

MEGApix[®] 5MP Turret IP Camera

DWC-MT95WiATW



User's Manual Ver. 01/22

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

Safety Notes

- This product is intended to be supplied by a Listed Power Unit, marked with 'Limited Power Source', 'LPS' on the unit, output rated minimum 12V/2 A or POE 48V/ 350mA or AC24V (depending on models), no more than 2000m altitude of operation and 60 degrees C.
- As for the modes with PoE function, the function of the ITE being investigated to IEC 60950-1 standard is considered not likely to require connection to an Ethernet network with outside plant routing, including campus environment and the ITE is to be connected only to PoE networks without routing to the outside plant.
- Do not try to disassemble the camera; to prevent electric shock, do not remove screws or covers.
- There are no user-serviceable parts inside. Please contact the nearest service center as soon as possible if there is any failure.
- Avoid incorrect operation, shock vibration, heavy pressing which can cause damage to the product.
- Do not use a corrosive detergent to clean the main body of the camera. If necessary, please use a soft dry cloth to wipe dirt; for hard contamination, use neutral detergent. Any cleanser for high-grade furniture is applicable.
- Avoid aiming the camera directly towards extremely bright objects, such as the sun, as this may damage the image sensor.
- Please follow the instructions to install the camera. Do not reverse the camera, or the reversing image will be received.
- Do not work the camera in case temperature, humidity and power supply are beyond the limited stipulations.
- Keep away from heat sources such as radiators, heat registers, stoves, etc.
- Do not expose the product to the direct airflow from an air conditioner.
- This manual is for using and managing the product. We may reserve the right of amending the typographical errors, inconsistencies with the latest version, software upgrades and product improvements, interpretation and modification. These changes will be published in the latest version without special notification.
- All pictures, charts, images in this manual are only for description and explanation of our products. In this manual, the trademarks, product names, service names, company names, products that are not owned by our company are the properties of their respective owners.

Disclaimer

- Concerning the product with internet access, the use of the product shall be wholly at your own risk. Our company shall be irresponsible for abnormal operation, privacy leakage, or other damages resulting from cyber-attack, hacker attacks, virus inspection, or other internet security risks; however, our company will supply timely technical support if necessary.
- Surveillance laws vary from country to country. Check all laws in your local region before using this product for surveillance purposes. We shall not take the responsibility for any consequences resulting from illegal operations.

Cybersecurity Recommendations

- Use a strong password. At least 8 characters or a combination of characters, numbers and upper- and lower-case letters should be used in your password.
- Change the passwords periodically to ensure that only authorized users can access the system (recommended time is 90 days).
- It is recommended to change the service default ports (like HTTP-80, HTTPS-443, etc.) to reduce the risk of outsiders being able to access.
- It is recommended to set a security system for your router. Important ports such as HTTP, HTTPS and dual ports cannot be closed.
- It is not recommended to expose the device to the public network. When it is necessary to be exposed to the public network, please set the external hardware security system and the corresponding security system policy.
- It is not recommended to use the v1 and v2 functions of SNMP.
- To enhance the security of WEB client access, please create a TLS certificate to enable HTTPS.
- Use black- and white- lists to filter the IP address. This will prevent everyone, except those specified IP addresses from accessing the system.
- If you add multiple users, limit the functions of guest accounts.
- If you enable UPnP, it will automatically try to forward ports in your router or modem. It is very convenient for users, but this will increase the risk of data leakage when the system automatically forwards ports. Disabling UPnP is recommended when the function is not used in real applications.
- Check the log. If you want to know whether your device has been accessed by unauthorized users or not, you can check the log. The system log will show you which IP addresses were used to log in to your system and what was accessed.

Regulatory Information

FCC Information

1. FCC compliance

The products have been tested and found in compliance with the council FCC rules and regulation's part 15 subpart B. These limits are designed to provide reasonable protection against harmful interference. This equipment generates uses and can radiate radio frequency energy and, if not installed and used following the instruction manual, may cause harmful interference to radio communication. However, there is no guarantee that interference will not occur in a particular installation. The user will be required to correct the interface at his own expense in case harmful interference occurs.

2. FCC conditions:

The operation of this product is subject to the following two conditions: (1) this device may not cause a harmful interface and (2) this device must accept any interference received, including interference that may cause undesired operation.

CE Information



EMC Directive 2014/30/EU

RoHS

The products have been designed and manufactured following Directive EU RoHS Directive 2011/65/EU and its amendment Directive EU 2015/863 on the restriction of the use of certain hazardous substances in electrical and electronic equipment.



2012/19/EU (WEEE directive): The Directive on waste electrical and electronic equipment (WEEE Directive). To improve the environmental management of WEEE, the improvement of collection, treatment and recycling of electronics at the end of their life is essential. Therefore, the product marked with this symbol must be disposed of responsibly.

Directive 94/62/EC: The Directive aims at the management of packaging and packaging waste and environmental protection. The packaging and packaging waste of the product in this manual refers to must be disposed of at designated collection points for proper recycling and environmental protection.

REACH(EC1907/2006): REACH concerns the Registration, Evaluation, Authorization and Restriction of Chemicals, which aims to ensure a high level of protection of human health and the environment through better and earlier identification of the intrinsic properties of chemical substances. The product in this manual refers to conforms to the rules and regulations of REACH. For more information on REACH, please refer to DG GROWTH or ECHA websites.

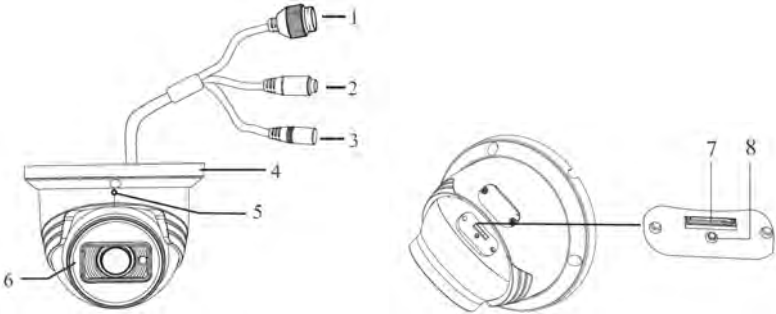
Table of Contents

1	Introduction	1
1.1	Product and Accessories	1
1.2	Parts identification	1
2	Installation	2
2.1	Installation	2
2.2	Cabling	3
2.3	Managing the SD Card	3
3	Network Setup	4
3.1	IP Finder	4
4	Live View	6
5	Network Camera Configuration	8
5.1	System Configuration	8
5.1.1	Basic Information	8
5.1.2	Date and Time	8
5.1.3	Local Config	9
5.1.4	Storage	9
5.2	Image Configuration	11
5.2.1	Display Configuration	11
5.2.2	Video / Audio Configuration	14
5.2.3	OSD Configuration	16
5.2.4	Video Mask	16
5.2.5	ROI Configuration	17
5.2.6	Zoom/Focus	18
5.3	Alarm Configuration	20
5.3.1	Motion Detection	20
5.3.2	Other Alarms	21
5.3.3	Alarm In	23
5.3.4	Alarm Out	23
5.4	Event Configuration	25
5.4.1	Video Tampering Detection	25
5.4.2	Line Crossing	26
5.4.3	Perimeter Intrusion	28
5.5	Network Configuration	30
5.5.1	TCP/IP	30
5.5.2	Port	31
5.5.3	DDNS	31
5.5.4	SNMP	33
5.5.5	802.1x	33
5.5.6	RTSP	33
5.5.7	UPNP	35
5.5.8	Email	35
5.5.9	FTP	36
5.5.10	HTTPS	36
5.5.11	QoS	38
5.6	Security Configuration	38
5.6.1	User Configuration	38
5.6.2	Online User	40
5.6.3	Block and Allow Lists	40
5.6.4	Security Management	41
5.7	Maintenance Configuration	42
5.7.1	Backup and Restore	42
5.7.2	Reboot	43
5.7.3	Upgrade	43
5.7.4	Operation Log	43
6	Search	44
6.1	Image Search	44
6.2	Video Search	46
6.2.1	Local Video Search	46
6.2.2	SD Card Video Search	47
7	Appendix	50
7.1	Troubleshooting	50
7.2	Dimensions	52
7.3	Specifications	53
	Warranty	55

