

Digital Video Recorder

User Manual

User Manual

About this Manual

This Manual is applicable to Turbo HD Digital Video Recorder (DVR).

The Manual includes instructions for using and managing the product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version in the company website.

Please use this user manual under the guidance of professionals.

Legal Disclaimer

REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE WHOLLY AT YOUR OWN RISKS. OUR COMPANY SHALL NOT TAKE ANY RESPONSIBILITES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, OUR COMPANY WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

SURVEILLANCE LAWS VARY BY JURISDICTION. PLEASE CHECK ALL RELEVANT LAWS IN YOUR JURISDICTION BEFORE USING THIS PRODUCT IN ORDER TO ENSURE THAT YOUR USE CONFORMS THE APPLICABLE LAW. OUR COMPANY SHALL NOT BE LIABLE IN THE EVENT THAT THIS PRODUCT IS USED WITH ILLEGITIMATE PURPOSES.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.

Regulatory Information

FCC Information

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

FCC compliance: 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.

FCC Conditions

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.

2. This device must accept any interference received, including interference that may cause undesired operation.

EU Conformity Statement

CE This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2014/30/EU, the LVD Directive 2014/35/EU, the RoHS Directive 2011/65/EU.



2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or

dispose of it at designated collection points. For more information see: www.recyclethis.info



2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may

include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see: www.recyclethis.info

Industry Canada ICES-003 Compliance

This device meets the CAN ICES-3 (A)/NMB-3(A) standards requirements.

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description	
	Provides additional information to emphasize or supplement important points of the main text.	
	Indicates a potentially hazardous situation, which if not avoided could result in equipment damage, data loss, performance degradation, or unexpected results.	
	Indicates a hazard with a high level of risk, which if not avoided, wDANGERresult in death or serious injury.	

Safety Instructions

- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.
- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region. Please refer to technical specifications for detailed information.
- Input voltage should meet both the SELV (Safety Extra Low Voltage) and the Limited Power Source with 100~240 VAC or 12 VDC according to the IEC60950-1 standard. Please refer to technical specifications for detailed information.
- Do not connect several devices to one power adapter as adapter overload may cause overheating or a fire hazard.
- Please make sure that the plug is firmly connected to the power socket.
- If smoke, odor or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.

Preventive and Cautionary Tips

Before connecting and operating your device, please be advised of the following tips:

- Ensure unit is installed in a well-ventilated, dust-free environment.
- Unit is designed for indoor use only.
- Keep all liquids away from the device.
- Ensure environmental conditions meet factory specifications.
- Ensure unit is properly secured to a rack or shelf. Major shocks or jolts to the unit as a result of dropping it may cause damage to the sensitive electronics within the unit.
- Use the device in conjunction with an UPS if possible.
- Power down the unit before connecting and disconnecting accessories and peripherals.
- A factory recommended HDD should be used for this device.
- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.
- The USB interface can only connect to mouse, keyboard or USB flash drive.
- Use only power adaptors listed in the user instructions.

Product Key Features

General

- C onnectable to Turbo HD and analog cameras;
- Supports UTC (Coaxitron) protocol for connecting camera over coax;
- Connectable to AHD cameras;
- Connectable to HDCVI cameras;
- Connectable to IP cameras;
- The analog signal inputs including Turbo HD, AHD, HDCVI, and CVBS can be automatically recognized without configuration;
- communication, and provide power to the cameras via coaxitron;
- Each channel supports dual-stream. And sub-stream supports up to WD1 resolution;
- Independent configuration for each channel, including resolution, frame rate, bit rate, image quality, etc.;
- The minimum frame rate for main stream and sub-stream is 1 fps;
- Encoding for both video stream and video & audio stream; audio and video synchronization during composite stream encoding;
- Supports enabling H.265+/H.264+ to ensure high video quality with lowered bit rate;
- H.265 Pro+/H.265 Pro/H.265/H.264+/H.264 encoding for the main stream, and H.265/H.264 encoding for the sub-stream of analog cameras;
- Connectable to H.265 and H.264 IP cameras;
- Defog level, night to day sensitivity, day to night sensitivity, IR light brightness, day/night mode, and WDR switch configurable for the connected analog cameras supporting these parameters;
- 4 MP/5 MP signal switch for the supported analog cameras;
- Watermark technology.

Local Monitoring

- 1/4/6/8/9/16/25/36/64 screen live view is supported, and the display sequence of screens is adjustable;
- Live view screen can be switched in group and manual switch and automatic cycle live view are also provided, the interval of automatic cycle can be adjusted;
- CVBS output only serves as the aux output or live view output.
- Quick setting menu is provided for live view;
- The selected live view channel can be shielded;
- Motion detection, video-tampering detection, video exception alarm, video loss alarm and VCA alarm functions;

- Privacy mask;
- Zooming in/out by clicking the mouse and PTZ tracing by dragging mouse;
- When specified CVBS camera is connected, you can control PTZ via Coaxitron and call the OSD of the camera.

HDD Management

- Up to 8 network disks (8 NAS disks, 8 IP SAN disks or n NAS disks + m IP SAN disks (n+m ≤ 8)) can be connected;
- Remaining recording time of the HDD can be viewed;
- Supports cloud storage;
- S.M.A.R.T. and bad sector detection;
- HDD sleeping function;
- HDD property: redundancy, read-only, read/write (R/W);
- HDD group management;
- HDD quota management; different capacity can be assigned to different channels.

Recording, Capture and Playback

- Holiday recording schedule configuration;
- Cycle and non-cycle recording modes;
- Normal and event video encoding parameters;
- Multiple recording types: manual, continuous, alarm, motion, motion | alarm, motion & alarm and event;
- The device will note that the exported AVI video may have problems if the frame rates of the continuous and event recording are different;
- 8 recording time periods with separated recording types;
- Supports Channel-Zero encoding;
- Main stream and sub-stream configurable for simultaneous recording;
- Pre-record and post-record for motion detection triggered recording, and pre-record time for schedule and manual recording;
- Searching record files and captured pictures by events (alarm input/motion detection);
- Customization of tags, searching and playing back by tags;
- Locking and unlocking of record files;
- Local redundant recording and capture;
- When Turbo HD, AHD, or HDCVI input is connected, the information including the resolution and frame rate will be overlaid on the bottom right corner of the live view for 5 seconds. When CVBS input is connected, the information such as NTSC or PAL will be overlaid on the bottom right corner of the live view for 5 seconds.
- Searching and playing back record files by camera number, recording type, start time, end time, etc.;

- Smart playback to go through less effective information;
- Zooming in for any area when playback;
- Multi-channel reverse playback;
- Supports pause, fast forward, slow forward, skip forward, and skip backward when playback, locating by dragging the mouse on the progress bar;
- 4/8/16-ch synchronous playback;
- Manual capture, continuous capture of video images and playback of captured pictures.

Backup

- Exports data by a USB, and SATA device;
- Exports video clips when playback;
- Video and Log and Player are selectable to export for backup;
- Management and maintenance of backup devices.

Alarm and Exception

- Configurable arming time of alarm input/output;
- Alarms for video loss, motion detection, video tampering, illegal login, network disconnected, IP confliction, record/capture exception, HDD error, and HDD full, etc.;
- Alarm triggers full screen monitoring, audio alarm, notifying surveillance center, sending email and alarm output;
- One-key disarms the linkage actions of the alarm input;
- PTZ linking for the VCA alarm;
- VCA detection alarm is supported;
- Supports POS triggered alarm;
- Supports coaxial alarm;
- System will automatically reboot when a problem is detected in an attempt to restore normal functionality;
- You can enable false alarm filer for the motion detection of the PIR cameras. Then only when the motion detection events and PIR events are both triggered, the motion detection alarm will be triggered.

Other Local Functions

- Operable by mouse and remote control;
- Three-level user management; admin user can create many operating account and define their operating permission, which includes the permission to access any channel;
- Completeness of operation, alarm, exceptions and log writing and searching;
- Manually triggering and clearing alarms;
- Importing and exporting of configuration file of devices;
- Getting cameras type information automatically;

- Unlock pattern for device login for the *admin*;
- Clear-text password available;
- GUID file can be exported for password resetting;
- Security question and reserved email can be configured for password resetting;
- Multiple connected analog cameras supporting Turbo HD or AHD signal can be upgraded simultaneously via DVR.

Network Functions

- Self-adaptive 100M or 1000M network interface;
- IPv6 is supported;
- TCP/IP protocol, PPPoE, DHCP, DNS, DDNS, NTP, SADP, SMTP, NFS, iSCSI, UPnP[™] and HTTPS are supported;
- Supports access by Guarding Vision. If you enable Guarding Vision, the device will remind you the internet access risk and ask you to confirm the "Terms of Service" and "Privacy Statement" before enabling the service. You should create a verification code to connect to the Guarding Vision;
- TCP, UDP and RTP for unicast;
- Auto/Manual port mapping by UPnPTM;
- Remote search, playback, download, locking and unlocking the record files, and downloading files broken transfer resume;
- Remote parameters setup; remote import/export of device parameters;
- Remote viewing of the device status, system logs and alarm status;
- Remote keyboard operation;
- Remote HDD formatting and program upgrading;
- Remote system restart and shutdown;
- Supports upgrading via remote FTP server;
- RS-485 transparent channel transmission;
- Alarm and exception information can be sent to the remote host;
- Remotely start/stop recording;
- Remotely start/stop alarm output;
- Remote PTZ control;
- Two-way audio and voice broadcasting;
- Output bandwidth limit configurable;
- Embedded WEB server;
- If DHCP is enabled, you can enable DNS DHCP or disable it and edit the Preferred DNS Server and Alternate DNS Server.

Development Scalability

- SDK for Windows and Linux system;
- Source code of application software for demo;
- Development support and training for application system.

TABLE OF CONTENTS

Product Key Features	5
Chapter 1 Introduction	17
1.1 Front Panel	17
1.2 IR Remote Control Operations	34
1.3 USB Mouse Operation	37
1.4 Rear Panel	37
Chapter 2 Getting Started	43
2.1 Start up the Device	43
2.2 Activate the Device	43
2.3 Configure Unlock Pattern for Login	45
2.4 Login to the Device	46
2.4.1 Log in via Unlock Pattern	46
2.4.2 Log in via Password	47
2.5 Enter Wizard to Configure Quick Basic Settings	47
2.6 Enter Main Menu	50
2.7 System Operation	52
2.7.1 Log out	52
2.7.2 Shut Down the Device	52
2.7.3 Reboot the Device	52
Chapter 3 Camera Management	54
3.1 Add the IP Cameras	54
3.1.1 Add the IP Camera Manually	54
3.1.2 Add the Automatically Searched Online IP Cameras	55
3.1.3 Connect PoC Cameras	55
3.1.4 Configure Signal Input Channel	56
3.1.5 Configuring 5 MP Long Distance Transmission	57
3.2 Enable the H.265 Stream Access	58
3.3 Upgrade the IP Camera	58
Chapter 4 Camera Settings	60
4.1 Configure OSD Settings	60
4.2 Configure Privacy Mask	61
4.3 Configure the Video Parameters	62

4.4 Configure the Day/Night Switch	62
4.5 Configure Other Camera Parameters	63
Chapter 5 Live View	64
5.1 Start Live View	64
5.1.1 Digital Zoom	64
5.1.2 Live View Strategy	65
5.2 Target Detection	65
5.3 Configure Live View Settings	66
5.4 Configure Live View Layout	66
5.5 Configure Auto-Switch of Cameras	68
5.6 Configure Channel-zero Encoding	68
5.7 Using an Auxiliary Monitor	69
Chapter 6 PTZ Control	70
6.1 PTZ Control Wizard	70
6.2 Configure PTZ Parameters	70
6.3 Set PTZ Presets, Patrols & Patterns	71
6.3.1 Set a Preset	71
6.3.2 Call a Preset	72
6.3.3 Set a Patrol	73
6.3.4 Call a Patrol	74
6.3.5 Set a Pattern	75
6.3.6 Call a Pattern	76
6.3.7 Set Linear Scan Limits	76
6.3.8 Call Linear Scan	77
6.3.9 One-touch Park	77
6.4 Auxiliary Functions	78
Chapter 7 Storage	79
7.1 Storage Device Management	79
7.1.1 Install the HDD	79
7.1.2 Add the Network Disk	79
7.1.3 Configure eSATA for Data Storage	
7.2 Storage Mode	82
7.2.1 Configure HDD Group	82
7.2.2 Configure HDD Quota	
7.3 Recording Parameters	85

7.3.1 Main Stream	85
7.3.2 Sub-Stream	86
7.3.3 Picture	86
7.3.4 Configure Advanced Recording Settings	86
7.4 Configure Recording Schedule	87
7.5 Configure Continuous Recording	89
7.6 Configure Motion Detection Triggered Recording	89
7.7 Configure Event Triggered Recording	89
7.8 Configure Alarm Triggered Recording	90
7.9 Configure Picture Capture	90
7.10 Configure Holiday Recording and Capture	91
7.11 Configure Redundant Recording and Capture	93
7.12 Configure 1080p Lite	94
7.12.1 Enable the 1080P Lite Mode	94
7.12.2 Disable the 1080P Lite Mode	95
Chapter 8 Disk Array	
8.1 Create Disk Array	96
8.1.1 Enable RAID	96
8.1.2 One-Touch Creation	97
8.1.3 Manual Creation	97
8.2 Rebuild Array	99
8.2.1 Configure Hot Spare Disk	
8.2.2 Automatically Rebuild Array	
8.2.3 Manually Rebuild Array	
8.3 Delete Array	
8.4 Check and Edit Firmware	
Chapter 9 File Management	
9.1 Search and Export All Files	
9.1.1 Search Files	
9.1.2 Export Files	
9.2 Search and Export Human Files	
9.2.1 Search Human Files	
9.2.2 Export Human Files	
9.3 Search and Export Vehicle Files	
9.3.1 Search Vehicle Files	105

9.3.2 Export Vehicle Files	105
9.4 Search History Operation	106
9.4.1 Save Search Condition	106
9.4.2 Call Search History	106
Chapter 10 Playback	
10.1 Play Video Files	107
10.1.1 Instant Playback	107
10.1.2 Play Normal Video	107
10.1.3 Play Smart Searched Video	108
10.1.4 Play Custom Searched Files	109
10.1.5 Play Tag Files	110
10.1.6 Play Event Files	112
10.1.7 Play by Sub-periods	113
10.1.8 Play Log Files	114
10.1.9 Play External File	114
10.2 Playback Operations	115
10.2.1 Set Play Strategy in Smart/Custom Mode	115
10.2.2 Edit Video Clips	115
10.2.3 Switch between Main Stream and Sub-Stream	116
10.2.4 Thumbnails View	116
10.2.5 Fast View	116
10.2.6 Digital Zoom	117
Chapter 11 Event and Alarm Settings	
11.1 Configure Arming Schedule	118
11.2 Configure Alarm Linkage Actions	118
11.2.1 Configure Auto-switch Full Screen Monitoring	118
11.2.2 Configure Audio Warning	119
11.2.3 Notify Surveillance Center	119
11.2.4 Configure Email Linkage	120
11.2.5 Trigger Alarm Output	120
11.2.6 Configure PTZ Linkage	120
11.3 Configure Motion Detection Alarm	121
11.4 Configure Video Loss Alarm	123
11.5 Configure Video Tampering Alarm	124
11.6 Configure Sensor Alarms	125

11.6.1 Configure Alarm Input	125
11.6.2 Configure One-Key Disarming	126
11.6.3 Configure Alarm Output	127
11.7 Configure Exceptions Alarm	128
11.8 Trigger or Clear Alarm Output Manually	129
Chapter 12 POS Configuration	131
12.1 Configure POS Settings	131
12.1.1 Configure POS Connection	131
12.1.2 Configure POS Text Overlay	135
12.2 Configure POS Alarm	136
Chapter 13 VCA Event Alarm	138
13.1 Human Body Detection	138
13.2 Face Detection	139
13.3 Vehicle Detection	140
13.4 Line Crossing Detection	141
13.5 Intrusion Detection	143
13.6 Region Entrance Detection	144
13.7 Region Exiting Detection	145
13.8 Unattended Baggage Detection	147
13.9 Object Removal Detection	148
13.10 Audio Exception Detection	149
13.11 Sudden Scene Change Detection	150
13.12 Defocus Detection	151
13.13 PIR Alarm	152
Chapter 14 Smart Analysis	154
14.1 Engine Configuration	154
14.2 Task Configuration	155
14.3 Face Search	157
14.4 Human Body Search	158
14.5 Vehicle Search	159
14.6 People Counting	159
14.7 Heat Map	160
Chapter 15 Human Body Detection	162
15.1 Enable Human Body Smart Analysis	162
15.2 Human Body Search	162

15.2.1 Search by Appearance	
15.2.2 Search by Picture	
15.2.3 Add Search Result as Sample Picture	164
Chapter 16 Network Settings	
16.1 Configure TCP/IP Settings	
16.2 Configure Guarding Vision	
16.3 Configure DDNS	167
16.4 Configure PPPoE	168
16.5 Configure NTP	
16.6 Configure SNMP	
16.7 Configure Email	
16.8 Configure Ports	
Chapter 17 System Maintenance	
17.1 Storage Device Maintenance	
17.1.1 Configure Disk Clone	
17.1.2 S.M.A.R.T Detection	174
17.1.3 Bad Sector Detection	
17.1.4 HDD Health Detection	176
17.2 Search & Export Log Files	
17.2.1 Search the Log Files	
17.2.2 Export the Log Files	
17.3 Import/Export IP Camera Configuration Files	179
17.4 Import/Export Device Configuration Files	
17.5 Upgrade System	
17.5.1 Upgrade by Local Backup Device	
17.5.2 Upgrade by FTP	
17.5.3 Upgrade by Guarding Vision	
17.6 Upgrade Camera	
17.7 Restore Default Settings	
17.8 System Service	
17.8.1 Network Security Settings	
17.8.2 Managing ONVIF User Accounts	
17.8.3 Managing IP Camera Activation	
Chapter 18 General System Settings	
18.1 Configure General Settings	

18.2 Configure Date & Time	189
18.3 Configure DST Settings	190
18.4 Configure Enhanced IP Mode	190
18.5 Manage User Accounts	191
18.5.1 Add a User	191
18.5.2 Set Permission for a User	192
18.5.3 Set Local Live View Permission for Non-Admin Users	194
18.5.4 Edit the Admin User	195
18.5.5 Edit the Operator/Guest User	197
18.5.6 Delete a User	197
18.6 Configure Password Security	198
18.6.1 Export GUID File	198
18.6.2 Configure Security Questions	198
18.6.3 Configure Reserved Email	199
18.7 Reset Password	200
18.7.1 Reset Password by GUID	200
18.7.2 Reset Password by Security Questions	201
18.7.3 Reset Password by Reserved Email	202
Chapter 19 Appendix	204
List of Applicable Power Adapter	204

Chapter 1 Introduction

1.1 Front Panel

Front Panel 1:

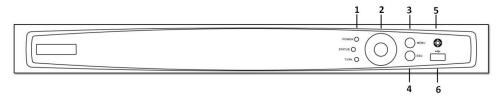


Figure 1-1 Front Panel

Table 1-1	Descriptionon of Front Panel
-----------	------------------------------

No.	Name	Function Description
1	POWER	Power indicator turns yellow when the power switch on the real panel is turned on.
	STATUS	Status indicator blinks red when data is being read from or written to HDD.
	Tx/Rx	Tx/Rx indictor blinks yellow when network connection is functioning properly.
2	DIRECTIONS	The DIRECTION buttons are used to navigate between different fields and items in menus.
		In the Playback mode, the Up and Down button is used to speed up and slow down recorded video. The Left and Right button will select the next and previous record files.
		In Live View mode, these buttons can be used to cycle through channels.
		In PTZ control mode, it can control the movement of the PTZ camera.
		The ENTER button is used to confirm selection in any of the menu modes.
	ENTER	It can also be used to tick checkbox fields.
		In Playback mode, it can be used to play or pause the video.

No.	Name	Function Description
		In single-frame Playback mode, pressing the button will advance the video by a single frame.
3	Menu	Access the main menu interface
4	ESC	Exit and back to the previous menu.
5	IR Receiver	Receiver for IR remote controller.
6	USB Interfaces	Universal Serial Bus (USB) ports for additional devices such as USB mouse and USB Hard Disk Drive (HDD).

Front Panel 2:

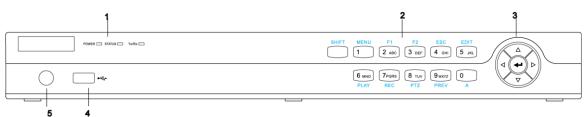


Figure 1-2 Front Panel

No.	Name		Function Description
	POWER		Turns yellow when the device s running.
1	STATUS		Flickers red when data is being read from or written to HDD, and turns yellow when the SHIFT function is realized.
	Tx/Rx		Flickers yellow when network connection is functioning properly.
2	Composite Keys 1/MENU	SHIFT	Switches between the numeric or letter input and functions of the composite keys.
		1/MENU	Enters numeral "1"; Accesses the main menu interface.

No.	Name		Function Description
			Enters numeral "2";
			Enters letters "ABC";
		2/ABC/F1	Uses the F1 button to select all items in a list field;
			Turns on/off PTZ light in PTZ Control mode, and use it to zoom out the image;
			Switches between main and spot video output in live view or playback mode.
			Enters numeral "3";
		3/DEE/E2	Enters letters "DEF";
		3/DEF/F2	Uses the F2 button to change the tab pages;
			Zooms in the image in PTZ control mode.
			Enters numeral "4";
		4/GHI/ESC	Enters letters "GHI";
			Exits and back to the previous menu.
			Enters numeral "5";
		5/JKL/EDIT	Enters letters "JKL";
			Deletes characters before cursor;
			Checks the checkbox and select the ON/OFF switch;
			Starts/stops record clipping in playback.
		6/MNO/PLAY	Enters numeral "6";
			Enters letters "MNO";

No.	Name		Function Description
			Accesses to playback interface in Playback mode.
			Enters numeral "7";
		7/PQRS/REC	Enters letters "PQRS";
			Accesses to manual record interface;
			Manually enables/disables record.
			Enters numeral "8";
		8/TUV/PTZ	Enters letters "TUV";
			Accesses PTZ control interface.
			Enters numeral "9";
		9/WXYZ/PREV	Enters letters "WXYZ";
			Multi-channel display in live view.
			Enters numeral "0";
		0/A	Shifts the input methods in the editing text field. (Upper and lowercase, alphabet, symbols or numeric input).
			Navigates between different fields and items in menus.
	DIRECTION		Uses the Up and Down buttons to speed up and slow down the playing of video files in Playback mode.
			The Left and Right button will select the next and previous record files.
			Cycles through channels in Live View mode.
3			Controls the movement of the PTZ camera in PTZ control mode.
	ENTER		Confirms selection in any of the menu modes.
			Checks the checkbox.
			Plays or pauses the playing of video files in Playback mode.
			Advances the video by a single frame in single- frame Playback mode.

No.	Name	Function Description
		Stops/starts auto switch in Auto-switch mode.
4	USB Interface	Universal Serial Bus (USB) ports for additional devices such as USB mouse and USB Hard Disk Drive (HDD).
5	IR Receiver	Receiver for IR remote control.

Front Panel 3:

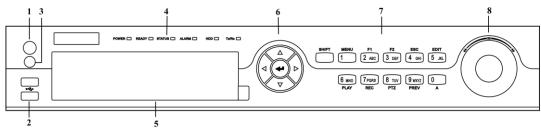


Figure 1-3 Front Panel

Table 1-3	Description of Front Panel
-----------	----------------------------

No.	Name	Function Description		
1	POWER ON/OFF	Power on/off switch.		
2	USB Interface	Connect to USB mouse or USB flash memory.		
3	IR Receiver	Receiver for IR remote control. devices.		
POWER		Power indicator lights in green when DVR is powered up.		
	READY	Ready indicator is normally green, indicating that the DVR is functioning properly.		
4	STATUS	Indicator turns green when DVR is controlled by an IR remote control with the address from 1~254;		
		Indicator turns red when the SHIFT button is used;		
		Indicator does not light when the DVR is controlled by a keyboard or by the IR remote control with the address of 255;		
		Indicator turns green when the DVR is controlled by IR remote control (with the address from 1~254) and keyboard at the		

		and the court had a court had a set	
		same time , and the SHIFT button is not used; Indicator turns orange : (a) when the DVR is controlled by IR remote control (with the address from 1~254) and keyboard at the same time and the SHIFT button is used as well; (b) when the DVR is controlled by IR remote control (with the address from 1~254) and the SHIFT button is used.	
	ALARM	Alarm indicator turns red when a sensor alarm is detected.	
	HDD	HDD indicator blinks in red when data is being read from or written to HDD.	
	Tx/Rx	TX/RX indictor blinks in green when network connection is functioning properly.	
5	DVD-ROM	Slot for DVD-ROM.	
	DIRECTION	The DIRECTION buttons are used to navigate between different fields and items in menus.	
		In Playback mode, the Up and Down button is used to speed up and slow down recorded video.	
		In All-day Playback mode, the Left/Right button can be used to select the recorded video of next/previous day; in Playback by Normal Video Search, the Left/Right button can be used to select the next/previous recorded file.	
6		In Live View mode, the directional buttons can be used to cycle through channels.	
		In PTZ control mode, it can control the movement of the PTZ camera.	
	ENTER	Confirm selection in any of the menu modes. It can also be used to tick checkbox fields.	
		In Playback mode, it can be used to play or pause the video.	
		In Single-frame Playback mode, pressing the ENTER button will advance the video by a single frame.	
		In Auto-switch mode, it can be used to stop /start auto switch.	
	SHIFT	Switch of compound keys between the numeric/letter input and functional control.	
7	1/MENU	Enter numeral "1";	
	_,	Access the main menu interface.	

		Enter numeral "2";
		Enter letters "ABC";
	2400/54	The F1 button can be used to select all items on the list;
	2ABC/F1	In PTZ Control mode, the F1 button can be used to zoom out (zoom-) the PTZ camera;
		In live view or playback mode, the F1 button can be used to switch between main and spot video output.
		Enter numeral "3";
		Enter letters "DEF";
	3DEF/F2	In PTZ Control mode, the F1 button can be used to zoom in (zoom+) the PTZ camera;
		The F2 button can be used to cycle through tab pages.
Ī		Enter numeral "4";
	4GHI/ESC	Enter letters "GHI";
		Exit and back to the previous menu.
Ī		Enter numeral "5";
		Enter letters "JKL";
	5JKL/EDIT	Delete characters before cursor;
		Select the checkbox and ON/OFF switch;
		Start/stop record clipping in playback.
Ī		Enter numeral "6";
		Enter letters "MNO";
	6MNO/PLAY	In Playback mode, it is used for direct access to playback interface.
		Enter numeral "7";
	7PQRS/REC	Enter letters "PQRS";
	/PQRS/REC	Manual record, for direct access to manual record interface; manually enable/disable record.
		Enter numeral "8";
	8TUV/PTZ	Enter letters "TUV";
		Access PTZ control interface.
		Enter numeral "9";
	9WXYZ/PREV	Enter letters "WXYZ";
		Multi-camera display in live view;
		In Playback mode or Menu \rightarrow Playback \rightarrow Tag playback interface,

		this button can be used to delete the selected tag.		
		Enter numeral "0";		
	0/A	Switch between input methods (upper and lowercase alphabet, symbols and numeric input).		
		In Playback mode, this button can be used to add the default tag.		
8	JOG SHUTTLE Control	Move the active selection in a menu. The inner ring will move the selection up and down; the outer ring will move it left and right.		
		In Playback mode, the inner ring is used to jump 30s forward/backward in video files. The outer ring can be used to speed up/slow down the video.		
		In Live View mode, it can be used to cycle through different channels.		
		In PTZ control mode, in can control the movement of the PTZ camera.		

