

MEGApix® 4MP Turret IP Camera

DWC-MTT4Wi28

DWC-TT4Wi36

DWC-TT4Wi6



User's Manual Ver. 04/17

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 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 use only 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 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 source 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 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 to 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

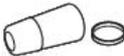
- 1 Product & Accessories5**
- 2 Parts and Description6**
- 3 Installation7**
- 4 Cabling8**
- 5 Remote Preview9**
- 6 Remote Live Surveillance.....10**
 - 6.1 System Configuration 10
 - 6.1.1 Basic Information 10
 - 6.1.2 Date and Time 11
 - 6.1.3 Local Config 11
 - 6.2 Image Configuration 11
 - 6.2.1 Display Configuration 11
 - 6.2.2 Video / Audio Configuration 13
 - 6.2.3 OSD Configuration 14
 - 6.2.4 Video Mask 15
 - 6.2.5 ROI Configuration 15
 - 6.3 Alarm Configuration 16
 - 6.3.1 Motion Detection 16
 - 6.3.2 Alarm Server 18
 - 6.4 Event Configuration 19
 - 6.4.1 Object Removal 19
 - 6.4.2 Exception 21
 - 6.4.3 Line Crossing 22
 - 6.4.4 Intrusion 24
 - 6.5 Network Configuration 26
 - 6.5.1 TCP/IP 26
 - 6.5.2 Port 28
 - 6.5.3 Server Configuration 28
 - 6.5.4 DDNS 28
 - 6.5.5 SNMP 30
 - 6.5.6 RTSP 31
 - 6.5.7 UPNP 31
 - 6.5.8 Email 32
 - 6.5.9 FTP 32
 - 6.6 Security Configuration 33
 - 6.6.1 User Configuration 33
 - 6.6.2 Online User 35
 - 6.6.3 Block and Allow Lists 35
 - 6.7 Maintenance Configuration 35
 - 6.7.1 Backup and Restore 35
 - 6.7.2 Reboot 36
 - 6.7.3 Upgrade 36
 - 6.7.4 Operation Log 37
- 7 Record Search.....38**
- 8 Appendix.....39**
- 9 Dimensions.....41**
- 10 Warranty Information.....42**
- 11 Limits and Exclusions43**

1 Product & Accessories

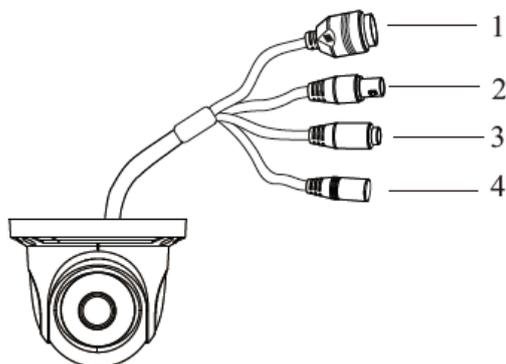


Default Login Information	
Username: admin	Password: admin

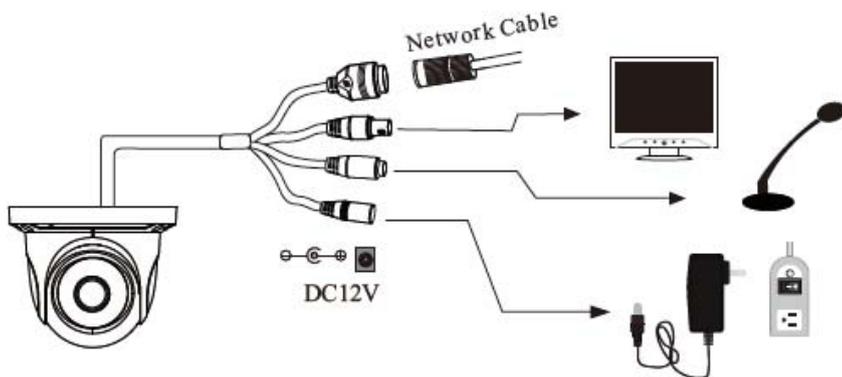
WHAT'S IN THE BOX

QSG Manual		1 Set	Tapping Screws PA 4x35 – 4pcs		1 Set
Mounting Template		1 Set	Plastic Plugs – 4pcs		1 Set
Waterproof Cap		1 Set	Torx Wrench		1 Set
Rubber Plug		1 Set			

2 Parts and Description

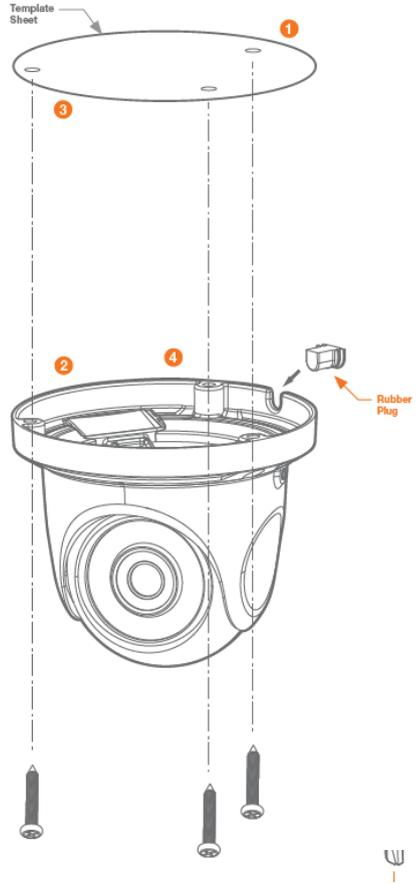
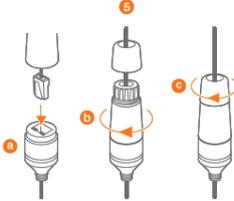


1	Network Cable	3	MIC IN Cable
2	CVBS Cable	4	Power Cable



3 Installation

1. Before installing the camera, make sure the mounting surface can bear three times the weight of your camera.
2. Do not let the cables get caught in improper places or the electric line cover to 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 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.



