



Network Camera User Manual

AI 360° Panoramic Fisheye

Version: V1.0

Date: 2026-07-16

Table of Contents

Chapter 1. Introduction	4
1.1 Copyright Statement	4
1.2 Safety Instruction	4
1.3 EU Conformity Statement	5
1.4 Revision History	5
Chapter 2. Product Description	5
2.1 Product Overview	5
2.2 System Requirements	5
Chapter 3. Configuration Flow	6
Chapter 4. Network Connection	7
4.1 Setting the Camera over the LAN	7
4.1.1 Connecting the Camera to the PC Directly	7
4.1.2 Connecting via a Switch or Router	7
4.2 Dynamic IP Connection	7
Chapter 5. Accessing the Network Camera	8
5.1 Assigning an IP Address	8
5.1.1 Assigning an IP Address Using Smart Tools	8
5.1.2 Assigning an IP Address via Browser	11
5.2 Accessing from the Web Browser	13
5.3 Accessing from Milesight Back-end Software	13
5.3.1 Accessing from Milesight NVR (Network Video Recorder)	13
Chapter 6. Live View	14
6.1 Live View Window	15
6.1.1 Video Channel Diagnosis	18
6.2 Fisheye Mode	18
6.3 PTZ Control	20
6.3.1 Set / Call a Preset / Patrol	21
6.4 Image Configuration	25
Chapter 7. Playback	26
Chapter 8. Settings	29
8.1 Media	29
8.1.1 Video	29
8.1.2 Image	31
8.1.3 Audio	44
8.2 Network	46
8.2.1 Basic	46
8.2.2 Advanced	57
8.3 Storage	67
8.3.1 Storage Management	67
8.3.2 Record Settings	69
8.3.3 Snapshot Settings	70
8.3.4 Explorer	72
8.4 Fisheye	73
8.5 Event	77
8.5.1 Basic Event	77
8.5.2 VCA Event	85
8.5.3 Object Counting	109

8.5.4 Heat Map	125
8.5.5 Attribute Extraction	131
8.5.6 Sound Classification	135
8.5.7 Privacy Protection	138
8.6 System	142
8.6.1 System Setting	142
8.6.2 Security	144
8.6.3 Logs	154
8.6.4 Maintenance	156
Chapter 9. Services	159

Chapter 1. Introduction

1.1 Copyright Statement

This manual may not be reproduced in any form or by any means to create any derivative work, such as translation, transformation, or adaptation, without the prior written permission of Milesight IoT Co., Ltd. (hereinafter referred to as Milesight).



reserves the right to change this manual and the specifications without prior notice. The latest specifications and user documentation for all Milesight products are available on our official website <http://www.milesight.com>

1.2 Safety Instruction

These instructions are intended to ensure that user can use the product correctly to avoid danger or property loss. The precaution measures are divided into “Warnings” and “Cautions”

Warnings: Serious injury or death may be caused if any of these warnings are neglected.

- This installation must be performed by a qualified service person and should strictly comply with the local electrical safety regulations
- To avoid risk of fire and electric shock, keep the product away from rain and moisture before installation.
- Do not touch components such as heat sinks, power regulators, and processors, as they may be hot
- Power Supply: DC 12V or PoE
- Please make sure the plug is firmly inserted into the power socket
- When the product is installed on a wall or ceiling, it should be firmly fixed
- If the product does not work properly, please contact your dealer. Never attempt to disassemble the camera yourself

Cautions: Injury or equipment damage may be caused if any of these cautions are neglected.

- Make sure that the power supply voltage is correct before using the camera
- Do not store or install the device in extremely hot or cold temperatures, dusty or damp locations, and do not expose it to high electromagnetic radiation
- Only use components and parts recommended by the manufacturer
- Do not drop the camera or subject it to physical shock
- To prevent heat accumulation, Do not block air circulation around the camera
- Laser beams may damage image sensors. The surface of image sensors should not be exposed to areas where laser beam equipment is used
- Use a blower to remove dust from the lens cover
- Use a soft, dry cloth to clean the surface of the camera. Stubborn stains can be removed using a soft cloth dampened with a small quantity of detergent solution, then wipe dry
- Do not use volatile solvents such as alcohol, benzene, or thinners, as they may damage the surface finish

- Save the packaging to ensure shipping containers are available for future transportation

1.3 EU Conformity Statement

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.

1.4 Revision History

Table 1.

Version	Revision Content	Release Date
V1.0	First release	July 2026

Chapter 2. Product Description

2.1 Product Overview

Milesight provides a comprehensive range of cost-effective and reliable network cameras to fully meet your requirements. Based on the embedded Linux operating system, Milesight network cameras could be easily accessed and managed either locally or remotely with great reliability. With built-in high-performance DSP video processing modules, the cameras feature low power consumption and high stability. They support state-of-the-art H.265/ H.264/MJPEG video compression algorithm and industry-leading HD dual-stream technology to achieve the highest level of video image quality under the limited network resources. It is fully functional, supporting a flexible and comprehensive alarm linkage mechanism, day and night auto switch and privacy masking, etc.

In practical applications, Milesight network cameras can either work independently in the LAN or be networked to form a powerful safety monitoring system. It is widely used in fields such as finance, education, industrial production, civil defense, health care for security's sake.

2.2 System Requirements

Operating System: Windows XP/Windows 7/8/10/11/Server 2000/Windows Server 2008

CPU: 1.66 GHz or higher

RAM: 1 GB or higher

Graphics memory: 128 MB or more

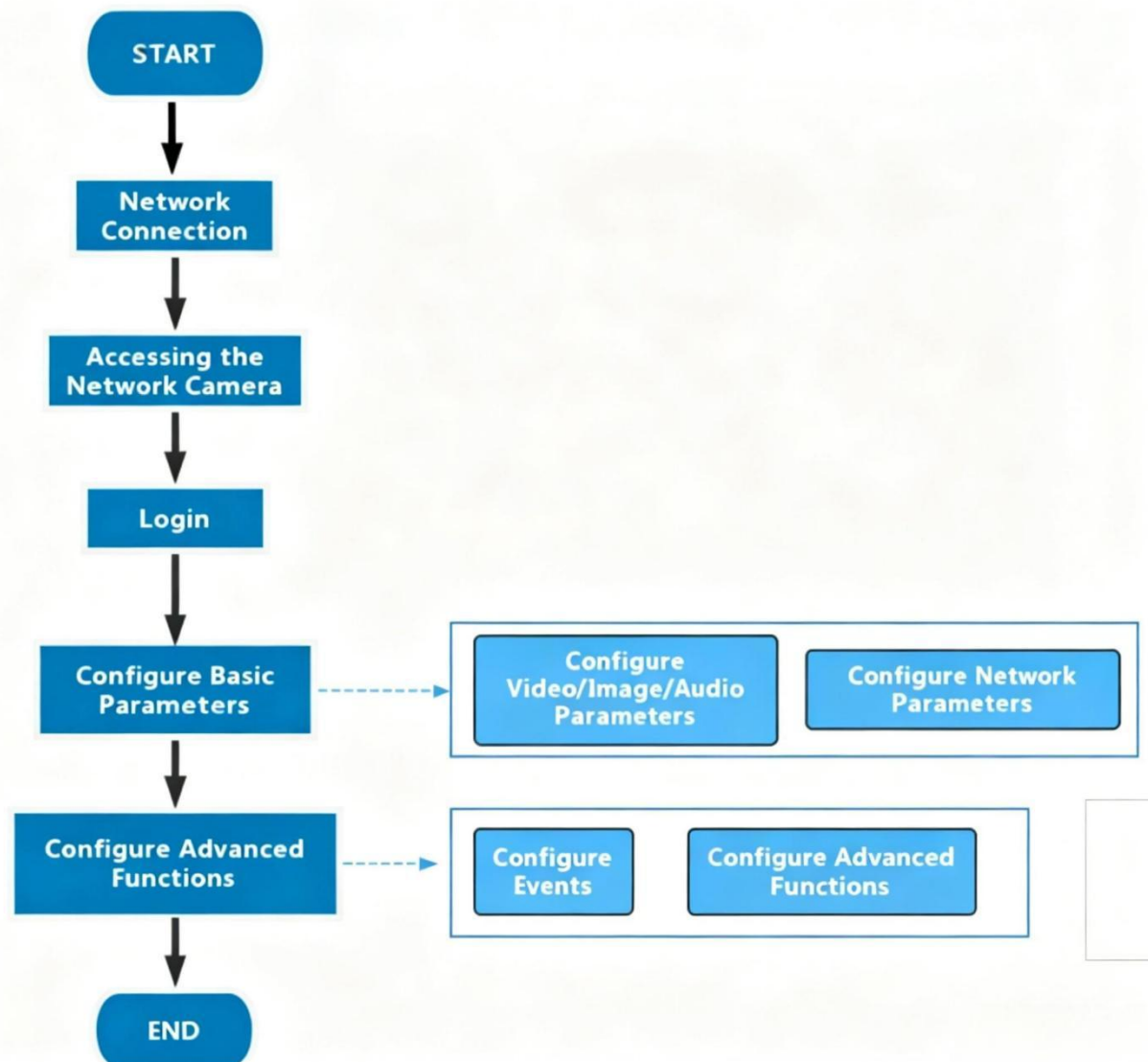
Internet Protocol: TCP/IP (IPv4/IPv6)

Web Browsers: Microsoft Edge, Google Chrome, Safari, Mozilla Firefox

Chapter 3. Configuration Flow

The configuration flow of the cameras is shown in the following figure.

 **Note:** The configuration must be based on the actual situation of different models.



More configuration details are shown in the following table.

Table 2. Description of flow

Configuration	Description	Reference
Network Connection	Connect the network camera. You can set the camera over the LAN or dynamic IP connection.	4.1 Setting the Camera over the LAN
Accessing the Network Camera	Accessing from IP address, web browser and Milesight back-end software are available.	5.1 Assigning an IP Address

Configure Basic Parameters	After login the camera, you can adjust the video/image/audio/network parameters as needed.	8.1 Media 8.2 Network
Configure Advanced Functions	Configure the advanced functions, such as VCA and people counting.	8.4 Event

Chapter 4. Network Connection

4.1 Setting the Camera over the LAN

Connecting the camera to a switch or router is the most common connection method. The camera must be assigned an IP address that is compatible with its LAN.

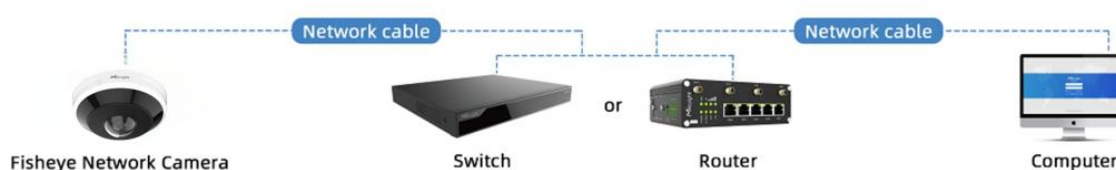
4.1.1 Connecting the Camera to the PC Directly

In this method, only the computer connected to the camera will be able to access it. The camera must be assigned a compatible IP address to the computer. Details are shown in the following figure.



4.1.2 Connecting via a Switch or Router

Refer to the following figure to set up the network camera over the LAN via a switch or router.



4.2 Dynamic IP Connection

Step1: Connect the network camera to a router.

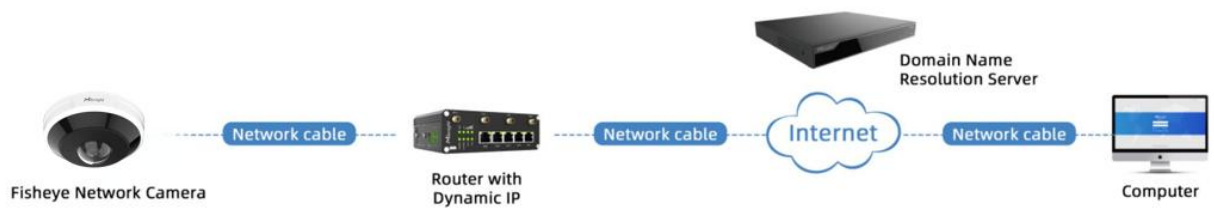
Step2: On the camera, assign a LAN IP address, the subnet mask, and the gateway.

Step3: On the router, set up port forwarding. E.g., 80, 8000, and 554 ports. The steps for port forwarding vary depending on different routers. Please look up the router's user manual for assistance with port forwarding.

Step4: Apply for a domain name from a domain name provider.

Step5: Configure the DDNS settings in the settings interface of the router.

Step6: Access the camera via the domain name.



Chapter 5. Accessing the Network Camera

5.1 Assigning an IP Address

The network camera must be assigned an IP address to be accessible. The default IP address of Milesight network cameras is 192.168.5.190.

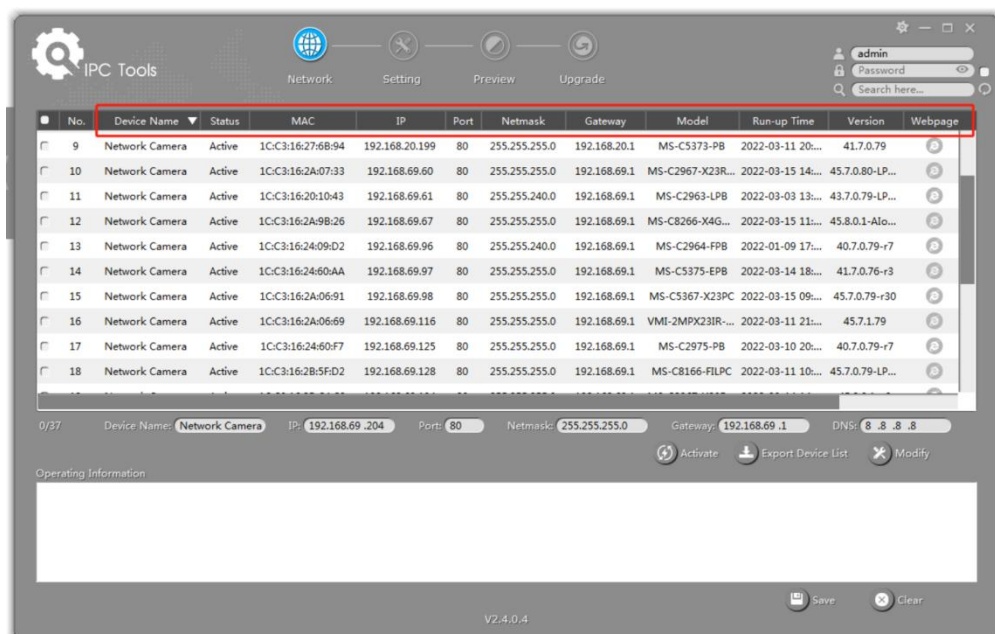
You can change the IP address of the camera via either Smart Tools or a browser. Please connect the camera to the same LAN as your computer.

5.1.1 Assigning an IP Address Using Smart Tools

Smart Tools is a software tool that can automatically detect multiple online Milesight network cameras in the LAN, set IP addresses, and manage firmware upgrades. It's recommended to use when assigning IP addresses for multiple cameras.

Step1: Install Smart Tools (The software can be downloaded from our website).

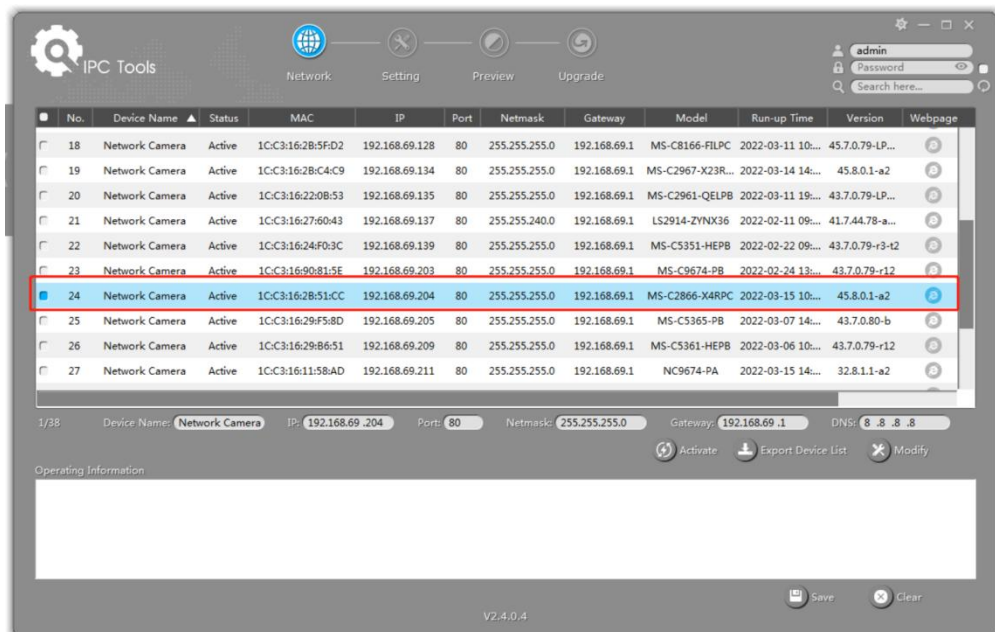
Step2: Start Smart Tools, click the IPC Tools page, then enter the device information, such as IP address, MAC address, status, port number, netmask, and gateway. Then all related Milesight network cameras in the same network will be displayed. Details are shown as the figure below.



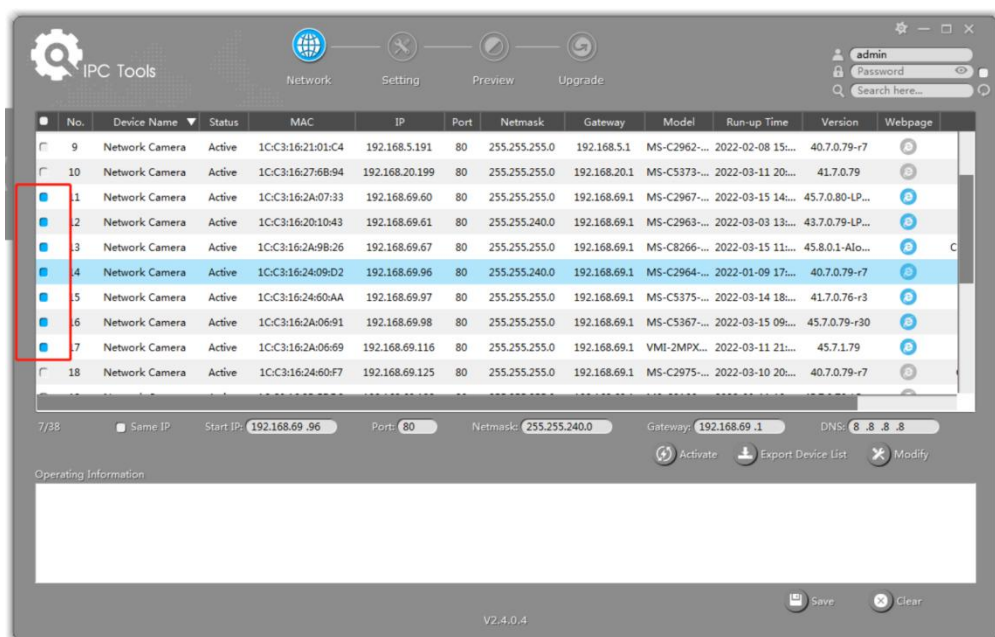
Step3: Select a camera or multiple cameras according to the MAC

addresses.

Select a single camera:



Select multiple cameras:

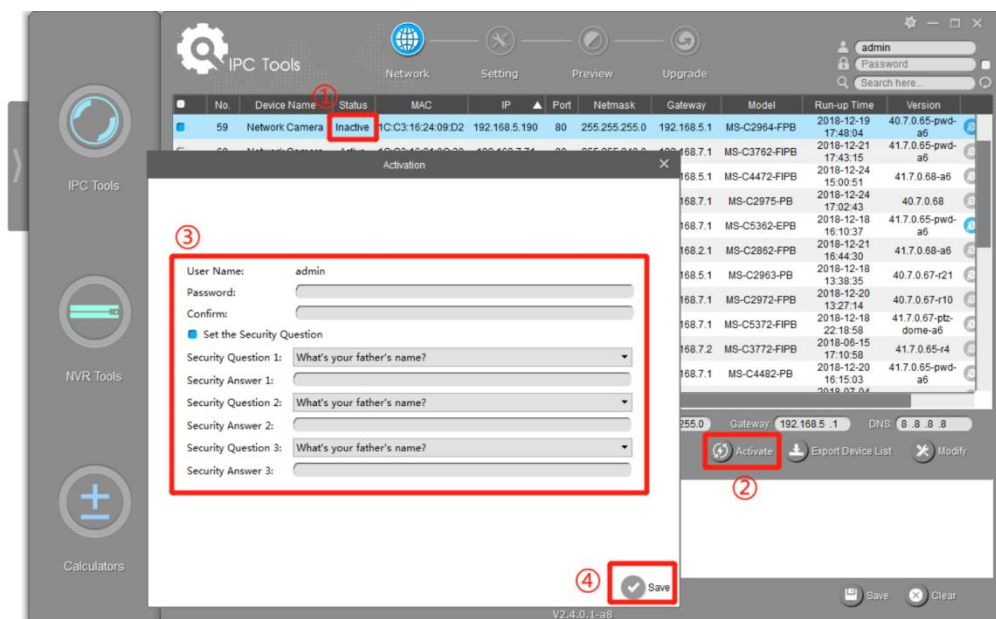


Step4: If the selected camera shows "Inactive" in the status bar, click "Activate" to set the password when using it for the first time. You can also set the security questions when activating the camera in case you forget the password (You can reset the password by answering three security questions correctly). Click 'Save' and it will indicate successful activation.

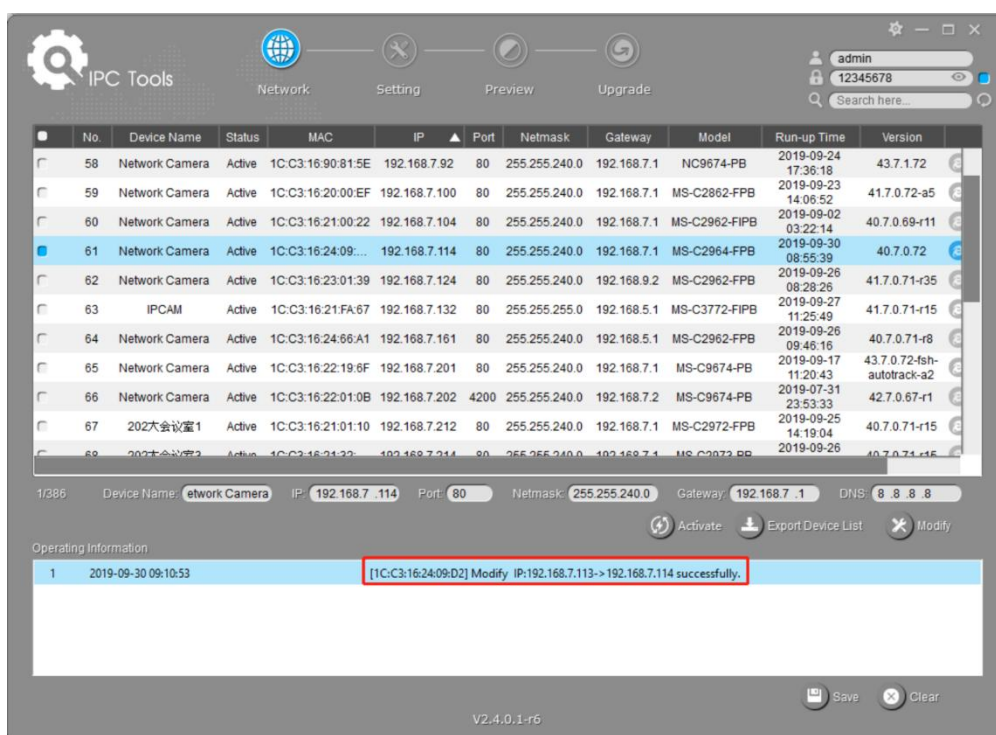


Note:

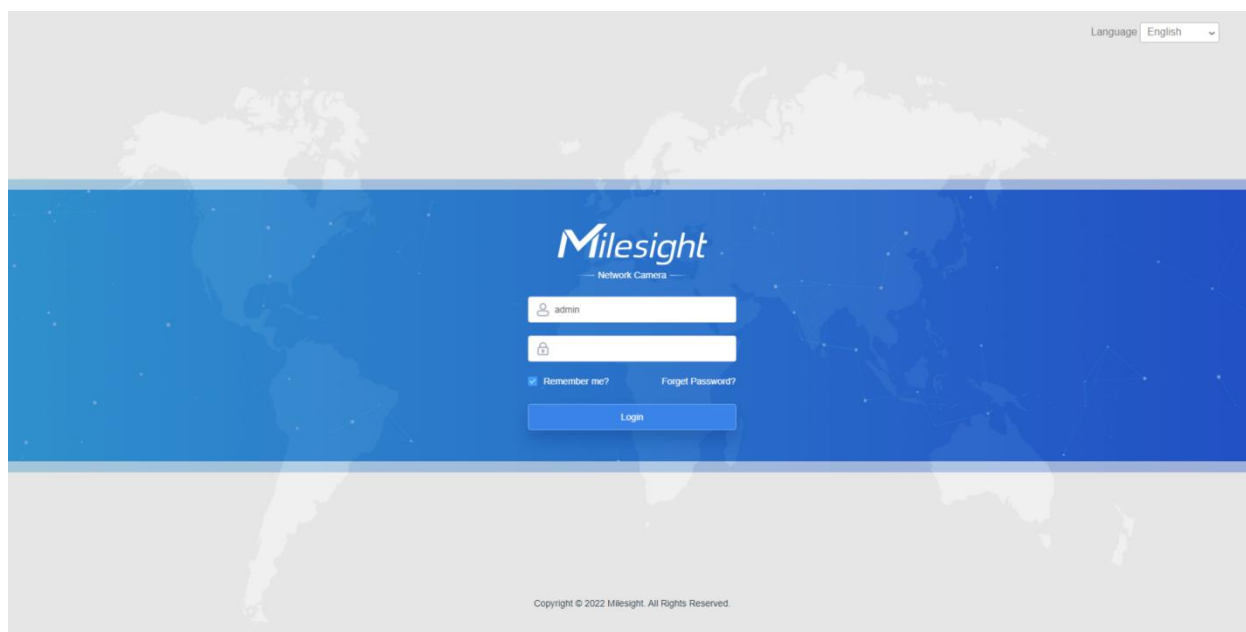
- The password must be 8 to 32 characters long, contain at least one number and one letter.
- You need to upgrade Smart Tools version to V2.4.0.1 or above to activate the camera.



Step5: After activation, you can change the IP address or other network values, and then click “Modify” button.



Step6: By double clicking the selected camera or the browser of interested camera, you can access the camera via web browser directly. The Internet Explorer window will pop up.



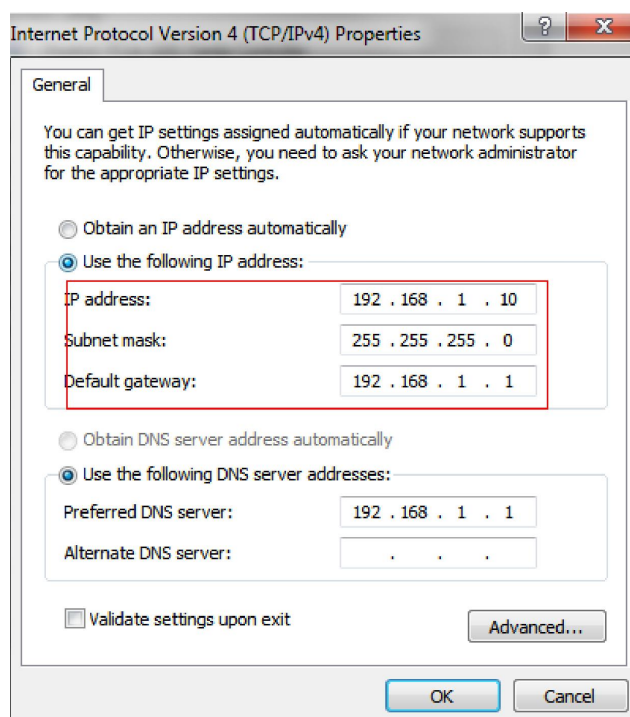
For more usage of Smart Tools, please refer to the Smart Tools User Manual.

5.1.2 Assigning an IP Address via Browser

If the network segment of the computer and that of the camera are different, please follow the steps below to change the IP address:

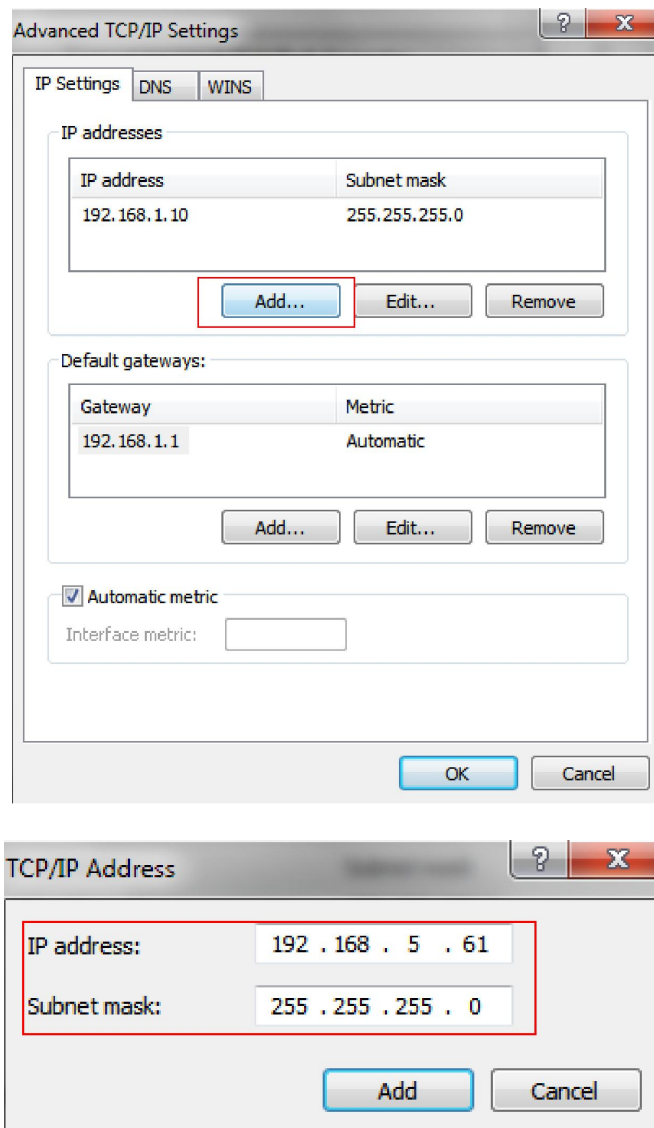
Step1: Change the computer's IP address to the 192.168.5.x subnet, here are two ways as shown below:

a. Start → Control Panel → Network and Internet → Network Connections → Local Area Connection, and double-click it.



b. Click "Advanced", and then click "IP settings"--> "IP address"--> "Add". In the pop-up window, enter an IP address that is in the same subnet with Milesight network camera (e.g. 192.168.7.41, but please note that this IP address must not conflict with existing IP

addresses on the network).



Step2: Open the browser. In the address bar, enter the default IP address of the camera: <http://192.168.5.190>;

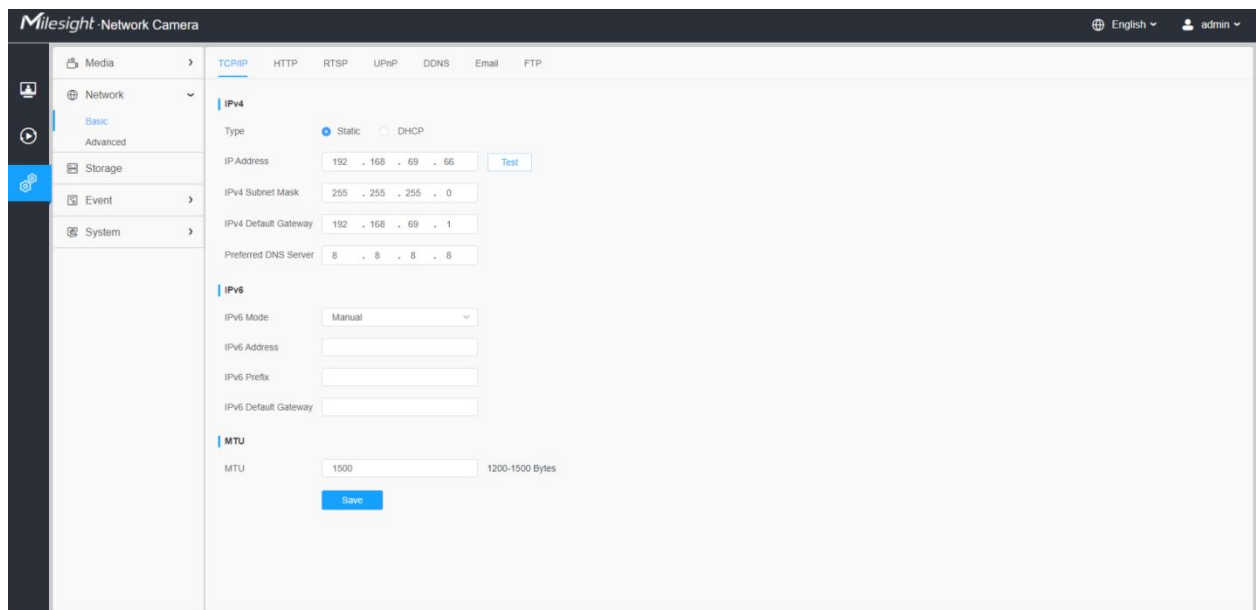
Step3: You need to set a password when using it for the first time. And you can also set three security questions for your device after activation. Then you can log in to the camera with the user name (admin) and a custom password.



Note:

- The password must be 8 to 32 characters long, contain at least one number and one letter.
- You can click the "forget password" in login page to reset the password by answering three security questions when you forget the password, if you set the security questions in advance.

Step4: After login, please select "Settings" --> "Network" --> "Basic" --> "TCP/IP". The Network Settings page appears (as shown in the figure below).



Step5: Change the IP address or other network values. Then click “Save” button.

Step6: The default IP address has been changed.

5.2 Accessing from the Web Browser

The camera can be used with most standard operating systems and browsers. The camera has been upgraded to support Plugin-Free Mode. In Plugin-Free Mode, you can preview the video on the browser without plugin. Currently, Plugin-Free Mode is supported in Firefox, Google Chrome, Safari, and Edge browsers for Windows, macOS, iOS, and Android systems. Both H.265 and H.264 video codecs are supported in Plugin-Free Mode for camera, and it will play the secondary stream by default.



Note:

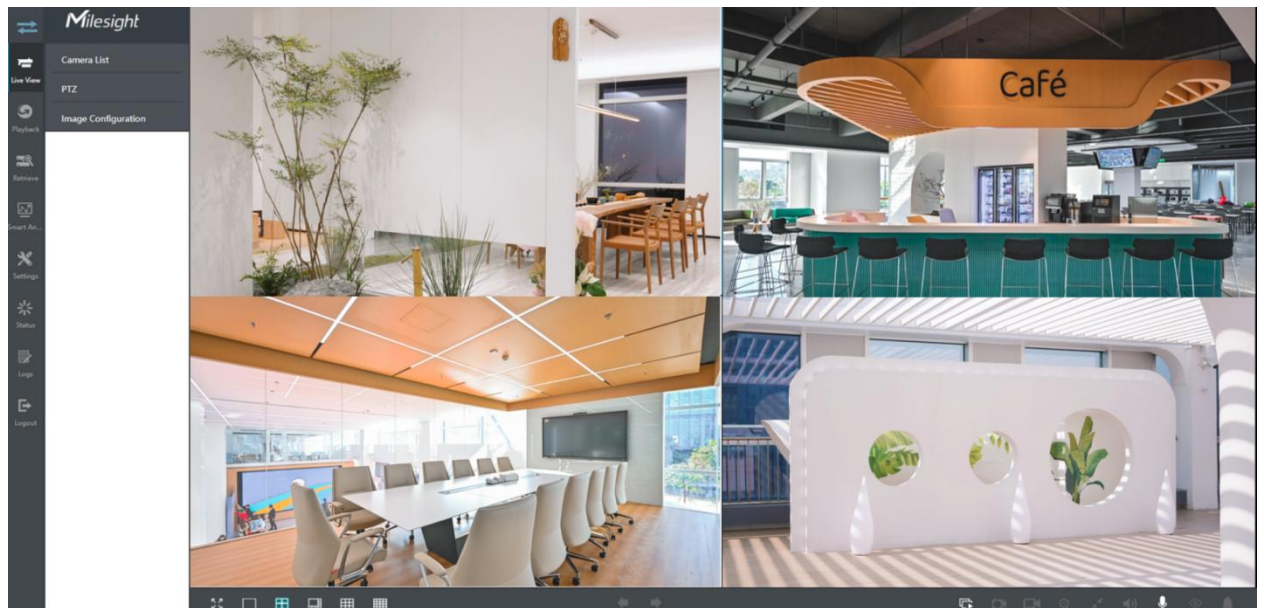
- For more details about setting the plugin-free mode of Milesight cameras, please refer to <https://milesight.freshdesk.com/a/solutions/articles/69000643388>.

5.3 Accessing from Milesight Back-end Software

5.3.1 Accessing from Milesight NVR (Network Video Recorder)

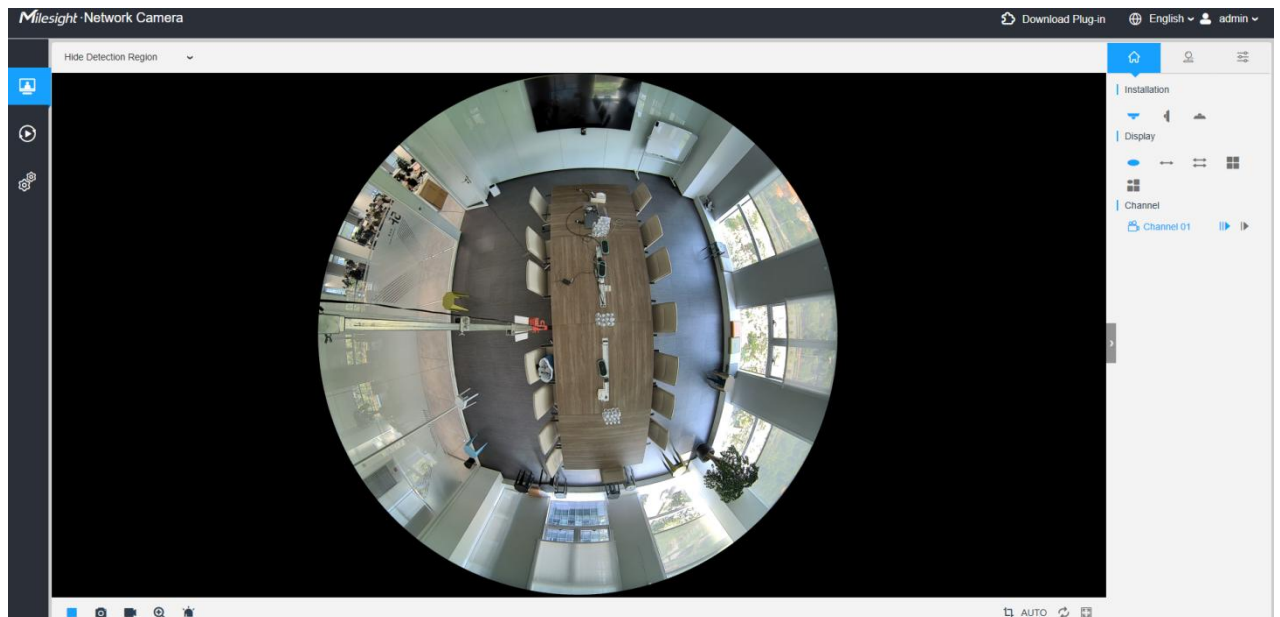
Milesight NVR Series can work with Milesight network cameras. Based on the embedded Linux operating system, Milesight NVR Series manages and stores HD video data. It owns multi-disk management systems, front end HD device management system, HD video analysis system and high-capacity system for video. Also, it adopts the technology of high flow capacity data network transmitting&transmission, with multi-channel video decoding, to achieve functions like intelligent management, safe storage, HD decoding, etc.

For detailed information about how to use the Milesight NVR Series, please refer to Milesight NVR User Manual.



Chapter 6. Live View

After logging in the network camera web GUI successfully, user is allowed to view live video as follows.



6.1 Live View Window

Display live video on the window.

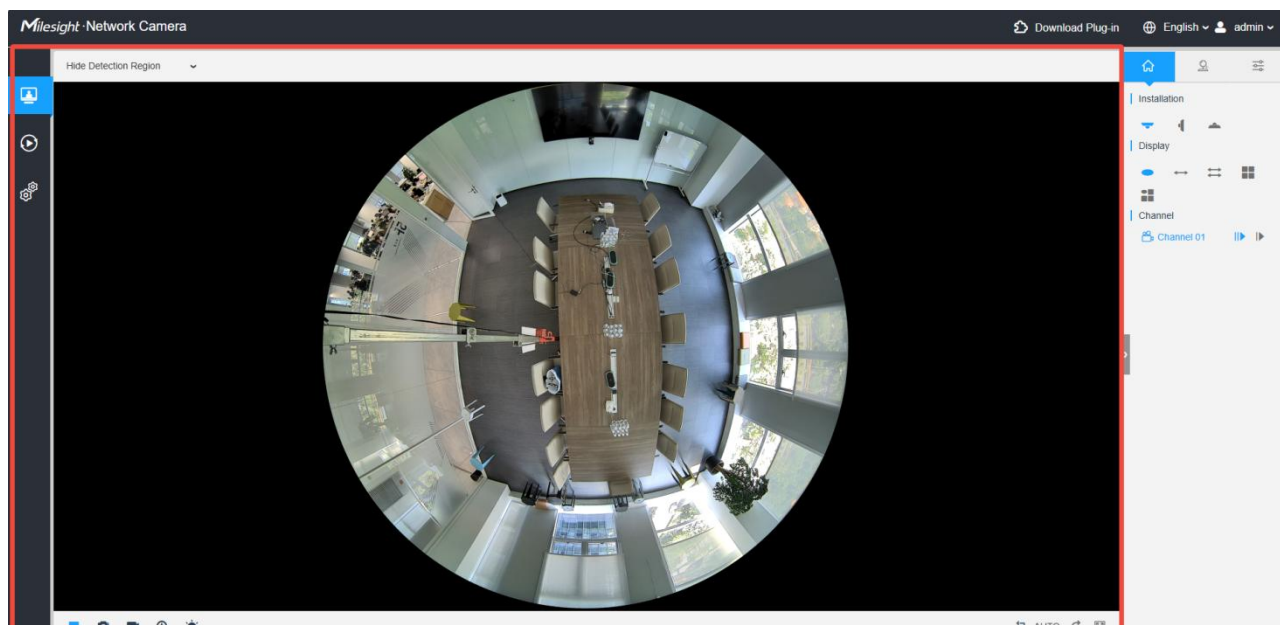
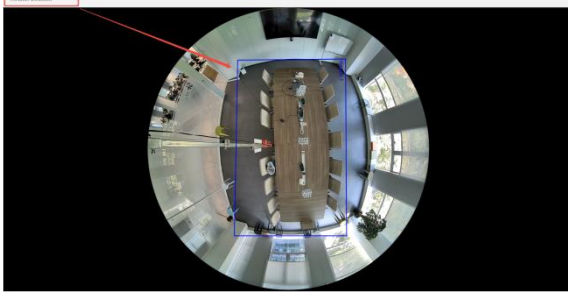


Table 3. Description of the buttons

No.	Parameter	Description
1	 Live Video	Click to access the live view page.
2	 Playback	Click to access the playback page.
3	 Settings	Click to access the configuration page.
4	 Download Plug-in	Click to download the plugin.
5	 English ▾	Click to select system language.
6	 admin ▾	Display the user name and click to logout.

7	Hide Detection Region	Choose the options (Hide Detection Region/Intrusion Detection/ Region Entrance/Region Exiting/Advanced Motion/Line Crossing/Loitering//Object Left/Object Remove//Object Counting/Attribute Extraction/Motion Detection /Regional People Counting, etc.) to hide/display detection region on the current video window. 
8	HTTP ▾	TCP: More reliable connection. UDP: More instantaneous connection, but if you cannot get the live view successfully, please turn into TCP connection. HTTP: Faster and safer connection especially in Internet environment.
9	Shortest Delay ▾	Shortest Delay: The most instantaneous mode. Balanced: A balanced mode between Shortest Delay and Fluent, maintains the fluency while keeps an acceptable delay. Fluent: The most fluent mode.
10	 Recording	When recording, the icon appears.
11	 VCA Event Alarm	When an alarm of VCA event was triggered, the icon appears.
12	 Object Counting Alarm	When an alarm of object counting is triggered, the icon appears.
13	 Motion Detection Alarm	When an alarm of Motion Detection is triggered, the icon appears.
14	 Sound Classification Alarm	When an alarm of Sound Classification is triggered, the icon appears.
15	 Alarm	Except for the kinds of alarms above, when other alarms were triggered, the icon appears.
16	 Stop/Play	Stop/Play live view.

17	 Snapshot	Click to capture the current image and save to the configured path. The default path is: C:\VMS\+-1\IMAGE-MANUAL.
18	 Start/Stop Recording	Click to Start Recording video and save to the configured path. The default path is C:\ProgramData\MPlayer. Click again to Stop Recording.
19	 Digital Zoom	When enabled, you can zoom in a specific area of video image with your mouse wheel.
20	 Manual Output	Manually trigger Camera Alarm Output.
21	 Mute On/Off	Controls the audio input from the camera's built-in microphone during web access.
22	 Start/Stop Talking	Turn on to start talking, so your voice from the camera's web is played through the camera's audio output for two-way audio.
23	 Pixel Counter	By clicking to enable the Pixel Counter function, you can either input the pixel value or draw on the live view to measure the object's size. 
Window	 Window Size	Click to display images at a window size.
	 Real Size	Click to display images at a real size.

	 Full Screen	Click to display images at full-screen.
--	--	---

6.1.1 Video Channel Diagnosis

The Video Channel Diagnosis provides real-time information about the video stream:

Bitrate: Current video bitrate

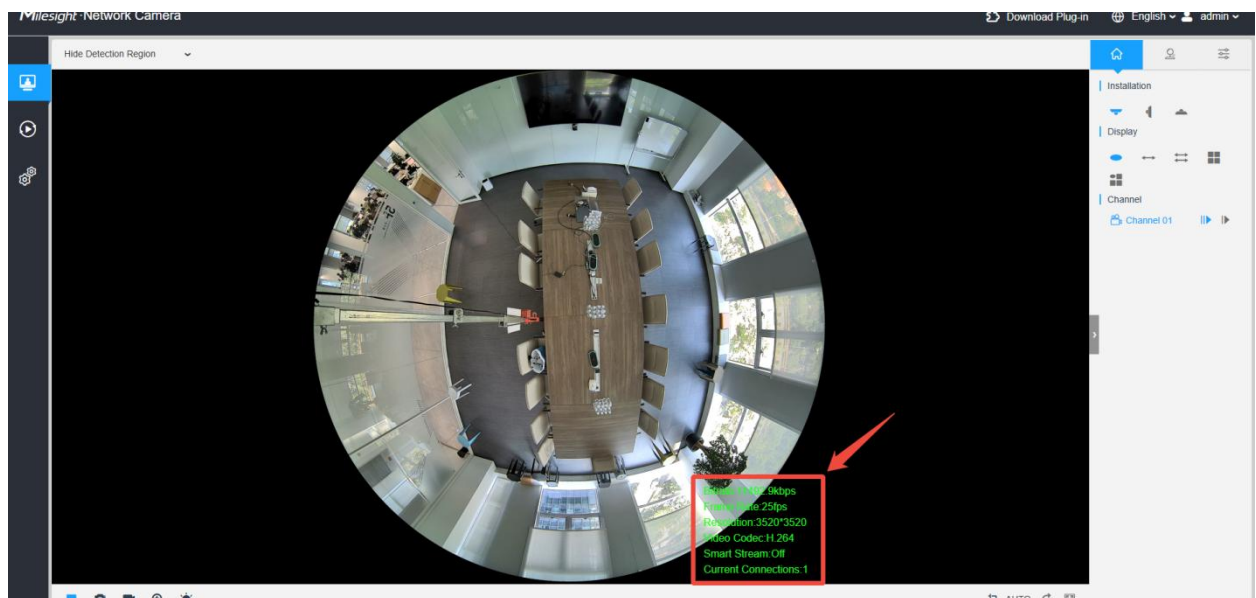
Frame Rate: Current frame rate

Resolution: Current resolution

Video Codec: Video encoding format (H.264/H.265)

Smart Stream: Smart Stream On/Off status

Current Connection: Active connection information



6.2 Fisheye Mode

Display Control allows you to select install type, display mode, window screen and channel of live view.

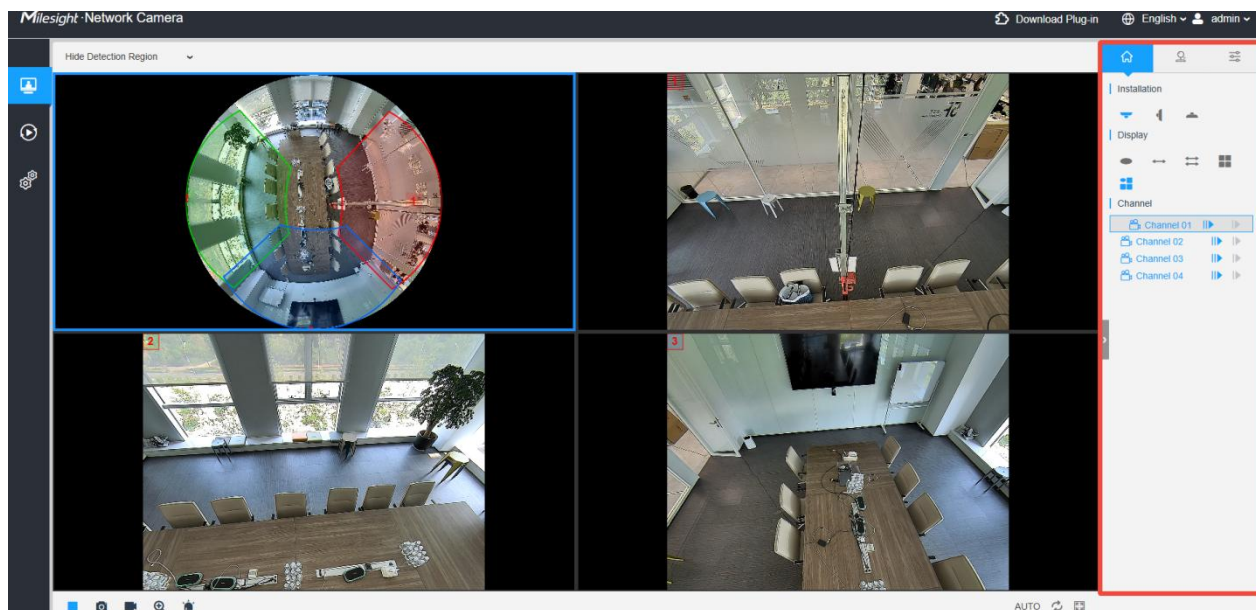


Table 4. Description of Display Control buttons

Item	Parameter	Description
Installation	 Ceiling Mounting	Camera is mounted on the ceiling (default)
	 Wall Mounting	Camera is mounted on the wall
	 Flat Mounting	Camera is placed on a flat surface
Display	 1O	Select live view of original fisheye view.
	 1P	Select live view of 360° panoramic view.
	 2P	Select live view of two 180° panoramic views.
	 4R	Select live view of four regional views.

 103R	Select live view of one original fisheye view and three regional views.
 Channel 01  (Only for Multi-Channel Mode)	Click to play this channel on any window of live view.

 Note:

- Original fisheye view: the whole wide-angle view of the fisheye camera is displayed.
- Panoramic view: the round fisheye image is transformed to rectangular image by certain calibration methods.
- Regional view: the close-up view of defined area in the original fisheye view or panoramic view.
- The available display modes may vary depending on the Installation mode (Ceiling/Wall/Flat).
- Different installation modes affect the dewarping algorithm and available display modes.

6.3 PTZ Control

PTZ Control allows you to use pan/tilt/zoom/preset/patrol function of PTZ, and set PTZ speed.

