

Network Video Recorder

User Manual

Legal Information

About this Manual

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 of this Manual at the company website Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks Acknowledgement

Trademarks and logos mentioned are the properties of their respective owners.

The terms HDMI and HDMI High-Definition Multimedia Interface, and the HDMI Logo are trademarks or registered trademarks of HDMI Licensing Administrator, Inc. in the United States and other countries.

LEGAL DISCLAIMER

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". OUR COMPANY MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL OUR COMPANY BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF OUR COMPANY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS. YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND OUR COMPANY SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, OUR COMPANY WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.

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



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 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: <u>http://www.recyclethis.info</u>.



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: <u>http://www.recyclethis.info</u>.

Industry Canada ICES-003 Compliance

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

Applicable Model

This manual is applicable to the models listed in the following table.

Series	Model
DS-7900NXI-14/S	DS-7916NXI-I4/S
	DS-7932NXI-14/S
DS-7900NXI-I4/16P/S	DS-7916NXI-I4/16P/S
	DS-7932NXI-I4/16P/S
DS-7800NXI-12/S	DS-7808NXI-12/S
	DS-7816NXI-I2/S
DS-7800NXI-12/P/S	DS-7808NXI-I2/8P/S
	DS-7816NXI-I2/16P/S
DS-7700NXI-14/S	DS-7716NXI-I4/S
	DS-7732NXI-14/S
DS-7700NXI-I4/16P/S	DS-7716NXI-I4/16P/S
	DS-7732NXI-I4/16P/S
DS-7600NXI-12/S	DS-7608NXI-12/S
	DS-7616NXI-I2/S
DS-7600NXI-I2/8P/S	DS-7608NXI-I2/8P/S
	DS-7616NXI-I2/16P/S

Table 1-1 Applicable Model

Symbol Conventions

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

Symbol	Description	
Danger	Indicates a hazardous situation which, if not avoided, will or could result in death or serious injury.	
A Caution	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.	
i Note	Provides additional information to emphasize or supplement important points of the main text.	

Safety Instruction

- 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.
- Firmly connect the plug to the power socket. Do not connect several devices to one power adapter. Power off the device before connecting and disconnecting accessories and peripherals.
- Shock hazard! Disconnect all power sources before maintenance.
- The equipment must be connected to an earthed mains socket-outlet.
- The socket-outlet shall be installed near the equipment and shall be easily accessible.
- *indicates hazardous live and the external wiring connected to the terminals requires installation by an instructed person.*
- Never place the equipment in an unstable location. The equipment may fall, causing serious personal injury or death.
- Input voltage should meet the SELV (Safety Extra Low Voltage) and the LPS (Limited Power Source) according to the IEC60950-1.
- High touch current! Connect to earth before connecting to the power supply.
- 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.
- Use the device in conjunction with an UPS, and use factory recommended HDD if possible.
- This product contains a coin/button cell battery. If the battery is swallowed, it can cause severe internal burns in just 2 hours and can lead to death.
- This equipment is not suitable for use in locations where children are likely to be present.
- CAUTION: Risk of explosion if the battery is replaced by an incorrect type.
- Improper replacement of the battery with an incorrect type may defeat a safeguard (for example, in the case of some lithium battery types).
- Do not dispose of the battery into fire or a hot oven, or mechanically crush or cut the battery, which may result in an explosion.
- Do not leave the battery in an extremely high temperature surrounding environment, which may result in an explosion or the leakage of flammable liquid or gas.
- Do not subject the battery to extremely low air pressure, which may result in an explosion or the leakage of flammable liquid or gas.
- Dispose of used batteries according to the instructions.
- Keep body parts away from fan blades and motors. Disconnect the power source during servicing.
- Keep body parts away from motors. Disconnect the power source during servicing.

Preventive and Cautionary Tips

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

- The device is designed for indoor use only. Install it in a well-ventilated, dust-free environment without liquids.
- Ensure recorder is properly secured to a rack or shelf. Major shocks or jolts to the recorder as a result of dropping it may cause damage to the sensitive electronics within the recorder.
- The equipment shall not be exposed to dripping or splashing and that no objects filled with liquids shall be placed on the equipment, such as vases.
- No naked flame sources, such as lighted candles, should be placed on the equipment.
- The ventilation should not be impeded by covering the ventilation openings with items, such as newspapers, table-cloths, curtains, etc. The openings shall never be blocked by placing the equipment on a bed, sofa, rug or other similar surface.
- For certain models, ensure correct wiring of the terminals for connection to an AC mains supply.
- For certain models, the equipment has been designed, when required, modified for connection to an IT power distribution system.
- **(+)** identifies the battery holder itself and identifies the positioning of the cell(s) inside the battery holder.
- + identifies the positive terminal(s) of equipment which is used with, or generates direct current.
 + identifies the negative terminal(s) of equipment which is used with, or generates direct current.
- Keep a minimum 200 mm (7.87 inch) distance around the equipment for sufficient ventilation.
- For certain models, ensure correct wiring of the terminals for connection to an AC mains supply.
- Use only power supplies listed in the user manual or user instruction.
- The USB port of the equipment is used for connecting to a mouse, keyboard, USB flash drive, or Wi-Fi dongle only.
- Use only power supplies listed in the user manual or user instruction.
- Do not touch the sharp edges or corners.
- When the device is running above 45 °C (113 °F), or its HDD temperature in S.M.A.R.T. exceeds the stated value, please ensure the device is running in a cool environment, or replace HDD(s) to make the HDD temperature in S.M.A.R.T. below the stated value.

Contents

Chapte	er 1 Basic Operation	1
1.1	Activate Your Device	1
	1.1.1 Default User and IP Address	1
	1.1.2 Activate via Local Menu	1
	1.1.3 Activate via SADP	2
	1.1.4 Activate via Client Software	3
	1.1.5 Activate via Web Browser	6
1.2	Configure TCP/IP Settings	6
1.3	IR Remote Control Operations	8
	1.3.1 Pair (Enable) the IR Remote to a Specific NVR (optional)	8
	1.3.2 Unpair (Disable) an IR Remote from a NVR	9
1.4	HDD Settings 1	3
1.5	Add Network Camera 1	3
	1.5.1 Add Automatically Searched Online Network Camera 1	4
	1.5.2 Add Network Camera Manually 1	4
	1.5.3 Add Network Camera Through PoE 1	5
	1.5.4 Configure Customized Protocol 1	7
1.6	Platform Access 1	8
	1.6.1 Configure ISUP 1	8
	1.6.2 Configure Guarding Vision 2	0
Chapte	er 2 Camera Settings 2	1
2.1	Configure Image Parameters 2	1
2.2	Configure OSD Settings 2	1
2.3	Configure Privacy Mask 2	2
2.4	Import/Export IP Camera Configuration Files 2	3
2.5	Upgrade IP Cameras 2	4

Chapter 3 Live View 25
3.1 Start Live View 25
3.1.1 Configure Live View Settings 25
3.1.2 Configure Live View Layout 26
3.2 Configure Auto-Switch of Cameras 27
3.3 Configure Live View Layout 28
3.3.1 Configure Custom Live View Layout 28
3.3.2 Configure Live View Mode 28
3.4 Configure Channel-Zero Encoding 29
3.5 Digital Zoom 29
3.6 3D Positioning 30
3.7 Live View Strategy 30
3.8 Use an Auxiliary Monitor
3.9 Facial Recognition 31
3.10 PTZ Control 34
3.10.1 Configure PTZ Parameters 34
3.10.2 Set a Preset 34
3.10.3 Call a Preset 35
3.10.4 Set a Patrol 35
3.10.5 Call a Patrol 37
3.10.6 Set a Pattern
3.10.7 Call a Pattern 38
3.10.8 Set Linear Scan Limit 39
3.10.9 One-Touch Park 39
3.10.10 Auxiliary Functions 40
Chapter 4 Recording and Playback 41
4.1 Recording 41
4.1.1 Configure Recording Parameters 41

	4.1.2 Enable the H.265 Stream Access	43
	4.1.3 ANR	43
	4.1.4 Manual Recording	43
	4.1.5 Configure Plan Recording	44
	4.1.6 Configure Continuous Recording	45
	4.1.7 Configure Motion Detection Triggered Recording	46
	4.1.8 Configure Event Triggered Recording	46
	4.1.9 Configure Alarm Triggered Recording	46
	4.1.10 Configure Picture Capture	47
	4.1.11 Configure Holiday Recording	47
	4.1.12 Configure Redundant Recording and Capture	48
4.2	Playback	49
	4.2.1 Instant Playback	49
	4.2.2 Play Normal Video	50
	4.2.3 Play Smart Searched Video	51
	4.2.4 Play Custom Searched Files	51
	4.2.5 Play Tag Files	52
	4.2.6 Play by Sub-periods	53
	4.2.7 Play Log Files	54
	4.2.8 Play External Files	54
4.3	Playback Operations	55
	4.3.1 Normal/Important/Custom Video	55
	4.3.2 Set Play Strategy in Important/Custom Mode	55
	4.3.3 Edit Video Clips	55
	4.3.4 Switch between Main Stream and Sub-Stream	56
	4.3.5 Thumbnails View	56
	4.3.6 Fast View	56
	4.3.7 Digital Zoom	56

Chapter 5 Event 58
5.1 Normal Event Alarm
5.1.1 Configure Motion Detection Alarms 58
5.1.2 Configure Video Loss Alarms 58
5.1.3 Configure Video Tampering Alarms 59
5.1.4 Configure Sensor Alarms 59
5.1.5 Configure Exceptions Alarms 59
5.2 VCA Event Alarm
5.2.1 Temperature Screening 60
5.2.2 Loitering Detection 61
5.2.3 People Gathering Detection 62
5.2.4 Fast Moving Detection
5.2.5 Parking Detection
5.2.6 Unattended Baggage Detection 65
5.2.7 Object Removal Detection
5.2.8 Audio Exception Detection 68
5.2.9 Defocus Detection
5.2.10 Sudden Scene Change Detection
5.2.11 PIR Alarm 71
5.2.12 Thermal Camera Detection 71
5.2.13 Configure Queue Management 72
5.3 Configure Arming Schedule
5.4 Configure Linkage Actions
5.4.1 Configure Auto-Switch Full Screen Monitoring
5.4.2 Configure Audio Warning 74
5.4.3 Notify Surveillance Center 74
5.4.4 Configure Email Linkage
5.4.5 Trigger Alarm Output 75

5.4.6 Configure Audio and Light Alarm Linkage	75
5.4.7 Configure PTZ Linkage	75
Chapter 6 Smart Analysis	77
6.1 Engine Configuration	77
6.2 Face Picture Comparison	78
6.2.1 Face Grading Configuration	78
6.2.2 Face Capture	79
6.2.3 Face Picture Library Management 8	30
6.2.4 Face Picture Comparison Alarm 8	31
6.2.5 Face Picture Search 8	32
6.3 Perimeter Protection	35
6.3.1 Line Crossing Detection	35
6.3.2 Intrusion Detection 8	37
6.3.3 Region Entrance Detection 8	38
6.3.4 Region Exiting Detection 8	39
6.4 Human Body Detection) 0
6.4.1 Human Body Detection) 0
6.4.2 Human Body Search) 1
6.5 Multi-Target-Type Detection) 2
6.6 Vehicle Detection) 3
6.6.1 Configure Vehicle Detection) 3
6.6.2 Vehicle Search) 3
6.7 Target Detection) 4
6.8 People Counting) 5
6.9 Heat Map) 5
Chapter 7 File Management) 7
7.1 Search Files) 7
7.2 Export Files) 7

7.3 Smart Search
hapter 8 Storage
8.1 SSD Management
8.1.1 Initialize SSD
8.1.2 SSD S.M.A.R.T. Detection
8.1.3 Upgrade SSD Firmware
8.2 Manage Local HDD 99
8.2.1 Configure HDD Group 99
8.2.2 Configure the HDD Property 100
8.2.3 Configure the HDD Quota 101
8.3 Add a Network Disk 101
8.4 Manage eSATA 102
8.4.1 Configure eSATA for Data Storage 102
8.4.2 Configure eSATA for Auto Backup 103
hapter 9 POS Configuration 105
hapter 9 POS Configuration1059.1 Configure POS Connection105
9.1 Configure POS Connection 105
9.1 Configure POS Connection
9.1 Configure POS Connection1059.2 Configure POS Text Overlay1089.3 Configure POS Alarm109hapter 10 Hot Spare Recorder Backup11110.1 Set Hot Spare Device11110.2 Set Working Recorder112
9.1 Configure POS Connection1059.2 Configure POS Text Overlay1089.3 Configure POS Alarm109hapter 10 Hot Spare Recorder Backup11110.1 Set Hot Spare Device11110.2 Set Working Recorder11210.3 Manage Hot Spare System112
9.1 Configure POS Connection1059.2 Configure POS Text Overlay1089.3 Configure POS Alarm109hapter 10 Hot Spare Recorder Backup11110.1 Set Hot Spare Device11110.2 Set Working Recorder11210.3 Manage Hot Spare System112hapter 11 Network Settings114
9.1 Configure POS Connection1059.2 Configure POS Text Overlay1089.3 Configure POS Alarm109hapter 10 Hot Spare Recorder Backup11110.1 Set Hot Spare Device11110.2 Set Working Recorder11210.3 Manage Hot Spare System112hapter 11 Network Settings11411.1 Configure DDNS114
9.1 Configure POS Connection1059.2 Configure POS Text Overlay1089.3 Configure POS Alarm109hapter 10 Hot Spare Recorder Backup11110.1 Set Hot Spare Device11110.2 Set Working Recorder11210.3 Manage Hot Spare System112hapter 11 Network Settings11411.1 Configure DDNS11411.2 17.3 Configure PPPOE114

11.6 Configure Port 119
11.7 Configure ONVIF 121
Chapter 12 User Management and Security 122
12.1 Manage User Accounts 122
12.1.1 Add a User 122
12.1.2 Edit the Admin User 123
12.1.3 Edit an Operator/Guest User 124
12.2 Manage User Permissions 124
12.2.1 Set User Permissions 124
12.2.2 Set Live View Permission on Lock Screen 127
12.3 Configure Password Security 128
12.3.1 Export GUID File 128
12.3.2 Configure Security Questions 129
12.3.3 Configure Reserved Email 129
12.4 Reset Password
12.4 Reset Password 130
12.4 Reset Password 130 12.4.1 Reset Password by GUID 130
12.4 Reset Password
12.4 Reset Password13012.4.1 Reset Password by GUID13012.4.2 Reset Password by Security Questions13112.4.3 Reset Password by Reserved Email131
12.4 Reset Password13012.4.1 Reset Password by GUID13012.4.2 Reset Password by Security Questions13112.4.3 Reset Password by Reserved Email13112.4.4 Reset Password by Guarding Vision132
12.4 Reset Password13012.4.1 Reset Password by GUID13012.4.2 Reset Password by Security Questions13112.4.3 Reset Password by Reserved Email13112.4.4 Reset Password by Guarding Vision132Chapter 13 System Management133
12.4 Reset Password 130 12.4.1 Reset Password by GUID 130 12.4.2 Reset Password by Security Questions 131 12.4.3 Reset Password by Reserved Email 131 12.4.4 Reset Password by Guarding Vision 132 12.4.1 Reset Password by Guarding Vision 133 12.4.2 Reset Password by Reserved Email 131 12.4.3 Reset Password by Guarding Vision 132 13.1 Configure Device 133
12.4 Reset Password13012.4.1 Reset Password by GUID13012.4.2 Reset Password by Security Questions13112.4.3 Reset Password by Reserved Email13112.4.4 Reset Password by Guarding Vision132Chapter 13 System Management13313.1 Configure Device13313.2 Configure Time133
12.4 Reset Password13012.4.1 Reset Password by GUID13012.4.2 Reset Password by Security Questions13112.4.3 Reset Password by Reserved Email13112.4.4 Reset Password by Guarding Vision132Chapter 13 System Management13313.1 Configure Device13313.2 Configure Time13313.2.1 Manual Time Synchronization134
12.4 Reset Password13012.4.1 Reset Password by GUID13012.4.2 Reset Password by Security Questions13112.4.3 Reset Password by Reserved Email13112.4.4 Reset Password by Guarding Vision132Chapter 13 System Management13.1 Configure Device13313.2 Configure Time13313.2.1 Manual Time Synchronization13413.2.2 NTP Synchronization134
12.4 Reset Password 130 12.4.1 Reset Password by GUID 130 12.4.2 Reset Password by Security Questions 131 12.4.3 Reset Password by Reserved Email 131 12.4.4 Reset Password by Guarding Vision 132 Chapter 13 System Management 133 13.1 Configure Device 133 13.2 Configure Time 133 13.2.1 Manual Time Synchronization 134 13.2.2 NTP Synchronization 134 13.2.3 DST Synchronization 134

13.3.3 Export Network Packet	136
13.3.4 Network Resource Statistics	136
13.4 Storage Device Maintenance	137
13.4.1 Bad Sector Detection	137
13.4.2 S.M.A.R.T. Detection	138
13.4.3 HDD Health Detection	139
13.4.4 Configure Disk Clone	139
13.4.5 Repair Database	140
13.5 Upgrade Device	141
13.5.1 Upgrade by Local Backup Device	141
13.5.2 Upgrade by FTP	141
13.5.3 Upgrade by Web Browser	142
13.5.4 Upgrade by Guarding Vision	142
13.6 Import/Export Device Configuration Files	143
13.7 Log Management	143
13.7 Log Management	
	143
13.7.1 Log Storage	143 144
13.7.1 Log Storage 13.7.2 Search & Export Log Files	143 144 145
13.7.1 Log Storage 13.7.2 Search & Export Log Files 13.7.3 Upload Logs to the Server	143 144 145 145
 13.7.1 Log Storage 13.7.2 Search & Export Log Files 13.7.3 Upload Logs to the Server 13.7.4 One-Way Authentication 	143 144 145 145 146
 13.7.1 Log Storage	143 144 145 145 146 147
 13.7.1 Log Storage	143 144 145 145 146 147 147
 13.7.1 Log Storage	143 144 145 145 146 147 147 148
 13.7.1 Log Storage 13.7.2 Search & Export Log Files 13.7.3 Upload Logs to the Server 13.7.4 One-Way Authentication 13.7.5 Two-Way Authentication 13.8 Export Diagnostic Information 13.9 Restore Default Settings 13.10 Security Management 	143 144 145 145 146 147 147 148 148
 13.7.1 Log Storage 13.7.2 Search & Export Log Files 13.7.3 Upload Logs to the Server 13.7.4 One-Way Authentication 13.7.5 Two-Way Authentication 13.8 Export Diagnostic Information 13.9 Restore Default Settings 13.10 Security Management 13.10.1 RTSP Authentication 	143 144 145 145 146 147 147 148 148 149
 13.7.1 Log Storage 13.7.2 Search & Export Log Files 13.7.3 Upload Logs to the Server 13.7.4 One-Way Authentication 13.7.5 Two-Way Authentication 13.8 Export Diagnostic Information 13.9 Restore Default Settings 13.10 Security Management 13.10.1 RTSP Authentication 13.10.2 ISAPI Service 	143 144 145 145 146 147 147 148 148 149 149

14.1 Glossary 151
14.2 Frequently Asked Questions 152
14.2.1 Why is there a part of channels displaying "No Resource" or turning black screen in multi-screen of live view? 152
14.2.2 Why is the video recorder notifying not support the stream type? 153
14.2.3 Why is the video recorder notifying risky password after adding network camera?
14.2.4 How to improve the playback image quality?
14.2.5 How to confirm the video recorder is using H.265 to record video? 153
14.2.6 Why is the timeline at playback not constant? 154
14.2.7 When adding network camera, the video recorder notifies network is unreachable.
14.2.8 Why is the IP address of network camera being changed automatically? 154
14.2.9 Why is the video recorder notifying IP conflict? 154
14.2.10 Why is image getting stuck when the video recorder is playing back by single or multi-channel cameras?
14.2.11 Why does my video recorder make a beeping sound after booting?
14.2.12 Why is there no recorded video after setting the motion detection? 155
14.2.13 Why is the sound quality not good in recording video?

Chapter 1 Basic Operation

1.1 Activate Your Device

1.1.1 Default User and IP Address

- Default administrator account: admin.
- Default IPv4 address: 192.168.1.64.

1.1.2 Activate via Local Menu

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.

Steps

1. Enter the admin password twice.

admin	

Weak	

☑ Export GUID	?
Security Question Configuration	
Reserved E-mail Settings	?
Create Channel Default Password	
Note:Valid password range [8-16]. You duse a combination of numbers, lowerca: uppercase and special character for you password with at least two kinds of then contained.	se, ur

Figure 1-1 Activate via Local Menu

Warning

We highly recommend you to create a strong password of your own choosing (using a minimum of 8 characters, including at least three kinds of 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 change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

- 2. Enter the password to activate the IP cameras.
- 3. Optional: Check Export GUID, Security Question Configuration, or Reserved E-mail Settings.
- 4. Click OK.

iNote

- 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.

What to do next

- When you have enabled **Export GUID**, continue to export the GUID file to the USB flash driver for the future password resetting.
- When you have enabled **Security Question Configuration**, continue to set the security questions for the future password resetting.
- When you have enabled **Reserved E-mail Settings**, continue to set the reserved email for the future password resetting.

1.1.3 Activate via SADP

SADP software is used for detecting the online device, activating the device, and resetting its password.

Before You Start

Get the SADP software from the supplied disk or the official website, and install the SADP according to the prompts.

Steps

- 1. Connect your video recorder power supply to an electrical outlet and turn on it.
- **2.** Run the SADP software to search the online recorders.
- **3.** Check the recorder status from the device list, and select the inactive recorder.

	▲ Device Type	Status	IPv4 Address	Port	Software Version	IPv4 Gateway	HTTP Por	t Device Serial No.	
001	D5-409000-2	Active	10.16.6.20	8000	V5.335u3d 2008	10.16.6.254	80	D5-408162-2012014041304	
002	DS-KHE305-A	Active	10.16.6.21	8000	V5.3.0build 1008	10.16.6.254	80	D5-KHEND AUGUSTRUNCH	
003	D5-K2802X-AL	Active	10.16.6.213	8000	V5.1.0646 1012	10.16.6.254	N/A	D5-K2602X-A020141207V5	
004	DS-19408-F/K2G	Active	10.16.6.179	8000	VL0.53build 180	10.16.6.254	N/A	D5 (1960) (1970) (1970)	The device is not activated.
005	DS-15408-018NG	Active	10.16.6.127	8000	V2.276w34 1877	10.16.6.254	N/A	D5 DISH CONCIDENTIAL	
006	UNKOWN-DEVICE-TYPE	Active	10.16.6.250	8000	V5426u/id 1812	10.16.6.254	80	20141119CCW84903406798	
/	007	25-2CD	2025PWD	4	Inactiv	e	1	92.168.1.64	
009	D5-19508N-046/420W	^{Acti} Se	lect ina	activ	ve devic	e.	80	Di UKORA MENDONALDI	You can modify the network parameters after the device activation. Activate Now
						Inpu	t an	d confirm	New Password:

Figure 1-2 Activate via SADP

4. Create and input the new password in the password field, and confirm the password.

iNote

We highly recommend you to create a strong password of your own choosing (using a minimum of 8 characters, including at least three kinds of 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 change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

5. Click Activate.

1.1.4 Activate via Client Software

The client software is versatile video management software for multiple kinds of devices.