6. Tighten the lock screws after you finish adjusting the view angle of the camera.
7. Remove the protection film softly to complete the installation

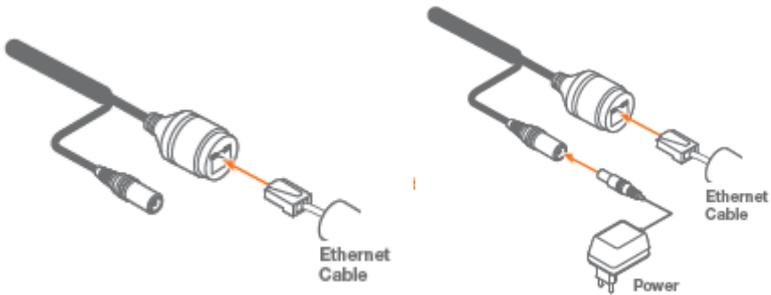


NOTE: To ensure moisture seal, make sure the O-ring is in place between 'a' and 'b'. In extreme environments use of an outdoor rated sealer is recommended.

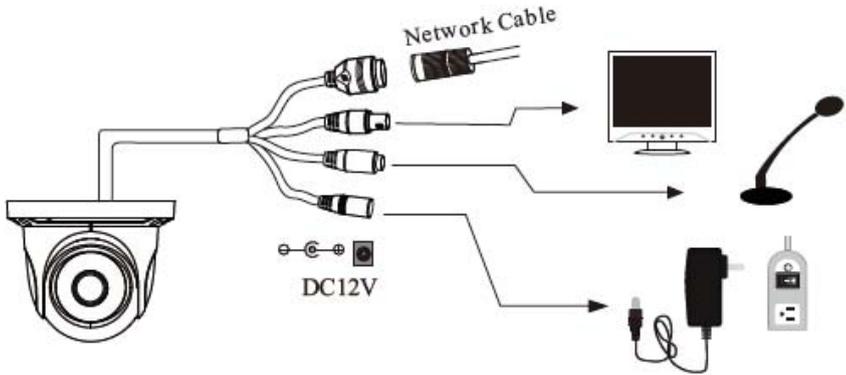
NOTE: When using the waterproof cap, crimp the RJ45 connector after passing the cable through the waterproof cap.

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 Remote Preview

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.

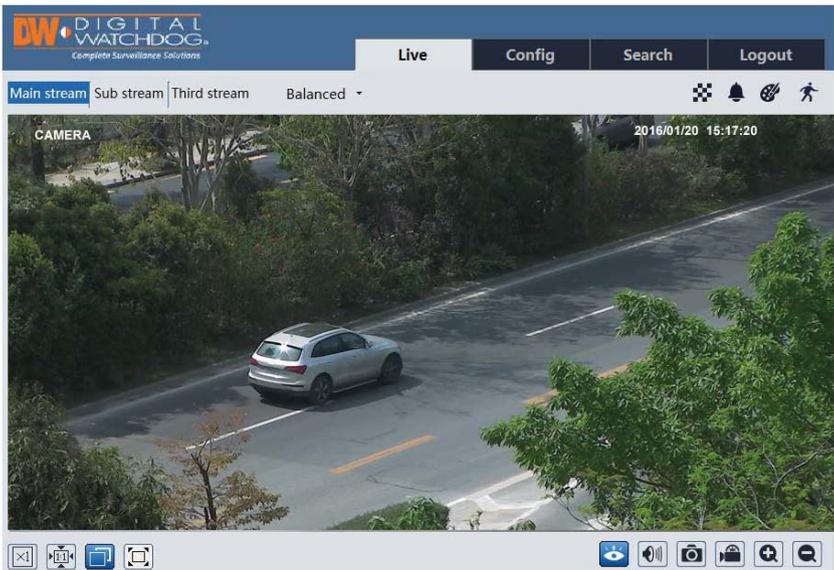


Input the username and password to log in.



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.

Icon	Description	Icon	Description
	Original size		Scene change indicator icon
	Appropriate size		Abnormal clarity indicator icon
	Auto		Color abnormal indicator icon
	Full screen		Motion alarm indicator icon
	Start/stop live view		Start/stop recording
	Enable/disable audio		Zoom in
	Snap		Zoom out

- When motion detection alarm is triggered, the people icon will turn red.
- In full screen mode, double click to exit.

6 Remote Live Surveillance

6.1 System Configuration

The “System” configuration includes three submenus: Basic Information, Date and Time and Local Config.

6.1.1 Basic Information

In the “Basic Information” interface, you can check the relative information of the device.

Device Type	xxxx
Brand	xxxx
Software Version	4.1.1.0(8234)
Software Build Date	2016-11-10
Kernel Version	20161109
Hardware Version	1.3
Onvif Version	2.3
OCX Version	1.1.3.5
MAC	00:18:ae:12:ab:1d

6.1.2 Date and Time

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



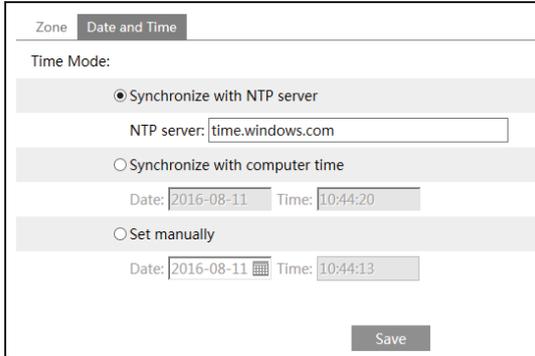
Zone Date and Time

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

DST

You can select the time zone and DST as required.

Click “Date and Time” tab to set the time mode.



Zone Date and Time

Time Mode:

Synchronize with NTP server

NTP server: time.windows.com

Synchronize with computer time

Date: 2016-08-11 Time: 10:44:20

Set manually

Date: 2016-08-11 Time: 10:44:13

Save

6.1.3 Local Config

Go to Config→System→Local Config. You can set the storage path of the captured pictures and video records. You can also enable or disable the video audio.



Picture Path C:\Users\Administrator\Favorites Browse

Record Path C:\Users\Administrator\Favorites Browse

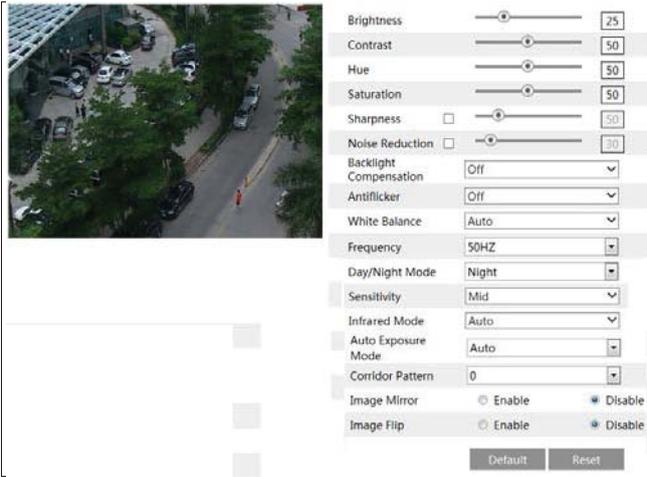
Video Audio Settings Enable Disable

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. You may set and adjust the picture’s brightness, contrast, hue and saturation, etc.