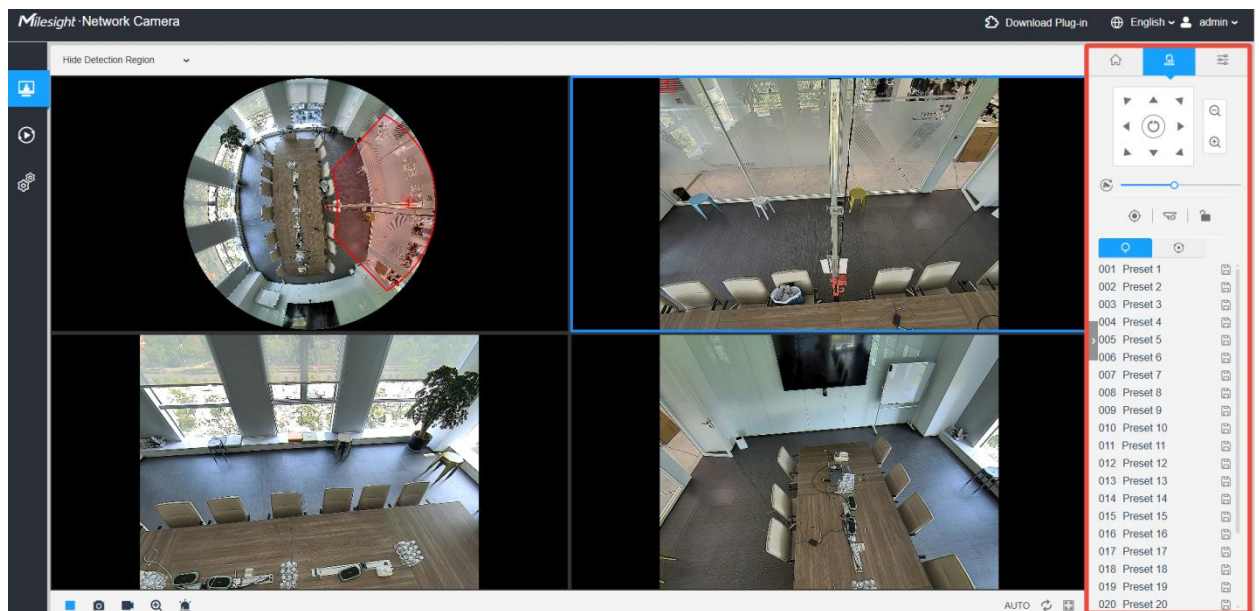
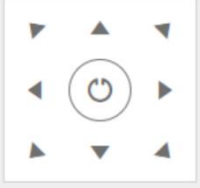


Table 5. Description of the buttons

No.	Parameter	Description
-----	-----------	-------------

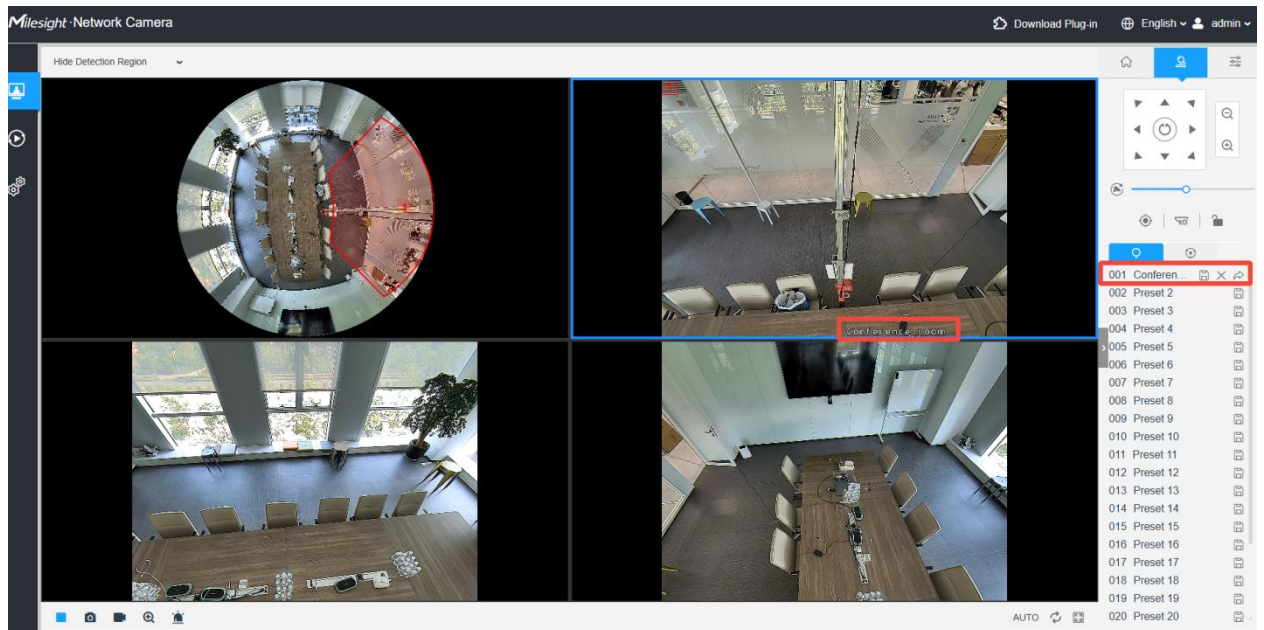
		Navigation key is used to control the direction. The rotation key is used for auto-rotation.
	PTZ Control	
		To adjust the speed of pan/tilt movements, from 1 to 10 .
	PTZ Speed	
		Click to zoom in and zoom out.
	Zoom-/Zoom+	
		Click to enable Manual Tracking. Click on a target in the live view to manually track it.
	Manual Tracking	
		Click to enable Auto Tracking mode, the camera can perform the digital Pan/Tilt/Zoom to track the moving objects automatically.  Note: • Auto Tracking is only supported in regional views.
	Auto Tracking	
		Click to lock/unlock the PTZ control. When PTZ Lock is enabled, all PTZ-related buttons (PTZ Control, Zoom) will be disabled to prevent accidental operation.
		Enable to set the preset positions for each regional view channel.
		Enable to set the patrol paths for each regional view channel.

6.3.1 Set / Call a Preset / Patrol

A preset is a predefined image position. You can click the call button from the preset list to quickly go to the desired image position.

Set a preset:

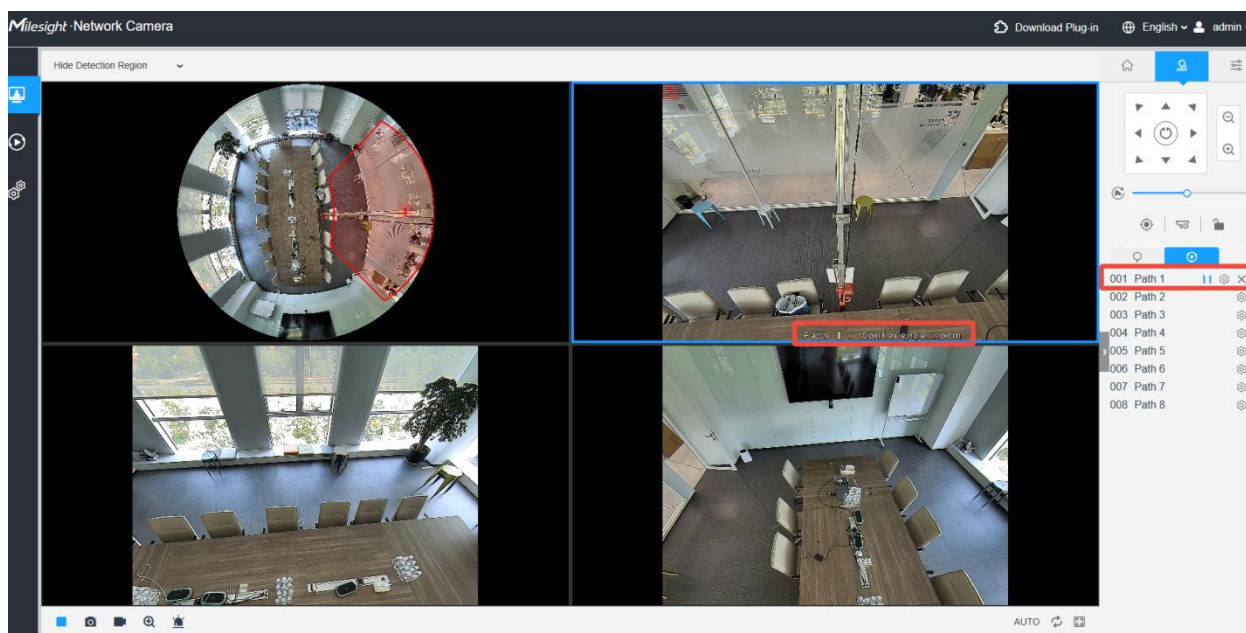
Step1: In the PTZ control panel, select a preset number from the preset list, and you can also customize the preset name displayed on the screen. The patrol name displayed on the screen will also be customized if you customize preset name and set a patrol as shown below;



Path 1 + × ↑ ↓

	Preset	Speed	Time
01	1	30	15
02	2	30	15
03	3	30	15

Save Cancel



Step2: Use the PTZ control buttons to move the lens to the interested position;

Step3: Click  to save the setting of the current preset;

Step4: Click  to delete the chosen preset.

 **Note:** Up to 300 presets can be configured (for each regional view channel).

Calling a preset:

Select a defined preset from the preset list and click  to call the preset.

001 road			
002 Preset 2			
003 Preset 3			
004 Preset 4			
005 Preset 5			
006 Preset 6			
007 Preset 7			
008 Preset 8			

Set / Call a patrol

A patrol is a memorized series of preset function. It can be configured and called on the patrol setting list. You can customize up to 8 patrols and it can be configured with 48 presets. Before configuring

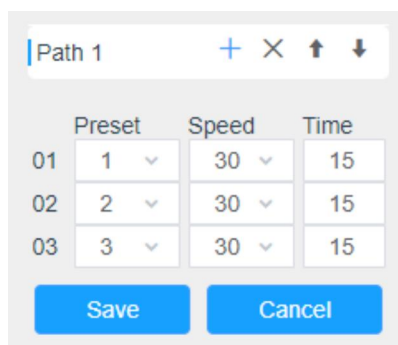
the patrol, you should make sure that the presets you want to add to the patrol have been defined.

Set a patrol:

Step1: In the PTZ control panel, click  to enter the patrol settings interface;

Step2: Select a patrol number, the setting icon will appear , click it;

Step3: Click  to add presets to this patrol, as shown in Figure;



	Preset	Speed	Time
01	1	30	15
02	2	30	15
03	3	30	15

Save Cancel

Step4: Configure the preset number, patrol speed and patrol time;

Table 6. Description of Patrol Settings

Name	Description
Patrol Speed	The speed of moving from one preset to another.
Patrol Time	The duration staying on one patrol point. The PTZ camera moves to another patrol point after the set patrol time.

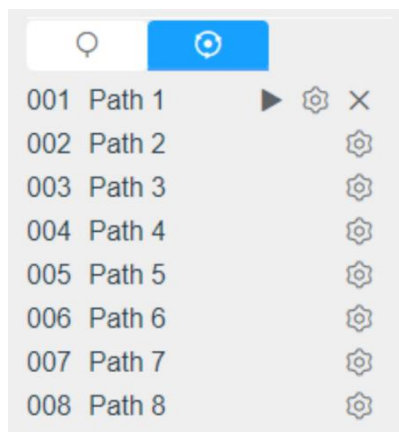
Step5: Click  to save the patrol settings.

 **Note:**

- Patrol Speed only works in Patrol mode.

Call a patrol:

In the PTZ control panel, select a defined patrol from the patrol list, and click  to call the patrol, as shown below.



 **Note:** The three buttons behind the Patrol list means: Play, Set and Delete.

6.4 Image Configuration

The Image Configuration panel on the Live View page provides quick access to image settings. Users can adjust Brightness, Contrast, Saturation, Sharpness, Digital Rotation and other image parameters directly on the live view page.

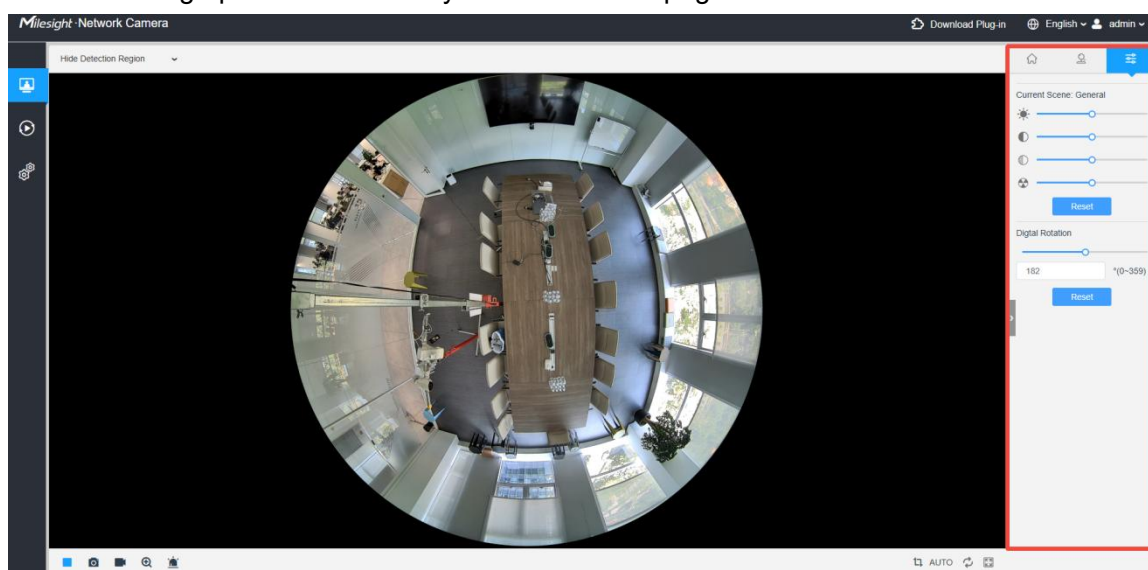
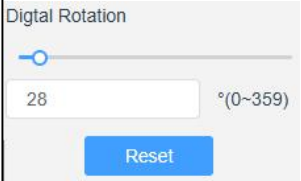


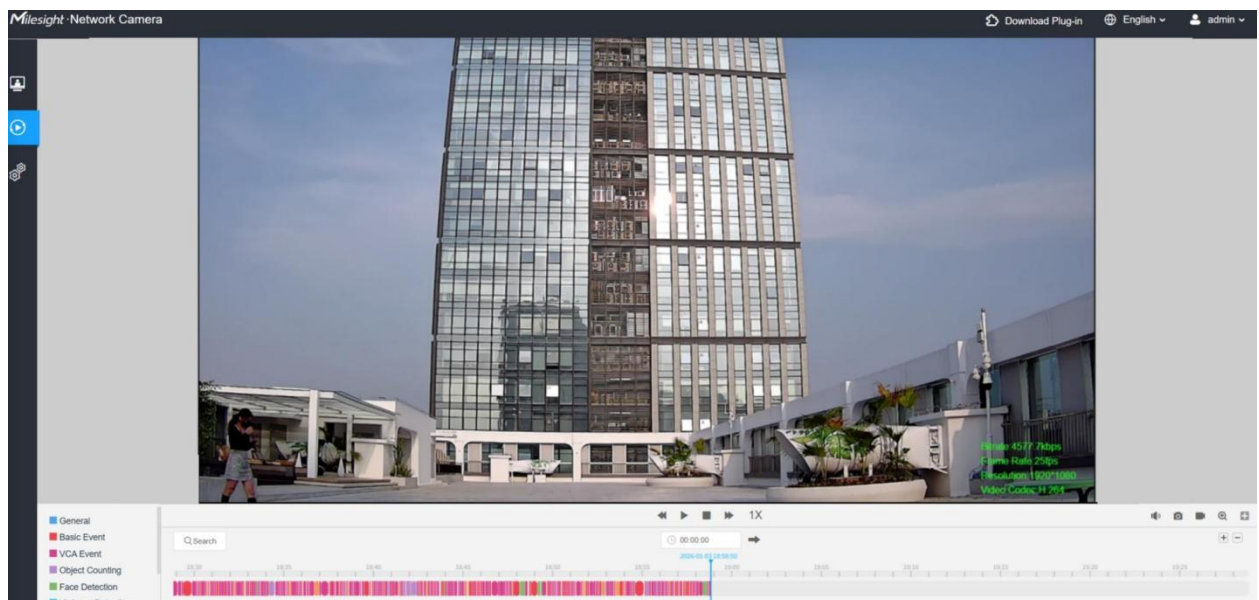
Table 7. Description

No.	Name	Description
	Configuration Scope: Global Current Scene: General  Reset	Brightness: Adjust the Brightness of the scene. Contrast: Adjust the color and light contrast. Saturation: Adjust the Saturation of the image. Higher Saturation makes colors appear more "pure" while lower one appears more "wash-out". Sharpness: Adjust the Sharpness of image. Higher Sharpness sharpens the pixel boundary and makes the image looks "more clear". Reset: Click to reset all configuration values on the current page to the default midpoint (50).

	Users can rotate the original view of the camera image either by dragging the slider or by directly entering a value in the web interface. This allows for easy adjustment of the image orientation without the need to physically reinstall or reposition the camera, improving installation convenience and usability.
---	--

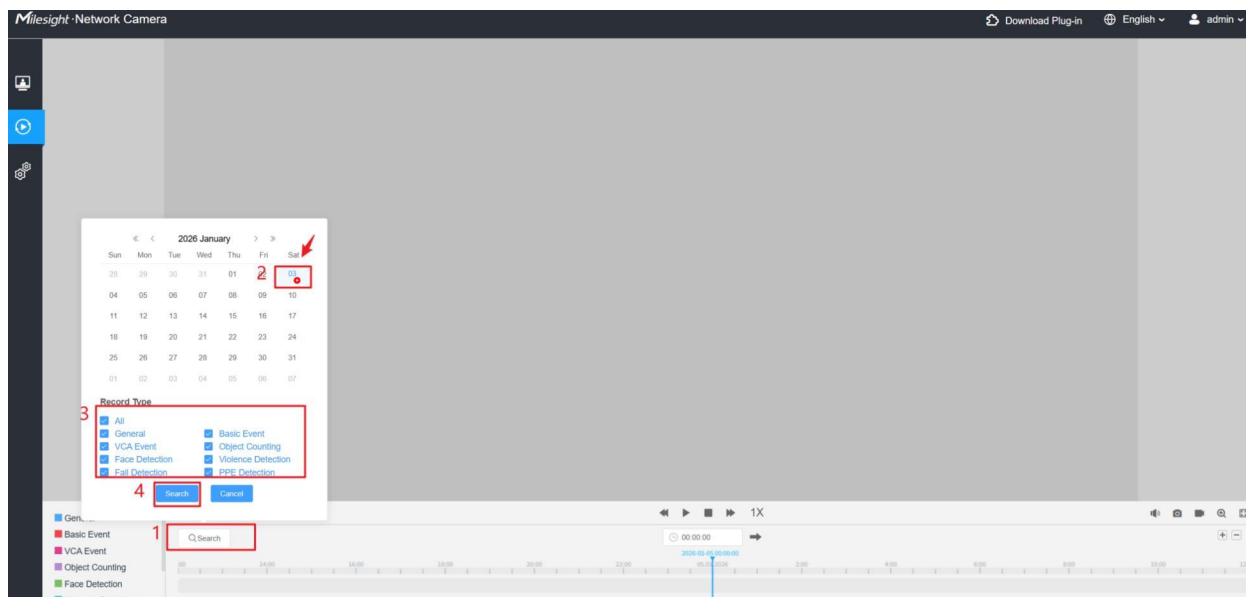
Chapter 7. Playback

Click  to enter playback interface. In this part, you can search and playback the recorded video files stored in SD cards or NAS. The Playback interface is as below:



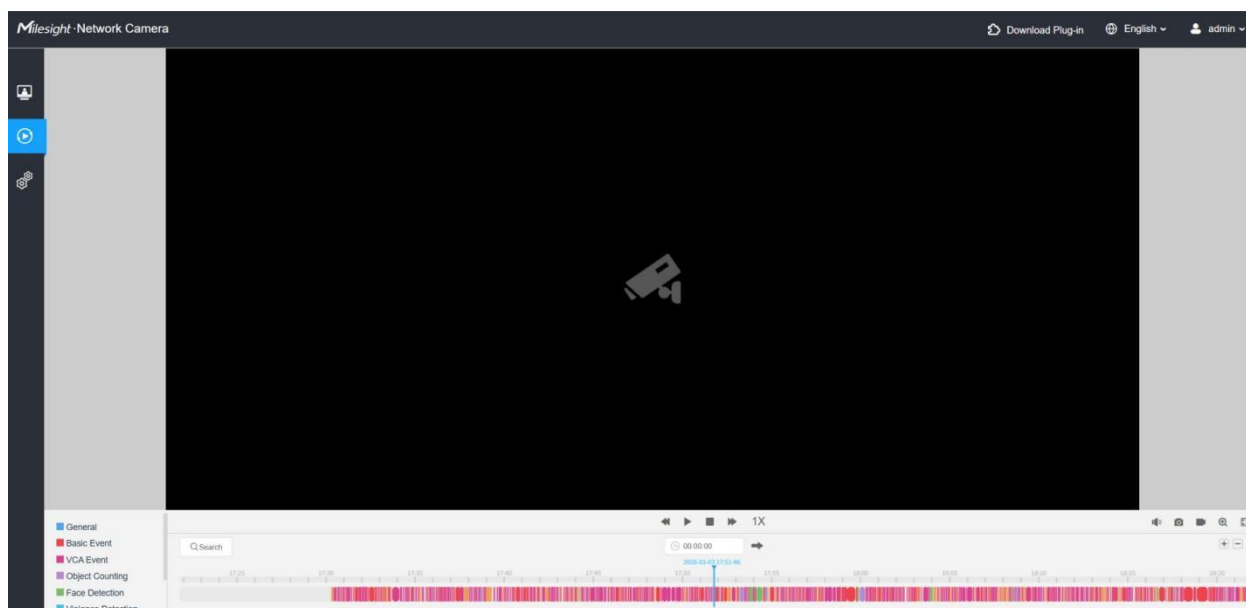
Step1: Click the Search button, choose the data and record type when the window pops up.

 **Note:** A red icon will appear under the corresponding date when there is a recording for that day users can quickly identify which dates have recordings.



Step2: The timeline displays the video files for the day and show different colors according to selected record type. Drag the progress bar with the mouse to locate the exact playback point as needed.

Note: You can also input the time and click  to locate the playback point in the filed. You can also click  to zoom out/in the progress bar.



Step3: Click  to play the video files found on this date. The toolbar on the bottom of playback interface can be used to control playing progress.

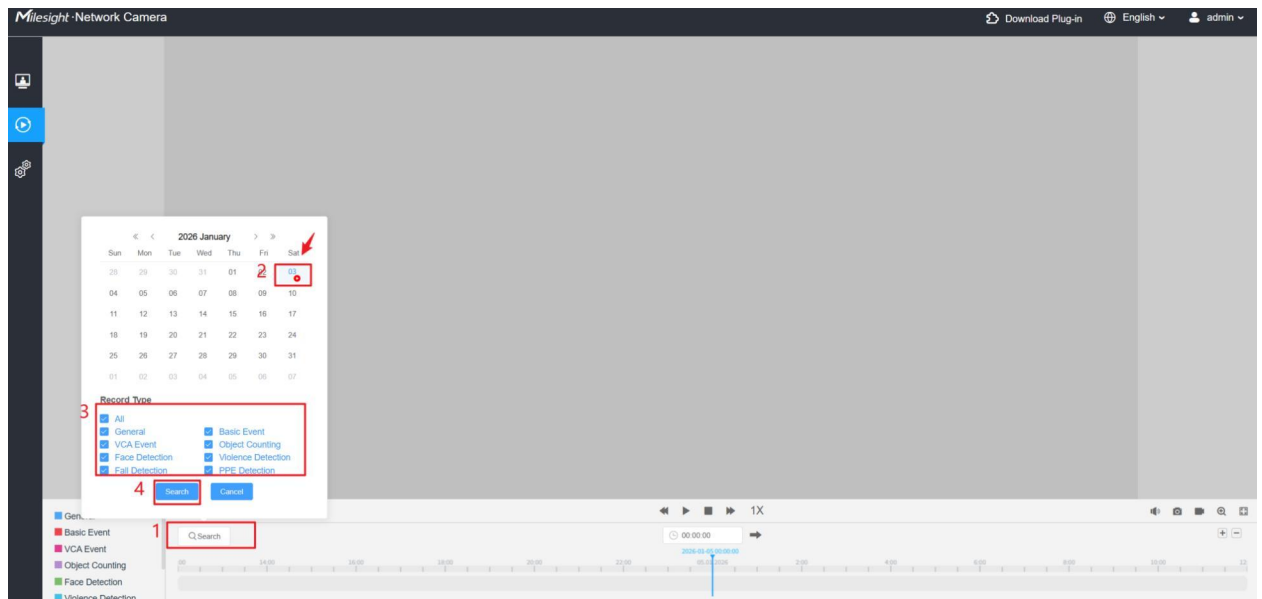
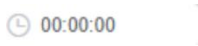


Table 8. Description of the buttons

No.	Parameter	Description
1	 Play/Pause	Play/Pause the video.
2	 Stop	Stop the video.
3	 Search Time	Select the time point that you want to locate.
4	 Jump	Click it to jump to the time point corresponding to the search.
5	 Mute	Click to disable/enable the audio.
6	 Snapshot	Click to take a snapshot.
7	 Start/Stop recording	Click to start/stop recording.
8	 Digital Zoom	Click to zoom on/off.

9	 Full Screen	Full Screen.
10	 Time Expand/Narrow	Time narrow/expand.

Chapter 8. Settings

8.1 Media

8.1.1 Video

Stream parameters can be set in this module, adapting to different network environments and demands.

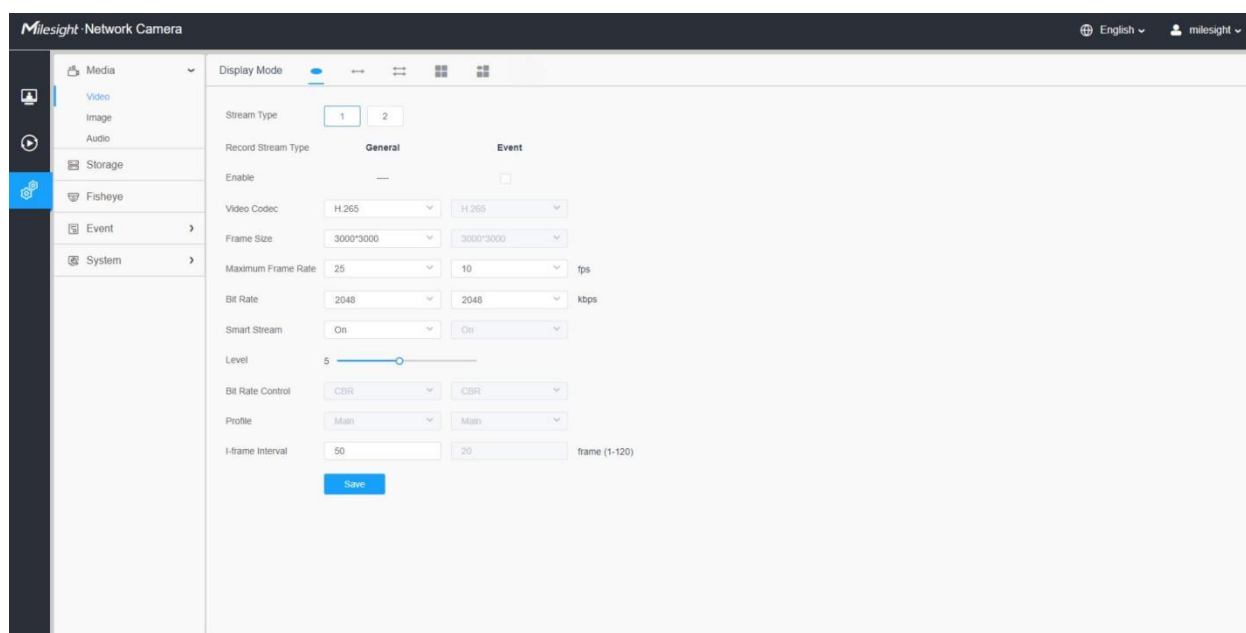


Table 9. Description of the buttons

Parameters	Function Introduction
Channel (Only for Multi-Channel Mode)	In Multi-Channel Mode, each dewarped view from the camera is an independent channel, so you can configure video settings for each channel separately. The number of available channels depends on the selected display mode: 1O and 1P display one channel, 2P displays two channels, and 4R and 1O3R display four channels.  Note: In Bundle-Stream Mode, all dewarped views are combined into a single channel. You can only configure video settings for this channel as a whole.
Display Mode	1O/1P/2P/4R/1O3R are available
Stream Type	Primary Stream/Secondary Stream are available.
Record Stream Type	General & Event are available only for Primary Stream. General refers to continuous record video, while Event includes events that can trigger alarms, such as Motion, Exception, LPR and so on. This item can separately set different bit rate and frame rate for different Recording Stream Types. If user chooses Event, video will be recorded according to the configuration of video stream type when an event happens, thereby greatly reducing the recording storage space.
Enable Event Stream	This item is optional only if you selected the Event. Note: The event stream type is supported only under the following conditions: 1. Channel 1 in 1O or 1O3R configurations in Multi-Channel Mode, or Channel 1 in 1O configuration in Bundle-Stream Mode; 2. The primary stream.
Video Codec	H.265/ H.264 are available.  Note: For more details about Milesight-H.264 VS H.265+, you can click to the YouTube: https://www.youtube.com/watch?v=Wkom8HQ00jI

Parameters	Function Introduction
Frame Size	Choose a proper stream resolution. The higher the resolution is, the more details the image has.
Maximum Frame Rate	Maximum refresh frame rate of per second and it is variable according to the mode. Range from 1 to 30/25.
Bit Rate	Transmitting bits of data per second. Set the bitrate to 32~16384 Kbps. The higher value corresponds to the higher video quality, and the higher bandwidth is required as well.
Smart Stream	Optional to turn On/Off Smart Stream mode. Smart Stream mode remarkably reduces the bandwidth and the data storage requirements for network cameras while ensuring the high quality of images, and it is a 10-level adjustable codec. Level: Level 1~10 are available as needed.
Bit Rate Control	CBR: Constant Bitrate. The rate of CBR output is constant. VBR: Variable Bitrate. VBR files vary the amount of output data per time segment.
Image Quality	Low/Medium/High are available, this item is optional only if you select VBR.
Profile	The option is for H.264, Main/High/Base can be selected as needed.
I-frame Interval	Set the I-frame interval to 1~120, 25 for the default. The number must be a multiple of the number of frames.

8.1.2 Image

General settings of image including the image adjustment, day/night setting and image enhancement can be set in this module. OSD (On Screen Display) content, privacy mask, ROI (Region of Interest), and video time can be displayed to enrich the image information.

8.1.2.1 General

General settings of image including the Image Adjustment, Day/Night Switch, Day/Night Parameters, Exposure, Backlight, White Balance, Image Enhancement, and Display can be set in this module.

[Digital Rotation]

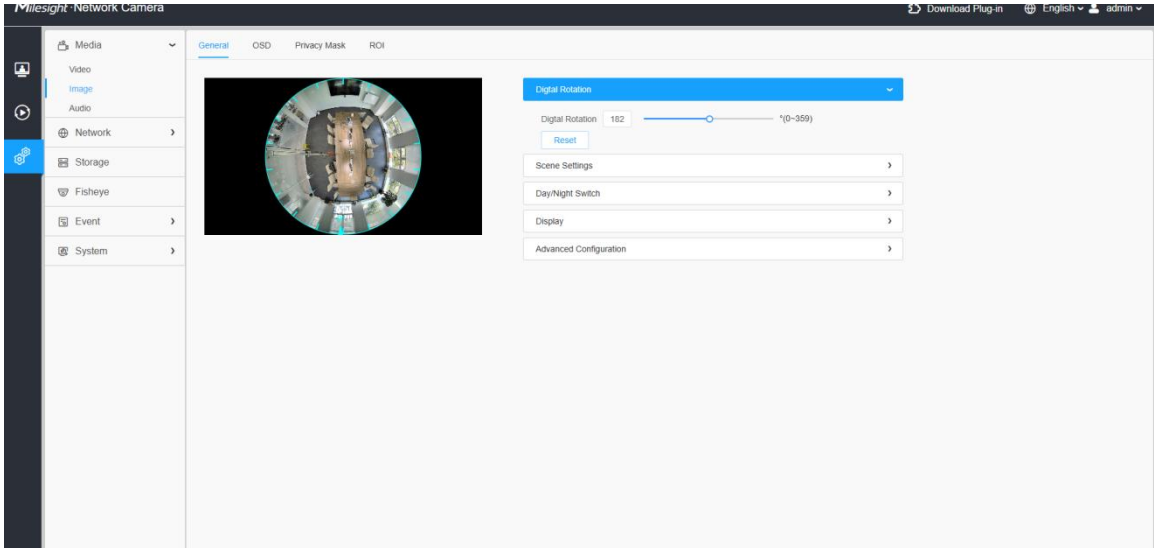
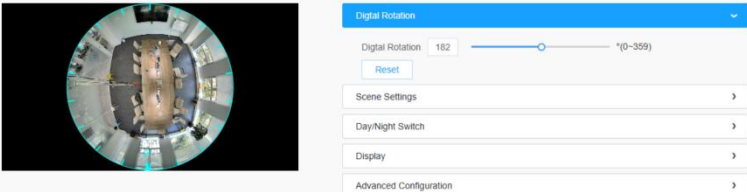


Table 10. Description of Patrol Settings

Name	Description
Digital Rotation	Users can rotate the original view of the camera image either by dragging the slider or by directly entering a value in the web interface. This allows for easy adjustment of the image orientation without the need to physically reinstall or reposition the camera, improving installation convenience and usability. To further assist with precise configuration, a scale is displayed on the original view, providing clear visual feedback during adjustment. 

[Scene Settings]

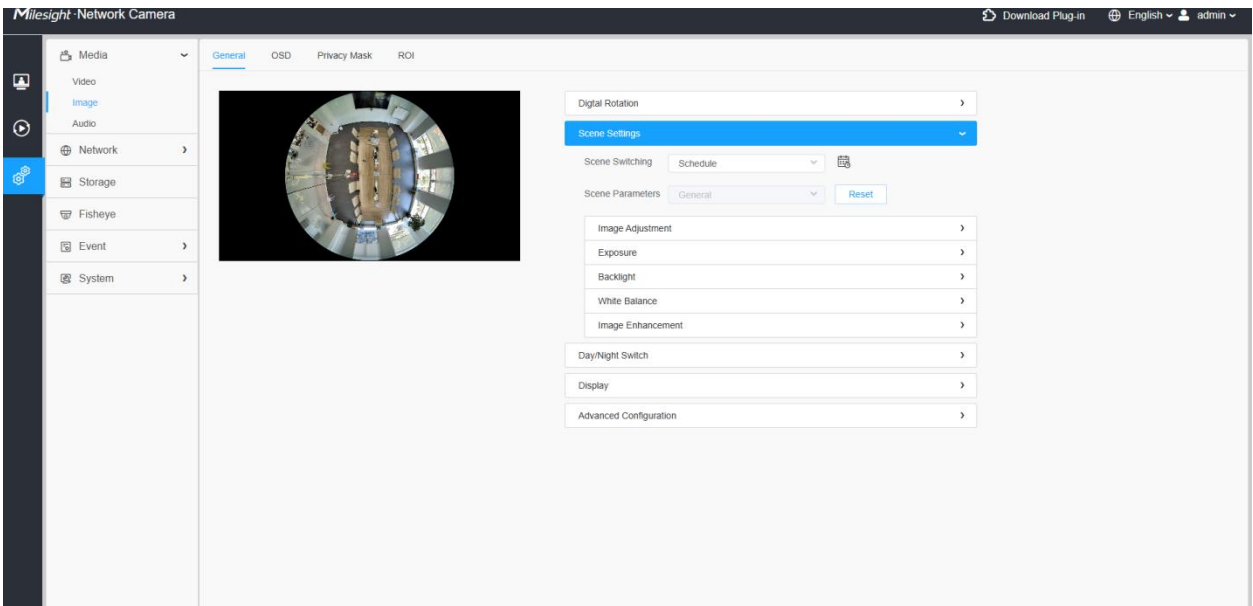
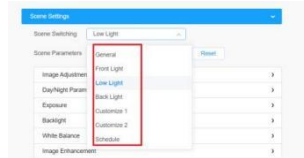
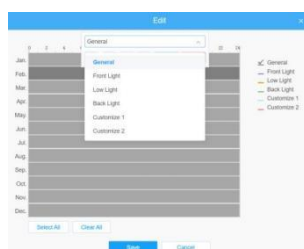


Table 11. Description of the buttons

Parameters	Function Introduction
Scene Switching	You can switch scenarios here. General, Front Light, Low Light, Back Light, Customize 1, Customize 2, and Schedule are available. You can set parameters for each scene displayed in the following figure:  General: Default scene mode optimized for typical surveillance environments such as brightly daytime, providing balanced image quality under normal lighting conditions. Front Light: A mode designed to counteract strong light sources coming from the front of the camera, preventing overexposure and ensuring clear visibility of subjects facing the light. Low Light: A mode designed to optimize image quality in nighttime or low- light environments, improving brightness and noise control. Back Light: A mode designed to address backlight environments to prevent subjects from appearing dark and backgrounds from being overexposed. Customize 1/Customize 2: These two modes allow you to save your own customized image settings for use in special scenarios. Schedule: The Schedule mode allows you to set a time-based timetable to automatically switch the camera's scene profiles. 

Scene Settings--> Image Adjustment

Digital Rotation

Scene Settings

Scene Switching

Schedule

Scene Parameters

General

Reset

Image Adjustment

Brightness

50

Contrast

50

Saturation

50

Sharpness

50

Reset

Exposure

Backlight

White Balance

Image Enhancement

Day/Night Switch

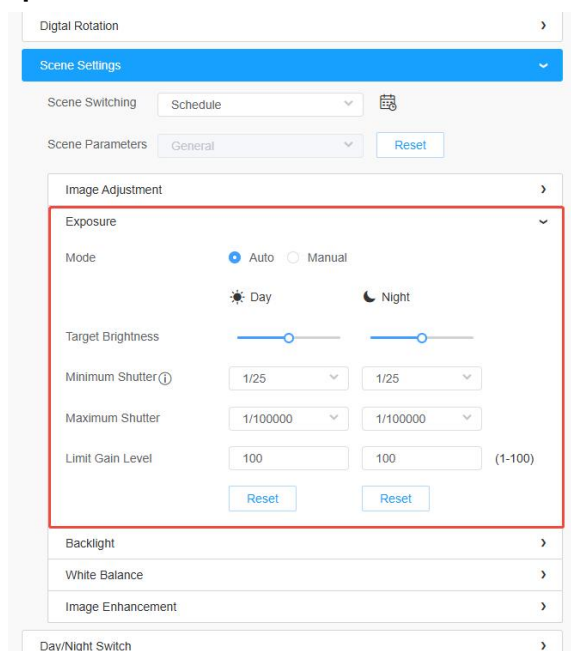
Display

Advanced Configuration

Table 12. Description of the buttons

Parameters	Function Introduction
Brightness	Adjust the Brightness of the scene.
Contrast	Adjust the color and light contrast.
Saturation	Adjust the Saturation of the image. Higher Saturation makes colors appear more "pure" while lower one appears more "wash-out".
Sharpness	Adjust the Sharpness of the image. Higher Sharpness sharpens the pixel boundary and makes the image look "more clear".
	Reset the image adjustment parameters to their default values.

Scene Settings--> Exposure



Digital Rotation >

Scene Settings >

Scene Switching Schedule >

Scene Parameters General > Reset

Image Adjustment >

Exposure >

Mode ☒ Auto ☐ Manual

Day Night

Target Brightness

Minimum Shutter ① 1/25 1/25

Maximum Shutter 1/100000 1/100000

Limit Gain Level 100 100 (1-100)

Reset Reset

Backlight >

White Balance >

Image Enhancement >

Day/Night Switch >

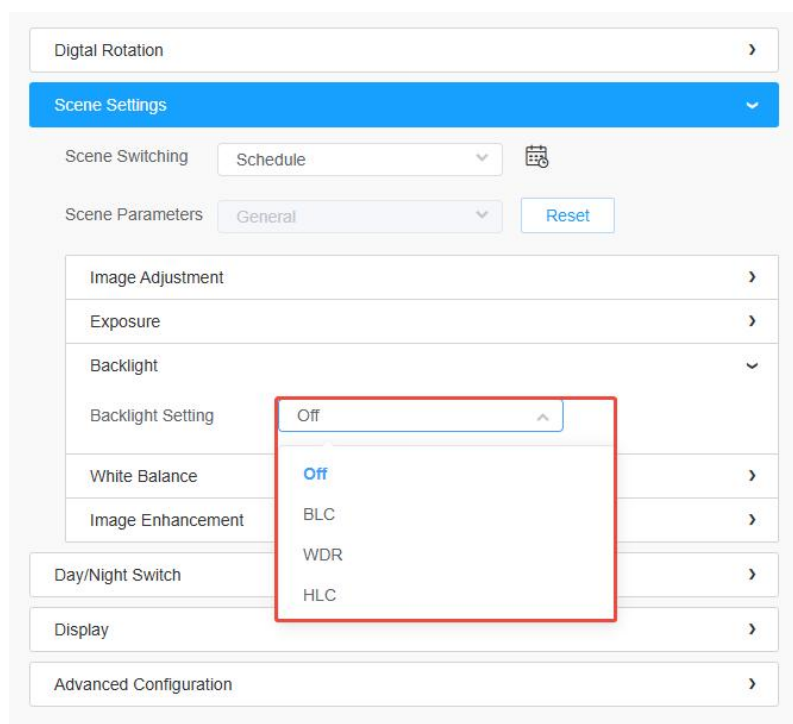
Table 13. Description of the buttons

Parameters	Function Introduction
Exposure Mode	Auto Mode and Manual Mode are available. Auto Mode: The camera will adjust the brightness according to the light environment automatically. Manual Mode: The camera will adjust the brightness according to the value you set, you can configure the shutter time from 1~1/100000s and set Gain Level from 1~100 (default value: 50), the higher the gain value is, the brighter the image is. If Power Line Frequency is set as 50 Hz, 1, 1/5, 1/10, 1/25, 1/50, 1/100, 1/250, 1/500, 1/750, 1/1000, 1/2000, 1/4000, 1/10000, and 1/100000 are available. If Power Line Frequency is set as 60 Hz, 1, 1/5, 1/15, 1/30, 1/60, 1/120, 1/250, 1/500, 1/750, 1/1000, 1/2000, 1/4000, 1/10000, and 1/100000 are available.

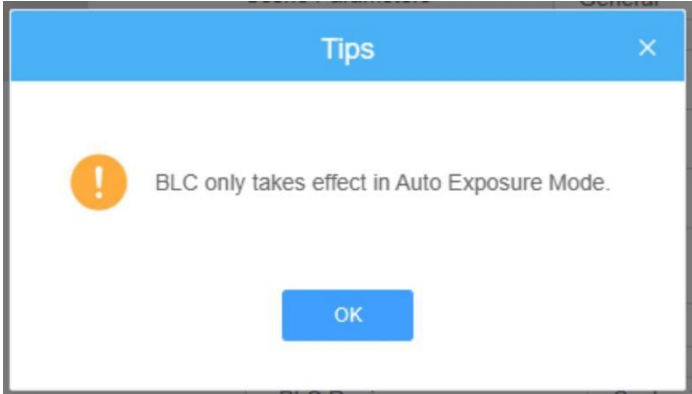
Target Brightness	When the exposure is set to Auto mode, the image brightness will be adjusted to the predefined value when exposure changes occur.
Minimum Shutter	Minimum Shutter is the same as Maximum Exposure Time. The default option is 1/25.
Maximum Shutter	Maximum Shutter is the same as Minimum Exposure Time. The default option is 1/100000.
Limit Gain Level	Set the maximum gain level to 1~100. The default value is 100.

**Note:**

1. Both Minimum Shutter and Maximum Shutter now support an Auto option. Enabling Auto activates Frame Rate Reduction technology, which improves static image quality in low-light environments by reducing the frame rate, extending the exposure time per frame, increasing brightness, and minimizing noise.
2. When the Shutter is set to Auto, static images will appear brighter with reduced noise, but moving objects may experience motion blur.

Scene Settings--> Backlight**Table 14. Description of the buttons**

Parameters	Function Introduction
------------	-----------------------

Backlight Mode	Backlight Setting: Off, BLC, WDR, HLC and Auto-WDR are available for detailed configurations. The default setting is "Off". Select BLC to customize its region or use the default center one; select WDR to set its level to High, Low, or Auto; select HLC to adjust its level from 0 to 100. Auto WDR: Automatically enables or disables WDR in high#contrast environments. This function is unavailable in Manual mode or when the frame rate exceeds 30 fps.  Note: - To enable WDR, BLC, and HLC, you must set the exposure to Auto mode.  - Do not support WDR while High Frame Rate is enabled.
----------------	---

Scene Settings--> White Balance

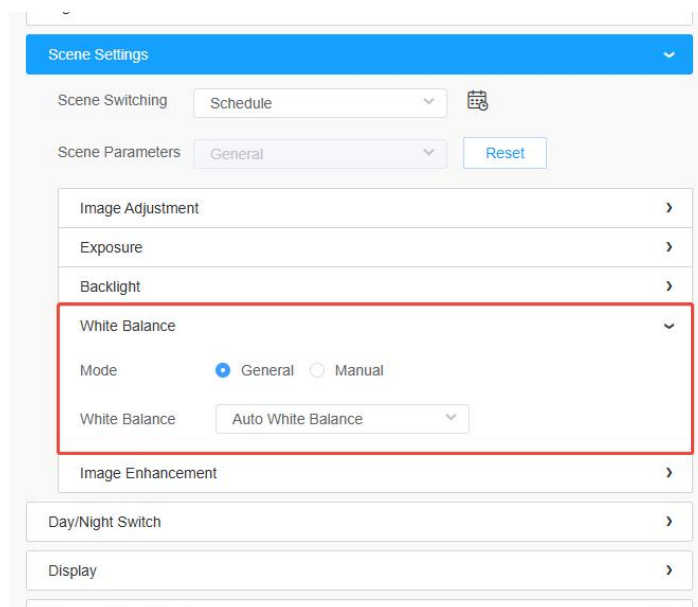


Table 15. Description of the buttons

Parameters	Function Introduction
White Balance	To restore white objects, remove color distortion caused by the light of the environment.

Mode	General and Manual are available. Manual > Manual White Balance Settings: Set Red Gain Level and Blue Gain Level manually. General Mode: Select a white balance mode as required • Auto White Balance: This option will automatically enable the White Balance function. • Incandescent Lamp: Select this option when light is similar with incandescent lamp. • Warm Light Lamp: Select this option when light is similar with warm light lamp. • Natural Light: Select this option when there is no other light but natural light. • Fluorescent Lamp: Select this option when light is similar with Fluorescent Lamp.
------	--

Scene Settings--> Image Enhancement

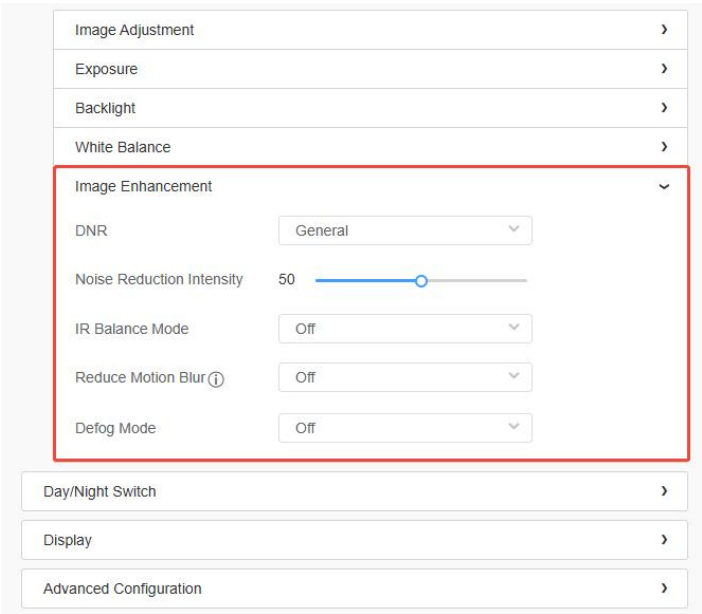
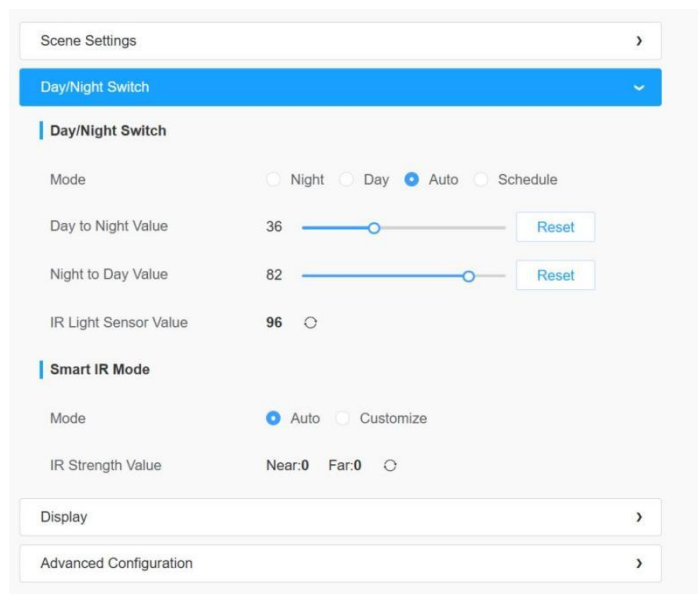


Table 16. Description of the buttons

Parameters	Function Introduction
DNR	Choose the DNR mode, General and Expert Mode are available. General: Automatically adjust noise reduction using algorithms. Expert Mode: You can manually adjust the 3D and 2D DNR settings to reduce image noise. DNR Expert Mode 2D DNR 50 3D DNR 50 IR Balance Mode Off Reduce Motion Blur ⓘ Off Defog Mode Off

Noise Reduction Intensity	Adjust the bar to set the DNR level, a higher level indicates stronger DNR capabilities, the range of adjustment is from 0 -100, with a default value of 50.
IR Balance Mode	There is an option to avoid IR overexposure. IR Balance Mode would avoid the problem of overexposure and darkness, and the IR LED will change according to the actual illumination.
Reduce Motion Blur	Enable this function to reduce the motion blur of objects effectively. You can adjust the deblur level from 1 to 100.  Note: When Reduce Motion Blur and Shutter Auto mode are enabled at the same time, only Reduce Motion Blur will take effect.  Note: For more details about Milesight Deblur, you can click to the YouTube: https://www.youtube.com/watch?v=-vynrami51s
Defog Mode	Better image effect in foggy weather. Anti-fog Intensity can be adjusted from 0 to 100, with a default value of 50.  Note: For more details about Milesight Defog, you can click to the YouTube: https://www.youtube.com/watch?v=a9od7Trao4U

[Day/Night Switch]



Scene Settings >

Day/Night Switch ▾

Day/Night Switch

Mode ☐ Night ☐ Day ☒ Auto ☐ Schedule

Day to Night Value 36 Reset

Night to Day Value 82 Reset

IR Light Sensor Value 96

Smart IR Mode

Mode ☒ Auto ☐ Customize

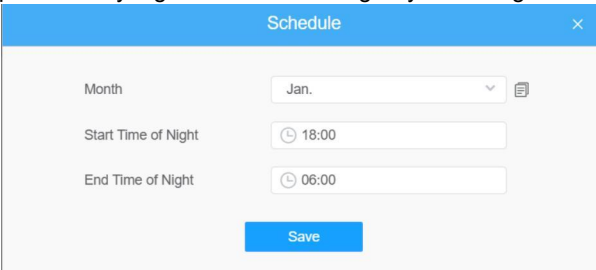
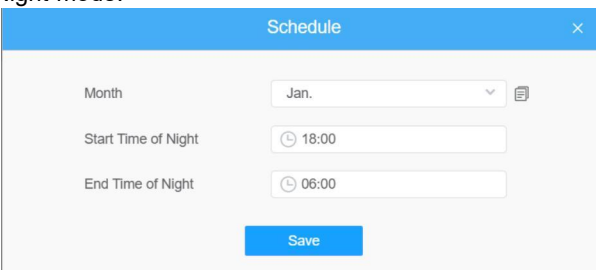
IR Strength Value Near:0 Far:0

Display >

Advanced Configuration >

Table 17. Description of the buttons

Parameters	Function Introduction
------------	-----------------------

Day/Night Switch	Night: Shown in live view based on Night Mode settings. Day: Shown in live view based on Day Mode settings. Auto: Shown in live view based on environment, set the sensitivity for switching Day Mode to Night Mode, or Night Mode to Day Mode. - Day to Night Sensitivity: You can set the sensitivity for switching Day Mode to Night Mode. You can click  to reset the value to 5. - Night to Day Sensitivity: This is the sensitivity for switching Night Mode to Day Mode. You can click  to reset the value to 5.  Note: The two parameters are only for Auto mode. - IR Light Sensor Value: When IR light sensor value is lower than day to night sensitivity value, it will switch Day Mode to Night Mode. When IR light sensor value is higher than night to day sensitivity value, it will switch Night Mode to Day Mode. Schedule: Shown in the live view based on your schedule. You can configure the month, start time, and end time to perform day/night switch. Click  to set the month, start time, and end time. Once done, the camera will perform day/night switch according to your configurations.  Month: Select a month for your schedule. Start time of Night: Set the time for starting the Night mode. End time of Night: Set the time for ending the Night mode. 
Smart IR Mode	Customize Mode: Allows you to adjust LED brightness from 0 to 100 to suit your environment. Click Reset to restore all LEDs to 50.

[Display]

Digital Rotation

Scene Settings

Day/Night Switch

Display

Power Line Frequency 50Hz

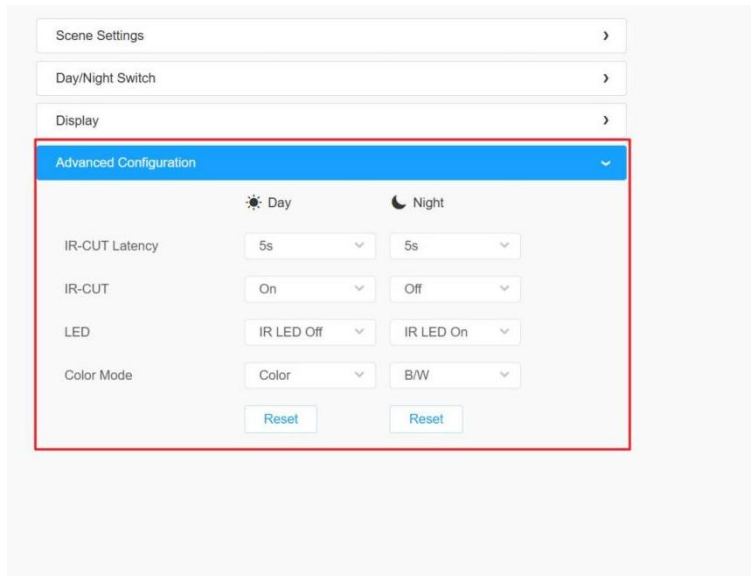
Advanced Configuration

Table 18. Description of the buttons

Parameters	Function Introduction
Power Line Frequency	60Hz and 50Hz are available to help prevent flickering and horizontal lines in the image.

[Advanced Configuration]

You can set the following parameters for Day and Night modes respectively.

**Table 19. Description of the buttons**

Parameters	Function Introduction
IR-CUT Latency	IR-CUT Latency sets the waiting time for the camera's infrared filter to engage or disengage when switching between day and night modes. Select the IR-cut latency time from 1 to 20 seconds.
IR-CUT	Select On to activate the infrared cut filter to block ambient infrared light. Select Off to allow infrared light to reach the sensor.
LED	LED is an auxiliary light source for cameras that emits invisible infrared light in low-light environments to supplement illumination for the camera, enabling the sensor to capture clear images in dark conditions. You can select IR LED On or IR LED Off.
Color Mode	Color Mode is the camera's imaging mode selection, which allows switching between Color and B/W modes to adapt to different lighting conditions and balance image color and night vision performance. Color and B/W are available.
	Click it to reset the configurations.