Before You Start

Get the client software from the supplied disk or the official website, and install the software according to the prompts.

Steps

1. Run the client software and the control panel of the software pops up, as shown below.

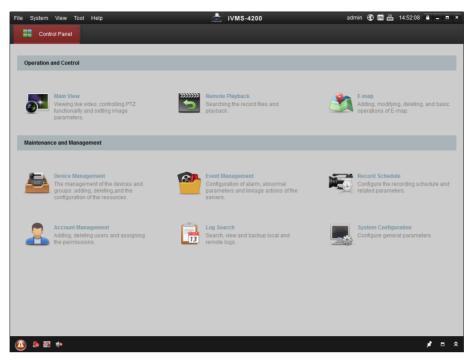


Figure 1-3 Control Panel

2. Click Device Management to enter the Device Management interface, as shown below.

			📥 iVMS-4200		admin 🐨	16:25:04	
📲 Control Panel 💆 De	evice Management						
Server 🗃 Group							
Organization	Device for Manag	gement (0)					
Encoding Device	Add Device	Modify De	elete Remote C VCA All	oca Activate	Refresh All	Filt	er
Add New Device Type	Nickname 🔺	IP	Device Serial No.		Security	Net Status	HDD Sta
	4)			
	Online Device (3)	Refresh Every 15s				
				set Password	Activate	Filter	
	Online Device (3			set Password	Activate	Filter	Ac
	Online Device (3	t 🗘 Add All	Modify Netinfo Re				
DVR/DVS/NVR/IPC/IPD/iVMS-4200	Online Device (3	t 🕀 Add All	Modify Netinfo Re Firmware Version XX Vx.x.xbuild xxxxxx Vx.x.xbuild xxxxxx	▼ Security	Server Port	Start time	:47 No
Encoding device: DVRDVSRVPAIPC/IPD/IVMS-4200 PCNVRV/VIS-4200 EncodeCard server	Online Device (3 Add to Clien IP 192.168.1.64	t Add All Device Type XX-XXXXXXXXXXX	Modify Netinfo Re Firmware Version XX Vx.x.xbuild xxxxxx	 Security Inactive 	Server Port 8000	Start time 2015-03-20 16:13:	51 Nc

Figure 1-4 Device Management Interface

- 3. Check the recorder status from the device list, and select an inactive recorder.
- 4. Click Activate to pop up the Activation interface.
- 5. Create a password and input the password in the password field, and confirm the password.

iNote

We highly recommend you to create a strong password of your own choosing (using a minimum of 8 characters, including at least three kinds of 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 change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

	Activation ×
User Name:	admin
Password:	•••••
	Strong
	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.
Confirm New Password	d: ••••••
	Ok Cancel

Figure 1-5 Activation

- 6. Click OK to start activation.
- 7. Click Modify Netinfo to pop up the Network Parameter Modification interface, as shown below.

	Modify Network Parameter	×
Device Information: MAC Address: Software Version: Device Serial No.: Network Information:	XX-XX-XX-XX-XX Vx.x.xbuild xxxxxx Xx-XXXXXXXXXXXXXXXXXXXXXXXXXXXXX	Сору Сору Сору
Port: ✓ IPv4(Enable) IP address: Subnet Mask: Gateway: ↓ IPv6(Disable) Password:	8000 192.168.1.64 255.255.255.0 192.168.1.1	
rassworu.	ОК	Cancel

Figure 1-6 Modify Network Parameters

- 8. Change the recorder IP address to the same subnet with your computer.
 - Modify the IP address manually.
 - Check Enable DHCP.
- 9. Input the password to activate your IP address modification.

1.1.5 Activate via Web Browser

You can get access to the recorder via web browser. You may use one of the following listed web browsers: Internet Explorer 6.0 and above, Apple Safari, Mozilla Firefox, and Google Chrome. The supported resolutions include 1024*768 and above.

Steps

1. Enter the IP address in web browser, and then press Enter.

tivation		
User Name	admin	
Password	•••••	Strong
	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.	Strong
Confirm	• • • • • • • • • • • •]
		ОК

Figure 1-7 Web Browser Activation

2. Set the password for the admin user account.

iNote

We highly recommend you to create a strong password of your own choosing (using a minimum of 8 characters, including at least three kinds of 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 change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

3. Click OK.

1.2 Configure TCP/IP Settings

TCP/IP settings must be properly configured before operating your over a network. Both IPv4 and IPv6 are available.

Steps

```
1. Go to System → Network → TCP/IP .
```

Working Mode	Net Fault-Tolerance +		
Select NIC	bond0 ~		
NIC Type	10M/100M/1000M Self-adaptiv		
IPv4 IPv6	3		
Enable DHCP			
IPv4 Address	0.01.001.00	Enable Obtain DNS Se.	
IPv4 Subnet Mas	k 🐻 . 📾 . 📾 . 🍙	Preferred DNS Server	(21.18)
IPv4 Default Gat	eway D. L	Alternate DNS Server	
MAC Address			
MTU(Bytes)	1500	If MTU is less than 1280, IPv6 related functions will be unave	silable.
Main NIC	LAN1 -		
Annha			
Apply			

Figure 1-8 TCP/IP Settings

2. Select Working Mode as Net-Fault Tolerance or Multi-Address Mode.

Net-Fault Tolerance

The two NIC cards use the same IP address, and you can select the main NIC to LAN1 or LAN2. In this way, in case of one NIC card failure, the device will automatically enable another standby NIC card so as to ensure the normal running of the system.

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. Select one NIC card as the default route. When the system connects with the extranet, the data will be forwarded through the default route.

- 3. Click IPv4 or IPv6 as you required.
- **4. Optional:** Check **Enable DHCP** to obtain IP settings automatically if a DHCP server is available on the network.
- 5. Set related parameters.

iNote

Valid MTU value range is from 500 to 1500.

6. Click Apply.

1.3 IR Remote Control Operations

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

iNote

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

The IR Remote is set at the factory to control the NVR (using default Device ID# 255) without any additional steps. Device ID# 255 is the default universal device identification number shared by the NVRs. You may also pair an IR Remote to a specific NVR by changing the Device ID#, as follows:

1.3.1 Pair (Enable) the IR Remote to a Specific NVR (optional)

You can pair an IR Remote to a NVR by creating a user-defined Device ID#. This feature is useful when using multiple IR Remotes and NVRs.

Steps

- 1. On the NVR:
 - 1) Go to General \rightarrow More Settings .
 - 1) Type a number (255 digits maximum) into the Device No. field.
- 2. On the IR Remote:
 - 1) Press DEV.
 - 1) Use the Number buttons to enter the Device ID# that was entered into the NVR.
 - 2) Press Enter button to accept the new Device ID#.

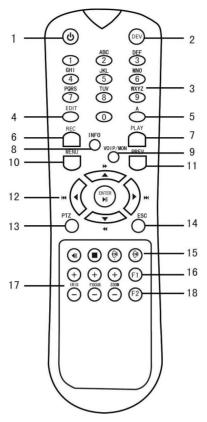


Figure 1-9 Remote Control

1.3.2 Unpair (Disable) an IR Remote from a NVR

To unpair an IR Remote from a NVR so that the unit cannot control any NVR functions, proceed as follows: Press the DEV key on the IR Remote. Any existing Device ID# will be erased from the unit's memory and it will no longer function with the NVR.

iNote

(Re)-enabling the IR Remote requires pairing to a NVR. See "Pair the IR Remote to a Specific NVR (optional)" above.

The keys on the remote control closely resemble the ones on the front panel.

Table 1-1 IR Remote Description

No.	Name	FunctionDescription
1	POWER ON/OFF	To Turn Power On:

No.	Name	FunctionDescription
		 If User Has Not Changed the Default NVR Device ID# (255): a. Press Power On/Off button (1). If User Has Changed the NVR Device ID#: a. Press DEV button. b. Press Number buttons to enter user-defined Device ID#. c. Press Enter button. d. Press Power button to start device.
		 To Turn NVR Off: If User Is Logged On: a. Hold Power On/Off button (1) down for five seconds to display the "Yes/No" verification prompt. b. Use Up/Down Arrow buttons (12) to highlight desired selection. c. Press Enter button (12) to accept selection.
		 If User Is Not Logged On: a. Hold Power On/Off button (1) down for five seconds to display the user name/password prompt. b. Press the Enter button (12) to display the on-screen keyboard. c. Input the user name. d. Press the Enter button (12) to accept input and dismiss the on-screen keyboard. e. Use the Down Arrow button (12) to move to the "Password" field. f. Input password (use on-screen keyboard or numeric buttons (3) for numbers). g. Press the Enter button (12) to accept input and dismiss the on-screen keyboard.
		 h. Press the OK button on the screen to accept input and display the Yes/No" verification prompt (use Up/Down Arrow buttons (12) to move between fields) i. Press Enter button (12) to accept selection. User name/password prompt depends on NVR is configuration. See "System Configuration" section.
2	DEV	Enable IR Remote: Press DEV button, enter NVR Device ID# with number keys, press Enter to pair unit with the NVR.

No.	Name	FunctionDescription
		Disable IR Remote: Press DEV button to clear Device ID#; unit will no longer be paired with the NVR.
3	Numerals	Switch to the corresponding channel in Live View or PTZ Controlmode
		Input numbers in Editmode
4	EDIT	Delete characters beforecursor
		Check the checkbox and select the ON/OFFswitch
5	A	Adjust focus in the PTZ Controlmenu
		Switch on-screen keyboards (upperand lower case alphabet, symbols, and numerals)
6	REC	Enter Manual Record settingmenu
		Call a PTZ preset by using the numericbuttons in PTZ control settings
		Turn audio on/off in Playbackmode
7	PLAY	Go to Playback mode
		Auto scan in the PTZ Controlmenu
8	INFO	Reserved
9	VOIP	Switches between main and spot output
		Zooms out the image in PTZ control mode
10	MENU	Return to Main menu (after successful login)
		N/A
		Show/hide full screen in Playback mode
11	DIRECTION	Navigate between fields and menu items
		Use Up/Down buttons to speed up/slow down recorded video, and Left/Right buttons to advance/rewind 30 secs in Playback mode
		Cycle through channels in Live View mode
		Control PTZ camera movement in PTZ control mode
12	ENTER	Confirm selection in any menu mode
		Checks checkbox
		Play or pause video in Playback mode

No.	Name	FunctionDescription
		Advance video a single frame in single-frame Playback mode
		Stop/start auto switch in auto-switch mode
13	PTZ	Enter PTZ Controlmode
14	ESC	Go back to previous screen
		N/A
15	RESERVED	Reserved
16	F1	Select all items on a list
		N/A
		Switch between play and reverseplay in Playback mode
17	PTZ Control	Adjust PTZcamera iris, focus, and zoom
18	F2	Cycle through tabpages
		Switch between channels in Synchronous Playback mode

Troubleshooting Remote Control

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:

- Batteries are installed correctly and the polarities of the batteries are not reversed.
- Batteries are fresh and not out of charge.
- IR receiver is not obstructed.
- No fluorescent lamp is used nearby.

If the remote still can't function properly, please change a remote and try again, or contact the device provider.

Steps

iNote

- Make sure you have installed batteries properly in the remote control. And you have to aim the remote control at the IR receiver in the front panel.
- If there is no response after you press any button on the remote, follow the procedure below to troubleshoot.
- Go to Menu → Settings → General → More Settings by operating the front control panel or the mouse.
- **2.** Check and remember NVR ID#. The default ID# is 255. This ID# is valid for all the IR remote controls.

- 3. Press DEV on the remote control.
- **4.** Enter the NVR ID# you set in step 2.
- 5. PressENTER on the remote.

1.4 HDD Settings

Ensure the video recorder storage media is well. You can install at least one HDD and initialize it.

1.5 Add Network Camera

Before you can get live video or record the video files, you must 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 been activated.

Steps

- 2. Click Custom Add tab on the title bar.

Add IP Camera (Custom)		\times
IP Camera Address	110.110.1.11	
Protocol	ONVIF	~
Management Port	80	
Transfer Protocol	Auto	-
User Name	admin	
Password	*****	
	Continue to A	dd Add

Figure 1-10 Add IP Camera

- **3.** Enter IP address, protocol, management port, and other IP camera information to add.
- 4. Enter the login user name and password of the IP camera.
- 5. Click Add to finish the adding of the IP camera.
- 6. Optional: Click Continue to Add to continue to add additional IP cameras.

1.5.1 Add Automatically Searched Online Network Camera

Steps

- **1.** Click con the main menu.
- 2. Click Number of Unadded Online Device at the bottom.
- **3.** Select the automatically searched online network cameras.
- 4. Click Add to add the camera which has the same login password with the video recorder.

1	:	≈ ☆						
+ Ad	d G	Refresh	P Activate				Enter a keyv	vord.
	No.	Status	Security	IP Address	Edit	Device Model	Protocol	Management
	1		Active	10.15.1.10		DS-2CD4112F-I	HIKVISION	8000

Figure 1-11 Add Automatically Searched Online Network Camera

iNote

If the network camera to add has not been activated, you can activate it in the network camera list of camera management interface.

1.5.2 Add Network Camera Manually

Before you view live video or record video files, you must add network cameras to the device.

Before You Start

Ensure the network connection is valid and correct, and the network camera is activated.

Steps

- **1.** Click con the main menu.
- 2. Click Custom Adding.
- **3.** Set **IP Camera Address**, **Protocol**, **Management Port**, **Transfer Protocol**, **User Name**, and **Password**. Management port ranges from 1 to 65535.

Add IP Camera (Custom)			×
No. Stat Sec	urity IP Address	Device Mo	del Proto
IP Camera Address			
Protocol	HIKVISION		•
Management Port	8000		
Transfer Protocol	Auto		-
User Name	admin		
Password			
Use Channel Defaul			
Use Default Port			
Verify Certificate			
	Search	Continue to Add	Add

Figure 1-12 Add Network Camera

- 4. Optional: Check Use Channel Default Password to use the default password to add the camera.
- **5. Optional:** Check **Use Default Port** to use the default management port to add the camera. For SDK service, the default port value is 8000. For enhanced SDK service, the default value is 8443.

iNote

The function is only available when you use HIKVISION protocol.

6. Optional: Check **Verify Certificate** to verify the camera with certificate. The certificate is a form of identification for the camera that provides more secure camera authentication. It requires to import the network camera certificate to the device first when you use this function. For details, refer to .

iNote

The function is only available when you use HIKVISION protocol.

- 7. Click Add.
- 8. Optional: Check Continue to Add to add other network cameras.

1.5.3 Add Network Camera Through PoE

The PoE interfaces enable the device system to pass electrical power safely, along with data, on Ethernet cabling to the connected PoE cameras. Supported PoE camera number varies with device module. If you disable the PoE interface, you can also connect to the online network cameras. And the PoE interface supports the Plug-and-Play function.

Add PoE Camera

Steps

- **1.** Go to Camera \rightarrow Camera \rightarrow PoE Settings .
- 2. Enable or disable long network cable mode by selecting Long Distance or Short Distance.

Long Distance

Long-distance (100 to 300 meters) network transmissions via PoE interface.

Short Distance

Short-distance (< 100 meters) network transmission via PoE interface.

iNote

- The PoE ports are enabled with the short distance mode by default.
- The bandwidth of IP camera connected to the PoE via long network cable (100 to 300 meters) cannot exceed 6 MP.
- The allowed max. long network cable may be less than 300 meters depending on different IP camera models and cable materials.
- When the transmission distance reaches 100 to 250 meters, you must use the CAT5E or CAT6 network cable to connect with the PoE interface.
- When the transmission distance reaches 250 to 300 meters, you must use the CAT6 network cable to connect with the PoE interface.
- Refer to the Appendix 20.3 List of IP Cameras Connected to PoE by Long Network Cable (100 300 m) for the list of IP cameras.

Channel	CLong Distance	⊖Short Distance	Channel Status	Actual Power
D1	۲	0	Disconnected	0.0W
D2		۲	Disconnected	0.0W
D5		۲	Disconnected	0.0W
D6		۲	Disconnected	0.0W
D7		۲	Disconnected	0.0W
08		۲	Disconnected	0.0W
D9		۲	Disconnected	0.0VV
D10		۲	Disconnected	0.0W
D11		۲	Disconnected	0.0W
D12		۲	Disconnected	0.0W
D13		۲	Disconnected	0.0W
D14		۲	Disconnected	0.0W
D15		۲	Disconnected	0.0VV
D16		۲	Disconnected	0.0W

Figure 1-13 Add PoE Camera

- 3. Click Apply.
- **4.** Connect PoE cameras to device PoE ports with network cables.
- 5. Go to Camera \rightarrow Camera \rightarrow IP Camera to view camera image and information.

Add Non-PoE Network Camera

You can disable the PoE interface by selecting the manual while the current channel can be used as a normal channel and the parameters can also be edited.

Steps

- **1.** Go to Camera \rightarrow Camera \rightarrow IP Camera .
- 2. Position the cursor on a window with no linked network camera and click $\underline{\mathbb{Z}}$.

Edit IP Camera			\times
IP Camera No	D1		
Adding Method	Manual	~	
IP Camera Address	192.168.254.2		
Protocol	HIKVISION	-	
Management Port	8000		
Channel Port	1	-	
Transfer Protocol	Auto	~	
User Name	admin		
Password			
		OK	(

Figure 1-14 Edit Network Camera

3. Select Adding Method as Manual.

Plug-and-Play

The camera is physically connected to the PoE interface. Its parameters cannot be edited. You can go to **System** \rightarrow **Network** \rightarrow **TCP/IP** to change IP address of PoE port.

Manual

Add IP camera without physical connection via network.

- 4. Enter IP address, User Name, and Password.
- 5. Click OK.

1.5.4 Configure Customized Protocol

To connect network cameras which are not configured with the standard protocols, you can configure the customized protocols for them. The system provides 16 customized protocols.

Steps

1. Go to **More Settings** \rightarrow **Protocol** .

Custom Protocol	Custom Protocol 1		-		
Protocol Name	Custom 1				
Stream Type	✓ Main Stream		Sub Str	eam	
Туре	RTSP	•	RTSP	•	
Transfer Protocol	Auto	•	Auto	•	
Port	554		554		
Path					
	Example: [Type]:/ rtsp://192.168.0.1				

Figure 1-15 Protocol Management

2. Set protocol parameters.

Туре

The network camera adopting custom protocol must support getting stream through standard RTSP.

Path

Contact the manufacturer of network camera for the URL (Uniform Resource Locator) of getting main stream and sub-stream.

iNote

The protocol type and the transfer protocol must be supported by the network camera to add.

3. Click OK.

After adding the customized protocol, you can see it in **Protocol**.

1.6 Platform Access

1.6.1 Configure ISUP

SDK is based on Intelligent Security Uplink Protocol (ISUP). It provides APIs, library files, and commands for the third-party platform to access devices such as NVRs, speed domes, DVRs, network cameras, mobile NVRs, mobile devices, decoding devices, etc. With this protocol, the third-party platform can realize functions like live view, playback, two-way audio, PTZ control, etc.

Steps

```
1. Go to System → Network → Advanced → Platform Access .
```

Access Type	ISUP -
Enable	
Server Address	
Server Port	7660
Registration Status	Offline
Device ID	720251740
Version	ISUP5.0 -
Encryption Password	******

Figure 1-16 ISUP Settings

2. Select Access Type as ISUP.

3. Check Enable.

iNote

Enabling ISUP will disable other platform access.

4. Set the related parameters.

Server Address

The platform server IP address.

Server Port

The platform server port, ranges from 1024 to 65535. The actual port shall be provided by the platform.

Device ID

Device ID shall be provided by the platform.

Version

ISUP protocol version, only V5.0 is available.

Encryption Password

Encryption password is required when using ISUP V5.0 version, it provides more secure communication between the device and platform. Enter it for verification after the device is registered to the ISUP platform. It cannot be empty, or "ABCDEF".

5. Click Apply to save the settings and restart the device.

What to do next

You can see the registration status (online or offline) after the device is restarted.

1.6.2 Configure Guarding Vision

Guarding Vision enables the mobile phone application and the service platform page (dev.guardingvision.com) to access and manage your connected NVR, providing a convenient remote access to the surveillance system.

Steps

- **1.** Go to System \rightarrow Network \rightarrow Advanced \rightarrow Platform Access .
- 2. Check Enable to activate the function. Then the service terms will pop up.
 - 1) Enter 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 with the service terms and privacy statement.
 - 4) Click **OK**.

i Note

- 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.
- Check Time Sync, the device will sync time with Hik-Connect instead of NTP server.
- 3. Optional: Configure following parameters.
 - Check Custom and enter Server Address as your desire.
 - Check **Enable Stream Encryption**, then verification code is required for remote access and live view.
- 4. Bind your device with a Guarding Vision account.
 - 1) Use a smart phone to scan the QR code on the device to download Guarding Vision.
 - 2) Use Guarding Vision to scan the device QR, and bind the device.

iNote

If the device is already bound with an account, you can click **Unbind** to unbind with the current account.

5. Click Apply.

What to do next

You can access and manage your video recorder through Guarding Vision app or .

Chapter 2 Camera Settings

2.1 Configure Image Parameters

You can customize image parameters, including day/night switch, backlight, contrast, and saturation in **Camera** \rightarrow **Display**.

Image Settings

Customize the image parameters including brightness, contrast, and saturation.

Exposure

Set the camera exposure time (1/10000 to 1 sec). A larger exposure value results in a brighter image.

Day/Night Switch

Set the camera to day, night, or auto switch mode according to time or the surrounding illumination condition. When the light diminishes at night, the camera can switches to night mode with high quality black and white image.

Backlight

Set the camera's wide dynamic range (0 to 100). When the surrounding illumination and the object have large differences in brightness, you can set the WDR value to balance the brightness level of the whole image.

