

MEGApix® 4MP bullet IP camera with analytics

DWC-MBT4Wi28
DWC-MBT4Wi36



User's Manual Ver. 12/18

Before installing and using the camera, please read this manual carefully.
Be sure to keep it handy for future reference.

Safety Information



CAUTION

RISK OF ELECTRIC SHOCK.
DO NOT OPEN.



CAUTION:

TO REDUCE THE RISK OF ELECTRIC SHOCK, DO NOT REMOVE COVER (OR BACK) NO USER-SERVICEABLE PARTS INSIDE. REFER SERVICING TO QUALIFIED SERVICE PERSONNEL.



Warning

This symbol indicates that dangerous voltage consisting of a risk of electric shock is present within this unit.



Precaution

This exclamation point symbol is intended to alert the user to the presence of important operating and maintenance (servicing) instructions in the literature accompanying the appliance.

WARNING

To prevent damage which may result in fire or electric shock hazard, do not expose this appliance to rain or moisture.

WARNING

1. Be sure to only use the standard adapter that is specified in the specification sheet. Using any other adapter could cause fire, electrical shock, or damage to the product.
2. Incorrectly connecting the power supply or replacing battery may cause an explosion, fire, electric shock, or damage to the product.
3. Do not connect multiple cameras to a single adapter. Exceeding the capacity may cause excessive heat generation or fire.
4. Securely plug the power cord into the power receptacle. Insecure connection may cause fire.
5. When installing the camera, fasten it securely and firmly. A falling camera may cause personal injury.
6. Do not place conductive objects (e.g. screw drivers, coins, metal items, etc.) or containers filled with water on top of the camera. Doing so may cause personal injury due to fire electric shock or falling objects.
7. Do not install the unit in humid, dusty, or sooty locations. Doing so may cause fire or electric shock.
8. If any unusual smells or smoke come from the unit, stop using the product. Immediately disconnect the power cord and contact the service center. Continued use in such a condition may cause fire or electric shock.
9. If this product fails to operate normally, contact the nearest service center. Never disassemble or modify this product in any way.
10. When cleaning, do not spray water directly onto parts of the product. Doing so may cause fire or electric shock.

Precaution

Operating

- Before using, make sure the power supply and all other parts are properly connected.
- While operating, if any abnormal condition or malfunction is observed, stop using the camera immediately and contact your dealer.

Handling

- Do not disassemble or tamper with parts inside the camera.
- Do not drop the camera or subject it to shock or vibration as this can damage the camera.
- Clean the clear dome cover with extra care. Scratches and dust can ruin the quality of the camera image.

Installation and Storage

- Do not install the camera in areas of extreme temperature, exceeding the allowed range.
- Avoid installing in humid or dusty environments.
- Avoid installing in places where radiation is present.
- Avoid installing in places where there are strong magnetic fields and electric signals.
- Avoid installing in places where the camera would be subject to strong vibrations.
- Never expose the camera to rain or water.

Important Safety Instructions

1. **Read these instructions.** - All safety and operating instructions should be read before installation or operation.
2. **Keep these instructions.** - The safety, operating and use instructions should be retained for future reference.
3. **Heed all warnings.** - All warnings on the product and in the operating instructions should be adhered to.
4. **Follow all instructions.** - All operating and use instructions should be followed.
5. **Do not use this device near water.** - For example: near a bath tub, wash bowl, kitchen sink, laundry tub, in a wet basement; near a swimming pool; etc.
6. **Clean only with dry cloth.** - Unplug this product from the wall outlet before cleaning. Do not use liquid cleaners.
7. **Do not block any ventilation openings. Install in accordance with the manufacturer's instructions.** - Slots and openings in the cabinet are provided for ventilation, to ensure reliable operation of the product, and to protect it from over-heating. The openings should never be blocked by placing the product on bed, sofa, rug or other similar surfaces. This product should not be placed in a built-in installation such as a bookcase or rack unless proper ventilation is provided and the manufacturer's instructions have been adhere to.
8. **Do not install near any heat sources such as radiators, heat registers, or other apparatus (including amplifiers) that produce heat.**
9. **Do not defeat the safety purpose of the polarized or grounding-type plug.** A polarized plug has two blades with one wider than the other. A grounding type plug has two blades and a third grounding prong. The wide blade or the third prong are provided for your safety. If the provided plug does not fit into your outlet, consult an electrician for replacement.
10. **Protect the power cord from being walked on or pinched particularly at plugs, convenience receptacles, and the point where they exit from the apparatus.**
11. **Only use attachments/accessories specified by the manufacturer.**
12. **Use only with cart, stand, tripod, bracket, or table specified by the manufacturer, or sold with the apparatus. When a cart is used, use caution when moving the cart/apparatus combination to avoid injury from tip-over.**
13. **Unplug the apparatus during lightning storms or when unused for long periods of time.**
14. **Refer all servicing to qualified service personnel.** Servicing is required when the apparatus has been damaged in any way, such as power supply cord or plug is damaged, liquid has been spilled or objects have fallen into the apparatus, the apparatus has been exposed to rain or moisture, does not operate normally, or has been dropped.



Disposal of Old Appliances



1. When this crossed-out wheel bin symbol is attached to a product it means the product is covered by the European Directive 2002/96/EC.
2. All electrical and electronic products should be disposed of separately from the municipal waste stream in accordance with laws designated by the government or the local authorities.
3. The correct disposal of your old appliance will help prevent potential negative consequences for the environment and human health.
4. For more detailed information about disposal of your old appliance, please contact your city office, waste disposal service or the shop where you purchased the product.



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.

Table of Contents

- 1 Product and Accessories6**
- 2 Parts and Description7**
- 3 Installation8**
- 4 Cabling9**
- 5 Live View10**
- 6 Camera Configuration.....13**
 - 6.1 System Configuration 13
 - 6.1.1 Basic Information 13
 - 6.1.2 Date and Time 13
 - 6.1.3 Local Config 14
 - 6.1.4 Storage 14
 - 6.2 Image Configuration 17
 - 6.2.1 Display Configuration 17
 - 6.2.2 Video / Audio Configuration 19
 - 6.2.3 OSD Configuration 20
 - 6.2.4 Video Mask 21
 - 6.2.5 ROI Configuration 22
 - 6.2.6 Lens Control 23
 - 6.3 PTZ Configuration 24
 - 6.4 Alarm Configuration..... 24
 - 6.4.1 Motion Detection 24
 - 6.4.2 Other Alarms 25
 - 6.4.3 Alarm In 27
 - 6.4.4 Alarm Out 28
 - 6.4.5 Alarm Server 28
 - 6.5 Event Configuration 29
 - 6.5.1 Video Tampering Detection 29
 - 6.5.2 Line Crossing 31
 - 6.5.3 Perimeter Intrusion 32

Table of Contents (Continue)

6.6 Network Configuration	36
6.6.1 TCP/IP	36
6.6.2 Port	37
6.6.3 Server Configuration	37
6.6.4 DDNS	38
6.6.5 SNMP	39
6.6.6 802.1x	40
6.6.7 RTSP	41
6.6.8 UPnP	42
6.6.9 E-mail	42
6.6.10 FTP	44
6.6.11 HTTPS	44
6.6.12 P2P (Optional)	46
6.6.13 QoS	46
6.7 Security Configuration	46
6.7.1 User Configuration	46
6.7.2 Online Users	48
6.7.3 Block and Allow Lists	48
6.7.4 Security Management	48
6.8 Maintenance Configuration	49
6.8.1 Backup and restore	49
6.8.2 Reboot	50
6.8.3 Upgrade	50
6.8.4 Operation log	50
7 Search	52
7.1 Image Search	52
7.2 Video Search	54
7.2.1 Local video search	54
7.2.2 SD card video search	55
8 Appendix.....	58
9 Dimensions.....	60
10 Warranty Information.....	61
11 Limits and Exclusions	62

1 Product & Accessories

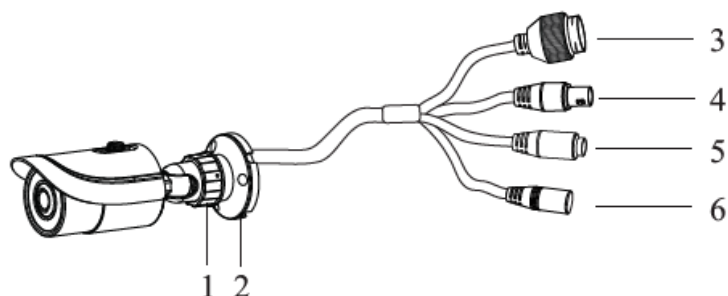


Default Login Information	
Username: admin	Password: admin

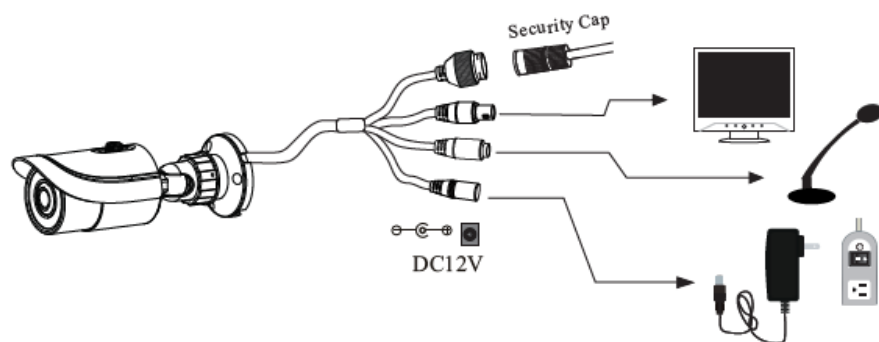
WHAT'S IN THE BOX

QSG Manual		1 Set	Tapping Screws PA 3x25 – 3pcs		1 Set
Mounting Template		1 Set	Plastic Plugs – 3pcs		1 Set
Waterproof Cap		1 Set	Machine Screw PWM 3x5 – 1pc		1 Set
Rubber Plug		1 Set			

2 Parts and Description



1	Fixed Ring	4	CVBS Cable
2	Mounting Base	5	MIC IN Cable
3	Network Cable	6	Power Cable

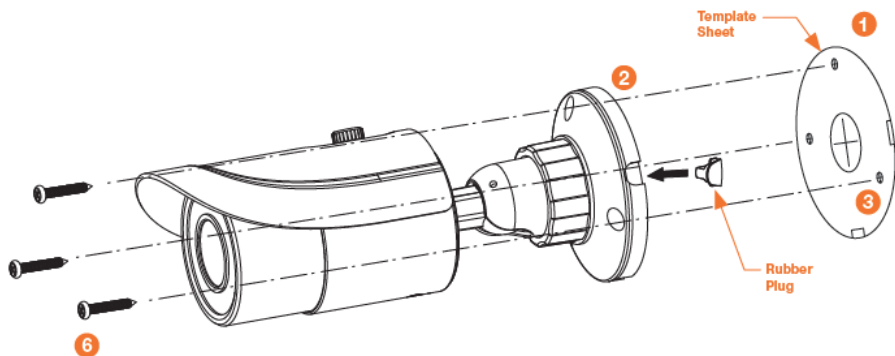
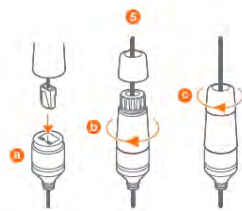


3 Installation

1. Before installing the camera, make sure the mounting surface can withstand three times the weight of your camera.
2. Do not let the cables get caught in improper places or the electric line cover can be damaged. This may cause a short or fire.
3. Using the mounting template sheet or the camera itself, mark and drill the necessary holes in the wall or ceiling.
4. Pass the wires through and make all necessary connections. See cabling section for more information.
5. To use the camera's water proof wiring:
 - a. Install the LAN cable into 'a'.
 - b. 'b' will be assembled to 'a' with a 1/4 turn.
 - c. Thread 'c' tightly to 'b'. Adjust the camera to obtain an optimum angle by loosening the lock screws.