8.1.2.2 OSD

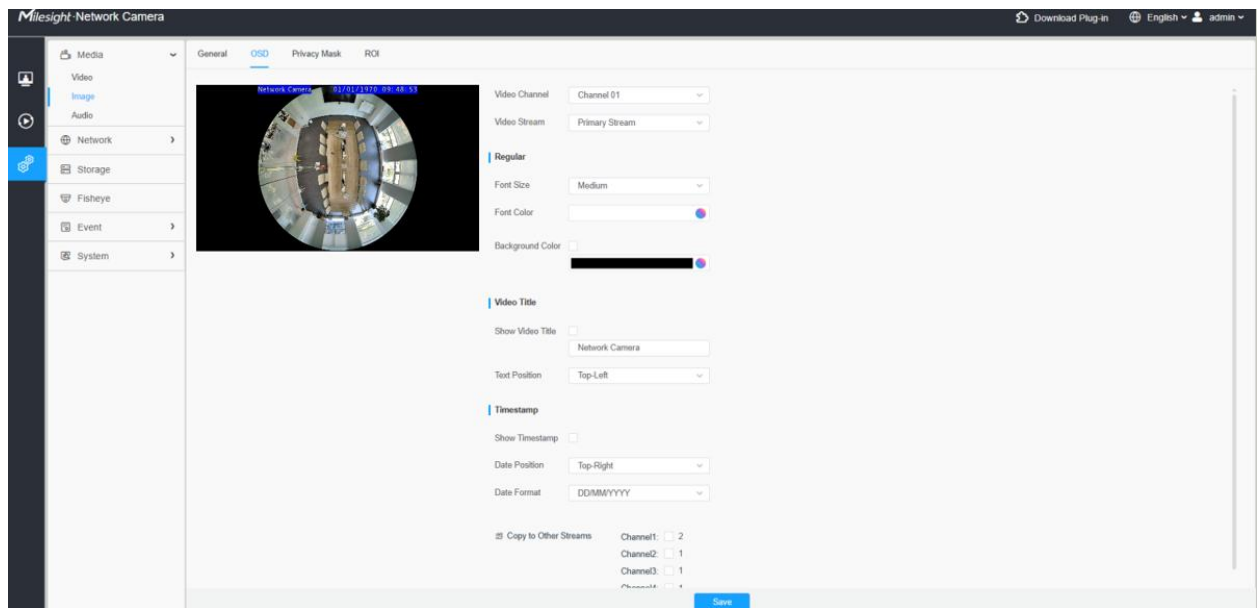


Table 20. Description of the buttons

Parameters	Function Introduction
Video Channel	Enable OSD configuration for different channels
Video Stream	Enable to set OSD for the primary stream and secondary stream.
Font Size	Smallest/Small/Medium/Large/Largest/Auto are available for title and date.
Font Color	Enable to set different color for title and date.
Background Color	Enable to set different colors for display information background on screen. You can set different colors for font and background of image, then the image OSD will show as below: 
Show Video Title	Check the check box to show video title.
Video Title	Customize the OSD content to be displayed as the video title.

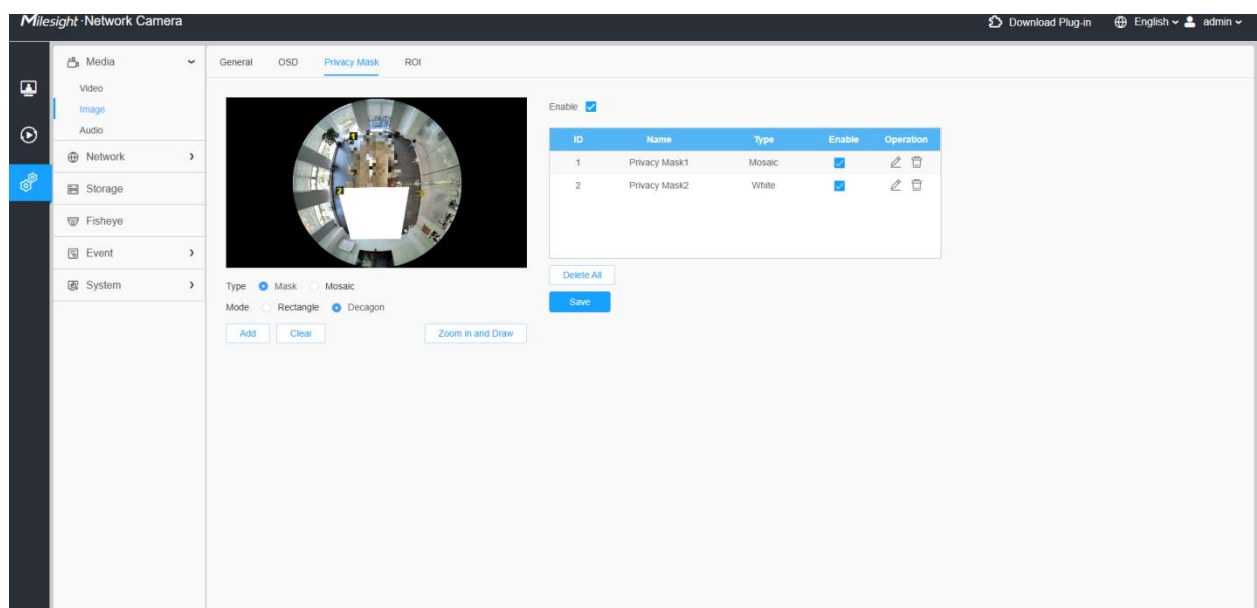
Text Position	OSD display position on the image.
Show Timestamp	Check the checkbox to display date on the image.
Date Position	Date display position on the image.
Date Format	The format of date.
Copy to Other Streams	Copy the settings to other streams and channels.

8.1.2.3 Privacy Mask

Privacy mask enables to cover certain areas on the live video to prevent certain spots in the surveillance area from being viewed and recorded.

Note:

1. This feature is only available in the original channel.
2. Privacy Mask can only be drawn when Digital Rotation is 0°.



You can configure privacy mask to cover certain areas on the live video.

Step1: Check the checkbox to enable the Privacy Mask function.

Step2: Select the mask type (Mask or Mosaic).

Step3: Draw the privacy mask area on the live video.

Note: Privacy Mask supports up to 8 areas. You can draw Rectangle, Polygon or Decagon shapes. Decagon provides a 10-sided polygon for more precise area coverage.

Table 21. Description of the buttons

Parameters	Function Introduction
Enable	Check the check box to enable the Privacy Mask function.

Type	Select the type to use for the privacy areas, there are two types available: Mask and Mosaic. Select the color to use for the privacy areas, there are eight colors available: White, Black, Blue, Yellow, Green, Brown, Red and Purple. When the privacy type is set to Mask, you can select a color for the privacy areas, eight colors are available: White, Black, Blue, Yellow, Green, Brown, Red and Purple. The Mosaic type is also available as an alternative privacy option.	
	Draw a privacy area on the live video as needed.	
	By clicking the 'Zoom in and Draw' button, you can activate a full-screen pop-up window to draw more accurate detection areas.	
Operation	 	Enable/disable the selected ROI areas.
Operation		Change the color of Mask area, there are eight colors available: White, Black, Blue, Yellow, Green, Brown, Red and Purple
		Delete the privacy mask area
	Clear the area you drew on the live video.	
	Clear all areas you drew before.	

8.1.2.4 ROI

Region of interest (ROI) is a selected subset of samples within a dataset identified for a particular purpose. Users can select up to 8 key regions of a scene to transmit through separate streams for targeted preview and recording.

By using Milesight ROI technology, more than 50% of bit rate can be saved and therefore less bandwidth demanded and the storage usage reduced. So according to this, you can set a small bit rate for high resolution.

 **Note:** For more details about how to set ROI, please refer to <https://milesight.freshdesk.com/a/solutions/articles/69000643441>.

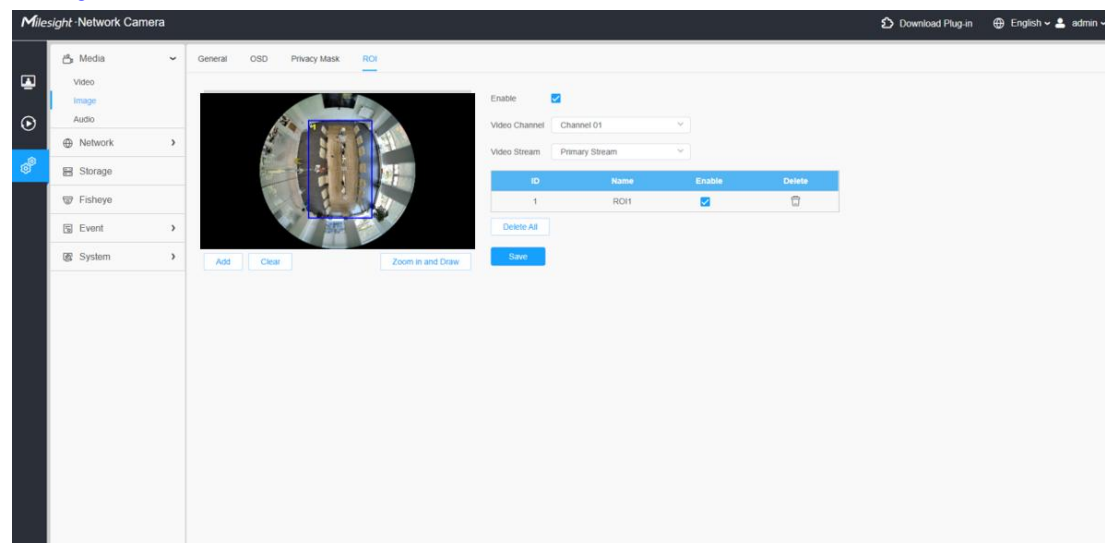
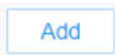
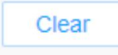


Table 22. Description of the buttons

Parameters	Function Introduction	
Enable	Check the checkbox to enable the ROI function.	
Video Channel	Enable ROI for different channels.	
Video Stream	Choose the video stream. Primary Stream and Secondary Stream are supported.	
ROI		Enable/disable the selected ROI areas.
		Delete the selected ROI areas.
	Drew a ROI area on the live video as needed.	
	Clear the area you drew on the live video.	
	By clicking the 'Zoom in and Draw' button, you can activate a full-screen pop-up window to draw more accurate detection areas.	
	Clear all areas you drew before.	

8.1.3 Audio

8.1.3.1 Audio

This audio function allows you to hear the sound from the camera or transmit your sound to the camera side. A two-way communication is also possible to be achieved with this feature. Alarm can be triggered when the audio input is above a certain alarm level you set, and configured audio can be played when an alarm occurs.

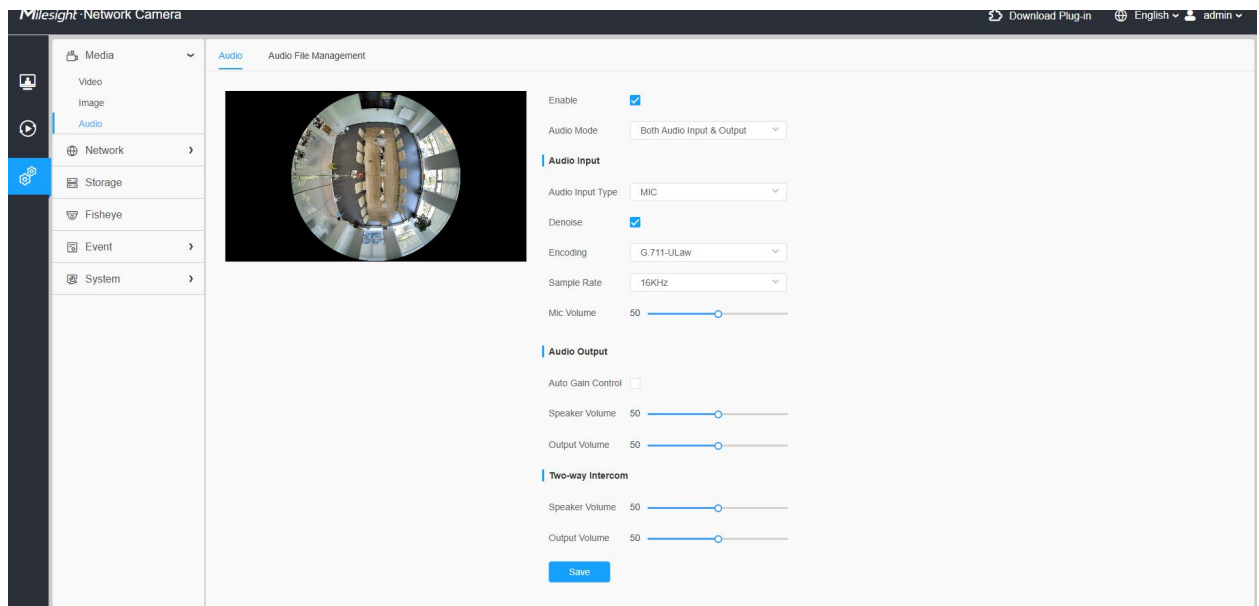
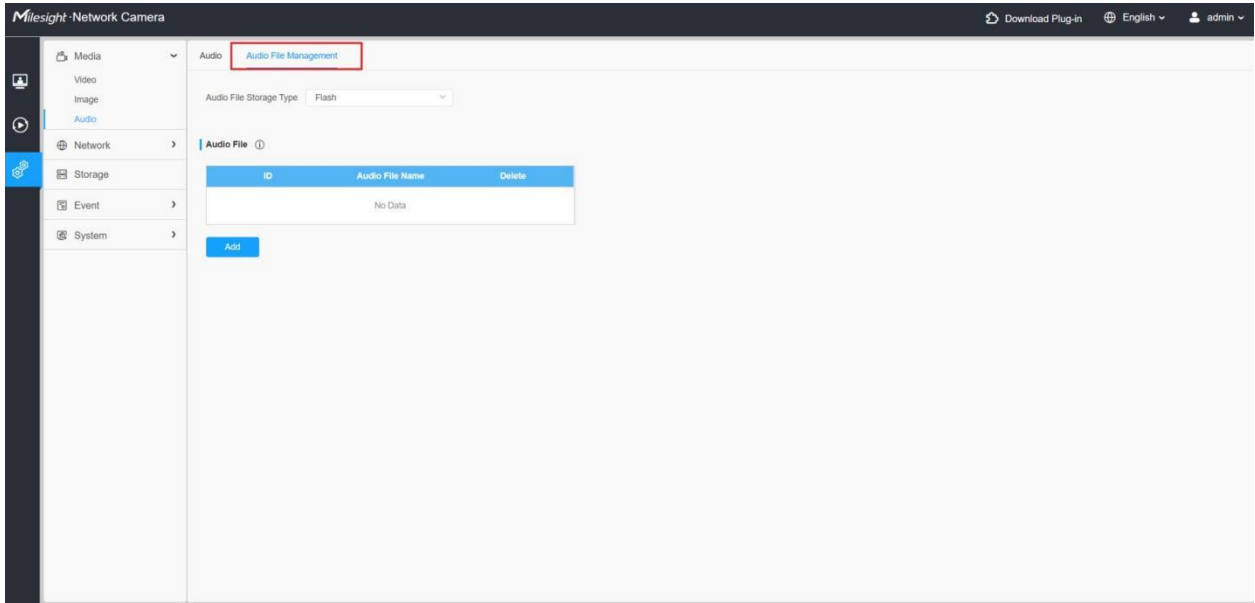


Table 23. Description of the buttons

Parameters	Function Introduction
Enable	Check on the checkbox to enable audio feature.
Audio Mode	Audio Input/Audio Output/Both Audio Input & Output are optional.
Audio Input	Audio Input Type: Mic is available only for models equipped with microphone. Line In is available only for models equipped with an audio input cable. Denoise: Check the check-box to enable this function, After enabling it, the noise detected can be filtered. Encoding: G.711-ULaw, G.711-ALaw, AAC LC and G.722 are available. Sample Rate: 8KHz, 16KHz, 32KHz, 44.1KHz, and 48KHz are available. Audio Bit Rate: The function is available only for AAC LC, and supports up to 96kbps. Mic Volume/Input Volume: Input audio volume level: 0-100.
Audio Output	This module is used to control the output volume when the camera triggers audio out in response to an event. Auto Gain Control: This function improve the quality of audio. Speaker Volume: Adjusts the output volume of the camera's built-in speaker. Range: 0–100. Output Volume: Adjusts the output volume of external devices connected via the camera's audio out interface. Range: 0–100.
Two-way Intercom	This module is used to control the output volume of the camera during two-way intercom communication. Speaker Volume: Adjusts the output volume of the camera's built-in speaker. Range: 0–100. Output Volume: Adjusts the output volume of external devices connected via the camera's audio out interface. Range: 0–100.

8.1.3.2 Auto File Management

You can upload up to 5 audio files manually to Flash or SD Card on the Audio web page and you can also edit the audio file's name when upload.



-  **Note:**
- Only support '.wav' audio files with codec type PCM/PCMU/PCMA, 64kbps or 128kbps bitrate and no more than 500k.

8.2 Network

8.2.1 Basic

8.2.1.1 TCP/IP

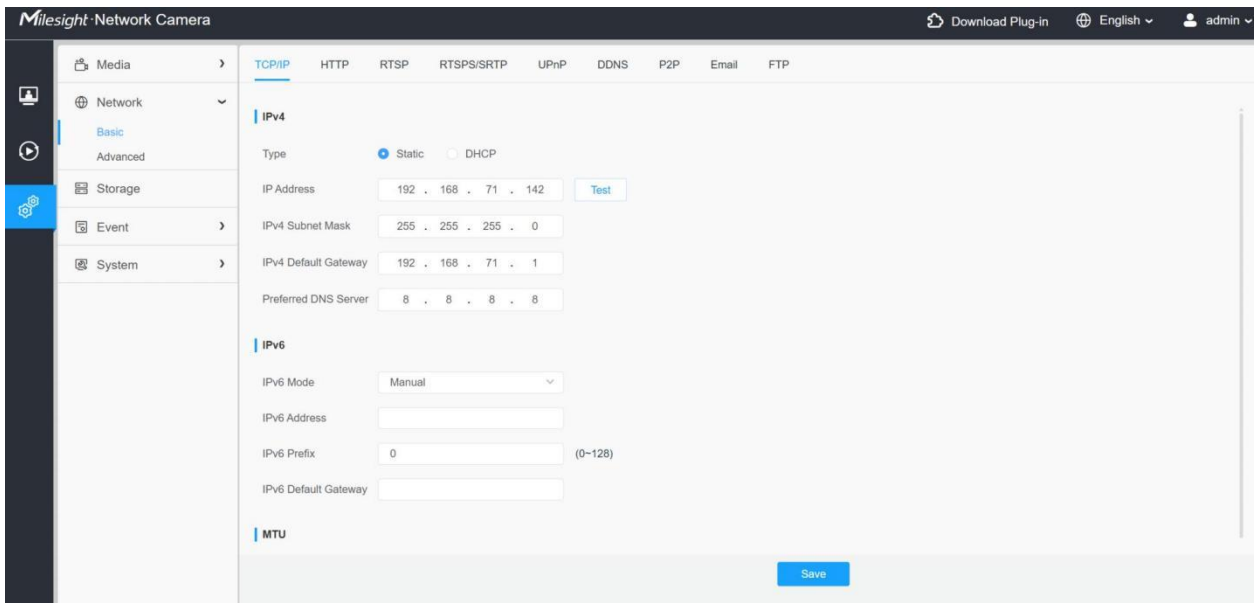


Table 24. Description of the buttons

Parameters	Function Introduction
------------	-----------------------

IPv4	Type: You can choose between Static and DHCP types to obtain the IPv4 address. • DHCP: The camera automatically obtains an IP address from the DHCP server . • Static: Allows you to manually assign a fixed IP address to the camera. IPv4 Address: An address that used to identify a network camera on the network.  Note: The Test button is used to test if the IP is conflicting. IPv4 Subnet Mask: It is used to identify the subnet where the network camera is located. IPv4 Default Gateway: The default router address. Preferred DNS Server: The DNS Server translates the domain name to IP address.
IPv6	IPv6 Mode: Choose different modes for IPv6: Manual/Route Advertisement/ DHCPv6. IPv6 Address: IPv6 Address used to identify a network camera on the network. IPv6 Prefix: Define the prefix length of IPv6 address: 0 to 128. IPv6 Default Gateway: The default router IPv6 address.
MTU	Maximum Transmission Unit. Enter a value from 1200 to 1500 as needed. The default value is 1500.
Save	Save the configurations.

8.2.1.2 HTTP

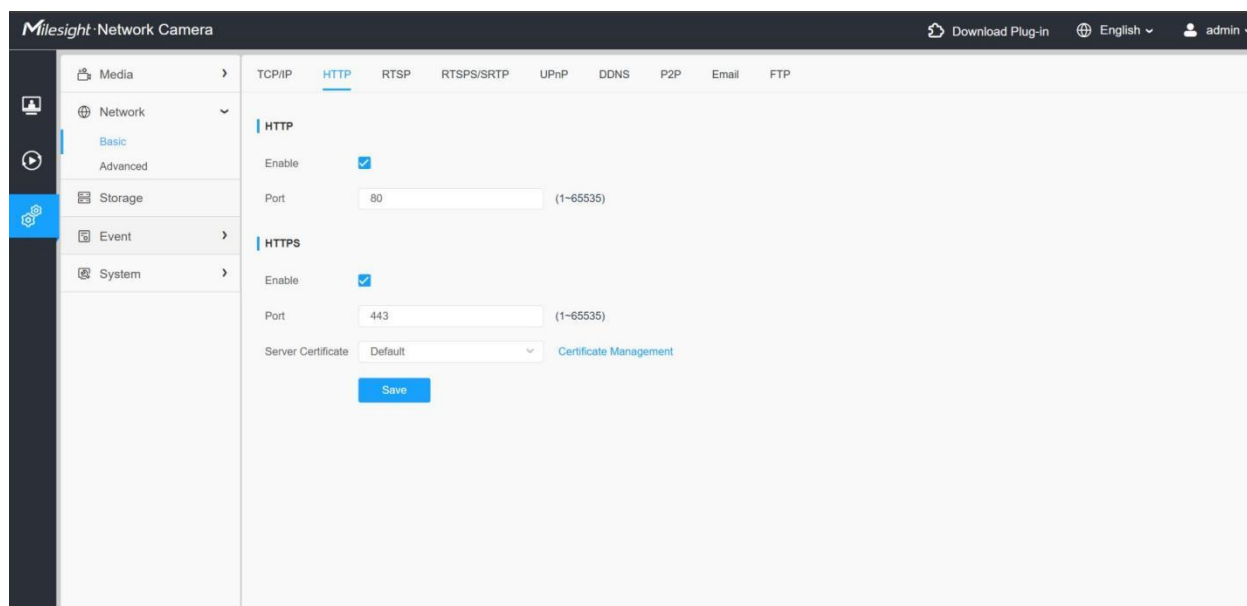


Table 25. Description of the buttons

Parameters	Function Introduction
HTTP	Enable: Start or stop using HTTP. Port: Enter a Web GUI login port from 1 to 65535. The default is 80, same with ONVIF port.

HTTPs	Enable: Start or stop using HTTPs. Port: Enter a Web GUI login port via HTTPS from 1 to 65535. The default is 443.  Note: For more details about how to enable HTTPs access, see https://milesight.freshdesk.com/a/solutions/articles/69000797384.
Server Certificate	You can select the certificates created in Certificate Management.
	Save the configurations.

Table 26. HTTP URL are as below:

Stream	URL
Main Stream	https://username:password@IP:port/ipcam/mjpeg.cgi
Secondary Stream	https://username:password@IP:port/ipcam/mjpegcif.cgi

8.2.1.3 RTSP

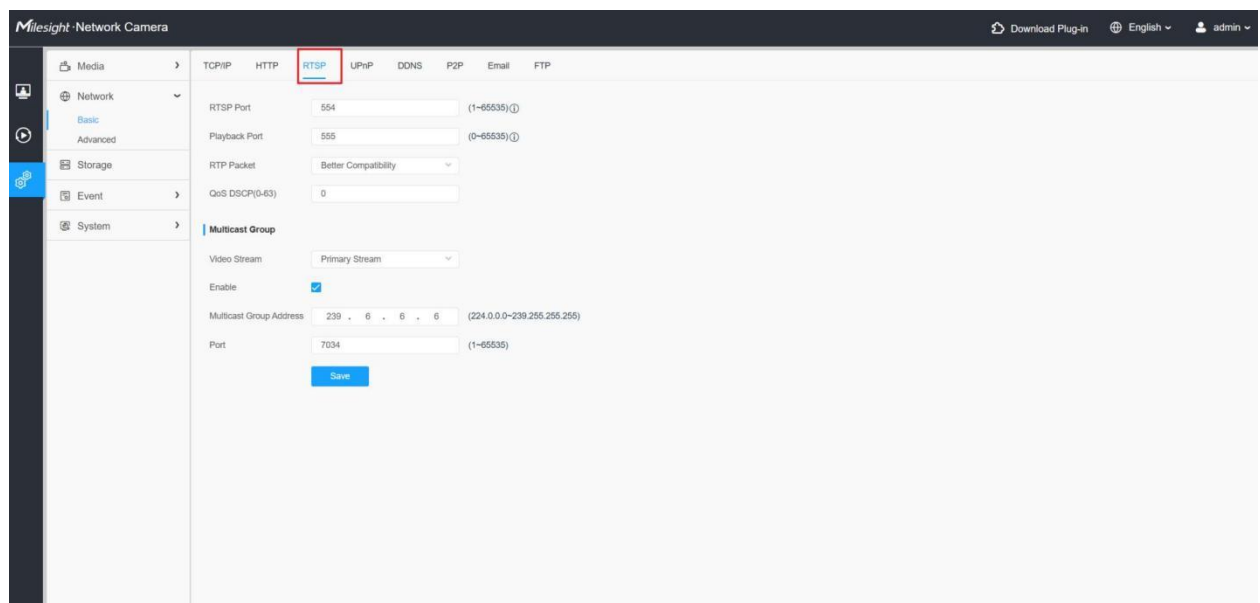


Table 27. Description of the buttons

Parameters	Function Introduction
RTSP Port	The port of RTSP (1~65535), the default is 554.
Playback Port	Playback Port The port of playback (0~65535), the default is 555.  Note: Port 0 means closing playback function.

RTP Packet	There are Better Compatibility and Better Performance two options, if your camera's image mess up, please switch this option.	
QoS DSCP	The valid value range of the DSCP is 0-63.	
Multicast Group	Channel	It supports enabling Multicast Group for different channels. Note: The available channels depend on the selected display mode (1O/1P/2P/4R/1O3R). In Bundle-Stream Mode, only Channel 1 is available.
	Stream Type	It supports enabling Multicast Group for different streams; both the Primary Stream and Secondary Stream are optional.
	Enable	Enable or disable the Multicast Group.
	Multicast Group Address	Support multicast function.
	Port	The port of multicast group, the default is 7034. The valid value range of the port is 1-65535.
		Save the configurations.

Table 28. RTSP URL are as below:

Channel	Stream	URL
Channel1	Primary Stream	rtsp://IP:RTSP Port/channel1/main
	Secondary Stream	rtsp://IP:RTSP Port/channel1/sub
Channel2	Primary Stream	rtsp://IP:RTSP Port/channel2/main
	Secondary Stream	rtsp://IP:RTSP Port/channel2/sub
Channel3	Primary Stream	rtsp://IP:RTSP Port/channel3/main
	Secondary Stream	rtsp://IP:RTSP Port/channel3/sub
Channel4	Primary Stream	rtsp://IP:RTSP Port/channel4/main
	Secondary Stream	rtsp://IP:RTSP Port/channel4/sub

**Note:**

- DSCP refers to the Differentiated Service Code Point; and the DSCP value is used in the IP header to indicate the priority of the data.
- A reboot is required for the settings to take effect.

8.2.1.4 RTSPS/SPTP

RTSP is a standard real-time streaming protocol for local/LAN and third-party video transmission, while SPTP is a smart P2P protocol for convenient remote monitoring of intranet cameras.

The screenshot shows the Milesight Network Camera web interface. The top navigation bar includes 'Download Plug-in', 'English', and 'admin'. The left sidebar has icons for Media, Network, Storage, Event, and System. The main content area is titled 'RTSPS/SRTSP' and contains the following configuration fields:

- RTSPS Port:** A text input field with the value '322' and a range indicator '(1-65535)'.
- Multicast Group:** A section with two tabs: 'Channel 1' and 'Channel 2'.
- Stream Type:** A dropdown menu with 'Primary Stream' selected.
- Enable:** A checkbox that is currently unchecked.
- RTSP Port:** A text input field with the value '5600' and a range indicator '(1-65535)'.
- Server Certificate:** A dropdown menu with 'Default' selected, and a link to 'Certificate Management'.
- Encryption Algorithm:** A dropdown menu with 'AES256' selected.
- Save:** A blue button at the bottom of the configuration section.

Table 29. Parameter Description

Parameter	Description
RTSPS Port	Enter the RTSPS port from 1-65535.
Channel	It supports enabling Multicast Group for different channels. Note: The available channels depend on the selected display mode (1O/1P/2P/4R/1O3R). In Bundle-Stream Mode, only Channel 1 is available.
Stream Type	It supports enabling Multicast Group for different streams; both the Primary Stream and Secondary Stream are optional.
Enable	Enable or disable the Multicast Group.
Port	The port of multicast group, the default is 5600. The valid value range of the port is 1-65535.
Server Certificate	You can select the certificates created in Certificate Management.
Encryption Algorithm	Select an encryption algorithm. AES128 and AES256 are available.
Save	Save the configurations.

8.2.1.5 UPnP

Universal Plug and Play (UPnP) is a networking architecture that provides compatibility among networking equipment, software and other hardware devices. The UPnP protocol allows devices to connect seamlessly and to simplify the implementation of networks in the home and corporate environments. With the function enabled, you don't need to configure the port mapping for each port, and the camera is connected to the Wide Area Network via the router.

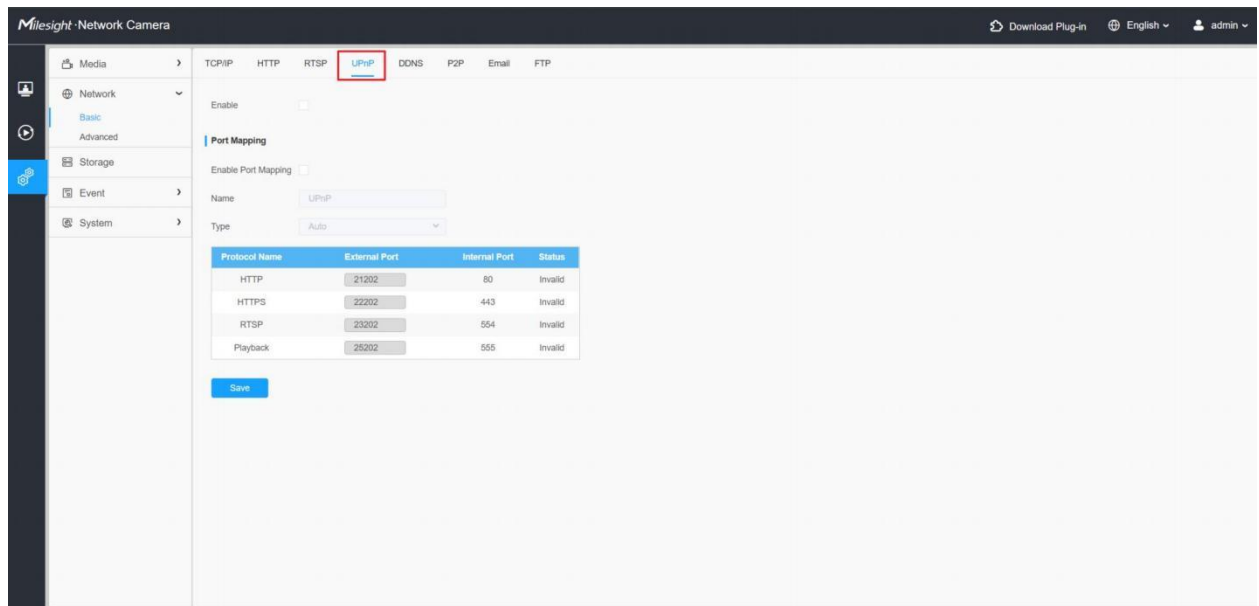


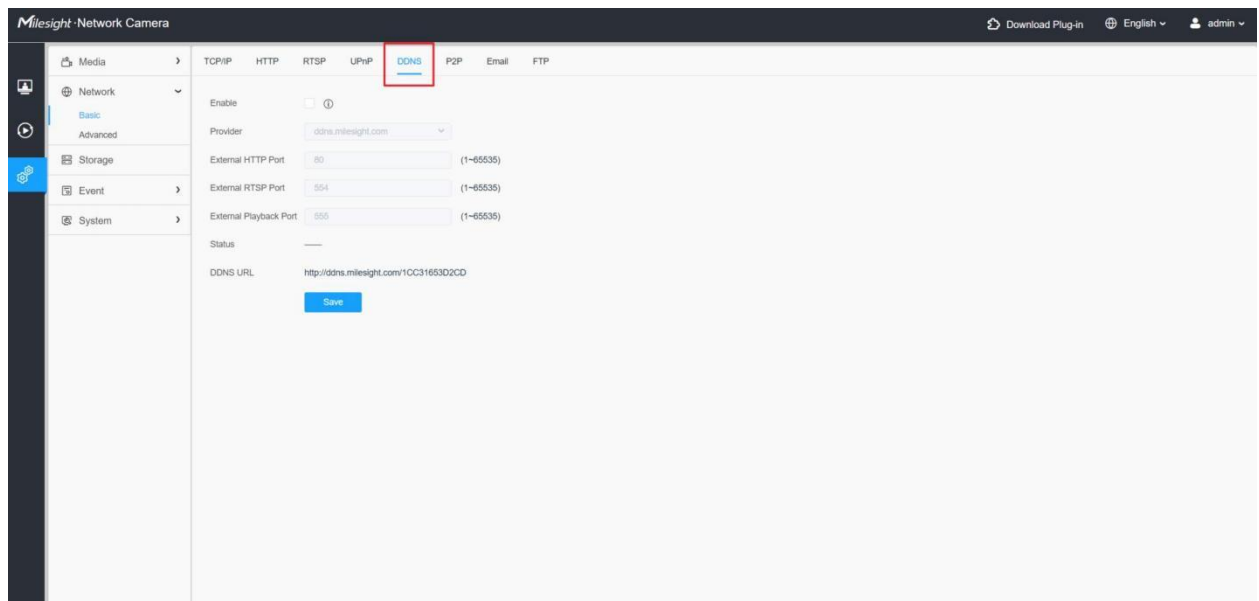
Table 30. Description of the buttons

Parameters	Function Introduction
Enable	Check the checkbox to enable the UPnP function.
Enable Port Mapping	Check the checkbox to enable the Port Mapping
Name	The name of the device detected online, which can be edited.
Type	Auto: Automatically obtain the corresponding HTTP and RTSP port, without any settings Manual: Need to manually set the appropriate HTTP port and RTSP Port. When choose Manual, you can customize the value of the port number by yourself
Save	Save the configurations.

8.2.1.6 DDNS

DDNS allows you to access the camera via domain names instead of IP address. It manages to change IP address and update your domain information dynamically. You need to register an account from a provider.

Note: For more details about how to set DDNS, please refer to <https://milesight.freshdesk.com/a/solutions/articles/69000643406>.



You can choose “ddns.milesight.com” as provider for DDNS. After enabling it, you can access the device via the URL “http://ddns.milesight.com/MAC address”.

Table 31. Description of the buttons

Parameters	Function Introduction
Enable DDNS	Check the checkbox to enable DDNS service.  Note: Recommend to enable and configure UPnP ports which can be used directly in DDNS.

Provider	Get support from DDNS provider: ddns.milesight.com, freedns.afraid.org, dyndns.org, www.no-ip.com, www.zoneedit.com. When ddns.milesight.com is selected here, enter the following information: • External HTTP Port: Enter an external HTTP port from 1 to 65535. • External RTSP Port: Enter an external RTSP port from 1 to 65535. • External Playback Port: Enter an external playback port from 1 to 65535. • DDNS URL: DDNS URL, which is automatically formed. • Status: DDNS running status. When freedns.afraid.org is selected here, enter the following information: • Hash: A string used for verification. • Host Name: Account name from the DDNS provider. • Status: DDNS running status. When dyndns.org is selected here, enter the following information: • Host IP: Enter the host IP. • User Name: Enter the user name. • Password: Enter your password. • Host Name: Account name from the DDNS provider. • Status: DDNS running status. When www.no-ip.com or www.zoneedit.com are selected here, enter the following information: • User Name: Enter the user name. • Password: Enter your password. • Host Name: Account name from the DDNS provider. • Status: DDNS running status. You can also customize the provider for DDNS and enter the following information: • DDNS URL: Enter the DDNS URL manually. • User Name: Enter the user name. • Password: Enter your password. • Status: DDNS running status.
Save	Save the configurations.

**Note:**

- Before using Milesight DDNS, forward HTTP Port and RTSP Port first.
- Make sure that the internal and the external port number of RTSP are the same.

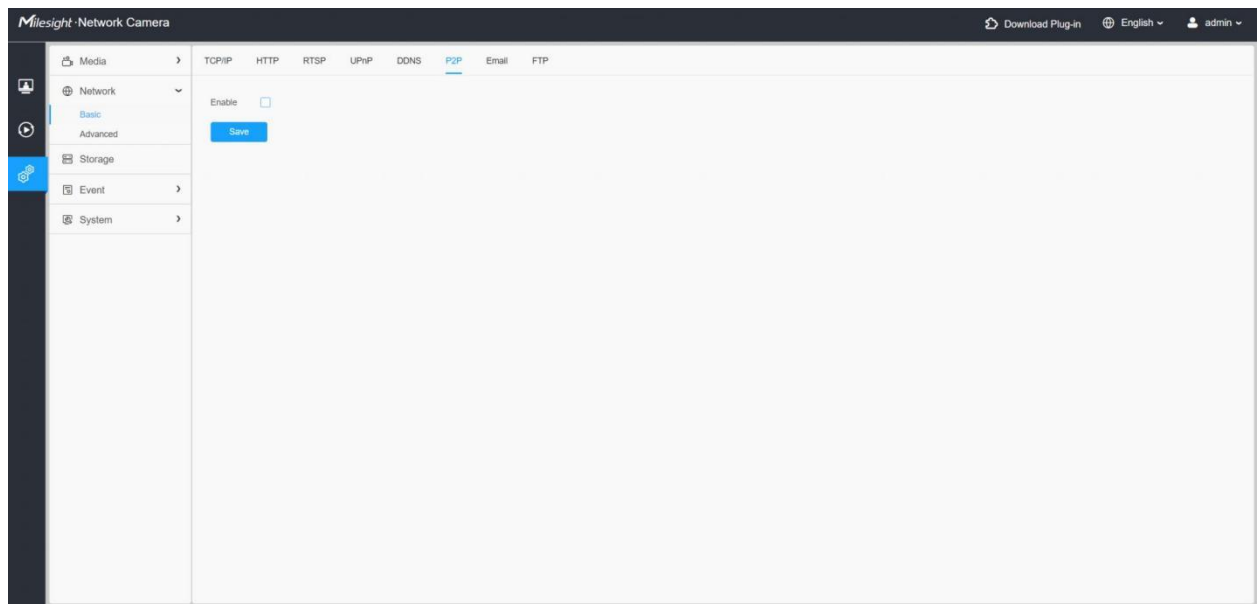
8.2.1.7 P2P

Peer-to-peer (P2P) protocols are network protocols that enable direct communication between nodes (peers) in a network, without requiring a central server or intermediary. These protocols are fundamental in various applications, including file sharing, distributed computing, and decentralized networks. Milesight camera supports P2P protocol, you can enable it within the Network interface.

You can enable P2P simply by ticking the checkbox.



Note: Before using P2P, please reach out to our support team to activate the P2P feature on our cloud.



8.2.1.8 Email

Alarm video files can be sent to specific mail account through SMTP server. You must configure the email settings correctly before using it.

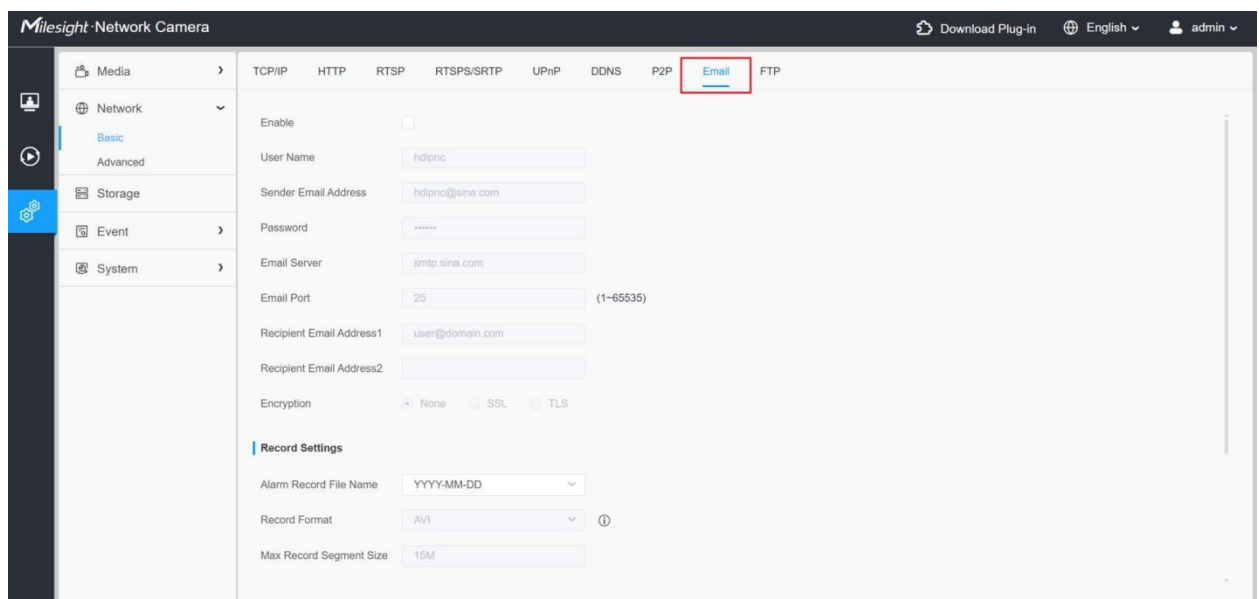


Table 32. Description of the buttons

Parameters	Function Introduction
Enable	Check the checkbox to enable Email function.
User Name	The sender's name. It is usually the same as the account name.
Sender Email Address	Email address to send video files attached emails.
Password	The password of the sender.

Email Server	The email server IP address or host name(e.g. smtp.gmail.com).
Email Port	The default TCP/IP port for SMTP is 25(not secured). For SSL/TLS port, it depends on the mail you use.
Recipient Email Address1	Email address to receive video files.
Recipient Email Address2	Email address to receive video files.
Encryption	Check the checkbox to enable SSL or TLS if it is required by the SMTP server. You can also select None.
Record Settings	Alarm Record File Name: Default(YYYY-MM-DD) /MM-DD-YYYY/ DD- MM-YYYY/ Add prefix/ Customize are available. Record Format: Selects the recording file format; MP4 and AVI are available. Max Record Segment Size: Limits the size of each recording file.
Snapshot Settings	Alarm Snapshot File Name: Default(YYYY-MM-DD) /MM-DD-YYYY/ DD- MM-YYYY/ Add prefix/ Customize are available. Timing Snapshot File Name: Default(YYYY-MM-DD) /MM-DD-YYYY/ DD- MM-YYYY/ Add prefix/ Customize are available.
	Save the configuration.
	Test whether the configurations are successful.



Note: You can refer to the following file name tip to customize the file name.

File Name Tip
 &Device - Device Name
 &Y - Year
 &M - Month
 &D - Day
 &h - hour
 &m - minute
 &s - second
 &ms - millisecond
 && - &

8.2.1.9 FTP

Alarm video files can be sent to specific FTP server. You must configure the FTP settings correctly before using it.

Table 33. Description of the buttons

Parameters		Function Introduction
FTP Server Settings	Enable	Check the checkbox to enable the FTP function.
	FTP Type	FTP and SFTP are optional.
	Server Address	FTP/SFTP server address.
	Server Port	The port of the FTP server. Generally it is 21. The port of the SFTP server. Generally it is 22.
	User Name	User name used to log in to the FTP/SFTP sever.
	Password	User password.
	FTP over SSL/TLS(FTPS)	Check the checkbox to encrypt the data transmitted between the camera and the FTP server via the SSL/TLS protocol to ensure the security of file transfers.
	Storage Path	Storage Path where video and image will be uploaded to the FTP server. Four FTP storage path types are available, including Root Directory, Parent Directory, Child Directory and Customize.
	Parent Directory	Choose IP Address/ Device Name/ Date as the folder name of Parent Directory, or customize the folder name.
	Multilevel Folder Name	If the storage path is more than two levels, enter Multilevel FTP storage path here manually.

	Child Directory	Choose IP Address/ Device Name/ Date as the folder name of Child Directory, or customize the folder name.
	Alarm Action File Name	Choose the default (YYYY-MM-DD) or customize the alarm action file name.
	Timing Snapshot File Name	Default(YYYY-MM-DD) /MM-DD-YYYY/ DD-MM-YYYY/ Add prefix/ Overwrite with the base file name are available. You can also customize one.
	Record Format	AVI and MP4 are optional.
Save		Save the configurations.
Test		Test whether the configurations are successful.

**Note:**

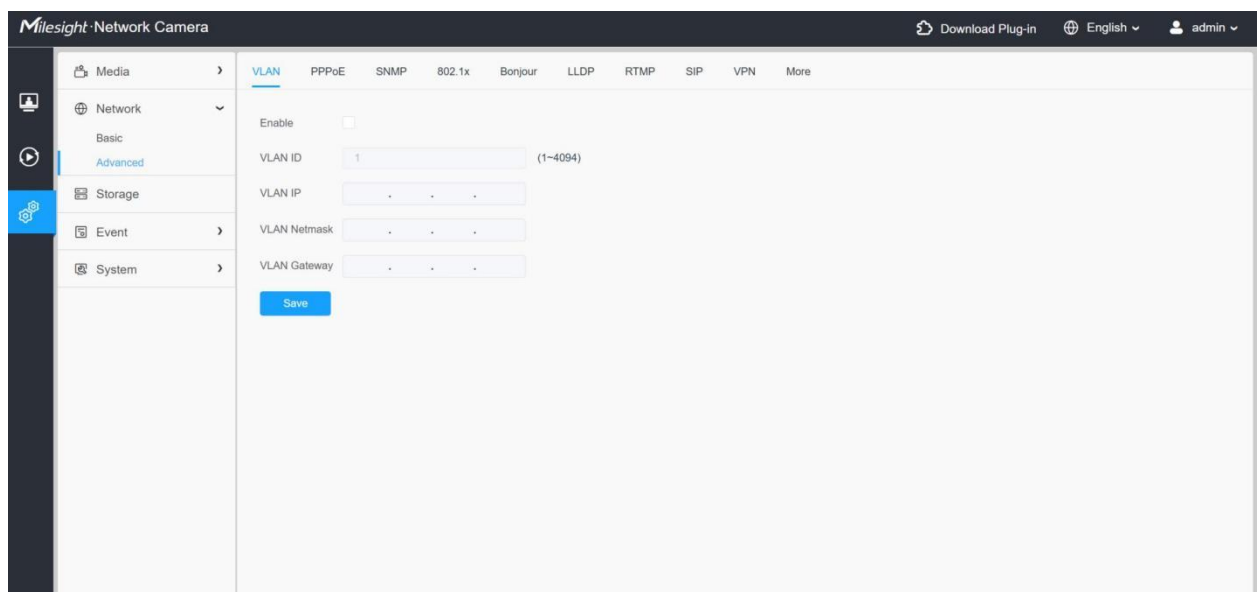
- Parent Directory will be under Root Directory, and Child Directory will be under Parent Directory.
- You can refer to the following file name tip to customize the file name.

8.2.2 Advanced

8.2.2.1 VLAN

A virtual LAN (VLAN) is any broadcast domain that is partitioned and isolated in a computer network at the data link layer (OSI layer 2). LAN is an abbreviation of local area network.

VLANs allow network administrators to group hosts together even if the hosts are not on the same network switch. This can greatly simplify network design and deployment, because VLAN membership can be configured through software. Without VLANs, grouping hosts according to their resource needs necessitates the labour of relocating nodes or rewiring data links.



Note: About how to set up VLAN in switches, please refer to your switches user manual.

8.2.2.2 PPPoE

This camera supports the PPPoE auto dial-up function. The camera gets a public IP address by ADSL dial-up after the camera is connected to a modem. You need to configure the PPPoE parameters of the network camera.

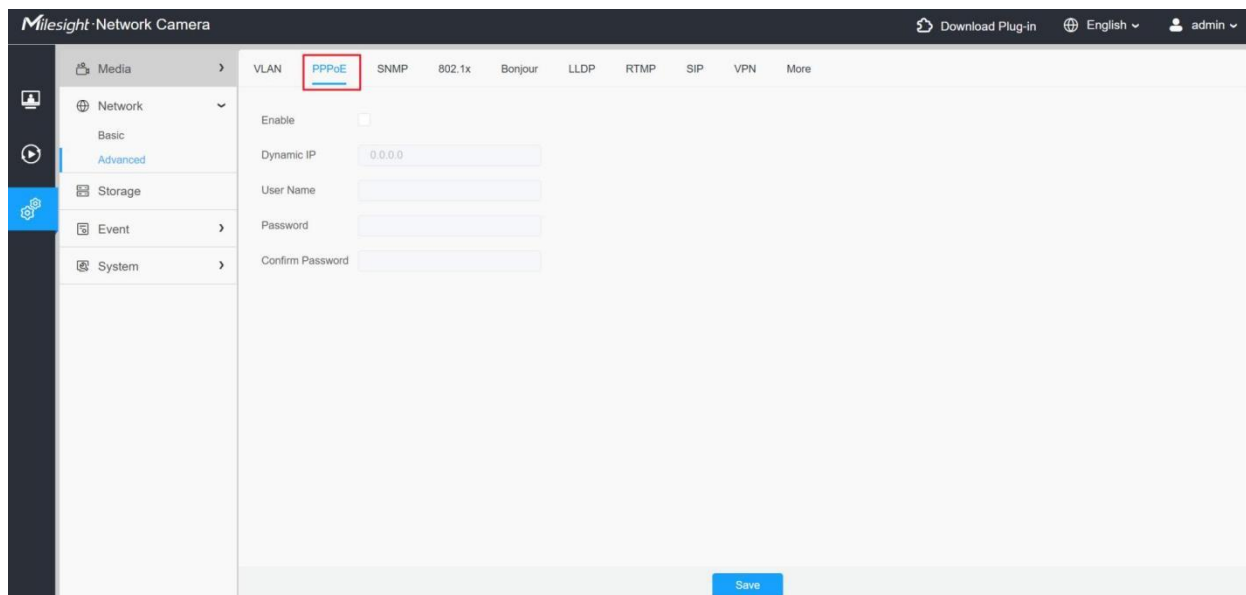


Table 34. Parameter Description

Parameter	Function Introduction
Enable	Check the checkbox to enable this function.
Dynamic IP	Enter a dynamic IP address. It is fixed and default.
User Name	Enter a user-name.
Password	Enter a password.
Confirm Password	Confirm the password.
Save	Click it to save the configurations.



Note:

- The obtained IP address is dynamically assigned via PPPoE, so the IP address always changes after rebooting the camera. To solve the inconvenience of the dynamic IP, you need to get a domain name from the DDNS provider (e.g. DynDns.com).
- The user-name and password should be assigned by your ISP.

8.2.2.3 SNMP

You can set the SNMP function to get camera status, parameters and alarm related information and manage the camera remotely when it is connected to the network.

Before setting the SNMP, please download the SNMP software and manage to receive the camera information via SNMP port. By setting the Trap Address, the camera can send the alarm event and exception messages to the surveillance center.

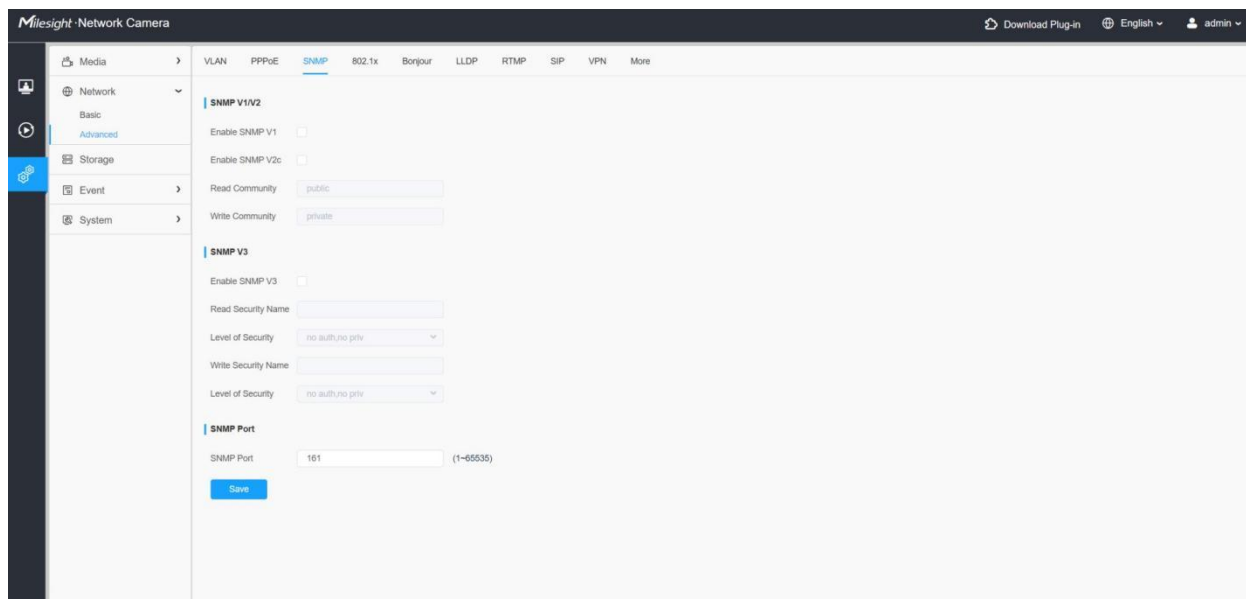


Table 35. Description of the buttons

Parameters	Function Introduction
SNMP v1/v2	The version of SNMP, please select the version of your SNMP software. Enable SNMP v1: Provide no security. Enable SNMP v2: Require password for access. Write Community: Input the name of Write Community. Read Community: Input the name of Read Community
SNMP v3	Enable SNMP v3: Provide encryption and the HTTPS protocol must be enabled. Read Security Name: Input the name of Read Security Community. Level of Security: There are three levels available: (auth, priv), (auth, no priv) and (no auth, no priv). Write Security Name: Input the name of Write Security Community. Level of Security: There are three levels available: (auth, priv), (auth, no priv) and (no auth, no priv).
SNMP Port	Enter a port of SNMP from 1 to 65535. The default value is 161.
Save	Save the configurations.

**Note:**

- The SNMP software settings must match the configurations you set here.
- A reboot is required for the settings to take effect.

8.2.2.4 802.1x

The IEEE 802.1X standard is supported by the network cameras, and when the feature is enabled, the camera data is secured and user authentication is needed when connecting the camera to the network protected by the IEEE 802.1X.