Image Enhancement

For optimized image contrast enhancement that reduces noise in video stream.

2.2 Configure OSD Settings

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

- **1.** Go to **Camera** \rightarrow **Display** .
- **2.** Select a camera as your desire.
- 3. Edit name in Camera Name.
- 4. Check Display Name, Display Date and Display Week to show the information on the image.
- 5. Set the date format, time format, and display mode.

Camera	[D2] IPdome	•			
Camera Name	IPdome		OSD Settings		\sim
08-28-2017 Mon 16 .	: 32 : 45		 Display Name Display Date Display Week Date Format Time For Display M OSD Font 	MM-DD-YYYY 24-hour Non-Transparent & No 16x16	•
		Camera 01	Image Settings Exposure		>
			Day/Night Switch		>
			Backlight		>
			Image Enhancement	1	>
	_				

Figure 2-1 OSD Configuration Interface

- 6. Drag the text frame on the preview window to adjust the OSD position.
- 7. Click Apply.

2.3 Configure Privacy Mask

The privacy mask protects personal privacy by concealing parts of the image from kive view or recording with a masked area.

- **1.** Go to Camera → Privacy Mask .
- 2. Select a camera to set privacy mask.
- 3. Check Enable.
- 4. Draw a zone on the window. The zone will be marked by different frame colors.

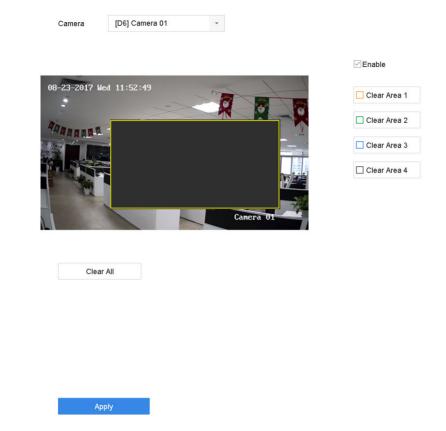


Figure 2-2 Privacy Mask Settings Interface

iNote

- Up to 4 privacy masks zones can be configured and the size of each area can be adjusted.
- You can clear the configured privacy mask zones on the window by clicking the corresponding clear zone 1 to 4 icons on the right of the window, or click **Clear All** to clear all zones.
- 5. Click Apply.

2.4 Import/Export IP Camera Configuration Files

The IP camera information, including the IP address, manage port, password of admin, etc., can be saved in Microsoft Excel format and backed up to the local device. The exported file can be edited on a PC, including adding or deleting the content, and copying the setting to other devices by importing the Excel file to it.

Before You Start

When importing the configuration file, connect the storage device that contains the configuration file to the device.

Steps

1. Go to Camera → IP Camera Import/Export .

- 2. Click IP Camera Import/Export, and the detected external device contents appear.
- 3. Export or import the IP camera configuration files.
 - Click **Export** to export the configuration files to the selected local backup device.
 - To import a configuration file, select the file from the selected backup device and click **Import**.

iNote

After the importing process is completed, you must reboot the device to activate the settings.

2.5 Upgrade IP Cameras

The IP camera can be remotely upgraded through the device.

Before You Start

Ensure you have inserted the USB flash drive to the device, and it contains the IP camera upgrade firmware.

Steps

- 1. On the camera management interface, select a camera.
- 2. Go to More Settings \rightarrow Upgrade .
- **3.** Select the firmware upgrade file from the USB flash drive.
- 4. Click Upgrade.

The IP camera will reboot automatically after the upgrading completes.

Chapter 3 Live View

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

3.1 Start Live View

- 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.

3.1.1 Configure Live View Settings

Live View settings can be customized. 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.

Steps

1. Go to System \rightarrow Live View \rightarrow 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 3-1 Live View-General

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 wait between switching of cameras when using auto-switch in Live View.

Enable Audio Output

Enable/disable audio output for the selected video output.

Volume

Adjust the Live View volume, 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.

3. Click OK.

3.1.2 Configure Live View Layout

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

Configure Custom Live View Layout

Steps

- **1.** Go to **System** \rightarrow **Live View** \rightarrow **View**.
- 2. Click Set Custom Layout.
- **3.** Click on the Custom Layout Configuration interface.
- 4. Edit the layout name.
- 5. Select a window division mode from the toolbar.

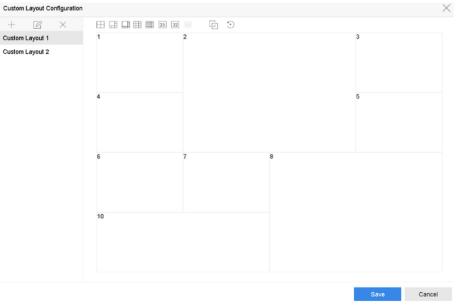


Figure 3-2 Configure Live View Layout

- 6. Select multiple windows and click 🗁 to joint the windows. The selected windows must be in rectangle area.
- 7. Click Save.

The successfully configured layout is displayed in the list.

8. Optional: Select a live view layout from the list and click *□* to edit the name, or click × to delete the name.

Configure Live View Mode

Steps

- **1.** Go to System \rightarrow Live View \rightarrow View .
- **2.** Select the video output interface.
- **3.** Select a layout or custom layout from the toolbar.
- **4.** Select a division window, and double-click on a camera in the list to link the camera to the window.

iNote

- You can also click-and-drag the camera to the desired window on the Live View interface to set the camera order.
- You can enter the number in the text field to quickly search the camera from the list.

5. Click Apply.

6. Optional: Click \Box to start live view for all channels, or click \Box to stop all live view channels.

3.2 Configure Auto-Switch of Cameras

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

Steps

- 1. Go to System → Live View → General .
- 2. Set 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 auto-switch. The range is from 5s to 300s.

- 3. Go to View Settings to set the view layout.
- 4. Click OK to save the settings.

3.3 Configure Live View Layout

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

3.3.1 Configure Custom Live View Layout

Steps

- 1. Go to System \rightarrow Live View \rightarrow View .
- 2. Click Set Custom Layout.
- **3.** Click on the Custom Layout Configuration interface.
- 4. Edit the layout name.
- 5. Select a window division mode from the toolbar.

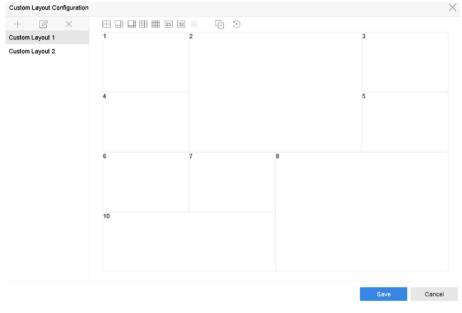


Figure 3-3 Configure Live View Layout

- 6. Select multiple windows and click 📄 to joint the windows. The selected windows must be in rectangle area.
- 7. Click Save.

The successfully configured layout is displayed in the list.

8. Optional: Select a live view layout from the list and click *□* to edit the name, or click × to delete the name.

3.3.2 Configure Live View Mode

- 1. Go to System \rightarrow Live View \rightarrow View .
- **2.** Select the video output interface.

- 3. Select a layout or custom layout from the toolbar.
- **4.** Select a division window, and double-click on a camera in the list to link the camera to the window.

iNote

- You can also click-and-drag the camera to the desired window on the Live View interface to set the camera order.
- You can enter the number in the text field to quickly search the camera from the list.

5. Click Apply.

6. Optional: Click \Box to start live view for all channels, or click \Box to stop all live view channels.

3.4 Configure Channel-Zero Encoding

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

Steps

- 1. Go to System → Live View → Channel-Zero .
- 2. Check Enable Channel-Zero Encoding.

Frame Rate	Full Frame	-
Max. Bitrate Mode	General	
Max. Bitrate(Kbps)	1792	

Figure 3-4 Channel-Zero Encoding

- **3.** Configure **Frame Rate**, **Max. Bitrate Mode**, and **Max. Bitrate**. A higher frame rate and bitrate require higher bandwidth.
- 4. Click Apply.

You can view all the channels on one screen via CMS or web browser.

3.5 Digital Zoom

Digital Zoom zooms into the live image in different magnifications (1x to 16x).

- 1. Start live view, click $\, \oplus \,$ from the toolbar.
- 2. Move the sliding bar or scroll the mouse wheel to zoom in/out the image to different magnifications (1x to 16x).



Figure 3-5 Digital Zoom

3.6 3D Positioning

3D Positioning zooms in/out a specific live image area.

Steps

- 1. Start live view, and click 🐻 .
- **2.** Zoom in/out the image.
 - Zoom in: Click on the desired position in the video image and drag a rectangle area in the lower right direction to zoom in.
 - Zoom out: Drag a rectangle area in the upper left direction to move the position to the center and enable the rectangle area to zoom out.

3.7 Live View Strategy

Steps

In the live view mode, click = to enter the digital zoom operation interface in full screen mode.
 Select the live view strategy to **Beal time**. **Belanced** or **Elyange**.

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

3.8 Use an Auxiliary Monitor

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

iNote

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

3.9 Facial Recognition

You can enter facial recognition interface to view real-time facial recognition results.

Before You Start

Ensure you have configured facial detection and face picture comparison function, refer to *Face Picture Comparison* for details.

- 1. Go to live view interface, and click 💽 in toolbar.
- **2.** Click □, □, or ⊞ to set window division.
- **3.** Select a window as you desired.
- **4.** Double click a camera from the camera list on the left bottom.



Figure 3-6 Facial Recognition

- **5.** Click **Records** to view the real-time facial recognition records of selected camera. The records will also be shown in the window on the right. You can view the facial detection number at the top, including the total number, succeeded number and failed number.
- **6. Optional:** For the unregistered face picture, you can double click it in records list, and add it to face picture library.

ĨiNote

For guest and operator user, it requires Local Parameters Settings permission to add unregistered face picture to face picture library.

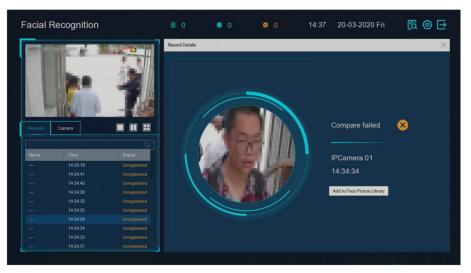


Figure 3-7 Add Unregistered Face Picture

7. Optional: Click on the upper right corner to configure the display settings as you desired.

Theme Facial Recognition Successful Face Pict Display Hide Picture to Show when Captured Library Picture Failed Face Picture C Display Hide Hide Picture C Display Hide Hide Picture C Display Hide Hide Picture C Display Hide Picture C Picture C	Display Settings	\times
Successful Face Pict Display Hide Picture to Show when Captured Library Picture		
Picture to Show when Captured Library Picture	Theme Facial Recognition	
	Successful Face Pict Display Hide	
Failed Face Picture C Oisplay Hide	Picture to Show when Captured Library Picture	
	Failed Face Picture C Display Hide	
OK Cancel		

Figure 3-8 Facial Recognition Display Settings

- **8. Optional:** Click **on** the upper right corner to search and export record.
 - 1) Set the search parameters as you desired.
 - 2) Click Search.
 - 3) Click Export Attendance Record or Export Check-in Record.

iNote

- Ensure you have inserted USB flash drive before export.
- You can click a record to review the attendance information of this individual in calendar.
- For guest and operator user, it requires "Local Video Export permission" (in "Camera Permission") to search and export record.

1 2 3 4 6 7 8 9 9 9 0 10 11 2 2 12	Q Library	Export Attendance Re	Export Check-in Re	cord				1						
1 1 2 2 3 3 4 4 5 5 6 6 7 7 8 9 9 9 10 10 111 11 12 12	Library										Ch	ack		hec
1 1 2 2 3 3 4 4 5 5 6 6 7 7 8 9 9 9 10 10 11 11 12 12	Library										1		0	
1 1 2 2 3 3 4 4 5 5 6 6 7 7 8 9 9 9 10 10 11 11 12 12			al (D Late (Day)	Leave Earl	Absence (Checked i	Unchecke	Norm				0	Abse	ence
2 2 3 3 4 4 5 5 6 6 7 7 8 8 9 9 9 9 10 10 11 12 12	test1	0	1	0	0	1	0	0	0		1		0	
3 3 4 4 5 5 6 6 7 7 8 8 9 9 10 10 11 11 12 12	test1	0	1	0	0	1	0			20	18 Jur	1		
4 4 5 5 6 6 7 7 7 8 8 9 9 10 10 11 11 12 12	test1	0	1	0	0	1	0	s	м	т	w	т	F	s
5 5 6 6 7 7 8 8 9 9 10 10 11 11 12 12	test1	0	1	0	0	1	0						1	2
6 6 7 7 8 8 9 9 10 10 11 11 12 12	test1	0	1	0	0	1	0							
7 7 8 8 9 9 10 10 11 11 12 12	test1	0	1	0	0	1	0	3	4	5	6	7	8	9
9 9 10 10 11 11 12 12	test1	0	1	0	0	1	0	10	11	12	13	14	15	16
9 9 10 10 11 11 12 12	test1	0	1	0	0	1	0	17	18	19	20	21	22	23
10 10 11 11 12 12	test1	0	1	0	0	1	0	24	25	26	27	28	29	30
11 11 12 12	test1	0	1	0	0	1	0	24				20	20	00
12 12	test1	0	1	0	0	1	0							
	test1	0	1	0	0	1	0							
	test1	0	1	0	0	1	0							
14 14	test1	0	1	0	0	1	0							
15 15	test1	0	1	0	0	1	0							
16 16	test1	0	1	0	0	1	0							
47 47	test4	0		0	0									

Figure 3-9 Face Recognition Search Record

3.10 PTZ Control

3.10.1 Configure PTZ Parameters

Follow these procedures to set the PTZ parameters. The PTZ parameters configuration must be done before you can control the PTZ camera.

Steps

- **1.** Click $\[the expansion]$ on the quick settings toolbar of the PTZ camera's Live View.
- 2. Click PTZ Parameters Settings to set the PTZ parameters.

PTZ Parameter Se	tings		\times
Baud Rate	9600		Ψ.
Data Bit	8		~
Stop Bit	1		~
Parity	None		~
Flow Ctrl	None		~
PTZ Protocol	PELCO-C		•
Address	0		
Address range: 0~	255		
		ОК	Cancel

Figure 3-10 PTZ Parameters Settings

3. Edit the PTZ parameters.

iNote

All the parameters should be exactly match the PTZ camera parameters.

4. Click OK to save the settings.

3.10.2 Set a Preset

Presets record the PTZ position and the status of zoom, focus, iris, etc.You can call a preset to quickly move the camera to the predefined position.

- **1.** Click $\[the]$ on the quick settings toolbar of the PTZ camera's live view.
- 2. Click directional buttons to wheel the camera to a location.
- 3. Adjust the zoom, focus and iris status.
- 4. Click in the lower right corner of Live View to set the preset.

1 - Preset 1	Call	Apply	Cancel	
--------------	------	-------	--------	--

Figure 3-11 Set Preset

- 5. Select the preset No. (1 to 255) from the drop-down list.
- 6. Enter the preset name.
- 7. Click Apply to save the preset.
- 8. Optional: Click Cancel cancel the location information of the preset.
- **9. Optional:** Click in the lower right corner of Live View to view the configured presets.



Figure 3-12 View the Configured Presets

3.10.3 Call a Preset

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

Steps

- **1.** Click $\[the expansion]$ on the quick settings toolbar of the PTZ camera's Live View.
- 2. Click in the lower right corner of Live View to set the preset.
- 3. Select the preset No. from the drop-down list.
- **4.** Click **Call** to call it, or click in the lower right corner of Live View, and click the configured preset to call it.



Figure 3-14 Call Preset (2)

3.10.4 Set a Patrol

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

- **1.** Click $\[the]$ on the quick settings toolbar of the PTZ camera's live view.
- 2. Click Patrol to configure patrol.

Aux Function	ux Function Patrol	
Patrol1		
🗱 Set	🕑 Call	Stop

Figure 3-15 Patrol Configuration

3. Select the patrol No.

4. Click Set.

Patrol S	ettings-Patrol 1			\times
+×	† ¥			
No	Preset	Speed	Duration	Edit
1	Preset 1	1	15	ß
2	Preset2	1	15	
			Apply	Cancel

Figure 3-16 Patrol Settings

5. Click + to add a key point to the patrol.

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



1) Configure key point parameters.

Preset

Determines the order the PTZ will follow while cycling through the patrol.

Speed

Defines the speed the PTZ will move from one key point to the next.

Duration

Refers to the duration to stay at the corresponding key point.

- 2) Click **Apply** to save the key points to the patrol.
- 6. Other Operation is as follows.

Operation	Description	Operation	Description
×	Select a key point to delete.	Ľ	Edit the added key point.
+	Adjust the key point order	ŧ	Adjust the key point order

7. Click Apply to save the patrol settings.

3.10.5 Call a Patrol

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

Steps

- **1.** Click $\[the]$ on the quick settings toolbar of the PTZ camera's live view.
- 2. Click Patrol on the PTZ control panel.

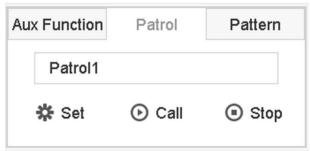


Figure 3-18 Patrol Configuration

- 3. Select a patrol.
- 4. Click Call to start the patrol.
- 5. Optional: Click Stop to stop the patrol.

3.10.6 Set a Pattern

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

Steps

- **1.** Click $\[the]$ on the quick settings toolbar of the PTZ camera's live view.
- 2. Click Pattern to configure a pattern.



Figure 3-19 Pattern Configuration

- 3. Select the pattern No.
- 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 PTZ movement is recorded as the pattern.

3.10.7 Call a Pattern

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

- **1.** Click $\[the expansion]$ on the quick settings toolbar of the PTZ camera's live view.
- 2. Click Pattern to configure pattern.

Au	x Function	Patrol	Pattern
	Pattern1		
	Reco	rd 🕞 Call	Stop

Figure 3-20 Pattern Configuration

- **3.** Select a pattern.
- 4. Click Call to start the pattern.
- 5. Optional: Click Stop to stop the pattern.

3.10.8 Set Linear Scan Limit

Linear Scan trigger a scan in the horizontal direction in the predefined range.

Before You Start

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

iNote

This function is supported only by some certain models.

Steps

- **1.** Click $\[the]$ on the quick settings toolbar of the PTZ camera's live view.
- **2.** Click directional buttons to wheel the camera to a location, and click **Left Limit** or **Right Limit** to link the location to the corresponding limit.



The speed dome linear scans from the left limit to the right limit, and you must set the left limit on the left side of the right limit. Also, the angle from the left limit to the right limit must be no more greater than 180°.

3.10.9 One-Touch Park

Certain speed dome models can be configured to start a predefined park action (scan, preset, patrol and etc.) automatically after a period of inactivity (park time).

Before You Start

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

Steps

- **1.** Click $\[the]$ on the quick settings toolbar of the PTZ camera's live view.
- 2. Click Park (Quick Patrol), Park (Patrol 1), or Park (Preset 1) to activate the park action.

Park (Quick Patrol)

The dome starts patrolling from the predefined preset 1 to preset 32 in order after the park time. Undefined presets 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.

iNote

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

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

3.10.10 Auxiliary Functions

You can operate the auxiliary functions including light, wiper, 3D positioning, and center on the PTZ control panel.

Before You Start

```
Make sure the connected IP camera supports the PTZ function, and is properly connected.
```

Steps

1.

Click $\stackrel{\bigcirc}{\frown}$ on the quick settings toolbar of the PTZ camera's live view. The PTZ control panel displays on the right of the interface.

2. Click Aux Function.



Figure 3-21 Aux Function Configuration

3. Click the icons to operate the aux functions. See the table for the icon descriptions.

Table 3-1 Description of Aux Functions Icons

Icon	Description
·····	Light on/off
	Wiper on/off
3	3D positioning
67	Center

Chapter 4 Recording and Playback

4.1 Recording

4.1.1 Configure Recording Parameters

Go to Camera → Video Parameters .

Main Stream

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)

It 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+

H.264+ combines intelligent analysis technology with predictive encoding, noise suppression, and long-term bit rate control to realize a lower bit rate, which plays a significant role in cutting storage costs and provides a higher return value for the investment.

Enable H.265+

H.265+ is an optimized encoding technology based on the standard H.265/HEVC compression. With H.265+, the video quality is almost the same as that of H.265/HEVC but with less transmission bandwidth and storage capacity required.

iNote

- A higher resolution, frame rate and bit rate 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.
- H.264+ or H.265+ encoding technology is only available for certain models.

Sub-Stream

Sub-stream is a second codec that runs alongside the main stream. It allows you to reduce the outgoing internet bandwidth without sacrificing your direct recording quality. Sub-stream is often exclusively used by apps to view live video. Users with limited internet speeds may benefit most from this setting.

Picture

The picture refers to the live picture capture in continuous or event recording type. (Storage \rightarrow Capture Schedule \rightarrow Advanced

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.

Capture Delay Time

The duration of capturing pictures.

Configure Advanced Recording Parameters

Steps

- **1.** Go to **Storage** \rightarrow **Schedule** \rightarrow **Record**.
- 2. Check Enable Schedule to enable scheduled recording.
- 3. Click Advanced to set the advanced parameters.

Advanced Parameters								
Record Audio:								
Pre-Record:	5s			-				
Post-Record:	Post-Record: 5s							
Stream Type:	Main Stre	am		•				
Expired Time (da	iy):	5						
Redundant Re	ecord/Captur	e						
	ОК		Cancel					

Figure 4-1 Advanced Record Settings

Record Audio

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.

Stream Type

Main stream and sub-stream are selectable for recording. When you select sub-stream, you can record for a longer time with the same storage space.

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.

4.1.2 Enable the H.265 Stream Access

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

Go to **Camera** \rightarrow **More Settings** \rightarrow **H.265 Auto Switch Configuration** to enable the function.

4.1.3 ANR

ANR (Automatic Network Replenishment) function enables the IP camera to save the recording files in the local storage when the network is disconnected, and when the network is resumed, it uploads the files to the device.

Steps

- Log in your device via web browser and go to Configuration → Storage → Schedule Settings → Advanced.
- 2. Check Enable ANR.
- 3. Click OK.

4.1.4 Manual Recording

You can click 📇 to manually start/stop recording videos at live view.

4.1.5 Configure Plan Recording

The camera would automatically start/stop recording according to the configured recording schedule.

Before You Start

- Ensure you have installed the HDDs to the device or added the network disks before storing the video files, pictures and log files.
- Before enabling **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. Refer to for details.