Front Panel 4:

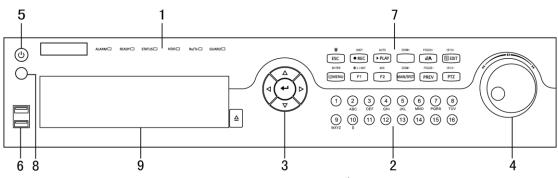


Figure 1-4 Front Panel

No.	Name		Function Description
1	Status Indicators	ALARM	Alarm indicator turns red when a sensor alarm is detected.
		READY	Turs blue when the device is functioning properly.

No.	Name		Function Description
		STATUS	Indicator turns blue when the device is controlled by an IR remote. Indicator turns red when controlled by a keyboard and orange when IR remote and keyboard is used at the same time. Indicator does not light when the device is
			controlled by the IR remote control with the address of 255. HDD indicator blinks in red when data is being
		HDD	read from or written to HDD.
		TX/RX	TX/RX indictor blinks in blue when network connection is functioning properly.
			Indicator turns blue when the device is armed;
		GUARD	Indicator does not light when the device is disarmed;
		COARD	The arm/disarm state can be initiated by pressing and holding on the ESC button for more than 3 seconds in live view mode.
	2 Alphanumeric Buttons		Switch to the corresponding channel in Live view or PTZ Control mode.
			Input numbers and characters in Edit mode.
2			Switch between different channels in Playback mode.
			The light of the button is blue when the corresponding channel is recording; it is red when the channel is in network transmission status; it is pink when the channel is recording and transmitting.
			The DIRECTION buttons are used to navigate between different fields and items in menus.
3	Control Buttons	DIRECTION	In the Playback mode, the Up and Down button is used to speed up and slow down recorded video. The Left and Right button will select the next and previous record files.

No.	Name		Function Description
			In Live View mode, these buttons can be used to cycle through channels.
			In PTZ control mode, it can control the movement of the PTZ camera.
			The ENTER button is used to confirm selection in any of the menu modes.
			It can also be used to tick checkbox fields.
		ENTER	In Playback mode, it can be used to play or pause the video.
			In single-frame Playback mode, pressing the button will advance the video by a single frame.
			In Auto-switch mode, it can be used to stop /start auto switch.
			Move the active selection in a menu. It will move the selection up and down.
			In Live View mode, it can be used to cycle through different channels.
4	JOG SHUTTLE Control		In the Playback mode: the outer ring is used to speed up or slow down the record files and the inner ring is used to jump 30s forward/backward in records files.
			In PTZ control mode, it can control the movement of the PTZ camera.
5	POWER		Power on/off switch.
6	USB Interfaces		Universal Serial Bus (USB) ports for additional devices such as USB mouse and USB Hard Disk Drive (HDD).
			Exit and back to the previous menu.

No.	Name		Function Description
		ESC	Arm/disarm the device in live view mode.
		REC/SHOT	Enter the Manual Record setting menu.
			In PTZ control settings, press the button and then you can call a PTZ preset by pressing Numeric button.
			It is also used to turn audio on/off in the Playback mode.
			Enter the Playback menu;
		PLAY/AUTO	Auto scan in the PTZ Control mode.
	Composi te Keys	ZOOM+	Zoom in the PTZ camera in the PTZ Control setting.
		A/FOCUS+	Adjust focus in the PTZ Control menu.
7			It is also used to switch between input methods (upper and lowercase alphabet, symbols and numeric input).
		EDIT/IRIS+	Edit text fields. When editing text fields, it will also function as a Backspace button to delete the character in front of the cursor.
			On checkbox fields, pressing the button will tick the checkbox.
			In PTZ Control mode, the button adjusts the iris of the camera.
			In Playback mode, it can be used to generate video clips for backup.
			Enter/exit the folder of USB device and eSATA HDD.
			Switch between main and spot output.

No.	Name	Function Description
	MAIN/SPOT/ ZOOM-	In PTZ Control mode, it can be used to zoom out the image.
		Select all items on the list when used in a list field.
	F1/ LIGHT	In PTZ Control mode, it will turn on/off PTZ light (if applicable).
		In Playback mode, it is used to switch between play and reverse play.
		Cycle through tab pages.
	F2/AUX	In synchronous playback mode, it is used to switch between channels.
		Press the button will help you return to the Main menu (after successful login).
	MENU/WIPE	Press and hold the button for 5 seconds will turn off audible key beep.
	R	In PTZ Control mode, the MENU/WIPER button will start wiper (if applicable).
		In Playback mode, it is used to show/hide the control interface.
	PREV/FOCUS	Switch between single screen and multi-screen mode.
	-	In PTZ Control mode, it is used to adjust the focus in conjunction with the A/FOCUS+ button.
		Enter the PTZ Control mode.
	PTZ/IRIS-	In the PTZ Control mode, it is used to adjust the iris of the PTZ camera.
8	IR Receiver	Receiver for IR remote control.

No.	Name	Function Description
9	DVD-R/W	Slot for DVD-R/W.

Front Panel 5:

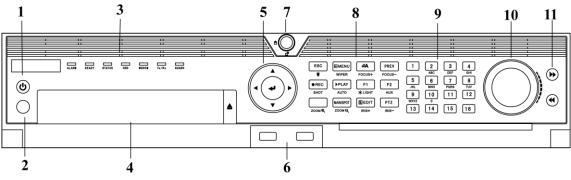


Figure 1-5 Front Panel

Table 1-5 Description of Front Panel

No.	Name		Function Description
1	POWER ON/OFF		Power on/off switch.
2	IR Receiver		Receiver for IR remote
		ALARM	Turns red when a sensor alarm is detected.
	Status Indicators	READY	Ready LED is normally blue, indicating that the device is functioning properly.
			Turns blue when device is controlled by an IR remote.
3		STATUS	Turns red when controlled by a keyboard and purple when IR remote and keyboard is used at the same time.
		HDD	Flashes red when data is being read from or written to HDD.
		MODEM	Reserved for future usage.

No.	Name		Function Description
		TX/RX	Flashes blue when network connection is functioning properly.
	-	GUARD	Guard LED turns blue when the device is in armed status; at this time, an alarm is enabled when an event is detected.
			The LED turns off when the device is unarmed. The arm/disarm status can be changed by pressing and holding on the ESC button for more than 3 seconds in live view mode.
4	DVD	0-R/W	Slot for DVD-R/W.
	Control Buttons	DIRECTION	The DIRECTION buttons are used to navigate between different fields and items in menus.
			In the Playback mode, the Up and Down button is used to speed up and slow down recorded video. The Left and Right button will select the next and previous record files.
			In Live View mode, these buttons can be used to cycle through channels.
_			In PTZ control mode, it can control the movement of the PTZ camera.
5		ENTER	The ENTER button is used to confirm selection in any of the menu modes.
			It can also be used to tick checkbox fields.
			In Playback mode, it can be used to play or pause the video.
			In single-frame Playback mode, pressing the button will advance the video by a single frame.
			In Auto-switch mode, it can be used to stop /start auto switch.

No.	Name		Function Description
6	USB Interfaces		Universal Serial Bus (USB) ports for additional devices such as USB mouse and USB Hard Disk Drive (HDD).
7	Front P	anel Lock	You can lock or unlock the panel by the key.
			Back to the previous menu.
		ESC	Press for Arming/disarming the device in Live View mode.
			Enter the Manual Record setting menu.
		REC/SHOT	In PTZ control settings, press the button and then you can call a PTZ preset by pressing Numeric button.
			It is also used to turn audio on/off in the Playback mode.
		PLAY/AUTO	The button is used to enter the Playback mode.
8	Composite Keys		It is also used to auto scan in the PTZ Control menu.
		ZOOM+	Zoom in the PTZ camera in the PTZ Control setting.
		A/FOCUS+	Adjust focus in the PTZ Control menu.
			It is also used to switch between input methods (upper and lowercase alphabet, symbols and numeric input).
		EDIT/IRIS+	Edit text fields. When editing text fields, it will also function as a Backspace button to delete the character in front of the cursor.
			On checkbox fields, pressing the button will tick the checkbox.

No.	Name	Function Description
		In PTZ Control mode, the button adjusts the iris of the camera.
		In Playback mode, it can be used to generate video clips for backup.
		Enter/exit the folder of USB device and eSATA HDD.
		Switch between main and spot output.
	MAIN/SPOT/Z OOM-	In PTZ Control mode, it can be used to zoom out the image.
		Select all items on the list when used in a list field.
	F1/ LIGHT	In PTZ Control mode, it will turn on/off PTZ light (if applicable).
		In Playback mode, it is used to switch between play and reverse play.
		Cycle through tab pages.
	F2/ AUX	In synchronous playback mode, it is used to switch between channels.
		Press the button will help you return to the Main menu (after successful login).
		Press and hold the button for 5 seconds will turn off audible key beep.
	MENU/WIPER	In PTZ Control mode, the MENU/WIPER button will start wiper (if applicable).
		In Playback mode, it is used to show/hide the control interface.

No.	Name	Function Description
	PREV/FOCUS-	Switch between single screen and multi-screen mode.
	PREV/FOCUS-	In PTZ Control mode, it is used to adjust the focus in conjunction with the A/FOCUS+ button.
		Enter the PTZ Control mode.
	PTZ/IRIS-	In the PTZ Control mode, it is used to adjust the iris of the PTZ camera.
		Switch to the corresponding channel in Live view or PTZ Control mode.
		Input numbers and characters in Edit mode.
9	Alphanumeric Buttons	Switch between different channels in Playback mode.
		The light of the button is blue when the corresponding channel is recording; it is red when the channel is in network transmission status; it is pink when the channel is recording and transmitting.
		Move the active selection in a menu. It will move the selection up and down.
		In Live View mode, it can be used to cycle through different channels.
10	JOG SHUTTLE Control	In the Playback mode: the ring is used to jump 30s forward/backward in video files.
		In PTZ control mode, it can control the movement of the PTZ camera.
11	SLOW DOWN/SPEED UP	Slow down/speed up in playback mode.

1.2 IR Remote Control Operations

The DVR may also be controlled with the included IR remote control.

Batteries (2×AAA) must be installed before operation.

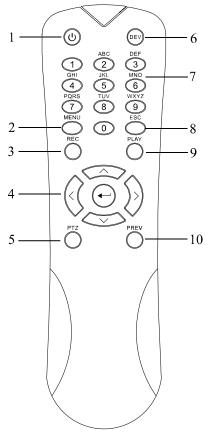


Figure 1-6 Remote Control

The keys on the remote control closely resemble the ones found on the front panel. Refer to Table 1-6, they include:

No.	Name	Description	
		Power on/off the device.	
1	POWER	Power on/off the device by pressing and holding the button for 5 seconds.	
		Press the button to return to the main menu (after successful login).	

Table 1-6 Description of the IR Remote Control Buttons

Network Video Recorder User Manual

No.	Name	Description	
	MENU Button	Press and hold the button for 5 seconds will turn off audible key beep.	
2		In PTZ Control mode, the MENU button will start wiper (if applicable).	
		In Playback mode, it is used to show/hide the control interface.	
		Enter the Manual Record setting menu.	
3	REC Button	In PTZ control settings, press the button and then you can call a PTZ preset by pressing Numeric button.	
		It is also used to turn audio on/off in the Playback mode.	
		Navigate between different fields and items in menus.	
	DIRECTION Button	In the Playback mode, the Up and Down button is used to speed up and slow down recorded video. The Left and Right button will select the next and previous record files.	
		In Live View mode, these buttons can be used to cycle through channels.	
4		In PTZ control mode, it can control the movement of the PTZ camera.	
	ENTER Button	Confirm selection in any of the menu modes.	
		It can also be used to <i>tick</i> checkbox fields.	
		In Playback mode, it can be used to play or pause the video.	
		In single-frame Playback mode, pressing the button will advance the video by a single frame.	
5	PTZ Button	In Auto-switch mode, it can be used to stop /start auto switch.	
6	DEV Enables/Disables Remote Control.		
-7	Alphanumeric	Switch to the corresponding channel in Live view or PTZ Control mode.	
7	Buttons	Input numbers and characters in Edit mode.	

Network Video Recorder User Manual

No.	Name	Description
		Switch between different channels in the Playback mode.
		Back to the previous menu.
8 ESC Button	ESC Button	Press for Arming/disarming the device in Live View mode.
0	DI AV Dutton	The button is used to enter the All-day Playback mode.
9	PLAY Button	It is also used to auto scan in the PTZ Control menu.
		Switch between single screen and multi-screen mode.
10	PREV Button	In PTZ Control mode, it is used to adjust the focus in conjunction with the A/FOCUS+ button.

Troubleshooting Remote Control:

Make sure you have installed batteries properly in the remote control. And you have to aim the remote control at the IR receiver on the front panel.

If there is no response after you press any button on the remote, follow the procedure below to troubleshoot.

- Step 1 Go to **Menu > Configuration > General > More Settings** by operating the front control panel or the mouse.
- Step 2 Check and remember the DVR No. The default DVR No. is 255. This number valid for all IR remote controls.
- Step 3 Press the DEV button on the remote control.
- Step 4 Enter the DVR No. in step 2.

Step 5 Press the ENTER button on the remote.

If the Status indicator on the front panel turns blue, the remote control is operating properly. If the Status indicator does not turn blue and there is still no response from the remote, please check the following:

Step 6 Batteries are installed correctly and the polarities of the batteries are not reversed.

Step 7 Batteries are fresh and not out of charge.

Step 8 IR receiver is not obstructed.

If the remote still cannot function properly, please change the remote and try again, or contact the device provider.

1.3 USB Mouse Operation

A regular 3-button (Left/Right/Scroll-wheel) USB mouse can also be used with this device. To use a USB mouse:

Step 1 Plug USB mouse into one of the USB interfaces on the front panel of the device.

Step 2 The mouse should automatically be detected. If in a rare case that the mouse is not detected, the possible reason may be that the two devices are not compatible, please refer to the recommended the device list from your provider.

The operation of the mouse:

Name	Action	Description
	Single-Click	 Live view: Select channel and show the quick set menu. Menu: Select and enter.
Left-Click	Double-Click	Live view: Switch between single-screen and multi- screen.
	Click and Drag	 PTZ control: pan, tilt and zoom. Video tampering, privacy mask and motion detection: Select target area. Digital zoom-in: Drag and select target area. Live view: Drag channel/time bar.
Right-Click	Single-Click	 Live view: Show menu. Menu: Exit current menu to upper level menu.
Scroll-Wheel	Scrolling up	Live view: Previous screen.Menu: Previous item.
	Scrolling down	Live view: Next screen.Menu: Next item.

Table 1-1	Description	of the	Mouse	Control
-----------	-------------	--------	-------	---------

1.4 Rear Panel



The rear panel varies according to different models. Please refer to the actual product. The following figures are for reference only.

Rear Panel 1:

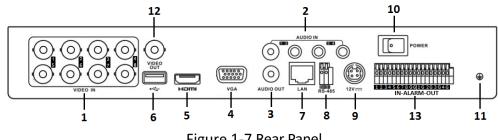
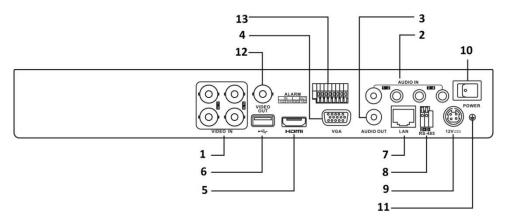


Figure 1-7 Rear Panel

Rear Panel 2:



Rear Panel 3:

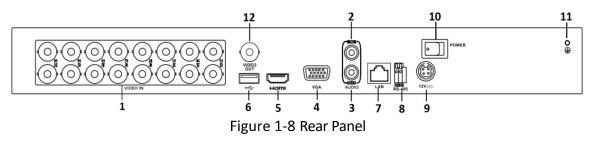


Table 1-7 Description of Rear Panel

No.	Item	Description
1	VIDEO IN	BNC interface for TVI HD and analog video input.
2	AUDIO IN	RCA connector
3	AUDIO OUT	RCA connector.

No.	Item	Description
4	VGA	DB15 connector for VGA output. Display local video output and menu.
5	HDMI	HDMI video output connector.
6	USB Interface	Universal Serial Bus (USB) port for additional devices.
7	Network Interface	Connector for network
8	RS-485 Interface	Connector for RS-485 devices.
9	Power Supply	48 VDC or 12 VDC.
10	Power Switch	Switch for turning on/off the device.
11	GND	Ground
12	VIDEO OUT	BNC connector for video output.
13	Alarm In/Out	Connector for alarm input and output.

Rear Panel 4:

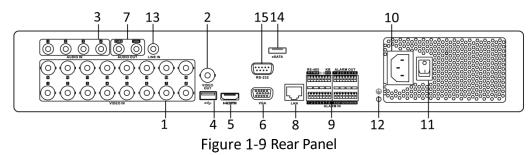


Table 1-8 C	Description of Rear Panel
-------------	---------------------------

No.	Item	Description
1	VIDEO IN	BNC interface for TVI HD and analog video input.
2	VIDEO OUT	BNC connector for video output.
3	AUDIO IN	RCA connector

No.	Item	Description
4	USB Port	Universal Serial Bus (USB) port for additional devices.
5	HDMI	HDMI video output connector.
6	VGA	DB15 connector for VGA output. Display local video output and menu.
7	AUDIO OUT	RCA connector.
8	Network Interface	Connector for network
		Connector for RS-485 devices. T+ and T- pins connect to R+ and R- pins of PTZ receiver respectively.
9	RS-485 and Alarm Interface	D+, D- pin connects to Ta, Tb pin of controller. For cascading devices, the first DVR's D+, D- pin should be connected with the D+, D- pin of the next DVR.
		Connector for alarm input.
		Connector for alarm output.
10	Power Supply	100 to 240 VAC power supply.
11	Power Switch	Switch for turning on/off the device.
12	GND	Ground
13	LINE IN	BNC connector for audio input.
14	eSATA	Connects external SATA HDD, CD/DVD-RW.
15	RS-232 Interface	Connector for RS-232 devices.

Rear Panel 5:

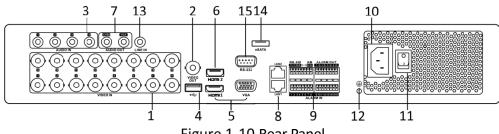


Figure 1-10 Rear Panel

Rear Panel 6:

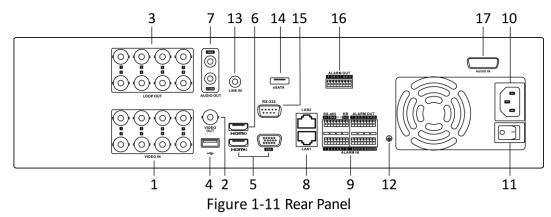


Table 1-9 Description of Rear Panel

No.	Item	Description
1	VIDEO IN	BNC interface for TVI HD and analog video input.
2	VIDEO OUT	BNC connector for video output.
3	AUDIO IN/ LOOP OUT (for 2U models)	RCA connector
4	USB Port	Universal Serial Bus (USB) port for additional devices.
5	HDMI1/VGA	Simultaneous HDMI1/VGA output. Display local video output and menu.
6	HDMI2	HDMI2 video output connector.
7	AUDIO OUT	RCA connector.
8	Network Interface	Connector for network

Network Video Recorder User Manual

No.	Item	Description
		Connector for RS-485 devices. T+ and T- pins connect to R+ and R- pins of PTZ receiver respectively.
9	RS-485 and Alarm Interface	D+, D- pin connects to Ta, Tb pin of controller. For cascading devices, the first DVR's D+, D- pin should be connected with the D+, D- pin of the next DVR.
		Connector for alarm input.
		Connector for alarm output.
10	Power Supply	100 to 240 VAC power supply.
11	Power Switch	Switch for turning on/off the device.
12	GND	Ground
13	LINE IN	BNC connector for audio input.
14	eSATA	Connects external SATA HDD, CD/DVD-RW.
15	RS-232 Interface	Connector for RS-232 devices.
16	ALARM OUT	Connector for alarm output.
17	AUDIO IN (for 2U models)	RCA connector

Chapter 2 Getting Started

2.1 Start up the Device

Purpose:

Proper startup and shutdown procedures are crucial to expanding the life of the device.

Before you start:

Check that the voltage of the extra power supply is the same with the device's requirement, and the ground connection is working properly.

Step 1 Connect the device power supply interface and electrical socket with delivered power cable. It is HIGHLY recommended that an Uninterruptible Power Supply (UPS) be used in conjunction with the device. The Power button on the front panel should be red, indicating the device is receiving the power.

2.2 Activate the Device

Purpose:

For the first-time access, you need to activate the device by setting an admin password. No operation is allowed before activation. You can also activate the device via Web Browser, SADP, or Client Software.

Step 1 Enter the admin password twice.

admin	

Weak	

Export GUID	0
Security Question Configuration	
Reserved E-mail Settings	0
Create Channel Default Password	
Note:Valid password range [8-16]. Yo use a combination of numbers, lower uppercase and special character for password with at least two kinds of th contained.	rcase, your

Figure 2-1 Set Admin Password

We highly recommend you create a strong password of your own choosing (Using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters.) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

Step 2 Enter the password to activate the IP camera(s) connected to the device.

Step 3 Optionally, check **Export GUID**, **Security Question Configuration**, or **Reserved E-mail Settings** for password resetting in the future.

Step 4 Click OK.

What to do next:

- 2 When you have enabled **Export GUID**, continue to export the GUID file to the USB flash drive for the future password resetting.
- 2 When you have enabled **Security Question Configuration**, continue to set the security questions for the future password resetting.

Question 1	Your father's name.	-	
Answer 1			
Question 2	Your mother's name.	*	
Answer 2			
Question 3	Your senior class teacher	s na 🔹	
Answer 3			

Figure 2-2 Set Security Questions

• When you have enabled **Reserved E-mail Settings**, continue to set the reserved email for the future password resetting.

Reserved E-mail Se	ettings	\times
Reserved E-mail		
	ОК	Cancel

Figure 2-3 Set the Reserved Email

- After the device is activated, you should properly keep the password.
- You can duplicate the password to the IP cameras that are connected with default protocol.

2.3 Configure Unlock Pattern for Login

Purpose:

For the admin user, you can configure the unlock pattern for device login.

Step 1 After the device is activated, you can enter the following interface to configure the device unlock pattern.

Step 2 Use the mouse to draw a pattern among the 9 dots on the screen. Release the mouse when the pattern is done.

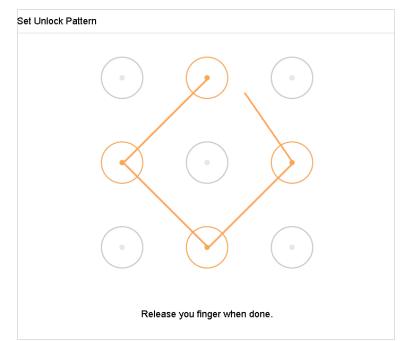


Figure 2-4 Draw the Pattern

- Connect at least 4 dots to draw the pattern.
- Each dot can be connected for once only.

Step 3 Draw the same pattern again to confirm it. When the two patterns match, the pattern is configured successfully.

If the two patterns are different, you must set the pattern again.

2.4 Login to the Device

2.4.1 Log in via Unlock Pattern

- Only the *admin* user has the permission to unlock the device.
- Please configure the pattern first before unlocking. Please refer to 2.2 Activate the Device

Step 1 Right click the mouse on the screen and select the menu to enter the interface.



Figure 2-5 Draw the Unlock Pattern

Step 2 Draw the pre-defined pattern to unlock to enter the menu operation.

- If you have forgotten your pattern, you can select the **Forgot My Pattern** or **Switch User** option to enter the normal login dialog box.
- When the pattern you draw is different from the pattern you have configured, you should try again.
- If you have drawn the wrong pattern for more than 5 times, the system will switch to the normal login mode automatically.

2.4.2 Log in via Password

Purpose:

If device has logged out, you must login the device before operating the menu and other functions.

Step 1 Select the User Name in the dropdown list.

HVR 4.0		
	Welcome	
	admin -	
	Password	
	Login	

Figure 2-6 Login Interface

Step 2 Input password.

Step 3 Click **OK** to log in.

- When you forget the password of the admin, you can click **Forgot Password** to reset the password.
- In the Login dialog box, if you enter the wrong password 7 times, the current user account will be locked for 60 seconds.

2.5 Enter Wizard to Configure Quick Basic Settings

Purpose:

By default, the Setup Wizard starts once the device has loaded.

The Setup Wizard can walk you through some important settings of the device. If you don't want to use the Setup Wizard at that moment, click the **Exit** button.

Step 1 Configure the date and time on the Date and Time Setup interface.

Date and Ti	ne Setup				
Time Zone	(GMT+08:00) Beijing, Urumd 👻				
Date Format	DD-MM-YYYY ~				
System Date	10-10-2017				
System Time	16:12:33				
⊡ Enable Wizard			Previous	Next	Exit

Figure 2-7 Date and Time Settings

Step 2 After the time settings, click **Next** to enter the Network Setup Wizard window, as shown in the following figure.

Network Setup					
Working Mode	Net Fault-Tolerance	Enable DHCP			
Select NIC	bond0 ~	IPv4 Address	10 . 15 . 1 . 19		
NIC Туре	10M/100M/1000M Self-adapi	IPv4 Subnet Mask	255 . 255 . 255 . 0		
Enable Obtain DNS Serv		IPv4 Default Gateway	10 . 15 . 1 . 254		
Preferred DNS Server					
Alternate DNS Server					
Main NIC	LAN1 -				
			Previous	Next	Exit

Figure 2-8 Network Settings

Step 3 Click **Next** after you configured the network parameters, which takes you to the **HDD Management** window.

]	Label	Capacity	Status	Property	Туре	Free Space	
	5	931.52GB	Normal	R/W	Local	876.00GB	
	7	931.52GB	Normal	RM	Local	831.00GB	
						Init	

Figure 2-9 HDD Management

Step 4 To initialize the HDD, click the **Init** button. Initialization removes all the data saved in the HDD.

Step 5 Click Next. You enter the Camera Setup interface to add the IP cameras.

- 1) Click **Search** to search the online IP Camera. Before adding the camera, make sure the IP camera to be added is in active status.
- 2) Click the **Add** to add the camera.

If the camera is in inactive status, you can select the camera from the list and click **Activate** to activate the cameras.

Camera Setup										
IP Address	Security	Amount	Device Model	P	rotocol	Management Port	Subnet Mask	Serial No	þ	MAC Address
Enable H.265 (For Initia	al Access)						+	Add	G Sear	ch 🖉 Activ
								Previous		Next

Figure 2-10 Search for IP Cameras

Step 6 Enter the Platform Access and configure the Guarding Vision settings.

Step 7 Click **Next** to enter the **Change Password** interface to create the new admin password if required.

