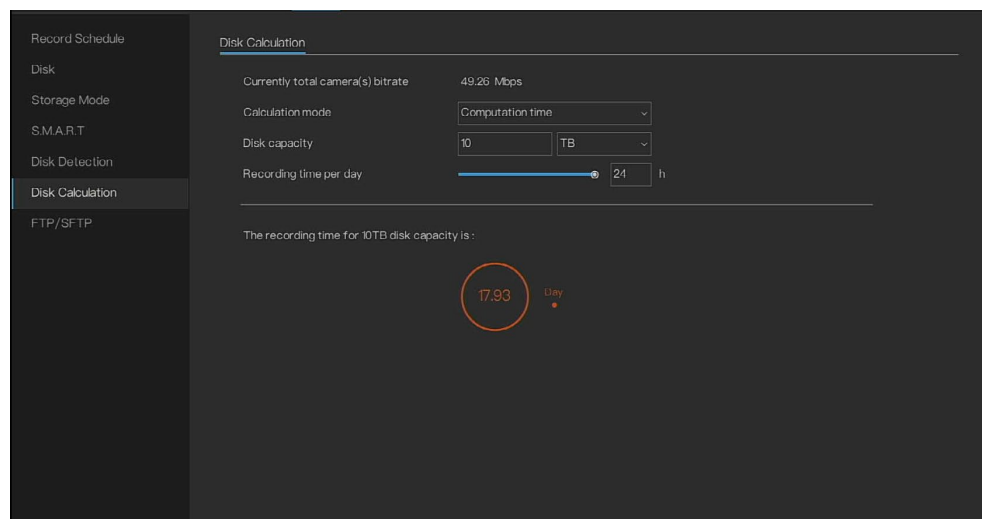
The Disk Calculation interface is displayed.

Figure 63 Disk Calculation



2. Choose the calculation mode for Computing capacity or Computation time.
3. Input value for Expect to save time.
4. Set the Recording time per day, the result is shown in figure.

Figure 64 Computation time



Note: The computation is based on the currently online cameras bitrate (includes main stream and sub stream).

FTP/SFTP

You can store and view the recorded videos and snapshots on the FTP server.

Purchase or download an FTP (File Transfer Protocol) or SFTP (Secret File Transfer Protocol) server and install it on your PC.

Note: For the created FTP user, you need to set the write permission; otherwise the uploading for recorded videos and snapshots will be failed.

- 1. Go to Main Menu > Storage > FTP/SFTP.
- 2. Select Mode as FTP or SFTP.

Figure 65 FTP

The screenshot shows the 'FTP/SFTP' configuration page. On the left is a sidebar menu with options: Record Schedule, Disk, Storage Mode, S.M.A.R.T, Disk Detection, Disk Calculation, and FTP/SFTP (which is highlighted). The main area is titled 'FTP/SFTP' and contains the following settings: 'Enable upload' is a toggle switch that is turned on; 'Mode' is a dropdown menu set to 'FTP'; 'FTP address' is an empty text field; 'FTP port' is a text field containing '21'; 'Account' is an empty text field; 'Password' is an empty text field with an eye icon for toggling visibility; 'FTP path' is an empty text field; 'Upload file size(0-64MB)' is a text field containing '5'; and a 'TEST' button. An 'APPLY' button is located at the bottom right of the main area.

Figure 66 SFTP

The screenshot shows the 'FTP/SFTP' configuration page with the 'Mode' dropdown set to 'SFTP'. The settings are: 'Enable upload' is a toggle switch that is turned on; 'Mode' is a dropdown menu set to 'SFTP'; 'SFTP address' is an empty text field; 'SFTP port' is a text field containing '22'; 'Account' is an empty text field; 'Password' is an empty text field with an eye icon for toggling visibility; 'SFTP path' is an empty text field; 'Upload file size(0-64MB)' is a text field containing '5'; and a 'TEST' button. An 'APPLY' button is located at the bottom right of the main area.

Configure the settings for the FTP/SFTP settings parameters.

Table 24 FTP/SFTP Parameters

Parameter	Description
Enable upload	Enable the FTP/SFTP upload function.

Parameter	Description
FTP address/SFTP address	IP address of FTP/SFTP server.
FTP Port/SFTP Port	The default is 21/22.
Account	Enter the account and password to log in to the FTP server.
Password	
FTP path/SFTP path	Create folder on FTP/SFTP server. - If you do not enter the name of remote directory, system automatically creates the folders according to the IP and time. - If you enter the name of remote directory, the system creates the folder with the entered name under the FTP/SFTP root directory first, and then automatically creates the folders according to the IP and time.
Upload file size(0-64MB)	Enter the length of the uploaded recorded video. - If the entered length is less than the recorded video length, only a section of the recorded video can be uploaded. - If the entered length is more than the recorded video length, the whole recorded video can be uploaded. - If the entered length is 0, the whole recorded video will be uploaded.

- Click TEST.

The system pops up a message to indicate success or failure. If failed, check the network connection or configurations.

- Click APPLY to complete the settings.

Configuring Events Settings

Note: An NVR can support up to 5 apps to receive push messages. To use the event message notification in app, go to Me > Settings > Event notification and enable the device below New event message notification.

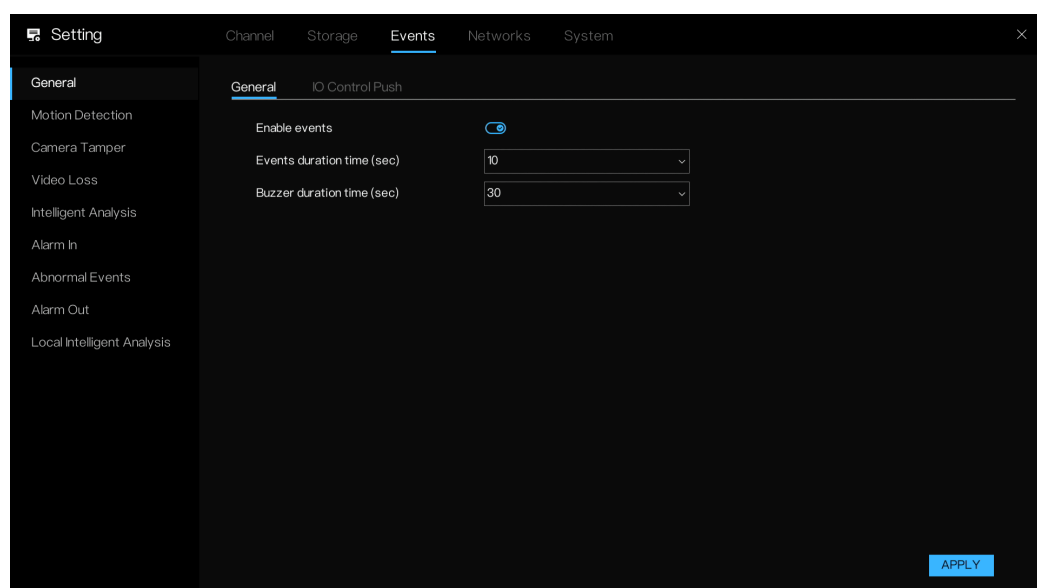
General

You can enable general event and IO Control Push.

- Go to Main Menu > Events > General > General.

The General interface is displayed.

Figure 67 General Page

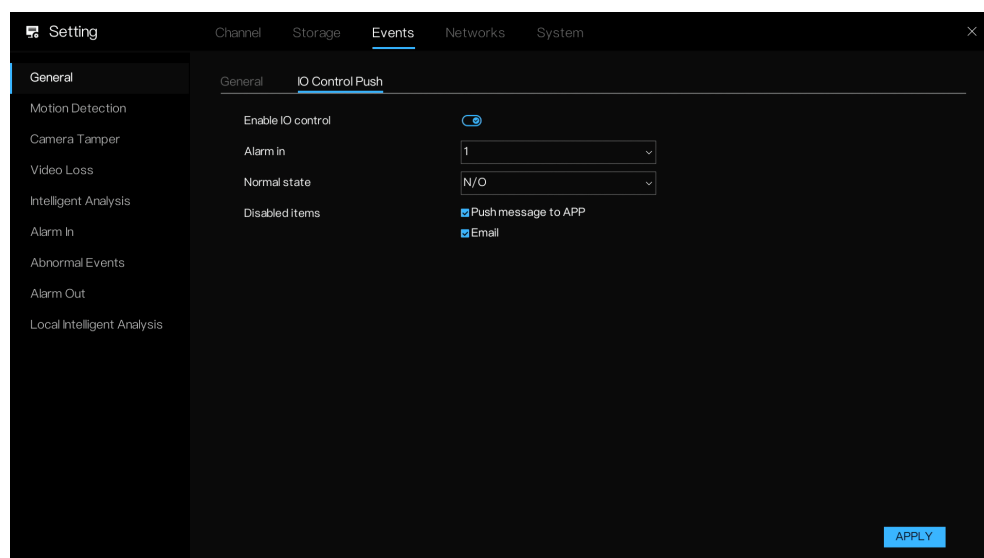


2. Enable events, set Events duration time(sec) and Buzzer duration time(sec).
3. Click APPLY to save the settings.

IO Control Push

1. Go to Main Menu > Events > General > IO Control Push.
The IO Control Push interface is displayed.

Figure 68 IO Control Push



2. Enable IO Control Push, choose the Alarm in from drop-down list.
3. Choose Normal state from drop-down list (N/C or N/O).
4. Select Disable items (Push message to APP and Email)

Note: If you select normally open and select the disabled items, the alarm input 1 will not push message in the normally open state. Only when the alarm in 1 is in the normally closed, it can push alarm message.

5. Click APPLY to save the settings.

Motion Detection

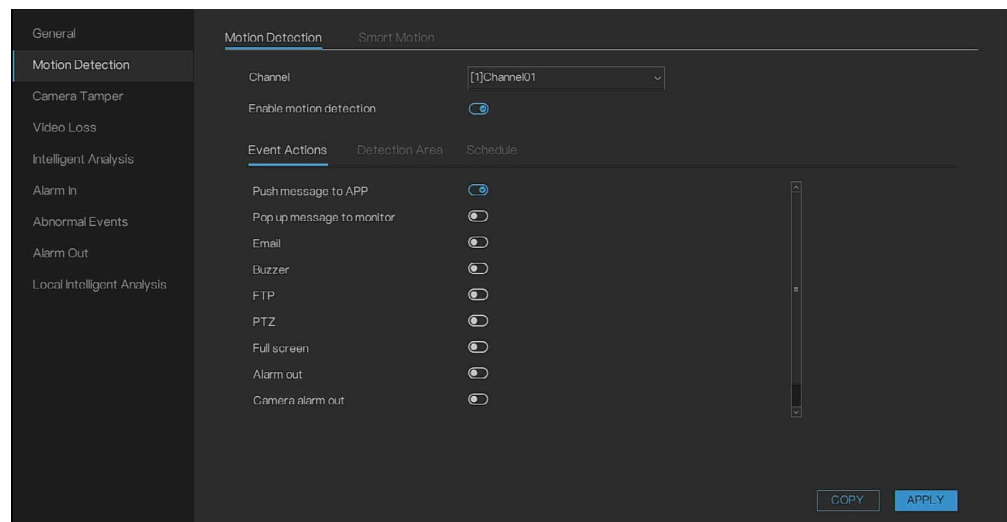
Motion Detection Settings

When the moving object appears and moves fast enough to reach the preset sensitivity value, the system activates the alarm.

1. Go to Main Menu > Events > Motion Detection.

The Motion Detection interface is displayed.

Figure 69 Motion Detection



2. Configure the settings for the motion detection parameters.

Table 25 Motion Detection Parameters

Parameter	Description
Channel	In the Channel list, select a channel to set the motion detection.
Enable	Enable or disable the motion detection function. When enable the function, the NVR is modified and the result can be synced to camera.

Parameter	Description
Event Actions	Push message to APP: enable a pop-up message to App which is managing the NVR Pop up message to monitor: enable a pop-up message in your UI monitor. Email: When an alarm occurs, the NVR device sends an email to the set mailbox to notify the user. You need to set the email first. For details, refer to Email. Buzzer: activate the buzzer when an alarm occurs. The duration is set in Event > General. FTP: enable it to send snapshot to FTP path. Set FTP in Storage > FTP interface. PTZ: enable it and select the Channel and Preset. When an alarm occurs, the NVR device associates the channel to perform the corresponding PTZ action. For example, activate the PTZ in channel one to turn to the preset point X. •Tripwire alarm supports to activate PTZ preset point only. •You need to set the corresponding PTZ actions first, see PTZ Control. Full Screen: enable to show the live video of channel by full screen when alarming. Alarm out: enable to linkage alarm out, the parameters should be set in Event > Alarm out interface. The alarm device (such as lights, sirens, etc.) is connected to the alarm output port. When an alarm occurs, the NVR device transmits the alarm information to the alarm device. Camera alarm out: enable to linkage the alarm out port of camera. Event recording: enable to record when the alarm is occur.
Detection Area	After a motion detection area is selected, double-click it to delete the selected area. Sensitivity: there are four level can be chosen, Low/Medium/High/Highest, it is not consistent with IPC. The highest the chosen is, the easier the alarms can be activated.
Schedule	Define a period during which the motion detection is active.

3. Click APPLY to save the settings.

Click COPY. In the Copy dialog box, select the additional channel(s) that you want to copy the motion detection settings to, and then click APPLY.

Figure 70 Copy Dialog Box



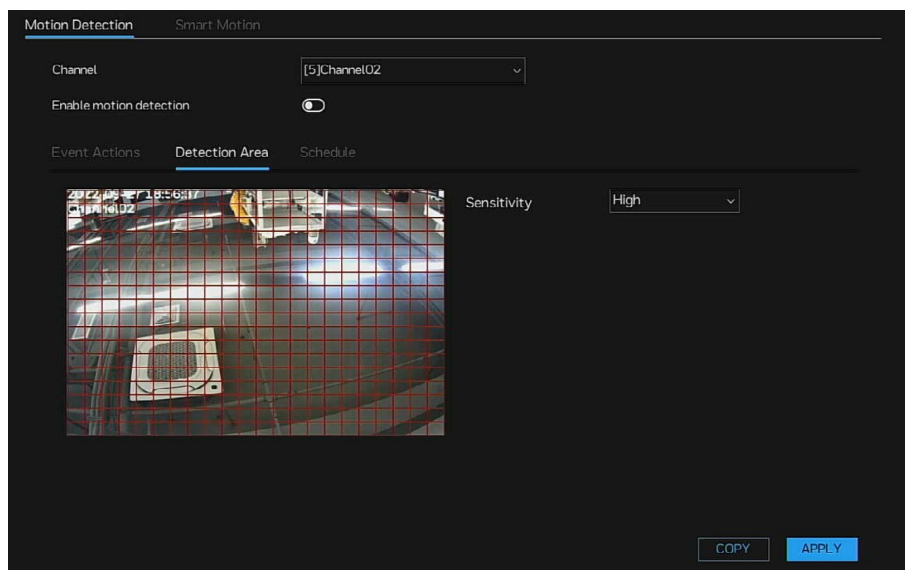
Setting the Motion Detection Area

1. On the live video screen, draw areas to arm.

You can configure several regions. Hold down and drag the left mouse button to draw a motion detection area, the default area is full screen.

- Note:**
- *Drag on the screen to select the region that you want to detect. When anyone of the several regions activates motion detect alarm, the channel where this region belongs to will activate motion detect alarm.*
 - *When the NVR is modified, the result can be synced to camera.*
 - *For PTZ cameras, the VA function are only available on home position.*

Figure 71 Region Setting

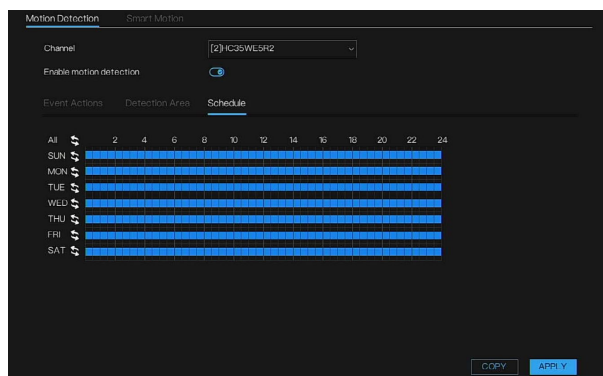


2. Click APPLY to complete the settings.

Setting Schedule

Note: *The system only activates the alarm in the defined period.*

Figure 72 Schedule Setting



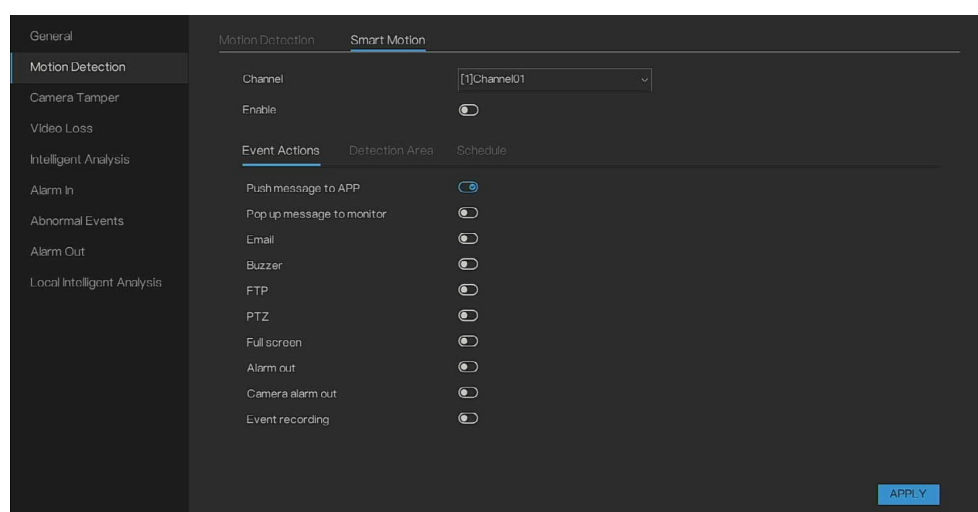
1. Set Schedule.
 - Hold down the left mouse button, drag and release mouse to select the arming time within 00:00-24:00 from Monday to Sunday.
 - Click  in the record schedule page to select the whole day or whole week.
 - click the time grids to choose one by one.
- Click  again or inverse selection to delete the selected record schedule.
2. Click APPLY to complete the settings.

Smart Motion

For some cameras can detect person or car, you can set the smart motion parameter in NVR that manage convenient the cameras.

Go to **Main Menu > Events > Motion Detection > Smart Motion**, the **Smart Motion** interface is displayed.

Figure 73 Smart Motion



To configure the linkage event actions of smart motion's, see [Table 25 Motion Detection Parameters](#).

Setting Smart Motion Area

Move the cursor to the drawing interface and click to generate a point. Move the cursor to draw a line, and then click to generate another point. This is how a line is generated. In this way, continue to draw lines to form any shape, and right-click to finish line drawing.

Click **REMOVE ALL** to remove detection area.

Figure 74 Smart Motion – Detection Area

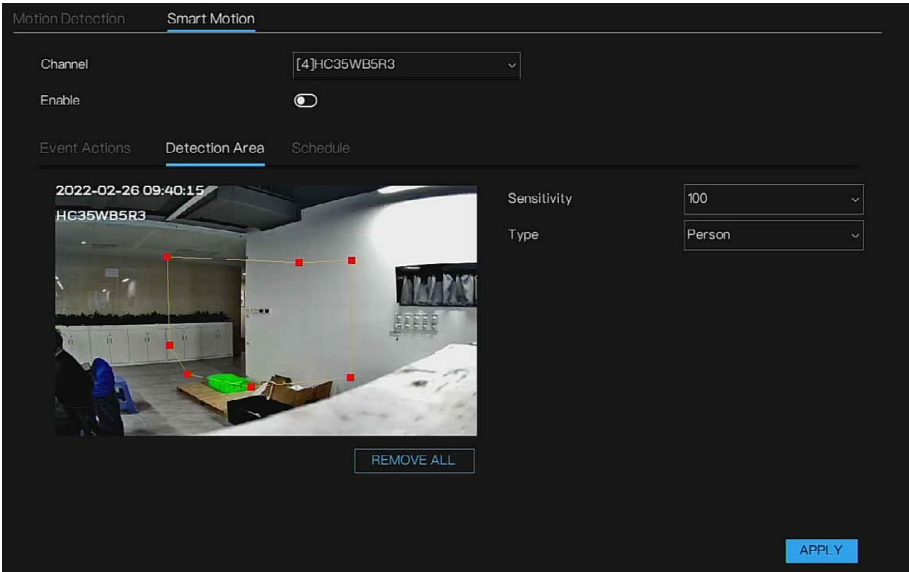


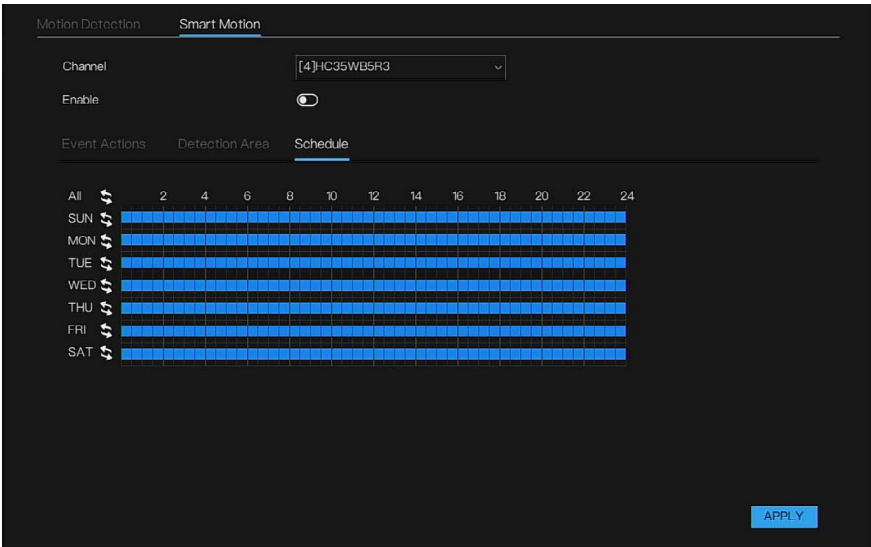
Table 26 Detection Area Setting Parameters

Parameter	Description
Sensitivity	Every region of every channel has an individual sensitivity value. The range is 0-100.The bigger the value is, the easier the alarms can be activated.
Type	Person: only detects people Car: only detects cars Person or car: detects person and car at the same time

Setting Smart Motion Schedule

To configure the schedule of smart motion’s, refer to [Setting Schedule](#).