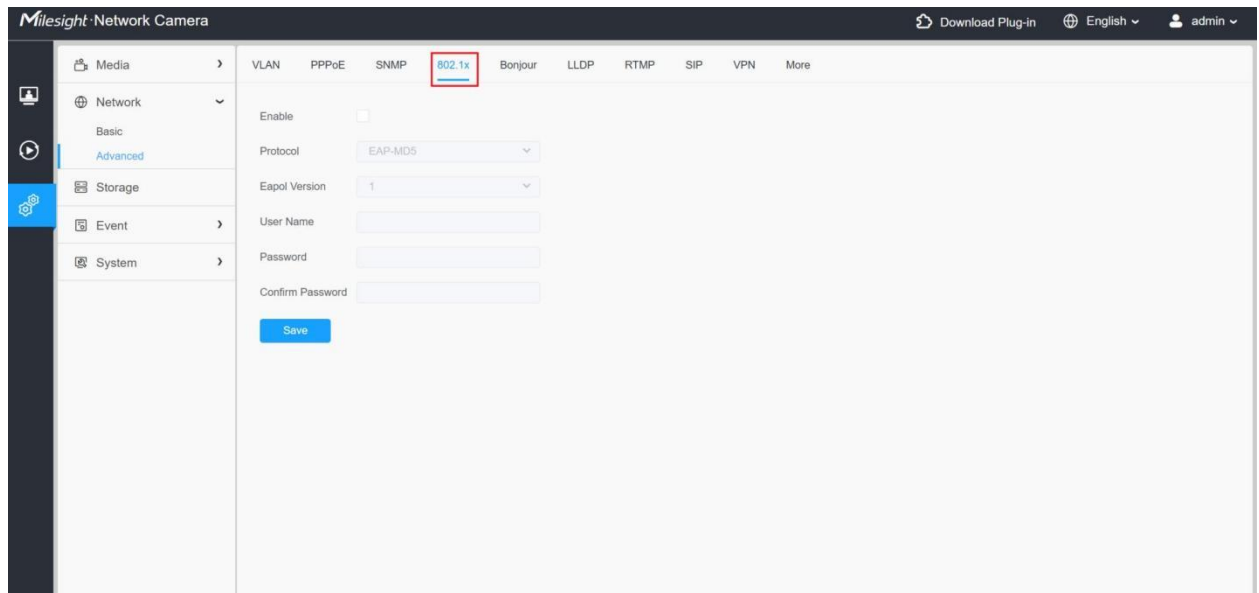


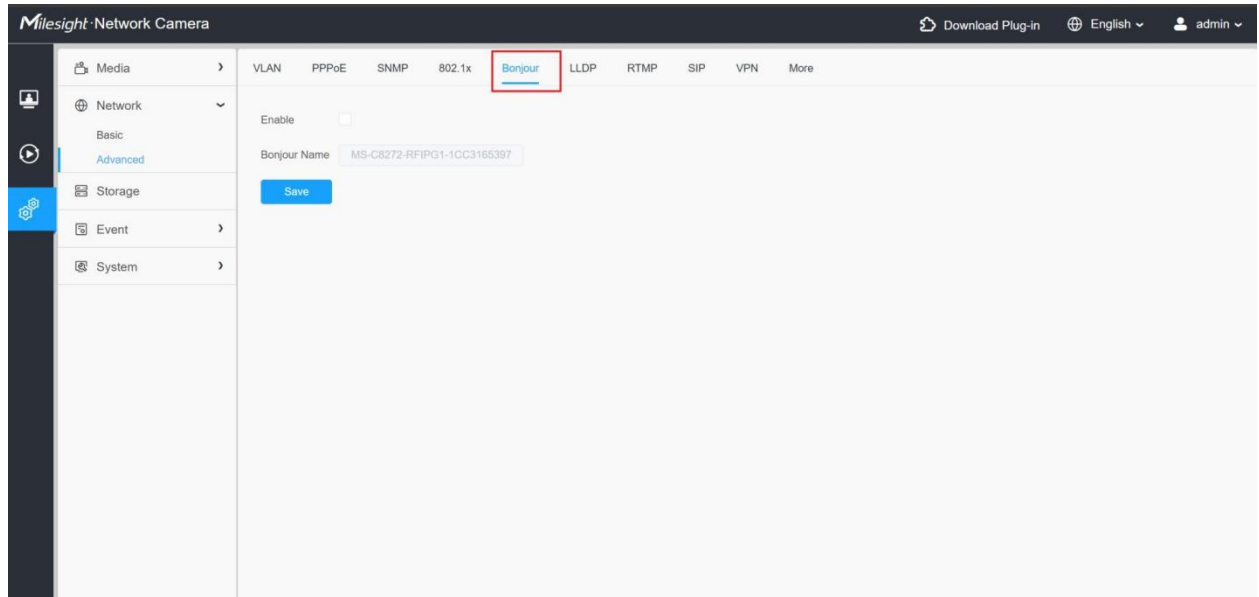
Table 36. Description the Buttons

Parameters		Function Introduction
Enable		Start or stop using 802.1x certification.
Protocol		Choose the protocol, EAP-MD5 and EAP-TLS are available.
EAP-MD5	Eapol Version	This version number helps ensure compatibility between devices implementing different versions of the EAPOL protocol. Version 1 and version 2 can be chosen.
	User Name	EAP-MD5 encryption account name.
	Password	EAP-MD5 encryption account password.
	Confirm Password	Re-enter the EAP-MD5 encryption account password.
EAP-TLS	Identify	EAP-TLS encryption account name.  Note: Please insert letters/digits/space/other standard characters, and make sure the amount of identify not more than 32.
	Eapol Version	Version 1 and version 2 can be chosen.
	Client Certificate	Upload and set the client certificate.
	Private Key	The key certificate in the client certificate.
	Private-key Password	Enter the password of the client certificate  Note: Please insert letters/digits/other standard characters, and make sure the amount of password not more than 32.
CA Certificate		Upload and set the CA certificate.

8.2.2.5 Bonjour

Bonjour is based on Apple's multicast DNS service. Bonjour devices can automatically broadcast their service information and listen to the service information of other devices.

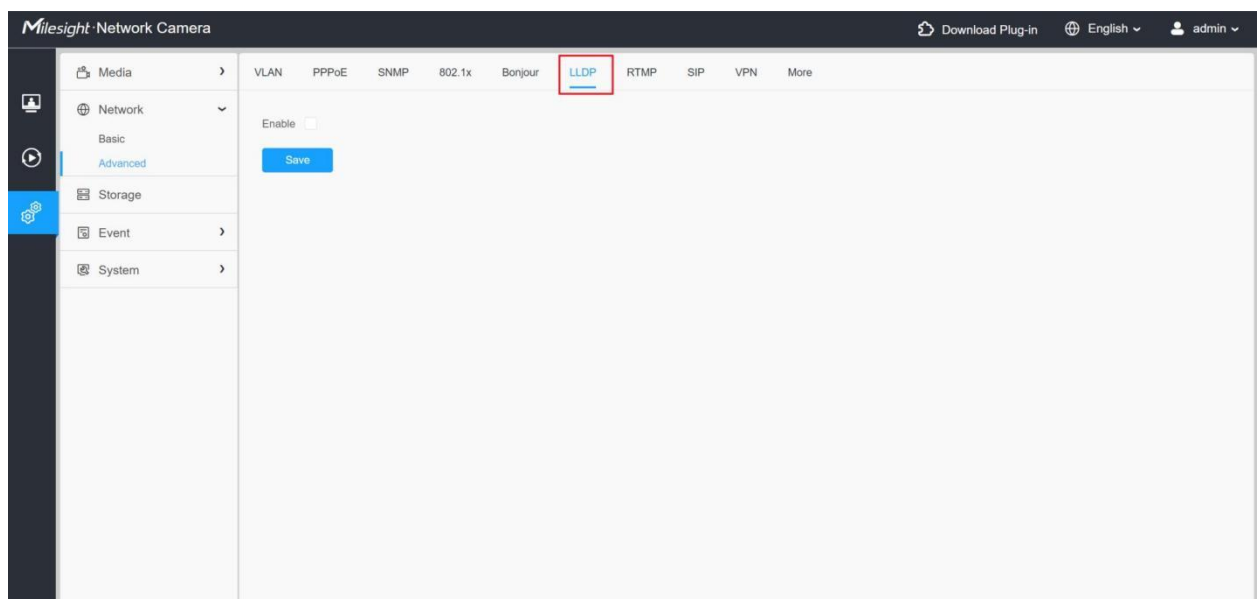
If you don't know the camera information, you can use the Bonjour service on the same LAN to search for network camera devices and then to access the devices.



8.2.2.6 LLDP

The Link Layer Discovery Protocol (LLDP) is a standardized network discovery protocol used by network devices to advertise their identity, capabilities, and neighbors on a local area network (LAN). It operates at the data link layer (Layer 2) of the OSI model. LLDP is defined by the IEEE 802.1AB standard. By using this protocol, devices can automatically discover and understand each other's presence and capabilities, which simplifies network management and configuration.

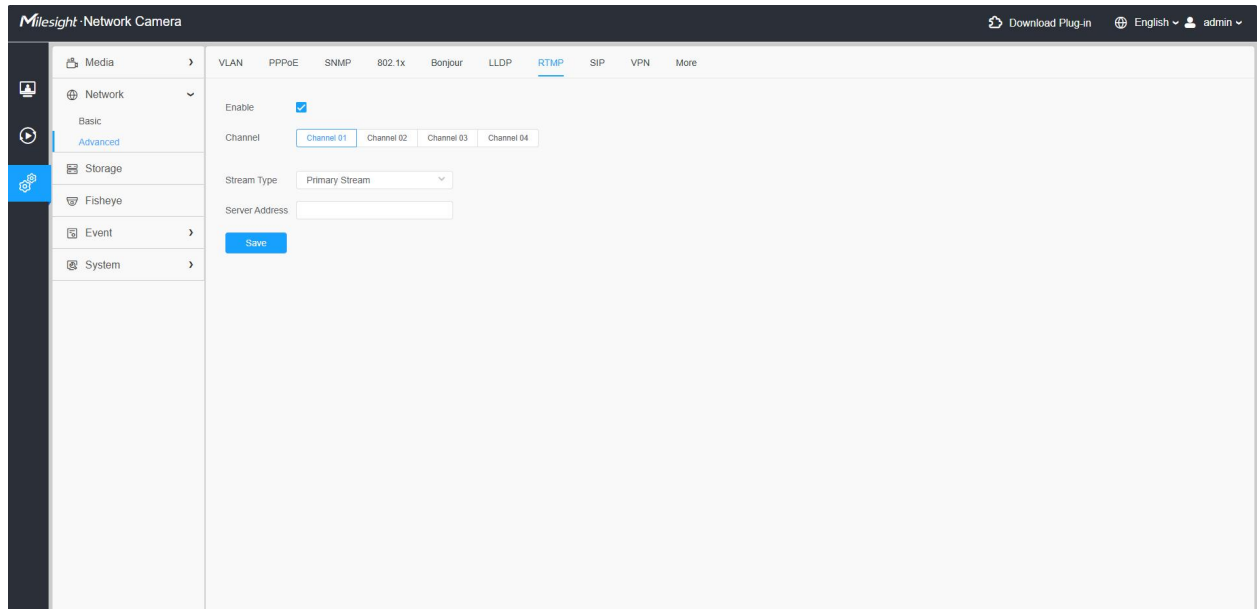
Once the LLDP protocol is enabled, you can obtain the camera's information on your switch that supports the LLDP protocol.



8.2.2.7 RTMP

Real-Time Messaging Protocol (RTMP) was initially a proprietary protocol for streaming audio, video and data over the Internet, between a Flash player and a server. RTMP is a TCP-based protocol which maintains persistent connections and allows low-latency

communication. It can realize the function of live broadcast so that customers can log in to the camera wherever there is a network.



Note:

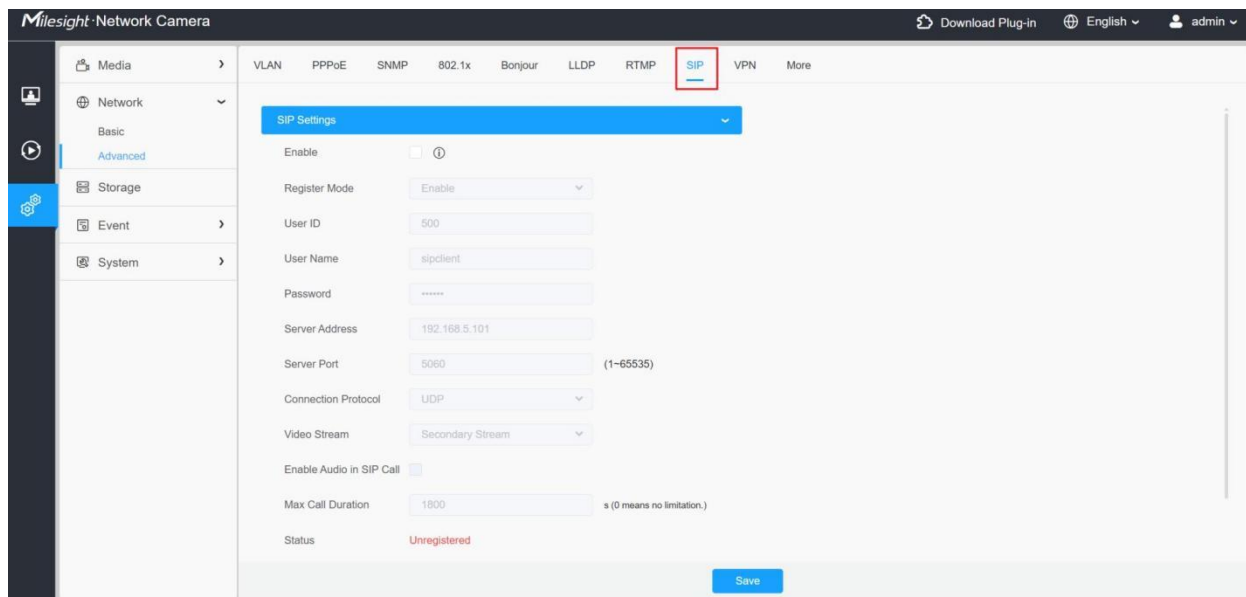
- For YouTube live broadcast, if you use a newly created account to live broadcast, you need to wait for 24hrs to activate the account for using live function.
- For RTMP, since G.711 is not available for YouTube, so you can only play video from Milesight Network Camera with H.264 video coding and AAC audio coding on YouTube.
- Server Address in Network Camera RTMP interface needs to be filled with the format: `rtmp://< Server URL >/< Stream key >`, remember it needs '/' to connect between < Server URL > and < Stream key >.
- For more details about how to use RTMP for live broadcast, please refer to <https://milesight.freshdesk.com/a/solutions/articles/69000643313>.

8.2.2.8 SIP

The Session Initiation Protocol(SIP) is a signaling communications protocol, widely used for controlling multimedia communication sessions such as voice and video calls over Internet Protocol (IP) networks. This page allows user to configure SIP related parameters. Milesight Network cameras can be configured as SIP endpoint to call out when alarm triggered; or allow permitted number to call in to check the video if the video IP phone is used.



Note: For more details about how to use SIP, please refer to <https://milesight.freshdesk.com/a/solutions/articles/69000643391>.



To use this function, the settings in SIP page must be configured properly. There are two ways to get video through SIP, one is to dial the IP address directly, the other is account registration mode. the details are as follows:

Method 1: IP Direct mode

Dial on the camera's IP address directly through SIP phone, so you can see the video.

Note: SIP phone and the camera should in the same network segment.

Method2: Account registration mode

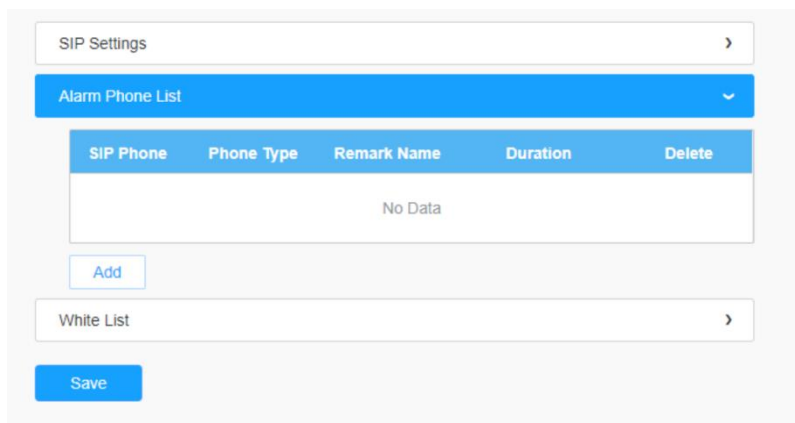
- Before using the SIP, you need to register an account for the camera from the SIP server;
- Register another user account for the SIP device from the same SIP server;
- Call the camera User ID from the SIP device, you will get the video on the SIP device.

[SIP Settings]

Table 37. Description of the buttons

Parameters	Function Introduction
------------	-----------------------

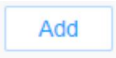
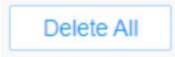
Enable	Start or stop using SIP.  Note: SIP supports Direct IP call.
Register Mode	Choose to use Enable mode or Disable mode. Enable mode means to use SIP with register account. Disable mode refers to use SIP without register account, just use the IP address to call.
User ID	SIP ID.
User Name	SIP account name.
Password	SIP account password.
Server Address	Server IP address.
Server Port	Server port.
Connection Protocol	UDP/TCP.
Video Stream	Choose the video stream.
Enable Audio in SIP Call	Enable/disable audio in SIP call.
Max Call Duration	The max call duration when use SIP.
Status	SIP registration status. Display “Unregistered” or “Registered” .

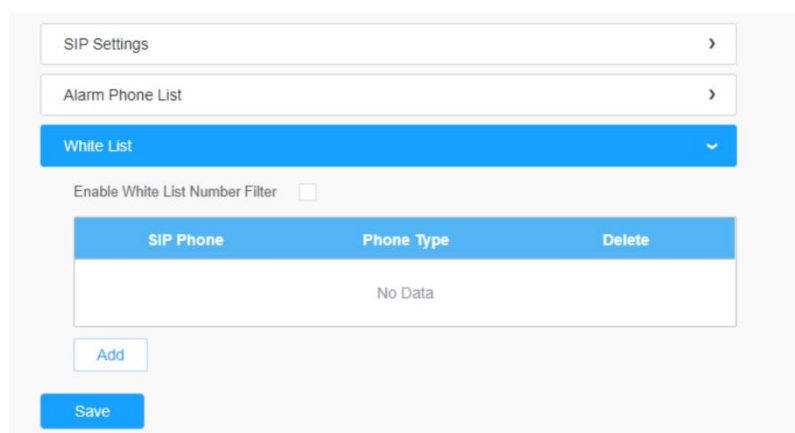
[Alarm Phone List]


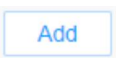
The screenshot shows the 'SIP Settings' configuration page. At the top, there is a 'SIP Settings' header with a right arrow. Below it is a blue bar labeled 'Alarm Phone List' with a dropdown arrow. Under this bar is a table with the following columns: 'SIP Phone', 'Phone Type', 'Remark Name', 'Duration', and 'Delete'. The table is currently empty, displaying 'No Data'. Below the table is an 'Add' button. At the bottom of the section is a 'White List' header with a right arrow and a 'Save' button.

Table 38. Description of the buttons

Parameters	Function Introduction
------------	-----------------------

	Add alarm phone to the camera. Phone Type: Phone Number(Call by phone number) & Direct IP Call(Check to accept peer to peer IP call). To Phone Number/IP Address: Call by phone number or IP address. Remark Name: Display name. Duration: The time schedule to use SIP.
	Delete the selected alarm phone.
	Delete all added alarm phone.

[White List]

Table 39. Description of the buttons

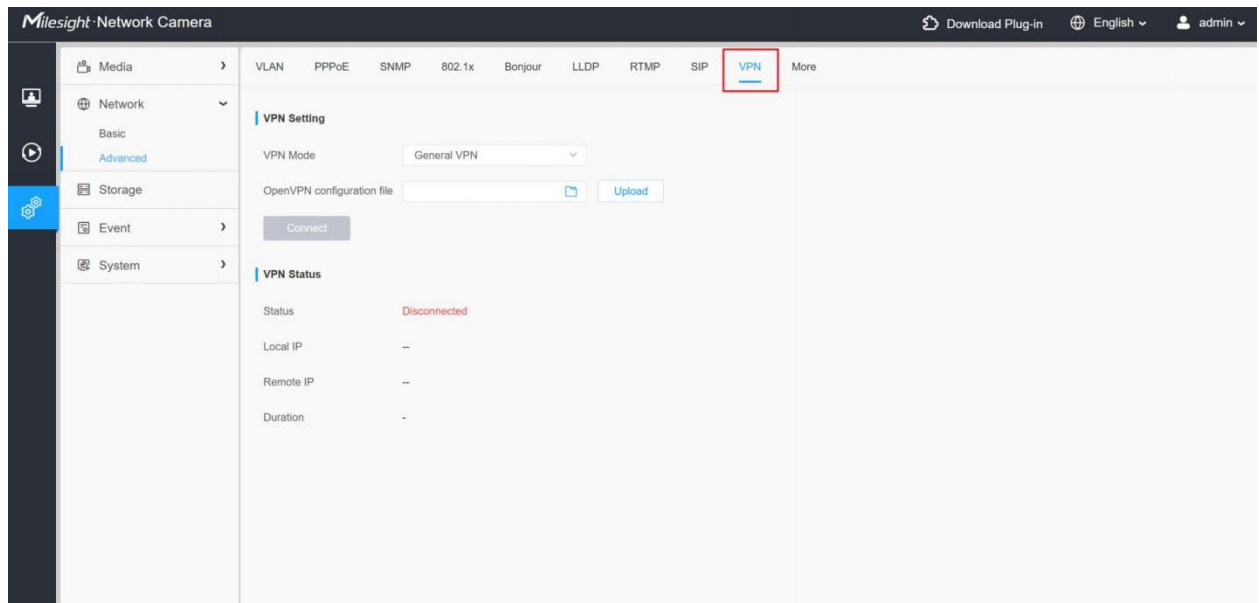
Parameters	Function Introduction
Enable White List Number Filter	When enabled, only the designated phone number or IP address can visit
	Phone Type: Phone Number(Call by phone number) & Direct IP Call. Phone Number/IP Address: Including the phone number or IP address on the white list.

8.2.2.9 VPN

VPN stands for Virtual Private Network. It is a network protocol that can provide you secure encrypted connection over the public internet. It is a significant technology in surveillance industry. Imagine that you have a network camera connected via public IP address, it's possible for others to log in or listen illegally if someone knows the specific IP address and forwarded port. Via VPN the camera streams and data will be transferred through an encrypted tunnel. This encrypted VPN tunnel makes it appear as though you are directly connected to the private network, keeping your online activity (including your browsing history) hidden. For Milesight camera, VPN feature allows us to log in the camera via a virtual IP, which makes it easier to configure the camera remotely.

For more details about How to use VPN on Milesight Camera, please refer to <https://milesight.freshdesk.com/support/solutions/articles/69000829102-how-to-use-vpn-o>

[n- milesight-network-camera.](#)



8.2.2.10 More

Here you can set more functions, like Push Message Settings and ONVIF Settings.

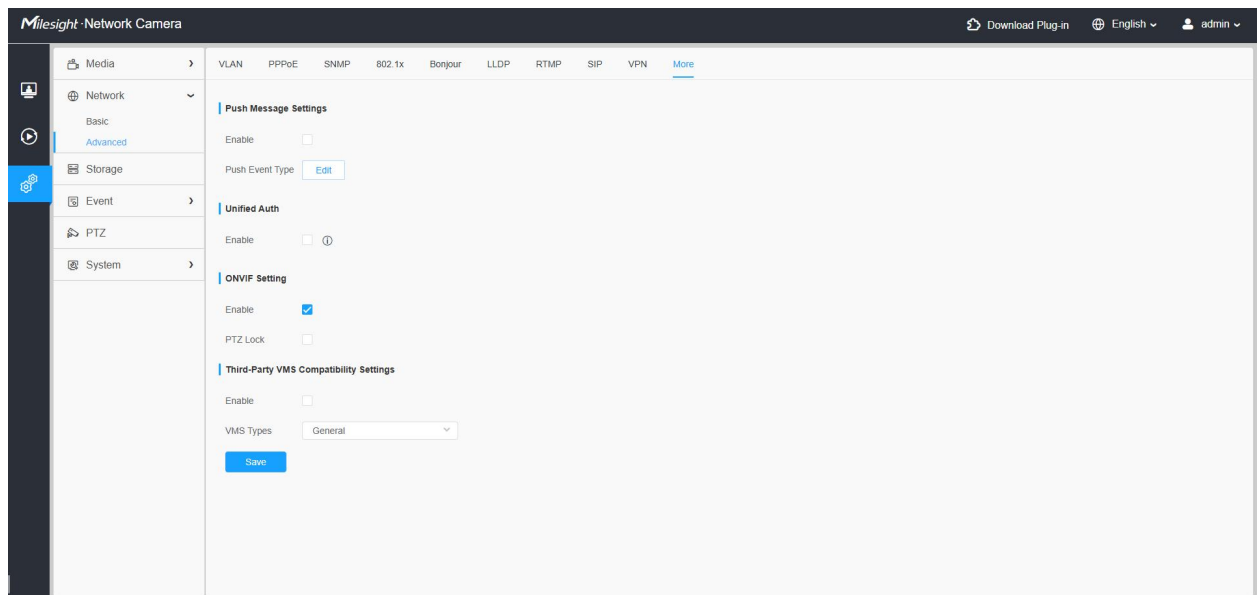
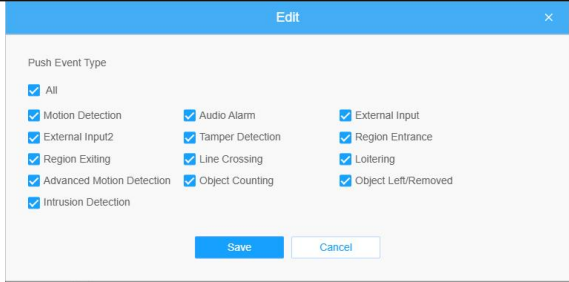


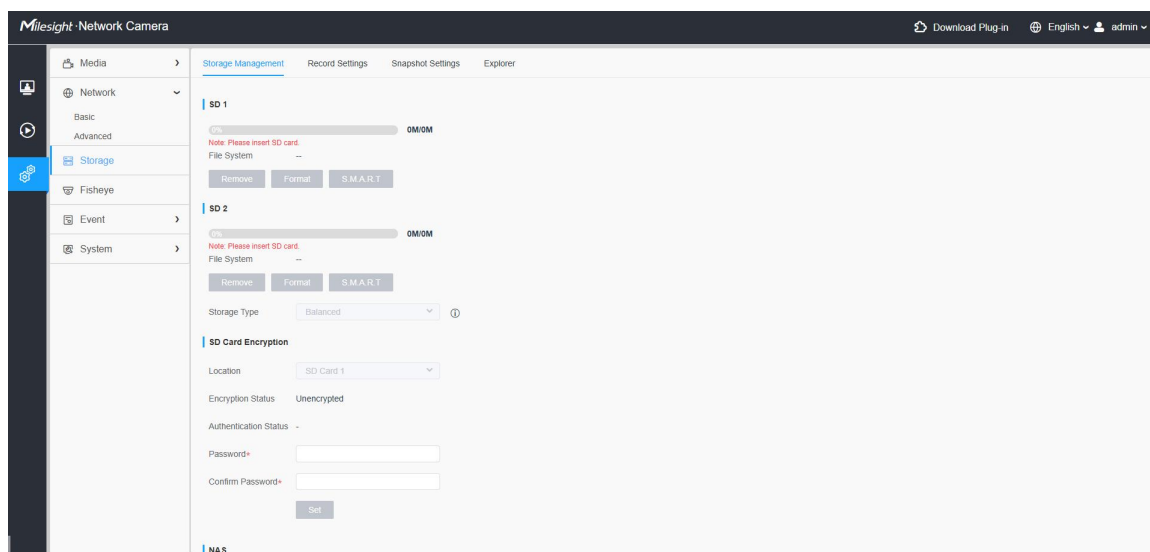
Table 40. Description of the buttons

Parameters	Function Introduction
Push Message Settings	Enable: Enable/disable the Push Message function. Push Event Type: You can click Edit to choose the types of Events' message which will be pushed to M-sight Pro and i-SightApp as shown below:

	
Unified Auth	Enable to let your browser remember login details for next time and enable passwordless login.
ONVIF Setting	Enable: Select to enable/disable the camera's ONVIF function; enabled by default, allowing third-party software to search, add and connect via ONVIF protocols. PTZ Lock: Intercepts ONVIF-initiated PTZ commands (ONVIF is the main way for third-party devices to control the camera); select to enable/disable it, and enabling locks the camera's operating settings to avoid unintended zoom or focus changes
Third-Party VMS Compatibility Settings	Enable: Check the checkbox to enable compatibility with third-party VMS systems. VMS Types: Select the desired third-party VMS type for compatibility.

8.3 Storage

8.3.1 Storage Management



- Insert the SD card into the SD card slot of the device. After that, it will be automatically detected, and the detailed information of the SD card will be displayed on the SD Card bar.
- In the SD card bar, you can click on  to remove the SD card or click on  to format the SD card and clear all files on it. It supports two file system formats including EXT4 and FAT32, and EXT4 is recommended to prevent data loss during card ejection or power failure, while FAT32 offers better compatibility for Operating systems.

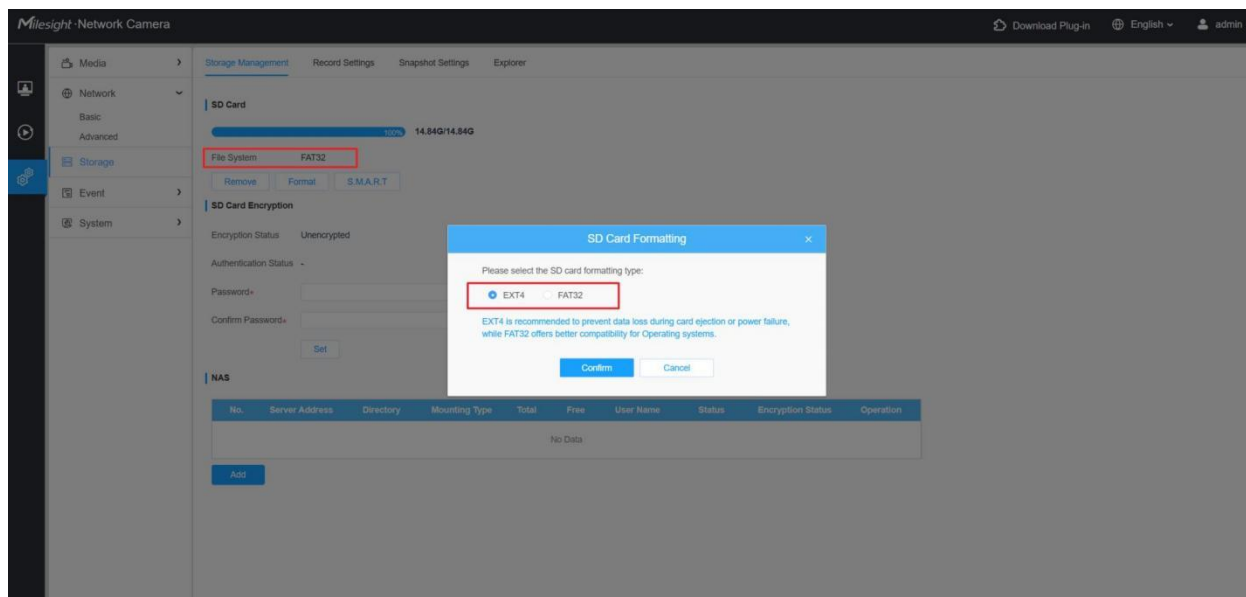
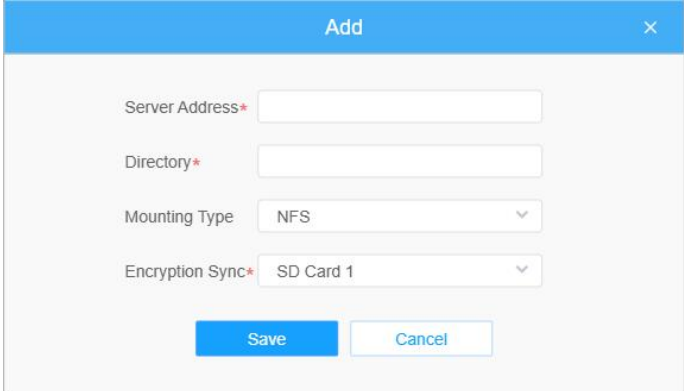


Table 41. Description of the buttons

Parameters	Function Introduction																																								
SD Card	The camera supports dual SD cards, each with up to 1TB capacity. Format: Format SD card, the files in SD card will be removed. Remove: Remove SD card. S.M.A.R.T: It is used to detect and display the SD card's health status. Click to view detailed health status information and the following window will displayed. <table border="1"> <thead> <tr> <th>Info</th><th>Data</th></tr> </thead> <tbody> <tr><td>version</td><td>v0.9.0(4dff9b6) arm64</td></tr> <tr><td>date</td><td>2025-04-11T15:40:44.000</td></tr> <tr><td>device</td><td>/dev/mmcblk0</td></tr> <tr><td>addTime</td><td>FALSE</td></tr> <tr><td>signature</td><td>0x70 0x58</td></tr> <tr><td>Longsys</td><td>TRUE</td></tr> <tr><td>SMARTVersions</td><td>2097152</td></tr> <tr><td>sizeofDevSMART</td><td>96</td></tr> <tr><td>originalBadBlock</td><td>80</td></tr> <tr><td>increaseBadBlock</td><td>0</td></tr> <tr><td>writeAllSectNum</td><td>13203026 Sector(512Byte)</td></tr> <tr><td>replaceBlockLeft</td><td>80</td></tr> <tr><td>degreeOfWear</td><td>0.03 Cycle</td></tr> <tr><td>sectorTotal</td><td>1999749120</td></tr> <tr><td>remainLifeTime</td><td>100%</td></tr> <tr><td>remainWrGBNum</td><td>3336.14TB</td></tr> <tr><td>lifeTimeTotal</td><td>3000.00 Cycle</td></tr> <tr><td>phyWrGBNum</td><td>0.03TB</td></tr> <tr><td>success</td><td>TRUE</td></tr> </tbody> </table> Storage Type: - Balanced Mode (Default): The system automatically allocates scheduled recordings and event recordings to SD Card 1 or SD Card 2 for optimal performance. - Note: Files are first stored on the SD card with more available space. - Primary-Secondary Mode: Scheduled recordings are saved to the primary SD card, while event recordings are saved to the secondary SD card. If one SD card fails or is removed, both scheduled and event recordings will be automatically saved to the remaining SD card.	Info	Data	version	v0.9.0(4dff9b6) arm64	date	2025-04-11T15:40:44.000	device	/dev/mmcblk0	addTime	FALSE	signature	0x70 0x58	Longsys	TRUE	SMARTVersions	2097152	sizeofDevSMART	96	originalBadBlock	80	increaseBadBlock	0	writeAllSectNum	13203026 Sector(512Byte)	replaceBlockLeft	80	degreeOfWear	0.03 Cycle	sectorTotal	1999749120	remainLifeTime	100%	remainWrGBNum	3336.14TB	lifeTimeTotal	3000.00 Cycle	phyWrGBNum	0.03TB	success	TRUE
Info	Data																																								
version	v0.9.0(4dff9b6) arm64																																								
date	2025-04-11T15:40:44.000																																								
device	/dev/mmcblk0																																								
addTime	FALSE																																								
signature	0x70 0x58																																								
Longsys	TRUE																																								
SMARTVersions	2097152																																								
sizeofDevSMART	96																																								
originalBadBlock	80																																								
increaseBadBlock	0																																								
writeAllSectNum	13203026 Sector(512Byte)																																								
replaceBlockLeft	80																																								
degreeOfWear	0.03 Cycle																																								
sectorTotal	1999749120																																								
remainLifeTime	100%																																								
remainWrGBNum	3336.14TB																																								
lifeTimeTotal	3000.00 Cycle																																								
phyWrGBNum	0.03TB																																								
success	TRUE																																								
SD Card Encryption	Each SD card can be encrypted individually for enhanced data security. Encryption Status: Show the encryption status of the SD card, including Encrypted and Unencrypted. Authentication Status: Display the authentication status. Password/ Confirm Password: Enter the password to lock you SD card.																																								

NAS	The network disk should be available within the network and properly configured to store the recorded files, etc. NAS (Network-Attached Storage), connecting the storage devices to the existing network, provides data and files services.  Server Address: IP address of NAS server. Directory: Input the NAS directory, e.g. “\path”. Mounting Type: NFS and SMB/CIFS are available. And you can set the user name and password to guarantee the security if SMB/CIFS is selected. Encryption Sync: You can select an SD card that supports synchronous encryption.  Note: - Up to 5 NAS disks can be connected to the camera. - For more details about how to use NAS on Milesight Network Camera, please refer to https://milesight.freshdesk.com/a/solutions/articles/69000797902.
-----	--

8.3.2 Record Settings

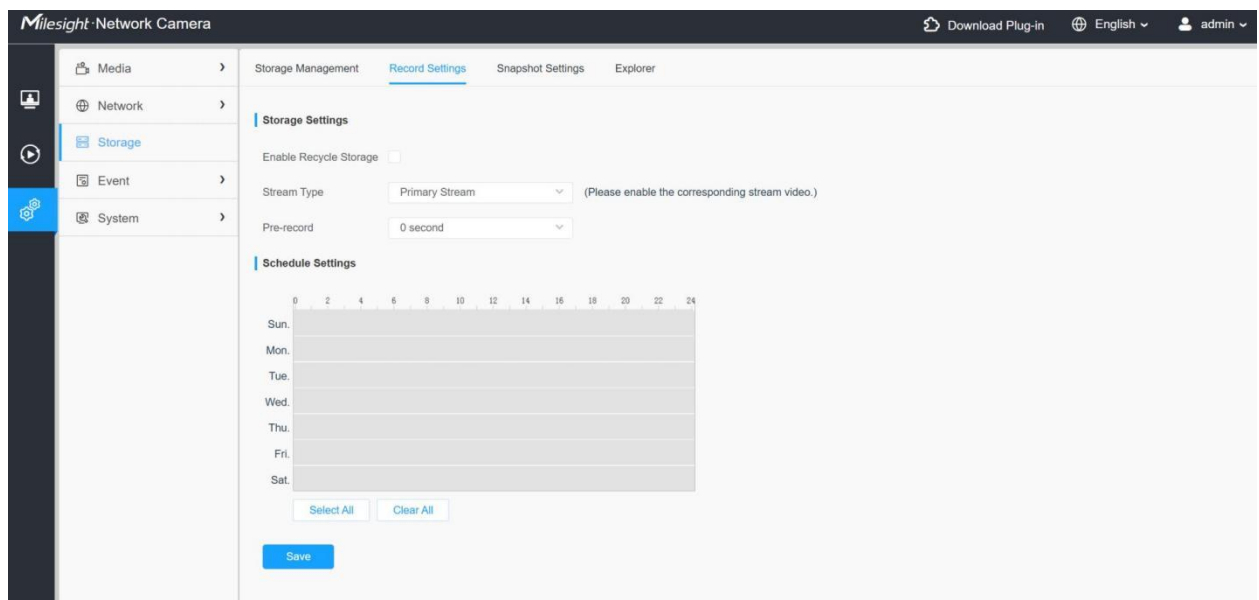
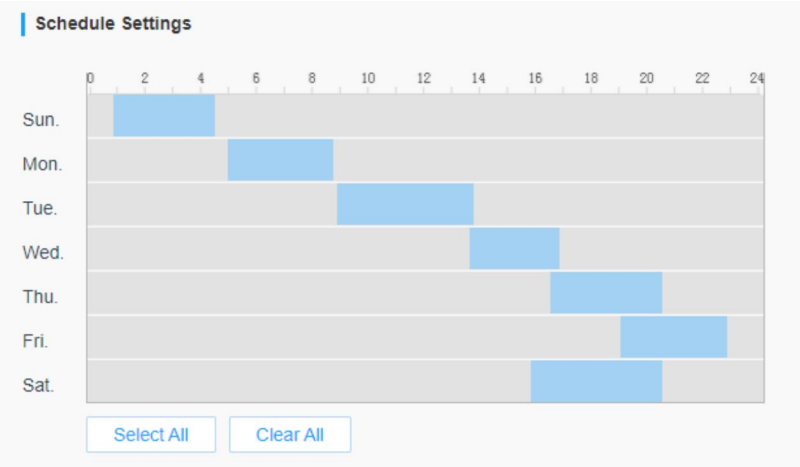
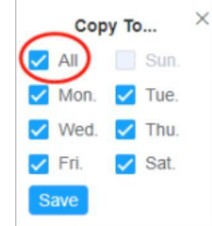
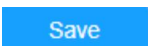


Table 42. Description of the buttons

Parameters	Function Introduction
------------	-----------------------

Enable Recycle Storage	Enable/Disable Recycle Storage, if you enable this option, it will delete the files when the free disk space reaches a certain value. - If one SD card is full and the recycle storage is disabled: New files will be saved to the SD card that still has available space. - If one or both SD cards are full and recycle storage is enabled: Each SD card will overwrite its own oldest files in a loop. - If both SD cards are full and recycle storage is disabled: Recording will stop.	
Stream Type	Select the Stream type, including Primary Stream and Secondary Stream.  Note: please enable the corresponding stream video.	
Pre Second	Reserve the record time before alarm, 0~10 sec.	
Schedule Settings	Edit record schedule as needed. Intuitive scheduling by drawing the time bar directly. 	
Parameters	Function Introduction	
Schedule Settings		Copy the schedule area to another date. The "All" button is handy to copy today's schedule to all days.
		Select all schedule.
		Clear all schedule.
		Save the configurations.

 **Note:** SD Card or NAS are available.

8.3.3 Snapshot Settings

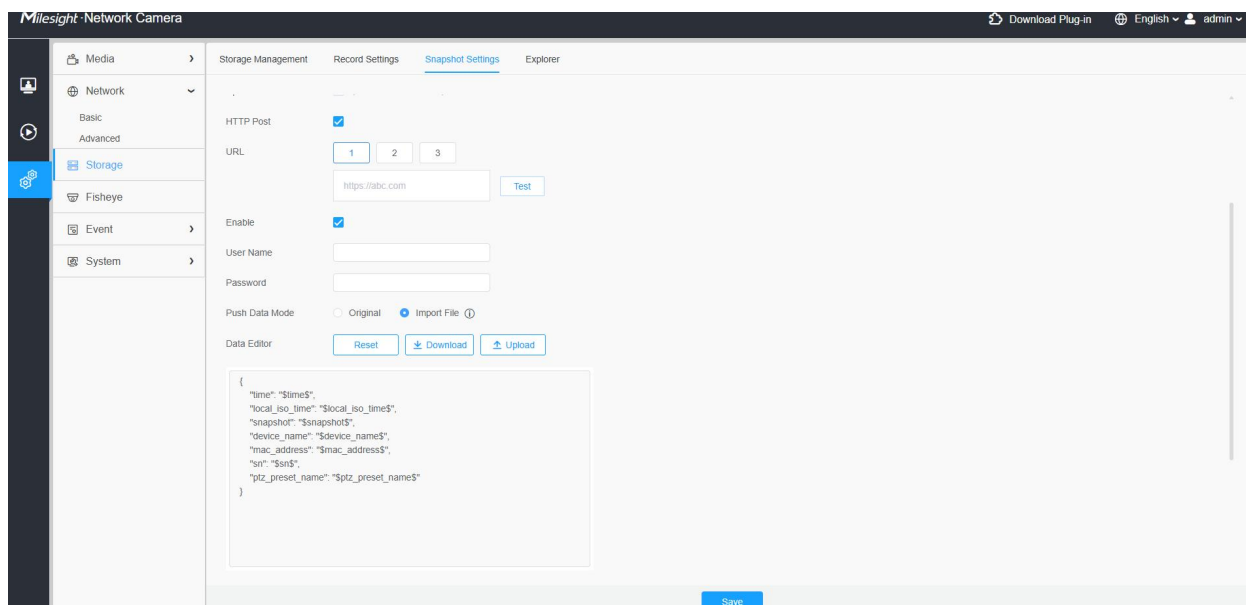
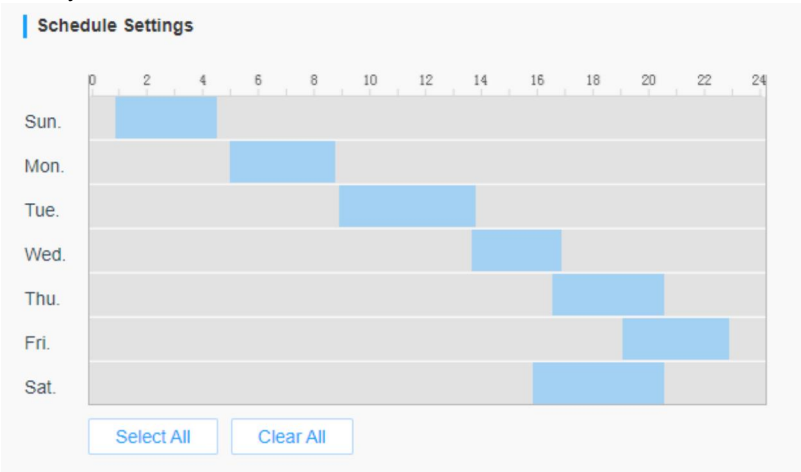
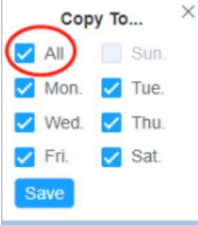


Table 43. Description of the buttons

Parameters	Function Introduction
Snapshot Settings	Enable Timing Snapshot: Check the checkbox to enable the Timing Snapshot function Interval: Set the snapshots interval, input the number and choose the unit(millisecond, second, minute, hour, day). Snapshot Quality: Selects the compression level for snapshots from three options: Low, Medium, and High. Higher quality gives better image detail at the cost of larger file size; lower quality reduces file size to save storage or bandwidth. Save to Storage: Save the snapshots into SD card or NAS, and choose the file name to add time suffix or overwrite the base file name. Upload Via FTP: Upload the snapshots via FTP. Upload Via Email: Upload the snapshots via Email. Note: If you choose to add time suffix, every snapshot picture will be saved, but if you choose to overwrite the base file name, only one latest picture will be saved. When you choose add overwrite the base file name to SD Card or NAS, it will create a file named "Snapshot" to place the snapshot. HTTP Post: Upload the snapshots via HTTP Post. Support uploading the snapshots to specified HTTP URL. HTTP Post supports the Push Data Mode, which enables data to be sent to third-party platforms for analysis and management. Two modes are available: Original and Import File. By default, the Original mode is selected. Original Mode: When Original is selected, the posted content follows the default Snapshot functionality and pushes the standard data content. Import File Mode: When Import File is selected, a Data Editor appears, allowing users to customize the format and content of the data being pushed. The result data file content is customizable using templates. You can edit, modify, and save the content in the editor. The template file will take effect after saving. For guidance on editing, please refer to the instructions available in the web interface.

	Edit record schedule as needed. Intuitive scheduling by drawing the time bar directly. 	
Schedule Settings		Copy the schedule area to another date. The "All" button is handy to copy today's schedule to all days.
Schedule Settings		Select all schedule.
Schedule Settings		Clear all schedule.
	Save the configurations.	

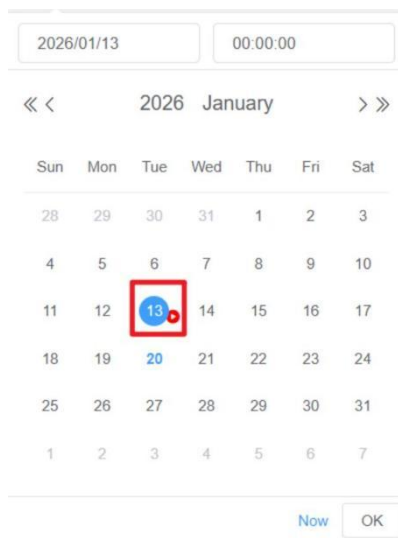
8.3.4 Explorer

Files will be seen on this page when they are configured to save into SD card or NAS. You can set time schedule every day for recording videos and save video files to your desired location.

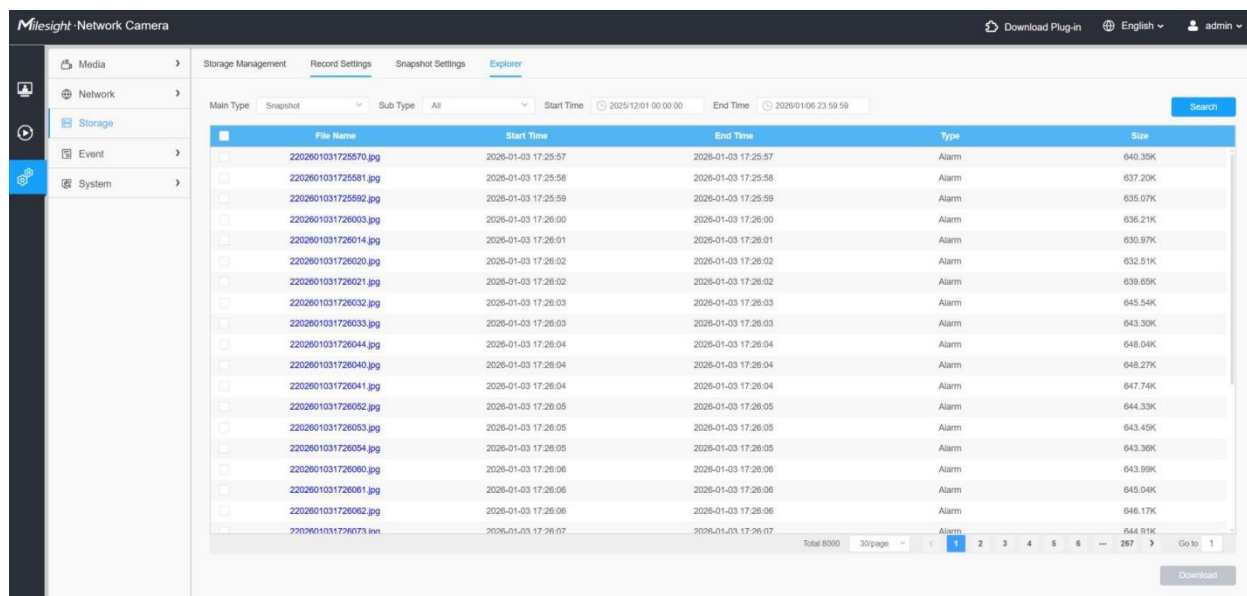


Note:

1. Files are visible once SD card is inserted. Don't insert or pull out SD card when power on
2. A red icon will appear under the corresponding date when there is a recording or snapshot exists for that day, allowing you to swiftly discern which dates possess files.



Video files are arranged by date. Set file type and start/end time to search out files. Each day files will be displayed under the corresponding date, from here you can copy and delete files etc. You can visit the files in SD card by ftp, for example, ftp://username:password@192.168.5.190 (user name and password are the same as the camera account and the IP followed is the IP of your device.).



8.4 Fisheye

[General]

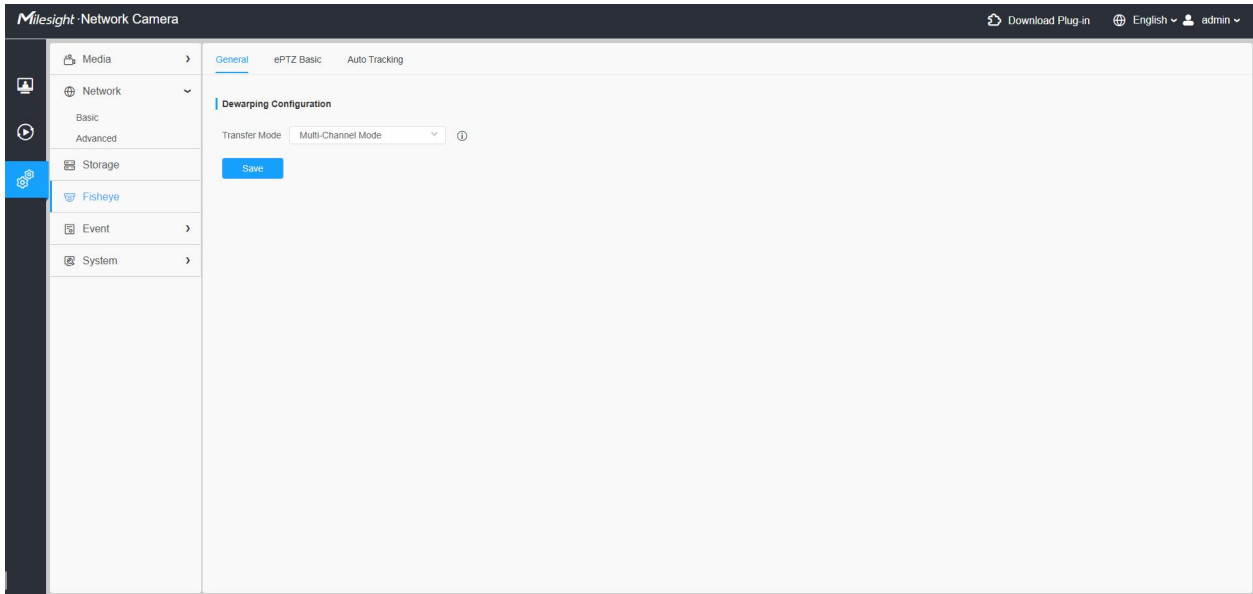


Table 44. Description of the buttons

Parameters	Function Introduction
Transfer Mode	Support to choose Bundle-Stream Mode or Multi-Channel Mode to meet different needs. Bundle-Stream Mode: the Bundle-Stream Mode combines all the channels into one and sends to NVR or VMS, which is easy for compatibility. Multi-Channel Mode: the Multi-Channel Mode sends all the original channels to NVR or VMS, so the channels can be modified separately.  Note: For more details about how to use two compatible modes of fisheye camera, please refer to https://milesight.freshdesk.com/a/solutions/articles/69000643424.