Steps

- **1.** Go to **Storage** \rightarrow **Schedule** \rightarrow **Record**.
- 2. Select a camera.
- 3. Check Enable Schedule.
- 4. Select a recording type.

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.

POS

Recording triggered by POS and alarm.

5. Drag the cursor on time bar to set the record schedule.

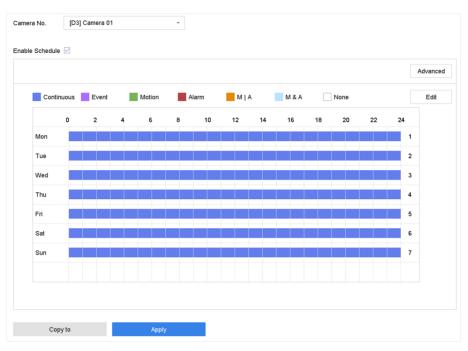


Figure 4-2 Record Schedule

iNote

- You can repeat the above steps to set schedule recording or capture for each day in the week.
- Continuous recording is applied to each day by default.
- 6. Optional: Copy the recording schedule to other camera(s).
 - 1) Click Copy to.
 - 2) Select camera(s) to duplicate with the same schedule settings.
 - 3) Click OK.
- 7. Click Apply.

4.1.6 Configure Continuous Recording

The device can continuously record the video within the configured time schedule.

- 1. Go to Camera → Encoding Parameters → Recording Parameters .
- 2. Set the continuous main stream/sub-stream recording parameters for the camera.
- 3. Go to Storage \rightarrow Recording Schedule .
- 4. Drag the mouse on the time bar to set the continuous recording schedule. Refer to *Configure Plan Recording* for details.

4.1.7 Configure Motion Detection Triggered Recording

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

Steps

- **1.** Go to System \rightarrow Event \rightarrow Normal Event \rightarrow Motion Detection .
- 2. Configure the motion detection and select the channel (s) to trigger the recording when motion event occurs. Refer to *Configure Linkage Actions* for details.
- 3. Go to Camera → Encoding Parameters → Recording Parameters .
- 4. Set the event main stream/sub-stream recording parameters for the camera.
- 5. Go to Storage \rightarrow Recording Schedule .
- **6.** Select the recording type to **Motion**.
- 7. Drag the mouse on the time bar to set motion detection recording schedule. Refer to *Configure Plan Recording* for details.

4.1.8 Configure Event Triggered Recording

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

Steps

- 1. Go to System → Event .
- 2. Configure the event detection and select the channel(s) to trigger the recording when event occurs. Refer to *Event* for details.
- 3. Go to Camera → Encoding Parameters → Recording Parameters .
- 4. Set the event main stream/sub-stream recording parameters for the camera.
- 5. Go to Storage \rightarrow Recording Schedule .
- 6. Select the recording type to Event.
- 7. Drag the mouse on the time bar to set the event detection recording schedule. Refer to *Configure Plan Recording* for details.

4.1.9 Configure Alarm Triggered Recording

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

- **1.** Go to **System** \rightarrow **Event** \rightarrow **Normal Event** \rightarrow **Alarm Input**.
- Configure the alarm input and select the channel(s) to trigger the recording when alarm occurs. Refer to *Event* for details.
- 3. Go to Camera \rightarrow Encoding Parameters \rightarrow Recording Parameters .
- 4. Set the event main stream/sub-stream recording parameters for the camera.
- 5. Go to Storage \rightarrow Recording Schedule .
- 6. Select the recording type to Alarm.

7. Drag the mouse on the time bar to set the alarm recording schedule. Refer to *Configure Plan Recording* for details.

4.1.10 Configure Picture Capture

The picture refers to the live picture capture in continuous or event recording type. Only certain models support this function.

Steps

- 1. Go to Camera → Encoding Parameters → Capture .
- **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.

3. Go to Storage \rightarrow Capture Schedule .

- 4. Select the camera to configure the picture capture.
- 5. Set the picture capture schedule. Refer to *Configure Plan Recording* for details.

4.1.11 Configure Holiday Recording

You may want to have different plan for recording on holiday, this function allows you to set the recording schedule on holiday for the year.

- 1. Go to System → Holiday .
- 2. Select a holiday item from the list.
- **3.** Click \square to edit the selected holiday.
- 4. Check Enable.

Edit				
Enable				
Holiday N	Holiday1			
Mode	By Month			•
Start Date	Jan	•	1	•
End Date	Feb	•	8	•

Apply OK Cancel

Figure 4-3 Edit Holiday Settings

- 5. Set Holiday Name, Mode, Start Date, and End Date.
- 6. Click OK.
- 7. Set the schedule for holiday recording. Refer to Configure Plan Recording for details.

4.1.12 Configure Redundant Recording and Capture

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.

Before You Start

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

- **1.** Go to **Storage** \rightarrow **Storage Device** .
- 2. Select a HDD from the list and click 🗹 to enter the Local HDD Settings interface.
- **3.** Set the HDD property to **Redundancy**.
- 4. Go to Storage → Schedule Settings → Record Schedule/Capture Schedule .
- 5. Click Advanced to set the camera recording parameters.

Advanced Paramete	ers					
Record Audio:						
Pre-Record:	5s	.				
Post-Record:	Post-Record: 5s					
Stream Type:	Main Stream	-				
Expired Time (da	y): 5					
Redundant Re	cord/Capture					
	ОК	Cancel				

Figure 4-4 Record Parameters

- 6. Check Redundant Record/Capture.
- 7. Click OK to save settings.

4.2 Playback

4.2.1 Instant Playback

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

After selecting the camera on **Live View**, you can move the cursor to the window bottom to access the toolbar, and click \odot to start instant playback.



Figure 4-5 Playback Interface

4.2.2 Play Normal Video

Go to **Playback**, select date and camera(s), and use the toolbar at the bottom to perform playback operations. Refer to **Playback Operations**. You can click camera(s) to execute simultaneous playback of multiple camera(s).

iNote

256x playing speed is supported.



Figure 4-6 Play Normal Video Interface

4.2.3 Play Smart Searched Video

In smart playback mode, the device can analyze videos that containing motion, line, or intrusion detection information, and mark them in red.

Go to **Playback**, click **Smart**, and then click motion detection (\square), line crossing detection (\square), or intrusion detection (\square) in the toolbar at the bottom to play the video as your desire.



Figure 4-7 Payback by Smart Search

4.2.4 Play Custom Searched Files

You can play video by customized search conditions.

- 1. Go to Playback.
- 2. Select camera(s) from the list.
- 3. Click Custom Search on the left bottom.
- 4. Enter search conditions, including Time, File Status, Event Type, etc.

lime -	Custom	- 1	2017-10-01 00:00:00) 🗎 2	017-10-23 23:59:59	iii	
Гад	A	F	ile Status	All	-		
Event Type	None	*					
Plate No.							
Area/Country	None	*					
					ty Conditions		Save
						Search	

Figure 4-8 Custom Search

5. Click Search.



Figure 4-9 Custom Searched Video Files

6. Select a file and start playing the video on search results interface.

4.2.5 Play Tag Files

Video tag allows you to record information, such as people and locations of a certain time point, during playback. You can use video tag(s) to search video files and position time point.

Add Tag Files

Steps

- 1. Go to Playback.
- 2. Search and play back the video file(s).
- **3.** Click 🖉 to add the tag.
- 4. Edit the tag information.
- 5. Click OK.

iNote

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

Play Tag Files

- 1. Go to Playback.
- 2. Click Custom Search at the left bottom.
- **3.** Enter search conditions, including time and tag keyword.

Time	Custom	-	2017-10-01 00:00:	201	7-10-23 23:59:59	Ē	
Tag	A		File Status	All	-		
Event Type	None	*					
Plate No.							
Area/Country	None	*					

Figure 4-10 Tag Search

4. Click Search.

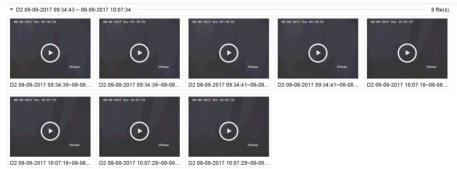


Figure 4-11 Searched Tag Files

5. Select a tag file, and play the video on the search results interface.

4.2.6 Play by Sub-periods

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

Steps

- 1. Go to Playback.
- 2. Click HH at the lower-left corner.
- 3. Select a camera.
- 4. Set the start time and end time for searching video.
- 5. Select the different multi-period at the lower-right corner, e.g., 4-Period.

iNote

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.

4.2.7 Play Log Files

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

Steps

- **1.** Go to **Maintenance** \rightarrow Log Information .
- 2. Click Log Search .
- 3. Set search time and type and click Search.

•	2017	-08-18 00:00:00	_ 2017-0	8-18 23:59:59		Search			
r T	уре	All	-						
r	Search	Result							Export A
	No	Major Type	Time	Minor Type	Parameter	Play	Details		
•	103	Alarm	18-08-2017 07:07:31	Motion Detection	N/A	•	0		
v	104	Alarm	18-08-2017 07:07:43	Motion Detection	N/A	•	()		
2	105	Alarm	18-08-2017 07:16:27	Motion Detection	N/A	•	1		
2	106	Alarm	18-08-2017 07:16:37	Motion Detection	N/A	•	1		
¥	107	🔤 Inform	18-08-2017 07:17:19	System Running	N/A	-	()		
2	108	😋 Inform	18-08-2017 07:17:19	System Running	N/A		()		
2	109	🔤 Inform	18-08-2017 07:18:00	HDD S.M.A.R.T.	N/A	-	0		
v	110	🔤 Inform	18-08-2017 07:18:00	HDD S.M.A.R.T.	N/A		()		
×	111	🖳 Inform	18-08-2017 07:27:20	System Running	N/A	-	0		
•	Total: 1	151 P: 2/12			< <			Go	
~					I	Export	Back		
~ :	Sudden	Change of Sound	Intensity Alarm Started						
~ :	Sudden	Change of Sound	Intensity Alarm Stopped						
	Face De	tection (Eace Can	ture) Alarm Started						

Figure 4-12 System Log Search Interface

4. Choose a log with a video file and click to start playing the log file.

4.2.8 Play External Files

You can play files from external storage devices.

Before You Start

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

- 1. Go to Playback.
- 2. Click 📄 at the lower-left corner.
- **3.** Click \triangleright , or double-click the file to play it.

4.3 Playback Operations

4.3.1 Normal/Important/Custom Video

During the playback, you can select the following three modes to play the video.

Normal

Video files from the continuous recording.

Important

Video files from the event and alarm recording triggered recording.

Custom

Video files searched by custom conditions.

4.3.2 Set Play Strategy in Important/Custom Mode

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.

iNote

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

4.3.3 Edit Video Clips

You can cut and export video clips during playback.

Steps

1. Go to Playback

- **2.** Click 😹 at the bottom toolbar.
- **3.** Set the start time and end time. You can click [x] to set the time period, or set a time segment on time bar.
- **4.** Click 🖹 to save the video clip to a storage device.

4.3.4 Switch between Main Stream and Sub-Stream

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

Icon	Description
Lo	Play the video in main stream.
°	Play the video in sub-stream.

iNote

The encoding parameters for the main stream and sub-stream can be configured in **Storage** → **Encoding Parameters** .

4.3.5 Thumbnails View

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

In the playback mode, position the cursor on time bar to get preview thumbnails.



Figure 4-13 Thumbnails View

You can click a thumbnail to enter the full-screen playback.

4.3.6 Fast View

Hold the mouse to drag on the time bar to get a fast view of the video files.

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

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

4.3.7 Digital Zoom

Digital Zoom zooms into the live image in different magnifications (1x to 16x).

Steps

1. Start live view, click $\, \oplus \,$ from the toolbar.

2. Move the sliding bar or scroll the mouse wheel to zoom in/out the image to different magnifications (1x to 16x).



Figure 4-14 Digital Zoom

Chapter 5 Event

5.1 Normal Event Alarm

5.1.1 Configure Motion Detection Alarms

Motion detection enables the device to detect the moving objects in the monitored area and trigger alarms.

Steps

- **1.** Go to System \rightarrow Event \rightarrow Normal Event \rightarrow Motion Detection .
- 2. Select a camera.
- 3. Check Enable.
- **4.** Set the motion detection rule.

For cameras have human and vehicle detection function.	Click Draw Area to draw the detection area(s) on the preview screen. Set Target Detection as Human Body or Vehicle to discard alarms which are not triggered by human body or vehicle.
For cameras do not have human and vehicle detection function.	Click Full screen to set the full-screen as the detection area, or drag on the preview screen to draw the customized detection area.

- **5.** Set **Sensitivity** (0-100). The sensitivity allows you to calibrate how readily movement triggers the alarm. A higher value results in the more readily to triggers motion detection.
- 6. Set the arming schedule. Refer to Configure Arming Schedule .
- 7. Set linkage actions. Refer to Configure Linkage Actions .

5.1.2 Configure Video Loss Alarms

Video loss detection detects video loss of a channel and takes alarm response action(s).

- **1.** Go to **System** \rightarrow **Event** \rightarrow **Normal Event** \rightarrow **Video Loss**.
- 2. Select a camera.
- 3. Check Enable.
- 4. Set the arming schedule. Refer to Configure Arming Schedule .
- 5. Set linkage actions. Refer to Configure Linkage Actions .

5.1.3 Configure Video Tampering Alarms

Video tampering detection triggered an alarm when the camera lens is covered and takes alarm response action(s).

Steps

- 1. Go to System → Event → Normal Event → Video Tampering .
- 2. Select a camera.
- 3. Check Enable.
- **4.** Set the video tampering area. Drag on the preview screen to draw the customized video tampering area.
- **5.** Set **Sensitivity** (0-2). 3 levels are available. The sensitivity calibrates how readily movement triggers the alarm. A higher value more readily triggers the video tampering detection.
- 6. Set the arming schedule. Refer to Configure Arming Schedule .
- 7. Set linkage actions. Refer to Configure Linkage Actions .

5.1.4 Configure Sensor Alarms

Set the handling action of an external sensor alarm.

Steps

- 1. Go to System → Event → Normal Event → Alarm Input .
- 2. Select an alarm input item from the list and click $\underline{\mathbb{Z}}$.
- 3. Select the alarm input type.
- 4. Edit the alarm name.
- 5. Check Input.
- 6. Set the arming schedule. Refer to Configure Arming Schedule .
- 7. Set linkage actions. Refer to Configure Linkage Actions .

5.1.5 Configure Exceptions Alarms

Exception events can be configured to take the event hint in the Live View window and trigger alarm output and linkage actions.

- **1.** Go to **System** \rightarrow **Event** \rightarrow **Normal Event** \rightarrow **Exception**.
- 2. Optional: Enable the event hint to display it in the live view window.
 - 1) Check Enable Event Hint.
 - 2) Click 💮 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 5-1 Event Hint Settings

3. Select an exception type.

Enable Event Hint	\checkmark	
Event Hint Config	<i>ξ</i> ^Ω	
Exception Type	HDD Full	•

Figure 5-2 Exceptions Handling

4. Set the linkage actions. Refer to Configure Linkage Actions .

5.2 VCA Event Alarm

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

iNote

- VCA detections must be supported by the connected IP camera.
- Refer to the network camera user manual for detailed VCA detection instructions.

5.2.1 Temperature Screening

After connecting to specified thermography cameras, the device can display temperature measurement results, and notify you with audio alert when normal or abnormal temperature is detected.

Before You Start

Ensure your thermography camera supports this function, and it is properly configured.

Steps

- **1.** Go to **System** \rightarrow **Event** \rightarrow **Smart Event** .
- 2. Select the optical channel of thermography camera.
- 3. Click Face Capture.
- 4. Optional: Check Save VCA Picture to save the captured pictures of face detection.
- 5. Set the arming schedule. Refer to Configure Arming Schedule .
- 6. Set linkage actions. Refer to *Configure Linkage Actions*. If you only requires to implement linkage actions when the thermography camera detects abnormal temperature. Click **More**, and check **Abnormal Body Temperature**.

iNote

The abnormal temperature is detected and defined by the thermography camera.

7. Click Audio Alert, and check Normal Temperature or Abnormal Temperature to enable desired audio alert when normal or abnormal temperature is detected by the camera.

Arming Schedule	Linkage Action	Audio Alert	More	
Normal Temp	erature			

Abnormal Temperature

Figure 5-3 Audio Alert

8. Click Apply.

What to do next

- You can check 🔄 of **Target Detection** in live view to view detection results.
- You can go to File Management → Smart Search → Search by Appearance to search detection results.

5.2.2 Loitering Detection

Loitering detection is used to detect whether a target stays within a specified area longer than the set time and trigger alarm for linked actions.

- 1. Go to Smart Analysis → Smart Event Settings → Other Events .
- 2. Select a camera.
- 3. Click Loitering Detection.

44444444444		LANK CONTRACTOR	Arming Area 1	
6	期四 10:54:53		Arming Area 1	
2013 Deceo	日 正明 17:10:25	1 Jacobia	Time Thres1	10 1
		C getting	Sensitivity 1	100 96
11	#1#			
12				
		the second second		
		Camera 01		
Draw Area Clea	ar			

Figure 5-4 Loitering Detection

- 4. Check Enable Loitering Detection.
- 5. Optional: Check Save VCA Picture to save the captured loitering detection pictures.
- 6. Set loitering detection parameters.
 - 1) Select Arming Area.

iNote

Up to 4 areas are selectable.

2) Set Time Threshold.

Time Threshold

The time of the target staying in the region. If the value is 10, an alarm is triggered after the target has stayed in the region for 10 s. Range: [1-10].

3) Set Sensitivity.

Sensitivity

Similarity of the background image to the object. The higher the value is, more easily the detection alarm will be triggered.

- 7. Set the arming schedule. Refer to Configure Arming Schedule .
- 8. Set the linkage actions. Refer to Configure Linkage Actions .
- 9. Click Apply.

5.2.3 People Gathering Detection

People gathering detection is used to detect whether the density of human bodies within a specified area exceeds the set value and trigger alarm for linked actions.

Steps

1. Go to Smart Analysis \rightarrow Smart Event Settings \rightarrow Other Events .

- 2. Select a camera.
- 3. Click People Gathering.

⊡Enable People Gathering D		
Area Settings Arming Schedule Linkage Action		
11111111111111111 03-06-2019 星期三 20∶18∶28	Arming Area 1	•
10W 2013#34 810B # 1 117 avor	Percentage 1	100 1
#1# 10		
Camera 01		
A manufacture of the second seco		
Draw Area Clear		
Apply		

Figure 5-5 People Gathering Detection

- 4. Check Enable People Gathering Detection.
- 5. Optional: Check Save VCA Picture to save the captured people gathering detection pictures.
- 6. Set people gathering detection parameters.
 - 1) Select Arming Area.

iNote

Up to 4 areas are selectable.

- 2) Click **Draw Area** to draw a quadrilateral in the preview window by specifying four vertices of the area.
- 3) Set Percentage.

Percentage

The density of human bodies within the area. If it exceeds the threshold value, the device will trigger alarm.

- 7. Set the arming schedule. Refer to Configure Arming Schedule .
- 8. Set the linkage actions. Refer to Configure Linkage Actions .
- 9. Click Apply.

5.2.4 Fast Moving Detection

Fast moving detection is used to detect suspicious running and chasing, over-speed, and fast moving. It will trigger alarm when an object is moving fast and send notification to arming host so that necessary actions can be taken in advance.

Steps

- 1. Go to Smart Analysis → Smart Event Settings → Other Events .
- 2. Select a camera.
- 3. Click Fast Moving.

Enable Fast Moving Detection Area Settings Arming Schedule Linkage Action		
11111111111111111 01-05-2013 星期五 20:31:31 20 ^{分 月10日} 月10日 月1日 月7:00-07 00 月10日 月1日 月10日 日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日	Arming Area 1 Sensitivity 1	100 100
Draw Area Clear		

Figure 5-6 Fast Moving Detection

- 4. Check Enable Fast Moving.
- 5. Optional: Check Save VCA Picture to save the captured fast moving detection pictures.
- 6. Set fast moving detection parameters.
 - 1) Select Arming Region. Up to 4 regions are selectable.
 - 2) Click **Draw Area** to draw a quadrilateral in the preview window by specifying four vertices of the area.
 - 3) Set Sensitivity.

Sensitivity

Similarity of the background image to the object. The higher the value is, more easily the detection alarm will be triggered.

- 7. Set the arming schedule. Refer to Configure Arming Schedule .
- 8. Set the linkage actions. Refer to Configure Linkage Actions .
- 9. Click Apply.

5.2.5 Parking Detection

Parking detection is used to detect parking violation in the area, applicable in expressway and oneway street.

- 1. Go to Smart Analysis → Smart Event Settings → Other Events .
- 2. Select a camera.

3. Click Parking.

Enable Parking Detection		
Area Settings Arming Schedule Linkage Action		
1111111111111111 03-06-2019 星期三 20:26:11	Arming Area 1	-
2013年04 11日 王明三 17:16:05 #1#	Time Thres5	20 5
	Sensitivity 1	100 100
C. MOTA 01		
Principal And		
Draw Area Clear		
Apply		

Figure 5-7 Parking Detection

- 4. Check Enable Parking Detection.
- 5. Optional: Check Save VCA Picture to save the captured parking detection pictures.
- 6. Set parking detection parameters.
 - 1) Select Arming Area.



Up to 4 areas are selectable.

2) Set Time Threshold.

Time Threshold

The time of a vehicle staying in the region. If the value is 10, an alarm will be triggered after the vehicle has stayed in the region for 10 s. Range: [5-20].

3) Set Sensitivity.

Sensitivity

Similarity of the background image to the object. The higher the value is, more easily the detection alarm will be triggered.

- 7. Set the arming schedule. Refer to Configure Arming Schedule .
- 8. Set the linkage actions. Refer to Configure Linkage Actions .
- 9. Click Apply.

5.2.6 Unattended Baggage Detection

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

Steps

- 1. Go to Smart Analysis → Smart Event Settings → Other Events .
- 2. Select a camera.
- 3. Click Unattended Baggage.

Enable Unattended Baggag		
Area Settings Arming Schedule Linkage Action		
The setting a mining obligate Linkage Action	Arming Area 1 Time Thres5 Sensitivity 1	3600 5 100 50
Apply		

Figure 5-8 Unattended Baggage Detection

- 4. Check Enable Unattended Baggage Detection.
- 5. Optional: Check Save VCA Picture to save the captured unattended baggage detection pictures.
- 6. Set the detection rules and detection areas.
 - 1) Select Arming Area.

iNote

Up to 4 areas are selectable.