Figure 75 Smart Motion – Schedule



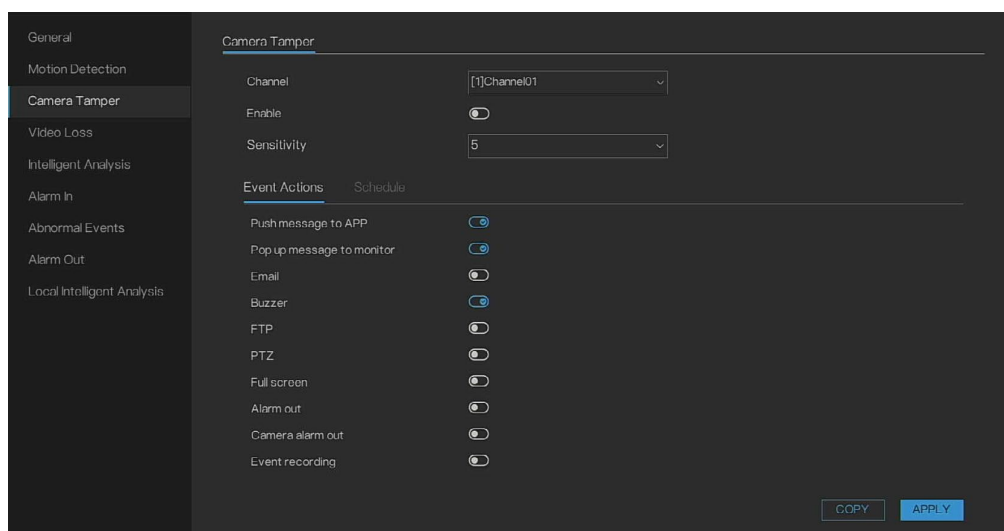
Camera Tampering

When the camera lens is covered, or the video is displayed in a single color because of sunlight status, the monitoring cannot be continued normally. To avoid such situations, you can configure the tamper alarm settings.

1. Go to Main Menu > Events > Camera Tamper.

The Camera Tamper interface is displayed.

Figure 76 Camera Tamper



2. To configure the settings for the tampering detection parameters, refer to [Motion Detection](#).

Note: The tampering function does not have detection area and sensitivity items.

Every channel has an individual sensitivity value. The range is from 1 to 5. The bigger the value is, the easier the alarms can be activated.

3. Click APPLY to complete the settings.

Click COPY, in the Copy to dialog box, select the additional channel(s) that you want to copy the motion detection settings to, and then click OK.

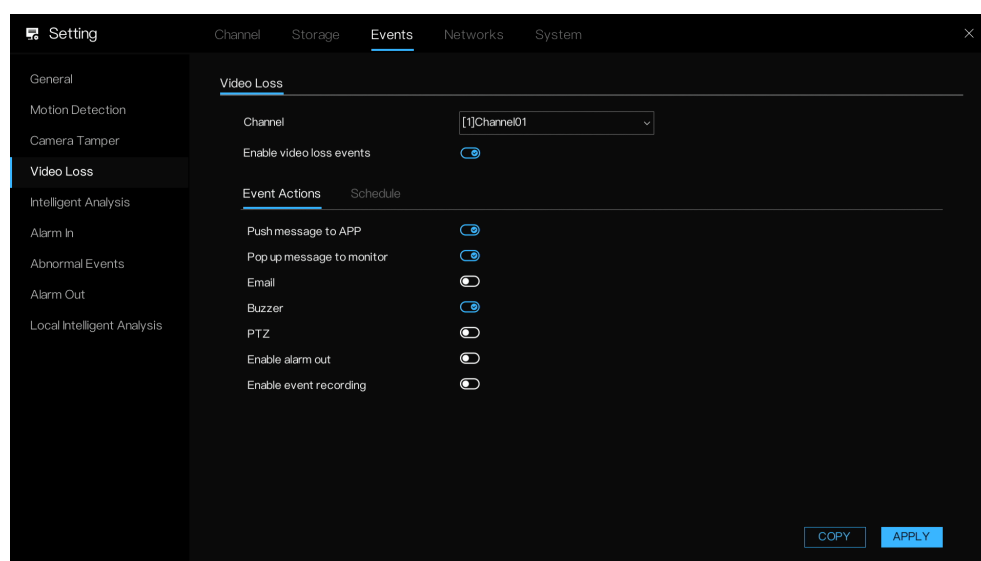
Video Loss

When the video loss occurs, the system activates the alarm.

1. Go to Main Menu > Events > Video Loss.

The Video Loss interface is displayed.

Figure 77 Video Loss



2. To configure the settings for the video loss detection parameters, refer to [Motion Detection](#).

The video loss function does not have detection area and sensitivity items.

3. Click APPLY to complete the settings.

Click COPY, in the Copy to dialog box, select the additional channel(s) that you want to copy the motion detection settings to, and then click OK.

Intelligent Analysis

Intelligent analysis includes Intrusion, Multi Loitering and Crowd Detection.

Note: When the Intelligent Analysis functions are set as Enable by NVR to receive the signals from channel cameras, some model cameras may not support remote configuration and the result may not be synced to cameras when the parameters are modified only by NVR. Therefore, Honeywell recommends you modify the setting by the camera web client at the same time.

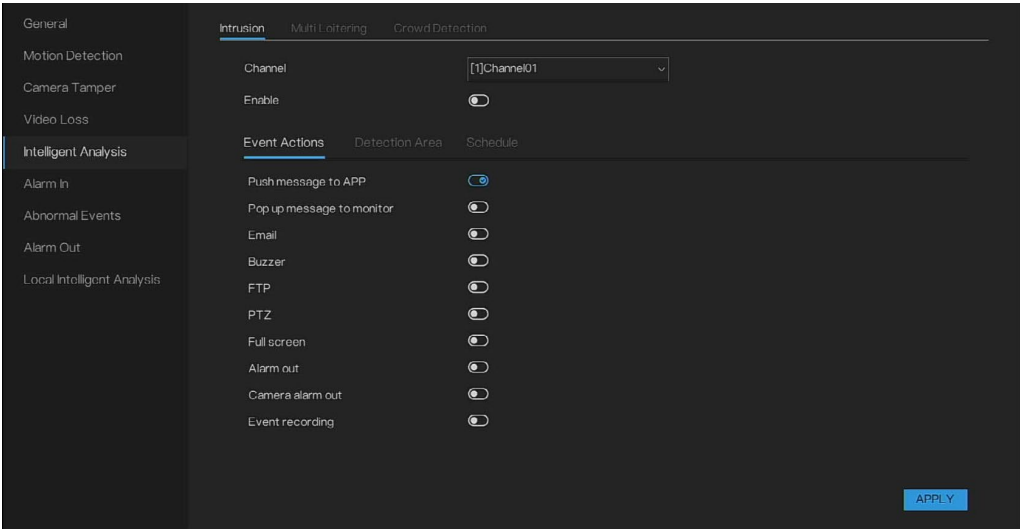
Intrusion

When channel camera captures someone is intruding to the setting area, it will trigger the intelligent analysis intrusion alarm of NVR

1. Go to Main Menu > Events > Intelligent Analysis > Intrusion.

The Intrusion interface is displayed.

Figure 78 Intrusion



2. To configure the settings for the intrusion parameters, see [Motion Detection](#).

The intrusion function does not have detection area and sensitivity items. The detection area is configured in cameras interface, so the parameter can be copied.

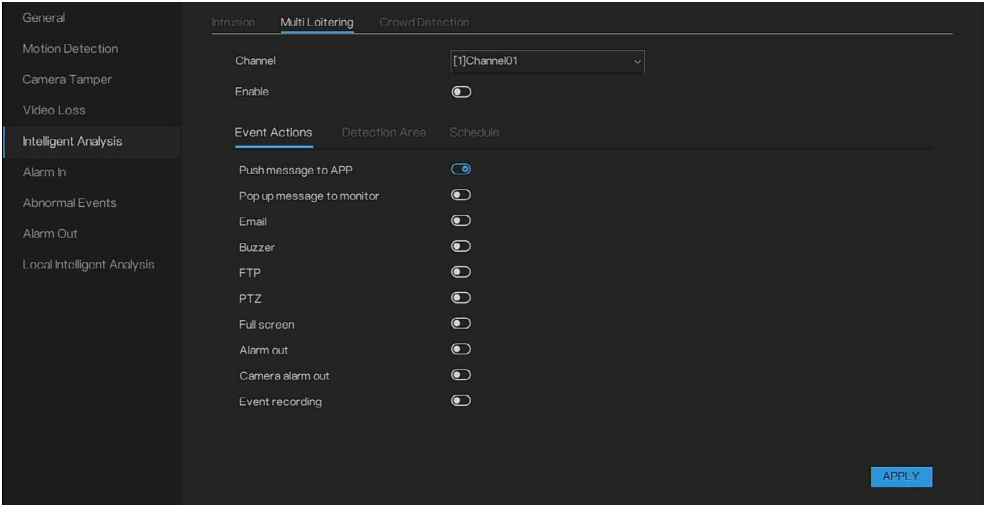
3. Click APPLY to complete the settings.

Multi Loitering

When channel camera is capture someone stay in the setting area, it will trigger the intelligent analysis multi loitering alarm of NVR

1. Go to Main Menu > Events > Intelligent Analysis > Multi Loitering.
The Multi Loitering interface is displayed.

Figure 79 Multi Loitering



2. To configure the settings for the multi loitering parameters, see [Motion Detection](#).

The multi loitering function does not have detection area and

sensitivity items. The detection area is configured in cameras interface, so the parameters can be copied.

3. Click APPLY to complete the settings.

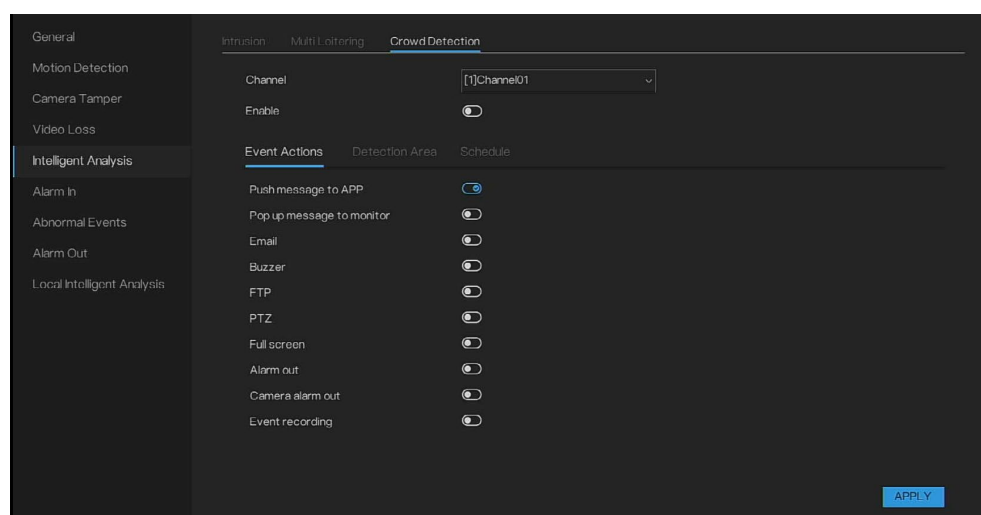
Crowd Detection

When channel camera is counting personnel in the setting area, it will trigger the intelligent analysis personnel count alarm of NVR

1. Go to Main Menu > Events > Intelligent Analysis > Crowd Detection.

The Crowd Detection interface is displayed.

Figure 80 Crowd Detection



2. To configure the settings for the Crowd Detection parameters, see [Motion Detection](#).

The Crowd Detection function does not have detection area and sensitivity items. The detection area is configured in cameras interface, so the parameters cannot be copied.

3. Click APPLY to complete the settings.

Alarm In

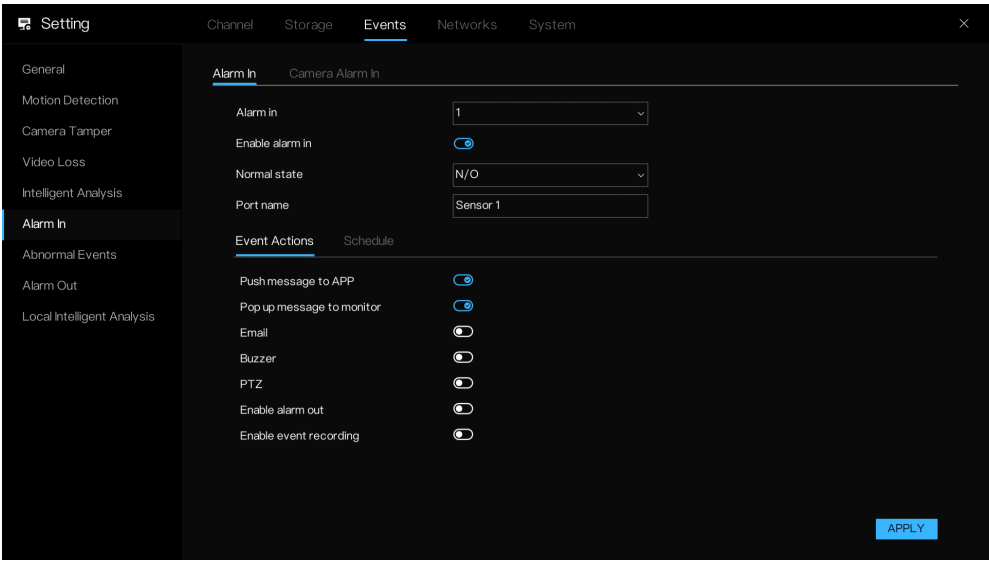
Alarm In Settings

After connecting the alarm device to the NVR alarm input port, system can trigger the corresponding alarm operations when there is alarm signal from the alarm input port to the NVR.

1. Go to Main menu > Events > Alarm In.

The Alarm In interface is displayed.

Figure 81 Alarm In



2. Set Alarm-in Port channel number and then select the enable check box to enable the function.
3. Configure parameters.

Table 27 Alarm-in Port Parameters

Parameter	Description
Alarm in	Select a port to set alarm, the alarm device is also connected to the correspond port.
Enable alarm in	Check the box  to enable the function.
Normal state	N/O (normal open) or N/C (normal close).
Port name	Input the port name, the name will show on the alarm information message.
Event Actions	Refer to Table 25 .
Schedule	Define a period during which the alarm is active. For details, see Motion Detection .

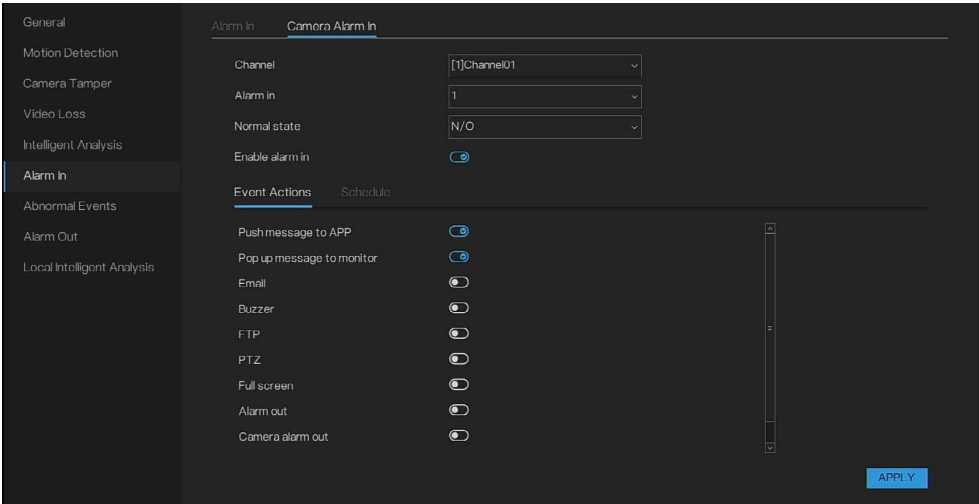
4. Click APPLY.

Camera Alarm In

After connecting the alarm device to the channel camera alarm input port, system can trigger the corresponding alarm operations when there is alarm signal from the alarm input port of camera.

1. Go to Main Menu > Events > Alarm In > Camera Alarm In.
The Camera Alarm In interface is displayed.

Figure 82 Camera Alarm in Port

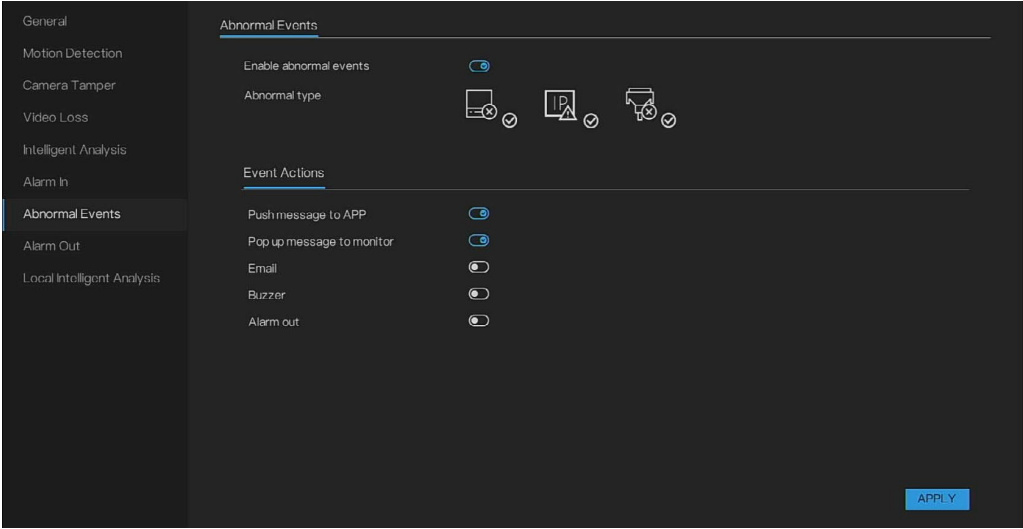


- 2. Select the Channel/Alarm in/Normal state.
- 3. Enable to open camera alarm in port. The following operations are same as [Alarm In Settings](#).
- 4. Click APPLY.

Abnormal Events

- 1. Go to Main Menu > Events > Abnormal events.
The Abnormal events interface is displayed.

Figure 83 Abnormal Events



- 2. Configure parameters.

Table 28 Abnormal Alarm Parameters

Parameter	Description
Enable abnormal events	Check the box  to enable the function.
Abnormal type	Disk alarm, IP address conflict, network disconnect

Parameter	Description
Event actions	Enable different event actions

1. Click APPLY to complete settings.

Alarm Out

The external alarm device is connected to the alarm out port.

1. Go to Main Menu > Events > Alarm out.

The Alarm Out interface is displayed.

Figure 84 Alarm Out

The screenshot shows the 'Setting' window with the 'Events' tab selected. Under 'Events', 'Alarm Out' is chosen. The configuration fields are as follows:

Parameter	Value
Port number	1
Port name	Name
Valid signal	Close
Alarm output mode	Switch mode

2. Configure parameters.

Table 29 Alarm Out Parameters

Parameter	Description
Port number	Correspond to real panel I/O port OUT 1
Port name	Input the port name. The name will show on the alarm information message.
Valid signal	Close: An alarm is generated when an external alarm signal is received. Open: An alarm is generated when no external alarm signal is received.
Alarm output mode	When the device receives I/O alarm signals, the device sends the alarm information to an external alarm device

3. Click APPLY to complete settings.

Local Intelligent Analysis

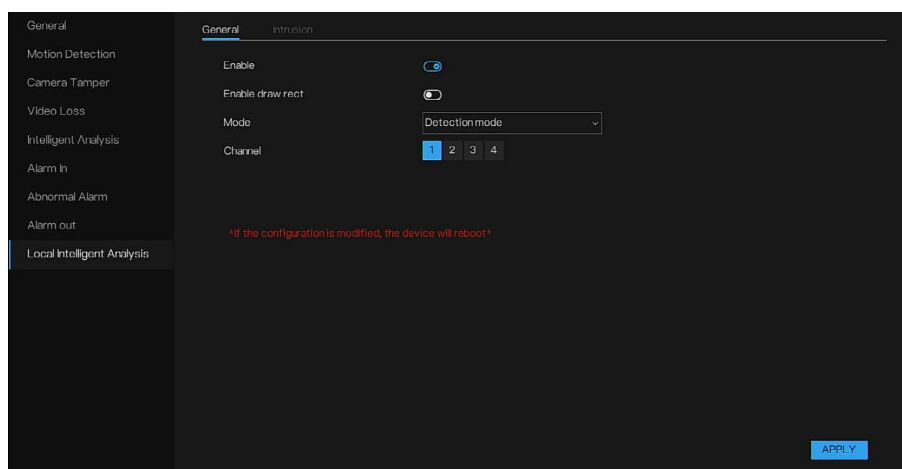
Note: This function is applicable for PoE NVRs only. It is not applicable for non-PoE NVRs.