NOTE: To ensure moisture seal, make sure the O-ring is in place between 'a' and 'b'. In extreme environments use of an outdoor rated sealer is recommended.

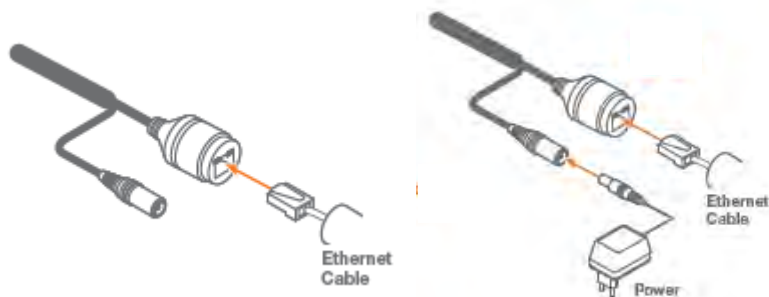
NOTE: When using the waterproof cap, crimp the RJ45 connector after passing the cable through the waterproof cap.



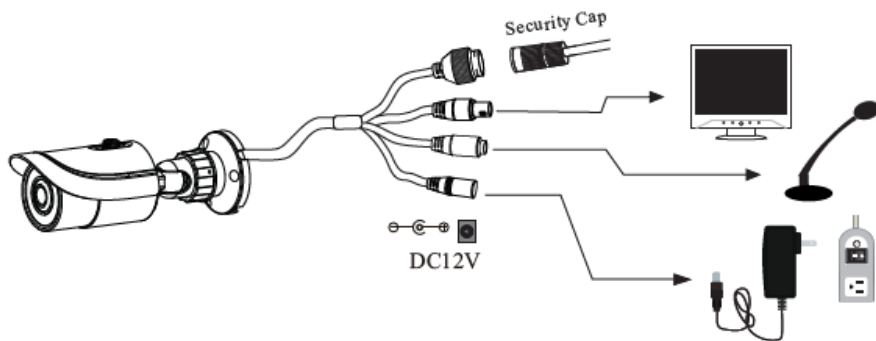
6. Mount the rubber plug to the gap of the mounting base. Then secure the mounting base with camera to the wall with screws.
7. Adjust the camera to obtain an optimum angle by using the camera's bracket. The camera's max angles are:
Pan: 0°~ 360°
Tilt: 0°~ 90°
8. When the proper view has been achieved, tighten the fixed screws to finish the installation.

4 Cabling

1. NETWORK CONNECTIONS – If you are using a PoE Switch, connect the camera using an Ethernet cable for both data and power.
2. NETWORK CONNECTIONS – If you are using a non-PoE switch, connect the camera to the switch using an Ethernet cable for data transmission and use a power adapter to power the camera.



Use the diagram below to connect all external devices to the camera:



5 Live View

To log in to the camera, open an Internet Explorer page and input the camera's IP address. If you are connecting to the camera for the first time, be sure to download the ActiveX control. After downloading, a login window will pop up as shown below.



DW DIGITAL WATCHDOG
Complete Surveillance Solutions

Name:

Password:

Stream Type:

Language:

☒ Remember me

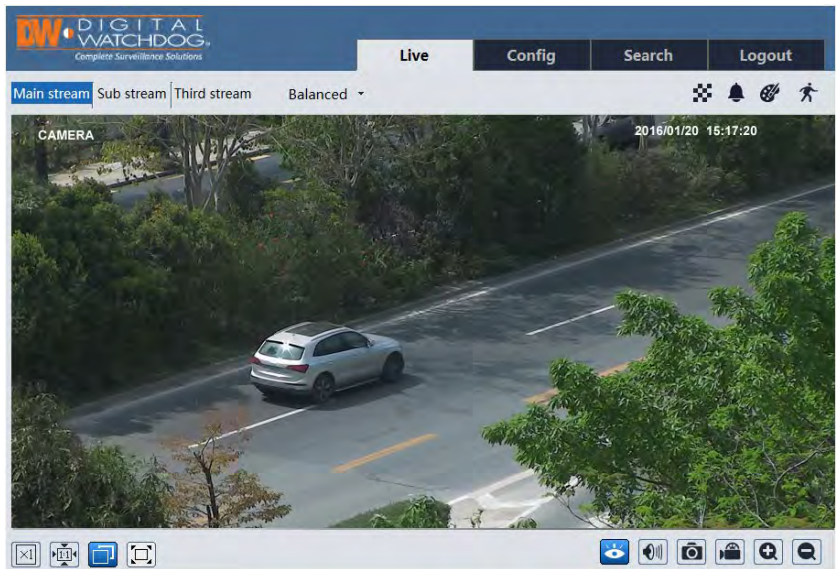
Login

Input the username and password to log in.



The default username is "admin"; the default password is "admin".

After you log in, you will see the following window.



The following table is the instructions of the icons on the remote preview interface.

The following table is the instructions of the icons on the live view interface.

Icon	Description	Icon	Description
	Original size		SD card recording indicator
	Fit correct scale		Color abnormal indicator
	Auto (fill the window)		Abnormal clarity indicator
	Full screen		Scene change indicator
	Start/stop live view		Line crossing indicator
	Start/stop two-way audio		Crowd density indicator
	Enable/disable audio		People counting indicator
	Snapshot		Object removal indicator
	Start/stop recording local		Intrusion indicator
	Zoom in		People intrusion indicator

Icon	Description	Icon	Description
	Zoom out		Sensor alarm indicator
	PTZ control		Motion alarm indicator
	AZ control (only available for the model with motorized zoom lens)		Face detection indicator

- Those smart alarm indicators will flash only when the camera supports those functions and the corresponding events are enabled.
- In full screen mode, double click on the mouse to exit or press the ESC key on the keyboard.

Click AZ control button to show AZ control panel. The descriptions of the control panel are as follows:

Icon	Description	Icon	Description
	Zoom -		Zoom +
	Focus -		Focus +
	One key focus (used when image is out of focus after manual adjustment)		

The camera can be installed in a compatible external PTZ enclosure through RS485. Click the PTZ icon to reveal the PTZ control panel. (This function is only available for the model with RS485 interface).

The descriptions of the control panel are as follows:

Icon	Description	Icon	Description
	Move upper left direction		Move upper right direction
	Move up		Stop movement
	Move left		Move right
	Move lower left direction		Move lower right direction
	Move down		Speed adjustment
	Zoom out		Zoom in
	Focus -		Focus +

	Iris -		Iris +
	Auto scan		Wiper
	Light		Radom scan
	Group scan		Preset

Select preset and click  to call the preset. Select and set the preset and then click  to save the position of the preset. Select the set preset and click  to delete it.

6 Camera Configuration

In the DW web client, choose “Config” to go to the configuration interface. Note: Wherever applicable, click the “Save” button to save the settings.

6.1 System Configuration

6.1.1 Basic Information

In the “Basic Information” interface, the system information of the device is listed.

Device Name	IPC
Product Model	XXXX
Brand	Customer
Software Version	4.2.1.0(14734)
Software Build Date	2017-12-12
Kernel Version	20171115
Hardware Version	1.3-1314205
Onvif Version	16.12(#2)
OCX Version	2.0.2.7
MAC	00:18:ae:58:23:eb

Some versions may support device ID and QR code. Having enabled P2P (see Network Configuration-P2P), the network camera can be quickly added to mobile surveillance client, by scanning the QR code or entering device ID.

6.1.2 Date and Time

Go to Config→System→Date and Time. Please refer to the following interface.

Zone

Date and Time

Time Zone: GMT+08 (Beijing, Hong Kong, Shanghai, Taipei) ▼

☐ DST

☒ Auto DST

☐ Manual DST

Start Time May ▼ First ▼ Tuesday ▼ 15 ▼ Hour

End Time August ▼ First ▼ Tuesday ▼ 15 ▼ Hour

Time Offset 30 Minutes ▼

Select the time zone and DST as required.
Click the “Date and Time” tab to set the time mode.

Zone **Date and Time**

Time Mode:

☐ Synchronize with NTP server

NTP server: Update period: Minutes

☐ Synchronize with computer time

Date Time

☒ Set manually

Date Time

6.1.3 Local Config

Go to Config→System→Local Config to set up the storage path of captured pictures and recorded videos on the local PC. There is also an option to enable or disable the bitrate display in the recorded files.

Picture Path

Record Path

Video Audio Settings ☐ Open ☒ Close

Show Bitrate ☒ Open ☐ Close

Local Face Information Storage ☐ Open ☒ Close (Maximum of 10000 pictures for Facial Recognition)

If the camera support face detection, local face information storage can be set up here. (Face detection function is only available for some specified versions).

6.1.4 Storage

This function is only available for the model with SD slot.

Go to Config→System→Storage to go to the interface as shown below.

Management Record Snapshot

Total picture capacity

Picture remaining space

Total recording capacity

Record remaining space

State

Snapshot Quota %

Video Quota %

Changes in the quota ratio need to be formatted before they become effective.

- SD Card Management

Click the “Format” button to format the SD card. All data will be cleared by clicking this button.

Click the “Eject” button to stop writing data to SD card. Then the SD card can be ejected safely.

Snapshot Quota: Set the capacity proportion of captured pictures on the SD card.

Video Quota: Set the capacity proportion of record files on the SD card.

- Schedule Recording Settings

1. Go to Config→System→Storage→Record to go to the interface as shown below.

The screenshot shows the 'Record' tab in a configuration menu. Under 'Record Parameters', there are three dropdown menus: 'Record Stream' set to 'Main', 'Pre Record Time' set to '3 Seconds', and 'Cycle Write' set to 'Yes'. Below this is a 'Schedule' section with a checkbox 'Enable Schedule Record' which is checked.

2. Set record stream, pre-record time, cycle writing.

Pre Record Time: Set the time to record before the actual recording begins.

3. Set schedule recording. Check “Enable Schedule Record” and set the schedule.

The screenshot shows the 'Week Schedule' and 'Holiday Schedule' sections. The 'Week Schedule' section has a header with 'Erase' and 'Add' buttons. Below it, there are seven rows for the days of the week (Sun. to Sat.), each with a timeline from 0 to 24 hours. The 'Holiday Schedule' section has a 'Date' input field with '07-12', 'Add' and 'Delete' buttons, and another timeline from 0 to 24 hours.

Weekly schedule

Set the alarm time from Monday to Sunday for a single week. Each day is divided in one hour increments. Green means scheduled. Blank means unscheduled. Note that if a specific time period is not scheduled for motion, the camera will not generate a motion alarm even if motion is enabled.

“Add”: Add the schedule for a special day. Drag the mouse to set the time on the timeline.

“Erase”: Delete the schedule. Drag the mouse to erase the time on the timeline.

Manual Input: Click it for a specific day to enter specific start and end times. This adds more granularities (minutes).

Day schedule

Set the alarm time for alarm a special day, such as a holiday.

Note: Holiday schedule takes priority over weekly schedule.

● Snapshot Settings

Go to Config→System→Storage→Snapshot to go to the interface as shown below.

Management	Record	Snapshot
Snapshot Parameters		
Image Format	JPEG	
Resolution	2592x1520	
Image Quality	High	
Event Trigger		
Snapshot Interval	1	Second
Snapshot Quantity	5	
Schedule		
☒ Enable Timing Snapshot		
Snapshot Interval	1	Second

Set the format, resolution and quality of the image saved on the SD card and the snapshot interval and quantity and the timing snapshot here.

Snapshot Quantity: The number you set here is the maximum quantity of snapshots. The actual quantity of snapshots may be less than this number. Supposing the occurrence time of an alarm event is less than the time of capturing pictures, the actual quantity of snapshots is less than the set quantity of snapshots.