[PTZ]

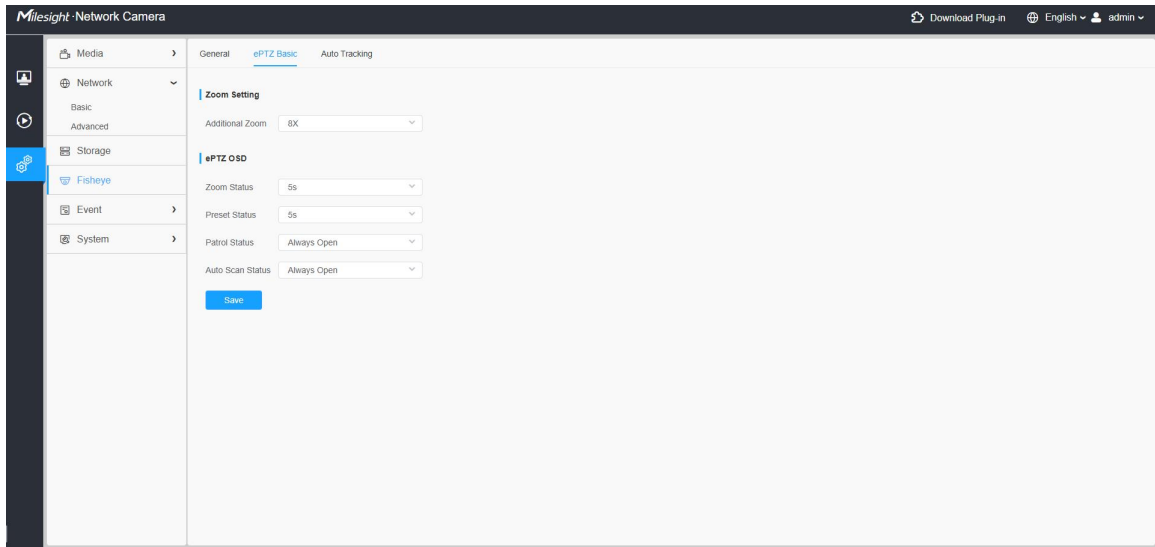


Table 45. Description of the buttons

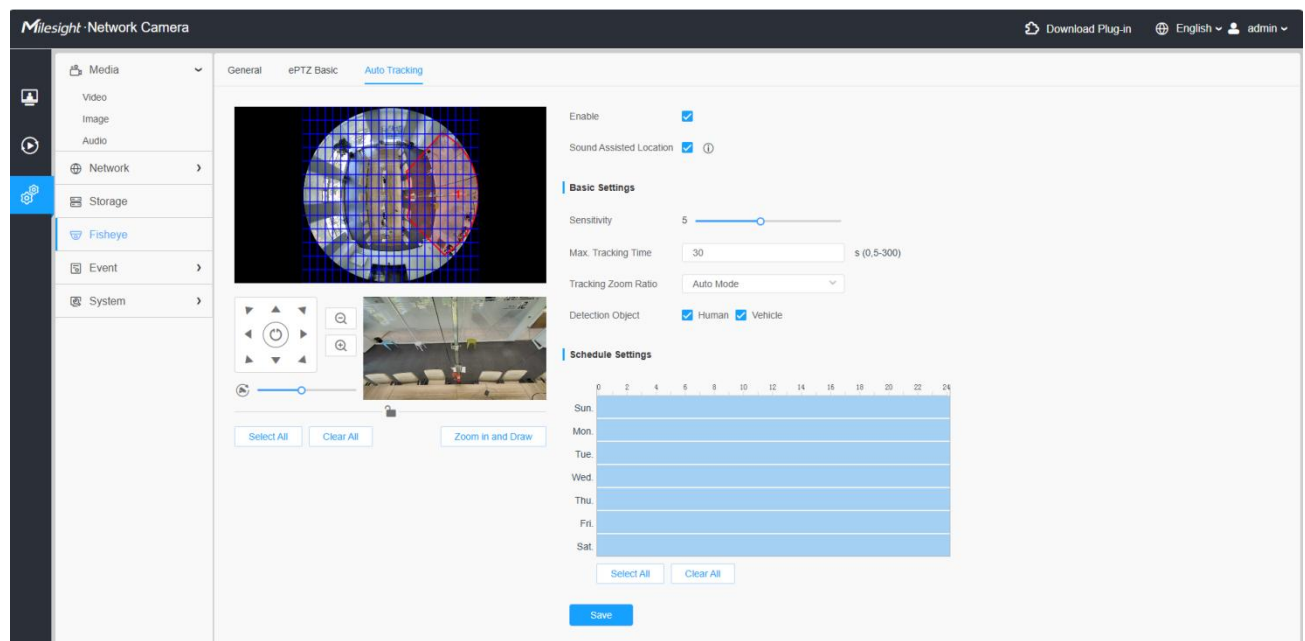
Parameters	Function Introduction
Additional Zoom	Allows you to set the maximum digital zoom level, up to 8X.
Zoom Status	Support to set display time of Zoom Status OSD. 2 seconds/5 seconds/10 seconds/Always Open/Always Close are available.
Preset Status	Support to set display time of Preset Status OSD. 2 seconds/5 seconds/10 seconds/Always Open/Always Close are available.
Patrol Status	Support to set display time of Patrol Status OSD. Always Open/Always Close are available.
Auto Scan Status	Support to set display time of Auto Scan Status OSD. Always Open/Always Close are available.

[Auto Tracking]

Auto Tracking allows the fisheye camera to automatically track moving objects within the configured region.

Note:

1. Auto Tracking cannot be used simultaneously with Violence Detection, Fall Detection, or Face Detection-Attribute Recognition. If you need to enable Auto Tracking, please disable these functions first. Conversely, when Auto Tracking is enabled, these AI functions cannot be enabled.
2. Only supported when Multi-Channel Mode 1O3R Display and VCA is enabled



Settings steps are shown as follows:

Step 1: Go to Event > AI Application Options, and enable VCA Event.

Step 2: Return to the Fisheye > Auto Tracking interface, and enable Auto Tracking

Step 3: Enable Sound Assisted Location to automatically detect and track targets that produce sound.

Note: To enable Sound Assisted Location, the following conditions must be met:

- ① a 12MP camera model;
- ② Audio Input set to MIC;
- ③ Live Video > Installation set to either Ceiling Mount or Flat Mount.

Step4: Set detecting sensitivity.

Step5: Set Max. Tracking Time which must be between 5~300s. The camera will stop tracking when the tracking time is used up.

Step6: Set Tracking Zoom Ratio including Auto Mode and Customize. The camera will automatically adjust tracking zoom ratio when Auto Mode is chosen. When Customize is chosen, user needs to set the tracking zoom ratio first by adjusting zoom button, then camera will automatically track the moving objects according to customized tracking zoom ratio and the object's proportion in the picture at the moment. At the same time, the object will always keep the same proportion in the picture during the tracking process.

Step7: Choose detection object. Check Human or Vehicle attribute, and the camera will alarm once detecting people or vehicle and triggering related events;

Step8: Set Auto Tracking schedule.

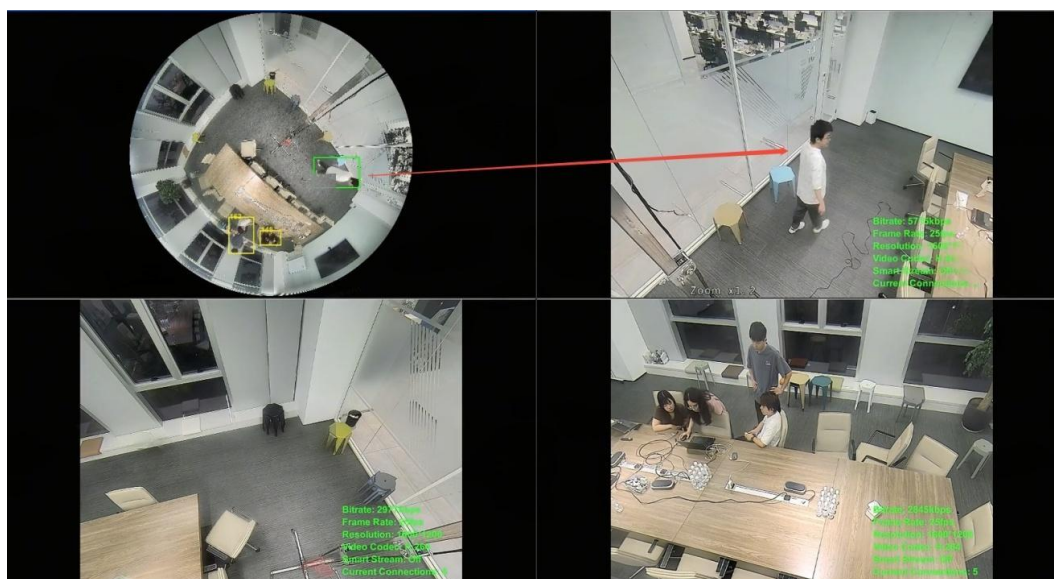
Step9: Draw the screen to set the detection region.

Step10: Click Save to save the configuration.

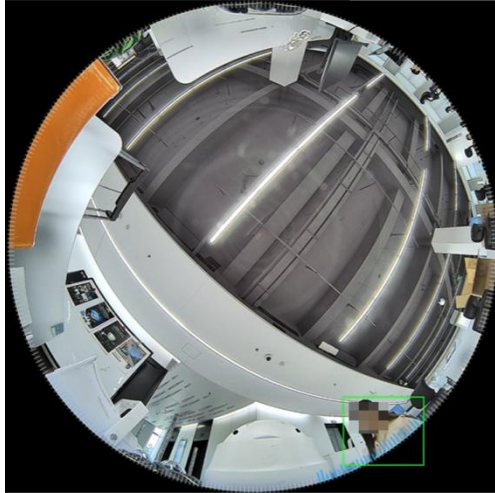
Step 11: Return to the Live View interface. The camera will assign Channel 2 as the dedicated tracking channel, as shown below.

Tracking can be triggered under the following conditions, with the following priority:

- ① Manual Tracking
- ② VCA Event-Triggered Tracking
- ③ Sound-Assisted Location Tracking
- ④ Auto Tracking



When Sound Assisted Location is enabled, the system displays a target box and a blue sound wave indicator in the original view to show the direction from which the sound is detected, as shown below.



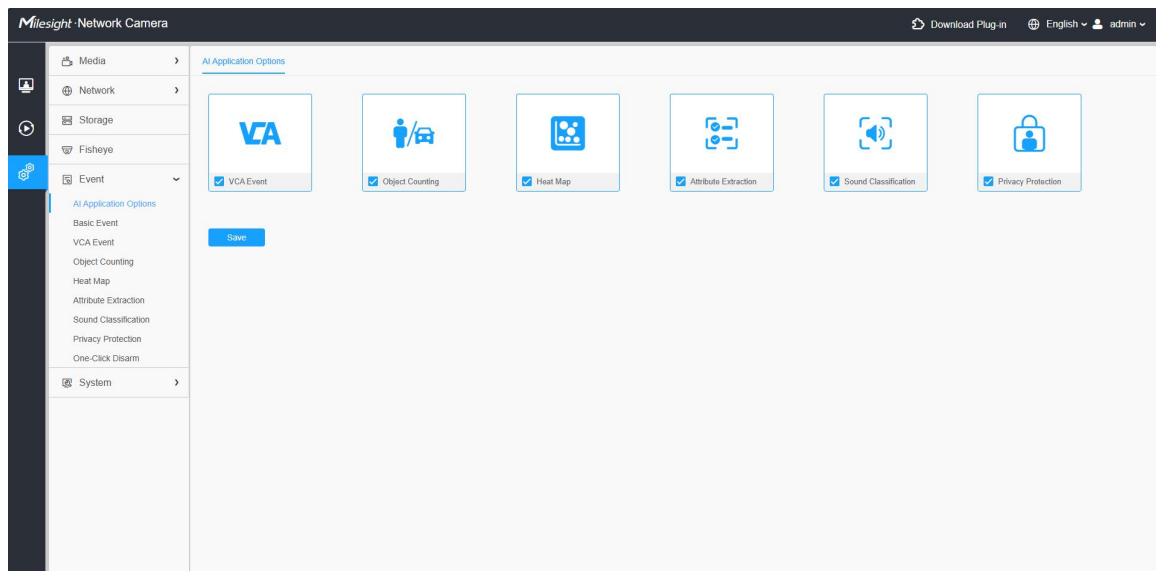
8.5 Event

Milesight event provides advanced, accurate smart video analytics for Milesight network cameras. It enhances the performance of network cameras through basic events and VCA events, enabling a comprehensive surveillance system and quicker response of cameras to different monitoring scenes.



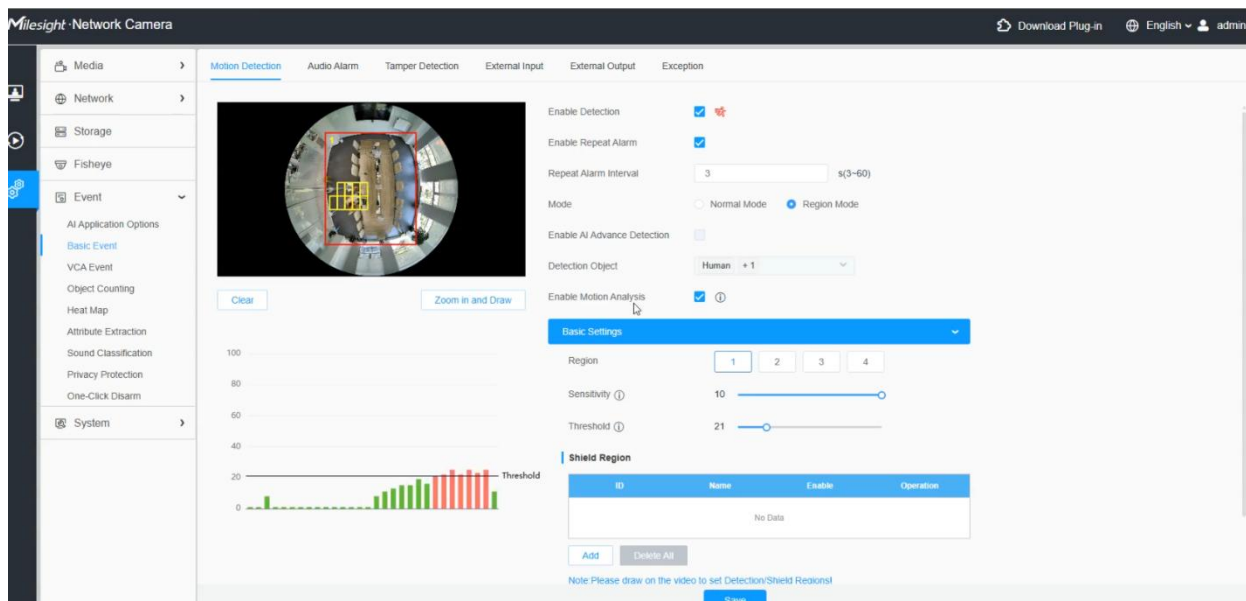
Note:

1. Before you utilizing the corresponding function, enable it first in the AI Application Options interface.



8.5.1 Basic Event

8.5.1.1 Motion Detection



Note: For details about how to configure Motion Detection, see <https://milesight.freshdesk.com/a/solutions/articles/69000643423>.

Configuration steps are shown as follows:

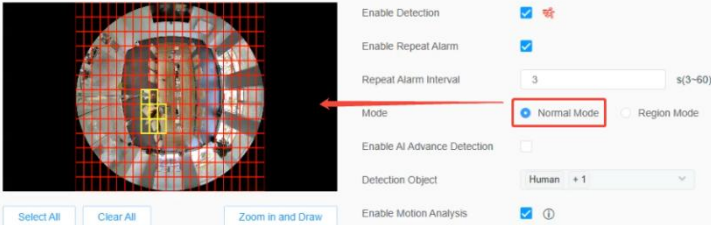
Step1: Choose Settings > Event > Basic Event > Motion Detection.

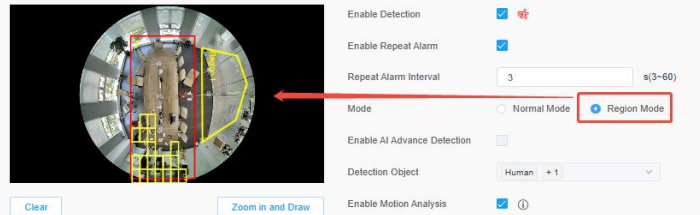
Step2: Check the check box to enable the function.

Step3: Check the check box to enable repeat alarms, enter the repeat interval from 3 to 60.

Step4: Select the detection mode and then draw the detection region.

Table 46. Description of the buttons

Parameters	Function Introduction
Enable Detection	Check the checkbox to enable the motion detection function.
Enable Repeat Alarm	Check this checkbox to enable repeat alarms.
Repeat Alarm Interval	Enter the repeat interval from 3 to 60.
Mode	Region Mode and Normal Mode are available. Normal Mode allows you to draw and customize detection zones freely across the entire live view  Region Mode allows you to configure up to four independent rectangular detection areas. To exclude specific zones from detection, you can also draw and add up to four shield regions using the same method. Detection regions are marked with blue boxes, which turn red when an event is triggered, while shield regions are indicated by yellow boxes.

	
Enable AI Advanced Detection	By enabling this option and choosing “Human” or “Vehicle” as the detection target, the system will only respond to movements of the selected type, filtering out background disturbances like swaying leaves.  Note: This option is only available in normal mode.
Enable Motion Analysis	When Motion Analysis is enabled, the moving region will turn yellow so that the user can know exactly where the motion occurred.  Note: Only support when HTTP is selected in Live View. 
	Click it to select the whole area.
	Click it to clear the selected areas.
	Click it to draw more precise detection regions in the pop-up window.
	Click it to save the configurations.

[Basic Settings]

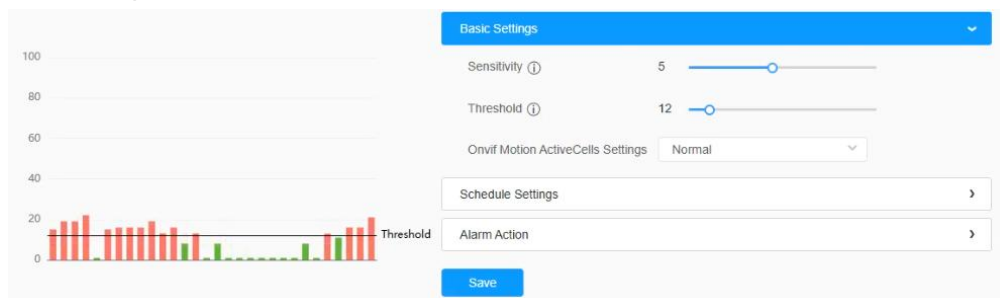


Table 47. Description of the buttons

Parameters	Function Introduction
------------	-----------------------

Threshold	Higher threshold requires a greater amount of motion area change to trigger an alarm.
Sensitivity	Higher sensitivity detects smaller movement to trigger alarm. Sensitivity level: 1~10.
Threshold Curve	The threshold curve displays whether the detection value exceeds the preset threshold over time, helping you visualize and fine-tune the motion detection settings.
Onvif Motion ActiveCells Settings	Normal and Compatible are available for the option. If the setting of motion region of the third-party software is different from ours, select Compatible here.

[Schedule Settings]

Step6: Set a motion detection schedule.

Table 48. Parameter Description

Parameter	Function Introduction
	Copy the schedule area to another date. The All button is handy to copy today's schedule to all days.
	Select all schedules.
	Clear all schedules.

[Alarm Action]

Step7: Set an alarm action.

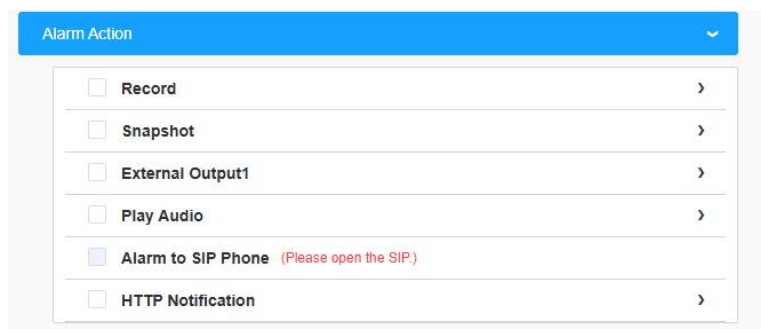


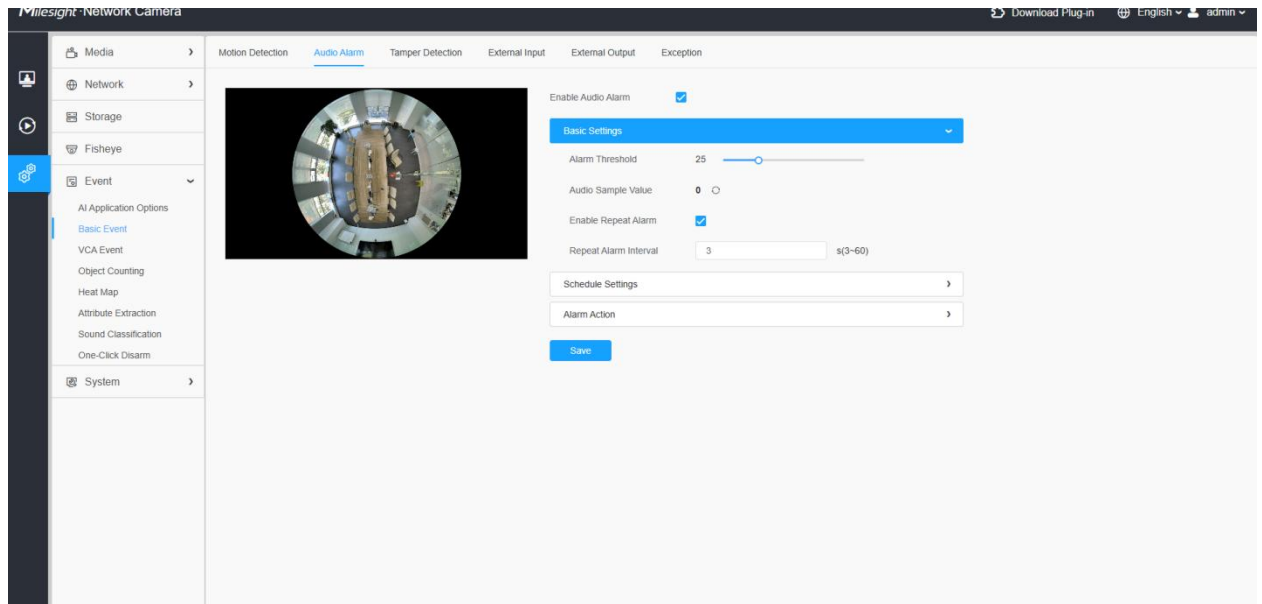
Table 49. Description of the buttons

Parameters	Function Introduction
Record	Duration: Selected the duration time of alarm. 5s/10s/15s/20s/25s/30s are available. Linkage: Alarm recording files can be saved to SD Card or NAS, uploaded via FTP, or sent via email.
Snapshot	Number: The number of snapshot, 1~5 are available. Interval: This cannot be edited unless you choose more than 1 to Snapshot. Linkage: Save alarm recording files into an SD card or NAS, upload the recording files via FTP, and send an alarm email.
External Output	If the camera is equipped with external outputs, you can enable the action after configuring the trigger duration. Two external output interfaces are available and can be configured independently. Action Time: Customize, 10 s, 30 s, 1 min., 5 min., and Constant are available for each output.
Play Audio	Auto/10 seconds/30 seconds/1 minute/5 minutes/10 minutes are available.  Note: Enable the Audio Speaker first.
Alarm to SIP Phone	Support to call the SIP phone after enabling the SIP function.
HTTP Notification	Support to push the alarm news to specified HTTP URL.  Note: • Three HTTP notifications at most can be added to the same event. • HTTP Notification supports Basic & Digest authentication.

8.5.1.2 Audio Alarm

Check the checkbox to enable the audio alarm function.

 **Note:** Enable the Audio Mic before using Audio Alarm function.



[Basic Settings]

Table 50. Description of the buttons

Parameters	Function Introduction
Alarm Threshold	Audio Alarm will be triggered when the thresholds reaches to a certain value from 0 to 100.
Audio Sample Value	The current value of the audio sample.
Enable Repeat Alarm	Check this checkbox to enable repeat alarms.
Repeat Alarm Interval	Enter the repeat interval from 3 to 60.

[Schedule Settings]

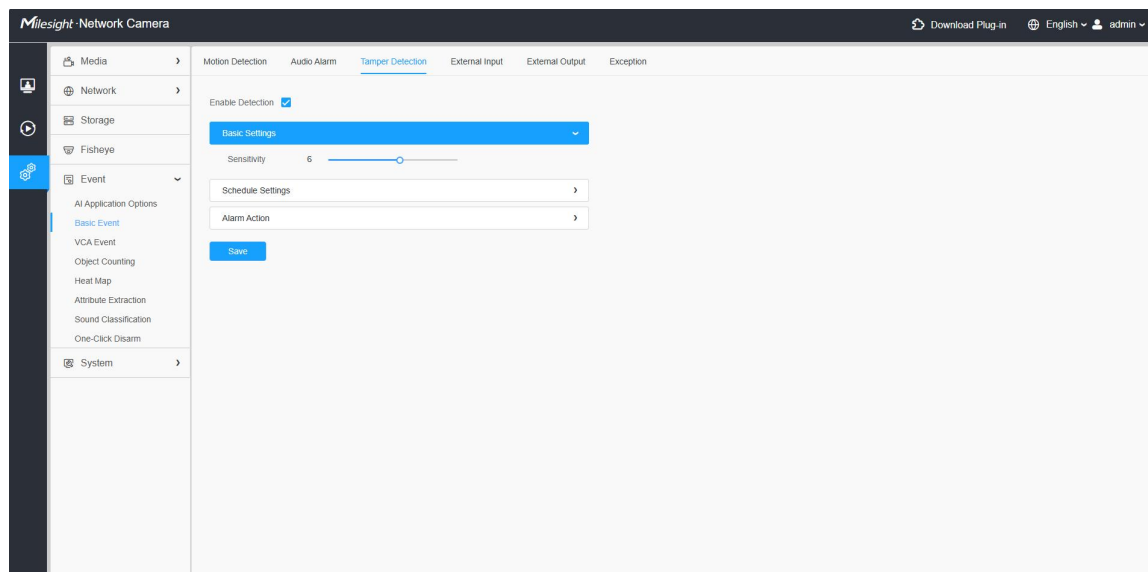
For details about Schedule Settings, see [8.5.1.1 Motion Detection](#)

[Alarm Action]

For details about Alarm Action, see [8.5.1.1 Motion Detection](#)

8.5.1.3 Tamper Detection

Tamper detection triggers an alarm if the device is blocked (detected by image changes), rotated, or dropped (detected by the acceleration sensor), and also supports defocus detection.



Settings steps are shown as follows:

Step1: Choose Settings > Event > Basic Event > Tamper Detection.

Step2: Enable Tamper Detection.

Sensitivity: Adjusts the detection sensitivity on a scale from 1 to 10. Higher sensitivity values allow the system to detect smaller changes in the image.

[Schedule Settings]

Step3: Set a detection schedule.

 **Note:** For details about Schedule Settings, see [8.5.1.1 Motion Detection](#)

[Alarm Action]

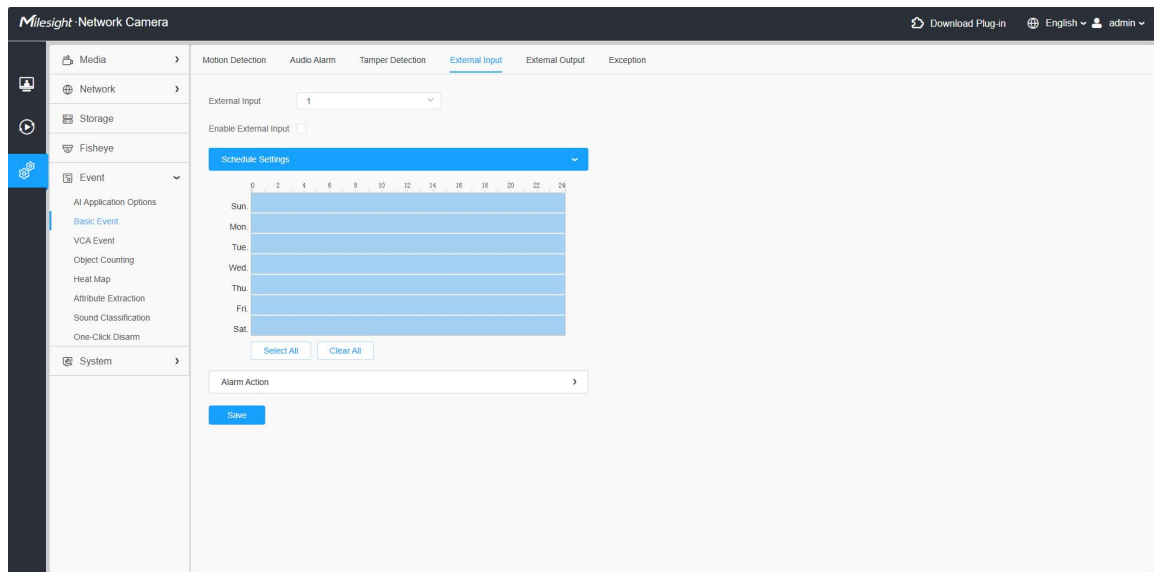
Step4: Set an alarm action.

 **Note:**

- For details about Alarm Action, see [8.5.1.1 Motion Detection](#)
- If you enable External Output and choose Constant External Output Action Time, when possible tampering is detected, the alarm time will be always constant till the alarm is released.

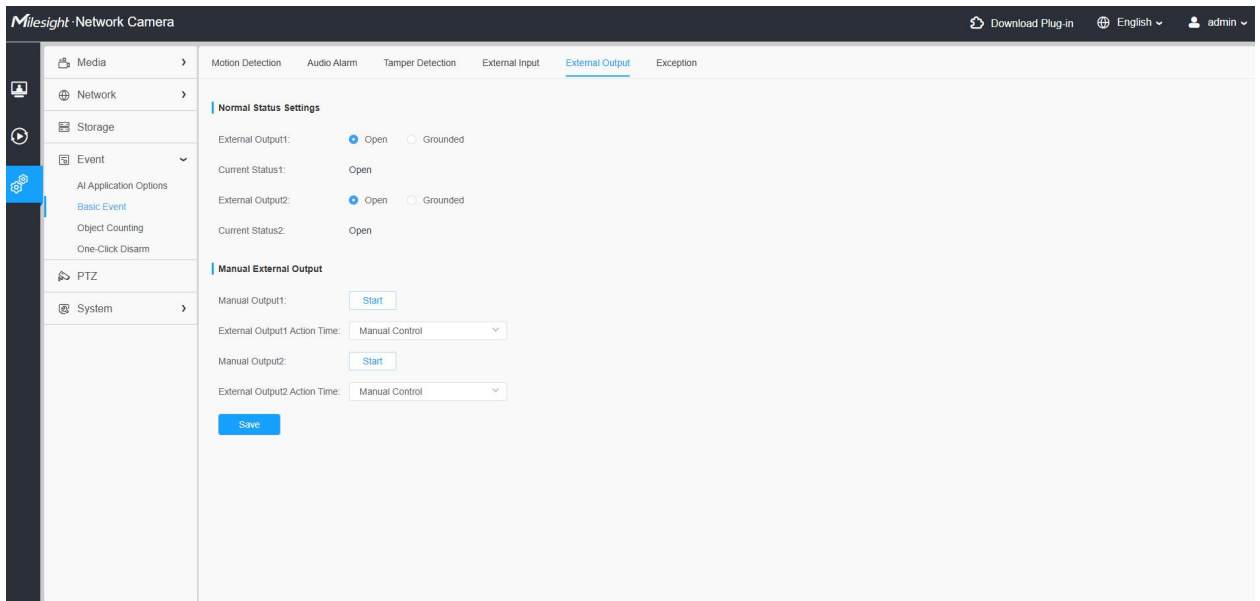
8.5.1.4 External Input

This interface enables the camera to integrate with external devices (e.g., door contacts, motion sensors, or panic buttons). When an external device is activated, the camera can automatically trigger alarms, record video, or perform other preset actions based on your configuration.



8.5.1.5 External Output

Supports configuration of two external output interfaces.



[Normal Status Settings]

Set the normal status first, when the Current Status is different with Normal Status, an alarm will be triggered.

[Manual External Output]

You can set the manual external output.

Table 51. Description of the buttons

Parameter	Function Introduction
Manual Output	Click it to start or stop manual external output.
External Output Action Time	Manual Control, Customize, 10 s, 1 min., 5 min., and 10 min. are available.

8.5.1.6 Exception

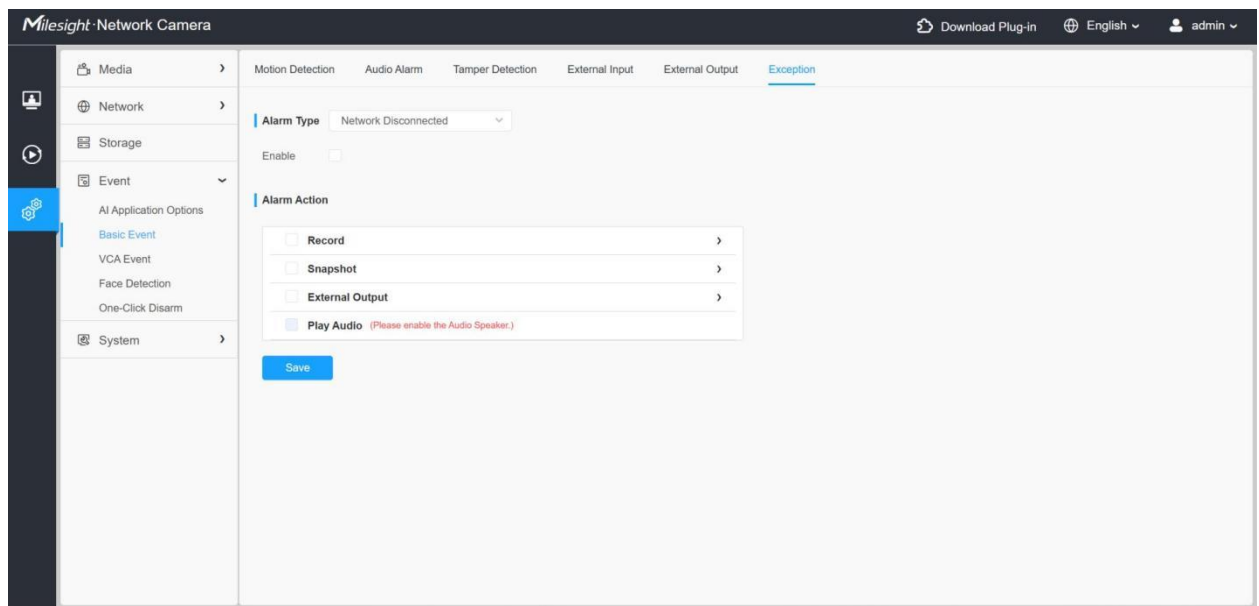


Table 52. Description of the buttons

Parameters	Function Introduction
Alarm Type	Network Disconnected, IP Address Conflicted, Record Failed, SD Card Full, SD Card Uninitialized, SD Card Error, and No SD Card are available. When Record Failed is selected, Repeat alarm can be enabled. You can enter the Repeat Alarm interval from 3 to 60(s). Check the checkbox to enable the alarm type you selected.
Alarm Action	For more details, see Table 3 (page 96) .

8.5.2 VCA Event

Smart Event uses VCA (Video Content Analysis) technology, which provides advanced, accurate smart video analysis for Milesight network cameras. Powered by AI chip, the new generation video analytics is capable of recognizing vast attributes of human, vehicle, and object pattern recognition models. As vehicle and human related events are very important in security monitoring, the filtering is supported to better optimize the efficiency.



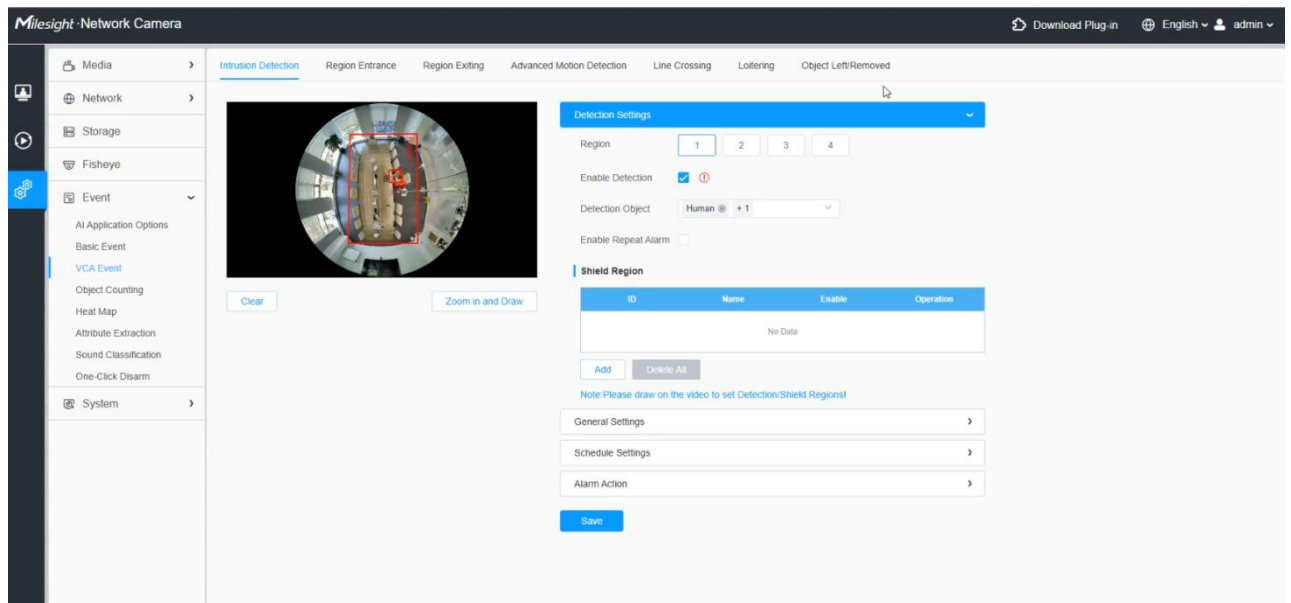
Note:

- VCA Event Detection supports three main target categories: humans, vehicles (including motorcycles, buses, cars, and trucks), and non-motor vehicles (including e-scooters and bicycles).
The available categories depend on the camera mounting type, as detailed below:
 - Flat Mount: Only human detection is supported, as this setup is typically used indoors and does not cover vehicles.
 - Ceiling Mount: Supports detection of humans and vehicles (including buses, cars, and trucks). Non-motor vehicles are not supported due to their small size and limited visibility in ceiling-mounted fisheye views.

- ③ Wall Mount: Supports detection of humans, vehicles (including motorcycles, buses, cars, and trucks), and non-motor vehicles (including e-scooters and bicycles) without the above limitations.
2. For more details about the Milesight AI Video Content Analysis information, please refer to <https://resource.milesight.com/milesight/security/document/a-milesight-technology-moment/a-milesight-technology-moment-milesight-vca.pdf>

8.5.2.1 Intrusion Detection

Intrusion detection is used to protect a specific area from potential threats of intrusion by suspicious people or other objects. Whether it is an intrusion from outside the region or a sudden appearance within the region, an alarm action will be triggered.



Settings steps are shown as follows:

[Detection Settings]

Detection Settings

Region

1234

Enable Detection

☐

Detection Object

Human @

Enable Repeat Alarm

☐

Shield Region

ID	Name	Enable	Operation
No Data			

Add

Delete All

Note: Please draw on the video to set Detection/Shield Regions!

General Settings

Schedule Settings

Alarm Action

Save

Step 1:

Go to Settings > Event > VCA Event > Intrusion Detection.

Step 2:

Select a region number, then draw a detection region directly on the live view. For more precise area selection, you can click Zoom in and Draw to adjust the region in greater detail. Up to four detection regions can be configured.

Step 3:

Enable Intrusion Detection.

Step 4:

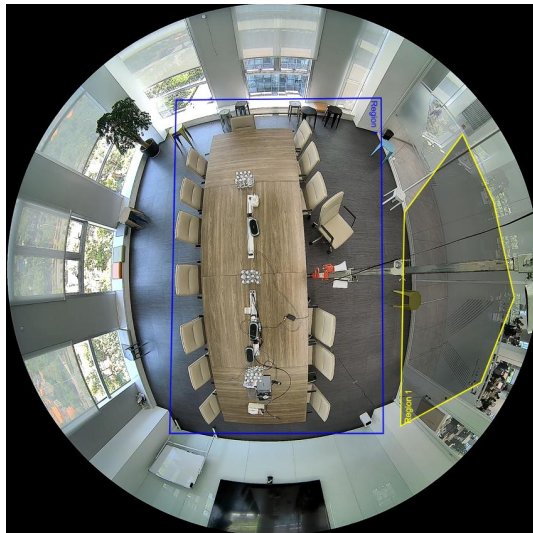
Select the detection objects. An alarm will be triggered when the selected object is detected.

Step 5:

Enable Repeat Alarm if you want the alarm to repeat. Set the Repeat Alarm Interval (3–60 seconds).

Step 6:

To exclude certain areas from detection, manually draw and add up to four Shield Regions. The method is the same as drawing detection regions. Detection regions are marked with a blue box, and shield regions with a yellow box.

**[General Settings]**

Step7: Set detecting sensitivity and object size limits, and set the trigger mode with General Mode or Bottom Mode.

General Settings

Min. Intrusion Duration

0

s(0~10)

Sensitivity

5

Trigger Mode

Bottom Mode

Object Size Filter

Edit

☒ Min. Size

☐ Max. Size

Note: Please draw on the video to set Detection Regions/Lines!

Schedule Settings

Alarm Action

Save

Table 53. Description of the buttons

Parameters	Function Introduction
Min. Intrusion Duration	Set the minimum time (0–10 seconds) that a target must remain within the detection region before the camera triggers an intrusion alarm. This helps reduce false alarms caused by brief or accidental entries.
Sensitivity	Level 1~10 are available, the default level is 5. The higher the sensitivity, the easier it is for moving objects to be recorded in the results.
Trigger Mode	Set the desired mode of the trigger logic including General Mode and Bottom Mode. General Mode: The alarm is triggered when the object's body roughly enters the detection area. Bottom Mode: the alarm will be triggered as soon as the bottom of the object enters the detection area. Suitable for scenarios that require sensitivity to intrusion status/ bottom detection preference.
Min. Size	Draw on the screen to set the maximum size of the detected object. Objects larger than this size will not be detected. The default maximum size is 320x240.
Max. Size	Draw the screen to set the maximum size of the detected object. When the object is larger than this size, it will not be detected. The default maximum size is 320*240.

[Schedule Settings]**Step8:** Set a detection schedule.

Detection Settings >

General Settings >

Schedule Settings ▾

0 2 4 6 8 10 12 14 16 18 20 22 24

Sun.

Mon.

Tue.

Wed.

Thu.

Fri.

Sat.

Select All Clear All

Alarm Action >

Save

 **Note:** For details about Schedule Settings, see [8.4.1.1 Motion Detection](#)

Step9: Set an alarm action.

Alarm Action

☐ Record	>
☐ Snapshot	>
☐ External Output1	>
☐ Play Audio	>
☐ Alarm to SIP Phone (Please open the SIP.)	>
☐ HTTP Notification	>
☐ ePTZ Auto Tracking (Please Enable the Auto Tracking.)	>

**Note:**

1. For details about Alarm Action, see [8.4.1.1 Motion Detection](#)
2. For fisheye camera models, VCA events can be linked to ePTZ auto tracking, enabling the camera to automatically track moving objects within the configured region. For more details about auto tracking, please refer to: [\[Auto Tracking\]](#).

8.5.2.2 Region Entrance

Region entrance helps to protect a special area from potential threat of suspicious person's or object's entrance. An alarm will be triggered when objects enter the selected regions by enabling region entrance.

Settings steps are shown as follows:

[Detection Settings]

Detection Settings

Region

1

2

3

4

Enable Detection
☐

Detection Object
Human
+ 1

Shield Region

ID	Name	Enable	Operation
No Data			

Add
Delete All

Note: Please draw on the video to set Detection/Shield Regions!

General Settings

Schedule Settings

Alarm Action

Save

Step 1:

Go to Settings > Event > VCA Event > Region Entrance.

Step 2:

Select a region number, then draw a detection region directly on the live view. For more precise area selection, you can click Zoom in and Draw to adjust the region in greater detail. Up to four detection regions can be configured.

Step 3:

Enable Region Entrance.

Step 4:

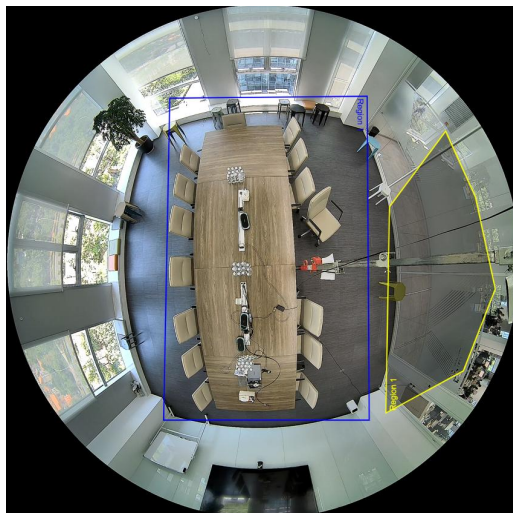
Select the detection objects. An alarm will be triggered when the selected object is detected.

Step 5:

Enable Repeat Alarm if you want the alarm to repeat. Set the Repeat Alarm Interval (3–60 seconds).

Step 6:

To exclude certain areas from detection, manually draw and add up to four Shield Regions. The method is the same as drawing detection regions. Detection regions are marked with a blue box, and shield regions with a yellow box.



[General Settings]

Step7: Set detecting sensitivity, choose Trigger Mode and object size limits.

The screenshot shows the 'Detection Settings' interface. At the top is a 'Detection Settings' header with a right arrow. Below it is a blue 'General Settings' section with a dropdown arrow. Inside 'General Settings', there is a 'Sensitivity' slider set to 5, a 'Trigger Mode' dropdown menu currently showing 'General Mode', and an 'Object Size Filter' section. The 'Object Size Filter' section includes an 'Edit' button and two radio buttons: 'Min. Size' (selected) and 'Max. Size'. Below these is a note: 'Note: Please draw on the video to set Detection Regions/Lines!'. At the bottom of the settings panel are three expandable sections: 'Schedule Settings', 'Alarm Action', and a 'Save' button.

Table 54. Description of the buttons

Parameters	Function Introduction
Sensitivity	Level 1~10 are available, the default level is 5. The higher the sensitivity, the easier it is for moving objects to be recorded in the results.
Trigger Mode	Set the desired mode of the trigger logic including General Mode and Bottom Mode. General Mode: The alarm is triggered when the object's body roughly enters the detection area. Bottom Mode: the alarm will be triggered as soon as the bottom of the object enters the detection area. Suitable for scenarios that require sensitivity to intrusion status/ bottom detection preference.
Min. Size	Draw on the screen to set the minimum size of the detected object. Objects smaller than this size will not be detected. The default minimum size is 3x3.
Max. Size	Draw on the screen to set the maximum size of the detected object. Objects larger than this size will not be detected. The default maximum size is 320x240.

[Schedule Settings]

Step8: Set a detection schedule.

Detection Settings

General Settings

Schedule Settings

0 2 4 6 8 10 12 14 16 18 20 22 24

Sun.

Mon.

Tue.

Wed.

Thu.

Fri.

Sat.

Select All Clear All

Alarm Action

Save

 **Note:** This part is the same as the regular schedule settings. You can refer to [8.4.1.1 Motion Detection](#)

[Alarm Action]

Step9: Set an alarm action.

Alarm Action

☐ Record

☐ Snapshot

☐ External Output1

☐ Play Audio

☒ Alarm to SIP Phone (Please open the SIP.)

☐ HTTP Notification

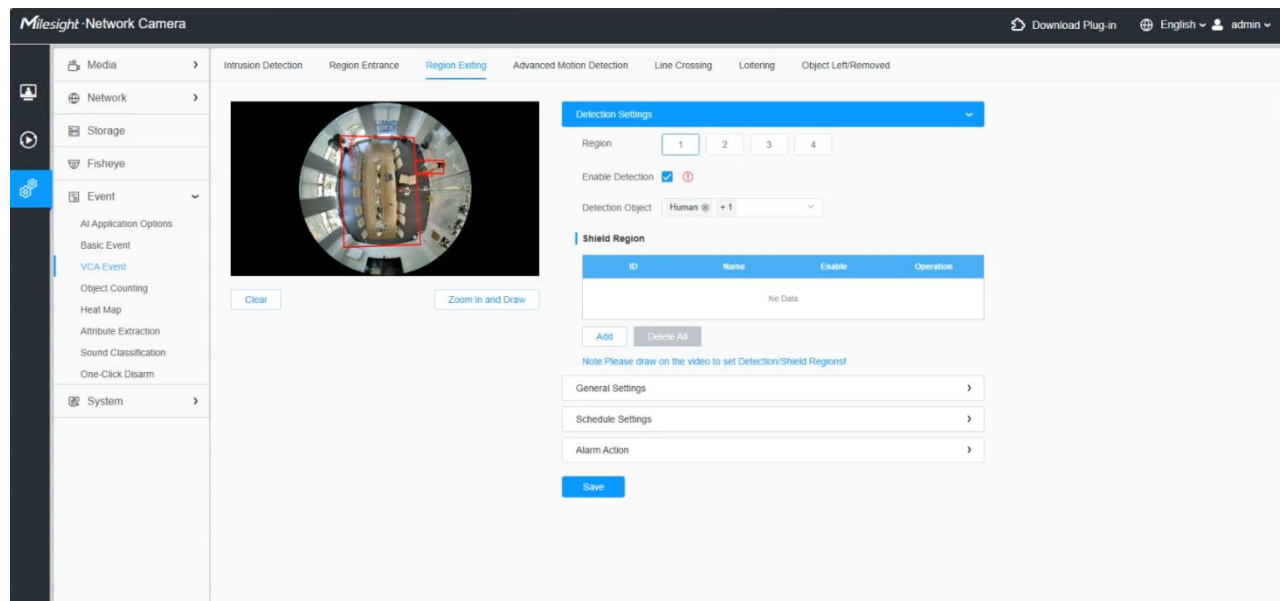
☒ ePTZ Auto Tracking (Please Enable the Auto Tracking.)

 **Note:**

1. For details about Alarm Action, see [8.4.1.1 Motion Detection](#)
2. For fisheye camera models, VCA events can be linked to ePTZ auto tracking, enabling the camera to automatically track moving objects within the configured region. For more details about auto tracking, please refer to: [\[Auto Tracking\]](#).

8.5.2.3 Region Exiting

Region exiting is to make sure that any person or object won't exit the area that is being monitored. Any exit of people or objects will trigger an alarm.



Settings steps are shown as follows:

[Detection Settings]

Detection Settings

Region

1234

Enable Detection

☐

Detection Object

Human @ +1

Shield Region

ID	Name	Enable	Operation
No Data			

Add

Delete All

Note: Please draw on the video to set Detection/Shield Regions!

General Settings

Schedule Settings

Alarm Action

Save

Step 1:

Go to Settings > Event > VCA Event > Region Exiting.

Step 2:

Select a region number, then draw a detection region directly on the live view. For more precise area selection, you can click Zoom in and Draw to adjust the region in greater detail. Up to four detection regions can be configured.

Step 3:

Enable Region Exiting.

Step 4:

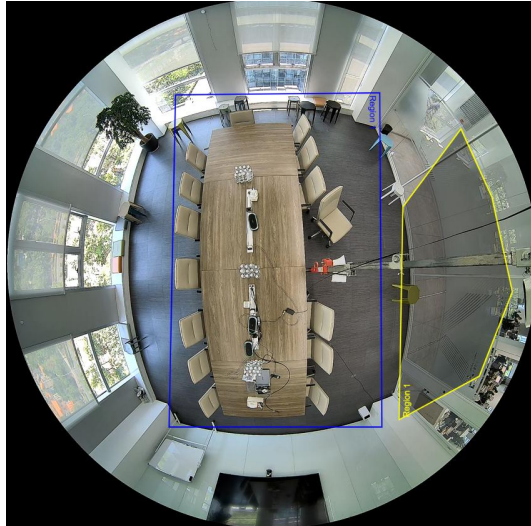
Select the detection objects. An alarm will be triggered when the selected object is detected.

Step 5:

Enable Repeat Alarm if you want the alarm to repeat. Set the Repeat Alarm Interval (3–60 seconds).

Step 6:

To exclude certain areas from detection, manually draw and add up to four Shield Regions. The method is the same as drawing detection regions. Detection regions are marked with a blue box, and shield regions with a yellow box.

**[General Settings]**

Step7: Set detecting sensitivity and object size limits, and set the trigger mode with General Mode or Bottom Mode.

Table 55. Description of the buttons

Parameters	Function Introduction
Sensitivity	Level 1~10 are available, the default level is 5. The higher the sensitivity, the easier it is for moving objects to be recorded in the results.

Trigger Mode	Set the desired mode of the trigger logic including General Mode and Bottom Mode. General Mode: The alarm is triggered when the object's body roughly enters the detection area. Bottom Mode: the alarm will be triggered as soon as the bottom of the object enters the detection area. Suitable for scenarios that require sensitivity to intrusion status/bottom detection preference.
Min. Size	Draw the screen to set the minimum size of the detected object. When the object is smaller than this size, it will not be detected. The default minimum size is 3*3.
Max. Size	Draw the screen to set the maximum size of the detected object. When the object is larger than this size, it will not be detected. The default maximum size is 320*240.

[Schedule Settings]

Step8: Set a detection schedule.

The screenshot shows the 'Detection Settings' interface. The 'Schedule Settings' tab is selected. It features a 24-hour timeline at the top and a grid for selecting detection hours for each day of the week (Sun. to Sat.). The grid shows all hours are currently selected (blue). Below the grid are 'Select All' and 'Clear All' buttons. At the bottom, there is an 'Alarm Action' dropdown menu and a 'Save' button.

Note: This part is the same as the regular schedule settings. You can refer to [8.4.1.1 Motion Detection](#)

[Alarm Action]

Step9: Set an alarm action.

Alarm Action

☐ Record	>
☐ Snapshot	>
☐ External Output1	>
☐ Play Audio	>
☒ Alarm to SIP Phone (Please open the SIP.)	
☐ HTTP Notification	>
☒ ePTZ Auto Tracking (Please Enable the Auto Tracking.)	

**Note:**

1. For details about Alarm Action, see [8.4.1.1 Motion Detection](#)
2. For fisheye camera models, VCA events can be linked to ePTZ auto tracking, enabling the camera to automatically track moving objects within the configured region. For more details about auto tracking, please refer to: [\[Auto Tracking\]](#).

8.5.2.4 Advanced Motion Detection

Different from traditional motion detection, advanced motion detection can filter out “noise” such as lighting changes, natural tree movements, etc. When an object moves in the selected area, it will trigger alarm.

Settings steps are shown as follows:

[Detection Settings]

Detection Settings

Region

1

2

3

4

Enable Detection
☐

Detection Object

Human

+ 1

Enable Repeat Alarm
☐

Shield Region

ID	Name	Enable	Operation
No Data			

Add
Delete All

Note: Please draw on the video to set Detection/Shield Regions!

General Settings

Schedule Settings

Alarm Action

Save

Step 1:

Go to Settings > Event > VCA Event > Advanced Motion Detection.

Step 2:

Select a region number, then draw a detection region directly on the live view. For more precise area selection, you can click Zoom in and Draw to adjust the region in greater detail. Up to four detection regions can be configured.

Step 3:

Enable Advanced Motion Detection.

Step 4:

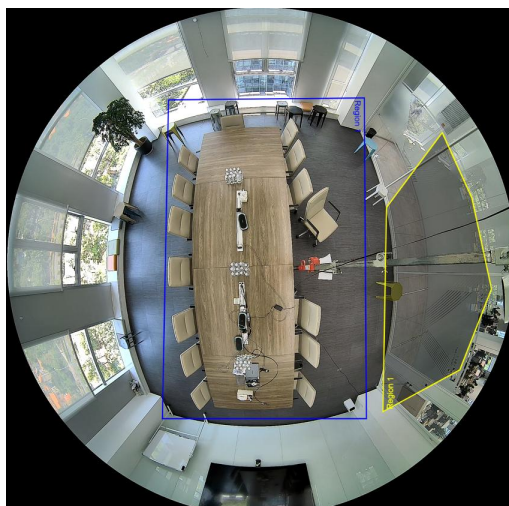
Select the detection objects. An alarm will be triggered when the selected object is detected.

Step 5:

Enable Repeat Alarm if you want the alarm to repeat. Set the Repeat Alarm Interval (3–60 seconds).

Step 6:

To exclude certain areas from detection, manually draw and add up to four Shield Regions. The method is the same as drawing detection regions. Detection regions are marked with a blue box, and shield regions with a yellow box.



[General Settings]

Step7: Set Ignore Short-Lived Motion time. If you set the time, when the moving duration of an object is within the setting time, the alarm will not be triggered.