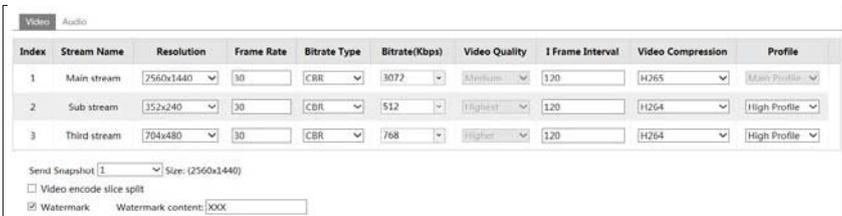


- **Brightness:** Set the brightness level of the camera's image.
- **Contrast:** Set the color difference between the brightest and darkest parts.
- **Hue:** Set the total color degree of the image.
- **Saturation:** Set the degree of color purity. The purer the color is, the brighter the image is.
- **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.
- **Backlight Compensation:**
 - Off: Close the backlight compensation function. It is the default mode.
 - WDR
 - As to the WDR scene, WDR will help the camera provide clear images when there are both very bright and very dark areas simultaneously in the field of the view by lowering the brightness of the highlight area and increasing the brightness of the lowlight area. High, middle and low can be selected.
 - There will be some record lost in a few seconds during mode changing from non-WDR to WDR mode.
 - HLC: Lower the brightness of the whole image by suppressing the brightness of the image's highlight area and reducing the size of the halo area.
 - BLC: The exposure will begin automatically according to the scene for the goal of seeing the darkest area of the image.
- **Anti-flicker:**
 - Off: Close the anti-flicker function.
 - 50HZ: Make sure the horizontal stripes will not appear in the image while the device is adjusting the exposure automatically according to the brightness of the scene when the electric supply is 50Hz.

- 60Hz: Make sure the horizontal stripes will not appear in the image while the device is adjusting the exposure automatically according to the brightness of the scene when the electric supply is 60Hz.
- **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.
- **Infrared Mode:** You may choose “ON”, “OFF” and “Auto” as required.
- **Exposure Mode:** You may choose “Auto” or “Manual” as required.
- **Corridor Pattern:** You can change the direction of the video image by using this function. 0, 90, 180 and 270 are available. The default value is 0. The video resolution should be 1080P or under 1080P if you use this function.
- **Image Mirror:** Reverse the current video image right and left.
- **Image Flip:** Turn the current video image upside down.

6.2.2 Video / Audio Configuration

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



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



Three video streams can be adjustable.

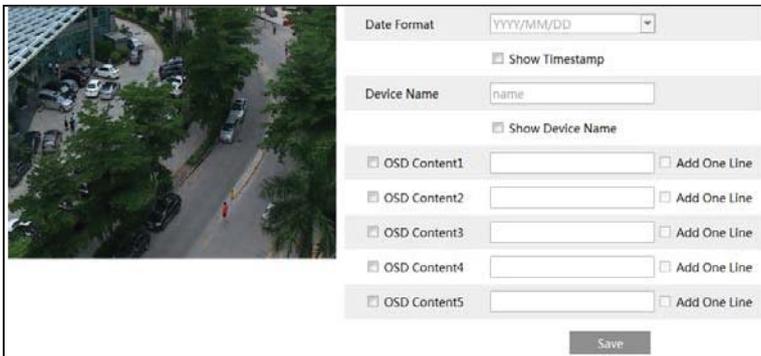
- **Resolution:** The higher the resolution is, the clearer the image is.
- **Frame rate:** The higher the frame rate is, the more fluency the video is. However, more storage room will be taken up.
- **Bitrate type:** Including CBR and VBR. CBR means that no matter how changeable the video resources are, the compression bitrate keeps constant. This will not only facilitate the image quality better in a constant bitrate but also help to calculate the capacity of

the recording. VBR means that the compression bitrate can be adjustable according to the change of the video resources. This will help to optimize the network bandwidth.

- **Bitrate:** Please choose it according to the actual network situation.
- **Video Quality:** When VBR is selected, you need to choose image quality. The higher the image quality you choose, the more bitrate will be required.
- **I Frame interval:** It is recommended to use the default value. If the value is over high, the read speed of the group of pictures will be slow resulting in the quality loss of the video.
- **Video Compression:** H264 and H265 are optional. Higher quality of image can be transferred under limited network bandwidth by using H265 video encoding, however, higher quality of the hardware is required.
- **Profile:** Baseline, main/high profiles are optional. Baseline profile is mainly used in interactive application with low complexity and delay. Main/high profile is mainly used for higher coding requirement.
- **Send Snapshot:** Please select it according to the actual situation.
- **Video encode slice split:** If enabled, you may get more fluency image even though using the low-performance PC.
- **Watermark:** If enabled, input the watermark content. You may check the watermark when playing back the local record in the search interface, lest the record files is tampered.
- **Audio Encoding:** G711A and G711U are selectable.
- **Audio Type:** MIC and LIN are selectable.

6.2.3 OSD Configuration

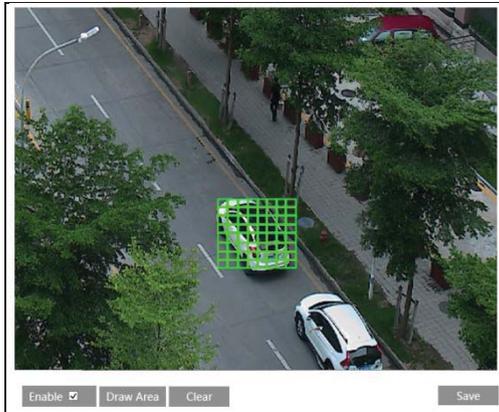
Go to Image→OSD interface as shown below.



