MEGApix® Facial Recognition 4K White Light IP Cameras

DWC-MSBD08BW: Bullet camera with fixed lens
DWC-MSBD08MW: Bullet camera with vari-focal lens
DWC-MSDG08BW: Vandal dome camera with fixed lens
DWC-MSDG08MW: Vandal dome camera with vari-focal lens
DWC-MSTE08BW: Turret camera with fixed lens
DWC-MSTE08MW: Turret camera with vari-focal lens

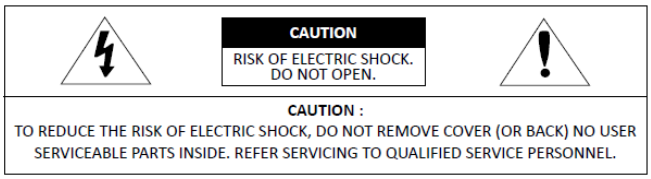


User's Manual Ver. 11/26

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

Safety Instruction

The following symbols or words may be found in this manual.



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

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

About the Manual

- This manual is suitable for many models. All examples, screenshots, figures, charts, and illustrations used in the manual are for reference, and actual products may be different from those in this Manual. The functions may vary by model. If your camera doesn't support one or more functions described in the manual, please skip the relevant instructions.
- Please read this user manual carefully to ensure that you can use the device correctly and safely.
- Within the maximum scope permitted by the law, the products described in this Manual (including hardware, software, firmware, etc.) are provided "AS IS". The information in this document (including URL and other Internet site reference data) is subject to change without notice. This Manual may contain technical inaccuracies or printing errors. This information will be periodically updated, and these changes will be added to the latest version of this Manual without prior notice.
- In this manual, the trademarks, product names, service names and company names that our company does not own are the property of their respective owners.

Use of the Product

- This product should not be used for illegal purposes.
- The company does not allow anyone to use the Company's products to infringe the privacy, personal information, and portrait rights of others. The user shall not use this product for any illegal use or any prohibited use under these terms, conditions, and declarations. When using this product, the user shall not damage, disable, overload or obstruct any of the hardware of this product in any way or interfere with the use of this product by any other users. Also, the user should not attempt to use the product or the software by hacking, stealing the password, or any other means.

Electrical Safety

- This product is intended to be supplied by a Listed Power Unit, marked with 'Limited Power Source', 'LPS' on the unit, output rated at a minimum of 12V or POE or AC24V (varies by model), no more than 5000m altitude of operation and Tma=60°C.
- As for the modes with PoE function, the function of the ITE being investigated under the IEC 62368-1 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.
- Improper handling and/or installation could run the risk of fire or electrical shock.
- The product must be grounded to reduce the risk of electric shock.
- ⚠ Warning: Wear anti-static gloves or discharge static electricity before removing the bubble or cover of the camera.

Environment

- Heavy stress, violent vibration or exposure to water is not allowed during transportation, storage and installation.

- Avoid aiming the camera directly towards extremely bright objects, such as the sun, as this may damage the image sensor.
- Keep away from heat sources such as radiators, heat registers, stoves, etc.
- Do not expose the product to direct airflow from an air conditioner.
- Do not block any ventilation openings and ensure proper ventilation around the camera.
- Do not place the device in a damp, dusty, extremely hot or cold environment, or in locations with strong electromagnetic radiation or unstable lighting.
- Make sure that no reflective surface (like shiny floors, mirrors, glass, lake surfaces and so on) is too close to the camera lens, resulting in image blur.

Operation and Daily Maintenance

- There are no user-serviceable parts inside. Please contact your installer or DW support if the product does not work properly.
- Please shut down the device and then unplug the power cable before you begin any maintenance work.
- ⚠ Warning: All the examination and repair work should be done by qualified personnel.
- Do not touch the CMOS sensor optic component. You can use a blower to clean the dust on the lens surface.
- Always use a dry, soft cloth to clean the device. If there is too much dust, using a cloth for cleaning (such as using a cloth) may result in poor IR/illumination LED functionality and/or IR/illumination LED reflection.
- The dome/lens cover is an optical device; please don't touch or wipe the cover surface directly during installation and use. For dust, use an oil-free soft brush or hair dryer to remove it gently; for grease or fingerprints, use an oil-free cotton cloth or paper soaked with detergent to wipe from the lens center outward. Change the cloth and wipe several times if it is not clean enough.

White Light Illuminator (if supported)

- DO NOT turn on the white light when you install or maintain the camera. Please wear appropriate eye protection when you want to test the white light.
- DO NOT stare at the operating light source. It will probably be harmful to your eyes.
- The white light illuminators and/or the IR LEDs should at no time be covered when the camera is running to prevent overheating and the possible risk of fire.

Privacy Protection

- When installing cameras in public areas, a warning notice shall be given reasonably and effectively and clarify the monitoring range.
- As the device user or data controller, you might collect the personal data of others, such as faces, car plate numbers, etc. As a result, you shall implement reasonable and necessary measures to protect the legitimate rights and interests of other people, avoiding data leakage and improper use, including but not limited to setting up access control, providing clear and visible notice to inform people of the existence of the surveillance area, providing required contact information and so on.

Disclaimer

With regard to the product with internet access, the use of the product shall be wholly at your own risk. Our company shall not be responsible for abnormal operation, privacy leakage or other damages resulting from cyber attack, hacker attack, virus infection, or other internet security risks; however, our company will provide timely technical support if 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 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 lowercase letters, should be used in your password.

- Regularly change the passwords of your devices 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 up the firewall on your router. But note that some important ports cannot be closed (like the HTTP port, HTTPS port and Data Port).
- 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 firewall and the corresponding firewall policy.
- It is not recommended to use the v1 and v2 functions of SNMP.
- In order to enhance the security of WEB client access, please create a TLS certificate to enable HTTPS.
- Use a blocklist and an allowlist to filter IP addresses. This will prevent everyone, except the specified IP addresses, from accessing the system.
- If you add multiple users, please limit the functions of guest accounts.
- If you enable UPnP, it will automatically try to forward ports on 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 unauthorized users have accessed your device, 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

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

1. FCC compliance

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

2. FCC conditions:

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

This device may not cause harmful interference.

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

EU Compliance Statement

This product and - if applicable - the supplied accessories too are marked with “CE” and comply therefore with the applicable harmonized European standards listed under the Directive 2014/30/EU (EMCD), Directive 2011/65/EU (RoHS).

Note: The products with an input voltage within 50 to 1000 VAC or 75 to 1500 VDC comply with Directive 2014/35/EU (LVD), and the rest of the products comply with Regulation (EU)2023/988(GPSR). Please check the specific power supply information for reference.



Directive 2012/19/EU (WEEE Directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information, see: www.recyclethis.info.

According to the Waste Electrical and Electronic Equipment Regulations 2013, products marked with this symbol cannot be disposed of as unsorted municipal waste in the United Kingdom. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information, see: www.recyclethis.info.

Packaging and Packaging Waste Regulation (EU) 2025/40: This Regulation establishes requirements for the entire life cycle of packaging as regards environmental sustainability and labeling, to allow its placing on the market. It also establishes requirements for extended producer responsibility, packaging waste prevention, such as the reduction of unnecessary packaging and the re-use or refill of packaging, as well as the collection and treatment, including recycling, of packaging waste.

REACH (Regulation (EC) No 1907/2006): 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 conforms to the rules and regulations of REACH. For more information on REACH, please refer to the DG GROWTH or ECHA websites.

TABLE OF CONTENTS

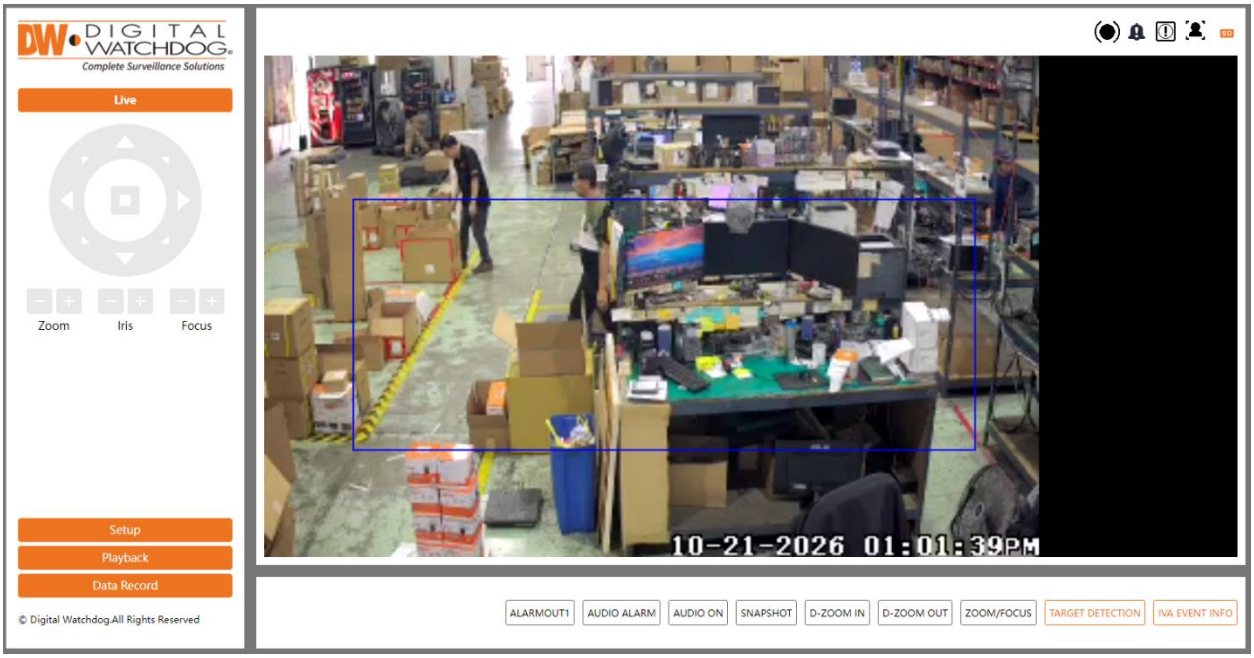
1 LIVE VIEW 8
2 NETWORK CAMERA CONFIGURATION 9
2.1 Camera Configuration 10
2.1.1 Camera Parameters 10
2.1.2 Video Configuration 12
2.1.3 Audio Configuration 13
2.1.4 OSD Configuration 13
2.1.5 Privacy Mask 15
2.1.6 ROI Configuration 15
2.1.7 Zoom/Focus 16
2.2 Network Configuration 17
2.2.1 IPv4 17
2.2.2 IPv6 18
2.2.3 Port 18
2.2.4 DDNS 19
2.2.5 SNMP 20
2.2.6 802.1x 21
2.2.7 RTSP 22
2.2.8 RTMP 23
2.2.9 UPnP 23
2.2.10 SMTP 23
2.2.11 FTP 25
2.2.12 HTTP Notification 27
2.2.13 HTTPS 29
2.2.14 QoS 30
2.3 AI Event Options 30
2.3.1 Installation Guidelines and Recommendations 30
2.3.2 Object Events 31
2.3.3 Line Crossing 31
2.3.4 Perimeter Intrusion 36
2.3.5 Face Recognition 38
2.4 Alarm Configuration 43
2.4.1 Motion Detection 43
2.4.2 SD Card Full 45
2.4.3 SD Card Error 45
2.4.4 Alarm In 46
2.4.5 Alarm Out 47
2.4.6 Audio Alarm 48
2.4.7 Tampering 48
2.5 Security Configuration 49
2.5.1 User Configuration 49
2.5.2 Online User 52
2.5.3 Block and Allow Lists 52
2.5.4 Security Service 52
2.5.5 Password Security 53
2.5.6 Authentication 53
2.6 System Configuration 54
2.6.1 Basic Information 54
2.6.2 Date and Time 54
2.6.3 Time Zone & DST 54
2.6.4 Local Configuration 55

2.6.5 Micro SD Management 55
2.6.6 Record Parameters 56
2.6.7 Schedule Record 56
2.6.8 Snapshot 57
2.7 Maintenance Configuration 58
2.7.1 Backup and Restore 58
2.7.2 Reboot 58
2.7.3 Upgrade 59
2.7.4 Operation Log 60
2.7.5 Maintenance Information 60
3 PLAYBACK 62
3.1 Picture Search 62
3.2 Video Search 63
4 FACE RECOGNITION RESULT SEARCH 65
5 Appendix 66
5.1 Appendix Troubleshooting 66
5.2 Appendix Communication Matrix 67
5.3 Appendix Product Specifications 70

NOTE: See the camera's installation and setup guide for hardware installation.

1 LIVE VIEW

After logging in, the following window will be shown. The live view interface of different cameras may be slightly different. The following pictures and descriptions are for reference only.



Button/Icon	Description	Icon	Description
ALARMOUT1	Turn the alarm output on/off.		Alarm output indicator
AUDIO ALARM	Turn an audio alarm on/off.		Sensor alarm indicator
AUDIO ON/OFF	Turn audio on/off	SD	SD card recording indicator
SNAPSHOT	Capture a JPEG of the camera's current view.		Motion alarm indicator
D-ZOOM IN	Zoom in		Color abnormal indicator
D-ZOOM OUT	Zoom out		Abnormal clarity indicator
ZOOM/FOCUS	AZ control (only available for the model with a motorized zoom lens)		Scene change indicator
TARGET DETECTION	Display captured face pictures		Intrusion indicator
IVA EVENT INFO	Rule information display		Line crossing indicator

Button/Icon	Description	Icon	Description
			Face detection indicator (only available for some models)

* Smart alarm indicators will flash only when the camera supports those functions and the corresponding events are enabled.

*After clicking the audio alarm icon, the sound warning will be triggered according to the set warning times (set under ***Setup>Alarm>Audio Alarm***).

* Click the ZOOM/FOCUS control button to show the control panel to the right of the main view

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

Descriptions of Rule Information



Color Descriptions of Target Recognition box:

- Green box: detect human
- Purple box: detect motor vehicle
- Light blue box: detect non-motor vehicle (motorcycle/bicycle)
- Target box after an event is triggered: turn yellow

Rule line or area color display:

- Rule line or area: blue
- Rule line or area after an event is triggered: turn from blue to red.

2 NETWORK CAMERA CONFIGURATION

In the Webcam client, choose “Setup” to go to the Setup interface.

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

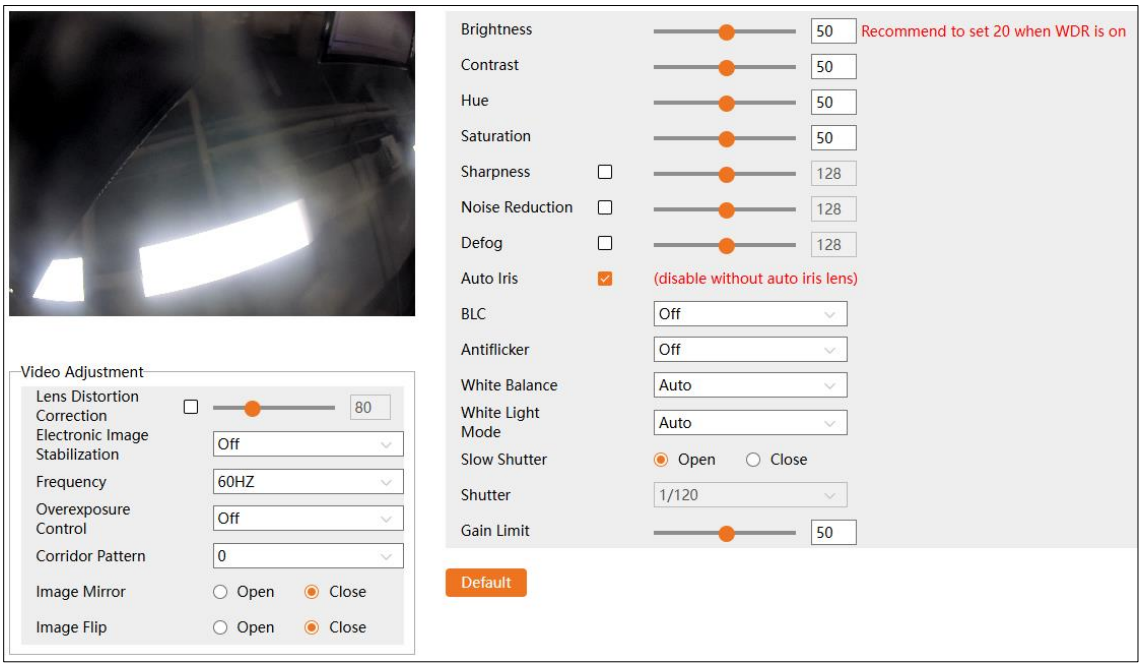
When entering the camera's Setup menu, the camera's "Basic Information" will show. This interface displays the product model, brand, firmware version, ONVIF version, MAC address, device ID, etc. To edit any of these options, go to the System Information menu on the right-side navigation menu.

2.1 Camera Configuration

2.1.1 Camera Parameters

Go to *Camera>Camera Parameters* as shown below. The image's brightness, contrast, hue, saturation and so on for common, day and night modes can be set up separately. The image effect can be quickly seen by switching the Configuration file.

Note: The camera parameters of different cameras may be slightly different. The following pictures and descriptions are for reference only. The real camera interface shall prevail.



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 clearer. Increasing the value will make the noise reduction effect better, but it will reduce the image resolution.

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

Auto Iris: If your camera is Auto Iris, please enable it (only varifocal models support this function).

Backlight Compensation (BLC):

- Off: deactivates 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 view by lowering the brightness of the bright area and increasing the brightness of the dark area.

Recording will be stopped for a few seconds while the mode is changing from non-WDR to WDR mode.

Note:

* Only some models support HWDR (true WDR). If your camera doesn't support HWDR, you can set (digital) WDR as needed.

* After enabling HWDR, the shutter and gain limits cannot be modified, and the slow shutter is closed by default. In addition, the anti-flicker function is automatically turned off and cannot be set.

- 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 in the darkest area of the image will be seen clearly.

Anti-flicker:

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

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

White light mode: Choose "Off", "Auto," or "Manual". Please select it as needed.

Slow Shutter: If enabled, when the ambient light drops to a certain level, the frame rate will be gradually reduced to maintain the brightness of the camera. It is recommended to enable this function for scenarios with high requirements in a low-light environment.

Shutter: Sets the upper limit of the effective exposure time. The exposure time will be automatically adjusted (within the set shutter limit value) according to the actual situation.

Gain Limit: Sets the upper limit of the gain. The gain value will be automatically adjusted (within the set gain limit value) according to the actual situation.

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 (only some models support this function).

Electronic Image Stabilization (EIS): Electronic image stabilization increases the stability of the video image by using jitter compensation technology (only some models support this function).

Frequency: 50 Hz and 60 Hz are optional.

Note: If the frequency is switched, the camera will reboot automatically.

Overexposure control: Choose “OFF”, “Low”, “Mid” or “High”. This function can automatically adjust the exposure parameter according to the actual effect on the image, effectively avoiding detail loss caused by image overexposure, so that the image will be more vivid. Please set it as needed.

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. (Only some models support this function).