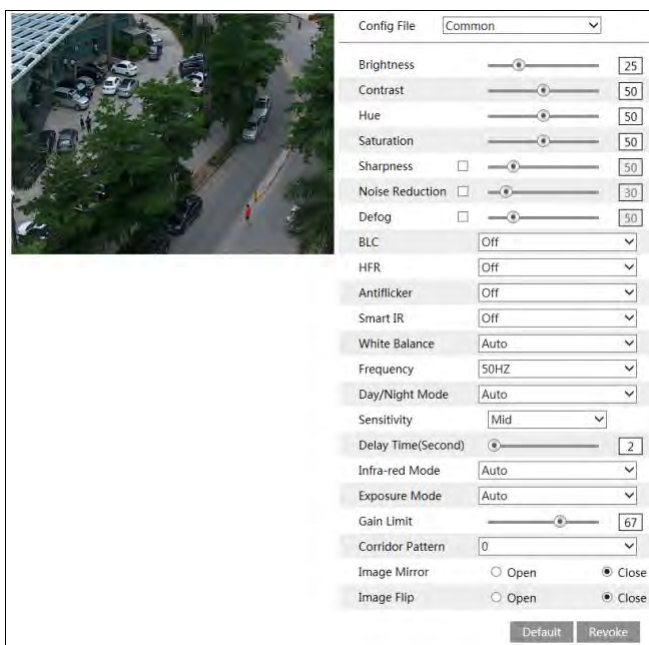
Timing Snapshot: Enable timing snapshot first and then set the snapshot interval and schedule. The setup steps of schedule are the same as the schedule recording (See [Schedule Recording](#)).

6.2 Image Configuration

Image Configuration includes Display, Video/Audio, OSD, Video Mask and ROI Config.

6.2.1 Display Configuration

Go to Image→Display interface as shown below. The image's brightness, contrast, hue and saturation and so on for common, day and night mode can be set up separately. The image effect can be quickly seen by switching the configuration file.



Brightness: Set the brightness level of the camera's image.

Contrast: Set the color difference between the brightest and darkest parts.

Hue: Set the total color degree of the image.

Saturation: Set the degree of color purity. The purer the color, the brighter the image is.

Sharpness: Set the resolution level of the image plane and the sharpness level of the image edge.

Noise Reduction: Decrease the noise and make the image more thorough. Increasing the value will make the noise reduction effect better but it will reduce the image

resolution.

Defog: Activating this function and setting an appropriate value as needed in foggy, dusty, smoggy or rainy environment to get clear images.

Backlight Compensation (BLC):

- **Off:** disables the backlight compensation function. It is the default mode.
- **HWDR**
 - ◆ WDR can adjust the camera provide a better image when there are both very bright and very dark areas simultaneously in the field of the view by lowering the brightness of the bright area and increasing the brightness of the dark area. High, middle and low can be selected.
 - ◆ Recording will be stopped for a few seconds while the mode is changing from non-WDR to WDR mode.
- **HLC:** lowers the brightness of the entire image by suppressing the brightness of the image's bright area and reducing the size of the halo area.
- **BLC:** If enabled, the auto exposure will activate according to the scene so that the object of the image in the darkest area will be seen clearly.

HFR: If this function is enabled, the system will restart and then the maximum value of the frame rate of the main stream can be set to 60 fps. (This function is not available for motorized zoom cameras).

Anti-flicker:

- **Off:** disables the anti-flicker function. This is used mostly in outdoor installations.
- **50Hz:** reduces flicker in 50Hz lighting conditions.
- **60Hz:** reduces flicker in 60Hz lighting conditions.

White Balance: Adjust the color temperature according to the environment automatically.

Frequency: 50Hz and 60Hz can be optional.

Day/night Mode: Please choose the mode as needed.

Sensitivity: High, middle and low can be selected for switching back and forth from day to night modes.

Infrared Mode: Choose "ON", "OFF" and "Auto" (This function is not available for the cameras without infrared lights).

Exposure Mode: Choose "Auto" or "Manual". If manual is chosen, the digital shutter speed can be adjusted.

Corridor Pattern: Corridor viewing modes can be used for situations such as long hallways. 0, 90, 180 and 270 are available. The default value is 0. The video resolution should be 1080P or below if this function is used.

Image Mirror: Turn the current video image horizontally.

Image Flip: Turn the current video image vertically.

Schedule Settings of Image Parameters:

Click the "Schedule" tab as shown below.

Camera Parameters

Schedule

Schedule

Full Time

Config File

Common

Set full time schedule for common, day, night mode and specified time schedule for day and night. Choose “Schedule” in the drop-down box of schedule as shown below.

Camera Parameters

Schedule

Schedule

Schedule

Time Range

0:00

4:00

8:00

12:00

16:00

20:00

24:00

Day

Night

Save

Drag “” icons to set the time of day and night. Blue means day time and blank means night time. If the current mode of camera parameters is set to schedule, the image configuration mode will automatically switch between day and night according to the schedule.

6.2.2 Video / Audio Configuration

Go to Image→Video / Audio interface as shown below. In this interface, set the resolution, frame rate, bitrate type, video quality and so on subject to the actual network condition.

Video

Audio

Index	Stream Name	Resolution	Frame Rate	Bitrate Type	Bitrate(Kbps)	Video Quality	I Frame Interval	Video Compression	Profile
1	Main stream	2560x1440	30	CBR	3072	Medium	120	H265	Main Profile
2	Sub stream	352x240	30	CBR	512	High	120	H264	High Profile
3	Third stream	704x480	30	CBR	768	High	120	H264	High Profile

Send Snapshot

1

Size: (2560x1440)

☐ Video encode slice split

☒ Watermark

Watermark content: XXXX

Click the “Audio” tab to go to the interface as shown below.

Video

Audio

Audio Encoding

G711A

Audio Type

MIC

Save

Three video streams can be adjustable.
Resolution: The size of image.

Frame rate: The higher the frame rate, the video is smoother.

Bitrate type: CBR and VBR are optional. Bitrate is related to image quality. CBR means that no matter how much change is seen in the video scene, the compression bitrate will be kept constant. VBR means that the compression bitrate will be adjusted according to scene changes. For example, for scenes that do not have much movement, the bitrate will be kept at a lower value. This can help optimize the network width usage.

Bitrate: it can be adjusted when the mode is set to CBR. The higher the bitrate, the better the image quality will be.

Video Quality: It can be adjusted when the mode is set to VBR. The higher the image quality, the more bitrate will be required.

I Frame interval: It determines how many frames are allowed between a “group of pictures”. When a new scene begins in a video, until that scene ends, the entire group of frames (or pictures) can be considered as a group of pictures. If there is not much movement in the scene, setting the value higher than the frame rate is fine, potentially resulting in less bandwidth usage. However, if the value is set too high, and there is a high frequency of movement in the video, there is a risk of frame skipping.

Video Compression: H264 and H265 are optional. If H.265 is chosen, make sure the client system is able to decode H.265.

Profile: For H.264. Baseline, main and high profiles are selectable.

Send Snapshot: How many snapshots to generate for an event.

Video encode slice split: If this function is enabled, smooth image can be gotten even though using the low-performance PC.

Watermark: When playing back the local recorded video in the search interface, the watermark can be displayed. To enable it, check the watermark box and enter the watermark text.

Audio Encoding: G711A and G711U are selectable.

Audio Type: MIC and LIN are selectable.

6.2.3 OSD Configuration

Go to Image→OSD interface as shown below.



Set time stamp, device name, OSD content and picture overlap here. After enabling the corresponding display and entering the content, drag them to change their position. Then Click the “Save” button to save the settings.

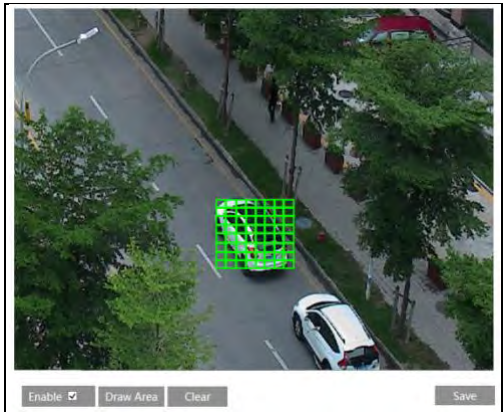


Picture Overlay Settings:

Check “OSD Content1”, choose “Picture Overlay” and click “Browse” to select the overlap picture. Then click “Upload” to upload the overlap picture. The pixel of the image shall not exceed 200*200, or it cannot be uploaded.

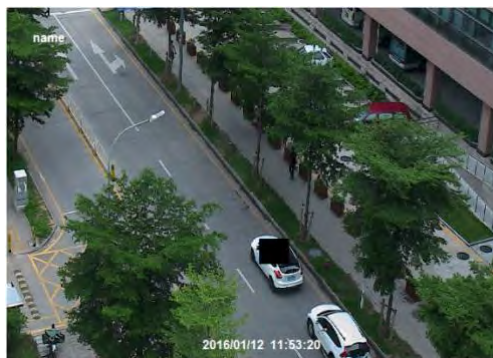
6.2.4 Video Mask

Go to Image→Video Mask interface as shown below. A maximum of 4 zones can be set up.



To set up video mask:

1. Enable video mask.
2. Click the “Draw Area” button and then drag the mouse to draw the video mask area.
3. Click the “Save” button to save the settings.
4. Return to the live to verify that the area have been drawn as shown as blocked out in the image.

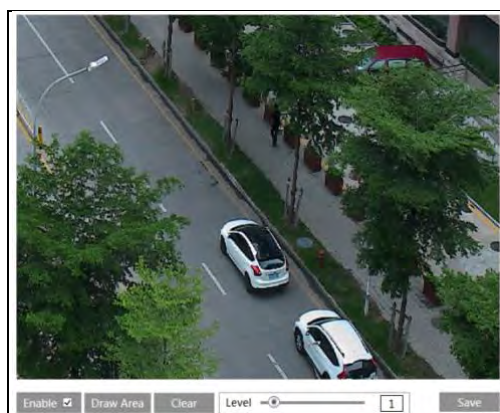


To clear the video mask:

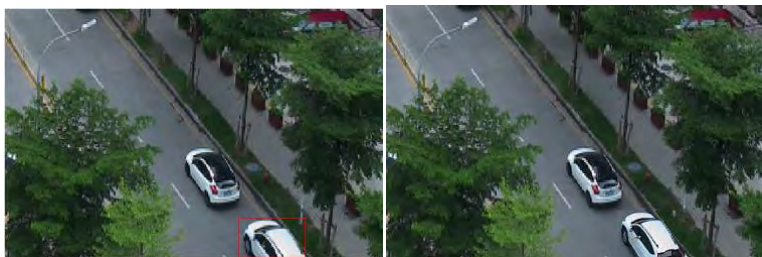
Click the “Clear” button to delete the current video mask area.

6.2.5 ROI Configuration

Go to Image→ROI Config interface as shown below. An area in the image can be set as a region of interest. This area will have a higher bitrate than the rest of the image, resulting in better image quality for the identified area.

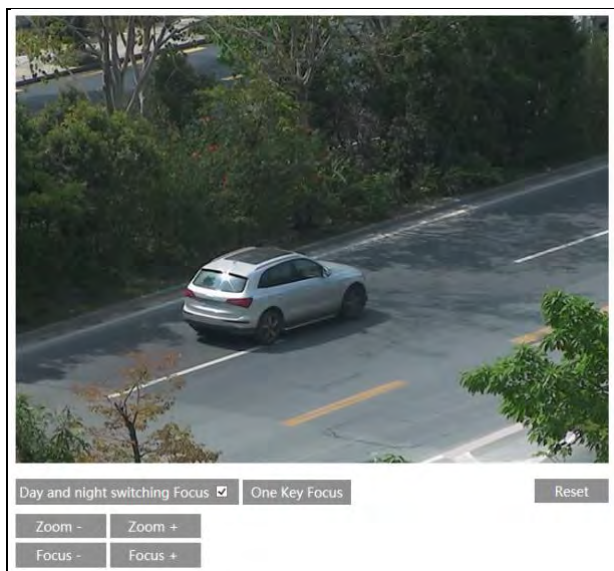


1. Check “Enable” and then click the “Draw Area” button.
2. Drag the mouse to set the ROI area.
3. Set the level.
4. Click the “Save” button to save the settings.