The local intelligent analysis is for NVR to manage the local intrusion alarm.

1. Go to Main Menu > Events > Local Intelligent Analysis.

The Local Intelligent Analysis interface is displayed.

Figure 85 Local Intelligent Analysis



2. Configure parameters.

Table 30 Local Intelligent Analysis Parameters

Parameter	Description
Enable	Enable this function and then you can set the parameter of alarm.
Enable draw rect	Enable draw rectangle, the detection rectangle will be showed on the live video of intrusion.
Mode	Choose detection mode.
Channel	Choose the channels Up to 4 channels to be chosen.

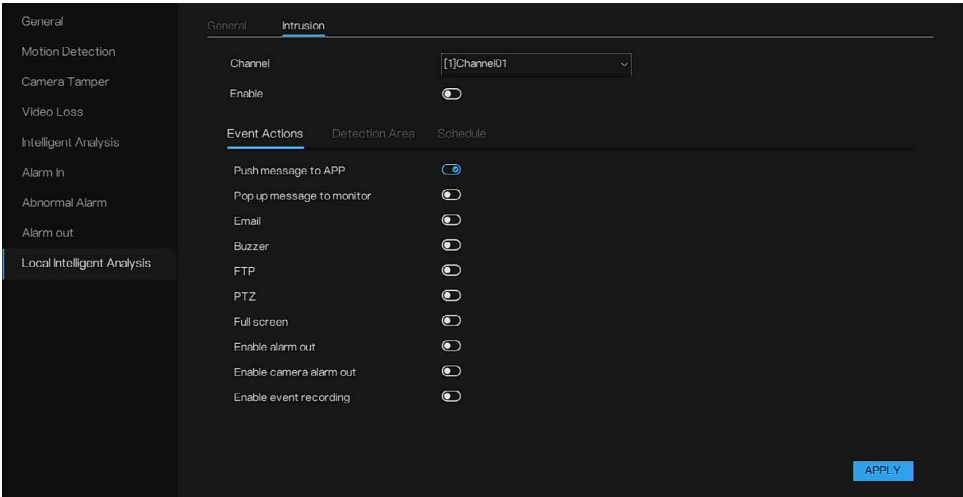
3. Click APPLY to complete settings.

Note: If you enable or disable the intrusion and modify the channels, the device will be reboot.

Intrusion

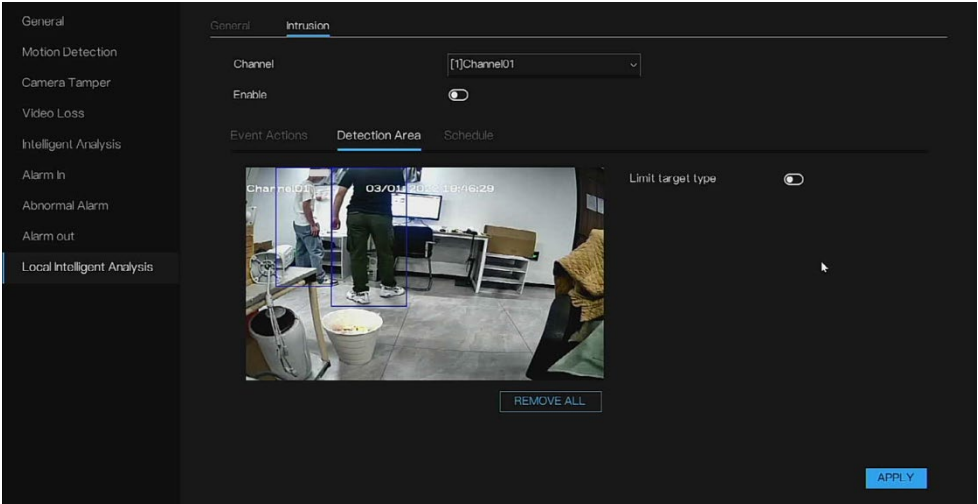
The intrusion refers to that an alarm is generated when the targets of specified types (such as person, car, and both person and car) enter the deployment area.

Figure 86 Intrusion Event Actions



The event actions, detection area, and schedule are set refer to Motion Detection.

Figure 87 Detection Area



To configure the settings for intrusion detection area, refer to [Setting Smart Motion Area](#)

Move the cursor to the drawing interface and click to generate a point. Move the cursor to draw a line, and then click to generate another point. This is how a line is generated. In this way, continue to draw lines to form any shape, and right-click to finish line drawing.

Click **REMOVE ALL** to remove detection area.

Configuring Network Settings

You can set NVR network parameters so that the NVR can communicate with devices in the same LAN.

Network

IP

User can input the IP address in browser address bar, so that you can remote access the NVR through Web page.

1. Go to Main Menu > Networks > Networks > IP.

The Networks interface is displayed.

Figure 88 Networks - IP

The screenshot shows the 'IP' configuration page. At the top, there are tabs for 'IP', 'Port', and 'IPv4 CCTV'. The 'IP' tab is selected. Below the tabs, there are several configuration options:

- DHCP**: A toggle switch is currently turned off.
- IP address**: A text box containing '192.168.0.121'.
- Subnet mask**: A text box containing '255.255.0.0'.
- Default gateway**: A text box containing '192.168.0.1'.
- Obtain DNS automatically**: A toggle switch is currently turned off.
- Preferred DNS server**: A text box containing '192.168.0.1'.
- Alternate DNS server**: A text box containing '8.8.8.8'.

An 'APPLY' button is located at the bottom right of the form.

2. Enable DHCP and the router can distribute the IP automatically.
Disable DHCP, you can modify the parameters manually.
3. Set parameters.

Table 31 IP Parameters

Parameter	Description
DHCP	Enable the DHCP function. The IP address, subnet mask and default gateway are not available for configuration once DHCP is enabled. • If DHCP is effective, the obtained information will display in the IP Address box, Subnet Mask box and Default Gateway box. • If you want to manually configure the IP information, disable the DHCP function first. If PPPoE connection is successful, the IP address, subnet mask, default gateway, and DHCP are not available for configuration.
IP Address	Enter the IP address and configure the corresponding subnet mask and default gateway. IP address and default gateway must be in the same network segment.
Subnet Mask	
Default Gateway	
Obtain DNS	Enable the function to get the DNS address automatically.

Parameter	Description
automaticall y	If you learn about the local DNS server IP, you can input the preferred DNS server and alternate DNS server manually.
Preferred DNS	In the Preferred DNS box, enter the IP address of DNS.
Alternate DNS	In the Alternate DNS box, enter the IP address of alternate DNS.

4. Click APPLY.

Configuring Router

1. Log in to the router to set the WAN port to enable the IP address to connect into the WAN.
2. Enable the UPnP function on the router.
3. Connect the Device with the LAN port on the router to connect into the LAN.
4. Go to Main Menu > Network > Network, configure the IP address into the router IP address range, or enable the DHCP function to obtain an IP address automatically.

Port

You can remote access the NVR Web through IP different ports.

1. Go to Main Menu > Networks > Networks > Port.

The Port interface is displayed.

Figure 89 Port Interface

The screenshot shows the 'Port' configuration page. It includes tabs for 'IP', 'Port', and 'POE'. The 'Port' tab is active, displaying three input fields: 'HTTP port' with the value '80', 'HTTPS port' with the value '443', and 'Control port' with the value '30143'. Below these fields, a red warning message reads: '*If the port parameters are modified then the device will reboot*'. An 'APPLY' button is positioned at the bottom right of the form.

2. Configure the settings for the connection parameters.

Note: If the port parameters are modified, then the device will be restarted.

Table 32 Port Parameters

Parameter	Description
HTTP Port	The default value setting is 80. You can enter the value according to your actual situation. If you enter other value, for example 70, you should enter 70 after the IP address when logging in the Device by browser.
HTTPS Port	HTTPS communication port. The default value setting is 443. You can enter the value according to your actual situation.
Control port	The default value setting is 30413. You can enter the value according to your actual situation.

3. Click APPLY to complete the settings.

POE

This function is only applicable for PoE NVR.

1. Go to Main Menu > Networks > Networks > POE.

Figure 90 POE

IP Port **POE**

Auto manage for PoE camera ☒

IP address 169 . 254 . 10 . 169

Subnet mask 255 . 255 . 0 . 0

Default gateway 169 . 254 . 10 . 1

The POE parameters are modified and the device will reboot

APPLY

2. The default Auto manage for PoE camera is open. Users can set the PoE camera IP parameters manually.
3. Click APPLY to complete the settings.

*Note: When the camera via POE, and the auto manage for POE camera is enabling, icon  can be shown in channel list.
The PoE parameters are modified and the device will reboot.*

IPv4CCTV

This function is used for non-PoE NVR with two network ports. The IPv4CCTV is for the LAN port. The LAN port is only used for adding cameras and not able to access the external network.

Note: This function is supported on select models.

1. Go to Main Menu > Networks > Networks > IPv4 CCTV.

Figure 91 IPv4 CCTV

IP	Port	IPv4 CCTV
IP address		192 . 168 . 7 . 159
Subnet mask		255 . 255 . 255 . 0
Default gateway		192 . 168 . 99 . 1

APPLY

2. Set the LAN's IP address parameters.

Note: WAN and LAN port cannot be set in the same network segment. You can add the cameras through LAN port access to local network, but you must plug WAN port in Internet for remote access.

3. Click APPLY to complete the settings.

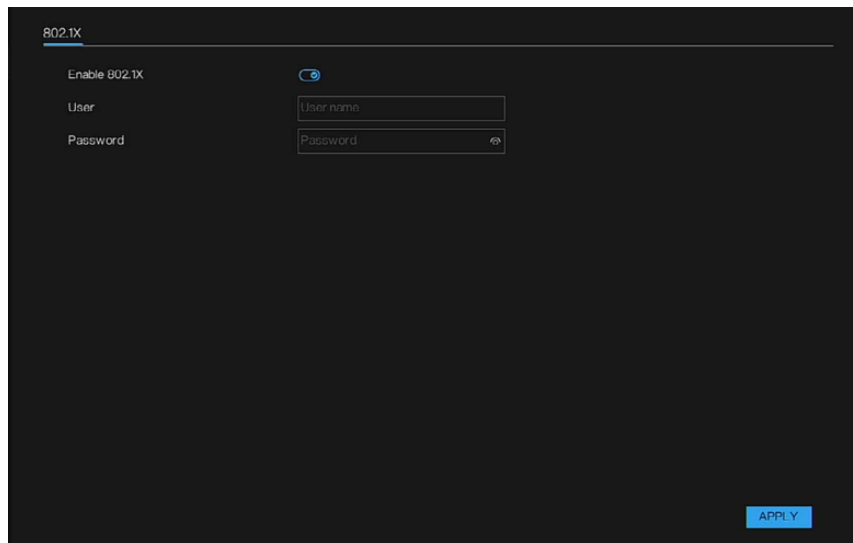
802.1X

The 802.1x protocol is an access control and authentication protocol based on Client/Server. It can restrict unauthorized users/devices from accessing LAN/WLAN through the access port. User can access the NVR through 802.1X account.

1. Go to Main Menu > Networks > 802.1X.

The 802.1X interface is displayed.

Figure 92 802.1X Interface



2. Enable function, enter the 802.1X account user name and password.
3. Click APPLY to complete the settings.

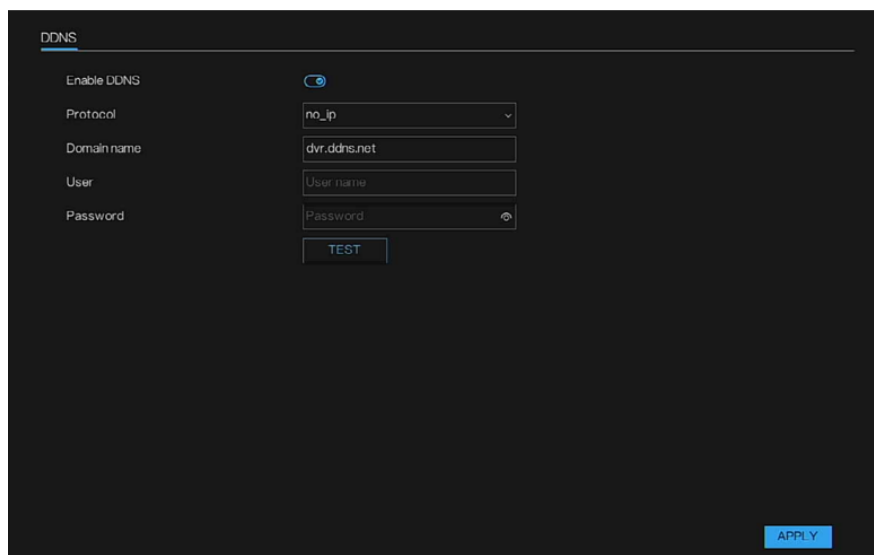
DDNS

DDNS (Dynamic Domain Name Server, dynamic domain name service).
User can use the DDNS account to access the NVR.

1. Go to Main Menu > Networks > DDNS.

The DDNS interface is displayed.

Figure 93 DDNS Interface



2. Enable function, choose the protocol from drop-down list, no_ip / autodns / dyndns / 3322.
3. Enter the domain name.
4. Enter the DDNS account user name and password.

5. Click APPLY to complete the settings.

Port Mapping

You can map the relationship between the LAN and the WAN to access the Device on the LAN through the IP address on the WAN.

1. Go to Main Menu > Networks > Port Mapping.

The Port Mapping interface is displayed.

Figure 94 Port Mapping Interface

2. Enable the function to start set the parameters.
3. You can choose auto or manual mode to set.
4. Configure the settings for the manual port parameters.

Table 33 Port Mapping Parameters

Parameter	Description
HTTP Port	The default value setting is 80. You can enter the value according to your actual situation. If you enter other value, for example, 70, and then you should enter 70 after the IP address when logging in the Device by browser.
HTTPS Port	HTTPS communication port. The default value setting is 443. You can enter the value according to your actual situation.
Control port	The default value setting is 30413. You can enter the value according to your actual situation.

Note: The manual port range should be 1025-66534.

5. Click APPLY to complete the settings.

In the browser, enter http:// IP: HTTP port. You can visit the LAN Device.

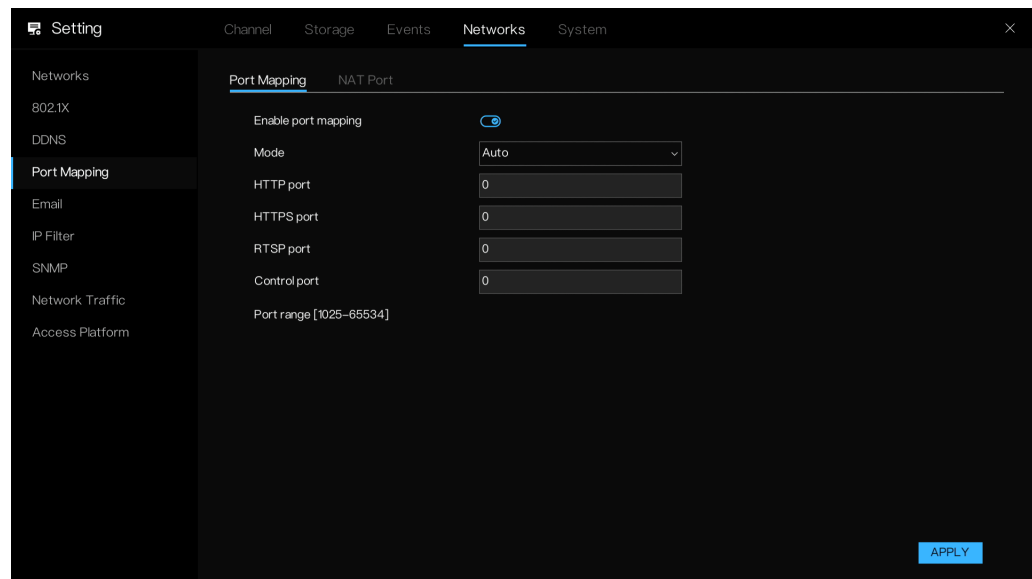
NAT Port

NAT port (network address translation) user can through NAT port to access the channels of NVR. User can set the start port, and it will generate the end port automatically. We will view the NAT port when we access the channel through clicking  icon at Web interface.

1. Go to Main Menu > Networks > Port Mapping > NAT Port.

The NAT Port interface is displayed.

Figure 95 NAT Port Interface



2. Enable the function to set port.
3. Click APPLY to complete the settings

Email

If the simple mail transfer protocol (SMTP) function is enabling, the device automatically sends alarm information to specified email addresses when an alarm is generated. User can use two mailboxes to send information.

You can configure the email settings to enable the system to send the email as a notification when there is an alarm event occurs.

1. Go to Main Menu > Networks > Email.

The Email interface is displayed.

Figure 96 Email Interface

Networks

802.1X

DDNS

Port Mapping

Email

P2P

IP Filter

SNMP

Network Traffic

Access Platform

Email Server 1

Email Server 2

SMTP server

SMTP server port

Username

Password

Email sender

Alarm receiver 1

Alarm receiver 2

Alarm receiver 3

TLS encryption

Sending interval(0-600s)

smtp.gmail.com

465

*****@gmail.com

Password

*****@gmail.com

*****@gmail.com

*****@gmail.com

TLS

Off

TLS

Starttls

APPLY

2. Configure the settings for the email parameters.

Table 34 Email Parameters

Parameter	Description
SMTP server	Enter the address of SMTP server of sender's email account.
SMTP server port	Enter the port value of SMTP server. The default value setting is 25. You can enter the value according to your actual situation.
Username	Enter the username and password of sender's email account.
Password	
Email sender	Enter the email address of mail receiver(s).
Alarm Receivers	Enter the emails of receivers that you want to receive the notification. The Device supports up to three mail receivers.
TLS encryption	Select the encryption type: TLS (default value), Starttls , Off . Set the parameter based on the encryption mode support by the SMTP server.
Sending Interval(0-600s)	This is the interval that the system sends an email for the same type of alarm event, which means, the system does not send emails caused by frequent alarm events. The value ranges from 0 to 600. 0 means that there is no interval.
TEST	Click TEST to test the email sending function. If the configuration is correct, the receiver's email account will receive the email. Before testing, click Apply to save the settings.

3. Click APPLY to complete the settings.

P2P

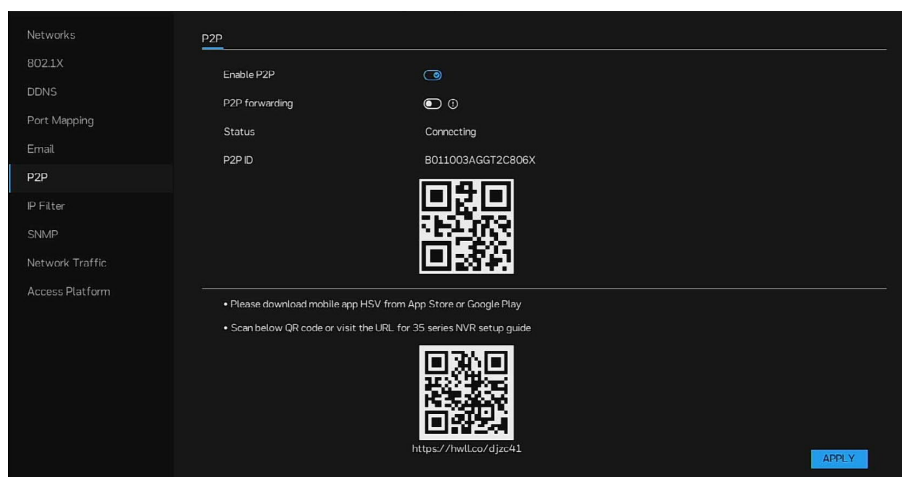
P2P is a kind of convenient private network penetration technology. You do not need to apply for dynamic domain name, doing port mapping or deploying transit server. You can add NVR devices through the below way to achieve the purpose of managing multiple NVR devices at the same time.

Note: Connect the NVR device to the Internet, otherwise P2P cannot run properly.

1. Go to Main Menu > Networks > P2P.

The P2P interface is displayed.

Figure 97 P2P Interface



2. Enable the P2P function.

After the P2P function is enabled and connected to the Internet, the system will collect your information for remote access, and the information includes but not limited to MAC address and device serial number.

3. Enable P2P forwarding.

The device information will be forwarded by the P2P servers to keep connecting when the connection between the mobile phone client/HSV platform and the device is failed.

- Note:*
- *There may be security risks to enable P2P forwarding. Please use this feature with caution.*
 - *Users can scan the below second QR code to get the NVR setup guide.*

You can start adding the device by:

- HSV mobile phone client: Use your mobile phone to scan the QR code to add the device into the mobile phone client.
- HSV PC client: You can choose P2P to add a device by HSV PC client.

For security, you must log in to the cloud account before adding a device via P2P.