Step8: Set detecting sensitivity and object size limits.

Table 56. Description of the buttons

Parameters	Function Introduction
Ignore Short-Lived Motion	The alarm will not be triggered when the moving duration of an object is within the setting time. Off/1s/2s/3s/4s/5s are available. Note: Ignore Short-Lived Motion time is to avoid false alarm caused by instant object movement within time setting.
Sensitivity	Level 1~10 are available, the default level is 5. The higher the sensitivity, the easier it is for moving objects to be recorded in the results. Note: The sensitivity can be configured to detect various movement according to different requirements. When the level of sensitivity is low, slight movement won't trigger the alarm.
Trigger Mode	Set the desired mode of the trigger logic including General Mode and Bottom Mode. General Mode: The alarm is triggered when the object's body roughly enters the detection area. Bottom Mode: the alarm will be triggered as soon as the bottom of the object enters the detection area. Suitable for scenarios that require sensitivity to intrusion status/bottom detection preference.
Min. Size	Draw the screen or input pixel number to set the minimum size of the detected object. When the object is smaller than this size, it will not be detected. The default minimum size is 3*3.
Max. Size	Draw the screen or input pixel number to set the maximum size of the detected object. When the object is larger than this size, it will not be detected. The default maximum size is 320*240.

[Schedule Settings]

Step9: Set a detection schedule.

 **Note:** This part is the same as the regular schedule settings. You can refer to [8.4.1.1 Motion Detection](#)

[Alarm Action]

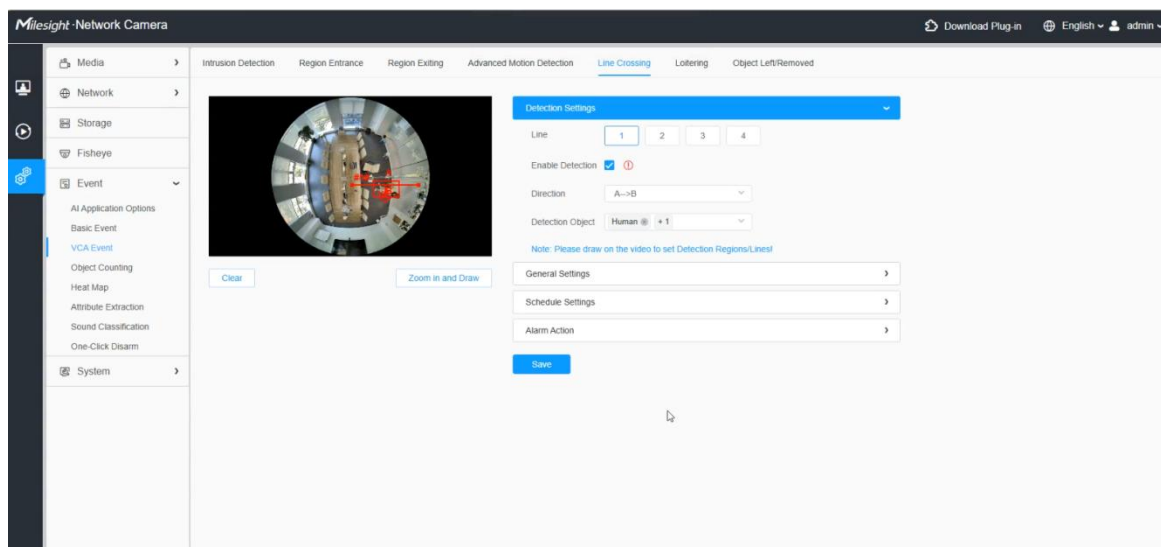
Step10: Set an alarm action.

 **Note:**

1. For details about Alarm Action, see [8.4.1.1 Motion Detection](#)
2. For fisheye camera models, VCA events can be linked to ePTZ auto tracking, enabling the camera to automatically track moving objects within the configured region. For more details about auto tracking, please refer to: [\[Auto Tracking\]](#).
3. If you enable External Output and choose Constant External Output Action Time, when object motion time is longer than the Ignore Short-Lived Motion time which you set in the selected regions, External Output Action alarm time will be always constant till the alarm is released.

8.5.2.5 Line Crossing

Line Crossing detection is designed to work in most indoor and outdoor environment. An event will be triggered every time when the camera detects objects crossing a defined virtual line.



Settings steps are shown as follows:

[Detection Settings]

Step 1:

Go to Settings > Event > VCA Event > Line Crossing.

Step 2:

Select a line number, then draw a detection line directly on the live view. For more precise area selection, you can click Zoom in and Draw to adjust the line in greater detail. Up to four detection lines can be configured.



Note:

Allows to set up to four lines at a time. There are three direction modes to choose for triggering alarm. "A-->B" means when there is any object crossing the line from the "A" side to the "B" side, the alarm will be triggered. "B-->A" vice versa. "A<--> B" means that the alarm will be triggered when objects cross line from either side.

Step 3:

Enable Detection.

Step 4:

Select the detection objects. An alarm will be triggered when the selected object is detected.

[General Settings]

Step 5: Set detecting sensitivity and object size limits.

Detection Settings >

General Settings ▾

Sensitivity 5

Trigger Mode General Mode ^

Object Size Filter General Mode
Bottom Mode

☒ Min. Size ☐ Max. Size

Note: Please draw on the video to set Detection Regions/Lines!

Schedule Settings >

Alarm Action >

Table 57. Description of the buttons

Parameters	Function Introduction
Sensitivity	Level 1~10 are available. The default level is 5. The higher the sensitivity, the easier it is for moving objects to be recorded in the results.
Trigger Mode	Set the desired mode of the trigger logic including General Mode and Bottom Mode. General Mode: The alarm is triggered when the object's body roughly enters the detection area. Bottom Mode: the alarm will be triggered as soon as the bottom of the object enters the detection area. Suitable for scenarios that require sensitivity to intrusion status/bottom detection preference.
Min. Size	Draw the screen to set the minimum size of the detected object. When the object is smaller than this size, it will not be detected. The default minimum size is 3*3.
Max. Size	Draw the screen to set the maximum size of the detected object. When the object is larger than this size, it will not be detected. The default maximum size is 320*240.

[Schedule Settings]**Step 6:** Set a detection schedule.

Note: This part is the same as the regular schedule settings. You can refer to [8.4.1.1 Motion Detection](#)

[Alarm Action]

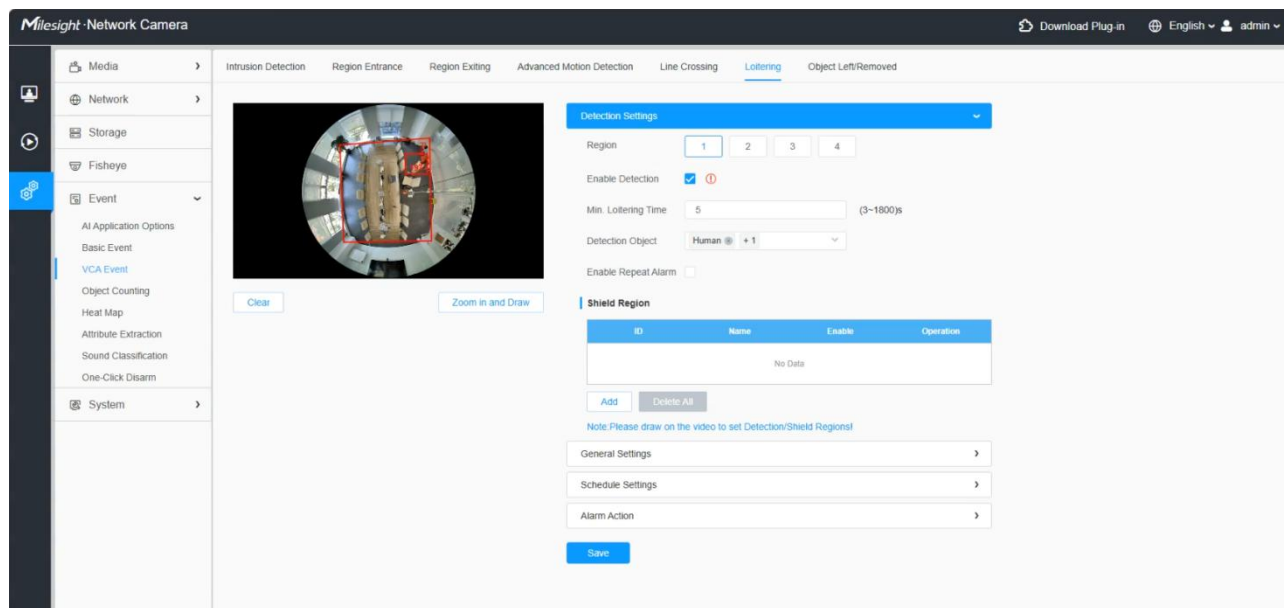
Step 7: Set an alarm action.

Note:

1. For details about Alarm Action, see [8.4.1.1 Motion Detection](#)
2. For fisheye camera models, VCA events can be linked to ePTZ auto tracking, enabling the camera to automatically track moving objects within the configured region. For more details about auto tracking, please refer to: [\[Auto Tracking\]](#).
3. If you enable External Output and choose Constant External Output Action Time, when objects cross a defined virtual line, External Output Action alarm time will be always constant till the alarm is released

8.5.2.6 Loitering

When objects are loitering in a defined area for a specific period of time, it would trigger an alarm.



Settings steps are shown as follows:

[Detection Settings]

Step 1:

Go to Settings > Event > VCA Event > Loitering.

Step 2:

Select a region number, then draw a detection region directly on the live view. For more precise area selection, you can click Zoom in and Draw to adjust the region in greater detail. Up to four detection regions can be configured.

Step 3:

Enable Detection.

Step 4:

Set Min. Loitering Time. After setting minimum loitering time from 3s to 1800s, any objects loitering in the selected area over the minimum loitering time will trigger the alarm.

Step 5:

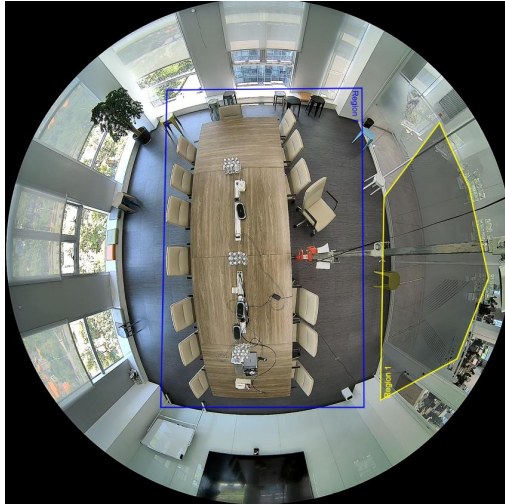
Select the detection objects. An alarm will be triggered when the selected object is detected.

Step 6:

Enable Repeat Alarm if you want the alarm to repeat. Set the Repeat Alarm Interval (3–60 seconds).

Step 7:

To exclude certain areas from detection, manually draw and add up to four Shield Regions. The method is the same as drawing detection regions. Detection regions are marked with a blue box, and shield regions with a yellow box.

**[General Settings]**

Step 8: Set object size limits.

General Settings

Trigger Mode
General Mode

Object Size Filter
General Mode
Bottom Mode

Edit

☒ Min. Size
☐ Max. Size

Note: Please draw on the video to set Detection Regions/Lines!

Schedule Settings
>

Alarm Action
>

Save

Table 58. Description of the buttons

Parameters	Function Introduction
------------	-----------------------

Trigger Mode	Set the desired mode of the trigger logic including General Mode and Bottom Mode. General Mode: The alarm is triggered when the object's body roughly enters the detection area. Bottom Mode: the alarm will be triggered as soon as the bottom of the object enters the detection area. Suitable for scenarios that require sensitivity to intrusion status/bottom detection preference.
Min. Size	Draw the screen to set the minimum size of the detected object. When the object is smaller than this size, it will not be detected. The default minimum size is 3*3.
Max. Size	Draw the screen to set the maximum size of the detected object. When the object is larger than this size, it will not be detected. The default maximum size is 320*240.

[Schedule Settings]

Step 9: Set a detection schedule.

 **Note:** This part is the same as the regular schedule settings. You can refer to [8.4.1.1 Motion Detection](#)

[Alarm Action]

Step 10: Set an alarm action.

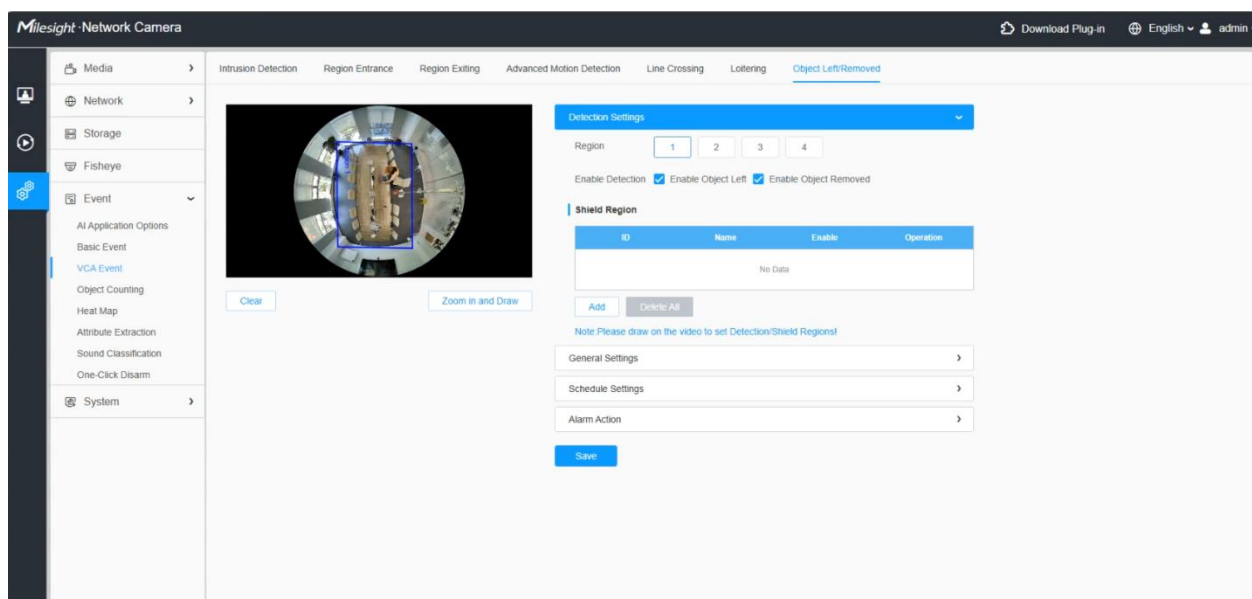
**Note:**

1. For details about Alarm Action, see [8.4.1.1 Motion Detection](#)
2. For fisheye camera models, VCA events can be linked to ePTZ auto tracking, enabling the camera to automatically track moving objects within the configured region. For more details about auto tracking, please refer to: [\[Auto Tracking\]](#).
3. If you enable External Output and choose Constant External Output Action Time, when objects loiter in the selected regions, External Output Action alarm time will be always constant till the alarm is released.

8.5.2.7 Object Left/Removed

Object Left can detect and prompt an alarm if an object is left in a pre-defined region.

Object Removed can detect and prompt an alarm if an object is removed from a pre-defined region.



Settings steps are shown as follows:

[Detection Settings]

Detection Settings

Region

1

2

3

4

Enable Detection

Enable Object Left

Enable Object Removed

Shield Region

ID	Name	Enable	Operation
No Data			

Add

Delete All

Note: Please draw on the video to set Detection/Shield Regions!

General Settings

Schedule Settings

Alarm Action

Save

Step 1:

Go to Settings > Event > VCA Event > Object Left/Removed.

Step 2:

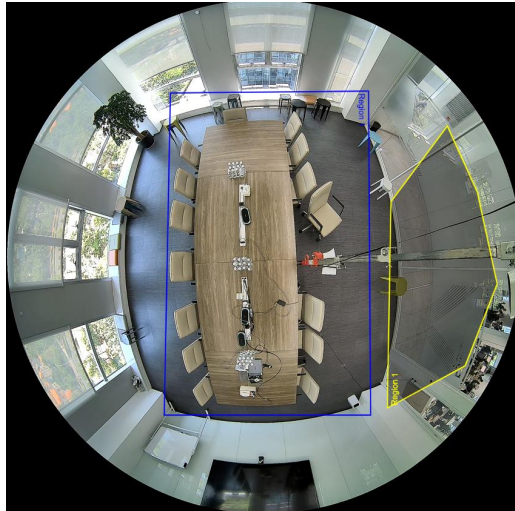
Select a region number, then draw a detection region directly on the live view. For more precise area selection, you can click Zoom in and Draw to adjust the region in greater detail. Up to four detection regions can be configured.

Step 3:

Enable Detection.

Step 4:

To exclude certain areas from detection, manually draw and add up to four Shield Regions. The method is the same as drawing detection regions. Detection regions are marked with a blue box, and shield regions with a yellow box.

**[General Settings]**

Step 5: Set Min. time, detecting sensitivity and object size limits.

Detection Settings >

General Settings v

Min. Time (5~1800)s

Sensitivity

Object Size Limits

Edit

☒ Min. Size

* Pixels (1*1~320*240)

☐ Max. Size

* Pixels (1*1~320*240)

Note: General Settings will take effect in all detection regions/lines!

Schedule Settings >

Alarm Action >

Save

Table 59. Description of the buttons

Parameters	Function Introduction
Min. Time	After setting Min. time from 5s to 1800s, any objects are left in the selected area or removed from the selected area over the minimum time will trigger the alarm.

Sensitivity	Level 1~10 are available, the default level is 5. The higher the sensitivity, the easier it is for moving objects to be recorded in the results.  Note: The sensitivity can be configured to detect various movement according to different requirements. When the level of sensitivity is low, slight movement won't trigger the alarm.
Min. Size	Draw the screen or input pixel number to set the minimum size of the detected object. When the object is smaller than this size, it will not be detected. The default minimum size is 3*3.
Max. Size	Draw the screen or input pixel number to set the maximum size of the detected object. When the object is larger than this size, it will not be detected. The default maximum size is 320*240.

[Schedule Settings]

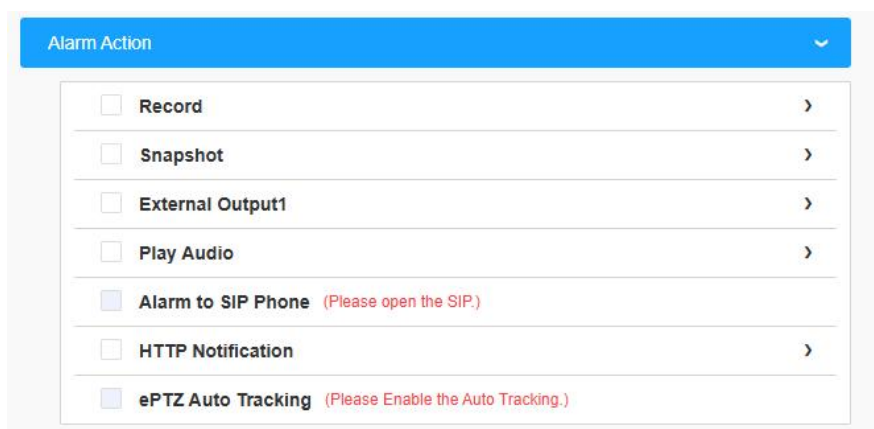
Step 6: Set a detection schedule.



 **Note:** This part is the same as the regular schedule settings. You can refer to [8.4.1.1 Motion Detection](#)

[Alarm Action]

Step 7: Set an alarm action.



 **Note:**

1. For details about Alarm Action, see [8.4.1.1 Motion Detection](#)
2. For fisheye camera models, VCA events can be linked to ePTZ auto tracking, enabling the

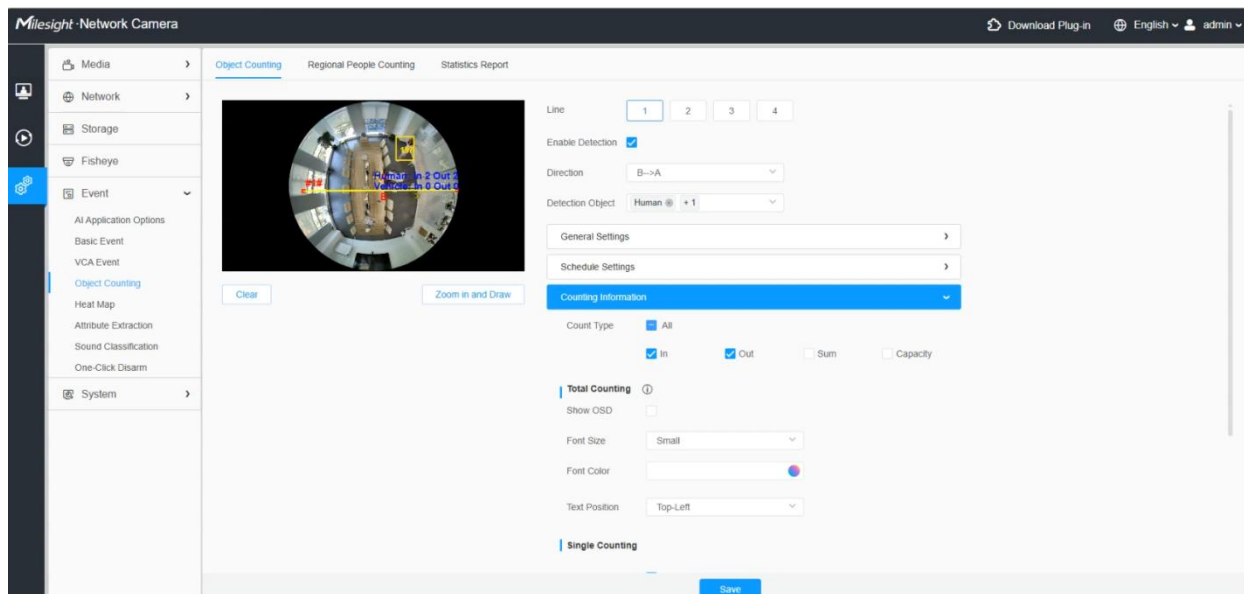
camera to automatically track moving objects within the configured region. For more details about auto tracking, please refer to: [\[Auto Tracking\]](#).

3. If you enable External Output and choose Constant External Output Action Time, when an object is left/removed from the selected regions, External Output Action alarm time will be always constant till the alarm is released.

8.5.3 Object Counting

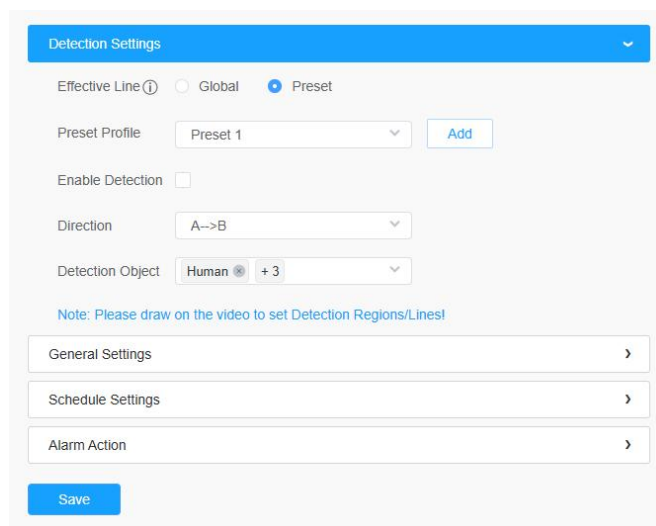
8.5.3.1 Object Counting

Object counting is able to count how many object enter or exit during the setting period.



Settings steps are shown as follows:

[Detection Settings]



Step 1:

Go to Settings > Event > AI Application Options, and enable Object Counting.

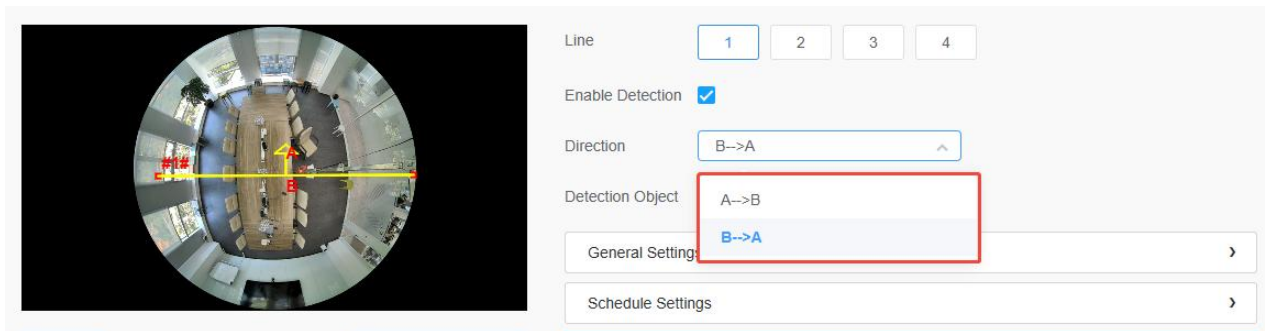
Step2:

Go to Settings > Event > VCA Event > Object Counting.

Step3: Select a region line, then draw a detection line and define its direction.

Alternatively, you can click the 'Zoom in and Draw' button to activate a full-screen

pop-up window, allowing you to draw more accurate detection lines. Up to four detection lines can be drawn.



Note:

Crossing along the direction of the arrow will record as “In”, opposite is “Out”.

Step 4:

Enable Detection.

Step 5:

Select a detection object.

[General Settings]

Step6: Set sensitivity, Trigger Mode and object size limits.

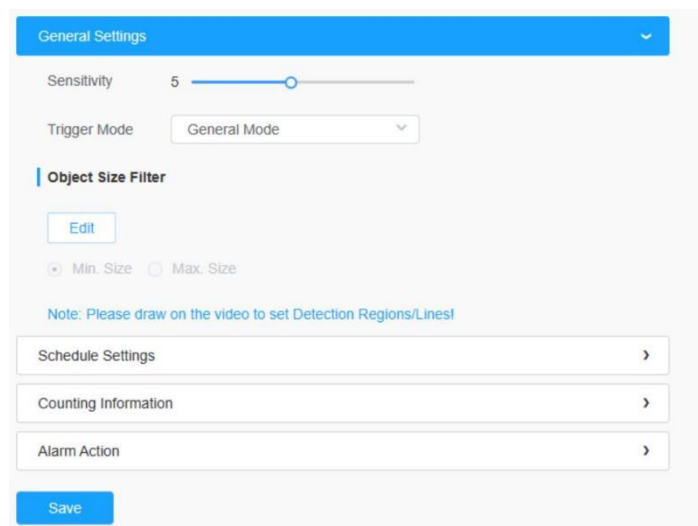


Table 60. Description of the buttons

Parameters	Function Introduction
Trigger Mode	Set the desired mode of the trigger logic including General Mode and Bottom Mode. General Mode: The alarm is triggered when the object's body roughly enters the detection area. Bottom Mode: the alarm will be triggered as soon as the bottom of the object enters the detection area. Suitable for scenarios that require sensitivity to intrusion status/bottom detection preference.
Sensitivity	Level 1~10 are available, the default level is 5. The higher the sensitivity, the easier it is for moving objects to be recorded in the results.

Min. Size	Draw the screen to set the minimum size of the detected object. When the object is smaller than this size, it will not be detected. The default minimum size is 3*3.
Max. Size	Draw the screen to set the maximum size of the detected object. When the object is larger than this size, it will not be detected. The default maximum size is 320*240.

[Schedule Settings]

Step7: Set a detection schedule.



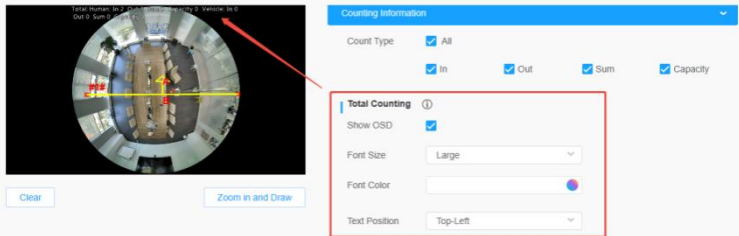
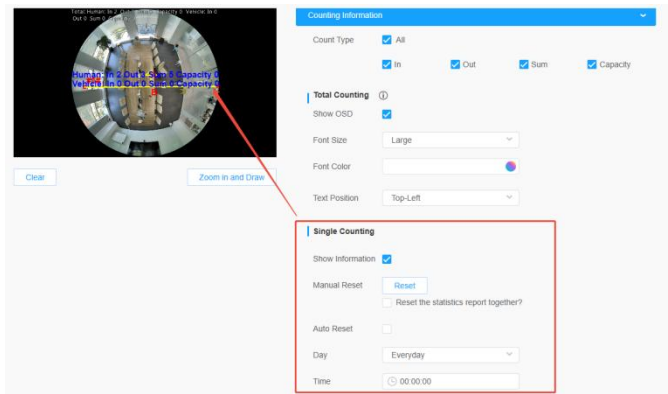
Note: This part is the same as the regular schedule settings. You can refer to [8.4.1.1 Motion Detection](#)

[Counting Information]

Step8: Set counting information.

Table 61. Description of the buttons

Parameters	Function Introduction
Count Type	Choose the information you want to display in Live Video.

Total Counting	Set counting OSD.  Note: The Total Counting OSD configuration is linked in all detection lines. Show OSD: Click to enable/disable the OSD shown. Font Size: The font size of the OSD display. Font Color: The font color of the OSD display. Text Position: The text position of the OSD display. 
Single Counting	Set Single Counting.  Note: The Total Counting OSD configuration is linked in all detection lines. Show Information: Click it to show the information.  Note: - When the detection object is set to "Human" or "Vehicle" only, the Line OSD will display "Human" or "Vehicle" accordingly to indicate the counting of these objects, Otherwise, this data will not be shown. - To hide the "Human" or "Vehicle" count in the Total OSD, you must deselect the corresponding detection object in all four lines. If at least one line has "Human" or "Vehicle" detection enabled, the Total OSD will continue to display the respective count.  Manual Reset: Reset the counting of each single line. You can choose to reset the statistics report together. Auto Reset: It is used to automatically clear the single counting information. Day: The day of Auto Reset. Time: The time of Auto Reset.

[Alarm Action]

Step9: Set alarm trigger and alarm action.

Table 62. Description of the buttons

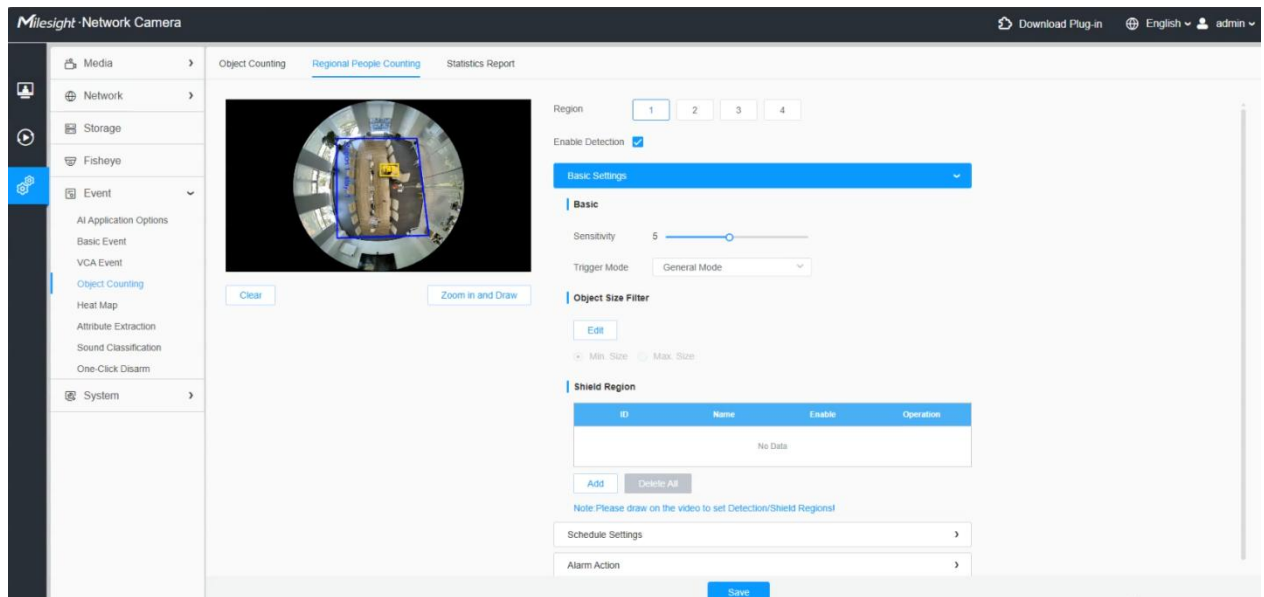
Parameters	Function Introduction
Alarm Trigger	Alarm will be triggered when the thresholds reaches to a certain value from 1 to 9999. Total Counting and Single Counting are available. You can set the Alarm Thresholds of In/Out/Capacity/Sum. Note: - For Total Counting, the thresholds are the sum of the total number of 4 detection lines. - For Single Counting, the threshold is for the selected detection line.
Alarm Action	This part is the same as the regular alarm settings. You can refer to 8.4.1.1 Motion Detection Note: - The alarm action is effective on 4 detection lines simultaneously. - If you enable External Output and choose Constant External Output Action Time, when the thresholds reach to a certain value you set, External Output Action alarm time will be always constant till the alarm is released.

8.5.3.2 Regional People Counting

When enabling Regional People Counting, users can check the real-time number of people and the time of each person's stay in the detection region.

Note:

- You can check the real-time number of people and the time of each person's stay in the detection region on Live View interface.



Settings steps are shown as follows:

[Detection Settings]

Region: 1 2 3 4

Enable Detection: ☐

Basic Settings >

Schedule Settings >

Alarm Action >

Save

Step 1:

Go to Settings > Event > AI Application Options, and enable Object Counting.

Step2:

Go to Settings > Event > VCA Event > Region People Counting.

Step 3:

Select a region number, then draw a detection region on the live view. You can also click Zoom in and Draw for more precise area selection. Up to four detection regions can be drawn.

Step 4:

Enable Detection.

[Basic Settings]

Basic Settings

Basic

Sensitivity 5

Trigger Mode General Mode

Object Size Filter

Edit

☒ Min. Size
☐ Max. Size

Note: Please draw on the video to set Detection Regions/Lines!

Schedule Settings

Alarm Action

Save

Step 5: Set sensitivity and object size limits.

Step 6:

To exclude certain areas from detection, manually draw and add up to four Shield Regions. The method is the same as drawing detection regions. Detection regions are marked with a blue box, and shield regions with a yellow box.

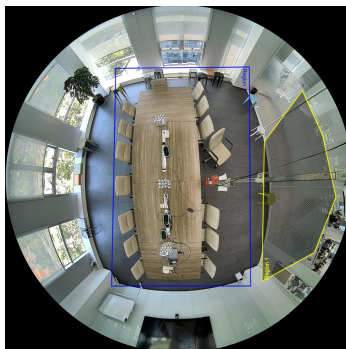


Table 63. Description of the buttons

Parameters	Function Introduction
Trigger Mode	Set the desired mode of the trigger logic including General Mode and Bottom Mode. General Mode: The alarm is triggered when the object's body roughly enters the detection area. Bottom Mode: the alarm will be triggered as soon as the bottom of the object enters the detection area. Suitable for scenarios that require sensitivity to intrusion status/bottom detection preference.
Sensitivity	Level 1~10 are available, the default level is 5. The higher the sensitivity, the easier it is for moving objects to be recorded in the results.
Min. Size	Draw the screen or input pixel number to set the minimum size of the detected object. When the object is smaller than this size, it will not be detected. The default minimum size is 3*3.
Max. Size	Draw the screen or input pixel number to set the maximum size of the detected object. When the object is larger than this size, it will not be detected. The default maximum size is 320*240.

[Schedule Settings]

Step 7: Set a detection schedule.

 **Note:** This part is the same as the regular schedule settings. You can refer to [8.4.1.1 Motion Detection](#)

[Alarm Action]

Step 8: Set alarm trigger and alarm action.

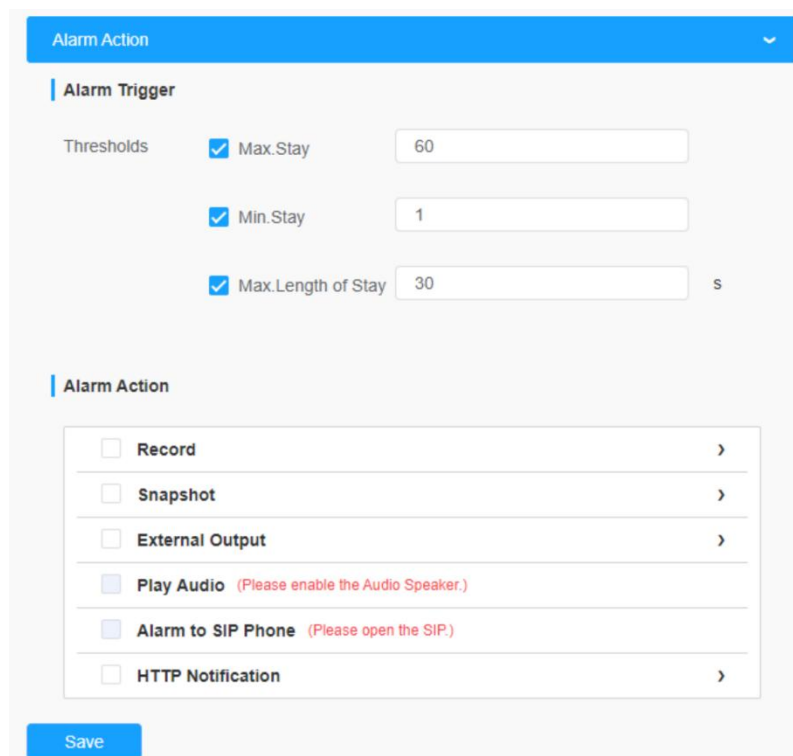
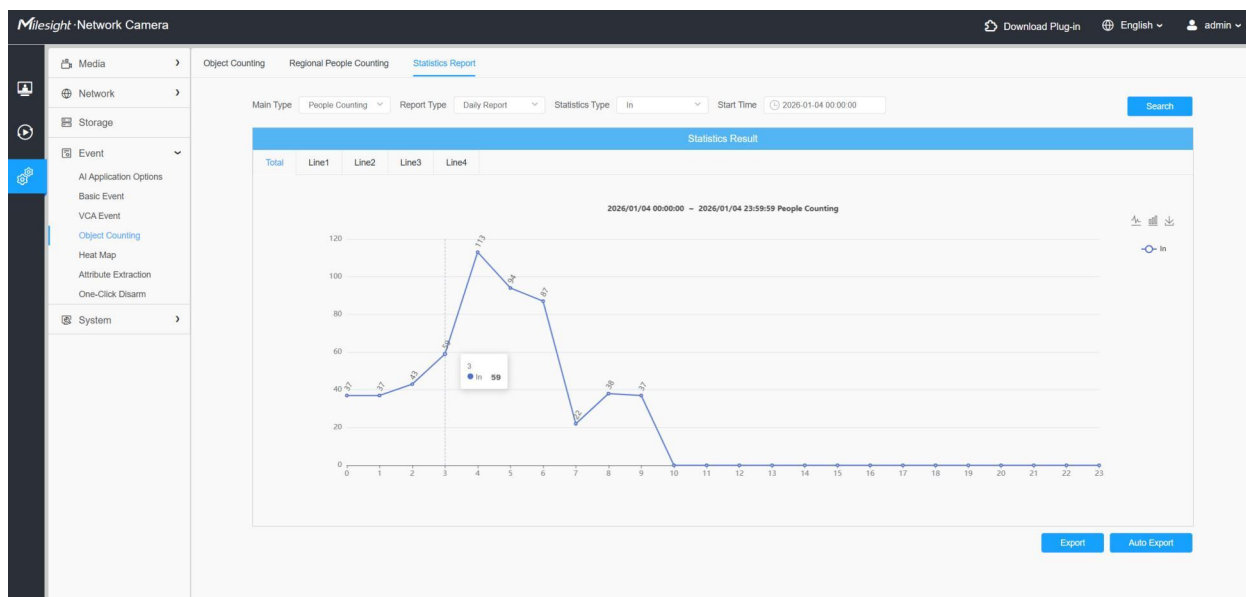


Table 64. Description of the buttons

Parameters	Function Introduction
Alarm Trigger	Alarm will be triggered when the Max./Min. Stay/Max. Length of Stay thresholds reaches to the value.  Note: The value must be in the range of 1 to 60.
Alarm Action	This part is the same as the regular alarm settings. You can refer to 8.4.1.1 Motion Detection  Note: - The alarm action is effective on 4 detection regions simultaneously. - If you enable External Output and choose Constant External Output Action Time, when the thresholds reach to a certain value you set, External Output Action alarm time will be always constant till the alarm is released.

8.5.3.3 Statistics Report

The results during the enabling period will be displayed on “Statistics Report” interface.



Step 1: Select Main Type.

Step2: Select Report Type including Daily Report, Weekly Report, Monthly Report and Annual Report.

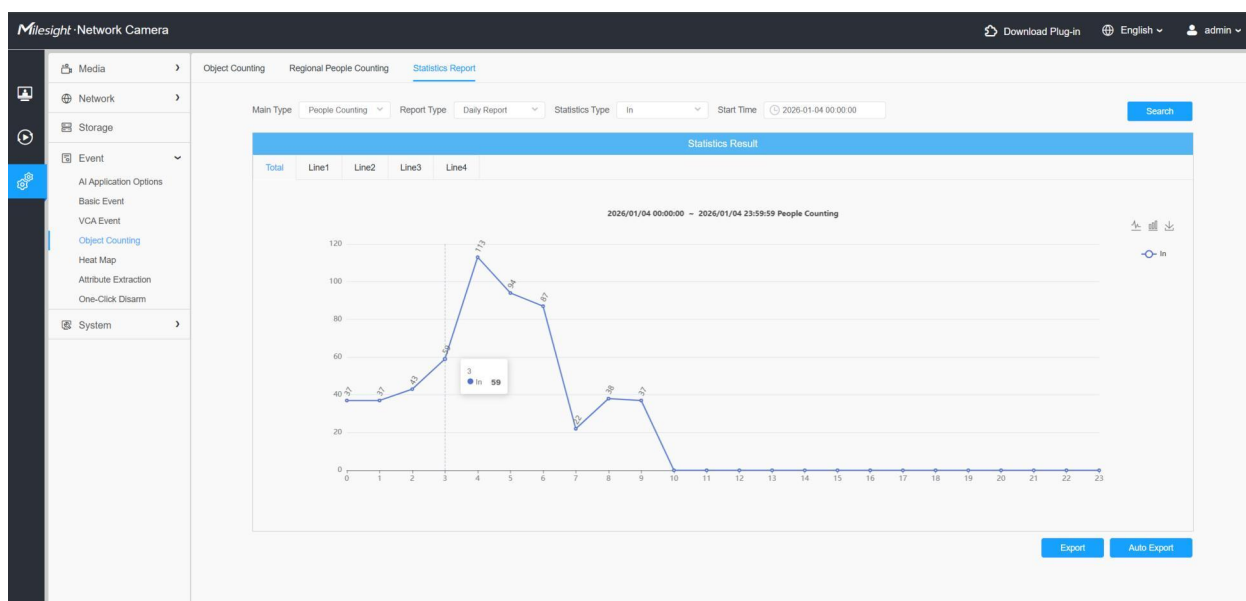
Step3: For people counting and vehicle counting, select Statistics Type including In, Out and Sum. For regional people counting, select Length of Stay including All, More Than and Less Than and set the time of more then/less then.

Note: For regional people counting, check the check box to search the report of regions as needed.

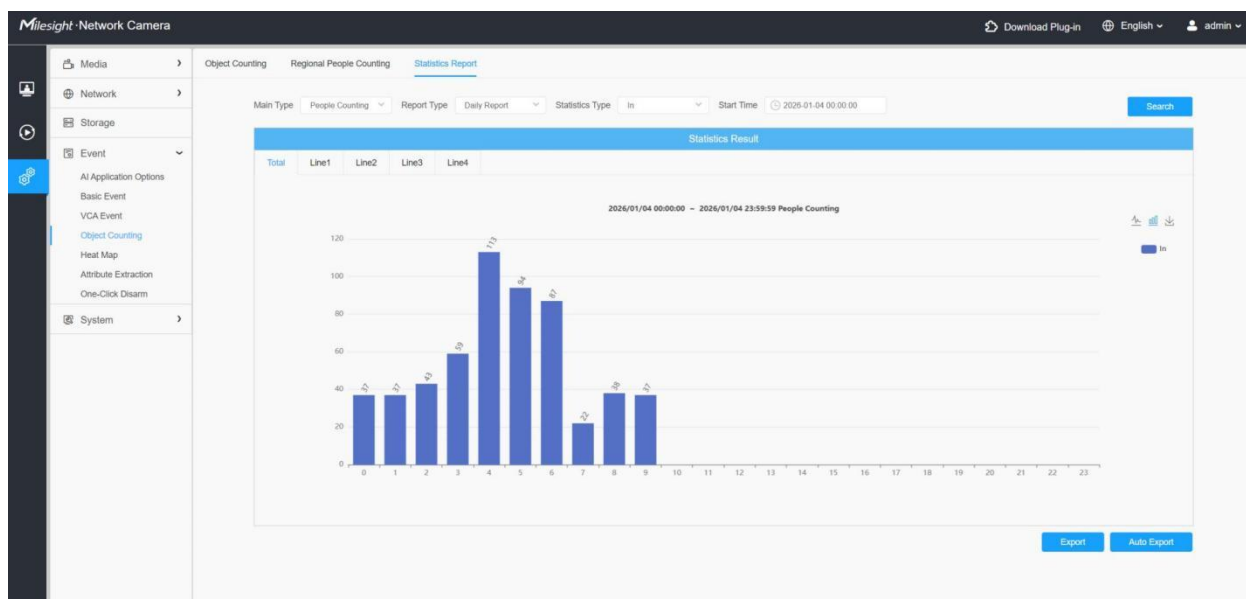
Step4: Select Start Time, then click "Search" button, the camera will automatically count the data for the day/ week/ month/ year (based on the report type selected by the user) from the start time and generate the corresponding report.

Step5: Moreover, you can also click "Line Chart" or "Bar Chart" to switch display mode of Statistics Report as shown below.

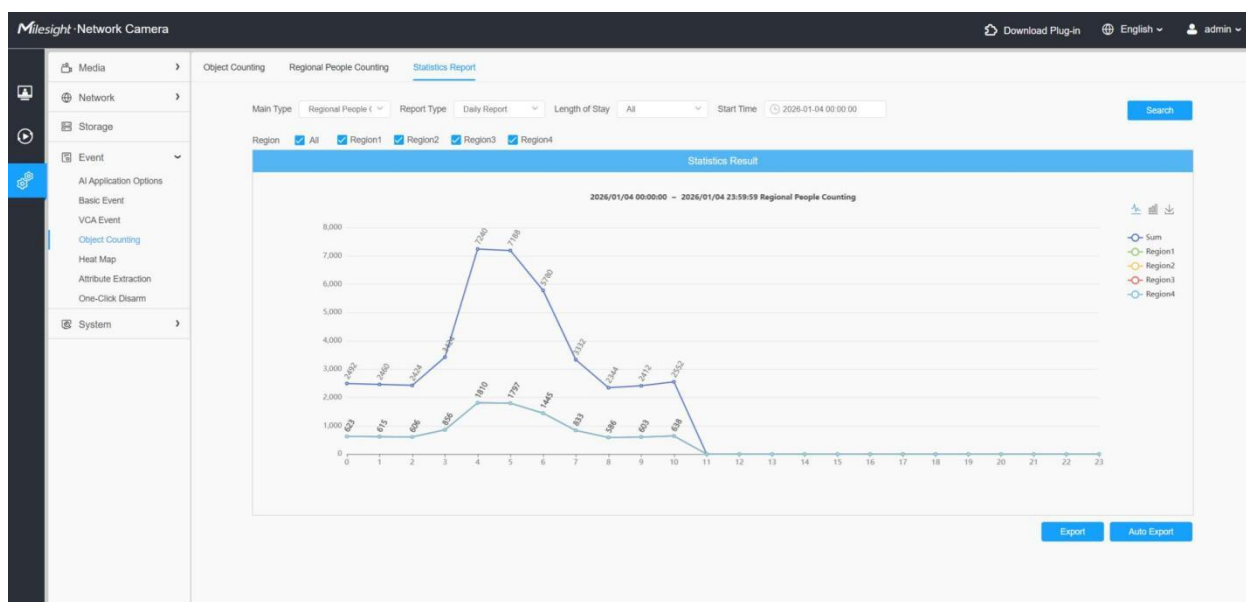
People Counting-Statistics Report (Line Chart)



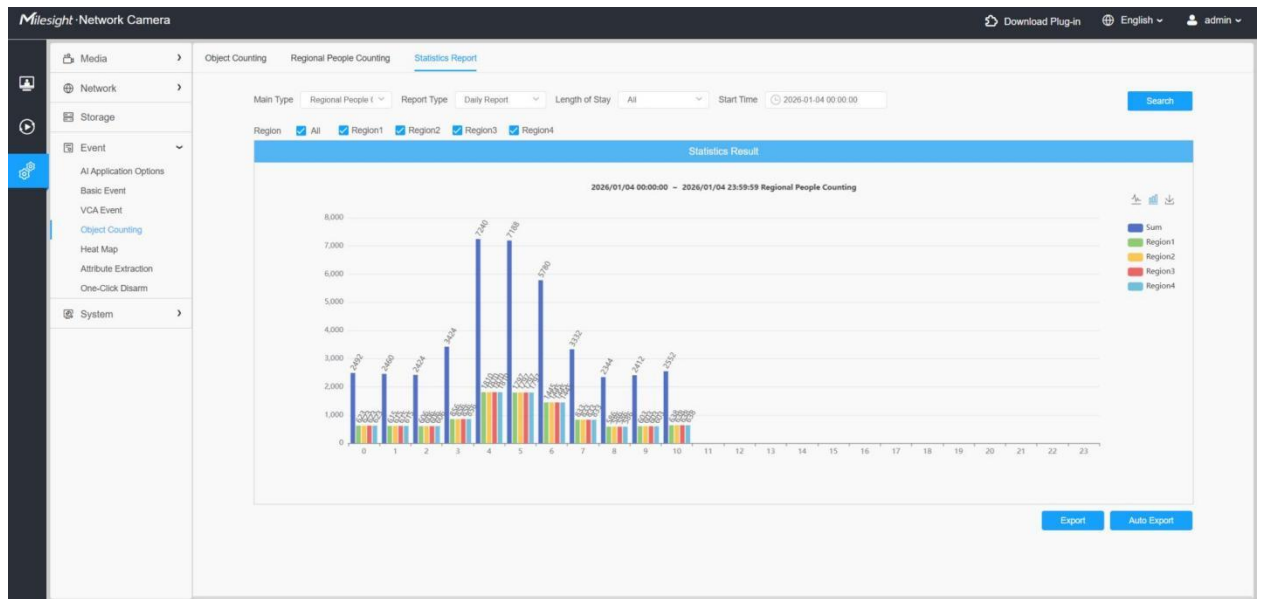
People Counting-Statistics Report (Bar Chart)



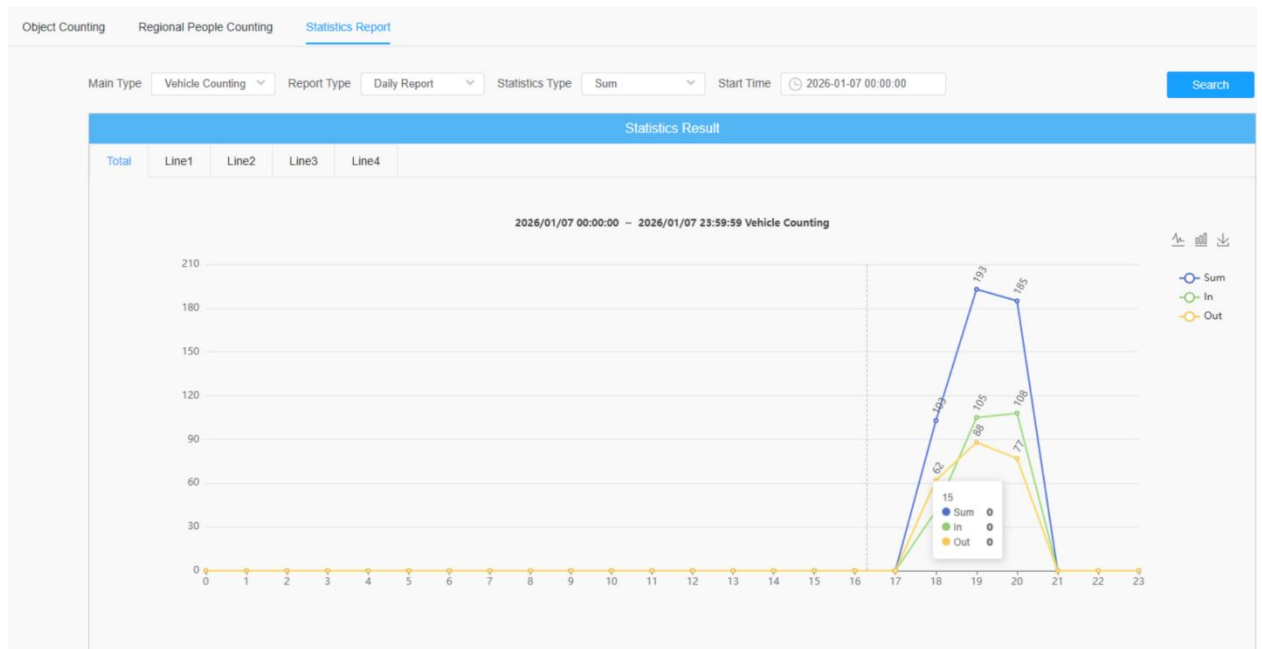
Regional People Counting-Statistics Report (Line Chart)



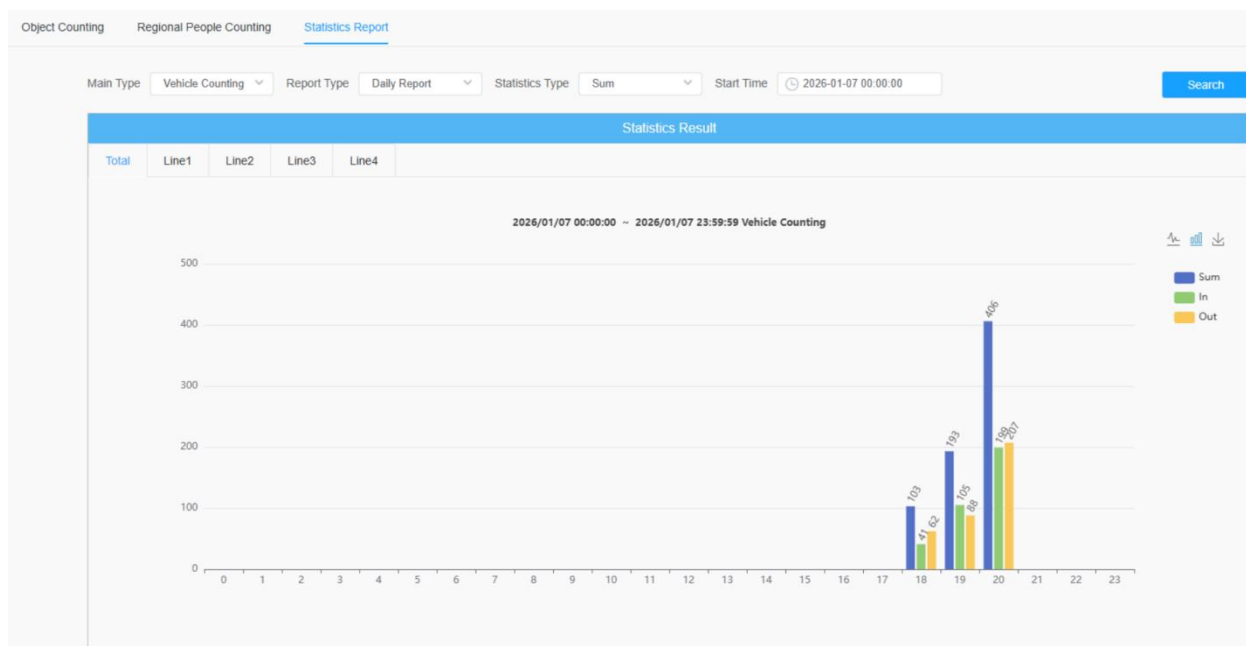
Regional People Counting-Statistics Report (Bar Chart)



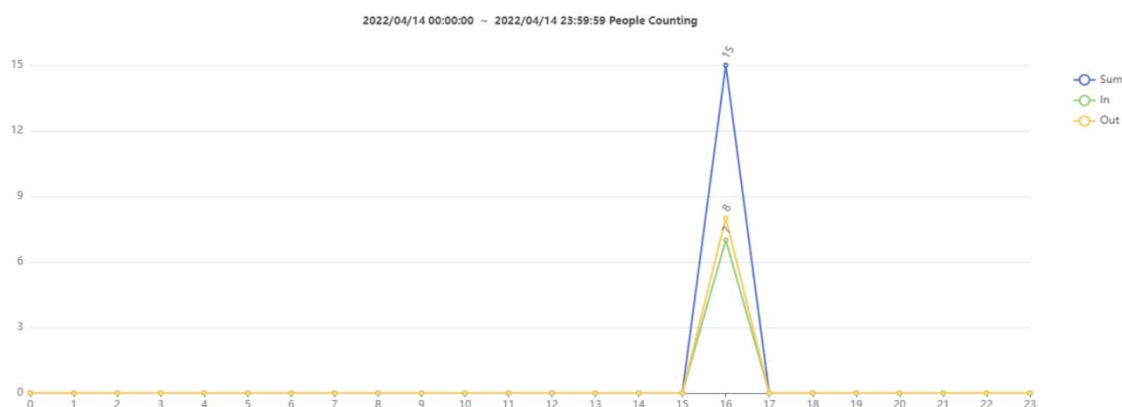
Vehicle Counting-Statistics Report (Line Char)



Vehicle Counting-Statistics Report (Bar Chart)



Step6: Click the Download button to download the screenshot of the statistical report chart.