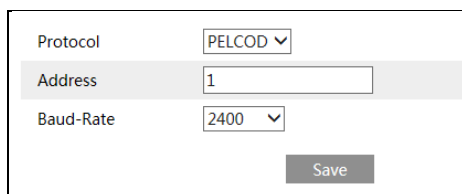
6.2.6 Lens Control

This function is only available for the model with motorized zoom lens. Within this section, zoom and focus can be controlled. If the image is out of focus after a manual adjustment, one key focus can be used to set the focus automatically.



6.3 PTZ Configuration

This function is only available for the models with RS485 interface. It can be used with a compatible external PTZ enclosure. Go to PTZ→Protocol interface as shown below.



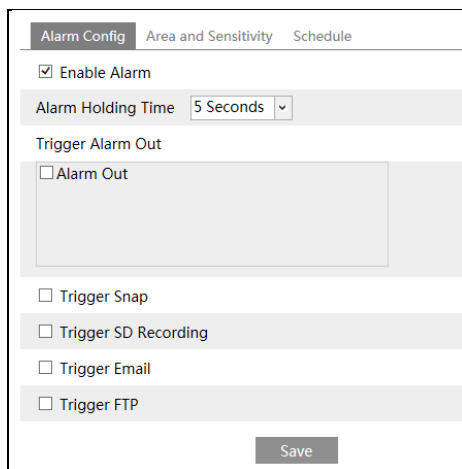
Protocol	PELCOD ▼
Address	1
Baud-Rate	2400 ▼
Save	

Set the protocol, address and baud rate according to the PTZ.

6.4 Alarm Configuration

6.4.1 Motion Detection

Go to Alarm→Motion Detection to set motion detection alarm.



Alarm Config	Area and Sensitivity	Schedule
☒ Enable Alarm		
Alarm Holding Time 5 Seconds ▼		
Trigger Alarm Out		
☒ Alarm Out		
☐ Trigger Snap		
☐ Trigger SD Recording		
☐ Trigger Email		
☐ Trigger FTP		
Save		

1. Check “Enable Alarm” check box to activate motion based alarms. If unchecked, the camera will not send out any signals to trigger motion-based recording to the NVR or CMS, even if there is motion in the video.

Alarm Out: If selected, this would trigger an external relay output that is connected to the camera on detecting a motion based alarm.

Trigger Snap: If selected, the system will capture images on motion detection and save the images on an SD card (this function is only available for the models with SD slot).

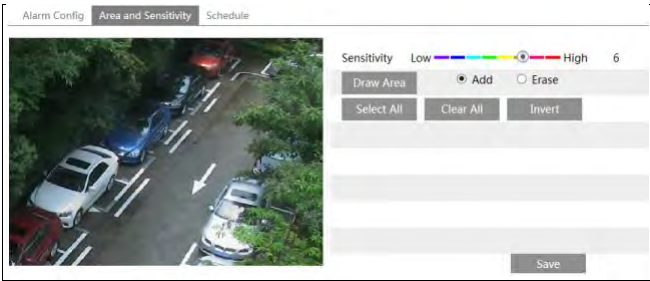
Trigger SD Recording: If selected, video will be recorded on an SD card on motion

detection (this function is only available for the models with SD card slot).

Trigger Email: If “Trigger Email” and “Attach Picture” are checked (email address must be set first in the Email configuration interface), the captured pictures and triggered event will be sent into those addresses.

Trigger FTP: If “Trigger FTP” and “Attach Picture” are checked, the captured pictures will be sent into FTP server address. Please refer to FTP configuration chapter for more details.

2. Set motion detection area and sensitivity. Click the “Area and Sensitivity” tab to go to the interface as shown below.



Move the “Sensitivity” scroll bar to set the sensitivity. Higher sensitivity value means that motion will be triggered more easily.

Select “Add” and click “Draw”. Drag the mouse to draw the motion detection area;

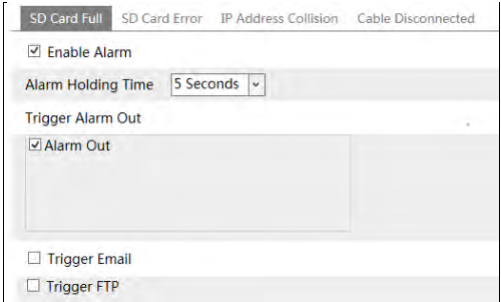
Select “Erase” and drag the mouse to clear motion detection area.

After that, click the “Save” to save the settings.

3. Set the schedule for motion detection. The schedule setup steps of the motion detection are the same as the schedule recording setup (See [Schedule Recording](#)).

6.4.2 Other Alarms

- SD Card Full
1. Go to Config→Alarm→Anomaly→SD Card Full.



2. Click “Enable alarm” and set the alarm holding time.
3. Set alarm trigger options. The setup steps are the same as motion detection. Please refer to motion detection chapter for details.

● SD Card Error

When there are some errors in writing SD card, the corresponding alarms will be triggered.

1. Go to Config→Alarm→Anomaly→SD Card Error as shown below.

SD Card Full SD Card Error IP Address Collision Cable Disconnected

☒ Enable Alarm

Alarm Holding Time 5 Seconds

Trigger Alarm Out

☒ Alarm Out

☐ Trigger Email

☐ Trigger FTP

2. Click “Enable alarm” and set the alarm holding time.
 3. Set alarm trigger options. Trigger alarm out, Email and FTP. The setup steps are the same as motion detection. Please refer to [motion detection](#) chapter for details.
- Note: SD card full and SD card error are only available for the models with SD slot.

● IP Address Conflict

1. Go to Config→Alarm→Anomaly→IP Address Collision as shown below.

SD Card Full SD Card Error IP Address Collision Cable Disconnected

☒ Enable Alarm

Alarm Holding Time 5 Seconds

Trigger Alarm Out

☒ Alarm Out

☐ Trigger Email

☐ Trigger FTP

2. Click “Enable alarm” and set the alarm holding time.
3. Trigger alarm out. When the IP address of the camera is in conflict with the IP address of other devices, the system will trigger the alarm out.

● Cable Disconnection

1. Go to Config→Alarm→Anomaly→Cable Disconnected as shown below.

SD Card Full SD Card Error IP Address Collision **Cable Disconnected**

☒ Enable Alarm

Alarm Holding Time 20 Seconds

Trigger Alarm Out

☒ Alarm Out

2. Click “Enable alarm” and set the alarm holding time.
3. Trigger alarm out. When the camera is disconnected, the system will trigger the alarm out.

6.4.3 Alarm In

This function is only available for some models. To set sensor alarm (alarm in):
Go to Config→Alarm→Alarm In interface as shown below.

Alarm Config Schedule

☒ Enable Alarm

Alarm Type NO

Alarm Holding Time 30 Seconds

Sensor Name

Trigger Alarm Out

☐ Alarm Out

☐ Trigger Snap

☐ Trigger SD Recording

☐ Trigger Email

☐ Trigger FTP

Save

1. Click “Enable alarm” and set the alarm type, alarm holding time and sensor name.
2. Set alarm trigger options. The setup steps are the same as motion detection. Please refer to [motion detection](#) chapter for details.
3. Click “Save” button to save the settings.
4. Set the schedule of the sensor alarm. The setup steps of the schedule are the same as the schedule recording setup. (See [Schedule Recording](#)).

6.4.4 Alarm Out

This function is only available for some models. Go to Config→Alarm→Alarm Out.

Alarm Out Mode	Alarm Linkage
Alarm Out Name	alarmOut1
Alarm Holding Time	30 Seconds

Alarm Out Mode: Alarm linkage, manual operation, day/night switch linkage and schedule are optional.

Alarm Linkage: Having selected this mode, select alarm out name and alarm holding time at the “Alarm Holding Time” pull down list box.

Manual Operation: Having selected this mode, click “Open” to trigger the alarm out immediately; click “Close” to stop alarm.

Alarm Out Mode	Manual Operation
Manual Operation	Open Close

Day/Night Switch Linkage: Having selected this mode, choose to open or close day/night switch linkage.

Alarm Out Mode	Day/night switch linkage
Day	Open
Night	Close

Schedule: Click “Add” and drag the mouse on the timeline to set the schedule of alarm out; click “Erase” and drag the mouse on the timeline to erase the set time schedule. After this schedule is saved, the alarm out will be triggered in the specified time.

Alarm Out Mode	Schedule
Time Range	0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 05:00-08:00 Manual Input

6.4.5 Alarm Server

Go to Alarm→Alarm Server interface as shown below.

Set the server address, port, heartbeat and heartbeat interval. When an alarm occurs, the camera will transfer the alarm event to the alarm server. If an alarm server is not needed, there is no need to configure this section.

Server Address	
Port	0
Heartbeat	Disable ▼
Heartbeat interval	30 Second

6.5 Event Configuration

For more accuracy, here are some recommendations for installation.

- Cameras should be installed on stable surfaces, as vibrations can affect the accuracy of detection.
- Avoid pointing the camera at the reflective surfaces (like shiny floors, mirrors, glass, lake surfaces and so on).
- Avoid places that are narrow or have too much shadowing.
- Avoid scenario where the object's color is similar to the background color.
- At any time of day or night, please make sure the image of the camera is clear and with adequate and even light, avoiding overexposure or too much darkness on both sides.

6.5.1 Video Tampering Detection

This function can detect changes in the surveillance environment affected by the external factors.

To set video tampering detection:

Go to Config→Event→Video Tampering Detection interface as shown below.

Detection Config	Sensitivity
☒ Scene change detection	
☒ Video blur detection	
☒ Abnormal color detection	
Alarm Holding Time	20 Seconds ▼
Trigger Alarm Out	
☐ Alarm Out	
☐ Trigger Snap	
☐ Trigger SD Recording	
☐ Trigger Email	
☐ Trigger FTP	

1. Enable the applicable detection that's desired.

Scene Change Detection: Alarms will be triggered if the scene of the monitor video has changed.

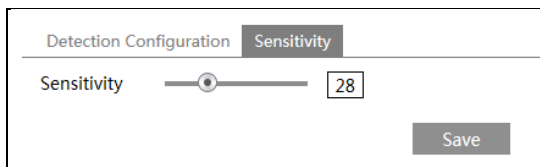
Video Blur Detection: Alarms will be triggered if the video becomes blurry.

Abnormal Color Detection: Alarms will be triggered if the video becomes obscured.

2. Set the alarm holding time and alarm trigger options. The setup steps are the same as motion detection. Please refer to motion detection chapter for details.

3. Click "Save" button to save the settings.

4. Set the sensitivity of the video tampering detection. Click "Sensitivity" tab to go to the interface as shown below.



Drag the slider to set the sensitivity value or directly enter the sensitivity value in the textbox. Click "Save" button to save the settings.

The sensitivity value of Scene Change Detection: The higher the value is, the more sensitive the system responds to the amplitude of the scene change.

The sensitivity value of Video Blur Detection: The higher the value is, the more sensitive the system responds to the blurriness of the image.

The sensitivity value of Abnormal Color Detection: The higher the value is, the more sensitive the system responds to the obscuring of the image.

※ The requirements of camera and surrounding area

1. Auto-focusing function should not been enabled for video tampering detection.
2. Try not to enable video tampering detection when light changes greatly in the scene.
3. Please contact us for more detailed application scenarios.

6.5.2 Line Crossing

Line Crossing: Alarms will be triggered if someone or something crosses the pre-defined alarm lines. It can replace the electronic fence, warning line of flood prevention, etc.

Go to Config→Event→Line Crossing interface as shown below.