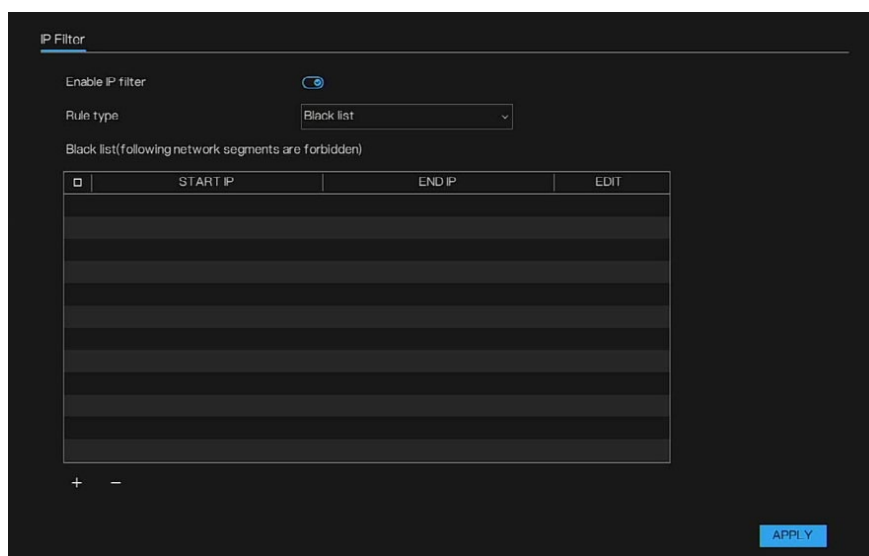
IP Filter

You can set whitelist which are allowed the IP address to access the NVR, or set blacklist which are forbidden the IP address to access the NVR.

1. Go to Main Menu > Networks > IP Filter.

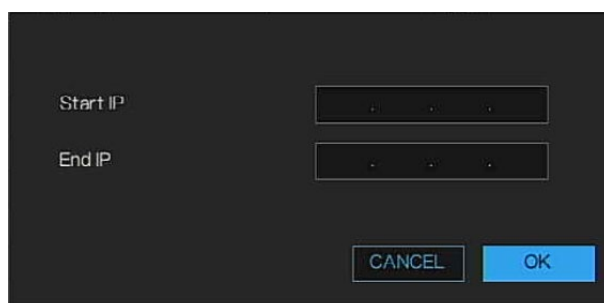
The **IP Filter** interface is displayed.

Figure 98 IP Filter



2. Enable the function, choose the rule type (blacklist or whitelist).
Black list: IP address in specified network segment to prohibit access.
White list: IP address in specified network segment to allow access
Select a name in the list and click Delete to delete the name from the list.
Select a name in the list and click Edit to edit the name in the list.
Only one rule type is available, and the last rule type set is efficient.

Figure 99 Add IP to Filter



3. Click OK to save the IP filter.
4. Select the setting IP, click – to delete the IP segments.
5. Click APPLY to complete the settings.

SNMP

You can connect the device with some software such as MIB Builder and MG-SOFT MIB Browser to manage and control the Device from the software.

- Install the software that can manage and control the SNMP, such as MIB Builder and MG-SOFT MIB Browser
- Obtain the MIB files that correspond to the current version from the technical support.

Note: This function is for some series only.

1. Go to Main Menu > Networks > SNMP.

The SNMP interface is displayed.

Figure 100 SNMPv1/2

SNMPv1/2 SNMPv3

SNMPV1	☒
SNMPV2C	☒
Write community	
Read community	
Trap address	
Trap port	162
Trap community	

APPLY

Figure 101 SNMPV3

The screenshot shows a configuration window for SNMPV3. At the top, there are tabs for 'SNMPv1/2' and 'SNMPV3', with 'SNMPV3' being the active tab. Below the tabs, there's a section for 'Read security' and a section for 'Write security'. Each section contains the following parameters: 'Security name' (text input), 'Security level' (dropdown menu set to 'noauth'), 'Auth algorithm' (dropdown menu set to 'MD5'), 'Auth password' (password input field), 'Encry algorithm' (dropdown menu set to 'DES'), and 'Encry password' (password input field). An 'APPLY' button is located at the bottom right of the window.

2. Configure the settings for the SNMP parameters and click APPLY.

Table 35 SNMP Parameters

Parameter	Description
SNMPV1	Version of SNMP. SNMPV1 and SNMPV2C use communities to establish trust between managers and agents. Agents support three community names, write community, read community and trap
SNMPV2C	
Write community	Name of write community.
Read community	The write community only can modify data.
Trap address	Name of read community.
Trap port	The write community only can read data.
Trap community	IP address of the trap.
SNMPV3	Management port of accepting message from trap.
Read security name	community string of trap.
Write security name	The trap community string allows the manager to receive asynchronous information from the agent.
Security level	Version of SNMP.
Auth algorithm	SNMPv3 uses community strings, but allows for secure authentication and communication between SNMP manager and agent.
Auth password	Name of read security.
Encry algorithm	Name of write security.
Encry password	Security Level between SNMP manager and agent, includes three levels:

- 3. Compile the two MIB files by MIB Builder.
- 4. Run MG-SOFT MIB Browser to load in the module from compilation.

- 5. On the MG-SOFT MIB Browser, enter the Device IP that you want to manage, and then select the version number to query.
- 6. On the MG-SOFT MIB Browser, unfold the tree-structured directory to obtain the configurations of the Device, such as the channels quantity and software version.

Network Traffic

At the **Network Traffic** interface, you can view the send rate and receive rate. The status of LAN(S) are shown in list.

Go to **Main Menu > Networks > Network Traffic**. The Network Traffic interface is displayed.

Figure 102 Network Traffic Interface



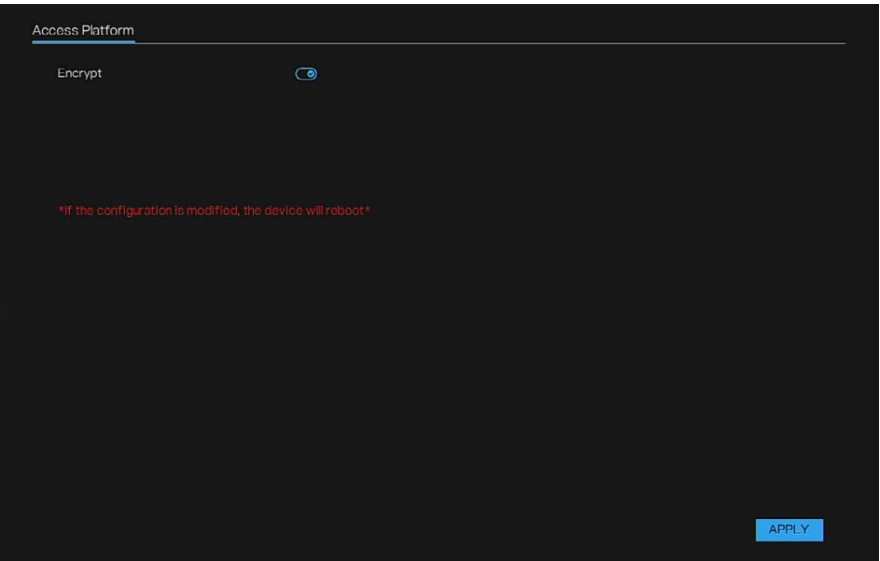
Access Platform

The NVR can access to HSV platform, enable to encrypt the connection.

- 1. Go to **Main Menu > Networks > Access Platform**.

The Access Platform interface is displayed.

Figure 103 Access Platform Interface



- 2. Encrypt the device, when you add the NVR to HSV platform, choose the private protocol(encrypt).
- 3. Click APPLY to save the settings.

Configuring System Settings

Information

Basic Information

Go to **Main Menu > System > Information**. You can check device basic information such as **System, Networks, Channel, Disk, and Alarm**.

Figure 104 Network Status

Information	System	Networks	Channel	Disk	Alarm
General	Status Online				
User Account	IP address 192.168.32.219				
Security Center	Subnet mask 255.255.0.0				
Layout	Default gateway 192.168.32.254				
Auxiliary Screen	MAC address 00:1E:A4:00:64:12				
Logs	DHCP On				
Maintenance	Preferred DNS server 192.168.32.254				
	Alternate DNS server 8.8.8.8				
	Total bandwidth 1000.00 Mbps				
	Received packets 13.14 Mbps				

Figure 105 System Status

Information	System Networks Channel Disk Alarm				
	General				
	Device ID		B011003AGDI18J29B6		
	Device name		Device		
	Device type		NVR		
	Model		NVR3908E2-P8E-J		
	Firmware version		122.2.0.20220524		
	HDD number		2		
	Channels supported		8		
	Alarm in		6		
	Alarm out		2		
	Audio in		1		
	Audio out		1		

Figure 106 Channel Status

Information	System Networks Channel Disk Alarm					
	General					
	CHANNE	NAME	STATUS	VIDEO FORMAT	RESOLUTION	BITRATE(KBPS)
	CH1	Channel01	Online	H264/H264	2592*1944/704*576	2048/700
	CH4	Channel04	Online	H264/H264	2304*1296/704*480	2048/700
	CH5	Channel05	Online	H264/H264	2304*1296/704*480	2048/700
	CH7	HCS-WLEBR2	Online	H264/H264	1920*1080/704*480	6144/1024

Figure 107 Disk Usage

Information	System Networks Channel Disk Alarm					
	General					
	DISK	CAPACITY	USED	SN	DISK MODEL	STATUS
	Disk1	1 TB	197 GB	Z9CEAV5B	ST1000VX005-2EZ102	Normal

Figure 108 Alarm Status

Information		System	Networks	Channel	Disk	Alarm
General						
User Account						
Security Center						
Layout						
Auxiliary Screen						
Logs						
Maintenance						
		CHANNEL	NAME	MODE	ENABLE	RECORDING CHANNEL
		Local-1	Sensor 1	N/O	On	
		Local-2	Sensor 2	N/O	On	
		Local-3	Sensor 3	N/O	On	
		Local-4	Sensor 4	N/O	On	
		Local-5	Sensor 5	N/O	On	
		Local-6	Sensor 6	N/O	On	
		Local->1		Close		
		Local->2		Close		

General

System

1. Go to Main Menu > System > General > System.

Figure 109 System

Information	System	Date And Time	Time Zone	DST	Sync Camera Time				
	General								
	User Account								
	Security Center								
	Layout								
	Auxiliary Screen								
	Logs								
	Maintenance								
	Device name	Device							
	Output resolution	1920x1080							
	Language	English							
- When auxiliary screen is enabled,output resolution only works for HDMI main monitor									
- When auxiliary screen is disabled,output resolution works for both HDMI & VGA									
APPLY									

2. Input the device name.
3. Choose the output resolution and language.
4. Click APPLY to complete the settings.

*Note: For device name, special characters such as {} *<>?!#\$\$~\ are not supported in the web interface.*
If you modify the Output resolution, the device will restart.
When the auxiliary screen is enabled, the output resolution only works for HDMI main monitor; When the auxiliary screen is disabled, the output resolution works for both HDMI & VGA. VGA supports up to 1080p.

Date And Time

1. Go to Main Menu > System > General > Date And Time.

Figure 110 Date and Time

2. Configure the settings for date and time parameters.

Table 36 Data and Time Parameters

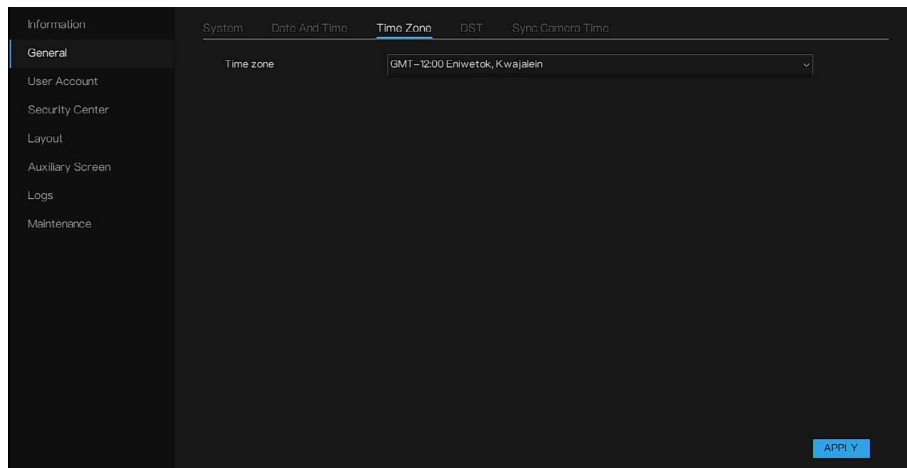
Parameter	Description
Date format	Select a date format for the system.
Time format	Select 12H or 24H for the time display style.
Enable NTP	Enable the NTP function to sync the Device time with the NTP server.  If NTP is enabled, device time will be automatically synchronized with server.
NTP server	Choose the NTP server to synchronize.
Sync time frequency (sec)	Sync the NTP server for the setting time.  Do not change the system time randomly; otherwise the recorded video cannot be searched. It is recommended to avoid the recording period or stop recording first before you change the system time.
Date (Time)	If user don't enable the sync time, you can modify the Date (Time) manually.

3. Click APPLY to save settings.

Time Zone

1. Go to Main Menu > System > General > Time zone.

Figure 111 Time Zone

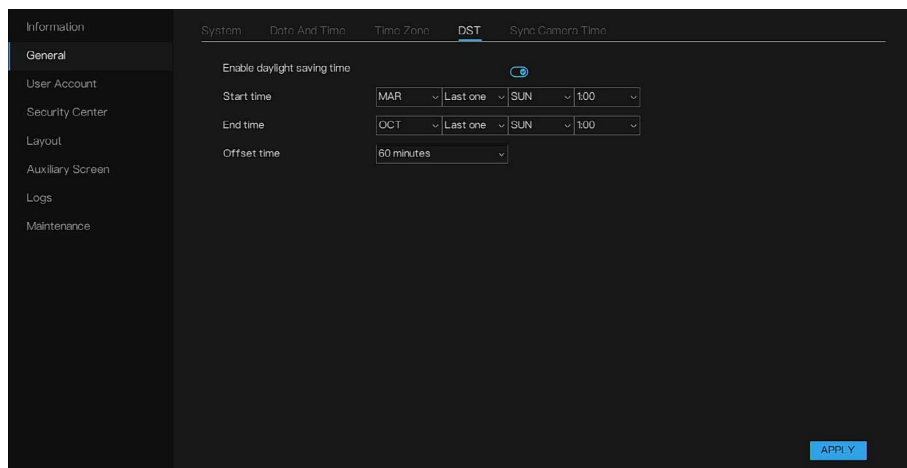


2. Choose time zone from the drop-down list.
3. Click APPLY to save settings.

DST

1. Go to Main Menu > System > General > DST.
2. Enable the daylight saving time function.

Figure 112 DST



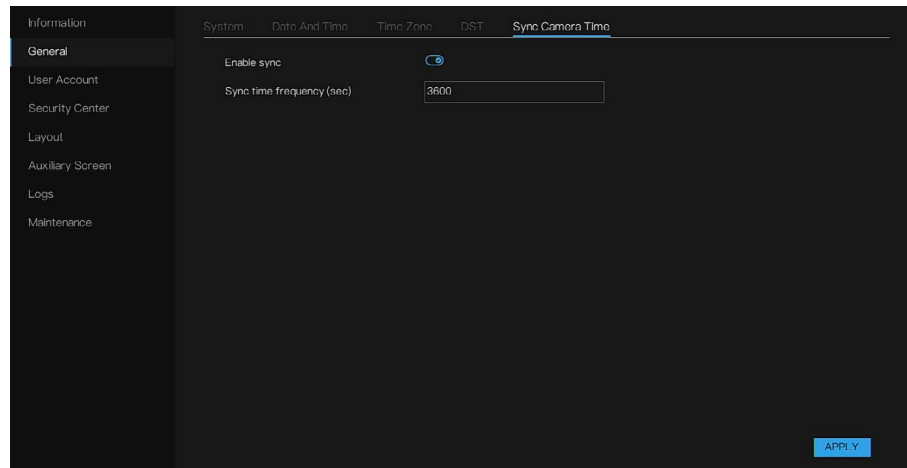
3. Configure the start time and end time for the DST. For the start time, the time will delay one hour (or half hours, it depends on the local rules).
4. Click APPLY to save settings.

Note: The DST setting will affect the recording time. The start time will null 60 minutes (default value) / 30 minutes / 120 minutes. The end time will have two parts recording.

Sync Camera Time

1. Go to Main Menu > System > General > Sync Camera Time.
2. Enable the sync camera time function.

Figure 113 Sync Camera Time



3. Input the sync time frequency.
4. Click APPLY to save settings.

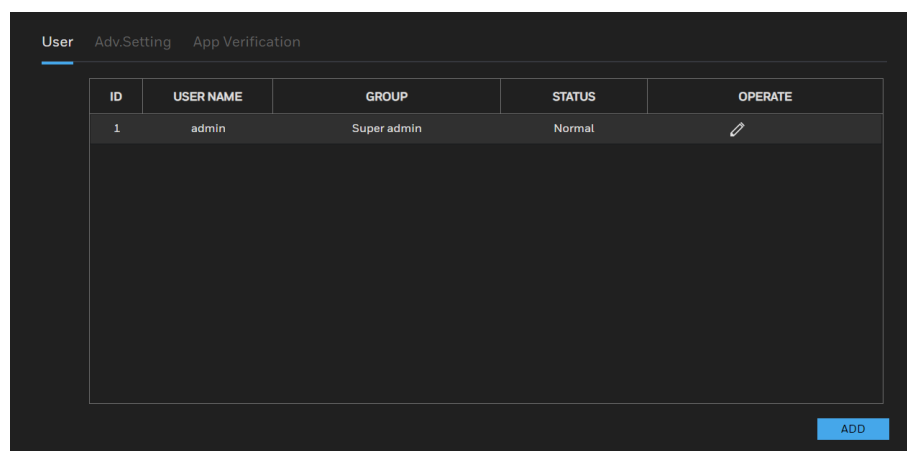
User Account

User

In User interface, you can edit the current account and create new users accounts.

1. Go to Main Menu > System > User Account > User.

Figure 114 User



2. Click  to modify account information, click OK to save the setting.

Figure 115 Edit User

Edit User

User name: admin

Password: *****

Confirm password: *****

Group: Super admin

Change password frequency: Never

☒ Live preview

☒ PTZ

☒ Playback

☒ Channel management

☒ Device management

☒ System management

☒ Backup

☒ System maintenance

☒	CHANNEL
☒	CH1
☒	CH2
☒	CH3
☒	CH4
☐	
☐	
☐	

Live preview

CANCEL OK

3. Click ADD to add new account.

Figure 116 Add User

Add User

User name:

Password: Password

Confirm password: Password

Group: Administrators

Change password frequency: Never

Password expire date: ☐

☒ Live preview

☒ PTZ

☒ Playback

☒ Channel management

☒ Device management

☒ System management

☒ Backup

☒	CHANNEL
☒	CH1
☒	CH2
☒	CH3
☒	CH4
☐	
☐	
☐	

Live preview

CANCEL OK

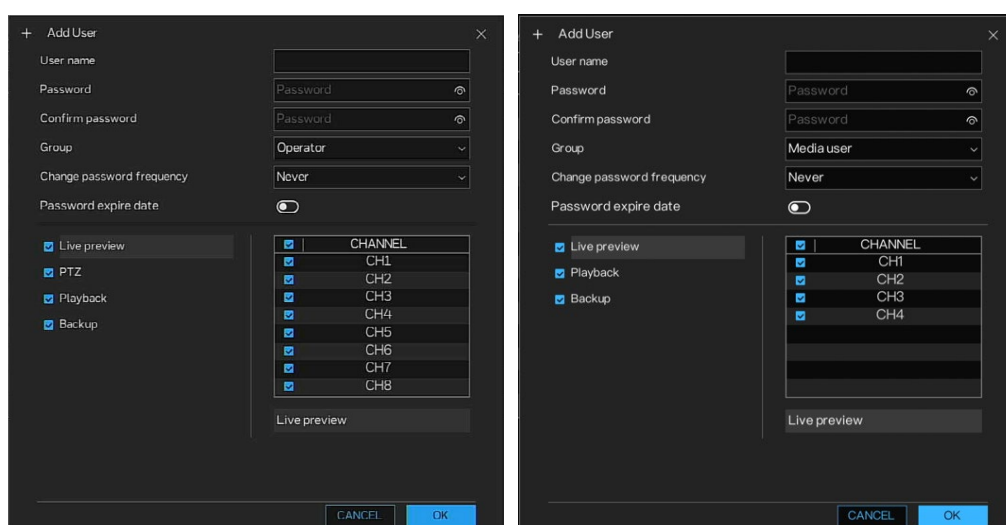
4. Enter the user name, password, select the group it belongs to from the drop-down list, set the change password frequency. Then you can

check the corresponding rights for current user.

Table 37 Add Interface Parameters

Parameter	Description
User Name	Enter a user name and password for the account.
Password	For user name should meet the rules: only these special characters are supported !@#\$%+*=~?&"'`()./':;<>?^ ~[] Password requirement; -The password must be between 8 to 20 -Upper & lower case letters -At least on number -Support the symbol -_@%^.~?#=\$+=";.& only and must contain at least one of them -The first character must be a number or letter -No space
Confirm password	Re-enter the password.
Group	Select a group for the account, there are three groups, administer/ operator /media user. The user rights must be within the group permission.
Change password frequency	To keep safety of device to modify the password regularly.
Password expire date	Enable to set the duration of user account.