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

Time Threshold

The time of the objects left in the region. If the value is 10, an alarm will be triggered after the object is left and stayed in the region for 10 s. Range: [5-20].

Sensitivity

Similarity of the background image to the object. The higher the value is, more easily the detection alarm will be triggered.

- 3) Click Draw Region and draw a quadrilateral in the preview window.
- 7. Set the arming schedule. Refer to Configure Arming Schedule .
- 8. Set linkage actions. Refer to Configure Linkage Actions .
- 9. Click Apply.

5.2.7 Object Removal Detection

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

Steps

- 1. Go to Smart Analysis → Smart Event Settings → Other Events .
- 2. Select a camera.
- 3. Click Object Removable.

Enable Obje	ect Removal Det			
Area Settings	Arming Schedule	Linkage Action		
Draw Area	Arming Schedule #1 #1 Clear Apply		Arming Area	- 3600 5 - 100 50

Figure 5-9 Object Removal Detection

- 4. Check Enable Object Removable Detection.
- 5. Optional: Check Save VCA Picture to save the captured object removable detection pictures.
- 6. Follow these steps to set the detection rules and detection areas.
 - 1) Select Arming Area.

iNote

Up to 4 areas 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 will be triggered after the object disappears from the region for 10 s. Range [5-20].

Sensitivity

The similarity degree of the background image. If the sensitivity is high, a very small object taken from the region will trigger the alarm.

- 3) Click **Draw Area** and draw a quadrilateral in the preview window by specifying four vertices of the detection region.
- 7. Set the arming schedule. Refer to Configure Arming Schedule .

- 8. Set the linkage actions. Refer to Configure Linkage Actions .
- 9. Click Apply.

5.2.8 Audio Exception Detection

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

Steps

- 1. Go to Smart Analysis → Smart Event Settings → Other Events .
- 2. Select a camera.
- 3. Click Audio Exception.

Face Detection Vehicle Line Crossin Audio Exception Defocus Sudden Scene		Region Entrance	Region Exiting	Unattended Ba	Object Removal
Camera [D1] IPCamera 01	- Save VCA Pi				
Exception Detection Arming Schedule Linkage Action					
Audio Loss Exception					
Sudden Increase of Sound Intens					
Sensitivity 1 100 50					
Sound Int 1 100 50					
Sudden Decrease of Sound Inten					
Sensitivity 1 100 50					
Appty					

Figure 5-10 Audio Exception Detection

4. Optional: Check Save VCA Picture to save the captured audio exception detection pictures.

5. Set the detection rules.

- 1) Select Exception Detection.
- 2) Check Audio Loss Exception, Sudden Increase of Sound Intensity Detection, and/or Sudden Decrease of Sound Intensity Detection.

Audio Loss Exception

Detects a steep sound rise in the surveillance scene. Set **Sensitivity** and **Sound Intensity Threshold** for the steep sound rise.

Sensitivity

The smaller the value is, the more severer the change would trigger the detection. Range [1-100].

Sound Intensity Threshold

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

Sudden Decrease of Sound Intensity Detection

Detects a steep sound drop in the surveillance scene. Detection sensitivity [1-100].

- 6. Set the arming schedule. Refer to Configure Arming Schedule .
- 7. Set the linkage actions. Refer to *Configure Linkage Actions*.
- 8. Click Apply.

5.2.9 Defocus Detection

Image blur caused by lens defocus can be detected.

Steps

- 1. Go to Smart Analysis → Smart Event Settings → Other Events .
- 2. Select a camera.
- 3. Click Defocus.

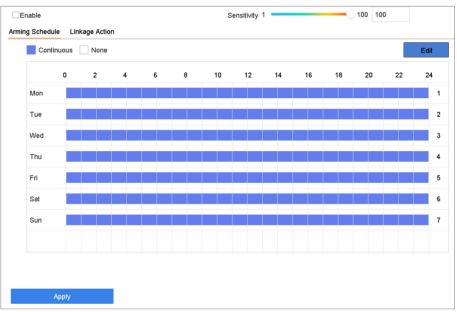


Figure 5-11 Defocus Detection

- 4. Check Enable.
- 5. Optional: Check Save VCA Picture to save the captured defocus detection pictures.
- 6. Set the detection sensitivity.

Sensitivity

Sensitivity range: [1-100]. The higher the value is, the more easily the defocus image will be detected.

- 7. Set the arming schedule. Refer to Configure Arming Schedule .
- 8. Set the linkage actions. Refer to Configure Linkage Actions .
- 9. Click Apply.

5.2.10 Sudden Scene Change Detection

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

Steps

- 1. Go to Smart Analysis → Smart Event Settings → Other Events .
- 2. Select a camera.
- 3. Click Sudden Scene Change.



Figure 5-12 Sudden Scene Change

- 4. Check Enable.
- 5. Optional: Check Save VCA Picture to save the captured sudden scene change detection pictures.
- **6.** Set the detection sensitivity.

Sensitivity

Ranges from 1 to 100, the higher the value, the more easily the change of scene can trigger the alarm.

- 7. Set the arming schedule. Refer to Configure Arming Schedule .
- 8. Set the linkage actions. Refer to Configure Linkage Actions .
- 9. Click Apply.

5.2.11 PIR Alarm

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.

Steps

- 1. Go to Smart Analysis → Smart Event Settings → Other Events .
- 2. Select a camera.
- 3. Click PIR Alarm.



Figure 5-13 PIR Alarm

- 4. Check PIR Alarm.
- 5. Optional: Check Save VCA Picture to save the captured of PIR alarm pictures.
- 6. Set the arming schedule. Refer to Configure Arming Schedule .
- 7. Set the linkage actions. Refer to *Configure Linkage Actions*.
- 8. Click Apply.

5.2.12 Thermal Camera Detection

The NVR supports the event detection modes of the thermal network cameras: fire and smoke detection, temperature detection, temperature difference detection, etc.

Before You Start

Add the thermal network camera to your device and make sure the camera is activated.

Steps

1. Go to Smart Analysis \rightarrow Smart Event Settings \rightarrow Other Events .

- **2.** Select a thermal camera.
- 3. Optional: Check Save VCA Picture to save the captured pictures of detection.
- 4. Select an event detection (Temperature Measurement Alarm, etc.).
- 5. Set the arming schedule. Refer to Configure Arming Schedule .
- 6. Set the linkage actions. Refer to *Configure Linkage Actions* .
- 7. Click Apply.

5.2.13 Configure Queue Management

After connecting with queue management camera, you can set the arming schedule and linkage action of queue management.

Before You Start

Ensure the recorder have connected with queue management camera.

Steps

- 1. Go to Smart Analysis → Smart Event Settings → Other Events .
- 2. Select a queue management camera.
- 3. Optional: Check Save VCA Picture to save the captured pictures of detection.
- 4. Set the arming schedule. Refer to Chapter Configure Arming Schedule for details.
- 5. Set the linkage actions. Refer to Chapter Configure Linkage Actions for details.
- 6. Click Apply.

5.3 Configure Arming Schedule

Steps

- 1. Click Arming Schedule.
- 2. Click Edit.
- 3. Select a day of the week and set the time period. Up to eight time periods can be set each day.

iNote

Time periods cannot repeat or overlapped.

Edit				
Weekday	Mon			•
Start/End Time	00:00-2	24:00		٢
Start/End Time	00:00-0	00:00		٢
Start/End Time	00:00-0	00:00		\odot
Start/End Time	00:00-0	00:00		٢
Start/End Time	00:00-0	00:00		\odot
Start/End Time	00:00-0	00:00		\odot
Start/End Time	00:00-0	00:00		\odot
Start/End Time	00:00-0	00:00		\odot
	Сору	Apply	ок	Cancel

Figure 5-14 Set Arming Schedule

- **4.** You can click **Copy** to copy the current day arming schedule settings to other day(s).
- 5. Click Apply to save the settings.

5.4 Configure Linkage Actions

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.

5.4.1 Configure Auto-Switch Full Screen Monitoring

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.

iNote

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

Steps

1. Go to System \rightarrow Live View \rightarrow General .

2. Set the event output and dwell time.

Event Output

Select the output to show the event video.

Full Screen Monitoring Dwell Time

Set the time in seconds to show the 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).

- **3.** Go to the **Linkage Action** interface of the alarm detection (e.g., motion detection, video tampering, face detection, etc.).
- 4. Select the Full Screen Monitoring alarm linkage action.
- 5. Select the channel(s) in Trigger Channel for full screen monitoring.

5.4.2 Configure Audio Warning

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

Steps

- **1.** Go to **System** \rightarrow **View** \rightarrow **General**.
- 2. Enable the audio output and set the volume.
- **3.** Go to **Linkage Action** interface of the alarm detection (e.g., motion detection, video tampering, face detection, etc.).
- 4. Select the Audio Warning alarm linkage action.

5.4.3 Notify Surveillance Center

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., iVMS-4200, iVMS-5200).

Steps

- **1.** Go to System \rightarrow Network \rightarrow Advanced \rightarrow More Settings .
- 2. Set the alarm host IP and alarm host port.
- **3.** Go to Linkage Action interface of the alarm detection (e.g., motion detection, video tampering, face detection, etc.).
- 4. Select Notify Surveillance Center.

5.4.4 Configure Email Linkage

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

- **1.** Go to System \rightarrow Network \rightarrow Advanced \rightarrow Email .
- 2. Set the email parameters.
- 3. Click Apply.

- **4.** Go to the **Linkage Action** interface of the alarm detection (e.g., motion detection, video tampering, face detection, etc.).
- 5. Select Send Email alarm linkage action.

5.4.5 Trigger Alarm Output

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

Steps

- **1.** Go to **Linkage Action** interface of the alarm detection (e.g., motion detection, face detection, line crossing detection, intrusion detection, etc.).
- 2. In Trigger Alarm Outputs Area, Select the alarm output (s) to trigger.
- 3. Go to System → Event → Normal Event → Alarm Output .
- 4. Select an alarm output item from the list.

5.4.6 Configure Audio and Light Alarm Linkage

For certain network cameras, you can set the alarm linkage action as audio alarm or light alarm.

Before You Start

- Ensure your camera supports audio and light alarm linkage.
- Ensure the audio output and volume are properly configured.

Steps

- 1. Go to the linkage action interface of the alarm detection (e.g., motion detection).
- 2. Set Audio and Light Alarm Linkage as your desire.
- 3. Click Apply.

5.4.7 Configure PTZ Linkage

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

Before You Start

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

- **1.** Go to **Linkage Action** interface of the alarm input or VCA detection (e.g., face detection, line crossing detection, intrusion detection, etc.).
- 2. Select the PTZ Linkage.
- **3.** Select the camera to perform the PTZ actions.
- **4.** Select the preset/patrol/pattern No. to call when the alarm events occur.

iNote

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

Chapter 6 Smart Analysis

6.1 Engine Configuration

Each engine processes a specified VCA type as its working mode. You can configure the engine working mode as your desire.

Steps

```
1. Go to Smart Analysis → Engine Settings → Engine Configuration .
```



Figure 6-1 Engine Configuration

2. Configure each engine usage. You can view the engine temperature and linked channel status of each function.

iNote

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.

3. Click Apply to save the settings.

6.2 Face Picture Comparison

The device supports the face picture comparison alarm and face capture for the connected camera based on face recognition feature.

Go to Smart Analysis \rightarrow Engine Settings \rightarrow Engine Configuration . Configure at least one engine usage as Facial Recognition. Refer to *Engine Configuration* for details.

iNote

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

6.2.1 Face Grading Configuration

Face grading is used for face picture selection. According to pupil distance, tilt angle and pan angle, it only uses face pictures which satisfy grading requirement for analysis. Larger pupil distance, smaller tilt and pan angle, better it would be for analysis.

Steps

1. Go to Smart Analysis \rightarrow Engine Settings \rightarrow Face Grading .

Enable Face G		V	2		
Pupil Distance	2	30	18		719
Tilt Angle (°)	\$	45	0		90
Pan Angle (°)	\$	45	0	0	90
Restore					
Restore					

Figure 6-2 Face Grading

2. Check Enable Face Grading.

3. Set Pupil Distance, Tilt Angle, and Pan Angle.

Pupil Distance

Pupil distance is the distance between two pupils. In order to get better detection result, the pupil distance shall not be less than 40, and the recommended value is 60.

Tilt Angle

Tilt angle is the angle between your view and horizontal plane.

Pan Angle

Pan angle is the angle between your view and vertical plane.

4. Click Apply.

What to do next

- After face picture modeling, you can view face grading score of each face picture via web browser in **Configuration** → **Face Picture Library**.
- You can click *¬* in **Smart Analysis** → **Face Picture Database** to select face picture by face grading score.

6.2.2 Face Capture

The face capture detects and captures faces appearing in the surveillance scene. Linkage actions can be triggered when a human face is detected.

Steps

- 1. Go to Smart Analysis → Smart Event Settings → Facial Recognition .
- 2. Click Face Capture.



Figure 6-3 Face Capture

- **3.** Select a camera to configure.
- 4. Check Enable Face Capture.
- 5. Optional: Check Save VCA Picture to save the captured pictures of face detection.
- 6. Set the detection sensitivity.

iNote

Sensitivity range: [1-5]. The higher the value is, the easier faces will be detected.

- 7. Set the arming schedule. Refer to Configure Arming Schedule .
- 8. Set linkage actions. Refer to Configure Linkage Actions .
- 9. Click Apply.

6.2.3 Face Picture Library Management

Face picture library is mainly used for face picture storage and face picture comparison.

Add a Face Picture Library

Steps

- **1.** Go to Smart Analysis \rightarrow Face Picture Database .
- 2. Click + .
- **3.** Enter the face picture library name.
- 4. Click OK.

iNote

You can click \blacksquare or \times to edit the library name or delete the library.

Upload Face Pictures to the Library

Face picture comparison is based on face pictures in the library. You can upload a single face picture or import multiple face pictures to the library.

Before You Start

- Ensure the picture format is JPEG or JPG.
- For each picture, ensure it only has one face.
- Import all pictures to a backup device in advance.

The picture must be in JPEG or JPG format.

Steps

- 1. Select a face picture library in the list.
- 2. Click Add or Import Face Picture Library.
- **3.** Import picture(s).
 - Add:

Select a picture to import and click Import.

- Import Face Picture Library:

Select multiple pictures to import and click Import.

What to do next

- Select pictures and click **Copy to** to copy the uploaded pictures of the current library to other library.
- Select a picture and click **Edit** to modify the picture information.
- Select a picture from the list and click **Delete** to delete the picture.
- Select a library and click **Export Face Picture Library** to export library to backup device.
- Click 🗄 or 📃 to view by figure or list.

6.2.4 Face Picture Comparison Alarm

Configure Face Picture Comparison

Compare detected face pictures with specified face picture library. Trigger alarm when comparison succeeded.

- 1. Go to Smart Analysis → Smart Event Settings → Facial Recognition .
- 2. Select a camera.
- 3. Click Face Picture Comparison.

Select Mode	Face Picture Comparison	Enable Face Picture Comparison
arm Parameters		Succeeded Linkage Failed
Comparison Fa	Compare failed	
Comparison Su	Welcome	
Lib	rary Name	Edit Similarity
tes		
444	lre2	
Enable Alarm C	output Pulse	
Арр	IY	

Figure 6-4 Face Picture Comparison

- 4. Set Mode as Face Picture Comparison.
- 5. Check Enable Face Picture Comparison.
- **6. Optional:** Check **Save VCA Picture** to save the captured pictures of VCA detection. After the face picture comparison is enabled, the comparison results will be uploaded for face comparison alarm. If the comparison produced a match, both the real-time face picture and the target picture from the library will be uploaded. If no match is produced, the real-time face picture is uploaded to center only. Up to 6 connected cameras can be configured for face picture comparison simultaneously.

7. Optional: Set Comparison Failed Prompt, Comparison Succeeded Prompt, and Enable Alarm Output Pulse.

Comparison Failed Prompt

It will display the prompt in live view **Target Detection** (with **Facial Detection** checked) or **Facial Recognition** when face picture comparison failed. You can click in live view to enter Facial Recognition interface.

Comparison Succeeded Prompt

It will display the prompt in **Facial Recognition** when face picture comparison succeeded. You can click of in live view to enter Facial Recognition interface.

Enable Alarm Output Pulse

It is usually linked with a gate. When a person is passing a gate, if the comparison succeeded, it will trigger a pulse to open the gate. The pulse is between 100 to 900 ms. You can set **Alarm Output Pulse (ms)** in **System** \rightarrow **Event** \rightarrow **Normal Event** \rightarrow **Alarm Output**.

- 8. Select face picture libraries and set similarity.
- 9. Set the arming schedule. Refer to Configure Arming Schedule .
- **10.** Set the linkage actions when face picture comparison succeeded or failed. Refer to *Configure Linkage Actions*.
- 11. Optional: Configure face grading parameters. Refer to Face Grading Configuration .
- **12.** Click **Apply** to save the settings.

6.2.5 Face Picture Search

Search by Face Picture Comparison Event

Search face picture by face picture comparison results.

Steps

- **1.** Go to Smart Analysis \rightarrow Smart Search \rightarrow Face Search \rightarrow Search by Event .
- **2.** Set the start time and end time.
- 3. Select a channel.
- 4. Select Event Type as Face Picture Comparison.
- 5. Click Start Search. The search result list displays 1 channel.
- **6.** Click **Channel** to select a channel as your desire. It will display search results for the selected channel.

What to do next

Refer to View Searching Result .

Search by Uploaded Picture

You can search the face pictures by uploaded picture.

Steps

```
1. Go to Smart Analysis → Smart Search → Face Search → Search by Picture .
```

Uplead Sample from Local	\bigcirc	\bigcirc	\bigcirc	\bigcirc	\bigcirc
Upload Sample from Face Picture Database N	lot more than 6 pictures for sa	nplecache. D/D			
IP Channel	[All] Camera		•		
Time Segment	Today	- 2020-01	-13 00:00: 🛅 -	2020-01-13 23:59: 🛅	
Similarity(50~100)	≥ 80				
					Start Search

Figure 6-5 Search by Uploaded Picture

- 2. Select a channel.
- 3. Select face pictures for search.
 - Click Upload Sample from Local and select face pictures from your local directory.
 - Click **Upload Sample from Face Picture Database** and select face pictures from created face picture libraries.
- **4.** Set the start time and end time.
- **5.** Set the **Similarity** value (range: 0 to 100). Device will analyze the similarity between samples and face pictures in library and show pictures the similarity of which are higher than the set one.
- 6. Click Start Search. The search result list displays 1 channel.
- **7.** Click **Channel** to select a channel as your desire. It will display search results for the selected channel.

What to do next

Refer to View Searching Result .

Search by Personal Name

Search face picture by personal name.

Steps

1. Go to Smart Analysis \rightarrow Smart Search \rightarrow Face Search \rightarrow Search by Name .

IP Channel	(All) Camera			
Time Segment	Today -	2020-01-13 00:00: 🛅 -	2020-01-13 23:59: 🛅	
Name				
				Start Search

Figure 6-6 Search by Personal Name

- **2.** Set the start time and end time of the face pictures to search.
- 3. Select a channel.
- 4. Enter a name.
- 5. Click Start Search. The search result list displays 1 channel.
- **6.** Click **Channel** to select a channel as your desire. It will display search results for the selected channel.

What to do next

Refer to View Searching Result .

Search by Appearance

Search face picture by appearance.

Steps

- 1. Go to Smart Analysis → Smart Search → Face Search → Search by Appearance .
- 2. Set search conditions.
- 3. Click Start Search. The search result list displays 1 channel.
- **4.** Click **Channel** to select a channel as your desire. It will display search results for the selected channel.

What to do next

Refer to View Searching Result .

View Searching Result

- Double click a file to view the related video.
- Click Add to Face Database to add the selected file(s) to a face picture library.
- Click Add to Sample to add the select file(s) as sample picture(s). You can use the sample picture(s) to search other pictures. Refer to *Search by Uploaded Picture*.
- Click **Export** to export the selected file(s) to a backup device. You can click **Select All** to select all files.

∎Note

- You can click <a>[a] to view export progress.
- You can click _____ to return to search interface.

6.3 Perimeter Protection

For certain models of iDS series. Go to Smart Analysis \rightarrow Engine Settings \rightarrow Engine Configuration . Configure at least one engine usage as Perimeter Protection. Refer to *Engine Configuration* for details.

6.3.1 Line Crossing Detection

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.

- 1. Go to Smart Analysis → Smart Event Settings → Perimeter Protection .
- 2. Select a camera.
- 3. Click Line Crossing.

Enable Line Crossing Detection				
Area Settings Arming Schedule	Linkage Action			
11-19-2019 Tue 16:34 13 0		Arming Area	1	•
A AN AND AN	#1#	Direction	A<->B	-
E Chille		Sensitivity	1	100 50
AND A BOARD		Target	Human	Vehicle
13591702 2003				
Draw Area Clear				
Apply				

Figure 6-7 Line Crossing Detection

- 4. Check Enable Line Crossing Detection.
- 5. Optional: Check Save VCA Picture to save the captured pictures of line crossing detection.
- 6. Optional: Check Enable AI by Device.

The device will analyze the video, and cameras only transmit video stream.

- 7. Set the line crossing detection rules and detection areas.
- 1) Select an arming area.
 - 2) Select 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) Set the detection sensitivity. The higher the value is, the more easily the detection alarm can be triggered.
- 4) Click Draw Region.
- 5) Draw a virtual line in the preview window.
- 8. Optional: Draw the maximum size/minimum size for targets.

i Note

Only the targets in the size ranging from maximum size to minimum size will trigger line crossing detection.

- 1) Click Max. Size/Min. Size.
- 2) Draw an area in preview window.

- 3) Click Stop Drawing.
- **9. Optional:** Select **Target of Interest** as **Human Body** or **Vehicle** to discard alarms which are not triggered by human body or vehicle.
- 10. Set the arming schedule. Refer to Configure Arming Schedule .
- 11. Set linkage actions. Refer to Configure Linkage Actions .
- 12. Click Apply.

6.3.2 Intrusion Detection

Intrusion detection function detects people, vehicles or other objects that enter and loiter in a predefined virtual region. Specific actions can be taken when an alarm is triggered.

Steps

- 1. Go to Smart Analysis → Smart Event Settings → Perimeter Protection .
- 2. Select a camera.
- 3. Click Intrusion.

Enable Intrusion Detection ea Settings Arming Schedule Linkage Action		
	Virtual Plane 1	•
	Time Thre 0	10 5
The second second	Sensitivity 1	100 50
	Target 🗌 Human	Vehicle
P3591T02 2001		
top Drawing Clear		

Figure 6-8 Intrusion Detection

- 4. Check Enable Intrusion Detection.
- 5. Optional: Check Save VCA Picture to save the captured intrusion detection pictures.
- 6. Optional: Check Enable AI by Device.