Detection ConfigAreaSchedule

☒ Enable

Alarm Holding Time

20 Seconds

Trigger Alarm Out

☐ Alarm Out

☐ Trigger Snap

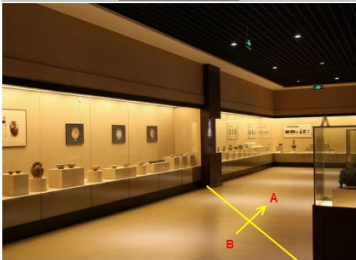
☐ Trigger SD Recording

☐ Trigger Email

☐ Trigger FTP

1. Enable line crossing alarm and set the alarm holding time.
2. Set alarm trigger options. The setup steps are the same as motion detection. Please refer to [motion detection](#) chapter for details.
3. Click “Save” button to save the settings.
4. Set area and sensitivity of the line crossing alarm. Click the “Area and Sensitivity” tab to go to the interface as shown below.

Detection ConfigArea and SensitivitySchedule



Alarm Line

1

Direction

A->B

Draw

Clear

Save

Set the alarm line and the direction. Up to 4 lines can be added. Multiple lines cannot be added simultaneously.

Direction: A<->B, A->B and A<-B optional. This indicates the direction of the intruder who crosses over the alarm line that would trigger the alarm.

A<->B: The alarm will be triggered when the intruder crosses over the alarm line from B to A or from A to B.

A->B: The alarm will be triggered when the intruder crosses over the alarm line from A to B.

A<-B: The alarm will be triggered when the intruder crosses over the alarm line from B to A.

Click the “Draw” button and then drag the mouse to draw an alarm line in the image. Click the “Stop” button to stop drawing. Click the “Clear” button to delete the cordons. Click the “Save” button to save the settings.

5. Set the schedule of the line crossing alarm. The setup steps of the schedule are the same as the schedule recording setup (See [Schedule Recording](#)).

※ Configuration of camera and surrounding area

1. Auto-focusing function should not be enabled for line crossing detection.
 2. Avoid the scenes with many trees or the scenes with various light changes (like many flashing headlights). The ambient brightness of the scenes shouldn't be too low.
 3. Cameras should be mounted at a height of 2.8 meters or above.
 4. Keep the mounting angle of the camera at about 45°.
 5. The detected objects should not be less than 1% of the entire image and the largest sizes of the detected objects should not be more than 1/8 of the entire image.
 6. Make sure cameras can view objects for at least 2 seconds in the detected area for accurate detection.
 7. Adequate light and clear scenery are crucial for line crossing detection.
 8. Please contact us for more detailed application scenarios.
- Here we take some improper application scenarios for instance.



There are so many trees near the road and cars running on the road, which make the scene too complex to detect the crossing objects.



The ground is covered with vegetation; at the right of the fence is a gym where people pass by frequently. The above mentioned environment is too complex to detect the crossing objects.

6.5.3 Perimeter Intrusion

Perimeter Intrusion: Alarms will be triggered if someone or something intrudes into the pre-defined areas. This function can be applicable to important supervision places, danger areas and prohibited areas, like military administrative zones, house breaking, scenic high danger areas, no man's areas, etc.

Go to Config > Event > Intrusion interface as shown below.

Detection Config
Area
Schedule

☒ Enable

Alarm Holding Time
20 Seconds

Trigger Alarm Out

☐ Alarm Out

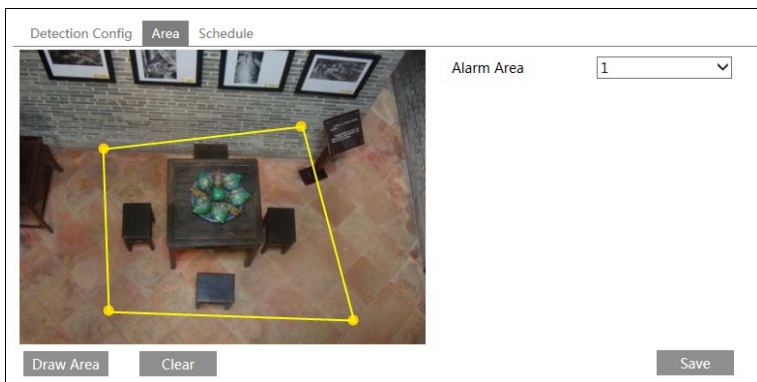
☐ Trigger Snap

☐ Trigger SD Recording

☐ Trigger Email

☐ Trigger FTP

1. Enable perimeter intrusion detection alarm and set the alarm holding time.
2. Set alarm trigger options. The setup steps are the same as motion detection. Please refer to motion detection chapter for details.
3. Click the "Save" button to save the settings.
4. Set the alarm area of the intrusion detection. Click the "Area" tab to go to the interface as shown below.



Set the alarm area number on the right side. Up to 4 alarm areas can be added. Click the “Draw Area” button and then click around the area where you want to set as the alarm area in the image on the left side (the alarm area should be a closed area). Click the “Stop Draw” button to stop drawing. Click the “Clear” button to delete the alarm area. Click the “Save” button to save the settings.

5. Set the schedule of the perimeter intrusion detection. The setup steps of the schedule are the same as schedule recording setup (See [Schedule Recording](#)).

※ Configuration requirements of camera and surrounding area

1. Auto-focusing function should not be enabled for intrusion detection.
 2. Avoid the scenes with many trees or the scenes with various light changes (like many flashing headlights). The ambient brightness of the scenes shouldn't be too low.
 3. Cameras should be mounted at a height of 2.8 meters or above.
 4. Keep the mounting angle of the camera at about 45°.
 5. The detected objects should not be less than 1% of the entire image and the largest sizes of the detected objects should not be more than 1/8 of the entire image.
 6. Make sure cameras can view objects for at least 2 seconds in the detected area for accurate detection.
 7. Adequate light and clear scenery are crucial to perimeter intrusion detection.
 8. Please contact us for more detailed application scenarios.
- Here we take some improper application scenarios for instance.



The camera's angle of depression is not wide enough; there are so many trees in the scene.

→ The environment is too complex to detect the intrusion.



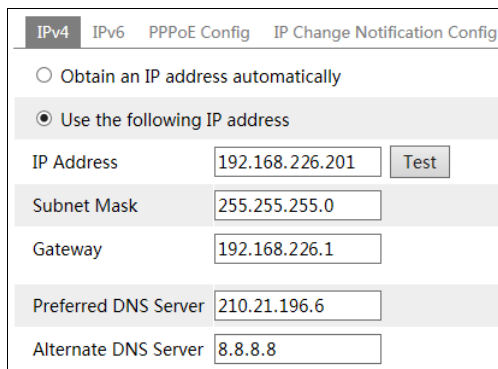
The camera's angle of depression is not wide enough; the street lamps at night lead to light interference; the swaying trees in a windy day lead to random interference.

→ All the above mentioned factors make the scene improper for intrusion detection.

6.6 Network Configuration

6.6.1 TCP/IP

Go to Config→Network→TCP/IP interface as shown below. There are two ways for network connection.

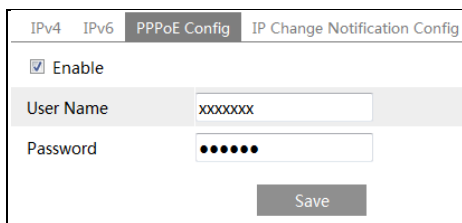


IPv4	IPv6	PPPoE Config	IP Change Notification Config
☐ Obtain an IP address automatically			
☒ Use the following IP address			
IP Address	192.168.226.201		Test
Subnet Mask	255.255.255.0		
Gateway	192.168.226.1		
Preferred DNS Server	210.21.196.6		
Alternate DNS Server	8.8.8.8		

Use IP address (take IPv4 for example)-There are two options for IP setup: obtain an IP address automatically by DHCP and use the following IP address. Please choose one of the options as needed.

Test: Test the effectiveness of the IP address by clicking this button.

Use PPPoE-Click the “PPPoE Config” tab to go to the interface as shown below. Enable PPPoE and then enter the user name and password from your ISP.



IPv4	IPv6	PPPoE Config	IP Change Notification Config
☒ Enable			
User Name	xxxxxxx		
Password	••••••		
Save			

Either method of network connection can be used. If PPPoE is used to connect internet, the camera will get a dynamic WAN IP address. This IP address will change frequently. To be notified, the IP change notification function can be used.

Click “IP Change Notification Config” to go to the interface as shown below.



IPv4	IPv6	PPPoE Config	IP Change Notification Config
☐ Trigger Email			
☐ Trigger FTP			
Save			

Trigger Email: when the IP address of the device is changed, the new IP address will be sent to the email address that has been set up.

Trigger FTP: when the IP address of the device is changed, the new IP address will be sent to FTP server that has been set up.

6.6.2 Port

Go to Config→Network→Port interface as shown below. HTTP port, Data port and RTSP port can be set.

HTTP Port	80
HTTPS Port	443
Data Port	9008
RTSP Port	554

HTTP Port: The default HTTP port is 80. It can be changed to any port which is not occupied.

HTTPS Port: The default HTTPS port is 443. It can be changed to any port which is not occupied.

Data Port: The default data port is 9008. Please change it as necessary.

RTSP Port: The default port is 554. Please change it as necessary.

6.6.3 Server Configuration

This function is mainly used for connecting network video management system.

☒ Enable	
Server Port	2009
Server Address	
Device ID	1
Save	

1. Check "Enable".
2. Check the IP address and port of the transfer media server in the ECMS/NVMS. Then enable the auto report in the ECMS/NVMS when adding a new device. Next, enter the remaining information of the device in the ECMS/NVMS. After that, the system will automatically allot a device ID. Please check it in the ECMS/NVMS.
3. Enter the above-mentioned server address, server port and device ID in the corresponding boxes. Click the "Save" button to save the settings.

6.6.4 DDNS

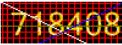
If the camera is set up with a DHCP connection, DDNS should be set for the internet.

1. Go to Config→Network→ DDNS.

Port	Server	DDNS	SNMP	RTSP	UPnP	Email	FTP
☒ Enable							
Server Type	mintdns ▼						
Server Address	www.dvrddns.com						
User Name							
Password							
Domain							
							Save

2. Apply for a domain name. Take www.dvrddns.com for example.

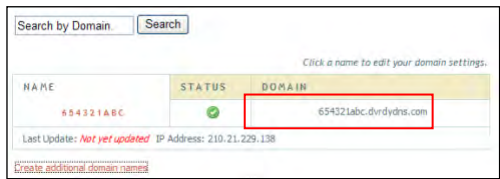
Enter www.dvrddns.com in the IE address bar to visit its website. Then Click the “Registration” button.

NEW USER REGISTRATION	
USER NAME	xxxx
PASSWORD	•••••
PASSWORD CONFIRM	•••••
FIRST NAME	xxx
LAST NAME	xxx
SECURITY QUESTION	My first phone number. ▼
ANSWER	xxxxxxxx
CONFIRM YOU'RE HUMAN	 New Captcha Enter the text you see above
Submit Reset	

Create domain name.

<i>You must create a domain name to continue.</i>	
Domain name must start with (a-z, 0-9). Cannot end or start, but may contain a hyphen and is not case-sensitive.	
	dvrddns.com ▼ Request Domain

After the domain name is successfully applied for, the domain name will be listed as below.



3. Enter the username, password, domain you apply for in the DDNS configuration interface.
4. Click the “Save” button to save the settings.

6.6.5 SNMP

To get camera status, parameters and alarm information and remotely manage the camera, the SNMP function can be used. Before using SNMP, please install an SNMP management tool and set the parameters of the SNMP, such as SNMP port, trap address.

1. Go to Config→Network→SNMP.
2. Check the corresponding version checkbox (Enable SNMPv1, Enable SNMPv2, Enable SNMPv3) according to the version of the SNMP software that will be used.
3. Set the values for “Read SNMP Community”, “Write SNMP Community”, “Trap Address”, “Trap Port” and so on. Please make sure the settings are the same as that of the SNMP software.