Figure 117 Permission



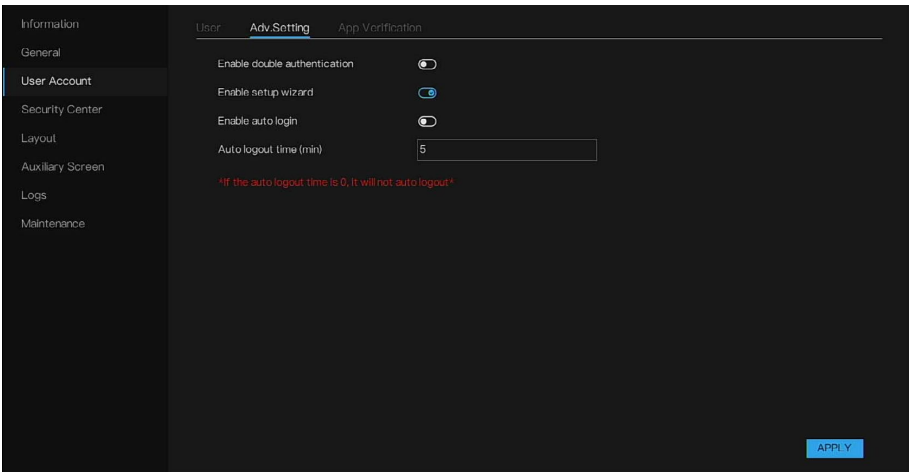
5. Click OK.

Click  to modify the corresponding user information, click  to delete the user.

Adv. Setting

- Go to Main Menu > System > User Account > Adv. Setting.
The Adv. Setting interface is displayed.

Figure 118 Advance Setting

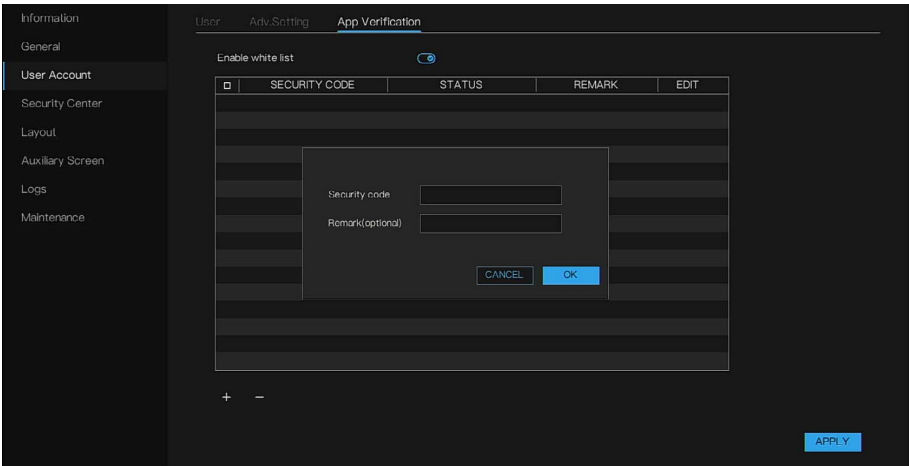


2. Enable Double Authorization which needs two accounts login for authorization. Only non-admin users need authentication after logging in for playback, and only admin users can be used for authentication.
3. Enable Setup Wizard and the wizard will be showing when device power on.
4. Enable Auto login and the device is always login. Else the device will auto logout after setting time.

App Verification

On the App verification page, you can add security code for the NVR, and then this NVR can be managed by App. When adding the NVR on App, you need to fill in the security you have set.

Figure 119 App Verification



For security code, there are three types of status:

Not activated: The security code is free to be set on the App.

Online/Offline: The APP bound with this security code is/isn't connecting to the NVR.

Figure 120 Input Security Code on App

10:30

< IP/Domain Save

Nickname

Protocol Private Protocol(encrypted) >

IP Address/DDNS

Port 30143

Username admin

Password

Security Code

- Note:**
- You can add maximum 20 security codes to an NVR and can modify the remarks of them. One security code applies to one APP client. A security code can only be set as numbers up to 32 digits.
 - One NVR can support maximum 8 APPs for connection and use at the same time, including UI, Web, App and platform.

Security Center

Note: This function is for admin user only.

Password

1. Go to Main Menu > System > Security Center > Password.
The Password interface is displayed.

Figure 121 Password

The screenshot shows the 'Security Center' menu on the left with 'Password' selected. The main area has three tabs: 'Password', 'Unlock Pattern', and 'Security Question'. Under the 'Password' tab, there are three input fields: 'Old password', 'New password', and 'Confirm password', each with a 'Password' placeholder and an eye icon. Below these fields are five password requirements: 'The password must be between 8 to 20', 'Upper & lower case letters', 'At least one number', 'Support the symbols ~!@%*~?~\$~+~& only and must contain at least one of them', and 'The first character must be a number or letter'. There is also a 'No space' requirement. An 'APPLY' button is at the bottom right.

2. Enter the old password, new password and confirm new password.
3. Click APPLY to save the settings.

Unlock Pattern

1. Go to Main Menu > System > Security Center > Unlock Pattern.

The Unlock Pattern interface is displayed.

Figure 122 Unlock Pattern

The screenshot shows the 'Security Center' menu on the left with 'Unlock Pattern' selected. The main area has three tabs: 'Password', 'Unlock Pattern', and 'Security Question'. Under the 'Unlock Pattern' tab, there is a 'Password' input field with a 'Password' placeholder and an eye icon. Below it is a toggle switch for 'Enable unlock pattern', which is currently turned on. Underneath the toggle is a 'PATTERN SETTING' button. An 'APPLY' button is at the bottom right.

2. Input password, and enable unlock pattern so that user login device by drawing pattern.
3. Click PATTERN SETTING to set pattern.
4. Click APPLY to save the setting.

Security Question

You can set security questions and answers. After you successfully answered security questions, you can reset admin account password.

1. Go to Main Menu > System > Security Center > Security Question.

The Security Question interface is displayed.

Figure 123 Security Question

2. Input the password.
3. Input proper security questions and answers.
4. Click APPLY.

After you successfully set security questions, you can answer the security questions to reset admin password.

Layout

Set viewing video mode, dwell time in display screen. The layout is set multiple pages to auto sequence.

1. Go to Main Menu > System > Layout.

The Layout interface is displayed.

Figure 124 Layout

2. Click + to add a new layout. The default layout is one splitting screen.
3. Input the layout name, select dwell time from the SEQ Dwell time drop-down list (the display screen will loop play the real time video according to setting time).

4. Choose the mode of splitting screen at the page bottom; set the display mode of channels by dragging channel to the specific location, or choose the location first, then click the channels to place. One splitting screen can play several channels, the auto sequence is playing as the set pages, for example the first split screen is set two pages (channel 1 and 2), the second split screen is set one page (channel 3), when enable to auto sequence, the showing is channel 1 and channel 3, then show channel 2 and channel 3.
5. Click APPLY to save the setting.

Note: User can add up to 16 layouts.

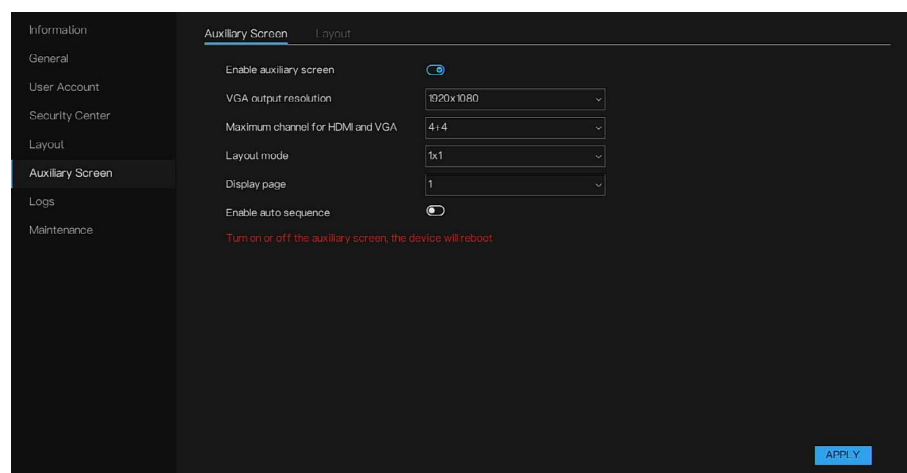
Auxiliary Screen

- Note:*
- This function is only applicable for the devices with 8 or more than 8 channels. The main screen is connected by HDMI and the auxiliary screen is connected by VGA. The most supported resolution is 1080p.
 - Devices for HN350401xx / HN35040100N only support copy screen which means when the device is connected to two monitors, the monitors display the same content.

1. Go to Main Menu > System > Auxiliary Screen.

The Auxiliary Screen interface is displayed.

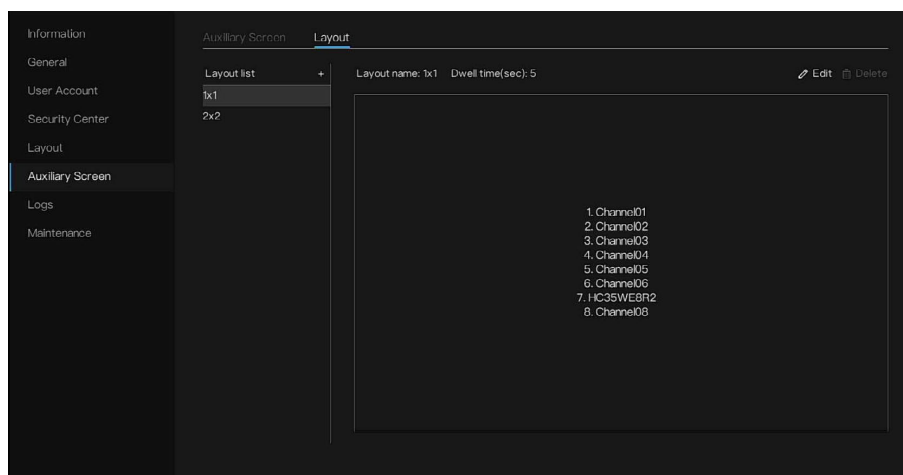
Figure 125 Auxiliary Screen



2. Enable the auxiliary screen.
3. Set the VGA output resolution. The most recommended resolution is 1920*1080.
4. Set the Maximum channel for HDMI and VGA as “half+half” of the channels number of the device. For example, if the device is 16 channels, the Maximum channel for HDMI and VGA will be “8+8”.

5. Layout mode can be set as 1x1, 2x2 or 1+7 if the device is 16 channels (the chosen mode is depending on the number of channels for the device).
6. Set the display page. The auxiliary screen shows according to the configured display page. The auxiliary screen display can be configured on Layout tab. The number of the display page depends on the configured layout mode. For example, if you set the layout mode as 2 x 2 for a device with 16 channels, you can choose 1/2/3/ 4 for Display page.

Figure 126 Auxiliary Screen – Layout



7. Enable the auto sequence and the auxiliary screen will automatically sequence according to the configured layout.
8. Click APPLY.

Logs

You can view and search the log information, or backup log to the USB device.

Note: The log record size should not be larger than 20M. If the logs number is larger than 163840, the oldest log will be covered. Users can search up to 16384 logs every time. If the number of searching logs is larger than 16384, you should reduce the search time.

When the parameters of device configuration are modified, all operation will be recorded to system logs, including App, local UI, HSV client and web interface. The detailed information will show the logs source. For 127.0.0.1, it comes from the client connected by P2P or MPC; For IP address, it comes from web interface or HSV client connected by local network; For local UI, it comes from local UI interface.

System Log

1. Go to Main Menu > System > Logs > System Log.

The System Logs interface is displayed.

Figure 127 Logs - System Log

Information

General

User Account

Security Center

Layout

Auxiliary Screen

Logs

Maintenance

System Log

Event Log

Start date

29/05/2022

Start time

23:36:54

End date

29/05/2022

End time

23:36:54

Type

Operationlog

SEARCH

EXPORT

ID	START TIME	CHANNEL	LOG TYPE	INFORMATION
1	29/05/2022 23:30:27	--	Login	[admin] 127.0.0.1 login
2	29/05/2022 23:28:55	--	Logout	[admin] 127.0.0.1 logout
3	29/05/2022 23:11:08	--	Login	[admin] 127.0.0.1 login
4	29/05/2022 21:48:12	--	Logout	[admin] 127.0.0.1 logout
5	29/05/2022 21:48:11	--	Power on	system
6	29/05/2022 21:17:10	--	Reboot	[admin] 127.0.0.1
7	29/05/2022 21:46:35	--	Login	[admin] 127.0.0.1 login
8	29/05/2022 21:31:38	--	Logout	[admin] 127.0.0.1 logout
9	29/05/2022 21:31:34	--	Power on	system
10	29/05/2022 21:30:33	--	Reboot	[admin] 127.0.0.1
11	29/05/2022 21:21:04	--	Login	[admin] 127.0.0.1 login
12	29/05/2022 21:20:49	--	Logout	[admin] 127.0.0.1 logout
13	29/05/2022 21:20:48	--	Power on	system
14	29/05/2022 21:19:45	--	Reboot	[admin] 127.0.0.1
15	29/05/2022 21:12:44	--	Login	[admin] 127.0.0.1 login

<<

1/2

>>

2. In the Start Time box and End Time box, enter the time period to search.
3. In the Type list, select the log type that you want to view and click SEARCH.
4. The search results are showing, click EXPORT to back up the result to USB disk.

Event Log

1. Go to Main Menu > System > Logs > Event Log.

The Event Logs interface is displayed.

Figure 128 Event Log

[illegible]

2. In the Start Time box and End Time box, enter the time period to search.
3. In the Type list, select the log type that you want to view and click

SEARCH.

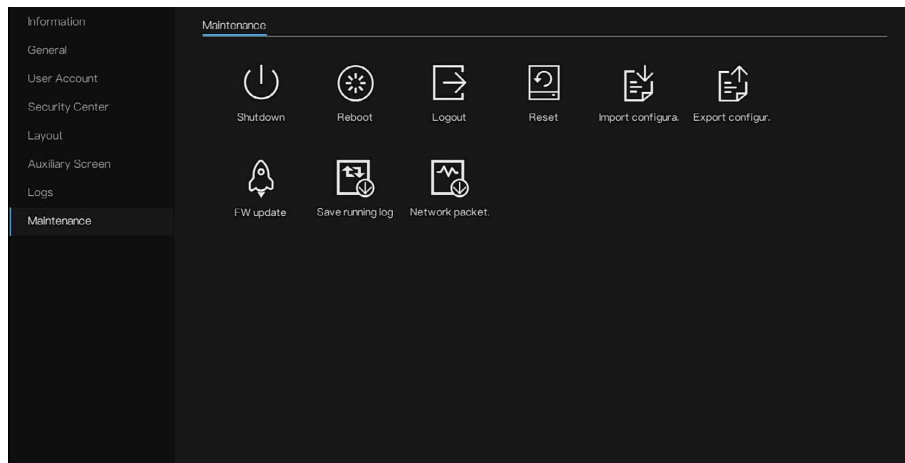
4. The search results are showing, click EXPORT to back up the result to USB disk.

Maintenance

1. Go to Main Menu > System > Maintenance.

The Maintenance interface is displayed.

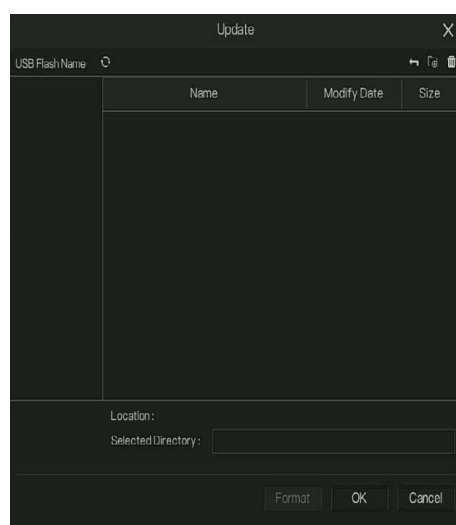
Figure 129 Maintenance



2. Click Shutdown/Reboot/Logout/Reset or update to operate NVR if you need.
3. Click FW Update to update the firmware.

Note: It takes about five minutes to update firmware and then will jump to login interface automatically. If you don't want to wait for five minutes, when the pop-up window shows update 99%, press F5 to refresh the web to go to the login interface.

Figure 130 Update Interface



4. Import and export configuration.

Note: Make sure the USB storage device is inserted; otherwise the upgrading cannot be performed.
When starting the Device, the system automatically checks whether there is a USB storage device connected and any U-boot upgrade file. If yes and the check result of the upgrade file is correct, the system will upgrade automatically.

Exporting System Settings

You can export or import the device system settings if there are several devices that require the same setup.

Note: The Import/Export interface cannot be opened if the backup operation is ongoing on the other interfaces.
When you open the Import/Export interface, the system refreshes the devices and sets the current directory as the first root directory.
Click Format to format the USB storage device.

1. Go to Main Menu > System > Maintenance > Import/Export Configuration.
2. Insert a USB storage device into one of the USB ports on the device.
3. Click Import Configuration / Export Configuration to refresh the interface.

Network Packet Capture

Note: If the NVR is plugged with the USB disk, click the network packet capture and set the relevant parameters of the packet capture. The captured data can be downloaded and used for device problem analysis.

1. Go to Main Menu > System > Maintenance > Network Packet Capture.
2. Click Network Packet Capture to enter.

Figure 131 Network Packet Capture interface

NIC	IP	STATUS	CAPTUR.
LAN1	192.168.0.247	—	☒

3. Choose the USB path to save the file.
4. Set the port, IP, number of packets captured. The default settings are All, you can choose custom to set.
5. Click START to capture. Click STOP to end capturing. You can analysis the file.

Configuring MAXPRO Cloud

This function is only applicable for some models.

Figure 132 MAXPRO Cloud Interface

Enable MAXPRO cloud integration ☒

MAXPRO cloud registration URL

MAXPRO cloud connection ●

* Record Schedule, Motion, SMD, and Local Intelligent Analysis will be unmodifiable when MPC is enabled *

DEFAULT APPLY

Note: Record Schedule, Motion, SMD and Local Intelligent Analysis page will be disabled when MAXPRO Cloud function is enabled.

Configuring Live View Settings

After you logged in, the system goes to main menu, click Live view. You can view the monitor video of each channel.

The displayed window amount may vary. The actual product shall prevail.

Live View

On the live view interface, you can view the monitor video of each channel. The corresponding channel displays date, time, and channel name after you overlay the corresponding information. Refer to the following table for detailed information.

Figure 133 Live View Interface

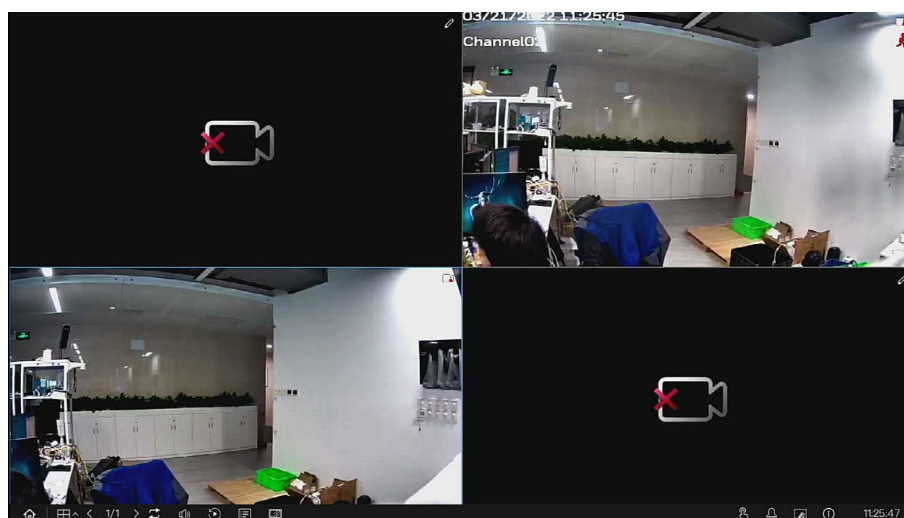
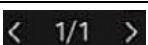


Table 38 Navigation Bar Icons

Icon	Description
	Main menu
	Layout, choose or set the layout to display live view.
	Switch to next page of layout.
	Auto sequence, click to play the live view automatically by layout screen.
	Volume, adjust the volume of Audio Out.
	Playback, click icon to enter the playback interface. The detail please refer to Playback
	Channel information, select to show channel No. or Stream information. Choose the channel, and the information can be showing on live view.

Icon	Description
	Live view strategy, there are three modes, fluency / balanced / real-time.
	Manual alarm, click to enter manual alarm pop-up window. Operate manually the NVR IO alarm input port and channel cameras alarm in ports.
	Event list, show real-time alarm messages.
	Mute alarm
	Clear alarm.
	Information, network, system, channel, disk, alarm information.
	The time of NVR.
	The current channel is recording.
	Alarm, the current channel has motion detection alarm.