You may set time stamp, device name and OSD content here. After enabling the corresponding display and entering the content, drag them to change their position. Then click "Save" button to save the settings.

6.2.4 Video Mask

Go to Image→Video Mask interface as shown below. You can set 4 mask areas at most.



To set up video mask:

1. Enable video mask.
2. Click "Draw Area" button and then drag the mouse to draw the video mask area.
3. Click "Save" button to save the settings.
4. Return to the live to see the following picture.

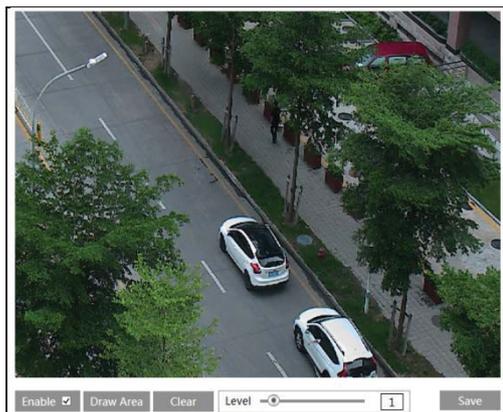


Clear the video mask:

Go to video mask interface and then click "Clear" button to delete the current video mask area.

6.2.5 ROI Configuration

Go to Image→ROI Config interface as shown below.



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

Now, you will see the selected ROI area is clearer than other areas especially in low bitrate condition.

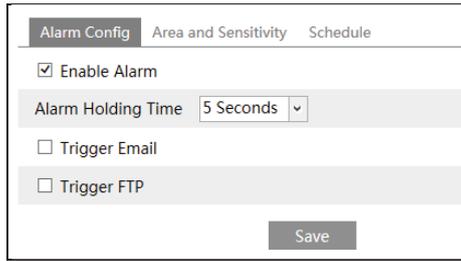


6.3 Alarm Configuration

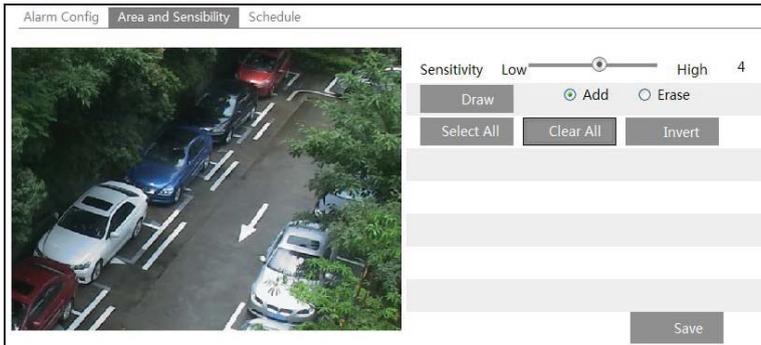
Alarm configuration includes two submenus: Motion Detection and Alarm Server.

6.3.1 Motion Detection

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



1. Check "Enable Alarm" check box to activate motion based alarm, choose alarm holding time and set alarm trigger options.
 - **Trigger Email:** If "Trigger Email" and "Attach Picture" checkbox is checked (email address shall 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" checkbox is 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 "Area and Sensitivity" tab to go to the interface as shown below.



- Move the "Sensitivity" scroll bar to set the sensitivity.
 Select "Add" and click "Draw" button and drag mouse to select the motion detection area;
 Select "Erase" and drag the mouse to clear motion detection area.
 After that, click "Save" to save the settings.
3. Set the schedule of the motion detection. Click "Schedule" tab to go to the interface as shown below.

Alarm Config Area and Sensitivity **Schedule**

Erase Add

Week Schedule

Sun.	00:00-16:45	Manual Input
Mon.	00:00-11:15	Manual Input
Tues.	05:00-18:30	Manual Input
Wed.		Manual Input
Thur.		Manual Input
Fri.		Manual Input
Sat.		Manual Input

Holiday Schedule

Date:

00:00-24:00 Manual Input

Week schedule

Set the alarm time from Monday to Sunday for alarm every day in one week. The lengthwise means one day of a week; the rank means 24 hours of a day. Green means selected area. Blank means unselected area.

“Add”: Add the schedule for a special day.

“Erase”: Delete holiday schedule.

Day schedule

Set alarm time for alarm in some time of a special day, such as holiday.

Set a date at the “Date” box, click “Add” button to add that date to the list box on the right side and then drag the scroll bar to set the schedule of that day.

Select a date in the list box on the right side, and click “Delete” to remove the schedule on that day.

Click “Save” button to save the settings.

Note: Holiday schedule is prior to Week schedule.

6.3.2 Alarm Server

Go to Alarm → Alarm Server interface as shown below.

You may input the alarm server address and port. When the alarm happens, the camera will automatically transfer the alarm event to the alarm server. If the alarm server is not used, there is no need for you to configure here.

Server Address

Port

OK

6.4 Event Configuration

Event configuration includes four submenus: Object Removal, Exception, Line Crossing and Intrusion.

Note: Some software versions of this series of cameras may not support the following functions. Please take actual displayed interface as final.

6.4.1 Object Removal

To set object removal:

Go to Config→Event→Object Removal interface as shown below.

Detection Config Area Schedule

Enable Detection

Enable Left Detection

Enable Item Missing Detection

Alarm Holding Time ▾

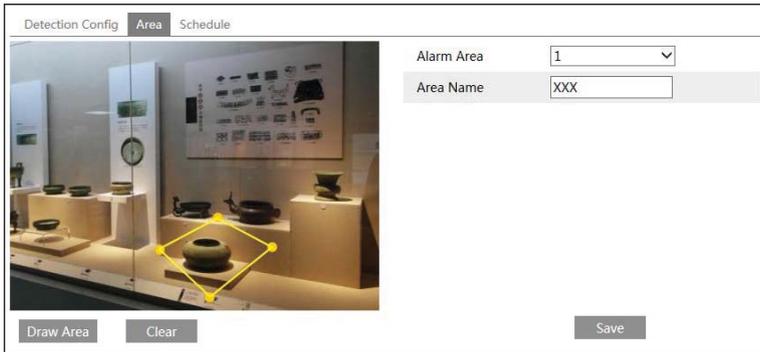
Trigger Alarm Out

Trigger Email

Trigger FTP

Save

1. Enable object removal detection and then select the detection type.
 - **Enable Left Detection:** The relevant alarms will be triggered if there are items left in the pre-defined alarm area.
 - **Enable Item Missing Detection:** The relevant alarms will be triggered if there are items missing in the pre-defined alarm area.
2. Set the alarm holding time and alarm trigger options. The setting steps are the same with that of motion detection. Please refer to motion detection chapter for details.
3. Click "Save" button to save the settings.
4. Set the alarm area of the object removal detection. Click "Area" tab to go to the interface as shown below.