Note: Please use the different version in accordance with the security level you required. The higher the version is, the higher the level of the security is.

SNMP v1/v2	
☐ Enable SNMPv1	
☐ Enable SNMPv2	
Read SNMP Community	
Write SNMP Community	
Trap Address	...
Trap Port	0
Trap community	
SNMP v3	
☐ Enable SNMPv3	
Read User Name	
Security Level	auth, priv
Authentication Algorithm	☒ MD5 ☐ SHA
Authentication Password	
Private-key Algorithm	☒ DES ☐ AES
Private-key Algorithm	
Write User Name	
Security Level	auth, priv
Authentication Algorithm	☒ MD5 ☐ SHA
Authentication Password	
Private-key Algorithm	☒ DES ☐ AES
Private-key Algorithm	
Other Settings	
SNMP Port	0

6.6.6 802.1x

IEEE802.X which is an access control protocol manages the device in connection with the local network by authentication. The setup steps are as follows:

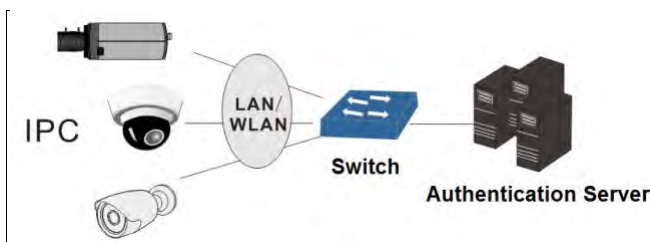
☒ Enable	
Protocol Type	EAP_MD5
EAPOL Version	1
User Name	test
Password	
Confirm Password	

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

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

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

The structure of 802.1x



- ① The network camera initiates the authentication of 802.1x protocol via web client and then the authentication is received by the switch supporting 802.1x protocol.
- ② The switch provides the camera with a physical or logic local network interface and verifies the camera.
- ③ Authentication server provides the entity of authentication service for the switch, stored the relative information of web client, realizing the authentication of web client. Please refer to the user manual of the connected switch for more details.

6.6.7 RTSP

Go to Config→Network→RTSP.

☒ Enable			
Port	554		
Address	rtsp://IP or domain name:port/profile1		
	rtsp://IP or domain name:port/profile2		
	rtsp://IP or domain name:port/profile3		
Multicast address			
Main stream	239.0.0.0	50554	☐ Automatic start
Sub stream	239.0.0.1	51554	☐ Automatic start
Third stream	239.0.0.2	52554	☐ Automatic start
Audio	239.0.0.3	53554	☐ Automatic start
☐ Allow anonymous login (No username or password required)			
Save			

Select “Enable” to enable the RTSP function.

Port: Access port of the streaming media. The default number is 554.

RTSP Address: The RTSP address (unicast) format that can be used to play the stream in a media player.

Multicast Address

Main stream: The address format is

“rtsp://IP address: rtsp port/profile1?transportmode=mcast”.

Sub stream: The address format is

“rtsp://IP address: rtsp port/profile2?transportmode=mcast”.

Third stream: The address format is

“rtsp://IP address: rtsp port/profile3?transportmode=mcast”.

Audio: Having entered the main/sub stream in a VLC player, the video and audio will play automatically.

If “Allow anonymous login...” is checked, there is no need to enter the username and password to view the video.

If “auto start” is enabled, the multicast received data should be added into a VLC player to play the video.

Note:1. This camera support local play through a VLC player. Enter the RTSP address (unicast or multicast, eg. rtsp://192.168.226.201:554/profile1?transportmode=mcast) in a VLC player to realize the simultaneous play with the web client.

2. The IP address mentioned above cannot be the address of IPv6.

3. Avoid the use of the same multicast address in the same local network.

4. When playing the video through the multicast streams in a VLC player, please pay attention to the mode of the VLC player. If it is set to TCP mode, the video cannot be played.

5. If the coding format of the video of the main stream is MJPEG, the video may be disordered at some resolutions.

6.6.8 UPNP

If this function is enabled, the camera can be quickly accessed through the LAN.

Go to Config→Network→UPnP. Enable UPNP and then enter UPnP name.



6.6.9 Email

If you need to trigger Email when an alarm happens or IP address is changed, please set the Email here first. Go to Config→Network→Email.

Port Server DDNS SNMP RTSP UPnP **Email** FTP

Sender

Sender Address: XXX@126.com

User Name: XXX@126.com

Password: ••••••

Server Address: smtp.126.com

Secure Connection: Unnecessary

SMTP Port: 25 Default

☐ Send Interval(S): 0 (0-3600)

Clear Test

Recipient

XXXX@126.com

Recipient Address:

Add Delete Save

Sender Address: sender's e-mail address.

User name and password: sender's user name and password.

Server Address: The SMTP IP address or host name.

Select the secure connection type at the "Secure Connection" pull-down list according to what's required.

SMTP Port: The SMTP port.

Send Interval(S): The time interval of sending email. For example, if it is set to 60 seconds and multiple motion detection alarms are triggered within 60 seconds, they will be considered as only one alarm event and only one email will be sent. If one motion alarm event is triggered and then another motion detection alarm event is triggered after 60 seconds, two emails will be sent. When different alarms are triggered at the same time, multiple emails will be sent separately.

Click the "Test" button to test the connection of the account.

Recipient Address: receiver's e-mail address.

6.6.10 FTP

After an FTP server is set up, captured pictures from events will be uploaded to the FTP server.

Go to Config→Network →FTP.

PortServerDDNSSNMPRTSPUPnPEmailFTP

Server Name	Server Address	Port	User Name	Upload Path
Add FTP Server Name Server Address Upload Path Port User Name Password Example/Dir/folder 21 Anonymous OK Cancel				
Add Modify Delete Save				

Server Name: The name of the FTP server.

Server Address: The IP address or domain name of the FTP.

Upload Path: The directory where files will be uploaded to.

Port: The port of the FTP server.

Use Name and Password: The username and password that are used to login to the FTP server.

6.6.11 HTTPS

HTTPS provides authentication of the web site and protects user privacy.

Go to Config Config→Network→HTTPS as shown below.

☒ Enable

Certificate installed

C=CN, ST=GD, L=SZ, O=embeddedsoftware, OU=IPC, H=localhost, E=com.cn, Issuer: C=CN, ST=GD, L=SZ, O=embeddedsoftware, OU=IPC, H=localhost, E=com.cn, Validity date: 2017-07-26 01:02:07 ~ 2022-07-26 01:02:07

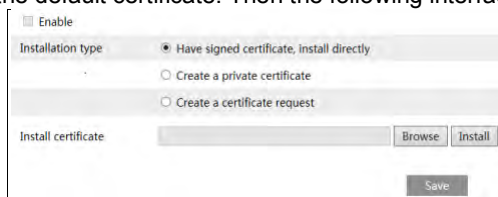
Delete

Attribute

Save

There is a certificate installed by default as shown above. Enable this function and save it. Then the camera can be accessed by entering https://IP: https port via the web browser (eg. https://192.168.226.201:443).

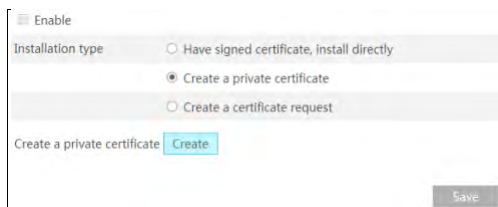
A private certificate can be created if users don't want to use the default one. Click "Delete" to cancel the default certificate. Then the following interface will be displayed.



The screenshot shows a web interface titled "Enable". Under the "Installation type" section, there are three radio button options: "Have signed certificate, install directly" (which is selected), "Create a private certificate", and "Create a certificate request". Below this, there is a text input field labeled "Install certificate" followed by "Browse" and "Install" buttons. At the bottom right, there is a "Save" button.

* If there is a signed certificate, click "Browse" to select it and then click "Install" to install it.

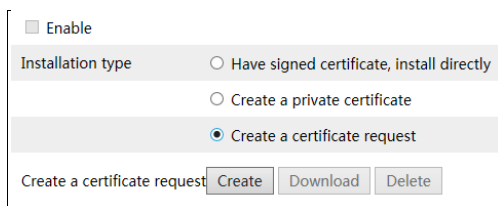
* Click "Create a private certificate" to enter the following creation interface.



The screenshot shows the "Create a private certificate" interface. It has the same "Enable" header and "Installation type" section as the previous form, but with "Create a private certificate" selected. Below the radio buttons, there is a "Create a private certificate" label followed by a blue "Create" button. A "Save" button is located at the bottom right.

Click the "Create" button to create a private certificate. Enter the country (only two letters available), domain (camera's IP address/domain), validity date, password, province/state, region and so on. Then click "OK" to save the settings.

* Click "Create a certificate request" to enter the following interface.



The screenshot shows the "Create a certificate request" interface. It has the same "Enable" header and "Installation type" section, but with "Create a certificate request" selected. Below the radio buttons, there is a "Create a certificate request" label followed by "Create", "Download", and "Delete" buttons.

Click "Create" to create the certificate request. Then download the certificate request and submit it to the trusted certificate authority for signature. After receiving the signed certificate, import the certificate to the device.

6.6.12 P2P (Optional)

If this function is enabled, the network camera can be quickly accessed by adding the device ID in mobile surveillance client or CMS/NVMS client via WAN. Enable this function by going to Config→Network→P2P interface.

☒ P2P

Save

6.6.13 QoS

QoS (Quality of Service) function is used to provide different quality of services for different network applications. With the deficient bandwidth, the router or switch will sort the data streams and transfer them according to their priority to solve the network delay and network congestion by using this function.

Go to Config→Network→QoS.

Video/Audio DSCP	13
Alarm DSCP	35
Manager DSCP	53

Video/Audio DSCP: The range is from 0 to 63.

Alarm DSCP: The range is from 0 to 63.

Manager DSCP: The range is from 0 to 63.

Generally speaking, the larger the number is, the higher the priority is.

6.7 Security Configuration

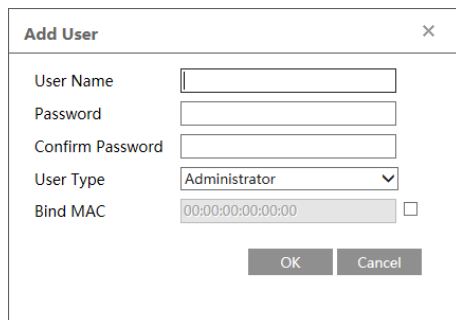
6.7.1 User Configuration

Go to Config→Security→User interface as shown below.

Add Modify Delete			
Index	User Name	User Type	Binding MAC
1	admin	Administrator	

Add user:

1. Click the “Add” button to pop up the following textbox.



The "Add User" dialog box contains the following fields and controls:

- User Name:** A text input field.
- Password:** A text input field.
- Confirm Password:** A text input field.
- User Type:** A dropdown menu with "Administrator" selected.
- Bind MAC:** A text input field containing "00:00:00:00:00:00" and an unchecked checkbox to its right.
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

2. Enter user name in “User Name” textbox.

3. Enter letters or numbers in “Password” and “Confirm Password” textbox.

4. Choose the use type. Administrator has all permissions. Normal user can only view the live video. Advanced user has the same permissions as an Administrator except for; user, backup settings, factory reset, and upgrading the firmware.

5. Enter the MAC address of the PC in “Bind MAC” textbox.

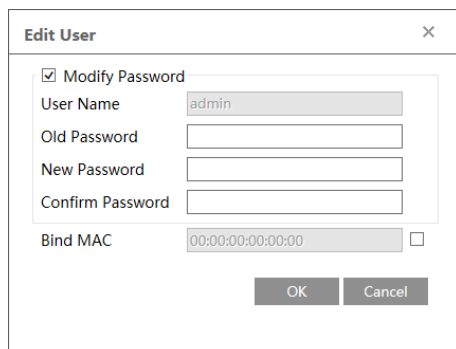
If this option is enabled, only the PC with the specified MAC address can access the camera for that user.