Figure 134 Manual Alarm

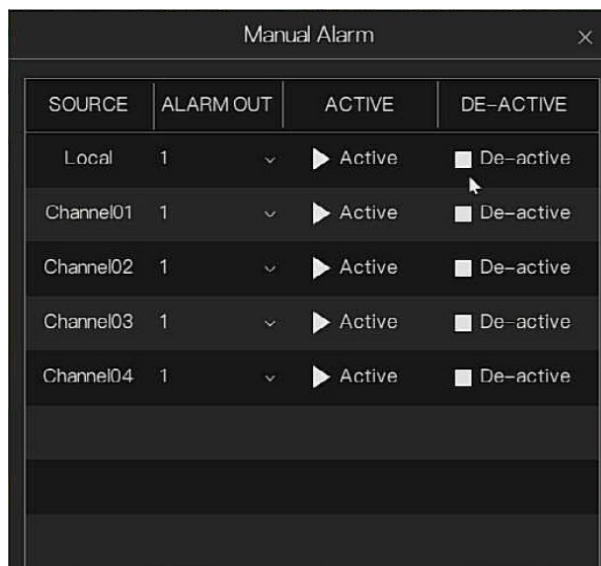


Figure 135 Events List Pop-up Window

Events List			×
CHANNEL	TYPE	START TIME	
Channel3	Motion detection	2022/03/29 11:19:56	
Channel3	Motion detection	2022/03/29 11:09:03	
Channel2	Motion detection	2022/03/29 10:48:42	
Channel3	Motion detection	2022/03/29 10:16:52	
Channel2	Motion detection	2022/03/29 10:16:38	
Channel2	Motion detection	2022/03/29 10:05:22	
Channel3	Motion detection	2022/03/29 10:05:11	
Channel3	Video loss	2022/03/29 10:02:17	
Channel2	Video loss	2022/03/29 10:02:16	
---	Network disconn.	2022/03/29 10:02:04	
Channel2	Motion detection	2022/03/29 09:59:49	
Channel3	Motion detection	2022/03/29 09:59:48	

Live View Control Interface

Move your mouse to the video of current channel and left-click mouse; you can see system pops up the live view control interface.

Right-click mouse on live view interface, the control bar hides.

- Note:**
- *Disable the navigation bar if it is displayed on the interface before using this function.*
 - *The live view control interface is different depending on the model, and the actual interface shall prevail.*

Figure 136 Live View Control Bar



Table 39 Live view Control Icons

Icon	Description
	Record: manual record The playback time bar shows as yellow
	Instant playback Click to replay instantly. Refer to Instant Playback .
	Audio Open or close the channel audio
	PTZ It uses for monitored and PTZ cameras, click icon to enter PTZ interface, more detail please refer to PTZ Control

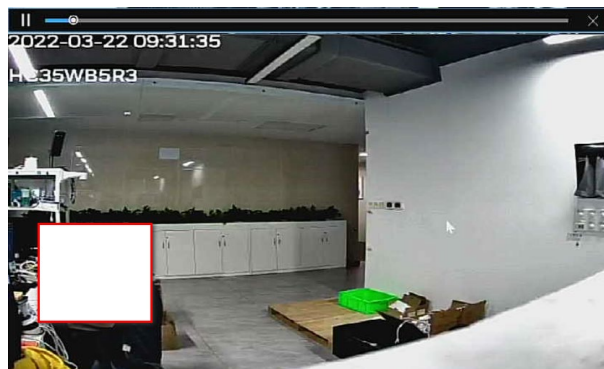
Icon	Description
	Digital zoom
	Image For the detail information, refer to Sensor Setting
	Two-way audio Refer to Two-way Talk .
	Snapshot Refer to Manual Snapshot .
	Wiper For PTZ cameras with wiper, click to control the camera wiper. Each time you click the icon, the camera wiper swipes once.

Instant Playback

You can play back the previous 5 minutes record of current channel.

Click  to go to the instant replay interface.

Figure 137 Instant Replay Interface



Instant replay is to playback the previous 5 minutes record of current channel.

- Move the slider to choose the time you want to start playing.
- Play, pause and close playback.
- The information such as channel name and recording status icon are shielded during instant playback and will not display until exited.
- During playback, screen split layout switch is not allowed.

PTZ Control

PTZ control panel performs the operations such as directing camera in eight directions, adjusting zoom, focus and iris settings, and quick positioning.

Left-click on the live view screen and then select PTZ. The PTZ control panel is displayed.

Figure 138 PTZ Control Panel

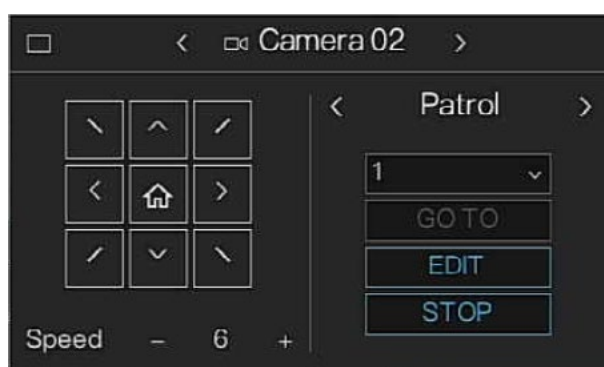


- Note:*
- The gray button means system does not support current function.
 - For some series products, the PTZ function is valid in one-window mode.

Table 40 PTZ Control Panel Parameters

Parameter	Description
Speed	Controls the movement speed. The bigger the value is, the faster the movement will be.
Zoom	: Zoom out : Zoom in
Focus	: Focus far : Focus near
Iris	: Image darker : Image brighter
PTZ movement	Supports eight directions
Preset	Move the PTZ camera to the point location, choose the ID, click SAVE to add to preset; Choose one ID and click GO TO, then the PTZ camera go to preset location directly. There are 255 preset points at NVR, but PTZ cameras can be set 400 preset points; The NVR can only adjust the 1 to 255 preset points of cameras.
Patrol	The NVR set the patrols to adjust serval preset.

Figure 139 Add Patrol Panel



Choose ID (There are four patrols can be added), click **EDIT** to start set;

Click + to add preset to patrol and set the duration of staying, repeat these steps for many times to add more presets to patrol.

***Note:** The added preset cannot be deleted. It can only be overwritten.*

Click **SAVE** to save patrol; Click **REMOVE ALL** to clear preset.

Digital Zoom

You can zoom in specified zone of current channel so that you can view the details. It supports zoom in function of multiple-channel. It includes the following two ways:

- Click , the icon switches to . Move the mouse to enlarge, it up to enlarge to 400%. the left mouse button is released digital zoom.
- Point to the center that you want to enlarge, rotate the wheel button to enlarge the area.

The digital zoom interface is shown as [Figure 140](#). When the image is in the enlarged status, you can drag the image toward any direction to view the other enlarged areas. Right click mouse to cancel zoom and go back to the original interface.

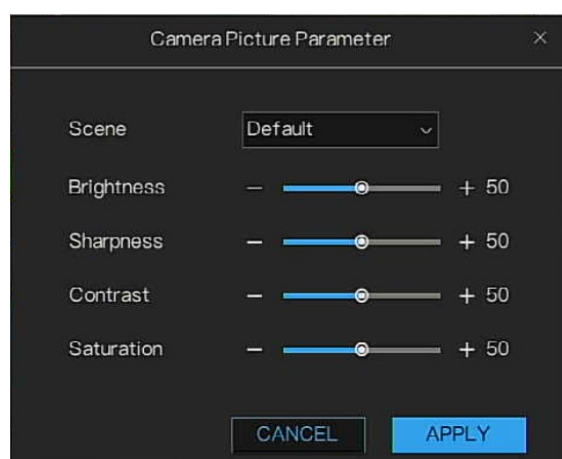
Figure 140 Digital Zoom Interface



Image

You can set the camera picture parameter, such as brightness, sharpness, contrast and saturation.

Figure 141 Camera Picture Parameter Interface



Two-way Talk

You can perform the voice interaction between the Device and the remote device to improve efficiency of emergency.

1. Click  to start two-way talk function the icon now is shown as . Now the rest two-way talk buttons of digital channel become null too.
2. Click  again, you can cancel two-way talk.

Manual Snapshot

You can take snapshots of the video and save into a USB storage device.

By clicking , you can take snapshots. The snapshots are automatically saved into the connected USB storage device. You can view the snapshots on your PC.

Note: When you haven't mounted the USB disk to NVR in advanced and click the snapshot icon, it will prompt "Please mount available devices first".

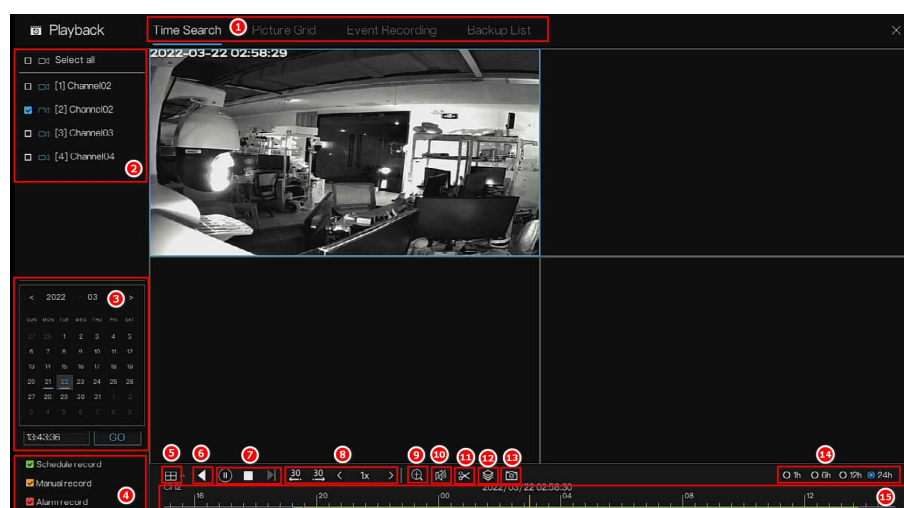
Playback

Time Interface

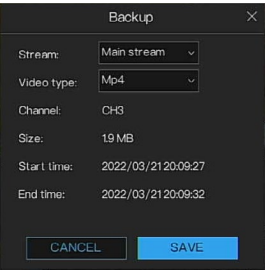
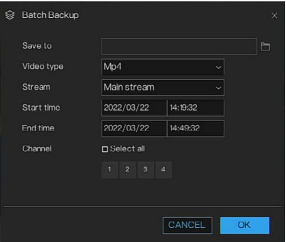
You can search and playback the recorded files on the NVR.

Go to **Main Menu > Playback**, or click  on live view button navigation bar, the playback interface is displayed.

Figure 142 Playback



No. / Icon	Description
1	Choose the playback type, Time Search/Picture Grid/Event Recording/Backup List .
2	Channel list Blue icon  have recording video White icon  have no recording video.
3	Calendar The marked blue dates indicate there's recording video (it means some channels have recording, but not for all channels at some time). Or set the detail time to go the recording video.
4	Different record, select schedule record (green), manual record (yellow), or alarm record(red). The colors are showing the time tar.
5	 : Split screen, display the searched recorded video or picture. It supports playing in single-channel, 4-channel, 9-channel, and 16-channel simultaneously, the actual interface shall prevail.
6	 : Reversed, it plays the key frame.
7	 : Pause / Stop / Next frame, click it to switch between play/pause. User can operate the record as same as live video.
8	 : 30s backward / 30s forward / triple speed- / triple speed +
9	 : Digital Zoom, click icon to enter one screen to digital zoom channel.
10	 : Audio, open or close the channel audio

No. / Icon	Description
11	 : click to start backup, click again to end backup and the pop-up window shows, click SAVE to save the record to USB disk which is mounting on NVR.  The stream and video type can be chosen.
12	 : Batch backup, click icon to enter the pop-up window set the batch backup. Choose the path to save, Video type (MP4 or AVI) and Stream (Main stream or sub stream). Set the Start time and End time . The set time will be the same for multiple channels video downloading. If there's no video for some channels within the set time, there will be no downloaded video for this channel. Choose channels. Click OK to download. The result shows at Backup List interface. 
13	 : Snapshot, snapshot the current image.
14	 Time bar, show the time of record.
15	Display the type and time period of the current recorded video. - Only one-time bar is displayed. - Click on the colored area to start manual record or alarm record. - Time bar colors: Green indicates schedule record; Red indicates alarm record; Yellow indicates manual record. - Click and hold the time bar, then you can drag to view the playback of the target time. - the vertical yellow line is centered, double click the detail time it will be showing on yellow line location.

- Note:**
- The video recording will lose an hour while DST start, because the DST working.
 - The NVR time had to back to last hour while the DST STOP working, so there will be twice video recording at DST end time.
 - When you play DST END TIME video recording, the NVR will always play first video recording, you can't choose the second video recording to play. If you want to play second video recording, you need to wait the first video recording play over and then the NVR will continue play second video recording.
 - If you want to download DST END TIME video recording, you need to choose the period of video recording more than the DST END TIME, then the DST END TIME video recording (the twice videos) will download.

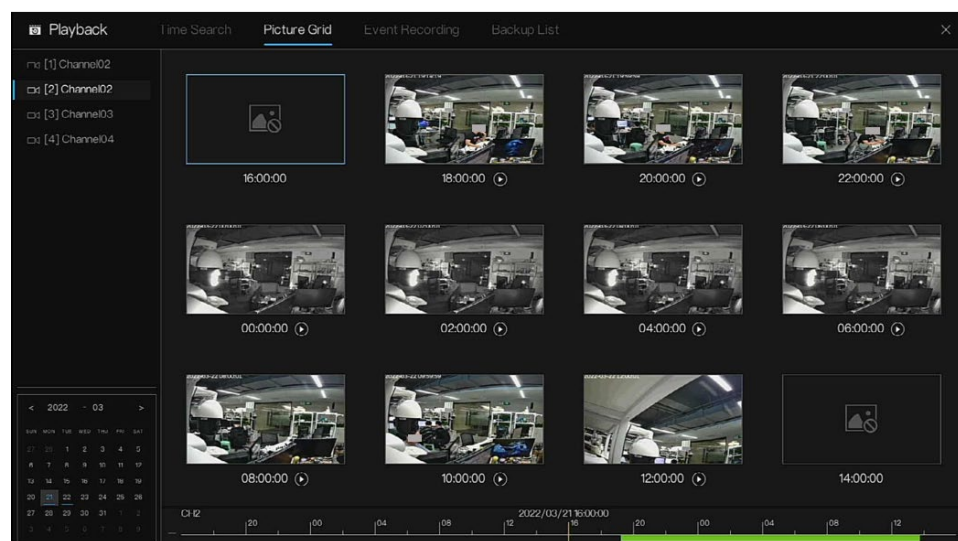
Picture Grid

Picture grid refers to evenly dividing the video of a channel by time range and searching for a video based on thumbnails divided by time range.

1. Go to Main Menu > Playback > Picture Grid.

The Picture Grid interface is displayed.

Figure 143 Picture Grid Interface



2. Select a camera in the camera list on the left side of the picture grid screen. Videos shot by the camera in the earliest time range on the current day are displayed as thumbnails in the window on the right side.
3. Select a day from calendar.
4. A day are dividend to 12 grids, two hours is one grid. double-click the image to dividend to 12 grids again. The minimum grid interval is one minute. Right – click to enlarge grid interval
5. Select a required thumbnail, click  to play the video.

Figure 144 Replay Interface



: Full screen to replay.

Event Recording

Note: Recording limitation: Only support 2 channel main stream and channel number +1 channel sub stream playback at the same time. Both local and remote share the limitation.

Figure 145 Event Recording Page

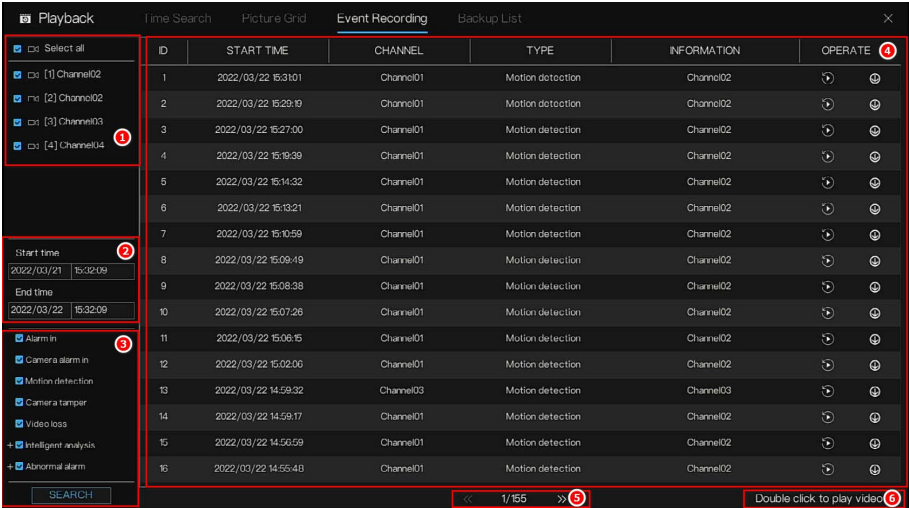
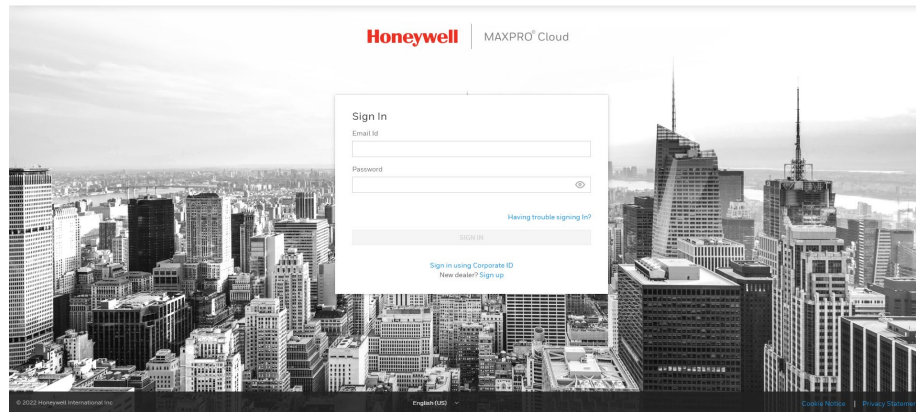


Table 41 Event Recording Parameters Description

No. / Icon	Description
1	Channel list, select to search channels event recording.
2	Set the start time and end time to search.
3	Select the alarm types, Alarm in / Camera alarm in /Motion detection /Camera tamper / Video loss / Intelligent analysis / Abnormal alarm.

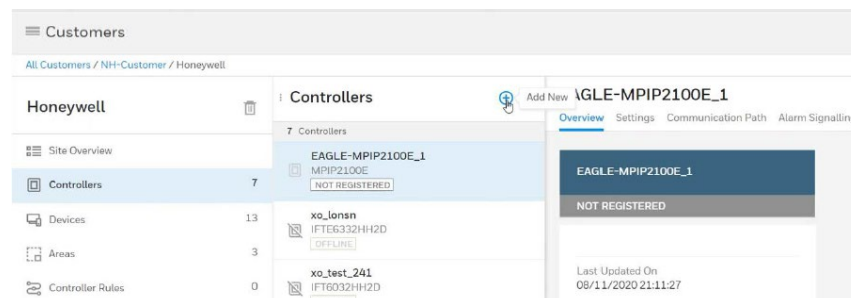
2. Access the MAXPRO Cloud sign in page (<https://mymaxprocloud.com/MPC/Signin>) from your web browser (Google Chrome version 63 or later).
3. Enter the MAXPRO customer user name and password and click SIGN IN.

Figure 147 MAXPRO Cloud Sign in Page



4. Click  and select Customers.
5. Select a customer and the site.
6. Click Controllers and click Add New.

Figure 148 Add New Controllers



7. To add the 35 Series NVR, select Video Recorder as the Controller Type.
8. Enter the MAC ID of the 35 Series NVR.
9. Enter the Controller Name.
10. Select the TimeZone. This TimeZone will be pushed to the NVR.

Figure 149 Add Controller

Add Controller

Controller Type*
Video Recorder

MAC ID * ?
XX:XX:XX:XX:XX:XX

Note: Primary and Secondary stream will default to H.264 compression for onsite and cloud.

Controller Name *
Video Recorder_1

TimeZone *
Select

Notes

CANCEL ADD CONTROLLER

11. Click ADD CONTROLLER. The success message indicates that the NVR is added successfully.

Enable MPC Integration on the 35 Series NVR

1. Login to the 35 Series NVR, go to Setting > MAXPRO Cloud > General Setting.

Figure 150 MAXPRO Cloud

Honeywell | NVR Liveview Playback Event Recording Setting

Camera
Storage
Events
Networks
System
MAXPRO Cloud
General Setting

General Setting

Enable MAXPRO cloud integration ☒

MAXPRO cloud registration URL <https://isom.mpv.mymaxprocloud.co>

MAXPRO cloud connection

* Record Schedule, Motion, SMD, and Local Intelligent Analysis will be unmodifiable when MPC is enabled *

DEFAULT APPLY

Enable MAXPRO cloud integration: Select this checkbox to enable integration with MAXPRO Cloud.

MAXPRO cloud registration URL: The MAXPRO Cloud registration URL.

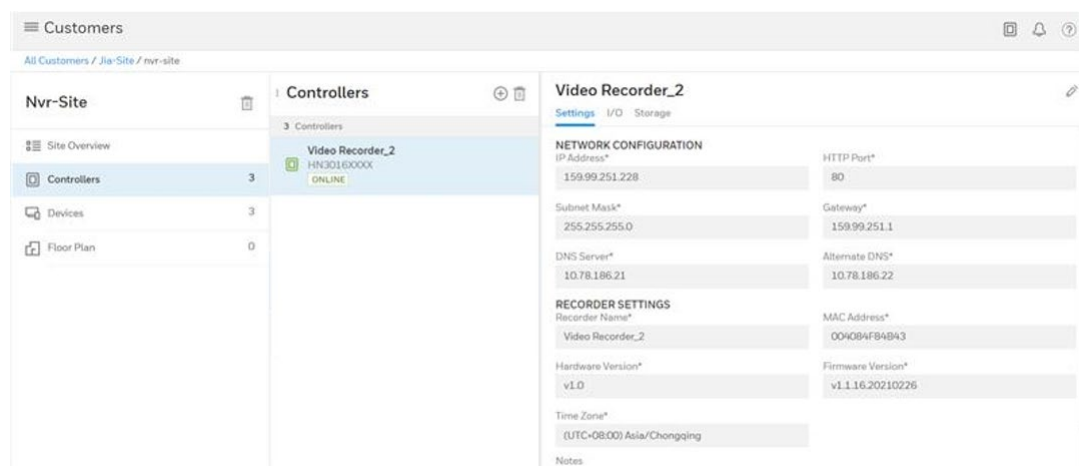
MAXPRO cloud connection: Show the MAXPRO cloud connection status.