Set the alarm area number and then input the alarm area name on the right side. You can add 4 alarm areas at most.

Click "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 "Stop Draw" button to stop drawing. Click "Clear" button to delete the alarm area. Click "Save" button to save the settings.

5. Set the schedule of the object removal detection. The setting steps of the schedule are the same with that of motion detection. Please refer to motion detection chapter for details.

※ Application Scenario Illustration

1. Object removal detection cannot determine the objects' ownership. For instance, there is an unattended package in the station. Object removal detection can detect the package itself but it cannot determine whether it is an ownership package.
2. Try not to enable object removal detection when light changes greatly in the scene.
3. Try not to enable object removal detection if there are complex and dynamic environments in the scene.
4. Adequate light and clear scenery are very important to object removal detection.
5. Please contact us for more detailed application scenarios.
6. 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 removal objects.



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

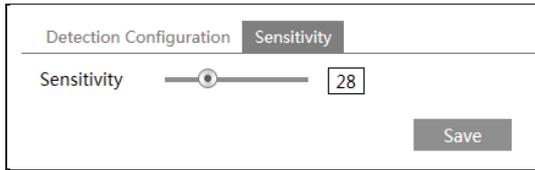
6.4.2 Exception

To set exception detection:

Go to Config→Event→Exception interface as shown below.

A screenshot of a web-based configuration interface for exception detection. The interface has two tabs: "Detection Configuration" (selected) and "Sensitivity". Under "Detection Configuration", there are three checked checkboxes: "Scene change detection", "Video blur detection", and "Video cast detection". Below these is a field for "alarmHoldingTime" set to "20 Seconds" with a dropdown arrow. There is a section for "triggerAlarmOut" which is currently empty. At the bottom, there are two unchecked checkboxes: "triggerEmail" and "triggerFTP". A "Save" button is located in the bottom right corner.

1. Enable the relevant detection as required.
 - **Scene Change Detection:** The relevant alarms will be triggered if the scene of the monitor video has changed.
 - **Video Blur Detection:** The relevant alarms will be triggered if the monitor video is blurry.
 - **Video Cast Detection:** The relevant alarms will be triggered if color cast happens to the monitor video.
2. Set the alarm holding time and alarm trigger options. The setting steps are the same with that of motion detection. Please refer to motion detection chapter for details.
3. Click "Save" button to save the settings.
4. Set the sensitivity of the exception detection. Click "Sensitivity" tab to go to the interface as shown below.



Drag the slider to set the sensitivity value or directly input 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 defocus of the device image. You should just the value according to the real situation.

The sensitivity value of Video Cast Detection: The higher the value is, the more sensitive the system responds to the color cast of the device image. You should also consider other factors.

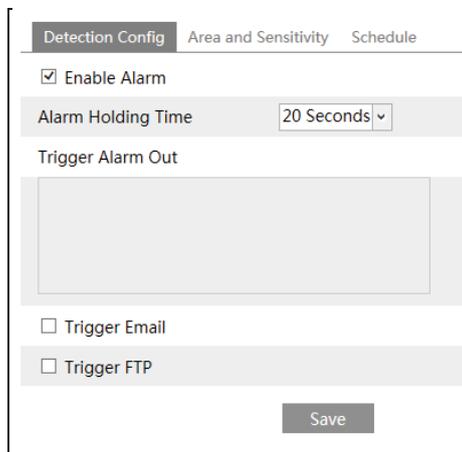
✘ **Application Scenario Illustration**

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

6.4.3 Line Crossing

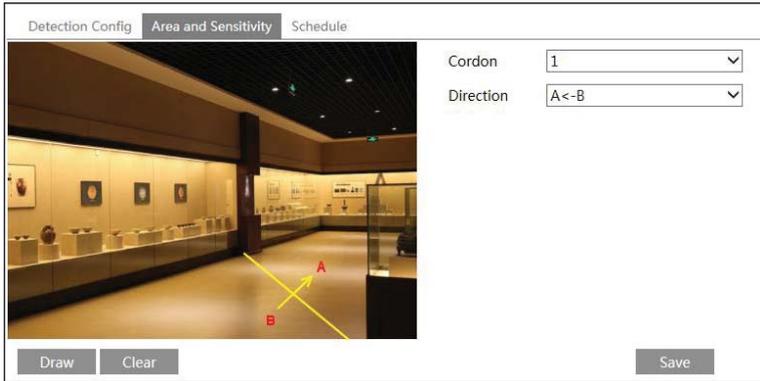
Line Crossing: The relevant alarms will be triggered if someone or something crosses the pre-defined alarm lines.

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



1. Enable line crossing alarm and set the alarm holding time.

2. Set alarm trigger options. The setting steps are the same with that of 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 "Area and Sensitivity" tab to go to the interface as shown below.



Set the cordon number and direction. You can add 4 cordons at most.

Direction: A<->B, A->B and A<-B optional. It is the crossing direction of the intruder who crosses over the alarm line.

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 "Draw" button and then drag the mouse to draw a cordon in the image on the left side. Click "Stop" button to stop drawing. Click "Clear" button to delete the cordons. Click "Save" button to save the settings.

5. Set the schedule of the line crossing alarm. The setting steps of the schedule are the same with that of motion detection. Please refer to motion detection chapter for details.

✳ Application Scenario Illustration

1. Auto-focusing function should not be enabled for line crossing detection. If enabled, the video image will change so greatly that the algorithm will stop working temporarily.
2. Try not to enable line crossing detection when light changes greatly in the scene.
3. Try to install the camera at a certain angle of depression.
4. Adequate light and clear scenery are very important to line crossing detection.
5. Adjust the camera to make the detection area in the center of the video image. Make sure no obstructions are in the main crossing area. It is strongly recommended to make the obstructions (like trees, bushes, flags, etc.) outside the detection area.
6. 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.