1 Introduction

1.1 Product and Accessories

WHAT'S IN THE BOX					
Quick setup and Installation guides		1 set	Tapping Screws - 3pcs		1 set
Mounting Template		1	Plastic Plugs - 3pcs		1 set
Waterproof Cap		1 set	Rubber Plug		1
Hexagonal Wrench 0.07" (2mm)		1			

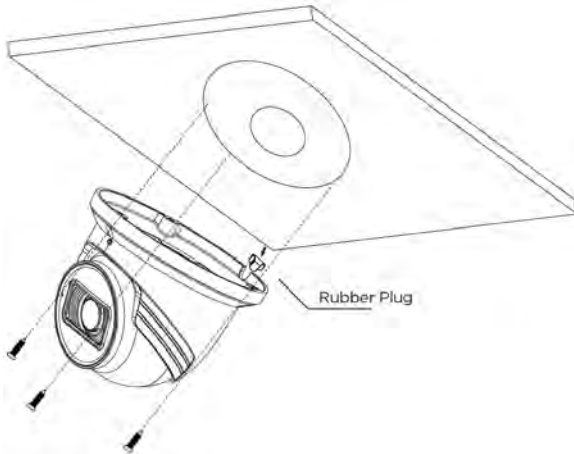


Number	Description	Number	Description
1	Network Cable	5	Rotation Screw
2	Audio Input	6	Built-in Microphone
3	Power Cable	7	Micro SD Card Slot
4	Mounting Base	8	Reset Button

2 Installation

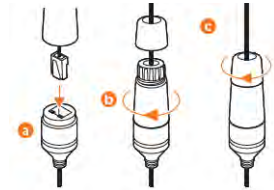
2.1 Installation

1. The mounting surface must be able to bear at least five times the weight of your camera.
2. Do not let the cables get caught in improper places or the electric line cover be damaged. This may cause a breakdown 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 wires through and make all necessary connections. See 2.2 Cabling for more information.
5. Attach the main body to the mount bracket by tightening the lock screw.



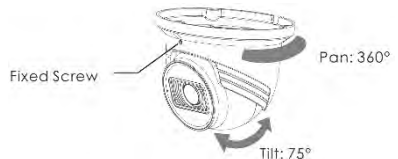
6. To use the camera's waterproof wiring:

- 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).



7. Using the hexagonal wrench included with the camera, loosen the lock screw at the base of the camera to adjust the camera module's position.

- a. Tilt: 75°
- b. Rotation: 360°



8. When the camera is in its desired view, secure the lock screw back

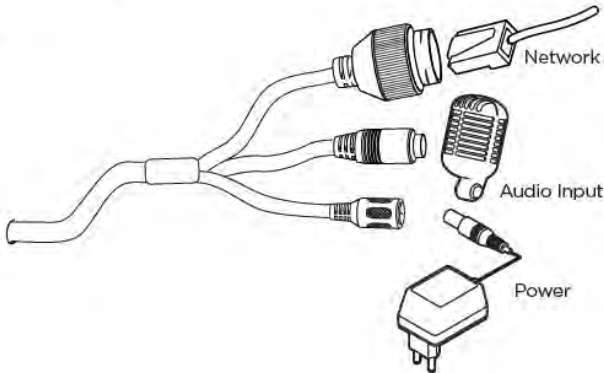
into place to complete the installation.

2.2 Cabling

1. When using a PoE Switch or PoE Injector, connect the camera using an Ethernet cable for both data and power.
2. When not using PoE Switch or PoE Injector, connect the camera to the switch using an Ethernet cable for data transmission and use a power adapter to power the camera.

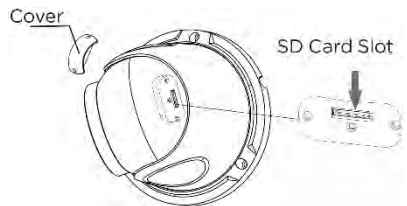
Power requirements	Power consumption
DC12V, PoE (IEEE 802.3af class 3). Adapter not Included.	<9W

3. Use the diagram below to connect power, network and audio to the camera.



2.3 Managing the SD Card

1. To install the camera's SD Card, locate the SD card slot at the base of the camera module by loosening the lock screw at the base of the camera.
2. Insert class 10 SD/SDHC/SDXC card into the SD card slot by pressing the SD card until clicks.
3. To remove the SD card, press the card inward until it clicks to release from the card slot then pull out from the slot.



3 Network Setup

3.1 IP Finder

Use the DW® IP Finder™ software to scan the network and detect all MEGApix® cameras, set the camera's network settings or access the camera's web client.



Network Setup

1. To install the DW IP Finder, go to <http://www.digital-watchdog.com>.
2. Enter "DW IP Finder" on the search box at the top of the page.
3. Go to the "Software" tab on the DW IP Finder page to download the installation file.
4. Follow the installation Wizard to install DW IP Finder. Launch DW IP Finder, enter the camera login, then click the "Scan Devices" button. The software will scan the selected network for ONVIF compliant devices and will list the results in the table. Double-click on a detected camera in the search results to configure the *Camera Settings* using DW IP Finder.



- i** Select DHCP to allow the camera to receive its IP address automatically from the DHCP server.
- i** Select "Static" to manually enter the camera's IP address, (Sub) Netmask, Gateway and DNS information.
* The camera's IP must be set to Static if connecting to Spectrum® IPVMS.
- i** Contact your network administrator for more information.

i Default TCP/IP information: DHCP

5. When connecting to the camera for the first time, a password must be set. To set up a password for your new camera:
 - a. Check the box next to your new camera from the IP Finder's search results. You can select multiple cameras.
 - b. Click "Bulk Password Assign" on the left.
 - c. In the pop-up window, enter admin/admin in the current username and password fields. Enter a new username and password to the right.
 - d. Press "change" to apply all changes.



6. Select a camera from the list by double-clicking on the camera's image or clicking on the 'Click' button under the IP Conf. column. The pop-up window will show the camera's current network settings, allowing admin users to adjust the settings as needed.
7. To access the camera's web page, go to the IP Config page and click on the 'View Camera Website'. To save the changes made to the camera's setting, input the username and password of the camera and click Apply.



i 'Port forwarding' has to be set in your network's router for external access to the camera.

4 Live View

Once the camera's network settings have been setup properly, you can access the camera's web viewer.

To open the camera using the DW IP Finder:

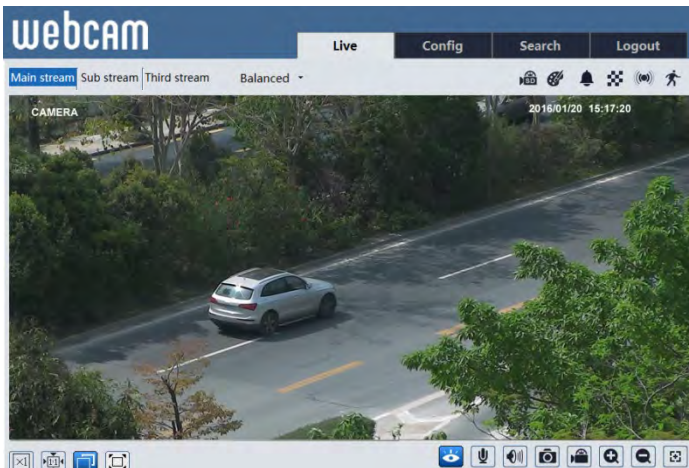
1. Find the camera using the DW IP Finder.
2. Double-click on the camera's view in the results table.
3. Press the 'View Camera Website'. The camera's web viewer will open up in your default web browser.
4. Enter the camera's username and password.

To open the camera using the web browser:




















1. Open a web browser (Internet Explorer® 8.0 or above).
2. Enter the camera's IP address and port in the address bar. Example: `http://<ipaddress>:<port>`. Port forwarding may be necessary to access the camera from a different network. Contact your network administrator for more information.
3. Enter the camera's username and password (default admin/admin).

If you are accessing the camera for the first time, install the ActiveX player for web files to view video from the camera.

After logging in, the following window will be shown.








NOTE: This camera's web client is available via Internet Explorer® only.