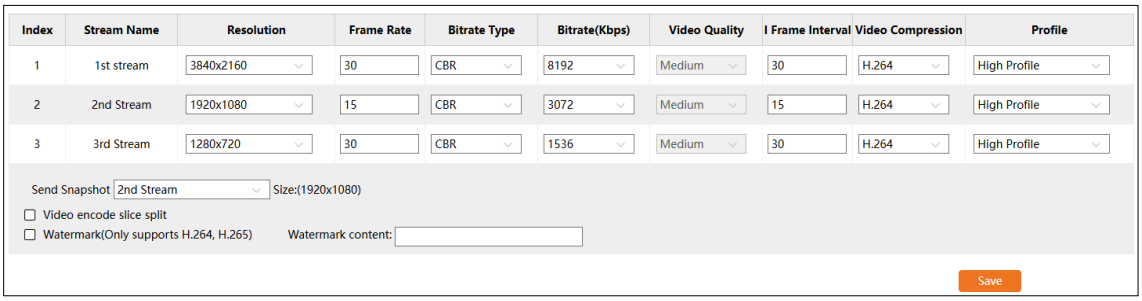
Image Mirror: Turn the current video image horizontally.

Image Flip: Turn the current video image vertically.

2.1.2 Video Configuration

Go to *Camera>Video* as shown below. In this interface, set the resolution, frame rate, bitrate type, video quality, and so on, subject to the actual network conditions.

Note: The video stream parameters of different camera series may be different. The following pictures and descriptions are for reference only. The real camera interface shall prevail.



Multiple video streams can be adjusted.

Resolution: The size of the image.

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

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 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 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, or H265 can be optional. MJPEG is not available for mainstream. If H.265 is chosen, make sure the client system can decode H.265. Compared to H.264, H.265 reduces the transmission bitrate at the same resolution, frame rate and image quality.

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

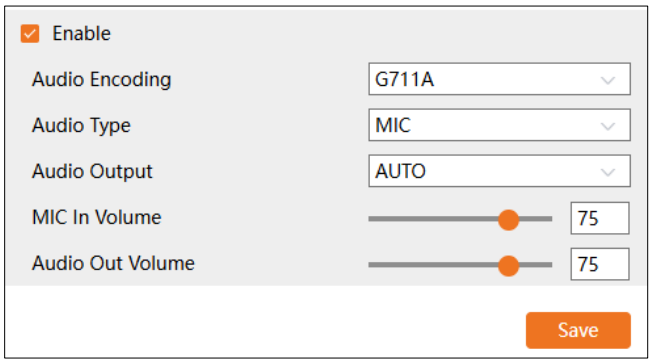
Send Snapshot: Set the snapshot stream.

Video encode slice split: If this function is enabled, a smooth image can be obtained even 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.

2.1.3 Audio Configuration

Go to *Camera>Audio* as shown below.



Audio Encoding: G711A and G711U are selectable.

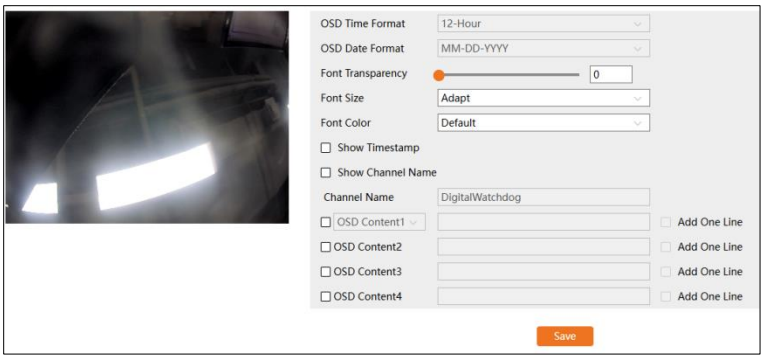
Audio Type: MIC or LINE. (If the internal MIC is used, choose "MIC". If you want to use an external line-level audio input device, choose "LINE".)

Audio Output (if supported): Talkback, Warning, or Auto can be optional. If "Talkback" is selected, the audio output will be used for two-way audio. If "Warning" is selected, the audio output will be used to play the predefined audio alarm. If "Auto" is selected, the system will output sound for two-way audio or warning voice as needed. But when warning and two-way audio are enabled simultaneously, two-way audio will be output first.

LINE IN/MIC IN/Audio Out Volume: Set the volume as needed.

2.1.4 OSD Configuration

Go to *Camera>OSD* as shown below.



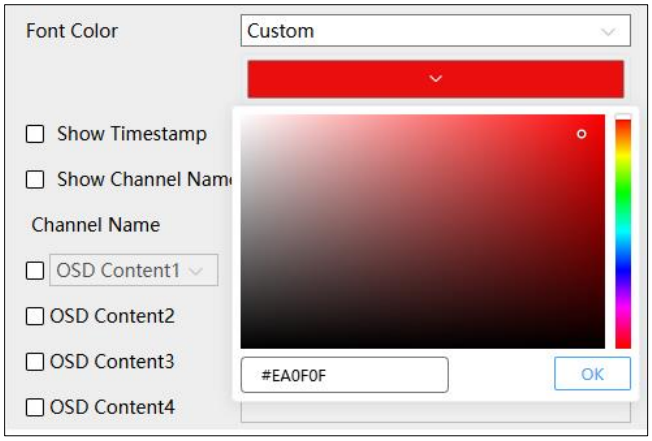
Set the OSD time format, OSD date format, OSD content and font transparency/size/color here. After enabling the corresponding display and entering the content, drag them to change their position. Then click the "Save" button to save the settings.

Note: The quantities of the OSD items are different for different models.

OSD Font Size: When the image resolution is less than 720P, the font size will be automatically changed to 16*16 and will not follow the font size you have set.

OSD Font Color: You can use the default font color (white) or customize the font color as needed.

To customize the font size and color:



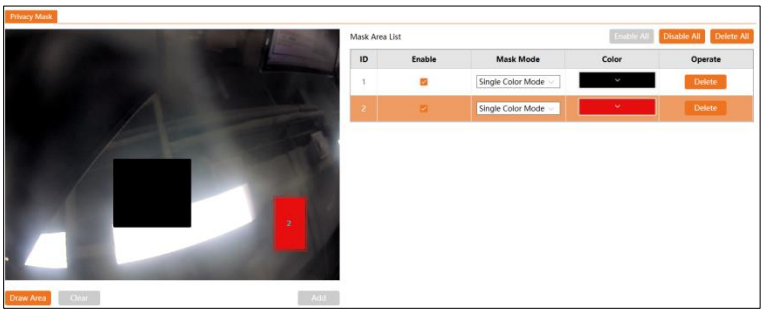
1. Select "Custom" and then click on the blank box under it.
2. Select a color on the color bar (right).
3. Click on the left color box to choose the desired color. Or you can directly enter the hexadecimal color code to set the color.
4. Click "OK" to save the font color settings.

Picture Overlap Settings (This function is only available for some models):

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

2.1.5 Privacy Mask

Go to *Camera>Privacy Mask* as shown below. A camera supports up to 4 separate privacy zones.

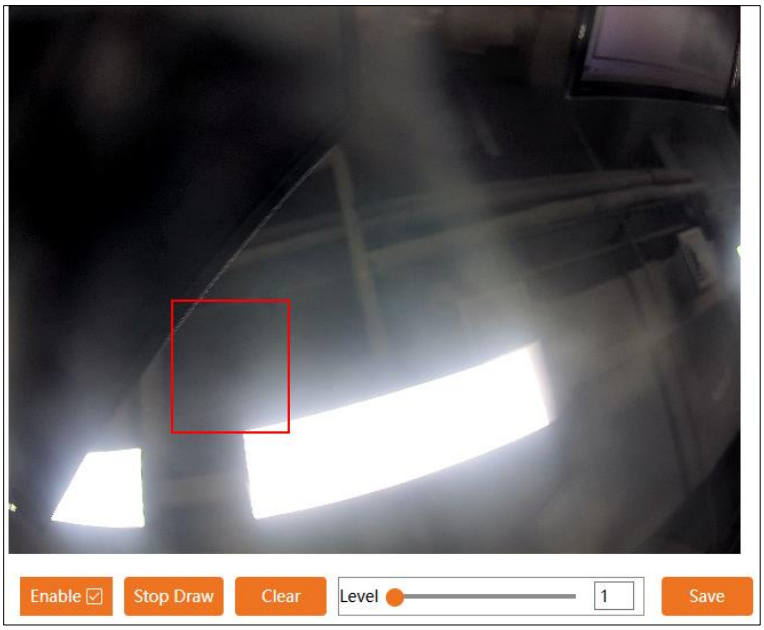


To set up a video mask:

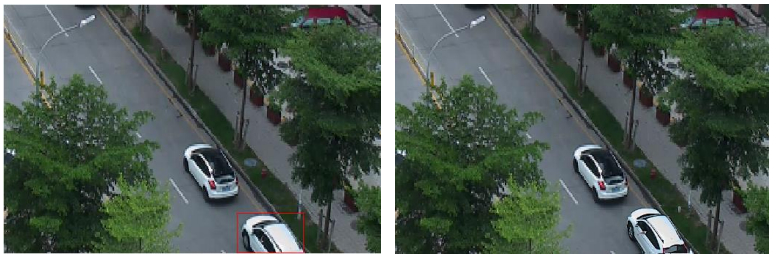
1. Click the “Draw Area” button and then drag the mouse on the left window to draw the video mask area.
2. Click the color block to select the desired color.
3. Enable/turn off the mask area as needed. After the video mask areas are set, you can turn on/off/delete mask areas as needed.
4. Return to the live view to verify that the area has been drawn as shown, as blocked out in the image.

2.1.6 ROI Configuration

Go to *Camera>ROI Config* 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.

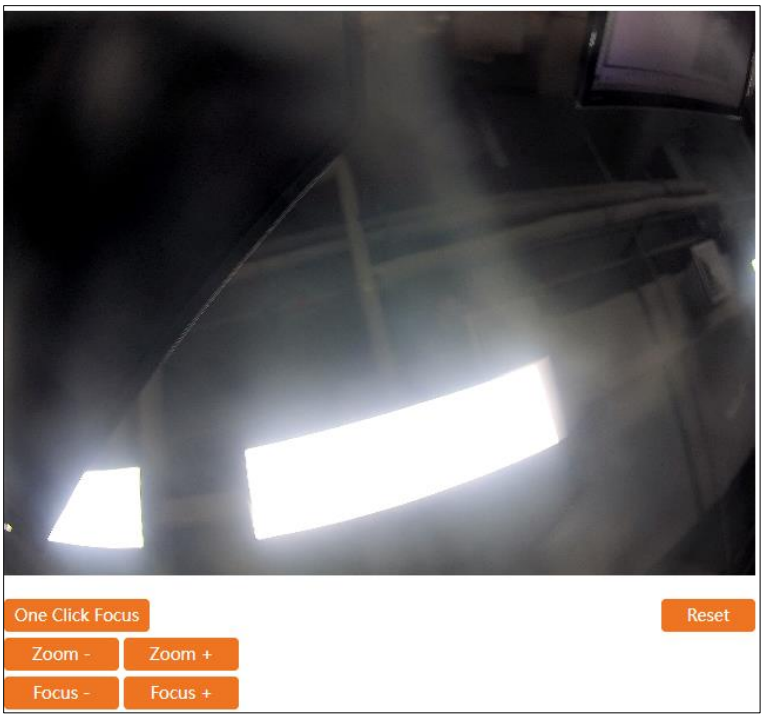


1. Check “Enable” and then click the “Draw Area” button.
2. Drag the mouse to set the ROI area.
3. Set the level.
4. Click the “Save” button to save the settings.



2.1.7 Zoom/Focus

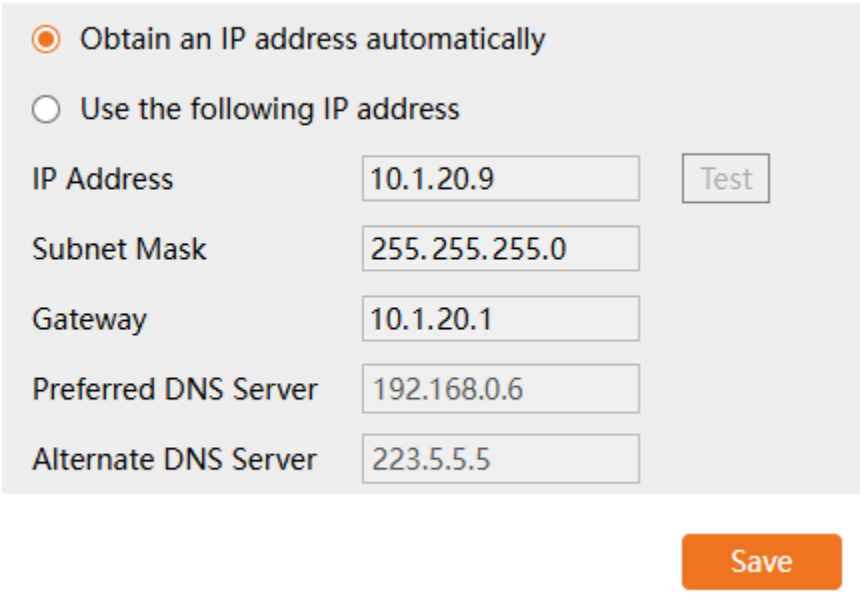
This function is only available for the model with a motorized zoom lens. Within this section, zoom and focus can be controlled. If the image is out of focus after a manual adjustment, one key can be used to set the focus automatically. Go to ***Setup>Camera> Zoom/Focus*** to set.



2.2 Network Configuration

2.2.1 IPv4

Go to *Setup>Network>IPv4*.



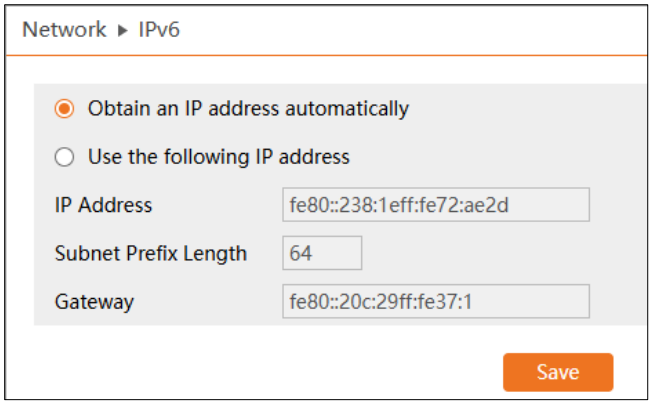
Use an IP address. There are two options for IP setup: obtain an IP address automatically via DHCP or use the following IP address. Please choose one of the options as needed.

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

2.2.2 IPv6

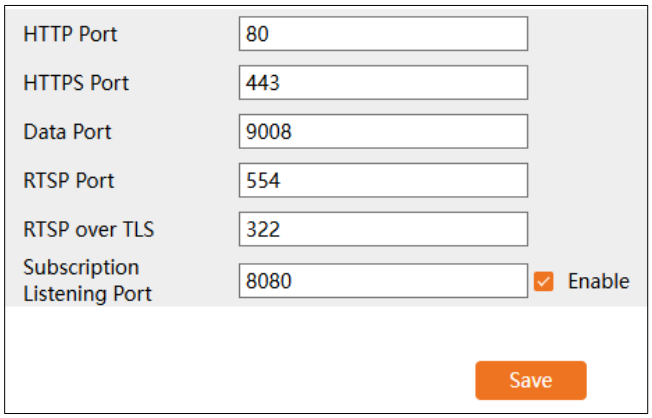
Go to *Setup>Network>IPv6*.

Use an IP address. There are two options for IP setup: obtain an IP address automatically by DHCP or use the following IP address. Please choose one of the options as needed.



2.2.3 Port

Go to *Setup>Network>Port* as shown below.



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

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

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

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

RTSP over TLS supports media stream transmission based on TLS channel encryption protection.

Subscription Listening Port: The port is used for a persistent connection of the third-party platform to push smart data.

2.2.4 DDNS

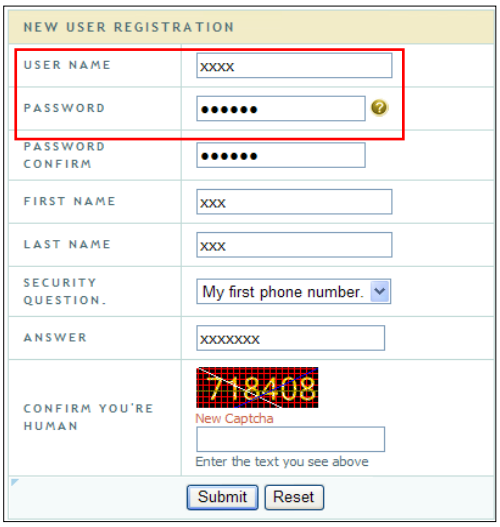
If the camera is set up with a DHCP connection, DDNS should be set for the internet.

1. Go to Setup>Network> DDNS.



2. Apply for a domain name. Take www.dvrdyndns.com, for example.

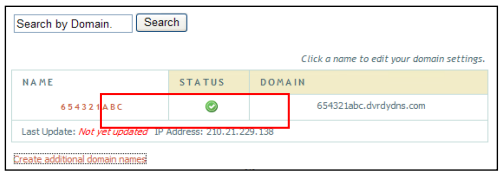
Enter www.dvrdydns.com in the web address bar to visit its website. Then click the “Registration” button.



Create a domain name.



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



3. Click “Edit” and then enter the username, password and domain you applied for in the DDNS Configuration interface.

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

2.2.5 SNMP

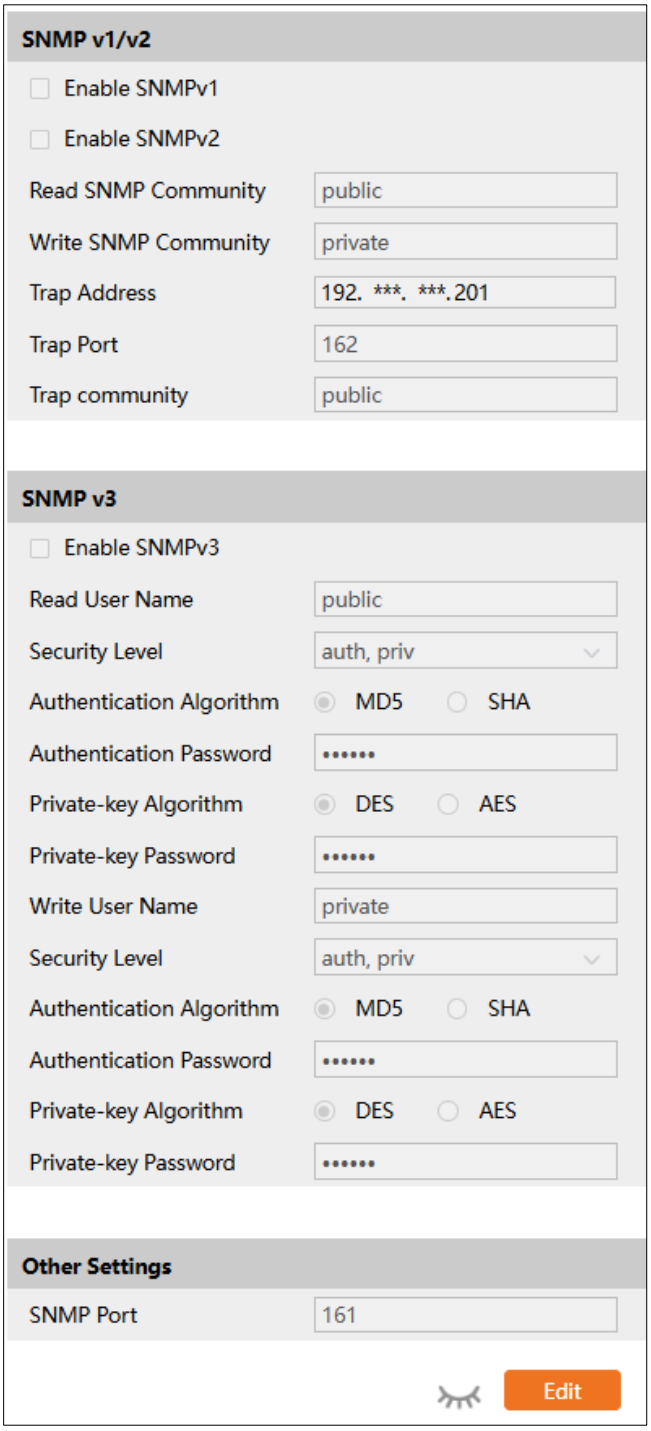
Only some models support this function.