2. Click APPLY.

Apply NVR Level Settings

1. Login to MAXPRO Cloud.
2. Click  and select Customers.
3. Select a customer and the site.
4. Select a connected device from the MAXPRO Cloud.

Figure 151 Select Connected Devices



Note: The device status is ONLINE, and the Settings, I/O, and Storage tabs are displayed on the controller page.

Settings: The Settings tab displays the device settings. Click the edit icon to enable editing. Most of the device settings do not allow update.

- Check the IP address, port, Subnet Mask, Gateway, DNS server, Firmware version, MAC address, and other details.
- Changing the **Recorder Name** is allowed, but the recorder name setting is applicable only on the MPC side.
- You can add a note in the **Notes** box which is applicable only for the cloud.
- The **Reboot** button can be used to manually reboot the NVR.
- The **Sync Device** button (primarily used for debug purpose only) can be used to synchronize some settings from the NVR to the MPC.

I/O: The I/O tab displays the device I/O settings. Only the on-board I/O (i.e., USB I/O) is supported and network I/O is not supported. Click the edit icon to enable editing.

- You can change the **Name** of an **Inputs** and can change the **Level** to **NO** (Normally Open) or **NC** (Normally Closed).
- The output behavior is set using **Output**. You can change the **Output**

name, **Trigger source** (i.e., the input source triggering the output), and **VMD** (i.e., the camera motion triggering the output). l

- You can manually trigger the output by clicking **Test Output** on MPC.

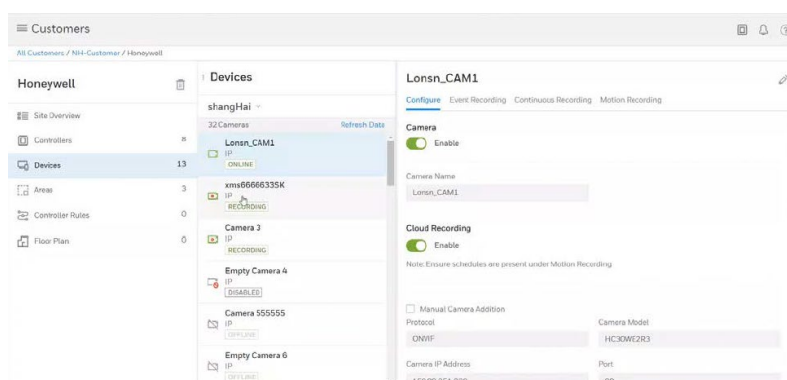
Storage: Displays the total capacity of the hard disks and the used space.

5. Click Save.

Apply Camera Level Settings

1. Click  and select Customers.
2. Select the customer and the site.
3. Click Devices and select a controller from the drop-down list. The camera list of the 35 Series NVR is displayed.

Figure 152 Devices



4. Select a camera and click edit to change the camera settings. Apply the Configure tab settings.

Note: MPC will change the decode of cameras as H.264 when add cameras with decode H.265.

Enable: This setting can be used to enable / disable a camera. Cameras with Disabled status on MPC is deleted on 35 Series NVR.

Camera Name: The editable field for the camera name.

Cloud Recording: Enable the **Cloud Recording** option to push the camera recordings to MAXPRO Cloud.

There are five types of recordings: **Continuous Recording**, **Event Recording** (alarm input triggered recording), **Motion Recording** (motion triggered recording), **User driven recording** (manual recording from live view on MPC), and **Rule driven recording** (recording triggered by a rule, such as which camera motion will set another camera recording). Apart from continuous recording, clips for the other four types of recordings are pushed to the cloud when this option is enabled.

Manual Camera Addition: Select the **Manual Camera Addition** checkbox and change the **Protocol**, **Camera Model**, **Camera IP address**, **Port**, **Username** and **Password** parameters and click **Save** to manually add a camera.

Discover Cameras: Click the **Discover Cameras** button to discover cameras. The cameras discovered from the network are displayed in the **Discovered Cameras** drop-down list. You can add the discovered cameras by entering only the username and password as the other parameters are automatically populated.

5. Click the play button to perform live preview for the camera. Cameras with MFZ function support focus, zoom, and autofocus. Click the stop button (at the bottom-left) to stop the live preview.

Figure 153 Live Preview

35NVRCam1

[Configure](#) [Event Recording](#) [Continuous Recording](#) [Motion Recording](#)



Recording Clip Duration: Set the **Pre Event** and **Post Event** recording duration in seconds for an event trigger, motion trigger, user driven, or rule driven Recording. The clip length will include Pre Event and the Post Event. Pre Event and Post Event can be set to a maximum of one hour, but the maximum clip length is limited to 90 seconds to save the cloud storage space.

Recording Settings: The **Recording Settings** are mapped to the event stream.

The **Camera Resolution** list displays the resolutions supported by the camera.

Live Settings: The **Live Settings** are mapped to the analytical stream on 35 Series NVR.

6. Select the Event Recording tab for the camera.
7. Click edit and select the alarm inputs that can trigger the recording channel and click Save. A maximum of three alarm inputs can be

selected.

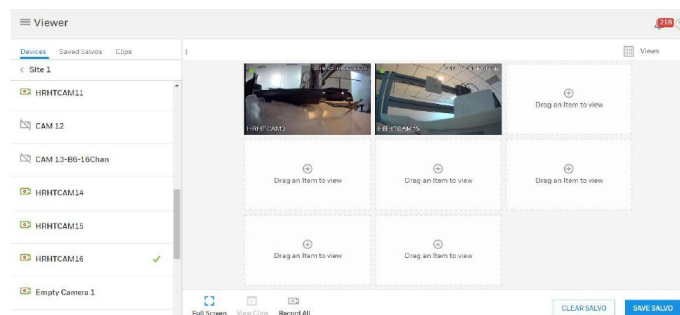
8. Set the Motion Recording and Continuous Recording click Save. The corresponding camera channel is triggered when the Event Recording or the Motion Recording is set.

Note: The Continuous Recording setting is applicable for the device and not MPC.

View Recordings on the MAXPRO Cloud

1. Click  and select Viewer.
2. Select the Devices tab.
3. Select a customer and the site and drag-and-drop up to eight cameras.

Figure 154 Device Tab-Camera List



4. You can perform user driven recording. Only the channels with live view can be recorded.

Record All: to manually record for multiple cameras

Record: to manually record for a single camera

5. Select the Clips tab and select a channel.
6. To search the clips:
 - a. Enter the Start Date and the End Date.
 - b. Select the event types which can be Motion, Schedule, Trigger, User Driven, or Rule Driven.
 - c. Select the storage option, which can be On Cloud (clips on MPC), On Site (clips on the device), or Both.
 - d. Click Apply.
7. Drag and drop to view a recorded clip. Up to six clips can playback simultaneously.

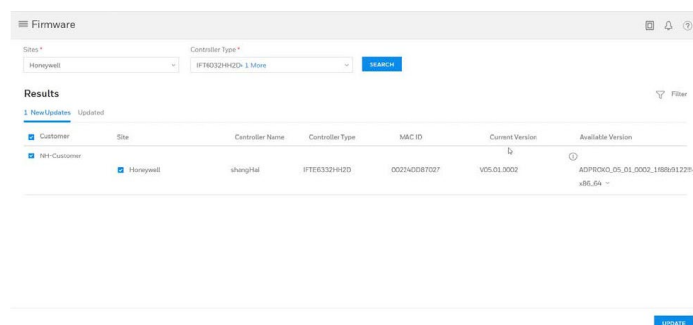
Upgrade Firmware

MPC allows the user to upgrade the firmware of 35 Series NVR.

To upgrade the firmware:

1. Click  and select Firmware.
2. Select the Sites and the Controller Type and click SEARCH.

Figure 155 Search Firmware



Customer	Site	Controller Name	Controller Type	MAC ID	Current Version	Available Version
NH-Customer	Honeywell	shangHai	IFTN32H4QD	00214D087027	V05.01.0002	ADPFC04_05_01_0002_118B601225-v85.64

3. Select the check-box under Site or Customer.
4. Select the firmware version for update from the Available Version.
5. Click UPDATE.

Check Alarms

Alarms notify the occurrence of alarms and events selected during setup that occur in any of the connected systems to the operators. Alarms require further action by the operator. Some of the typical alarms are: Input, Motion, Hard disk error, Video Loss, Video OK, Video Disconnect, Camera Disconnect.

Alarms with no severity are events. Every event and alarm is sent as a notification.

To view the **Alarms** page:

1. Click  and select Alarms.

Figure 156 Alarm List

The screenshot shows the 'Alarms & Events' window with a list of 500 live alarms. The table displays the following data:

Device	Status	Entity	Time	Date	Action
Hardware Trigger Liasinout2/shangtai	MAJOR	Honeywell	21:27:43	08/11/2020	ACKNOWLEDGE
Video Loss Lenson_CAM1/shangtai	MAJOR	Honeywell	20:11:24	08/11/2020	ACKNOWLEDGE
Video OK Lenson_CAM1/shangtai	MAJOR	Honeywell	20:11:24	08/11/2020	ACKNOWLEDGE
Video Loss Lenson_CAM1/shangtai	MAJOR	Honeywell	20:11:15	08/11/2020	ACKNOWLEDGE
Video OK Lenson_CAM1/shangtai	MAJOR	Honeywell	20:11:15	08/11/2020	ACKNOWLEDGE
Hardware Trigger Lenson_ISS1_Input1/shangtai	MAJOR	Honeywell	20:16:41	08/11/2020	ACKNOWLEDGE
Video OK Camera236/shangtai	MAJOR	Honeywell	20:11:21	08/11/2020	ACKNOWLEDGE

The upper-right corner of the Alarms tab displays the following options:

Filter: The filter option enables to filter through the list of alarms based on:

- **Entities:** Controllers, Cameras, Doors, and Rules.
- **Time:** View Archived Events, Today, Yesterday, and Custom.
- **Events:** Access, Video and Intrusion.
- **Sites:** You can select and search the site.

Actions: Enables you to perform the following for the alarms that appear in the Alarm window.

- **Freeze Alarm Stream:** Stop receiving new or unacknowledged alarms in the new window. You can click this command again to start receiving the alarms. This feature is useful when the Alarm window contains many unacknowledged alarms and it becomes difficult to manage them. You can stop receiving the alarms momentarily and start receiving again when needed.
- **Acknowledge:** Acknowledge the selected alarm. It enables you to acknowledge an alarm to accept that the necessary response action is being taken.

WEB OPERATION

This chapter is intended for remote users of the NVRs. It describes how to access Honeywell's 35 Series Network Video Recorder remotely using a browser-based web client.

This chapter contains the following sections:

- [Network Connection](#), page 120
- [Web Login](#), page 121
- [Web Main Menu](#), page 122

- Note:*
- *The interfaces in the Manual are used for introducing the operations and only for reference. The actual interface might be different dependent on the model you purchased. If there is inconsistency between the Manual and the actual product, the actual product shall govern.*
 - *Besides Web, you can use our HDCS to login the device. For detailed information, refer to HDCS user guide.*

Network Connection

Ensure that the following conditions are met:

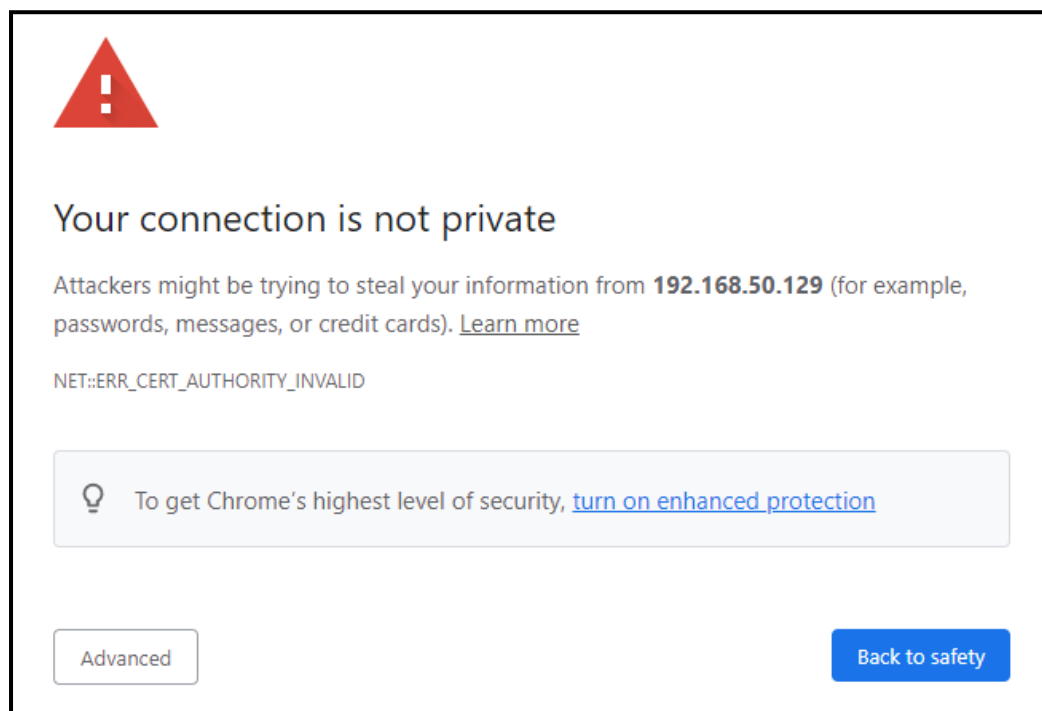
- Ensure that the network connection is good.
- Ensure that the NVR and PC network setup is correct. See the network setup: **Main Menu > Network > Network**.
- Ping to ensure that the network connection is good. Ping *** ***(where *** ***(is the NVR's IP address)). The return TTL should be less than 225.

Web Login

*Note: The factory default IP of the Device is 192.168.0.121.
The Device supports monitoring on Chrome and Microsoft Edge to perform the functions.*

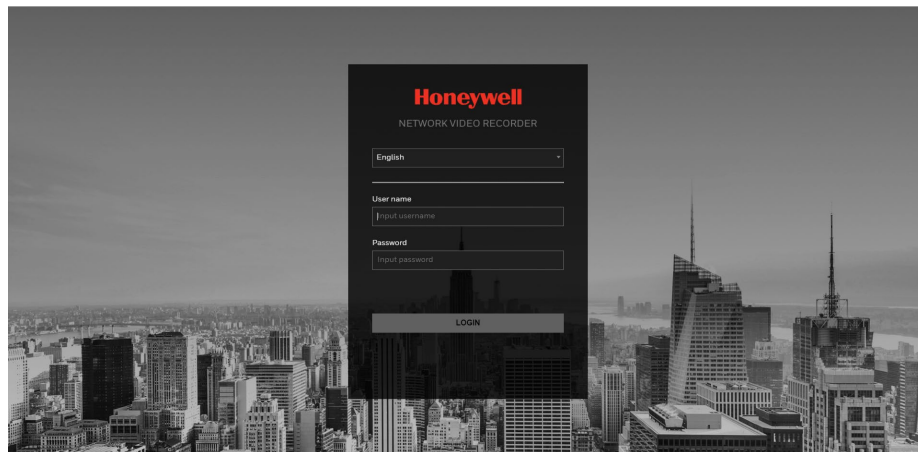
1. Open a Web browser window. Enter the NVR IP address in the address field.
For example, if your NVR's IP address is 192.168.50.129, then enter http:// 192.168.50.129 in the address field.
2. Press Enter on the keyboard and the following window is displayed. Click Advanced.

Figure 157 Security Problem



3. Click Proceed to 192.168.50.129 (unsafe). The following window is displayed.

Figure 158 Login



4. Enter the User name and Password.

The default administrator account is admin. The password is the one that was configured during initial settings.

5. Click LOGIN.

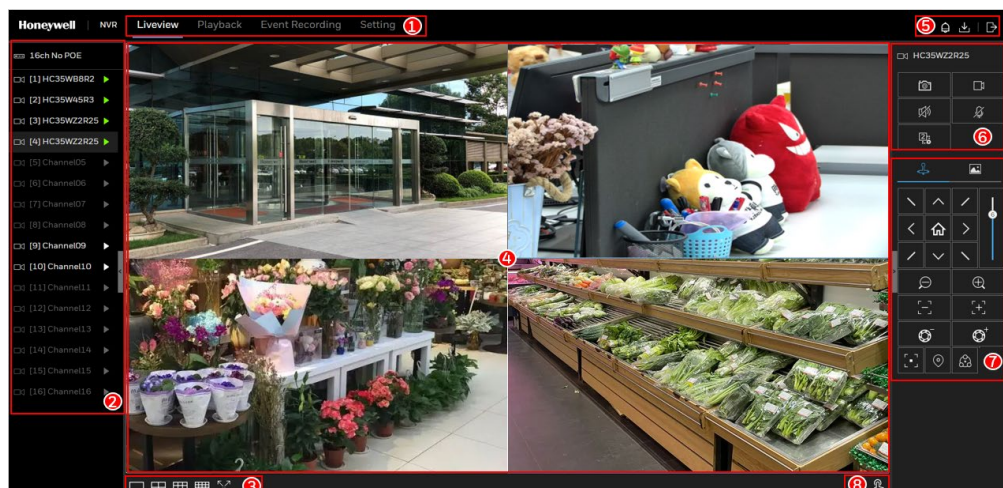
Web Main Menu

Live View

After you have logged in the Web, the main menu is displayed.

For detailed operations, refer to [Local Basic Operation](#).

Figure 159 Liveview Page



There are four sections on the page: **Liveview**, **Playback**, **Event Recording** and **Setting**.

Table 42 Liveview Icons & Parameters

No. / Icon	Description
1	Click to switch functions: Live Video , Playback , Event Recording and Setting .
2	Channel list with online status: - high light for online - gray for offline
3	    Single screen and 4/9/16 split screens  Full screen, click ESC key to exit the full screen.
4	Play live video
5	 Event list Click to show pop-up window for detailed alarm information. Click the icon again to unfold pop-up window.  Download list Click to show backup downloading task list.  Logout the current user.
6	 Snapshot, capture the current live video scene.  Recording, record the video to local folder. The recording time is recommended longer than 10s. If the time duration is too short, the recording may be missed.  Audio, enable or disable audio  Two-way audio, be connected to external speaker and louder for intercom.  Switch 2 (Sub) stream or 1 (main)stream.
7	PTZ keyboard (refer to PTZ Control) and image parameters (refer to Sensor Setting)
8	 Manual alarm, click to trigger alarm manually.

Playback

Click **Playback** to play the recording video if you install disk and enable the recording function.

Note: The Playback in Web can support maximum 1CH 8MP/2CH 4MP/4CH 1080P with H.264. The playback is also affected by user's PC performance.

Figure 160 Playback Page



Table 43 Playback Icons & Parameters

No. / Icon	Description
1	Channel list Device has recording video Device doesn't have recording video Selected device Unselected device
2	Calendar Set the detail time to precisely search recording video.
3	Select different record: Schedule record , Manual record , or Event record .
4	Reversed Play/pause Triple speed Single screen/4 split screens Sync/async You can set the different channels to play synchronously or asynchronous. Sync mode indicates the selected channels play video synchronously. Async mode indicates user play different time period record. Backup Batch backup
5	Types of time bar
6	Time bar, show the time of record
7	Record operation, refer to the same icons in Table 42 .

- Note:** *Stream pulling limitation:*
- *HN350401**/HN350802**/HN351602**/HN35040100N/HN35080100N/HN35160200N: the main stream supports 5 channels and the sub stream supports channels with No. of channels plus one.*
 - *HN350802xxC: the main/sub stream supports 9 channels*
 - *HN35160xxxC: the main/sub stream supports 17 channels*
 - *HN353204xx/HN35320400N: the main stream supports 5 channels and the sub stream supports 17 channels*
 - *The client downloading is also counted as the number of channels, and the local downloading in queue is counted as one channel.*
 -

Event Recording

Search the event recording through the setting condition.