Icon	Description	Icon	Description
	Original size		Zoom in and out
	Fit correct scale		AZ control (only available for the model with motorized zoom lens)
	Auto (fill the window)		SD card recording indicator
	Fullscreen		Sensor alarm (on supported models)
	Start/stop live view		Motion alarm (on supported models)
	Start/stop two-way audio (on supported models)		Color abnormal
	Enable/disable audio (on supported models)		Abnormal clarity
	Snapshot		Scene change
	Start/stop local recording (on supported models)		Line crossing
	Perimeter Intrusion		

Those smart alarm indicators will flash only when the camera supports those functions and the events are enabled.

In full-screen mode, double-click on the mouse to exit or press the ESC key on the keyboard.

Click the AZ control button to show the AZ control panel. This is available on supported models.

Icon	Description	Icon	Description
	Zoom -		Zoom +
	Focus -		Focus +
	One key focus (use after manual lens adjustment and the image is out of focus)		

5 Network Camera Configuration

In the camera's web client, click on the "Config" tab on the top right to go to the setup menu.

Note: Where applicable, click the "Save" button to save changes to the settings.

5.1 System Configuration

5.1.1 Basic Information

Basic Information lists the system information of the device including model, name, firmware version, Mac address and more.

Config Home ▶ System ▶ Basic Information	
Device Name	DWC-MV95Wi28TW
Product Model	DWC-MV95Wi28TW
Brand	DigitalWatchdog
Software Version	5.0.1.0(20945)
Software Build Date	2021-07-01
Kernel Version	02030246
Hardware Version	1.5-1515121
Onvif Version	20.06
Video Structured Version	1.0.0
OCX Version	2.1.7.9
MAC	00:18:ae:bf:fc:c0

5.1.2 Date and Time

Under Config > System >Date and Time, users can adjust the camera's date, time, DST and time zone.

The time zone and DST must be set up when accessing the camera for the first time.

Config Home ▶ System ▶ Date and Time	
Zone: Date and Time	
Zone	GMT-08 (Las Vegas, San Francisco, Vancouver)
<input checked="" type="radio"/> DST	
<input checked="" type="radio"/> Auto DST	
<input type="radio"/> Manual DST	
Start Time	January First Sunday 00 Hour
End Time	February First Monday 00 Hour
Time Offset	120 Minutes
<input type="button" value="Save"/>	

Zone: Date and Time	
Time Mode:	
<input type="radio"/> Synchronize with NTP server	
NTP server:	time.windows.com Update period: 1440 Minutes
<input type="radio"/> Synchronize with computer time	
Date	2018-01-08 Time 14:58:21
<input checked="" type="radio"/> Set manually	
Date	2018-01-09 Time 15:03:28

5.1.3 Local Config

To set up the storage path for images and videos on the local PC, go to Config > System > Local Config. Users can also enable or disable the bitrate display in the recorded files.

Save snapshots to	<input type="text" value="C:\Program Files\NetIPCamera"/>	<input type="button" value="Browse"/>
Save recording files to	<input type="text" value="C:\Program Files\NetIPCamera"/>	<input type="button" value="Browse"/>
Audio Recording	<input type="radio"/> Open	<input checked="" type="radio"/> Close
Bitrate Overlay	<input type="radio"/> Open	<input checked="" type="radio"/> Close
Local Smart Snapshot Storage	<input type="radio"/> Open	<input checked="" type="radio"/> Close

If “Local smart snapshot storage” is enabled, captured pictures triggered by smart events (line crossing, perimeter intrusion, etc.) will be saved to the local PC.

5.1.4 Storage

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

Management	Record	Snapshot
Total picture capacity	<input type="text" value="14829 MB"/>	
Picture remaining space	<input type="text" value="5068 MB"/>	
Total recording capacity	<input type="text" value="14784 MB"/>	
Record remaining space	<input type="text" value="0 MB"/>	
State	<input type="text" value="Normal"/>	
Snapshot Quota	<input type="text" value="50"/> %	
Video Quota	<input type="text" value="50"/> %	

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 the SD card. Then the SD card can be ejected safely.

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

Video Quota: Set the limit 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.

Management **Record** Snapshot

Record Parameters

Record Stream:

Pre Record Time: (H264,H265,MJPEG)

Cycle Write:

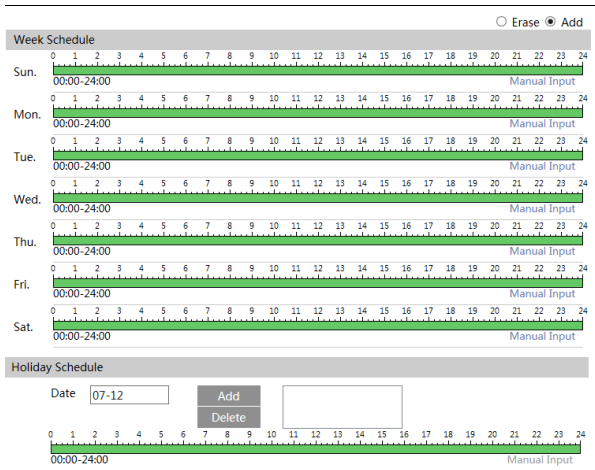
Timing

Enable Schedule Record

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.



Weekly schedule

Set the alarm time from Monday to Sunday for a single week. Each day is divided into one-hour increments. Green means scheduled. Blank means unscheduled.

“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	704x576	
Image Quality	Low	
Event Trigger		
Snapshot Interval	1	Second
Snapshot Quantity	5	
Timing		
<input checked="" type="checkbox"/>	Enable Timing Snapshot	
Snapshot Interval	5	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 the schedule are the same as the scheduled recording (See [Schedule Recording](#)).

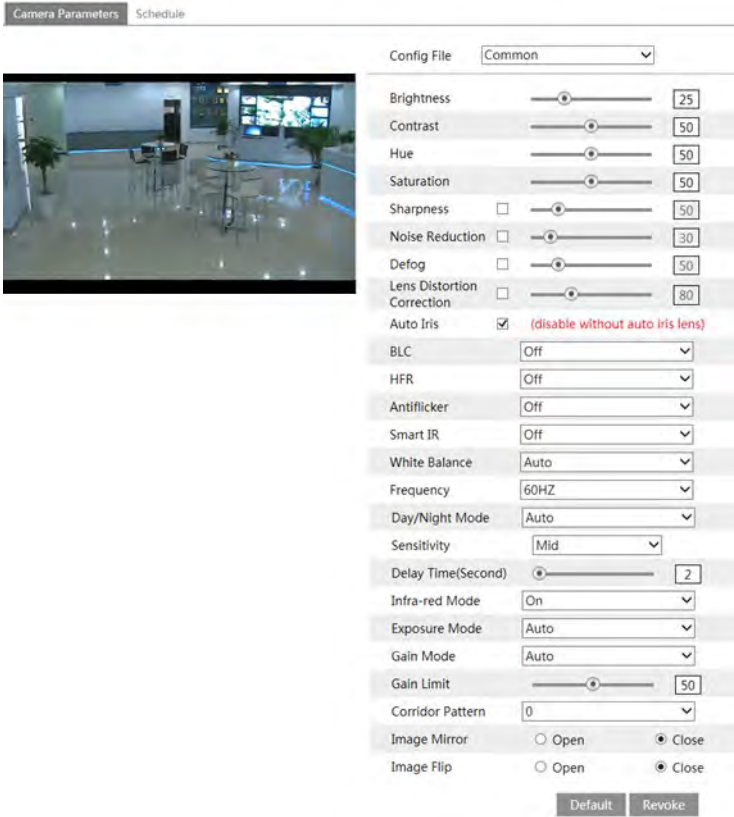
5.2 Image Configuration

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

5.2.1 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:** Clear the camera's image in a foggy, dusty, smoggy, or rainy environment.

Lens Distortion Correction: When the image appears distorted to some extent, please enable this function and adjust the level according to the actual scene to correct the distortion. (On supported models.)

Auto Iris: If your camera is auto Iris, please enable it.

Backlight Compensation (BLC):

- Off: disables the backlight compensation function. It is the default mode.
- HWDR: WDR can adjust the camera to 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.

The 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: High Frame Rate. If "ON" is selected, the system will restart and then the maximum value of the frame rate of the mainstream can be set to 60 fps /50fps.

Antiflicker:

- 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.

Smart IR: Choose "ON" or "OFF". This function can effectively avoid image overexposure and underexposure by controlling the brightness of the IR lights according to the actual conditions to make the image more realistic. Please enable it as needed.

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

Frequency: 50Hz and 60Hz can be optional.

Day/Night Mode: Choose "Auto", "Day", "Night", or "Timing".