The device will analyze the video, and cameras only transmit video stream.

- 7. Set the detection rules and detection areas.
 - 1) Select a virtual panel. Up to 4 virtual panels are selectable.
 - 2) Set Time Threshold, and Sensitivity.

Time Threshold

The time an object loiter in the region. When the duration of the object in the defined detection area exceeds the threshold, the device will trigger an alarm.

Sensitivity

Sensitivity is the object size which is able to trigger an alarm. The higher the sensitivity is, the more easily the detection alarm will be triggered.

- 3) Click Draw Area.
- 4) Draw a quadrilateral in the preview window.
- 8. Optional: Draw the maximum size/minimum size for targets.

iNote

Only the targets in the size ranging from maximum size to minimum size will trigger Intrusion detection.

- 1) Click Max. Size/Min. Size.
- 2) Draw an area in preview window.
- 3) Click Stop Drawing.
- **9. Optional:** Select **Target of Interest** as **Human Body** or **Vehicle** to discard alarms which are not triggered by human body or vehicle.
- 10. Set the arming schedule. Refer to Configure Arming Schedule .
- 11. Set linkage actions. Refer to Configure Linkage Actions .
- 12. Click Apply.

6.3.3 Region Entrance Detection

Region entrance detection detects objects that enter a predefined virtual region.

Steps

- 1. Go to Smart Analysis → Smart Event Settings → Perimeter Protection .
- 2. Select a camera.
- 3. Click Region Entrance Detection.

Enable Region Entrance De		
Area Settings Arming Schedule Linkage Action		
	Arming Area 1	•
	Sensitivity 1	100 50
F3591T02 2001	Target 🗌 Human	Vehicle
Stop Drawing Clear		

Figure 6-9 Region Entrance Detection

4. Check Enable Region Entrance Detection.

- 5. Optional: Check Save VCA Picture to save the captured pictures of region entrance detection pictures.
- 6. Optional: Check Enable AI by Device.

The device will analyze the video, and cameras only transmit video stream.

- 7. Set detection rules and detection areas.
 - 1) Select Arming Region. Up to 4 regions are selectable.
 - 2) Set **Sensitivity**. The higher the value is, the easier the detection alarm will be triggered. Its range is [0-100].
 - 3) Click **Draw Region**, and draw a quadrilateral in the preview window.
- **8. Optional:** Draw the maximum size/minimum size for targets. Only the targets in the size ranging from maximum size to minimum size will trigger line crossing detection.
 - 1) Click Max. Size/Min. Size.
 - 2) Draw an area in preview window.
 - 3) Click Stop Drawing.
- **9. Optional:** Select **Target of Interest** as **Human Body** or **Vehicle** to discard alarms which are not triggered by human body or vehicle.
- 10. Set the arming schedule. Refer to Configure Arming Schedule .
- 11. Set linkage actions. Refer to Configure Linkage Actions .
- 12. Click Apply.

6.3.4 Region Exiting Detection

Region exiting detection detects objects that exit from a predefined virtual region.

- 1. Go to Smart Analysis → Smart Event Settings → Perimeter Protection .
- 2. Select a camera.
- 3. Click Region Exiting.

Enable Region Exiting Dete		
Area Settings Arming Schedule Linkage Action		
	Arming Area 1	•
	Sensitivity 1	100 50
	Target 🗌 Human	Vehicle
P359;T02 2001		
Stop Drawing Clear		
Apply		

Figure 6-10 Region Exiting Detection

- 4. Check Enable Region Exiting Detection.
- 5. Optional: Check Save VCA Picture to save the captured region exiting detection pictures.
- 6. Optional: Check Enable AI by Device.

The device will analyze the video, and cameras only transmit video stream.

- 7. Follow these steps to set the detection rules and detection areas.
 - 1) Select Arming Region. Up to 4 regions are selectable.
 - 2) Set **Sensitivity**. The higher the value is, the more easily the detection alarm will be triggered. Its range is [0-100].
 - 3) Click **Draw Region** and draw a quadrilateral in the preview window.
- **8. Optional:** Draw the maximum size/minimum size for targets. Only the targets in the size ranging from maximum size to minimum size will trigger line crossing detection.
 - 1) Click Max. Size/Min. Size.
 - 2) Draw an area in preview window.
 - 3) Click Stop Drawing.
- **9. Optional:** Select **Target of Interest** as **Human Body** or **Vehicle** to discard alarms which are not triggered by human body or vehicle.
- 10. Set the arming schedule. Refer to Configure Arming Schedule .
- 11. Set linkage actions. Refer to Configure Linkage Actions .
- 12. Click Apply.

6.4 Human Body Detection

6.4.1 Human Body Detection

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

Before You Start

The connected camera supports the human body detection.

- 1. Go to Smart Analysis \rightarrow Smart Event Settings \rightarrow Other Events .
- 2. Select a camera.
- 3. Click Human Body.
- 4. Check Save VCA Picture to save the captured pictures of human body detection.
- 5. Check Target of Interest (Human Body) to discard non-human body pictures and videos which are not triggered by human body detection. The feature is only available for local human body detection.
- 6. Set detection area.

	Area Capture Area 1 Enable Area 🗹 Area Name AREA01	•
		8
Draw Area Clear		

Figure 6-11 Human Body Detection

- 1) Select the detection area. Up to 8 detection areas are selectable.
- 2) Check Enable Area to enable the selected detection area.
- 3) Edit the area name.
- 4) Click Draw Area to draw a quadrilateral in the preview window and then click Stop Drawing.
- 7. Set the arming schedule. Refer to Configure Arming Schedule .
- 8. Set linkage actions. Refer to Configure Linkage Actions .
- 9. Click Apply to activate the settings.

6.4.2 Human Body Search

Search by Human Body Event

Search pictures by human body detection alarms.

- 1. Go to Smart Analysis → Smart Search → Human Body Search → Search by Event .
- **2.** Set the start time and end time.
- 3. Select a channel.
- 4. Select Event Type as Human Body Alarm.
- 5. Click Start Search. The search result list displays 1 channel.
- 6. Click **Channel** to select a channel as your desire. It will display search results for the selected channel.
- 7. Optional: Export search results.
 - 1) Select result file(s) from the search result interface, or check **Select All** to select all files.
 - 2) Click **Export** to export the selected file(s) to a backup device.

iNote

- You can click a to view export progress.
- You can click to return to search interface.

Search by Appearance

Search human body pictures according to manually specified search conditions.

Steps

- **1.** Go to Smart Analysis \rightarrow Smart Search \rightarrow Human Body Detection \rightarrow Search by Appearance .
- 2. Specify search conditions.
- 3. Click Start Search. The search result list displays 1 channel.
- **4.** Click **Channel** to select a channel as your desire. It will display search results for the selected channel.
- 5. Optional: Export search results.
 - 1) Select result file(s) from the search result interface, or check Select All to select all files.
 - 2) Click Export to export the selected file(s) to a backup device.

iNote

- You can click a to view export progress.
- You can click to return to search interface.

6.5 Multi-Target-Type Detection

For certain cameras that support multi-target-type detection, faces, human bodies and vehicles can be detected simultaneously in a scene. The camera analyzes the video, so ensure your camera supports multi-target-type detection.

Before You Start

Ensure the camera supports multi-target-type detection.

- **1.** Go to Smart Analysis \rightarrow Smart Event Settings \rightarrow Video Structuralization .
- 2. Select a camera.
- 3. Check Enable Multi-Target-Type Detection.
- 4. Optional: Check Save VCA Picture to save the captured intrusion detection pictures.
- 5. Set detection area.
 - 1) Click Draw Area.
 - 2) Adjust the red frame on the image to draw the detection area. It is full screen by default.
 - 3) Click Stop Drawing.

- **6. Optional:** Set **Capture Quality**. The captured picture will be stored to the device, high quality brings higher resolution, but it takes larger storage space. Picture quality will not affect detection accuracy.
- 7. Set the arming schedule. Refer to *Configure Arming Schedule* .
- 8. Set the linkage method. Refer to Configure Linkage Actions .
- 9. Click Apply.

6.6 Vehicle Detection

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.

6.6.1 Configure Vehicle Detection

Vehicle detection, available in the road traffic monitoring, is tend to detect the passed vehicle on the road, and capture its license plate at the same time.

Steps

- 1. Go to Smart Analysis → Smart Event Settings → Vehicle Detection .
- 2. Select a camera.
- 3. Click Vehicle.
- 4. Check Enable Vehicle Detection.
- 5. Optional: Check Save VCA Picture to save the captured vehicle detection pictures.
- 6. Configure rules, including Area Settings, Picture, Overlay Content, and Blocklist and Allowlist. Area Settings

Up to 4 lanes are selectable.

Blocklist and Allowlist

You can export the file first to see its format, and edit it and import it to the device.

7. Click Apply.

iNote

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

- 8. Set the arming schedule. Refer to Configure Arming Schedule .
- 9. Set the linkage actions. Refer to Configure Linkage Actions .

6.6.2 Vehicle Search

You can search and view the matched vehicle pictures.

Steps

- 1. Go to Smart Analysis → Smart Search → Vehicle Search .
- 2. Select the IP camera for the vehicle search.
- 3. Set search conditions.

Search by Appearance	•					
IP Channel	[All] Camera			•		
Time Segment	Today	-	2017-09-19 00:00:00	-	2017-09-19 23:59:59	
Vehicle Brand	All	•	Vehicle Color	All	~	
Vehicle Model	All	•	License Plate N			

Figure 6-12 Vehicle Search

- 4. Click Start Search. The search result list displays 1 channel.
- **5.** Click Channel to select a channel as your desire. It will display search results for the selected channel.
- 6. Export search results.

Select result file(s) from the search result interface, or check Select All to select all files.
 Click Export to export the selected file(s) to a backup device.

iNote

You can click a to view export progress.

6.7 Target Detection

In live view mode, the target detection function can achieve smart detection, facial detection, vehicle detection, and human body detection during the last 5 seconds and the following 10 seconds.

Steps

- **1.** In Live View mode, click Target Detection to enter the target detection interface.
- Select different detection types: smart detection (), vehicle detection (), face detection (), face detection (), and human body detection ().
- 3. Select the historical analysis (💿) or real-time analysis (🔜) to obtain the results.

iNote

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

4. Optional: You can select channels that require picture capture. The unselected channels will not capture picture.

1) Click 🖙 at the left bottom of live view interface.

- 2) Select channel(s), the checked channel(s) will capture picture. All channels are selected as default.
- 3) Click Finish.

6.8 People Counting

People counting calculates the number of people entering or leaving a certain configured area and creates daily/weekly/monthly/annual reports for analysis.

Steps

- 1. Go to Smart Analysis → Smart Report → Counting .
- **2.** Select a camera.
- **3.** Select the report type.
- 4. Set Date to analyze.



Figure 6-13 People Counting

5. Optional: Click Export to export the report in Microsoft Excel format.

6.9 Heat Map

Heat map is a graphical representation of data. The heat map function is used to analyze how many people visited and stayed in a specific area.

Before You Start

The function must be supported by the connected IP camera and the corresponding parameters must be set.

- 1. Go to Smart Analysis → Smart Report → Heat Map .
- 2. Select a camera.
- 3. Select the report type.
- 4. Set Date to analyze.



Figure 6-14 Heat Map

5. Click Counting.

iNote

As shown in the figure above, red color block (255, 0, 0) indicates the most trafficked area, and blue color block (0, 0, 255) indicates the less-popular area.

The results will be displayed in graphics marked in different colors.

6. Optional: Click Export to export the statistics report in Microsoft Excel format.

Chapter 7 File Management

7.1 Search Files

Specify detailed conditions to search videos and pictures.

Steps

- 1. Go to File Management → All Files/Human Files/Vehicle Files .
- 2. Specify detailed conditions, including time, camera, event type, etc.

iNote

- For All Files, select Time, Camera, File Type, Event type.
- For Human Files, select Time, Camera and File Type to search.
- For Vehicle Files, select Time, Camera, File Type, Plate No., Area/Country.
- **3.** Click **Search** to display results. The matched files will be displayed.
- 4. Select Target Picture or Source Picture in the menu bar to display related pictures only.
 - Target Picture: Display the search results of vehicle close-ups.
 - Source Picture: Display the search results of original pictures captured by camera.

7.2 Export Files

Export files for backup purposes to a USB device, or eSATA HDD.

Steps

- 1. Search files. Refer to Search Files for details.
- 2. Select files.
- 3. Click Export.
- **4. Optional:** For vehicle files, check **Backup License Plate Statistics Info** to export license plate statistics information later.
- 5. Select the file to export as Video and log and click OK.
- 6. Select the backup device and folder path.
- 7. Click OK.

7.3 Smart Search

You can search human body files, face files and vehicles in **File Management** → **Smart Search** . Refer to **Human Body Search Face Picture Search** , and **Vehicle Search** for details.

Chapter 8 Storage

8.1 SSD Management

8.1.1 Initialize SSD

For the device that has pre-installed SSD on main board, you can view the SSD space distribution or initialize the SSD.

Steps

- 1. Go to Storage → Storage Management → SSD Management .
- 2. Click Format.
- 3. Click Yes to initialize SSD.



Initializing SSD will erase its data, including those in face picture library, and cancel the alarms linked to the library. The device will restart after initialization.

8.1.2 SSD S.M.A.R.T. Detection

Self-monitoring, analysis, and reporting technology (S.M.A.R.T.) is a monitoring system included in computer hard disk drives (HDDs) and solid-state drives (SSDs) that detects and reports on various indicators of drive reliability, with the intent of enabling the anticipation of hardware failures. You can run the S.M.A.R.T. detection for your SSD.

Steps

- 1. Go to Maintenance → HDD Operation → S.M.A.R.T
- 2. Set HDD No. as SSD.
- 3. Set Self-Test Type.
- 4. Click Self-Test to start the S.M.A.R.T. SSD self-evaluation.

8.1.3 Upgrade SSD Firmware

You can use a USB flash drive to upgrade your SSD firmware.

Before You Start

Prepare a USB flash drive that contains the SSD firmware, and insert the USB flash drive to your device USB interface.

Steps

1. Go to Storage \rightarrow Storage Management \rightarrow SSD Management .

- 2. Click Firmware Upgrade.
- **3.** Select **Device Name** as the USB flash drive that contains the SSD firmware.
- 4. Select the SSD firmware.
- 5. Click Upgrade.

8.2 Manage Local HDD

8.2.1 Configure HDD Group

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

Steps

- 1. Go to Storage → Storage Mode .
- 2. Select Mode as Group.
- 3. Click Apply.
- 4. Go to Storage \rightarrow Storage Device .
- 5. Select a HDD.

+ Add	\bigcirc Init					Total Capacity	1863.03GB	Free Space	1702.00GB
	Label	Capacity	Status	Property	Туре	Free Space	Group	Edit	Delete
 Image: A start of the start of	5	931.52GB	Normal	R/W	Local	871.00GB	2	Z	×
	7	931.52GB	Normal	R/W	Local	831.00GB	1		×

Figure 8-1 Storage Device

6. Click 🗹 to enter Local HDD Settings interface.

Local HDD Settin	gs			
HDD No.	5			
HDD Property	● R/W	⊖ Read-only	⊖ Redundan.	
Group		○4 ○5 ○6 I ○12 ○13 ○14		
HDD Capacity	931.52GB			
			ок	Cancel

Figure 8-2 Local HDD Settings

- 7. Select a group number for the HDD.
- 8. Click OK.

iNote

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

9. Go to Storage → Storage Mode .

- **10.** Select group number from the list.
- **11.** Select related camera(s) to save videos and pictures on the HDD group.
- 12. Click Apply.

8.2.2 Configure the HDD Property

HDD property can be set as R/W, Read-only, or Redundant.

Before You Start

Set the storage mode to Group. For detailed steps, refer to Configure HDD Group

Steps

1. Go to **Storage** \rightarrow **Storage Device** .

- **2.** Click **of** desired HDD.
- 3. Select HDD Property.

R/W

HDD supports both read and write.

Read-only

Files in read-only HDD will not be overwritten.

Redundant

Save the videos and pictures not only in the R/W HDD but also in the redundant HDD. It effectively enhances the data safety and reliability. Ensure at least another HDD which is in Read/Write status exists.

4. Click OK.

8.2.3 Configure the HDD Quota

Each camera can be configured with an allocated quota for storing videos or pictures.

Steps

- 1. Go to Storage → Storage Mode .
- 2. Select Mode as Quota.
- 3. Select a camera to set quota.
- 4. Enter the storage capacity in the text fields of Max. Record Capacity (GB) and Max. Picture Capacity (GB).
- 5. Click **Copy to** to copy the quota settings of the current camera to other cameras.
- 6. Click Apply.

iNote

- When the quota capacity is set to 0, all cameras will use the total capacity of HDD for videos and pictures.
- Reboot the video recorder to activate the new settings.

8.3 Add a Network Disk

You can add the allocated NAS or IP SAN disk to the device, and use it as a network HDD. Up to 8 network disks can be added.

- 1. Go to Storage → Storage Device .
- 2. Click Add.

Custom Add			
NetHDD	NetHDD 1		•
Туре	NAS		•
NetHDD IP	120 . 36 . 2 . 39		
NetHDD Directory	/nas/device1/11		⊗ Search
		ОК	Cancel

Figure 8-3 Add NetHDD

- 3. Select NetHDD type.
- 4. Enter NetHDD IP address and click Search to search the available NetHDD.
- 5. Select the desired NetHDD.
- 6. Click OK.
- 7. The added NetHDD will be displayed in the HDD list. Select the newly added NetHDD and click Init.

8.4 Manage eSATA

8.4.1 Configure eSATA for Data Storage

When there is an external eSATA device connected to your video recorder, you can configure the eSATA usage as data storage and manage the eSATA.

Steps

- **1.** Go to **Storage** \rightarrow **Advanced** .
- 2. Select eSATA Usage as Export or Record/Capture.

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 8-4 eSATA Mode

What to do next

If eSATA usage is set as **Record/Capture**, enter the storage device interface to edit its property or initialize it.

8.4.2 Configure eSATA for Auto Backup

If you made an automatic backup plan, the video recorder will back up the local videos of 24 hours ahead of the backup start time to eSATA.

Before You Start

Ensure the device has correctly connected with an external eSATA hard drive, and its usage type is set as **Export**. Refer to *Manage eSATA* for details.

Steps

- **1.** Go to **Storage** \rightarrow **Auto Backup** .
- 2. Check Auto Backup.
- 3. Set the backup start time in Start Backup at.

iNote

If the day experiences a failed backup, the video recorder will back up the videos 48 hours ahead of the backup start time in the next day.

- 4. Select channels for backup.
- 5. Select Backup Stream Type as your desire.
- 6. Select Overwrite type.
 - **Disable**: When HDD is full, it will stop writing.
 - Enable: When HDD is full, it will continue to write new files by deleting the oldest files.
- 7. Click Apply.

	Unplanned.					
Settings						
at	00:00		0			
al(s) for Back	kup				Se	lect All
				LD6		D8
□D10	□D11	□D12	D13	D14	□D15	D1
D18	D19	D20	□D21	D22	D23	D24
D26	D27	D28	D29	D30	D31	⊡D3:
n Type	Main Stream	am 🔿 Sub-	Stream 💿 E	Jual-Stream		
	eSATA		•			
	Disable	Enab	le			
	at el(s) for Back D2 D10 D18 D26	att 00.00 el(s) for Backup D2 D2 D3 D10 D11 D18 D19 D26 D27 n Type Main Street eSATA	et 00.00 (eta) for Backup	eKs for Backup	D2 D3 D4 D5 D6 D10 D11 D12 D13 D14 D18 D19 D20 D21 D22 D26 D27 D28 D29 D30 nType Main Stream Sub-Stream Dual-Stream	at 00.00

Figure 8-5 Configure eSATA for Auto Backup

Chapter 9 POS Configuration

The device can be connected to a POS machine/server, and receive a transaction message to overlay on the image during Live View or playback, as well as trigger a POS event alarm.

9.1 Configure POS Connection

Steps

- 1. Go to System → POS .
- 2. Click Add.

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

Figure 9-1 POS Settings

- **3.** Select a POS device from the drop-down list.
- 4. Check Enable.

iNote

The number of POS devices supported by each device is the half of its number of channel, e.g., 8 POS devices are supported for the DS-9616NI-I8 model.

5. Select POS Protocol.



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

Universal Protocol

Click **Advanced** 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	\checkmark
End Line Identifier		Hex	\checkmark
Case Sensitive	\checkmark		
Filtering Identifier	\checkmark		
Enable XML Prot	\checkmark		
	ОК	Can	cel

Figure 9-2 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. Serial port and virtual serial port connection types are supported.

Click **Custom** to configure the AVE settings. Select **Rule** as **VSI-ADD** or **VNET**. Set the address bit of the POS message to send. Click **OK** to save the settings.

NUCLEUS

Click the **Custom** to configure the NUCLEUS settings.

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.

iNote

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

6. Select **Connection Mode** and click **Parameters** to configure the parameters for each connection mode.

TCP Connection

When using TCP connection, the port must be set from 1 to 65535, and the port for each POS machine must be unique.

Set the **Allowed Remote IP Address** of the device sending the POS message.

UDP Connection

When using UDP connection, the port must be set from 1 to 65535, and the port for each POS machine must be unique.

Set the Allowed Remote IP Address of the device sending the POS message.

USB-to-RS-232 Connection

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

USB-to-RS-232 Setting	S		
Serial Port Number	1		-
Baud Rate	4800		-
Data Bit	5		-
Stop Bit	1		-
Parity	None		•
Flow Ctrl	None		•
		ок	Cancel

Figure 9-3 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** \rightarrow **Configuration** \rightarrow **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	\checkmark					
Enable Destination P	\checkmark					
Destination Address	20 . 18 . 1 . 24					
Destination Port	10030					
	OK Cancel					

Figure 9-4 Sniff Settings

9.2 Configure POS Text Overlay

Steps

- 1. Go to System \rightarrow POS .
- 2. Click Channel Linkage and Display.

Channel Linkage and Display Arming Schedule Event Linkage				
	Linked Channel	[D1] IPCam	era 02	
	Character Encod	UTF-8		•
	Overlay Mode	Page		-
	Font Size	Large	Medium	Small
	Font Color			
	Display for(s)	30		
	Timeout(s)	5		
	Privacy Settings	1634	0921	543
		For example, the	entered card numb	er will be shown
	Overlay POS in			

Figure 9-5 Overlay Character Settings

- 3. Select linked channel to overlay the POS characters.
- 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 mod

- 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 within the defined time, the transaction ends.
- **5.** In **Privacy Settings**, set the POS privacy information to not display on the image, e.g., the card number, user name, etc.