Change Password			
New Admin Password			
Admin Password			
New Password			
	Strong		
Confirm	> ₇₇₅ ⊗		
Unlock Pattern			
	Note: Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.		

Figure 2-11 Change Password

You can enter click the 🔤 to show the characters input.

- 1) Check the checkbox of New Admin Password.
- 2) Enter the original password in the text field of Admin Password
- 3) Input the same password in the text field of **New Password** and **Confirm**.
- 4) Check the **Unlock Pattern** to enable the unlock pattern login.

We highly recommend you create a strong password of your own choosing (Using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters.) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

Step 8 Click **OK** to complete the startup Setup Wizard.

2.6 Enter Main Menu

After you have completed the wizard, you can right click on the screen to enter the main menu bar. Refer to the following figure and table for the description of main menu and sub-menus.

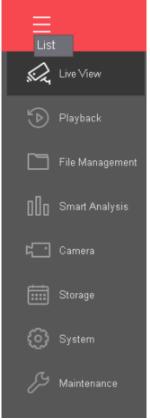
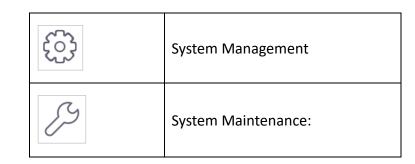


Figure 2-12 Main Menu Bar

Icon	Description
	Live View
۲ ۵	Playback
	File Management
000	Smart Analysis
	Camera Management
	Storage Management

Table 2-1 Description of Icons



2.7 System Operation

2.7.1 Log out

Purpose:

After logging out, the monitor turns to the live view mode and if you want to perform any operations, you need to enter user name and password to log in again.



Step 1 Click On the menu bar.

Step 2 Click Logout.

I NOTE

After you have logged out the system, menu operation on the screen is invalid. It is required to input a user name and password to unlock the system.

2.7.2 Shut Down the Device

U on the menu bar. Step 1 Click

Step 2 Click the Shutdown.

Step 3 Click the Yes.

Do not conduct power off operation again when the system is shutting down.

2.7.3 Reboot the Device

Purpose:

From the Shutdown menu, you can also reboot the device.

Step 1 Click on the menu bar.

Step 2 Click **Reboot** to reboot the device.

Chapter 3 Camera Management

3.1 Add the IP Cameras

3.1.1 Add the IP Camera Manually

Purpose:

Before you can get live video or record the video files, you should add the network cameras to the connection list of the device.

Before you start:

Ensure the network connection is valid and correct, and the IP camera to add has already been activated.

Step 1 Click on the main menu bar.

Step 2 Click **Camera > IP Camera > Custom Add** on the title bar or click in the idle channel window to enter the Add IP Camera interface.

Step 3 Enter IP address, protocol, management port, and other information of the IP camera to add.

Step 4 Enter the login user name and password of the IP camera.

Add IP Camera (Custom)				>
No. Stat Secu	rity	IP Address	Device Mo	odel
1 — 📀 Ac	tive	10.15.1.10	DS-2CD4	112F-I
IP Camera Address	10.1	5.1.10		
Protocol	ON	VIF		•
Management Port	80			
Transfer Protocol	Auto	0		-
User Name	adm	in		
Password				
Use IP Camera Activ				
		Search	Continue to Add	Add

Figure 3-1 Add IP Camera

Step 5 Click Add to finish the adding of the IP camera.

Step 6 (Optional) Click Continue to Add to continue to add other IP cameras.

3.1.2 Add the Automatically Searched Online IP Cameras

Step 1 On the **IP Camera** interface, click the **Number of Unadded Online Device** to expand the panel.

Step 2 Select the automatically searched online devices.

Step 3 Click Add.

	\approx \Rightarrow						
+ Add	G Refresh	P Activate				Enter a key	word.
No.	Status	Security	IP Address	Edit	Device Model	Protocol	Management
1		Active	10.15.1.10	C	DS-2CD4112F-I	HIKVISION	8000

Figure 3-2 Add IP Camera

- If the IP camera to add has not been activated, you can activate it from the IP camera list on the camera management interface.
- For Acusense series, when IP camera is added, the device will automatically switch the resolution to WD1/D1 and switch the bit rate to 512 Kbps.

3.1.3 Connect PoC Cameras

Before you start

- Ensure your device supports PoC (Power over Coaxitron) cameras connection.
- Connect the PoC camera to the DVR.

Purpose

-K/P series DVR support PoC (Power over Coaxitron) cameras connection. DVR will detect the connected PoC cameras automatically, manage the power consumption via the coaxial communication, and provide power to the cameras via coaxitron.

Step 1 Go to Menu > Camera > PoC Information.

- Step 2 Turn on the PoC for the channel(s) as your desire.
- Step 3 Check the status of connected PoC camera.

- If the power consumption of the DVR is lower than that of AF camera, when AF or AT camera is connected, there is no video and "Insufficient Power for PoC" is overlaid on the live view image.
- If the power consumption of the DVR is higher than that of the AF camera and lower than that of the AT camera, when AF camera is connected, it is powered on normally; when AT camera is connected, it is powered on and then powered off, and there is no video and "Insufficient Power for PoC" is overlaid on the live view image.
- If the power consumption of the DVR is higher than that of the AT camera, when AF or AT camera is connected, it is powered on normally.

Step 4 Check the connected AF or AT camera number and the connectable camera number.



Figure 3-3 PoC Status

- Only specified PoC camera is supported.
- The maximum connectable AT/AF camera number varies with different models.

Please turn off the PoC function if the camera does not support PoC, or the camera is not produced by the same manufacturer. Otherwise, it may result in permanent damage to the camera or DVR.

3.1.4 Configure Signal Input Channel

Purpose

You can configure the analog and IP signal input types.

Step	1	Click	~

on the main menu bar.

Step 2 Click Camera > Analog.

OHD/CVBS	OIP	
•		
	•	
•		
•		
•		
•		
•		
٠		
٠		
19		
٢		
	• • • • • • • •	 . .

Figure 3-4 Signal Input Status

Step 3 Check the checkbox to select different signal input types: HD/CVBS and IP. If you select HD/CVBS, four types of analog signal inputs including Turbo HD, AHD, HDCVI, and CVBS can be connected randomly for the selected channel. If you select IP, IP camera can be connected for the selected channel.

Step 4 Click Apply to save the settings.

You can view the max. accessible number of IP cameras in the Max. IP Camera Number text field. Refer to the specifications for the max. accessible IP camera number of different models.

3.1.5 Configuring 5 MP Long Distance Transmission

This chapter is only applicable to HUHI and HTHI series DVR.

Purpose

For HUHI and HTHI series DVR, you can configure 5 MP long distance transmission on the Signal Input Status interface.

Step 1 Click

on the main menu bar.

Step 2 Click Camera > Analog.

Step 3 Click where the 5 MP Long Distance Transmission Settings interface.



Figure 3-5 5 MP Long Distance Transmission Settings

Step 4 Select channel(s) to enable 5 MP Long Distance Transmission.

Step 5 Click OK.

Step 6 Click **Apply** to save the settings.

3.2 Enable the H.265 Stream Access

Purpose:

The device can automatically switch to the H.265 stream of IP camera (which supports H.265 video format) for the initial access.

Step 1 Click

 $^{
m J}$ on the main menu bar.

Step 2 Click **Camera > IP Camera > More Settings > H.265 Auto Switch Configuration** at the top taskbar.

Step 3 Check Enable H.265 (For Initial Access).

Step 4 Click **OK**.

3.3 Upgrade the IP Camera

Purpose:

The IP camera can be remotely upgraded through the device.

Plug the U-flash drive with the IP camera's firmware upgrade file to the device.

Step 1 Click

on the main menu bar.

Step 2 On the camera management interface, select a camera.

Step 3 Click **Camera > IP Camera > More Settings > Upgrade** at the top taskbar.

Step 4 Select the firmware upgrade file from the U-flash drive.

Step 5 Click Upgrade.

Result:

The IP camera will reboot automatically after the upgrading completes.

Chapter 4 Camera Settings

4.1 Configure OSD Settings

Purpose:

You can configure the OSD (On-screen Display) settings for the camera, including date/time, camera name, etc.

Step 1 Click on the main menu bar.

Step 2 Click Display.

Step 3 Select the camera from the drop-down list.

Step 4 Edit the name in the **Camera Name** text field.

Step 5 Check the checkbox of the **Display Name**, **Display Date** and **Display Week** if you want to show the information on the image.

Step 6 Set the date format, time format, and display mode.

Camera Name	IPdome			
		OSD Settings		
08-28-2017 Mon 1	16 : 32 : 45	 Display Name Display Date Display Week 		
		Date Format	MM-DD-YYYY	*
		Time For	24-hour	*
		Display M	Non-Transparent & No	*
		OSD Font	16×16	
		Exposure Day/Night Switch		
		Backlight		8
		Image Enhancemen		15

Figure 4-1 OSD Configuration Interface

Step 7 You can use the mouse to click and drag the text frame on the preview window to adjust the OSD position.

Step 8 Click the **Apply** button to apply the settings.

4.2 Configure Privacy Mask

Purpose:

The privacy mask can be used to protect personal privacy by concealing parts of the image from view or recording with a masked area.

Step 1 Click on the main menu bar.

Step 2 Click Privacy Mask.

Step 3 Select the camera to set privacy mask.

Step 4 Click the checkbox of **Enable** to enable this feature.

Step 5 Use the mouse to draw a zone on the window. The zones will be marked with different frame colors.

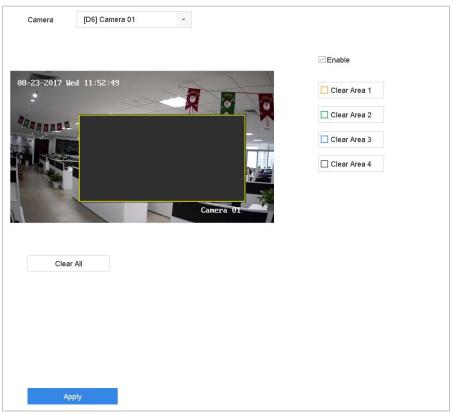


Figure 4-2 Privacy Mask Settings Interface

Up to 4 privacy masks zones can be configured and the size of each area can be adjusted.

Related Operation:

The configured privacy mask zones on the window can be cleared by clicking the corresponding Clear Zone1-4 icons on the right side of the window, or click **Clear All** to clear all zones.

Step 6 Click **Apply** to save the settings.

4.3 Configure the Video Parameters

Purpose:

You can customize the image parameters including the brightness, contrast, saturation for the live view and recording effect.

Step 1 Click on the main menu bar.

Step 2 Click Display.

Step 3 Select the camera from the drop-down list.

Step 4 Adjust the slider or click on the up/down arrow to set the value of the brightness, contrast or saturation.

Step 5 Click Apply to save the settings.

4.4 Configure the Day/Night Switch

Purpose:

The camera can be set to day, night or auto switch mode according to the surrounding illumination conditions.

Step 1 Click on the main menu bar.

Step 2 Click **Display.**

Step 3 Select the camera from the drop-down list.

Step 4 Select Day/Night Switch to Day, Night, Auto or Auto-Switch.

Auto: The camera switches between the day mode and the night mode according to the illumination automatically.

The sensitivity ranges from 0 to 7, and the higher sensitivity results in the more easily to trigger the mode switch.

The switch time refers to the interval time between the day/night switch. You can set it from 5 sec to 120 sec.

Auto-Switch: The camera switches the day mode and the night mode according to the start time and end time you set.

Step 5 Click the **Apply** to save the settings.

4.5 Configure Other Camera Parameters

Purpose:

For the connected camera, you can configure the camera parameters including the exposure mode, backlight and image enhancement.

Step 1 Click on the main menu bar.

Step 2 Click Display.

Step 3 Select the camera from the drop-down list.

Step 4 Configure the camera parameters.

- **Exposure**: Set the exposure time (1/10000 to 1 sec) of camera. The larger exposure value results in the brighter image.
- **Backlight**: Set the wide dynamic range (0 to 100) of the camera. When the surrounding illumination and the object have larger difference in brightness, you should set the WDR value.
- Image Enhancement: For optimized image contrast enhancement.

Step 5 Click the **Apply** to save the settings.

Chapter 5 Live View

Live view shows you the video image getting from each camera in real time.

5.1 Start Live View

Click on the main menu bar to enter the live view.

- You can select a window and double click a camera from the list to play the video from the camera in the selected window.
- Use the toolbar at the playing window bottom to realize the capture, instant playback, audio on/off, digital zoom, live view strategy, show information and start/stop recording, etc.

5.1.1 Digital Zoom

Purpose:

Digital Zoom is for zooming in the live image. You can zoom in the image to different proportions (1 to 16X).

Step 1 In the live view mode, click \bigcirc from the toolbar to enter the digital zoom interface.

Step 2 You can move the sliding bar or scroll the mouse wheel to zoom in/out the image to different proportions (1 to 16X).



Figure 5-1 Digital Zoom

5.1.2 Live View Strategy

Step 1 In the live view mode, click $\overrightarrow{}$ to enter the digital zoom operation interface in full screen mode.

Step 2 Select the live view strategy to Real-time, Balanced or Fluency.

5.2 Target Detection

Purpose:

In live view mode, the target detection function can be used to detect the human motion/face/vehicle/human body during the last 5 seconds and the following 10 seconds.

Step 1 In the live view mode, click **Target Detection** tab to enter the target detection interface.

Step 2 Check the checkbox of the icons to select different detection types: motion detection (), vehicle detection (), face detection () and human body detection ().

Step 3 You can select the historical analysis () or the real-time analysis () to btain the results.



Figure 5-2 Target Detection

Result:

The smart analysis results of the detection are displayed in the list. Optionally, click a result in list to play the related video.

5.3 Configure Live View Settings

Purpose:

Live View settings can be customized according to different needs. You can configure the output interface, dwell time for screen to be shown, mute or turning on the audio, the screen number for each channel, etc.

Step 1 Go to System > Live View > General.

Video Output Interface	VGA/HDMI	-	Event Output VGA/HDMI
Live View Mode	2 * 2	•	Full Screen Monitoring Dwell Time 10s
Dwell Time	5s	•	
Enable Audio Output			
Volume	1	5	
	_		
Apply			

Figure 5-3 Live View-General

Step 2 Configure the live view parameters.

- Video Output Interface: Select the video output to configure.
- Live View Mode: Select the display mode for live view, e.g., 2*2, 1*5, etc.
- **Dwell Time**: The time in seconds to dwell between switching of cameras when enabling autoswitch in Live View.
- Enable Audio Output: Enable/disable audio output for the selected video output.
- **Volume**: Adjust the volume of live view, playback and two-way audio for the selected output interface.
- **Event Output**: Select the output to show event video.
- Full Screen Monitoring Dwell Time: Set the time in seconds to show alarm event screen.

Step 3 Click **OK** to save the settings.

5.4 Configure Live View Layout

Step 1 Go to System> Live View>View.

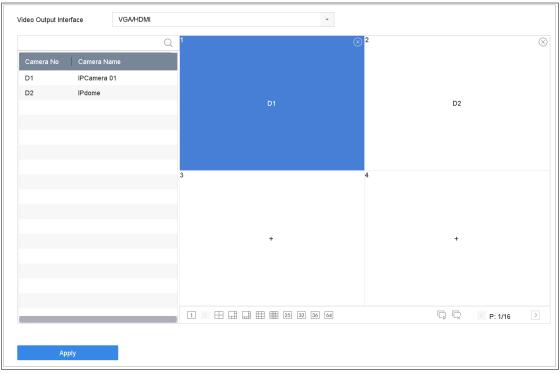


Figure 5-4 Live View

Step 2 Select the video output interface, e.g., HDMI/ VGA or channel-zero.

Step 3 Select a window division mode from the toolbar.

Step 4 Select a division window, and double-click on the camera from the list to set the camera to the window.

You can enter the number in the text field to quickly search the camera from the list.

You can also click-and-drag the camera to the desired window on the live view interface to set the camera order.

Related Operation:

• Click button to start live view for all the channels.



to stop all the live view.

Step 5 Click **Apply** to save the settings.

5.5 Configure Auto-Switch of Cameras

Purpose:

You can set the auto-switch of cameras to play in different display modes.

Step 1 Go to System > Live View > General.

Step 2 Set the video output interface, live view mode and dwell time.

- Video Output Interface: Select the video output interface.
- Live View Mode: Select the display mode for live view, e.g., 2*2, 1*5, etc.
- **Dwell Time:** The time in seconds to dwell between switching of cameras when enabling autoswitch. The range is from 5s to 300s.

Step 3 Go to View to set the view layout.

Step 4 Click **OK** to save the settings.

5.6 Configure Channel-zero Encoding

Purpose:

You can enable the channel-zero encoding when you need to get a remote view of many channels in real time from web browser or CMS (Client Management System) software, in order to decrease the bandwidth requirement without affecting the image quality.

Step 1 Go to System > Live View > General.

Step 2 Select the video output interface to **Channel-Zero**.

Step 3 Go to System > Live View > Channel-Zero.

Step 4 Check the checkbox to enable the channel-zero.

Enable Channel-Zero Encoding			
Frame Rate	Full Frame	•	
Max. Bitrate Mode	General	•	
Max. Bitrate(Kbps)	1792	•	
(and a	l		
Apply			

Figure 5-5 Live View- Channel-Zero Encoding

Step 5 Configure the **Frame Rate**, **Max. Bitrate Mode** and Max. Bitrate. The higher frame rate and bitrate settings result in the higher requirement of bandwidth.

Step 6 Click Apply.

Result:

You can view all of the channels in one screen using the CMS or web browser.

5.7 Using an Auxiliary Monitor

Certain features of the Live View are also available while in an Aux monitor. These features include:

- **Single Screen:** Switch to a full screen display of the selected camera. Camera can be selected from a dropdown list.
- **Multi-screen:** Switch between different display layout options. Layout options can be selected from a dropdown list.
- **Next Screen:** When displaying less than the maximum number of cameras in Live View, clicking this feature will switch to the next set of displays.
- **Playback:** Enter into Playback mode.
- **PTZ Control:** Enter PTZ Control mode.
- Main Monitor: Enter Main operation mode.

In the live view mode of the main output monitor, the menu operation is not available while Aux output mode is enabled.

Chapter 6 PTZ Control

6.1 PTZ Control Wizard

Before you start

Please make sure the connected IP camera supports the PTZ function and is properly connected.

Purpose

Follow the PTZ control wizard to guide you through the basic PTZ operation.

Step 1 Click $\stackrel{\checkmark}{\rightharpoonup}$ on the quick settings toolbar in the live view interface. The PTZ control wizard will pop up as below.

PTZ Control Wizard			
1. Drag the image to adjust PTZ view.	2. Click in the image to focus automatically.		
, →			
3. Scroll up/down to zoom in/out.	4. Click the lower-right corner icon to set the preset.		
●			
Do not show this prompt again.	ОК.		

Figure 6-1 PTZ Control Wizard

Step 2 Follow the wizard to adjust the PTZ view, focus, and zoom in/out the camera.

Step 3 (Optional) Check Do not show this prompt again.

Step 4 Click **OK** to exit.

6.2 Configure PTZ Parameters

Purpose

Follow the procedure to set the parameters for PTZ. The configuration of the PTZ parameters should be done before you control the PTZ camera.

Step 1 Click $\stackrel{\text{def}}{\longrightarrow}$ on the quick settings toolbar in the live view interface. The PTZ control panel displays on the right of the interface.

PTZ Parameter Set	ings			\times
Baud Rate	9600		~	
Data Bit	8		-	
Stop Bit	1		-	
Parity	None		~	
Flow Ctrl	None			
PTZ Protocol	PELCO-C		•	
Address	0			
Address range: 0~2	55			
		ок		Cancel

Step 2 Click PTZ Parameters Settings to set the PTZ parameters.

Figure 6-2 PTZ Parameters Settings

Step 3 Edit the parameters of the PTZ camera.

All the parameters should be exactly the same as the PTZ camera parameters.

Step 4 Click **OK** to save the settings.

6.3 Set PTZ Presets, Patrols & Patterns

Before you start:

Please make sure that the presets, patrols and patterns should be supported by PTZ protocols.

6.3.1 Set a Preset

Purpose:

Follow the steps to set the preset location which you want the PTZ camera to point to when an event takes place.

Step 1 Click $\stackrel{\smile}{\rightharpoonup}$ on the quick settings toolbar in the live view interface.

Step 2 Use the directional buttons on the PTZ control panel to wheel the camera to the location where you want to set preset, and the zoom and focus operations can be recorded in the preset as well.

Step 3 Click 🛄 in the lower right corner of live view to set the preset.



Step 4 Select the preset No. (1~255) from the drop-down list.

Step 5 Enter the preset name in the text field.

Step 6 Click **Apply** to save the preset.

Step 7 Repeat steps 2-6 to save more presets.

Step 8 (Optional) Click **Cancel** to cancel the location information of the preset.

Step 9 (Optional) Click in the lower right corner of live view to view the configured presets.



Figure 6-4 View the Configured Presets

6.3.2 Call a Preset

Purpose:

This feature enables the camera to point to a specified position such as a window when an event takes place.

Step 2 Click in the lower right corner of live view.

Step 3 Select the preset No. from the drop-down list.

Step 4 Click **Call** to call it.

1	-	Preset 1	Call	Apply	Cancel
Figure 6 F Call Preset (1)					

Figure 6-5 Call Preset (1)

Or click in the lower right corner of live view, and click the configured preset to call it.



Figure 6-6 Call Preset (2)

6.3.3 Set a Patrol

Purpose:

Patrols can be set to move the PTZ to different key points and have it stay there for a set duration before moving on to the next key point. The key points are corresponding to the presets.

Step 2 Click **Patrol** to configure patrol.

Aux Function	Patrol	Pattern
Patrol1		
🗱 Set	🕑 Call	Stop

Figure 6-7 Patrol Configuration

Step 3 Select the patrol No. in the text field.

Step 4 Click **Set** to enter the Patrol Settings interface.

Patrol Settings-Patrol 1				
+×	t ↓			
No	Preset	Speed	Duration	Edit
1	Preset 1	1	15	Ľ
2	Preset2	1	15	Ľ
			Apply	Cancel

Figure 6-8 Patrol Settings

Step 5 Click 📌 to add key point for the patrol.

KeyPoint		
Preset	Preset 1	•
Speed	1	
Duration	15	-
	Apply	Cancel

Figure 6-9 Key Point Configuration

1) Configure key point parameters.

Preset: It determines the order at which the PTZ will follow while cycling through the patrol.

Speed: It defines the speed at which the PTZ will move from one key point to the next.

Duration: It refers to the time span to stay at the corresponding key point.

2) Click **Apply** to save the key points to the patrol.

Step 6 (Optional) Click \square to edit the added key point.

KeyPoint		
Preset	Preset 1	-
Speed	1	-
Duration	15	
	Apply	Cancel
	Apply	Cancer

Figure 6-10 Edit Key Point

Step 7 (Optional) Select a key point and click X to delete it.

Step 8 (Optional) Click 📫 or 🦊 to adjust the key point order.

Step 9 Click **Apply** to save the settings of the patrol.

Step 10 Repeat steps 3-9 to set more patrols.

6.3.4 Call a Patrol

Purpose:

Calling a patrol makes the PTZ to move according to the predefined patrol path.

Step 1 Click $\stackrel{{}_{\scriptstyle{\leftarrow}}}{\rightharpoonup}$ on the quick settings toolbar in the live view interface.

The PTZ control panel displays on the right of the interface.

Step 2 Click Patrol on the PTZ control panel.

Aux Function		Patrol	Pattern
	Patrol1		
	🗱 Set	🕑 Call	Stop

Figure 6-11 Patrol Configuration

Step 3 Select a patrol in the text field.

Step 4 Click Call to call it.

Step 5 (Optional) Click Stop to stop calling it.

6.3.5 Set a Pattern

Purpose:

Patterns can be set by recording the movement of the PTZ. You can call the pattern to make the PTZ movement according to the predefined path.

Step 1 Click $\stackrel{\checkmark}{\rightharpoonup}$ on the quick settings toolbar in the live view interface.

The PTZ control panel displays on the right of the interface.

Step 2 Click Pattern to configure pattern.

Aux Function	Patrol	Pattern
Pattern1		
Recor	d 🕑 Call	Stop

Figure 6-12 Pattern Configuration

Step 3 Select the pattern No. in the text field.

Step 4 Set the pattern.

- 1) Click Record to start recording.
- 2) Click corresponding buttons on the control panel to move the PTZ camera.
- 3) Click Stop to stop recording.

The movement of the PTZ is recorded as the pattern.

Step 5 Repeat steps 3-4 to set more patterns.

6.3.6 Call a Pattern

Purpose:

Follow the procedure to move the PTZ camera according to the predefined patterns.

Step 1 Click $\stackrel{\smile}{\rightharpoonup}$ on the quick settings toolbar in the live view interface.

The PTZ control panel displays on the right of the interface.

Step 2 Click Pattern to configure pattern.

Aux Function		Patrol	Pattern
	Pattern1		
(Recor	d 🕞 Call	Stop

Figure 6-13 Pattern Configuration

Step 3 Select a pattern in the text field.

Step 4 Click Call to call it.

Step 5 (Optional) Click Stop to stop calling it.

6.3.7 Set Linear Scan Limits

Before you start:

Please make sure the connected IP camera supports the PTZ function, and is properly connected.

Purpose:

The linear scan can be enabled to trigger the scan in the horizontal direction in the predefined range.

INOTE

This function is supported by some certain models.

Step 1 Click $\stackrel{{\scriptstyle\checkmark}}{\rightharpoonup}$ on the quick settings toolbar in the live view interface.

The PTZ control panel displays on the right of the interface.

Step 2 Click the directional buttons to wheel the camera to the location where you want to set the limit, and click **Left Limit** or **Right Limit** to link the location to the corresponding limit.

The speed dome starts linear scan from the left limit to the right limit, and you must set the left limit on the left side of the right limit, as well the angle from the left limit to the right limit should be no more than 180°.

6.3.8 Call Linear Scan

Before operating this function, make sure the connected camera supports the linear scan and is in specified protocol.

Purpose:

Follow the procedure to call the linear scan in the predefined scan range.

Step 1 Click $\stackrel{{}_{\scriptstyle\smile}}{\rightharpoonup}$ on the quick settings toolbar in the live view interface.

Step 2 Click Linear Scan to start the linear scan and click it again to stop it.

Step 3 (Optional) Click Restore to clear the defined left limit and right limit data.

INOTE

Reboot the camera to take the settings into effect.

6.3.9 One-touch Park

i NOTE

Before operating this function, make sure the connected camera supports the linear scan and is in specified protocol.

Purpose

For some certain model of the speed dome, it can be configured to start a predefined park action (scan, preset, patrol and etc.) automatically after a period of inactivity (park time).

Step 1 Click $\stackrel{{}_{\scriptstyle{\leftarrow}}}{\rightharpoonup}$ on the quick settings toolbar in the live view interface.

Step 2 Click Park (Quick Patrol), Park (Patrol 1) or Park (Preset 1) to activate the park action.

Park (Quick Patrol): The dome starts patrol from the predefined preset 1 to preset 32 in order after the park time. The undefined preset will be skipped.

Park (Patrol 1): The dome starts moving according to the predefined patrol 1 path after the park time.

Park (Preset 1): The dome moves to the predefined preset 1 location after the park time.