Step7: Click "Export" button to pop up the Export window as shown below, and you can choose File Format to export the report to local. For people counting Statistics Report, you can check the check box to export the report of different lines as needed.

People Counting-Export, Vehicle Counting-Export

Export

File Format ☐ CSV

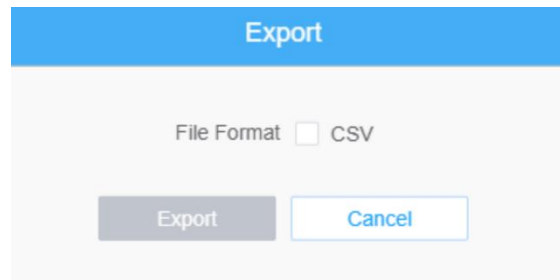
Line ☒ All

☒ Total ☒ Line1 ☒ Line2

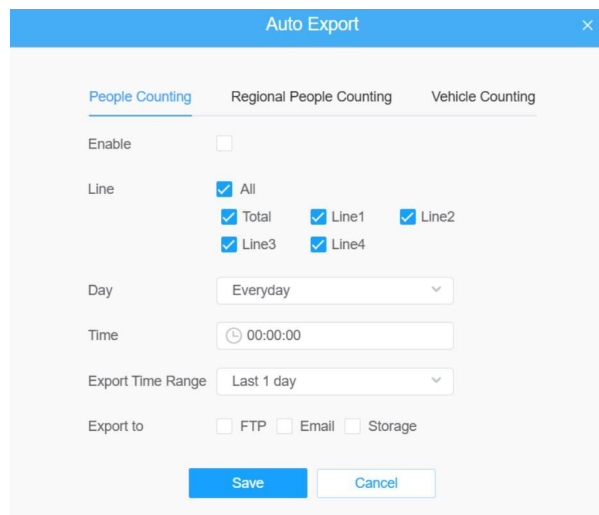
☒ Line3 ☒ Line4

Export Cancel

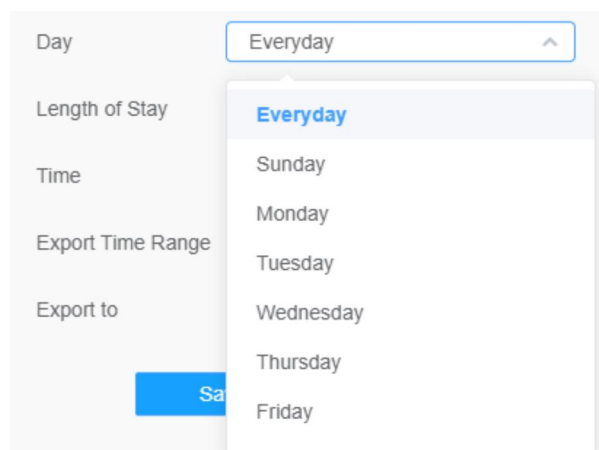
Regional People Counting-Export



Step8: Click "Auto Export" button to pop up the Statistics Report Settings as shown below. People Counting-Auto Export



- Check the check box to enable the auto export of people counting, then select the lines as needed.
- Set Day. User can choose Everyday to export daily reports, while choosing others to export reports on a specific day of the week;



- Set Time. User can choose the time of day to export the Statistics Report automatically, click the calendar icon to pop up the following Quick Selection;

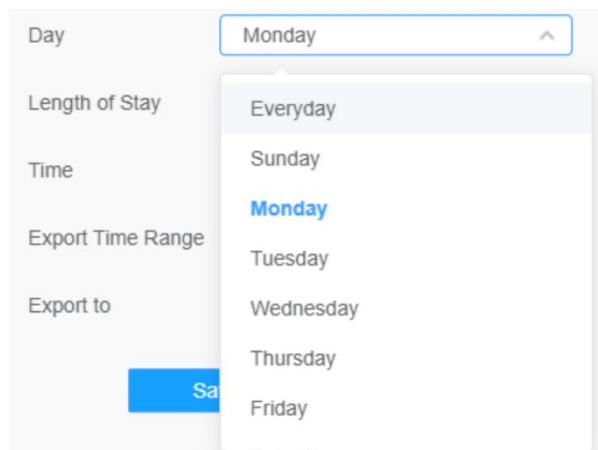
- Set Export Time Range;

- Set the destination path of the automatically exported report. The report can be exported to FTP/Email/Storage automatically as the form of an Excel spreadsheet according to the day, time and export time range you set. Then click “Save”.

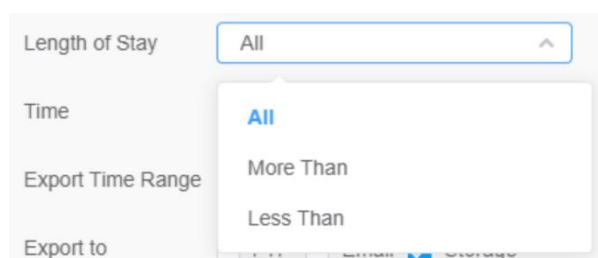
Note: If the current Statistics Report is generated, it will be saved as a csv form.

Regional People Counting-Auto Export

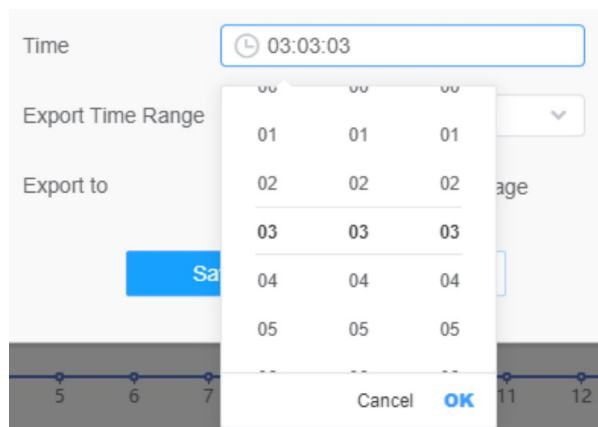
- Check the check box to enable the auto export of regional people counting.
- Set Day. User can choose Everyday to export daily reports, while choosing others to export reports on a specific day of the week;



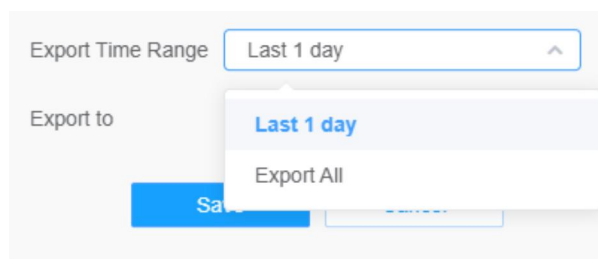
- Set Length of Stay.



- Set Time. User can choose the time of day to export the Statistics Report automatically, click the calendar icon to pop up the following Quick Selection;



- Set Export Time Range;



- Set the destination path of the automatically exported report. The report can be exported to FTP/Email/Storage automatically as the form of an Excel spreadsheet according to the day, time and export time range you set. Then click “Save”.

Export to ☐ FTP ☐ Email ☒ Storage

[Save](#) [Cancel](#)

 **Note:** If the current Statistics Report is generated, it will be saved as a csv form.

Vehicle Counting-Auto Export

Auto Export ×

People Counting Regional People Counting Vehicle Counting

Enable ☐

Line ☒ All ☒ Total ☒ Line1 ☒ Line2 ☒ Line3 ☒ Line4

Day

Time

Export Time Range

Export to ☐ FTP ☐ Email ☐ Storage

[Save](#) [Cancel](#)

- Check the check box to enable the auto export of people counting, then select the lines as needed.
- Set Day. User can choose Everyday to export daily reports, while choosing others to export reports on a specific day of the week;

Day

Length of Stay

Time

Export Time Range

Export to

[Save](#)

Everyday

Sunday

Monday

Tuesday

Wednesday

Thursday

Friday

- Set Time. User can choose the time of day to export the Statistics Report automatically, click the calendar icon to pop up the following Quick Selection;

- Set Export Time Range.

- Set the destination path of the automatically exported report. The report can be exported to FTP/Email/Storage automatically as the form of an Excel spreadsheet according to the day, time and export time range you set. Then click “Save”.

8.5.4 Heat Map

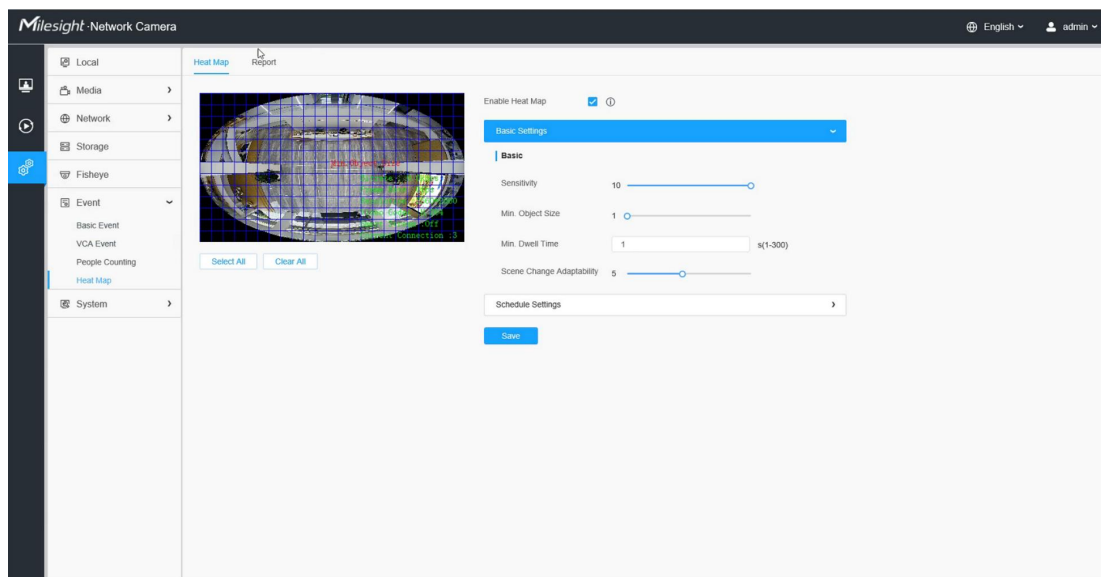
Heat Map function can analyze customers movement to reveal insights for better business management with the intuitive and accurate statistical analysis results in time or space pattern as needed.

8.5.4.1 Heat Map



Note:

- Only allowed to view reports within one days without a SD card or NAS.
- For more details about how to set Heat Map, please refer to <https://milesight.freshdesk.com/a/solutions/articles/69000643314>.



Step1: Enable Heat Map function.

[Basic Settings]

Enable Heat Map ☐

Basic Settings

Basic

Sensitivity 5

Min. Object Size 10

Min. Dwell Time 30 s(1-300)

Scene Change Adaptability 5

Schedule Settings

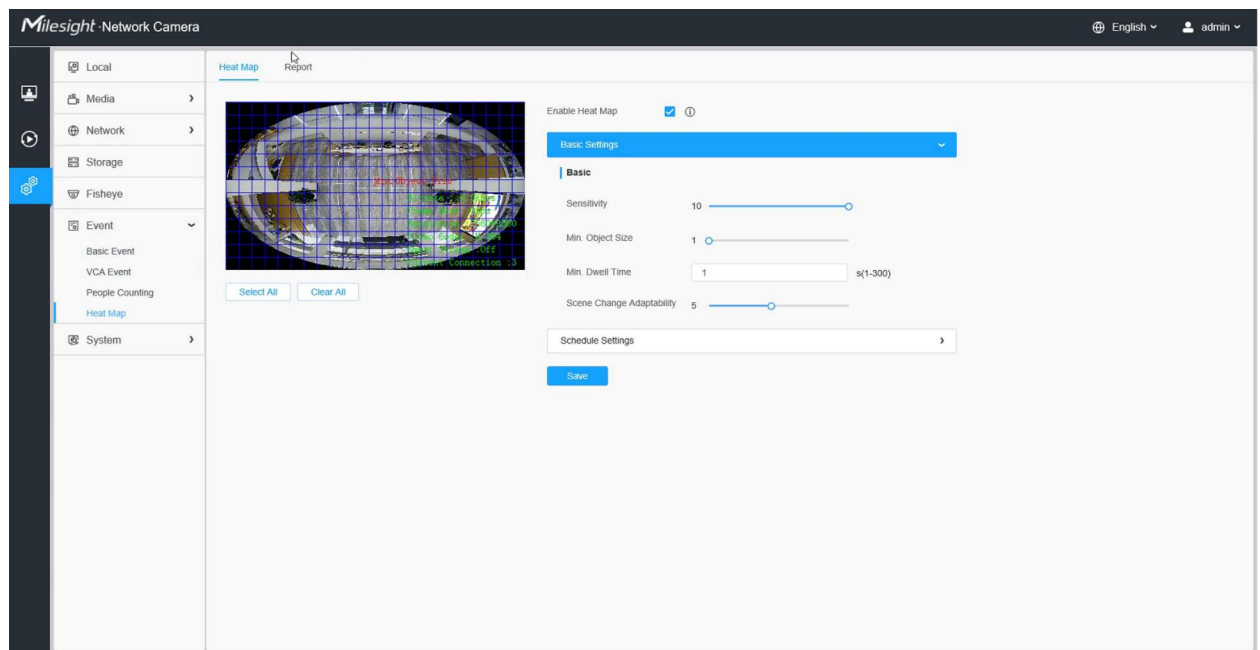
Save

Table 65. Description of the buttons

Parameters	Function Introduction
Sensitivity	Level 1~10 are available, the default level is 5. The higher the sensitivity, the easier it is for moving objects to be recorded in the results.
Min. Object Size	Set the minimum object size from 1 to 100, the default value is 10. Objects smaller than this value will not be recorded in the result.

Min. Dwell Time	Set the minimum dwell time from 1 to 300, the default value is 30. If the object stays in the area longer than the set "Minimum Dwell Time", it will not be recorded in the result.
Scene Change Adaptability	Level 1~10 are available, the default level is 5. Scene Change Adaptability indicates the camera's adaptability to scene changes, which can increase the accuracy of detection. The camera better adapts to faster changing scenes if the value is higher.

Step2: Set Heat Map Region. Draw the screen to set the detection area. You can click "Select All" button to select all areas, or "Clear All" button to remove the current drawn area.



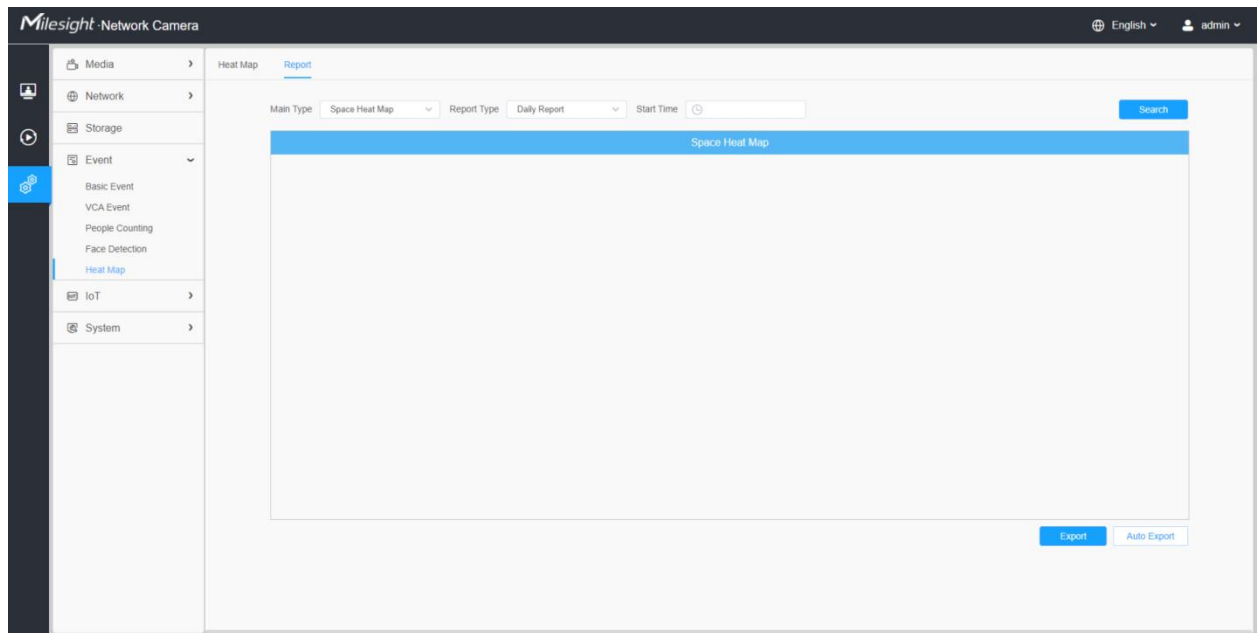
[Schedule Settings]

Step3: Schedule Settings.

 **Note:** This part is the same as the regular schedule settings. You can refer to [8.5.1.1 Motion Detection](#)

8.5.4.2 Report

The heat map results will be displayed on this interface.



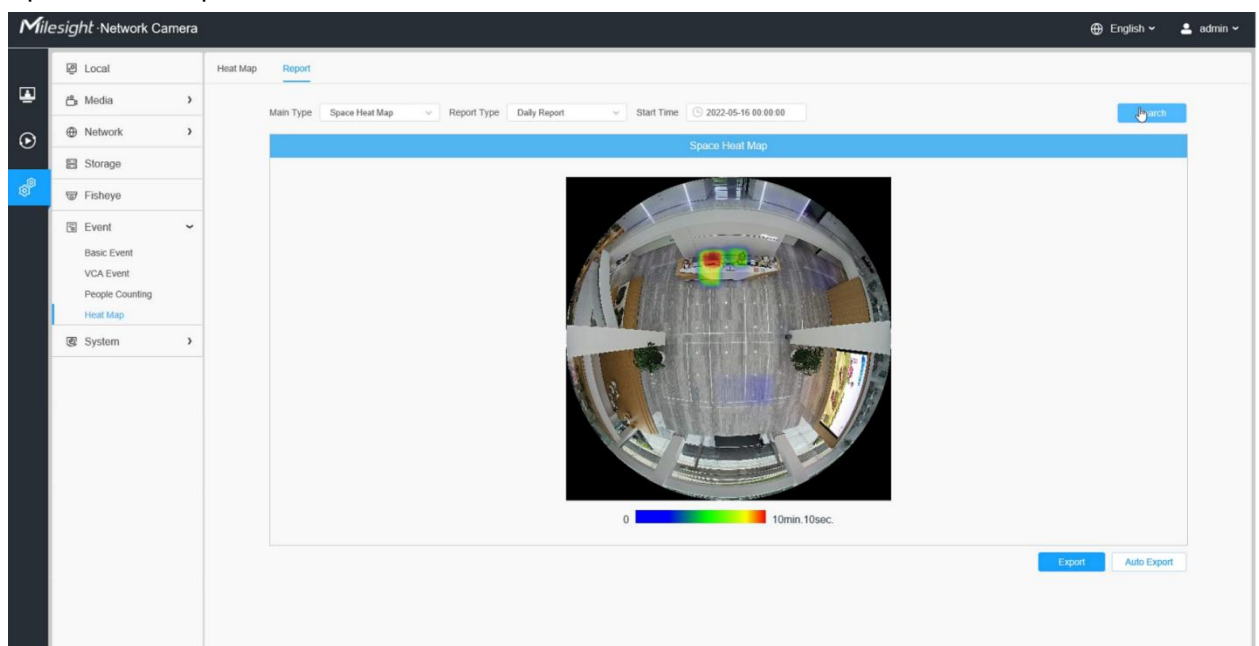
Step1: Select Main Heat Map Type.

- [Space Heat Map]: Space Heat Map will be presented as a picture with different colors. Different colors represent different heat values. Red represents the highest and blue represents the lowest.
- [Time Heat Map]: Time heat map will be presented as a line chart to show the heat at different times.

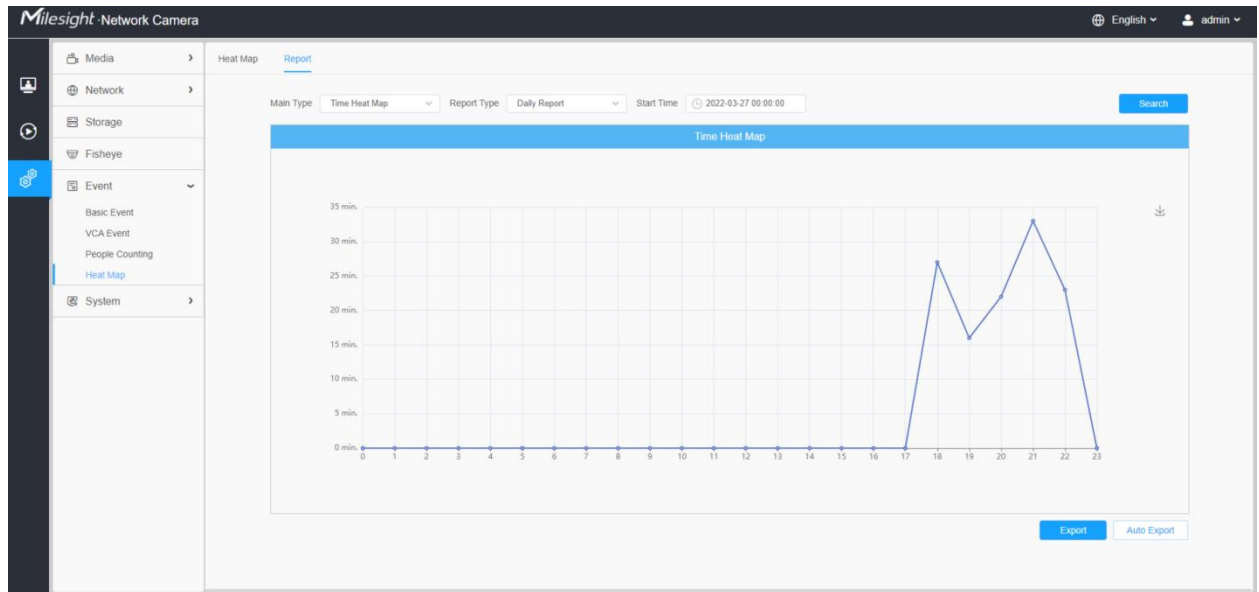
Step2: Select Report Type including Daily Report, Weekly Report, Monthly Report and Annual Report.

Step3: Select Start Time, then click the "Search" button, the camera will automatically count the data for the day/ week/ month/ year (based on the report type selected by the user) from the start time and generate the corresponding report as shown below.

Space Heat Map



Time Heat Map



Step4: Click the "Report Export" button to export the report to local.

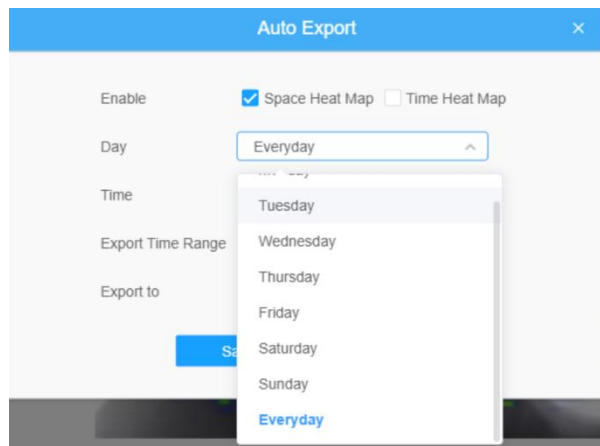
Step5: Click the "Auto Export" button to pop up the Heat Map Report Settings as shown below.

The 'Auto Export' dialog box is shown with a blue header and a close button. It contains the following settings:

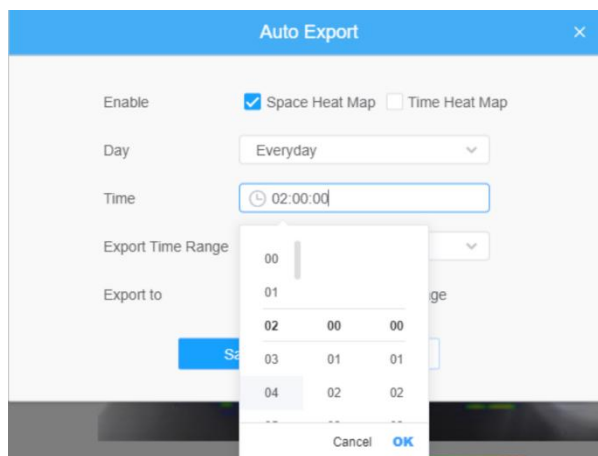
- Enable:** Two checkboxes, 'Space Heat Map' and 'Time Heat Map', both of which are currently unchecked.
- Day:** A dropdown menu set to 'Everyday'.
- Time:** A time picker set to '00:00:00'.
- Export Time Range:** A dropdown menu set to 'Last 1 day'.
- Export to:** Three checkboxes, 'FTP', 'Email', and 'Storage', all of which are currently unchecked.

At the bottom of the dialog are 'Save' and 'Cancel' buttons.

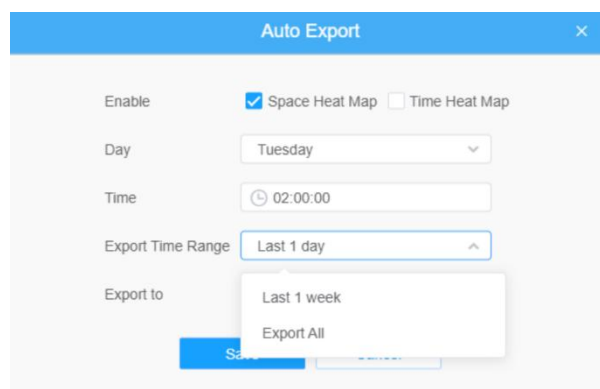
- Set Export Type. User can check Space Heat Map or Time Heat Map or both. When either Space Heat Map or Time Heat Map is checked, the gray item becomes editable as shown below;
- Set Day. User can choose Everyday to export daily reports, while choosing others to export reports on a specific day of the week;



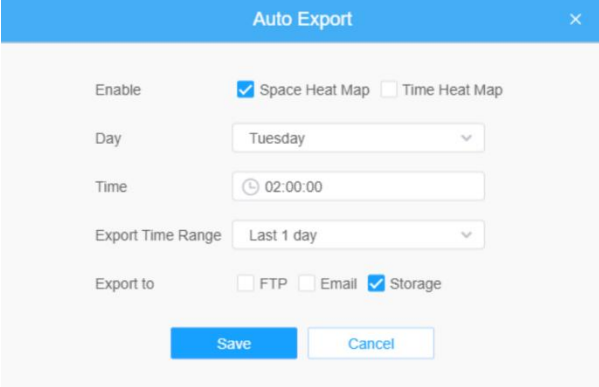
- Set Time. User can choose the time of day to export the heat map automatically, click the calendar icon to pop up the following Quick Selection;



- Set Export Time Range.



- Set the destination path of the automatically exported report. The report can be exported to FTP/ Email/Storage automatically as the form of an Excel spreadsheet or a picture according to the day, time and export time range you set. Then click “Save”.



The 'Auto Export' dialog box is shown with the following settings:

- Enable:** ☒ Space Heat Map, ☐ Time Heat Map
- Day:** Tuesday
- Time:** 02:00:00
- Export Time Range:** Last 1 day
- Export to:** ☐ FTP, ☐ Email, ☒ Storage

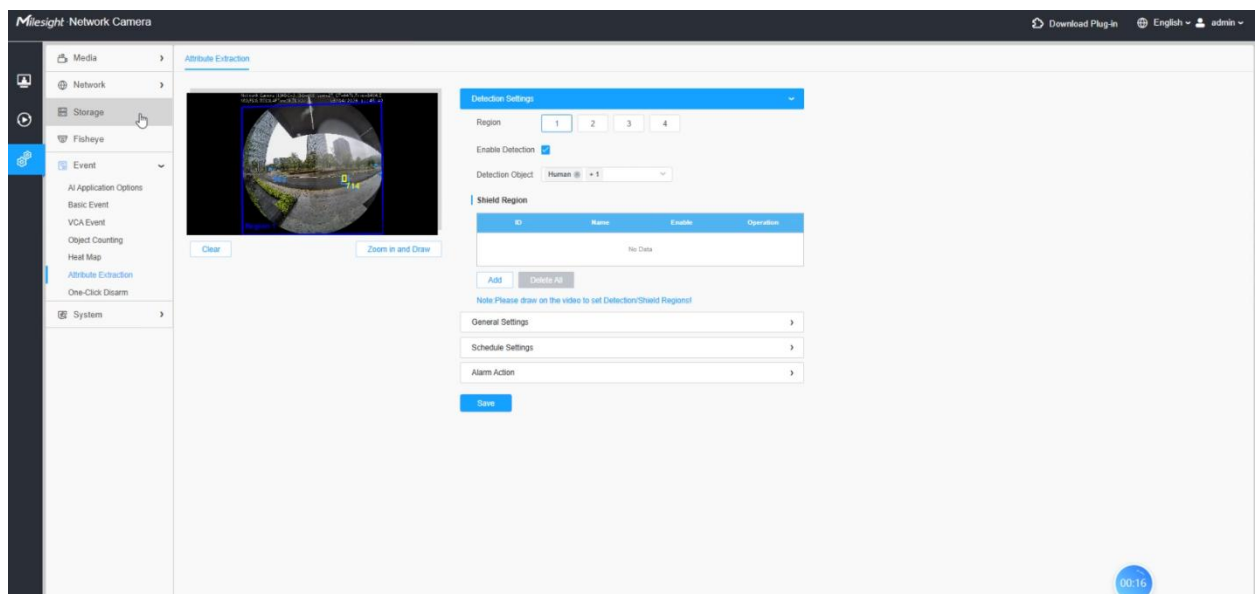
Buttons: Save, Cancel

If the current Space Heat Map is generated, it will be saved as a png image. If the current Time Heat Map is generated, it will be saved as a csv form.

8.5.5 Attribute Extraction

Milesight's camera features intelligent AI-powered Attribute Recognition technology, enabling real-time and accurate differentiation between humans and vehicles. The system analyzes multiple attributes—such as upper and lower body clothing colors (black, white, gray, red, yellow, green, blue, purple, orange, and brown), hats, vehicle types (Bicycle, Motorcycle, E-scooter, Car, Bus, Truck) and colors (black, white, gray, red, yellow, green, blue, purple, and brown for Car, Bus, Truck), and more—to enhance target identification.

This advanced recognition capability significantly improves security efficiency across a wide range of surveillance scenarios.



[Detection Settings]

Step 1: Go to Settings > Event > AI Application Options, enable Attribute Extraction.

Step 2:

Select a region number, then draw a detection region on the live view. You can also click Zoom in and Draw for more precise area selection. Up to four detection regions can be drawn.

Step 3:

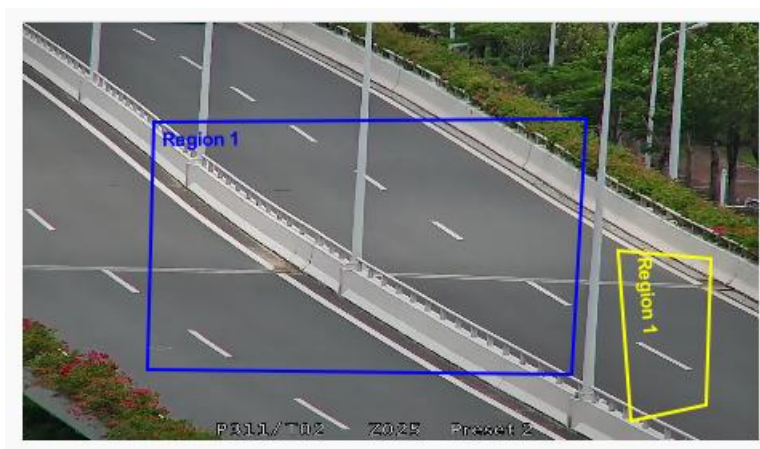
Enable Detection.

Step 4:

Select the detection object(s): Human or Vehicle. An alarm will be triggered when the selected object is detected.

Step 5:

To exclude certain areas from detection, manually draw and add up to four Shield Regions. The method is the same as drawing detection regions. Detection regions are marked with a blue box, and shield regions with a yellow box.



[General Settings]

Step 6: Set detecting object size limits, and select the detection mode with Optimal

Mode, Quick Mode or Real-Time Mode.

Table 66. Description of the buttons

Parameters	Function Introduction
Detection Mode	Optimal Mode, Quick Mode, Real-Time Mode are available, Optimal Mode: In this mode, it will push the most accurate attribute analysis result when the target stays longer than the "Optimal Duration" or leaves the detection area. Quick Mode: In this mode, it will push attribute analysis results once the target's confidence level exceeds the "Quality Threshold". The same target will only be pushed once within the same area. Real-Time Mode: In this mode, it will continuously push attribute analysis results with higher accuracy in real time. If a target's confidence level increases in a later detection, the camera will push the updated data. For the same target within the same area, multiple data entries may be sent.
Optimal Duration	This setting is only applicable in Optimal Mode. It defines the optimal dwell time starting from when the target enters the detection area.
Quality Threshold	Levels from 1 to 100 are available for both human and vehicle detection, with the default set to 50. If the target's confidence level is below the set "Quality Threshold", attribute detection will not be performed.
Min. Size	Draw on the screen to set the minimum size of the detected object. Objects larger than this size will be detected.
Max. Size	Draw the screen to set the maximum size of the detected object. When the object is larger than this size, it will not be detected.

[Schedule Settings]

Step 7: Set a detection schedule.

 **Note:** This part is the same as the regular schedule settings. You can refer to [8.4.1.1 Motion Detection](#)

Detection Settings

General Settings

Schedule Settings

0 2 4 6 8 10 12 14 16 18 20 22 24

Sun.

Mon.

Tue.

Wed.

Thu.

Fri.

Sat.

Select All Clear All

Alarm Action

Save

[Alarm Action]

Step 8: Set an alarm action.

HTTP Notification: Support to send alarm notifications to specified HTTP URL. After filling in the basic information, you can click the test button to verify HTTP connectivity.

Detection Settings

General Settings

Schedule Settings

Alarm Action

☐ HTTP Notification

URL 1 2 3

https://abc.com Test

Enable ☐

Trigger Interval 0 (0-900) s

HTTP Method Get

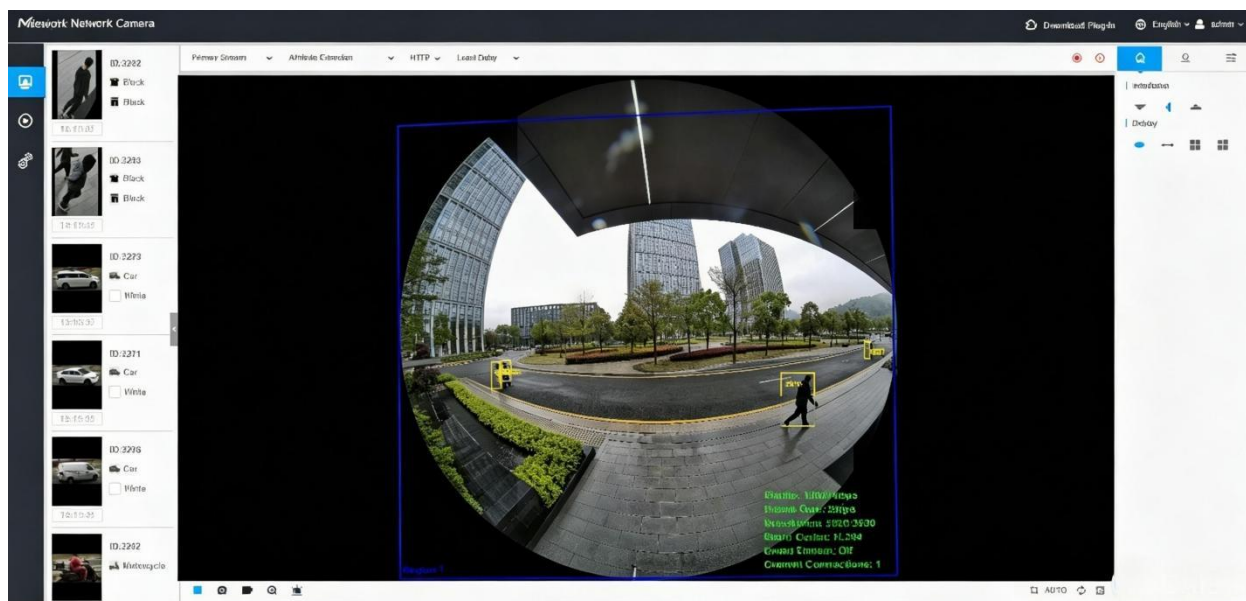
User Name

Password

Save

When Attribute Extraction is enabled, the attributes of detected humans or vehicles are displayed on the left side of the Live View interface. These attributes include upper and lower clothing color, presence of a hat, vehicle type, and more. This feature is particularly useful in specialized scenarios, making it easier to locate specific individuals or vehicles.

The extracted data can also be seamlessly transferred to a back-end system for centralized management, significantly enhancing overall user experience and operational efficiency.



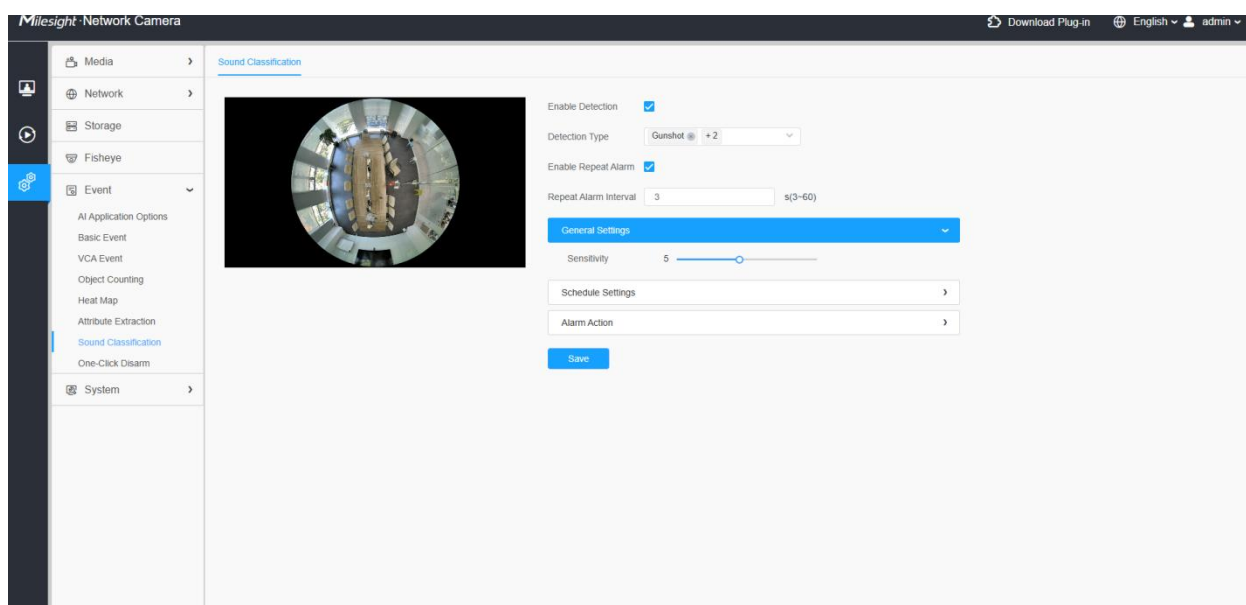
8.5.6 Sound Classification

Sound Classification supports instant detection of gunshots, glass breaking, and screaming sounds. If screaming, gunshots, or glass breaking are detected, an alarm will be triggered immediately.



Note:

For more details about how to use Sound Classification, see <https://youtu.be/gpMI-egXiOg>.



You can configure the function according to the following steps:

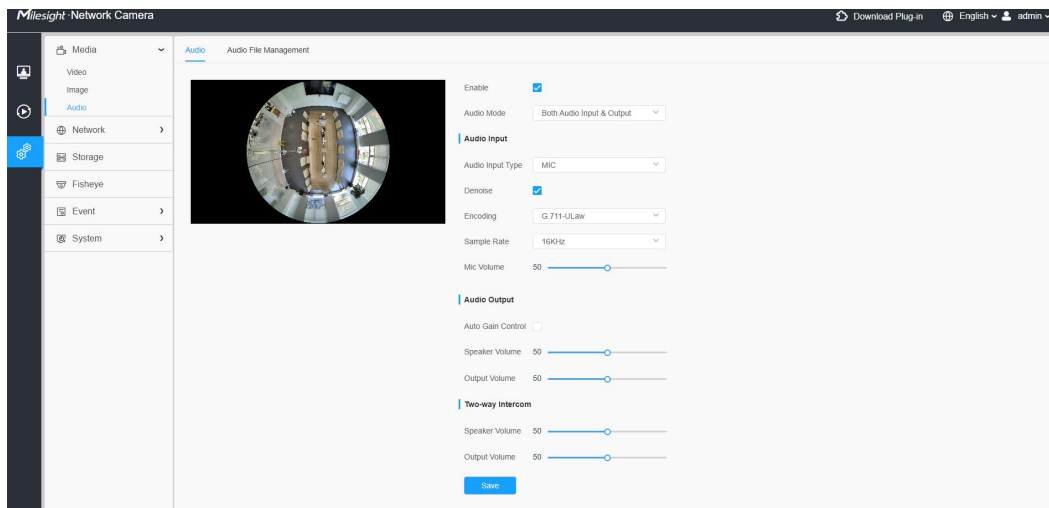
[Enable Detection]

Step1: Choose Settings > Event > AI Application Options > Sound Classification.

Step2: Check the checkbox to enable the function.



Note: Before enabling the function, choose Settings > Media > Audio > Enable to enable the Audio Mic first. For details about Audio, see [8.1.3 Audio](#).



Step3: Select a detection type. Gunshot, Glassbreak, and Screaming are available.

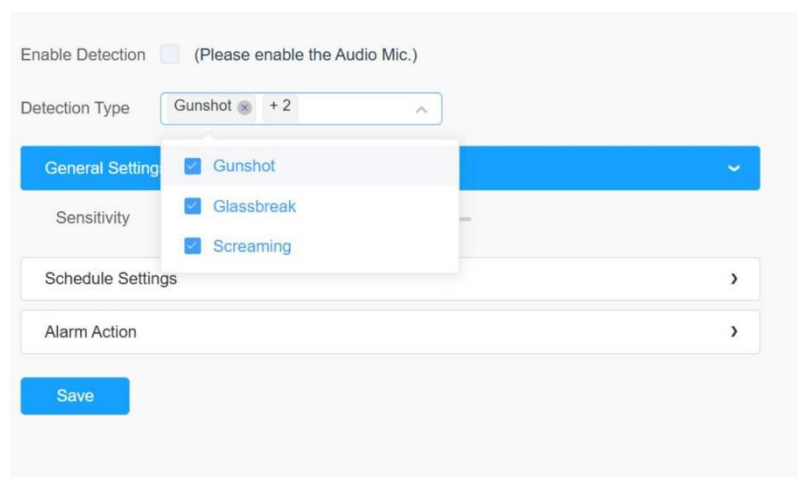


Table 67. Parameter Description

Parameter	Function Introduction
Enable Detection	Check the check-box to enable this function.
Detection Type	Select a detection type. Gunshot, Glassbreak, and Screaming are supported.
Enable Repeat Alarm	Check this checkbox to enable repeat alarms.
Repeat Alarm Interval	Enter the repeat interval from 3 to 60.

[General Settings]

Step4: Configure the sensitivity from 1 to 10. The default value is 5.

Enable Detection ☒

Detection Type Gunshot +2

General Settings

Sensitivity 5

Schedule Settings

Alarm Action

Save

[Schedule Settings]

Step5: Set a detection schedule.

 **Note:** For more details, see [Motion Detection \(page 96\)](#).

Enable Detection ☒

Detection Type Gunshot +2

General Settings

Schedule Settings

0 2 4 6 8 10 12 14 16 18 20 22 24

Sun.

Mon.

Tue.

Wed.

Thu.

Fri.

Sat.

Select All Clear All

Alarm Action

Save

[Alarm Action]

Step6: Set an alarm action.

 **Note:** For more details, see [8.5.1.1 Motion Detection](#)

General Settings

Schedule Settings

Alarm Action

☐ Record

Duration 5 s

Linkage

☐ Save to Storage (Please mount storage device.)

☐ Upload via FTP (Please enable the FTP.)

☐ Send Email ⓘ (Please enable the Email.)

Email Triggered Interval 30 s

☐ Snapshot

☐ External Output

☐ Play Audio

☐ Alarm to SIP Phone (Please open the SIP.)

☐ HTTP Notification

Save

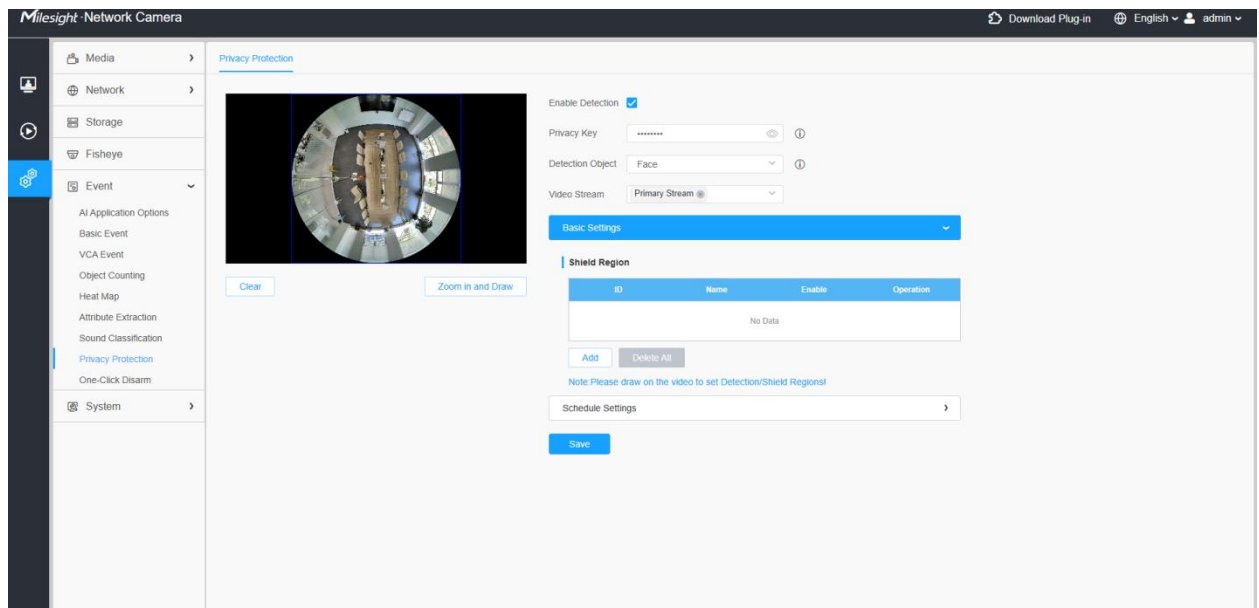
Step7: Click Save to save your configurations. When the camera detects gunshots, glass breaking, or screaming, an alarm icon  will appear in the upper right corner of the live view interface.

8.5.7 Privacy Protection

Privacy Protection masks detected faces or bodies in video streams. It supports the primary stream and the secondary stream. It supports H.265 and H.264 encoding and is GDPR compliant.

 Note:

1. This feature is only available in the original view (10 mode).
2. You can remove mosaics via Smart Tools. Download Smart Tools, and choose **IPC Tools > Others**. Select a video file path and enter a private key. Then, click **Demosaic** to remove the mosaics.
2. If Privacy Protection is enabled, the frame rate cannot exceed 30 fps.
3. For more details about how to use Privacy Protection, see <https://youtu.be/D6KqYmb6q-E>.



You can configure the function according to the following steps:

[Enable Detection]

Step1: Go to **Settings > Event > AI Application Options**, enable **Privacy Protection**, then back to **Privacy Protection** interface.

Step2: Draw a detection region on the live view.

Step3: Check the checkbox to enable the function.

Step4: Enter a privacy key.

Step5: Select a detection object (human or face).

Step6: Select a video stream.

Table 71. Parameter Description

Parameter	Function Introduction
Enable Detection	Check the check-box to enable this function.

Privacy Key	Enter a privacy key.  Note: The key is used for encrypting and decrypting mosaics. After it is set, the mosaic on video files can be removed using this key in Smart Tools.
Detection Object	Human and Face are supported.  Note: In the AI Application Options, VCA must be enabled before you can select Human, and Face Detection must be enabled before you can select Face. Face is not supported in Corridor Mode.
Video Stream	Primary Stream and Secondary Stream are supported.

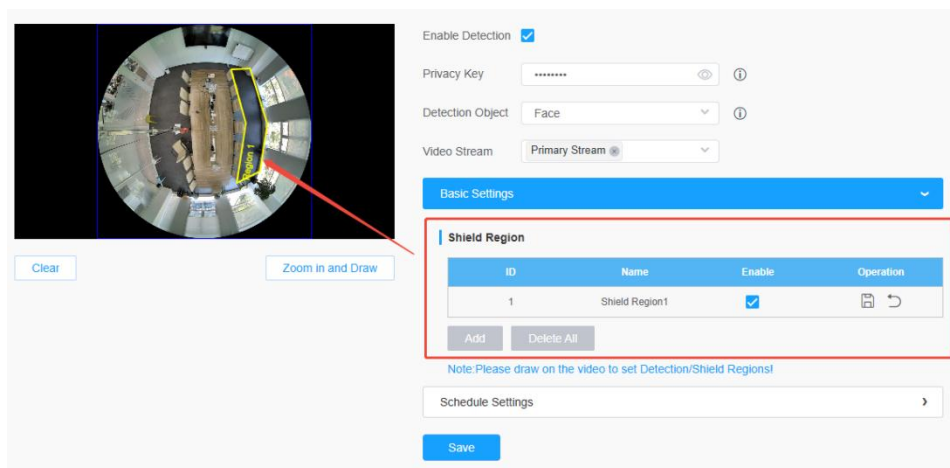
[Basic Settings]**Step6:** Add a shield region.

Table 72.

Parameter	Function Description
Shield Region	Shield Region lets you define detection areas in the surveillance feed, preventing those regions from being recorded or displayed to protect sensitive information. Click Add to add a shield region. Up to 4 regions are supported.
	Click it to delete all regions you drawn.

[Schedule Settings]**Step7:** Set a detection schedule. **Note:** For more details, see [8.4.1.1 Motion Detection](#)

Enable Detection ☒

Basic Settings

Schedule Settings

0 2 4 6 8 10 12 14 16 18 20 22 24

Sun.

Mon.

Tue.

Wed.

Thu.

Fri.

Sat.

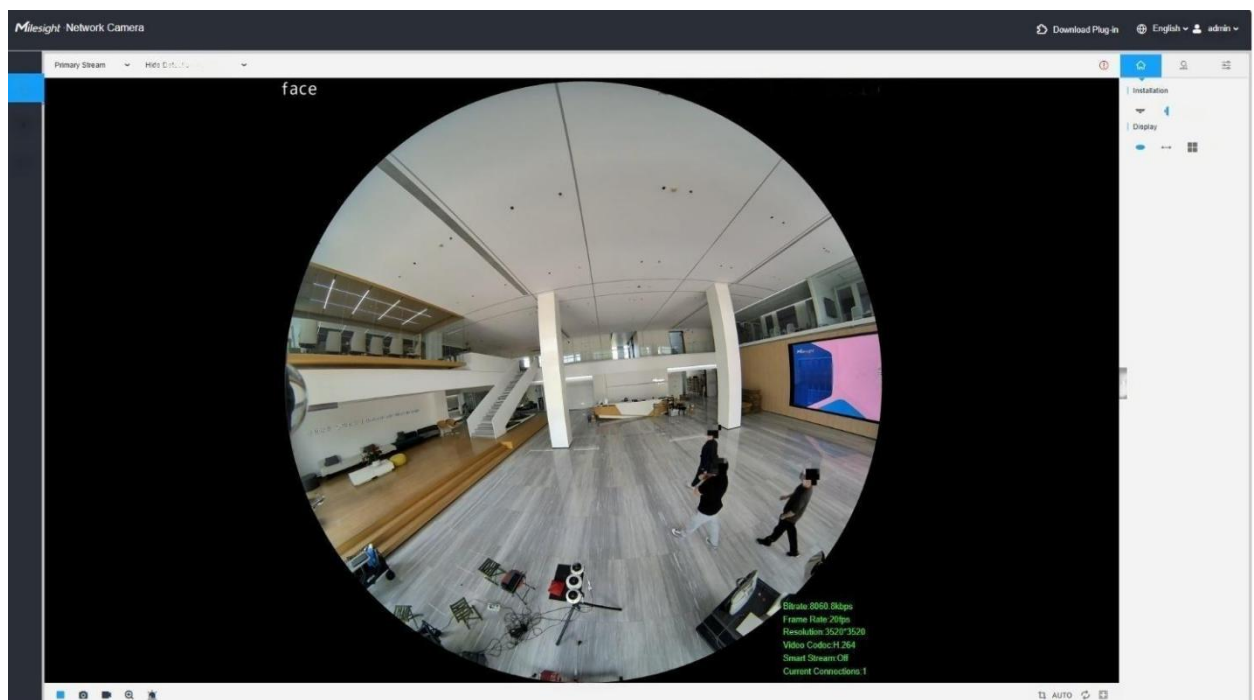
Select All Clear All

Alarm Action

Save

Step8: Click **Save** to save your configurations.