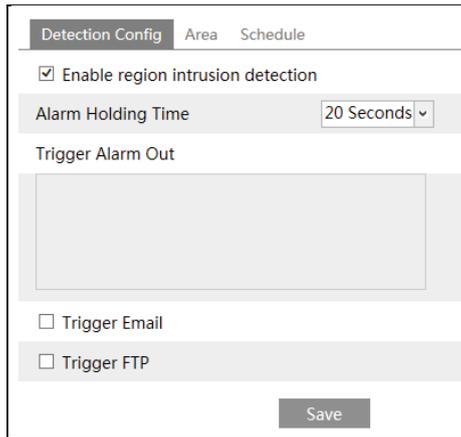


The ground is covered with vegetation; at the right of the fence is a gym where people pass by frequently. The above mentioned environment is too complex to detect the crossing objects.

6.4.4 Intrusion

Intrusion: The relevant alarms will be triggered if someone or something intrudes into the alarm areas or moves in the pre-defined alarm areas.

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



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



7. Set the alarm area number on the right side. You can add 4 alarm areas at most.
8. Click "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 "Stop Draw" button to stop drawing. Click "Clear" button to delete the alarm area. Click "Save" button to save the settings.
9. Set the schedule of the intrusion detection. The setting steps of the schedule are the same with that of motion detection. Please refer to motion detection chapter for details.

※ Application Scenario Illustration

1. Auto-focusing function should not be enabled for intrusion detection. If enabled, the

video image will change so greatly that the algorithm will stop working temporarily.

2. Try not to enable intrusion detection when light changes greatly in the scene.
3. Try to install the camera at a certain angle of depression.
4. Adequate light and clear scenery are very important to intrusion detection.
5. Adjust the camera to make the detection area in the center of the video image. The detected object should be in the detection area for about two seconds at least. Make sure no obstructions are in the main crossing area. It is strongly recommended to make the obstructions (like trees, bushes, flags, etc.) outside the detection area.
6. 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 above mentioned 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.

6.5 Network Configuration

6.5.1 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

Subnet Mask

Gateway

Preferred DNS Server

Alternate DNS Server

Save

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

Use PPPoE-Click “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

Password

Save

You can choose either way of the network connection. If you use PPPoE to connect internet, you will get a dynamic WAN IP address. This IP address will change frequently. You may use the function of IP change notification.

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

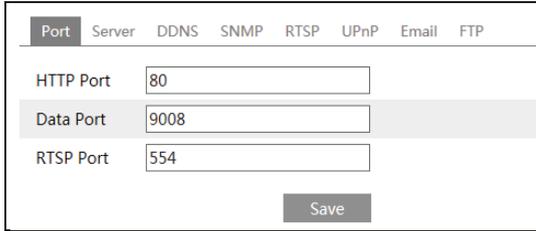
Save

Trigger Email: when the IP address of the device is changed, a new IP address will be sent to the appointed mailbox automatically

Trigger FTP: when the IP address of the device is changed, a new IP address will be sent to FTP server.

6.5.2 Port

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



Port	Server	DDNS	SNMP	RTSP	UPnP	Email	FTP
HTTP Port	<input type="text" value="80"/>						
Data Port	<input type="text" value="9008"/>						
RTSP Port	<input type="text" value="554"/>						

Save

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

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

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

6.5.3 Server Configuration

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



Port	Server	DDNS	SNMP	RTSP	UPnP	Email	FTP
<input checked="" type="checkbox"/>	Enable						
Server Port	<input type="text" value="10"/>						
Server Address	<input type="text"/>						
Device ID	<input type="text" value="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, input the remaining information of the device in the ECMS/NVMS. After that, the system will auto allot a device ID. Please check it in the ECMS/NVMS.
3. Input the above-mentioned server address, server port and device ID in the responding boxes. Click "Save" button to save the settings.

6.5.4 DDNS

If your camera is set to use PPPoE as its default network connection, DDNS should be set for network access. Before you set the DDNS, please make sure you have registered a domain name on the DDNS server.

1. Go to Config→Network→ DDNS.

Port	Server	DDNS	SNMP	RTSP	UPnP	Email	FTP
<input checked="" type="checkbox"/> Enable							
Server Type	mintdns ▾						
Server Address	www.dvrdydns.com						
User Name	<input type="text"/>						
Password	<input type="text"/>						
Domain	<input type="text"/>						
							Save

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

<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.	
<input type="text"/>	dvrdydns.com ▾ <input type="button" value="Request Domain"/>

After you successfully request your domain name, you will see your domain in the list.

Search by Domain:

Click a name to edit your domain settings.

NAME	STATUS	DOMAIN
654321ABC	✔	654321abc.dvrdydns.com

Laet Update: *Not yet updated* IP Address: 210.21.229.138

[Create additional domain names](#)

- Input the username, password, domain you apply for in the DDNS configuration interface.
- Click "Save" button to save the settings.

6.5.5 SNMP

To get camera status, parameters and alarm information and remotely manage the camera, you can set the SNMP function. Before using the SNMP, please download the SNMP software and set the parameters of the SNMP, such as SNMP port, trap address.

- Go to Config→Network→SNMP.

SNMP v1/v2

Enable SNMPv1

Enable SNMPv2

Read SNMP Community

Write SNMP Community

Trap Address

Trap Port

Trap community

SNMP v3

Enable SNMPv3

Read User Name

Security Level

Authentication Algorithm MD5 SHA

Authentication Password

Private-key Algorithm DES AES

Private-key Algorithm

Write User Name

Security Level

Authentication Algorithm MD5 SHA

Authentication Password

Private-key Algorithm DES AES

Private-key Algorithm

Other Settings

SNMP Port

2. Check the corresponding version checkbox (Enable SNMPv1, Enable SNMPv2, Enable SNMPv3) according to the version of the SNMP software you download.
3. Set the “Read SNMP Community”, “Write SNMP Community”, “Trap Address”, “Trap Port” and so on. Please make sure the settings are the same as that of your 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.

6.5.6 RTSP

Go to Config→Network→RTSP.

1. Select “Enable”.
2. **RTSP Port:** Access port of the streaming media. The default number is 554.
3. **RTSP Address:** The RTSP address you need to input in the media player.
4. Check “Allow anonymous login...”.

6.5.7 UPnP

If you enable this function, you can quickly access the camera via LAN and you don’t need to configure the port mapping when the camera is connected to the WAN via the router.

Go to Config→Network→UPnP. Enable UPnP and then input UPnP name.