The park time can only be set via the speed dome configuration interface. The value is 5s by default.

Step 3 Click Stop Park (Quick Patrol), Stop Park (Patrol 1) or Stop Park (Preset 1) to inactivate it.

6.4 Auxiliary Functions

Before you start

Please make sure the connected IP camera supports the PTZ function, and is properly connected.

Purpose

You can operate the auxiliary functions including light, wiper, and center on the PTZ control panel.

Step 1 Click $\stackrel{\checkmark}{\rightharpoonup}$ on the quick settings toolbar in the live view interface.

Step 2 Click Aux Function.



Figure 6-14 Aux Function Configuration

Step 3 Click the icons to operate the aux functions. See the table for the description of the icons.

Icon	Description
·•	Light on/off
	Wiper on/off
Ģ	Center

Table 6-1 Description of Aux Functions Icons

Chapter 7 Storage

7.1 Storage Device Management

7.1.1 Install the HDD

Before startup of the device, install and connect the HDD to the device. Refer to the Quick Start Guide for the installation instructions.

7.1.2 Add the Network Disk

You can add the allocated NAS or disk of IP SAN to device, and use it as network HDD.

Adding NAS

Step 1 Go to Storage > Storage Device.

Step 2 Click Add to enter the Custom Add interface.

Step 3 Select the type to NetHDD.

Step 4 Select the type to NAS.

Step 5 Enter NetHDD IP in the text field.

Step 6 Click Search to search the available NAS disks.

Custom Add				
NetHDD	NetHDD 1		•	
Туре	NAS		-	
NetHDD IP	120 . 36 . 2 . 39			
NetHDD Directory	/nas/device1/11		\otimes	Search
	L			
		ок	c	ancel

Figure 7-1 Add NAS Disk

Step 7 Select the NAS disk from the list, or you can manually enter the directory in the text field of NetHDD Directory.

Step 8 Click **OK** to complete the adding of the NAS disk.

Result:

After having successfully added the NAS disk, return to the HDD Information menu. The added NetHDD will be displayed in the list.

Adding IP SAN

- Step 1 Go to Storage > Storage Device.
- Step 2 Click Add to enter the Custom Add interface.
- Step 3 Select **NetHDD** from the drop-down list.

Step 4 Select Type to IP SAN.

Step 5 Enter NetHDD IP in the text field.

Step 6 Click **Search** to search the available IP SAN disks.

Step 7 Select the IP SAN disk from the list.

Step 8 Click **OK** to complete the adding of the IP SAN disk.

Up to 1 IP SAN disk can be added.

Custom Add			
NetHDD	NetHDD 1		•
Туре	IP SAN		•
NetHDD IP	120 . 36 . 2 . 39		
NetHDD Directory	iqn.2008-06.storos.1-2		Search
		ок	Cancel

Figure 7-2 Add IP SAN Disk

Result:

After having successfully added the IP SAN disk, return to the **HDD Information** menu. The added NetHDD will be displayed in the list.

If the installed HDD or NetHDD is uninitialized, please select it and click **Init** for initialization.

7.1.3 Configure eSATA for Data Storage

Purpose:

When there is an external eSATA device connected to device, you can configure eSATA for the data storage, and you can manage the eSATA in the device.

Step 1 Click Storage>Advanced.

Step 2 Select the usage type to **Export** or **Record/Capture** from the dropdown list of **Usage**.

- **Export**: Use the eSATA for backup.
- **Record/Capture:** Use the eSATA for record/capture. Refer to the following steps for operating instructions.

eSATA	eSATA1	~
Usage	Record/Capture	•

Figure 7-3 Set eSATA Mode

Step 3 When **Usage** type is selected to **Record/Capture**, enter the storage device interface.

Step 4 Edit the property of the selected eSATA, or initialize it is required.

7.2 Storage Mode 7.2.1 Configure HDD Group

Purpose:

Multiple HDDs can be managed in groups. Video from specified channels can be recorded onto a particular HDD group through HDD settings.

Step 1 Go to Storage > Storage Device.

Step 2 Select the HDD to set the group.

+ Add	i Çin	it				Total Capa	acity 1863.03GB	Free Space	1702.00GB
	Label	Capacity	Status	Property	Туре	Free Space	Group	Edit	Delete
~	5	931.52GB	Normal	R/W	Local	871.00GB	2		×
	7	931.52GB	Normal	R/W	Local	831.00GB	1	Ľ	×

Figure 7-4 Storage Device

Step 3 Click for enter the Local HDD Settings interface.

Local HDD Settir	ngs			
HDD No.	5			
HDD Property	• RW	⊖ Read-only	⊖ Redundan.	
Group		○4 ○5 ○6 I ○12 ○13 ○14		
HDD Capacity	931.52GB			

Figure 7-5 Local HDD Settings

Step 4 Select the Group number for the current HDD.

Step 5 Click OK.

Regroup the cameras for HDD if the HDD group number is changed.

Step 6 Go to Storage > Storage Mode.

Step 7 Select Mode to Group.

Step 8 Select the group No. from **Record on HDD Group**.

Step 9 Select the IP camera(s) to record/capture on the HDD group.

 Mode
 Quota
 Group

 Record on HDD Group
 2
 *

 IP Camera
 D1
 D2
 D3
 D4
 D5
 D6
 D7
 D8

 D9
 D10
 D11
 D12
 D13
 D14
 D15
 D16

 D17
 D18
 D19
 D20
 D21
 D22
 D23
 D24

 D25
 D26
 D27
 D28
 D29
 D30
 D31
 D32

 D33
 D34
 D35
 D36
 D37
 D38
 D39
 D40

 D41
 D42
 D43
 D44
 D45
 D46
 D47
 D48

 D49
 D50
 D51
 D52
 D53
 D54
 D55
 D56

Figure 7-6 Storage Mode-HDD Group

Step 10 Click Apply.

Reboot the device to activate the new storage mode settings.

7.2.2 Configure HDD Quota

Purpose:

Each camera can be configured with allocated quota for the storage of recorded files or captured pictures.

Step 1 Go to Storage > Storage Mode.

Step 2 Select Mode to Quota.

Step 3 Select a camera to set quota.

Step 4 Enter the storage capacity of Max. Record Capacity (GB) and Max. Picture Capacity (GB).

Mode	● Quota O Group	
Camera	[D1] IPCamera 01	
Used Record Capacity	18.00GB	
Used Picture Capacity	2048.00MB	
HDD Capacity (GB)	1863	
Max. Record Capacity (GB)	1500	
Max. Picture Capacity (GB)	50 🛞	
🔺 Free Quota Space 313	GB	
Copy to	Apply	

Figure 7-7 Storage Mode-HDD Quota

Step 5 (Optional) You can click **Copy to** if you want to copy the quota settings of the current camera to other cameras.

Step 6 Click **Apply** to apply the settings. Reboot the device to activate the new storage mode settings.

When the quota capacity is set to 0, all cameras will use the total capacity of HDD for record and picture capture.

7.3 Recording Parameters

7.3.1 Main Stream

The Main Stream refers to the primary stream that affects data recorded to the hard disk drive and will directly determine your recording quality and image size.

Comparing with the sub-stream, the main stream can provide a higher quality video with higher resolution and frame rate.

Frame Rate (FPS - Frames Per Second): refers to how many frames are captured each second. A higher frame rate is advantageous when there is movement in the video stream, as it maintains image quality throughout.

Resolution: Image resolution is a measure of how much detail a digital image can hold: the greater the resolution, the greater the level of detail. Resolution can be specified as the number of pixel-columns (width) by the number of pixel-rows (height), e.g.,1024×768.

Bitrate: The bit rate (in kbit/s or Mbit/s) is often referred to as speed, but actually defines the number of bits/time unit and not distance/time unit.

Enable H.264+ Mode: The H.264+ mode helps to ensure the high video quality with a lowered bitrate. It can effectively reduce the need of bandwidth and HDD storage space.

A higher resolution, frame rate and bitrate setting will provide you the better video quality, but it will also require more internet bandwidth and use more storage space on the hard disk drive.

7.3.2 Sub-Stream

The sub-stream is a second codec that runs alongside the mainstream. It allows you to reduce the outgoing internet bandwidth without sacrificing your direct recording quality.

The sub-stream is often exclusively used by smartphone applications to view live video. Users with limited internet speeds may benefit most from this setting.

7.3.3 Picture

The picture refers to the live picture capture in continuous or event recording type.

Picture Quality: set the picture quality to low, medium or high. The higher picture quality results in more storage space requirement.

Interval: the interval of capturing live picture.

7.3.4 Configure Advanced Recording Settings

Step 1 Go to Storage > Record Schedule.

- Step 2 Check Enable Schedule to enable scheduled recording.
- Step 3 Click Advanced to set the recording parameters.

Record Audio:	4	
Pre-Record:	5s	-
Post-Record:	5s	
Stream Type:	Main Stre	•
Expired Time (day):	0	

Figure 7-8 Advanced Record Settings

- Record Audio: Check the checkbox to enable or disable audio recording.
- **Pre-record**: The time you set to record before the scheduled time or event. For example, when an alarm triggers the recording at 10:00, and if you set the pre-record time as 5 seconds, the camera records at 9:59:55.
- **Post-record:** The time you set to record after the event or the scheduled time. For example, when an alarm triggered recording ends at 11:00, and if you set the post-record time as 5 seconds, it records till 11:00:05.
- **Expired Time**: The expired time is period for a recorded file to be kept in the HDD. When the deadline is reached, the file will be deleted. If you set the expired time to 0, the file will not be deleted. The actual keeping time for the file should be determined by the capacity of the HDD.
- **Redundant Record/Capture**: By enabling redundant record or capture you save the record and captured picture in the redundant HDD. See *Chapter Configure Redundant Recording and Capture*.
- **Stream Type**: Main stream and sub-stream are selectable for recording. When you select substream, you can record for a longer time with the same storage space. For Acusense series, the default value is dual stream, this value cannot be edited.

Step 4 Click **OK** to save the settings.

7.4 Configure Recording Schedule

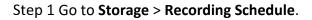
Set the record schedule, and then the camera automatically starts/stops recording according to the configured schedule.

Before you start

Make sure you have installed the HDDs to the device or added the network disks before you storing the video files, pictures and log files.

Refer to the *Quick Start Guide* for the HDD installation.

Refer to *Chapter 7.1.2* Add the Network Disk for network HDD connections.



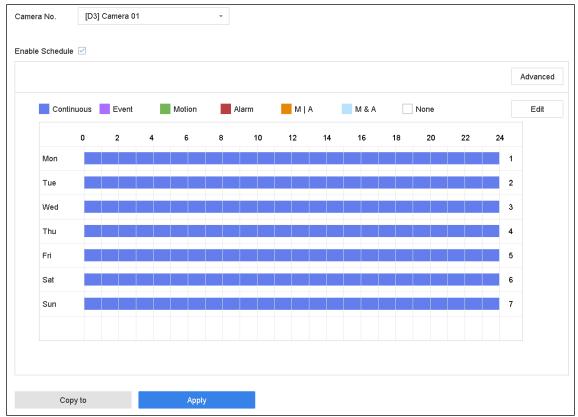


Figure 7-9 Recording Schedule

Step 2 Select a camera.

Step 3 Check Enable Schedule.

Step 4 Select a record type. The record type can be **Continuous**, **Motion Detection**, **Alarm**, **Motion | Alarm**, **Motion & Alarm**, and **Event**.

Different recording types are configurable.

Continuous: scheduled recording.

Event: recording triggered by all event triggered alarm.

Motion: recording triggered by motion detection.

Alarm: recording triggered by alarm.

M/A: recording triggered by either motion detection or alarm.

M&A: recording triggered by motion detection and alarm.

Step 5 Select a day and click-and-drag the mouse on the time bar to set the record schedule.

Step 6 Repeat the above steps to schedule recording or capture for other days in the week.

The all-day continuous recording is configured for the device by factory default.

Step 7 Click Apply to save the settings.

i NOTE

To enable Motion, Alarm, M | A (motion or alarm), M & A (motion and alarm) and Event triggered recording and capture, you must configure the motion detection settings, alarm input settings and other events as well. Please refer to Chapter 10 and Ofor details.

7.5 Configure Continuous Recording

Step 1 Go to Camera > Encoding Parameters > Recording Parameters.

Step 2 Set the parameters for the camera.

Step 3 Go to Storage > Recording Schedule.

Step 4 Select the recording type to **Continuous**.

Step 5 Drag the mouse on the time bar to set the continuous recording schedule. Refer to Chapter 7.4 Configure Recording Schedule for details.

7.6 Configure Motion Detection Triggered Recording

You can configure the recording triggered by the motion detection event.

Step 1 Go to System > Event > Normal Event > Motion Detection.

Step 2 Configure the motion detection and select the channel (s) to trigger the recording when motion event occurs. Refer to 11.2 Configure Alarm Linkage Actions for details.

Step 3 Go to Camera > Video Parameters.

Step 4 Set the event main stream/sub-stream recording parameters for the camera.

Step 5 Go to Storage > Schedule > Record.

Step 6 Select the recording type to Motion.

Step 7 Drag the mouse on the time bar to set the motion detection recording schedule. Refer to Chapter 7.4 Configure Recording Schedule for details.

7.7 Configure Event Triggered Recording

Purpose:

You can configure the recording triggered by the motion detection, motion detection and alarm, face detection, vehicle detection, line crossing detection, etc.

Step 1 Go to System > Event.

Step 2 Configure the event detection and select the channel (s) to trigger the recording when event occurs. Refer to Chapter 11 Event and Alarm Settings and Chapter 13 VCA Event Alarm for details.

Step 3 Go to Camera > Video Parameters.

Step 4 Set the event main stream/sub-stream recording parameters for the camera.

Step 5 Go to Storage > Schedule > Record.

Step 6 Select the recording type to Event.

Step 7 Drag the mouse on the time bar to set the event detection recording schedule. Refer to Chapter 7.4 Configure Recording Schedule for details.

7.8 Configure Alarm Triggered Recording

Purpose:

You can configure the recording triggered by the motion detection, face detection, vehicle detection, line crossing detection, etc.

Step 1 Go to System > Event > Normal Event > Alarm Input.

Step 2 Configure the alarm input and select the channel (s) to trigger the recording when alarm occurs. Refer to Chapter 11 Event and Alarm Settings and Chapter 13 VCA Event Alarm for details.

Step 3 Go to Camera > Video Parameters.

Step 4 Set the event main stream/sub-stream recording parameters for the camera.

Step 5 Go to Storage > Schedule > Record.

Step 6 Select the recording type to Alarm

Step 7 Drag the mouse on the time bar to set the alarm recording schedule. Refer to Chapter 7.4 Configure Recording Schedule for details.

7.9 Configure Picture Capture

Purpose:

The picture refers to the live picture capture in continuous or event recording type.

Step 1 Go to Storage > Capture Schedule > Advanced.

Step 2 Set the picture parameters.

- **Resolution**: set the resolution of the picture to capture.
- **Picture Quality**: set the picture quality to low, medium or high. The higher picture quality results in more storage space requirement.
- Interval: the interval of capturing live picture.

Step 3 Go to Storage > Capture Schedule.

Step 4 Select the camera to configure the picture capture.

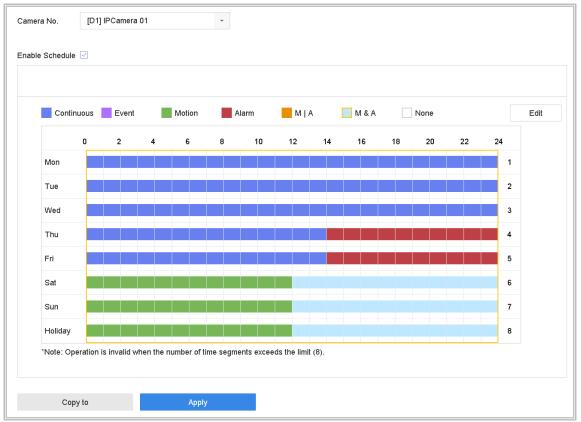


Figure 7-10 Set Picture Capture Schedule

Step 5 Set the picture capture schedule. Refer to Chapter 7.4 Configure Recording Schedule for details.

7.10 Configure Holiday Recording and Capture

Purpose:

Follow the steps to configure the record or capture schedule on holiday for that year. You may want to have different plan for recording and capture on holiday.

Step 1 Go to **System > Holiday**.

Step 2 Select a holiday item from the list and click

Step 3 Check the **Enable** to configure the holiday.

Edit						
Enable						
Holiday N	Holiday1					
Mode	By Month					•
Start Date	Jan		•	1		*
End Date	Feb		•	8		•
			_			
		Apply		ОК	Cancel	

Figure 7-11 Edit Holiday Settings

- 1) Edit the holiday name.
- 2) Select the mode to by date, by week or by month.
- 3) Set the start and end date of the holiday.
- 4) Click **OK**.

Step 4 Set the schedule for the holiday recording. Refer to Chapter 7.4 Configure Recording Schedule for details.

7.11 Configure Redundant Recording and Capture

Purpose:

Enabling redundant recording and capture, which means saving the record files and captured pictures not only in the R/W HDD but also in the redundant HDD, will effectively enhance the data safety and reliability.

You must set the storage mode to *Group* before you set the HDD property to Redundancy. For detailed information, please refer to Chapter 7.2.1 Configure HDD Group. There should be at least another HDD which is in Read/Write status.

Step 1 Go to Storage > Storage Device.

Step 2 Select a HDD from the list and Click is to enter the Local HDD Settings interface.

Step 3 Set the HDD property to **Redundancy**.

Local HDD Settir	ıgs			
HDD No.	5			
HDD Property	RW	◯ Read-only	 Redundan 	
Group		○4 ○5 ○6		
	○9 ○10 ○1	1 0 12 0 13 0 14	015 016	
HDD Capacity	931.52GB			
			ок	Cancel

Figure 7-12 HDD Property-Redundancy

Step 4 Go to Storage > Schedule Settings > Record Schedule/Capture Schedule.

Step 5 Click Advanced to set the camera recording parameters.

Advanced Parameters				
Record Audio:				
Pre-Record:				•
Post-Record:	5s			-
Stream Type:	Main Stream	1		•
Expired Time (da	iy):	5		
Redundant Re	ecord/Capture			
	ок		Cance	

Figure 7-13 Record Parameters

Step 6 Check the checkbox of **Redundant Record/Capture**.

Step 7 Click **OK** to save settings.

7.12 Configure 1080p Lite

Purpose

When the 1080P Lite Mode is enabled, the encoding resolution at 1080P Lite (real-time) is supported. If not, up to 1080P (non-real-time) is supported.

This chapter is applicable to HQHI series DVR.

7.12.1 Enable the 1080P Lite Mode

Step 1 Go to Menu > Record > Advanced.

Network Video Recorder User Manual

Overwrite		
Enable HDD Sleeping		
1080P Lite Mode		
H.264+/H.265+ for All the Analo	Enable	Disable
Apply		

Figure 7-14 Advanced Interface

- Step 2 Check the checkbox of **1080P Lite Mode** and click **Apply** to pop up the attention box. After enabling 1080p lite mode, the 3 MP signal is not accessible to analog channel.
- Step 3 Click Yes in popup message box to reboot the device to have new settings taken effect.

7.12.2 Disable the 1080P Lite Mode

- Step 1 Go to Menu > Record > Advanced.
- Step 2 Uncheck the checkbox of **1080P Lite Mode** and click **Apply**. The following attention box pops up.
- Step 3 Click **Yes** in popup message box to reboot the device to activate the new settings or **No** to restore the old settings.

Chapter 8 Disk Array

This chapter is applicable for Pro and Ultra series DVR.

Purpose:

Disk array is a data storage virtualization technology that combines multiple physical disk drive components into a single logical unit. An array stores data over multiple HDDs to provide enough redundancy so that data can be recovered if one disk fails. Data is distributed across the drives in one of several ways called "RAID levels", depending on what level of redundancy and performance is required.

8.1 Create Disk Array

Purpose:

The device supports the disk array that is realized by software. You can enable the RAID function as required. Two ways are available for creating array: one-touch configuration and manual configuration. The following flow chart shows the process of creating array.

8.1.1 Enable RAID

Purpose:

Perform the following steps to enable the disk array function.

Step 1 Go to Storage > Advanced.

Overwrite	
eSATA	eSATA1 ~
Usage	Record/Capture ~
Enable HDD Sleeping	
Enable RAID	
Use the enterprise-class ⊢	DD.
Apply	

Figure 8-1 Advanced

Step 2 Check Enable RAID.

Step 3 Click Apply.

Step 4 Reboot device to take effect the settings.

8.1.2 One-Touch Creation

Purpose:

One-touch configuration helps you to quickly create the disk array. By default, the array type created by one-touch configuration is RAID 5.

Before you start:

- Enable RAID function. For details, refer to Chapter 8.1.1 Enable RAID.
- Install at least 3 HDDs. If more than 10 HDDs are installed, 2 arrays will be created. To maintain reliable and stable running of the HDDs, it is recommended to use enterprise-level HDDs with the same model and capacity.

Step 1 Go to Storage > RAID Setup > Physical Disk.

One-touch Config	⊖ Create					
■No.	Capacity Array	Туре	Status	Model	Hot Spare	Task
1	1863.02GB	Normal	Functional	ST2000VX000-1CU164		None
2	2794.52GB	Normal	Functional	ST3000VX000-9YW166		None
5	1863.02GB	Normal	Functional	ST2000VX000-1CU164	B	None
9	2794.52GB	Normal	Functional	ST3000VX000-1CU166		None
10	1863.02GB	Normal	Functional	ST2000VX000-1CU164	E.	None

Figure 8-2 Physical Disk

Step 2 Click One-touch Config.

Step 3 Edit the array name in Array Name text filed and click OK to start configuring.

If you install 4 HDDs or more, a hot spare disk for array rebuilding will be created.

Step 4 A message box will pop up when the array creation is completed, click **OK** on it.

Step 5 Optionally, the device will automatically initialize the created array. Go to **Storage > RAID Setup > Array** view the information of created array.

8.1.3 Manual Creation

Purpose:

Manually create the array of RAID 0, RAID 1, RAID 5, RAID 6, and RAID 10.

Step 1 Go to Storage > RAID Setup > Physical Disk.

Step 2 Click Create.

Create Array				
Array Name				
RAID Level	RAID 5			-
Initialization Type	Initialize (Fas	it)		•
Physical Disk	1 2	5	9 🗌 10	
America Compositor (Estim	-t			
Array Capacity (Estin	ialeu). UGB			
		ОК	Ca	ncel

Table 8-1 Create Array

Step 3 Enter the array name.

Step 4 Select RAID Level as RAID 0, RAID 1, RAID 5, RAID 6, or RAID 10 as required.

Step 5 Select the physical disks to constitute array.

Table 8-2 Required Number of HDD

RAID Level	Required Number of HDD
RAID 0	At least 2 HDDs.
RAID 1	At least 2 HDDs.
RAID 5	At least 3 HDDs.
RAID 6	At least 4 HDDs.
RAID 10	The number of HDD must be an even ranges from 4 to 16.

Step 6 Click OK.

Step 7 Optionally, the device will automatically initialize the created array. Go to **Storage > RAID Setup > Array** view the information of created array.

No	Name	Free Space	Physical Disk	Hot S Status	Level	Rebuild	Delete	Task
1	Array01	3725/3725G	1 5 10	Functional	RAID 5	Ľ	×	Initialize (Fast)(Running) 43%

Figure 8-3 Array List

8.2 Rebuild Array

Purpose:

The status of array includes Functional, Degraded and Offline. To ensure the high security and reliability of the data stored in array, you should take immediate and proper maintenance at arrays according their status.

- Functional: No disk loss in the array.
- Offline: The number of lost disks has exceeded the limit.
- Degraded: If amount of HDD fail in array, array degrades. You should recover it to Functional by array rebuilding.

8.2.1 Configure Hot Spare Disk

Purpose:

Hot spare disks are required for disk array automatic rebuilding.

Step 1 Go to Storage > RAID Setup > Physical Disk.

No.	Capacity	Array	Туре	Status	Model	Hot Spare	Task
1	1863.02GB	Array01	Array	Functional	ST2000VX000-1CU164		None
2	2794.52GB		Normal	Functional	ST3000VX000-9YW166	Ľ	None
5	1863.02GB	Array01	Array	Functional	ST2000VX000-1CU164	-	None
□9	2794.52GB		Normal	Functional	ST3000VX000-1CU166	Ľ	None
10	1863.02GB	Array01	Array	Functional	ST2000VX000-1CU164	-	None

Figure 8-4 Physical Disk

Step 2 Click of an available HDD to set it as the hot spare disk.

8.2.2 Automatically Rebuild Array

Purpose:

The device can automatically rebuild degraded arrays with the hot spare disks.

Before you start:

Г

Create hot spare disks. For details, refer to Chapter 8.2.1 Configure Hot Spare Disk.

Step 1 The device will automatically rebuild the degraded arrays with the hot spare disks. Go to **Storage > RAID Setup > Array** to view rebuilding progress.

No.	Name	Free Space	Physical Disk	Hot Spare	Status	Level	Rebuild	Delete	Task
1	Array01	3725/3725G	2 5 10		Degraded	RAID 5		×	Rebuild(Running) 0%

Figure 8-5 Array List

8.2.3 Manually Rebuild Array

Purpose:

If no hot spare disks are configured, rebuild the degraded array manually.

Before you start:

At least one available physical disk should exist for rebuilding the array.

Step 1 Go to Storage > RAID Setup > Array.

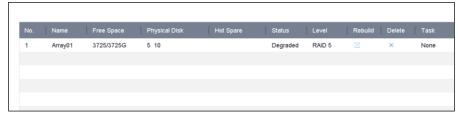


Figure 8-6 Array List

Step 2 Click degraded array.

Rebuild Array	
Array Name	Array01
RAID Level	RAID 5
Array Disk	5 10
Physical Disk	2 9
	OK Cancel

Figure 8-7 Rebuild Array

Step 3 Select the available physical disk.

Step 4 Click OK.

Step 5 Click **OK** on the pop up message box "Do not unplug the physical disk when it is under rebuilding".

8.3 Delete Array

Deleting array will delete all the data saved in it.

Step 1 Go to Storage > RAID Setup > Array.

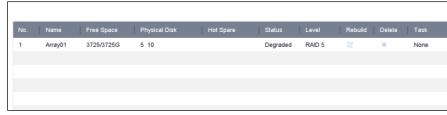


Figure 8-8 Array List

Step 2 Click \times of array to delete.



Figure 8-9 Attention

Step 3 Click **Yes** on the popup message box.

8.4 Check and Edit Firmware

Purpose:

You can view the information of the firmware and set the background task speed on the Firmware interface.

Step 1 Go to Storage > RAID Setup > Firmware.

Version	1.1.0.0003
Physical Disk Count	16
Array Count	16
Virtual Disk Count	0
RAID Level	0 1 5 6 10
Hot Spare Type	Global Hot Spare
Support Rebuild	Yes
Background Task Speed	Medium Speed -

Figure 8-10 Firmware

Step 2 Optionally, set the **Background Task Speed**.

Step 3 Click Apply.

Chapter 9 File Management

9.1 Search and Export All Files

9.1.1 Search Files

Purpose

Specify detailed conditions to search videos and pictures.

Step 1 Go to File Management > All Files.