The defined privacy information will be displayed using ***on the image instead.

6. Check Overlay POS in Live View. When this feature is enabled, the POS information is overlaid on the Live View image.

i Note

Drag the frame to adjust the textbox size and position on POS settings interface preview screen.

7. Click Apply to activate the settings.

9.3 Configure POS Alarm

A POS event can trigger channels to start recording, or trigger full screen monitoring or an audio warning, notifying the surveillance center, send e-mail, etc.

- 1. Go to Storage → Recording Schedule .
- **2.** Set the POS event's arming schedule.
- 3. Go to System → POS .
- 4. Click Event Linkage on the POS adding or editing interface.

Normal Linkage	Trigger Alarm Output	Trigger Channel	
☑ Full Screen Monitoring	⊡Local->1	⊡D1	
Audible Warning	Local->2	⊡D2	
Send Email	✓Local->3	D 3	
	Local->4	D4	
	10.15.2.250:8000->1		
vtice: please confirm the e	event output in "Live View" settings	menu is the same with the real	event output.

Figure 9-6 Set Trigger Cameras of POS

- 5. Select the normal linkage actions.
- 6. Select one or more alarm output(s) to trigger.
- **7.** Select one or more channels to record or become full-screen monitoring when a POS alarm is triggered.
- 8. Click Apply to save the settings.

Chapter 10 Hot Spare Recorder Backup

Video recorders can form an N+1 hot spare system. The system consists of several working video recorders and a hot spare video recorder; when the working video recorder fails, the hot spare video recorder switches into operation, thus increasing the reliability of the system. Contact your dealer for details of models that support the hot spare function.

A bidirectional connection shown in the figure below is required to be built between the hot spare video recorder and each working video recorder.



Figure 10-1 Building a Hot Spare System

10.1 Set Hot Spare Device

Hot spare devices takes over working device tasks when working device fails.

Steps

- **1.** Go to **System** → Hot Spare .
- 2. Select Work Mode as Hot Spare Mode.

÷	General	Work Mode	Hot Spare Mode -
2	User		
	Network >		
	Event >		
	Live View >		
	Holiday Settings		
Ð			

Figure 10-2 Hot Spare

- 3. Click Apply.
- **4.** Click **Yes** in the pop-up attention box to reboot the device.

iNote

- The camera connection will be disabled when the device works in hot spare mode.
- It is highly recommended to restore the device defaults after switching the working mode of the hot spare device to normal mode to ensure the normal operation afterward.

10.2 Set Working Recorder

Steps

- **1.** Go to **System** \rightarrow **Hot Spare** .
- 2. Select Work Mode as Normal Mode.
- 3. Check Enable.
- 4. Enter IP address, user name, and admin password of the hot spare recorder.

Work Mode	Normal Mode
Enable	
IPv4 address of the hot spare device	10 . 15 . 1 . 106
User Name of Hot Spare Device	admin
Password of the hot spare device	*******
Working Status	Connected
*Notice: After the hot spare is enabled, y otherwise, this function is not available.	you must link the working device to the hot spare device,

Figure 10-3 Hot Spare

5. Click Apply.

10.3 Manage Hot Spare System

Steps

- 1. Go to System → Hot Spare in the hot spare recorder.
- 2. Check working recorders on the device list and click Add to link the working recorder to the hot spare recorder. The working recorder working status descriptions are as follows:

No record

The working recorder works properly.

Backing up

If the working recorder goes offline, the hot spare recorder will record the videos of the network camera connected to the working device. The video back up functions for one working recorder at a time.

Synchronizing

When the working recorder comes back online, the lost videos will be restored by the video synchronization function. The video synchronization function can be enabled for one working recorder at a time.

iNote

A hot spare recorder can connect up to 32 working recorders.

Work Mode	Hot Spare Mode	-		
Device List				
🔲 No.	IP Address			
1	10.15.2.107			
Add				
Add Working Dev				
	Connection Status	Working Status	Delete	
Working Dev	Connection Status	Working Status	Delete	_
Working Dev	Connection Status	Working Status	Delete	
Working Dev	Connection Status	Working Status	Delete	
Working Dev	Connection Status	Working Status	Delete	
Working Dev	Connection Status	Working Status	Delete	
Working Dev	Connection Status	Working Status	Delete	
Working Dev	Connection Status	Working Status	Delete	
Vorking Dev	Connection Status	Working Status	Delete	

Figure 10-4 Add Working Recorder

Chapter 11 Network Settings

11.1 Configure DDNS

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 the DynDNS, PeanutHull, or NO-IP services with your ISP before configuring DDNS settings.

Steps

1. Go to System → Network → TCP/IP → DDNS

Enable			
DDNS Type	DynDNS -	User Name	test
Server Address	member.dyndns.org	Password	******
Device Domain Name	1233dyndns.com		
Status	DDNS is disabled.		

Figure 11-1 DDNS Settings

- 2. Check Enable.
- 3. Select DDNS Type as DynDNS.
- **4.** Enter Server Address for DynDNS (i.e., members.dyndns.org).
- 5. Under Device Domain Name, enter the domain name obtained from the DynDNS Website.
- 6. Enter User Name and Password registered in the DynDNS Website.
- 7. Click Apply.

11.2 17.3 Configure PPPoE

If the device is connected to Internet through PPPoE, you need to configure user name and password accordingly under System \rightarrow Network \rightarrow TCP/IP \rightarrow PPPoE.

Contact your Internet service provider for details about PPPoE service.

11.3 Configure Port Mapping (NAT)

Two ways are provided for port mapping to realize the remote access via the cross-segment network, UPnP[™] and manual mapping.

Before You Start

If you want to enable the UPnP[™] function of the device, you must enable the UPnP[™] function of the router to which your device is connected. When the network working mode of the device is set as multi-address, the Default Route of the device should be in the same network segment as that of the LAN IP address of the router.

Universal Plug and Play (UPnP[™]) can permit the device seamlessly discover the presence of other network devices on the network and establish functional network services for data sharing, communications, etc. You can use the UPnP[™] function to enable the fast connection of the device to the WAN via a router without port mapping.

Steps

1. Go to System \rightarrow Network \rightarrow TCP/IP \rightarrow NAT .

						_
Port Type	Edit	External Port	External IP Address	Port	UPnP Status	
					Inactive	
		554			Inactive	
Server Port		8000			Inactive	
		443		443	Inactive	
inhanced SDK Servic	:e 🗹	8443		8443	Inactive	

Figure 11-2 Port Mapping Setting

2. Check Enable.

3. Select Mapping Type as Manual or Auto.

- Auto: If you select **Auto**, the port mapping items are read-only, and the external ports are set by the router automatically.
- Manual: If you select **Manual**, you can edit the external port on your demand by clicking to activate **External Port Settings**.

iNote

- You can use the default port No., or change it according to actual requirements.
- External Port indicates the port No. for port mapping in the router.
- The value of the RTSP port No. should be 554 or between 1024 and 65535, while the value of the other ports should be between 1 and 65535 and the value must be different from each

other. If multiple devices are configured for the UPnP[™] settings under the same router, the value of the port No. for each device should be unique.

4. Enter the virtual server setting page of router; fill in the blank of **Internal Source Port** with the internal port value, the blank of **External Source Port** with the external port value, and other required contents.



- Each item should be corresponding with the device port, including server port, http port, RTSP port and https port.
- The virtual server setting interface below is for reference only, it may be different due to different router manufactures. Please contact the manufacture of router if you have any problems with setting virtual server.



Figure 11-3 Setting Virtual Server Item

11.4 Configure SNMP

You can configure SNMP settings to get device status and parameter information.

Before You Start

Download the SNMP software to receive device information via the SNMP port. By setting the trap address and port, the device is allowed to send alarm events and exception messages to the surveillance center.

```
1. Go to System \rightarrow Network \rightarrow Advanced \rightarrow SNMP.
```

V2 ~
161
public
private
162

Figure 11-4 SNMP Settings

- 2. Check Enable. A message will pop up to notify about a possible security risk. Click Yes to continue.
- **3.** Configure the SNMP settings as needed.

Trap Address

SNMP host IP address.

Trap Port

Port of the SNMP host.

4. Click Apply.

iNote

You can configure SNMP v2 and SNMP v3 parameters via web browser in **Configuration** \rightarrow **System** \rightarrow **Advanced Settings** \rightarrow **SNMP**.

11.5 Configure Email

The system can be configured to send an e-mail notification to all designated users when a specified event occurs such as when 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 also be connected to either an intranet or the Internet depending on the location of the e-mail accounts to which you want to send notifications.

Steps

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			

1. Go to System → Network → Advanced → Email .

Figure 11-5 Email Settings

2. Configure the email settings.

Enable Server Authentication

Check to enable the function if the SMTP server requires user authentication and enter the 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 sender's name.

Sender's Address

The sender's address.

Select Receivers

Select the receiver. Up to 3 receivers can be configured.

Receiver

The receiver's name.

Receiver's Address

The e-mail address of the user to be notified.

Enable Attached Picture

Check to send e-mail with attached alarm images. The interval is the time between sending two subsequent alarm images.

3. Click Apply.

4. Optional: Click Test to send a test email.

11.6 Configure Port

You can configure different types of ports to enable relevant functions.

Steps

1. Go to System \rightarrow Network \rightarrow Advanced \rightarrow More Settings .

Alarm Host IP	
Alarm Host Port	0
Server Port	8000
HTTP Port	80
Multicast IP	
RTSP Port	554
Enhanced SDK Ser	8443
Apply	

Figure 11-6 Port Settings

2. 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 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. Both IPv4 and IPv6 are available for multicast IP address. For IPv4, it covers Class-D IP ranging from 224.0.0.0 to 239.255.255.255 and it is recommended to use an 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 to control streaming media servers. The port is 554 by default.

Enhanced SDK Service Port

The enhanced SDK service adopts TLS protocol over the SDK service that provides safer data transmission. The port is 8443 by default.

3. Click Apply.

11.7 Configure ONVIF

ONVIF protocol allows the connection with third-party cameras. The added user accounts have the permission to connect other devices via ONVIF protocol.

Steps

- **1.** Go to **Maintenance** \rightarrow **System Service** \rightarrow **ONVIF**.
- 2. Check Enable ONVIF to enable the ONVIF access management.

iNote

ONVIF protocol is disabled by default.

- 3. Click Add.
- 4. Enter User Name, and 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.

- 5. Select Level as Media User, Operator or Admin.
- 6. Click OK.

Chapter 12 User Management and Security

12.1 Manage User Accounts

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 users and configure user parameters.

12.1.1 Add a User

Steps

- **1.** Go to **System** \rightarrow **User** .
- 2. Click Add to enter the operation permission interface.
- 3. Input the admin password and click OK.
- **4.** In the Add User interface, enter the information for a new user.

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. We also recommend that you reset your password regularly. Especially in the high security systems, 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: An Operator user level has Two-way Audio permission in Remote Configuration and all operating permissions 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 that logs onto the device. If it is configured and enabled, it allows only the remote user with this MAC address to access the device.

5. Click OK.

In the User Management interface, the added new user is displayed on the list.

12.1.2 Edit the Admin User

For the admin user account, you can modify your password and unlock pattern.

Steps

- 1. Go to System → User .
- 2. Select the admin user from the list.
- 3. Click Modify.

Edit User		\times
User Name	admin	
Password	*****	Discard C
Confirm	******	
Note:Va	lid password range (8-16). You can u	ISE
Password S		
Password 5		
User's MAC Ad	00 : 00 : 00 : 00 : 00 : 00	Γ
Unlock Patt	Enable Unlock Pattern	>
GUID File	□Export ⑦)
Security Qu	\odot	
Reserved E		⑦ Modify
	ОК	Cancel

Figure 12-1 Edit User (Admin)

- **4.** Edit the admin user information as desired, including a new admin password (strong password is required) and MAC address.
- 5. Edit the unlock pattern for the admin user account.
 - 1) Check **Enable Unlock Pattern** to enable the use of an 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.
- 6. Check Export of GUID File to export the GUID file for the admin user account.

iNote

When the admin password is changed, export the new GUID to the connected USB flash drive in the Import/Export interface for the future password resetting.

- 7. Configure security question for password resetting.
- 8. Configure reserved email for password resetting.

9. Click OK to save the settings.

12.1.3 Edit an Operator/Guest User

You can edit the user information, including user name, password, permission level, and MAC address.

Steps

- **1.** Go to **System** \rightarrow **User** .
- 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 12-2 Edit User (Operator/Guest)

- **3.** Edit the user information as desired, including the new password (strong password is required) and MAC address.
- 4. Click OK.

12.2 Manage User Permissions

12.2.1 Set User Permissions

For an added user, you can assign the different permissions, including local and remote operation of the device.

- **1.** Go to **System** \rightarrow **User** .
- **2.** Select a user from the list, and then click 🞯 to enter the permission settings interface.

Permission			\times
Local Configuration	Remote Configuration	Camera Configuration	1
✓Local Log Search			
Local Parameters	Settings		
Local Camera Ma	nagement		
Local Advanced O	peration		
Local Shutdown /	Reboot		
	Apply	ок	Cancel

Figure 12-3 User Permission Settings Interface

- **3.** Set the user's operating permissions for Local Configuration, Remote Configuration, and Camera Configuration for the user.
 - 1) Set 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

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.

2) Set 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 port settings.

Remote Video Output Control

Sending remote button control signals.

Two-Way Audio

Operating the 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.

3) Set 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).

Local Live View

View live video of the selected camera(s) in local.

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

12.2.2 Set Live View Permission on Lock Screen

The admin user can set live view permission for specific cameras in the screen lock status of device.

- The admin user can set this permission for user accounts.
- When the normal user (Operator or Guest) has no local live view permission for specific camera (s), the live view permission for such camera (s) on lock screen status cannot be configured (live view not allowed by default).

- **1.** Go to **System** \rightarrow **User**.
- 2. Click Live View Permission on Lock Screen.
- 3. Input admin password and click Next.

Local Live V	/iew					\times
Camera					Select All	
⊡ D1	✓ D2	D 3	✓ 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	
All the	e users will h	ave the live v	/iew permissi	ion of selecte	ed channels.	
-			·			
		App	bly	ок	Cancel	

Figure 12-4 Set Live View Permissions on Lock Screen

- **4.** Set the permissions.Select the camera (s) to allow live view when the current user account is in logout status.
- 5. Click OK.

12.3 Configure Password Security

12.3.1 Export GUID File

The GUID file can help you to reset password when you forget it. You can export GUID file via web browser. Please keep the GUID file properly.

Before You Start

Ensure you are on the same network segment with your device.

- 1. Go to Configuration → System → User Management → User Management .
- 2. Select the admin user.
- 3. Click Account Security Settings.
- 4. Click Modify.

Security Question Config		
Security Question1	Your father's name?	
Answer		
Security Question2	Your mother's name?	
Answer		
Security Question3	Your head teacher's name in senior high schoo $oldsymbol{ u}$	
Answer		
Export GUID File		
Export		
Password Recovery via E	E-mail 🕐	
Password Recovery via E-ma	a	

Figure 12-5 Export GUID File

- 5. Click Export in Export GUID File.
- 6. Enter the admin password.
- 7. Save the GUID file to a directory as your desire.

12.3.2 Configure Security Questions

The security questions can help you to reset password when you forget your password, or encounter security issues. You can configure security questions via web browser.

Before You Start

Ensure you are on the same network segment with your device.

Steps

- 1. Go to Configuration → System → User Management → User Management .
- 2. Select the admin user.
- 3. Click Account Security Settings.
- 4. Click Modify.

Security Question Con	
Security Question1	Your father's name?
Answer	
Security Question2	Your mother's name?
Answer	
Security Question3	Your head teacher's name in senior high schoo \checkmark
Answer	
Export GUID File ᠀	
Export	
Password Recovery v	ia E-mail 🕜
Password Recovery via E-	mail
	OK

Figure 12-6 Configure Security Questions

- 5. Set the security questions.
- 6. Click OK.
- 7. Enter the admin password.
- 8. Click OK.

12.3.3 Configure Reserved Email

The reserved email will help you to reset password when you forget your password.

Steps

- 1. Check **Reserved E-mail** when you are activating the device, or click **Modify** when you are editing the admin user account.
- 2. Enter reserved email address.

Edit User		×
User Name	admin	
Password	****	Modify
User's MAC Ad	00 : 00 : 00 : 00 : 00 : 00	
Unlock Patt	🛛 Enable Unlock Pattern 👘 🛞	
GUID File	Export (?)	
Security Qu	0	
Reserved E	z******@*******.com	⑦ Modify
	ОК	Cancel

Figure 12-7 Configure Reserved Email

3. Click OK.

12.4 Reset Password

When you forget the admin password, you can reset the password by importing the GUID file, answering security questions, or entering verification code from your reserved email.

12.4.1 Reset Password by GUID

You can reset password by GUID via web browser.

Before You Start

Ensure you have the correct GUID file.

- 1. On the user login interface, click Forgot password?.
- 2. Select Verification Mode as GUID File Verification.
- 3. Click Browse to locate the GUID file.
- 4. Click Next.

5. Enter a new password.

Warning

We highly recommend you to create a strong password of your own choosing (using a minimum of 8 characters, including at least three kinds of 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 change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

- **6.** Confirm the new password.
- 7. Click Next.

12.4.2 Reset Password by Security Questions

You can reset password by answering security questions via web browser.

Before You Start

Ensure you have configured the security questions when you activate the device or edit the admin user account.

Steps

- 1. On the user login interface, click Forgot password?.
- 2. Select Verification Mode as Security Question Verification.
- **3.** Enter the answers of each question.
- 4. Click Next.
- 5. Enter a new password.

Warning

We highly recommend you to create a strong password of your own choosing (using a minimum of 8 characters, including at least three kinds of 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 change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

6. Click Next.

12.4.3 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 *Configure Reserved Email*)

Steps

1. On the user login interface, click Forgot Password.

- 2. On the password reset type interface, Select Verify by Reserved Email.
- 3. Click OK.
- **4.** Click **Next** if you accept the legal disclaimer. You can use a smartphone to scan the QR code and read the legal disclaimer.
- 5. 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.
 - a. Insert a USB flash drive to your device.
 - b. Click **Export** to export the QR code to USB flash drive.
 - c. Email the QR code to *pw_recovery@device-service.com* as attachment.
- 6. Check your reserved email, and you will receive a verification code within 5 minutes.
- 7. Enter the verification code.
- 8. Click OK to set the new password.

12.4.4 Reset Password by Guarding Vision

Before You Start

Ensure your device has enabled Guarding Vision, and bound with a registered Guarding Vision account.

- 1. On the user login interface, click Forgot Password.
- 2. On the password reset type interface, select Verify by Guarding Vision.
- 3. Log in to Guarding Vision app with the account that has bound with your device.
- **4.** Use Guarding Vision to scan the QR code. Thereafter, you will have a verification code from Guarding Vision.
- **5.** Enter the verification code.
- 6. Click OK.

Chapter 13 System Management

13.1 Configure Device

Steps

- **1.** Go to **System** → **General** .
- 2. Configure the following settings.

Language

The default language used is English.

Output Standard

Set the output standard to NTSC or PAL, which must be the same as the video input standard.

Resolution

Configure video output resolution.

Device Name

Edit device name.

Device No.

Edit the device serial number. The Device No. can be set in the range of 1 to 255, and the default No. is 255. The number is used for the remote and keyboard control.

Auto Logout

Set the 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 the 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.

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

13.2 Configure Time

13.2.1 Manual Time Synchronization

Steps

- 1. Go to System → General .
- **2.** Configure the date and time.
- 3. Click Apply to save the settings.

13.2.2 NTP Synchronization

Connection to a network time protocol (NTP) server can be configured on your device to ensure the system's date and time accuracy.

Steps

- 1. Go to System \rightarrow Network \rightarrow TCP/IP \rightarrow NTP .
- 2. Check Enable.
- **3.** Configure NTP settings as need.

Interval (min)

Time interval between two time synchronization with NTP server

NTP Server

IP address of the NTP server

NTP Port

Port of the NTP server

4. Click Apply

13.2.3 DST Synchronization

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).

Steps

- **1.** Go to **System** \rightarrow **General** .
- 2. Check Enable DST.
- 3. Set DST mode as 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.

- **4.** Set the DST Bias. Set the time (30/60/90/120 minutes) offset from the standard time.
- 5. Click Apply to save the settings.

13.3 Network Detection

13.3.1 Network Traffic Monitoring

Network traffic monitoring is the process of reviewing, analyzing and managing network traffic for any abnormality or process that can affect network performance, availability and/or security.

Steps

- 1. Go to Maintenance → Network → Traffic .
- 2. You can view the real-time network traffic status, including MTU (Maximum Transmission Unit), and network throughput.



Figure 13-1 Network Traffic

13.3.2 Test Network Delay and Packet Loss

Network delay is caused by slow response of the device when oversized data information is not limited during transmission under certain network protocol, e.g. TCP/IP. Packet loss test is for testing network packet loss rate that is the ratio of lost data packet and total number of transmitted data packet.

- **1.** Go to Maintenance \rightarrow Network \rightarrow Network Detection .
- 2. Select a network card in Select NIC.

- 3. Enter the destination IP address in Destination Address.
- 4. Click Test.

Network Delay, Packet	Loss Test		
Select NIC	LAN1	•	
Destination Address	10.6.114.33		Test

Figure 13-2 Test Network Delay and Packet Loss

13.3.3 Export Network Packet

After the recorder accessing network, you can use USB flash drive to export network packet.

Before You Start

Prepare a USB flash drive to export network packet.

Steps

- **1.** Insert the USB flash drive.
- 2. Go to Maintenance → Network → Network Detection .
- **3.** Select network card in **Select NIC**.
- **4.** Select the USB flash drive in **Device Name**. You can click **Refresh** if the connected local backup device cannot be displayed.

Network Packet Ex	port			
Device Name	USB Flash Disk 1-1	•	Refresh	Status
LAN1	10.6.114.17	3,132Kbps		Export

Figure 13-3 Export Network Packet

- 5. Optional: Click Status to view the network status.
- 6. Click Export.

iNote

It will export 1 MB data each time as default.

13.3.4 Network Resource Statistics

The remote access, including web browser and client software, will consume output bandwidth. You can view the real-time bandwidth statistics.