After you enable it and set the UPnP name, you will see the UPnP name by clicking “Network” on the desktop of your computer which is in the same local area network. Then double click this name to access the camera quickly.

6.5.8 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.

The screenshot shows a configuration page with tabs for Port, Server, DDNS, SNMP, RTSP, UPnP, Email, and FTP. The 'Email' tab is active. Under the 'Sender' section, there are input fields for Sender Address (XXX@126.com), User Name (XXX@126.com), Password (masked with dots), Server Address (smtp.126.com), Secure Connection (Unnecessary), SMTP Port (25, Default), and Send Interval(S) (0, 0-3600). There are 'Clear' and 'Test' buttons. Under the 'Recipient' section, there is a list with 'XXX@126.com' selected, a 'Recipient Address' input field, and 'Add', 'Delete', and 'Save' buttons.

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 actual needs.

SMTP Port: The SMTP port.

Send Interval(S): Set it as needed.

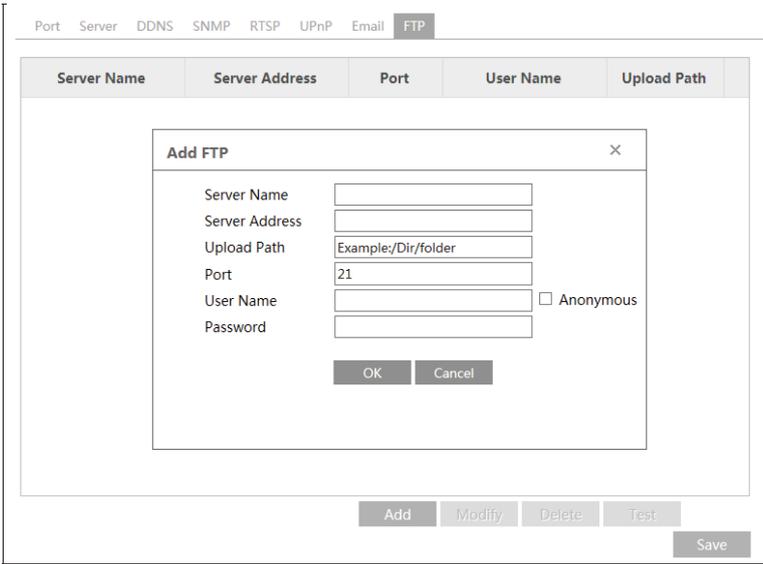
Click “Test” button to test the effectiveness of the account.

Recipient Address: Receiver’s e-mail address.

6.5.9 FTP

After you set the FTP server, the captured pictures on an alarm will be uploaded to the FTP server.

Go to Config→Network →FTP.



To Add FTP:

Server Name: The name of the FTP.

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

Upload Path: The path of uploading the files.

Port: The port of the FTP.

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

6.6 Security Configuration

6.6.1 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 "Add" button to pop up the following textbox.

The 'Add User' dialog box includes 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 currently showing 'Administrator'.
- Bind MAC:** A text input field containing '00:00:00:00:00:00' with a checkbox to its right.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom.

2. Input user name in "User Name" textbox.
3. Input letters or numbers in "Password" and "Confirm Password" textbox.
4. Choose the use type.
5. Input the MAC address of the PC in "Bind MAC" textbox.
6. After binding physical address to the IP-CAM, you can access the device on this PC only. If the MAC address was "00:00:00:00:00:00" which means it can be connected to any computers.
7. Click "OK" button and then the new added user will display in the user list.

Modify user:

1. Select the user you need to modify password and physical address in the user configuration list box.
2. The "Edit user" dialog box pops up by clicking "Modify" button.

The 'Edit User' dialog box includes the following fields and controls:

- Modify Password**
- User Name:** A text input field containing 'admin'.
- 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' with a checkbox to its right.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom.

3. Input old password of this user in the "Old Password" text box.
4. Input new password in the "New password" and "Confirm Password" text box.
5. Input computer's MAC address as required.
6. Click "OK" button to save the settings.

Delete user:

1. Select the user you want to delete in the user configuration list box.
2. Click "Delete" button to delete the user.

Note: The default super administrator cannot be deleted.

6.6.2 Online User

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

6.6.3 Block and Allow Lists

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

IP Address Filter Settings

Enable IP address filtering

Block the following IP address Allow the following IP address

[Empty List Box]

[Add] [Delete]

0.0.0.0

Block the following MAC Address

Enable MAC address filtering

Block the following MAC address Allow the following MAC address

[Empty List Box]

[Add] [Delete]

00:00:00:00:00:00

[Save]

Setting steps are as follows:

Check "Enable IP address filtering" check box.

Select "Block the following IP address", input IP address in the IP address list box and click "Add" button. The operation step of "Allow the following IP address" and MAC address filter settings are the same with "Block the following IP address".

After you set the IP address or MAC address, the system will block or allow the user using the added IP address or MAC address to access the camera.

6.7 Maintenance Configuration

6.7.1 Backup and Restore

Go to Config→Maintenance→Backup & Restore.

The screenshot shows a web interface with three main sections:

- Import Setting:** Contains a text input field labeled "Path" followed by a "Browse..." button and an "Import Setting" button below it.
- Export Settings:** Contains an "Export Settings" button.
- Default Settings:** Contains a "Load Default" button.

- **Import & Export Settings**

You can import or export the setting information from PC or to device. Click "Browse" to select save path for import or export information on PC. Click "Import Setting" or "Export Setting" button.

- **Default Settings**

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

6.7.2 Reboot

Go to Config→Maintenance→Reboot.
Click "Reboot" button to reboot the device.

Timed Reboot Setting:

Enable "Time Settings", set the date and time and then click "Save" button to save the settings.

6.7.3 Upgrade

Go to Config→Maintenance→Upgrade. In this interface, you can upgrade the system.

The screenshot shows a web interface titled "Upgrade System" with a "Path" input field, a "Browse" button, and an "Upgrade" button.

1. Click "Browse" button to select the save path of the upgrade file
2. Click "Upgrade" button to start upgrading the application program.
3. The device will restart automatically
4. After you successfully update the software, click "OK" button to close IE and then re-open IE to connect IP-Cam.

Caution! You can't disconnect to PC or close the IP-CAM during upgrade.