Step 2 Specify detailed conditions, including time, camera, event type, etc.

Time	Custom	•	2018-04-24 00:	00:00 🛗	2018-04-24	23:59:59 🛗
Camera	[All] Camera		•			
Tag			File Status	All		•
Event Type	None	-				
Plate No.						
Area/Country	None	•				
			Empty Conditions	S	earch	Save

Figure 9-1 Search All Files

Step 3 Click Search to display results. The matched files will be displayed.

9.1.2 Export Files

Purpose

Export files for backup purposes using USB device (USB flash drive, USB HDD, USB optical disc drive), SATA optical disc drive or eSATA HDD.

Step 1 Search files to export. For details, see 9.1.1 Search Files.

Step 2 Click to select files and click Export.

Step 3 Select the file to export as Video and Log and click OK.

Step 4 Click **OK** to export files to backup device.

9.2 Search and Export Human Files

9.2.1 Search Human Files

Purpose

Specify detailed conditions to search human pictures and videos.

Before you start

Configure human body detection function for the cameras you want to search and export human pictures and videos.

Step 1 Go to File Management > Human Files.

Step 2 Select Time and Camera to search.

Time	Custom	2017-10-24 00:00:00	2017-10-24 23:59:59		
Camera	[All] Camera		-		
			Empty Conditions	Search	Save

Figure 9-2 Search Human Files

Step 3 Click Search to display results. The matched files are displayed in thumbnail or list.

Step 4 Select Target Picture or Source Picture in menu bar to display related pictures only.

- **Target Picture**: Display the search results of people close-up.
- **Source Picture**: Display the search results of original picture captured by camera.

9.2.2 Export Human Files

Purpose

Export files for backup purposes using USB device (USB flash drive, USB HDD, USB optical disc drive), SATA optical disc drive or eSATA HDD.

Step 1 Search for the human files to export. For details, see 9.2.1 Search Human Files.

Step 2 Click to select files and click Export.

Step 3 Select the file to export as Video and Log and click OK.

Step 4 Click **OK** to export files to backup device.

9.3 Search and Export Vehicle Files

9.3.1 Search Vehicle Files

Purpose

Specify detailed conditions to search vehicle pictures and videos.

Before you start

Configure vehicle detection function for the cameras you want to search and export vehicle pictures and videos.

Step 1 Go to File Management > Vehicle Files.

Step 2 Specify detailed conditions, including **Time, Camera**, **Plate No.**, and **Area/Country**.

Time	Custom -	2017-10-24 00:00:00	2017-10-24 23:59:59		
Camera	[All] Camera		•		
Plate No.					
Area/Country	None ~				
			Empty Conditions	Search	Save

Figure 9-3 Search Vehicle Files

Step 3 Click Search to display results. The matched files are displayed in thumbnail or list.

Step 4 Select **Target Picture** or **Source Picture** in menu bar to display related pictures only. Select **Video** or **Picture** to specify the file type.

- **Target Picture**: Display the search results of vehicle close-up.
- **Source Picture**: Display the search results of original picture captured by camera.

9.3.2 Export Vehicle Files

Purpose

Export files for backup purposes using USB device (USB flash drive, USB HDD, USB optical disc drive), SATA optical disc drive or eSATA HDD.

Step 1 Search for the vehicle files to export. For details, see 9.3.1 Search Vehicle Files.

Step 2 Click to select files and click **Export**.

Step 3 Select the file to export as Video and Log and click OK.

Step 4 Click **OK** to export files to backup device.

9.4 Search History Operation

9.4.1 Save Search Condition

Purpose

You can save the search conditions for future reference and quick search.

Step 1 Go to File Management > All Files/People Appearance File/Vehicle File.

Step 2 Set the search conditions.

Step 3 Click Save.

Step 4 Enter a name in text field and click **Finished**. The saved search conditions will be displayed in **Search Condition**.

9.4.2 Call Search History

Purpose:

You can quickly search files by calling search history.

Step 1 Go to File Management > All Files/Human Files/Vehicle Files.

Step 2 Click a search condition in Search Condition to quickly search files.

Chapter 10 Playback

10.1 Play Video Files

10.1.1 Instant Playback

Purpose:

Instant Playback enables the device to play the recorded video files in last five minutes. If no video is found, it means there is no recording during the last five minutes.

Step 1 On the live view window of the selected camera, move the cursor to the window bottom to access the toolbar.

Step 2 Click

to start instant playback.



Figure 10-1 Playback Interface

10.1.2 Play Normal Video

Purpose:

In the normal playback mode, you can achieve the advanced playback operations which will satisfy more complicated requirements.

Step 1 Go to Playback.

Step 2 Select one or more cameras in the **Channel** list to start playing the video.

Step 3 Select a date in the calendar.

• Use the toolbar in the bottom part of playback interface to control the playing and realize a series of operations. Refer to Chapter 10.2 Playback Operations.



Figure 10-2 Playback Interface

Normal	Smart	Custom	Tag 🛑	2017-10-22 00:00:00		1 Day	•••••••
12:00	14:00	16:00	18:00 20:00	22:00 10423	02:00 04:00 06:00	08:00	10:00 12:00
	*					■Normal ■Event	

Figure 10-3 Toolbar of Playback

• Click the channel(s) to execute simultaneous playback of multiple channels.

- The playing speed of 256X is supported.
- HGHI-K series do not support play reverse of smart stream.

10.1.3 Play Smart Searched Video

Purpose:

In the smart playback mode, the device can analyze the video containing the motion, line or intrusion detection information, mark it in red color and play the smart searched video.

The smart playback must be in the single-channel playing mode.

Step 1 Go to Playback.

Step 2 Start playing the video of camera.

Step 3 Click Smart.

Step 4 From the toolbar at the bottom of the playing window, click the motion/line crossing/ intrusion icon for search.



Figure 10-4 Playback by Smart Search

Step 5 Set the rules and areas for smart search of line crossing detection, intrusion detection or motion detection event triggered recording.

• Line Crossing Detection

- 5) Click the 🔛 icon.
- 6) Click on the image to specify the start point and end point of the line.

Intrusion Detection

- 7) Click the icon.
- 8) Specify 4 points to set a quadrilateral region for intrusion detection. Only one region can be set.

Motion Detection

- 9) Click the icon.
- 10) Hold the mouse on the image to draw the detection area manually.
- 11) Click Search \bigcirc to search the matched video and start to play it.

10.1.4 Play Custom Searched Files

Purpose:

You can play the files by custom search with different conditions.

Step 1 Go to Playback.

Step 2 Select a camera or cameras from the list.

Step 3 Click **Custom Search** on the left bottom to enter the **Search Condition** interface.

Step 4 Enter the search conditions for the files, e.g., time, file status, event type, etc.

Time	Custom	*	2017-10-01 00:00:0	0	2017-10-23 23:59:59	
Тад	A		File Status	All	-	
Event Type	None	•				
Plate No.						
Area/Country	None	•				

Empty Conditions Search Save	Search	Save

Figure 10-5 Custom Search

Step 5 Click Search.

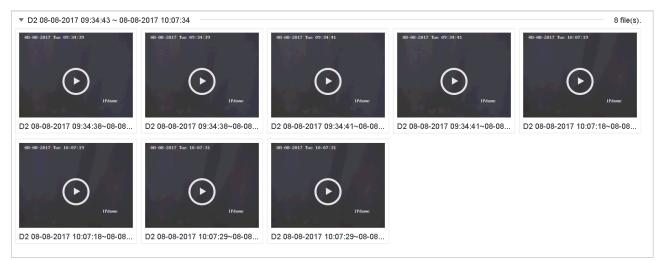


Figure 10-6 Custom Searched Video Files

Step 6 On the search results interface, select a file and click to start playing the video.

10.1.5 Play Tag Files

Purpose:

Video tag allows you to record related information like people and location of a certain time point during playback. You can use video tag(s) to search for video files and position time point.

Before playing back by tag:

Add Tag Files

Step 1 Go to Playback.

Step 2 Search and play back the video file(s).

Step 3 Click 🖾 to add the tag.

Step 4 Edit the tag information.

Step 5 Click OK.

Max. 64 tags can be added to a single video file.

Edit Tag Files

Step 1 Go to Playback.

Step 2 Click Tag.

The available tags are white marked and displayed in the time bar.

Step 3 Point the white marked tag in the time bar to access the tag information.

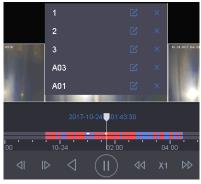


Figure 10-7 Edit Tag Files

Step 4 Click for edit the tag name.

Step 5 Click **OK**.

Play Tag Files

Step 1 Go to Playback.

Step 2 Click **Custom Search** on the left bottom to enter the Search Condition interface.

Step 3 Enter the search conditions for the tag files, including the time and the tag keyword.

Network Video Recorder User Manual

Fime	Custom	*	2017-10-01 00:00:	00	2017-10-23 23:59:59		
Гад	A		File Status	All	~		
Event Type	None	•					
Plate No.							
Area/Country	None	-					
					Empty Conditions	Search	Save

Figure 10-8 Tag Search

Step 4 Click Search.

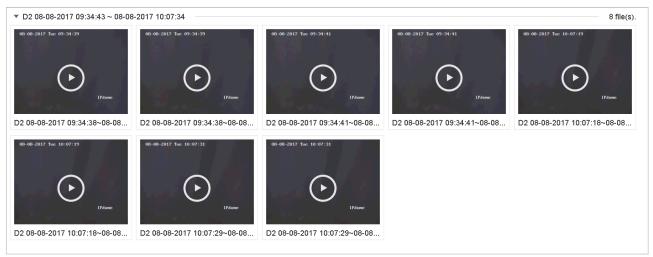


Figure 10-9 Searched Tag Files

Step 5 On the search results interface, select a tag file and click to start playing the video.

10.1.6 Play Event Files

Purpose

Play back video files on one or several channels searched by event type (e.g., alarm input, motion detection, line crossing detection, face detection, vehicle detection, etc.).

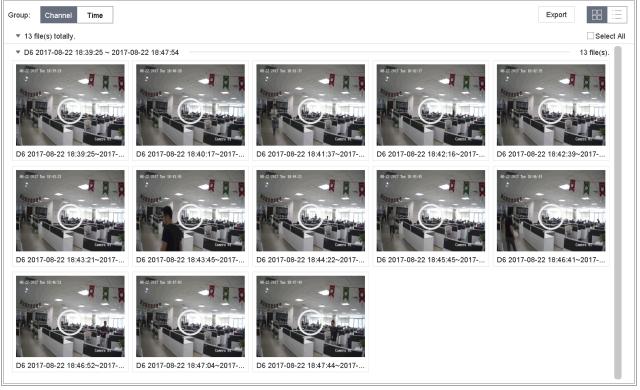
Step 1 Go to Playback.

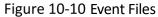
Step 2 Click **Custom Search** on the left bottom to enter the Search Condition interface.

Step 3 Enter the search conditions for the event files, e.g., time, event type, file status, vehicle information (for vehicle detection event), etc.

Step 4 Click Search.

Step 5 On the search results interface, select an event video file/picture file and double click to start playing the video.





Step 6 You can click

button to play 30s backward or forward.

- Refer to Chapter 11 and Chapter 13 VCA Event Alarmfor details for event and alarm settings.
- Refer to Chapter 7.7 Configure Event Triggered Recording for the event triggered recording/capture settings.

10.1.7 Play by Sub-periods

 \triangleleft

or

Purpose:

The video files can be played in multiple sub-periods simultaneously on the screens.

Step 1 Go to Playback.

Step 2 Select

eal icon at the left bottom corner to enter the sub-period playing mode.

Step 3 Select a camera.

Step 4 Set the start time and end time for searching video.

Step 5 Select the different multi-period at the right bottom corner, e.g., 4-Period.

According to the defined number of split-screens, the video files on the selected date can be divided into average segments for playback. E.g., if there are video files existing between 16:00 and 22:00, and the 6-screen display mode is selected, then it can play the video files for 1 hour on each screen simultaneously.

10.1.8 Play Log Files

Purpose:

Play back record file(s) associated with channels after searching system logs.

Step 1 Go to Maintenance>Log Information.

Step 2 Click Log Search tab to enter Playback by System Logs.

Step 3 Set search time and type and click Search.

No.	Major Type	Time	Minor Type	Parameter	Play	Details
5	Alarm	2017-10-25 00:04:30	Motion Detection Started	N/A		0
6	Alarm	2017-10-25 00:04:42	Motion Detection Stopped	N/A		0
7	Alarm	2017-10-25 00:06:04	Motion Detection Started	N/A		0
8	T Operation	2017-10-25 00:06:18	Local Operation: Playback By Time	N/A		0
9	Alarm	2017-10-25 00:06:19	Motion Detection Stopped	N/A		0
10	Alarm	2017-10-25 00:06:41	Motion Detection Started	N/A	•	0
11	Information	2017-10-25 00:06:46	System Running Status	N/A	-	0
12	Information	2017-10-25 00:06:46	System Running Status	N/A	-	0
13	Alarm	2017-10-25 00:07:02	Motion Detection Stopped	N/A	•	0
14	Alarm	2017-10-25 00:07:59	Motion Detection Started	N/A	•	0
15	Alarm	2017-10-25 00:08:15	Motion Detection Stopped	N/A	•	0
16	Alarm	2017-10-25 00:08:27	Motion Detection Started	N/A	•	0
17	T Operation	2017-10-25 00:08:43	Local Operation: Playback By Time	N/A	-	0
18	Coperation	2017-10-25 00:08:46	Local Operation: Playback By Time	N/A		0
19	Alarm	2017-10-25 00:08:57	Motion Detection Stopped	N/A	•	0
20	T Operation	2017-10-25 00:09:13	Local Operation: Playback By Time	N/A		0
21	Alarm	2017-10-25 00:09:22	Motion Detection Started	N/A	•	0
22	Alarm	2017-10-25 00:09:35	Motion Detection Stopped	N/A	•	0

Figure 10-11 System Log Search Interface

Step 4 Choose a log with video file and click

to start playing the log file.

10.1.9 Play External File

Purpose:

You can play files from the external storage devices.

Before You Start:

Connect the storage device with the video files to your device.

Step 1 Go to Playback.

Step 2 Click the icon at the left bottom corner.

Step 3 Select and click the 🖻 button or double click to play the file.

10.2 Playback Operations

10.2.1 Set Play Strategy in Smart/Custom Mode

Purpose:

When you are in the smart or custom video playback mode, you can set the playing speed separately for the normal video and the smart/custom video, or you can select to skip the normal video.

In the Smart/Custom video playback mode, click

to set the play strategy.

• When **Do not Play Normal Videos** is checked, the device will skip the normal video and play the smart (motion/line crossing/intrusion) video and the custom (searched video) only in the normal speed (X1).

• When **Do not Play Normal Videos** is unchecked, you can set the play speed for the normal video the smart/custom video separately. The speed range is from X1 to XMAX.

You can set the speed in the single-channel play mode only.

Play Strategy		
Do not Play Normal Videos	\checkmark	
Normal Video		. X8
Play Speed of Smart/Custom	· · · · · ·	• X1
	ОК	Cancel

Figure 10-12 Play Strategy

10.2.2 Edit Video Clips

You can take video clips during the playback and export the clips.

In the video playback mode, click it is start video clipping operation.

Set the start time and end time of the video clipping.



10.2.3 Switch between Main Stream and Sub-Stream

You can switch between the main stream and the sub-stream during the playback.



🔘: Play the video in main stream.

- 🗐 : Play the video in sub-stream.

10.2.4 Thumbnails View

With the thumbnails view on the playback interface, you can conveniently locate the required video files on the time bar.

In the video playback mode, move the mouse to the time bar to get the preview thumbnails of the video files.



Figure 10-13 Thumbnails View

You can select and click on a required thumbnail to enter the full-screen playback.

10.2.5 Fast View

You can hold the mouse to drag on the time bar to get the fast view of the video files.

In the video playback mode, use the mouse to hold and drag through the playing time bar to fast view the video files.

Release the mouse to the required time point to enter the full-screen playback.

10.2.6 Digital Zoom

In the video playback mode, click

from the toolbar to enter the digital zoom interface.

You can move the sliding bar or scroll the mouse wheel to zoom in/out the image to different proportions (1 to16X).



Figure 10-14 Digital Zoom

Chapter 11 Event and Alarm Settings

11.1 Configure Arming Schedule

Step 1 Select the Arming Schedule tab.

Step 2 Choose one day of a week and set the time segment. Up to eight time periods can be set within each day.

Time periods shall not be repeated or overlapped.

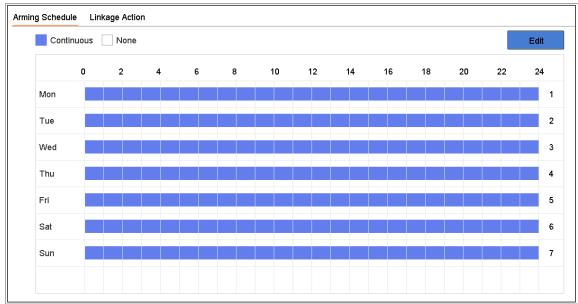


Figure 11-1 Set Arming Schedule

Step 3 Click **Apply** to save the settings.

11.2 Configure Alarm Linkage Actions

Purpose:

Alarm linkage actions will be activated when an alarm or exception occurs, including Event Hint Display, Full Screen Monitoring, Audible Warning (buzzer), Notify Surveillance Center, Trigger Alarm Output and Send Email.

11.2.1 Configure Auto-switch Full Screen Monitoring

Purpose:

When an alarm is triggered, the local monitor displays in full screen the video image from the alarming channel configured for full screen monitoring. And when the alarm is triggered simultaneously in several channels, you must configure the auto-switch dwell time.

Step 1 Go to System > View > General.

Step 2 Set the event output and dwell time.

- Event Output: Select the output to show event video.
- Full Screen Monitoring Dwell Time: Set the time in seconds to show alarm event screen. If alarms are triggered simultaneously in several channels, their full-screen images will be switched at an interval of 10 seconds (default dwell time).

Step 3 Go to the **Linkage Action** interface of the alarm detection (e.g., motion detection, video tampering, face detection, etc.).

Step 4 Select the Full Screen Monitoring alarm linkage action.

Step 5 Select the channel(s) in **Trigger Channel** settings you want to make full screen monitoring.

Auto-switch will terminate once the alarm stops and back to the live view interface.

11.2.2 Configure Audio Warning

Purpose:

The audio warning enables the system to trigger an audible *beep* when an alarm is detected.

Step 1 Go to System>View>General.

Step 2 Enable the audio output and set the volume.

Step 3 Go to the **Linkage Action** interface of the alarm detection (e.g., motion detection, video tampering, face detection, etc.).

Step 4 Select the Audio Warning alarm linkage action.

11.2.3 Notify Surveillance Center

Purpose:

The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., CMS).

Step 1 Go to System > Network > Advanced > More Settings.

Step 2 Set the alarm host IP and alarm host port.

Step 3 Go to the **Linkage Action** interface of the alarm detection (e.g., motion detection, video tampering, face detection, etc.).

Step 4 Select the Notify Surveillance Center.

11.2.4 Configure Email Linkage

Purpose:

The system can send an email with alarm information to a user or users when an alarm is detected.

Please refer to Chapter 16.7 Configure Email for details of Email configuration.

Step 1 Go to System>Network>Advanced.

Step 2 Configure the Email settings.

Step 3 Go to the **Linkage Action** interface of the alarm detection (e.g., motion detection, video tampering, face detection, etc.).

Step 4 Select the Send Email alarm linkage action.

11.2.5 Trigger Alarm Output

Purpose:

The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and all other events.

Step 1 Go to the **Linkage Action** interface of the alarm input or event detection (e.g., motion detection, face detection, line crossing detection, intrusion detection, etc.).

Step 2 Click the Trigger Alarm Output tab.

Step 3 Select the alarm output (s) to trigger.

Step 1 Go to System> Event>Normal Event>Alarm Output.

Step 2 Select an alarm output item from the list.

Refer to Chapter 11.6.3 Configure Alarm Output for the alarm output settings.

11.2.6 Configure PTZ Linkage

Purpose:

The system can trigger the PTZ actions (e.g., call preset/patrol/pattern) when the alarm event, or VCA detection events occur.

Make sure the PTZ or speed dome connected supports PTZ linkage.

Step 1 Go to the **Linkage Action** interface of the alarm input or VCA detection (e.g., face detection, line crossing detection, intrusion detection, etc.).

Step 2 Select the PTZ Linkage.

Step 3 Select the camera to perform the PTZ actions.

Step 4 Select the preset/patrol/pattern No. to call when the alarm events occur.

PTZ Linkage		
PTZ Linkage	[D1] IPCamera 01	•
• Preset No.	5	•
OPatrol No.	1	*
OPattern No.	1	-

Figure 11-2 PTZ Linkage

You can set one PTZ type only for the linkage action each time.

11.3 Configure Motion Detection Alarm

Purpose:

The motion detection enables the device to detect the moving objects in the monitoring area and trigger the alarm.

Step 1 Go to System > Event > Normal Event > Motion Detection.

Camera [[D2] IPdome -	
En:	Enable	
Area Arming So	g Schedule Linkage Action	
	Sensitivity 0	100 60
Full Screen	n Clear	
Aţ	Apply	

Figure 11-3 Set Motion Detection

Step 2 Select the camera to configure the motion detection.

Step 3 Check Enable.

Step 4 Set the motion detection area.

• Full screen: click to set the full-screen motion detection for the image.

• Customized area: use the mouse to click and drag on the preview screen to draw the customized motion detection area (s).

You can click **Clear** to clear the current motion detection area settings and draw again.

Step 5 Set sensitivity (0-100). The sensitivity allows you to calibrate how readily movement triggers the alarm. The higher value results in the more readily to trigger the motion detection.

Step 6 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 7 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

11.4 Configure Video Loss Alarm

Purpose:

The video loss detection enables to detect video loss of a channel and take alarm response action(s).

Step 1 Go to System > Event > Normal Event > Video Loss

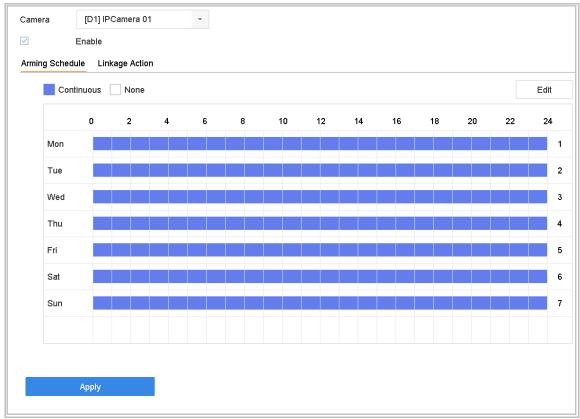


Figure 11-4 Set Video Loss Detection

Step 2 Select the camera to configure the video loss detection.

Step 3 Check Enable.

Step 4 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 5 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

11.5 Configure Video Tampering Alarm

Purpose:

The video tampering detection enables to trigger alarm when the camera lens is covered and take alarm response action(s).

Step 1 Go to System> Event>Normal Event>Video Tampering.

Step 2 Select the camera to configure the video tampering detection.

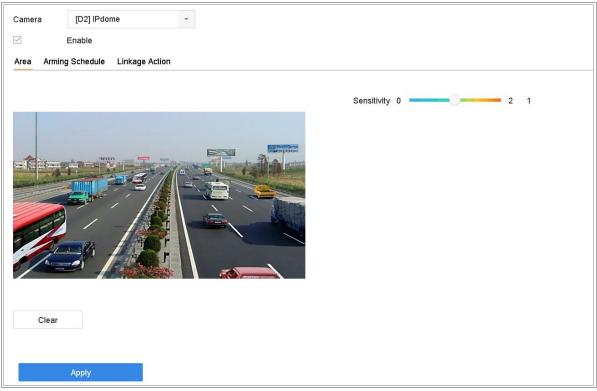


Figure 11-5 Set Video Tampering Setting

Step 3 Check Enable.

Step 4 Set the video tampering area. Use the mouse to click and drag on the preview screen to draw the customized video tampering area.

You can click **Clear** to clear the current area settings and draw again.

Step 5 Set sensitivity level (0-2). 3 levels are available. The sensitivity allows you to calibrate how readily movement triggers the alarm. The higher value results in the more readily to trigger the video tampering detection.

Step 6 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 7 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

11.6 Configure Sensor Alarms

Purpose:

Set the handling action of an external sensor alarm.

11.6.1 Configure Alarm Input

Step 1 Go to System> Event>Normal Event>Alarm Input

Step 2 Select an alarm input item from the list and click

Edit	:									\times	
Alaı	rm Inpu	Local<-1	•	Туре		N.O		•			
Alai	rm Name										
Set	tings	🔿 Nonuse	🔿 Input) (Dne-Ke	y Dis				
	Normal	Linkage									
	□Full Sci	reen Monito	□Audible Warning		□Not	ify Sur	veilland	;e			
	Trigger	Alarm Out	□Send Email								
									Copy to	Apply	

Figure 11-6 Alarm Input

Step 3 Select the alarm input type to **N.C** or **N.O**.

Step 4 Edit Alarm Name.

Step 5 Select Input.

Step 6 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 7 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

Step 8 Click Apply and follow the message box to reboot device to take effect the settings.

11.6.2 Configure One-Key Disarming

Purpose:

The one-key disarming enables the device to disarm the alarm input 1 by one-key operation.

Step 1 Go to System> Event>Normal Event>Alarm Input

Step 2 Select the alarm input1 item from the list and click

Step 3 Select the alarm input type to N.C or N.O.

Step 4 Edit the alarm name.

Step 5 Check the radio button of Enable One-Key Disarming.

Edit			×
Alarm Input No. Local<-1 Alarm Name A	• Туре	N.O -	
Settings ONonuse OInput	• One-Key Dis		
Normal Linkage			
Full Screen Monitori	Audible Warning	☑ Notify Surveillance	
Trigger Alarm Output	Send Email		
		Copy to	Apply

Figure 11-7 One-Key Alarm Disarming

Step 6 Select the alarm linkage action (s) you want to disarm for the local alarm input1.

When the alarm input 1 (Local<-1) is enabled with one-key disarming, the other alarm input settings are not configurable.

Step 7 Click Apply to save the settings.

11.6.3 Configure Alarm Output

Purpose:

Trigger an alarm output when an alarm is triggered.

Step 1 Go to System> Event>Normal Event>Alarm Output.

Step 2 Select an alarm output item from the list and click \square

Step 3 Edit Alarm Name.

Step 4 Select Dwell Time (the alarm duration) from 5s to 600s, or Manually Clear.

Manually Clear: You should manually clear the alarm when the alarm occurs. Refer to Chapter 11.8 Trigger or Clear Alarm Output Manually for detailed instructions.

Step 5 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

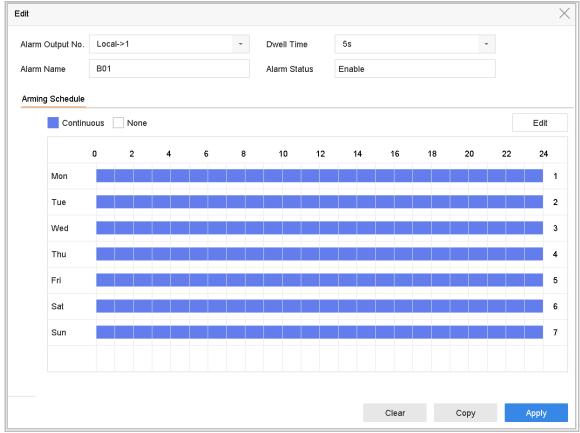


Figure 11-8 Alarm Output

Step 6 (Optional) You can click **Copy** to copy the same settings to other alarm output (s). Step 7 Click **Apply**.