6. Click the “OK” button and then the newly added user will be displayed in the user list.

Modify user:

1. Select a user to modify password and MAC address if necessary in the user configuration list box.

2. The “Edit user” dialog box pops up by clicking the “Modify” button.



The "Edit User" dialog box contains the following fields and controls:

- Modify Password:** A checked checkbox.
- User Name:** A text input field with "admin" entered.
- Old Password:** A text input field.
- New Password:** A text input field.
- Confirm Password:** A text input field.
- Bind MAC:** A text input field containing "00:00:00:00:00:00" and an unchecked checkbox to its right.
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

3. Enter the old password of the user in the “Old Password” text box.

4. Enter the new password in the “New password” and “Confirm Password” text box.

5. Enter computer’s MAC address as necessary.

6. Click the “OK” button to save the settings.

Note: To change the access level of a user, the user must be deleted and added again with the new access level.

Delete user:

1. Select the user to be deleted in the user configuration list box.
2. Click the “Delete” button to delete the user.

Note: The default administrator account cannot be deleted.

6.7.2 Online User

Go to Config→Security→Online User to view the user who is viewing the live video.

Index	Client Address	Port	User Name	User Type	
1	192.168.17.232	55760	admin	Administrator	<button>Kick Out</button>

An administrator user can kick out all the other users (including other administrators).

6.7.3 Block and Allow Lists

Go to Config→Security→Block and Allow Lists as shown below.

IP/MAC Address Filter Settings

☒ Enable address filtering

☒ Block the following address

☐ Allow the following address

Add

Delete

0.0.0.0

☒ IPv4 ☐ IPv6 ☐ MAC

Save

The setup steps are as follows:

Check the “Enable address filtering” check box.

Select “Block/Allow the following address”, IPv4/IPv6/MAC and then enter IP address or MAC address in the address box and click the “Add” button.

6.7.4 Security Management

Go to Config→Security→Security Management as shown below.

Security Service

☒ Enable “locking once illegal login” function

☒ Enable anonymous login with a private protocol (http://host[:port]/AnonymousLive/1/1/2/3)

Save

In order to prevent against malicious password unlocking, “locking once illegal login”

function can be enabled here. If this function is enabled, login failure after trying six times will make the login interface locked. The camera can be logged in again after a half hour or after the camera reboots.

For some specified versions, anonymous login with a private protocol can be enabled here. If this function is enabled, enter `http://host:port/Anonymous/1[2/3]` (eg. `http://192.168.226.201:80/Anonymous/1`) via web browser to access the camera. 1 indicates main stream; 2 indicates sub stream; 3 indicates third stream. Only video can be viewed by this means and no other operations can be done. If no such function, please skip the instruction.

6.8 Maintenance Configuration

6.8.1 Backup and Restore

Go to Config→Maintenance→Backup & Restore.

The screenshot shows a web interface for 'Backup and Restore' settings. It is divided into three main sections: 'Import Setting', 'Export Settings', and 'Default Settings'. The 'Import Setting' section has a 'Path' input field with a 'Browse' button and an 'Import Setting' button. The 'Export Settings' section has an 'Export Settings' button. The 'Default Settings' section has a 'Keep' label and three checkboxes: 'Network Config', 'Security Configuration', and 'Image Configuration'. Below these checkboxes is a 'Load Default' button.

- Import & Export Settings

Configuration settings of the camera can be exported from a camera into another camera.

1. Click "Browse" to select the save path for import or export information on the PC.
2. Click the "Import Setting" or "Export Setting" button.

- Default Settings

Click the "Load Default" button to restore all system settings to the default factory settings.

6.8.2 Reboot

Go to Config→Maintenance→Reboot.

Click the “Reboot” button to reboot the device.

Timed Reboot Setting:

If necessary, the camera can be set up to reboot on a time interval. Enable “Time Settings”, set the date and time and then click the “Save” button to save the settings.

6.8.3 Upgrade

Go to Config→Maintenance→Upgrade. In this interface, the camera firmware can be updated.

The screenshot shows a web interface for upgrading the camera firmware. It is divided into two main sections: "Local upgrade" and "Online upgrade".

Local upgrade section:

- There is a text input field labeled "Path".
- To the right of the "Path" field are two buttons: "Browse" and "Upgrade".

Online upgrade section:

- There is a text input field labeled "Upgrade file path".
- To the right of the "Upgrade file path" field is a "Save" button.
- Below the input fields is a table with three columns: "Current version", "Server version", and "Operate".
- The "Current version" column contains the text "4.2.1.0".
- The "Server version" column is empty.
- The "Operate" column contains two buttons: "Check version" and "Upgrade".

1. Click the “Browse” button to select the save path of the upgrade file
2. Click the “Upgrade” button to start upgrading the firmware.
3. The device will restart automatically

Caution! Do not close the browser or disconnect the camera from the network during the upgrade.

For some specified models, online upgrade is available. The setting steps are as follows. If no such function, please skip the instruction.

1. Create the upgrade file location and save it.
2. Check the latest version by clicking “Check version”.
3. Click “Upgrade” to update the firmware online.

6.8.4 Operation Log

To query and export log:

1. Go to Config→Maintenance→Operation Log.

Main Type:	All log	Sub Type:	All log		
Start Time:	2015-07-14 00:00:00	End Time:	2015-07-14 23:59:59	Search	Export

Index	Time	Main Type	Sub Type	User Name	Login IP
1	2015-07-14 11:15:18	Operation	Log In	admin	192.168.12.53
2	2015-07-14 11:12:02	Exception	Disconnected		192.168.12.53
3	2015-07-14 19:12:17	Exception	Disconnected		192.168.12.52

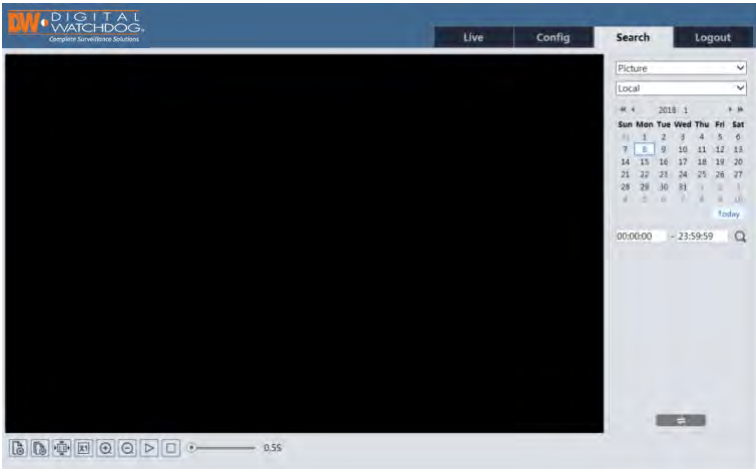
2. Select the main type, sub type, start and end time.
3. Click “Search” to view the operation log.
4. Click “Export” to export the operation log.

7 Search

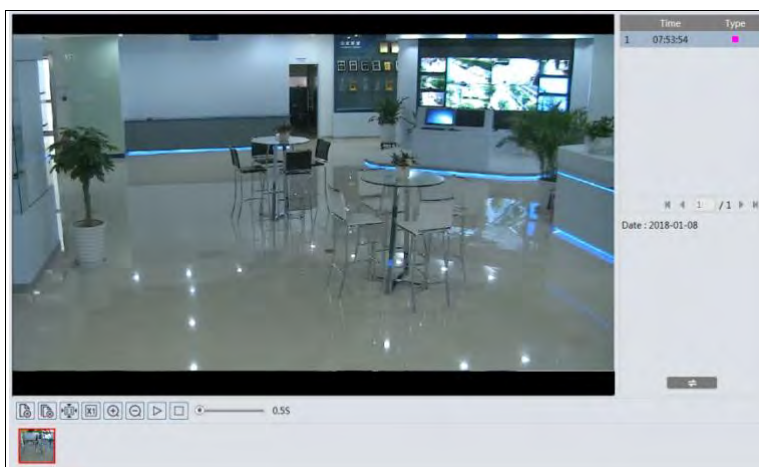
7.1 Image Search

Click Search to go to the interface as shown below. Images that are saved on the SD card can be found here.

Note: If there is no SD card installed in the camera or the SD card is not compatible with the camera, a pop-up message will show stating that there is no card.



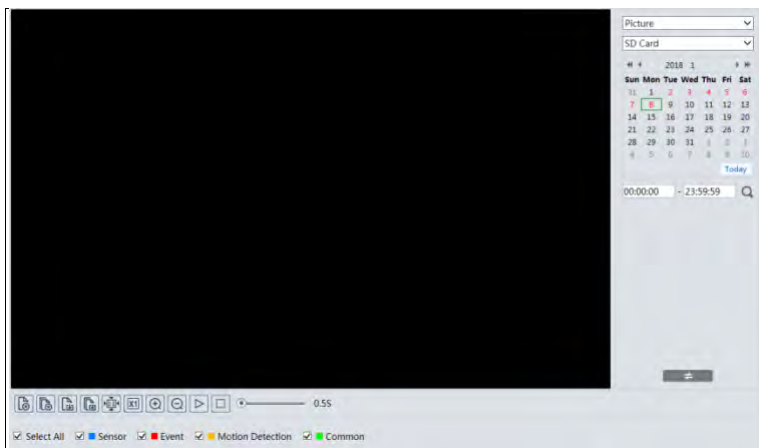
- Local Image Search
 1. Choose “Picture”—“Local”.
 2. Set time: Select date and choose the start and end time.
 3. Click  to search the images.
 4. Double click a file name in the list to view the captured photos as shown above.



Click  to return to the previous interface.

● SD Card Image Search

1. Choose “Picture”—“SD Card”.



2. Set time: Select date and choose the start and end time.
 3. Choose the alarm events at the bottom of the interface.
 4. Click  to search the images.
 5. Double click a file name in the list to view the captured photos.
- Click  to return to the previous interface.

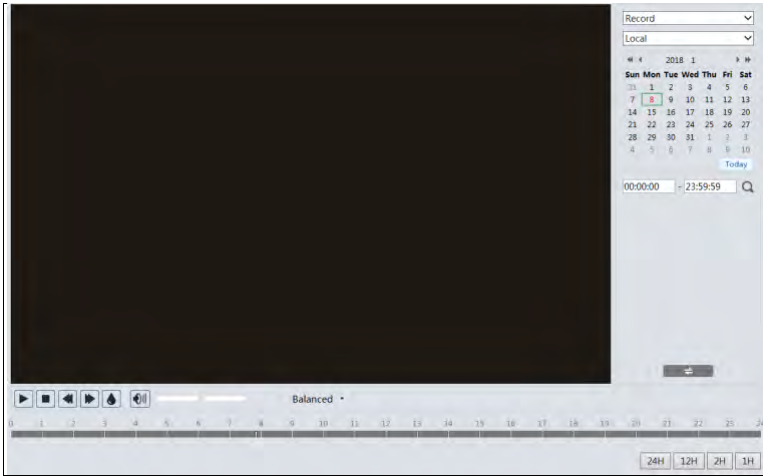
The descriptions of the buttons are shown as follows.

Icon	Description	Icon	Description
	Close: Select an image and click this button to close the image.		Close all: Click this button to close all images.
	Save: Click this button to select the path for saving the image on the PC.		Save all: Click this button to select the path for saving all pictures on the PC.
	Fit size: Click to fit the image on the screen.		Actual size: Click this button to display the actual size of the image.
	Zoom in: Click this button to digitally zoom in.		Zoom out: Click this button to digitally zoom out.
	Slide show play: Click this button to start the slide show mode.		Stop: Click this button to stop the slide show.
	Play speed: Play speed of the slide show.		

7.2 Video Search

7.2.1 Local Video Search

Click Search to go to the interface as shown below. Videos were recorded locally to the PC can be played in this interface.