Infra-red Mode: Choose "Auto", "ON" or "OFF".

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

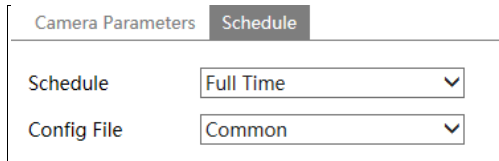
Gain Mode: Choose "Auto" or "Manual". If "Auto" is selected, the gain value will be automatically adjusted according to the actual situation. If "Manual" is selected, the gain value shall be set manually. The higher the value is, the brighter the image is.

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.

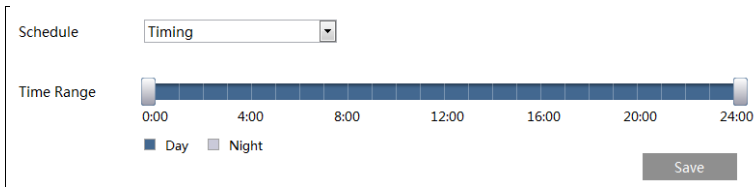
Image Mirror: Turn the current video image horizontally.

Image Flip: Turn the current video image vertically.

Schedule Settings of Image Parameters:
Click the “Schedule” tab as shown below.



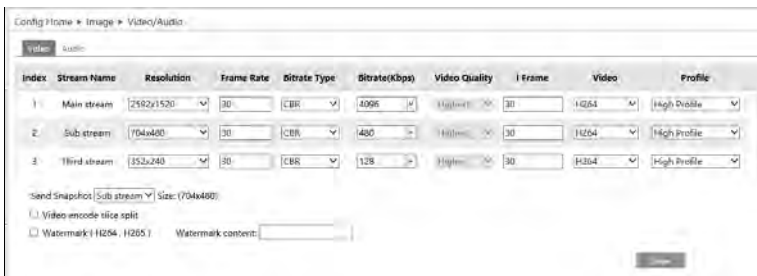
Set a full schedule for common, day, night mode and specified schedule for day and night. Choose “Schedule” in the drop-down box of schedule as shown below.



Drag “” icons to set the time of day and night. Blue means daytime and blank means nighttime. 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.

5.2.2 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.



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

The screenshot shows a settings window with two tabs: 'Video' and 'Audio'. The 'Audio' tab is active. Below the tabs, there is a checked checkbox labeled 'Enable'. Underneath, there are two dropdown menus: 'Audio Encoding' is set to 'G711A' and 'Audio Type' is set to 'LIN'. At the bottom right of the panel is a 'Save' button.

Three video streams can be adjustable.

Resolution: Adjust the stream's resolution from the available options in the drop-down menu.

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 bandwidth 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: MJPEG, H264, H265 can be optional. MJPEG is not available for the mainstream. Compared to H.264, H.265 reduces the transmission bitrate under the same resolution, frame rate and image quality.

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

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

Videos encode slice split: Enable this function to get an improved image when using a low-performance PC.

Watermark: When playing back the locally 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: LIN. MIC can be optional for the model with built-in MIC.

5.2.3 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.

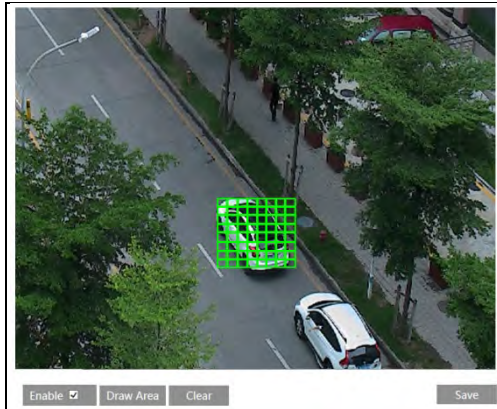


Picture Overlay Settings:

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

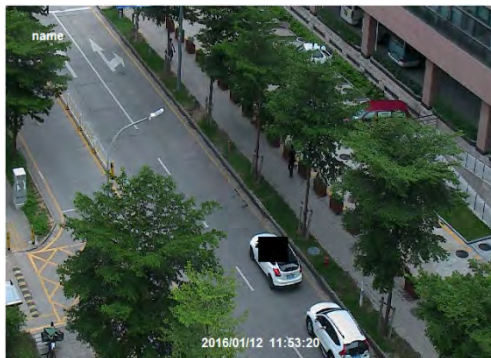
5.2.4 Video Mask

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



To set up a 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 has been drawn as blocked out in the image.

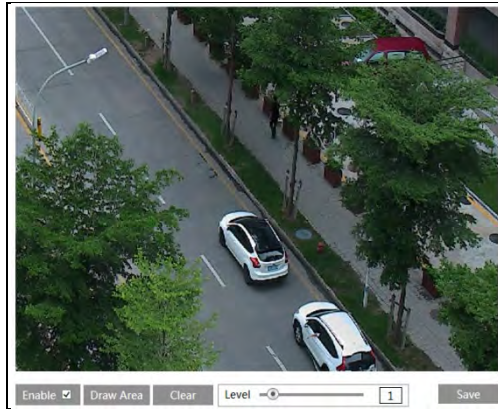


To clear the video mask:

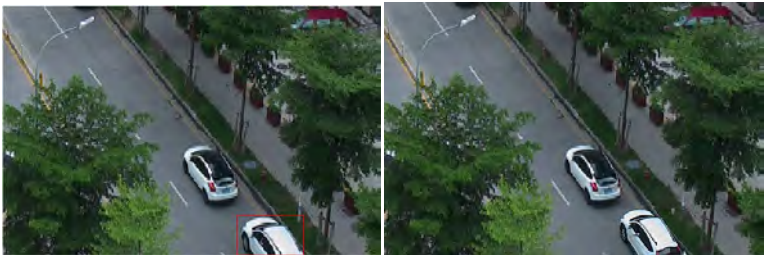
Click the “Clear” button to delete the current video mask area.

5.2.5 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.



5.2.6 Zoom/Focus

This function is only available for models with a 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. Go to Config > Image > Zoom/Focus interface to set.



Day and night switching Focus

One Key Focus

Reset

Zoom - Zoom +

Focus - Focus +

5.3 Alarm Configuration

5.3.1 Motion Detection

Go to Alarm > Motion Detection to set a motion detection alarm.

The screenshot shows a web interface for configuring motion detection. At the top, there is a breadcrumb trail: "Config Home > Alarm > Motion Detection". Below this, there are three tabs: "Alarm Config" (which is selected), "Area and Sensitivity", and "Schedule". Under the "Alarm Config" tab, there is a checked checkbox for "Enable". Below that is a field for "Alarm Holding Time" set to "5 Seconds" with a dropdown arrow. A section titled "Trigger Alarm Out" contains a large, empty rectangular area with a checkbox for "Alarm Out". Below this are four more checkboxes: "Trigger SD Snap", "Trigger SD Recording", "Trigger Email", and "Trigger FTP". At the bottom center of the form is a "Save" button.

1. Check the “Enable” 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.

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

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 to those addresses.

Trigger FTP: If “Trigger FTP” and “Attach Picture” are checked, the captured pictures will be sent to an FTP server address. Please refer to the 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. A higher sensitivity value means that motion will be triggered more easily.

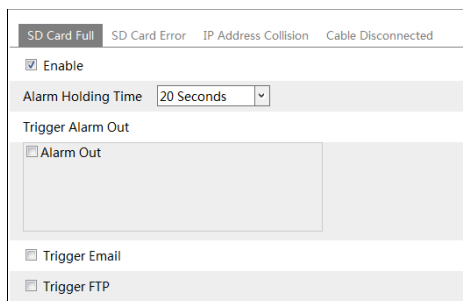
Select “Add” and click “Draw”. Drag the mouse to draw the motion detection area; Select “Erase” and drag the mouse to clear the motion detection area. After that, click the “Save” to save the settings.

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](#)).

5.3.2 Other Alarms

● SD Card Full

1. Go to Config > Alarm > Anomaly > SD Card Full.



2. Click “Enable” and set the alarm holding time.

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

● SD Card Error

When there are errors in writing on the SD card, an alarm 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 Holding Time 20 Seconds ▾

Trigger Alarm Out

Alarm Out

Trigger Email

Trigger FTP

2. Click “Enable” 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 the [motion detection](#) chapter for details.

● IP Address Conflict

This function is only available for models with alarm output.