11.7 Configure Exceptions Alarm

Purpose:

The exception events can be configured to take the event hint in the live view window, trigger alarm output and linkage actions.

Step 1 Go to System > Event > Normal Event > Exception.

Step 2 (Optional) Enable the event hint if you want to display the event hint in the live view window.

1) Check Enable Event Hint.

2) Click 0 to select the exception type (s) to take the event hint.

Event Hint Settings		
All		
HDD Full		
Network Disconnected		
⊡IP Conflicted		
⊡lllegal Login		
⊡Video Signal Loss		
⊡Alarm Input Triggered		
⊡Video Tamper Detected		
—		
	ОК	Cancel

Figure 11-9 Event Hint Settings

Step 3 Select the exception type from the drop-down list to set the linkage actions.

Enable Event Hint 🗹	
Event Hint Config ^ද ್ರಿ	
Exception Type HDD Full	-
Normal Linkage	Trigger Alarm Output
Audible Warning	⊡Local->1
	✓Local->2
☑ Notify Surveillance Center	Local->3
✓ Send Email	Local->4
	10.15.2.250:8000->1
Apply	

Figure 11-10 Exceptions Handling

Step 4 Set the normal linkage and alarm output triggering. Refer to 11.2 Configure Alarm Linkage Actions.

11.8 Trigger or Clear Alarm Output Manually

Purpose:

Sensor alarm can be triggered or cleared manually. When **Manually Clear** is selected for the dwell time of an alarm output, the alarm can be cleared only by clicking **Clear**.

Step 1 Go to System> Event>Normal Event>Alarm Output.

Step 2 Select the alarm output you want to trigger or clear and click

Step 3 Click **Trigger/Clear** to trigger or clear an alarm output.

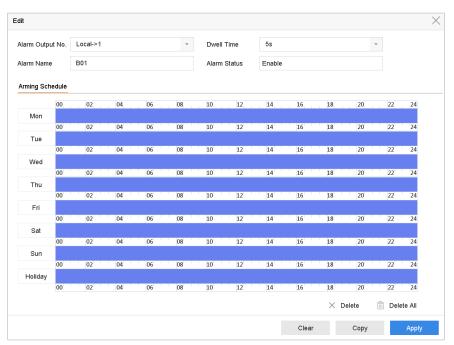


Figure 11-11 Alarm Output

Chapter 12 POS Configuration

The device can be connected with the POS machine/server, and receive the transaction message for overlay on the image during the live view or playback, as well as trigger the POS event alarm.

This chapter is only applicable to Pro and Ultra series DVR.

12.1 Configure POS Settings

12.1.1 Configure POS Connection

Step 1 Go to System > POS Settings.

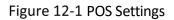
Step 2 Click **Add** to enter the POS adding interface.

Step 3 Select a POS from the drop-down list.

Step 4 Check Enable.

The amount of POS devices supported for each device is the half of its channel amount.

Add POS					
Enable			POS Name	POS 3	•
POS Protocol	AVE	- Custom	Connection Mode	Sniff	- Parameters



Step 5 Select the POS protocol to Universal Protocol, EPSON, AVE or NUCLEUS.

When the new protocol is selected, you should reboot the device to activate the new settings.

Universal Protocol

Click the **Advanced** button to expand more settings when selecting the universal protocol. You can set the start line identifier, line break tag and end line tag for the POS overlay characters, and the case-sensitive property of the characters. You can also optionally check the filtering identifier and the XML protocol.

Start Line Identifier		Hex		\checkmark
Line Break	0D0A	Hex		 ✓
End Line Identifier		Hex		~
Case Sensitive	\checkmark			
Filtering Identifier	\checkmark			
Enable XML Prot	\checkmark			
	ОК	c	ancel	

Figure 12-2 Universal Protocol Settings

• EPSON

The fixed start and end line tag are used for EPSON protocol.

• AVE

The fixed start and end line tag are used for AVE protocol. And the serial port and virtual serial port connection types are supported.

- 1) Click the **Custom** to configure the AVE settings.
- 2) Se the rule to VSI-ADD or VNET.
- 3) Set the address bit of the POS message to send.
- 4) Click **OK** to save the settings.

Rule	VSI-ADD	•
Address	0	
	ОК	Cancel

Figure 12-3 AVE Settings

- NUCLEUS
 - 1) Click the **Custom** to configure the NUCLEUS settings.
 - 2) Enter the employee No. shift No. and the terminal No. in the field. The matching message sent from the POS device will be used as the valid POS data.

The NUCLEUS protocol must be used in the RS-232 connection communication.

Step 6 Select the connection mode to TCP Reception, UDP Reception, Multicast, RS-232, USB-to-RS-232 or Sniff, and click **Parameters** to configure the parameters for each connection mode.

- TCP Connection
 - 1) When using TCP connection, the port must be set from 1 to 65535, and the port for each POS machine must be unique.
 - 2) Set the Allowed Remote IP Address of the device sending the POS message.

TCP Connection Setti	ngs				
Port	10010				
Allowed Remote IP A	192 . 0	. 0	. 64		
				ОК	Cancel

Figure 12-4 TCP Connection Settings

- UDP Connection
 - 1) When using UDP connection, the port must be set from 1 to 65535, and the port for each POS machine must be unique.
 - 2) Set the **Allowed Remote IP Address** of the device sending the POS message.
- USB-to-RS-232 Connection

Configure the port parameters of USB-to-RS-232 convertor, including the serial number of port, baud rate, data bit, stop bit, parity and flow ctrl.

Network	Video	Recorder	User	Manual
I VCLWOIK	VIUCO	necoraci	Ober	wianuai

USB-to-RS-232 Settin	igs		
Serial Port Number	1		•
Baud Rate	4800		-
Data Bit	5		-
Stop Bit	1		•
Parity	None		•
Flow Ctrl	None		•
		ОК	Cancel

Figure 12-5 USB-to-RS-232 Settings

• RS-232 Connection

Connect the device and the POS machine via RS-232. The RS-232 settings can be configured in Menu>Configuration>RS-232. The Usage must be set to Transparent Channel.

Multicast Connection

When connecting the device and the POS machine via Multicast protocol, set the multicast address and port.

• Sniff Connection

Connect the device and the POS machine via Sniff. Configure the source address and destination address settings.

Sniff Settings							
Enable Source Port F							
Source Address	18 . 16 . 1 . 1						
Source Port	10020						
Enable Destination A.	. 🗹						
Enable Destination P.							
Destination Address	20 . 18 . 1 . 24						
Destination Port	10030						
	OK Cancel						

Figure 12-6 Sniff Settings

12.1.2 Configure POS Text Overlay

Step 1 Go to System > POS Settings.

Step 2 Click Channel Linkage and Display tab.

Step 3 Select the linked channel to overlay the POS characters.

Step 4 Set the characters overlay for the enabled POS.

- Character encoding format: currently the Latin-1 format is available.
- Overlay mode of the characters to display in scrolling or page mode.
- Font size and font color.
- Display time (sec) of the characters. The value ranges 5 -3600 sec.
- Timeout of POS event. The value ranges 5 -3600 sec. When the device has not received the POS message over the defined time, the transaction is finished.
- Step 5 In the **Privacy Settings**, set the POS privacy information to not display on the image, e.g., the card number, or the user name, etc.

Result: The defined privacy information will be displayed in ***on the image instead.

Step 6 (optional) Check the checkbox to enable the **Overlay POS in Live View**. When this feature is enabled, the POS information can be overlain on the live view image.

Linked Channel	[D1] IPCan	nera 01	-
Character Encod	Latin-1(iso	-8859-1)	
Overlay Mode	Page		-
Font Size	Large	Medium	Small
Font Color			
Display for	30		
Timeout	5		
Privacy Settings	1634	0921	543
	For example, the e	ntered card number w	ill be shown as **
Overlay POS in	~		

Figure 12-7 Overlay Character Settings

You can adjust the size and position of textbox on the preview screen of POS settings interface by dragging the frame.

Step 7 Click **Apply** to activate the settings.

12.2 Configure POS Alarm

Purpose:

The POS event can trigger channels to start recording, or trigger full screen monitoring, audio warning, notifying the surveillance center, sending email and so on.

Step 1 Go to Storage > Recording Schedule.

Step 2 Set the arming schedule of the POS event.

Step 3 Go to System > POS Settings.

- Step 4 On the POS adding or editing interface, click the Event Linkage tab.
- Step 5 Select the normal linkage actions: full screen monitoring, audio warning or send Email.
- Step 6 Select one or more alarm output (s) to trigger.
- Step 7 Select one or more channels to record or become full-screen monitoring when POS alarm is triggered.

Normal Linkage	Trigger Alarm Output	Trigger Channel	
✓ Full Screen Monitoring	⊡Local->1	⊡D1	
✓ Audible Warning	Local->2	✓D2	
✓ Send Email	⊡Local->3	D3	
	□Local->4	D4	
	10.15.2.250:8000->1		
otice: please confirm the eve	ent output in "Live View" settings me	nu is the same with the real	event output.

Network Video Recorder User Manual

Figure 12-8 Set Trigger Cameras of POS

Step 8 Click **Apply** to save the settings.

Chapter 13 VCA Event Alarm

The device supports receiving the VCA detections sent by connected IP cameras. Enable and configure the VCA detection on the IP camera settings interface first.

- VCA detections must be supported by the connected IP camera.
- Refer to the User Manual of Network Camera for the detailed instructions for the VCA detection.

13.1 Human Body Detection

Purpose:

The human body detection is used to detect the human body appearing in the monitoring scene, and capture the human body pictures.

This feature is available only when the connected camera supports the human body detection.

Step 1 Go to System > Event > Smart Event.

Step 2 Click Human Body.

Step 3 Select the camera to configure the human body detection.

- Step 4 Check Save VCA Picture to save the captured pictures of human body detection.
- Step 5 Check **Target of Interest (Human Body)** to discard non-human body pictures and videos which are not triggered by human body detection.

Step 6 Set detection area.

- 1) Select the detection area to configure from the **Area** drop-down list. Up to 8 detection areas are selectable.
- 2) Check the checkbox of Enable Area to enable the selected detection area.
- 3) Edit the area name in the Scene Name. The scene name can contain up to 32 characters.

Target of Interest (Human Body) rea Settings Arming Schedule Linkage Action		
	Area Capture Area 1 ~	
	Enable Area 🗹	
	Area Name Area01	
····		
Draw Area Clear		

Figure 13-1 Human Body Detection

4) Click **Draw Area** to draw a quadrilateral in the preview window and then click **Stop Drawing**.

Related Operation: You can click **Clear** to clear the existing virtual line and re-draw it.

Step 7 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 8 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

Step 9 Click **Apply** to activate the settings.

13.2 Face Detection

Purpose:

Face detection function detects the face appears in the surveillance scene. Linkage actions will be triggered when a human face is detected.

Step 1 Go to System > Event > Smart Event.

Step 2 Click Face Detection.

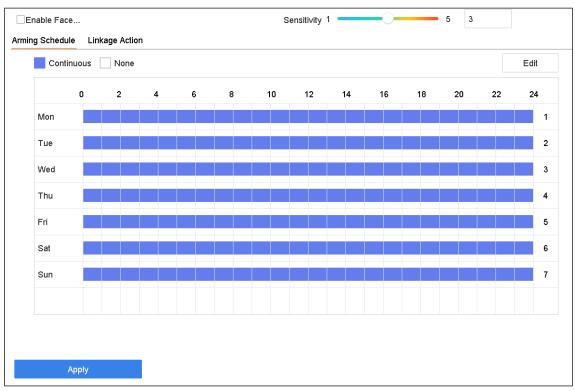


Figure 13-2 Face Detection

Step 3 Select a camera to configure.

Step 4 Check Enable Face Detection.

Step 5 Optionally, check **Save VCA Picture** to save the captured pictures of face detection.

Step 6 Drag the **Sensitivity** slider to set the detection sensitivity. Sensitivity range: [1-5]. The higher the value is, the more easily the face can be detected.

Step 7 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 8 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

Step 9 Click Apply.

13.3 Vehicle Detection

Purpose:

Vehicle Detection is available for the road traffic monitoring. In Vehicle Detection, the passed vehicle can be detected and the picture of its license plate can be captured. You can send alarm signal to notify the surveillance center and upload the captured picture to FTP server.

Step 1 Go to System > Event > Smart Event.

Step 2 Click Vehicle.

Enable Veh	icle Detection					
Area Settings	Arming Schedule	Linkage Action	Picture	Overlay Content	Blacklist and Whitelist	
					Lane Num	~
	Apply					

Figure 13-3 Vehicle Detection

Step 3 Select a camera to configure.

Step 4 Check Enable Vehicle Detection.

Step 5 Optionally, check **Save VCA Picture** to save the captured pictures of vehicle detection.

Step 6 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 7 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

Step 8 Configure rules, including **Area Settings**, **Picture**, **Overlay Content**, and **Blacklist and Whitelist**. Area Settings: Up to 4 lanes are selectable.

Step 9 Click Save.

Refer to the User Manual of Network Camera for the detailed instructions for the vehicle detection.

13.4 Line Crossing Detection

Purpose:

Line crossing detection detects people, vehicles, and objects crossing a set virtual line. The detection direction can be set as bidirectional, from left to right or from right to left.

Step 1 Go to System > Event > Smart Event.

Step 2 Click Line Crossing.

Enable Line	e Crossing Detec				
Area Settings	Arming Schedule	Linkage Action			
			Arming Area	1	•
		José A			
			Direction	A<->B	
1 day		the second second	Sensitivity	1	100 50
		6	-t-		
#1#		Anna I			
0		A			
\backslash		B			
		The second second			
Draw Area	Clear				
	Apply				

Figure 13-4 Line Crossing Detection

Step 3 Select a camera to configure.

Step 4 Check Enable Line Crossing Detection checkbox.

Step 5 Optionally, check **Save VCA Picture** to save the captured pictures of line crossing detection.

Step 6 Follow the steps to set the line crossing detection rules and detection areas.

- 1) Select an Arming Region to configure.
- 2) Select the Direction as A<->B, A->B, or A<-B.

A<->B: Only the arrow on the B side shows. When an object goes across the configured line with both directions can be detected and alarms are triggered.

A->B: Only the object crossing the configured line from the A side to the B side can be detected.

B->A: Only the object crossing the configured line from the B side to the A side can be detected.

- 3) Drag the Sensitivity slider to set the detection sensitivity. Sensitivity range: sensitivity. The higher the value is, the more easily the detection alarm can be triggered.
- 4) Click Draw Region and set two points in the preview window to draw a virtual line.

Step 7 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 8 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

Step 9 Click Apply.

i NOTE

For Acusense series, you can select **Target Detection** as **Human Body** or **Vehicle**. Only the target of selected type will trigger the alarm.

13.5 Intrusion Detection

Purpose:

Intrusion detection function detects people, vehicle or other objects which enter and loiter in a pre-defined virtual region, and some certain actions can be taken when the alarm is triggered.

Step 1 Go to System > Event > Smart Event.

Step 2 Click Intrusion.

Area Settings Arming Schedule Linkage Action		
	Virtual Plane 1 Time Thres0	- 10 0
MAN THE	Sensitivity 1	100 50
#1#	Percentage 1	100 1
Draw Area Clear		

Figure 13-5 Intrusion Detection

Step 3 Select a camera to configure.

Step 4 Check Enable Intrusion Detection.

Step 5 Optionally, check **Save VCA Picture** to save the captured pictures of intrusion detection.

Step 6 Follow the steps to set the detection rules and detection areas.

- 1) Select a Virtual Panel to configure.
- 2) Drag the sliders to set Time Threshold, Sensitivity, and Percentage.
 - Time Threshold: The threshold for the time of the object loitering in the region. When the duration of the object in the defined detection area is longer than the threshold, device will trigger an alarm. Its range is [0s-2s] for analog cameras.
 - Sensitivity: The size of the object that can trigger the alarm. The higher the value is, the more easily the detection alarm can be triggered. Its range is [1-100].
 - Percentage: The ratio of the in-region part of the object that can trigger the alarm. For example, if the percentage is 50%, when the object enters the region and occupies half of the whole region, device will trigger an alarm. Its range is [1-100].
- 3) Click Draw Region and draw a quadrilateral in the preview window by specifying four vertexes of the detection region.

Step 7 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 8 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

Step 9 Click Apply.

For Acusense series, you can select **Target Detection** as **Human Body** or **Vehicle**. Only the target of selected type will trigger the alarm.

13.6 Region Entrance Detection

Purpose:

Region entrance detection function detects objects that enter a pre-defined virtual region from the outside place.

Step 1 Go to System Management > Event Settings > Smart Event.

Step 2 Click the Region Entrance Detection item.

Enable Region Entrance De Area Settings Arming Schedule Linkage Action		
Stop Drawing Clear	Arming Area 1 Sensitivity 1	- 100 50
Apply		

Figure 13-6 Region Entrance Detection

Step 4 Check Enable Region Entrance Detection checkbox.

Step 5 Optionally, check **Save VCA Picture** checkbox to save the captured pictures of region entrance detection.

Step 6 Follow the steps to set the detection rules and detection areas.

- 1) Select an Arming Region to configure. Up to 4 regions are selectable.
- 2) Drag the sliders to set Sensitivity.

Sensitivity: The higher the value is, the more easily the detection alarm can be triggered. Its range is [0-100].

3) Click **Draw Region** and draw a quadrilateral in the preview window by specifying four vertexes of the detection region.

Step 7 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 8 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

Step 9 Click Apply.

13.7 Region Exiting Detection

Purpose:

Region exiting detection function detects objects that exit from a pre-defined virtual region.

Step 1 Go to System > Event > Smart Event.

Step 2 Click Region Exiting.

Enable Region Exiting Dete Area Settings Arming Schedule Linkage Action		
	Arming Area 1 Sensitivity 1	• 100 50
#1#		
Stop Drawing Clear		
Apply		

Figure 13-7 Region Exiting Detection

Step 3 Select a camera to configure.

Step 4 Check Enable Region Exiting Detection.

Step 5 Optionally, check **Save VCA Picture** to save the captured pictures of region exiting detection.

Step 6 Follow the steps to set the detection rules and detection areas.

- 1) Select an Arming Region to configure. Up to 4 regions are selectable.
- 2) Drag the sliders to set Sensitivity.

Sensitivity: The higher the value is, the more easily the detection alarm can be triggered. Its range is [0-100].

3) Click Draw Region and draw a quadrilateral in the preview window by specifying four vertexes of the detection region.

Step 7 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 8 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

Step 9 Click Apply.

13.8 Unattended Baggage Detection

Purpose:

Unattended baggage detection function detects the objects left over in the pre-defined region such as the baggage, purse, dangerous materials, etc., and a series of actions can be taken when the alarm is triggered.

Step 1 Go to System > Event > Smart Event.

Step 2 Click Unattended Baggage.

Enable Unattended Baggag		
Area Settings Arming Schedule Linkage Action		
	Arming Area 1	.
	Time Thres5	3600 5
	Sensitivity 1	100 50
#1#		
the second secon		
Stop Drawing Clear		
Apply		

Figure 13-8 Unattended Baggage Detection

Step 3 Select a camera to configure.

Step 4 Check Enable Unattended Baggage Detection.

Step 5 Optionally, check **Save VCA Picture** to save the captured pictures of unattended baggage detection.

Step 6 Follow the steps to set the detection rules and detection areas.

- 1) Select an Arming Region to configure. Up to 4 regions are selectable.
- 2) Drag the sliders to set Time Threshold and Sensitivity.

Time Threshold: The time of the objects left over in the region. If the value is 10, alarm is triggered after the object is left and stayed in the region for 10s. Its range is [5s-20s].

Sensitivity: Similarity degree of the background image. The higher the value is, the more easily the detection alarm can be triggered.

3) Click **Draw Region** and draw a quadrilateral in the preview window by specifying four vertexes of the detection region.

Step 7 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 8 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

Step 9 Click Apply.

13.9 Object Removal Detection

Purpose:

Object removal detection function detects the objects removed from the pre-defined region, such as the exhibits on display, and a series of actions can be taken when the alarm is triggered.

Step 1 Go to System > Event > Smart Event.

Step 2 Click Object Removable.

Enable Object Removal Det		
Area Settings Arming Schedule Linkage Action		
	Arming Area 1	•
All the second sec	Time Thres5	3600 5
	Sensitivity 1	100 50
#1#		
Draw Area Clear		
Apply		

Figure 13-9 Object Removal Detection

Step 3 Select a camera to configure.

Step 4 Check Enable Object Removable Detection.

Step 5 Optionally, check **Save VCA Picture** to save the captured pictures of object removable detection.

Step 6 Follow the steps to set the detection rules and detection areas.

1) Select an Arming Region to configure. Up to 4 regions are selectable.

2) Drag the sliders to set Time Threshold and Sensitivity.

Time Threshold: The time of the objects removed from the region. If the value is 10, alarm is triggered after the object disappeared from the region for 10s. Its range is [5s-20s].

Sensitivity: The similarity degree of the background image. Usually, when the sensitivity is high, a very small object taken from the region can trigger the alarm.

3) Click **Draw Region** and draw a quadrilateral in the preview window by specifying four vertexes of the detection region.

Step 7 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 8 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

Step 9 Click Apply.

13.10 Audio Exception Detection

Purpose:

Audio exception detection detects the abnormal sounds in the surveillance scene, such as the sudden increase/decrease of the sound intensity.

Step 1 Go to System > Event > Smart Event.

Step 2 Click Audio Exception.

xception Detection Arming Schedule Linkage Action	Exception Detection Arming Schedule
Audio Loss Exception	Audio Loss Exception
Sudden Increase of Sound Intens	Sudden Increase of Sound Intens
Sensitivity 1 100 50	Sensitivity 1
Sound Int 1 100 50	Sound Int 1
Sudden Decrease of Sound Inten	Sudden Decrease of Sound Inten
Sensitivity 1 100 50	Sensitivity 1
Apply	Apply

Figure 13-10 Audio Exception Detection

Step 3 Select a camera to configure.

Step 4 Optionally, check **Save VCA Picture** to save the captured pictures of audio exception detection.

Step 5 Follow the steps to set the detection rules.

1) Select Exception Detection.

2) Select Audio Loss Exception, Sudden Increase of Sound Intensity Detection, or Sudden Decrease of Sound Intensity Detection.

Audio Loss Exception: Detects the sound steep rise in the surveillance scene. You can set the detection sensitivity and threshold for sound steep rise. You need to configure its Sensitivity and Sound Intensity Threshold.

Sensitivity: The smaller the value is, the more severe the change should be to trigger the detection. Range [1-100].

Sound Intensity Threshold: It can filter the sound in the environment. The louder the environment sound, the higher the value should be. Adjust it according to the environment. Range [1-100].

Sudden Decrease of Sound Intensity Detection: Detects the sound steep drop in the surveillance scene. You need set the detection sensitivity [1-100].

Step 6 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 7 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

Step 8 Click Apply.

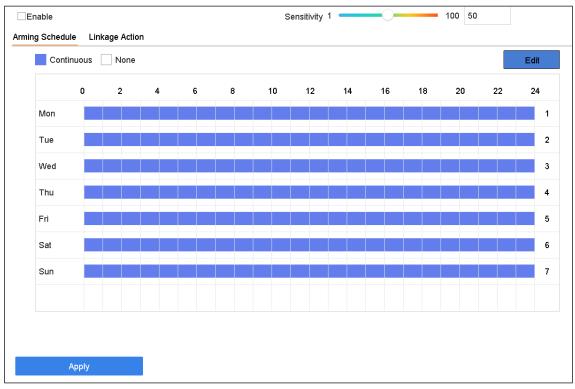
13.11 Sudden Scene Change Detection

Purpose:

Scene change detection detects the change of surveillance environment affected by the external factors, such as the intentional rotation of the camera.

Step 1 Go to System > Event > Smart Event.

Step 2 Click Sudden Scene Change.



Network Video Recorder User Manual

Figure 13-11 Sudden Scene Change

Step 4 Check Enable Sudden Scene Change Detection.

Step 5 Optionally, check **Save VCA Picture** to save the captured pictures of sudden scene change detection.

Step 6 Drag the **Sensitivity** slider to set the detection sensitivity. Sensitivity range: [1-100]. The higher the value is, the more easily the change of scene can trigger the alarm.

Step 7 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 8 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

Step 9 Click Apply.

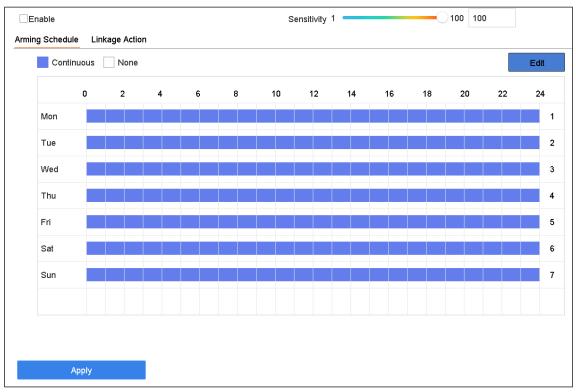
13.12 Defocus Detection

Purpose:

The image blur caused by defocus of the lens can be detected.

Step 1 Go to System > Event > Smart Event.

Step 2 Click **Defocus**.



Network Video Recorder User Manual

Figure 13-12 Defocus Detection

Step 4 Check Enable Defocus Detection.

Step 5 Optionally, check **Save VCA Picture** to save the captured pictures of defocus detection.

Step 6 Drag the **Sensitivity** slider to set the detection sensitivity. Sensitivity range: [1-100]. The higher the value is, the more easily the defocus image can be detected.

Step 7 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 8 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

Step 9 Click Apply.

13.13 PIR Alarm

Purpose:

A PIR (Passive Infrared) alarm is triggered when an intruder moves within the detector vision field. The heat energy dissipated by a person, or any other warm blooded creature such as dogs, cats, etc., can be detected.

Step 1 Go to System > Event > Smart Event.

Step 2 Click **PIR Alarm**.



Figure 13-13 FIR Alarm

Step 4 Check PIR Alarm.

Step 5 Optionally, check Save VCA Picture to save the captured pictures of PIR alarm.

Step 6 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 7 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions. Step 8 Click **Apply**.

Chapter 14 Smart Analysis

With the configured VCA detection, the device supports the smart analysis for people counting and heat map.

14.1 Engine Configuration

The chapter is only available for certain models of iDS series.

Purpose:

Each engine processes a specified VCA event type as its working mode. You shall configure the engine working mode according to the VCA event type.

Step 1 Go to Smart Analysis > Smart Analysis > Engine Configuration.

ingine Config	guration
ngine Config	guration and Us
-	
Engine 1	Working
Picture R	ecognition -
0/4	0%
Linked	Usage
	pply

Figure 14-1 Engine Configuration

Step 2 Configure each engine usage as **Picture Recognition - Human Face** or **Picture Recognition -Human Body**. You can view the working status, usage rate, and applied channel of smart analysis engine.