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 SNMP parameters, such as the SNMP port and trap address.

1. Go to Setup>Network>SNMP.

2. Click “Edit” and then check the corresponding version checkbox (Enable SNMPv1, Enable SNMPv2, Enable SNMPv3) according to the version of the SNMP software that will be used.

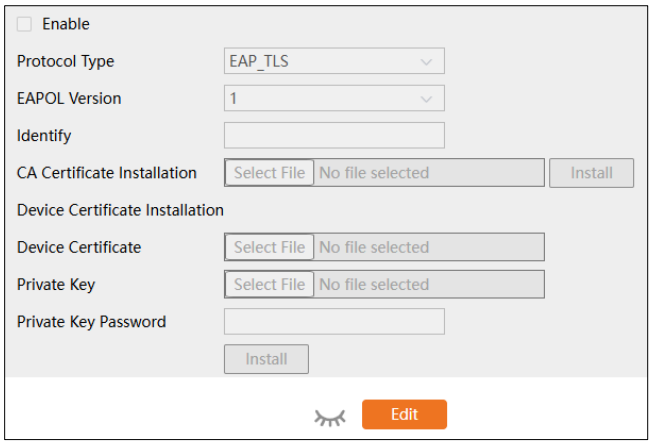
3. Set the values for “Read SNMP Community”, “Write SNMP Community”, “Trap Address”, “Trap Port” and so on. Please make sure the settings are the same as those of the SNMP software.



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

2.2.6 802.1x

If it is enabled, the camera's data can be protected. When the camera is connected to the network protected by IEEE 802.1x, user authentication is needed.



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

Click "Edit" to start the setup.

Protocol type: Choose "EAP_MD5" or "EAP_TLS" as needed.

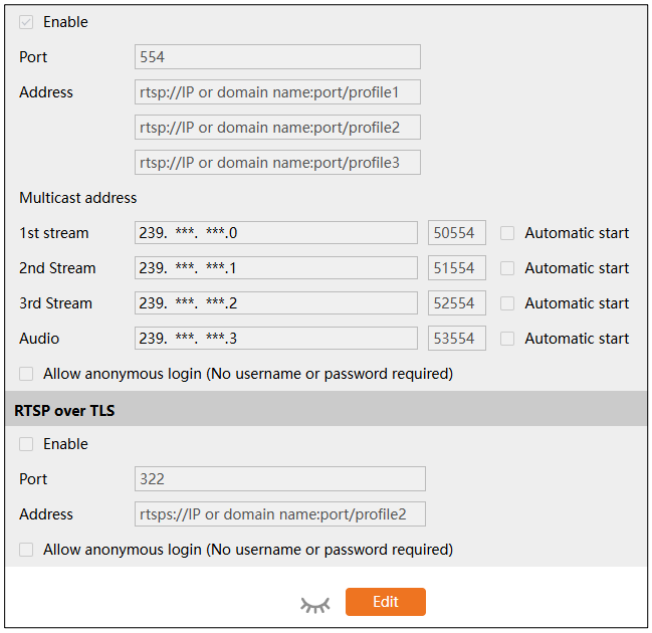
Select EAP-TLS as the EAP method. Enter your ID issued by the CA and then upload the related CA certificate, device certificate and private key. Before connecting the camera to the protected network with 802.1X, apply for a digital certificate from a Certificate Authority (i.e., your network administrator) that can be validated by a RADIUS server.

Select EAP_MD5 as the EAP method. You need to enter the username and password.

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

2.2.7 RTSP

Go to Setup→Network→RTSP.



Click "Edit" and then 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: After entering the main/sub stream in a VLC player, the video and audio will play automatically.

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

If "auto start" is enabled, the multicast received data should be added to a player (eg., VLC player) to play the video.

RTSP over TLS: Enable RTSP stream encryption by using TLS.

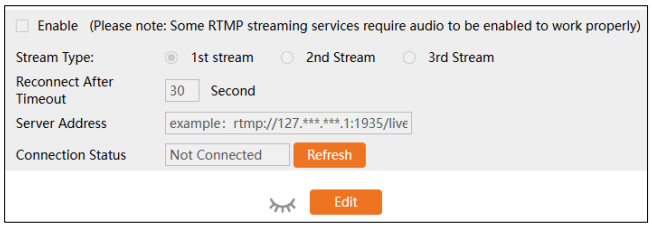
1. The IP address mentioned above cannot be an IPv6 address.

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

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

2.2.8 RTMP

You can access third parties (like YouTube) to realize live video viewing through the RTMP protocol. Go to *Setup>Network>RTMP*.



Click “Edit” and then check “Enable”, select the stream type and set the reconnection time after timeout and server address as needed.

Server address: Enter the server address allocated by the third-party server.

After that, click “Save” to save the settings. Then click “Refresh” to view the connection status.

2.2.9 UPnP

Only some models support this function.

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

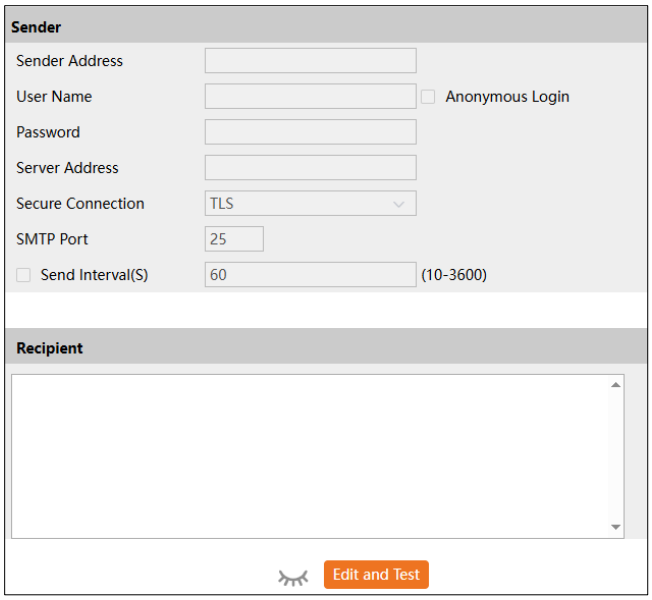
Go to *Setup>Network>UPnP*. Enable UPnP and then enter the UPnP name.



2.2.10 SMTP

If you need to trigger an E-mail when an alarm happens, or an IP address is changed, please set the E-mail here first.

Go to *Setup>Network>SMTP*.



Click “Edit and Test” to set the sender and the recipient.

Sender Address: sender’s e-mail address.

Username and password: sender’s username and password (you don’t have to enter the username and password if “Anonymous Login” is enabled).

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 for sending an e-mail. 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 e-mail will be sent. If one motion alarm event is triggered and then another motion detection alarm event is triggered after 60 seconds, two e-mails will be sent. When different alarms are triggered at the same time, multiple e-mails will be sent separately.

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

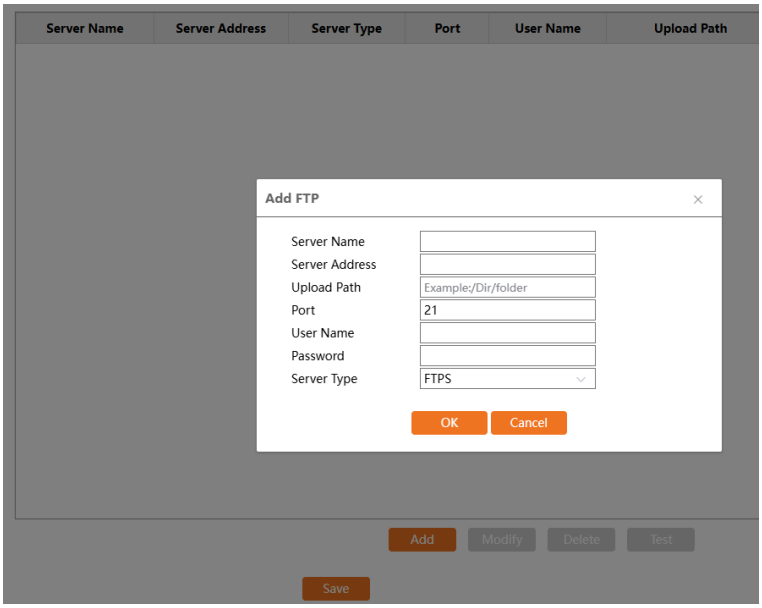
Recipient Address: receiver’s e-mail address.

2.2.11 FTP

Only some models support this function.

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

1. Go to *Setup>Network>FTP*.



2. Click “Edit and Test” and then click “Add” to add the information about the FTP server. After that, click “Save” to save the settings.

   Server Name: The name of the FTP server.

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

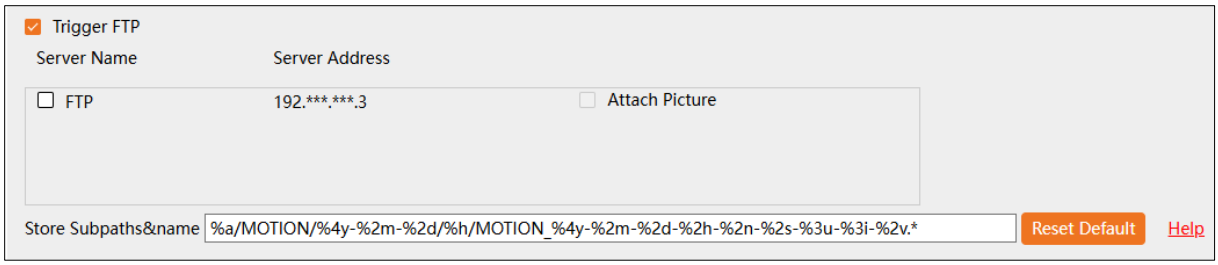
   Upload Path: The directory where files will be uploaded.

   Port: The port of the FTP server.

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

   Server Type: FTP or FTPS

3. In the event setting interface (like motion detection, perimeter intrusion, line crossing, etc.), trigger FTP as shown below.



If “Trigger FTP” and “Attach Picture” are checked, the captured pictures will be sent to the FTP server address.

Sub Storage Path& Name: Click “Help” to view the rule and then set it as needed.

Meanings of the default Path & Name Settings (taking motion detection as an example):

“%a/MOTION/%4y-%2m-%2d/%h” stands for the sub storage path

“MOTION_%4y-%2m-%2d-%2h-%2n-%2s-%3u-%3i.*” stands for the file name

When a motion alarm is triggered and “Trigger FTP” and “Attach Picture” are checked, a JPG file named “MOTION_Year Month Day Hour Minute Second_Event number” and a txt file named “MOTION_Year Month Day Hour Minute Second_Event number” will be generated under the FTP root directory> MAC address>MOTION>Year-Month-Day>Hour

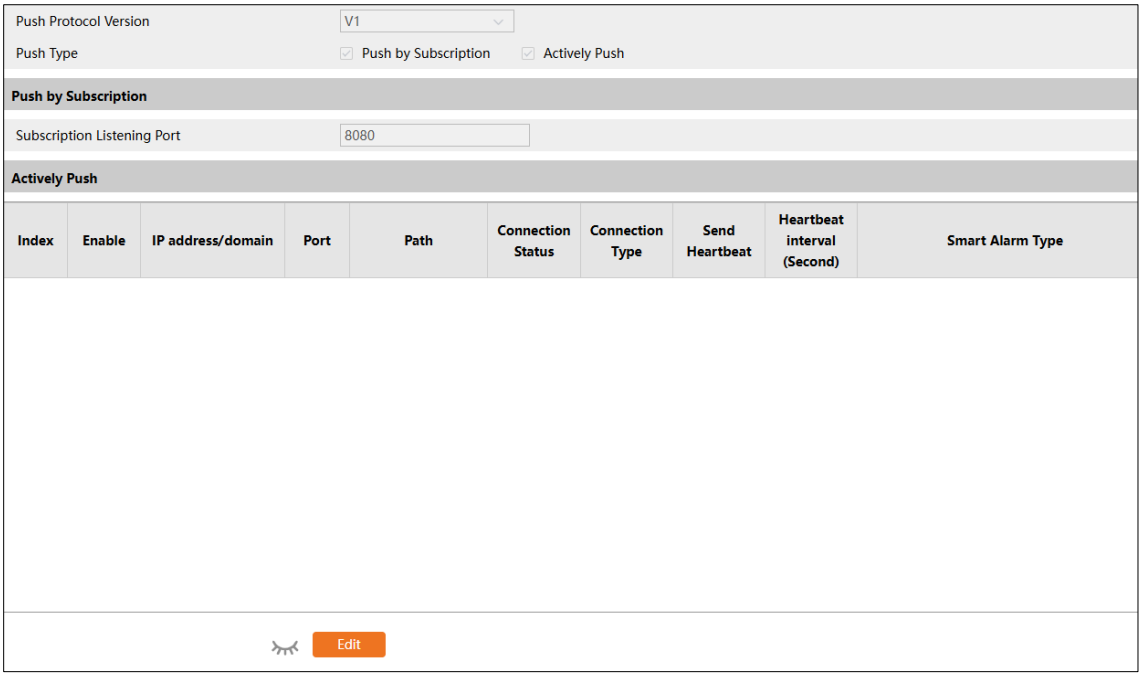
“MOTION” refers to the event type. You can modify the event name as needed (for example, Motion). You can also change the display order and contents of the sub storage path and file name.

If the sub storage path and name box are empty, the snapshot will be uploaded and named according to the default settings.

If you only enter the file name rule, the snapshot will be uploaded to the root directory of the FTP server.

2.2.12 HTTP Notification

Go to *Setup>Network >HTTP Notification.*



Click “Edit”.

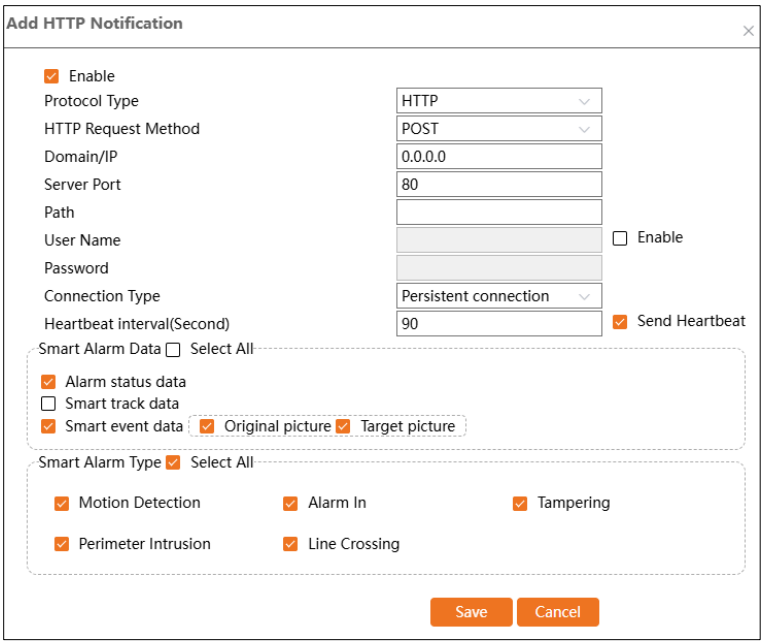
Push Protocol Version: Choose “V1” or “V2” as needed. It is recommended to use V2.

Push Type: “Push by Subscription” and/or “Actively Push” can be selected.

Push by Subscription: Push the target trajectory (moving coordinate) to the API test tool with a persistent connection. If enabled, the system will push the target trajectory upon detecting a target. If disabled, the system will push the target trajectory only when triggering a smart event (such as line crossing detection, region intrusion detection, etc.)

If the subscription listening port is occupied, you can modify it.

Actively Push: Click “Add” to add an HTTP notification.



Protocol type: HTTP

HTTP Request Method: Choose “POST” or “GET” as needed.

Domain/IP: The IP address/domain name of the third-party platform.

Server port: The server port of the third-party platform.

Path: Enter the subdomain of the above server; for example, the URL of alarm information push: “/SendAlarmStatus”.

Username and password: Please enable and enter as needed.

Connection Type: Choose “Persistent connection” or “Short connection” as needed. A persistent connection is always pushed with an established connection. A short connection will be disconnected after it is successfully pushed and re-established for the next push.

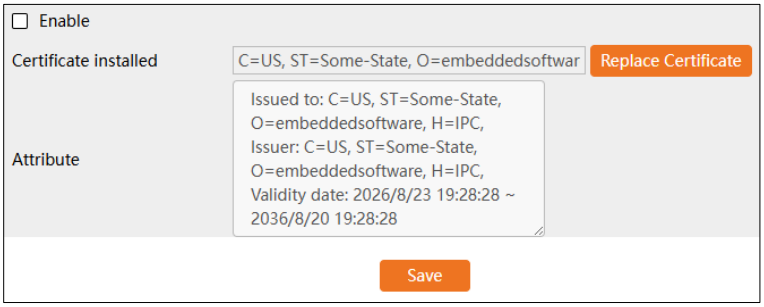
If “Persistent Connection” is selected, enable “Send heartbeat” and set the heartbeat interval as needed to maintain the connection. A short connection doesn’t have heartbeat sending or heartbeat interval options.

Enable “Send heartbeat” and set the heartbeat interval as needed. Check smart alarm data and type. After the above parameters are set, click “Save” to save the settings. Select one URL and click “Test” to test the connection to the URL. Then the camera will automatically connect to the third-party platform. The online status can be viewed in the above interface. After the camera is successfully connected, it will send the selected alarm data to the third-party platform once the selected smart alarm is triggered.

2.2.13 HTTPS

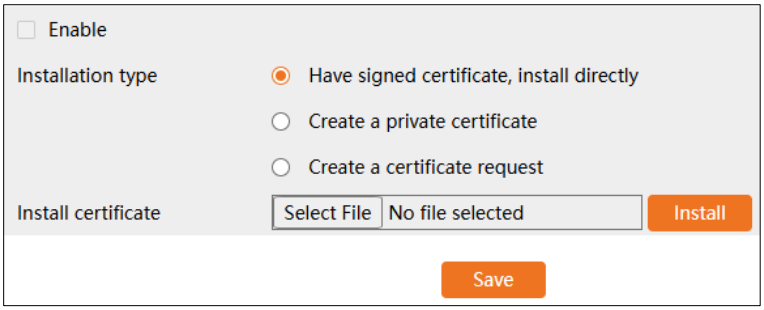
HTTPS provides authentication of the website and protects user privacy.

Go to ***Setup>Network>HTTPS*** as shown below.