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 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 IP address of the camera conflicts with the IP address of other devices, the system will trigger the alarm out.

● Cable Disconnection

This function is only available for the models with the Alarm Out interface.

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

SD Card Full SD Card Error IP Address Collision Cable Disconnected

Enable

Alarm Holding Time 20 Seconds ▾

Trigger Alarm Out

Alarm Out

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

5.3.3 Alarm In

This function is available for cameras with alarm input support. To set sensor alarm (alarm in):

Go to Config > Alarm > Alarm In interface as shown below.

Alarm Config Schedule

Enable

Alarm Type NO

Alarm Holding Time 20 Seconds

Sensor Name

Trigger Alarm Out

Alarm Out

Trigger SD Snap

Trigger SD Recording

Trigger Email

Trigger FTP

Save

1. Click “Enable” 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 the [motion detection](#) chapter for details.
3. Click the “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](#)).

5.3.4 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	20 Seconds
Alarm Type	NC

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

Alarm Linkage: Select an alarm out name, alarm holding time at the “Alarm Holding Time” pull-down list box and alarm type.

Manual Operation: Select the alarm type and click “Open” to trigger the alarm out immediately; click “Close” to stop the alarm.

Alarm Out Mode	Manual Operation
Alarm Type	NC
Manual Operation	<input type="button" value="Open"/> <input type="button" value="Close"/>

Day/Night Switch Linkage: Select the alarm type and then choose to open or close the alarm out when the camera switches to day mode or night mode.

Alarm Out Mode	Day/night switch linkage
Alarm Type	NC
Day	Close
Night	Close

Timing: Select the alarm type. Then 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 schedule. After this schedule is saved, the alarm out will be triggered in the specified time.

Alarm Out Mode	Timing
Alarm Type	NC

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

Manual Input

5.4 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 a 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.

5.4.1 Video Tampering Detection

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

To set Video Tampering detection:

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

The screenshot shows the 'Video Tampering Detection' configuration page. At the top, there is a breadcrumb trail: 'Config Home > Event > Video Tampering Detection'. Below this, there are two tabs: 'Detection Config' (selected) and 'Sensitivity'. The 'Detection Config' section contains several checkboxes: 'Scene change detection', 'Video blur detection', and 'Abnormal Color Detection'. Below these is a field for 'Alarm Holding Time' set to '20 Seconds'. Underneath is a section titled 'Trigger Alarm Out' with a checkbox for 'Alarm Out'. At the bottom of the configuration area, there are four more checkboxes: 'Trigger SD Snap', 'Trigger SD Recording', 'Trigger Email', and 'Trigger FTP'. A 'Save' button is located at the bottom right of the interface.

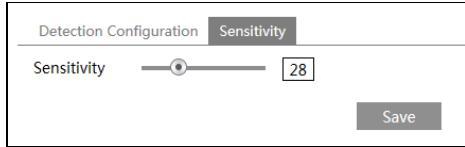
1. Enable the applicable detection that's desired.

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 the motion detection chapter for details.
3. Click the “Save” button to save the settings.
4. Set the sensitivity of the Video Tampering detection. Click the “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 the “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 the camera and surrounding area**

1. Auto-focus should not be 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.

5.4.2 Line Crossing

Line Crossing: Alarms will be triggered if the target crosses the pre-defined alarm lines.

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



1. Detection Target:

Human: Select it and then alarms will be triggered if someone crosses the pre-defined alarm lines.

Motor Vehicle: Select it and then alarms will be triggered if a vehicle with four or more wheels (e.g., a car, bus, or truck) crosses the pre-defined alarm lines.

2. Set the alarm holding time.

3. Set alarm trigger options. The setup steps are the same as motion detection. Please refer to the [motion detection](#) chapter for details.

4. Click the “Save” button to save the settings.

5. Set area and sensitivity of the line crossing alarm. Click the “Area and Sensitivity” tab to go to the interface as shown below.



Set the alarm line number and 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 someone or a vehicle cross over the alarm line.

A<->B: Alarms will be triggered when someone or a vehicle cross over the alarm line from B to A or from A to B.

A->B: Alarms will be triggered when someone or a vehicle cross over the alarm line from A to B.

A<-B: Alarms will be triggered when someone or a vehicle cross over the alarm

line from B to A.

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

6. 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 the 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.

5.4.3 Perimeter Intrusion

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

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

The screenshot shows the configuration interface for Perimeter Intrusion. At the top, there are navigation tabs: "Detection Config" (selected), "Area", and "Schedule". Below the tabs, there is a section for "Enable" with a checked checkbox. The "Detection Target" section includes two checked checkboxes: "Human" and "Motor Vehicle", each with a "Sensitivity" slider and a numeric input field set to "50". The "Alarm Holding Time" is set to "20 Seconds" with a dropdown arrow. The "Trigger Alarm Out" section has an unchecked checkbox. Below that, there are three unchecked checkboxes: "Trigger SD Snap", "Trigger SD Recording", and "Trigger Email". At the bottom, there is an unchecked checkbox for "Trigger FTP" and a "Save" button.

1. **Detection Target:**

Human: Select it and then alarms will be triggered if someone intrudes into the pre-defined area.

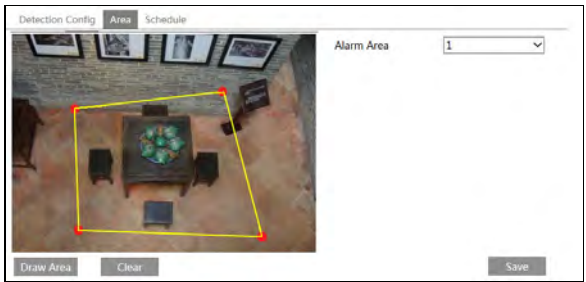
Motor Vehicle: Select it and then alarms will be triggered if a vehicle with four or more wheels (e.g., a car, bus, or truck) intrudes into the pre-defined area.

2. Set the alarm holding time.

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

4. Click the “Save” button to save the settings.

5. Set the alarm area for perimeter 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 it 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.

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

※ **Configuration requirements of the camera and surrounding area**

1. Auto-focusing function should not be enabled for perimeter 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.

5.5 Network Configuration

5.5.1 TCP/IP

Go to Config > Network > TCP/IP interface as shown below. There are two ways to setup the network connection.

IPv4	IPv6	PPPoE Config	IP Change Notification Config
<input type="radio"/> Obtain an IP address automatically			
<input checked="" type="radio"/> 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.

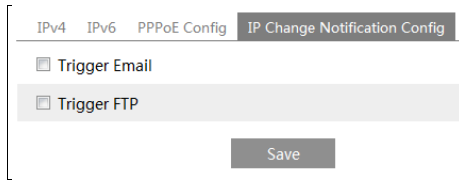
Test: Test the effectiveness of the IP address by clicking this button.

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

IPv4	IPv6	PPPoE Config	IP Change Notification Config
<input checked="" type="checkbox"/> Enable			
User Name	xxxxxxx		
Password	●●●●●●		
Save			

Either method of network connection can be used. If PPPoE is used to connect the 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.



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 an FTP server that has been set up.

5.5.2 Port

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

HTTP Port	<input type="text" value="80"/>
HTTPS Port	<input type="text" value="443"/>
Data Port	<input type="text" value="9008"/>
RTSP Port	<input type="text" value="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. (Some models may not support)

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.

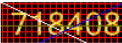
5.5.3 DDNS

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	B02.1X	RTSP	UPnP	Email	FTP	HTTPS	CoS
<input type="checkbox"/> Enable										
Server Type		www.dyndns.com								
User Name		<input type="text"/>								
Password		<input type="password"/>								
Domain		<input type="text"/>								
<input type="button" value="Save"/>										

2. Apply for a domain name. Take www.dvrdydns.com for example. Enter www.dvrdydns.com in the IE address bar to visit its website. Then click the "Registration" button.

NEW USER REGISTRATION	
USER NAME	<input type="text" value="XXXX"/>
PASSWORD	<input type="password" value="•••••"/>
PASSWORD CONFIRM	<input type="password" value="•••••"/>
FIRST NAME	<input type="text" value="XXX"/>
LAST NAME	<input type="text" value="XXX"/>
SECURITY QUESTION.	My first phone number. ▾
ANSWER	<input type="text" value="XXXXXXXX"/>
CONFIRM YOU'RE HUMAN	 New Captcha <input type="text"/> Enter the text you see above
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

Create domain name.