6.7.4 Operation Log

To query and export log:

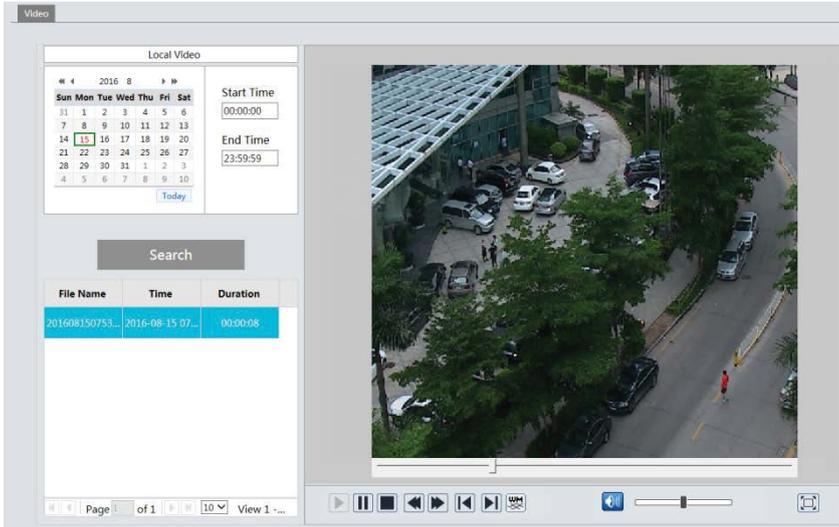
1. Go to Config→Maintenance→Operation Log.

Main Type:	<input type="text" value="All log"/>	Sub Type:	<input type="text" value="All log"/>		
Start Time:	<input type="text" value="2015-07-14 00:00:00"/>	End Time:	<input type="text" value="2015-07-14 23:59:59"/>	<input type="button" value="Search"/>	<input type="button" value="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 Record Search

Click Search to go to the interface as shown below. You can play the local video record. Before playing, please set the storage path of the video record in the local configuration interface and make sure there are record files.



Choose the date and the start time and end time and then click “Search” button to search the record files. Double click the record file to play the record. The descriptions of the buttons on the playback interface are as follows.

Icon	Description	Icon	Description
	Play button. After pausing the video, click this button to continue playing.		Pause button.
	Stop button.		Speed down.
	Speed up.		Click it to play the previous record.
	Click it to play the next record.		Open/close watermark.
	Click it to enable / disable audio; drag the slider to adjust the volume after enabling audio.		Full screen. Click it to display full screen. Double click to exit full screen.

8 Appendix

Appendix 1 Q& A

Q: How to find my password if I forget it?

A: Reset the device to the default factory settings.

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

Q : Fail to connect devices through IE browser, why?

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

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

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

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

Q : IP tool cannot search devices, why?

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

Q : IE cannot download ActiveX control. How can I do?

- a. IE browser blocks ActiveX. Please do setup as below.
 1. Open IE browser. Click Tools-----Internet Options....



2. Select Security-----Custom Level....
 3. Enable all the sub options under "ActiveX controls and plug-ins".
 4. Then click OK to finish setup.
- b. Other plug-ins or anti-virus blocks ActiveX. Please uninstall or close them.

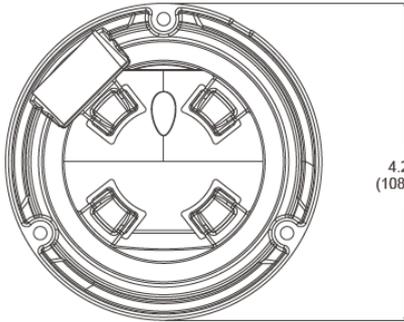


Q: No sound can be heard, why?

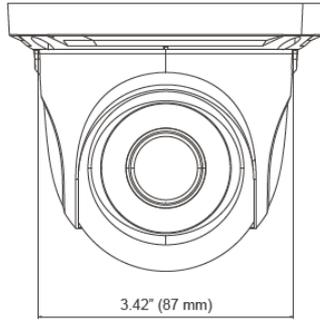
A: Audio input device is not connected. Please connect and try again.

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

9 Dimensions



4.25"
(108 mm)



3.42" (87 mm)

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

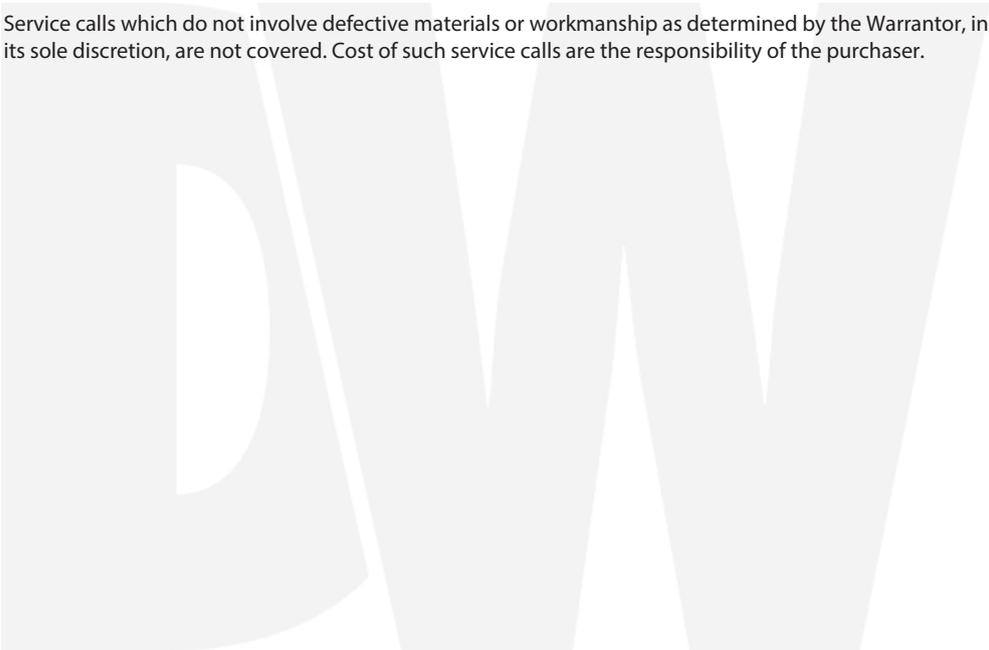
There are no express warranties except as listed above. The Warrantor will not be liable for incidental or consequential damages (including, without limitation, damage to recording media) resulting from the use of these products, or arising out of any breach of the warranty. All express and implied warranties,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