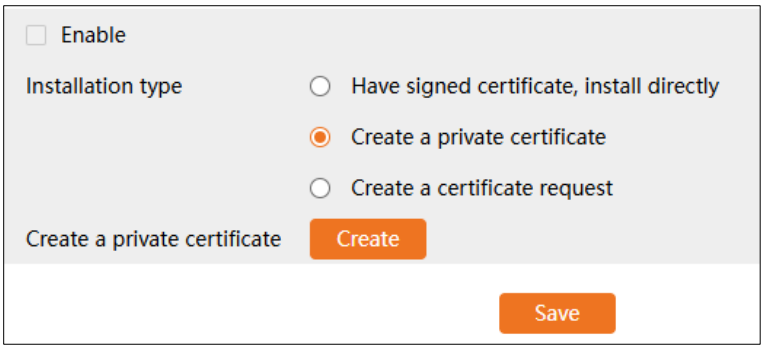
There is a certificate installed by default, as shown above. Enable this function and save it. Then the camera can be accessed by entering https://IP:port via a web browser (eg. https://192.168.226.201:443).

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



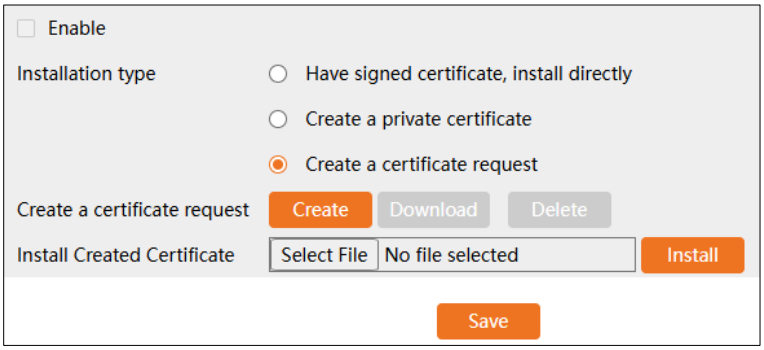
* If there is a signed certificate, click "Select File" to select it and then click "Install" to install it.

* 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.

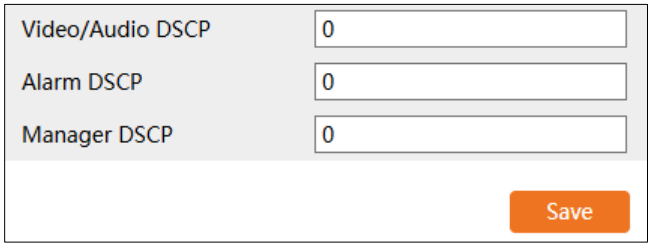


Click “Create” to create the certificate request. Then download the certificate request and submit it to the trusted certificate authority for signature. After receiving the signed certificate, import the certificate to the device.

2.2.14 QoS

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

Go to *Setup>Network>QoS*.



- **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.
- The larger the number is, the higher the priority is.

2.3 AI Event Options

2.3.1 Installation Guidelines and Recommendations

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 reflective surfaces (like shiny floors, mirrors, glass, lake surfaces and so on).

- Avoid places that are narrow or have too much shadowing.
- Avoid scenarios where the object's color is similar to the background color.
- At any time of day or night, please make sure the image from the camera is clear and has adequate, even lighting, avoiding overexposure or too much darkness on both sides.

2.3.2 Object Events

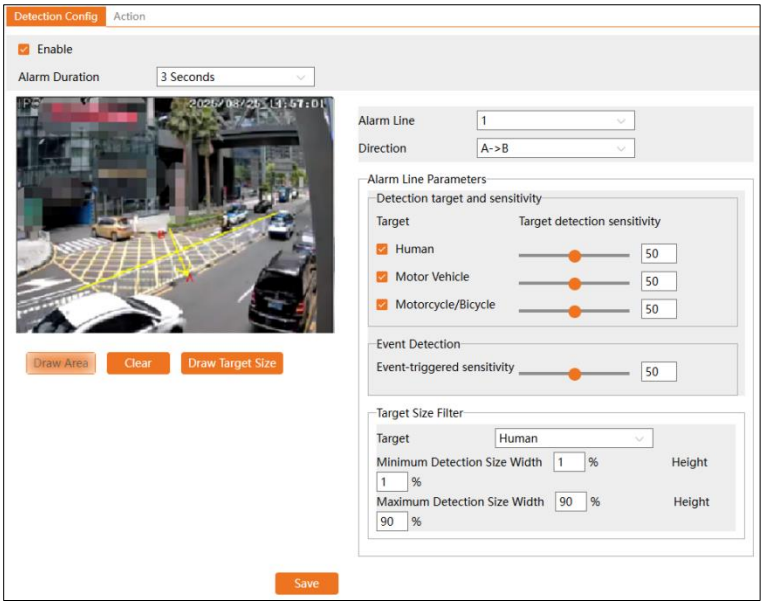
The camera supports two AI Event types: Face Recognition and Object Events. Only one can be selected at a time. The cameras ship with Object Events enabled by default. Object events can be used to detect, classify and track objects, humans and vehicles across detection lines and zones.

To enable Face Recognition, insert an SD card to establish the facial recognition database first, then enable facial recognition. The camera will reboot and be set to Face Recognition mode.

2.3.3 Line Crossing

Line Crossing: Alarms will be triggered if the target crosses the predefined alarm lines.

Go to S*etup>AI Event Options>Line Crossing* as shown below.



1. Enable line crossing detection.

2. Set alarm duration.

3. Set alarm lines, targets, sensitivity and target size filter for line crossing detection.

Set the alarm line number and direction. Four lines can be added. Multiple lines cannot be added simultaneously.

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

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

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

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

Click the “Draw 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.

Note: If the set rule line is very close to the edge of the screen, it may be difficult for the target to trigger the alarm. Please make sure that there is at least one full target-sized space between the rule line and the edge of the screen.

Detection Target:

Human: Select it, and then alarms will be triggered if someone crosses the predefined alarm lines.

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

Motorcycle/Bicycle: Select it, and then alarms will be triggered if a vehicle with two wheels (eg., a motorcycle or bicycle) crosses the predefined alarm lines.

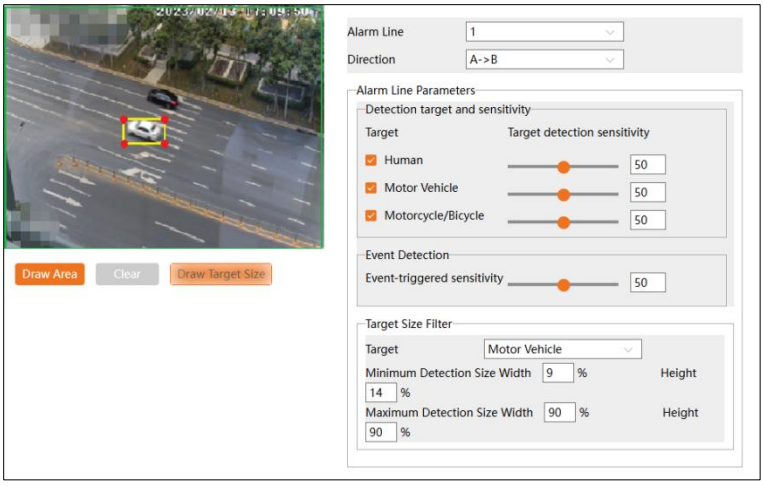
All three types of objects can be selected simultaneously. Please select the detection objects as needed. If no object/target is selected, alarms will not be triggered even if line crossing detection is enabled.

Target Detection Sensitivity: The higher the value, the easier it is for the alarm to be triggered by targets.

Event Triggered Sensitivity: It refers to the percentage of the body part of an object that goes across the alarm line. The higher the value of sensitivity is, the more easily the alarm can be triggered.

To set the target size filter:

Click “Draw Target Size” to draw the maximum and minimum sizes of a specific target as shown below.



Target: choose “Human”, “Motor Vehicle,” or “Motorcycle/Bicycle” as needed.

The green box is the maximum target detection box; the yellow box is the minimum target detection box.

Click the green box to edit the maximum target detection box; click the yellow box to edit the minimum target detection box.

Drag one of the four corners of the green or yellow box to change the box size. The corresponding size value on the right will be changed too. You can also enter a digital number to change the box size directly.

Click and drag the green or yellow box to move its position.

Finally, click “Save” to save the settings.

After the target size range is set, only the target whose size is between the minimum value and the maximum value can be detected.

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

5. Click “Action” to configure the alarm linkage items. The setup steps are the same as the sensor alarm. Please refer to Alarm In for details.

※ Configuration requirements of the camera and surrounding area

1. The auto-focusing function should not be enabled for line crossing detection.

2. Avoid scenes with many trees or 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. The recommended depression angle of the camera is from 30° to 45° (See Outdoor Mounting example).

For pedestrians, their heads and main bodies should be clearly visible in the video.



For vehicles, the depression angle should not be more than the recommended value. A sideways or horizontal viewing angle is recommended for a video (see below).



5. Make sure cameras can view objects for at least 2 seconds in the detected area for accurate detection.

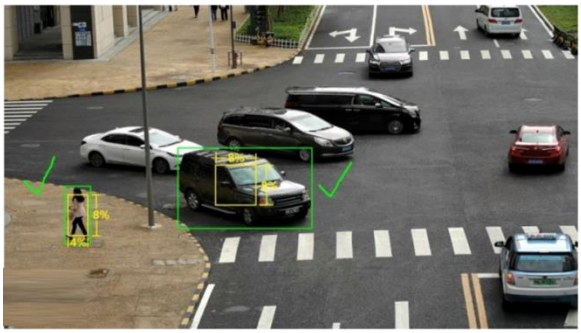
6. Adequate lighting and clear scenery are crucial for line crossing detection.

7. Please adjust the installation position or focus to meet the requirements of the target recognition size.

The recommended target recognition size:

Percentage	Human	Motor Vehicle	Motorcycle/Bicycle
Minimum Width × Height	4% × 8%	8% × 8%	4% × 4%
Maximum Width × Height	50%× 50%	50%× 50%	50%× 50%

Note: The percentage means that a target occupies that percentage of the entire image. For example: In a 1080P (1920×1080) video image, the minimum resolution of human is 80×160 (w =1920×4%=80, h=1920×8%=160).



Correct example



Wrong example

The target recognition box meets the minimum size requirements. The yellow box stands for the minimum recognition size. The green box stands for the set target box.

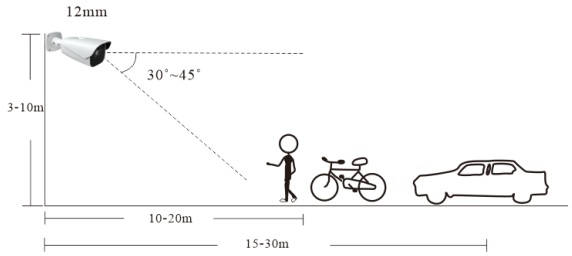
The yellow box stands for the minimum recognition size. The green box stands for the set target box. These two target recognition boxes don't meet the minimum size. Therefore, you need to adjust the camera position or focus as needed.

8. Installation suggestion:

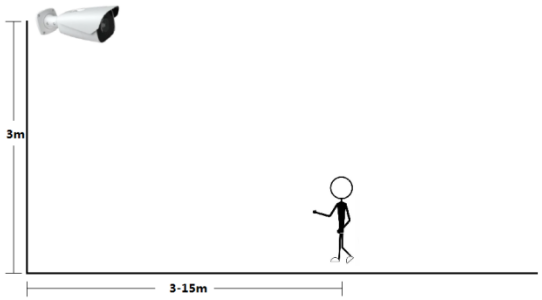
Outdoor mounting:

The optimal detection distance varies due to different focal lengths. Please refer to the following table.

Focal Length	Installation Height(m)	Human/Motorcycle/Bicycle		Motor Vehicle	
		Maximum Distance(m)	Optimal Distance(m)	Maximum Distance(m)	Optimal Distance(m)
2.8mm	3-10	8	4-8	15	10-15
3.6mm	3-10	10	5-10	20	15-20
12mm	3-10	25	10~20	35	15~30
22mm	3-10	45	30~40	70	20~50



Example for 12mm focal length

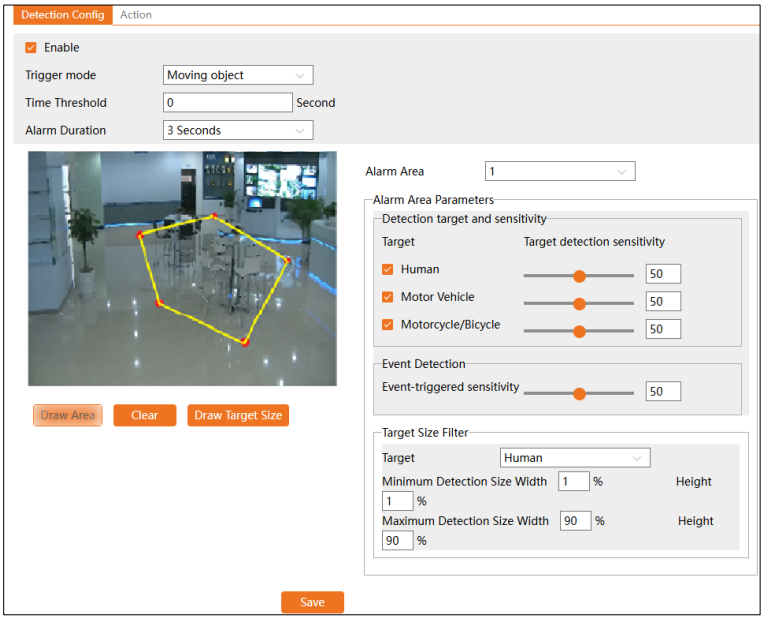


Indoor Mounting

2.3.4 Perimeter Intrusion

Perimeter Intrusion: Alarms will be triggered if the target enters and stays in the predefined areas. This function can be applied to important supervision places, danger areas and prohibited areas, like military administrative zones, high-danger areas, no-man's areas, etc.

Go to ***Setup> AI Event Options> Perimeter Intrusion***, as shown below.



1. Enable perimeter intrusion detection and the detection target.

2. Set trigger mode, time threshold and alarm duration.

Trigger Mode: Choose "Moving object" or "All objects" as needed. If "Moving object" is selected, alarms will be triggered when an object intrudes into the predefined area; if the object stops moving on the alarm line, the region intrusion alarm stops too. If "All objects" is selected, alarms will be triggered when an object remains still on the alarm line or intrudes into the predefined area.

Time Threshold: It refers to the threshold for the time the object/target stays in the region. If an object entering and staying in the predefined area exceeds the time threshold, alarms will be triggered.

Alarm duration: It is the time that the alarm remains active after an alarm ends.

3. Set alarm areas, targets, sensitivity and target size filter for region intrusion detection.

Set the alarm area number. Four alarm areas can be added.

Click the "Draw Area" button and then click around the area where you want to set the alarm area in the image (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.

Note: If the set rule line is very close to the edge of the screen, it may be difficult for the target to trigger the alarm. Please make sure that there is at least one full target-sized space between the rule line and the edge of the screen.

Detection Target:

Human: Select it, and then alarms will be triggered if someone intrudes into the predefined area.

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

Motorcycle/Bicycle: Select it, and then alarms will be triggered if a vehicle with two wheels (eg., a motorcycle or bicycle) intrudes into the predefined area.

All three types of objects can be selected simultaneously. Please select the detection objects as needed. If no object/target is selected, alarms will not be triggered even if intrusion detection is enabled.

Target Detection Sensitivity: The higher the value, the easier it is for the alarm to be triggered by targets.

Event Triggered Sensitivity: It refers to the percentage of the body part of an object that enters the alarm area. The higher the value of sensitivity is, the more easily the alarm can be triggered.

Target size filter setup: The setup steps of the target size filter are the same as the line crossing target size filter setup (See Line Crossing for details).

5. Click “Action” to configure the alarm linkage items. The setup steps are the same as the sensor alarm. Please refer to Alarm In for details.

※ Configuration requirements of the camera and surrounding area

The requirements are similar to line crossing detection. Please refer to the Configuration requirements of the camera and the surrounding area for line crossing detection for details.

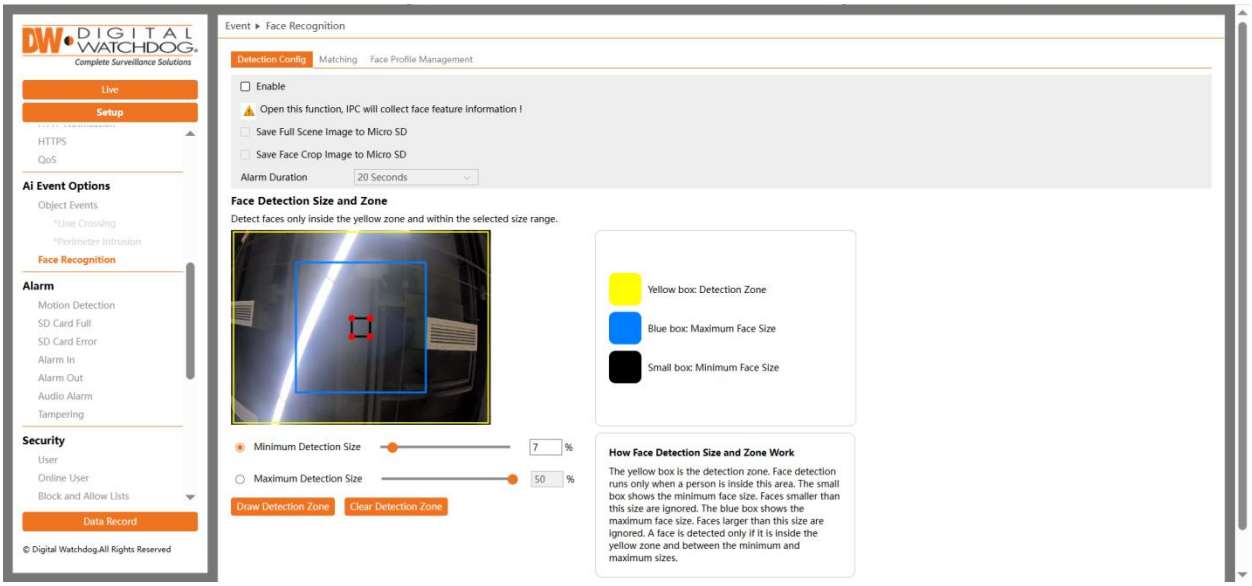
2.3.5 Face Recognition

The face detection function detects, classifies, and tracks faces appearing in the monitoring scene. Alarms will be triggered when a face is detected, and the face will be compared to the face profile database for possible matches.

Note: If you plan to use the camera for face detection, install an SD card in the camera **before** enabling the Face Recognition AI Event.

The setting steps are as follows:

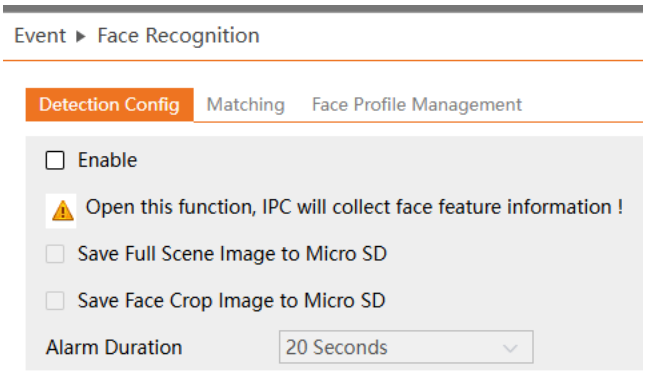
1. Go to *Setup>AI Event Options>Face Recognition* as shown below.



2. Enable the face detection function.

Save Source Information to SD Card: If checked, the whole picture will be saved to the SD card when a face is detected.