You must create a domain name to continue.

Domain name must start with (a-z, 0-9). Cannot end or start, but may contain a hyphen and is not case-sensitive.

<input type="text" value=""/>	dvr dy dns.com ▾	<input type="button" value="Request Domain"/>
-------------------------------	--	---

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

Search by Domain		<input type="button" value="Search"/>
<i>Click a name to edit your domain settings.</i>		
NAME	STATUS	DOMAIN
654321ABC	✔	654321abc.dvr dy dns.com
Last Update: <i>Not yet updated!</i> IP Address: 210.21.229.138		
Create additional domain names		

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

5.5.4 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.

5.5.5 802.1x

If it is enabled, the camera’s data can be protected. When the camera is connected to the network protected by the IEEE802.1x, user authentication is needed.

<input checked="" type="checkbox"/> 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 find 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.

Username and password: The username and password must be the same as the username and password applied for and registered in the authentication server.

5.5.6 RTSP

Go to Config > Network > RTSP.

<input checked="" type="checkbox"/> 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 <input type="checkbox"/> Automatic start
Sub stream	239.0.0.1 51554 <input type="checkbox"/> Automatic start
Third stream	239.0.0.2 52554 <input type="checkbox"/> Automatic start
Audio	239.0.0.3 53554 <input type="checkbox"/> Automatic start
<input type="checkbox"/> Allow anonymous login (No username or password required)	
<input type="button" value="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

Mainstream: 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 “autostart” is enabled, the multicast received data should be added to 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, e.g., 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.

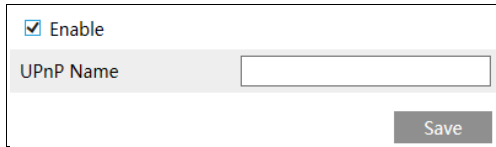
3. Avoid the use of the same multicast address in the same local network.

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 mainstream is MJPEG, the video may be disordered at some resolutions.

5.5.7 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.



Enable

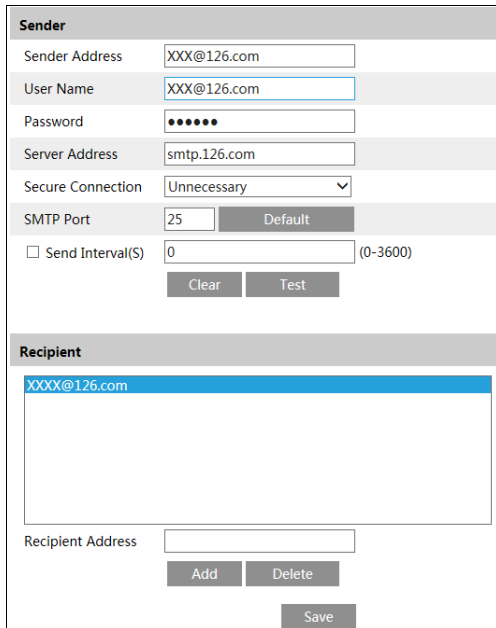
UPnP Name

Save

5.5.8 Email

If you need to trigger an email when an alarm is triggered or the IP address is changed, please set the Email here first.

Go to Config > Network > Email.



Sender

Sender Address

User Name

Password

Server Address

Secure Connection

SMTP Port Default

Send Interval(S) (0-3600)

Clear Test

Recipient

XXXX@126.com

Recipient Address

Add Delete Save

Sender Address: sender's e-mail address.

Username and password: sender's username and password.

Server Address: The SMTP IP address or hostname.

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 the 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.

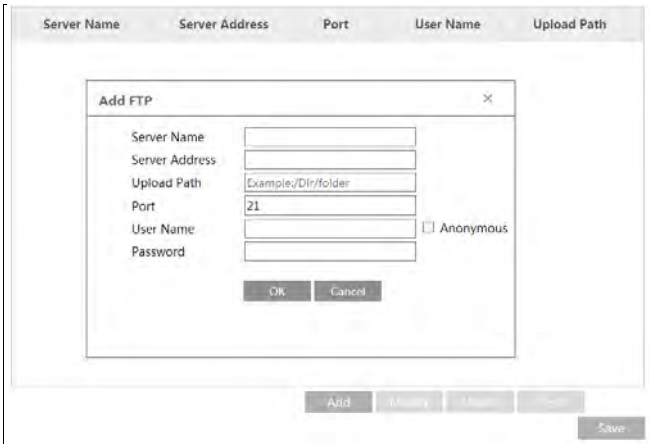
Click the “Test” button to test the connection of the account.

Recipient Address: receiver’s e-mail address.

5.5.9 FTP

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

Go to Config > Network > FTP.



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.

Username and Password: The username and password that are used to log in to the FTP server.

5.5.10 HTTPS

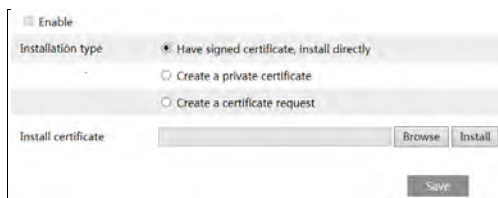
HTTPS supplies authentication of the website and protects user privacy.

Go to Config > Network > HTTPS as shown below.



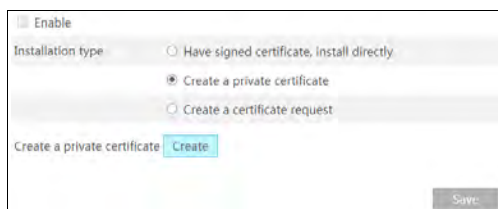
There is a certificate installed by default as shown above. Enable this function and save it. Then the camera can be accessed by entering https://IP: https port via the web browser (e.g., https://192.168.226.201:443).

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.



* 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.



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.

Enable

Installation type

Have signed certificate, install directly

Create a private certificate

Create a certificate request

Create a certificate request

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

5.5.11 QoS

QoS (Quality of Service) function is used to supply 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

Alarm DSCP

Manager DSCP

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.

5.6 Security Configuration

5.6.1 User Configuration

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

<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/>			
Index	User Name	User Type	Binding MAC
1	admin	Administrator	

Add user:

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

2. Enter the username in the “Username” textbox.
3. Enter the password in the “Password” and “Confirm Password” textbox. Please set the password according to the requirement of the password security level (Go to Config > Security > Security Management > Password Security interface to set the security level).
It is recommended to set a high-level password that shall be composed of numbers, special characters, upper- or lower-case letters for your account security.
4. Choose the user type. The administrator has all permissions. Normal users 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 the “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 change the 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.

Edit User [X]

Modify Password

User Name: admin

Old Password: []

New Password: []

Level: []

9~15 characters, including at least two of the following categories:
numbers, special characters, upper case letters, lower case letters.

Confirm Password: []

Bind MAC: 00:00:00:00:00:00

[OK] [Cancel]

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 boxes.
5. Enter the 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 removed and added again with the new access level.

Delete user:

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

Note: The default administrator account cannot be removed.

5.6.2 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	[Kick Out]

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

5.6.3 Block and Allow Lists

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



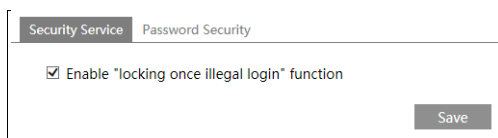
The setup steps are as follows:

Check the “Enable address filtering” check box.

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

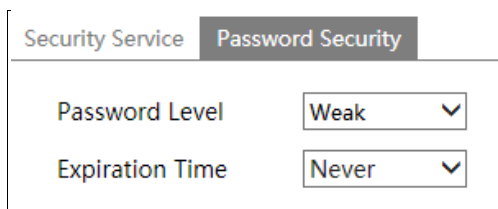
5.6.4 Security Management

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



To prevent malicious password unlocking, the “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.

- **Password Security**



Please set the password level and end time as needed.

Password Level: Weak, Medium, or Strong.

Weak level: Numbers, special characters, upper- or lower-case letters can be used. You can choose one of them or any combination of them when setting the password.

Medium Level: 9-15 characters, including at least two of the following categories:

numbers, special characters, upper case letters, lower case letters.
Strong Level: 9-15 characters. Numbers, special characters, upper case letters and lower-case letters must be included.
For your account security, it is recommended to set a strong password and change your password regularly.