• If the engine has been bound with channel(s), switching engine working mode will unbind the engine and channel(s), and cancel the related smart event of the channel.

Step 3 Click **Apply** to save the settings.

14.2 Task Configuration

The chapter is only available for certain models of iDS series.

Purpose:

You can view the task status in task configuration. Smart analysis results are used for filtering the pictures when searching interested human body and vehicle pictures.

Before you start

Check **Save VCA Pictures** for human body detection/vehicle detection, line crossing detection, intrusion detection, region entrance, or region exiting.

Step 1 Go to Smart Analysis > Smart Analysis > Task Configuration.

sk Cont	iguration Eng	ine Configuration			
🛚 Edit	▷ Enab	led Disabled			
	Camera	Camera Name	Analysis Mode	Start Time	Status
	A1	Camera 01	Picture Recognition	2018-04-19	Disable
	A2	Camera 02	Picture Recognition	2018-04-19	Disable
	A3	Camera 03	Picture Recognition	2018-04-19	Disable
	A4	Camera 04	Picture Recognition	2018-04-19	Disable
	A5	Camera 05	Picture Recognition	2018-04-19	Disable
	A6	Camera 06	Picture Recognition	2018-04-19	Disable
	A7	Camera 07	Picture Recognition	2018-04-19	Disable
	A8	Camera 08	Picture Recognition	2018-04-19	Disable
	A9	Camera 09	Picture Recognition	2018-04-19	
	A10	Camera 10	Picture Recognition	2018-04-19	Disable
	A11	Camera 11	Picture Recognition	2018-04-19	Disable
	A12	Camera 12	Picture Recognition	2018-04-19	Disable
	A13	Camera 13	Picture Recognition	2018-04-19	Disable
	A14	Camera 14	Picture Recognition	2018-04-19	Disable

Figure 14-2 Task Configuration

Step 2 Check cameras to enable corresponding analysis mode. Ensure engine is available for the selected analysis mode.

Step 3 Enable auto analysis.

- 1) Click Edit.
- 2) (Optional) Check Enable of Display Status and Notify Surveillance Center.
- 3) Set **Start Time** of video to analyze.
- 4) Click **OK**.

Auto Analysis			×
Camera No. D1			
Camera Na Camera 01			
Analysis Mode Display Status	Notify Surveill	Start Time	
Video Structurali 🗌 Enable		2018-03-14	13:40:14
Video Structurali Enable	Enable	2018-03-14	13:40:14
Picture Recognit Enable	Enable	2018-03-14	13:40:14
Picture Recognit Enable		2018-03-14	13:40:14
Picture Recognit Enable		2018-03-14	13:40:14
		ОК	Cancel

Figure 14-3 Auto Analysis

Step 4 Check cameras and click Enabled to start analyzing.

Task status includes 3 conditions: **Disabled**, **Waiting**, and **Enabled**.

- **Disabled**: No analysis task is enabled on the camera.
- Waiting: The analysis task of the camera is enabled. Device is waiting to analyze data.
- **Enabled**: The analysis task of the camera is enabled and device is analyzing data of the camera.

14.3 Face Search

The chapter is not available for Acusense series.

Purpose:

When there are detected face picture captured and saved in HDD, you can enter the Face Search interface to search the picture and play the picture related video file according to the specified conditions.

Before you start:

Please refer to *Chapter 13.2 Face Detection* for configuring the face detection.

Step 1 Go to Smart Analysis > Smart Search > Face Search.

Step 2 Select the IP camera for the face search.

Search by Event						
IP Channel	[All] Camera			•		
Time Segment	Today	•	2017-09-19 00:00:00	-	2017-09-19 23:59:59	r landa
Event Type	All	•				

Figure 14-4 Face Search

- Step 3 Specify the start time and end time for search the captured face pictures or video files.
- Step 4 Click Start Search to start searching.
- Step 5 Double click on a face picture to play its related video file in the view window on the top right Play the face picture related video file.
- Step 6 To export the captured face pictures to local storage device, connect the storage device to the device and click **Export**.

14.4 Human Body Search

The chapter is only available for iDS series.

Purpose:

You can search and view the matched captured human body pictures.

Step 1 Go to Smart Analysis > Smart Search > Human Body Detection.

Step 2 Select the camera for the human body search.

Step 3 Set search conditions.

hannel	[All] Camera		•		
Time Segment	Today	-	2018-06-19 00:00:]-[2018-06-19 23:59: 🛅
Event Type	Human Body Ala	n -			

Figure 14-5 Plate Search

Step 4 Click Start Search.

14.5 Vehicle Search

The chapter is only available for iDS series.

Purpose:

You can search and view the matched captured vehicle pictures.

Step 1 Go to Smart Analysis > Smart Search > Vehicle Search.

Step 2 Select the IP camera for the vehicle search.

Step 3 Set search conditions.

Search by Appearanc	e			
Channel	[All] Camera		+	
Time Segment	Today	•	2018-06-19 00:00: 🛅 -	2018-06-19 23:59:
License Plate				

Figure 14-6 Plate Search

Step 4 Click Start Search.

14.6 People Counting

Purpose:

The Counting is used to calculate the number of people entered or left a certain configured area and form in daily/weekly/monthly/annual reports for analysis.

Step 1 Go to Smart Analysis > Smart Search > Counting.

Step 2 Select a camera.

Step 3 Select the report type to **Daily Report**, **Weekly Report**, **Monthly Report**, or **Annual Report** as you desired.

Step 4 Set the **Date** to analyze. Then it will generate the people counting graphic.

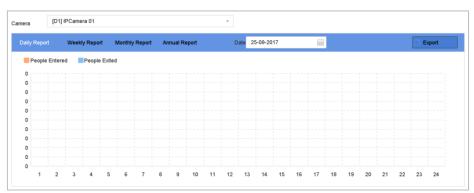


Figure 14-7 People Counting Interface

Step 5 (Optional) Click **Export** to export the report in excel format.

14.7 Heat Map

Purpose:

Heat map is a graphical representation of data. The heat map function is usually used to analyze how many people visited and stayed in a specified area.

The heat map function must be supported by the connected camera, and the corresponding configuration must be set.

Step 1 Go to Smart Analysis > Smart Search > Heat Map.

Step 2 Select a camera.

Step 3 Select the report type to **Daily Report**, **Weekly Report**, **Monthly Report**, or **Annual Report** as you desired.

Step 4 Set the **Data** to analyze.

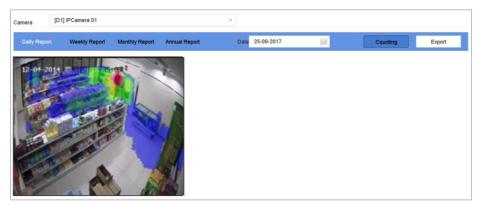


Figure 14-8 Heat Map Interface

Step 5 Click **Counting**. Then, there will generate the result graphic in different colors.

As shown in the figure above, red color block (255, 0, 0) indicates the most welcome area, and blue color block (0, 0, 255) indicates the less-popular area.

Step 6 (Optional) Click **Export** to export the statistics report in excel format.

Chapter 15 Human Body Detection

The chapter is only available for Deep Learning series.

15.1 Enable Human Body Smart Analysis

Purpose

The human body detection can detect the human body appearing in the monitoring scene, and capture the human body pictures.

- Step 1 Go to Smart Analysis > Smart Analysis > Engine Configuration. Configure the engine usage of at least one engine as Picture Recognition-Human Body. For details, refer to 14.1 Engine Configuration.
- Step 2 Go to Smart Analysis > Smart Analysis > Task Configuration to enable the task for camera. For details, refer to 14.2 Task Configuration.

15.2 Human Body Search

15.2.1 Search by Appearance

Purpose

Search human body pictures by specified human body appearance.

Search by Manually Specified Human Body Appearance

Purpose

Search human body pictures according to manually specified search conditions.

Before you start

Import human body pictures you want to search.

Step 1 Go to Smart Analysis > Smart Search > Human Body Detection > Search by Appearance.

Network Video Recorder User Manual

	Channel	[All] Camera		-	
	Time Segment	Today	•	2018-09-13 00:00: 🛅 -	2018-09-13 23:59: 🛅
	Event Type	Human Body Alar	-		
(↑)					
Upload					
Sample from Local					

Figure 15-1 Search by Appearance

Step 2 Specify search conditions.

Step 3 Click Start Search.

Search by Human Body Appearance Automatically Obtained from Uploaded Sample

Purpose

Search human body pictures according to human body appearance automatically obtained from uploaded sample pictures.

Before you start

Import a human body picture in USB flash drive and connect it to device.

- When there are multiple targets existing in the same picture, up to 30 target pictures can be analyzed and displayed.
- The maximum allowed picture size is 3840*2160.
- The picture must be in jpg or jpeg format.
- The picture name (with the suffix) cannot exceed 64 characters.
- Make sure the picture you uploaded is clear and recognizable.

Step 1 Go to Smart Analysis > Smart Search > Human Body Detection > Search by Appearance.

- Step 2 Click **Upload Sample from Local.** Device will analyze the appearance of human body in the uploaded sample picture.
- Step 3 Specify Time Segment and Event Type.
- Step 4 Click **Start Search**. Human body pictures match the appearance of uploaded human body picture will be listed.

15.2.2 Search by Picture

Purpose

To increase search accuracy, upload several pictures of one person to compare with captured human body pictures.

Before you start

Import human body pictures in USB flash drive and connect it to device.

- When there are multiple targets existing in the same picture, up to 30 target pictures can be analyzed and displayed.
- The maximum allowed picture size is 3840*2160.
- The picture must be in jpg or jpeg format.
- The picture name (with the suffix) cannot exceed 64 characters.
- Make sure the picture you uploaded is clear and recognizable.

Step 1 Go to Smart Analysis > Smart Search > Human Body Detection > Search by Picture.

Step 2 Click Upload Sample from Local.

Step 3 Select a picture in USB flash drive and click Import.

Step 4 Select related pictures and click Upload.

Step 5 Specify search conditions.

• **Similarity**: Device will analyze the similarity between samples and captured human body pictures and show pictures the similarity of which are higher than the set one.

Step 6 Click Start Search. Search results will be arranged in similarity ascending order.

15.2.3 Add Search Result as Sample Picture

Purpose

You can add searched human body pictures as sample pictures. And then search human body pictures by the sample pictures.

Step 1 Search human body pictures.

Step 2 In search result interface, click to select a picture and click Add to Sample.

Step 3 Return to search condition settings interface, the selected sample will be listed.

Chapter 16 Network Settings

16.1 Configure TCP/IP Settings

Purpose

TCP/IP settings must be properly configured before operating the device over network.

Step 1 Go to System > Network > TCP/IP.

Working Mode	Net Fault-Tolerance	*	
Select NIC	bond0	v	
NIC Туре	10M/100M/1000M Self-adap	Ψ.	
Enable DHCP		Enable Obtain DNS	
IPv4 Address	10 . 15 . 2 . 107	Preferred DNS Server	
IPv4 Subnet Mask	255 . 255 . 255 . 0	Alternate DNS Server	
IPv4 Default Gateway	10 . 15 . 2 . 254		
MAC Address	a4:14:37:aa:09:a3		
MTU(Bytes)	1500		
Main NIC	LAN1	Ŧ	

Figure 16-1 TCP/IP Settings

Step 2 Select Net-Fault Tolerance or Multi-Address Mode under Working Mode.

- **Net-Fault Tolerance**: The two NIC cards use the same IP address, and you can select the main NIC to LAN1 or LAN2. By this way, in case of one NIC card failure, the device will automatically enable the other standby NIC card so as to ensure the normal running of the whole system.
- Load Balance: By using the same IP address and two NIC cards share the load of the total bandwidth, which enables the system to provide two Gigabit network capacity.
- Multi-address Mode: The parameters of the two NIC cards can be configured independently. You can select LAN1 or LAN2 under Select NIC for parameter settings. You can select one NIC card as default route. And then the system is connecting with the extranet the data will be forwarded through the default route.

Step 3 Configure other IP settings as needed.

- Check **Enable DHCP** to obtain IP settings automatically if a DHCP server is available in the network.
- Valid range of MTU value is 500 to 1500.

Step 4 Click Apply.

16.2 Configure Guarding Vision

Purpose

Guarding Vision provides mobile phone application and platform service to access and manage your connected devices, which enables you to get a convenient remote access to the surveillance system.

Step 1 Go to System > Network > Advanced > Platform Access.

Step 2 Check Enable to activate the function. Then the service terms will pop up.

- 1) Enter the verification code in **Verification Code**.
- 2) Scan the QR code to read the service terms and privacy statement.
- 3) Check **The Guarding Vision service will require internet access. Please read Service Terms and Privacy Statement before enabling the service** if you agree the service terms and privacy statement.
- 4) Click **OK** to save the settings.

- Guarding Vision is disabled by default.
- The verification code is empty by default. It must contain 6 to 12 letters or numbers, and it is case sensitive.

Step 3 (Optional) Check Custom to enter the server address as your desire.

Step 4 (Optional) Check **Enable Stream Encryption**, verification code is required for remote access and live view.

Step 5 (Optional) Click **Unbind** if the device requires to unbind with the current Guarding Vision account.

Step 6 Click Apply.

What to do next:

After configuration, you can access and manage your devices through Guarding Vision app or website.

16.3 Configure DDNS

Purpose

You can set Dynamic DNS service for network access. Different DDNS modes are available: **DynDNS**, **PeanutHull**, and **NO-IP**.

Before You Start

You must register DynDNS, PeanutHull and NO-IP services with your ISP before configuring DDNS settings.

Step 1 Go to System > Network > TCP/IP > DDNS.

Step 2 Check Enable.

Step 3 Select DynDNS under DDNS Type.

PeanutHull and NO-IP are also available under DDNS Type, and required information should be entered accordingly.

Step 4 Enter Server Address for DynDNS (i.e. members.dyndns.org).

Step 5 Under **Device Domain Name**, enter the domain name obtained from the DynDNS website.

Step 6 Enter the User Name and Password registered in the DynDNS website.

Enable			
DDNS Type	DynDNS -	User Name	test
Server Address	member.dyndns.org	Password	******
Device Domain Name	1233dyndns.com		
Status	DDNS is disabled.		

Figure 16-2 DDNS Settings

Step 7 Click Apply.

16.4 Configure PPPoE

If the device is connected to Internet through PPPoE, you need to configure user name and password accordingly under **System** > **Network** > **TCP/IP** > **PPPoE**.

Contact your Internet service provider for details about PPPoE service.

16.5 Configure NTP

Purpose

Connection to a network time protocol (NTP) server can be configured on your device to ensure the accuracy of system date and time.

Step 1 Go to System > Network > TCP/IP > NTP.

ТСР/ІР	DDNS	PPPoE	NTP NAT
Enable			
Interval (r	min)		180
NTP Ser	ver		au.pool.ntp.org
NTP Por	ł		123
	Appl	v	

Figure 16-3 NTP Settings

Step 2 Check Enable.

Step 3 Configure NTP settings as need.

- Interval (min): Time interval between two time synchronizations with NTP server.
- **NTP Server**: IP address of the NTP server.
- **NTP Port**: Port of the NTP server.

Step 4 Click Apply.

16.6 Configure SNMP

Purpose

You can configure SNMP settings to get device status and parameter information.

Before You Start

Download the SNMP software to receive device information via SNMP port. By setting the trap address and port, the device is allowed to send alarm event and exception message to the surveillance center.

Step 1 Go to System > Network > Advanced > SNMP.

Enable	
SNMP Version	V2 -
SNMP Port	161
Read Community	public
Write Community	private
Trap Address	
Trap Port	162

Figure 16-4 SNMP Settings

Step 2 Check **Enable**. A message box will pop up to prompt possible security risk and click **Yes** to continue.

Step 3 Configure the SNMP settings as needed.

- Trap Address: IP address of the SNMP host.
- **Trap Port**: Port of the SNMP host.

Step 4 Click Apply.

16.7 Configure Email

Purpose

The system can send an Email to designated users when a specified event occurs, such as an alarm or motion event is detected, or the administrator password is changed, etc.

Before You Start

The device must be connected to a local area network (LAN) that contains an SMTP mail server. The network must be connected to either an intranet or the Internet depending on the location of the e-mail accounts to send notification.

User Name		SMTP Server		
Password		SMTP Port	25	
Sender	test01	Enable SSL/TLS		
Sender's Address	test01@hotmail.com			
Select Receivers	Receiver 1 -			
Receiver	test02			
Receiver's Address	test02@hotmail.com			
Enable Attached Picture				
Interval	2s ~			
Test	Apply			

Step 1 Go to System > Network > Advanced > Email.

Figure 16-5 Email Settings

Step 2 Configure the following Email settings.

- Enable Server Authentication: Check to enable the function if the SMTP server requires user authentication and enter user name and password accordingly.
- **SMTP Server**: The IP address of SMTP Server or host name (e.g., smtp.263xmail.com).
- **SMTP Port**: The SMTP port. The default TCP/IP port used for SMTP is 25.
- Enable SSL/TLS: Check to enable SSL/TLS if required by the SMTP server.
- Sender: The name of the sender.
- Sender's Address: Sender's Address.
- **Select Receivers**: Select the receiver. Up to 3 receivers can be configured.

- **Receiver**: The name of the receiver.
- **Receiver's Address**: The Email address of user to be notified.
- **Enable Attached Picture**: Check to enable the function if you want to send email with attached alarm images. The interval is the time between two adjacent alarm images.

Step 3 Click Apply.

Step 4 (Optional) Click Test to send a test email.

16.8 Configure Ports

You can configure different types of ports to enable relevant functions.

Go to **System > Network > Advanced > More Settings** and configure port settings as needed.

• Alarm Host IP/Port: With a remote alarm host configured, the device will send the alarm event or exception message to the host when an alarm is triggered. The remote alarm host must have the client management system (CMS) software installed.

The **Alarm Host IP** refers to the IP address of the remote PC on which the CMS software (e.g., CMS) is installed, and the **Alarm Host Port** (7200 by default) must be the same as the alarm monitoring port configured in the software.

- Server Port: Server port (8000 by default) should be configured for remote client software access and its valid range is 2000 to 65535.
- **HTTP Port**: HTTP port (80 by default) should be configured for remote web browser access.
- **Multicast IP**: Multicast can be configured to enable live view for cameras that exceed the maximum number allowed through network. A multicast IP address covers Class-D IP ranging from 224.0.0.0 to 239.255.255.255 and it is recommended to use the IP address ranging from 239.252.0.0 to 239.255.255.255.

When adding a device to the CMS software, the multicast address must be the same as that of the device.

- **RTSP Port**: RTSP (Real Time Streaming Protocol) is a network control protocol designed for use in entertainment and communications systems to control streaming media servers. The port is 554 by default.
- **Output Bandwidth Limit**: You can check the checkbox to enable output bandwidth limit.
- **Output Bandwidth**: After enable the output bandwidth limit, input the output bandwidth.

- The output bandwidth limit is used for the remote live view and playback.
- The default output bandwidth is the maximum limit.

Network Video Recorder User Manual

Email Platform A	ccess	More Settings
Alarm Host IP		
Alarm Host	0	
Server Port	8000	
HTTP Port	80	
Multicast IP		
RTSP Port	554	
Output Ban		
Output Ban	2	
Apply		

Figure 16-6 Port Settings

Chapter 17 System Maintenance

17.1 Storage Device Maintenance

17.1.1 Configure Disk Clone

Purpose:

Select the HDDs to clone to eSATA HDD.

Before you start:

Connect an eSATA disk to the device.

Step 1 Go to Maintenance > HDD Operation > HDD Clone.

Clone Sourc	e					
Label	Capacity	Status	Property	Туре	Free Space	Group
1	1863.02GB	Normal	R/W	Local	1858.00GB	1
2	2794.52GB	Normal	R/W	Local	2794.00GB	1
5	1863.02GB	Normal	R/W	Local	1862.00GB	1
9	2794.52GB	Normal	R/W	Local	2794.00GB	1
1 0	1863.02GB	Normal	R/W	Local	1862.00GB	1
Clone Destin	nation					
eSATA	eSATA1				•	Refresh
Capacity	2794.52GB					Clone

Figure 17-1 HDD Clone

Step 2 Check the HDD to clone. The capacity of selected HDD must match the capacity of clone destination.

Step 3 Click Clone.

Step 4 Click Yes on popup message box to continue clone.

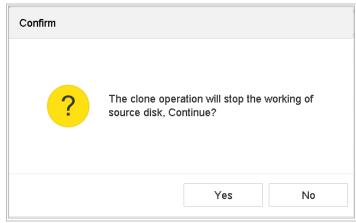


Figure 17-2 Message Box

17.1.2 S.M.A.R.T Detection

Purpose:

The device provides HDD detection function including S.M.A.R.T. and Bad Sector Detection technique. The S.M.A.R.T. (Self-Monitoring, Analysis and Reporting Technology) is a monitoring system for HDD to detect and report on various indicators of reliability in the hopes of anticipating failures.

Step 1 Go to Maintenance > HDD Operation > S.M.A.R.T.

Step 2 Select the HDD to view its S.M.A.R.T information list.

Step 3 Select the self-test types as Short Test, Expanded Test or Conveyance Test.

Step 4 Click **Self-Test** to start the S.M.A.R.T. HDD self-evaluation.

Step 5 The related information of the S.M.A.R.T. is shown on the interface. You can check the HDD status.

IDD No.	5	-					
elf-Test Type	Short Test	*	Self-Test	Not tested			
emperature	36		Self-Evaluation	Pass			
Vorking Time	. 390		All-Evaluation	Functional			
ID 0x1	Attribute Name	Status OK	Flags 2f	Threshold	Value	Worst 200	Raw Value
	Spin Up Time	ок	27	21	113	107	7316
0x3			32	0	98	98	2657
0x3 0x4	Start/Stop Count	OK					0
	Start/Stop Count Reallocated Sector	ок	33	140	200	200	0
0x4			33 2e	140 0	200 200	200 200	0
0x4 0x5	Reallocated Sector	ок					
0x4 0x5 0x7	Reallocated Sector Seek Error Rate	ок ок	2e	0	200	200	0

Figure 17-3 S.M.A.R.T Settings Interface

If you want to use the HDD even when the S.M.A.R.T. checking is failed, you can check **Continue to use the disk when self-evaluation is failed**.

17.1.3 Bad Sector Detection

Step 1 Go to Maintenance > HDD Operation > Bad Sector Detection.

Step 2 Select the HDD No. in the dropdown list you want to configure.

Step 3 Select **All Detection** or **Key Area Detection** as the detection type.

Step 4 Click Self-Test to start the detection.

HDD No. 5 All Detection Key Area De... Self-Test Pause Cancel 📕 Functional 📕 Bad Shield Detecting Process Testing... 2% HDD Capacity 931.52GB Block Size 232.88MB Error Count 0 Error Information Figure 17-4 Bad Sector Detection

Network Video Recorder User Manual

- You can also pause/resume or cancel the detection.
- After testing completed, click **Error information** to see the detailed damage information.

17.1.4 HDD Health Detection

Purpose:

You can view the health status of Seagate HDD that generated after October 1th, 2017 and provides capacity ranges from 4 TB to 8 TB. The function helps you to troubleshoot HDD problems. Compared with S.M.A.R.T function, health detection shows HDD status with more details.

Step 1 Go to Maintenance > HDD Operation > Health Detection.

16 HDD (s) in total. The detectio	n is only ava	ailable for the Seaga	ate H	HDD.			SETERANE
No. 1	HDD is healthy.	No.2	HDD is healthy.		No.3	HDD is healthy.	No.4	HDD is healthy.
No.5	HDD is healthy.	No.6	HDD is healthy.		No.7	HDD is healthy.	No.8	HDD is healthy.
No.9	HDD is healthy.	No.10	HDD is healthy.		No.11	HDD is healthy.	No.12	HDD is healthy.
No.13	HDD is healthy.	No. 14	HDD is healthy.		№.15	HDD is healthy.	No.16	HDD is healthy.

Figure 17-5 Health Detection

Step 2 Click a HDD to view details.

17.2 Search & Export Log Files

Purpose:

The operation, alarm, exception and information of the device can be stored in log files, which can be viewed and exported at any time.

17.2.1 Search the Log Files

Step 1 Go to Maintenance > Log Information.

Step 2 Set the log search conditions.

Step 3 Click Search to start search log files.

The matched log files will be displayed in the list shown below.

No.	Major Type	Time	Minor Type	Parameter	Play	Details
1	Exception	2017-10-09 00:01:53	HDD Error	N/A	—	()
2	Operation	2017-10-09 00:01:53	Abnormal Shutdown	N/A		()
3	Operation	2017-10-09 00:01:54	Power On	N/A	-	()
4	Information	2017-10-09 00:01:54	Local HDD Information	N/A		()
5	🔔 Exception	2017-10-09 00:04:01	HDD Error	N/A	-	()
6	Operation	2017-10-09 00:04:01	Abnormal Shutdown	N/A		()
7	Cperation	2017-10-09 00:04:02	Power On	N/A	-	()
8	Information	2017-10-09 00:04:02	Local HDD Information	N/A		()
9	🔔 Exception	2017-10-09 00:06:09	HDD Error	N/A	-	()
10	Operation	2017-10-09 00:06:09	Abnormal Shutdown	N/A		()
11	Information	2017-10-09 00:06:10	Local HDD Information	N/A	-	()
12	Cperation	2017-10-09 00:06:10	Power On	N/A		()
13	🔔 Exception	2017-10-09 00:08:18	HDD Error	N/A	-	()
14	Cperation	2017-10-09 00:08:18	Abnormal Shutdown	N/A	-	()
15	Operation	2017-10-09 00:08:19	Power On	N/A	-	()
16	Information	2017-10-09 00:08:19	Local HDD Information	N/A	-	()
17	🔔 Exception	2017-10-09 00:12:01	HDD Error	N/A	-	()
18	Operation	2017-10-09 00:12:01	Abnormal Shutdown	N/A	-	()

Figure 17-6 Log Search Results

Up to 2000 log files can be displayed each time.

Related Operation:

• Click it to view its detailed information.

• Click by to view the related video file.

17.2.2 Export the Log Files

Before You Start:

Connect a storage device to your device.

Step 1 Search the log files. Refer to Chapter 17.2.1 Search the Log Files.

Step 2 Select the log files you want to export, and click **Export**.

Or you can click **Export ALL** on the Log Search interface to export all the system logs to the storage device.

System Log Ex	port					\times
Device Na	USB Flash Disł	< 1-1		≁.txt	•	Ģ
Name	Size	Туре	Edit Date	De	Play	
2017082	41.3	File	22-08-2017	. ×	-	
+ New Folde	er 💿 El	rase		Free Space	8993.111	ИВ
				Export	Back	

Figure 17-7 Export Log Files

Step 3 Select the storage device from the dropdown list of **Device Name**.

Step 4 Select the format of the log files to be exported. Up to 15 formats are selectable.

Step 5 Click **Export** to export the log files to the selected storage device.

Related Operation:

- Click **New Folder** to create new folder in the storage device.
- Click **Format** to format the storage device before log export.

17.3 Import/Export IP Camera Configuration Files

Purpose:

The information of added IP camera can be generated into an excel file and exported to the local device for backup, including the IP address, manage port, password of admin, etc. And the exported file can be edited on your PC, like adding or deleting the content, and copy the setting to other devices by importing the excel file to it.