Save Face Information to SD Card: If checked, the captured face picture will be saved to the SD card when a face is detected.



3. Set the alarm duration.

4. Set the alarm detection area.

Click “Draw Area” and drag the border lines of the rectangle to modify its size. Move the rectangle to change its position. Click “Stop Draw” to stop drawing the area. Click “Clear” to clear the area. Then set the detectable face size by defining the maximum value and the minimum value (The default size range of a single face image is from 3% to 50% of the entire image).

5. Set face comparison trigger options. Click “Comparison” to go to the following interface.

Similarity threshold: When the similarity of the captured face picture and the face picture added to the face database exceeds the similarity threshold, alarms will be triggered.

Push Unregistered Face Event: Push the comparison alarm information of the stranger. After it is enabled, the comparison information of the stranger will be shown in the left comparison area of the live interface.

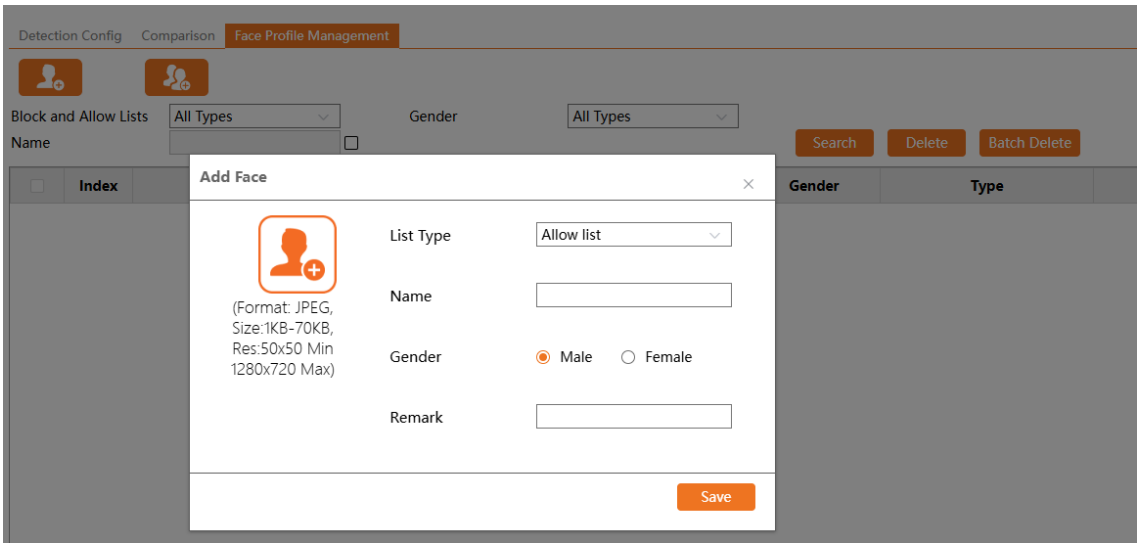
Interval of Detection: Within the set period, delete repeated comparison results. If 30 seconds is selected, the camera will capture the same target once every 30 seconds during its continuous tracking period.



Select the list type and then check the alarm action options. Actions will be triggered when the captured face is matched successfully with the face image of the selected list.

6. Face profile management.

Click the “Face Profile Management” tab. This will open the following interface.



There are four ways to add face pictures.

1. Adding face pictures one by one

Click  to pop up an add user box. Then click  to select a face picture saved on the local PC. Please select the picture according to the specified format and size limit. After that, fill out the relevant information for the face picture and click “Save” to add it.

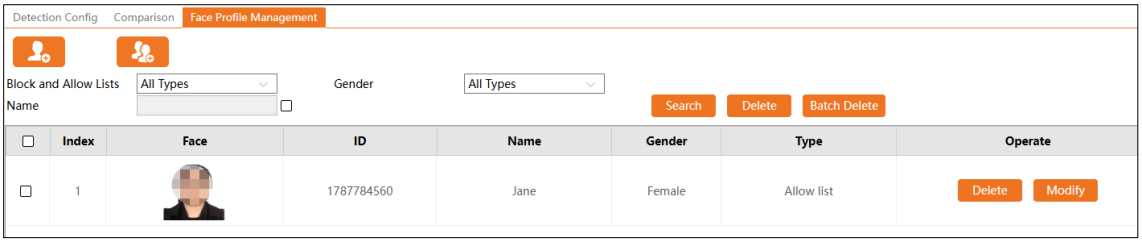
2. Adding face pictures in bulk

   Click  and then add multiple face pictures at once according to the prompted rules.

3. Add face pictures by using the face album management tool

4. Add the captured picture in live mode (See ***Add captured face pictures to the face database***).

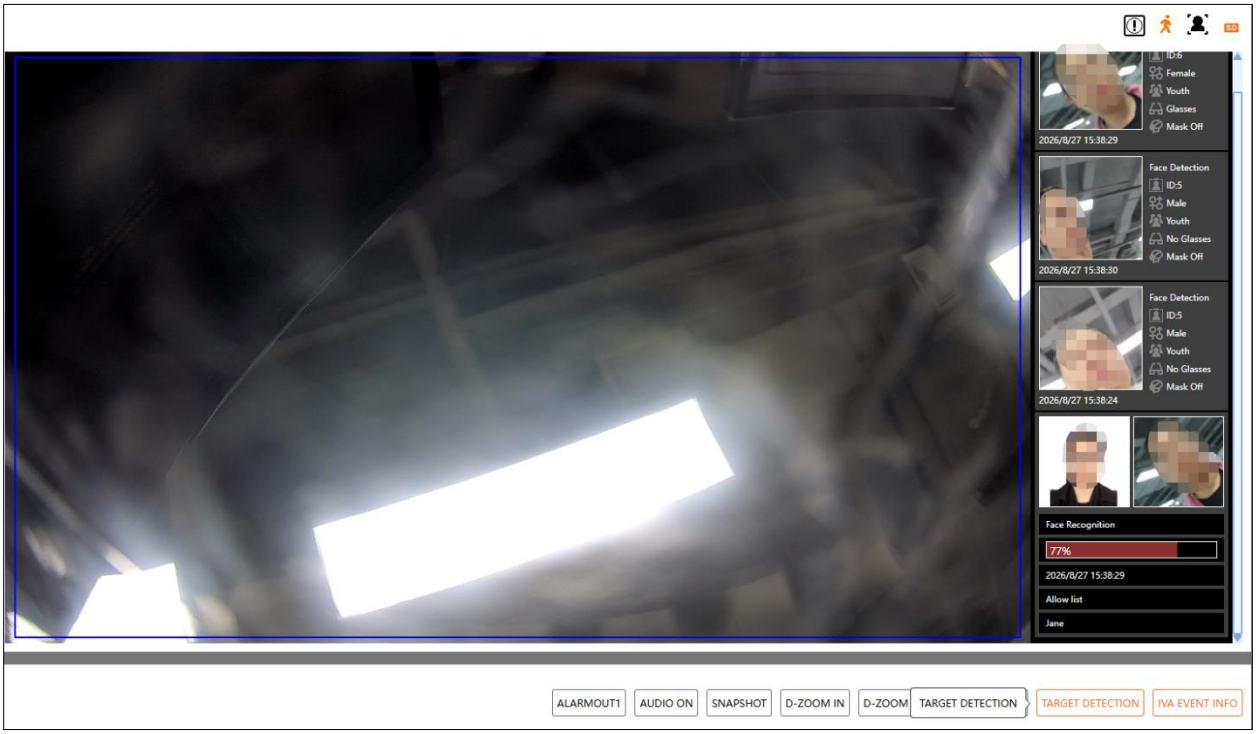
After adding face pictures, you can search for them by name, gender and so on.



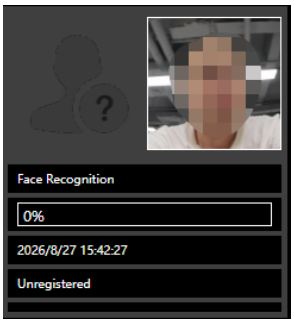
Click “Modify” to change the person’s information, and click “Delete” to delete this face picture.

Face Match View

After all face comparison settings are set successfully, enter the live view interface. Click “TARGET DETECTION” to view the captured face pictures and face comparison information.

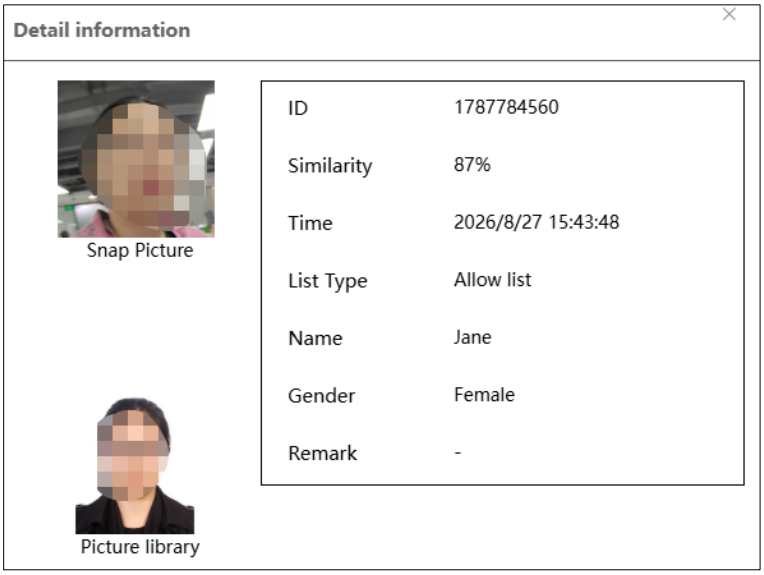


You can view the detailed face comparison information, such as the similarity, capture time, list type, etc. If “Push Unregistered Face Event” is enabled, the stranger comparison information will be displayed as shown below.



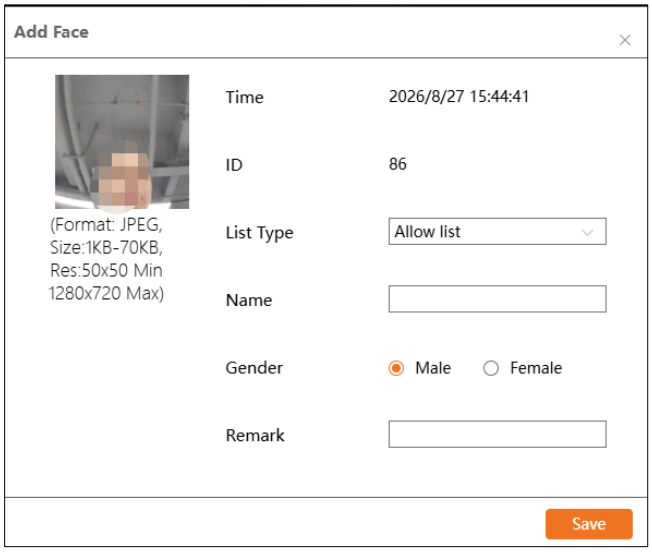
View the comparison details.

In area ②, click the compared face picture to bring up the following window. In this interface, you can view the detailed comparison information.



Add captured face pictures to the face database

Click a captured picture. This will bring up a face picture adding box.



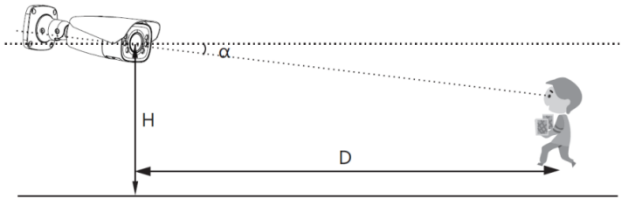
Fill out the relevant information and click “Save” to add this face picture.

※ Configuration requirements of the camera and the surrounding area

1. Cameras must be installed in an area with stable and adequate light sources.

2. The installation height ranges from 2.0m to 3.5m, adjustable according to the focal length of different lenses and object distances.

3. The depression angle of the camera should be less than or equal to 15°.



4. The object distance depends on the focal length of the lens mounted in the camera.

5. In order to guarantee the captured face recognition rate, the requirements for face capture are: the left or right turn angle is less than about 30°; the pitching angle is less than 20°.

6. Face illumination must be uniform; if the brightness is low or there is a large area of shadow, light filling is needed.

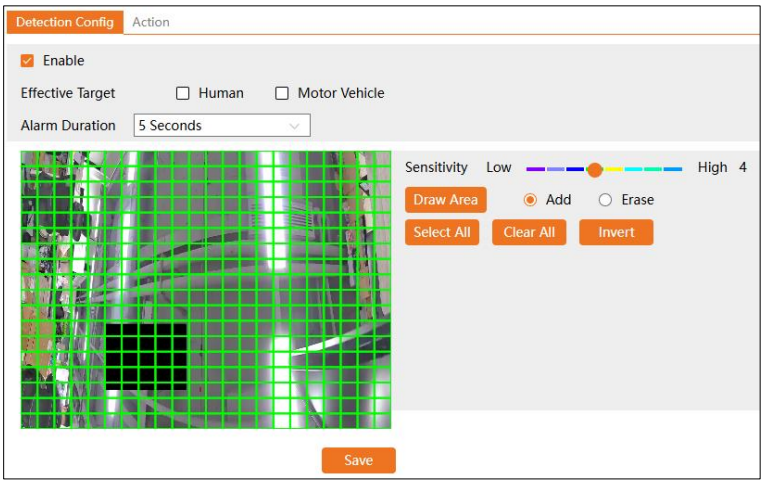
7. When dealing with backlight scenarios, enabling BLC, HLC, or WDR can help improve video quality and visibility. These features compensate for extreme lighting conditions and ensure better surveillance results.

8. The following scenes are not applicable, such as crowded scenes (airport, railway station, square, etc.), and so on.

2.4 Alarm Configuration

2.4.1Motion Detection

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



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.

   a. **Effective Target**: Choose “Human” or “Motor Vehicle”. If “Human/Motor Vehicle” is enabled, the camera will only detect the movement of a human/motor vehicle. If no target is enabled, alarms will be triggered when a moving object appears in the image, including a human, a vehicle or other moving objects. (Some models only support “Human”).

   Note: If Face Recognition is enabled, this option will not be available.

   b. **Alarm duration**: It refers to the time that the alarm remains active after an alarm ends. The default duration is 5 seconds. If the alarm duration is set to 10 seconds, once the camera detects motion, an alarm will be activated once, and no additional motion will be detected for 10 seconds. If another motion is detected during this period, it will be considered continuous movement; otherwise, it will be considered a single motion.

2. Set motion detection area and sensitivity.

   a. Clear all grids. Then move the “Sensitivity” scroll bar to set the sensitivity. A higher sensitivity value means that motion will be triggered more easily.

   b. 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.

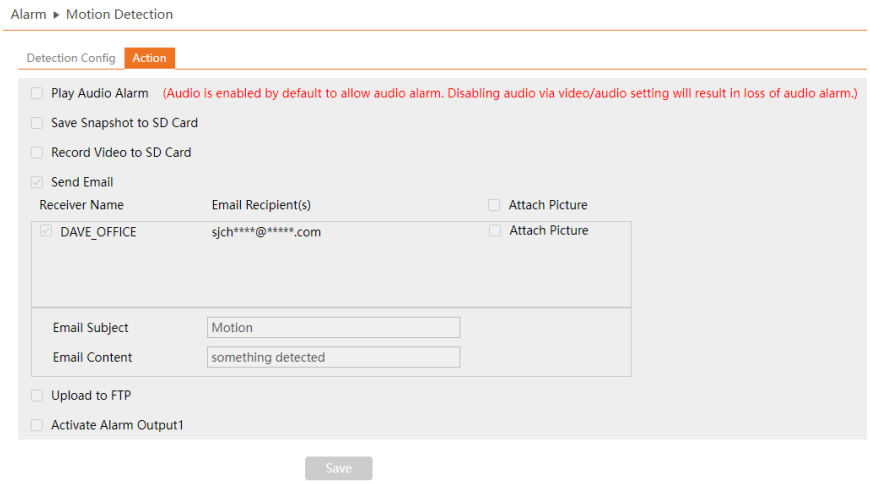
   c. You can set different sensitivity levels for different areas.

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

Note:

* Areas without colored grids mean the sensitivity is 0 and are considered blocked areas.
* After detecting a moving object in the detection area, an alarm will be triggered when the number of red grid lines exceeds the threshold of the sensitivity level.

3. Click “Action” to configure the alarm linkage items.



Play Audio Alarm: A warning sound will be played when a motion-based alarm is triggered. After checking it, select the voice file. If "Default" is selected, the audio file is the sound set in the audio alarm interface (see Audio Alarm for details). If "Specified" is selected, you can specify the warning voice and language for the motion alarm. (Only some models support this function)

Save Snapshot to SD Card: The system will capture images on motion detection and save the images on the SD card in the camera (card is not included).

Record Video to SD Card: Video will be recorded on the SD card in the camera when motion is detected (card not included).

Send E-mail: Send a notification when motion is detected to an e-mail address (a sender's e-mail must be set first in the E-mail Configuration interface). Check the box next to "Attach Picture" to include an image of the motion event with the e-mail.

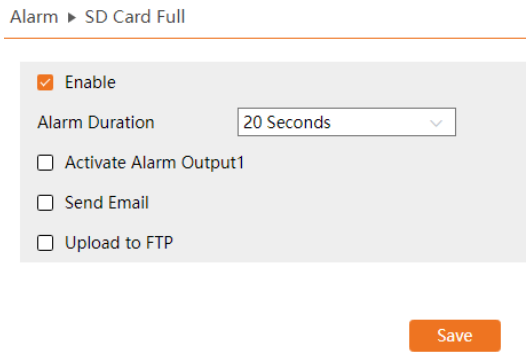
Upload to FTP: When motion is detected, the captured pictures will be sent to the FTP server address. You can set the sub storage path and name as needed. See FTP Configuration for more details.

Activate Alarm Output1: When motion is detected, an external relay output connected to the camera will be activated.

After that, click "Save" to save the settings.

2.4.2 SD Card Full

1. Go to *Setup>Alarm>SD Card Full*.



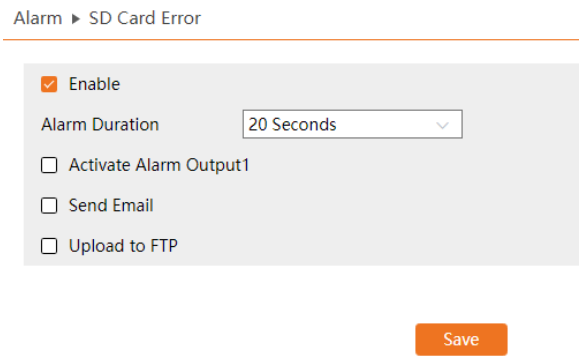
2. Click “Enable”.

3. Set the alarm duration and alarm trigger options. Users can also activate an alarm output, send an e-mail or upload an alert to a set FTP server as needed. The setup steps are the same as for motion detection. Please refer to Motion Detection for details.

2.4.3 SD Card Error

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

1. Go to *Setup>Alarm>SD Card Error*.



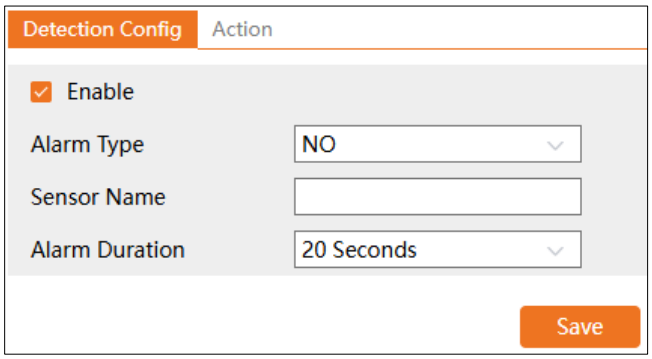
2. Click “Enable”.