Step9: Return to the Live View interface and select **Privacy Protection** from the top menu to display the detection region on the screen. Any human or face detected within the zones will be automatically masked according to your settings, and an icon will appear in the upper-right corner.



8.5.8 One-Click Disarm

Easily control alarm linkage actions with a single click. Enabling this triggers an alarm

and generates logs while disabling the specified alarm linkage actions.

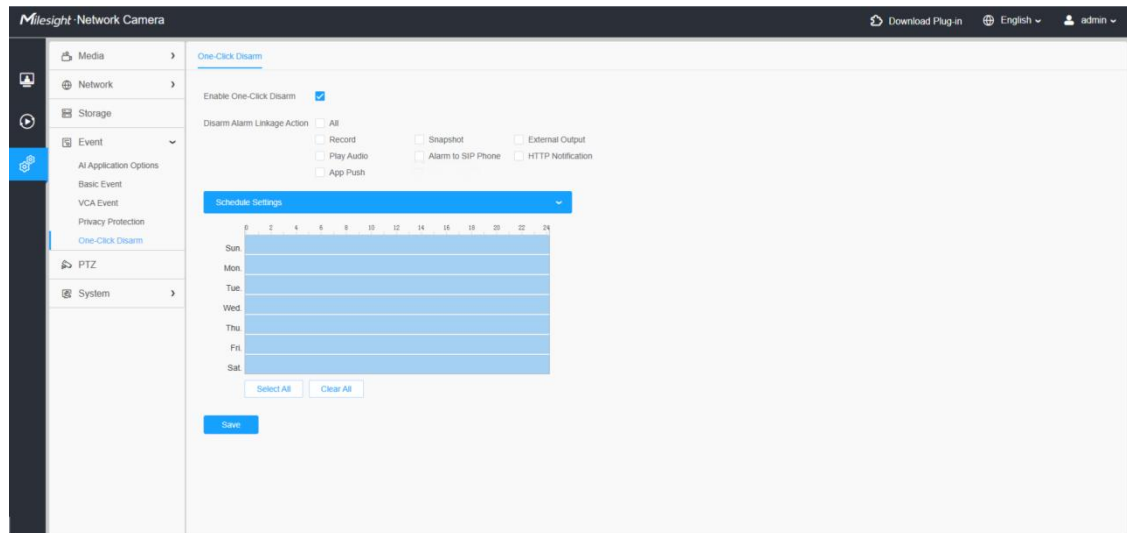
- Enable One-Click Disarm: Specified alarm linkage actions will be disabled temporary , original Alarm Action configurations will not be deleted.
- Disarm Alarm Linkage Action: To temporarily disable configured alarm actions, simply check the checkbox and set a disarm schedule.

Table 68. Description of the buttons

Parameters	Function Introduction
Record	Do not record when the event is triggered.
Snapshot	Do not take a snapshot when the event is triggered.
External Output	Do not trigger the external output when the event is triggered.
Play Audio	Do not play the audio file when the event is triggered.
Alarm to SIP Phone	Do not call the SIP phone after enabling the SIP function.
HTTP Notification	Do not send alarm notifications to the specified HTTP URL.
App Push	Do not push the alarm message to the app.

- Disarm by Schedule: Alarm linkage actions are disabled during the specified time periods.

For the schedule settings, please refer to [8.4.1.1 Motion Detection](#)



8.6 System

Here you can configure System Setting, Security, Logs and Maintenance.

8.6.1 System Setting

Here you can check System information and Date&Time.

8.6.1.1 System Info

This section describes all information about the hardware and software of the camera.

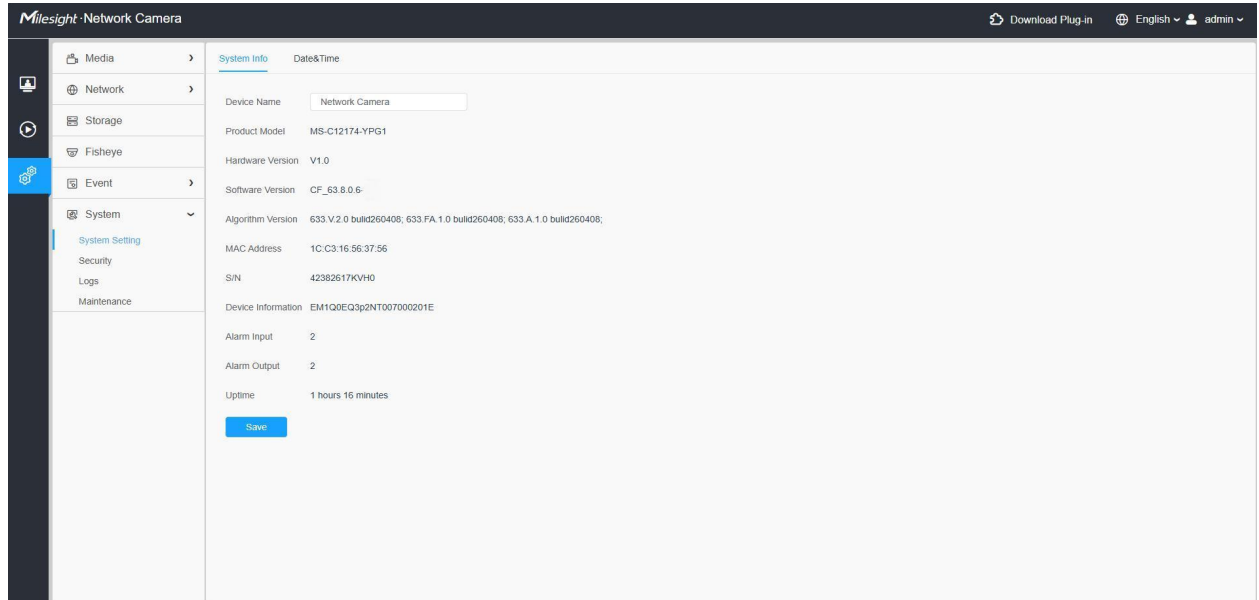


Table 69. Description of the buttons

Parameters	Function Introduction
Device Name	A customizable name, which will be shown in file names of video files.
Product Model	The product model of the camera.
Hardware Version	The hardware version of the camera.
Software Version	The software version of the camera, which can be upgraded.
Algorithm Version	Display Current Algorithm Version.
MAC Address	Media Access Control address.
S/N	Stock Number.
Device Information	The device information, including information about alarm I/O and clipper chip.
Alarm Input	The number of Alarm Input interface.  Note: The Alarm Input will appear only when the camera have alarm input/ output interface.
Alarm Output	The number of Alarm Output interface.  Note: The Alarm Output will appear only when the camera have alarm input/ output interface.
Uptime	The elapsed time since the last restarted of the device.
	Save the configurations.

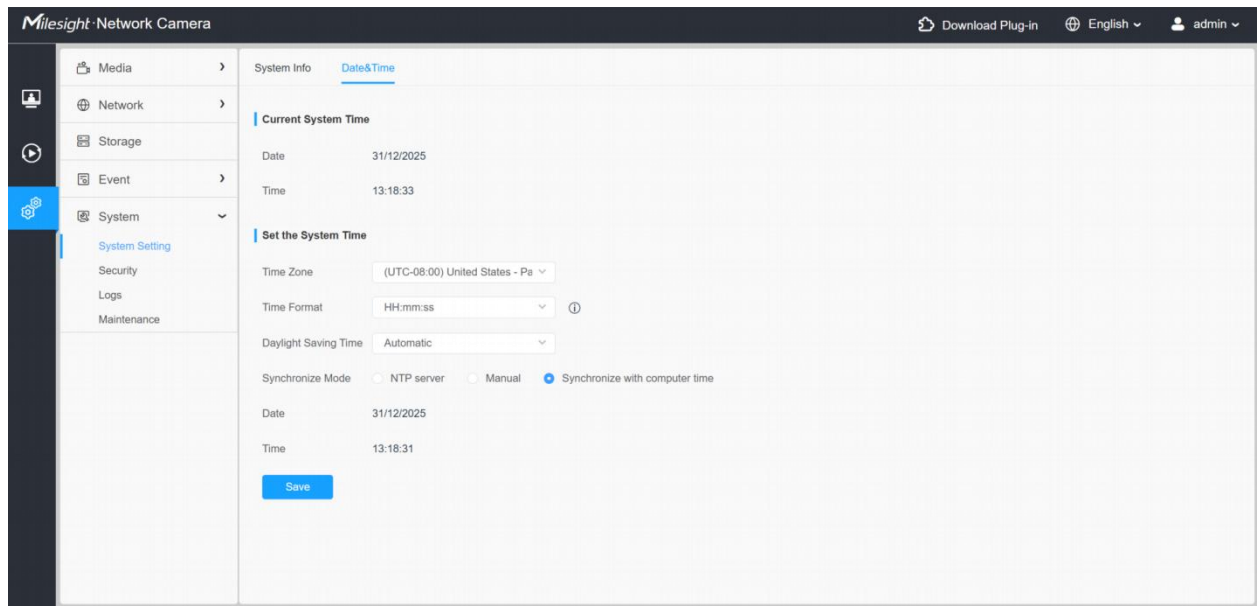


Table 70. Parameter Description

Parameters	Function Introduction
Current System Time	Current Date&Time of the system.
Set the System Time	Time Zone: Choose a time zone for your location.
	Daylight Saving time: Select Disabled, Manual, or Automatic as a daylight saving time mode.
	Time Format: Choose a time format. HH:mm:ss displays time in 24-hour format (e.g., 14:30:25), while hh:mm:ss tt uses 12-hour format with AM/PM indicators (e.g., 02:30:25 PM).
	Synchronize Mode: Select a time synchronization mode from NTP server, Manual, and Synchronize with computer time. NTP server: Input the address of NTP server. Server Address: Input the server address. NTP Sync: Regularly update your time according to the interval time. Interval: Input an interval from 1 to 43,200 (min). Manual: Set the system time manually. Synchronize with computer time: Synchronize the time with your computer.
Save	Save the configurations.

8.6.2 Security

Here you can configure User, Access List, Security Service, Watermark, etc.

8.6.2.1 User

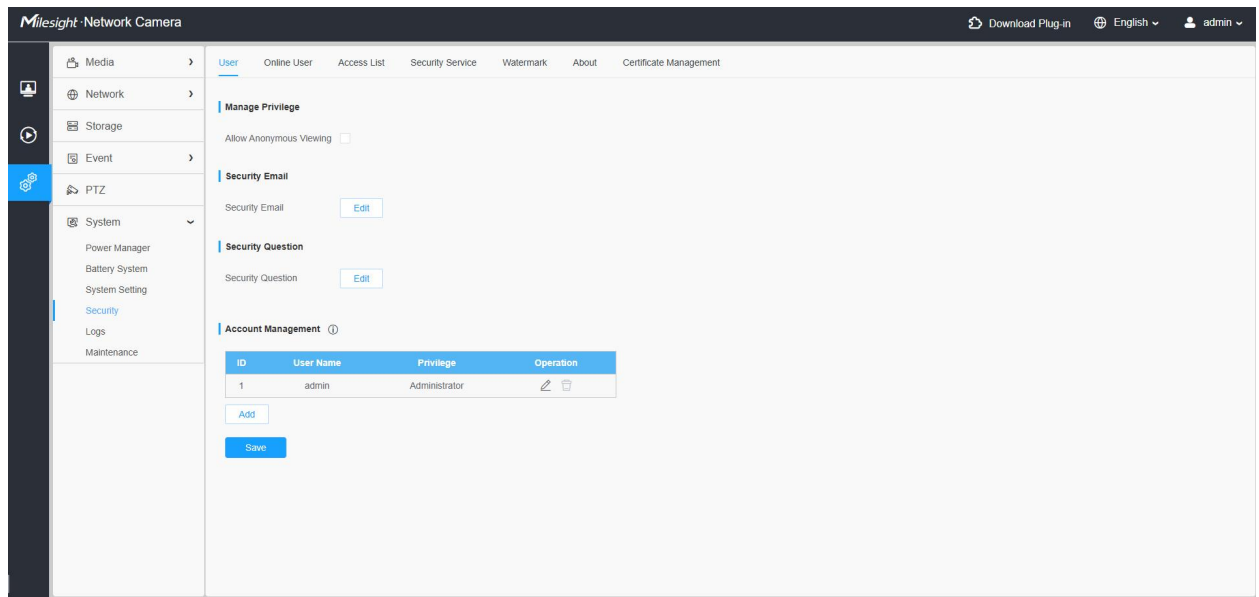
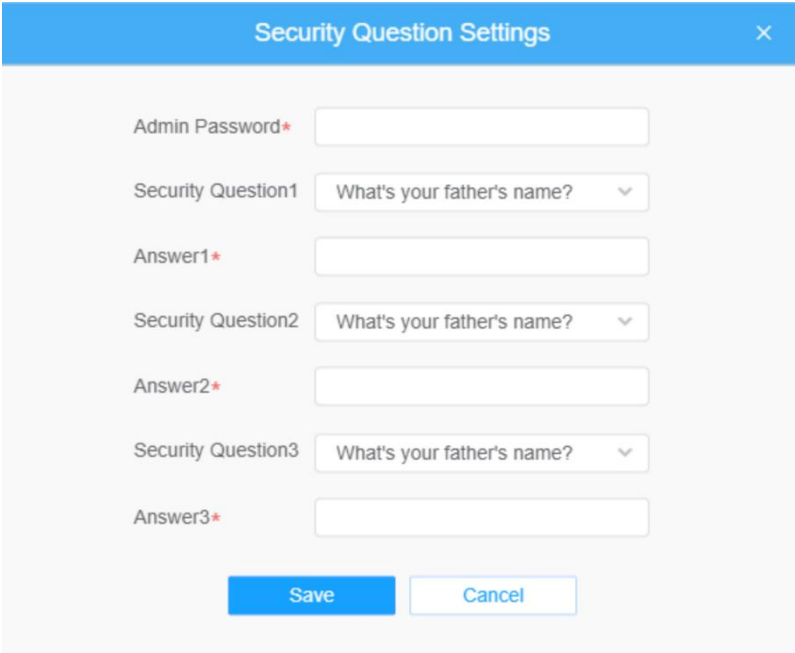
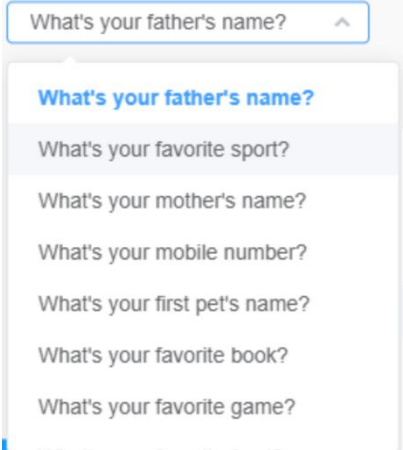


Table 71. Description of the buttons

Parameters	Function Introduction
Manage Privilege	Allow Anonymous Viewing: Check the check box to enable visit from whom doesn't have an account of the device.  Note: This method may cause video leakage.
Security Email	It allows you to reset your password through the email you set, enhancing both user experience and account security. Click Edit to set your security email. Enter the admin password and security email address and click Save. Once done, the configuration is complete.

Security Question	Click the Edit button to set three security questions for your camera. In case that you forget the password, you can click “Forget Password” button on login page to reset the password by answering three security questions correctly.  There are twelve default questions below, you can also customize the security questions. 
Account Management	Click the Add button, it will display Account Management page. You can add an account to the camera by entering Admin Password, User Level, User Name, New Password, Confirm, and edit user privilege by clicking . The added account will be displayed in the account list. Admin Password: You can add an account only after you enter the correct admin password. User Level: Set the privilege for the account. User Name: Input user name for creating an account. New Password: Input password for the account.

Confirm: Confirm the password.

8.6.2.2 Online User

Here real-time status of user logging in camera will be shown.

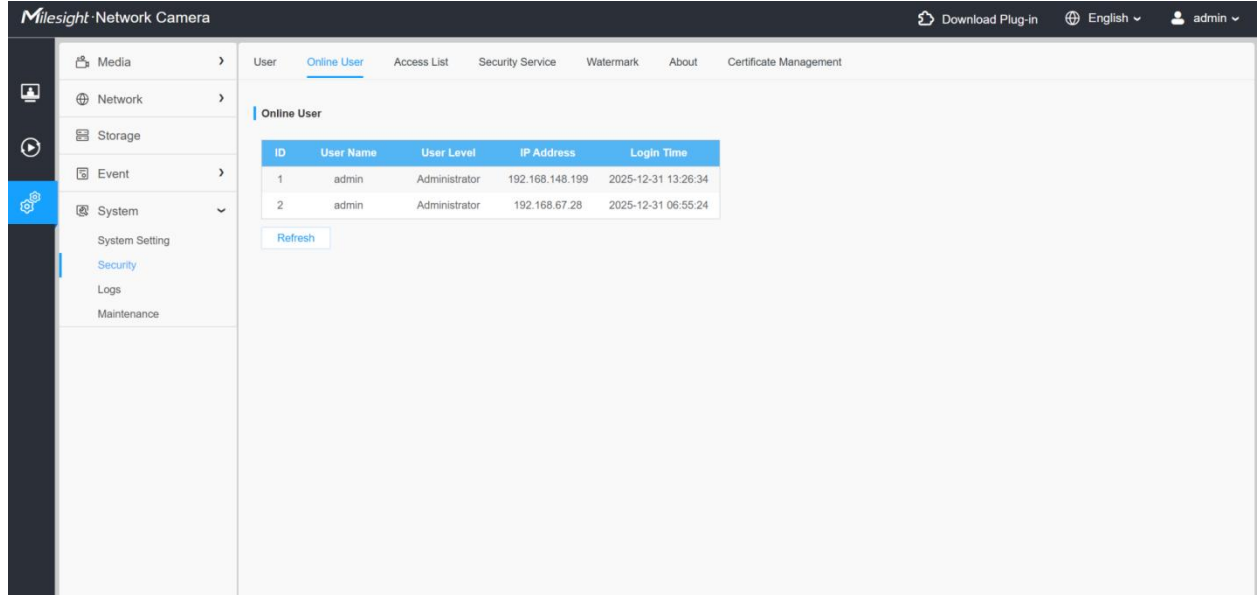


Table 72. Description of the buttons

Parameters	Function Introduction
Refresh	Click it to get the latest status of user accessing to camera.
ID	Record serial number of user logging in camera.  Note: • There are at most 30 records shown at the list. • There is only one record if the same user logging on camera by the same IP address.
User Name	Name of user logging in camera.
User Level	Level of user logging in camera.
IP Address	Device IP address where user logging in camera web located.
Login Time	Camera system time of user logging in camera.

8.6.2.3 Access List

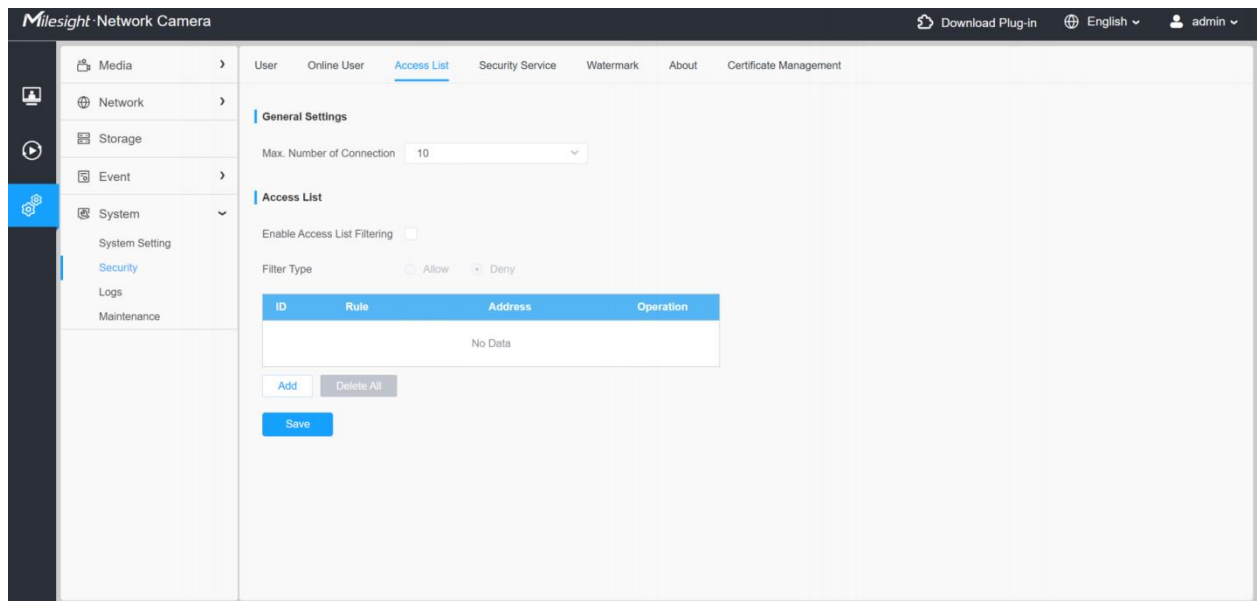
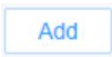
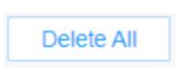


Table 73. Description of the buttons

Parameters	Function Introduction	
General Settings	Max. Number of Connection: Select the maximum number of concurrent streaming (including the number of channels displayed for currently logged-in users, RTSP connections, and ONVIF connections. Options include No Limit, 1~20.	
Access List	Enable Access List Filtering: Able to access or restrict access for some IP address.	
Access List	Filter type: Allow or deny access.	
Access List		Rule: IP Address, Network Address, IP Range, MAC Address are available. IP address: A unique numerical label assigned to a single device on a network. Input the address to get the access to the device. Network Address: A subnet address that represents a group of devices on the same network. Address: The base IP address of the subnet you want to control. Mask: A 32-bit number that defines which part of the IP address represents the network and which part represents the host. IP Range: A continuous sequence of IP addresses. Mac Address: A unique physical hardware address embedded in your camera's network interface.
Access List		Delete all the access list.

Access List		Edit the selected IP on access list.
		Delete the selected IP on access list.
	Save the configurations.	

8.6.2.4 Security Service

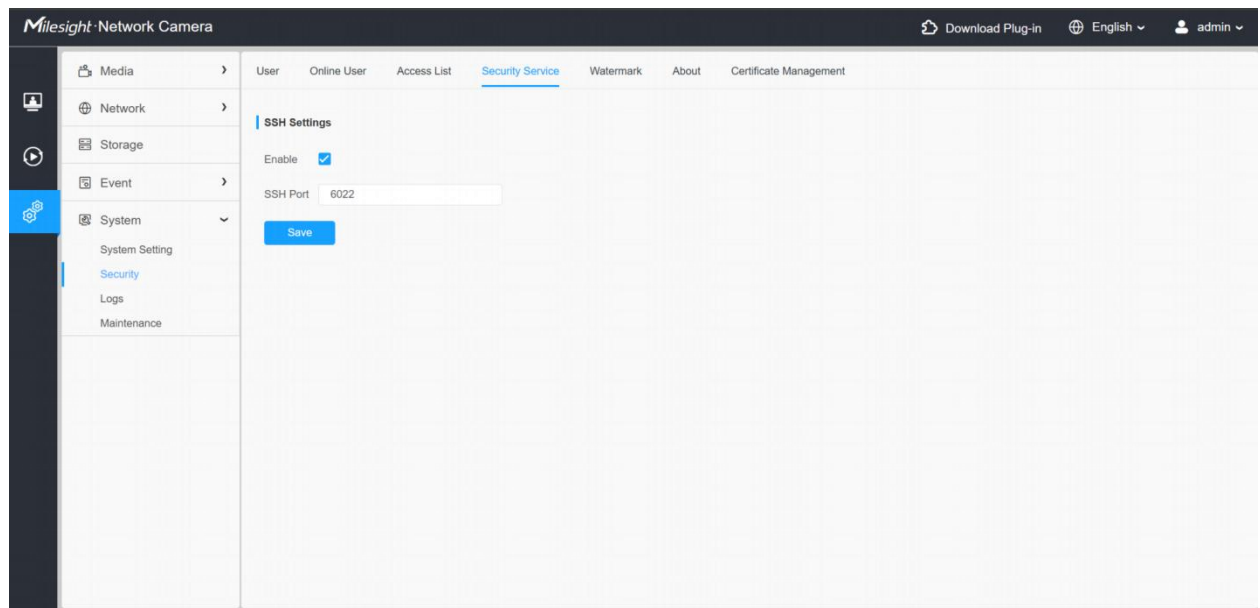
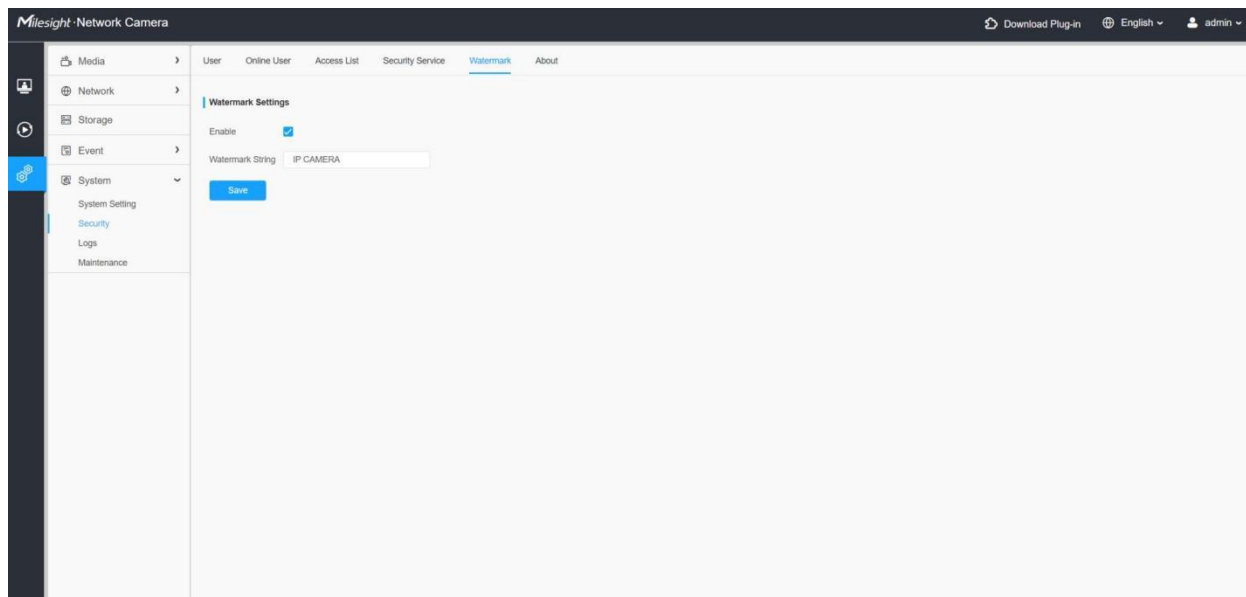


Table 74. Description of the buttons

Parameters	Function Introduction
SSH Settings	Secure Shell (SSH) has many functions: it can replace Telnet and also provides a secure channel for FTP, POP, even for PPP. Check the check box to enable the function and enter an SSH port. Enable ☒ SSH Port 6022  Note: Enabling this feature poses security risks!
	Save the configurations.

8.6.2.5 Watermark



Watermarking is an effective method to protect information security, realizing anti-counterfeiting traceability and copyright protection. Milesight Network cameras supports Watermark function to ensure information security.

8.6.2.6 About

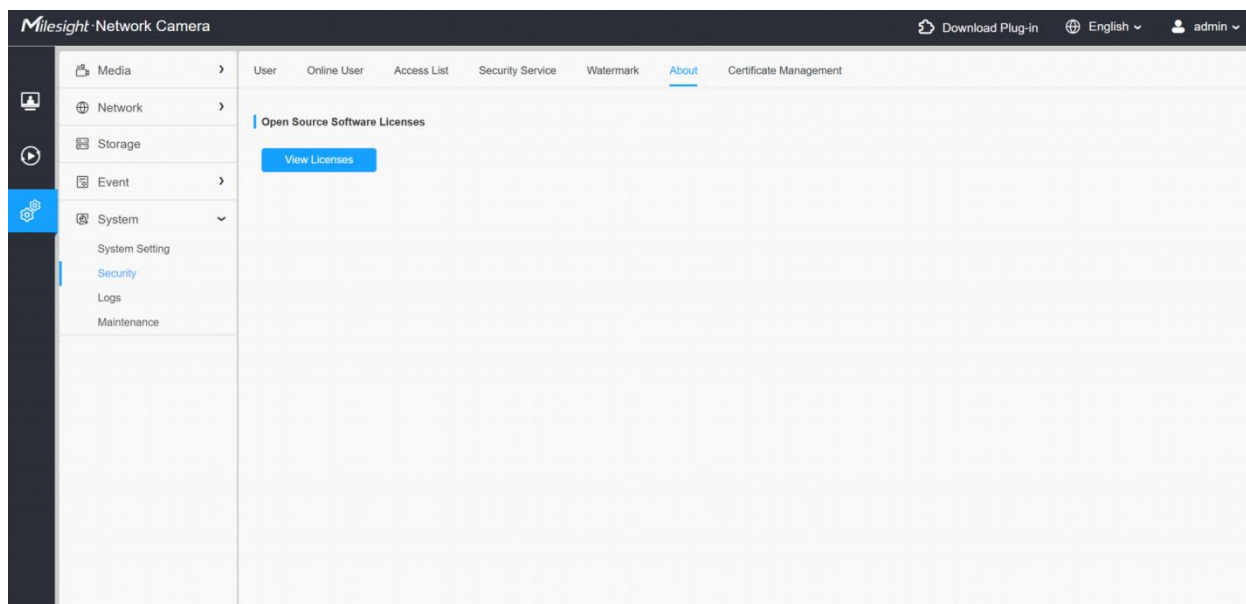


Table 75. Parameter Description

Parameters	Function Introduction
Open Source Software Licenses	Click View Licenses to view open source software licenses about the camera.

8.6.2.7 Certificate Management

This section describes the information about certificate management.

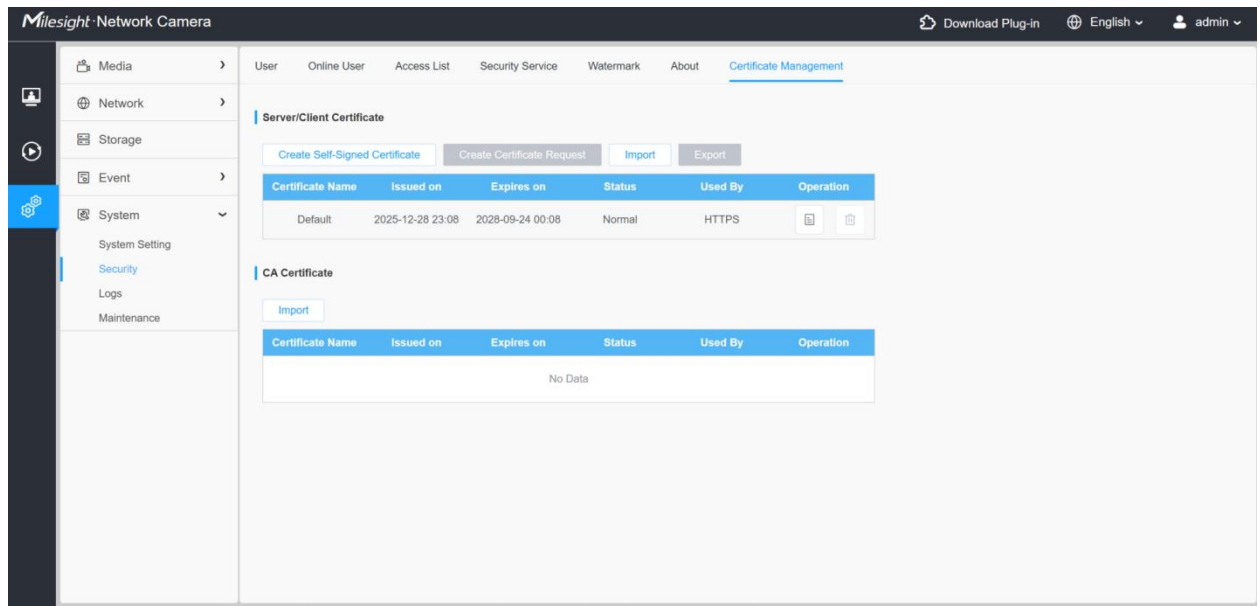
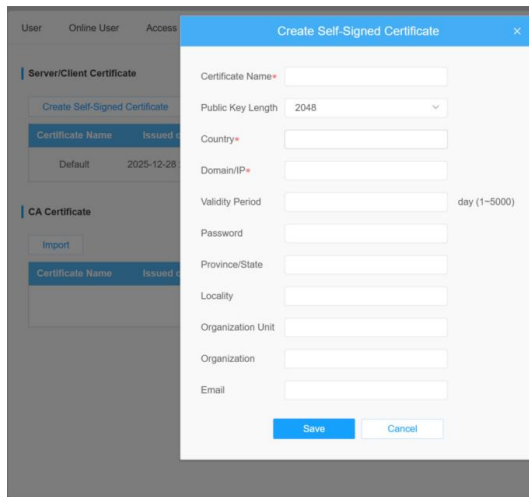
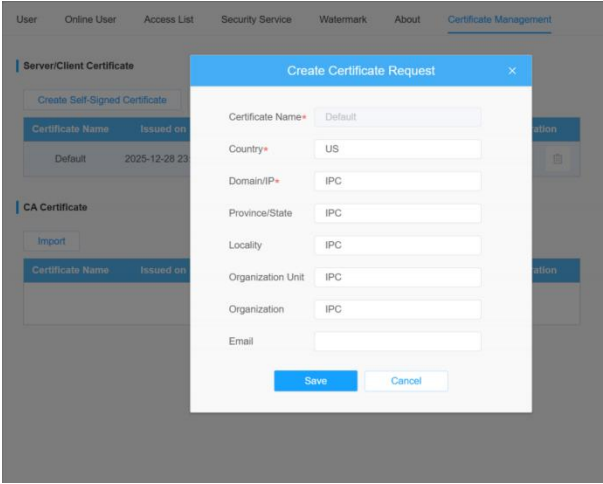
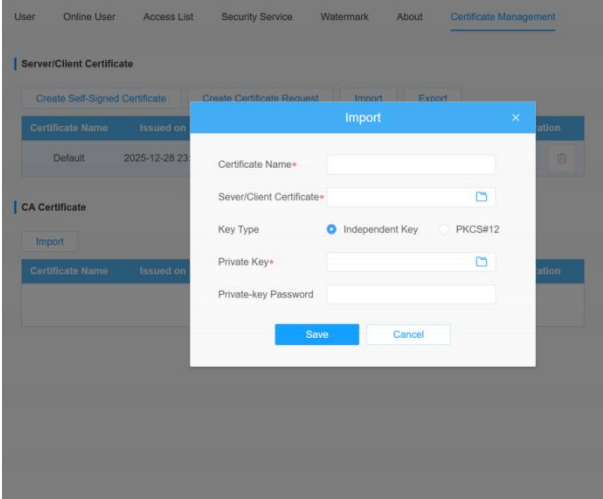


Table 76. Parameter Description

Parameters	Function Introduction
Server/Client Certificate	Create Self-Signed Certificate: Click it to create a self- signed certificate. When you click it, the following buttons are displayed. Certificate Name: Enter a certificate name. Public Key Length: Select 1024 or 2048 for the public key length. Country: Enter a country. Domain/IP: Enter a domain or an IP. Validity Period: Enter a validity period (day) from 1 to 5,000. Password: Enter a password. Province/State: Enter a province or state. Locality: Enter a locality. Organization Unit: Enter an organization unit. Organization: Enter an organization. Email: Enter an email address.



Server/Client Certificate	Create Certificate Request: Click it to create a certificate request. When creating a certificate request, you are advised to enter the following buttons: Certificate Name, Country, Domain/IP, Province/State, Locality, Organization Unit, Organization, and Email. 
Server/Client Certificate	Import: Import a certificate. Certificate Name: Enter a certificate name. Sever/Client Certificate: Import a sever or client certificate. Key Type: Select Independent Key or PKCS#12. Private Key: Import a private key. Private-key Password: Enter a private-key password.  Export: Click it to export the certificate.

Server/Client Certificate

User	Online User	Access List	Security Service	Watermark	About	Certificate Management
Server/Client Certificate						
Create Self-Signed Certificate Create Certificate Request Import Export						
Certificate Name	Issued on	Expires on	Status	Used By	Operation	
Default	2025-12-28 23:08	2028-09-24 00:08	Normal	HTTPS	 	

Certificate Name: Certificate name.

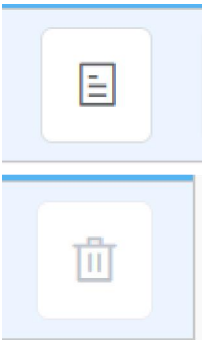
Issued On: The Issue time of the certificate.

Expires On: The validate period of the certificate.

Status: The status of the certificate.

Used By: The application method of the certificate.

Operation: The following icons are displayed under the column of Operation.



Click the first icon to see the detailed information of the certificate; click the latter to delete the certificate.

CA Certificate

You can import CA certificates by clicking Import and configuring Certificate Name and CA Certificate. There also have Certificate Name, Issued On, Expires On, Status, Used By, and Operation options.

User

Online User

Access List

Security Service

Watermark

About

Certificate Management

Server/Client Certificate

Create Self-Signed Certificate

Create Certificate Request

Import

Export

Certificate Name	Issued on	Expires on	Status	Used By	Operation
Default	2025-12-30 22:19	2028-09-25 23:19	Normal	HTTPS	

CA Certificate

Import

Certificate Name	Issued on	Expires on	Status	Used By	Operation
No Data					

User	Online User	Access List	Security Service	Watermark	About	Certificate Management		
Server/Client Certificate								
Create Self-Signed Certificate Create Certificate Request Import Export								
Certificate Name	Issued on	Expires on	Status	Used By	Operation			
Default	2025-12-30 22:19	2028-09-25 23:19	Normal	HTTPS	 			
CA Certificate								
Import								
Certificate Name=								
CA Certificate=								
Save Cancel								

8.6.3 Logs

The section describes the information about Logs, Security Audit Logs, and Remote Logs.

8.6.3.1 Logs

Time	Main Type	Sub Type	Param	User	IP	Detail
2025-05-06 18:07:07	Smart	Intrusion Detection	-	-	-	region:1
2025-05-06 18:06:36	Smart	Intrusion Detection	-	-	-	region:1
2025-05-06 18:06:23	Smart	Intrusion Detection	-	-	-	region:1
2025-05-06 18:05:17	Smart	Intrusion Detection	-	-	-	region:1
2025-05-06 18:05:15	Smart	Intrusion Detection	-	-	-	region:1
2025-05-06 18:04:58	Smart	Intrusion Detection	-	-	-	region:1
2025-05-06 18:04:56	Smart	Intrusion Detection	-	-	-	region:1
2025-05-06 18:04:40	Smart	Intrusion Detection	-	-	-	region:1
2025-05-06 18:04:19	Smart	Intrusion Detection	-	-	-	region:1
2025-05-06 18:04:17	Smart	Intrusion Detection	-	-	-	region:1
2025-05-06 18:03:57	Smart	Intrusion Detection	-	-	-	region:1
2025-05-06 18:03:55	Smart	Intrusion Detection	-	-	-	region:1
2025-05-06 18:03:36	Smart	Intrusion Detection	-	-	-	region:1
2025-05-06 18:03:34	Smart	Intrusion Detection	-	-	-	region:1
2025-05-06 18:02:18	Smart	Intrusion Detection	-	-	-	region:1
2025-05-06 18:02:16	Smart	Intrusion Detection	-	-	-	region:1
2025-05-06 18:02:13	Smart	Intrusion Detection	-	-	-	region:1
2025-05-06 17:59:23	Smart	Intrusion Detection	-	-	-	region:1

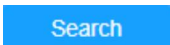


Note:

This interface is used to record logs (including All Types, Event, Operation, Information, Exception, and Smart). Before configuring it, ensure a storage device is available.

Logs can only be stored on the SD card or NAS.

Table 77. Description of the buttons

Parameters	Function Introduction
Main Type	Five main types are supported: All Types, Event, Operation, Information, Exception, and Smart.
Sub Type	Configure Main Type first, and then select the sub type to narrow the range of logs.
Start Time	The start time of logs.
End Time	The end time of logs.
	Search the logs.

Export	Export the logs.
Go to	Enter the log page number to navigate to the target page.

8.6.3.2 Security Audit Logs

Time	Main Type	Sub Type	Param	User	IP	Detail
2025-07-16 11:21:54	Operation	Login Remotely	-	admin	192.168.70.175	-
2025-07-16 10:43:11	Operation	RTSP Session Stop	-	admin	192.168.70.175	HTTP
2025-07-16 10:41:18	Operation	RTSP Session Start	-	admin	192.168.70.175	HTTP
2025-07-16 10:41:15	Operation	RTSP Session Stop	-	admin	192.168.70.175	HTTP
2025-07-16 10:34:20	Operation	RTSP Session Start	-	admin	192.168.70.175	HTTP
2025-07-16 10:34:18	Operation	Login Remotely	-	admin	192.168.70.175	-
2025-07-16 10:01:53	Operation	RTSP Session Stop	-	admin	192.168.70.175	HTTP
2025-07-16 09:52:19	Operation	RTSP Session Start	-	admin	192.168.70.175	HTTP
2025-07-16 09:52:16	Operation	Login Remotely	-	admin	192.168.70.175	-

The Security Audit Logs interface records critical operations and exception information related to the camera. The Main Type options include: All Types, Operation, Information, and Exception. Compared to the standard Logs interface, the information category here excludes Basic Event, VCA, and Advanced Events.

- These logs contain vital data for device security and exception tracking.
- The logs must be persistently stored and must not be lost even after the camera reboots.

Table 78. Description of the buttons

Parameters	Function Introduction
Main Type	Five main types are supported: All Types, Event, Operation, Information, Exception, and Smart.
Sub Type	Configure Main Type first, and then select the sub type to narrow the range of logs.
Start Time	The start time of logs.
End Time	The end time of logs.

Search	Search logs.
Export	Export logs.
Go to	Enter the log page number to navigate to the target page.

8.6.3.3 Remote Logs

This section is about how to forward logs to a third-party server for centralized management.

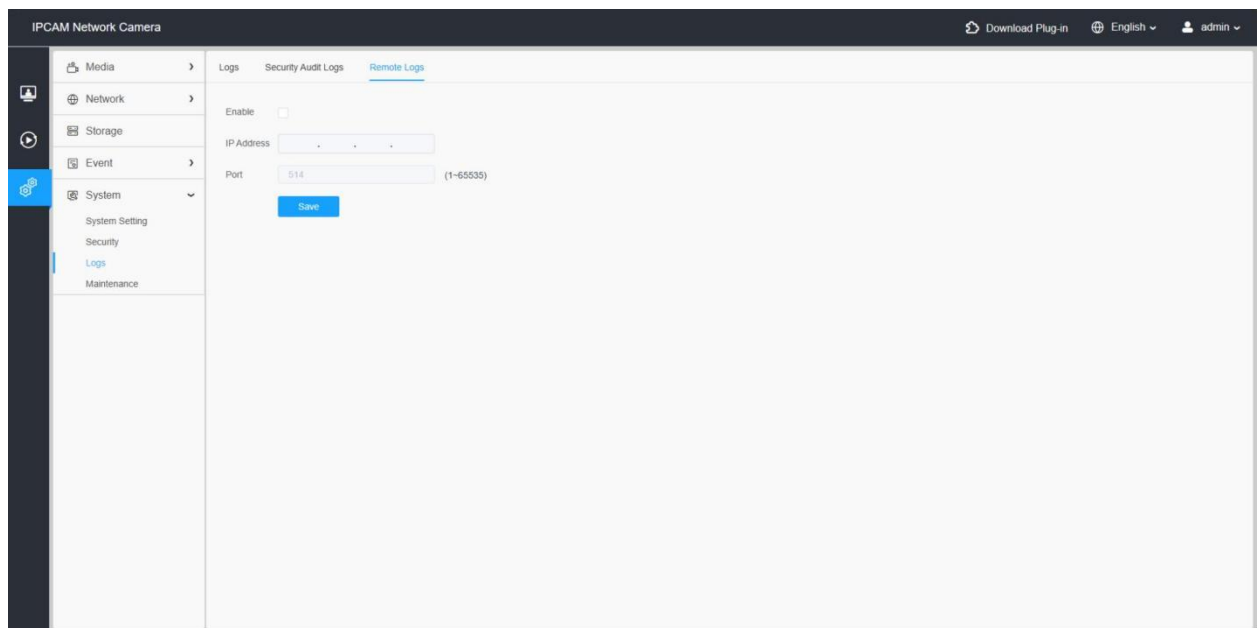


Table 79. Parameter Description

Parameter	Function Introduction
Enable	Turn on this option to activate log forwarding.
IP Address	Enter the destination IP address of the server that can receive the logs.
Port	Specify a port number used by the receiving server to accept log data.

8.6.4 Maintenance

This section describes how to configure System Maintenance and Auto Reboot.

8.6.4.1 System Maintenance

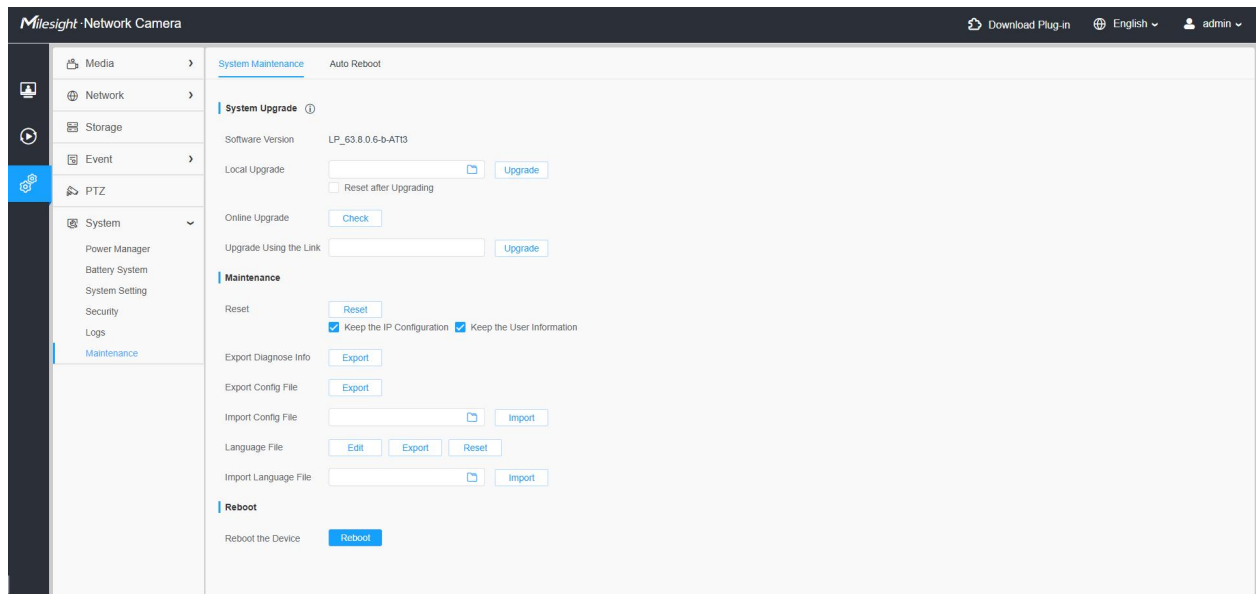
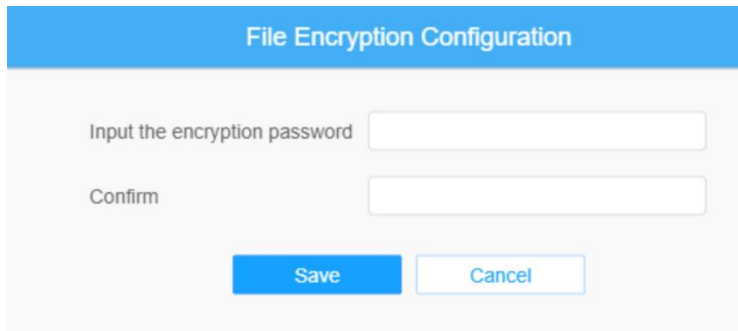
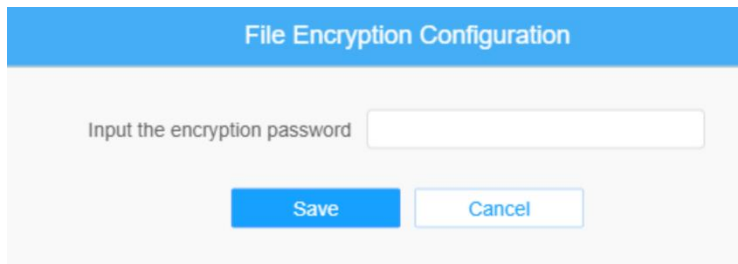


Table 80. Description of the buttons

Parameters	Function Introduction
System Upgrade	Software Version: The software version of the camera. Local Upgrade: Click  to select a upgrade file, click the "Upgrade" button to upgrade the version. After the system reboots successfully, the update is done. You can check Reset after Upgrading to reset the camera after upgrading it. Online Upgrade: Click Check to verify if the current firmware version is the latest one and then click OK to upgrade to this version. The current version is the latest version will be displayed, if your camera is already the latest version. Tips ×  The current version is the latest version. OK
System Upgrade	Upgrade Using the Link: When you have uploaded the upgrading file to the cloud, like Google Driver, etc., you can input the link address and then click Upgrade to upgrade.  Note: Do not disconnect the power of the device during the update.

	The device will be restarted to complete the upgrading.
Maintenance	Reset: Click Reset to reset the camera. Keep the IP Configuration: Check this option to keep the IP configuration when resetting the camera. Keep the User information: Check this option to keep the user information when resetting the camera. Export Diagnose Info: Click Export to export logs and system information of the device operation status.  Note: Must be in the format of ".txt". Export Config File: Click Export and a window will pop up as shown below:  The dialog box titled "File Encryption Configuration" contains two input fields: "Input the encryption password" and "Confirm". Below the fields are two buttons: "Save" (blue) and "Cancel" (white with blue border). Enter and confirm your password again, and then click Save to export configuration file.
Maintenance	Import Config File: A window will be popped up after clicking the  icon. Click OK to update the configurations. The File Encryption Configuration will be displayed after the above steps. Enter a password and click Save to import the configuration file.  The dialog box titled "File Encryption Configuration" contains one input field: "Input the encryption password". Below the field are two buttons: "Save" (blue) and "Cancel" (white with blue border).  Note: Export and import the same configuration file. Password must be the same. Language File: You can edit, export, and reset the language file here. Import Language File: Click the Import button to import the language file, and then click OK to import the language file.  Note: You can customize the interface language by modifying or importing the predefined language translation packs.
Reboot	Click Reboot to restart the device immediately.

8.6.4.2 Auto Reboot

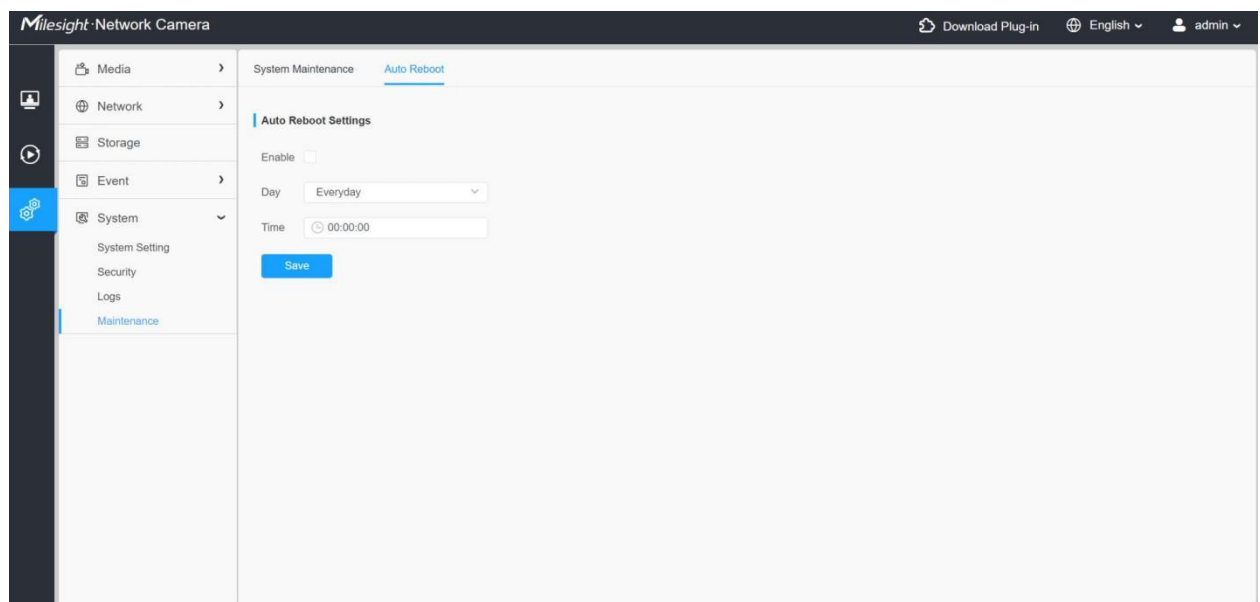


Table 81. Parameter Description

Parameter	Function Introduction
Enable	Check the checkbox to enable this function. You can configure Day and Time for the camera. Once done, the camera will reboot automatically.

Chapter 9. Services

Milesight provides customers with timely and comprehensive technical support services. End-users can contact your local dealer to obtain technical support. Distributors and resellers can contact directly with Milesight for technical support.

Technical Support Mailbox: support@milesight.com

Web: <http://www.milesight.com>

Online Problem Submission System: <http://www.milesight.com/service/feedback.asp>

MILESIGHT CHINA

TEL: +86-592-5922772

Add: Building C09, Software Park Phase III, Xiamen 361024, Fujian, China