5.7 Maintenance Configuration

5.7.1 Backup and Restore

Go to Config > Maintenance > Backup & Restore.

Import Setting

Path

Export Settings

Default Settings

Keep

Network Config

Security Configuration

Image Configuration

- **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 except those you want to keep.

5.7.2 Reboot

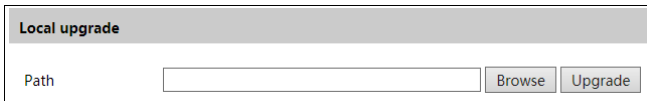
Go to Config > Maintenance > Reboot.
Click the “Reboot” button to reboot the device.

Timed Reboot Setting:

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

5.7.3 Upgrade

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



The screenshot shows a web interface titled "Local upgrade". It features a text input field labeled "Path" with a "Browse" button to its right. Further to the right is an "Upgrade" button.

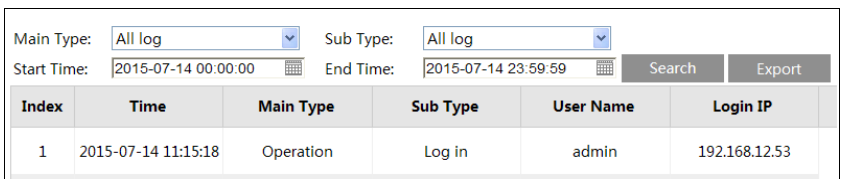
1. Click the “Browse” button to select the save path of the upgrade file
2. Click the “Upgrade” button to start upgrading the firmware.
3. The device will restart automatically

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

5.7.4 Operation Log

To query and export log:

1. Go to Config > Maintenance > Operation Log.



The screenshot shows the "Operation Log" interface. At the top, there are two dropdown menus for "Main Type" and "Sub Type", both set to "All log". Below these are "Start Time" and "End Time" fields with calendar icons, set to "2015-07-14 00:00:00" and "2015-07-14 23:59:59" respectively. To the right of these fields are "Search" and "Export" buttons. Below the filters is a table with the following data:

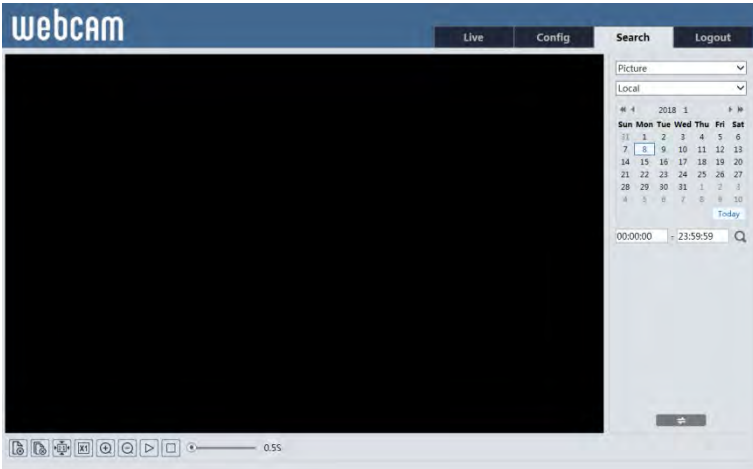
Index	Time	Main Type	Sub Type	User Name	Login IP
1	2015-07-14 11:15:18	Operation	Log in	admin	192.168.12.53

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


6 Search

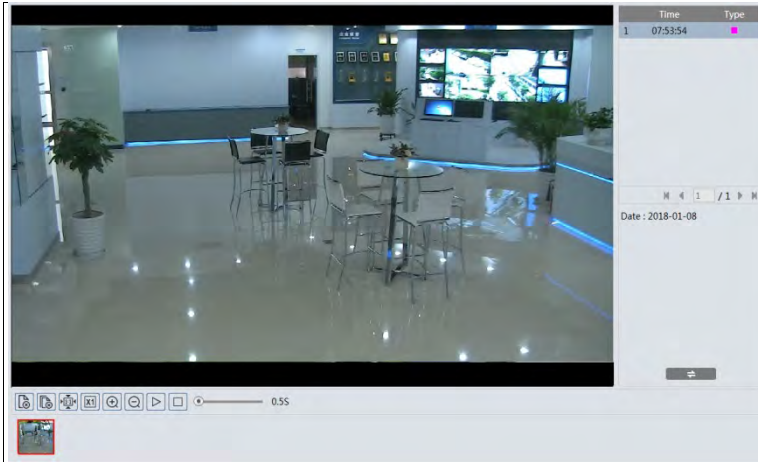
6.1 Image Search


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



● Local Image Search

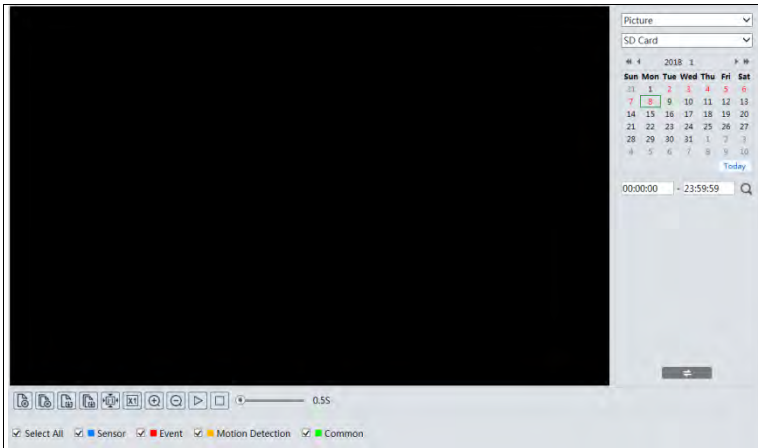
1. Choose “Picture”— “Local”.
2. Set time: Select date and choose the start and end time.
3. Click  to search the images.
4. Double click a file name in the list to view the captured photos as shown above.





Click  to return to the earlier 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 earlier interface.

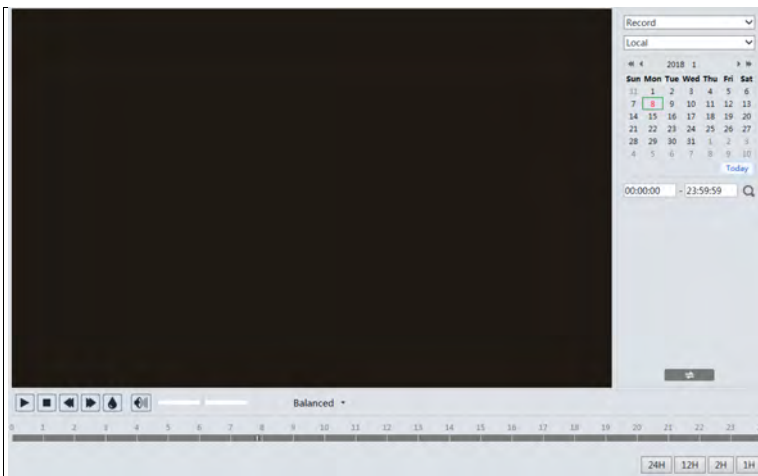
The descriptions of the buttons are shown as follows.


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.		

6.2 Video Search








6.2.1 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.

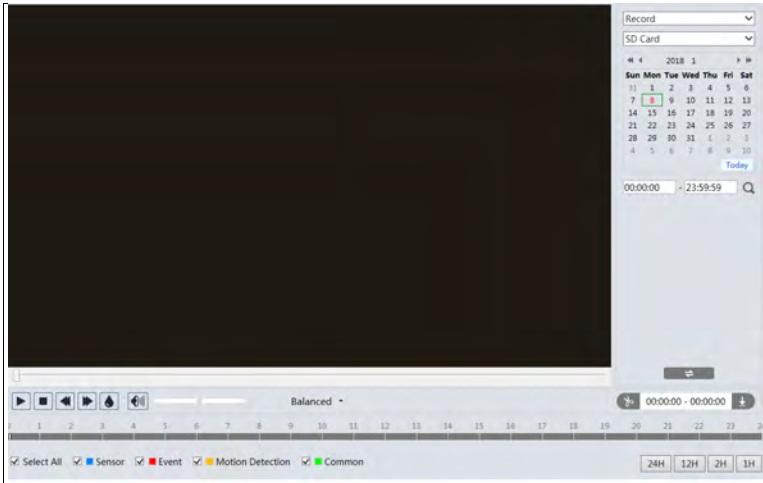


Icon	Description	Icon	Description
	Play button. After pausing the video, click this button to continue playing.		Pause button
	Stop button		Speed down
	Speed up		Watermark display
	Enable/disable audio; drag the slider to adjust the volume after enabling audio.		