3. Set the alarm duration and alarm trigger options. Trigger alarm out, E-mail, and FTP as needed. The setup steps are the same as for motion detection. Please refer to Motion Detection for details.

2.4.4 Alarm In

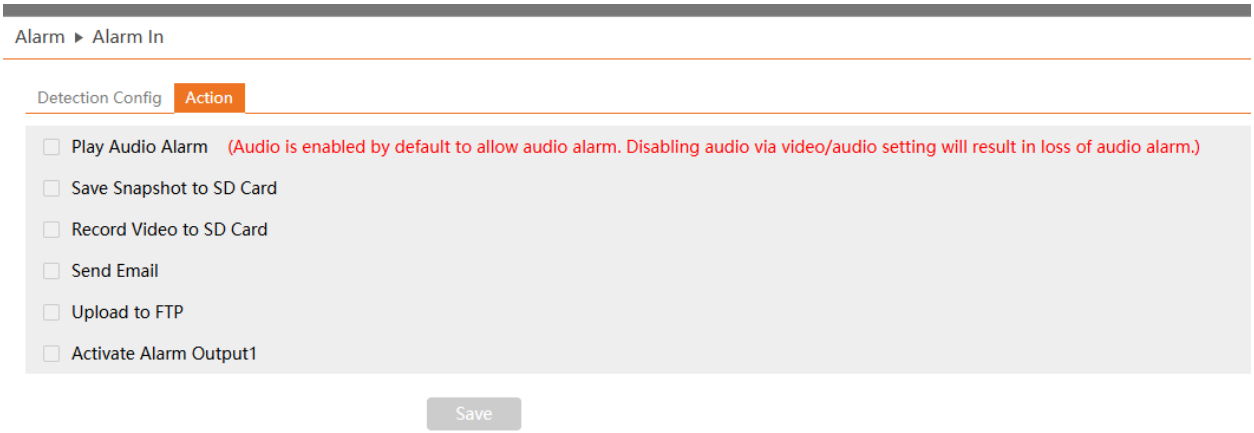
This function is only available for some models. To set the sensor alarm (Alarm In):

Go to *Setup>Alarm>Alarm In* as shown below.



1. Click “Enable” and set the alarm type, alarm duration and sensor name.

2. Click “Action” to configure the alarm linkage items.



Play Audio Alarm: A warning sound will be played when a motion-based alarm is triggered. After checking it, select the voice file. If “Default” is selected, the audio file is the sound set in the audio alarm interface (see Audio Alarm for details). If “Specified” is selected, you can specify the warning voice and language for the motion alarm. (Only some models support this function)

Save Snapshot to SD Card: The system will capture images on motion detection and save the images on the SD card in the camera (card is not included).

Record Video to SD Card: Video will be recorded on the SD card in the camera when motion is detected (card not included).

Send E-mail: Send a notification when motion is detected to an e-mail address (a sender’s e-mail must be set first in the E-mail Configuration interface). Check the box next to “Attach Picture” to include an image of the motion event with the e-mail.

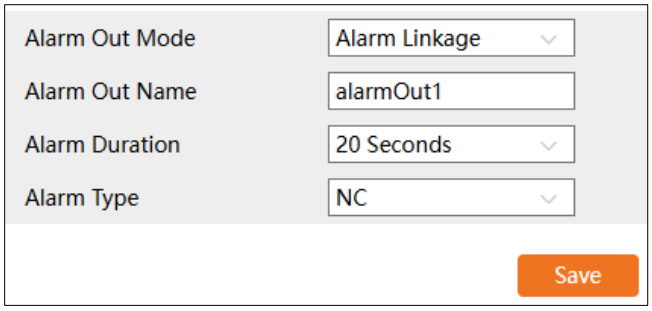
Upload to FTP: When motion is detected, the captured pictures will be sent to the FTP server address. You can set the sub storage path and name as needed. See FTP Configuration for more details.

Activate Alarm Output1: When motion is detected, an external relay output connected to the camera will be activated.

After that, click "Save" to save the settings.

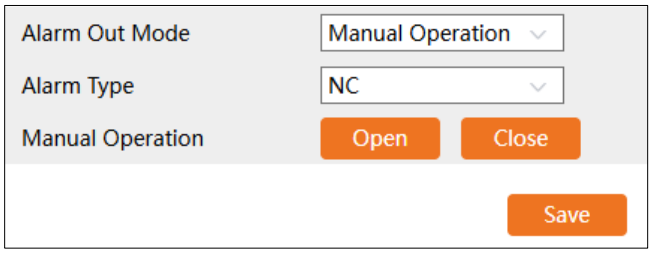
2.4.5 Alarm Out

This function is only available for some models. Go to ***Setup>Alarm>Alarm Out***.

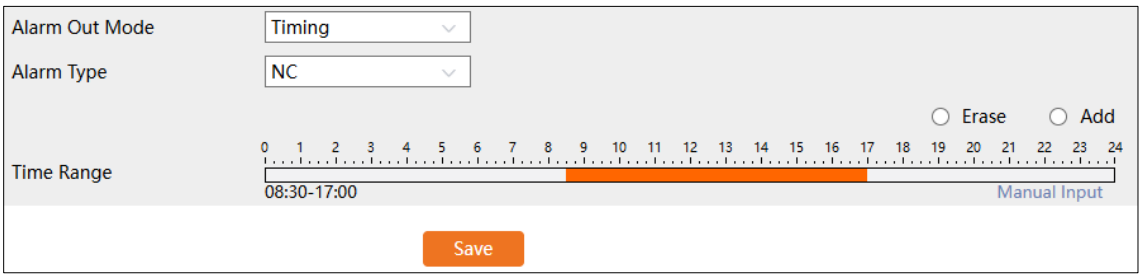


Alarm Out Mode: Alarm linkage, manual operation, day/night switch linkage and timing are optional.

- **Alarm Linkage**: After selecting this mode, select the alarm out name, alarm duration at the "Alarm duration" drop-down list box and alarm type.
- **Manual Operation**: After selecting this mode, select the alarm type and click "Open" to trigger the alarm out immediately; click "Close" to stop the alarm.



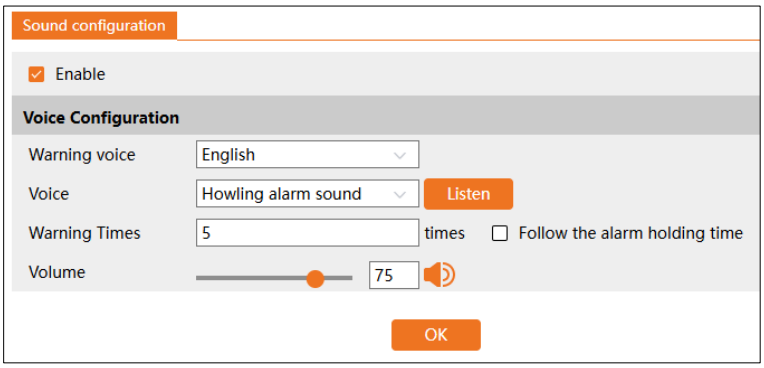
- **Timing**: Select the alarm type. Then click "Add" and drag the mouse on the timeline to set the alarm schedule; click "Erase" and drag the mouse on the timeline to erase the set schedule. After this schedule is saved, the alarm will be triggered at the specified time.



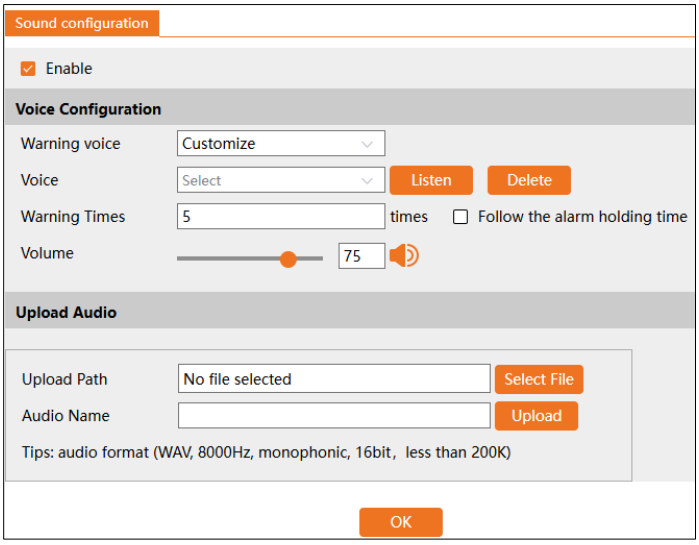
2.4.6 Audio Alarm

Go to *Alarm>Audio Alarm* as shown below.

Enable audio alarm. Audio needs to also be enabled in the audio configuration interface, or the warning voice cannot play either.



- Select the warning voice. Select "English" to view a drop-down of alarm sounds and voices included with the camera.
- Select "Customize" to upload your own alarm sound. Click "Select File" or "Browse" to choose the audio file you want to upload, and then enter the audio name. Click "Upload" to upload the audio file.
- After you upload the audio file, you can select the audio name from the audio list and click "Listen" to listen to it. Click "Delete" to delete the audio.
- **Follow the alarm holding time:** The warning voice will stop when the alarm duration ends.

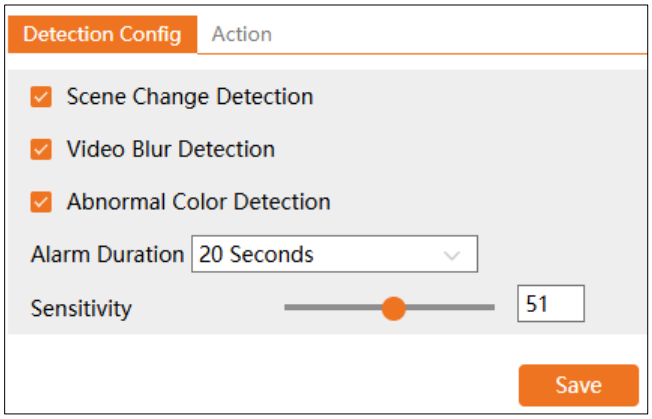


- Set the alarm's volume from 1 to 100.
- Click "OK" to save the settings.

2.4.7 Tampering

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

1. Go to *Setup>Alarm>Tampering* as shown below.



2. Check the box next to the events you want to enable.
    a. **Scene Change Detection**: Alarms will be triggered if the scene of the monitored video has changed.
    b. **Video Blur Detection**: Alarms will be triggered if the video becomes blurry.
    c. **Abnormal Color Detection**: Alarms will be triggered if the image is abnormal due to color deviation.
3. Set the alarm duration from the available drop-down options.
4. Set the sensitivity of the tampering detection (default is 51).
    a. **The sensitivity value of Scene Change Detection**: The higher the value is, the more sensitive the system is to the amplitude of the scene change.
    b. **The sensitivity value of Video Blur Detection**: The higher the value, the more sensitive the system is to the blurriness of the image.
    c. **The sensitivity value of Abnormal Color Detection**: The higher the value, the more sensitive the system is to the color shift of the image.
5. Click "Save" to save the settings.
6. Click "Action" to configure alerts the camera can send once tampering is detected. The setup steps are the same as for motion detection. Please refer to Motion Detection for details.

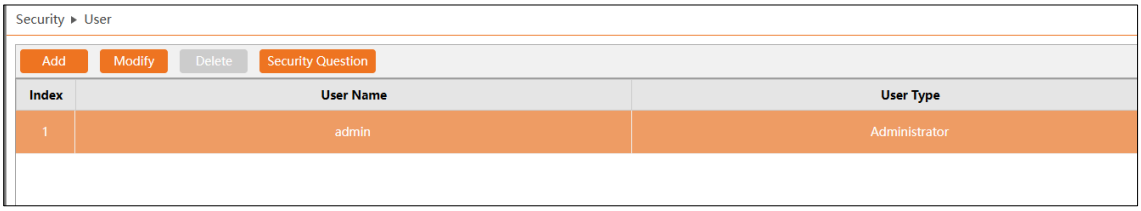
Note: Requirements for the camera and surrounding area:

1. The auto-focus should not be enabled for exception detection.
2. In scenes where the lighting conditions change drastically throughout the day, tampering detection may not be accurate.
3. Contact your installer for more detailed application scenarios.

2.5 Security Configuration

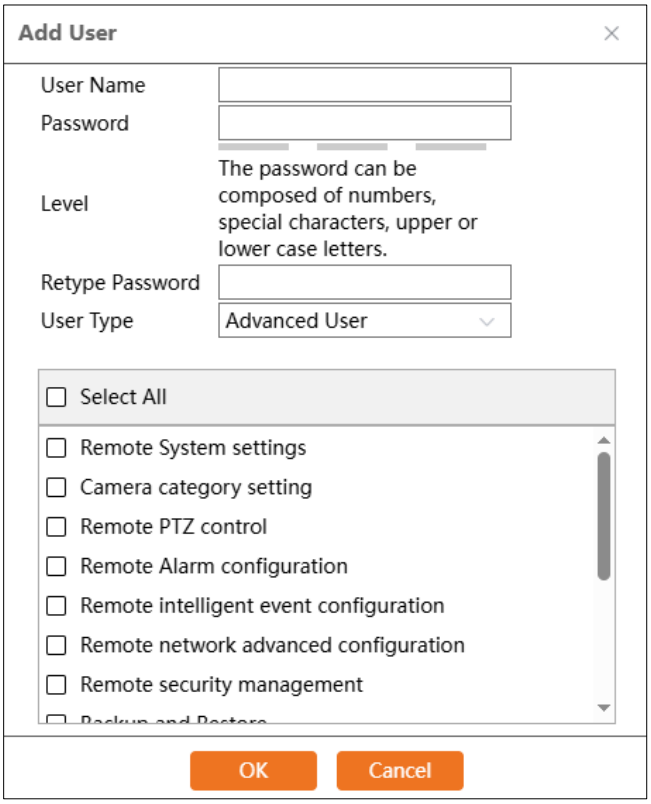
2.5.1 User Configuration

Go to **Setup>Security>User** as shown below.



Add user:

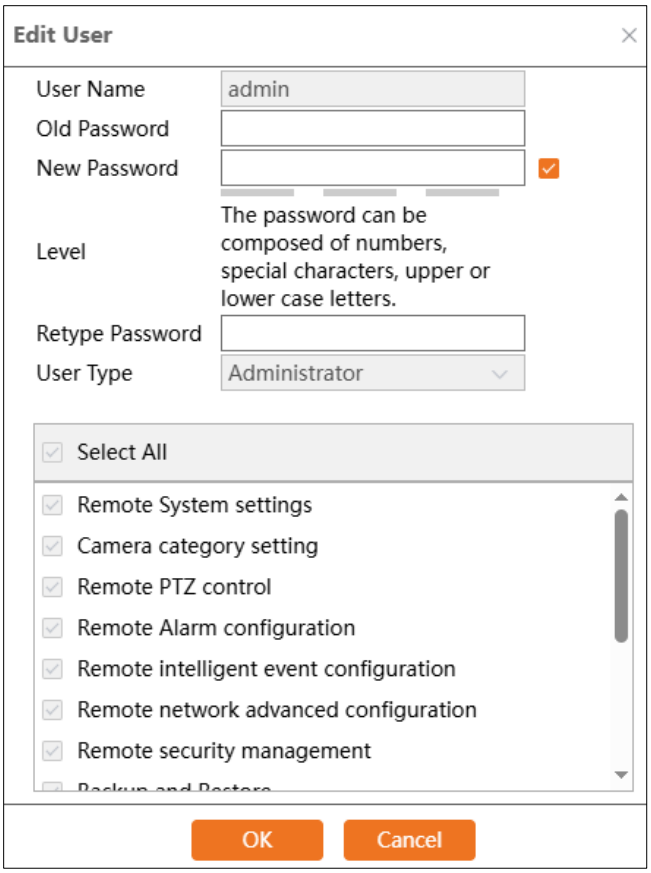
1. Click the “Add” button to open the following text box.



2. Enter the user name in the “User Name” text box.
3. Enter the password in the “Password” and “Confirm Password” text boxes. Please set the password according to the requirements of the password security level (Go to Setup> Security> Password Security to set the security level).
4. Choose the user type and select the desired user permissions.
5. Click the “OK” button, and then the newly added user will be displayed in the user list.

Modify user:

1. Select a user to modify the password, if necessary, in the user Configuration list box.
2. The “Edit user” dialog box pops up when you click the “Modify” button.



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. Select the user permissions for advanced or normal users.
6. Click the “OK” button to save the settings.

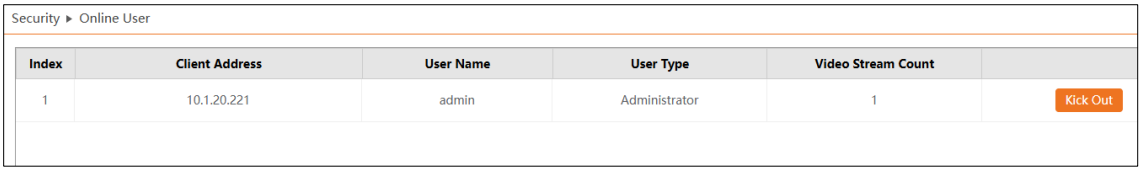
Delete user:

1. Select the user to be deleted in the user Configuration list box.
2. Click the “Delete” button to delete the user. The default administrator account cannot be deleted.

Safety Question Settings: Set the questions and answers for the admin to reset the password after you forget it.

2.5.2 Online User

Go to *Setup>Security>Online User* to view all current users viewing live video from the camera.

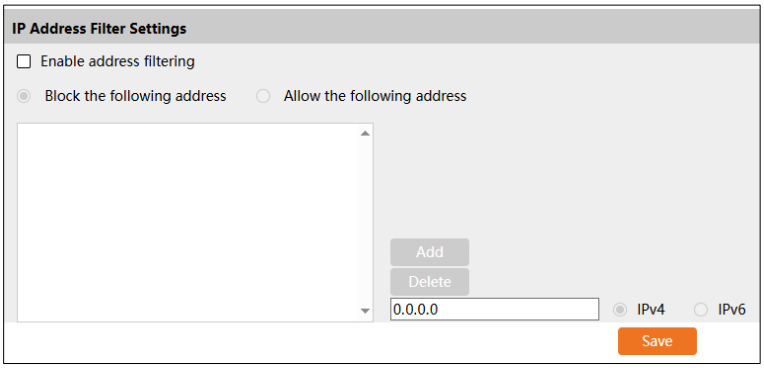


Admin users can view the number of video streams, IP address and user type for each active user.

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

2.5.3 Block and Allow Lists

Go to *Setup>Security>Block and Allow Lists*.

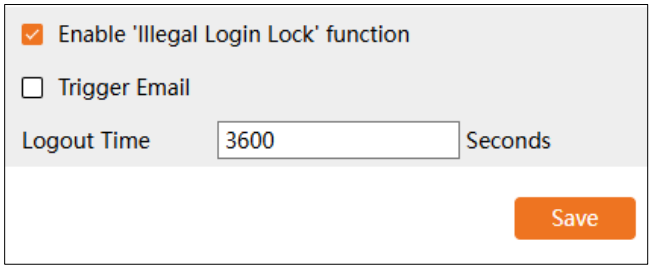


Check the “Enable address filtering” checkbox.