- 1. Choose “Record”—“Local”.
- 2. Set search time: Select the date and choose the start and end time.
- 3. Click to search the images.
- 4. Double click on a file name in the list to start playback.



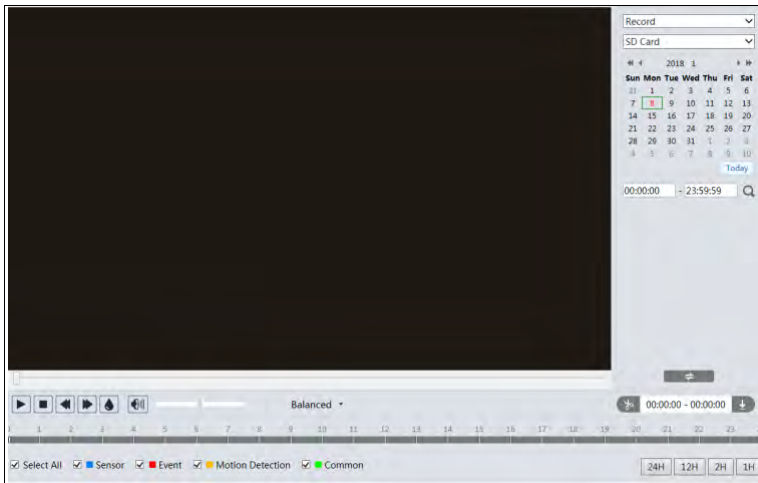
Icon	Description	Icon	Description
	Play button. After pausing the video, click this button to continue playing.		Pause button
	Stop button		Speed down
	Speed up		Watermark display
	Enable / disable audio; drag the slider to adjust the volume after enabling audio.		

7.2.2 SD Card Video Search

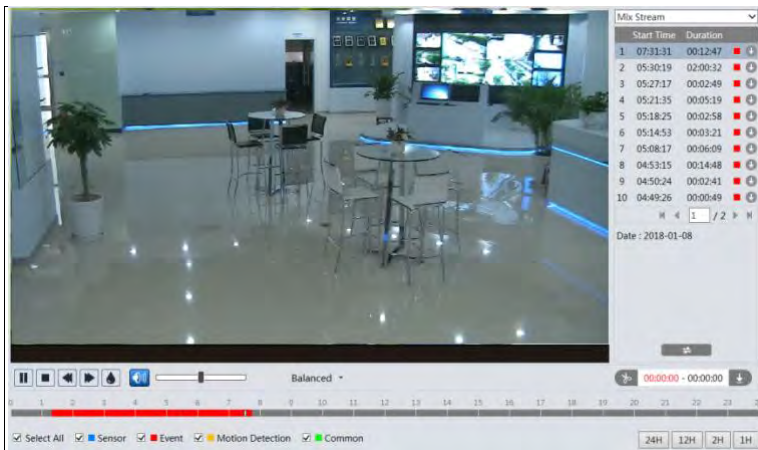
Click Search to go to the interface as shown below. Videos that were recorded on the SD card can be played in this interface.

Note: If the camera doesn't support SD card, please skip the instructions of SD card video search.

1. Choose "Record"—"SD Card".
2. Set search time: Select the date and choose the start and end time.
3. Click  to search the images.



4. Select the alarm events at the bottom of the interface.
5. Select mix stream (video and audio stream) or video stream as needed.
6. Double click on a file name in the list to start playback.



The time table can be shown in 24H/12H/2H/1H format by clicking the corresponding buttons.

Video clip and downloading

1. Search the video files according to the above mentioned steps.
2. Select the start time by clicking on the time table.
3. Click  to set the start time and then this button turns blue ().
4. Select the end time by clicking on the time table. Then click  to set the end time.

5. Click  to download the video file in the PC.

Index	Process	Record	Start Time	End Time	Path	Operate
1	100%	Cut	2018-01-16 01:1...	2018-01-16 01:1...	Favorites	Open

[Set up](#) D:\Favorites [Clear List](#) [Close](#)

Click “Set up” to set the storage directory of the video files.

Click “Open” to play the video.

Click “Clear List” to clear the downloading list.

Click “Close” to close the downloading window.

8 Appendix

Appendix 1 Troubleshooting

How to find the password?

A: Reset the device to the default factory settings.

Default IP: 192.168.226.201; User name: admin; Password: 123456

Fail to connect devices through IE browser.

A: Network is not well connected. Check the connection and make sure it is connected well.

B: IP address is not available. Reset the IP address.

C: Web port number has been changed: contact administrator to get the correct port number.

D: Exclude the above reasons. Restore to default setting by IP-Tool.

IP tool cannot search devices.

It may be caused by the anti-virus software in your computer. Please exit it and try to search device again.

IE cannot download ActiveX control.

A. IE browser may be set up to block ActiveX. Follow the steps below.

① Open IE browser and then click Tools-----Internet Options.

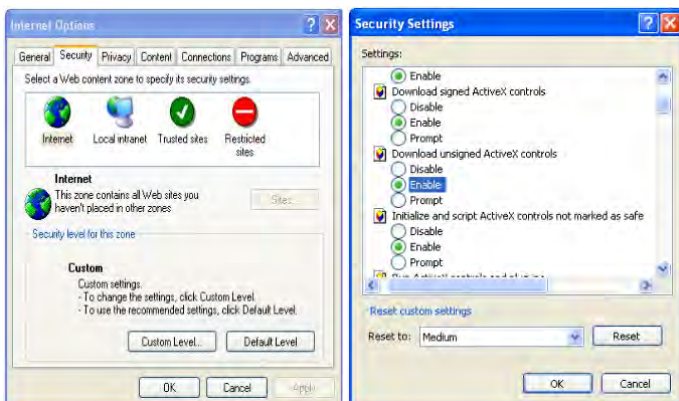


② Select Security-----Custom Level....

③ Enable all the options under "ActiveX controls and plug-ins".

④ Click OK to finish setup.

B. Other plug-ins or anti-virus blocks ActiveX. Please uninstall or close them.

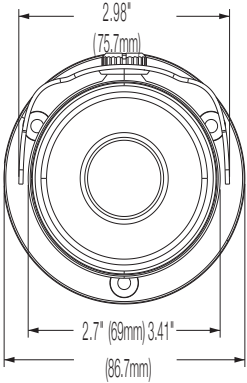
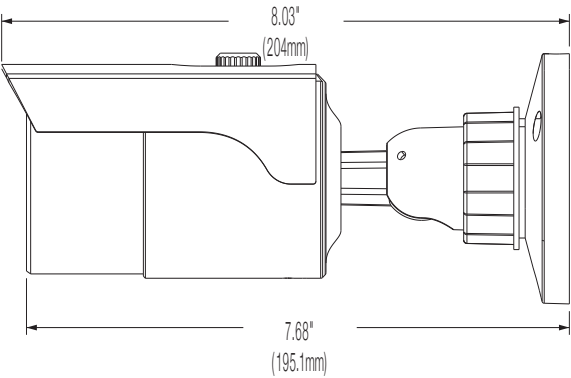


No sound can be heard.

A: Audio input device is not connected. Please connect and try again.

B: Audio function is not enabled at the corresponding channel. Please enable this function.

9 Dimensions



10 Warranty Information

Digital Watchdog (referred to as “the Warrantor”) warrants the Camera against defects in materials or workmanships as follows:

Labor: For the initial five (5) years from the date of original purchase if the camera is determined to be defective, the Warrantor will repair or replace the unit with new or refurbished product at its option, at no charge.

Parts: In addition, the Warrantor will supply replacement parts for the initial five (5) years.

To obtain warranty or out of warranty service, please contact a technical support representative at 1+ (866) 446-3595, Monday through Friday from 9:00AM to 8:00PM EST.

A purchase receipt or other proof of the date of the original purchase is required before warranty service is rendered. This warranty only covers failures due to defects in materials and workmanship which arise during normal use. This warranty does not cover damages which occurs in shipment or failures which are caused by products not supplied by the Warrantor or failures which result from accident, misuse, abuse, neglect, mishandling, misapplication, alteration, modification, faulty installation, set-up adjustments, improper antenna, inadequate signal pickup, maladjustments of consumer controls, improper operation, power line surge, improper voltage supply, lightning damage, rental use of the product or service by anyone other than an authorized repair facility or damage that is attributable to acts of God.

11 Limits and Exclusions

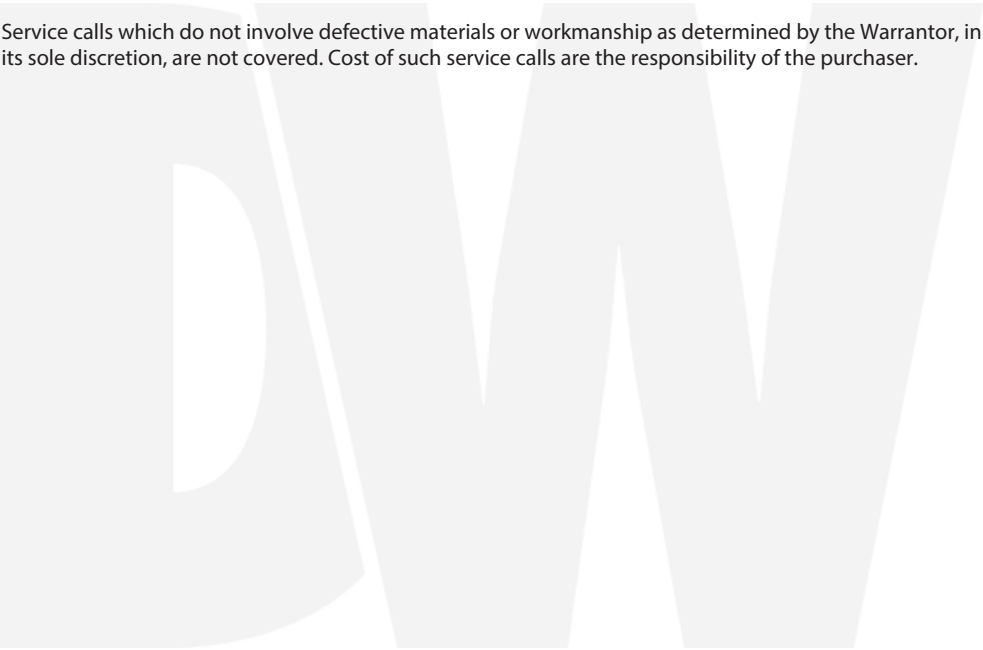
There are no express warranties except as listed above. The Warrantor will not be liable for incidental or consequential damages (including, without limitation, damage to recording media) resulting from the use of these products, or arising out of any breach of the warranty. All express and implied warranties, including the warranties of merchantability and fitness for particular purpose, are limited to the applicable warranty period set forth above.

Some states do not allow the exclusion or limitation of incidental or consequential damages or limitations on how long an implied warranty lasts, so the above exclusions or limitations may not apply to you. This warranty gives you specific legal rights, and you may also have other rights from vary from state to state.

If the problem is not handled to your satisfaction, then write to the following address:

Digital Watchdog, Inc.
ATTN: RMA Department
5436 W Crenshaw St
Tampa, FL 33634

Service calls which do not involve defective materials or workmanship as determined by the Warrantor, in its sole discretion, are not covered. Cost of such service calls are the responsibility of the purchaser.





Complete Surveillance Solutions

Headquarters Office: 5436 W Crenshaw St, Tampa, FL 33634
Sales Office: 16220 Bloomfield Ave., Cerritos, California, USA 90703

PH: 866-446-3595 | FAX: 813-888-9262

www.Digital-Watchdog.com

technicalsupport@dwcc.tv

Technical Support PH:

USA & Canada 1+ (866) 446-3595

International 1+ (813) 888-9555

French Canadian 1+ (514) 360-1309

Technical Support Hours: Monday-Friday
9:00am to 8:00pm Eastern Standard Time