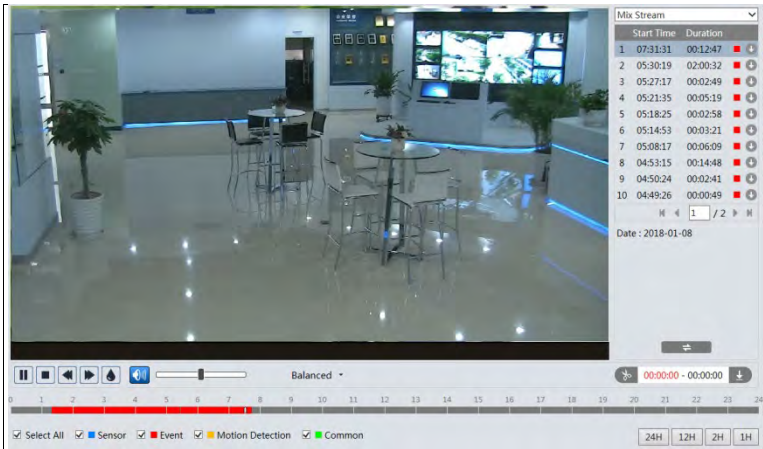
6.2.2 SD Card Video Search

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

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 timetable 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 steps above.
2. Select the start time by clicking on the timetable.
3. Click  to set the start time and then this button turns blue ().
4. Select the end time by clicking on the timetable. Then click  to set the end time.

5. Click  to download the video file on 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.

7 Appendix

7.1 Troubleshooting

How to find the password?

A: Reset the device to the default factory settings.

Default IP: 192.168.226.201; Username: 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 the default setting by IP-Tool.

IP tool cannot search devices.

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

Internet Explorer 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.

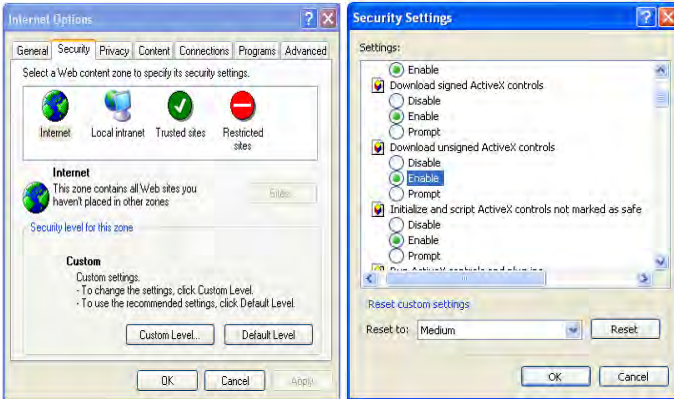


② Select Security-----Custom Level....

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

④ Click OK to finish the setup.

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

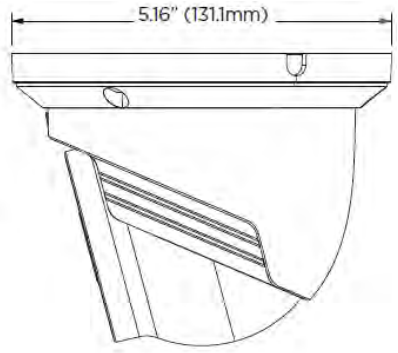
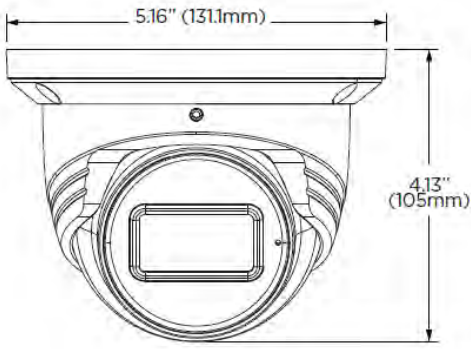


No sound can be heard.

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.

7.2 Dimensions



7.3 Specifications

	DWC-MT95WW2 8TW	DWC-MT95W2 8TW	DWC-MT95W3 6TW	DWC-MT95WIATW
IMAGE				
Image sensor	5MP 1/2.7" CMOS			
Total pixels	2592 × 1944			
Minimum scene illumination	0.0 lux (B/W)	0.02 lux (color)		0.01 lux (color)
		0.0 lux (B/W)		
S/N ratio	≥50dB			
LENS				
Focal length	2.8mm, F1.0	2.8mm, F1.6	3.6mm, F1.6	2.8 - 12mm, F1.4
Lens type	Fixed lens			Vari-focal lens with motorized zoom and auto-focus
Field of view (FoV)	94.8°	98.5°	81.4°	95.1° - 30°
IR distance	2 white light LEDs, 98ft range	100ft range		164ft range
I/O				
Audio in / out	1 audio input and 1 microphone built-in			
Audio compression	G.711A / U			
OPERATIONAL				
Shutter mode	Auto, manual			
Shutter speed	1/30s - 1/100000s			
Auto gain control	Auto			
Day / night	Auto, day (color), night (B/W), schedule			
Smart DNR™ 3D digital noise reduction	3D DNR			
Wide dynamic range (WDR)	True WDR low, middle, high			
Wide dynamic range (WDR) dB	120dB			
Privacy zone	4 programmable privacy masks			
Camera analytics	Line crossing, perimeter intrusion, video tampering detection (scene change, video blur, abnormal color detection), object classification (differentiate humans from objects)			
Backlight compensation (BLC)	Yes			
DeFog	Yes			
Mirror and flip	Yes			
Alarm notifications	Notifications via email or FTP server			
Memory slot	Micro SD / SDHC / SDXC card up to 256GB (card not included)			
NETWORK				
LAN	802.3 compliance 10/100 LAN			
Video compression type	H.265, H.264, MJPEG			
Resolution	Mainstream: 5MP, 4MP, 2K, 3MP, 2.1MP/1080p, 720p (60Hz: 1 - 30fps; 50Hz: 1-25fps) Sub-stream: 720P, D1, CIF, 480×240 (60Hz: 1 - 30fps; 50Hz: 1-25fps) Third stream: D1, CIF, 480×240 (60Hz: 1 - 30fps; 50Hz: 1-25fps)			
Frame rate	Up to 30fps at all resolutions			
Video bitrate	64 Kbps - 8 Mbps			
Bitrate control	Multi-streaming CBR/VBR at H.264/ H.265 (controllable frame rate and bandwidth)			
Streaming capability	Dual stream at different rates and resolutions			
IP	IPv4, IPv6			
Protocol	UDP, IPv4, IPv6, DHCP, NTP, RTSP, RTP, RTCP, ICMP, IGMP, PPPoE, DDNS, SMTP, FTP, SNMP, HTTP, 802.1x, UPnP, HTTPS, QoS			
Security	IP filtering, MAC filtering, authentication (ID/PW), SSL/TSL			
ONVIF conformance	Yes			

Web viewer	OS: Windows*	
	Browser: Internet Explorer	
Video management software	DW Spectrum* IPVMS	
ENVIRONMENTAL		
Operating temperature	-22°F - 140°F (-30°C - 60°C)	
Operating humidity	0-95% RH (non-condensing)	
IP rating	IP67-rated	
IK rating	IK10 impact-resistant	
Other certifications	FCC, CE, ROHS, POE, ONVIF	
ELECTRICAL		
Power requirement	DC 12V, PoE IEEE 802.3af Class 3. (Adapter not included)	
Power consumption	<7W	<9W
MECHANICAL		
Material	Metal turret housing	
Dimensions	4.66" x 3.58" (118.6 x 91 mm)	5.16" x 4.13" (131.1 x 105 mm)
Weight	1.01 lbs. (0.46 kg)	1.45 lbs. (0.66 kg)
Warranty	3 year warranty	3 year warranty

* Specifications are subject to change without notice.

Warranty - Australia only

Cameras, Recorders, Servers: 3 Years from date of purchase
Servers with a Dell service tag - check the Dell website