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

2.5.4 Security Service

Go to *Setup>Security>Security Service*.

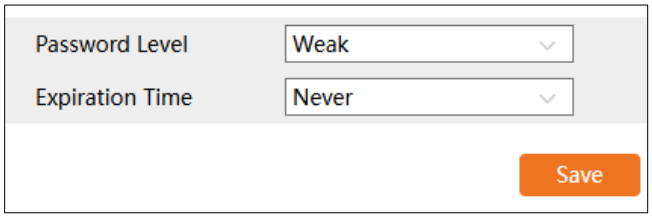


To prevent malicious password unlocking, the “Illegal Login Lock” function locks the login interface after five (5) failed login attempts. The camera can be logged in to again after half an hour or after the camera reboots.

Trigger E-mail: If enabled, an e-mail will be sent when logging in/out or an illegal login lock occurs.

Logout time: Set the logout time as needed. For example, after 3600 seconds, you will be automatically logged out after 3600s and then you need to enter the username and password again to log in.

2.5.5 Password Security



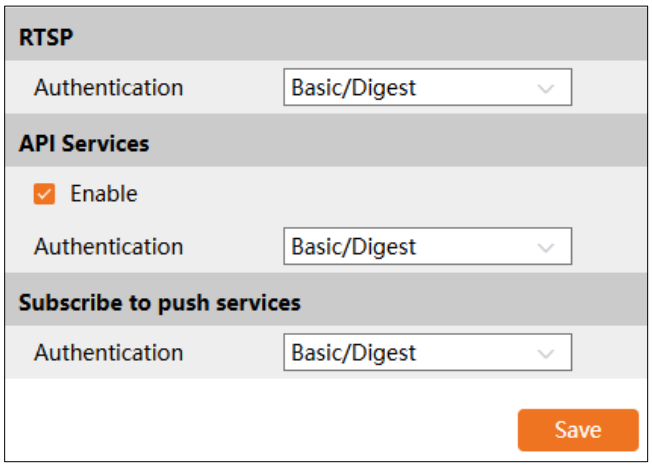
Please set the password level and expiration time as needed.

Password Level: Weak, Medium or Strong.

- Weak level: Numbers, special characters and upper- or lowercase letters can be used. You can choose one of them or any combination of them when setting the password.
- Medium Level: 8~16 characters, including at least two of the following categories: numbers, special characters, uppercase letters and lowercase letters.
- Strong Level: 8~16 characters. Numbers, special characters, uppercase letters and lowercase letters must be included.

For your account security, it is recommended to set a strong password and change your password regularly.

2.5.6 Authentication



- RTSP Authentication: “Digest” or “Basic/Digest” can be selected.
- API Service Authentication: “Digest” or “Basic/Digest” can be selected.
- Push Subscription Authentication: “Digest” or “Basic/Digest” can be selected.

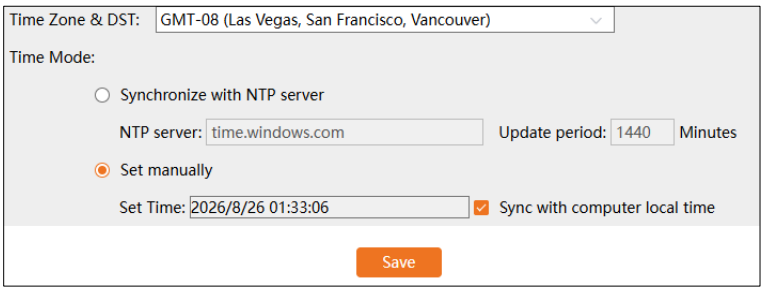
2.6 System Configuration

2.6.1 Basic Information

In the "Basic Information" interface, the system information of the device is listed, such as product model, brand, firmware version, ONVIF version, MAC address, device ID, etc. In addition, you can modify the device name as needed.

2.6.2 Date and Time

Go to *Setup>System>Date and Time*. Please refer to the following interface.



Select the time zone and time mode as needed.

Note: The time zone of the camera and the computer must be the same. If the camera's time zone is not the same as the computer's time zone, a warning message will be shown next to the drop-down.

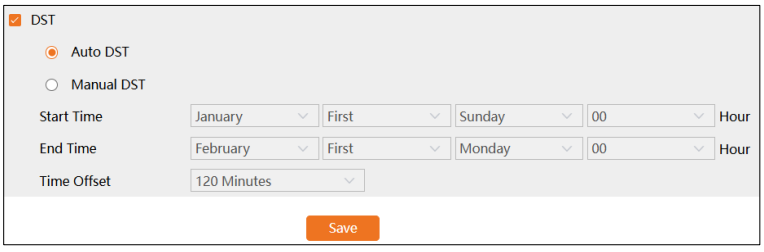
Time Mode:

- Synchronize with NTP server: Specify an NTP server to synchronize the time.
- Set manually: Set the system time manually, or you can synchronize the time with the local computer's time.

2.6.3 Time Zone & DST

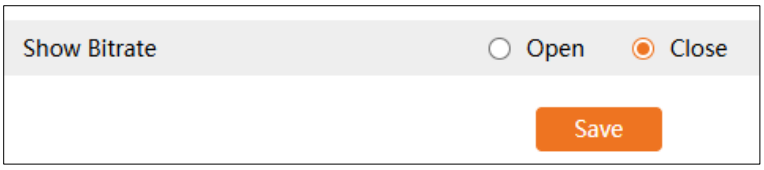
Go to *Setup>System>Time Zone & DST*.

Set the daylight saving time settings automatically or manually. If Manual DST is checked, enter the start and end dates for DST in your region.



2.6.4 Local Configuration

Go to *Setup> System> Local Config* to set up the storage path for captured pictures and recorded videos on the local PC. There is also an option to turn audio on or off in the recorded files.

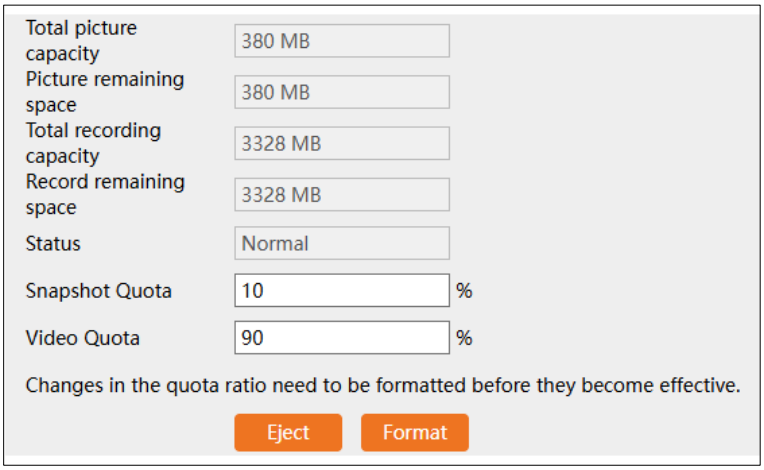


Show Bitrate: turn the bitrate display on or off for the live video.

2.6.5 Micro SD Management

Note: To enable the camera's Facial Recognition Analytics, an SD card 16GB or larger must be installed in the camera **before** operations.

Go to *Setup>System>Micro SD Management*.



- Click the "Format" button to format the SD card. All data will be cleared when you click 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 capacity proportion of captured pictures on the SD card.
- **Video Quota**: Set the capacity proportion of recorded files on the SD card.

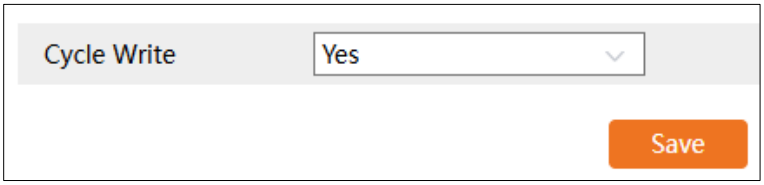
Note: This camera supports the ANR (Automatic Network Replenishment) function. The offline video recording files can be searched in the search interface.

1. When the camera's network is disconnected (for example, the network cable is unplugged), the camera will automatically trigger recording and store the recorded files on the SD card.
2. After the IPC is added to the NVR supporting the ANR function and the ANR function of the IPC is enabled in the NVR, the IPC will automatically trigger recording and store the recorded

files on the SD card when the network between the NVR and the IPC is disconnected. After resuming the connection, the IPC will automatically upload the recorded files during the offline period to the NVR.

2.6.6 Record Parameters

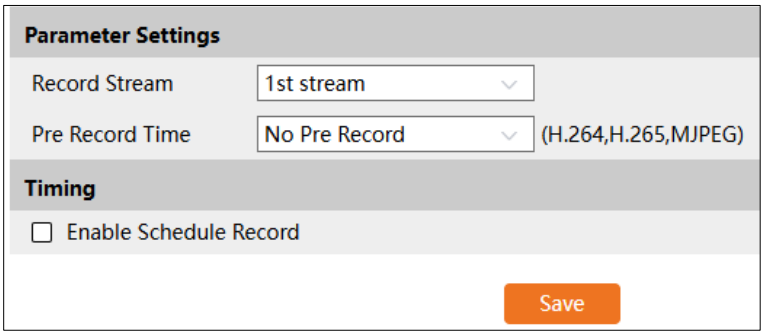
Go to *Setup>System> Record Parameters*.



Overwrite (Cycle Write): The earliest record data will be replaced by the latest when the SD card is full.

2.6.7 Schedule Record

Go to *Setup>System>Schedule Record*.

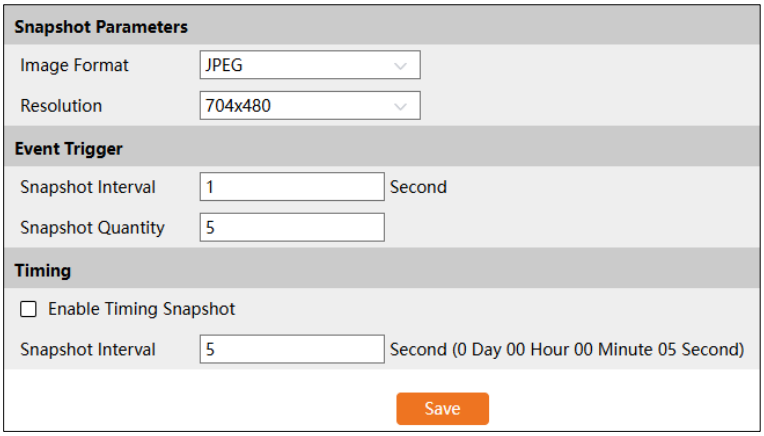


Pre-Record Time: Set the time to record before the actual recording begins.

Schedule Record: Check “Enable Schedule Record”.

2.6.8 Snapshot

Go to *Setup>System>Snapshot*.



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

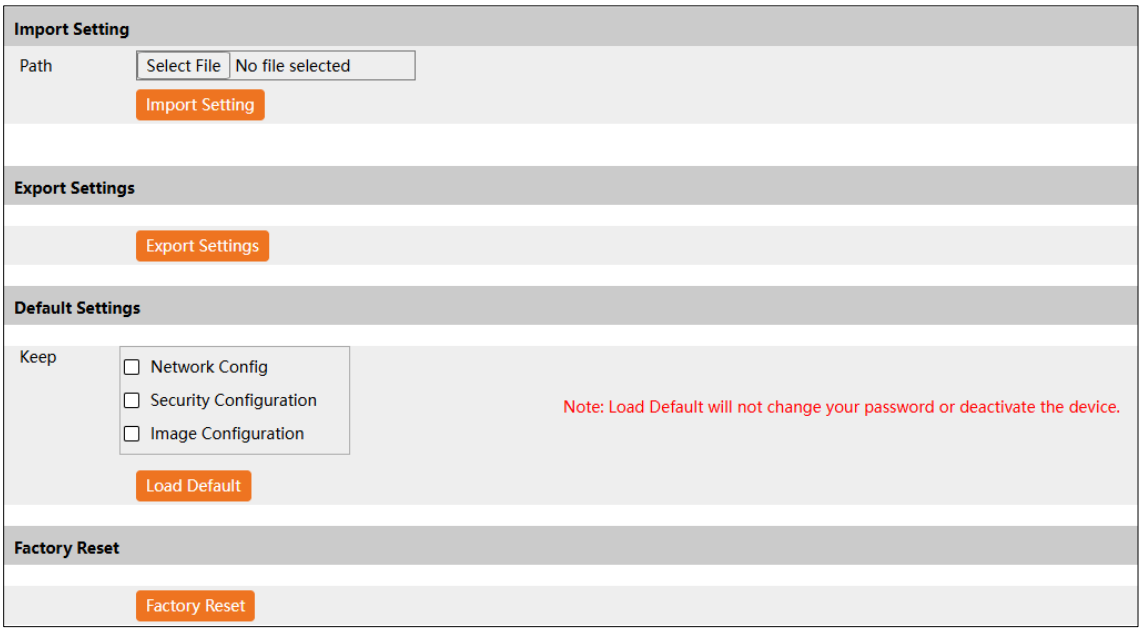
Snapshot Quantity: The number you set here is the maximum quantity of snapshots. The actual quantity of snapshots may be less than this number. If the occurrence time of an alarm event is less than the time of capturing pictures, the actual quantity of snapshots is less than the set quantity of snapshots.

Timing Snapshot: Enable timing snapshot first and then set the snapshot interval.

2.7 Maintenance Configuration

2.7.1 Backup and Restore

Go to *Setup>Maintenance>Backup and Restore*.



Import & Export Settings

Configuration settings of the camera can be exported from one camera to another camera.

1. Click "Select File" to select the save path for import or export information on the PC.
2. Click the "Import Setting" or "Export Setting" button. Enter the password to confirm the action.

* The customized audio files are not supported for export or import.

Restore Default Parameters

Click the "Restore Default Parameters" button and then verify the password to restore all parameters to the default parameters except those you want to keep.

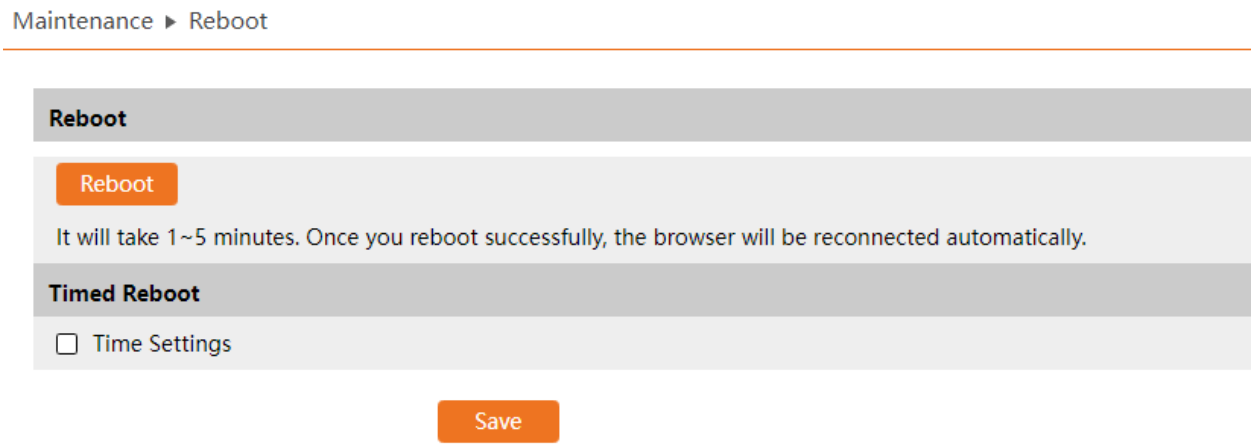
Restore Factory Settings

Click the "Restore Factory Settings" button and then verify the password to restore all system settings to the default factory settings.

2.7.2 Reboot

Go to *Setup>Maintenance>Reboot*.

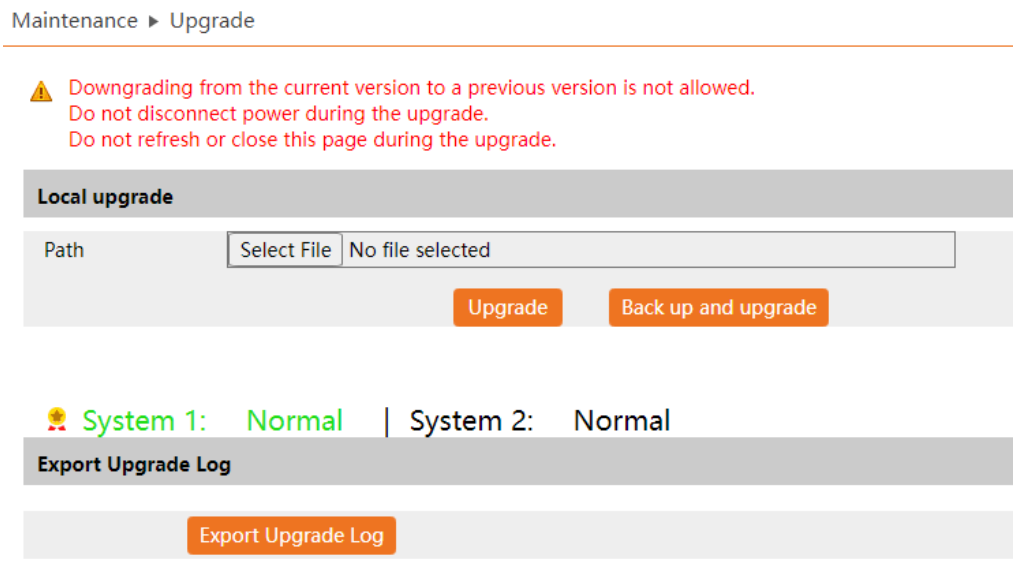
Click the "Reboot" button and then enter the password to reboot the device.



Scheduled Reboot Setting: The camera can be set up to reboot at a time interval. Enable "Time Settings", set the date and time, click the "Save" button and then enter the password to save the settings.

2.7.3 Upgrade

Go to *Setup>Maintenance>Upgrade* to update the camera's firmware.



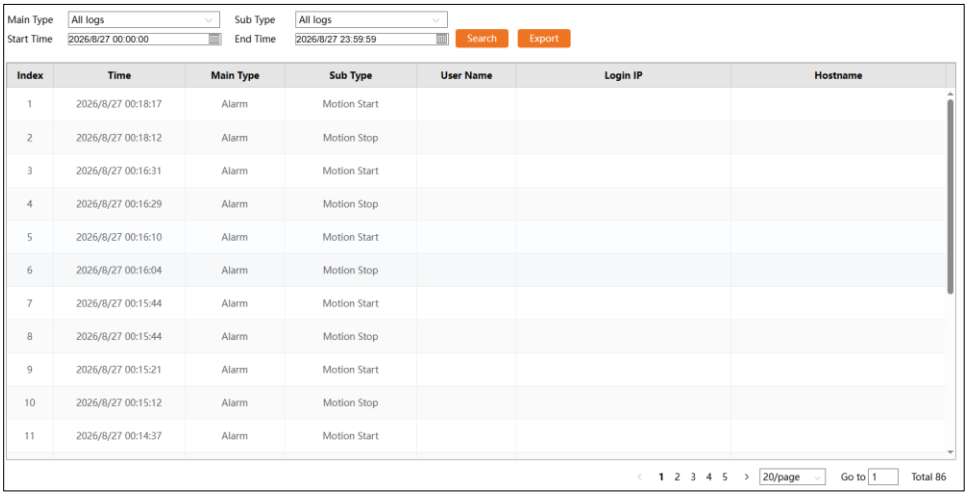
Local Upgrade

1. Click the "Select File" button to select the save path of the upgrade file.
2. Click the "Upgrade" or "Back up and upgrade" button to start upgrading the firmware.
3. Enter the correct password, and then the device will restart automatically. If "Back up and upgrade" is selected, the Configuration file will be exported to your local PC before starting the upgrade.