Before You Start:

Connect a storage device to your device. For importing the configuration file, the storage device must be with the file.

Step 1 Go to Camera > IP Camera Import/Export.

Step 2 Click the **IP Camera Import/Export** tab, and the content of detected plugged external device appears.

Step 3 Export or import the IP camera configuration files.

• Click **Export** to export configuration files to the selected local backup device.

• To import a configuration file, select the file from the selected backup device and click the **Import** button.

After the importing process is completed, you must reboot the device to activate the settings.

17.4 Import/Export Device Configuration Files

Purpose:

The configuration files of the device can be exported to local device for backup; and the configuration files of one device can be imported to multiple devices if they are to be configured with the same parameters.

Connect a storage device to your device. For importing the configuration file, the storage device must be with the file.

Before You Start:

Connect a storage device to your device. For importing the configuration file, the storage device must be with the file.

Step 1 Go to Maintenance >Import/Export

Device Name USB Fla	sh Disk 1-1	File Format	*.bin 👻			\bigcirc Refresh
+ New Folder	Le Import	È Export			Total Free Capacity	9165.35MB
Name	Size	Туре	Modify Date	Delete	Play	
📄 devCfg_759708301	1260.94KB	File	18-08-2017 18:28:09	×		

Figure 17-8 Import/Export Config File

Step 2 Export or import the device configuration files.

• Click **Export** to export configuration files to the selected local backup device.

• To import a configuration file, select the file from the selected backup device and click **Import**.

After having finished the import of configuration files, the device will reboot automatically.

17.5 Upgrade System

Purpose:

The firmware on your device can be upgraded by local backup device or remote FTP server.

17.5.1 Upgrade by Local Backup Device

Before You Start:

Connect your device with a local storage device with update firmware file.

Step 1 Go to Maintenance > Upgrade > Local Upgrade to enter the local upgrade interface.

Device Name	USB Flash Disk 1-1	File Format *.day	v;*.mav;*.iav			C Refresh
① Upgrade						
File Name	File Size	File Type	Edit Date	Delete	Play	

Figure 17-9 Local Upgrade Interface

Step 2 Select the update file from the storage device.

Step 3 Click Upgrade to start upgrading.

Step 4 After the upgrading is complete, the device will reboot automatically to activate the new firmware.

17.5.2 Upgrade by FTP

Before you start:

Ensure the network connection of the PC (running FTP server) and the device is valid and correct. Run the FTP server on the PC and copy the firmware into the corresponding directory of your PC.

Step 1 Go to Maintenance > Upgrade > FTP to enter the local upgrade interface.

FTP Server Address	192 . 0 . 0 . 68
Upgrade	

Figure 17-10 FTP Upgrade Interface

Step 2 Enter IP address of FTP Server Address.

Step 3 Click **Upgrade** to start upgrading.

Step 4 After the upgrading is complete, reboot the device to activate the new firmware.

17.5.3 Upgrade by Guarding Vision

Purpose:

After logging the device into Guarding Vision, the device would periodically check for the latest firmware from Guarding Vision. If an upgrade firmware is available, the device will notify you when you log in. You can also manually check for the latest firmware.

Before You Start:

Ensure the device has successfully connected to Guarding Vision, and it requires to install at least one read-write HDD for firmware downloading.

Step 1 Go to Maintenance > Upgrade > Online Upgrade.

Step 2 Click **Check Upgrade** to manually check and download the latest firmware from Guarding Vision.

The device will automatically check for the latest firmware every 24 hours. If it detects available upgrade firmware, the device will notify you when you log in.

Step 3 (Optional) You can switch on **Download Latest Package Automatically** to automatically download the latest firmware package.

Step 4 Click Upgrade Now.

17.6 Upgrade Camera

Purpose

You can upgrade multiple connected analog cameras supporting Turbo HD or AHD signal simultaneously with DVR.

- Step 1 Go to Maintenance > Upgrade > Camera Upgrade.
- Step 2 Check the checkbox(es) of the analog camera(s) for upgrading.

The analog camera must support Turbo HD or AHD signal.

- Step 3 Select the update file from the backup device.
- Step 4 Click **Upgrade** to start upgrading.

17.7 Restore Default Settings

Step 1 Go to Maintenance > Default.

Restore Defaults	Reset all settings to factory default except network and admin password settings
Factory Defaults	Restore device to inactive status and all settings including network and password
Restore to Inactive	Leave all settings unchanged except restore device to inactive status without amdin password

Figure 17-11 Restore Defaults

Step 2 Select the restoring type from the following three options.

Restore Defaults: Restore all parameters, except the network (including IP address, subnet mask, gateway, MTU, NIC working mode, default route, server port, etc.) and user account parameters, to the factory default settings.

Factory Defaults: Restore all parameters to the factory default settings.

Restore to Inactive: Restore the device to the inactive status.

The device will reboot automatically after restoring to the default settings.

17.8 System Service

17.8.1 Network Security Settings

Disable SADP Services

Purpose

You can disable SADP service to enhance the access security, e.g., when you are in the untrusted network environment.

Step 1 Go to System > System Service > System Service.

Step 2 Uncheck Enable SADP to disable the service.

HTTP

You can choose to disable the HTTP, or set the HTTP authentication when it is enabled as demand to enhance the access security.

By default, the HTTP service is enabled.

Set HTTP Authentication

Purpose

If you need to enable the HTTP service, you can set the HTTP authentication to enhance the access security.

Step 1 Go to System > System Service > System Service.

Enable HTTP		
HTTP Authentication Type	digest	•

Figure 17-12 HTTP Authentication

Step 2 Check the **Enable HTTP** to enable the HTTP service.

Step 3 Select the **digest** as the **HTTP Authentication** in the drop-down list.

Step 4 Click Save to save the settings.

Two authentication types are selectable: **digest** and **digest/basic**. For security reasons, it is recommended to select digest as the authentication type.

Disable HTTP

Purpose

The admin user account can disable the HTTP service from the GUI or the web browser.

After the HTTP is disabled, all its related services, including the ISAPI, Onvif and Gennetc, will terminate as well.

Step 5 Go to System > System Service > System Service.

Step 6 Uncheck the **Enable HTTP** to disable the HTTP service.

RTSP Authentication

Purpose

You can specifically secure the stream data of live view by setting the RTSP authentication.

Step 1 Go to System > System Service > System Service.

Enable RTSP		
RTSP Authentication Type	digest	•

Figure 17-13 RTSP Authentication

Step 2 Select the authentication type.

Two authentication types are selectable: **digest** and **digest/basic**. If you select **digest**, as the RTSP authentication, only the request with digest authentication can access the video stream by the RTSP protocol via the IP address. For security reasons, it is recommended to select digest as the authentication type.

Step 3 Click Save to save the settings.

17.8.2 Managing ONVIF User Accounts

Purpose

For the third-party camera connection to the device via ONVIF, you can enable ONVIF function and manage the user accounts.

Step 1 Go to System > System Service > ONVIF.

Step 2 Check Enable ONVIF to enable the ONVIF access management.

Step 3 Click **Add** to enter the Add User interface.

Add User		\times
User Name	01	
Password	*****	
	Strong	
Confirm	*****	
Level	Media User	•
	Note: Valid password range [8-16]. You combination of numbers, lowercase, up and special character for your password least two kinds of them contained.	percase
	ок	Cancel

Figure 17-14 Add User

Step 4 Edit the user name, and enter the strong password.

Step 5 Select the user level to Media User, Operator and Admin.

Step 6 Click **OK** to save the settings.

Result:

The added user accounts have the permission to connect other devices to the device via ONVIF protocol.

ONVIF protocol is disabled by default.

17.8.3 Managing IP Camera Activation

Purpose:

When you activate the device for the first-time access, you can set the activation password for the IP camera (s) as well. Refer to Chapter 2.2 Activate the Device. And you can also manage the password to enhance the security.

Step 1 Go to System > System Service > IP Camera Activation.

Step 2 Check the **Change Password** to enable the permission.

Step 3 Enter the admin password of the device to obtain the permission.

Change Password	⊻	
IP Camera Activation Pa	a	
numbers, lowercase	d range [8-16]. You can use a combination of , uppercase and special character for your password ds of them contained.	

Figure 17-15 Change IP Camera Activation Password

Step 4 In the text filed of the **IP Camera Activation Password**, enter the new strong password for the cameras.

Step 5 Click **Apply** to have the following pop-up attention box.

Confirm	
?	Duplicate the password to IP cameras that are connected with default protocol.
	Yes No

Figure 17-16 Attention

Step 6 Click **Yes** to duplicate the current password to the IP cameras which are connected with the default protocol.

Chapter 18 General System Settings

18.1 Configure General Settings

Purpose:

You can configure the BNC output standard, VGA output resolution, mouse pointer speed through the System > General interface.

Step 1 Go to System > General.

Time Zone	(GMT+08:00) Beijing, Urur	mc -	VGA2/HDMI2 Resolution		1920	*1080	/60HZ(10	80P)	-			
Date Format	DD-MM-YYYY	-	Mouse Pointer Spe	ed		Slow				— Fa	st	
System Date	22-08-2017		Enable DST									
System Time	11:34:09	\oplus	DST Mode			⊖ Auto		 Manu 	al			
Device Name	Network Video Recorder		Start Time	Apr	•	1st	•	Sun	•	2	0	: 0
Device No.	255		End Time	Oct	•	last	Ŧ	Sun	•	2	89	: 00
Auto Log out	Never	•	DST Bias			60 M	inutes	1		•		
Enable Wizard												
Enable Password												

Figure 18-1 General Settings Interface

Step 2 Configure the following settings.

Language: The default language used is English.

Output Standard: Select the output standard to NTSC or PAL, which must be the same with the video input standard.

Resolution: Configure the resolution of the video output.

Device Name: Edit the name of the device

Device No.: Edit the serial number of the device. The Device No. can be set in the range of 1^{255} , and the default No. is 255. The number is used for the remote and keyboard control.

Auto Logout: Set timeout time for menu inactivity. E.g., when the timeout time is set to 5 *Minutes*, then the system will exit from the current operation menu to live view screen after 5 minutes of menu inactivity.

Mouse Pointer Speed: Set the speed of mouse pointer; 4 levels are configurable.

Enable Wizard: Enable/disable the Wizard when the device starts up.

Enable Password: Enable/disable the use of the login password.

Step 3 Click **Apply** to save the settings.

18.2 Configure Date & Time

Step 1 Go to System > General.

Step 2 Configure the date and time.

Time Zone: Select the time zone.

Date Format: Select the date format.

System Date: Select the system date.

System Time: Set the system time.

Time Zone	(GMT+08:00) Beijing, Urumo	-
Date Format	DD-MM-YYYY	•
System Date	22-08-2017	
System Time	11:34:09	

Figure 18-2 Date and Time Settings

Step 3 Click Apply to save the settings.

18.3 Configure DST Settings

Purpose:

The DST (daylight saving time) refers to the period of the year when clocks are moved one period ahead. In some areas worldwide, this has the effect of creating more sunlit hours in the evening during months when the weather is the warmest.

We advance our clocks ahead a certain period (depends on the DST bias you set) at the beginning of DST, and move them back the same period when we return to standard time (ST).

Step 1 Go to System > General.

Step 2 Check Enable DST.

Enable DST					
DST Mode		A	uto 💿	Manual	
Start Time	Ap -	1s [.] ~	Su -	2	: 00
End Time	Oc -	las 🤟	Su -	2	: 00
DST Bias		6	0 Minutes	v]

Figure 18-3 DST Settings Interface

Step 3 Select the DST mode to Auto or Manual.

- Auto: Automatically enable the default DST period according to the local DST rules.
- Manual: Manually set the start time and end time of the DST period, and the DST bias.
- DST Bias: Set the time (30/60/90/120 minutes) offset from the standard time.
- **Example:** The DST begins at 2:00 a.m. on the second Sunday of March and ends at 2:00 a.m. on the first Sunday of November, with 60 minutes ahead.

Step 4 Click the **Apply** button to save the settings.

18.4 Configure Enhanced IP Mode

Check Enhanced IP Mode.

Enabling Enhanced IP Mode will allow you to connect to the maximum number of cameras and make Smart Event unavailable in analog channel.

This function is only available for Acusense series.

18.5 Manage User Accounts

Purpose:

The *Administrator* user name is *admin* and the password is set when you start the device for the first time. The *Administrator* has the permission to add and delete user and configure user parameters.

18.5.1 Add a User

Step 1 Go to System > User.

+ Add	🖉 Modify 🛛 🗙 Delete					
No	User Name	Security	Priority	User's MAC Address	Permission	
1	admin	Strong Password	Admin	00:00:00:00:00:00	0	

Figure 18-4 User Management Interface

Step 2 Click Add to enter the operation permission interface.

Step 3 Enter the admin password and click Next.

	\times
A01	

Strong	

Note:Valid password range [8-16]. You can u	se
Operator	•
00 :00 :00 :00 :00 :00	
	ОК
	******* Strong ******* Note:Valid password range [8-16]. You can u Operator

Figure 18-5 Add User

Step 4 In the Add User interface, enter the information for new user, including **User Name**, **Password**, **Confirm** (password), **User Level** (Operator/Guest) and **User's MAC Address**.

Strong Password recommended–We highly recommend you create a strong password of your own choosing (Using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters.) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

• User Level: Set the user level to Operator or Guest. Different user levels have different operating permission.

Operator: The *Operator* user level has permission of Two-way Audio in Remote Configuration and all operating permission in Camera Configuration by default.

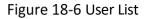
Guest: The Guest user has no permission of Two-way Audio in Remote Configuration and only has the local/remote playback in the Camera Configuration by default.

• User's MAC Address: The MAC address of the remote PC which logs onto the device. If it is configured and enabled, it only allows the remote user with this MAC address to access the device.

Step 5 Click **OK** to finish the new user account adding.

Result: In the User Management interface, the added new user is displayed on the list.

1-	Linea Marra	0.000	Detailty		- Demolation	
10	User Name	Security	Priority	User's MAC Address	Permission	
	admin	Strong Password	Admin	00:00:00:00:00	0	
2	A01	Strong Password	Operator	00:00:00:00:00:00	0	
3	A02	Strong Password	Operator	00:00:00:00:00:00	\bigcirc	



18.5.2 Set Permission for a User

For the added user, you can assign the different permissions, including the local and remote operation for the device.

Step 1 Go to System > User.

Step 2 Select a user from the list and then click the \leq button to enter the permission settings interface.

Permission			\times
Local Configuration	Remote Configuration	Camera Configura	lion
✓Local Log Search			
Local Parameters	Settings		
Local Camera Mar	nagement		
Local Advanced O	peration		
Local Shutdown /	Reboot		
	Apply	ОК	Cancel

Figure 18-7 User Permission Settings Interface

Step 3 Set the operating permission of Local Configuration, Remote Configuration and Camera Configuration for the user.

Local Configuration

Local Log Search: Searching and viewing logs and system information of device.

Local Parameters Settings: Configuring parameters, restoring factory default parameters and importing/exporting configuration files.

Local Camera Management: The adding, deleting and editing of IP cameras.

Local Advanced Operation: Operating HDD management (initializing HDD, setting HDD property), upgrading system firmware, clearing I/O alarm output.

Local Shutdown Reboot: Shutting down or rebooting the device.

Remote Configuration

Remote Log Search: Remotely viewing logs that are saved on the device.

Remote Parameters Settings: Remotely configuring parameters, restoring factory default parameters and importing/exporting configuration files.

Remote Camera Management: Remote adding, deleting and editing of the IP cameras.

Remote Serial Port Control: Configuring settings for RS-232 and RS-485 ports.

Remote Video Output Control: Sending remote button control signal.

Two-Way Audio: Realizing two-way radio between the remote client and the device.

Remote Alarm Control: Remotely arming (notify alarm and exception message to the remote client) and controlling the alarm output.

Remote Advanced Operation: Remotely operating HDD management (initializing HDD, setting HDD property), upgrading system firmware, clearing I/O alarm output.

Remote Shutdown/Reboot: Remotely shutting down or rebooting the device.

Camera Configuration

Remote Live View: Remotely viewing live video of the selected camera (s).

Local Manual Operation: Locally starting/stopping manual recording and alarm output of the selected camera (s).

Remote Manual Operation: Remotely starting/stopping manual recording and alarm output of the selected camera (s).

Local Playback: Locally playing back recorded files of the selected camera (s).

Remote Playback: Remotely playing back recorded files of the selected camera (s).

Local PTZ Control: Locally controlling PTZ movement of the selected camera (s).

Remote PTZ Control: Remotely controlling PTZ movement of the selected camera (s).

Local Video Export: Locally exporting recorded files of the selected camera (s).

Step 4 Click **OK** to save the settings.

Only the admin user account has the permission of restoring factory default parameters. 18.5.3 Set Local Live View Permission for Non-Admin Users

Step 1 Go to System > User.

Step 2 Click 🗹 of admin user.

Step 3 Enter admin password and click **OK**.

Step 4 Select cameras that non-admin user can view in local and click OK.

Camera					Select All	 ✓
 ∠D1	∠ D2	✓ D3	✓ D4	✓ D5	✓ D6	
✓ D7	∠ D8	🗹 D9	✓D10	∠ D11	✓D12	
✓D13	✓D14	🗹 D15	🗹 D16	∠ D17	✓ D18	
🗹 D19	✓D20	✓ D21	✓ D22	∠ D23	✓ D24	
✓ D25	✓ D26	✓ D27	✓ D28	✓D29	✓ D30	
✓D31	✓ D32	✓ D33	✓ D34	🗹 D35	✓ D36	
🗹 D37	✓ D38	✓ D39	✓ D40	✓ D41	✓ D42	
✓ D43	✓ D44	✓ D45	✓ D46	✓ D47	✓ D48	
🗹 D49	🗹 D50	🗹 D51	🗹 D52	🗹 D53	🗹 D54	

Figure 18-8 Enable Live View Permission

Step 5 Click 🗹 of non-admin user.

Step 6 Enter Camera Configuration interface.

Step 7 Select Camera Permission as Local Live View.

Step 8 Select cameras to live view.

Step 9 Click OK.

18.5.4 Edit the Admin User

Purpose:

For the admin user account, you can modify your password and unlock pattern.

Step 1 Go to System > User.

Step 2 Select the admin user from the list.

Step 3 Click Modify.

User Name	admin		
Password	******		Discard C
Confirm	*******		
Note:Va	lid password range (8-16). You o	an use	9
Password S			
	00 : 00 : 00 : 00 : 00	: OC	
		: OC	
User's MAC Ad	00 : 00 : 00 : 00 : 00		
User's MAC Ad Unlock Patt	00 : 00 : 00 : 00 : 00 ⊡Enable Unlock Pattern	٢	

Figure 18-9 Edit Admin User

Step 4 Edit the admin user information as demand, including the new admin password (strong password is required), and MAC address.

Step 5 Edit the unlock pattern for the admin user account.

- 1) Check **Enable Unlock Pattern** to enable the use of unlock pattern when logging in to the device.
- 2) Use the mouse to draw a pattern among the 9 dots on the screen, and release the mouse when the pattern is done.

Step 6 Check **Export** of **Export GUID** to export the GUID file for the admin user account.

When the admin password is changed, export the new GUID to the connected USB flash drive for the future password resetting.

Step 7 Configure security question for password resetting.

Step 8 Configure reserved email for password resetting.

Step 9 Click **OK** to save the settings.

18.5.5 Edit the Operator/Guest User

Purpose:

You can edit the user information, including user name, password, permission level and MAC address. Check the checkbox of **Change Password** if you want to change the password, and input the new password in the text field of **Password** and **Confirm**. A strong password is recommended.

Step 1 Go to **System** > **User**.

Step 2 Select a user from the list and click Modify.

Edit User		\times
User Name	A01	
Password	****	Discard C
Confirm	****	
Note:Valid p	assword range [8-16]. You can use	
Password Stre		
User Level	Operator -	
User's MAC Ad	00 :00 :00 :00 :00 :00	
		ОК

Figure 18-10 Edit User (Operator/Guest)

Step 3 Edit the user information as demand, including the new password (strong password is required), and MAC address.

18.5.6 Delete a User

Purpose:

The admin user account has the permission to delete the operator/guest user account.

Step 1 Go to System > User.

Step 2 Select a user from the list.

Step 3 Click **Delete** to delete the selected user account.

18.6 Configure Password Security

18.6.1 Export GUID File

Purpose:

The GUID file will help you to reset password when you forget your password.

Step 1 Check **Export GUID** when you are activating the device, or check **Export** when you are editing the admin user account.

Step 2 Insert a USB flash drive to your device, and export the GUID file to the USB flash drive.

Ģ	GUID Import/Expor	t					\times
[Device Na US	B Flash Disł	x 1-1		* **	•	g
	Name	Size	Туре	Edit Date	De	Play	
	😂 mobileD		Fol	02-01-2018	×	—	
	😑 printscr		Fol	02-01-2018	×	-	
	🗎 1.22-1.b	6075	File	21-01-2018	\times	-	
	🗎 1.22-2.b	6075	File	21-01-2018	×	-	
	🗎 1.22-3.b	6075	File	21-01-2018	×	-	
	🗎 1.22-4.b	6075	File	21-01-2018	×	-	
	🗎 1.22-5.b	6075	File	21-01-2018	×	-	
	🗎 1.22-6.b	6075	File	21-01-2018	×	-	
	New Folder	🖑 Ei	ase		Free Spac	e 14.00GB	
				E	Export	Back	

Figure 18-11 Export GUID File

Please keep your GUID file properly for future password resetting.

18.6.2 Configure Security Questions

Purpose:

The security question configuration will help you to reset password when you forget your password or encounter security issues.

- Step 1 Check **Security Question Configuration** when you are activating the device, or click when you are editing the admin user account.
- Step 2 Set three security questions and answers.

3

Step 3 Click OK.

Security Question Configuration	on		×
Question 1	10. Your favorite book.	•	
Answer 1	А		
Question 2	11. Your favorite color.	•	
Answer 2	Blue		
Question 3	13. Your favorite flower.	·	
Answer 3	Rose		
	ок		Cancel

Figure 18-12 Configure Security Questions

18.6.3 Configure Reserved Email

Purpose:

The reserved email will help you to reset password when you forget your password.

- Step 1 Check **Reserved E-mail** when you are activating the device, or click **Modify** when you are editing the admin user account.
- Step 2 Enter reserved email address.

Step 3 Click OK.

User Name	admin		
Password	*****		Modify
User's MAC Ad	00 : 00 : 00 : 00 : 00	: 00	
Unlock Patt	Enable Unlock Pattern	٢	
GUID File	Export	0	
Security Qu	٢		
Reserved E	z******@******.com		⑦ Modify

Figure 18-13 Configure Reserved Email

18.7 Reset Password

When you forget the admin password, there are three ways to reset the password, including importing the GUID file, answering security questions, and using your reserved email.

18.7.1 Reset Password by GUID

Before You Start

The GUID file must be exported and saved in the USB flash drive after you have activated the device or edited the admin user account. (Refer to 18.6.1 Export GUID File).

Step 1 On the user login interface, click Forgot Password.

Step 2 Select the password resetting type to Verify by GUID.

Step 3 Insert the USB flash drive that contains GUID file to the device.

Step 4 Click OK.

	Reset P	assword		
Please Choose t	he GUID File			
Device Name	USB Flash Disk 1-1			- G Refresh
Name	1	Size	Туре	Edit Date
😅 System Vo	lume Information		Folder	08-07-2018 15:1
H GUID_C07	590835_201808090343	128B	File	08-09-2018 03:4
⊨ GUID_C29	025066_201808141431	128B	File	08-14-2018 14:3
				iport Cancel

Figure 18-14 Import GUID File

Step 5 Select the GUID file from the USB flash drive and click **Import** to import the file to the device.

- Step 6 After the GUID file is successfully imported, enter the reset password interface to set the new admin password.
- Step 7 Click **OK** to set the new password. You can export the new GUID file to the USB flash drive for future password resetting.

When the new password is set, the original GUID file will be invalid.

18.7.2 Reset Password by Security Questions

Before You Start

Ensure you have configured the security questions when you are activating the device or editing the admin user account. (Refer to 18.7.2 Reset Password by Security Questions).

Step 1 On the user login interface, click Forgot Password.

Step 2 Select the password resetting type to Verify by Security Question.

- Step 3 Input the correct answers of the three security questions.
- Step 4 Click **OK** to set the new password.

	Verify by Security Question	
Question 1	Your father's name.	
Answer 1		
Question 2	Your mother's name.	
Answer 2		
Question 3	Your senior class teacher's na	me.
Answer 3		
	ок	Cancel

Figure 18-15 Verify by Security Question

18.7.3 Reset Password by Reserved Email

Before You Start

Ensure you have configured the reserved email when you are activating the device or editing the admin user account. (Refer to 18.6.3 Configure Reserved Email)

Step 1 On the user login interface, click Forgot Password.

Step 2 Select the password resetting type to Verify by Reserved Email.

Step 3 Click OK.

Step 4 Obtain the verification code. There are two ways to get the verification code.

- Use Guarding Vision app to scan the QR code.
- Send the QR code to email server.
- 1) Insert a USB flash drive to your device.
- 2) Click **Export** to export the QR code to USB flash drive.
- 3) Email the QR code to *pw_recovery@device-service.com* as attachment.



Figure 18-16 Verify by Reserved Email

Step 5 Check your reserved email, and you will receive a verification code within 5 minutes.

Step 6 Enter the verification code.

Step 7 Click **OK** to set the new password.

Chapter 19 Appendix

List of Applicable Power Adapter

Use only power supplies listed in the user instructions.

Power Adapter Model	Specifications	Manufacturer
MSA-C1500IC12.0-18P-DE	12 V, 1.5 A	0000201935
		MOSO Technology Co., Ltd.
ADS-25FSG-12 12018GPG	CE, 100 to 240 VAC, 12 V, 1.5 A, 18 W, Φ5.5 × 2.1 × 10	0000200174
		Shenzhen Honor Electronic
		Co., Ltd.
MSA-C1500IC12.0-18P-US	12 V, 1.5 A	0000201935
		MOSO Technology Co., Ltd.
TS-A018-120015AD	100 to 240 VAC, 12 V, 1.5 A, 18 W, Φ5.5 × 2.1 × 10	0000200878
		Shenzhen Transin
		Technologies Co., Ltd.
MSA-C2000IC12.0-24P-DE	12 V, 2 A	0000201935
		MOSO Technology Co., Ltd.
ADS-24S-12 1224GPG	CE, 100 to 240 VAC, 12 V, 2 A, 24 W, Φ2.1	0000200174
		Shenzhen Honor Electronic
		Co., Ltd.
MSA-C2000IC12.0-24P-US	US, 12 V, 2 A	0000201935
		MOSO Technology Co., Ltd.
ADS-26FSG-12 12024EPCU	US, 12 V, 2 A	0000200174
		Shenzhen Honor Electronic
		Co., Ltd.
KPL-040F-VI	12 V, 3.33 A, 40 W	0000203078
		Channel Well Technology Co.,
		Ltd.
MSA-Z3330IC12.0-48W-Q	12 V, 3.33 A	0000201935
		MOSO Technology Co., Ltd.
MSP-Z1360IC48.0-65W	48 V, 1.36 A	0000201935
		MOSO Technology Co., Ltd.
KPL-050S-II	48 V, 1.04 A	0000203078

	Channel Well Technology Co.,
	Ltd.



UD14618N