Steps

1. Go to Maintenance → Network → Network Stat .

Refresh		
Туре	bandwidth	
IP Camera	5,120Kbps	
Remote Live View	0bps	
Remote Playback	0bps	
Net Receive Idle	155Mbps	
Net Send Idle	160Mbps	

Figure 13-4 Network Resource Statistics

- 2. View the bandwidth statistics, including IP Camera, Remote Live View, Remote Play, Net Total Idle, etc.
- 3. Optional: Click Refresh to obtain the latest data.

13.4 Storage Device Maintenance

13.4.1 Bad Sector Detection

- 1. Go to Maintenance → HDD Operation → Bad Sector Detection .
- **2.** Select the HDD No. you want to configure in the dropdown list.
- 3. Select All Detection or Key Area Detection as the detection type.
- 4. Click Self-Test to start the detection.

	Detecting Process	Testing 2
	HDD Capacity	931.52GB
	Block Size	232.88MB
	Error Count	0
	Error Information	
	Error information	

Figure 13-5 Bad Sector Detection

iNote

- You can pause/resume or cancel the detection.
- After testing has been completed, you can click **Error information** to see the detailed damage information.

13.4.2 S.M.A.R.T. Detection

HDD detection functions such as the adopting of the S.M.A.R.T. and the Bad Sector Detection techniques. S.M.A.R.T. (Self-Monitoring, Analysis and Reporting Technology) are HDD monitoring systems to detect various reliability indicators in the hopes of anticipating failures.

Steps

- 1. Go to Maintenance → HDD Operation → S.M.A.R.T.
- 2. Select the HDD to view its S.M.A.R.T. information list.
- 3. Set Self-Test Type.
- 4. Click Self-Test to start the S.M.A.R.T. HDD self-evaluation.

Test Typ	be Short Test	-	Self-Test	Not tested			
perature.	36		Self-Evaluation	Pass			
rking Time 390			All-Evaluation	Functional			
A.R.T Inf	Attribute Name Raw Read Error R	Status OK	Flags 2f	Threshold 51	Value 200	Worst 200	Raw Value 8
0x3	Spin Up Time	ок	27	21	113	107	7316
	Start/Stop Count	ок	32	0	98	98	2657
0x4		ок	33	140	200	200	0
0x4 0x5	Reallocated Sector		2e	0	200	200	0
	Reallocated Sector Seek Error Rate	OK	Ze	•			
0x5		ок ок	32	0	88	88	9369
0x5 0x7	Seek Error Rate					88 100	9369 0

Figure 13-6 S.M.A.R.T. Settings Interface

iNote

To use the HDD even when the S.M.A.R.T. checking has failed, check **Continue to use the disk** when self-evaluation is failed.

The related information of the S.M.A.R.T. is shown, and you can check the HDD status.

13.4.3 HDD Health Detection

You can view the health status of a 4 TB to 8 TB Seagate HDD that generated after October 1, 2017. Use this function to help troubleshoot HDD problems. Health Detection shows a more detailed HDD status than the S.M.A.R.T. function.

Steps

1. Go to Maintenance \rightarrow HDD Operation \rightarrow Health Detection .

System Info Log Information	>	16 HDD (s)	in total. The detectio	n is only ava	ailable for the Seaga	ate HDD.			() STRANK
Import/Export Upgrade Default	>	No.1	HDD is healthy.	No.2	HDD is healthy.	No.3	HDD is healthy.	No.4	HDD is healthy.
	> ~	№.5	HDD is healthy.	No.6	HDD is healthy.	No.7	HDD is healthy.	No.8	HDD is healthy.
HDD Clone Health Detection		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.	No.15	HDD is healthy.	No.16	HDD is healthy.

Figure 13-7 Health Detection

2. Click a HDD to view details.

13.4.4 Configure Disk Clone

Select the HDDs to clone to the eSATA HDD.

Before You Start

Connect an eSATA disk to the device.

Steps

1. Go to **Maintenance** \rightarrow **HDD Operation** \rightarrow **HDD Clone**.

lone Source						
Label	Capacity	Status	Property	Туре	Free Space	Group
1	1863.02GB	Normal	RAV	Local	1858.00GB	1
2	2794.52GB	Normal	RAW	Local	2794.00GB	1
5	1863.02GB	Normal	RW	Local	1862.00GB	1
9	2794.52GB	Normal	R/W	Local	2794.00GB	1
□10	1863.02GB	Normal	R/W	Local	1862.00GB	1
Clone Destination	on					
SATA	eSATA1				•	Refresh
Capacity	2794.52GB					Clone

Figure 13-8 HDD Clone

- **2.** Check the HDD to clone. The capacity of the selected HDD must match the capacity of the clone destination.
- 3. Click Clone.
- 4. Click Yes on the pop up message box to create the clone.

13.4.5 Repair Database

Repairing database will rebuild all databases. It might help to improve your system speed after upgrade.

Steps

- 1. Go to Storage → Storage Device .
- 2. Select the drive.
- 3. Click Repair Database.
- 4. Click Yes.

iNote

- Repairing database will rebuild all databases. Existing data will not be affected, but local search and playback functions will not be available during the process, you can still achieve search and playback functions remotely via web browser, client software, etc.
- Do not pull out the drive, or shut down the device during the process.
- You can see the repairing progress at Status.

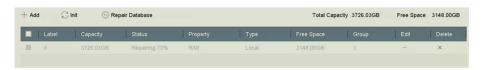


Figure 13-9 Repair Database

13.5 Upgrade Device

Your device firmware can be upgraded with a local backup device or remote FTP server.

13.5.1 Upgrade by Local Backup Device

Before You Start

Connect your device to a local storage device that contains the firmware update file.

Steps

- **1.** Go to **Maintenance** \rightarrow **Upgrade** .
- 2. Click Local Upgrade to enter the local upgrade interface.

Device Name US	B Flash Disk 1-1	Ŧ	File Format	*.dav;*.mav;*.iav	•		C Refresh
① Upgrade							
File Name	File Size		File Type	Edit Date	Delete	Play	

Figure 13-10 Local Upgrade Interface

- **3.** Select the firmware update file from the storage device.
- 4. Click Upgrade to start upgrading.

After the upgrade is completed, the device will reboot automatically to activate the new firmware.

13.5.2 Upgrade by FTP

Before You Start

Ensure the network connection of the PC (running FTP server) and the device are valid and correct. Run the FTP server on the PC and copy the firmware into the corresponding directory of your PC.

- **1.** Go to **Maintenance** \rightarrow **Upgrade** .
- 2. Click FTP to enter the local upgrade interface.

Figure 13-11 FTP Upgrade Interface

- 3. Enter FTP Server Address.
- 4. Click Upgrade to start upgrading.
- **5.** After the upgrading is complete, reboot the device to activate the new firmware.

13.5.3 Upgrade by Web Browser

You can upgrade the device by web browser

After logging in to the device via web browser, go to **Configuration** \rightarrow **System** \rightarrow **Maintenance** \rightarrow **Upgrade**. Click **Browse** to upload the firmware, and upgrade the device.

13.5.4 Upgrade by Guarding Vision

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.

Steps

- **1.** Go to **Maintenance** \rightarrow **Upgrade** \rightarrow **Online Upgrade**.
- 2. Click Check Upgrade to manually check and download the latest firmware from Guarding Vision.

i Note

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.

- **3. Optional:** You can switch on **Download Latest Package Automatically** to automatically download the latest firmware package.
- 4. Click Upgrade Now.

13.6 Import/Export Device Configuration Files

The device configuration files can be exported to a 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.

Before You Start

Connect a storage device to your device. To import the configuration file, the storage device must contain the file.

Steps

1. Go to Maintenance → Import/Export .

Device Name USB	Flash Disk 1-1	 File Format *.bit 	n -			\bigcirc Refres
+ New Folder	🕒 Import	🗅 Export			Total Free Capacity	9165.35M
Name	Size	Туре	Modify Date	Delete	Play	
devCfg_7597083	01 1260.94KB	File	18-08-2017 18:28:09	×		

Figure 13-12 Import/Export Config File

- **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 importing configuration files, the device will reboot automatically.

13.7 Log Management

13.7.1 Log Storage

You can customize the log storage disk and log storage period.

Steps

1. Go to **Storage** \rightarrow **Advanced**.

Log Storage Mode	Custom	τ.	
Log Storage Period		90	Day
Log Disk/Array No.	2	103	
Apply			

Figure 13-13 Log Storage

2. Set Log Storage Mode.

System	Each disk will allocate a certain space to store about 400,000 logs. When logs
Default	are full, old logs will be overwritten.
Custom	You can set Log Storage Period and allocate Log Disk for log storage. When

the log disk is full, logs that exceed the period will be overwritten.

3. Click Apply.

13.7.2 Search & Export Log Files

The device operation, alarm, exception, and information can be stored in log files, which can be viewed and exported at any time.

Steps

1. Go to **Maintenance** → Log Information .

0						
Time 20	17-08-18 00:00:00	. 2017-08	8-18 23:59:59	Ē	Search	
Major Type	Al	-				
Minor Type	Select All					

Figure 13-14 Log Search Interface

- 2. Set the log search conditions, including the time, major type and minor type.
- 3. Click Search to start searching the log files.
- **4.** The matched log files will be displayed on the list, as shown below.

гT	ype	Ali	-							
r	Search	Result							E	Expor
•	No	Major Type	Time	Minor Type	Parameter	Play	Details			
	103	Alarm	18-08-2017 07:07:31	Motion Detection	N/A	•	0			
	104	Alarm	18-08-2017 07:07:43	Motion Detection	N/A	•				
	105	Alarm	18-08-2017 07:16:27	Motion Detection	N/A	•				
	106	Alarm	18-08-2017 07:16:37	Motion Detection	N/A	•				
	107	🔵 Inform	18-08-2017 07:17:19	System Running	N/A					
	108	😋 Inform	18-08-2017 07:17:19	System Running	N/A					
	109	😋 Inform	18-08-2017 07:18:00	HDD S.M.A.R.T.	N/A					
	110	😋 Inform	18-08-2017 07:18:00	HDD S.M.A.R.T.	N/A					
	111	🔵 Inform	18-08-2017 07:27:20	System Running	NA	-	0			
	Total: 1	151 P: 2/12			К	< > >		Go		
						Export	Back			
2	Sudden	Change of Sound	Intensity Alarm Started							
2	Sudden	Change of Sound	Intensity Alarm Stopped							

Figure 13-15 Log Search Results

iNote

Up to 2,000 log files can be displayed each time.

5. Related Operation:

(i)	Click or double-click it to view detailed information.
	Click it to view the related video file.
Export/Export ALL	Click it to export all the system logs to the storage device.

13.7.3 Upload Logs to the Server

You can upload system logs to the server for backup.

Steps

1. Go to System → Network → Advanced → Log Server Settings .

Enable	$\overline{\mathbf{v}}$			
Upload Time Interval (h)	1			
Server IP Address	1.0.00			
Port	100			
Test	Apply			

Figure 13-16 Log Server Settings

- 2. Check Enable
- 3. Set Upload Time, Server IP Address, and Port.
- 4. Optional: Click Test to test if parameters are valid.
- 5. Click Apply.

13.7.4 One-Way Authentication

You can install a CA certificate (from the server) to your device to authorize the server via web browser, this would improve the log communication security.

Before You Start

- Download the CA certificate from the server.
- Ensure log server parameters are valid.

Steps

1. Go to **Configuration** → **Network** → **Advanced Settings** → **Log Server Configuration** .

Enable			
Log Server Address	位19.201.168		
Log Server Port	8042		
Upload Time Interval (h)	T		
	Test		
Client Certificate			
Create Certificate Request	Create No file.		
Download Certificate Req.	. Download		
Delete Certificate Request	Delete		
Install Generated Certificat	e	Browse	Install
CA Certificate			
Install		Browse	Install
🖹 Save			

Figure 13-17 One-Way Authentication

- 2. Install the CA certificate in CA Certificate.
- 3. Optional: Click Test to test if the connection is valid.
- 4. Click Save.

13.7.5 Two-Way Authentication

You can install a CA certificate (from the server) to your device to authorize the server, and create a certificate (from your device) to authorize your device by the server. This would improve the log communication security. Two-way authentication can be configured via web browser.

Before You Start

- Download the CA certificate from the server.
- Ensure log server parameters are valid.

Steps

1. Go to **Configuration** \rightarrow **Network** \rightarrow **Advanced Settings** \rightarrow **Log Server Configuration**.

Enable	
Log Server Address	10.10.201.168
Log Server Port	9042
Upload Time Interval (h)	T
	Test
Client Certificate	
Create Certificate Request	Create No file.
Download Certificate Req.	Download
Delete Certificate Request	Delete
Install Generated Certificat	Browse Install
CA Certificate	
Install	Browse Install
🖹 Save	

Figure 13-18 Two-Way Authentication

- 2. Install the CA certificate in CA Certificate.
- **3.** Click **Create** in **Client Certificate**, and follow the pop-up to create the certificate.
- 4. Click **Download** to download the certificate file to a desired location.
- **5.** Upload the downloaded certificate file to the server, and the server will return the certificate key.
- 6. Open the certificate as a text file, and modify it by the certificate key as the server returned.
- 7. Install the modified certificate in **Client Certificate**.
- 8. Optional: Click Test to test if the connection is valid.
- 9. Click Save.

13.8 Export Diagnostic Information

When exceptions occur, you can export diagnostic information via web browser, and check it.

Steps

- 1. Go to **Configuration** → **System** → **Maintenance** → **Diagnose** via web browser.
- 2. Check Export Diagnostic Information.
- 3. Click Save.
- 4. Click Diagnose Information.
- 5. Set the saving path and file name as your desire.
- 6. Save the file.

13.9 Restore Default Settings

Steps

1. Go to **Maintenance** \rightarrow **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 13-19 Restore Default Settings

2. Select the restore 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 recorder to inactive status.

iNote

The recorder will reboot automatically after restoring to the default settings.

13.10 Security Management

13.10.1 RTSP Authentication

You can specifically secure the stream data of live view by setting the RTSP authentication.

Steps

1. Go to System → System Service → System Service .

Enable RTSP	
RTSP Authentication Type	digest

Figure 13-20 RTSP Authentication

-

2. Select RTSP Authentication Type.

i Note

Two authentication types are selectable, if you select **digest**, 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.

- 3. Click Apply.
- 4. Restart the device to take effect the settings.

13.10.2 ISAPI Service

ISAPI (Internet Server Application Programming Interface) is an open protocol based on HTTP, which can realize the communication between the system devices (e.g., network camera, NVR, etc.). The device is as a server, the system can find and connect the device.

Steps

- **1.** Go to **System** \rightarrow **System** Service \rightarrow System Service .
- 2. Check Enable ISAPI.
- 3. Click Apply.
- 4. Restart the device to take effect the settings.

13.10.3 HTTP Authentication

If you need to enable the HTTP service, you can set HTTP authentication to enhance access security.

Steps

```
1. Go to Maintenance \rightarrow System Service \rightarrow System Service .
```

HTTP Authentication Type digest -

Figure 13-21 HTTP Authentication

2. Check Enable HTTP.

3. Select HTTP Authentication Type.

i Note

Two authentication types are selectable, for security reasons, it is recommended to select **digest** as the authentication type.

- 4. Click Apply to save the settings.
- 5. Restart the device to take effect the settings.

13.10.4 IP Camera Occupation Detection

After enabling the feature, when search IP camera in Number of Unadded Online Device interface, the status of IP camera the has been added by other device will show as \triangle

- 1. Go to System \rightarrow System Service \rightarrow System Service .
- 2. Check Enable IP Camera Occupation Detection.
- 3. Click Apply to save the settings. And reboot device to take effect the settings.

Chapter 14 Appendix

14.1 Glossary

Dual-Stream

Dual-stream is a technology used to record high resolution video locally while transmitting a lower resolution stream over the network. The two streams are generated by the DVR, with the main stream having a maximum resolution of 1080P and the sub-stream having a maximum resolution of CIF.

DVR

Acronym for Digital Video Recorder. A DVR is device that is able to accept video signals from analog cameras, compress the signal and store it on its hard drives.

HDD

Acronym for Hard Disk Drive. A storage medium which stores digitally encoded data on platters with magnetic surfaces.

DHCP

Dynamic Host Configuration Protocol (DHCP) is a network application protocol used by devices (DHCP clients) to obtain configuration information for operation in an Internet Protocol network.

HTTP

Acronym for Hypertext Transfer Protocol. A protocol to transfer hypertext request and information between servers and browsers over a network.

ΡΡΡοΕ

PPPoE, Point-to-Point Protocol over Ethernet, is a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames. It is used mainly with ADSL services where individual users connect to the ADSL transceiver (modem) over Ethernet and in plain Metro Ethernet networks.

DDNS

Dynamic DNS is a method, protocol, or network service that provides the capability for a networked device, such as a router or computer system using the Internet Protocol Suite, to notify a domain name server to change, in real time (ad-hoc) the active DNS configuration of its configured hostnames, addresses or other information stored in DNS.

Hybrid DVR

A hybrid DVR is a combination of a DVR and NVR.

NTP

Acronym for Network Time Protocol. A protocol designed to synchronize the clocks of computers over a network.

NTSC

Acronym for National Television System Committee. NTSC is an analog television standard used in such countries as the United States and Japan. Each frame of an NTSC signal contains 525 scan lines at 60Hz.

NVR

Acronym for Network Video Recorder. An NVR can be a PC-based or embedded system used for centralized management and storage for IP cameras, IP Domes and other DVRs.

PAL

Acronym for Phase Alternating Line. PAL is also another video standard used in broadcast televisions systems in large parts of the world. PAL signal contains 625 scan lines at 50Hz.

PTZ

Acronym for Pan, Tilt, Zoom. PTZ cameras are motor driven systems that allow the camera to pan left and right, tilt up and down and zoom in and out.

USB

Acronym for Universal Serial Bus. USB is a plug-and-play serial bus standard to interface devices to a host computer.

14.2 Frequently Asked Questions

14.2.1 Why is there a part of channels displaying "No Resource" or turning black screen in multi-screen of live view?

Reason

- 1. Sub-stream resolution or bitrate settings is inappropriate.
- 2. Connecting sub-stream failed.

Solution

 Go to Camera → Video Parameters → Sub-Stream. Select the channel, and turn down the resolution and max. bitrate (resolution shall be less than 720p, max. bitrate shall be less than 2048 Kbps).

iNote

If your video recorder notifies not support this function, you can log in to the camera, and adjust video parameters via web browser.

2. Properly set the sub-stream resolution and max. bitrate (resolution shall be less than 720p, max. bitrate shall be less than 2048 Kbps), then delete the channel and add it back again.

14.2.2 Why is the video recorder notifying not support the stream type?

Reason

The camera encoding format mismatches with the video recorder.

Solution

If the camera is using H.265/MJPEG for encoding, but video recorder does not support H.265/MJPEG, change the camera encoding format to the same as video recorder.

14.2.3 Why is the video recorder notifying risky password after adding network camera?

Reason

The camera password is too weak.

Solution

Change the camera password.

Warning

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.

14.2.4 How to improve the playback image quality?

Reason

Recording parameter settings are inappropriate.

Solution

Go to **Camera** \rightarrow **Video Parameters**. Increase resolution and max. bitrate, and try again.

14.2.5 How to confirm the video recorder is using H.265 to record video?

Solution

Check if the encoding type at live view toolbar is H.265.

14.2.6 Why is the timeline at playback not constant?

Reason

- 1. When the video recorder is using event recording, it only records video when event occurs. Hence the video may not be continuous.
- 2. Exception occurs, such as the device offline, HDD error, record exception, network camera offline, etc.

Solution

- 1. Ensure the recording type is continuous recording.
- 2. Go to **Maintenance** → Log Information . Search the log file during the video time period. See if there are unexpected events, such as HDD error, record exception, etc.

14.2.7 When adding network camera, the video recorder notifies network is unreachable.

Reason

- 1. The IP address or port of network camera is incorrect.
- 2. The network between video recorder and camera is disconnected

Solution

- 1. Go to **Camera** → **Camera** → **IP Camera** . Click grid of the selected camera, and edit its IP address and port. Ensure the video recorder and camera is using the same port.
- Go to Maintenance → Network → Detection . Enter the IP address of network camera in Destination Address, and click Test to see if the network is reachable.

14.2.8 Why is the IP address of network camera being changed automatically?

Reason

When network camera and video recorder are using the same switch but in different subnet, the video recorder will change the IP address of network camera to the same subnet as itself.

Solution

When adding camera, click **Custom Add** to add camera.

14.2.9 Why is the video recorder notifying IP conflict?

Reason

The video recorder uses the same IP address as other devices.

Solution

Change the IP address of video recorder. Ensure it is not the same as other devices.

14.2.10 Why is image getting stuck when the video recorder is playing back by single or multi-channel cameras?

Reason

HDD read/write exception.

Solution

Export the video, and play it with other devices. If it plays normally on other device, change your HDD, and try again.

14.2.11 Why does my video recorder make a beeping sound after booting?

Reason

- 1. The front panel is not fastened (for the device which its front panel is removable).
- 2. HDD error, or do not have HDD.

Solution

- 1. If it makes continuous beeps, and your device's front panel is removable, ensure the front panel is fastened.
- If it makes non-continuous beeps (3 long, 2 short), take HDD error as an example, check if the device has installed HDD. If not, you can go to System → Event → Normal Event → Exception, and uncheck Event Hint Configuration to disable HDD error event hint. Check if the HDD is initialized. If not, go to Storage > Storage Device to initialize the HDD. Check if the HDD is broken. You can change it, and try again.

14.2.12 Why is there no recorded video after setting the motion detection?

Reason

- 1. The recording schedule is incorrect.
- 2. The motion detection event setting is incorrect.
- 3. HDD exception.

Solution

- 1. The recording schedule is setup correctly by following the steps listed in Configuring Record/ Capture Schedule.
- 2. The motion detection area is configured correctly. The channels are being triggered for motion detection (See Configuring Motion Detection).
- Check if the device has installed HDD.
 Check if the HDD is initialized. If not, go to Storage > Storage Device to initialize the HDD.
 Check if the HDD is broken. You can change it, and try again.

14.2.13 Why is the sound quality not good in recording video?

Reason

- 1. The audio input device does not have a good effect in sound collection.
- 2. Interference in transmission.
- 3. The audio parameter is not properly set.

Solution

- 1. Check if the audio input device is working properly. You can change another audio input device, and try again.
- 2. Check the audio transmission line. Ensure all lines are well connected or welded, and there is no electromagnetic interference.
- 3. Adjust the audio volume according to the environment and audio input device.