Figure 161 Event Recording page

ID	START TIME	CHANNEL	TYPE	INFORMATION	OPERATE
1	11/03/2022 12:25:40	Channel02	Video loss	Channel02	⏮ ⏭
2	11/03/2022 12:23:32	Channel02	Video loss	Channel02	⏮ ⏭
3	11/03/2022 12:21:19	Channel02	Video loss	Channel02	⏮ ⏭
4	11/03/2022 12:19:16	Channel02	Video loss	Channel02	⏮ ⏭
5	11/03/2022 12:18:05	Channel02	Video loss	Channel02	⏮ ⏭
6	11/03/2022 12:17:16	Channel02	Video loss	Channel02	⏮ ⏭
7	11/03/2022 12:15:13	Channel02	Video loss	Channel02	⏮ ⏭
8	11/03/2022 12:13:47	Channel02	Video loss	Channel02	⏮ ⏭
9	11/03/2022 12:12:45	Channel02	Video loss	Channel02	⏮ ⏭
10	11/03/2022 12:10:26	Channel02	Video loss	Channel02	⏮ ⏭
11	11/03/2022 12:08:54	Channel02	Video loss	Channel02	⏮ ⏭
12	11/03/2022 12:06:12	Channel02	Video loss	Channel02	⏮ ⏭
13	11/03/2022 11:58:39	Channel02	Video loss	Channel02	⏮ ⏭
14	11/03/2022 11:54:11	Channel02	Video loss	Channel02	⏮ ⏭
15	11/03/2022 11:53:10	Channel02	Video loss	Channel02	⏮ ⏭
16	11/03/2022 11:51:38	Channel02	Video loss	Channel02	⏮ ⏭
17	11/03/2022 11:49:59	Channel02	Video loss	Channel02	⏮ ⏭
18	11/03/2022 11:47:00	Channel02	Video loss	Channel02	⏮ ⏭
19	11/03/2022 11:42:31	Channel02	Video loss	Channel02	⏮ ⏭
20	11/03/2022 11:39:32	Channel02	Video loss	Channel02	⏮ ⏭

Table 44 Event Recording Icons & Parameters

No. / Icon	Description
1	Channel list Select to search channels event recording.
2	Set the start time and end time to search.
3	Select the alarm types.
4	Searching result ⏮ Play the recording video ⏭ Download the event recording

No. / Icon	Description
5	- Shows the number of searching result. - Switch the page

Setting

The **Setting** operation is the same as the local operation. Please refer to [Local Basic Operation](#)

Figure 162 Setting Page

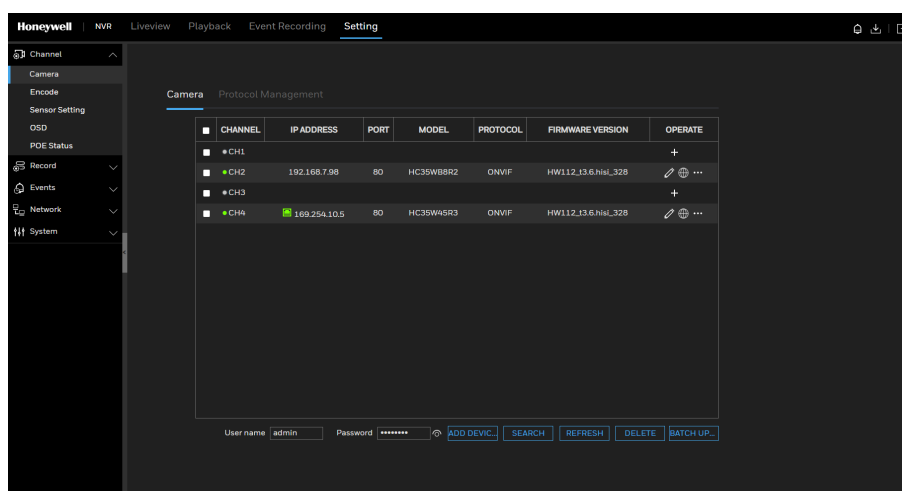
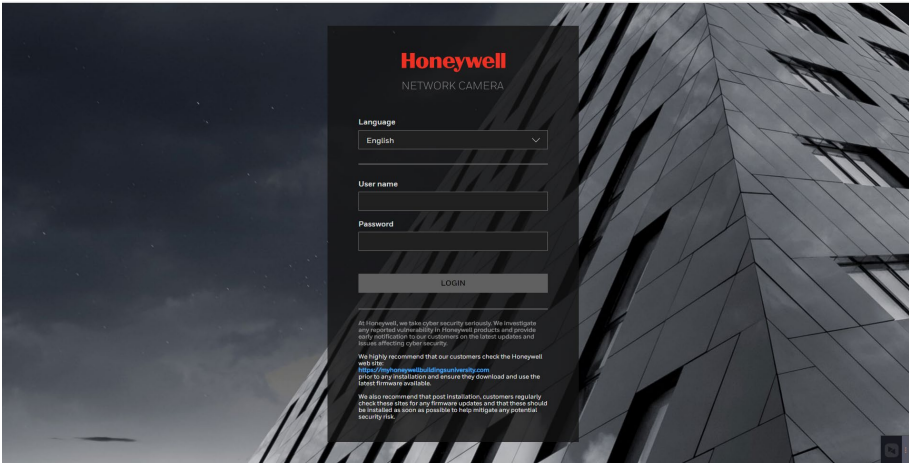


Table 45 Setting Symbols

Icon	Description
	Perform Channel operation such as camera/encode/OSD configuration, sensor setting and PoE status checking. For detailed operations, refer to Configuring Camera .
	You can manage the Record resources (such as storage mode) and storage space. For detailed operations, refer to Configuring Storage Settings .
	Search for Event information and perform event operation such as alarm input/output setting. For detailed operations, refer to Configuring Events Settings .
	Set Network functions, such as DDNS , Email and P2P . For detailed operations, refer to Configuring Network Settings and Web Mode .
	Configure basic System information. For detailed operations, refer to Configuring System Settings .

To visit the camera web page, go to **Setting > Channel > Camera > Camera**, click  on the camera list. Please enable NAT port in advance.

Figure 163 IPC Login Page



Web Mode

When you access the NVR through web client, go to **Setting > Networks > Web Mode**, set **HTTPS** (HTTPS only or HTTP & HTTPS), **Certificate Request**, **Upload Files**, and **CA Certificate**.

There are three modes for security certificate. The **Certificate Request** is the priority, and the second option is **Upload Files**. When these two modes are invalid, the default option is **CA Certificate**.

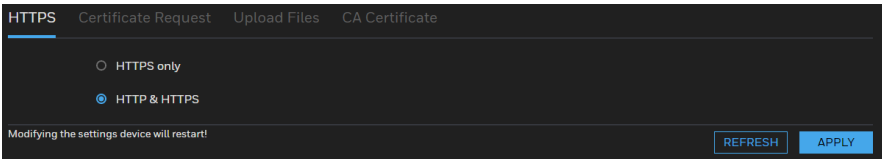
HTTPS

Go to **Setting > Networks > Web Mode > HTTPS**.

This section explains how to enable authentication and encrypted communication. It helps protect streaming data transmission over the Internet on higher security level.

Note: Honeywell strictly recommends using HTTPS only.

Figure 164 HTTPS



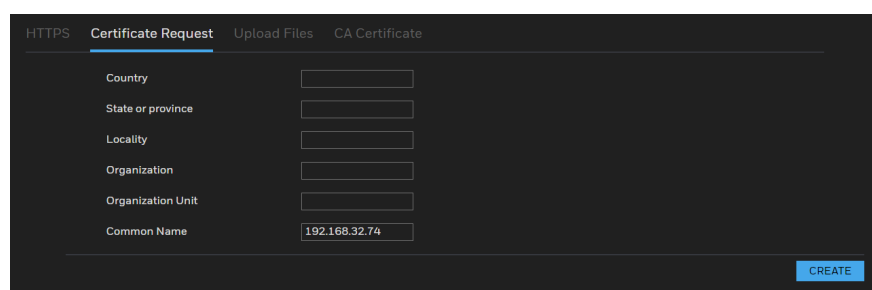
HTTPS only: Select it and the web browser can only be accessed via HTTPS with higher security level.

HTTP & HTTPS: Select it and the web browser can be accessed via HTTP or HTTPS.

Certificate Request

1. Go to Setting > Networks > Web Mode > Certificate Request.

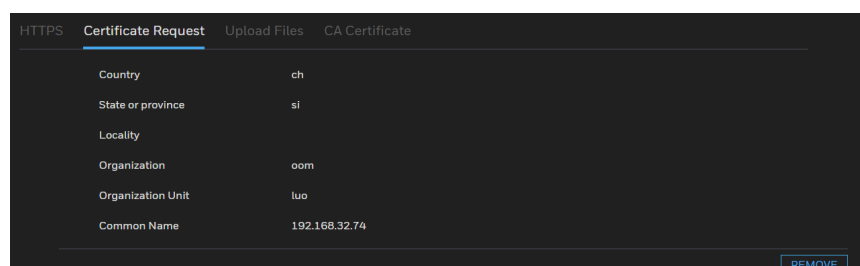
Figure 165 Certificate Request



The screenshot shows the 'Certificate Request' tab in the web interface. It contains a form with the following fields: Country, State or province, Locality, Organization, Organization Unit, and Common Name. The 'Common Name' field is pre-filled with '192.168.32.74'. A 'CREATE' button is located at the bottom right of the form.

2. Input the parameters of certificate request.
3. Click CREATE.
4. Click EXPORT to save the CSR request file (certreq.pem).
5. Use CSR request file to obtain the SSL certificate file.
6. At web page, Click CHOOSE FILE to choose the combination file.
7. Click UPLOAD.

Figure 166 Certificate Page



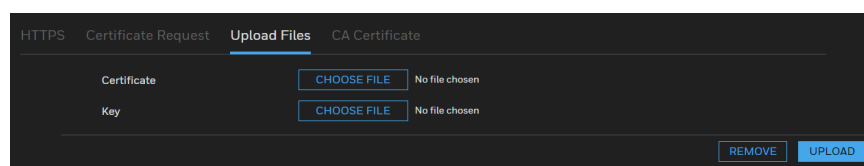
The screenshot shows the 'Certificate Request' tab with the form filled out. The 'Common Name' field is pre-filled with '192.168.32.74'. A 'REMOVE' button is located at the bottom right of the form.

After the file is uploaded successfully, if you want to remove the file, click **REMOVE**.

Upload Files

1. Go to Setting > Networks > Web Mode > Upload Files. You can import the Certificate file and Key file from third party here.

Figure 167 Upload Files Page

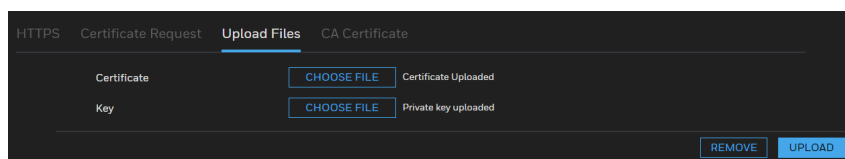


The screenshot shows the 'Upload Files' tab in the web interface. It contains a form with two fields: Certificate and Key. Each field has a 'CHOOSE FILE' button and a 'No file chosen' text. A 'REMOVE' button and an 'UPLOAD' button are located at the bottom right of the form.

2. In the Certificate field, click CHOOSE FILE to select a certificate file you have already applied from 3rd party or CA domain.
3. In the Key field, click CHOOSE FILE to select a certificate key you have already applied from 3rd party or CA domain.

4. Click UPLOAD.

Figure 168 Uploaded Files



After the files are uploaded successfully, if you want to remove the files, click **REMOVE**.

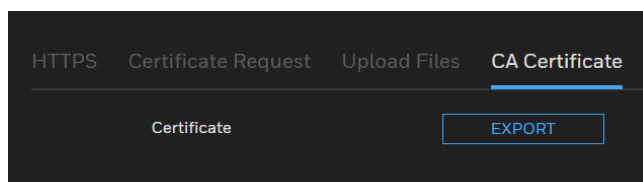
- Supported certificate type: HTTPS protocol.
- Supported certificate file format: *.cert format.
- Supported Key format: PEM format.

CA Certificate

The NVR uses HTTPS, a secure communication protocol that verifies the identities of visited websites and servers and encrypts data exchanged between the client and the server. When you log in to the NVR's web client for the first time, some browsers may display a warning that the connection is not private/secure. To access the web client, you must install a Honeywell-signed security certificate.

1. Go to Setting > Networks > Web Mode > CA Certificate.

Figure 169 CA Certificate Page



2. Click EXPORT to save the root certificate (ca.crt) on your local computer.
3. Go to the directory where you saved the CA certificate and double-click the certificate. Click Open. The Certificate window opens.
4. In the Certificate window, on the General tab, click Install Certificate to open the Certificate Import Wizard.
5. Click Next to continue.
6. Click Place all certificates in the following store, browse to Trusted Root Certification Authorities, and then click OK.
7. Click Next, and then click Finish to close the Certificate Import Wizard. A confirmation dialog box appears with the message "The import was successful."
8. Click OK, and then click OK to close the Certificate window. And now your browser will not display a warning that the connection is not private/secure.

Please ensure to install the certificate to ensure a secure communication with the NVR and to avoid delays in the web page navigation.

Questions	Solutions
NVR cannot boot up properly.	• Input power is not correct. • Power connection is not correct. • Power switch button is damaged. • Program upgrade is wrong. • HDD malfunction or something wrong with HDD ribbon. • Front panel error. • Main board is damaged.
NVR often automatically shuts down or stops running.	• Input voltage is not stable or it is too low. • HDD malfunction or something wrong with the ribbon. • Front video signal is not stable. • Working environment is too harsh, too much dust. • Hardware malfunction.
System cannot detect hard disk.	• HDD is broken. • HDD ribbon is damaged. • HDD cable connection is loose. • Main board SATA port is broken.
There is no video output whether it is one-channel, multiple-channel or all-channel output.	• Program is not compatible. Upgrade to the latest version. • Brightness is 0. Restore factory default setup. • Check your screen saver. • NVR hardware malfunctions.
I cannot search local records.	• HDD ribbon is damaged. • HDD is broken. • Upgraded program is not compatible. • The recorded file has been overwritten. • Record function has been disabled.
Video is distorted when searching local records.	• Video quality setup is too low. • Program read error, bit data is too small. There is mosaic in the full screen. Restart the NVR to solve this problem. • HDD data ribbon error. • HDD malfunction. • NVR hardware malfunctions.
Time display is not correct.	• Setup is not correct. • Battery contact is not correct, or voltage is too low.

Questions	Solutions
NVR cannot control PTZ.	• Front panel PTZ error • PTZ decoder setup, connection or installation is not correct. • Cable connection is not correct. • PTZ setup is not correct. • The distance is too far.
I cannot log in client-end or web.	• Use Windows 2007 or higher vision to view the web interface. • Upgrade display card driver. • Network connection error. • Network setup error. • Password or user name is invalid. • Client-end is not compatible with NVR program. • The browser should choose Google Chrome, Microsoft Edge and upgrade to the latest version
There is only mosaic no video when preview or playback video file remotely.	• Network fluency is not good. • Client-end resources are limit. • Current user has no right to monitor.
Network connection is not stable.	• Network is not stable. • IP address conflict. • MAC address conflict. • PC or device network card is not good.
Burn error /USB back error.	• Burner and NVR are in the same data cable. • System uses too much CPU resources. Stop record first and then begin backup. • Data amount exceeds backup device capacity. It may result in burner error. • Backup device is not compatible. • Backup device is damaged.
Alarm signal cannot be disarmed.	• Alarm setup is not correct. • Alarm output has been open manually. • Input device error or connection is not correct. • Some program versions may have this problem. Upgrade your system.
Alarm function is null.	• Alarm setup is not correct. • Alarm cable connection is not correct. • Alarm input signal is not correct. • There are two loops connect to one alarm device.
Record storage period is not enough.	• HDD capacity is not enough. • HDD is damaged.
Cannot playback the downloaded file.	• There is no media player, the file support VLC player to play. • The downloaded file is error.
The Movies & TV player of Windows cannot play the downloaded recording.	The recording video format is H265 encode type (MP4), we recommend to use VLC to play.
Forgot local menu operation password or network password	Contact your local technical support for help. We can guide you to solve this problem.

Questions	Solutions
There is no video. The screen is in black.	- IPC IP address is not right. - IPC port number is not right. - IPC account (user name/password) is not right. - IPC is offline.
The displayed video is not full in the monitor.	Check current resolution setup. If the current setup is 1920*1080, then you need to set the monitor resolution as 1920*1080.
There is no HDMI output.	- Displayer is not in HDMI mode. - HDMI cable connection is not right.
The video is not fluent when I view in multiple-channel mode from the client-end.	- The network bandwidth is not sufficient. The multiple-channel monitor operation needs at least 100M or higher. - Your PC resources are not sufficient. For 16-ch remote monitor operation, the PC shall have the following environment: Quad Core, 2G or higher memory, independent displayer, display card memory 256M or higher.
I cannot connect to the IPC	- Make sure that the IPC has booted up. - Make sure IPC network connection is right and it is online - IPC IP is in the blacklist. - The device has connected to the too many IPC. It cannot transmit the video. - Check the IPC port value and the time zone are the same as the NVR. - Make sure current network environment is stable.
After I reset the NVR resolution, my monitor cannot display.	The default resolution is 1920*1080, if you set higher resolution, you should make sure the monitor support that resolution, otherwise you should login to Web interface to switch the default resolution.
After I login the Web, I cannot find the remote interface to add the IPC.	Clear the Web controls and load again.
There is IP and gateway, I can access the internet via the router. But I cannot access the internet after I reboot the NVR.	Use command PING to check you can connect to the gateway or not. Use telnet to access and then use command " Ipconfig -all " to check device IP address. If you see the subnet mask and the gateway has changed after the reboot. Upgrade the applications and set again.
The Camera can't connect with 35S NVR.	Reset the camera, and activate it to set password. Access the camera's web to open DHCP, and plug to PoE port of NVR. Set the NVR channel password and the camera's password to be the same.
The Camera's I/O parameters can't be set by 35 NVR.	Set the camera's I/O parameters by camera web client or go to camera web client by selecting Setting > Channel > Camera > Camera by NVR web client, click  on the camera list. Please enable NAT port in advance.
Unable to configure camera's MD parameters by 35S NVR	Set the camera's MD parameters by camera web client or go to camera web client by selecting Setting > Channel > Camera > Camera by NVR web client, click  on the camera list. Please enable NAT port in advance.
For some ONVIF IP cameras connected to the NVR, their IP addresses cannot be automatically assigned via NVR.	Manually set the IP addresses of the IP cameras via web.

Daily Maintenance

- Use the brush to clean the board, socket connector and the chassis regularly.
- The device shall be soundly earthed in case there is audio/video disturbance. Keep the device away from the static voltage or induced voltage.
- Unplug the power cable before you remove the audio/video signal cable.
- Always shut down the device properly. Use the shutdown function in the menu, or you can press the power button in the rear pane to shut down the device. Otherwise, it may result in HDD malfunction.
- Make sure the device is away from the direct sunlight or other heating sources. Keep the device ventilated.
- Check and maintain the device regularly

Honeywell Building Technologies – Security Americas (Head Office)

Honeywell Commercial Security
715 Peachtree St. NE
Atlanta, GA 30308
Tel: +1 800 323 4576

Honeywell Building Technologies – Security Mexico

Mexico: Av. Santa Fe 94, Torre A, Piso 1, Col. Zedec,
CP 012010, CDMX, México.
Colombia: Edificio Punto 99, Carrera 11a.
98-50, Piso 7, Bogota, Colombia.
Tel: 01.800.083.59.25

Honeywell Building Technologies – Security Middle East/N. Africa

Emaar Business Park, Building No. 2, Sheikh Zayed Road
P.O. Box 232362
Dubai, United Arab Emirates
security_meta@honeywell.com
Tel: +971 4 450 5800

Honeywell Building Technologies – Security Europe/South Africa

Building 5 Carlton Park,
King Edward Avenue
Narborough, Leicester, LE19 0LF
United Kingdom
Tel: +44 (0) 1163 500714

Honeywell Building Technologies – Security Northern Europe

Stationsplein Z-W 961, 1117 CE Schiphol-Oost, Netherlands
Tel: +31 (0) 299 410 200

Honeywell Building Technologies – Security Deutschland

Johannes-Mauthe-Straße 14
D-72458 Albstadt
Germany
Tel: +49 (0) 7431 801-0

Honeywell Building Technologies – Security France

Immeuble Lavoisier
Parc de Haute Technologie
3-7 rue Georges Besse
92160 Antony, France
Tel: +33 (0) 1 40 96 20 50

Honeywell Building Technologies – Security Italia SpA

Via Achille Grandi 22,
20097 San Donato Milanese (MI), Italy

Honeywell Building Technologies – Security España

Josefa Valcárcel, 24
28027 – Madrid, España
Tel.: +34 902 667 800

Honeywell Building Technologies – Security Россия и СНГ

121059 Moscow,
Ul, Kiev 7
Russia
Tel: +7 (495) 797-93-71

Honeywell Building Technologies – Security Asia Pacific

Building #1, 555 Huanke Road,
Zhang Jiang Hi-Tech Park Pudong New Area,
Shanghai, 201203, China
Tel: 400 840 2233

Honeywell Building Technologies – Security and Fire (ASEAN)

Honeywell International Sdn Bhd
Level 25, UOA Corp Tower, Lobby B
Avenue 10, The Vertical, Bangsar South City
59200, Kuala Lumpur, Malaysia
Email: buildings.asean@honeywell.com
Technical support (Small & Medium Business):

Vietnam: +84 4 4458 3369
Thailand: +66 2 0182439 Indonesia: +62 21 2188 9000
Malaysia: +60 3 7624 1530
Singapore: +65 3158 6830
Philippines: +63 2 231 3380

Honeywell Home and Building Technologies (India)

HBT India Buildings
Unitech Trade Centre, 5th Floor,
Sector – 43, Block C, Sushant Lok Phase – 1,
Gurgaon – 122002, Haryana, India
Email: HBT-IndiaBuildings@honeywell.com
Toll Free Number: 000 800 050 2167
Tel: +91 124 4975000

Honeywell Building Technologies – Security and Fire (Korea)

Honeywell Co., Ltd. (Korea)
5F SangAm IT Tower,
434, Worldcup Buk-ro, Mapo-gu,
Seoul 03922, Korea
Email: info.security@honeywell.com
Customer support: HSG-CS-KR@honeywell.com; +82 1522-8779
Tel: +82-2-799-6114

Honeywell Building Technologies – Security & Fire (Pacific)

Honeywell Ltd
9 Columbia Way
BAULKHAM HILLS NSW 2153
Email: hsf.comms.pacific@Honeywell.com
Technical support:
Australia: 1300 220 345
New Zealand: +64 9 623 5050