Export Upgrade Log: If an upgrade error occurs, the upgrade log can be exported to help the technician analyze and solve the problem.

2.7.4 Operation Log

1. Go to Setup>Maintenance>Operation Log.



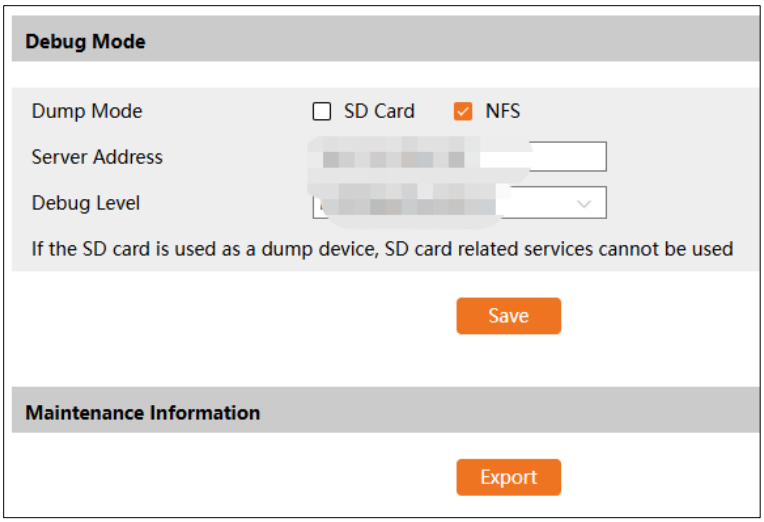
2. Select the main type, subtype, start and end time.
3. Click “Search” to view the operation log.
4. Click “Export” to export the operation log.

2.7.5 Maintenance Information

Debug mode is used to record and collect the required system data so that the technician can quickly find out and analyze the problem and help us improve service.

Before enabling the mode, you are advised to consult our technical support.

When a device failure occurs, you can export the maintenance information and send it to the technicians, so that they can quickly find out and analyze the problem. Go to ***Setup→Maintenance Information*** to export.

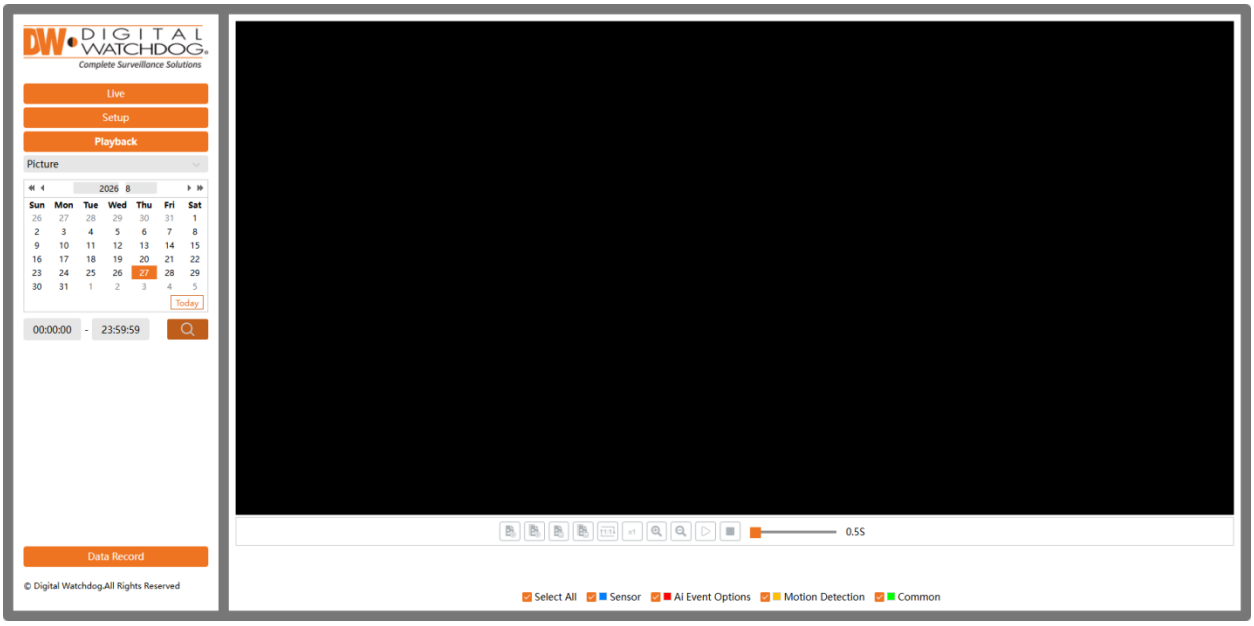

Debug Mode
Dump Mode
SD Card
NFS
Server Address
Debug Level
If the SD card is used as a dump device, SD card related services cannot be used
Save
Maintenance Information
Export

3 PLAYBACK

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

3.1 Picture Search

1. From the drop-down, choose “Picture”.



2. Set time: Select a date and choose the start and end time.
3. Choose the alarm events at the bottom of the interface.
4. Click to search. Results will show under the calendar search. The type of alarm will be indicated by the ‘Type’ color next to the timestamp.
5. Double-click a file name in the list to view the captured photos.



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.	x1	Actual size: Click this button to display the actual size of the image.
	Zoom in: Click this button to zoom in digitally.		Zoom out: Click this button to zoom out digitally.
	Slide show play: Click this button to start the slide show mode.		Stop: Click this button to stop the slide show.
0.5S	Play speed: Play speed of the slide show.		

3.2 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”.
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. 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
	Turn audio on/off; drag the slider to adjust the volume after enabling audio.		

Note:

and cannot be displayed in the above interface via the plug-in-free browser.

For plug-in-free playback, the playback mode switch (balanced/real-time/fluent mode) and downloading functions are not supported either.

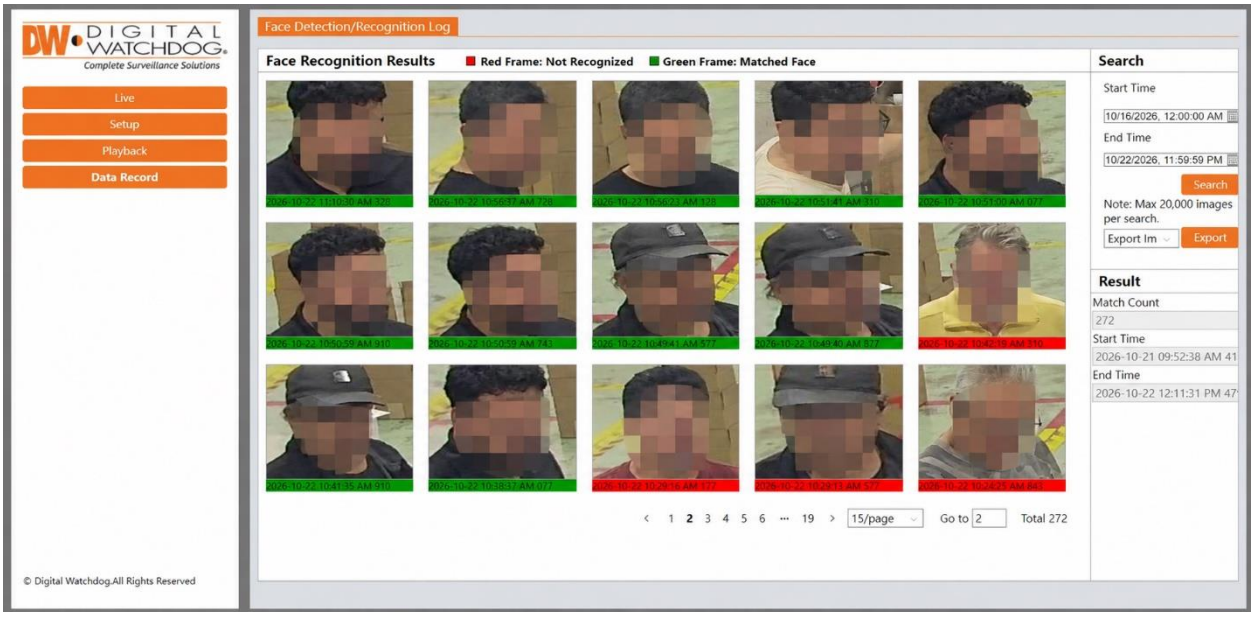
For fluent playback, it is recommended to use the plug-in-required browser to play the recorded video with 2MP or above resolution.

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

4 FACE RECOGNITION RESULT SEARCH

Click *Data Record* to open the face recognition search.

Set the start time and end time, and click “Search” to view the face recognition result.



A red time tag means there is no comparison result. A green time tag means there is a comparison result. Click the picture with the green time tag, and then the face comparison information can be viewed as shown below.



5 Appendix

5.1Appendix Troubleshooting

Q: How to find the password?

A: The password for ***admin*** can be reset through the “Edit Safety Question” function.

Click “Forgot Password” in the login window and then enter the corresponding answer to the selected question in the pop-up window. After you correctly answer all questions, you can reset the password for the ***admin***. If you forget the answer to the question, this method will be invalid. Please contact your installer or DW Support for help.

B: The passwords of other users can be reset by the ***admin***.

Q: Fail to connect devices via a web browser.

A: The network is not properly connected. Check the connection and make sure it is connected properly.

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

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

D: If the above reasons apply. Restore the default settings using the IP-Tool.

Q: IP Tool cannot search for devices.

The antivirus software on your computer may be causing this. Please exit it and try to search for the device again.

Q: No sound can be heard.

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

B: The audio function is not enabled on the corresponding channel. Please enable this function.

5.2 Appendix Communication Matrix

Protocol/Service	Source Device	Source Port	Destination Device	Destination Port（Listening）	Connection Type	Enabled by Default (Yes/No)	Destination Port Setupurable (Yes/No)	Description
HTTP	Web/Onvif Client	-	IPC	80	TCP	No	Yes	Port 80 is used to provide HTTP Web Server and ONVIF services.
HTTPS	Web/Onvif Client	-	IPC	443	TCP	Yes	Yes	Port 443 is used to provide HTTPS Web Server and ONVIF services.
Data Communication Protocol	Private Protocol Client（NVR/NVMS/SDK/ OCX Plug-in)	-	IPC	9008	TCP	Yes	Yes	Port 9008 can be used to transmit an audio-video stream, and the private protocol client can manage and control IPCs through this port.
Subscribe to the service.	Third-party Platform	-	IPC	8080	TCP	Yes	Yes	Port 8080 is a long-lived connection port, which is used to push intelligent data to a third-party platform.
RTSP	RTSP Client	-	IPC	554	TCP	Yes	Yes	Port 554 is used to provide real-time RTSP streaming media transmission service.
RTSPS	RTSPS Client	-	IPC	332	TCP	Yes	Yes	Port 332 is used to provide real-time and secure RTSP streaming media transmission service.
Multicast Search Protocols	IPC	9407	234.55.55.56	23456	UDP	Yes	No	Port 9407 is used to send multicast to 234.55.55.56:23456, which can be searched by IPTOOL/NVMS/NVR; port 23456 is used to receive the multicast information from IPTOOL/NVMS/NVR.
	IPTOOL/NVMS/NVR	-	IPC	23456	UDP	Yes	No	

ONVIF	Other ONVIF Devices	-	IPC	3702	UDP	Yes	No	Port 3702 is used to find ONVIF devices and make an ONVIF service query.
SNMP	Network Management System	-	IPC	161	UDP	No	Yes	Port 161 is used to provide SNMP service.
	IPC	162	Network Management System	-	UDP	No	Yes	As an SNMP client, the device uses port 162 to send trap information to the network management system. (When enabling the SNMP function, port 162 will not be enabled by default. Only when sending the trap information can it be enabled temporarily. After the information is sent successfully, the port will be turned off.
RTMP	IPC	Random Port (1024-65535)	RTMP Server	-	UDP	No	No	The device uses a random port to push audio-video streaming media data to the RTMP server.
UPnP	Other UPnP Devices	-	IPC	Random Port (49152-65535)	TCP	No	No	Port 49152 is used for network communication with other UPnP devices. If it is already occupied, the port number is automatically increased by 1 until an available port is found.
	Other UPnP Devices	-	239.255.255.250	1900	UDP	No	No	Port 1900 is used to receive the multicast reports sent by other UPnP devices, so that these UPnP devices can be found on the network. The random port is used to send multicast to port 1900, so that the IPC can be found by other UPnP
	IPC	Random Port (1024-65535)	239.255.255.250	1900	UDP	No	No	

								devices on the network (1900 is the default port of the SSDP protocol).
NAT	IPC	2 Random Ports (1024-65535)	NAT Server	-	UDP	No	No	These two random ports are used to communicate with the NAT server, enabling the network penetration function.

5.3 Appendix Product Specifications

	DWC-MSBD08BW	DWC-MSBD08MW	DWC-MSDG08BW	DWC-MSDG08MW	DWC-MSTE08BW	DWC-MSTE08MW
IMAGE						
Image sensor	4K 1/1.8" CMOS sensor					
Total pixels	3840 (H) × 2160 (V)					
Minimum scene illumination	0.0005 lux (color)					
	0 lux (WL Illumination)					
Color temperature	3000K	3000K	6000K	6000K	3000K	3000K
WL wavelength (lumen)	300 lm	560 lm	150 lm	200 lm	274 lm	369 lm
S/N ratio	≥50dB					
Test monitor video output	N/A	Local video output CVBS	N/A	Local video output CVBS	N/A	N/A
LENS						
Focal length	2.8mm, F1.0	2.8~12mm@F1.0	2.8mm, F1.0	2.8~12mm@F1.0	2.8mm, F1.0	2.8~12mm@F1.0
Lens type	Fixed lens	Vari-focal lens with motorized zoom and autofocus	Fixed lens	Vari-focal lens with motorized zoom and autofocus	Fixed lens	Vari-focal lens with motorized zoom and auto-focus
Field of view (HFoV)	110°	104°~55°	110°	104°~55°	110°	104°~55°
Illumination type	3 white light LEDs	4 white light LEDs	2 white light LEDs	4 white light LEDs	3 white light LEDs	3 white light LEDs
Illumination distance	98ft range	164ft range	65ft range	98ft range	98ft range	98ft range
I/O						
Audio in/out	1 audio input and 1 microphone built-in/ 1 output					
Audio compression	G.711A / U					
Alarm in/out	1 input/1 output					
Event trigger	Motion detection, SD card error, SD card full, IP address conflict, Network disconnection, sensor alarm, audio alarm					
INTELLIGENT VIDEO ANALYTICS						
AI-based analytics	Classification of humans, vehicles, motorcycles, bicycles and face detection and tracking.					
Analytics filters	Line crossing, perimeter intrusion, tampering, Object Classification, and facial recognition.					
OPERATIONAL						
Shutter mode	Auto, manual					
Shutter speed	1/30s ~ 1/100000s					
Slow shutter	N/A					
Auto gain control	Auto					
Day and night	Color only					
3D Digital Noise Reduction	3D DNR					

Wide Dynamic Range (WDR)	True WDR, 120dB					
White balance	Yes					
Privacy zones	4 programmable privacy masks					
Backlight compensation (BLC)	Yes					
Mirror and flip	Yes					
Alarm notifications	Notifications via e-mail or FTP server					
Memory slot	Micro SD / SDHC / SDXC card up to 1TB (card not included)					
NETWORK						
LAN	802.3 compliance 10/100 LAN					
Video compression type	H.265, H.264, MJPEG					
Resolution	4K/8MP (3840×2160)					
Main Stream	4K, 6MP, 4MP, 2K/1080p					
Sub Stream	2.1MP/1080p (1~15fps), 720P, D1, 640 ×360					
Third Stream	720P, D1, 640 ×360, VGA, CIF, 480×240					
Frame rate	Up to 30fps at all resolutions					
Video bitrate	32 Kbps ~ 12 Mbps					
Bitrate control	Multi-streaming CBR/VBR at H.264/ H.265 (controllable frame rate and bandwidth)					
Streaming capability	Triple Streaming					
IP	IPv4, IPv6					
Protocol	DHCP, Port, RTSP, RTMP, DDNS, SNMP, SMTP, FTP, HTTP POST, 802.1x, UPnP, HTTPS, QoS					
Security	IP filtering, MAC filtering, authentication (ID/PW), SSL/TLS					
ONVIF conformance	Yes					
Web viewer	OS: Windows OS, Mac OS, Linux OS					
	Browser: Microsoft Edge, Google Chrome, Mozilla Firefox, Safari					
Video management software	DW Spectrum, COVA					
ENVIRONMENTAL						
Startup temperature	-22°F ~ 140°F (-30°C ~ 60°C)					
Operating temperature	-22°F ~ 140°F (-30°C ~ 60°C)					
Operating humidity	0–95% RH (non-condensing)					
IK rating	N/A	N/A	IK10	IK10	N/A	N/A
IP rating	IP67-rated	IP67-rated	IP67-rated	IP67-rated	IP67-rated	IP67-rated
Other certifications	FCC, CE, ROHS, ONVIF, NDAA					
ELECTRICAL						
Power requirement	DC 12V, PoE, adapter not included					

Power consumption	DC 12V: max 7.5W, 625mA PoE: max 7.5W, 156mA	DC 12V: max 11.1W, 925mA PoE: max 12.5W, 260mA	DC 12V: max 7.5W, 625mA PoE: max 7.5W, 156mA	DC 12V: max 10.7W, 891mA PoE: max 10.8W, 225mA	DC 12V: max 7.5W, 625mA PoE: max 7.5W, 156mA	DC 12V: max 11.1W, 925mA PoE: max 12.6W, 262mA
MECHANICAL						
Material	Metal bullet housing	Metal bullet housing	Metal vandal dome, polycarbonate domes	Metal vandal dome, polycarbonate domes	Metal turret, polycarbonate lens cover	Metal turret, polycarbonate lens cover
Dimensions	8.69″ x 3.16″ x 2.77″ (220.8 × 80.5 × 70.6mm)	10.7″ x 3.85″ x 3.52″ (272 × 98× 89.5mm)	4.6″ x 3.54″ (117 × 90mm)	5.43″ x 3.93″ (138 × 100mm)	5.14″ x 5.32″ (130.6 × 135.25mm)	5.14″ x 5.32″ (130.6 × 135.25mm)
Weight	1.52 lbs (690 gr)	2.29 lbs (1040gr)	1.41 lbs (640gr)	2.05 lbs (930gr)	1.54 lbs (0.7 kg)	1.54 lbs (0.7 kg)
Warranty	5 year warranty	5 year warranty	5 year warranty	5 year warranty	5 year warranty	5 year warrnty

Warranty Information

Go to https://digital-watchdog.com/page/rma-landing-page/ to learn more about Digital Watchdog's warranty and RMA.

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

A purchase receipt or other proof of the original purchase date is required before warranty service is rendered. This warranty only covers failures due to defects in materials and workmanship that arise during normal use. This warranty does not cover damages that occur 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.

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 using these products or arising out of any breach of the warranty. All express and implied warranties, including the warranties of merchantability and fitness for a 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; you may also have other rights 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
16220 Bloomfield Ave
Cerritos, CA 90703

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.